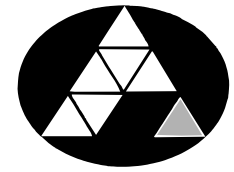
POHJOIS-KARJALAN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Esa Heittokangas

IPV6-OPETUSVERKKO POHJOIS-KARJALAN AMMATTIRKOKEAKOULUSSA

Opinnäytetyö
Kesäkuu 2011



OPINNÄYTETYÖ
Kesäkuu 2011
Tietotekniikan koulutusohjelma
karjalankatu 3
80200 JOENSUU
p. (013) 260 600

Tekijä
Esa Heittokangas

Nimeke
IPv6 Opetusverkko

Pohjois-Karjalan ammattikorkeakoulu

Tiivistelmä

Internet on noussut nykypäivänä suureen osaan ihmisten elämää viime aikoina. Yritykset ja laitokset pyrkivät verkostoimaan itseään yhä enemmän. Asiointia verkossa on myös helpotettu laitteiden hinnan laskun sekä tarjonnan lisäämisen avulla. Internetin käytön lisääntyminen tuo myös mukanaan ongelmia. Kaikki päätelaitteet tarvitsevat itselleen oman uniikin IP-osoitteen, jolla toimia verkossa. Tällä hetkellä käytössä olevat osoiteavaruudet eivät riitä tulevaisuudessa kaikkiin käyttäjien laitteisiin, jolloin on siirryttävä uuten tekniikkaan. IPv6-protokolla on uusi tekniikka, joka mahdollistaa enemmän uusien laitteiden liittymistä yhteiseen Internetiin.

Opinnäytetyön aiheena oli perehtyä IPv6-protokollaan ja toteuttaa tietoliikenneverkko Pohjois-Karjalan ammattikorkeakoulun laboratoriossa. Opinnäytetyön käytännön osiossa käytettiin apuna vmWaren vSphere -virtualisointiohjelmaa sekä Microsoftin Server2008R2-palvelinohjelmistoa. Käytetty laitteisto oli Cisco -merkkisiä reitittimiä sekä kytkimiä. Laitteisto ja tarvittavat ohjelmat oli saatavilla koulun laboratoriossa.

Tutkimuksessa käytetty lähdemateriaali on alan kirjallisuutta, luotettavaa Internet-opetusmateriaalia sekä Microsoft -ohjemateriaalia. Työn tuloksista selviää mahdolliset kehitysmahdollisuudet opinnäytetyölle. Johtopäätökset osio sisältää yleismietteitä työstä kokonaisuudessaan.

Kieli
Suomi

Sivuja
37

Avainsanat

IPv6, IPv4, Protokolla

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

THESIS
June 2011
Degree Programme in Information Technology
Karjalankatu 3
FIN 80200 JOENSUU
FINLAND
Tel. 358-13-260 600

Author
Esa Heittokangas

Title
IPv6 Educational Network

North Karelia University of Applied Sciences

Abstract

The Internet has recently grown to a large part of people's everyday lives. Companies and institutions are seeking to network themselves more and more. Surfing on the Internet has been facilitated by the decrease in prices of equipment and increase in supply. Since the Internet use among people has increased it has also brought a problems along. All the devices need their own unique IP-address. Someday there will be a time when the addresses are all in use. IPv6-protocol is a new technology which allows a lot more connections to the Internet.

The aim of this thesis was to focus on the IPv6 protocol and carry out telecommunication network in the laboratory of North Karelia University of Applied Sciences. The programs which were used in the practical part of the thesis were vmWare vSphere client and Microsoft Server 2008R2. The Equipment used were Cisco routers and switches. The equipment was located in the school laboratory.

The source material used in the theoretical section is business literature, educational material found in the Internet. Microsoft 2008 server manual was also used. The results also shows the potential development opportunities for this thesis. Conclusions section contains general ideas about the thesis.

