Metropolia

TEKNIIKKA

Tietotekniikka

Tietoverkot

INSINÖÖRITYÖ

IPv6-KÄYTTÖÖNOTTOSUUNNITELMA

Työn tekijä: Ilana Kiuru

Työ hyväksytty: 22.5. 2014

Marko Uusitalo
lehtori

TIIVISTELMÄ

Työn tekijä: Ilana Kiuru

Työn nimi: IPv6-käyttöönottosuunnitelma

Päivämäärä: 22.5.2014 **Sivumäärä:** 35 s. + 1 liite

Koulutusohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkot

Työn ohjaaja: lehtori Marko Uusitalo

Tämä insinöörityö on tehty Capgemini Finland Oy:lle, sillä yritys haluaa tarjota asiakkailleen IPv6-pohjaisia palveluita. Insinöörityön tavoitteena on laatia yrityksen käyttöön suunnitelma IPv6-teknologian käyttöönottamiseksi.

Käytössä oleva IPv4-teknologia alkaa olla riittämätön vastaamaan nykyisien verkkojen tarpeisiin. Tästä syystä on kehitetty uusia teknologioita, joilla pystyttäisiin paremmin toteuttamaan nykyisiä verkkoja. IPv6 kehitettiin vuonna 1998, ja se sisältää suuria parannuksia IPv4-teknologiaan verrattuna. IPv6:n käyttöönotto on aloitettu vuonna 2006.

Suurimpana ongelmana voidaan pitää IPv4-osoitteiden loppumista, joka on ollut nähtävissä jo 1980-luvun lopulla Internetin yleistyessä. IPv4-osoitteet muodostuvat 32 bitistä, joten osoitteita on olemassa 2^{32} kappaletta. IPv6-osoitteet puolestaan muodostuvat 128 bitistä ja osoitteita on olemassa 2^{128} kappaletta. Myös osoitteiden esitystapa on erilainen: IPv4-osoitteet esitetään neljällä desimaaliarvolla, jotka on erotettu toisistaan pisteillä, kun taas IPv6-osoitteet esitetään kahdeksalla heksadesimaaliluvulla, jotka erotetaan toisistaan kaksoispisteiden avulla. IPv4:ssä käytössä ollut vaihteleva verkkoprefiksi ei ole käytössä IPv6:ssa, vaan verkot on jaettu valmiiksi tietyn kokoisiin osiin.

Käyttöönottosuunnitelman yhtenä osana oli tilata yrityksen käyttöön operaattoririippumattomia IPv6-osoitteita. Osoitteita tilataan RIPE NCC:ltä täyttämällä tähän tarkoitukseen käytössä oleva pyyntölomake.

Osana työtä oli selvittää yrityksen verkkolaitteiden ja niiden ohjelmistojen IPv6-yhteensopivuus ja tuki. Selvitykseen käytettiin pääsääntöisesti laitevalmistajien verkkosivuja sekä kyseltiin tietoja laitevalmistajilta sähköpostitse.

Työn lopputuloksena saatiin yritykselle IPv6-käyttöönottosuunnitelma, jonka toteutuksesta vastaa yrityksen verkkoasiantuntijat.

Avainsanat: IPv6, IPv6-käyttöönottosuunnitelma

Metropolia

ABSTRACT

Name: Ilana Kiuru

Title: IPv6 implementation plan

Date: 22.5.2014 **Number of pages:** 35 pages + 1 attachment

Department: Information Technology **Study Programme:** Data Networks

Instructor: Marko Uusitalo

This final project has been done for Capgemini Finland Oy because the company wishes to offer its customers services based on IPv6 technology. The objective is to create an implementation plan for IPv6 for the company to use.

Currently used IPv4 technology is starting to be insufficient to fill the needs of current networks. New technologies have been developed to execute current networks better. IPv6 was developed in 1998 and it includes huge improvements compared to IPv4 technology Implementation of IPv6 has been started in 2006.

Exhaustion of IPv4 addresses can be considered as the biggest problem. This has been forecasted since late 1980 when internet started to become widespread. IPv4 addresses consist of 32 bits and there are 2^{32} unique addresses. IPv6 addresses on the other hand consist of 128 bits and there are total of 2^{128} addresses. The representation of IPv4 addresses is four decimals that are separated with dots. IPv6 address representation is eight hexadecimal numbers that are separated with colons. The variable length network prefix that is used in IPv4 is not used in IPv6. IPv6 network subnet sizes are predefined.

Part of the implementation plan was to order Provider Independent IPv6 addresses for the company. The addresses are requested from RIPE NCC by filllin in a request form that is used for this purpose.

One part of the work was to define the IPv6 compatibility and support of the company's network devices and their software. The research was mainly done by reading through the device manufacturers' internet pages and by asking for support details from manufacturers via email.

The result was an IPv6 Implementation plan for the company. The company's network specialists are responsible for the actual implementation.

Keywords: IPv6, IPv6 implementation plan

SISÄLLYS

1 JOHDANTO

Nykyisin käytössä olevan IPv4-teknologian puutteellisuus on luonut paineita uusiin teknologioihin siirtymiselle. Yhtenä suurimmista syistä uusien teknologioiden kehittämiselle voidaan pitää IPv4-osoitteiden riittämättömyyttä, eli allokoimattomien IPv4-osoitteiden resurssien kulumista loppuun.

Jokaiselle noodille (engl. node), kuten tietokone, palvelin tai tulostin, on IP-verkossa annettu yksilöllinen IP-osoite, jota käytetään sen tunnistamiseen ja paikallistamiseen tiedonvälityksessä muiden, samassa verkossa olevien noodien kanssa. IPv4-osoitteiston rakenne ei tarjoa tarpeellista määrää julkisesti reititettäviä osoitteita, jotta jokaisella laitteella tai palvelulla voisi olla erillinen osoite.

Allokoitavien IPv4-osoitteiden loppuminen on ollut huolenaiheena jo 1980-luvun lopusta lähtien, kun Internet alkoi kasvaa dramaattisesti. Odotettu vajaus on ollut kantava voima monien uusien teknologioiden kehittämiselle ja käyttöönottamiselle.

Yritykset hidastaa IPv4-osoitteiden loppuunkulumista aloitettiin 1990-luvun alussa ongelman havaitsemisen jälkeen. Ongelmaa on yritetty lieventää useilla muutoksilla osoiteallokoinnissa ja verkon reititysinfrastruktuurissa. Esimerkiksi NAT (Network Address Translation) on sallinut palveluntarjoajien ja yritysten esittää yksityisen verkon osoiteavaruus vain yhdellä julkisesti reititettävällä IP-osoitteella reitittimen verkkoliitännässä sen sijaan, että verkon jokaiselle laitteelle olisi allokoitu oma julkinen osoite.

Maailmanlaajuisesti IP-osoitteita hallinnoi IANA (Internet Assigned Numbers Authority) ja alueellisesti viisi paikallista Internet-rekisteriä, jotka ovat vastuussa osoitteiden jakamisesta oman alueensa paikallisille palveluntarjoajille. IPv4-osoitteita on suunnilleen 4,3 miljardia kappaletta, IANA jakaa niiden osajoukkoja Internet-rekistereille likimäärin 16,8 miljoonan (eli 2^{24}) osoitteen lohkoissa, lohkojen verkkoprefiksi /8. IANA allokoi viimeiset viisi jäljellä olevaa osoitelohkoa alueellisille Internet-rekistereille helmikuussa 2011, yhden kunkin alueen rekisterille. Nykyisin paikalliset IP-rekisterit ovat tilanteessa, jossa ne eivät enää voi jakaa viimeistä /8-osoitelohkoa, eikä asiakkaille ole tarjolla tarvittavaa määrää IPv4-osoitteita. Tästä syystä NAT-protokolla on tarpeellinen, jotta IPv4:n käyttöä voidaan vielä jatkaa.

Uusi versio Internet-protokollasta, IPv6, kehitettiin vuonna 1998. On arvioitu, että siirtyminen IPv6:een on ainoa mahdollinen pitkän tähtäimen ratkaisu IPv4-osoitteiden loppuun kulumisen ratkaisemiseksi. Internetin tekniset standardit ja verkkolaitteiden myyjät kannattavat IPv6:n käyttöön ottamista. IPv6 sisältää useita parannuksia, kuten 32-bittisen IPv4-osoiteformaatin korvaamisen 128-bittisillä osoitteilla, jolloin kapasiteetti nousee n. 3.4×10^{38} osoitteeseen. IPv6:n käyttöönottoa maailmanlaajuisesti on aktiivisesti aloitettu vuonna 2006. Capgemini Groupilla IPv6:n käyttöönotto on useassa maassa suunnitteluasteella, eikä sitä ole missään yrityksen toimipaikassa vielä otettu käyttöön tuotannossa.

1.1 Ympäristö ja lähtötilanne

Työ on tehty Capgemini Finland Oy:lle, joka on osa Capgemini Groupia, yhtä maailman johtavista konsultointi-, teknologia- ja ulkoistuspalveluja tarjoavista yrityksistä.

Capgemini toimii lähes 40 maassa ympäri maailmaa, ja sen pääkonttori sijaitsee Pariisissa. Capgemini Finlandilla on toimipisteitä Espoossa, Lappeenrannassa, Tampereella ja Turussa. Maailmanlaajuisesti yrityksellä on n. 110 000 työntekijää, joista n. 1000 henkilöä työskentelee Capgemini Finlandin palveluksessa.

Yrityksen asiakkaat ovat jo jonkin aikaa kyselleet mahdollisuutta ottaa IPv6-teknologia käyttöön omissa organisaatioissaan. Jotta yritys voisi tarjota IPv6-pohjaisia palveluita asiakkailleen, on yrityksen ensin otettava kyseinen teknologia käyttöön omassa infrastruktuurissaan.

1.2 Tavoitteet

Tämän insinöörityön tavoitteena on laatia yritykselle suunnitelma IPv6-tekniikan käyttöönottamiseksi. Vaikka yritys toimii globaalisti useassa maassa, on yrityksen verkkoratkaisut toteutettu lokaalisti joka maassa erikseen. Suunnitelma koskee yrityksen verkkoa vain Suomessa, eikä tule käyttöön muissa maissa, joissa yrityksellä on toimipisteitä.

Ensisijaisesti tavoitteena on kartoittaa yrityksessä käytössä olevien laitteistojen IPv6-yhteensopivuus ja miettiä mahdollisia ratkaisuja ja parannusehdo-

tuksia yrityksen infrastruktuurin uudistamiseksi, jotta IPv6-teknologian käyttöönotto olisi mahdollista ja sujuisi suhteellisen helposti ja vaivattomasti.

Työssä kuvataan ne työvaiheet, joita tarvitaan yrityksen laitekannan kartoittamiseksi sekä laitteiston IPv6-yhteensopivuuden selvittämiseksi.

Työn lopputuloksena on yrityksen käyttöön laadittu yksityiskohtainen suunnitelma IPv6-teknologian käyttöönotosta. Suunnitelma sisältää sen toteuttamiseksi tarvittavat investoinnit, kuvauksen tarvittavista työvaiheista sekä analyysin suunnitelman toteutuksen vaikutuksista yrityksessä. Suunnitelman toteuttaminen ei kuulu tämän insinöörityön tavoitteisiin, vaan jää yrityksen itse toteutettavaksi.

2 IPV6:N TEORIAA

Ennen käyttöönottosuunnitelman laatimista piti tutustua IPv6:een hieman tarkemmin. Tehtävänä oli perehtyä IPv6:n toimintaan sekä selvittää sen tarjoamia etuja ja mahdollisia haittoja nykyiseen käytössä olevaan IPv4-teknologiaan verrattuna.

2.1 IPv6-osoitteet

Jokaisella Internetiin kytketyllä laitteella tulee olla tunniste. IP-osoitteet ovat numeerisia osoitteita, joita käytetään laitteiden tunnistamiseen. Kaksi yleisintä IP-protokollan käytössä olevaa versiota ovat IPv4 ja IPv6, joiden osoitteet tulevat rajallisesta määrästä numeroita. IPv4-osoitteet muodostuvat 32 bitistä ja osoitteita on olemassa 4 294 967 296 (2^{32}) kappaletta. IPv6-osoitteet muodostuvat 128 bitistä ja osoitteita on olemassa 340 282 366 920 938 463 463 374 607 431 768 211 456 (2^{128}) kappaletta. Kaikkia IP-avaruuksien osoitteita ei voida jakaa laitteille, joita käytetään Internetiin pääsyssä. Jotkin IP-osoitteet on varattu muuhun käyttöön kuten yksityisiin verkkoihin. Näin ollen jaettavissa olevien IP-osoitteiden määrä on pienempi kuin osoitteiden kokonaismäärä. [2.]

