Juuso Lehtonen

IPv6-verkon suunnittelu ja implementointi yritysverkoissa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

16.4.2014

Metropolia

Tekijä Otsikko Sivumäärä Aika	Juuso Lehtonen IPv6-verkon suunnittelu ja implementointi yritysverkoissa 37 sivua + 1 liitettä 16.4.2014
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaajat	lehtori Erik Pätynen tietoliikennekonsultti Matti Nikula

Työ tehtiin Cygate Oy:lle. Työn aiheena oli IPv6 (Internet protokolla versio 6) -verkon suunnittelu ja toteutus yritysverkoissa. IPv4 (Internet protokolla versio 4) -osoitteiden loputtua, on todennäköistä, että tulevaisuudessa Cygaten asiakkaat tarvitsevat asiantuntijoita päivittämään omia verkkojaan IPv6-toiminnallisuuteen. Näin ollen on Cygaten kannalta tärkeää omata kokemusta IPv6-toteutuksesta.

Työssä käytiin aluksi läpi IPv6:n keskeiset ominaisuudet, minkä jälkeen perusteltiin IPv6-käyttöönoton hyödyt ja tarve pohjautuen edellä läpi käytyihin asioihin. Kun IPv6:n perusteet ja syyt toteutukselle saatiin kuvattua, siirryttiin tarkemmin tutkimaan käyttöönoton kannalta tarpeellisia siirtymämenetelmiä. Lopuksi kuvattiin käyttöönotossa tarvittavan suunnitelman vaiheet.

Työn käytännön osiona päivitettiin osa Cygaten toimistoverkosta IPv6:een. Suunnitelma päivitykselle pohjautui teoriaosuudessa kuvattuun prosessiin. Käytännön osion päämäärä oli saada aikaan perustoiminnallisuus IPv6:lla, niin että toimistoverkosta oli mahdollista liikennöidä internetiin päin pelkästään IPv6:n avulla. Teorian ja käytännön pohjalta haluttiin lisäksi saada aikaan dokumentti, jonka pohjalta olisi mahdollista kuvata Cygaten asiakkaille IPv6-käyttöönotossa tarvittavat vaiheet ja tehdä heidän tarpeitaan vastaava muutossuunnitelma.

Käytännön osiota tehtäessä tuli ilmi, ettei täydellinen dynaaminen IPv6-toimivuus ole vielä mahdollinen ilman kattavaa testausta. Tästä huolimatta työ loi pohjan ja näkymän seuraavaksi tehtäville IPv6-päivityksille toimistoverkossa.

Tulokseksi saatiin toimiva yhteys toimistoverkosta internetiin, kuten oli suunniteltu sekä tarvittava dokumentti Cygaten asiakkaita varten. Työ onnistui näin ollen suunnitellusti, eikä huomattavia ongelmia määritellyn tavoitteen suhteen ilmennyt.

Avainsanat	IPv6, IPv4, IPv6-siirtymä, siirtymäsuunnitelma, IPv6-muutossunnitelma

Author Title Number of Pages Date	Juuso Lehtonen Planning and implementing IPv6 network in corporation environment 37 pages + 1 appendix 16 April 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructors	Matti Nikula, Senior Consultant Erik Pätynen, Senior Lecturer

This thesis was made for Cygate Oy. The topic was the implementation and planning of an IPv6 network in corporation environment. It is likely that in the future the customers of Cygate will need experts to help them upgrade their existing IPv4 networks into IPv6. Therefore, it is important for Cygate to have experience of such implementations. Hence the goal of the project described in this thesis was to get familiar with IPv6 and partly implement it for Cygate and then create a document for customers, which could work as a core resource while planning IPv6.

First, the most relevant features of IPv6 were investigated, which created a basis for the explanation of why IPv6 is needed and why it should be implemented. After describing the basics of IPv6 and reasons for the implementation, a more specific look was taken into the necessary transition mechanisms needed for the deployment. Finally, steps for creating a deployment plan were described. This deployment plan was then used in the project for establishing basic IPv6 connectivity from Cygate's own office network to the internet.

As a result, a working IPv6 connection to the internet was achieved and the necessary document for the customers of Cygate was created to help them with future implementations. In conclusion, this project created a starting point for the future IPv6 upgrades for both Cygate and its customers and therefore reached its goal.

Keywords	IPv6, IPv4, IPv6 transition, transition plan

Sisällys

Lyhenteet

BGP	*Border Gateway Protocol*. Reititysprotokolla.
CE	*Customer Edge*. Asiakkaan reunareititin.
DHCP	*Dynamic Host Configuration Protocol*. Protokolla, jonka avulla päätelaitteille voidaan jakaa automaattisesti IP-osoitteita.
DNS	*Domain Name System*. Nimipalvelu, jonka avulla IP-osoitteita muutetaan nimiksi, ja toisinpäin.
ICMP	*Internet Control Message Protocol*. Protokolla, joka tarjoaa keinon kontrolloida paketinvälitystä verkon laitteiden välillä.
IP	*Internet Protocol*. Verkkokerroksen protokolla, joka tarjoaa keinon välittää dataa tietyin osoittein määriteltyjen lähteiden ja kohteiden välillä.
IPAM	*IP Address Management*. IP-osoitteiden hallintapalvelu.
ISATAP	*Intra-Site Automatic Tunnel Addressing Protocol*. Tunnelointimekanismi.
KB	*Knowledge Base*. Laitevalmistajilta usein löytyvät ns. tietämyskanta.
NAT-PT	*Network Address Translation - Protocol Translation*. Käännösmekanismi, jota voidaan käyttää IPv6:n käyttöönotossa.
NAT64	*Network Address Translation 64*. Käännösmekanismi, jota voidaan käyttää IPv6:n käyttöönotossa.
PE	*Provider Edge*. Palveluntarjoajan reunareititin.
RFC	*Request for comments.* RFC:t ovat dokumentteja, joissa julkaistaan internetiä koskevia standardeja.
RIPE	*The Réseaux IP Européens Network Coordination Centre*. Euroopan alueella toimiva rekisterivirasto, joka mm. jakaa IP-osoitteita.

RIR	*Regional Internet Registry*. Alueellinen reskiterivirasto. Katso RIPE.
SLAAC	*Stateless Address Autoconfiguration*. SLAAC:n avulla päätelaitteet muodostavat itselleen IPv6-osoitteen.
TB	*Tunnel Broker*. Tunnelointimekanismi, jota voidaan käyttää IPv6:n käyttöönotossa.
TEREDO	Tunnelointimekanismi, jota voidaan käyttää IPv6:n käyttöönotossa.

1 Johdanto

Nykyiset tietoverkot perustuvat pääosin IPv4:ään eli internet protokolla versio 4:ään. IPv4 on suunniteltu kuljettamaan datapaketteja tietoverkoissa eri laitteiden välillä. Se määriteltiin ensimmäisen kerran RFC791:ssa (Request for Comments), jonka mukaan internet protokolla tarjoaa keinon välittää dataa tietyin osoittein määriteltyjen lähteiden ja kohteiden välillä. RFC:t ovat dokumentteja, joissa julkaistaan internetiä koskevia standardeja. [1.]

Kyseiset lähde- ja kohdeosoitteet sisältyvät IPv4-paketin otsakkeeseen muiden IPv4-protokollan käyttämien tietojen ohella. Osoitteet ovat 32-bittisiä, joten niiden tarjoama osoiteavaruus on yhteensä 2^32, mikä tarkoittaa noin 4,2 miljardia osoitetta. Jokainen verkkolaite tarvitsee verkossa toimiakseen oman uniikin IP-osoitteen.

Internetyhteyteen kykenevien laitteiden lisääntyessä, ja maailman populaation kasvaessa kyseinen osoiteavaruus on käynyt pieneksi. Euroopassa IPv4-osoitteet julistettiin käytännössä loppuneiksi 14.9.2012 [2; 3].

Osoitteiden loppuminen on tärkein syy IPv6-protokollan kehittämiseen. Osoitteiden lisäämisen ohella IPv6:tta on luonnollisesti pyritty kehittämään tietoturvallisempaan suuntaan ja paikkaamaan aiemmassa versiossa havaittuja puutteita.

Insinöörityön tarkoitus on tutustua IPv6-protokollan implementointiin yritysympäristössä, keskittyen kuitenkin toimistoverkon toteuttamiseen. Työssä pyritään kuvaamaan IPv6:n käyttöönoton kannalta huomionarvoiset seikat.

Insinöörityö toteutetaan Cygate Oy:lle, joka on tietoturvallisten verkkoratkaisujen johtava tomittaja Pohjoismaissa. Cygaten tomialaan kuuluu verkkoratkaisujen ylläpito, asennus ja suunnittelu. Cygate työllistää noin 500 työntekijää.

Työn käytännön osiona päivitetään osa Cygaten toimistoverkosta IPv6:een. Toteutuksen yhteydessä pyritään samalla kertaa tuottamaan Cygaten asiakkaille esitettävä dokumentti, jonka avulla voidaan perustella IPv6:n tarpeellisuus, sekä mudostaa alustava suunnitelma toteutuksesta asiakkaan verkkoympäristössä.

2 IPv6-protokolla

IPv6-protokolla on yksinkertaisesti uudistettu versio IPv4:stä. IPv6 toimii samaan tapaan verkkotasolla, ja sen tarkoitus on edelleen alkuperäisen RFC791:n mukainen, eli siirtää dataa laitteelta toiselle määriteltyjen lähde- ja kohdeosoitteiden mukaisesti [1]. IPv6 on määritelty jo vuonna 1998 RFC2460:ssa. [4.]

Tärkeimmät uudistukset IPv4:ään nähden ovat laajennettu osoiteavaruus, otsakkeen yksinkertaistaminen, tuki laajennuksille ja lisäoptioille, sekä datavirran ns. merkitsemismahdollisuus [4]. Tässä luvussa pyritään kuvaamaan nämä ominaisuudet lyhyesti, tämän työn kannalta keskeisiä asioita silmällä pitäen.

2.1 IPv6-osoitteet

IPv6:ssa osoiteavaruutta IPv4:ään nähden on laajennettu. Laajennus on huomattava, sillä siinä missä IPv4:n osoitteet rajoittuvat 32:een bittiin ja tarjoavat n. 4,2 miljardia osoitetta yhteensä, IPv6 tarjoaa 128-bittisiä osoitteita, mikä riittää tarjoamaan jokaiselle yksittäiselle elävälle ihmiselle biljoonia osoitteita.

IPv6-osoitteiden esitys

IPv6-osoitteet esitetään kahdeksassa neljän heksadesimaaliluvun, eli 16 bitin lohkossa. Lohkot erotetaan toisistaan kaksoispisteillä. Osoitteet eivät ole merkkikokoriippuvaisia.

Koska IPv6-osoitteiden kirjoittaminen on 32-merkkisen esitystapansa tähden epäkäytännöllistä, on kehitetty kirjoitusta helpottavia sääntöjä:

- Jokaisen lohkon aloittavat nollat voidaan jättää huomiotta.

- Peräkkäiset nollat voidaan tiivistää tuplakaksoispisteellä, kuitenkin vain kerran yhtä osoitetta kohden.

Esimerkiksi osoite 1234:0000:0000:43FF:001C:0000:1111:AAAA voidaan kirjoittaa muotoon 1234::43FF:1C:0:1111:AAAA. [5, s. 700.]

IPv6-osoitetyypit

IPv6-osoitteista puhuttaessa on ymmärrettävä, että IPv6-osoitteita ei määritetä verkon laitteille (node), kuten reitittimille, vaan verkkoliitynnöille (interfaces).

IPv6-osoitteita on kolmenlaisia: unicast, multicast ja anycast. Unicast-osoite on yksittäisen verkkoliitynnän osoite. Unicast-osoitteeseen lähetetyt paketit reititetään näin ollen vain sille liitynnälle, jolle osoite on määritelty. Unicast-osoitteita on monen tyyppisiä, tärkeimpänä ns. globaali unicast osoite (global unicast) ja paikallinen linkkiosoite (link-local).

Globaali unicast osoite on verrannollinen IPv4:n julkisiin osoitteisiin. Osoite koostuu pääosin kolmesta osasta: Globaalista reitityspredfiksistä, aliverkon tunnisteesta ja verkkoliitynnän tunnisteesta. Globaaliin prefiksin koko on 48 bittiä, ja siihen sisältyy mm. palveluntarjoajan prefiksi. Tätä seuraavat mainitut aliverkon tunniste ja verkkoliitynnän tunniste, joiden koot ovat vastaavasti 16 ja 64 bittiä. Aliverkon tunnisteen avulla organisaatiot voivat luoda oman osoitehierarkiansa. [5, s. 705; 11.]

Paikallinen linkkiosoite luodaan jokaiselle IPv6 verkkoliitynnälle automaattisesti. Paikallisilla linkkiosoitteilla on valmiiksi määritetty prefiksi FE80::/10, jota seuraa 64-bittinen verkkoliitynnän tunniste. Nimensä mukaisesti paikalliset linkkiosoitteet toimivat lokaalisti linkeissä, ja niitä käytetään mm. automaattiseen osoitteen konfigurointiin ja naapurien löytämiseen.

Multicast-osoitteet määrittävät useita verkkoliityntöjä kerralla. Multicast-osoitteeseen kohdistetut paketit lähetetään kaikille multicast-ryhmään määritellyille liitynnöille. Yksi verkkoliityntä voi kuulua moneen eri multicast-ryhmään.