Language	Pages
Finnish	37

Keywords

IPv6, IPv4, Protocol

Käytetyt lyhenteet

6to4	Tunnelointimenelmä, joka on automaattinen. Menetelmässä kuljetetaan IPv6-protokollan paketit IPv4-verkon ylitse liitettynä IPv4-paketteihin.
DAD	Duplicate Address Detection. Tarkistaaa onko verkossa kahta samanlaista IP-osoitetta.
DHCP	Dynamic Host Configuration Protocol. Protokolla, joka jakaa automaattisesti verkko-osoitteita.
DNS	Domain Name System. Nimipalvelujärjestelmä, jolla IP-osoitteet muutetaan nimiksi.
IP	Internet Protocol. Vastuussa tietoliikennepakettien toimittamisesta.
IPSec	Internet Protocol Security. Tietoturvaprotokolla, joka varmistaa tiedon eheyden ja huolehtii todennuksesta sekä salauksesta.
IPv4	Internet Protokolla version 4. Nykyinen tietoliikennepakettien siirtotekniikka.
IPv6	Internet Protocol version 6. Uusi tuleva tietoliikennepakettien siirtotekniikka.
MAC	Media Access Control. Yksilöi laitteen verkkosovittimen tietoliikenneverkossa.
RIP	Routing Information Protocol. Verkkojen sisäinen reititysprotokolla.

Sisältö

1 Johdanto

Internet on kasvava käsite nykypäivänä. Internetiä käytetään maailman laajuisesti päivittäin erilaisiin tarpeisiin. Internetin käyttäjien käyttötarkoitukset vaihtelevat lähinnä käyttökokemuksen ja iän perusteella, mutta eivät aina. Vanhemmat ihmiset eivät välttämättä käytä Internetiä muuhun, kuin laskujen maksamiseen ja verkkolehtien selaamiseen. Edistyneemmät käyttäjät voivat käyttää Internetiä esimerkiksi erilaisten yhteisöpalvelujen käyttöön, tiedostojen lähettämiseen ja videoleikkeitten katseluun sekä verkkolevyjen käyttöön. Suurin osa näistä käyttäjistä rajautuu nuoriin ja keski-ikäisiin käyttäjiin.

Internetin käyttäjämäärän kasvun myötä myös mobiililaitteiden käyttö verkossa on lisääntynyt. Tämä tarkoittaa sitä, että uusia laitteita kytketään lähes päivittäin yhteiseen suureen verkkoon ja ne tarvitsevat oman osoitteen toimiakseen tässä suuressa kokonaisuudessa. Jonakin päivänä tulee tilanne, jolloin käyttäjän kytkemä laite ei saakaan omaa IP-osoitetta eikä näin toimikaan verkossa. Tämän estämiseksi on pyritty kehittelemään erilaisia keinoja välttääkseen samanlaisten osoitteiden esiintymisen verkossa. Yksi merkittävimmistä tulevista muutoksista tulee kuitenkin olemaan nykyisestä IPv4-protokollasta uuteen IPv6-protokollaan siirtyminen.

Uuden tekniikan tullessa maailmanlaajuisesti käyttöön on myös otettava huomioon monia seikkoja. Suoraan kääntyminen protokollasta toiseen ei onnistu vaan on kartoitettava, kuinka laitteisto käyttäytyy uudessa ympäristössä ohjelmiston kanssa. IPv6:ssa on hyvinä puolina se, että siinä on erittäin hyvä liikkuvuus, laatu ja laajennettavuusmahdollisuudet. Protokolla sisältää myös hyvän tietoturvatason, joka on toteutettu IPSecillä.

Tässä opinnäytetyössä taustateoria hankittiin verkkomateriaalia sekä aiempaa kokemusta apuna käyttäen. Lisäksi työssä käytettiin apuna alan ammattikirjallisuutta sekä ohjemateriaaleja. Työssä tehtiin taustatutkimusta IPv6 -ja IPv4-protokollista sekä niiden eroista. Lisäksi rakennettiin tietoliikenneverkko ja pyrittiin kartoittamaan, kuinka erilaiset laitteet ja ohjelmistot yhdessä käyttäytyvät IPv6-protokollan kanssa.

