

Ville Palkki

Esimerkkiyrityksen IPv6-lähiverkko

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

24.5.2013

Tekijä Otsikko	Ville Palkki Esimerkkiyrityksen IPv6-lähiverkko
Sivumäärä Aika	22 sivua + 1 liite 24.5.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja	yliopettaja Matti Puska
<p>Insinööriyön tavoitteena oli suunnitella ja toteuttaa esimerkkiyrityksen IPv6-lähiverkko. Toisena tavoitteena oli suunnitella esimerkkiyrityksen siirtyminen IPv4-protokollasta IPv6-protokollaan.</p> <p>Työssä käsiteltiin IPv6-protokollaa ensin teoreettisesti ja tämän jälkeen suunniteltiin sekä rakennettiin toimiva IPv6-lähiverkko. Aluksi työssä käytiin läpi IPv6-protokollan etuja verrattuna vanhaan IPv4-protokollaan. Teoriaosuudessa selvitettiin myös IPv6-protokollan rakennetta ja lähetysformaatteja. Teorian lopuksi käytiin läpi IPv6:n autokonfiguraatiota sekä siirtymätekniikoita IPv4-protokollasta IPv6-protokollaan.</p> <p>Esimerkkiyrityksen IPv6-lähiverkon rakentaminen aloitettiin lähiverkon topologian suunnittelemisesta. Seuraavassa vaiheessa lähiverkolle päätettiin osoitesuunnitelma. Yrityksen IPv6-lähiverkko rakennettiin ja konfiguroitiin topologian ja osoitesuunnitelman avulla. Verkon toiminta varmistettiin yhteyskokeiluita käyttäen.</p> <p>Kaksoispinoteknologia todettiin tehokkaaksi, vaikkakin mahdollisesti hieman kalliiksi, tavaksi siirtyä IPv4:stä IPv6:een. Uuden IPv6-protokollan konfigurointi huomattiin myös muistuttavan paljon vanhan IPv4-protokollan konfigurointia, mikä helpottaa verkkoasiantuntijoiden sopeutumista IPv6-protokollaan.</p>	
Avainsanat	IPv4, IPv6, kaksoispino, lähiverkko, IP-protokolla

Author Title	Ville Palkki Creating an IPv6 local area network
Number of Pages Date	22 pages + 1 appendix 24 May 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor	Matti Puska, Principal Lecturer
<p>The purpose of the project described in this thesis was to plan and build an IPv6 local area network for an example company. The project also had another objective which was to design a transition plan from IPv4 to IPv6 for the company.</p> <p>The first half of the thesis focuses on theoretical aspects of the project. The thesis first discusses the differences between IPv4 and IPv6. The thesis makes clear what advantages the transition into IPv6 will bring to users. The theoretical section then advances to the structure of IPv6 and its message formats. The first half ends in an explanation of IPv6 auto-configuration and the basic idea of transition technologies.</p> <p>The technical part of the thesis starts by outlining the topology and addressing plans for the network. In practice, the network was built according to the plans and tested with the help of a ping utility tool.</p> <p>The results indicated that the dual-stack method is a very efficient transition solution. The cost of this procedure might be high for some companies if they possess old network equipment. Finally, the thesis shows that the configuration is quite similar between IPv4 and IPv6 which results in easy transition for network engineers.</p>	
Keywords	IPv4, IPv6, Dual-stack, Local Area Network, Internet protocol

Sisällys

Lyhenteet

1	Johdanto	1
2	Teoria	1
2.1	IPv6-protokollan uudistukset	1
2.2	IPv6-osoitteen formaatti	3
2.3	IPv6-lähetysformaatit	3
2.4	IPv6-osoiteavaruus	5
2.5	IPv6:n autokonfiguraatio	7
2.6	Siirtymätekniikat	7
3	Esimerkkiyrityksen IPv6-lähiverkko	9
3.1	Yrityksen IPv6-lähiverkon verkkotopologia	9
3.2	Osoitesuunnitelma yrityksen IPv6-lähiverkolle	11
3.3	Käytetyt laitteet ja ohjelmaversiot	11
3.4	Laitteiden määrittelyt	12
3.5	Testaus	15
4	Yhteenveto	19
	Lähteet	21

Liitteet

Liite 1. Reitittimen 1 konfiguraatio

Lyhenteet

6to4	siirtymismekanismi IPv4:stä IPv6:een, mikä mahdollistaa IPv6-protokollan liikenteen kuljettamisen IPv4-verkon yli IPv4-pakettien sisällä.
AfriNIC	RIR-organisaatio, jonka vastuualue on Afrikka.
APNIC	RIR-organisaatio, jonka vastuualue on Oseania ja osa Aasiaa.
ARIN	RIR-organisaatio, jonka vastuualue on Pohjois-Amerikka.
DHCP	<i>Dynamic Host Configuration Protocol</i> . Verkkoprotokolla, joka jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille.
DHCPv6	<i>Dynamic Host Configuration Protocol version 6</i> . Uusin versio DHCP-protokollasta.
DNS	<i>Domain Name System</i> . Internetin nimipalvelujärjestelmä, jonka tehtävänä on kääntää käyttäjien antamia verkkosivujen osoitteita numeeriseen muotoon.
IANA	<i>Internet Assigned Numbers Authority</i> . On vastuussa IP-osoitteiden jakamisen maailmanlaajuisesta koordinoinnista sekä autonomisen järjestelmän numeroinnista.
IETF	<i>Internet Engineering Task Force</i> . Kehittää ja vastaa Internet-protokollien standardoinnista.
IOS	<i>Internetwork Operating System</i> . Ciscon reitittimien ja kytkimien käyttämä käyttöjärjestelmä.
IPv4	<i>Internet Protocol version 4</i> . Huolehtii IP-tietoliikennepakettien toimituksesta Internet-verkossa.
IPv6	<i>Internet Protocol version 6</i> . Uusin versio IP-protokollasta.

LACNIC	RIR-organisaatio, jonka vastuualue on Latinalainen Amerikka ja osa Karibian saarista.
MAC	<i>Media Access Control</i> . Verkkosovittimen Ethernet-verkossa käytössä oleva ainutlaatuinen tunnistus.
QoS	<i>Quality of Service</i> . Luokittelee ja priorisoi tietoliikennettä mm. lähettämällä tärkeiksi merkityt tietoliikennepaketit ennen muita paketteja.
RIPE NCC	RIR-organisaatio, jonka vastuualue on Eurooppa, Lähi-itä ja Keski-Aasia.
RIR	<i>Regional Internet Registry</i> . Valvova organisaatio, joka rekisteröi ja jakaa IP-osoitteita tietyille alueille maailmassa.
VLAN	<i>Virtual Local Area Network</i> . Mahdollistaa verkon jakamisen loogisiin osiin välittämättä siitä missä laitteet sijaitsevat fyysisesti.

1 Johdanto

Tätä työtä kirjoittaessani lähes 99 % Internetin liikenteestä reitittyy IPv4-protokollan välityksellä. Tämä tulee tulevina vuosina muuttumaan, koska IPv4-osoitteet alkavat olla loppuun käytettyjä kaikkialla maailmassa. Ratkaisu tähän ongelmaan tulee olemaan IPv6-protokolla, joka tarjoaa massiivisen määrän uusia IP-osoitteita käytettäväksi. IPv4 ja IPv6 tulevat olemaan yhtä aikaa käytössä vielä monia vuosia. IPv6:n käyttö tulee laajenemaan räjähdysmäisesti, kun viimeisetkin vapaana olevat IPv4-osoitteet on otettu käyttöön. (20.)