2.1.1 IPv6-osoitetyypit

IPv6-osoitteita on kolmea eri tyyppiä:

- Unicast-osoitteet, joilla merkitään yksittäistä rajapintaa. Paketti, joka lähetetään unicast-osoitteeseen, toimitetaan kyseisen osoitteen iden-

tifioimalle laitteelle. Kuten IPv4:ssä, myös IPv6:ssa yhdellä noodilla voi olla useampi kuin yksi verkkorajapinta ja jokaiselle rajapinnalle on oltava määriteltynä oma unicast-osoitteensa.

- Multicast-osoitteet, joilla osoitetaan rajapintojen joukkoa. Tyypillisesti rajapinnat kuuluvat eri noodeihin. Multicast-osoitteeseen lähetetty paketti toimitetaan kaikille sen osoitteen identifioimille laitteille

- Anycast-osoite, jolla myös osoitetaan rajapintojen joukkoa ja tyypillisesti rajapinnat kuuluvat eri noodeihin. Anycast-osoitteeseen lähetetty paketti toimitetaan yhdelle sen osoitteen identifioimalle laitteelle, yleensä ”lähimmälle” laitteelle, jonka määrittely riippuu reititysprotokollan etäisyydenmittaustavasta. Mikä tahansa unicast-osoite voitaisiin määritellä anycast-osoitteeksi, kunhan kaikki noodit, jotka on konfiguroitu vastaamaan osoitteeseen, ovat tietoisia osoitteen statuksesta anycast-osoitteena unicast-osoitteen sijaan. [1, s. 138-139, 142, 145.]

IPv4:ssä käytössä olleita broadcast-osoitteita ei ole käytössä IPv6:ssa, vaan niiden funktiot on korvattu multicast- ja anycast-osoitteilla. Broadcast-osoitteen toiminnallisuus saavutetaan lähettämällä paketteja multicast-osoitteeseen. Multicast-osoitteiden rajoitetummat joukot, kuten ”kaikki reitittimet paikallisessa linkissä”, tarjoavat multicast-toiminnallisuutta tehokkaammin kuin IPv4:ssä. Noodit, jotka ovat kiinnostuneita liikenteestä, joka aikaisemmin lähetettiin broadcastina voivat hyväksyä multicast-osoitteita kun taas noodit, jotka eivät ole kiinnostuneita kyseisestä liikenteestä, voivat jättää kyseiseen osoitteeseen lähetetyt paketit huomiotta. Broadcastit eivät pystyneet ratkaisemaan tiedon (kuten reititysinformaation) monistumista Internetissä riittävästi, kun taas multicast tarjoaa skaalautuvamman ratkaisun ongelmaan. [1, s. 142-143.]

2.1.2 Osoitteiden esitystapa

IPv4-osoitteet esitetään yleensä neljällä desimaaliarvolla (0 - 255), jotka erotellaan toisistaan pisteillä. Esimerkkejä IPv4-osoitteiden merkinnästä:

- 10.0.0.1

- 192.168.1.150. [1, s. 144.]

IPv6-osoitteet ovat neljä kertaa pidempiä kuin IPv4-osoitteet, joten ne ovat myös vaikeammin käsiteltäviä. Yleisin tapa merkitä IPv6-osoitteita on sarjoittaa ne kahdeksaan peräkkäiseen 16-bittiseen lukuun, joiden merkintään käytetään heksadesimaalilukuja ja jotka on erotettu toisistaan kaksoispisteillä: XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX. Esimerkkejä IPv6-osoitteista:

- FEDC:BA98: 7654:3210:FEDC:BA98:7654:3210
- 1080:0:0:0:8:800:200C:417. [1, s. 144.]

IPv6-osoitteet sisältävät usein pitkiä jonoja 0-bittejä. Jotta 0-bittejä sisältävien osoitteiden kirjoitus olisi helpompaa, niiden tiivistämiseen on olemassa oma syntaksi. Merkki ”::” osoittaa useita peräkkäisiä 16-bittisiä nollia ja sitä voidaan käyttää vain kerran yhdessä IPv6-osoitteessa. Tiivistettyjen bittien määrä voidaan helposti päätellä, mikäli ”::”-merkkiä on käytetty vain kerran yhdessä osoitteessa, mutta jos merkkiä käytettäisiin useammin, ei olisi mitenkään mahdollista päätellä, kuinka monta merkkiä on tiivistetty jokaisessa erillisessä tiivistyskerrassa. Esimerkki osoitteiden tiivistämisestä on esitetty taulukossa 1. [1, s. 145.]

Taulukko 1. IPv6-osoitteiden standardimuotoinen ja tiivistetty esitystapa

Osoitetyyppi	**Standardimuotoinen esitystapa**	**Tiivistetty esitystapa**
Unicast-osoite	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast-osoite	FF01:0:0:0:0:0:0:101	FF01::101
Loopback-osoite	0:0:0:0:0:0:0:1	::1
Märittelemätön osoite	0:0:0:0:0:0:0:0	::

2.1.3 IPv6-osoitteiden verkkoprefiksit

Jokainen IP-osoite voidaan jakaa kahteen osaan: verkko-osaan ja host-osaan. Verkko-osio määrittelee tietyn verkon ja host-osio määrittelee tietyn noodin, esimerkiksi tietokoneen, paikallisessa LAN-verkossa. [2.]

IP-osoitteet on jaettu verkkoihin eri kokoisina lohkoina. Lohkon koko kirjoitetaan ”/”-merkin perään kertomaan, kuinka monta bittiä osoitteen alusta on varattu verkon määritykseen. Tästä voidaan laskea osoiteavaruudelle jäävien bittien määrä. Mitä pienempi numero ”/”-merkin perässä on, sitä enemmän osoitteita kyseinen lohko sisältää. [2]

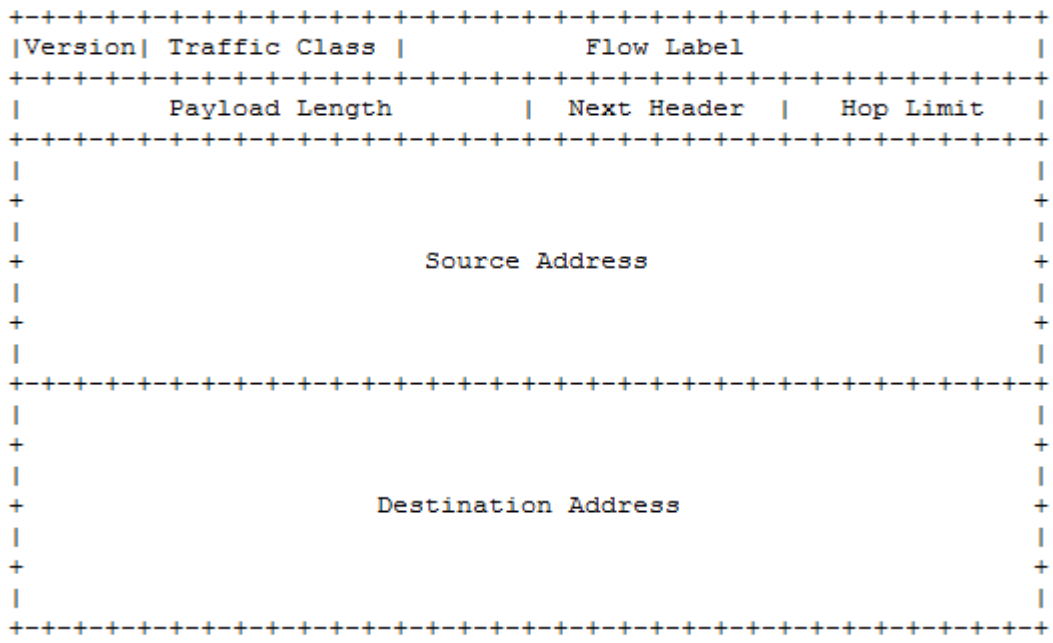
Toisin kuin IPv4:ssä, jossa verkkoprefiksin pituus voi vaihdella, IPv6 on rakennettu niin, että kaikilla LAN-verkoilla on 64-bittinen prefiksi. Näin ollen jokaisessa IPv6-verkossa on 18 446 744 073 709 551 616 osoitetta. IPv6-osoitteiden verkkoprefiksit ja verkkojen suhteelliset koot on esitetty tarkemmin taulukossa 2. [2]

Taulukko 2. IPv6-osoitteiden verkkoprefiksit ja verkkojen suhteelliset koot

/128	1 IPv6-osoite	Verkkorajapinta
/64	1 IPv6-aliverkko	18 446 744 073 709 551 616 IPv6-osoitetta
/56	256 LAN-segmenttiä	Yleinen prefiksi yhdelle tilaajasaitille
/48	65 536 LAN-segmenttiä	Yleinen prefiksi yhdelle tilaajasaitille
/32	65 636 /48 tilaajasaittia	IPv6-minimiallokointi paikalliselle palveluntarjoajalle
/24	16 777 216 tilaajasaittia	256 kertaa suurempi kuin IPv6-minimiallokointi

2.1.4 IPv6-osoitteiden otsikkoformaatti

Ipv6-osoitteiden otsikot esitetään aina standardimuotoisesti. Ohessa kuvattuna IPv6-osoitteen otsikon tarkempi sisältö. [3]



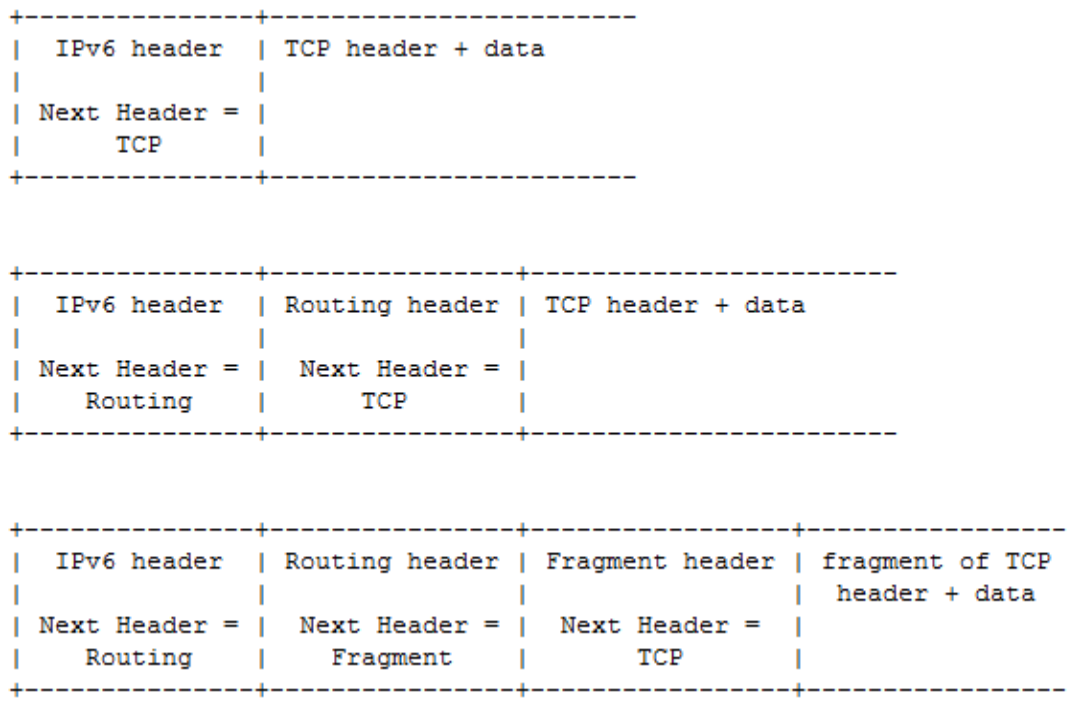
Kuva 1. Ipv6-osoitteen otsikkoformaatti

- Version: Internet-protokollan versio 6, kuvaukseen käytetään 4 bittiä.
- Traffic Class: 8-bittinen osoiteluokka. Osoiteluokkakenttää IPv6-otsikossa käyttävät paketin alkuperäinen lähettäjälaite sekä pakettia eteenpäin toimittavat reitittimet. Kentän avulla eri tyyppiset ja eri prioriteetin IPv6-paketit tunnistetaan ja erotellaan toisistaan.
- Flow Label: 20-bittinen kenttä, jota Ipv6-paketin lähde voi käyttää merkitsemään sellaisten pakettien järjestystä, jotka vaativat reitittimiltä erityskäsittelyä. Laitteet, jotka eivät tue tämän kentän toimintoja, merkitsevät kentän arvoksi 0 lähettäessään pakettia, siirtävät kentän muuttumattomana lähettäessään pakettia eteenpäin ja jättävät kentän huomiotta vastaanottaessaan pakettia.
- Payload Length: 16-bittinen merkitsemätön kokonaisluku, joka kertoo otsikkoa seuraavan paketin koon tavuissa. Myös mahdolliset laajennusotsikot ovat osa kuorman kokoa.
- Next Header: 8-bittinen valitsija, joka identifioi IPv6-otsikkoa seuraavan otsikon.
- Hop Limit: 8-bittinen merkitsemätön kokonaisluku. Jokainen laite, joka lähettää paketin eteenpäin pienentää arvoa yhdellä. Mikäli luku vähenee nollaan asti, paketti hylätään, eikä sitä toimiteta eteen päin.