1.1 Opinnäytetyön tavoite

Tämän opinnäytetyön tavoitteena oli rakentaa IPv6-protokollaa hyväksikäyttävä tietoliikenneverkko Pohjois-Karjalan ammattikorkeakoulun tietotekniikan koulutusohjelman opetuskäyttöön. Lisäksi tavoitteena oli selvittää, kuinka erilaiset käyttöjärjestelmät toimivat keskenään IPv6-protokollan kanssa. Tietoliikenneverkkoon täytyi saada tiettyjä palveluja. Nämä palvelut olivat IPv6/IPv4-tunnelointi sekä DHCP - ja DNS-roolit.

2 Opinnäytetyön tausta

Tässä opinnäytetyön osiossa käsitellään IPv6-protokollaa ja sen ominaisuuksia sekä IPv4-protokollaa. Luvussa käsitellään tärkeimpiä käsitteitä ja käydään läpi perustietoja IPv6-protokollasta verrattuna vanhempaan tekniikkaan. IPv4-protokollaan ei tässä opinnäytetyössä tulla paljonkaan perehtymään, koska se ei olennaisesti liity opinnäytetyöhöni. Työssä pyritään tuomaan kuitenkin perustietoa ja pohjaa tietoliikenneverkon rakentamista varten myöhemmässä osiossa.

2.1 IPv6 –ja IPv4-protokollat

Tällä hetkellä käytössä oleva verkkotekniikka, IPv4-protokolla alkaa olla aikansa elänyt tekniikka. Uusien laitteiden kytkeytyminen verkkoon on jokapäiväinen asia. Tämä tarkoittaa sitä, että jokainen laite tarvitsee oman uniikin IP-osoitteen toimiakseen Internetissä. Yksinkertaisesti päädytään siihen, että osoitteet loppuvat kesken ja jokin ratkaisu on keksittävä sen estämiseksi.

IPv4:n ongelmana on se, että se tarjoaa vain 32-bittisen osoiteavaruuden. Tällöin saadaan käyttöön noin neljä miljardia osoitetta. Valtavan käyttäjämäärän ja laitteistojen takia kyseinen määrä osoitteita on kohta käytetty loppuun. IP-osoitteiden loppumisen ajankohdasta on esitetty monenlaisia eri näkemyksiä. Euroopan alueen IPv4-osoitteiden on vuonna 2007 arvioitu loppuvan vuonna 2011 [2].

Osoitteiden mahdollinen loppuminen on ollut jo jonkin aikaa tiedossa. IP-osoitteiden loppumista on yritetty estää käyttämällä osoitteenmuunnostekniikoita ja muokkaamalla osoitteiden jakamista tehokkaammaksi. Näitä tekniikoita ei kuitenkaan voi loputtomiin asti käytännössä soveltaa. Osoitteenmuutoksella tarkoitetaan sitä, että suuriakin määriä laitteita voidaan ohjata ulkoverkkoon yhdellä tai muutamalla osoitteella, vaikka sisäverkossa ne käyttäisivätkin omaa uniikkia osoitetta. Osoitteenmuutokset tehdään useinmiten reitittimelle, jonka kautta verkkoliikennettä jaetaan sisäverkosta ulkoverkkoon ja päinvastoin [1].

Tällä hetkellä uutena asiana on tullut langattomien laitteiden lisääntyvä käyttö. Tietokoneiden hintojen halpeneminen ja tehokkaampien verkkoyhteyksien saatavuus on mahdollistanut paljon uusia käyttäjiä.