Anycast-osoite on tarkoitettu multicastin tavoin joukolle verkkoliityntöjä, mutta toisin kuin multicastissa, anycast-osoitteisiin kohdistetut paketit lähetetään vain lähimpänä sijaitsevalle liitynnälle. Lähin anycast-joukon liityntä määrittyy käytössä olevan reititysprotokollan mukaan. Käytännössä Anycast-osoite on globaali unicast-osoite, joka määritetään yhden verkkoliitynnän sijaan usealle. Anycast-osoite ei voi olla lähdeosoite. [5, s. 711; 6; 7; 8.]

IPv6:n ominaisuuksiin kuuluu, että yhdellä liitynnällä voi olla useita osoitteita, poislukien paikallinen linkkiosoite, joita liitynnällä voi olla vain yksi.

IPv6-osoitteiden automaattinen konfigurointi

IPv4:ssä käytettyjen manuaalisen osoitteen konfiguroinnin, sekä DHCP:n (Dynamic Host Configuration Protocol) lisäksi on IPv6:ssa toteutettu mahdollisuus niin sanottuun tilattomaan osoitteen autoconfigurointiin (stateless Address Autoconfiguration, SLAAC). SLAAC:n avulla päätelaitteet muodostavat itselleen IPv6-osoitteen käyttämällä reitittimien multicastilla mainostamaa paikallisen verkon prefiksiä, sekä omaa verkkoliitynnän tunnistettaan. Verkkoliitynnän tunniste on yleensä EUI-64 formaattia, mikä tarkoittaa sen muodostuneen laitteen 48-bittisestä MAC-osoitteesta ja siihen lisätystä FFFE-heksadesimaaliarvosta. SLAAC hyödyntää viestimiseen ICMPv6-protokollaa, joka on kuvattu lyhyesti luvussa 2.4. [5, s. 724.]

2.2 IPv6-datapaketin otsake

IPv6-protokollassa datapaketin otsakemalli koostuu kahdeksasta osiosta. Näitä ovat versio, liikenneluokka, vuon leima, tietosisällön pituus, seuraava otsake, elinaika, sekä lähde- ja kohdeosoite. Näiden lisäksi tulevat mahdolliset laajennusotsakkeet. Taulukossa 1 on lyhyesti kuvattu jokaisen osion tarkoitus.

Taulukko 1. IPv6-otsakkeen kentät.

Osio	**Koko (bit)**	**Tehtävä**
Versio	4	kertoo IP-protokollan versionumeron.
Liikenneluokka	8	pakettiin määritetään haluttu liikenneluokka pakettien mahdollista priorisointia varten.
Vuon leima	20	paketti voidaan merkitä osaksi tiettyä liikennevuota.
Tietosisällön pituus	16	kertoo paketin kuorman ja laajennusotsakkeiden yhteisen koon tavuina.
Seuraava otsake	8	kertoo perusotsakkeen jälkeisen informaation tyypin, tarkoittaen esimerkiksi TCP/UDP-pakettia, tai laajennusotsakkeita.
Elinaika	8	kertoo suurimman mahdollisen paketin hyppyjen määrän, eli sen eliniän. Jokainen reititin vähentää kentän lukua yhdellä. Kun luku 0 saavutetaan, paketti hylätään.
Lähdeosoite	128	Sisältää lähdeosoitteen.
Kohdeosoite	128	Sisältää kohdeosoitteen.

Suuri muutos datapaketin otsakkeessa verrattaessa IPv4:ään on otsakkeen yksinkertaistettu malli; kahdeksan osiota neljäntoista sijaan. Huomattavaa on muun muassa fragmentoinnin poikkeama -kentän puuttuminen. IPv6:ssa fragmentointia eivät enää suorita reitittimet, vaan käytännössä lähdelaitteen tehtävä on määrittää paketin käyttämän reitin sallima maksimikoko paketille (MTU, Maximum transmission unit).

Laajennuotsakkeita on seitsemän erilaista. Taulukossa 1 mainittu seuraava otsake kenttä kertoo arvonsa perusteella, mikä laajennusotsakkeista seuraa perusotsaketta. Mikäli laajennusotsakkeita on paketin yhteydessä monta, ne on aina esitettävä tietyssä järjestyksessä. Taulukossa 2 on lueteltuna laajennusotsaketyypit selityksineen, siinä järjestyksessä kuin niiden otsakeketjussa kuuluisi olla.

Taulukko 2. IPv6-laajennuotsakkeet

Otsake	**Tehtävä**
hop-by-hop -otsake	Jokainen reititin paketin matkalla prosessoi hop-by-hop Otsakkeen. Otsaketta voidaan käyttää mm. reititinhälytysviestien kuljettamiseen.
kohdeoptio-otsake	Otsaketta käytetään hop-by-hop -otsakkeen jälkeen ja se prosessoidaan kaikissa kohteissa, jotka reititysotsake määrittää. Otsake voi myös tulla turvaotsakkeiden jälkeen.
reititysotsake	Käytetään mm. lähdepohjaiseen reititykseen. IPv6 lähde määrittää tietyt noodit, joiden kautta paketin täytyy kulkea matkalla kohteeseensa.
paloitteluotsake	Käytetään,mikäli lähteen täytyy suorittaa paketin fragmentointia sen ollessa liian suuri reitin MTU:n nähden.
turvaotsakkeet	Toimivat IPsec:n ollessa käytössä. Käytetään autentikointiin, sekä paketin eheyden ja luotettavuuden turvaamiseksi.
protokollaotsake	Käytetään kuljetuskerroksen datan siirtoon.

Paketin kulkumatkalla olevat laitteet eivät lue useimpia laajennusotsakkeita ollenkaan. Ainoastaan hop-by-hop -otsake, joka kuljettaa muun muassa reititinhälytysviestejä, luetaan aina, jos sellainen on paketissa mukana.

2.3 Datavirran merkitseminen

Datavirran merkitsemismahdollisuus sisältyy IPv6-otsakkeen vuon leima -kenttään. Tarkoitus on nopeuttaa pakettien prosessointia leimaamalla samaan lähetykseen kuuluvat paketit, jolloin kyseiset paketit käsitellään reitittimissä samalla tapaa, ilman että niitä tarvitsee erikseen käydä läpi. Merkitseminen tapahtuu paketin lähteessä. Vuon leima sekä lähde- ja kohdeosoitteet yhdessä tekevät vuosta uniikin. On mahdollista olla monta samanaikaista vuota lähteestä kohteeseen, kuin myös samanaikaista muuta merkitsemätöntä liikennettä. Mikäli liikenne on merkitsemätöntä, vuon leima -kentän arvo on 0.

Käytännössä paketin matkalla sijaitsevat reitittimet prosessoivat vuon ensimmäisen paketin otsaketiedot, minkä jälkeen ne tallentavat tiedot välimuistiinsa, jota käytetään myöhemmin saman vuon pakettien reititykseen. [9; 10.]

2.4 Internet Control Message Protocol version 6

Internet Control Message Protocol version 6 (ICMPv6) tarjoaa nimensä mukaisesti keinon kontrolloida paketinvälitystä verkon laitteiden välillä. Mikäli pakettien prosessoinnissa tapahtuu virheitä, ICMPv6 tiedottaa siitä erityyppisillä virheviesteillä. IPv4:ssä käytetyn ICMP:n tavoin ICMPv6:een sisältyy myös ping-työkalu, jolla voidaan todeta tietyn laitteen tavoitettavuus verkkotasolla lähettämällä ICMPv6:een sisältyviä "Echo Request" ja "Echo Reply" -viestejä. [13; 14.]

Erona IPv4:n käyttämään ICMP-protokollaan on mainittava ICMPv6:n Neighbor Discovery (ND), eli naapurien etsintä. ND hyödyntää viittä erilaista ICMP-pakettityyppiä, joiden avulla pystytään muun muassa tunnistamaan samassa verkkosegementissä olevia naapureita sekä varmistamaan verkon laitteille konfiguroitujen osoitteiden ainutlaatuisuus. Naapurien etsintää käytetään myös esimerkiksi aikaisemmin mainittujen paikallisten linkkiosoitteiden selvittämiseen, sekä IPv4:n käyttämän ARP:n (Address Resolution Protocol) korvaajana. [7; 12; 15.]

2.5 Nimipalvelu ja dynaaminen osoitteiden konfigurointi

Nimipalvelu eli Domain Name System (DNS) sekä ns. dynaaminen osoitteiden konfigurointi eli Dynamic Host Configuration Protocol (DHCP) ovat molemmat IPv4:n käyttämiä protokollia. DNS muuttaa IP-osoitteita nimiksi tai toisinpäin ja DHCP jakaa IP-osoitteita automaattisesti päätelaitteille etukäteen määritellystä osoiteavaruudesta. Molemmat protokollat ovat käytössä myös IPv6:ssa. DHCP on rakennettu uudelleen ja tunnetaan nimellä DHCPv6, ja DNS:ään on määritelty tarvittavat lisäykset ja muutokset RFC3596:ssa (DNS Extensions to Support IP Version 6) [16]. Protokollien toiminnallisuus on lähes vastaava IPv4:ään nähden; DHCPv6:ssa muutos on lähinnä viestinvälityksessä – IPv4:ssä käytössä olevien broadcast-viestien sijaan käytetään IPv6:n multicastia [6]. DNS:ssä on otetty käyttöön uusi AAAA-tietuetyyppi (Resource Record Type). [17.]

3 Syyt toteuttaa IPv6 yritysverkossa

Aiemmin mainittujen ominaisuuksien vuoksi voidaan todeta tärkeimmät syyt IPv6:n käyttöönotolle: IPv4-osoitteiden loppumisen myötä IPv6-protokollaa tullaan käyttämään yhä laajemmin, mikä tarkoittaa, että yritysten on mukauduttava ja valmistauduttava ottamaan uusi protokolla vastaan. Tietysti on otettava huomioon myös oman yrityksen IPv4-osoitteiden mahdollinen loppuminen. Kun vanhat osoitteet loppuvat, on hyvä olla uusi protokolla uusine osoitteineen toimintavalmiina. Osaltaan IPv6:n käyttöönotto saattaa myös yksinkertaistaa verkonhallintaa sekä nopeuttaa reititystä muun muassa reititystaulujen koon pienentymisen ansiosta.

3.1 IPv4-osoitteiden loppuminen

Paikallisten palveluntarjoajien on tällä hetkellä vielä mahdollista hakea RIPE:ltä (The Réseaux IP Européens Network Coordination Centre) /22 -kokoisia osoiteblokkeja. Tämä kuitenkin pätee vain siinä tilanteessa, että palveluntarjoaja kykenee perustelemaan tarpeen, sekä omaa jo ennalta IPv6-osoiteavaruuden. Palveluntarjoajasta riippumattomia IPv4-osoiteavaruuksia ei enää jaeta. [26.]

Näin ollen yksittäisten yritysten on yhä vaikeampaa saada uusia IPv4-osoitteita, mikä saattaa osoittautua ongelmaksi, jos aikomuksena on esimerkiksi laajentaa tai lisätä uusia julkisia palveluita. Jos IPv4-osoitteita ei ole saatavilla, yritys ei voi toteuttaa suunnitelmiaan, mikäli sillä ei ole IPv6-toiminnallisuutta. Lisäksi tulevaisuudessa myös muiden yritysten tai organisaatioiden palvelut saattavat toimia ainoastaan IPv6:lla samaisesta syystä johtuen, jolloin kommunikointi ja mahdollinen yhteistyö näiden kanssa vaikeutuu. Mitä kauemmas tulevaisuuteen mennään, sitä todennäköisemmin myös esimerkiksi ohjelmistokehityksessä jätetään IPv4-toiminnallisuus pois, jolloin on mahdollista, että kaikilla verkkolaitteilla ei enää ole muuta kuin IPv6 käytössään.

3.2 Tehokkaampi reititys ja pakettien prosessointi

Luvussa 2 käsiteltiin useita reitityksen ja pakettien prosessoinnin kannalta huomionarvoisia asioita. Ensimmäisenä näistä on mainittava multicast-osoitteet, jotka IPv6:ssa korvaavat IPv4:ssä käytetyt broadcast osoitteet. Kun broadcastia ei ole, välttyvät useat laitteet, muun muassa kytkimet, turhilta lähetyksiltä, mikä todennäköisesti vähentää osin verkon laitteiden prosessorikuormaa. Myös mahdollisen ns. broadcast-myrskyn riski häviää, mikä lisää verkon käytettävyyttä.

Prosessointia nopeuttaa huomattavasti myös kohdassa 2.2 selitetty yksinkertaistettu otsakemalli. Lisäominaisuudet on jätetty laajennusotsakkeiden huoleksi. Laajennusotsakkeita lukevat pääosin vain lähde- ja kohdelaitteet, joten välimatkalla olevien reitittimien kuorma vähenee, ja näin ollen myös reititys on nopeampaa.

Otsakkeeseen liittyen on huomattava myös tarkistussumman puuttuminen. IPv4-protokollaa käytettäessä jokaisen paketin matkalla olevan reitittimen on laskettava uusi tarkistussumma aina, kun elinaika kentän arvo laskee. IPv6 ei käytä tarkistussummaa otsakkeessa, joten prosessointiaika vähenee.

Lisäksi kohdassa 2.3 kuvattu datavirran merkitsemismahdollisuus vähentää pakettien prosessointiaikaa yhdistämällä tietystä lähteestä tiettyyn kohteeseen meneviä paketteja yhdeksi virraksi ja käyttämällä näihin tietovirtoihin kuuluviin paketteihin samanlaista reititystä.