- Source Address: Paketin lähettäjän 128-bittinen osoite.
- Destination Address: Paketin aiotun vastaanottajan 128-bittinen osoite. [3.]

2.1.5 IPv6-laajennusotsikot

IPv6:ssa valinnaista internet-tason informaatiota voidaan sisällyttää erillisiin otsikoihin, jotka sijaitsevat paketin IPv6-otsikon ja ylemmän tason otsikon välissä. IPv6-paketti voi sisältää yhden tai useampia laajennusotsikoita, mutta välttämättä paketilla ei ole yhtään laajennusotsikkoa. Tällaisia laajennusotsikoita identifioidaan selkeästi eroteltavilla Next Header -arvoilla. [3.]



Kuva 2. IPv6-laajennusotsikoiden rakenne

Yleensä paketin toimituspolun varrella sijaitsevat laitteet eivät tutki tai käsittele laajennusosoitteita. Laajennusosoitteiden sisältämä tieto käsitellään vasta kun paketti saavuttaa IPv6-otsikon Destination Address -kentässä identifioidun laitteen. Kun paketti saavuttaa päämääränsä, IPv6-otsikon käsittelyssä siirrytään Next Header -kentän osoittaman laajennusotsikon käsittelyyn. Mikäli laajennusotsikoita ei ole käytössä paketilla, siirrytään käsittelemään ylemmän tason otsikkoa. Laajennusotsikot täytyy aina käsitellä siinä järjestyksessä kuin ne paketissa ilmenevät. Vastaanottaja ei voi esimerkiksi

etsiä paketista tietyntyyppisiä laajennusotsikoita ja käsitellä niitä ennen kuin se on käsitellyt kaikki edeltävät laajennusotsikot. [3.]

Laajennusotsikoiden käsittelyssä poikkeuksena on Hop-by-Hop Options -otsikko, joka sisältää sellaista informaatiota, jota jokaisen paketin toimituspolun varrella olevan laitteen täytyy käsitellä. Mikäli tämä otsikko on käytössä paketilla, tulee sen sijaita välittömästi IPv6-otsikon jälkeen. IPv6-otsikon Next Header -kentän arvo 0 ilmaisee tämän otsikon mukana oloa paketissa. [3.]

Mikäli otsikkoa käsittelevän laitteen tulisi siirtyä käsittelemään laajennusotsikkoa, mutta otsikon Next Header -arvoa ei voida tunnistaa tai jonkin muun kuin IPv6-otsikon Next Header -arvo on 0, laitteen tulisi hylätä paketti ja lähettää paketin lähettäjälle ICMP Parameter Problem -viesti, jossa ICMP Code -arvo on 1 ja ICMP Pionter -kenttä sisältää alkuperäisen paketin tunnistamattoman arvon. [3.]

IPv6:n täysi käyttöönotto sisältää seuraavien laajennusotsikoiden implementoinnin:

- Hop-by-Hop Options -otsikkoa käytetään kun paketti sisältää informaatiota, jota jokaisen paketin toimituspolun varrella olevan laitteen täytyy käsitellä.
- Routing- eli reititysotsikko, jota käytetään merkitsemään yhtä tai useampaa laitetta, joiden kautta paketin tulee kulkea matkalla kohteeseensa.
- Fragment- eli pirstaleotsikkoa käytetään lähetettäessä paketteja, jotka ovat kooltaan niin suuria, ettei niitä voida toimittaa yhdessä osassa.
- Destination Options -otsikkoa käytetään lähetettäessä sellaista informaatiota, jota vain paketin vastaanottajalaitteen tarvitsee tutkia.
- Authentication- eli autentikointiotsikko tarjoaa yhteydetöntä eheyttä ja datan alkuperän autentikointia IP-datagrameille.
- Encapsulating Security Payload -otsikko tarjoaa useita tietoturvapalveluita sekä IPv6:lle että IPv4:lle. [3.]

2.2 IPv6:n toiminnallisuudet

IPv6 tarjoaa muitakin muutoksia ja parannuksia kuin suuremman osoiteavaruuden. IPv4:n skaalautuvuudessa esiintyy puutteita, sillä yksityiset IPv4-verkot ja maailmanlaajuinen Internet ovat kasvaneet huomattavasti. IP-noodien ja -verkkojen konfigurointiin ja ylläpitoon käytettyjen automaattisten työkalujen puute on hidastanut IP:n kehitystä. Vaikka joitakin IPv6:een tehtyjä päivityksiä on kokeiltu jo IPv4:ssä, tarkoittavat perusprotokollan parannukset sitä, että uudet ominaisuudet toimivat paremmin. IPv6:n parannelluista toiminnallisuuksista on kerrottu tarkemmin seuraavissa kappaleissa. [1, s. 135-136.]

2.2.1 Autokonfiguraatio

Alkuperäinen automaattiseen IP-konfigurointiin käytetty protokolla vuodelta 1985 oli Boot-protokolla (BOOTP). Se määrittelee mekanismin, jolla noodit voivat lähettää broadcastina paikallisille linkeilleen kyselyn, jossa ne pyytävät BOOTP-palvelimen osoitetta, josta ne voivat ladata itselleen IP-osoitteen. DHCP, eli Dynamic Host Configuration -protokolla, perustuu BOOTP-protokollaan, mutta se tarjoaa mekanismin, jolla noodit voivat ladata tarvitsemansa konfiguraatiot DHCP-palvelimilta. [1, s. 136.]

Sekä BOOTP että DHCP luokitellaan ”tilallisiksi autokonfiguraatioprotokolliksi”, sillä ne vaativat, että BOOTP/DHCP-palvelin, joka ylläpitää tekemiensä osoiteallokaatioiden tilaa, konfiguroi verkossa olevat noodit. Toisin sanoen palvelimelle on allokoitu IP-osoitelohko, josta se jakaa edelleen osoitteita niitä pyytäville noodeille. Mikäli IP-osoitteita tarjoava palvelin on tavoittamattomissa, eivät laitteet pysty muodostamaan yhteyttä. Verkkojen laajetessa jokaiselle aliverkolle täytyy allokoida oma osoitelohkonsa, joka puolestaan luo uusia ongelmia pyyntöjen tasapainottamiseen kyseisten palvelinten välillä. [1, s. 136.]

”Tilaton autokonfiguraatioprotokolla”, jossa noodit voivat yhdistyä verkkoon riippumatta yhdestäkään palvelimesta, tarjoaa joustavuutta ja skaalautuvuutta verkkojen kasvaessa ja noodien liikkuessa. IPv6 tarjoaa tällaisen protokollan (Stateless Autoconfiguration Protocol) sekä myös päivitetyn version DHCP:stä, eli DHCPv6:n. [1, s. 136.]

2.2.2 Neigbor Discovery -protokolla

Neigbor Discovery IPv6:lle on standardi, joka määrittelee mekanismin, jolla saman linkin takana olevat IPv6-noodit voivat käyttää Neigbor Discovery -protokollaa todentaakseen toistensa läsnäolon, saadakseen selville toistensa linkkitason osoitteet, löytääkseen reitittimet ja ylläpitääkseen aktiivisiin naapureihin johtavien polkujen tavoitettavuusinformaatiota. Neigbor Discovery -protokolla IPv6:lle korvaa tehokkaasti ARP:n (Address Resolution Protocol), jota käytetään yhdistämään linkkitason verkko-osoitteita IPv6-osoitteisiin.

2.2.3 Anycast

Kuten kappaleessa 2.1.1 todettiin, IPv6-osoitteita on kolmea eri tyyppiä. Unicast-osoite osoittaa yksittäistä verkkorajapintaa. Multicast-osoite osoittaa verkkorajapintojen joukkoa ja tähän osoitteeseen lähetetyt paketit toimitetaan kaikkiin joukon osoittamiin laitteisiin. Anycast-osoitetta puolestaan on mahdotonta erottaa unicast-osoitteesta. Ainoana erona on, että yksi tai useampi rajapinta voidaan määrittää vastaamaan paketteihin, jotka lähetetään anycast-osoitteeseen, kuitenkin niin että vain yksi joukon jäsenistä vastaa tiettyyn yksittäiseen anycast-pakettiin. Anycast-osoitteeseen lähetetyt paketit siis lähetetään mille tahansa joukon rajapinnoista, mutta vain yhdelle joukon rajapinnoista. Anycast-osoitejoukon ”lähin” rajapinta vastaa anycast-pakettiin. Käytössä oleva reititysprotokolla puolestaan määrittelee etäisyyden anycast-paketin lähettävän ja vastaanottavan rajapinnan välillä. [1, s. 138-139, 142, 145.]

2.2.4 Mobiili IPv6

Kannettavien tietokoneiden yleistyessä on tullut esiin tarve mobiilille IP-protokollalle, joka mahdollistaa yhden IP-osoitteen käyttämisen tietokoneella kaikkeen kommunikaatioon riippumatta siitä, mihin verkkoon tietokone on kytketty. Teknologia kuitenkin poikkeaa matkapuhelinverkossa käytettävästä teknologiasta, sillä matkapuhelinverkossa tiedon luovutus tapahtuu linkkitasolla, toisin kuin mobiilissa IP-verkossa, jossa tiedon luovutus hoidetaan yleensä verkkotasolla. [1, s. 139-140, 291-292.]

IP-noodi voi vastaanottaa sen kotiosoitteeseen lähetettyjä paketteja mistä tahansa. Kun noodi yhdistyy verkkoon, se kuuntelee liikkuvuusagentin lähettämiä viestejä, joiden perusteella noodi päättelee, onko se kotiverkossaan

vai jossakin muussa verkossa. Kun noodi sijaitsee kotiverkossaan, se käyttäytyy kuten mikä tahansa noodi. Kun noodi sijaitsee vieraassa verkossa, se pyytää itselleen kyseisen verkon liikkuvuusagentilta niin sanotun care-of-osoitteen, jonka se ilmoittaa oman kotiverkkonsa liikkuvuusagentille. Noodin kotiverkossa oleva liikkuvuusagentti lähettää noodin kotiosoitteeseen saapuvat paketit edelleen noodille tunneloimalla liikenteen vierasverkkoon care-of osoitteen avulla. [1, s. 140, 291-292.]

2.3 IPv6:een siirtyminen

IPv6:een siirtymisen odotetaan olevan asteittainen prosessi, jossa IPv6-teknologia otetaan käyttöön IPv4:n rinnalla ja järjestelmiä päivitetään pikkuhiljaa tukemaan IPv6:tta. Kaikkien järjestelmien päivitys suoraan IPv6:een olisi täysin mahdotonta, ottaen huomioon Internetiin kytkettyjen verkkojen ja noodien määrän. Laitevalmistajat ja kehittäjät ottavat vähitellen IPv6-teknologiaa käyttöön eri alustoille sitä mukaa, kun sille todetaan olevan tarvetta. IPv4:n ja IPv6:n täytyy toimia rinnakkain vielä pitkän aikaa, mahdollisesti ikuisesti. [1, s.75-77.]