Siirtyminen IPv4-protokollasta IPv6-protokollaan tuo laajemman osoiteavaruuden lisäksi monia muita etuja. Tarve uusille IP-osoitteille laittoi liikkeelle IPv6-protokollan kehityksen, mutta samalla tähän uuteen protokollaan kehiteltiin lukuisia parannuksia.

Insinööriyön tarkoituksena on suunnitella ja toteuttaa täysin toimiva IPv6-lähiverkko esimerkkiyritykselle. Työ sisältää myös teoreettisen suunnitelman yrityksen siirtymisestä IPv4-lähiverkosta IPv6-lähiverkkoon käyttäen kaksoispinoteknologiaa (dual-stack technology).

2 Teoria

2.1 IPv6-protokollan uudistukset

Ensimmäinen syy, miksi IPv4-protokollasta pitäisi siirtyä IPv6-protokollaan, on laajempi IP-osoiteavaruus (IP address space). Tämä ei ole kuitenkaan ainoa muutos tässä uudistuksessa. Mitä parannuksia IPv6 tuo tullessaan?

IPv4-osoite on 32-bittiä pitkä, ja sen IP-osoitteiden mahdollinen lukumäärä lasketaan kaavalla 2^{32} . Tulokseksi tulee lähes 4,3 biljoonaa eri IP-osoitetta, joista lähes kaikki on jo käytössä. IPv6-osoite suunniteltiin tarjoamaan lähes loppumaton määrä IP-osoitteita, ettei sama ongelma tulisi vastaan seuraavilla sukupolvillakaan. IPv6-osoite on pituudeltaan 128-bittiä ja IP-osoitteiden lukumäärä lasketaan vastaavasti kaavalla 2^{128} . Tulokseksi syntyy noin 3.4×10^{38} eri IP-osoitetta, mikä auki kirjoitettuna olisi yli 300 triljoonaa triljoonaa osoitetta.

Taulukko 1. IPv4- ja IPv6-osoitteiden kokonaislukumäärät (3.)

IPv4-osoitteiden kokonaislukumäärä 2^{32}	IPv6-osoitteiden kokonaislukumäärä 2^{128}
4 294 967 296	340 282 366 920 938 463 463 374 607 431 768 211 456

Taulukko 1 näyttää vielä IPv4- ja IPv6-osoitteiden kokonaislukumäärät auki laskettaessa. (2, s. 369.; 3.)

IPv6-osoitteen laajentaminen näin suureksi mahdollistaa IP-osoitteiden hierarkkisen levittämisen sekä palveluntarjoaja- että organisaatiotasolla. Laajentaminen myös mahdollistaa laitteiden IP-osoitteiden luonnin pelkän MAC-osoitteen (Media Access Control) avulla. Tämä helpottaa laitteiden autokonfiguraatiota. Laaja IPv6-osoite parantaa turvallisuutta porttiskannaushyökkäystä (port scanning attack) vastaan. Porttiskannaushyökkäys yrittää etsiä kohteesta haavoittuvuuksia skannaamalla kohteen portteja yksitellen läpi. Laajennetun IPv6-osoitteen ansiosta tämän hyökkäysmallin tehokkuus heikentyy huomattavasti. (2, s. 369; 16.)

IPv4:n yleislähetys (broadcast) on korvattu paremmalla ryhmälähetyksellä (multicast) ja aivan uusi lähetystyyppi, jokulähetys (anycast), on lisätty protokollaan. Myös QoS:lle (Quality of Service) on tehty parannuksia, jotka parantavat tukea multimedialle ja muille QoS:ää käyttäville sovelluksille. (2, s. 369.)

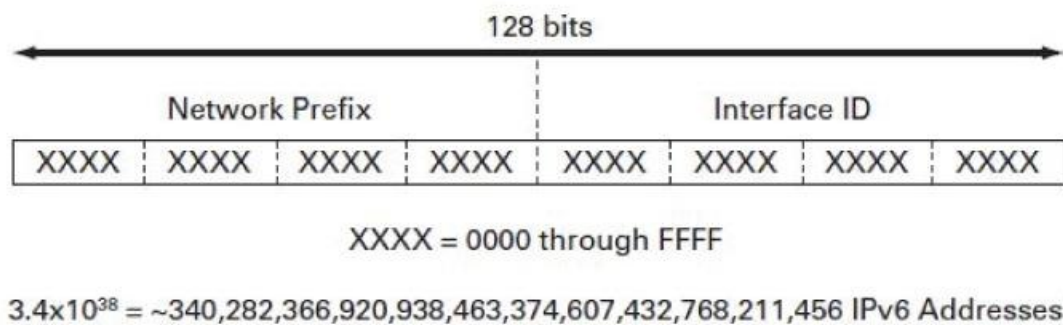
IPv6-protokolla parantaa IP-pakettien reitittämisenopeutta jättämällä reitittimiltä kokonaan pois muutaman tehtävän, jotka ovat olleet käytössä IPv4-protokollassa. Suurikokoiset IP-paketit täytyy jakaa osiin siirron ajaksi ja koota jälleen takaisin yhdeksi kokonaisuudeksi määränpäässä. Tämä on yksi reitittimen tehtävistä, kun käytössä on IPv4. IPv6:ssa paketin osiin jakaminen ja kokoaminen on suunniteltu lähde- ja päätelaitteiden tehtäviksi, joten reitittimille jää enemmän aikaa IP-pakettien eteenpäin toimittamiselle. IPv6 jättää myös IP-pakettien eheystarkistuksen (integrity check) pois reitittimien toimenkuvasta, mikä puolestaan maksimoi reitittimien siirtonopeuksia. (6; 7.)

IPv6 parantaa tukea mobiililaitteiden verkkojen väliselle siirtymiselle. IPv6 mahdollistaa saman IP-osoitteen pitämisen vaikka siirtyisi verkosta toiseen. Tämä poistaa tarpeen kolmioreitittämiselle (triangular routing), jossa mobiililaitteelle tarkoitettu data joudutaan lähettämään mobiililaitteen palveluntarjoajan kautta. Tämän ansiosta mobiililaitteiden nopeudet ja yhteydet ovat paremmat sekä luotettavammat. (6; 7.)

2.2 IPv6-osoitteen formaatti

IPv6-osoite on 128 bittiä pitkä ja se on jaettu kahdeksaan 16 bitin kokoiseen ryhmään. Jokaisessa ryhmässä on neljä heksadesimaalista lukua ja ryhmien jako merkitään kaksoispisteellä. 2001:0db8:72ab:0000:0000:be03:3002:0001 on esimerkki IPv6-osoitteesta. Osoitetta on mahdollista lyhentää merkitsemällä kaikki peräkkäiset nollat kahdella kaksoispisteellä. Tätä lyhennystä on mahdollista käyttää vain yhden kerran osoitteessa. Jokaisen 16 bitin ryhmän edeltävät nollat (leading zeros) on myös mahdollista jättää osoitteesta pois. 2001:db8:72ab::be03:3002:1 on lyhennetty versio esimerkiosoitteesta. (1.)

Tämän lisäksi IPv6-osoitteen 128-bittiä on jaettavissa kahteen eri osaan, jotka ovat verkon etuliite (network prefix) sekä liitännän identiteetti (interface ID). (1.)



330522

Kuva 1. IPv6-osoitteen formaatti (1.)

Kuva 1 näyttää, miten 128 bittiä jakautuvat yleisesti IPv6-osoitteessa. Ensimmäiset 64 bittiä kuuluvat verkon etuliitteeseen ja loput 64 bittiä liitännän identiteettiin.