Suorituskykyä prosessoinnin osalta lisää myös lähdelaitteen tekemä MTU-tutkinta (MTU-discovery), minkä ansiosta datapaketit voivat kulkea tarvitsemansa reitin kokonaan ilman tarvetta paketin pirstaloinnille.

Itse reititykseen suoraan vaikuttavista tekijöistä mainitsemisen arvoinen on mahdollinen reititystaulujen koon väheneminen. Tämä näkyy erityisesti palveluntarjoajien kohdalla, sillä nämä voivat tiivistää asiakkaidensa aliverkkoja mainostumaan yhtenä verkkona internetiin päin, mikä käytännössä hyödyttää myös yrityksiä palveluntarjoajan runkoverkon toimiessa näin nopeammin. Yritykset itsekin voivat tietysti yhdistää aliverkkojensa mainostusta sisäisesti ja vähentää omien reititystaulujensa kokoa, mikä täten tehostaa myös yritysten sisäistä reititystä.

3.3 Yksinkertaisempi verkonhallinta

IPv6:ssa ei käytetä osoitteenmuunnosta (NAT, Network Address Translation) siinä mielessä, kuin se on IPv4:ssä toteutettu. IPv4:ssä osoitteenmuunnosta käytetään muuttamaan ns. sisäverkon osoitteita julkisiksi, mikä on pakollista, koska IPv4:ssä julkisia osoitteita ei ole tarpeeksi, jotta niitä riittäisi kaikille sisäverkon laitteille. Kuten todettua, IPv6:ssa osoitteita on tarpeeksi, eikä osoitteenmuunnosta näin ollen tarvita. Verkon konfigurointi ja hallinta on huomattavasti helpompaa ilman osoitemuunnoksia, joita voi nykyisellään tapahtua useaankin otteeseen paketin matkatessa paikasta A paikkaan B. NAT tosin on sisällytetty IPv6:een nimellä NAT-PT (NAT Protocol Translation), mutta sen tarkoitus on toimia transitiomekanismina IPv4:n ja IPv6:n välillä, esimerkiksi kääntämällä tarpeen tullen IPv4-osoitteita IPv6-osoitteiksi, mikä mahdollistaa kommunikoinnin eri verkkoprotokollaa käyttävien verkkojen välillä. NAT-PT:tä käsitellään tarkemmin tuonnempana.

Tärkeä elementti verkonhallintaa mietittäessä on myös luvussa 2.1 kuvattu osoitteiden autokonfiguraatio. Mikäli verkon suunnitteluvaiheessa jätetään pois DHCPv6:lla tehtävä IPv6-osoitteiden jako, ja päätetään käyttää autokonfiguraatiota, yksinkertaistuu verkon konfigurointi. Tosin tällöin osoitteiden hallinta saattaa vaikeutua, johtuen loogisuuden puutteesta osoitteiden allokoinnissa eri aliverkoissa.

3.4 Sisäänrakennettu IP Security

IP security eli IPsec on IPv4:äänkin implementoitu tietoturvaa tarjoava rajapinta [18]. Toisin kuin IPv4:ssä, IPv6:ssa IPsec on alusta asti suunniteltu osaksi protokollaa, minkä osoittavat sitä varten olemassaolevat laajennusotsakkeet IPv6-paketissa. AH- ja ESP-otsakkeet tarjoavat keinon salata IPv6 –paketin sisältö ja varmistaa sen eheys. Todellista uutta tietoturvaa sisäänrakennetut otsakkeet eivät käytännössä tuo, koska kuten edellä on mainittu, IPsec on aktiivisesti käytössä myös IPv4:ssä. Todellinen hyöty onkin todennäköisesti lähinnä varmistus siitä, että tulevissa verkkolaitteissa IPsec on aina tarjolla. Myös NAT:n häviämisen myötä täydellinen päästä päähän –yhteys eli yhteys päätelaitteiden välillä, on helpommin mahdollista salata IPsec:n avulla [18; 21].

4 Transitiomekanismit

IPv4-verkoista IPv6:een siirtymistä varten on kehitetty useita erilaisia ratkaisuja. Ne voidaan jakaa kolmeen kategoriaan: kaksoispino, tunnelointi ja käännösmekanismit.

4.1 Kaksoispino

Kaksoispino (Dual Stack) on nimensä mukaisesti tekniikka, jonka avulla verkkolaite ajaa kahta protokollapinoa samanaikaisesti. Laitteella on IPv4 ja IPv6 -reititystaulut ja verkkoliitynnöille määritetään IPv4, sekä IPv6-osoitteet. Tekniikka on käytännössä hyvin toimiva, sillä olemassa oleva IPv4-toteutus säilyttää toimivuutensa kokonaisuudessaan. Kaksoispinon avulla voidaan hitaasti edetä kohti täydellistä IPv6-toteutusta sitä mukaa, kun verkon sovellukset ja laitteet päivitetään IPv6-kelpoisiksi. Varjopuolena kaksoispino vie huomattavasti verkkolaitteen resursseja joutuessaan ylläpitämään kahden eri protokollan tarvitsemia tietoja. [5, s. 826]

Kaksoispinon toimivuus vaatii, että verkossa on IPv6:tta tukeva DNS-palvelin, jotta kumpikin protokolla kykenee muuttamaan osoitteita nimiksi, ja toisinpäin. Tapauksissa, joissa verkkolaite saa nimipalvelimelta vastauksena sekä IPv4, että IPv6 osoitteet, päättävät RFC3848:ssa kuvatut osoitteenvalinta-algoritmit mitä osoitetta käytetään.

Koska kaksoispino on transitiomekanismi, algoritmien oletuspäätös on suosia IPv6-osoitteita. Tätä politiikkaa voidaan kuitenkin tarpeen tullen muokata. [5, s. 826; 6; 17]

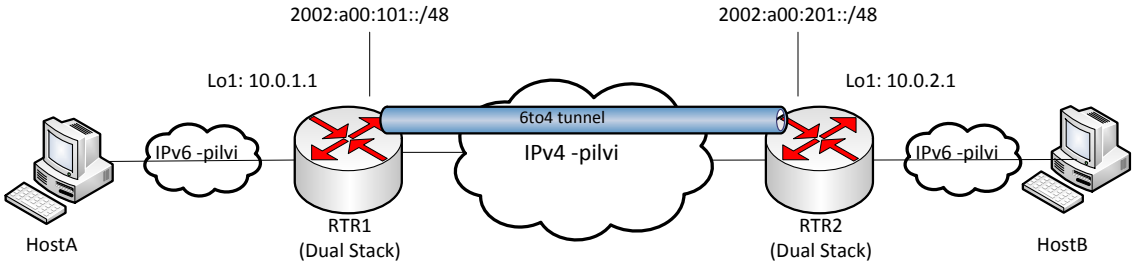
4.2 Tunnelointi

IPv4-verkoissa tunnelointia käytetään muun muassa yhdistämään yrityksen sivukonttorit sisäverkon resursseihin luomalla virtuaalinen point-to-point linkki internetin yli, eli niin sanotusti yhdistämään eri puolilla internetiä sijaitsevat IPv4-verkoista muodostuvat saarekkeet toisiinsa. Transitiomekanismina ajatus on samanlainen: Yrityksen verkkoon saattaa IPv6-toteutuksen yhteydessä jäädä ns. IPv6-saaria, koska tietyt verkon laitteet eivät tue kaksoispinoa. Kyseiset saaret voidaan yhdistää toisiinsa luomalla tunneleita, jotka sijoittavat IPv6-paketit IPv4-pakettien sisään. Tunneli muodostetaan kaksoispinoa tukevien reunalaitteiden välille. Kun IPv6-paketti saavuttaa reunalaitteen, se enkapsuloidaan ja tunneloidaan IPv4-verkon välityksellä, minkä jälkeen toinen reunalaite dekapsuloi paketin.

Tunneli voidaan muodostaa manuaalisesti, tai automaattisesti. Automaattisia tunnelointiteknologioita ovat muun muassa 6to4 ja ISATAP (Intra-Site Automatic Tunnel Addressing Protocol).

4.2.1 6to4-tunnelointi

6to4 on teknologia, joka hyödyntää IPv4-pilven reunalla olevien reitittimien IPv4-osoitteita muodostaakseen tunnelin IPv6-saarekkeiden välille. 6to4-tunnelointia varten on varattu RFC 3056:ssa määritelty prefiksi 2002::/16. Reunareitittimet ovat kaksoispinoreitittimiä. Kuvassa 1on esitetty yksinkertainen 6to4-topologia.



Kuva 1. 6to4-tunneli – esimerkki.

Kuvassa RTR1:n takana oleva HostA pyrkii kommunikoimaan RTR2:n takana olevan HostB:n kanssa. Reitittimet ovat kaksoispinoreitittimiä, joiden välillä on IPv4-verkko. RTR1:n IP-osoite on 2002:a00:101::/48, mikä muodostuu 2002::/16 prefiksistä ja reitittimen RTR1 osoitteesta 10.0.1.1. RTR2:n IP-osoite vastaavasti 2002:a00:201::/48. Kun RTR1 vastaanottaa paketin HostA:lta, se lukee ensin kohdeosoitteen, jonka prefiksi on 2002:a00:201::/48, minkä jälkeen se tietää reititystaulunsa perusteella, että paketti on reititettävä tunneliin. RTR1 ottaa tarvittavat 2002::/16 -prefiksin jälkeen tulevat bitit IPv6-kohdeosoitteesta ja saa näin kohdeosoitteeksi IPv4-osoitteen 10.0.2.1, jolloin se tietää, minkä reitittimen kanssa tunneli on muodostettava. Tämän jälkeen RTR1 muodostaa tunnelin itsensä ja saadun kohdeosoitteen välille, ja enkapsuloi IPv6-datan IPv4-paketin sisään, joka lähetetään tunnelia pitkin RTR2:lle. RTR2 dekapsuloi paketin ja lähettää sen IPv6-kohdeosoitteeseen.

6to4-tunnelin haittana on sen pakotettu prefiksi 2002::/16. Suurin osa reititysprotokollista käyttää naapurinmuodostukseen ja päivityksiin paikallisia linkkiosoitteita, jotka eivät vastaa tätä ennaltamääritettyä prefiksiä, eivätkä näin ollen voi toimia. Samasta syystä ei myöskään NAT toimi 6to4-tunneleissa. [5, s. 846]

4.2.2 ISATAP-tunnelointi

Intra-Site Automatic Tunnel Addressing Protocol –tunnelointiteknologian idea on perusajatukseltaan samanlainen kuin 6to4-teknologia. Myös ISATAP-tunneloinnissa käytetään IPv4-osoitteita, jotka sisällytetään IPv6-osoitteeseen heksadesimaalimuodossa. ISATAP:ssa IPv4-osoitteen 32-bittiä sijoitetaan kuitenkin IPv6-osoitteen viimeiseen neljään oktettiin, jolloin niistä muodostuu verkkoliitynnän

tunnisteen loppuosa. Kokonaisuudessaan verkkoliitynnän tunniste muodostuu valmiiksi määritellystä 32-bittisestä heksadesimaaliarvosta 0000:5EFE, jonka perään lisätään IPv4-osoite heksadesimaalina. 64-bittinen prefiksi ei ole ennaltamäärätty, vaan se voi olla niin globaali, kuin lokaalikin. Taulukossa 3 on kuvattu ISATAP-tunnelin käyttämän osoitteen muodostuminen

Globaali / lokaali prefiksi (64 bit)	Valmiiksi määritelty arvo (32 bit)	IPv4-osoite heksadesimaalina
2001::	0000:5EFE	c0a8:0a01
FE80::	0000:5EFE	c0a8:0a01

Taulukko 3. ISATAP-osoitteen muodostuminen. Käytetty IPv4-osoite on 192.168.10.1.

ISATAP-tunneli voidaan samaan tapaan muodostaa joko päätelaitteen ja reitittimen välillä, tai reittimeltä reitittimelle. ISATAP:n nimessä ilmenevä Intra-Site viittaa sen suunnitellun toiminnalisuudeltaan yrityksen yhden toimipisteen sisällä toimivaksi, joten ajatuksena on, että tunneli muodostettaisiin päätelaitteilta yhdelle keskitetylle kaksoispinoreitittimelle

ISATAP-tunnelin heikkoutena on 6to4:n tapaan useimpien reititysprotokollien toimimattomuus, sillä ISATAP ei tue multicastia, jota reititysprotokollat yleensä käyttävät. Sen sijaan staattiset reitit ja BGP toimivat. OSPFv3 voidaan lisäksi saada toimimaan konfiguroimalla naapurimainostukset käyttämään unicastia multicastin sijaan. Kyseiset naapurit tulee kuitenkin erikseen määritellä. ISATAP ei myöskään toimi NAT:n läpi. [5, s. 857.]

4.2.3 Teredo-teknologia

Kuten edellä käy ilmi, mikäli IPv4-paketin reitti kulkee NAT:ia tekevän laitteen läpi, ei 6to4- tai ISATAP-tunneleita voi muodostaa teknologioiden rajoitusten tähden. Tämän takia on kehitetty tunnelointimekanismi nimeltä Teredo. Periaate Teredon toimivuudelle on sen kyky käyttää IPv6-paketin enkapsulointiin IPv4 UDP-paketteja, jotka kykenevät liikennöimään NAT-laitteiden läpi ongelmitta. [5; 20.]