3 IPV6-OSOITTEIDEN TILAAMINEN

IPv6-käyttöönottosuunnitelman tekemiseen liittyi myös IPv6-osoitelohkon tilaaminen yrityksen käyttöön. Ennen osoitteiden tilaamista täytyi tutustua RIPEn ja RIPE NCC:n toimintaan yleisellä tasolla, IPv6-osoitepolitiikkaan sekä IPv6-osoiteavaruuksien allokaatioiden ja jakojen perusperiaatteisiin.

3.1 RIPE

RIPE (Réseaux IP Européens) on yhteisfoorumi, joka on avoin kaikille tahoille, jotka ovat kiinnostuneita laajan alueen IP-verkoista. RIPE aloitti toimintansa vuonna 1989, kun ryhmä Euroopassa sijaitsevia IP-verkko-operaattoreita aloitti säännölliset tapaamiset jakaakseen kokemuksia ja suorittaakseen teknistä koordinaatiotyötä. He alkoivat vaihtaa tietoa ja loivat tietokannan operationaalisen datan säilyttämistä varten. Toiminnan kasvaessa koordinointityön määrä laajeni nopeasti ja vuonna 1990 operaattorit päättivät rahoittaa koordinointikeskuksen (RIPE NCC), joka perustamisensa jälkeen on työllistänyt kokoaikaisen henkilökunnan, joka toteuttaa työtä heidän puolestaan. [4; 5.]

RIPEn tavoitteena on varmistaa tarvittava hallinnollinen ja tekninen yhteistyö sekä Internetin toiminnan mahdollistamiseksi että yleiseurooppalaisen IP-verkon operoimiseksi ja laajentamiseksi. RIPEn koordinoiva elin on perustettu huomioiden, että IP-verkot kasvavat Euroopan paikallisverkkojen (LAN, Local Area Network) ulkopuolelle sekä laajenevat kansallisten ja kansainvälisten laajaverkkojen (WAN, Wide Area Network) yli Euroopassa. [4; 6.]

RIPEn toimintapuitteet:

- RIPE toimii foorumina teknisen informaation vaihtamiseen ja IP-verkkotyöskentelyn asiantuntemuksen luomiseen.
- RIPElle merkityksellinen alue on Eurooppa.
- Kaikkia osapuolia, jotka operoivat laajan alueen IP-verkkoja, kannustetaan osallistumaan.
- RIPE edistää ja koordinoi IP-verkkojen yhteyttä Euroopan ja muiden maanosien välillä.
- RIPE laatii sopimukset yleisistä verkon hallintakäytännöistä ja toisiinsa yhteydessä olevien verkkojen operatiivisesta hallinnasta
- RIPE toimii keskeisenä pisteenä osanottajien muille yleisille toiminnoille, jotka liittyvät IP-verkkotyöskentelyyn.
- Kaikki RIPEn tuottamat dokumentit tulevat olemaan julkisesti saatavilla.
- RIPE ei ole verkkopalveluntarjoaja. RIPEn kanssa yhdessä toimivat IP-verkot pysyvät niille kuuluvien organisaatioiden määräysvallan alla. [6.]

RIPEn toimintaan osallistumisella ei ole jäsenyysvaatimuksia. Sen toiminnot suoritetaan vapaaehtoispohjalta ja päätökset muodostuvat yhteisymmärryksestä. Työtä toteutetaan useissa työryhmissä, joista jokaisella on yksi tai useampia sähköpostilistoja, joiden avulla keskustellaan asiaankuuluvista aiheista ja kysymyksistä. RIPEn työryhmät kokoontuvat vuoden ympäri RIPEn tapaamisissa, jotka ovat viisipäiväisiä tapahtumia, joissa Internet-palveluntarjoajat, verkko-operaattorit ja muut kiinnostuneet osanottajat Eu-

roopasta ja ympäröiviltä seuduilta kokoontuvat. RIPEn tapaamiset ovat avoimia kaikille. Vaikka tapaaminen on ensisijaisesti tekninen, on se myös sosiaalinen tapahtuma. [4; 7.]

3.2 RIPE NCC

Vaikka RIPE NCC ja RIPE ovat nimiltään samankaltaisia, ne ovat kuitenkin erillisiä kokonaisuuksia. RIPE NCC (Network Coordination Centre) perustettiin virallisesti huhtikuussa 1992. RIPE-yhteisö päätti perustaa RIPE NCC:n vuonna 1990, kehitti sen ensimmäisen toimintasuunnitelman vuonna 1991 ja auttaa edelleen toimintasuunnitelman laatimisessa vuosittain. Tammikuussa 1998 RIPE NCC:stä tuli laillinen yksikkö, jonka toimintoihin RIPE-yhteisö jatkaa panoksensa tarjoamista RIPEn tapaamisissa ja RIPEn monenlaisissa työryhmissä. [5.]

RIPE NCC on itsenäinen, voittoa tuottamaton jäsenorganisaatio, joka tukee Internetin infrastruktuuria teknisen yhteistyön avulla palvelualueellaan. Sen huomattavin toimintamuoto on toimia RIR:nä (Regional Internet Registry eli alueellinen Internet-rekisteri), joka tarjoaa maailmanlaajuisia Internet-resursseja ja niihin liittyviä palveluita (kuten IPv4 ja IPv6) jäsenilleen. Jäseninä on pääasiassa Internet-palveluntarjoajia (ISP eli Internet Service Provider), telekommunikaatio-organisaatioita ja suuria yrityksiä, jotka ovat sijoittuneet Eurooppaan, Lähi-itään ja Keski-Aasian joihinkin osiin. [8.]

Osaa RIPE NCC:n alkuperäisistä toiminnoista toteutetaan edelleen, kuten dokumenttivaraston luominen ja ylläpito sekä RIPEn tapaamisten organisointi. IP-osoiteavaruuksien jakelu ei ollut alkuperäisten toimintojen joukossa, vaan se lisättiin vuonna 1992, kun sille huomattiin olevan tarvetta. RIPE NCC tarjoaa palveluita myös yleisesti Internet-yhteisön hyödyksi, kuten RIPE-tietokannan kehitys ja ylläpito sekä hallinnollinen tuki RIPE-yhteisölle. [5; 8.]

3.3 Luvitusprosessi

IPv6-osoitteiden allokaatioperiaatteet vaihtelevat hieman riippuen siitä, millaisia osoitteita yritykset tarvitsevat käyttöönsä. Yrityksien on mahdollista hakea käyttöönsä kahdenlaisia IP-osoitteita:

- Operaattorikohtaiset PA-osoitteet (engl. Provider Aggregatable) ovat palveluntarjoajille edelleenallokointia tai -jakelua varten allokoituja IP-osoiteavaruuksia. Nämä osoitteet on sidottu palveluntarjoajaan ja osoitteita voidaan käyttää vain kyseisen operaattorin tarjoamissa lähiverkoissa. Operaattorikohtaisten IPv6-osoitteiden allokoitavan avaruuden oletuskokoa merkitään aliverkon peitteellä /32, joka sisältää 65 536 kappaletta /48-verkkoja. Nämä verkot puolestaan sisältävät 65 536 kappaletta /64 LAN-segmenttejä, jotka sisältävät yli 18 triljoonaa yksittäistä IPv6-osoitetta.

- Operaattoririippumattomat PI-osoitteet (engl. Provider Independent) puolestaan eivät ole sidottuja tiettyyn palveluntarjoajaan, joten käytössä olevia IP-osoitteita ei tarvitse vaihtaa uusiin vaikka Internet-palveluntarjoaja vaihtuisi. Osoitteita voidaan allokoida yrityksille vain niiden omaan käyttöön, eivätkä yritykset saa jakaa lohkoja tällaisesta osoiteavaruudesta edelleen omille asiakkailleen. Operaattoririippumattomien IPv6-osoitteiden allokoitavan avaruuden koko on /48, joka sisältää 65 536 kappaletta /64-aliverkkoja. [1, s.144; 2]

Yrityksellä jo käytössään olevat IPv4-osoitteet ovat operaattoririippumattomia, ja tarve oli hankkia myös IPv6-osoitteet operaattoririippumattomina. Tästä syystä tässä työssä keskitytään luvitusprosessiin vain operaattoririippumattomien osoitteiden osalta. Saadakseen operaattoririippumattomia IPv6-osoitteita käyttöönsä yrityksen tulee demonstroida, että se tulee olemaan multihomattu ja täyttää RIPE NCC:n erikseen määrittelemät vaatimukset, jotka on listattu tarkemmin myöhemmin tässä kappaleessa. [9.]

Multihomaus (engl. multihoming) on tekniikka, jota käytetään verkkoyhteyden luotettavuuden kasvattamiseen. Yleisimmät tavat multihomauksen toteuttamiseen ovat:

- Yksi linkki, jolla on useita IP-osoitteita.

- Useita verkkorajapintoja, joista jokaisella on yksi tai useita IP-osoitteita.

- Useita linkkejä, joilla kaikilla on useita IP-osoitteita.

- Useita linkkejä, joilla on kaikilla sama IP-osoite. Yleensä puhuttaessa multihomauksesta, tarkoitetaan tätä tekniikkaa. [11.]

RIPE NCC määrittelee, että saadakseen operaattoririippumattomia IP-osoitteita yrityksellä tulee olla sopimuksellinen suhde RIPE NCC:hen. Toivottavampi malli on, että loppukäyttäjäyrityksen sopimuksellinen suhde olisi tehty palveluntarjoajan kanssa eikä suoraan RIPE NCC:n kanssa. Lisäksi on määritelty, että kaikissa sopimuksissa tulisi olla vähintäänkin seuraavat tiedot:

- Maininta siitä, että palveluntarjoajat ovat vastuussa yhteydenpidosta resurssien haltijaan pitääkseen rekisteröintitiedot ajan tasalla.
- Maininta siitä, että resurssien haltija on velvoitettu tarjoamaan palveluntarjoajalle ajantasaista tietoa, ja että osa tai kaikki annetuista tiedoista julkaistaan RIPEn WHOIS-tietokannassa.
- Maininta siitä, että operaattoririippumattomia resursseja ei saa edelleenjakaa kolmannelle osapuolelle.
- Maininta siitä, että resurssien haltija on velvoitettu maksamaaan vuosittaisen maksun palveluntarjoajalle resursseista.
- Selkeä maininta, että resurssit palautetaan RIPE NCC:lle, jos
    - resurssien haltijaa ei tavoiteta
    - vuosittaista maksua palveluntarjoajalle ei ole suoritettu
- Selkeä maininta, että resurssien käyttö on suhteutettu RIPEn menettelytapoihin, jotka on julkaistu RIPEn verkkosivuilla, ja jotka voivat muuttua aika ajoin. [9; 10.]

RIPE NCC jakaa operaattoririippumattomia IPv6-osoitteita loppukäyttäjäyrityksille asianmukaisesti lähetetyllä pyyntölomakkeella, joka voidaan lähettää suoraan RIPE NCC:lle tai toimittaa Internet-palveluntarjoajan kautta. Yrityksellä jo käytössä olevat IPv4-osoitteet on tilattu paikallisen palveluntarjoajan kautta, joten yrityksellä on voimassa oleva sopimus palveluntarjoajan kanssa IP-osoitteiden hankkimisesta. Tästä syystä päätettiin myös IPv6-osoitteet hankkia saman sopimuksen puitteissa palveluntarjoajan kautta, eikä suoraan

RIPE NCC:ltä. Koska vastaavanlainen hakemus on aikoinaan täytetty tilattaessa IPv4-osoitteita, pystyttiin osa lomakkeeseen tarvittavista tiedoista kopioimaan vanhasta hakemuksesta vain tarkistamalla, että tieto on edelleen ajankohtainen ja paikkansapitävä. [9.]

IPv6-osoiteavaruuslohkon hakukaavake liitteenä (liite 1).