2.3 IPv6-lähetysformaatit

Täsmälähetys

IPv6:n yleisin osoitemuoto on täsmälähetys (unicast), joka lähettää viestin yhteen kohteeseen. Globaali täsmälähetysosoite on ainutlaatuinen osoite, jonka avulla eri

laitteet kommunikoivat keskenään Internetin välityksellä. Globaalin täsmälähetysosoitteen 128 bittiä jakautuvat yleisesti kolmeen eri kategoriaan.

Taulukko 2. Globaalin täsmälähetysosoitteen jaottelu (11.)

3-bittiä	45-bittiä	16-bittiä	64-bittiä
001	Globaali reititysetuliite	Aliverkon identiteetti	Liitännän identiteetti

Taulukko 2 näyttää, miten 64-bittinen verkon etuliite on nyt jaettu kahteen osaan, globaaliin reititysetuliitteeseen (global routing prefix) sekä aliverkon identiteettiin (subnet ID). IANA on määritellyt, että kaikki tämän hetkisten globaalien täsmälähetysosoitteiden etuliitteet alkavat binääriarvolla 001. Globaali reititysetuliite on normaalisti 48 bittiä pituudeltaan, mutta voi RIR-organisaation käytännöistä riippuen olla jopa 56 bittiä pitkä. Aliverkon identiteetti on taas normaalisti 16 bittiä, mutta voi laskea 8 bittiin asti RIR-organisaation käytäntöjen vuoksi. (8; 9; 11; 12.)

Toinen täsmälähetystyyppi globaalin täsmälähetysosoitteen lisäksi on linkkilokaaliosoite (link-local address). Nämä osoitteet ovat tarkoitettu vain yksittäisen verkon sisäiseen käyttöön ja määräytyvät laitteen MAC-osoitteen mukaan. Näitä osoitteita ei koskaan reititetä verkon ulkopuolelle. Linkkilokaaliosoite mahdollistaa pienten lähiverkkojen toteuttamisen nopeasti ja yksinkertaisesti. Linkkilokaaliosoitteen etuliite on normaalisti fe80::/10. (8; 9; 12.)

Ryhmälähetykset

IPv6:n ryhmälähetykset korvaa IPv4:n yleislähetysten. IPv4:n yleislähetys lähettää viestin kaikille verkkoon kuuluville kohteille. Tämän takia vaarana oli, että yleislähetysviestit jäivät pyörimään yhdistettyjen kytkimien väliin aiheuttaen yleislähetysmyrskyn (broadcast storm) ja täten estävän tavallisen liikenteen verkossa. IPv6:n ryhmälähetyksessä viesti lähetetään vain kohteille, jotka kuuluvat kyseiseen ryhmälähetysryhmään (multicast group). Ryhmälähetysosoite alkaa aina heksadesimaaliarvolla ff. Kaksi käytetyintä ryhmälähetysosoitetta on ff02::1 ja ff02::2. Ff02::1 lähettää viestin lähiverkon segmentin jokaiselle solmulle (node), kun taas ff02::2 lähettää viestin lähiverkon segmentin jokaiselle reitittimelle. (8; 9; 10.)

Jokulähetys

Jokulähetys on IPv6:n uusi lähetystyyppi. Jokulähetyksellä voi olla monia kohteita, mutta viesti toimitetaan vain ensimmäiselle kohteelle, jonka viesti saavuttaa. Tämä mahdollistaa kuorman tasapainottamisen sekä automaattisen varajärjestelmän. Vaikka yksi palvelin olisikin saavuttamattomissa, niin jokulähetysviesti menisi perille seuraavalle mahdolliselle palvelimelle. Jokulähetys ei käytä mitään erityistä osoitealuetta. Jokulähetysosoite luodaan automaattisesti, kun sama täsmälähetysosoite konfiguroidaan useampaan kuin yhteen liitántään. (9;15.)

2.4 IPv6-osoiteavaruus

IPv6-osoitteiden jako tapahtuu hierarkkisesti. Tavalliset kotikäyttäjät ja yritykset saavat IP-osoitteensa palveluntarjoajilta. Palveluntarjoajat taas saavat IP-osoitteet oman alueensa RIR-organisaatiolta (Regional Internet Registry). Maailman eri alueisiin jakautuvat RIR-organisaatiot saavat IP-osoitteet IANA:lta (Internet Assigned Numbers Authority), kun tarvetta uusille IP-osoitteille syntyy. (5.)



Kuva 2. RIR-organisaatioiden jakautuminen maailmalla (4.)

Kuva 2 näyttää alueet, joista eri RIR-organisaatiot ovat vastuussa. AfriNIC toimii Afrikan alueella. APNIC on vastuussa Oseanista sekä osasta Aasiaa. ARIN hoitaa Pohjois-Amerikan alueen. LACNICin vastuualue on Latinalainen Amerikka ja osa Karibian saarista. RIPE NCC:n alueeseen kuuluu Eurooppa, Lähi-itä ja Keski-Aasia. (4; 5.)

Taulukko 3. IANA:n jakama IPv6-osoiteavaruus (22.)

IPv6-etuliite	Allokointi
0000::/8	Varattu IETF:lle
0100::/8	Varattu IETF:lle
0200::/7	Varattu IETF:lle
0400::/6	Varattu IETF:lle
0800::/5	Varattu IETF:lle
1000::/4	Varattu IETF:lle
2000::/3	Globaali täsmälähetys
4000::/3	Varattu IETF:lle
6000::/3	Varattu IETF:lle
8000::/3	Varattu IETF:lle
a000::/3	Varattu IETF:lle
c000::/3	Varattu IETF:lle
e000::/4	Varattu IETF:lle
f000::/5	Varattu IETF:lle
f800::/6	Varattu IETF:lle
fc00::/7	Ainutlaatuinen lokaali täsmälähetys
fe00::/9	Varattu IETF:lle
fe80::/10	Linkkilokaali täsmälähetys
fec0::/10	Varattu IETF:lle
ff00::/8	Ryhmälähetys

Taulukko 3 käy läpi IANA:n jakaman IPv6-osoiteavaruuden. Globaalitäsmälähetykselle varattu 2000::/3 IPv6-osoitelohko (IPv6 address block) käsittää 1/8 osaa koko IPv6-osoiteavaruudesta. Monia osoitelohkoja on varattu Internet Engineering Task Forcen (IETF) käyttöön. IETF on organisaatio, joka kehittää ja vastaa Internet-protokollien standardoinnista. Käyttämätöntä IPv6-osoiteavaruutta on vielä paljon jäljellä. IANA tulee allokoimaan ja määrittelemään uusia tarkoituksia käyttämättömille IPv6-osoitteille tarpeen mukaan. Ainutlaatuiseen lokaaliin täsmälähetysjoukkoon kuuluu IPv6-

osoitelohko 2001:db8::/32, jota tulisi käyttää esimerkkidokumentaatioissa. (22; 23; 24; 25.)

2.5 IPv6:n autokonfiguraatio

IPv6 tarjoaa kaksi erilaista autokonfiguraatiomahdollisuutta laitteille. Toista näistä muodoista kutsutaan nimellä tilallinen autokonfiguraatio (stateful autoconfiguration). Tilallinen autokonfiguraatio vaatii toimiakseen verkkoon asennettua ja liitettyä DHCPv6-palvelinta (Dynamic Host Configuration Protocol version 6). DHCPv6-palvelin jakaa IP-osoitteita uusille laitteille, jotka kytketään kiinni samaan lähiverkkoon missä kyseinen palvelin myös sijaitsee. (13.)