RFC 4380:ssa on määritelty Teredon käyttämät kolme komponenttia: Teredo-asiakasohjelma (Client), Teredo-palvelin (Server), sekä Teredo-välittäjä (Relay). Asiakasohjelma on päätelaite, jolla on IPv4-yhteys, mutta joka pyrkii saamaan

yhteyden IPv6-Internetiin. Toimintaperiaatteena on, että asiakasohjelma muodostaa ICMPv6 Echo Requestin (ping) ja lähettää sen kohti itselleen konfiguroitua Teredo-palvelinta. Palvelin lähettää ping-paketin kohti IPv6-internetia. Kun kohteena oleva IPv6-noodi saa paketin, se vastaa Echo Replylla, joka lähetetään Teredo-välittäjälle. Tämän jälkeen välittäjä ottaa yhteyden alkuperäiseen päätelaitteeseen. Teredo-palvelin on näin ollen se laite, joka avustaa asiakasohjelmaa tunnistamaan välissä olevan NAT:n, jos sellainen on. Välittäjä on puolestaan IPv6-reititin, joka mainostaa IPv6-internetiin Teredo-asiakasohjelmille ennalta määritettyä prefiksiä 2001:0000:/32 ja vastaanottaa Teredo-asiakasohjelmille menevää liikennettä. [19; 20.]

Teredon haittana on Teredo-välittäjien suuri kaistantarve. Teredo ei myöskään toimi symmetristen NAT:ien läpi. Tätä varten on kehitetty joitakin standardoimattomia, mahdollisia tietoturvariskejä sisältäviä teknologioita, mutta ne eivät ole täydellisiä, eivätkä tarjoa todellista ratkaisua. [6; 19]

4.2.4 Tunnel broker -teknologia

Tunnel broker on RFC3053:ssa määritelty vaihtoehtoinen 6to4:n ja muiden teknologioiden rinnalle kehitetty tapa yhdistää eristäytyneitä IPv6-saarekkeita IPv4-internetin yli toisiinsa. Kyseinen RFC kuvailee Tunnel brokeria virtuaaliseksi IPv6-palveluntarjoajaksi sellaisille käyttäjille, joilla on olemassa oleva IPv4-yhteys. [22.]

Tunnel broker koostuu kahdesta erillisestä komponentista: Tunnel Brokerista (TB) sekä Tunnel Serveristä (TS). TB:n tehtävä on nimensä mukaisesti toimia välittäjänä IPv6-yhteyttä hakevan laitteen sekä TS:n kesken. TB lähettää konfigurointikomentoja koskien tunneleiden luontia, poistoa tai muokkaamista TS:lle, joka on käytännössä kaksoispinona toimiva reititin, jolla on yhteys julkiseen internetiin. TB on myös kykeneväinen rekisteröimään käyttäjänsä osoitteen DNS:ään. [22.]

TB-käyttäjän tulee tiedottaa TB:lle IPv4-osoitteensa, nimi DNS:ää varten sekä tieto siitä, mikä rooli sillä on eli onko kyseessä yksittäinen työasema vai reititin. Jos kyseessä on reititin, jonka takana on useita laitteita, jotka tarvitsevat yhteyden, on TB:lle ilmoitettava myös jonkinlainen määrä tarvittavista osoitteista, jolloin TB osaa allokoida oikeanlaisen prefiksin yhteyksiä varten. [22.]

Tunnel brokerin tapauksessakaan toimivuus sisäisellä IPv4-osoitteella NAT-laitteen takaa ei ole varmaa [22].

4.3 Käännösmekanismit

Luvussa 3.2 mainittiin IPv4:n käyttämä NAT eli Network Address Translation. NAT:ia käytetään yksinkertaistetusti sanottuna kääntämään IPv4-osoitteita toisiksi IPv4-osoitteiksi. Transitiomekanismina ajatus on samanlainen, mutta osoitteita käännetään IPv4:stä IPv6:een ja toisin päin.

4.3.1 NAT-protokollakäännös

NAT Protocol Translation (NAT-PT) kääntää sen sijaan IPv4-osoitteita IPv6-osoitteiksi ja päinvastoin. NAT-PT:tä käytettäessä tarkoitukseen valittu reititin suorittaa käännöksen IPv4 ja IPv6 -verkkojen rajalla. Muut verkkolaitteet eivät tiedä käännöksestä. [5, s. 865.]

NAT-PT -reititin pitää yllä käännöstauluja molempien verkkojen suuntiin, joten käytännössä reitittimen on oltava kaksoispinoreititin. Lisäksi jotta NAT-PT olisi toimiva, on NAT-PT -reittimeen konfiguroitava ns. Domain Name Service application layer gateway eli DNS-ALG. DNS-ALG kääntää IPv6-osoitteita DNS-kyselyjen ja vastausten sisällä niiden vastaaviksi IPv4-osoitteiksi ja toisinpäin. [5, s. 865.]

RFC4966 kuitenkin käytännössä määrittää NAT-PT:n statuksen historialliseksi sen lukuisten ongelmien takia, jotka liittyvät mm. DNS-ALG:iin [28].

4.3.2 NAT64-käännösmekanismi

NAT64:n toiminnallisuus on samantyyppinen kuin NAT-PT:nkin. NAT64 toimii kuitenkin vain yhteyksillä, jotka aloitetaan IPv6:n puolelta. Mikäli yhteys halutaan toimivaksi IPv4:stä IPv6:een, konfiguraatio on tehtävä staattisesti eli manuaalisesti yksitellen ilman automatiikkaa. NAT64:ää varten tarvitaan DNS64-mekanismia eli omaa DNS-palvelinta. Palvelin voi kuitenkin sijaita missä tahansa verkossa, toisin kuin NAT-PT:n tapauksessa, jossa NAT-PT:tä tekevän reitittimen oli oltava DNS-kyselyn reitillä.

5 IPv6-siirtymän suunnittelu ja toteutus

Tässä osiossa kuvataan IPv6-siirtymän tarvitsemat vaiheet. Lähtökohtana on ensin kartoittaa koko yritysverkon infrastruktuurin tila, minkä jälkeen voidaan suunnitella, mitkä osat verkosta voidaan mahdollisesti suoraan päivittää uuteen IP-versioon tai mitä muutoksia on tehtävä, jotta halutut osat saadaan päivitettyä. Lopullisena päämääränä on tietysti koko verkon IPv6-toiminnallisuus, mutta on epätodennäköistä, että sellainen siirtymä tapahtuisi yritysverkossa lyhyen ajan sisällä. Ajatus onkin, että verkon eri osa-alueet siirtyvät IPv6:een hallittuina kokonaisuuksina.

Luonnollisesti jokaisella yrityksellä on omat prioriteettinsa, eikä suunnitelma luultavasti koskaan voi olla täysin samanlainen, joten sitä on vaikea kuvata täsmällisesti. Niinpä seuraavissa luvuissa kuvataankin perustavanlaatuisesti ne kohdat, jotka suunnitelman vähintäänkin tulisi sisältää, jotta se voisi olla toimiva.

5.1 Päivitettävän alueen rajaus

Liikkeelle on hyvä lähteä rajaamalla päivitettävä alue. Päätös on järkevää tehdä perustuen tiettyyn päämäärään. Halutaanko perustoiminnallisuus sisäverkosta ulospäin, vaiko mahdollisesti jonkin tietyn sovelluksen tai palvelun toimivuus sekä sisäverkossa että mahdollisesti DMZ:n (Demilitarized Zone) kautta ulos internetiin päin? Kun tiedetään mitä halutaan, voidaan rajata päivitystä jollakin tasolla vaativat verkkosegmentit.

Perusverkkosegmenteiksi voidaan lukea Internet, DMZ ja sisäverkko, jotka jokaiselta yritykseltä varmasti löytyvät. Sisäverkkoon voidaan lisäksi erillisenä kokonaisuutena sisällyttää langaton verkko (WLAN, Wireless Local Area Network).

Mikäli yritys on vasta lähtemässä toteuttamaan IPv6:tta, on todennäköistä, että ensimmäinen tehtävä on ns. internet-reunan toiminnallisuuden takaaminen. Tämä tarkoittaa, että on varmistettava palveluntarjoajan kykenevyys IPv6-yhteyden tarjoamiseen, sekä huomioitava omien reunalaitteiden IPv6-toimivuus. Myös IPv6-osoiteavaruus on haettava palveluntarjoajalta. Osoitteiden hakemista käsitellään tarkemmin luvussa 5.4.

5.2 Verkkolaitteiden kartoitus

Yritysverkot harvoin sisältävät vain yhden laitevalmistajan laitteita, puhumattakaan yhtenevistä käyttöjärjestelmäversioista. Tämän takia ensimmäiseksi tulisi selvittää mitä laitteita verkossa on, ja näiden laitteiden kykenevyys toimia IPv6:lla. Mikäli mahdollista, laitteet olisi hyvä jaotella verkkosegmentein omiin osioihinsa, jolloin saadaan helposti yleiskuva siitä, mitkä alueet ovat heti, tai lähes valmiita IPv6-siirtymää varten. Taulukossa 4 on kuvattu osa Excel-tiedostoa, jossa on esimerkkitapaus laitteiden jaottelusta.

Taulukko 4. Laitteiden kartoitus – esimerkki.

DMZ					
Laitteen nimi	Tyyppi	Valmistaja	Ohjelmistoversio	IPv6-tuki	Tuki pävityksen avulla?
DMZ-FW-1	Palomuuri	Palo Alto	xx	Kyllä	-
DMZ-RTR-1	Reititin	Cisco	yy	Kyllä	-
DMZ-RTR-2	Reititin	Juniper	zz	Ei	Kyllä
Office					
Laitteen nimi	Tyyppi	Valmistaja	Ohjelmistoversio	IPv6-tuki	Tuki pävityksen avulla?
Office-FW-1	Palomuuri	Checkpoint	nn	Ei	Ei
Laite2					
Laite3					
Laite4					

On huomioitavaa, että kyseessä on vain esimerkki, sillä usein laitevalmistajilta löytyy heidän mukaansa IPv6-tuki, mutta todellisuudessa useita ominaisuuksia puuttuu. Näin ollen esimerkiksi muutossuunnitelman luomisen jälkeen, kun tiedetään laitteilta vaadittavat ominaisuudet, voidaan täydentää taulukkoon mahdolliset puutteet ja tämän jälkeen päivittää ne uudempaan tarvittavaa ominaisuutta tukevaan versioon.

5.3 Palveluiden kartoitus

Palvelut on kartoitettava samaan tapaan kuin verkkolaitteetkin. IPv6:n käyttöönoton kannalta tärkeimpiä palveluita ovat luonnollisesti nimipalvelu (DNS) ja osoitteenjako (DHCP), joten niiden kykenevyys IPv6:een tulisi tarkistaa ensin. Lisäksi on otettava huomioon verkonvalvonta ja esimerkiksi sähköpostiliikenne, sekä verkkolaitteiden käyttämä aikapalvelu (Network Time Protocol, NTP). Yrityksellä saattaa olla

käytössään myös useita ohjelmistoja ja ohjelmistoversioita palveluita pyörittävillä alustoilla. Laitteiden ja palveluiden kartoitus kannattaa tehdä yhdessä ja jaotella samankaltaisesti, jotta hyvä yleiskuva IPv6-kykeneväisyystä muodostuu molempien osa-alueiden osalta.

5.4 IPv6-osoitteiden hankkiminen

Korkein IP-osoitteita jakava taho on IANA (Internet Assigned Numbers Authority), jonka alla toimivat alueelliset rekisterivirastot (RIR, Regional Internet Registry). Euroopan alueella toimiva RIR on RIPE. Alueelliset virastot jakavat osoitteet eteenpäin paikallisille rekisterivirastoille (LIR, Local Internet Registry), joita usein ovat mm. palveluntarjoajat. [23; 24.]

Organisaatio, tai yritys, jolla on vain yksi internet palveluntarjoaja todennäköisesti saa osoiteavaruutensa suoraan kyseiseltä operaattorilta. Jos yrityksellä kuitenkin on useampia palveluntarjoajia, on sen haettava niinsanottua tarjoajasta riippumatonta (PI, Provider Indepenedent) osoiteavaruutta suoraan RIR:ltä, tai tarvittavat kriteerit täyttävältä LIR:ltä. Saadakseen PI osoiteavaruuden, on yrityksen tai organisaation kyettävä osoittamaan sen olevan, tai tulevan olemaan useamman internet palveluntarjoajan varassa. Lisäksi on täytettävä tietyt vaatimukset, jotka mm. RIPE listaa dokumentissaan ” Contractual Requirements for Provider Independent Resource Holders in the RIPE NCC Service Region”, eli “sopimuksenmukaiset vaatimukset tarjoajasta riippumattomien resurssien haltijoille”. [24; 25.]

Yrityksen tulisi aina pyrkiä hakemaan palveluntarjoajasta riippumaton osoiteavaruus, sillä muutoin se on sidottu palveluntarjoajaan, jolta avaruus on saatu. Tämä johtuu siitä, että palveluntarjoajat jakavat osoiteavaruudet itselleen osoitetusta prefiksistä. Kyseinen prefiksi taas reititetään ainoastaan kyseisen palveluntarjoajan kautta, joten samaa avaruutta ei ole mahdollista käyttää, mikäli palveluntarjoaja vaihtuu [27]. Tässä tapauksessa yrityksen olisi luotava koko osoitehierarkiansa alusta asti uudelleen, mikä luonnollisesti aiheuttaisi huomattavan työmäärän.