2.2 IPv6-protokolla ja ominaisuudet

1990-luvun alussa aloitettiin suunnittelemaan IPv4-protokollalle korvaajaa, IPv6-protokolla. Suurin muutos näiden protokollien välillä on se, että IPv6 on laajennettu 128-bittiseksi osoiteavaruudeltaan. Tämä tarkoittaa sitä, että IP-osoitteet riittäisivät todella pitkäksi aikaa eikä uutta protokollaa tarvitse olla heti suunnittelemassa eikä vaihtamassa. Osoitteiden määrän tarve on kasvussa eksponentiaalisesti ja uuteen tekniikkaan siirtyminen on väistämätöntä [2].

Uuden verkkoprotokollan suuunnitteluvaiheessa oli tarkoituksena aluksi tehdä IPv5-protokolla. IPv5-protokollan piti olla kokeellinen verkkoprotokolla reaaliaikaiselle videon toistamistamiselle. Tämä projekti jätettiin kuitenkin melko kehitys asteelle ja lopetettiin, koska ajateltiin sen aiheuttavan suurta sekaannusta käyttäjien keskuudessa. Tällöin aloitettiin IPv6-protokollan suunnittelu ja toteutus [2].

IPv6-protokollan käyttöönottoa on vähitellen aloitettu Euroopassa, Japanissa ja osassa Aasian maita. Näissä maissa on käytetty lähes kaikki IP-osoitteet, joten laajentuminen IPv6:een on välttämätöntä. Virallisesti Japani on aloittanut muuttamaan käytettävää protokollaansa uuteen IPv6:een jo vuonna 2000, koska varsinkin siellä on kyseessä verkkolaitteiden suuri kasvu, joka johtuu suuresta asukasmäärästä sekä tekniikan kehitysvauhdista [2].

IPv6-protokollaan siirtymistä on pyritty helpottamaan erilaisin keinoin. Esimerkiksi automaattinen konfigurointi eli tilaton -ja tilallinen osoitekonfigurointi auttavat asettamaan IP-osoitteita helposti laitteille. IPv6 osoitteiden fyysinen kirjoittaminen on työlästä, joten osoitekonfigurointimenetelmät hoitavat sen käyttäjän puolesta [2].

Protokolla tarjoaa yksinkertaisemman otsikkorakenteen kuin edeltäjänsä. IPv6 sisältää myös paljon enemmän tietoturvan kannalta parempaa tekniikkaa sekä muunneltavuusmahdollisuuksia. IPv6-protokollan verkoissa voidaan langattomasti liikkua verkosta toiseen ilman yhteyskatkoja [2].

Uuteen protokollaan siirtyminen on tuottanut jonkin verran varteenotettavia muutoksia. Vanhat verkkolaitteet on todennäköisesti vaihdettava uusiin tai päivitettävä, jos niissä ei ole ennestään uudelle protokollalle tukea. Vanhat käyttöjärjestelmät sekä ohjelmistot on päivitettävä uusiin, jotta ongelmat saataisiin mahdollisimman vähäisiksi. Tämä tuo yrityksille ja yksityisille käyttäjille lisäkustannuksia, koska mahdollisesti uudet laitehankinnat ovat edessä ja etenkin vanhemmissa yrityksissä. Nykyisin saadaan edullisesti laitteistoja, joissa on jo IPv6-protokollan tuki. Kerralla toteutetut hankinnat muodostavat kustannuspiikin verrattuna siihen, että laitteistoja hankittaisiin vähitellen.

2.2.1 IPv6-otsikkorakenne

IPv6-protokolla sisältää yksinkertaistetumman otsikkorakenteen verrattuna IPv4-protokollaan. Otsikkorakenne on IPv6-protokollassa tiivistetympi ja pelkistetympi. IPv6-osoitteiden otsikot sisältävät kahdeksan kenttää, kun taas IPv4 sisältää neljätoista. Yksittäisiä kenttiä on poistettu tai vähennetty muuttamalla ne valinnaiseksi. Näin säästetään aikaa, joka muuten menisi pakettien prosesessoimiseen. Pääotsikko IPv6-protokollassa sisältää kahdeksan erilaista kenttää:

Version: Sisältää 4-bittisen versionumeron.