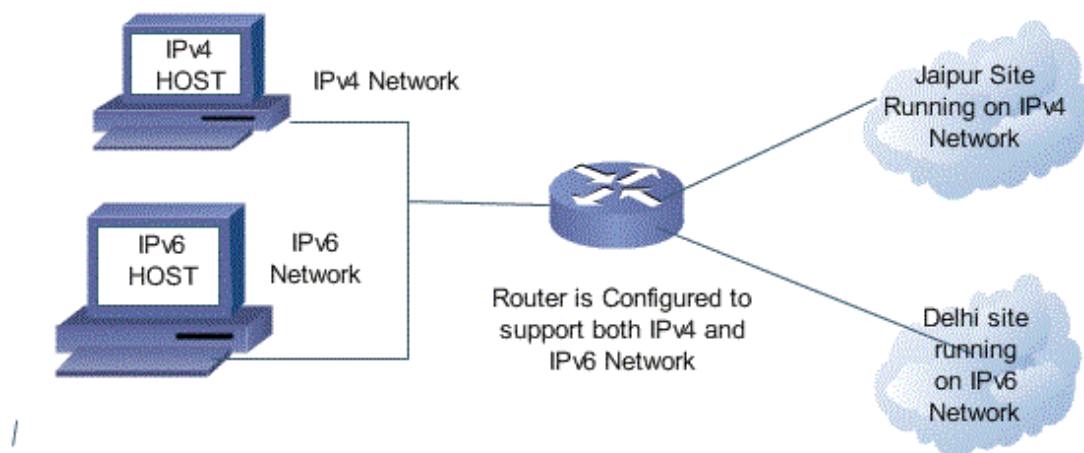
Toista autokonfiguraatiomuotoa kutsutaan tilattomaksi autokonfiguraatioksi (stateless autoconfiguration). Tämä on kokonaan uusi IPv6:n mahdollistama autokonfiguraatiomuoto, joka toimii ilman DHCP-palvelinta. Aluksi laite generoi itsellensä linkkilokaaliosoitteen, jossa verkon etuliitteeseen kuuluvat 64-bittiä on ennalta määrätty ja liitännän identiteetin 64-bittiä saadaan tyypillisesti laitteen MAC-osoitteen avulla. Linkkilokaaliosoitteen avulla laite pystyy olemaan yhteydessä muiden samassa lähiverkossa olevien laitteiden kanssa. Laite voi tämän jälkeen ottaa yhteyden reitittimeen, joka osaa sitten kertoa laitteelle kumman tyylinen autokonfiguraatio verkossa on käytössä. Jos käytössä on tilallinen autokonfiguraatio, niin reititin ohjaa laitteen hakemaan IP-osoitetta DHCPv6-palvelimelta. Tilattoman autokonfiguraation ollessa käytössä, reitittimellä on tiedossa palveluntarjoajalta saatu verkon etuliite ja kertoo tämän tiedon laitteelle. Laite konfiguroi globaalin IP-osoitteen itsellensä tämän tiedon avulla ja on sitten valmis kommunikoimaan lähiverkon ulkopuolellakin. Globaalin IP-osoitteen liitännän identiteetti luodaan yleensä tässäkin vaiheessa laitteen MAC-osoitteen avulla. (13; 14.)

2.6 Siirtymätekniikat

Kaksoispino

Kaksoispinoverkolla (dual-stack network) tarkoitetaan verkkoa, joka tukee yhtäaikaaisesti sekä IPv4- että IPv6-protokollaa. Kaksoispino suosii IPv6-protokollan

käyttöä tilanteissa, joissa pitää valita IPv4- tai IPv6-protokollan käytön väliltä. Kaksoispino mahdollistaa IPv4-liikenteen käsittelyn normaalisti, vaikka IPv6-liikennettä ei olisi mukana ollenkaan.



Kuva 3. Kaksoispinoteknologialla toteutettu lähiverkko (21.)

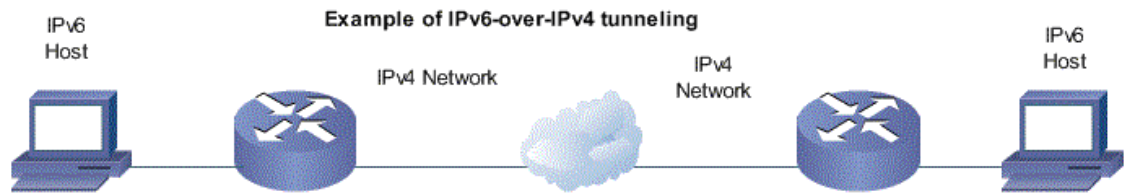
Kuva 3 näyttää esimerkin kaksoispinoteknologialla toteutetusta lähiverkosta. Lähiverkon yksi työasema käyttää IPv4-protokollaa ja toinen IPv6-protokollaa. Molemmat työasemat on liitetty reitittimeen, joka on konfiguroitu tukemaan molempia IP-protokollia. Reititin pystyy reitittämään liikennettä eteenpäin riippumatta siitä, onko kohteena IPv4- vai IPv6-verkko. (21.)

Kaksoispinoteknologialla on vain yksi heikkous. Verkon jokaisen laitteen täytyy tukea sekä IPv4- että IPv6-protokollaa. Monilla yrityksillä on todennäköisesti vanhoja reitittimiä ja kytkimiä, joilla ei ole tukea IPv6-protokollalle. Tämänlaisessa tapauksessa yrityksen pitäisi ensin päivittää kaikki verkon laitteet tukemaan IPv6-protokollaa, mikä tulisi mahdollisesti kalliiksi. Verkon työasemia ja niihin asennettuja sovelluksia voi kuitenkin päivittää vähitellen tukemaan IPv6-protokollaa. Nämä työasemat ja niiden sovellukset voivat käyttää IPv4-protokollaa siihen asti, kun tarvittavat toimenpiteet on tehty IPv6-protokollan tukemiseksi. (17; 18; 19.)

Tunnelointi

Toinen tapa IPv6-liikenteen kuljettamiselle verkoissa, jotka eivät suoraan tue IPv6-protokollaa, on tunnelointi. Tunneloinnissa IPv6-paketit kuljetetaan IPv4-verkoissa

IPv4-pakettien sisällä. Tämä on myös mahdollista toteuttaa käänteisesti eli kuljettaa IPv4-paketteja IPv6-verkoissa IPv6-pakettien sisällä. Tunnelointi lisää valitettavasti lähetysten viivettä ja vähentää liikenteen turvallisuutta. (18; 19.)