5.5 IP-osoitteiden jako

Kuten aiemmista luvuista on käynyt ilmi, IPv6-kelpoiset laitteet pystyvät muodostamaan itselleen automaattisesti globaalin unicast-osoitteen laitteen MAC-osoitteesta muodostetun EUI-64 -formaatin sekä reitittimen mainostaman paikallisen verkon prefiksin avulla. Vaihtoehtoisesti voidaan käyttää DHCPv6:tta.

Yritysympäristössä DHCPv6:n käyttäminen on suotavaa, jotta osoitteiden hallinta pysyisi mahdollisimman yksinkertaisena. Autokonfigurointia käytettäessä olisi pidettävä kirjaa verkon MAC-osoitteista, eikä osoitteiden jaossa välttämättä olisi silminnähtävää logiikkaa, mikä mahdollisesti vaikeuttaisi koko verkon hallintaa. Lisäksi, DHCPv6:tta tarvitaan todennäköisesti joka tapauksessa mm. DNS-palvelintietojen välittämiseksi päätelaitteille.

Se, kuinka yrityksen sisällä halutaan jakaa sille allokoidut osoitteet eri verkkosegementeille, riippuu yrityksen omasta politiikasta. Palveluntarjoajien allokoimat IP-avaruudet ovat yleensä luokkaa /48, /56 tai /64 tarpeesta riippuen. Koska tyypillisesti verkkoliitynnän tunnisteen osuus koko IPv6-osoitteesta on viimeiset 64 bittiä, jää organisaatiolle mahdollisuus /48 -maskin avaruudesta käyttää 16 bittiä oman hierarkiansa luomiseen.

Aliverkotus kannattaa muodostaa lokaation, mahdollisen käyttötarkoituksen tai molempien perusteella. Taulukossa 5 on esimerkkinä jaettu /48 lohko osiin:

Taulukko 5. Esimerkki aliverkotuksesta.

	Alue:	**verkko:**	**aliverkko:**
Yritys X		1234:1234:1234::/48	
	Suomi		2000:1234:1234:0000::/50
	Ruotsi		2000:1234:1234:4000::/50
	Hollanti		2000:1234:1234:8000::/50
	Saksa		2000:1234:1234:c000::/50
Suomi		2000:1234:1234:0000::/50	
	Helsinki		2000:1234:1234:0000::/52
	Jyväskylä		2000:1234:1234:1000::/52
	Kajaani		2000:1234:1234:2000::/52
	Oulu		2000:1234:1234:3000::/52

Aliverkotusta on järkevää jatkaa, niin että saadaan esimerkiksi /64 –maskin määrittämiä käyttäjäverkkoja.

5.6 Muutossuunnitelma

Kun laitteet ja palvelut on kartoitettu ja tiedetään päämäärä, joka halutaan saavuttaa, on seuraava askel muutossuunnitelman tekeminen. Muutossuunitelmassa määritetään käytettävät transitiomenetelmät, allokoidaan tarkat IPv6-osoitteet verkkosegmenteille ja niiden laitteille sekä eritellään päivitettävät laitteet. Lisäksi määritellään tarvittavat resurssit ja jaetaan roolit toteutukseen osallistuville osapuolille. Muutossuunnitelmaan tulisi myös sisältyä mahdollisten riskien määrittely ja palautussuunnitelma ongelmien varalta. Lopuksi luodaan konfiguraatio ja päätetään järjestys, jossa konfiguraatio toteutetaan. Riskeistä riippuen myös mahdollinen testaaminen laboratorioympäristössä tulisi järjestää.

Laitteiden päivitys

Rajatun alueen ja laitteiden kartoituksen perusteella päätetään, mitkä laitteet tarvitsevat ohjelmistopäivityksen, tai mitkä laitteet vaihdetaan uudempiin. Laite täytyy mahdollisesti vaihtaa uudempaan, mikäli se ei komponenttiensa puolesta kykene suoriutumaan esimerkiksi kaksoispinototeutuksen aiheuttamasta lisäkuormasta prosessorille. Mikäli laite vaihdetaan kokonaan, on sitä varten tehtävä oma suunnitelma ja huomioitava riskit.

Ohjelmistopäivitystä sen sijaan saatetaan tarvita, mikäli nykyinen versio ei tue haluttuja IPv6:n ominaisuuksia. Kuten aiemmin on todettu, laitevalmistajat saattavat ilmoittaa laitteen tai version tukevan IPv6:tta, vaikka useita oleellisia ominaisuuksia puuttuisikin. Ohjelmistopäivitystä tehtäessä täytyy selvittää mihin versioon siirrytään ja mikä on päivityspolku. Luonnollisesti myös ohjelmistopäivitys vaatii oman suunnitelmansa.

Osoitteiden jako verkkoliitynnöille ja verkkokuvat

Osoitteiden jakoa varten laitteiden välisille linkeille ja muille tarvittaville liitynnöille on hyvä muodostaa jonkinlainen politiikka, jotta logiikka pysyy samana ja näin ollen vähentää riskejä virheille myös konfigurointivaiheessa. Huomioitavia allokointeja ovat mm. käyttäjäverkkojen oletusyhdyskäytävät ja edellämainitut linkkiverkot laitteiden välillä.

Kun tiedetään tarkat aliverkot ja merkittävien liityntyöjen yksittäiset osoitteet, voidaan päivittää olemassa olevat IPv4-verkkokuvat sisältämään myös IPv6-osoitteet. Selkeyden vuoksi voi olla järkevää tehdä omat kuvat IPv6:tta varten, vaikka topologia olisikin sama.

Resurssit ja roolienjako

Jos kyseessä on laaja toteutus isossa yhtiössä, on todennäköisesti tarpeen kommunikoida eri vaiheiden toteutus useiden osastojen ja henkilöiden kanssa. Esimerkiksi yrityksen lähiverkko (LAN, Local Area Network) ja laajaverkko (WAN, Wide Area Network) voivat olla eri tiimien, tai dedikoitujen henkilöiden vastuulla. Lisäksi palvelinpuoli on useimmiten erikseen. Eri tiimeillä on todennäköisesti myös 1-3 tason asiantuntijoita, joten on päätettävä kuinka osaava henkilö tarvitaan, ja tämän jälkeen nimetä jokaisesta tiimistä tarpeellinen määrä muutokseen osallistuvia henkilöitä.

Riskit, testaus ja palautumissuunnitelma

Verkon toimivuus on yritykselle usein liiketoiminnan kannalta ehdotonta, jolloin katkokset yhteyksissä voivat aiheuttaa huomattavia liiketaloudellisia vahinkoja. Näin ollen on tärkeää listata etukäteen mihin palveluihin, tai yhteyksiin tehtävät toimenpiteet voivat mahdollisesti vaikuttaa. Mahdollisten vaikutusten perusteella arvioidaan toteutuksen riskialttius ja testataan muutos laboratorioympäristössä siltä osin, kuin on käytettävissä olevilla laboratoriolaitteilla mahdollista, tai nähdään tarpeelliseksi.

Siltä varalta, että muutoksen toteutuksen jälkeen ei saada jotakin yrityksen toiminnan kannalta kriittistä palvelua toimimaan, tarvitaan palautussuunnitelma, jossa käydään selkeästi läpi, mitä tehdään jotta voidaan siirtyä takaisin tilanteeseen ennen muutoksen aloittamista. Usein tämä tarkoittaa lähinnä tehtyjen toimenpiteiden perumista järjestyksessä takaperin vaihe kerrallaan. Aina palautuminenkaan ei kuitenkaan ole

varmaa, mikäli suunnitelmaa ei ole voitu testata – jokin laite voi hajota, tai jonkin ominaisuuden päälle kytkeminen sekoittaa verkon liikennettä niin, että pelkkä aiemman kumoaminen ei riitä, vaan on etsittävä ilmenneen vian syytä analysoimalla liikennettä tarkemmin. Tästä johtuen muutokset tulisi aina pyrkiä tekemään toimistotuntien ulkopuolella niin, että myös korjauksille on aikaa, jos jokin menee pieleen.

Konfigurointi

Konfiguraatiot on järkevää tehdä ennalta ja käydä läpi ennen muutosta. Useimmat toteutukset vaativat vähintäänkin osoitteiden, reittien ja palomuurisääntöjen konfiguroinnin. Tärkeää on joissakin tapauksissa huomioda konfiguraatiojärjestys, sillä esimerkiksi työasemat pyrkivät yleensä ensisijaisesti yhdistämään IPv6-osoitteella, mikäli niillä sellainen on. Näin ollen IPv6:n aktivointi sisäverkossa voisi aiheuttaa turhia katkoksia, jos yhteyttä sisäverkosta muualle ei ole konfiguroitu ensin.

5.7 Dokumentointi

Muutoksen edetessä, vaiheet tulisi dokumentoida, jotta kaikki mahdollinen tieto on tallessa tulevaa varten. Mikäli jokin kohta suunnitelmassa ei onnistu, tai suoritetaan toisin kuin on suunniteltu, on tärkeää olla olemassa dokumentaatio, jonka pohjalta voidaan esimerkiksi mahdollisessa vikatilanteessa toimia. Dokumentointiin tulisi sisältyä muutoksessa mukana olleet henkilöt, heidän tekemisensä, konfiguraatiot, mahdolliset ongelmat ja niiden korjaus, sekä ajan tasalle saatetut verkkokuvat. Mikäli yrityksellä on käytössä jokin sisäinen tiketöintijärjestelmä, sitä on hyvä käyttää tähän tarkoitukseen. Mikäli dokumentaatio tai osa siitä säilötään fyysisesti johonkin, tulisi olla olemassa myös keskitetty tietokanta tai muu vastaava, mistä tieto dokumenttien sijainnista osataan hakea.

6 Cygaten toimistoverkon päivitys

6.1 Alueen rajaus

Cygaten lopullisena päämääränä on koko verkon päivittäminen IPv6:een. Osia verkosta on jo aiemmin päivitetty IPv6 kelpoisiksi, mutta projekti on yhä kesken.Tässä luvussa kuvataan käytännön toteutus yhdestä verkon osa-alueen päivityksestä IPv6:een perustuen edellisessä luvussa kuvattuun prosessiin.

Cygaten verkon internet-reuna on jo aiemmin päivitetty täyteen IPv6-toiminnallisuuteen, mikä tarkoittaa, että Cygaten reunalaitteilla (CE, Customer Edge) on BGP (Border Gateway Protocol) -naapuruus palveluntarjoajien reunalaitteisiin (PE, Provider Edge). Seuraavaksi tarkoitus on muodostaa perustoimivuus Cygaten Perkiöntien toimistoverkon työasemilta internetiin päin. Sisältyvät verkkosegmentit ovat näin ollen internet ja sisäverkko. Seuraavia vaiheita ajatellen otetaan kuitenkin esimerkiksi osoitteen jaossa osaksi huomioon muiden Cygaten toimipisteiden sisäverkot sekä joitakin DMZ-transit -verkkoja.

6.2 Verkkolaitteiden ja palveluiden kartoitus

Taulukossa 6 on esitetty ne L3-tason laitteet, jotka ovat reitillä sisäverkosta internetiin. Koska Internet-reunaa päivitettäessä on jo tehty kattava kartoitus Cygaten verkkolaitteista ja palveluista, sitä ei ole järkevää kokonaisuudessaan tehdä uudelleen. Taulukosta on jätetty pois siirtokerroksen kytkimet, joiden IPv6-tuella ei ole tämän toteutuksen kannalta merkitystä. Tämä voidaan todeta jo nyt, sillä päämääränä ei ole päivittää lukuisia sisäverkon palveluita toimimaan IPv6:lla, mikä tarkoittaa, että IPv4-toiminnallisuus tulee joka tapauksessa säilymään kaikkialla sisäverkossa. Tämän perusteella myös kytkimien hallinta voidaan vielä jättää IPv4:n varaan.

Taulukko 6. Laitteiden kartoitus – huomioitavaa –kohta on lisätty jälkeenpäin

Internet						
Laitteen nimi	Tyyppi	Valmistaja	Malli	Ohjelmistoversio	IPv6-tuki	Huomioitavaa
bbrtr1	Reititin	Juniper	xxx	yyy	Kyllä	-
bbrtr2	Reititin	Juniper	xxx	yyy	Kyllä	-
internet-fw1	Palomuuri	Stonesoft	zzz	zzz	Kyllä	-
Sisäverkko						
Laitteen nimi	Tyyppi	Valmistaja	Malli	Ohjelmistoversio	IPv6-tuki	Huomioitavaa
csw1	L3-kytkin	Juniper	xxx	xxx	Kyllä	DHCPv6-relay tarvitaan
office-fw02	Palomuuri	Palo Alto	yyy	yyy	Kyllä	-

Alustavaan toimivuuteen sisäverkosta internetiin vaaditaan lähinnä DHCP- ja DNS-palvelut. Nämä löytyvät sisäverkosta IPAM:n (IP Address Management) ohella Infoblox alustalta taulukon 7 mukaisesti.

Taulukko 7. Alusta DHCP:lle, DNS:lle ja IPAM:lle sisäverkossa.

Valmistaja	Malli	Ohjelmistoversio	IPv6-tuki	Huomioitavaa
Infoblox	IB-XXX	x.y.z-d	Kyllä	-

6.3 Osoitteiden jako

Cygatelle on myönnetty palveluntarjoajasta riippumaton /48 -osoiteavaruus fdd2:f3e8:7ae8::/48. Kyseinen avaruus on jaettu kahteen osaan – sisä- ja ulkoverkkoon. Syntyneet /49 -maskin blokit on vielä jaettu kahdeksaan /52 -maskin blokkiin osin käyttötarkoituksen ja osin sijainnin perusteella. Jaottelu jatkuu /56 -maskilla lähinnä käyttötarkoituksen perusteella, mistä päästään /64 -käyttäjäverkkoihin ja /112 –transitverkkoihin taulukon 8 mukaisesti.