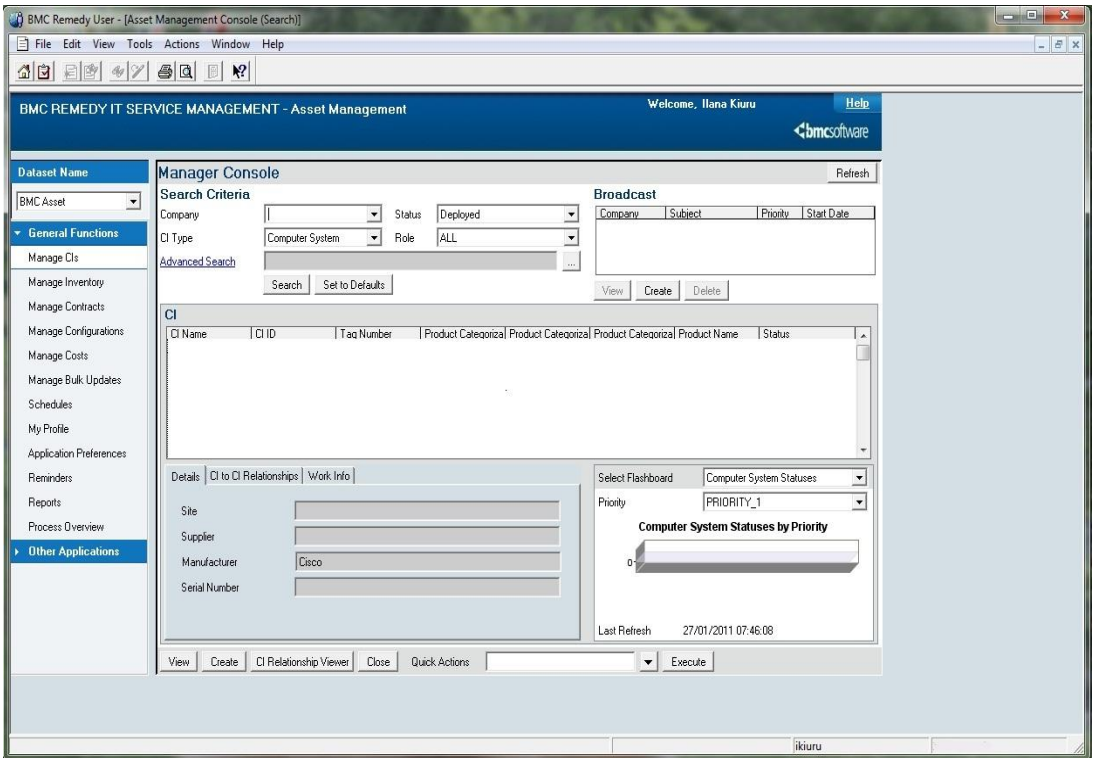
4 LAITTEISTON NYKYTILAN KARTOITUS

Ennen IPv6-käyttöönottosuunnitelman laatimista täytyi selvittää yrityksen laitteiston tämänhetkinen tilanne, jotta tiedetään, täytyykö laitteistoa uusia tai päivittää ennen kuin IPv6 voidaan ottaa käyttöön. Tarkoituksena oli kartoittaa, mitä laitteita on käytössä ja mitä ohjelmistoversioita niissä on asennettuna. Tässä kappaleessa on kuvattu, kuinka laitteiden tietoja on haettu ja miten niiden IPv6-yhteensopivuutta on selvitetty.

4.1 Laitetietojen hakeminen tietokannasta

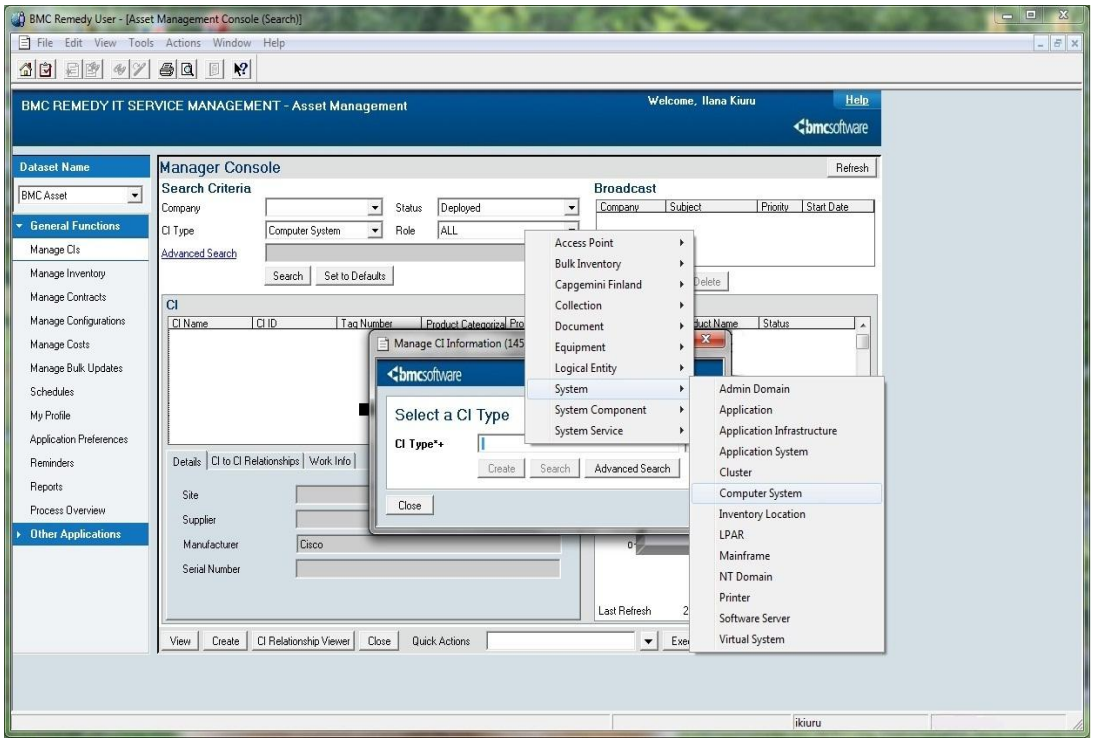
Yrityksessä tiedot laitekannasta on tallennettu CMDB:hen. CMDB on lyhenne sanoista Configuration Management Database, ja se on BMC Softwaren toimittama ohjelmisto. Tietokanta sisältää yrityksen oman laitteiston lisäksi myös tiedot yrityksen ylläpitämistä asiakaslaitteista.

Käyttöliittymä on kohtuullisen yksinkertainen käyttää, ja tietojen hakeminen on helppoa. Järjestelmään kirjaudutaan sisään ja avataan Asset Management Console, jonka kautta laitetietoja hallinnoidaan. Asset Management Consolen pääikkunan näkymä on kuvattu kuvassa 1.



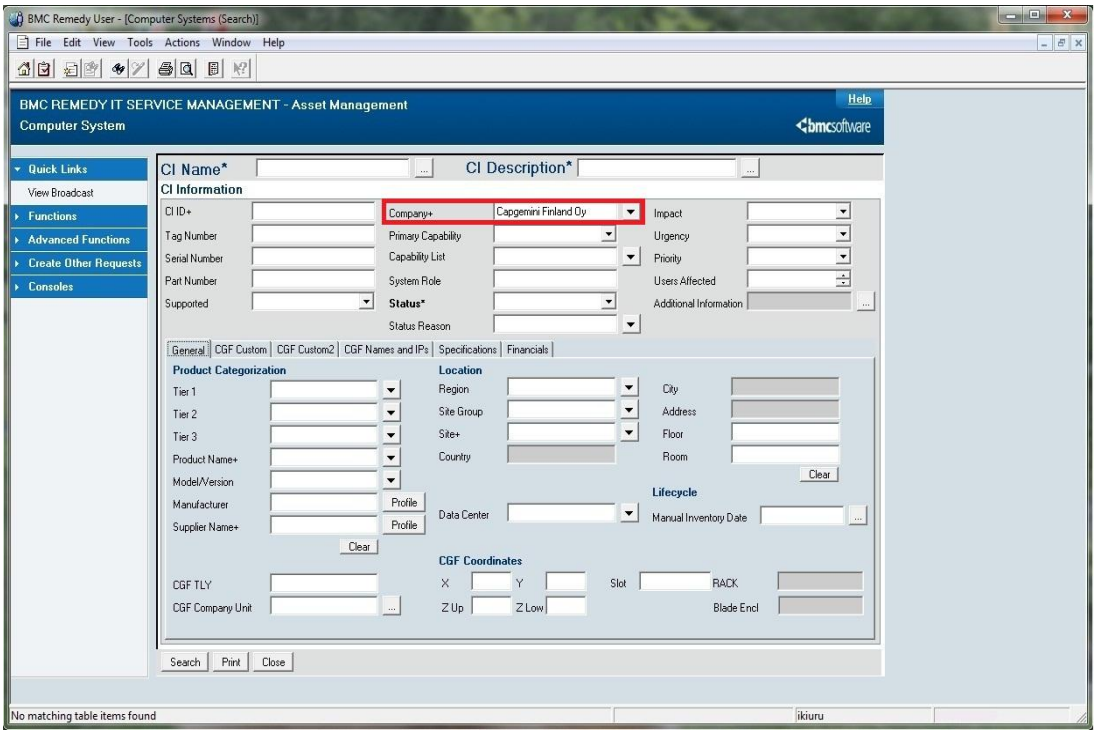
Kuva 3. CMDB:n Asset Management Consolen pääikkuna

Oikealla olevasta valikosta voidaan valita, mitä tietoja halutaan muokata tai tarkastella. Etsittäessä tietoja laitteista tarkastelun kohteena on CI eli Configuration Item. Ikkunan vasemmassa reunassa sijaitsevan valikon vaihtoehto Manage CIs avaa uuden valikon, jonka avulla vielä tarkennetaan hakua valitsemalla laitteen tyyppi. Tässä tapauksessa oikea valinta on Computer System, joka löytyy valikosta System-kohdan alta. Hakuvalinnat on kuvattu tarkemmin kuvassa 2.



Kuva 4. Laitetyypin valinta

Kun oikea laitetyyppi on valittu, saadaan hakuikkuna auki valitsemalla Search. Hakuikkunassa voidaan laitteita hakea käyttäen hakuehtona mitä tahansa yksittäistä tietoa, jota laitteista voidaan tietokantaan tallettaa. Hakuehtoja tarkennetaan syöttämällä haluttuja arvoja useampaan kenttään, jolloin voidaan rajata saatujen tulosten määrää. Tässä tapauksessa hakuehdoksi määriteltiin vain yrityksen nimi Company-kenttään, jolloin hakutuloksena saadaan lista kaikista yrityksen omista verkkolaitteista. Hakuehtojen valinta on näytetty kuvassa 3.



Kuva 5. Hakuehdot

Haun tulokset voidaan tallettaa raportiksi, joka voidaan avata esimerkiksi Excel-taulukkona, jolloin tuloksia on helppo tutkia. Raporttia luotaessa voidaan vielä erikseen määritellä, mitä tietoja haun tuloksena löytyneistä laitteista halutaan tallettaa lopulliseen raporttiin valitsemalla niiden kenttien nimet, joiden sisältö halutaan raportille sisällyttää.

4.2 Tietojen rajaaminen saaduista hakutuloksista

Koska käyttöönottosuunnitelman kannalta oli oleellista selvittää vain tiettyjen laitteiden IPv6-yhteensopivuus, rajattiin selvitys ainoastaan reitittimiin, palomuureihin, reitittäviin kytkimiin, kuormanjakajiin ja WLAN Controllereihin. Tässä vaiheessa yrityksen muiden verkkolaitteiden, kuten työasemien, palvelimien ja verkkotulostimien IPv6-yhteensopivuutta ei ollut tarpeen tutkia. Suunnitelman laatimisessa keskityttiin ainoastaan oman yrityksen infrastruktuuriin, eikä otettu kantaa asiakkaiden laitteistoihin.

Koska hakuehtojen perusteella hakua ei rajattu sen tarkemmin, vaan haettiin järjestelmästä kaikki oman yrityksen laitteet, oli tuloksista tarpeen karsia turhat laitteet pois jälkikäteen. Kaikista haetuista laitteista oli lisäksi otettu raporttiin hieman enemmän tietoja kuin tarvittiin, sillä tuloksien rajaaminen jäl-

keenpäin on nopeampaa kuin uuden haun suorittaminen jonkin puuttuvan tiedon takia.

4.3 Laitteiston ohjelmistoversioiden selvittäminen

Vaikka laitetietokantaan on tallennettu tiedot laitteiden valmistajista ja malleista, oli tietojen hakemisen ja rajaamisen jälkeen vielä tarpeen selvittää kaikkien tutkittavien laitteiden ohjelmistoversiot IPv6-yhteensopivuuden tutkimista varten. Ohjelmistoversioiden selvittäminen oli tärkeää, sillä osassa laitteista IPv6-yhteensopivuus ja sen laajuus vaihtelee riippuen laitteeseen asennetusta ohjelmistosta.