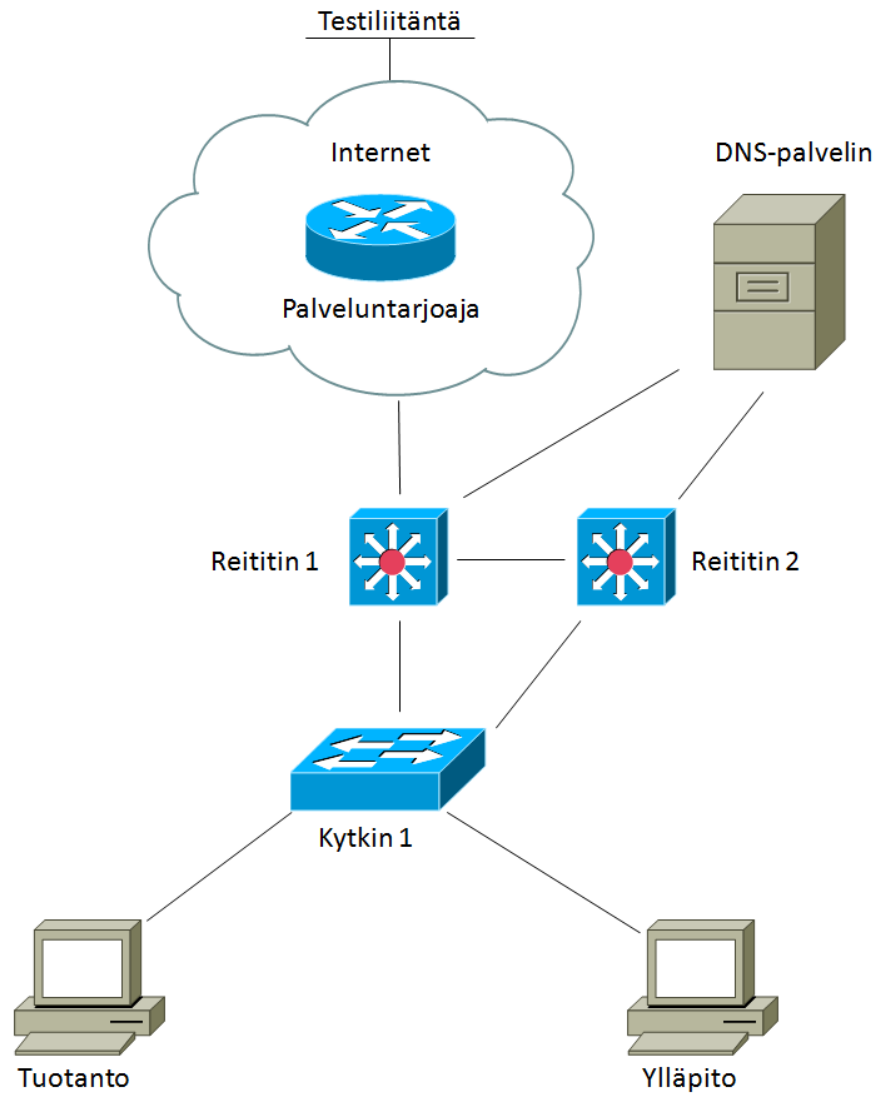
Kuva 4. 6to4-tunnelointitekniikalla toteutettu verkko (21.)

Kuvassa 4 on kaksi IPv6-protokollaa käyttävää työasemaa, jotka on liitetty kiinni kahteen eri reitittimeen. Näiden kahden verkon välissä on vain IPv4-protokollaa käyttävä verkko-osuus, joten työasemat eivät voi kommunikoida keskenään pelkän IPv6-protokollan avulla. Kahden reitittimen väliin rakennetaan 6to4-tunneli, joka mahdollistaa IPv6-protokollan liikenteen kuljettamisen IPv4-verkon läpi IPv4-pakettien sisällä. IPv6-liikenne paketoitetaan ensimmäisellä reitittimellä ja puretaan auki saavutettuaan toisen reitittimen. (21.)

3 Esimerkkiyrityksen IPv6-lähiverkko

3.1 Yrityksen IPv6-lähiverkon verkkotopologia

Esimerkkiyrityksenä toimii yritys, jossa työskentelee 20 työntekijää. Yritys saa yhteyden Internetiin yhden reitittimen kautta. Internetyhteyttä kuvaa palveluntarjoajan reitittimeen konfiguroitu testiliitäntä (loopback). Jos yhteyskokeilut (ping tests) toimivat testiliitännään saakka ongelmitta, niin laitteella on yhteys Internetiin.



Kuva 5. IPv6-lähiverkon verkkotopologia.

Kuva 5 näyttää esimerkkiyrityksen IPv6-lähiverkon verkkotopologian. Työasemat kuvaavat yrityksen kahta aliverkkoa, tuotantoa ja ylläpitoa. Esimerkissä aliverkot koostuvat vain yhdestä työasemasta, mutta voivat käytännössä olla kymmenien tai satojen työasemien suuruisia. Yrityksen lähiverkon topologia on suunniteltu siten, että verkon kaksi aliverkkoa on liitettyinä kytkimeen mahdollistaen virtuaalilähiverkkojen toteuttamisen helposti. Reititin 1 toimii lähiverkon yhteytenä palveluntarjoajaan sekä reitittää yrityksen sisäistä liikennettä. Reititin 2 on taas valmiina reitittämään yrityksen sisäistä liikennettä, jos ongelmia syntyisi reitittimen 1 kanssa. Yrityksen DNS-palvelin (Domain Name System) on saavutettavissa reitittimien 1 ja 2 kautta. Tämä mahdollistaa yhteyden DNS-palvelimeen vaikka toisessa reitittimessä olisi jotain ongelmia. Esimerkkiyrityksen DNS-palvelin on toteutettu virtuaalinekonetta käyttäen,

jossa on vain yksi verkkosovitin. Yksi verkkosovitin mahdollistaa DNS-palvelimen liittämisen vain toiseen reitittimistä. Tämän vuoksi DNS-palvelimen yhteys reitittimeen 1 on vain teoriatasolla.

3.2 Osoitesuunnitelma yrityksen IPv6-lähiverkolle

Oletetaan, että yritys saa palveluntarjoajalta 2001:db8:aaaa::/48 IPv6-osoitelohkon käyttöönsä. Tämä tarkoittaa, että yrityksen IPv6-osoitteiden globaali reititysetuliite määräytyy valmiiksi palveluntarjoajan mukaan. Aliverkon identiteetti on kuitenkin kokonaan yrityksen käytettävissä, ja aliverkot on mahdollista suunnitella alusta alkaen omilla ehdoilla. Yritys on päätnyt jakamaan lähiverkon kahteen suureen osaan, jotka ovat tuotanto ja ylläpito. Tuotannolle määritellään aliverkko 2001:db8:aaaa:4::/64 käyttöön ja ylläpito saa käyttöönsä aliverkon 2001:db8:aaaa:5::/64.

Tämän lisäksi molemmat aliverkot konfiguroidaan omiin virtuaalilähiverkkoihin. VLAN (Virtual Local Area Network) mahdollistaa verkkolaitteiden liittämisen haluttuihin lähiverkkoihin vaikka kaikki laitteet eivät fyysisesti sijaitsisikaan toistensa lähellä. Esimerkiksi yrityksen ensimmäisessä kerroksessa oleva laite voi olla samassa virtuaalilähiverkossa yrityksen toisessa kerroksessa sijaitsevien verkkolaitteiden kanssa. Näin ei ole tarvista lähteä siirtämään ensimmäisen kerroksen laitetta toisen kerroksen laitteiden viereen fyysisesti tai ryhtyä yhdistämään tätä yksinäistä konetta pitkillä verkkojohdoilla haluamaansa lähiverkkoon. Miksi yritys haluaa jakaa lähiverkon kahteen eri osaan? Lähiverkon jakaminen kahdeksi aliverkoiksi mahdollistaa erilaisten sääntöjen asettamisen. Ylläpidolle olisi mahdollista konfiguroida ylimääräisiä oikeuksia kuten etäyhteyden ottamisen verkon reitittimiin ja kytkimeen. Tämä helpottaisi ylläpidon työtä, kun konfiguraatiotehtäviä tehdessä ei olisi pakko siirtyä itse laitteen luokse. Tuotannon aliverkkoon kuuluvat laitteet eivät tässä tapauksessa voisi vahingossakaan ottaa etäyhteyttä reitittimiin tai kytkimeen vaikka haluaisivatkin.

3.3 Käytetyt laitteet ja ohjelmaversiot

Esimerkkiyrityksen lähiverkossa on käytössä kolme reititintä, kytkin ja kolme työasemaa, joista yksi toimii DNS-palvelimena. Reitittiminä toimii kolme kappaletta Cisco 2801 -reititintä, joissa on käytössä IOS-versio (Internetwork Operating System)

12.4(24)T5. Kytkimen malli on Cisco Catalyst 3550 -sarjan Cisco WS-C3550-24, joka käyttää IOS-versiota 12.2(44)SE2. Kolmessa työasemassa on käytössä Windows 7 Enterprise -käyttöjärjestelmät. Yhdelle näistä työasemista on asennettu Ubuntu Server-käyttöjärjestelmän versio 12.10 käyttämällä Oracle VM VirtualBox-virtuaalikoneohjelman versiota 4.2.6. DNS-palvelinohjelmana käytettiin BIND-ohjelman versiota 9.8.1. Kyseinen työasema toimii yrityksen DNS-palvelimena.