Taulukko 8. Cygaten IPv6-prefiksin aliverkotus yleisellä tasolla.

	Tarkoitus:	**verkko:**	**aliverkko:**
Ulkoverkot		fdd2:f3e8:7ae8:0000::/49	
	Ulkoverkot		fdd2:f3e8:7ae8:0000::/52
	DMZ-verkot		fdd2:f3e8:7ae8:1000::/52

	Vapaa		fdd2:f3e8:7ae8:2000::/52
	Vapaa		fdd2:f3e8:7ae8:3000::/52
	Vapaa		fdd2:f3e8:7ae8:4000::/52
	Vapaa		fdd2:f3e8:7ae8:5000::/52
	varattu tulevaan		fdd2:f3e8:7ae8:6000::/52
	varattu tulevaan		fdd2:f3e8:7ae8:7000::/52
Sisäverkot		fdd2:f3e8:7ae8:8000::/49	
	varattu tulevaan		fdd2:f3e8:7ae8:8000::/52
	varattu tulevaan		fdd2:f3e8:7ae8:9000::/52
	toimipaikat		fdd2:f3e8:7ae8:a000::/52
	Vapaa		fdd2:f3e8:7ae8:b000::/52
	sisäverkot2		fdd2:f3e8:7ae8:c000::/52
	Vapaa		fdd2:f3e8:7ae8:d000::/52
	Vapaa		fdd2:f3e8:7ae8:e000::/52
	Vapaa		fdd2:f3e8:7ae8:f000::/52

6.4 Muutossuunnitelma

Muutoksessa käytetään transitiomenetelmänä yksinkertaista kaksoispinototeutusta, jossa Cygaten runkokytkimelle, runkoreitittimelle, internet-palomuurille sekä sisäverkon palomuurille konfiguroidaan tarvittavat verkkoliityntöjen IPv6-osoitteet. Lisäksi konfiguroidaan staattiset reitit ja palomuurisäännöt, jotta saadaan aikaan vähintäänkin internetselailun IPv6:lla mahdollistava toteutus toimistoverkosta käsin. Muutoksessa otetaan huomioon myös seuraava askel, joka on DHCPv6-palvelun käyttöönotto.

Seuraavaksi käydään läpi mahdolliset laitepäivitykset sekä IPv6-osoitteiden tarkempi allokointi sisäverkoille ja niiden verkkoliitynnöille. Roolinjako ja resurssien määrittely on jätetty osiona pois suunnitelmasta, sillä niiden tarve on vähäinen.

Riskit määritellään lyhyesti ja arvioinnin jälkeen päätetään, minkä prioriteetin tiketti luodaan Cygaten järjestelmään. Myös palautussuunnitelma määritellään ja testauksen tarpeellisuudesta päätetään.

Lopuksi tehdään konfiguraatio jokaiselle laitteelle. Konfiguraatiot myös selitetään, ja kerrotaan miksi ne tehdään.

6.4.1 Laitteiden päivitys

Prosessorinkäytön, tai muistinkulutuksen kannalta muutoksessa mukana olevia laitteita ei ole tarpeen päivittää. Kuvan 2 komennoilla on kaikilta laitteilta varmistettu muistinkäyttö toimistoaikana, kun liikennemäärät ovat korkeimmillaan. Kuten voidaan todeta, luvut kytkimellä eivät ole järin isoja. Runkokytkimellä suoritettu komento kuvaa koko järjestelmän muistinkäyttöä. Aktiivinen käyttö ei ole enempää kuin 38 % ja vapaanakin on 28 %, joten ongelmaa ei ole havaittavissa.

```
csw1         > show system memor
fpc0:
--------------------------------------------------
System memory usage distribution:
       Total memory: 1022976 Kbytes (100%)
    Reserved memory:   18464 Kbytes (  1%)
       Wired memory:   65344 Kbytes (  6%)
      Active memory:  396944 Kbytes ( 38%)
    Inactive memory:   71844 Kbytes (  7%)
       Cache memory:  180256 Kbytes ( 17%)
        Free memory:  289412 Kbytes ( 28%)
Memory disk resident memory:  120184 Kbytes
VM-Kbytes(  %  ) Resident(  %  ) Map-name
   383468(36.57)   111472(10.89) kernel
```

Kuva 2. Runkokytkimen muistinkäyttö.

Runkoreitittimellä puolestaan ehkä tärkeimpänä tulee huomioida komennon lopusta löytyvät tuloste – WCPU: 98 %. WCPU tarkoittaa Weighter CPU:ta eli ns. punnittua prosessorin kuormaa, joka mitataan tietyiltä ajanjaksoilta. 98 % kuulostaa suurelta, mutta kuten sanottua kyseessä on runkoreititin, jolla on BGP-naapuruus palveluntarjoajan kanssa, mikä tarkoittaa sen pitävän lukua kymmenistä tuhansista prefikseistä. Näin ollen yksi tai kaksi merkintää lisää reititystaulussa ei tule merkitsemään laitteelle mitään. Kuvan 3 komento esittää runkoreitittimen kuorman.

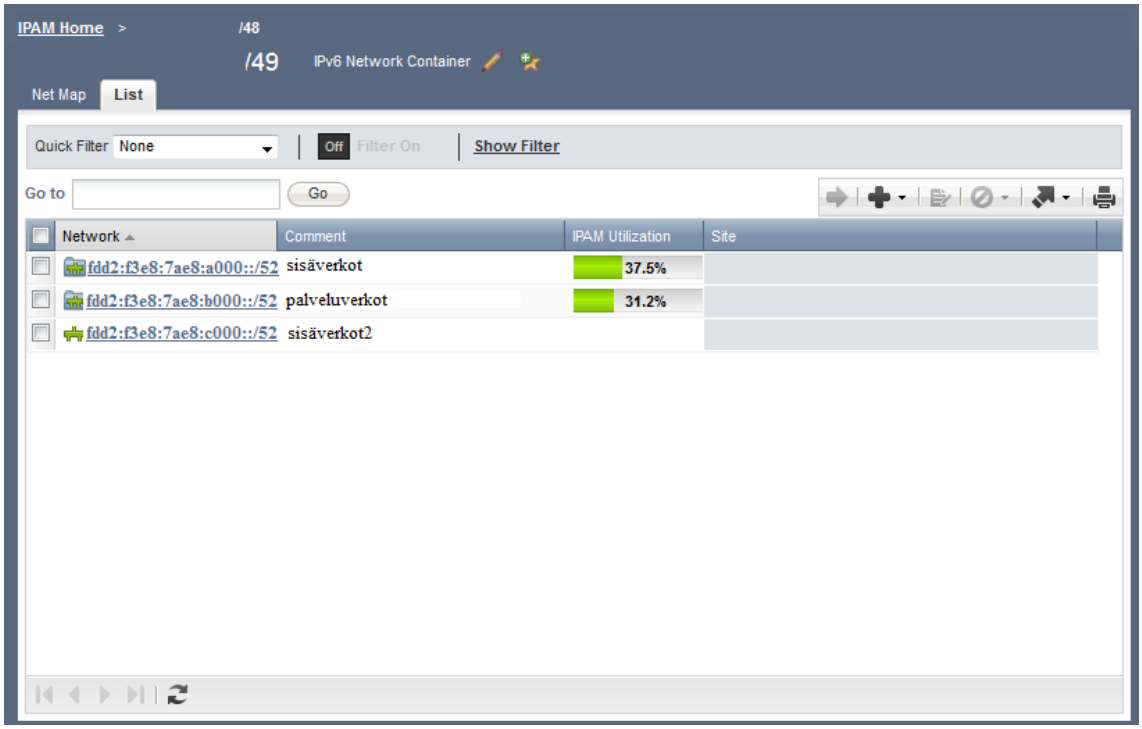
```
                bbrtr    show system processes summary
last pid: 22841;  load averages:  0.00,  0.03,  0.03  up 277+13:22:38    07:47:26
128 processes: 3 running, 98 sleeping, 27 waiting

Mem: 958M Active, 211M Inact, 189M Wired, 119M Cache, 112M Buf, 510M Free
Swap: 2915M Total, 2915M Free

  PID USERNAME  THR PRI NICE   SIZE    RES STATE    TIME   WCPU COMMAND
   11 root        1 171   52     0K    16K RUN    6344.6 98.00% idle
```

Kuva 3. Runkoreitittimen muistinkäyttö.

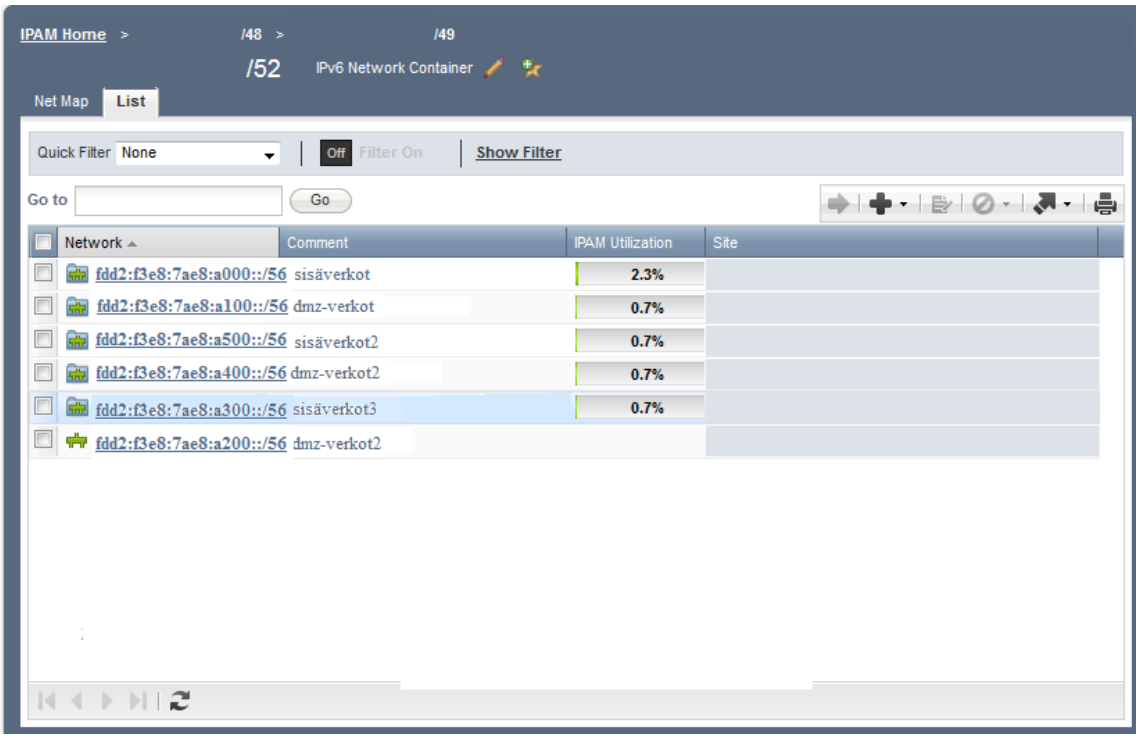
Lopullisen dynaamisen toimivuuden kannalta on kuitenkin ensiarvoisen tärkeää, että Cygaten runkokytkin kykenee välittämään sisäverkon työasemien DHCP-kyselyt eteenpäin Infobloxeille. Tämän tähden varmistettiin Juniperin dokumentaatiosta, että kytkimen ohjelmistoversio tukee DHCPv6-pakettien välitystä. Mainitun dokumentaation mukaan ominaisuus on IPv6:ssa nimellä DHCPv6-relay. Kyseisen ominaisuuden oikeanlaisesta konfiguroinnista oli kuitenkin hyvin vähän informaatiota, sillä kyseessä ei ole vastine IPv4-komennolle, vaan täysin uusi ns. komentoperhe. Ominaisuus on tulevaisuudessa testattava laboratorioympäristössä huolellisesti ennen implementointia. [32.]

6.4.2 Osoitteiden jako verkkoliitynnöille ja verkkokuvat

Kuten kartoitusvaiheessa todettiin, Cygaten IPAM eli IP-osoitteiden hallinta toimii Infoblox-alustalla. Muutosta varten jaettiin luvussa 6.3 esitetyt /52 -verkot vielä pienempiin osiin, minkä jälkeen määritettiin verkkoliityntöjen osoitteet. Kuvassa 4 esitetty sisäverkkojen jako IPAM:ssa.



Kuva 4. IPv6-sisäverkot.