Suuri osa yrityksen käytössä olevista suunnitelman kannalta oleellisista laitteista on Cisco Systemsin laitteita, joten niiden ohjelmistoversiot oli helppo selvittää kirjautumalla sisälle laitteisiin SSH-yhteyden avulla ja kirjoittamalla komento ”show version”, joka näyttää IOS- eli käyttöjärjestelmäversion lisäksi muutakin hyödyllistä tietoa laitteesta.

Yrityksen käytössä olevat palomuurit ovat Juniperin NetScreen -laitteita, joten niiden hallintaan käytetään Juniperin NSM (Network and Security manager) -ohjelmistoa.

Ohjelmistoon kirjauduttaessa täytyy käyttäjätunnuksen ja salasanan lisäksi kirjautumisruudulle määritellä myös palvelin. Juniperin hallintasovelluksen kirjautumisruutu on esitelty kuvassa 4.

Kuva 6. Network and Security Managerin kirjautumisikkuna

5 LAITTEISTON IPV6-YHTEENSOPIVUUS JA PÄIVITYSTARPEET

IETF eli The Internet Engineering Task Force on julkaissut dokumentteja, joissa määritellään IPv6:n käyttöönottoon tarvittavia vaatimuksia. IETF:n tavoitteena on saada Internet toimimaan paremmin tuottamalla korkealaatuisia, oleellisia teknisiä dokumentteja, jotka vaikuttavat tapaan, jolla Internetiä suunnitellaan, käytetään ja hallinnoidaan. IETF:n dokumentti RFC 4294, joka julkaistiin huhtikuussa 2006, määrittelee yleisiä toiminnallisuuksia, joita laitteistojen tulee tukea toimiakseen Ipv6-ympäristöissä. Joulukuussa 2011 julkaistu dokumentti RFC 6434 syrjäytti aikaisemman RFC 4294 -dokumentin. [12]

Tärkeimpiä IPv6:n käyttöönottoon tarvittavia toiminnallisuuksia on selitetty tarkemmin seuraavissa luvuissa.

5.1 IP-alitaso

IPv6-laitteen tulee tukea yhtä tai useampaa IPv6-linkkitason määrittelyä. Mitä linkkitason määrityksiä käyttöönotossa pitäisi olla mukana riippuu siitä millä linkkitasolla laite toimii. Laitteen on mahdollista tukea Ipv6:tta vain osassa laitteen rajapintoja. Fyysisten linkkitasojen lisäksi IPv6:tta voidaan tunneloida protokollien kautta. [12.]

Koska Ipv6 toimii uusien tason 2 teknologioiden päällä, pitäisi ainakin seuraavien teknologioiden löytyä laitteista:

- IPv6-pakettien lähetys Ethernet-verkkojen yli
- IPv6 ATM-verkkojen yli
- IPv6-pakettien lähetyksen määrittely Frame Relay -verkkojen yli
- IPv6-pakettien lähetys IEE 1394 -verkkojen yli
- IPv6-, IPv4- ja ARP (Address Resolution Protocol) -pakettien lähetys kuituverkkojen yli
- IPv6:n lähetys Ipv6-muunnos alitason kautta IEEE 802.16 -verkkojen yli

- IPv6 PPP:n yli
- IPv6-pakettien lähetys IEEE 802.15.4 -verkkojen yli WiMAX- ja FireWire-verkkoja varten. Yrityksellä ei tällä hetkellä ole Suomessa käytössä kyseisiä verkkotyyppejä. [12]

5.2 IP-taso

IP-tasolla laitteesta pitäisi tukea seuraavia toiminnallisuuksia.

Yleinen IPv6-tuki

IPv6-määritysten tulee olla tuettuja. Laitteen täytyy pystyä käsittelemään laajennusotsikoita. Kaikki tunnistamattomat laajennusotsikot tulee käsitellä IPv6:n otsikkomääritysten mukaisesti. Laitteen tulee noudattaa IPv6:n pakettinlähetyssääntöjä. Laitteiden täytyy aina pystyä lähettämään, vastaanottamaan ja prosessoimaan pirstaleotsikoita. [12.]

Neighbor Discovery IPv6:lle

Neighbor Discovery -määritysten tulee olla tuettuja laitteissa. Koska Neighbor Discovery käyttää linkkitason multicast-pakettienlähetystekniikkaa joihinkin toimintoihinsa, on mahdollista, että joillekin linkkityypeille on määritelty vaihtoehtoisia protokollia tai mekanismeja näiden palveluiden käyttöönottamiseksi. [12.]

Default Router Preferences and More-Specific Routes

"Default Router Preferences and More-Specific Routes" -määrittely tarjoaa tukea laitteille, jotka on kytketty useisiin eri verkkoihin, joissa jokaisessa on reitittimiä, jotka mainostavat itseään oletusreitittimenä. Tämä määrittely auttaa tapauksissa, joissa jokin reititin voi tarjota yhteyttä laitteisiin, joihin toiset reitittimet eivät ole yhteydessä, ja väärän oletusreitittimen valinta voi johtaa yhteyden epäonnistumiseen. [12.]

Secure Neighbor Discovery

Secure Neigbor Discovery (SEND) ja kryptografisesti generoitu osoite (Cryptographically Generated Address, CGA) tarjoavat tavan turvata Neigbor Discovery -viestienvaihtoa. SEND on uusi teknologia, sillä vastaavaa toiminnallisuutta ei ole ollut IPv4:ssä, mutta sillä on huomattavaa potentiaalia tietyn-

tyyppisten hyökkäysten havaitsemisessa. IPv6-laitteet voivat tarjota SEND-toimintoja, mutta toiminto ei ole pakollinen. [12.]

Path MTU Discovery ja pakettien koko

Link MTU on suurin lähetysyksikkö, eli suurin paketin tavukoko, joka voidaan kuljettaa linkin yli yhdessä osassa. [12.]

Path MTU on kaikkien lähde- ja kohdelaitteen välisen polun linkkien pienin link MTU. [12.]

Path MTU Discovery on prosessi, jolla laite oppii polun Path MTU:n. [12.]

Path MTU Discovery Ipv6:lle tulisi olla tuettu, jotta laitteet voivat havaita ja hyödyntää 1280 tavua suurempia path MTU:ita. Path MTU Discoveryyn liittyy kuitenkin toiminnallinen ongelma, joka esiintyy silloin kun palomuurit estävät ICMP Packet Too Big -viestejä. Path MTU Discovery on riippuvainen näistä viesteistä määritelläkseen minkä kokoisia viestejä laite voi lähettää onnistuneesti. [12.]

IPv6-jumbogramit

IPv6-jumbogramit ovat vapaaehtoisia laajennuksia, jotka mahdollistavat 65535 tavua suurempien IP-datagramien lähetyksen. IPv6-jumbogramit sopivat käytettäväksi vain sellaisilla poluilla, joiden jokainen linkki tukee Jumbogrameja, kuten kampuksilla tai konesaleissa. [12.]

ICMP (Internet Control Message Protocol) IPv6:lle

ICMPv6:n tulee olla tuettu. Lisäksi laitteet voivat tukea laajennettua ICMP:tä moniosaisten viestien tukemiseksi. [12.]

Osoitteisto

Ipv6:n osoitearkkitehtuurin tulee olla tuettu. Laitteiden tulee tukea Ipv6:n tilatonta osoitteenmuodostusta (Stateless Address Autoconfiguration). Myös oletusosoitteiden valinta (Default Address Selection) IPv6:lle pitää olla tuettu, sillä IPv6-laitteiden täytyy pystyä käsittelemään useita samanaikaisesti konfiguroituja osoitteita. Kaikkien laitteiden tulisi myös mahdollistaa tilallinen osoitteenmuodostus (Stateful Address Autoconfiguration) eli DHCPv6, jota voidaan käyttää osoitteiden hankkimiseen ja konfigurointiin. [12.]

Multicast Listener Discovery (MLD) IPv6:lle

Laitteet, joiden tulee vastaanottaa ja käsitellä multicast-liikennettä, täytyy tukea MLDv1:tä. Myös Neigbor Discovery on riippuvainen multicast-liikenteestä. MLDv2 puolestaan laajentaa MLDv1:n toimintoja tukemalla lähdespesifistä multicastia. [12.]

5.3 Yrityksen laitteiston IPv6-yhteensopivuus

Kun laitteiston ohjelmistoversiotiedot oli etsitty ja dokumentoitu, piti laitteista selvittää niiden IPv6-yhteensopivuus ja -tuki.

Tutkittavia laitteita oli useampia kappaleita, mutta monet laitteet olivat keskenään samanlaisia, joten tehtäväksi jäi selvittää IPv6-yhteensopivuudet seuraaville verkkolaitteille:

- Palomuurit:
    - Juniper NetScreen ISG 1000 (Ohjelmistoversio 6.2.0r4.0)
    - Juniper NetScreen SSG 550M (Ohjelmistoversio 6.2.0r4.0)
    - Cisco ASA 5500 Series - ASA5520 (Ohjelmistoversio 8.2(2))
- Reitittimet:
    - Cisco 7201 (Ohjelmistoversio 12.4(24)T2)
- Kytkimet:
    - Cisco WS-C3550-12T (Ohjelmistoversio 12.2(44)SE6)
    - Cisco 6509 (Ohjelmistoversio 12.2(33)SXI)
    - Cisco Nexus 7000 Series, N7K-C7010 (Ohjelmistoversio 4.2(4))
- WLAN-kontrollerit:
    - Cisco AIR-CT5508-K9 (ohjelmistoversio 6.0.196.0)

Kytkinten ja reitittimien osalta paras keino laitteen tukemien ominaisuuksien tarkasteluun oli Cisco Feature Navigator, joka löytyy osoitteesta

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. Cisco Feature Navigatorin avulla voidaan hakea yksittäisen laitteen tukemia ominaisuuksia esimerkiksi laitteen ohjelmistoversion avulla. Lisäksi sen avulla voi vertailla kahden eri laitteen tai ohjelmiston ominaisuuksia keskenään. Palomuurien ja WLAN-kontrollereiden osalta laitteiden IPv6-yhteensopivuustietoja etsittiin laitevalmistajien verkkosivuilta. Ciscon Nexus-kytkinten osalta yhteensopivuustietoja ei löytynyt Cisco Feature -navigaattorista, eikä myöskään tarpeeksi laajoja tietoja ollut helposti saatavilla valmistajan verkkosivuilla, joten näiden laitteiden osalta lähetettiin sähköpostia valmistajalle ja pyydettiin tarkempaa selvitystä kyseisen kytkinmallin IPv6-tuen laajuudesta.

Yrityksen ei ole tarkoitus siirtyä käyttämään kokonaan vain IPv6-teknologiaa, vaan tarkoituksena on ensin ottaa kyseinen tekniikka testikäyttöön yrityksen sisällä, jotta IPv6:tta voitaisiin myöhemmin tarjota myös asiakasyritysten käyttöön. Näin ollen IPv6-yhteensopivuustietoja haettaessa tuli ottaa huomioon, että laitteiden pitää tukea IPv6:tta rinnakkain IPv4:n kanssa. Lisäksi laitteiden IPv6-tuen ei välttämättä tässä vaiheessa tarvitse olla niin laaja kuin sen pitäisi olla, jos siirryttäisiin suoraan käyttämään vain IPv6:tta yrityksen verkkolaitteissa.

Laitteiden IPv6-yhteensopivuuksia tarkasteltaessa todettiin, että tuki on yrityksen käyttötarpeeseen nähden riittävä seuraaville laitteille:

- Palomuurit:
    - Juniper NetScreen ISG 1000
    - Juniper NetScreen SSG 550M
    - Cisco ASA 5500 Series - ASA5520
- Reitittimet:
    - Cisco 7201
- Kytkimet:
    - Cisco 6509
- WLAN Controllerit:

- Cisco AIR-CT5508-K9

Cisco WS-C3550-12T -kytkimien IPv6-tuki on tällä hetkellä huomattavan rajallinen. Tutkittaessa kytkimen ominaisuuksia huomattiin, että tarjolla ei ole sellaisia ohjelmistopäivityksiä, joilla kytkimiin saataisiin riittävä IPv6-tuki. Näin ollen piti tutkia, mitkä kytkimet voisi ottaa käyttöön korvaaviksi laitteiksi. Ominaisuuksiltaan C3550-kytkintä vastaavia laitteita, joissa IPv6-tuki on laajempi, löytyi kaksi kappaletta: Cisco CAT3750, jossa ohjelmistoversion pitäisi olla vähintään 12.2(44)SE6 sekä Cisco CAT3650, jonka ohjelmistoversion tulisi olla 12.2(44)SE6 tai uudempi.