3.4 Laitteiden määrittelyt

Reitittimet ja kytkimet

IPv6-lähiverkon konfigurointi reitittimien ja kytkimien kannalta ei poikkea paljoakaan IPv4-lähiverkosta. Monet komennot ovat lähes identtisiä IPv4-komentojen kanssa. Esimerkiksi IPv4:n komento "show ip route" muuttuu IPv6:ssa "show ipv6 route" komennoksi. Tämä helpottaa siirtymistä IPv4:stä IPv6:een, kun IPv6-komennot ovat sisäistettävissä kohtuullisen helposti ja nopeasti.

Kaksoispinon konfigurointi on myös erittäin yksinkertaista. Laitteiden liitännöille konfiguroidaan erikseen IPv4- ja IPv6-osoitteet, tarvittavat reititystiedot molemmalle protokollalle sekä aktivoidaan IPv6-reititys laitteessa komennolla "ipv6 unicast-routing". Mitään muuta mutkikasta konfigurointia ei tarvitse, vaan laite on valmis reitittämään sekä IPv4- että IPv6-liikennettä.

Palveluntarjoajareitittimeen on konfiguroitu testiliitäntä, joka kuvaa esimerkiverkon internetyhteyttä. Tähän reitittimeen on myös määritelty staattinen reitti kohti yrityksen lähiverkkoa, jotta yrityksen yhteyskokeilut testiliitääntään osaavat palata takaisin esimerkkiyrityksen lähiverkkoon. Kyseinen staattinen reitti kuvaa palveluntarjoajan ja yrityksen välistä reititystä. Yrityksen kytkimeen on määritelty virtuaalilähiverkot tuotanto ja ylläpito. Virtuaalilähiverkko tuotanto on liitetty toiseen työasemaan ja ylläpito toiseen. Kytkimeen on myös määritelty virtuaalilähiverkoille yhteydet yrityksen reitittimiin, jotka pystyvät sitten reitittämään virtuaalilähiverkkojen välisen liikenteen.

Yrityksen lähiverkon reitittimet ovat konfiguroitu reitittämään liikennettä virtuaalilähiverkkojen välillä. Virtuaalilähiverkot eivät pysty normaalisti kommunikoimaan keskenään ilman verkkolaitetta, joka on konfiguroitu kuljettamaan

liikenteen verkkojen välillä. Jos toiseen reitittimeen tulee jokin ongelma ja se ei pysty hoitamaan virtuaalilähiverkkojen reititystä, niin toinen vapaana oleva reititin ottaa kyseisen työn tehtäväkseen. Reitittimien 1 ja 2 välinen yhteys voi helpottaa vianetsintätilanteissa. Esimerkiksi yrityksen verkon kytkin menee jostain syystä epäkuntoon. Ensin reitittimen välinen toimivuus todetaan yhteyskokeiluilla. Tämän jälkeen huomataan, etteivät yhteyskokeilut kytkimeen palaa kumpaankaan reitittimeen. Tässä tapauksessa vika on luultavasti kytkimessä ja vianetsintä kannattaa aloittaa siitä. Reitittimeen 2 on lisäksi määritelty yhteys DNS-palvelimen ja reitittimen välille.

Työasemat

IPv6 ei tuota vaikeuksia työasemien kanssa sillä kaikki nykyajan käyttöjärjestelmät tukevat IPv4- ja IPv6-protokollaa. Työasemat saavat yleensä IPv6-osoitteet IPv6-autokonfiguraation avulla tai DHCPv6-palvelimelta. Työntekijät eivät edes huomaa siirtymistä IPv4:stä IPv6:een, koska kaikki tapahtuu automaattisesti. Ongelmia voi teoreettisesti syntyä työasemiin asennettujen sovellusten kanssa. Oletetaan tilanne, jossa yrityksen lähiverkko tukee vain IPv6-protokollaa. Tässä tapauksessa voi työasemilla olla sovelluksia, jotka vaativat IPv4-protokollan olemassaoloa toimiakseen verkossa. Tämänlaista tapausta ei pitäisi kuitenkaan syntyä, jos yritys pitää huolen sovellusten päivittämisestä eikä lopeta IPv4-protokollan tukea liian aikaisin. Esimerkkiyrityksen työasemien IPv6-osoitteet on määritelty manuaalisesti, koska esimerkiverkossa ei ollut käytössä DHCPv6-palvelinta tai IPv6-autokonfiguraatiota.

DNS-palvelin

Yrityksen DNS-palvelin toteutettiin virtuaalikoneetta käyttäen. Virtuaalikoneeseen asennettiin Ubuntu Server -käyttöjärjestelmä. Käyttöjärjestelmään asennettiin BIND-ohjelma, jonka avulla käyttöjärjestelmä voi toimia DNS-palvelimena. DNS-palvelimen tehtävänä on kääntää käyttäjien antamia verkkosivujen osoitteita numeeriseen muotoon, jota tietokoneet käyttävät keskenään kommunikoidessaan. DNS-palvelimien ansiosta käyttäjien ei tarvitse muistaa pitkiä ja monimutkaisia numerosarjoja halutessaan tietyille internetsivuille, vaan he pääsevät niihin käsiksi kirjoittamalla lyhyitä ja helposti muistettavia internetosoitteita. Yrityksen DNS-palvelin konfiguroitiin kääntämään osoite esimerkki.fi numeeriseen muotoon.

Reitittimen 1 määrittelyesimerkki

Määrittelyesimerkkinä käydään läpi reitittimen 1 määityksiä, jotka löytyvät myös liitteestä 1. Ensimmäisenä IPv6-protokollan reititys aktivoidaan komennolla

```
ipv6 unicast-routing
```

Tämän jälkeen määritellään palveluntarjoajareitittimeen yhteydessä olevalle liitännälle IPv6-osoite ja avataan kyseinen liitäntä komennoilla

```
interface Serial0/1/1

ipv6 address 2001:DB8:AAAA:1::1/64

no shutdown
```

Myös reitittimeen 2 yhteydessä oleva liitäntä avataan samoilla komennoilla

```
interface Serial0/1/0

ipv6 address 2001:DB8:AAAA:2::1/64

no shutdown
```

Samat määritelmät toistetaan liitانتään, joka on kiinni yrityksen lähiverkon kytkimeen, komennoilla

```
interface FastEthernet0/0

ipv6 address 2001:DB8:AAAA:3::1/64

no shutdown
```

Reitittimellä on myös kaksi aliliitaintää (subinterfaces), jotta se pystyy reitittämään virtuaalilähiverkkojen välistä liikennettä. Aliliitännät toteutetaan komennoilla

```
interface FastEthernet0/0.4

encapsulation dot1q 4

ipv6 address 2001:DB8:AAAA:4::4/64
```

```
interface FastEthernet0/0.5

encapsulation dot1Q 5

ipv6 address 2001:DB8:AAAA:5::5/64
```

Seuraavaksi reitittimen reititystauluun konfiguroidaan oletusreitti kohti palveluntarjoajareititintä. Tämä oletusreitti takaa kaiken liikenteen reitityksen kohti palveluntarjoajaa ja sitä kautta Internetiin. Määritelmä toteutetaan komennolla

```
ipv6 route ::/0 2001:DB8:AAAA:1::2
```