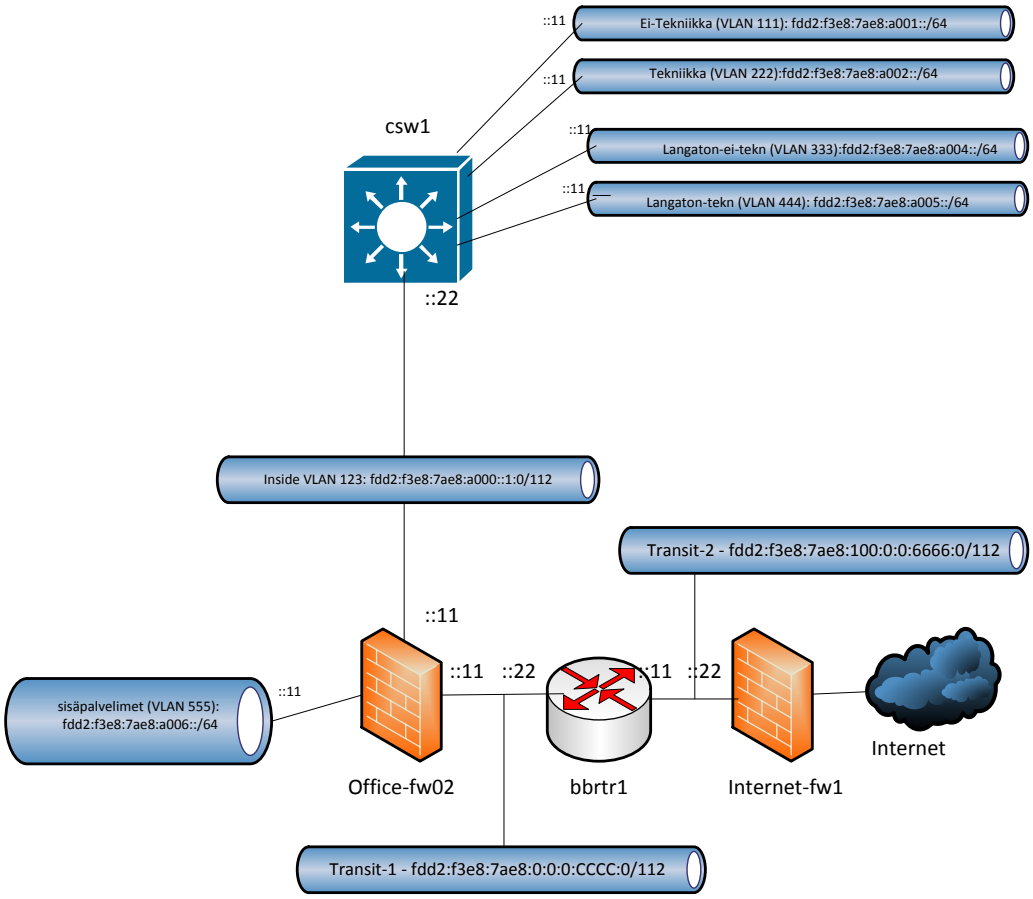


Kuva 5. Toimiston sisäverkot

Kuvassa 5 toimiston sisäverkot on jaettu edelleen /64 -maskin käyttäjäverkkoihin ja /112 -maskin transitverkkoihin. Osoitteet linkkiverkoille on allokoitu Cygaten politiikan mukaan. Esimerkiksi Helsingin sisäverkkoblokin fdd2:f3e8:7ae8:a000::/56 alta saadaan Inside VLAN 123:lle allokoitu transitverkko fdd2:f3e8:7ae8:a000::0:0:1:0/112. Kaikki luvussa 6.3 esitetyt käytössä olevat /52 -blokit on jaettu samaan tapaan, kuin yllä jaettu fdd2:f3e8:7ae8:a000:::/56 -verkko. Näiden pohjalta on myös allokoitu seuraavat osoitteet muutoksessa ja konfiguraatiossa tarvittaville osoitteille:

- office-fw02 sisäverkon liityntä ethernet 1/2.200 - fdd2:f3e8:7ae8:a000::1:11/112
- csw1 liityntä kohti office-fw02:ta: fdd2:f3e8:7ae8:a000::1:22/112
- office-fw02 ulkoverkon liityntä ethernet 1/1.3 - fdd2:f3e8: :0:0:0:CCCC:11/112

Kaikki allokoidut verkot päivitettiin Cygaten olemassaoleviin IPv4-verkkokuviin. Ymmärrettävyyden ja selkeyden vuoksi tätä työtä varten piirrettiin kuitenkin yksinkertainen toimistoverkkoa kuvaava topologia, joka on esitetty kuvassa 6.



Kuva 6. IPv6-toimistoverkon havainnollistava L3-tason topologia.

6.4.3 Riskit, testaus ja palautumissuunnitelma

Muutosta ei tehdä Cygaten tuotantoympäristöön, vaan toimistoverkon laitteille, joten tuotantoympäristö ei sinällään ole vaarassa. Kuten todettua, muutos on myös verrattain pieni ja näin ollen myös suhteellisen helposti peruttavissa. Mahdollinen riski on IPv6:tta aktivoitaessa runkokytkimellä, että reititinmainostukset alkavat automaattisesti toimimaan, minkä seurauksena esimerkiksi työasemat saattaisivat saada IPv6-osoitteen, jolloin ne yrittäisivät ottaa käytössä oleviin palveluihin yhteyttä IPv6:n avulla IPv4:n sijaan. Tämä ei tietenkään onnistuisi, vaan johtaisi liikenteen hidastumiseen tai toimimattomuuteen.

Edellä mainitun varalta selvitettiin, että JUNOS:iin, joka on runkokytkimen käyttöjärjestelmä, täytyy erikseen konfiguroida mainostukset päälle, jos ne haluaa käyttöön [29]. Näin ollen riskiä ei pitäisi olla. Laitteelta varmistettiin vielä, etteivät mainostukset ole päällä seuraavaa komentoa käyttäen:

- show ipv6 router-advertisement

Tuloste on tyhjä, joten mainostukset eivät ole päällä [29; 30]. Koska suurta riskiä ei ole olemassa, muutosta ei erikseen testata, vaan se suoritetaan suoraan käytössä olevaan ympäristöön. Varotoimenpiteenä tämä kuitenkin tehdään toimistotuntien ulkopuolella.

Palautumissuunnitelma on yksinkertaisesti asetettujen konfiguraatioiden poistaminen alkaen runkokytkimestä. Mikäli ongelmia esiintyy konfiguraatioiden poistamisen jälkeen, voidaan liikennettä tutkia tarkemmin JUNOS:n debug-komennoilla. Kyseisten komentojen käytöstä löytyy tietoa Juniperin ns. tietämyskannasta (KB, Knowledge Base), muun muassa KB16233:ssa on käyty läpi oleellisia komentoja tähän liittyen [31].

6.4.4 Konfiguraatiot ja niiden selitykset

Aluksi lisätään staattiset reitit runkoreitittimelle (bbrtr1) ja kohti toimiston sisäverkkoja sekä sisäisiä palveluverkkoja:

- set routing-instances netti routing-options rib netti.inet6.0 static route fdd2:f3e8:7ae8:a000::/52 next-hop fdd2:f3e8:7ae8:00:0:0:CCCC:11/112

- set routing-instances netti routing-options rib netti.inet6.0 static route fdd2:f3e8:7ae8:b000::/52 next-hop fdd2:f3e8:7ae8:00:0:0:CCCC:11/112

Bbrtr1:llä on olemassa useita reititysinstansseja, joilla on omat reititystaulunsa. Edellä olevalla komennolla lisätään staattiset reitit netti-instanssissa kohti Palo Alton ethernet 1/1.3 -verkkoliityntää, jonka osoite on fdd2:f3e8:7ae8:00:0:0:CCCC:11/112.

Tarvittava staattinen 0-reitti eli oletusreitti kohti Internetiä on jo olemassa, joten sitä ei tarvitse lisätä.

Seuraavaksi konfiguroidaan Palo Altolle eli office-fw02:lle verkkoliityntöjen IPv6-osoitteet, minkä jälkeen lisätään tarkat staattiset reitit kohti Helsingin toimistoverkkoja. Konfiguraatiot tehdään Palo Alton graafisen hallintakäyttöliittymän kautta. Reitit tehdään seuraavasti:

- fdd2:f3e8:7ae8:a001::/64 – kohti csw1 - fdd2:f3e8:7ae8:a000::1:22/112
- fdd2:f3e8:7ae8:a002::/64 – kohti csw1 - fdd2:f3e8:7ae8:a000::1:22/112
- fdd2:f3e8:7ae8:a004::/64 – kohti csw1 - fdd2:f3e8:7ae8:a000::1:22/112
- fdd2:f3e8:7ae8:a005::/64 – kohti csw1 - fdd2:f3e8:7ae8:a000::1:22/112

Myös office-fw02:lla oletusreitti kohti internetiä bbrtr1:n kautta on valmiina, joten sitäkään ei tarvitse konfiguroida. Reittien lisäyksen jälkeen lisätään myös tarvittavat palomuurisäännöt, jotta liikenne pääsee muurista läpi. Testin vuoksi sallitaan trust-zonesta (Inside vlan 123) kohti transit-1:tä kaikki liikenne

Reittiä kohti sisäpalvelimia ei tarvita, sillä kyseinen palvelinverkko on ns. suoraankytketty (directly connected), joten muuri tietää automaattisesti reitin sitä kohti.

Lopuksi siirrytään runkokytkimen konfigurointiin. Ensin luodaan oletusreitti kohti sisäpalomuurin sisäistä verkkoliityntää:

- set routing-options rib inet6.0 static route 0::/0 next-hop fdd2:f3e8:7ae8:a000::1:11/112

Runkokytkimellä on olemassa kaksi instanssia, mutta kommenossa ei tällä kertaa ole tarpeellista määrittää sitä erikseen, sillä kyseessä on globaali instanssi, joten oletusarvoisesti reitti ilmestyy sen reititystauluun.

Csw1:n verkkoliitynnöille lisätään IPv6-osoitteet seuraavasti:

- set interfaces vlan unit 111 family inet6 address fdd2:f3e8:7ae8:a001::11/64

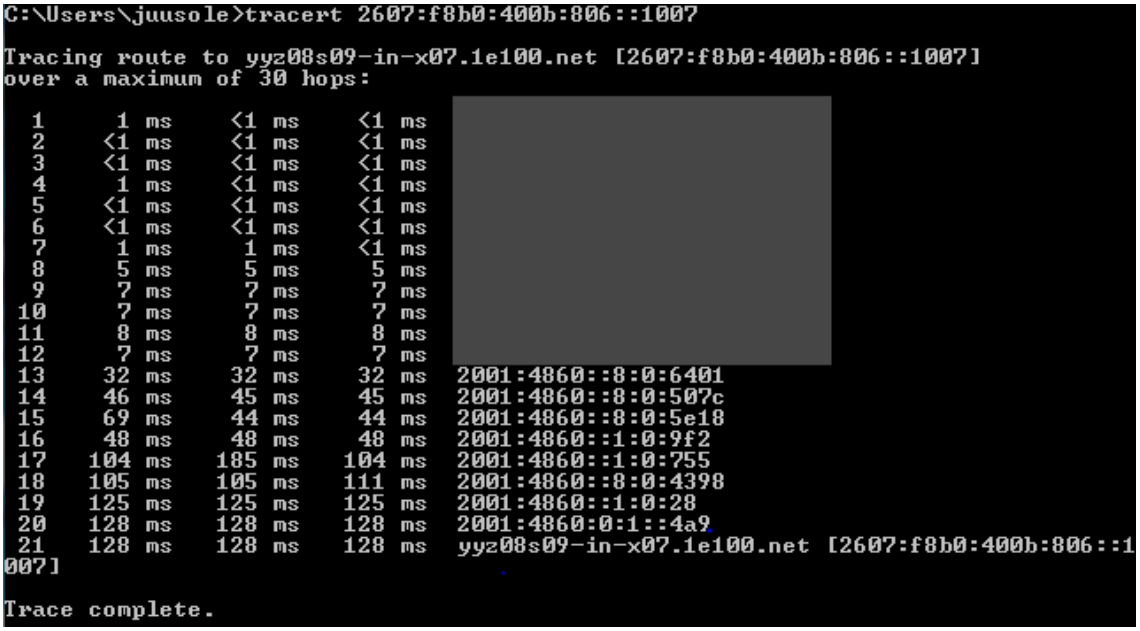
- set interfaces vlan unit 222 family inet6 address fdd2:f3e8:7ae8:a002::11/64
- set interfaces vlan unit 333 family inet6 address fdd2:f3e8:7ae8:a004::11/64
- set interfaces vlan unit 444 family inet6 address fdd2:f3e8:7ae8:a005::11/64

Kyseisten liityntöjen osoitteet toimivat oletusyhdyskäytävinä omien verkkojensa työasemille. Reittejä myöskään näitä verkkoja kohti ei tarvita, koska nekin ovat suoraankytkettyjä.

Internet-fw1 oli konfiguroitu jo aiemmin reittiensä osalta. Testiä varten konfiguroitiin kuitenkin vielä palomuurisääntö, joka salli väliaikaisesti kaiken IPv6 liikenteen ulospäin internetiin sekä sisäänpäin ping-työkalun tarvitsemat palvelut:

- IPv6 DEST. Unreachable
- IPv6 Echo Reply
- IPv6 Time Exceeded

Lopuksi testattiin yhteys muun muassa ottamalla selaimella yhteys Googleen, sekä traceroute-työkalulla selvitettiin reitti yhteen Googlen julkisista IP-osoitteista. Koska DHCP tai DNS –palvelut eivät olleet käytettävissä, annettiin Tekniikka-VLAN 222:ssa sijaitsevalle työasemalle staattinen IPv6-osoite fdd2:f3e8:7ae8:a002::3/64. Aluksi häiriötä aiheuttivat internet-fw1:ltä puuttuva IPv6 Echo Reply-palvelun puuttuminen säännöstä sekä työaseman palomuurin kokonaan estämä IPv6. Palomuuri oli pakko ottaa pois käytöstä. Kuvassa 7 esitetään kyseinen reitinselvitys.



Kuva 7. IPv6-yhteys Googleen.