Traffic Class: Liikenneluokka-kenttä on 8-bittinen ja määrittää paketit erilaisiin loogisiin ryhmiin.

Flow Label: Vuontunniste, joka koostuu 20-bitistä. Vuontunniste sallii tietynlaisen liikenteen, joihin on liitetty lipukkeet. Tätä käytetään erityisesti pakettien siirron nopeuttamiseen.

Payload Length: Määrittelee kuorman pituuden tavuina. Kooltaan se on 16-bittinen.

Next Header: Määrittelee mikä otsikko tulee seuraavana IPv6-paketin otsikon jälkeen.

Hop Limit: Määrittelee kuinka monta hyppyä IPv6-pakettti voi edetä. 8-bitin suuruinen kenttä kertoo myös paketin eliniän.

Source Address: 128-bittiä pitkä paketin lähdeosoite, kertoo mistä paketti on tullut.

Destination Address: Kooltaan 128-bittinen paketin vastaanottajan osoite [2].

Yksinkertaistettu otsikko tarjoaa siis tehokkaamman reitityksen verkossa eikä vaadi verkkokerroksen tarkistussumman laskua, mikä on vanhemmassa protokollassa hyvin ominaista. Otsikkorakenteeseen on yksinkertaistettu lisäotsikointi, joka sijaitsee pääotsikon ja kuljetuskerroksen välissä. Lisäotsikoilla on erilaisia tarkoituksia, esimerkiksi reitittäminen, autentikointi ja salaus [2].

2.2.2 Osoitteistus

IPv4-protokollassa käytetään tuttua 32-bittistä IP-osoitetta, joka on jaoteltu 8-bitin sarjoihin. IPv6-protokollassa osoitteistus ei mene niin yksinkertaisesti. IPv6-protokollassa käytetään 128-bittistä IP-osoitetta ja se tarvitsee erilaisen esitysmallin, koska sen koko on suurempi ja se käyttää myös 16-bittistä heksadesimaaliesitystä.

Esimerkki IPv4-osoitteesta:
198.162.1.10

Esimerkki IPv6-osoitteesta:
2002:0000:00000:00001:0100:C9CC:C6A2:60DF

Tiivistettynä IPv6-osoite on seuraavanlainen:
2002::1:100:C9CC:C6A2:60DF

Nollien jättäminen osoitteeseen ei ole välttämätöntä, mutta ne voi tiivistää yhdeksi nollaksi tai jättää pois kokonaan ja käyttää kahta kaksoispistettä peräkkäin. Kaksoispisteiden tiivistämistä voi käyttää vain kerran osoitteessa. Tiivistäminen tekee osoitteista luettavampia ja pituudeltaan lyhyempiä [3].

2.2.3 Tunnelit

Ipv6-protokollassa käytetään menetelmää nimeltä tunnelointi. Tällä menetelmällä saadaan uuden protokollan tarjoamat IP-paketit lähetettyä vanhan IPv4-protokollan verkon yli. Tätä tekniikkaa käytetään, kun pyritään vaihtamaan kaikki verkkoliikenne IPv6-protokollaan. Tunneloinnin pystyy tekemään isäntälaite sekä reititin [2]. Erilaisia tunnelimenetelmiä on seuraavanlaisia:

- IPv6-verkon yli IPv4-verkkoon, jossa IPv6-paketit on sidottu IPv4-protokollan paketteihin. Tämä tekniikka vaatii reitittimeen molemmat protokollat konfiguroituna.

- 6to4 tunnelointi menetelmä, jossa IPv6 paketit tunneloidaan isännältä IPv4-verkon ylitse reitittimelle.

- IPv6 paketit tunneloidaan isännältä IPv4-verkon ylitse toiselle isännälle.

- Viimeinen tekniikka, jossa tunneloidaan IPv6 paketit reitittimeltä IPv4-verkon ylitse isännälle [2].

Opinnäytetyöni käytännön vaiheessa tutkin käyttämällä tunnelointimenetelmää, jossa IPv6-paketit lähetetään IPv4-verkon ylitse toiseen IPv6-verkkoon.