Viimeiseksi reitittimeen määritellään myös yrityksen lähiverkon kahden aliverkon tiedot reititystauluun, jotta reititin osaa reitittää verkon sisäisen liikenteen oikein ja lähettää muun liikenteen palveluntarjoajalle. Nämä toteutetaan komennoilla

```
ipv6 route 2001:DB8:AAAA:4::/64 FastEthernet0/0

ipv6 route 2001:DB8:AAAA:5::/64 FastEthernet0/0
```

3.5 Testaus

Yrityksen IPv6-lähiverkon toimivuus on mahdollista todeta yhteyskokeiluilla. Yksi tärkeä yhteyskokeilu on tuotannon ja ylläpidon työasemien välinen yhteyskokeilu, joka takaa verkon sisäisen kommunikoinnin toimivuuden. Molempien virtuaalilähiverkkojen työasemien yhteyskokeilut palveluntarjoajan testiliitانتään ovat tärkeitä, koska se simuloi kyseisten laitteiden yhteyttä Internetiin. Myös yhteyskokeilu virtuaalilähiverkkojen työkoneiden välillä, kun toinen reitittimistä irrotetaan tarkoituksella lähiverkosta, näyttää, onko varajärjestelmä toimiva vai ei. DNS-palvelimen toimivuus on mahdollista tarkastaa tekemällä yhteyskokeilu työasemalta johonkin osoitteeseen, jota DNS-palvelin on määritetty kääntämään.

Ensimmäinen yhteyskokeilu suoritettiin tuotantovirtuaaliverkon työasemasta ylläpitovirtuaalilähiverkon työasemaan.

```
Pinging 2001:db8:aaaa:5::1 with 32 bytes of data:

Reply from 2001:db8:aaaa:5::1: time<1ms
```

```

Reply from 2001:db8:aaaa:5::1: time<1ms

Reply from 2001:db8:aaaa:5::1: time<1ms

Reply from 2001:db8:aaaa:5::1: time<1ms

Ping statistics for 2001:db8:aaaa:5::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Yhteyskokeilu onnistui, ja tämän avulla todettiin virtuaalilähiverkkojen välisen liikenteen olevan kunnossa. Tämän jälkeen selvitettiin ovatko työasemien yhteydet kunnossa palveluntarjoajareitittimen testiliitانتään asti. Ensin tuotantovirtuaalilähiverkon työasemasta otettiin yhteys testiliitانتään.

```

Pinging 2001:db8:bbbb:1::1 with 32 bytes of data:

Reply from 2001:db8:bbbb:1::1: time=27ms

Reply from 2001:db8:bbbb:1::1: time=23ms

Reply from 2001:db8:bbbb:1::1: time=23ms

Reply from 2001:db8:bbbb:1::1: time=23ms

Ping statistics for 2001:db8:bbbb:1::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 23ms, Maximum = 27ms, Average = 24ms

```

Yhteyskokeilun vastaus palasi tässäkin tapauksessa takaisin ja tuotantovirtuaalilähiverkon työaseman yhteys Internetiin varmistettiin. Seuraavaksi sama yhteyskokeilu toteutettiin ylläpitovirtuaalilähiverkon työasemalle.

Pinging 2001:db8:bbbb:1::1 with 32 bytes of data:

Reply from 2001:db8:bbbb:1::1: time=27ms

Reply from 2001:db8:bbbb:1::1: time=23ms

Reply from 2001:db8:bbbb:1::1: time=23ms

Reply from 2001:db8:bbbb:1::1: time=23ms

Ping statistics for 2001:db8:bbbb:1::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 23ms, Maximum = 27ms, Average = 24ms

Yhteyskokeilu oli jälleen onnistunut, mikä varmisti molempien työasemien internetyhteyksien olevan kunnossa. Tämän jälkeen suoritettiin jälleen työasemien välinen yhteyskokeilu, mutta tällä kertaa reititin 1 otettiin tarkoituksella irti lähiverkosta.

Pinging 2001:db8:aaaa:5::1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 2001:db8:aaaa:5::1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Yhteyskokeilu ei näyttänyt aluksi toimivan ollenkaan. Yhteyskokeilun vastaus pysyi samanlaisena noin 35 sekuntia, mutta muuttui tämän jälkeen.

Pinging 2001:db8:aaaa:5::1 with 32 bytes of data:

Request timed out.

Request timed out.

Reply from 2001:db8:aaaa:5::1: time<1ms

Reply from 2001:db8:aaaa:5::1: time<1ms

Ping statistics for 2001:db8:aaaa:5::1:

Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Yhteys palasi kuntoon kesken kokeilun, ja se varmistettiin vielä viimeisellä yhteyskokeilulla.

Pinging 2001:db8:aaaa:5::1 with 32 bytes of data:

Reply from 2001:db8:aaaa:5::1: time<1ms

Reply from 2001:db8:aaaa:5::1: time<1ms

Reply from 2001:db8:aaaa:5::1: time<1ms

Reply from 2001:db8:aaaa:5::1: time<1ms

Ping statistics for 2001:db8:aaaa:5::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Työasemien välinen yhteys rupesi jälleen toimimaan noin 35 sekunnin viiveen jälkeen. Työasemien välisen liikenteen reitittämisestä huolehtinut reitittimen 1 poistaminen verkosta katkaisi yhteyden väliaikaisesti. Reititin 2 huomasi tilanteen pienen viiveen jälkeen ja ryhtyi tämän jälkeen huolehtimaan työasemien välisen liikenteen reitityksestä. Viimeisenä yhteyskokeiluna suoritettiin ylläpidon työasemasta

yhteyskokeilu osoitteeseen esimerkki.fi, joka oli konfiguroitu käännettäväksi numeeriseen muotoon yrityksen DNS-palvelimessa.

```
Pinging  esimerkki.fi  [2001:db8:aaaa:6::1]  with  32
bytes of data:

Reply from 2001:db8:aaaa:6::1:  time=3ms

Reply from 2001:db8:aaaa:6::1:  time<1ms

Reply from 2001:db8:aaaa:6::1:  time<1ms

Reply from 2001:db8:aaaa:6::1:  time<1ms

Ping statistics for 2001:db8:aaaa:6::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Myös yrityksen DNS-palvelimen saatiin todistettua toimivaksi tällä yhteyskokeilulla. Yrityksen yhteyksien todettiin olevan kunnossa sekä varajärjestelmän toimivuudelle saatiin varmistus.

4 Yhteenveto

Monelle yritykselle siirtyminen IPv4:stä IPv6:een voi kuulostaa työläältä ja kalliilta toimenpiteeltä. IPv6-protokollaa ei kuitenkaan olla rakennettu tyhjältä pöydältä, vaan lukuisia IPv4-protokollan ominaisuuksia on siirretty uuteen protokollaan muutamien uudistusten myötä. Yritysten verkkoasiantuntijat saattavat aluksi olla hieman epävarmoja aloittaessaan konfiguroimaan IPv6-protokollaa, mutta tulevat huomaamaan yllättävän paljon samanlaisuuksia IPv4-protokollan konfiguroimisen kanssa. Näin ollen mitään suurta uudelleenkouluttamista ei pitäisi IPv6:een siirtyminen vaatia.

Jos yritys on kohtuullisen uusi tai kaikki yrityksen verkkolaitteet ovat ajan tasalla, niin työssä käsitelty kaksoispinoteknologia voisi olla vartenotettava vaihtoehto

siirtymisessä kohti IPv6-protokollaa. Tulevina vuosina yritysten potentiaalisilla asiakkailla voi mahdollisesti olla vain IPv6-protokollaa käyttäviä laitteita. Jos yritys ei ole vielä päivittänyt internetsivujensa toimivuutta IPv6-laitteiden kanssa, niin voi suurienkin voittojen livahtaminen ohi olla mahdollista.