6.5 Dokumentointi

Muutosta varten luotiin Cygaten järjestelmään muutostiketti, jonka kuvauksessa käytiin muutoksessa tehtävät toimenpiteet lyhyesti läpi ja jonka muutosmanageri hyväksyi.

Kun muutos oli hyväksytty ja sen ajankohta päätetty, tehtiin aiemmissa luvuissa kuvatut toimenpiteet ja dokumentoitiin tiketin lokiin muutoksen vaiheet ja käytetyt konfiguraatiot sekä testauksen tulokset. Verkkokuvia säilytetään Cygaten sisäisessä Sharepointissa, mistä käsin ne myös päivitettiin.

7 Yhteenveto

Työ eteni aloituksen jälkeen hyvin; tietoa oli runsaasti tarjolla, eikä suurempia ongelmia ilmennyt. Päänvaivaa aiheutti lähinnä uuden tiedon erotteleminen vanhasta, sillä IPv6-protokolla on koko ajan kehityksen alla ja siihen liittyviä osia julistetaan jatkuvasti vanhentuneiksi. Teknisesti ehkä vaikeinta oli oikeasti ymmärtää erityyppisten osoitteiden tarkoitus ja rakenne. Lukujen kirjoittamista hidasti myös huomattavasti

joidenkin termien kääntäminen järkevän kuuloisesti suomeksi tai käännösten etsiminen muualta.

Johdannossa kuvattua päämäärää ajatellen työ myös onnistui melkoisen hyvin. Tarkoitus oli päivittää osa toimistoverkosta IPv6:een, ja niin myös tehtiin. Toteutus tosin jäi hiukan kaavailtua pienemmäksi johtuen lähinnä Cygaten verkkoon liittyvistä muista välttämättömistä muutoksista, joita ennen IPv6:tta ei ollut järkevää ottaa käyttöön. Samalla saatiin aikaan myös aiemmin mainittu asiakkaalle esitettävä dokumentti, joka toivottavasti yrityksessä myös otetaan tulevaisuudessa käyttöön. Dokumentista tosin muodostui hiukan erilainen, kuin itse kuvittelin – käytännössä pelkkä runko, jonka pohjalta asiakkaan kanssa on mahdollista pikaisesti käydä läpi IPv6-toteutukseen liittyviä asioita.

Käytännön osiossa tehty muutos onnistui odotetusti kokonaisuudessaan hyvin, eikä odottamattomia ongelmia ilmennyt. Konfiguraatiot saatiin laitteille sisään nopeasti ja yhteys testattiin toimivaksi toimistoverkosta internetiin. Ongelmaksi tulevaisuuden näkymien osalta muodostui runkokytkimeltä puuttuva DHCP:n multicast-pakettien välitys eteenpäin DHCP-palvelimelle IPv4-toteutusta vastaavalla tavalla. Vastaava IPv4-komento on yhden rivin komento, kun taas DHCPv6-relay vaatii useita komentoja toimiakseen oikein. Tämä tulee todennäköisesti aiheuttamaan huomattavia viivästyksiä todellisen dynaamisen toimivuuden saavuttamiseksi, sillä testauksen on oltava täysin uusille komennoille kattava katkoksien välttämiseksi. Kun DHCP saadaan toimimaan oikein, on edessä seuraava vaihe eli muutoksen ulottaminen vähitellen Cygaten muille toimipaikoille sekä DMZ:lla sijaitseville ulkoisille palveluille ja yhteyksille. Sisäverkon palveluissa on IPv6:n suhteen huomattavia puutteita, joten natiivia IPv6:tta ei toimistoverkkoon saada, ennen kuin lukuisat alustat ja sovellukset on saatettu ajan tasalle.

Lähteet

1 Internet Protocol. 1981.Verkkodokumentti. IETF. http://www.ietf.org/rfc/rfc791.txt. Luettu 15.10.2013.

2 IPv4 Exhaustion. 2013. Verkkodokumentti. RIPE. <http://www.ripe.net/internet-coordination/ipv4-exhaustion>. Luettu 15.10.2013.

3 IPv4-osoitteet loppuivat koko Euroopasta. 2012. Tietoviikko. <http://www.tietoviikko.fi/kaikki_uutiset/nyt+se+sitten+kavi+ipv4osoitteet+loppuivat+koko+euroopasta/a839436>. Luettu 15.10.2013.

4 Internet Protocol, Version 6. 1998. Verkkodokumentti. IETF. <http://www.ietf.org/rfc/rfc2460.txt>. Luettu 15.10.2013.

5 Teare, Diane. 2010. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide. Cisco Press.

6 Raittinen, Tomi. 2010. Transition to IP Version 6. Insinöörityö. Metropolia Ammattikorkeakoulu.

7 Al-Rifai, Ali. 2013. IPv6-palveluntarjonta siirtymävaiheessa. Insinöörityö. Metropolia Ammattikorkeakoulu.

8 RFC 2373. 2013. Verkkodokumentti. TKK. <http://www.tml.tkk.fi/Opinnot/Tik110.350/Tehtavat/rfc/2373_10.html>. Luettu 18.10.2013.

9 IPv6 Header Deconstructed. 2008. Verkkodokumentti. IPv6.com. <http://www.ipv6.com/articles/general/IPv6-Header.htm>. Luettu 18.10.2013.

10 IPv6 Flow Label Specification. 2011. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc6437>. Luettu 18.10.2013.

11 IP Version 6 Addressing Architecture. 2006. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc4291>. Luettu 19.10.2013.

12 Kurvinen, Christian. 2012. IPv6-protokolla ja turvalliset yritysverkot (VPN). Insinöörityö. Metropolia Ammattikorkeakoulu.

13 Hurttila, Simo. 2011. Verkonvalvontapalvelun testaus IPv6-ympäristössä. Insinöörityö. Metropolia Ammattikorkeakoulu.

14 Internet Control Message Protocol (ICMPv6). 2006. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc4443>. Luettu 10.1.2014.

15 Neighbor Discovery for IP Version 6 (IPv6). 1998. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc2461>. Luettu 10.1.2014.

16 DNS Extensions to Support IP Version 6. 2003. Verkkodokumentti. IETF. <http://www.ietf.org/rfc/rfc3596.txt>. Luettu 10.1.2014.

17 Vatiainen, Heikki. IPv6: DNS, reititys, infra. 2009. Verkkodokumentti. Arch Red Oy. <http://www.archred.fi/julkaisut/ipv6-materiaalia-suomeksi/ipv6-perusrakenteet/copy_of_lyhyt-johdanto-ipv6-een/>. Luettu 10.1.2014.

18 IPsec for IPv6. 2012. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-ipsec.html#GUID-49E06011-398B-43E0-8482-D9C8D609AF73>. Luettu 11.1.2014.

19 Teredo tunneling. 2014. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Teredo_tunneling>. Luettu 11.1.2014.

20 Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs). 2006. Verkkodokumentti. IETF. <http://www.ietf.org/rfc/rfc4380.txt>. Luettu 11.1.2014.

21 IPv6 Security Brief. 2011. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-678658.html>. Luettu 14.1.2014.

22 IPv6 Tunnel Broker. 2001. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc3053>. Luettu 14.1.2014.

23 Number Resources. 2014. Verkkodokumentti. IANA. <https://www.iana.org/numbers>. Luettu 15.1.2014.

24 IPv6 Address Allocation and Assignment Policy. 2009. Verkkodokumentti. RIPE. <http://www.ripe.net/ripe/docs/ripe-481#rir>. Luettu 15.1.2014.

25 Contractual Requirements for Provider Independent Resource Holders in the RIPE NCC Service Region. 2009. Verkkodokumentti. RIPE. <http://www.ripe.net/ripe/docs/ripe-452>. Luettu 15.1.2014.

26 Request an IPv4 /22 From the Last /8. 2010. Verkkodokumentti. RIPE. <http://www.ripe.net/lir-services/resource-management/allocations-and-assignments/request-an-ipv4-22-from-the-last-8>. Luettu 15.1.2014.

27 IPv6 Provider Independent (PI) Assignments. 2013. Verkkodokumentti. RIPE. <http://www.ripe.net/ripe/docs/ripe-589#IPv6_PI_Assignments>.

28 Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status. 2007. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc4966>. Luettu 5.2.2014.

29 Configuring IPv6 Interfaces and Enabling Neighbor Discovery. 2014. Verkkodokumentti. Juniper Networks. <http://www.juniper.net/techpubs/en_US/junos13.3/topics/topic-map/ipv6-interfaces-neighbor-discovery.html>. Luettu 5.2.2014.

30 Show ipv6 router-advertisement. 2014. Verkkodokumentti. Juniper Networks. <http://www.juniper.net/techpubs/en_US/junos13.3/topics/reference/command-summary/show-ipv6-router-advertisement.html>. Luettu 10.4.2014.

31 How to use 'Flow Traceoptions' and the 'security datapath-debug' in SRX series. 2014. Verkkodokumentti. Juniper Networks. <http://kb.juniper.net/InfoCenter/index?page=content&id=KB16233&actp=search&viewlocale=en_US&searchid=1311552312909&smlogin=true>. Luettu 10.4.2014.

32 Dhcpv6 (DHCP Relay Agent). 2013. Verkkodokumentti. Juniper Networks. <http://www.juniper.net/techpubs/en_US/junos12.3/topics/reference/configuration-statement/dhcpv6-edit-forwarding-options.html>. Luettu 11.4.2014.

Dokumentti asiakkaalle

1. Johdanto

IPv4-osoitteiden loppumisen myötä IPv6-protokollaa tullaan käyttämään yhä laajemmin, mikä tarkoittaa, että yritysten on mukauduttava ja valmistauduttava ottamaan uusi protokolla vastaan. Huomioon on otettava myös oman yrityksen IPv4-osoitteiden mahdollinen loppuminen. Kun vanhat osoitteet loppuvat, on hyvä olla uusi protokolla uusine osoitteineen toimintavalmiina.

Nykyisellään yksittäisten yritysten on yhä vaikeampaa saada uusia IPv4-osoitteita, mikä saattaa osoittautua ongelmaksi, jos aikomuksena on esimerkiksi laajentaa, tai lisätä uusia julkisia palveluita. Jos IPv4-osoitteita ei ole saatavilla, yritys ei voi toteuttaa suunnitelmiaan, mikäli sillä ei ole IPv6-toiminnallisuutta. Lisäksi, tulevaisuudessa myös muiden yritysten, tai organisaatioiden palvelut saattavat toimia ainoastaan IPv6:lla samaisesta syystä johtuen, jolloin kommunikointi ja mahdollinen yhteistyö näiden kanssa vaikeutuu. Mitä kauemmas tulevaisuuteen mennään, sitä todennäköisemmin myös esimerkiksi ohjelmistokehityksessä jätetään IPv4-toiminnallisuus pois, jolloin on mahdollista että kaikilla verkkolaitteilla ei enää ole muuta kuin IPv6 käytössään. Näin ollen on tärkeää tähdätä tulevaisuuteen ja vähintäänkin kartoittaa IPv6-kykenevyys.

2. Scopen määrittely

Tehdään verkkosegmenteittäin:

2.1 Internet

- Palveluntarjoajan IPv6-kykenevyys selvitettävä
- IPv6-osoitteiden hankkiminen, pyrittävä saamaan PI (Provider Independent)-prefiksi, eli palveluntarjoajasta riippumaton prefiksi, jolloin ISP:n vaihtuessa ei ole tarvetta uudelle osoitteistukselle
- Omien reunalaitteiden IPv6-kykenevyys

2.2 DMZ

- Ulospäin tarjottavien palveluiden IPv6-kykenevyys
- DMZ -palvelinten IPv6-kykenevyys
- DMZ -verkkolaitteiden IPv6-kykenevyys

2.3 Sisäverkko

- Sisäverkon palveluiden IPv6-kykenevyys
- Sisäverkon palvelinten IPv6-kykenevyys
- Sisäverkon verkkolaitteiden IPv6-kykenevyys

2.4 Sisäverkko - WLAN

- Kohdassa 2.3 mainitut

3. Kartoitus

3.1 Laitteiden kartoitus

- Listataan verkkolaitteet, palvelimet, työasemat yms.
- Jokaiselta laitteelta selvitetään sen IPv6 -kykenevyys
- Listataan ainakin valmistaja, käyttöjärjestelmän versio ja tyyppi ja IPv6-kelpoisuus (valmistajan mukaan)
- Jos laite ei ole IPv6-kelpoinen, selvitetään onko toimivuus mahdollista saavuttaa ohjelmistopäivityksellä, vai pitääkö laite vaihtaa kokonaan
- Huomioitavaa, että kaikki IPv6-ominaisuudet eivät ole läheskään kaikilla ns. IPv6-kelpoisilla laitteilla tuettuja, joten tarkemman suunnitelman yhteydessä täytyy selvittää tarvittavat ominaisuudet

3.2 Palveluiden kartoitus

- Listataan verkon palvelut samaan tapaan kuin laitteet
- Versiot ja tuki IPv6:lle

4. Muutossuunnitelma

- Mitä transitiomenetelmiä käytetään
- Osoitteiden allokointi
- Tarvittavien laitteiden päivitys
- Riskien määritys
- Palautussuunnitelman luonti
- Resurssien ja roolien jako / määritys (osallistuvat henkilöt, työnjako)
- Testaus laboratorioympäristössä
- Konfiguraatiot
- Toteutus ja testaus

5. Lopetus

- Dokumentointi
- Muutoksen vaiheet
- Tehdyt toimenpiteet
- Konfiguraatiot talteen
- Verkkokuvat

- Mahdolliset tulevat toimenpiteet / seuraava vaihe