2.2.4 Automaattinen konfigurointi

IPv6-protokollan tärkeimpiä asioita on sen osoitteiden automaattinen konfigurointi. Se on uusi kehitetty tekniikka ja voidaan toteuttaa myös ilman DHCP-protokollaakin. Pääasiassa tämä tarkoittaa sitä, kun laite kytketään verkkoon se rekisteröi automaattisesti kaiken tarvittavan itseensä. Tästä johtuen sitä ei tarvitse enää manuaalisesti konfiguroida verkkoon. Kyseessä on tilaton autokonfiguraatio. Tässä tekniikassa IP-osoitteen alkuosa vaihdetaan ja loppuosaa ei muuteta. Loppuosa muodostuu staattisesti käyttäen verkkolaitteen uniikkia MAC-osoitetta. IPv6-osoitteiden lähettäminen DNS-palvelimelta ole vielä mahdollista tilattomassa autokonfiguraatiossa. Tähän pyritään löytämään ratkaisua, koska IPv6-protokolla on vielä kehitysasteella. Tilallisessa autokonfiguroinnissa käytetään perinteiseen DHCP-protokollaan [1]. Näitä menetelmiä voidaan käyttää yhtä aikaa samassa verkossa. Reitittimen mainosviestiin on merkitty lipuke, joka osoittaa kumpaa menetelmää käytetään kyseisessä verkossa [2].

Tekniikkaa onkin todella hyvä käyttää IPv6-verkossa, koska protokolla ei tarjoa helppoa IP-osoitetta, niinkuin vanha protokolla. Menetelmä siis säästää aikaa ja auttaa käyttäjiä käyttämään laitteita, vaikka he eivät niitä hyvin hallitse.

2.2.5 Tietoturva

Internetin kasvavan käytön takia tietoturva on hyvin tärkeää. Hyökkäyksiä verkon kautta päätelaitteisiin tapahtuu päivittäin ja suojausten täytyy olla kunnossa. Päätelaitteiden omia suojausohjelmia ei pidä unohtaa, vaan pitää ne päivitettyinä. Myös verkonliikenne on suojattava, jotta vältetään mahdolliset hyökkäykset.

Tietoturva on toteutettu IPv6-protokollassa tehokkaasti alusta alkaen IPSec:n avulla. Tätä tekniikkaa käyttäen voidaan salata liikennettä verkossa. Kyseinen tekniikka on sulautettu IPv6-protokollaan. IPSec käyttää kolmea eri protokollaa varmistaakseen tietoliikenteen turvallisuuden: autentikointi, salaus -ja avaintenhallintaprotokolla. Autentikoinnin avulla pystytään varmistamaan, että lähettäjä on oikea. Tietoturva paranneltu IPv6-protokollassa verrattuna IPv4-protokollaan. Tämä on ymmärrettävää, koska uuden protokollan avulla voidaan käyttää yhä enemmän laitteita verkossa [2].

2.2.6 DHCP ja DNS

DHCP on tekniikka, jolla pystytään jakamaan IP-osoitteita automaattisesti tietoliikenneverkossa verkkolaitteille. Kytkeytyessään verkkolaite alkaa hakemaan reitittimeltä IP-osoitetta. Reitittimellä on määritetty tietty osoitealue, josta osoitteet laitteille jaetaan. Esimerkiksi kannettava tietokone liittyessään 192.168.1.0 verkkoon, voi saada 192.168.1.100 osoitteen itselleen, jos DHCP määrittelyissä osoitealue on esimerkiksi 192.168.1.100 – 192.168.1.110. Osoitealue mahdollistaa 11 koneen liittymisen verkkoon. DHCP:tä yleensä käytetään Internet osoitteiden jakamiseen tai paikallisessa lähiverkon luonnissa.