Suunnitelman laatimisvaiheessa kyseltiin laitevalmistajalta Cisco Nexus N7K-C7010 -kytkimen IPv6-yhteensopivuustietoja, ja saatiin vastaukseksi, että IPv6-tuki on vasta suunnitelmissa. Kyseisten laitteiden korvaaminen uusilla vastaavilla laitteilla, joissa olisi IPv6-tuki, olisi huomattavan suuri investointi. Tästä syystä itse suunnitelma on ehdotettu toteutettavaksi vasta, kun kyseiset laitteet tukevat IPv6:ta. Nykyisin laitetoimittajan sivuilta etsittäessä voidaan nähdä, että IPv6-tuki löytyy myös kyseiselle laitteelle. Suurin osa IPv6-toiminnallisuuksista kuitenkin vaatii ”Enterprise Services Package” -lisenssin, jotta ne saadaan laitteessa toimimaan.

6 IPV6 JA TIETOTURVA

Tietoturvan saavuttaminen on käytännössä monimutkainen tehtävä. Mm. toiminnalliset prosessit, protokollat avaintenjakomekanismit ja sertifikaattien hallinta vaikuttavat todellisuudessa saavutettavaan tietoturvan tasoon. Minkä tahansa yksittäisen osatekijän huono soveltuvuus voi pienentää tietoturvaratkaisun tehokkuutta huomattavasti. [12.]

IPsec on Internet-tason tietoturvaratkaisu, joka mahdollistaa turvallisen kommunikaatiotavan laitteiden välillä. IPsec on tarpeeksi joustava, jotta yksittäiset TCP-yhteydet voidaan suojata. Vaikka Ipsec:iä voidaan käyttää manuaalisten avainten kanssa, joissakin tapauksissa käytöllä on rajoitettu soveltuvuus, eikä tätä suositella käytettäväksi. [12.]

Nykyään tietoturvateknologioiden määrä lisääntyy nopeasti, mutta mikään lähestymistapa ei ole näyttänyt ihanteelliselta teknologialta kaikille tarpeille ja ympäristöille. Tämän takia IPsec tuskin tulee syrjäyttämään muita teknologioita. Aikaisemmin IPv6-määritykset sanelivat IPsec:in käyttöönoton pa-

kolliseksi ja suosittelivat avaintenhallintaan IKE:ä. Nykyään IPv6-määritykset vain suosittelevat IPsec:in käyttöä ja automaattisen avaintenhallinnan oletusprotokolla on IKEv2. IPsec-arkkitehtuuri vaatii sekä manuaalisen että automaattisen avaintenhallinnan käyttöönottoa. [12.]

6.1 IPv6:n tietoturvahyödyt

IPv6 mahdollistaa päästä päähän salauksen. Vaikka sama teknologia on sovitettu myös IPv4:lle, on se vain vaihtoehtoinen lisä, joka ei ole yleisesti käytössä. Salaus ja yhtenäisyyden tarkistus, joita käytetään nykyisissä VPN-tunneleissa, on IPv6:n perusosa, joka on tarjolla kaikille yhteyksille ja jota kaikki IPv6-yhteensopivat laitteet ja järjestelmät tukevat. IPv6:n laaja käyttöönotto tekee man-in-the-middle-hyökkäyksistä näin ollen huomattavasti hankalampia. [13.]

IPv6 tukee myös tietoturvallisempaa nimenpäättelyä. Secure Neighbor Discovery (SEND) -protokolla mahdollistaa yhteyttä otettaessa kryptografisen vahvistuksen, että laite on se laite, joka se väittää olevansa. Tämä vaikeuttaa nimipohjaisia hyökkäyksiä. Vaikka tämä ei korvaa sovellus- tai palvelutason varmistusta, se tarjoaa yhteyksille parannetun luottotason. IPv4:n yli hyökkääjän on kohtuullisen helppo uudelleenohjata liikennettä kahden todellisen laitteen välillä ja manipuloida tai tutkia liikennettä, IPv6 puolestaan tekee tämän hyvin vaikeaksi. [13.]

Lisätty tietoturva riippuu täysin IPv6:n kunnollisesta suunnittelusta ja käyttöönotosta. IPv6:n monimutkaisempi ja joustavampi infrastruktuuri aiheuttaa suuremman työmäärän, mutta oikein konfiguroituna IPv6-verkot ovat huomattavasti tietoturvallisempia kuin aikaisemmat verkot. [13.]

6.2 IPv6:n ongelmia

Tähän mennessä verkkorikolliset eivät ole kiinnittäneet huomiota IPv6:een. Siitä huolimatta on jo törmätty laajalle levinneisiin haittaohjelmiin, jotka hyödyntävät IPv6-pohjaisia komenna ja hallitse (command-and-control) -kykyjä. Väärinkäytöt lisääntyvät tilanteissa, joissa esimerkiksi palvelin mahdollistaa IPv6:n käytön, mutta palomuuri ei tarjoa samaa tukea. [13.]

Asianmukainen käyttöönotto ja konfigurointi on todellinen ongelma. Ongelmia ilmenee varmasti, jos IPv6:tta yritetään ottaa käyttöön samalla tavalla

kuin IPv4:ää. Ylläpitäjien tulee ottaa käyttöön uusi lähetymistapa verkkoihin, vianselvitykseen, kofigurointiin ja tietoturvalokien valvontaan. [13.]

Tällä hetkellä siirtyminen suoraan IPv4:stä IPv6:een ei ole mahdollista, joten teknologia täytyy ottaa käyttöön osittain. Ipv6:n kuljettamiseen IPv4:n yli joudutaan käyttämään tunnelointiteknologioita, jotka ovat myös mahdollinen tietoturvariski. [13.]

6.3 IPv6:een siirtymisessä huomioitavaa

IPv6:een siirtyminen tulee tapahtumaan jossain vaiheessa. Useat palvelut ovat jo tarjolla IPv6:n kautta ja suuret palveluntarjoajat, operaattorit ja verkkopalvelut ovat aktiivisesti siirtymässä käyttämään IPv6:tta. Mobiilioperaattorit ovat yrittäneet saada IPv6:tta implementoitua laajemmin tukeakseen nopeita verkkojaan. Yritysten tulisi tehdä käyttöönottosuunnitelma IPv6:n käyttöönottamiseksi, mikäli yrityksellä ei sellaista vielä ole. Suunnittelussa ja konfiguroinnissa tulee kuitenkin ottaa huomioon muutamia seikkoja siirtymistä varten. [13.]

Ipv4:ää ja IPv6:tta täytyy aluksi käyttää rinnakkain. Tämän rinnakkain käytön aikana tulisi olla varovainen tunneloinnin käytössä. Tunnelit tarjoavat tärkeitä yhteyksiä IPv4- ja IPv6-komponenttien välillä ja mahdollistavat osittaisen Ipv6:n käytön verkossa, joka pohjautuu edelleen IPv4-teknologiaan, mutta ne aiheuttavat myös tietoturvariskejä. Tunneleiden käyttö tulisi pitää minimissä ja niitä tulisi käyttää vain, jos se on pakollista. Työkalujen, jotka tajoavat automaattista tunnelointia, asetukset tulisi tarkistaa huolellisesti. Liikenteen tunnelointi myös vaikeuttaa tietoturvajärjestelmien kykyä tunnistaa hyökkäyksiä. [13.]

IPv6-verkon malli on hyvin erilainen IPv4-verkkon nähden, joten olemassa olevien asetusten kopioiminen ei tarjoa ihanteellista ratkaisua. Verkot tulisi suunnitella kokonaan uudelleen, jotta IPv6:sta saadaan suurin hyöty. Verkon arkkitehtuuria tulisi huomioida sekä Internet-linkin että lähiverkon osalta. [13.]

Koko verkkoinfrastruktuurin tulisi olla IPv6-yhteensopiva ja ajantasainen. Kytkimiin ja reitittimiin tulisi päivittää viimeisimmät laiteohjelmisto- ja ohjelmistoversiot. IPv6 saattaa tuoda mukanaan riskejä protokollatasolla ja van-

hanaikainen verkkoinfrastruktuuri saattaa jättää laitteet haavoittuviksi hyökkäyksille. [13.]

Työasemien tietoturvassa pitäisi olla käytössä tiedon hävikinesto ja verkkotietoturva. Myös palomuurit voi joutua konfiguroimaan uudelleen. [13.]

IPv6:tta ei saisi mahdollistaa ennen kuin siihen on täysi valmius. Useat sovellusalustat tarjoavat IPv6:tta vakiona, mutta nämä ominaisuudet tulisi ottaa pois päältä, kunnes IPv6 on kunnolla konfiguroitu. Monet nykyiset palomuurit keskittyvät vain IPv4:ään, eivätkä suodata IPv6-liikennettä ollenkaan, mikä altistaa järjestelmän tietoturvariskeille. Tarpeettomat palvelut tulisi kytkeä pois päältä ja tarvittavien palveluiden käyttämät portit ja protokollat tulisi tarkistaa huolellisesti. IPv6:n käyttäminen oletuksena saattaa mahdollistaa hyökkäykset, jotka ohittavat tietoturvaohjaukset. [13.]

7 KÄYTTÖÖNOTTOSUUNNITELMAN LAATIMINEN

Yrityksellä on käytössään valmiita pohjia muutoksien käyttöönottosuunnitelmien tekemistä varten, joten tällaista valmista pohjaa käytettiin myös IPv6-käyttöönottosuunnitelman laatimiseen. Suunnitelman osiot on kuvattu tarkemmin seuraavissa luvuissa.

7.1 Tehtävänanto

Muutoksen tavoitteet

Aluksi suunnitelmaan tuli kuvata muutoksen tavoitteet, eli suunnitelman tarkoitus sekä suunnitelman toteutuksesta saavutettava lopputulos.

Perustelut

Tähän osioon piti kuvailla ja listata syyt miksi muutos pitäisi toteuttaa. Lisäksi osioon tuli kuvata mitä lisäarvoa suunnitelman toteuttamisella on nykytilanteeseen nähden.

Suunnittelu

Suunnitelman yleinen aikataulutus piti mainita, eli arvioida milloin suunnitelma tullaan toteuttamaan.

Viitedokumentit

Lisäksi suunnitelmaan piti listata kaikki erilliset dokumentit, joita tarvitaan suunnitelman toteuttamiseksi sekä ilmoittaa kyseisten dokumenttien sijainti.

7.2 Lähestymistapa

Toimenpidekohtainen suunnitelma

Lyhyt yleiskuvaus suunnitelman vaatimista toimenpiteistä. Toimenpiteet kuvataan yksityiskohtaisemmin kohdassa toimenpiteiden ja resurssien suunnittelu.

Riskianalyysi

Kohtaan listattiin muutokseen liittyvät riskit sekä haittojen minimoimiseksi suoritettavat toimenpiteet, mikäli toteutuksessa havaitaan ongelmia. Riskeihin lueteltiin kaikki kohdat, jotka voivat mennä väärin, mikäli muutosta ei toteuteta oikein. Lisäksi piti kuvata vaikutukset järjestelmien ja palveluiden tavoitettavuuteen. Riskien ilmaantumisen mahdollisuudet tuli arvioida asteikolla: korkea, keskinkertainen, matala. Lisäksi jokaiselle riskille tuli määritellä toimenpiteet, jotka ongelmien sattuessa minimoivat niiden vaikutukset.

Vaikutusten analysointi

Tähän osioon piti arvioida käyttöönoton vaikutukset käyttäjäympäristöön, ylläpitoympäristöön, muihin järjestelmiin sekä turvallisuuteen.

Perääntymisen toimintatavat

Tähän kappaleeseen piti määritellä mitä tulee tehdä, jos käyttöönotto ei suju toivotulla tavalla. Piti määritellä, kuinka voidaan varmistua siitä, että käyttöönotto ei ole onnistunut ja kuka tämän voi varmistaa. Tähän kappaleeseen piti myös listata toimenpiteet, joilla aikaisemmat vaiheet voidaan palauttaa sekä nimetä henkilö, joka tekee päätöksen palautuksesta. Palautuksen vaatima aikataulu tuli myös arvioida tähän kappaleeseen.

Tunnetut ongelmat

Suunnitelmaan piti myös kirjoittaa kaikki etukäteen tiedossa olevat ongelmat ja niiden käsittely. Myös tiedossa olevat aikaisemmin käsitellyt ongelmat ovat oleellisia suunnitelman kannalta.