Esimerkkiyrityksen IPv6-lähiverkon konfigurointi onnistui yhteyskokeiluiden perusteella hyvin. Alussa oli hieman vaikeuksia uusien komentojen kanssa, mutta nekin kävivät nopeasti tutuiksi. Esimerkkiyrityksen IPv4- ja IPv6-protokollaa tukevat verkkolaitteet antavat yritykselle hyvän mahdollisuuden kaksoispinoteknologian käyttöön. Tämä myös mahdollistaa helpon ja toimivan ratkaisun yrityksen siirtymiselle IPv6-protokollaan. Jos vanhat laitteet eivät ole ongelma, kaksoispinoteknologia on tehokkain tapa siirtyä IPv4-protokollasta IPv6-protokollaan.

Lähteet

- 1 Overview of IPv6. 2013. Verkkodokumentti. Cisco Systems.
<http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/vA5_1_0/configuration/rtg_brdg/guide/ipv6.html>. Luettu 14.3.2013.
- 2 Kozierok, Charles M.. 2005. The TCP/IP Guide. No Starch Press, Inc.
- 3 IPv6 Address Allocation. 2004. Verkkodokumentti. BogPeople.
<<http://www.bogpeople.com/networking/ipv6/ipv6.shtml>>. Luettu 2.4.2013.
- 4 History of the Regional Internet Registries. 2013. Verkkodokumentti. APNIC.
<www.apnic.net/about-APNIC/organization/history-of-apnic/history-of-the-regional-internet-registries>. Luettu 2.4.2013.
- 5 Number Resources. 2013. Verkkodokumentti. IANA.
<<http://www.iana.org/numbers>>. Luettu 2.4.2013.
- 6 Why switch to IPv6. 2013. Verkkodokumentti. Sophos.
<<http://www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6.aspx>>. Luettu 22.4.2013.
- 7 Unsung benefits of IPv6. 2012. Verkkodokumentti. davidlyness.com.
<<https://davidlyness.com/post/unsung-benefits-of-ipv6/>>. Luettu 22.4.2013.
- 8 Types of IPv6 Addresses. 2013. Verkkodokumentti. OmniSecu.com.
<<http://www.omniseku.com/tcpip/ipv6/types-of-ipv6-addresses.htm>>. Luettu 23.4.2013.
- 9 Understand IPv6 Addresses. 2006. Verkkodokumentti. Enterprise Networking Planet.
<<http://www.enterprisenetworkingplanet.com/netsp/article.php/3633211/Understand-IPv6-Addresses.htm>>. Luettu 23.4.2013.
- 10 What is Broadcast Storm. 2013. Verkkodokumentti. OmniSecu.com.
<<http://www.omniseku.com/cisco-certified-network-associate-ccna/what-is-broadcast-storm.htm>>. Luettu 23.4.2013.
- 11 RFC 3587. 2003. Verkkodokumentti. Internet Engineering Task Force.
<<http://tools.ietf.org/html/rfc3587>>. Luettu 23.4.2013.
- 12 IPv6. 2013. Verkkodokumentti. ZYTRAX.
<<http://www.zytrax.com/tech/protocols/ipv6.html>>. Luettu 23.4.2013.

- 13 IPv6 Auto-Configuration. 2013. Verkkodokumentti. msdn.
<<http://msdn.microsoft.com/en-us/library/ms172318.aspx>>. Luettu 24.4.2013.
- 14 IPv6 Autoconfiguration and Renumbering. 2005. Verkkodokumentti. The TCP/IP Guide.
<http://www.tcpipguide.com/free/t_IPv6AutoconfigurationandRenumbering.htm>. Luettu 24.4.2013.
- 15 IPv6 Multicast and Anycast Addressing. 2005. Verkkodokumentti. The TCP/IP guide. <http://www.tcpipguide.com/free/t_IPv6MulticastandAnycastAddressing-5.htm>. Luettu 24.4.2013.
- 16 RFC 5157. 2008. Verkkodokumentti. Internet Engineering Task Force.
<<http://www.ietf.org/rfc/rfc5157.txt>>. Luettu 25.4.2013.
- 17 Dual Stack Network. 2013. Verkkodokumentti. Technopedia.
<<http://www.techopedia.com/definition/19025/dual-stack-network>>. Luettu 1.5.2013.
- 18 IPv6 and IPv4 Co-existence. 2010. Verkkodokumentti. IT Expert Voice.
<<http://itexpertvoice.com/home/ipv6-and-ipv4-co-existence/>>. Luettu 1.5.2013.
- 19 IPv6: Dual stack where you can; tunnel where you must. 2007. Verkkodokumentti. Network World.
<<http://www.networkworld.com/news/tech/2007/090507-tech-uodate.html>>. Luettu 1.5.2013.
- 20 IPv6. 2013. Verkkodokumentti. Google.
<<http://www.google.com/ipv6/statistics.html>>. Luettu 4.5.2013.
- 21 How to configure Cisco Router with IPv6. 2013. Verkkodokumentti. Computer-NetworkingNotes.com. <<http://computernetworkingnotes.com/ipv6-features-concepts-and-configurations/configure-routers-with-ipv6.html>>. Luettu 4.5.2013.
- 22 Internet Protocol Version 6 Address Space. 2013. Verkkodokumentti. Internet Assigned Numbers Authority. <<http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml>>. Luettu 4.5.2013.
- 23 IPv6 Address Space Allocation. 2005. Verkkodokumentti. The TCP/IP guide. <http://www.tcpipguide.com/free/t_IPv6AddressSpaceAllocation-3.htm>. Luettu 4.5.2013.
- 24 The Internet Engineering Task Force. 2013. Verkkodokumentti. Internet Engineering Task Force. <<http://www.ietf.org/>>. Luettu 4.5.2013.
- 25 RFC 3849. 2004. Verkkodokumentti. Internet Engineering Task Force. <<http://tools.ietf.org/html/rfc3849>>. Luettu 4.5.2013.

Reitittimen 1 konfiguraatio

```
!  
  
hostname R1  
  
!  
  
ip cef  
  
ipv6 unicast-routing  
  
ipv6 cef  
  
!  
  
interface FastEthernet0/0  
  
no ip address  
  
duplex auto  
  
speed auto  
  
ipv6 address 2001:DB8:AAAA:3::1/64  
  
!  
  
interface FastEthernet0/0.4  
  
encapsulation dot1Q 4  
  
ipv6 address 2001:DB8:AAAA:4::4/64  
  
!
```

```
interface FastEthernet0/0.5
```

```
encapsulation dot1Q 5
```

```
ipv6 address 2001:DB8:AAAA:5::5/64
```

```
!
```

```
interface FastEthernet0/1
```

```
no ip address
```

```
shutdown
```

```
duplex auto
```

```
speed auto
```

```
!
```

```
interface Serial0/1/0
```

```
no ip address
```

```
ipv6 address 2001:DB8:AAAA:2::1/64
```

```
!
```

```
interface Serial0/1/1
```

```
no ip address
```

```
ipv6 address 2001:DB8:AAAA:1::1/64
```

```
!
```

```
ipv6 route 2001:DB8:AAAA:4::/64 FastEthernet0/0
```

```
ipv6 route 2001:DB8:AAAA:5::/64 FastEthernet0/0
```

```
ipv6 route ::/0 2001:DB8:AAAA:1::2
```

```
!
```

```
line con 0
```

```
exec-timeout 0 0
```

```
logging synchronous
```

```
line aux 0
```

```
line vty 0 4
```

```
login
```

```
!
```

```
end
```