DHCP konfigurointiin olennaisesti liittyen IPv6-laitteet lähettävät viestejä toisilleen (Neighbor Solicitation), joilla tarkistetaan onko verkossa kahta samanlaista IP-osoitetta. Tämä tekniikka on nimeltään DAD. IPv6-protokollassa on osoitteen ratkaisemiselle tekniikka nimeltä Address Resolution. Tällä tekniikalla määritetään laitteiden MAC-osoitteet, jotta laitteet voivat toimia keskenään [1].

Router Discovery on menetelmä, jolla havaitaan reitittimet verkossa. Tällä tekniikalla voidaan esimerkiksi määrittää IPv6-otsikon elinaika-kentän arvoja ja konfiguroida laitteet käyttämään tilatonta autokonfigurointia [1].

DNS eli nimipalvelu ei ole muuttunut juuri lainkaan siirryttäessä IPv6-protokollaan. Nimipalvelun tarkoitus on helpottaa loppukäyttäjää navigoimaan verkkolaitteita. Opinnäytetyöni tietoliikenneverkossa DNS-palvelu on hyvin suuressa roolissa, koska IPv6-osoitteiden fyysinen kirjoittaminen on kovin työlästä. Palvelimelle ja laitteille asetetaan nimi, joka helpottaa ping komentojen käyttöä verkossa. Nimipalvelua on suositeltavaa käyttää lähiverkossa sekä IPv6 verkkoympäristössä [2].

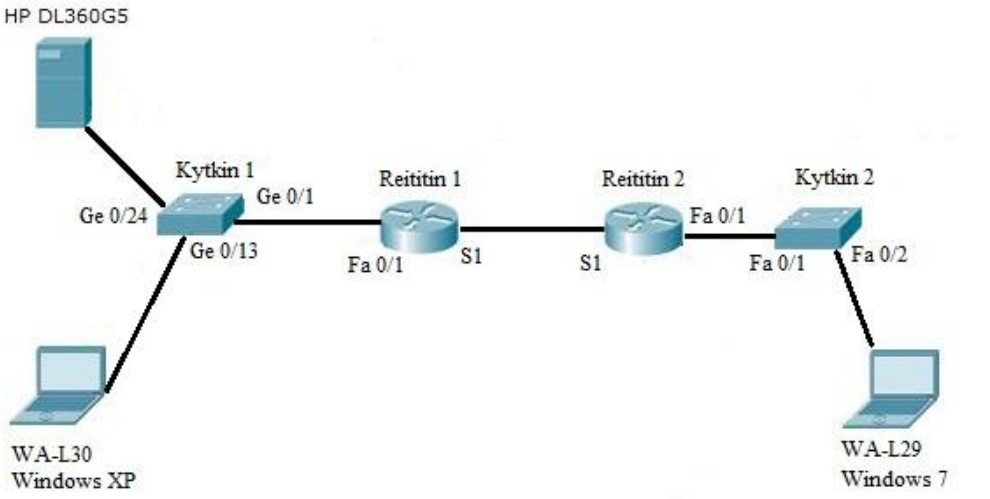
Nimipalvelu tarjoaa verkko-osoitteet selkeälukuisempina, kuin se normaalisti olisi tavalliselle käyttäjälle. Verkko-osoitteet ovat tutuista sanoista muodostettuja, kun ne oikeasti muodostuvat IP-osoitteista. DNS kääntää ne helpompilukuiseksi. Reititys täytyy muistaa konfiguroida verkossa ennen DNS:än toimimista. Tilaton

autokonfiguraatio ei sisällä vielä DNS-palvelua, mutta tilallisessa versiossa se hoidetaan reitittimen mainostamisella [1].