Dokumentaatio

Tähän suunnitelman osaan listattiin sellaiset dokumentit, joihin täytyy tehdä muutoksia käyttöönoton takia sekä mahdolliset uudet dokumentit, joita suunnitelman käyttöönottamisesta johtuen pitää luoda.

Seuranta

Suunnitelman kannalta oleellista oli myös miettiä miten toimitaan silloin kun käyttöönotto on tehty ongelmitta. Tehtävänä oli miettiä miten onnistuneen käyttöönoton jälkeen seurataan muutoksen vaikutuksia, ja mitä tahoja pitää informoida muutoksen jälkeen.

Konfiguraationhallinta

Tämä osio liittyy laitetietokannan ylläpitoon. Laitteiden osalta piti myös kuvata, mitkä ominaisuudet tai arvot muuttuvat käyttöönoton jälkeen, jotta uudet arvot voidaan lisätä laitetietokantaan.

7.3 Suunnittelu

Toimenpiteiden ja resurssien suunnittelu

Tähän osioon piti kuvailla suunnitelman käyttöönoton vaatimia resursseja. Tarkoituksena oli laatia yksityiskohtainen suunnitelma jokaisesta käyttöönoton vaatimasta toimenpiteestä ja miettiä, kuinka paljon aikaa kukin toimenpide vaatii sekä minkä tasoista asiantuntijuutta vaaditaan kyseisen toimenpiteen suorittamiseen.

Testaussuunnitelma ennen käyttöönottoa

Tähän suunnitelman osioon oli tarkoitus kuvata, kuinka suunnitelmaa testataan ennen käyttöönottoa, jotta päästään haluttuun lopputulokseen. Testaus on yritysympäristöissä erityisen tärkeää, jotta voidaan todentaa suunnitelman toiminnallisuudet ja uuden konfiguraation toiminta ennen käyttöönottoa

tuotantoympäristössä. Samalla saadaan selville onko jotain jäänyt huomaamatta suunnittelussa. Testauksella pyritään myös havaitsemaan mahdolliset ongelmat, joita ei ole tullut esille suunnitteluvaiheessa.

Testaussuunnitelma käyttöönoton jälkeen

Tähän osioon piti määritellä käyttöönoton jälkeen tehtävät testaukset, joilla tarkastetaan käyttöönoton onnistuminen ja varmistetaan, että haluttu lopputulos on saavutettu.

Kommunikaatiosuunnitelma

Suunnitelman yhtenä osana oli miettiä, mitä tietoja pitää kertoa suunnitelmaan liittyen ja milloin tarvittavista asioista tiedotetaan. Tehtävänä oli myös suunnitella kuka hoitaa tiedotuksen ja mille tahoille suunnitelmasta pitää lähettää tietoa.

7.4 Liitteet ja lisäykset

Suunnitelman viimeinen osio on tarkoitettu ylimääräisten suunnitelmien, kuten esimerkiksi teknisen suunnitelman kuvailemiseen. Tähän osioon oli tarkoitus liittää kaikki suunnitelman toteutuksessa vielä mahdollisesti tarvittavat tiedot, joita ei ole kerrottu suunnitelman aikaisemmissa osioissa.

8 SUUNNITELMAN TOTEUTUS

Käyttöönottosuunnitelman toteutus ei kuulunut tämän työn tekemiseen. Suunnitelman toteuttavat yrityksen verkko-osaston arkkitehtuuripuolen asiantuntijat yhdessä ylläpitopuolen asiantuntijoiden kanssa.

Suunnitelman laatimiseen ei kuulunut uusien laitekonfiguraatioiden luominen, eikä yritykselle varatun IPv6-osoitelohkon aliverkotus. Näistä tehtävistä vastaavat suunnitelman toteutuksessa mukana olevat verkko-asiantuntijat.

Suunnitelmassa esitetyt muutokset yrityksen laitekantaan ovat vain ehdotuksia. Viime kädessä päätöksen laitekannan uusimisesta tekee verkko-osaston esimies yhdessä käyttöönottosuunnitelman toteutuksesta vastaavan projektipäällikön kanssa.

9 YHTEENVETO

Tässä insinöörityössä luotiin yrityksen käyttöön suunnitelma IPv6-teknologian käyttöönottoa varten.

Työ aloitettiin määrittelemällä, mitä taustatietoja vaaditaan suunnitelman kirjoittamiseen. Tämän jälkeen aloitettiin taustatietojen kerääminen. Ensimmäisenä kartoitettiin laitteet, joiden IPv6-yhteensopivuutta piti tutkia. Laitteista kerättiin tarvittavat malli- ja versiotiedot, jonka jälkeen niiden IPv6-yhteensopivuutta lähdettiin tutkimaan.

Laitteiden IPv6-yhteensopivuustietoja etsittiin Internetistä laitevalmistajien sivuilta. Kun yhteensopivuustiedot oli saatu tarkistettua, aloitettiin käyttöönottosuunnitelman kirjoittaminen. Suunnitelma kirjoitettiin valmiille pohjalle noudattamalla siinä valmiiksi olevaa ohjeistusta.

Työn tuloksena saatiin yritykselle suunnitelma IPv6-teknologian käyttöönotosta. Suunnitelman toteuttavat yrityksen verkko-osaston asiantuntijat, jotka myös tekevät suunnitelman toteuttamiseksi tarvittavat laitekonfiguraatiot ja yrityksen käyttöön varatun IPv6-osoitelohkon aliverkotuksen. Suunnitelmassa ehdotettiin, että käyttöönotto tapahtuisi vasta, kun Cisco Nexus N7K-C7010 -kytkimille on saatavissa IPv6-tuki. Suunnitelmassa otettiin myös huomioon mahdollisuus, että kyseiset laitteet korvattaisiin sellaisilla kytkimillä, joille IPv6-tuki oli jo valmiiksi riittävällä tasolla.

VIITELUETTELO

[1] Pete Loshin. 2004. *IPv6 Theory, Protocol and Practice.* Morgan Kaufmann Publishers, San Francisco, California.

[2] Understanding IP Addressing. [Verkkodokumentti]. [Viitattu 31.8.2011]. Saatavissa: http://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing?searchterm=IPv6+network+prefixes.

[3] Internet Protocol, Version 6 (IPv6) Specification. [Verkkodokumentti]. Joulukuu 1998 [Viitattu 18.4.2014]. Saatavissa: https://tools.ietf.org/html/rfc2460.

[4] About RIPE. [Verkkodokumentti]. [Viitattu 21.1.2011]. Saatavissa: http://ripe.net/ripe/about.html.

[5] The history of RIPE. [Verkkodokumentti]. [Viitattu 21.1.2011]. Saatavissa: http://ripe.net/ripe/history.html.

[6] RIPE Terms of Reference. [Verkkodokumentti]. 29.11.1989 [Viitattu 21.1.2011]. Saatavissa: http://ripe.net/ripe/docs/ripe-001.

[7] About RIPE Meetings. [Verkkodokumentti]. [Viitattu 21.1.2011]. Saatavissa: http://www.ripe.net/ripe/meetings/ripe-meetings.

[8] RIPE NCC - What we do. [Verkkodokumentti]. [Viitattu 21.1.2011]. Saatavissa: http://www.ripe.net/lir-services/ncc/functions.

[9] IPv6 Address Allocation and Assignment Policy. [Verkkodokumentti]. 9/2009 [Viitattu 7.1.2011]. Saatavissa: http://www.ripe.net/ripe/docs/ripe-512.

[10] Contractual Requirements for Provider Independent Resource Holders in the RIPE NCC Service Region. [Verkkodokumentti]. Helmikuu 2009 [Viitattu 31.8.2011]. Saatavissa: http://www.ripe.net/ripe/docs/ripe-452.

[11] Multihoming - Wikipedia, the free encyclopedia. [Verkkodokumentti]. 28.7.2011 [Viitattu 5.9.2011]. Saatavissa: http://en.wikipedia.org/wiki/Multihoming.

[12] IPv6 Node Requirements. [Verkkodokumentti]. Joulukuu 2011 [Viitattu 20.4.2014] Saatavissa: https://tools.ietf.org/html/rfc6434.

[13] Why IPv6 Matters for Your Security. [Verkkodokumentti]. [Viitattu 5.5.2014] Saatavissa: http://www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6.aspx.

RIPE NCC

Document ID: ripe-467
Date: May 2009

```
% IPv6 PI Assignment Request Form

% RIPE NCC members (LIRs) and Direct Assignment Users can use this form
% to request an IPv6 PI assignment. Please see
% Supporting Notes for the IPv6 Provider Independent (PI) Assignment
% Request Form for instructions on how to complete this form.
% http://ripe.net/ripe/docs/ipv6-pi-support.html
%
%
% Please note that the End User should have a signed "End User
% Assignment Agreement" with either the sponsoring LIR or the RIPE NCC.


#[GENERAL INFORMATION]#
%
% Please add your RegID.

request-type: pi-ipv6
form-version: 1.0
x-ncc-regid:

#[ADDRESS SPACE USER]#
%
% Who will use the requested address space?

legal-organisation-name: Capgemini Finland Oy
organisation-location: Espoo, FI
website-if-available: http://www.fi.capgemini.com/

% Is this request being sent by a sponsoring LIR on behalf of
% an End User? (Yes/No)

end-user-of-sponsoring-lir: Yes

% If yes, please attach a copy of the signed "End User Assignment
% Agreement" and the company registration papers of the End User.

% Also please confirm that the "End User Assignment Agreement"
% contains all of the elements listed in paragraph 2.0 of "Contractual
% Requirements for Provider Independent Resource Holders in the
% RIPE NCC Service Region".(Yes/No)

confirmation: Yes

% Does this End user already have address space that can be used for
% this assignment? (yes/no)

space-available: No

#[INITIAL INFORMATION]#
%
% Why is PI address space required rather than PA address space?
```

```
why-pi: We are planning of a Multihomed Internet access implementation,
Multihomed solutions should be operational by the end of year 2011.

% Is the End User requesting extra address space for routing and/or
% administrative reasons? (Yes/No)

routing-reasons: No

% Is the End User aware of the consequences and disadvantages
% of PI address space? (Yes/No)

Confirmation: Yes

#[ADDRESSING PLAN]#
%
% When will the End User use this IPv6 PI assignment?
%
%       Subnet       Within     Within   Within
%       size (/nn)   3 months   1 year   2 years   Purpose

subnet: /48                      X                 Office LAN

number-of-subnets: 1


% Will the End User return any address space?

address-space-returned: No

#[EQUIPMENT DESCRIPTION]#
%
% What equipment will be used and how will it use the requested
% address space?

equipment-name: Switches, Routers, Firewalls
manufacturer-name: Cisco, Juniper
model-number: n/a
other-data: multiple devices

equipment-name: Servers, Workstations
manufacturer-name: Multiple manufacturers
model-number: n/a
other-data: multiple devices



#[NETWORK DESCRIPTION]#
%
% Please add more information if you think it will help us understand
% this request. If the End User is requesting more than a /48 please
% explain why:

#[PEERING CONTACTS]#
%
% Please list the Autonomous System numbers and email contact addresses
% of the peering partners for the requested IPv6 PI assignment.

peering:    ELISA-MNT
peering:    RH8196-RIPE
peering:    Riku.Hakkarainen@elisa.fi
```

```
peering:    AS 719

peering:    TSF DATANET-AS
peering:    lir@sonera.com
peering:    AS 5515

#[NETWORK DIAGRAM]#
%
% You can attach a network diagram or other supporting documentation,
% particularly if the End User is requesting more than /48.
%
% Have you attached any files/documents to this request? (Yes/No)

file-attached: Yes


#[DATABASE TEMPLATE(S)]#
%
% Please complete all of the fields below.

inet6num:
netname:        CAP-IPV6-NET
descr:          Capgemini Finland Oy
country:        FI
org:            ORG-CF3-RIPE
admin-c:        CH581-RIPE
tech-c:         CH581-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-lower:      RIPE-NCC-END-MNT
mnt-by:         CAP-FIN-MNT
mnt-routes:     CAP-FIN-MNT
mnt-domains:    CAP-FIN-MNT
changed:        hostmaster@ripe.net
source:         RIPE



#[END of REQUEST]#

Best Regards,

XXX XXX, Capgemini Finland Oy
```