3 IPv6-opetusverkko

Tässä opinnäytetyön osiossa toteutettiin tietoliikenneverkko, IPv6-protokollaa käyttäen. Tietoliikenneverkko simuloidaan Pohjois-Karjalan ammattikorkeakoulun laboratoriossa. Ammattikorkeakoulu tarjoaa verkkolaitteet ja ohjelmistot, joilla simulointi onnistuu. Suuressa roolissa tässä työssä tulee olemaan Windows server 2008R2-palvelinohjelma, jota käytetään virtuaaliyhteydellä palvelinohjelmana. Tämä on asennettuna fyysisellä palvelimella HP DL360GS:llä, joka sijaitsee erillisessä huoneessa. Virtuaalipalvelimen hallintaohjelmana käytettiin Vmware vSphere Client ohjelmaa.

Tarkoituksena oli selvittää, kuinka erilaiset käyttöjärjestelmät toimivat keskenään IPv6-protokollan kanssa. Lisäksi merkittävänä tutkimiskohteena oli IPv6/IPv4-tunnelointi, DHCP ja DNS-nimipalvelu.



Kuva 1. Kytkentäkaavio.

Kuvassa 1 on nähtävissä kytkentäkaavio, jossa HP DL360G5 palvelin sijaitsee koulun erillisessä palvelinhuoneessa. Tältä palvelimelta simuloidaan Windows Server 2008R2 palvelinohjelma jolta jaetaan DHCP -ja DNS-palveluja. Kytkin 1 on reitittävä Cisco

Catalyst 3560G, jossa on GigabitEthernet liitäntöjä. Näiden avulla mahdollistetaan nopeat yhteydet HP DL360GS palvelimelle. Molemmat reitittimet ovat Cisco 1700 mallisia, sekä kytkin 2 on Cisco 2950. Päätelaitteista WA-L30 oli Windows XP ja WA-L29 Windows 7 käyttöjärjestelmällä varustettuja kannettavia tietokoneita.

(Kuvan 1) testauslaitteille asetetut IP-osoitteet:

HP DL360GS verkkokortti	10.10.10.10
WA-L30, Ethernet	DHCP
WA-L29, Ethernet	2002:A01:101:1::2
Reititin 1, Tunnel0	2002:A01:101::1
Reititin 1, FastEthernet0/1	2002:A01:101:1::1
Reititin 1, Serial 1	10.1.1.1
Reititin 2, Tunnel0	2002:A01:102::1
Reititin 2, FastEthernet0/1	10.1.2.2
Reititin 2, Serial 1	10.1.1.2
Kytkin 2, Vlan 1	10.1.2.1

3.1 Reitittimen konfiguraatio

Seuraavaksi tietoliikenneverkon konfiguroinnissa oli reitittimet. Reitittimille täytyi tehdä asetukset IPv6-protokollaa varten. Reitittimelle täytyi asettaa komento IPv6 unicast-routing. Tällä asetettiin reitittimen reititysasetukset toimimaan myös IPv6-protokollalla. Seuraavaksi täytyi luoda RIP-reititysprotokolla sekä oletusreitti seuraavanlaisesti:

```
ipv6 route 2002::/16 Tunnel0
ipv6 router rip koe
```

Tämän jälkeen konfiguroin Serial1 porttia. Reititys tapahtui serial portin kautta, jolloin siihen täytyi asettaa IPv4-osoitteen lisäksi myös IPv6 asetuksia seuraavanlaisesti:

```
interface Serial1
 ip address 10.1.1.1 255.255.255.0
 ipv6 enable
 ipv6 rip koe enable
```

Viimeisenä konfiguraatiovaatimuksena oli luoda IPv6/IPv4-tunneli reitittimien välille. Reitittimelle tehtiin Tunnel0, jolle asetettiin IPv6-osoite. Tunnel0 konfiguraatioesitys oli seuraavanlainen:

```
interface Tunnel0
ipv6 address 2002:A01:101::1/64
 ipv6 rip koe enable
 tunnel source Serial1
 tunnel mode ipv6ip 6to4
```

Reitittimet oli yhdistetty toisiinsa serial1 portin kautta, jolloin tunneli täytyi konfiguroida samaan porttiin. Tunnelille asetettiin IPv6-osoite ja liitettiin RIP reititysprotokolla. Reitittimelle 1 oli nyt luotu IPv6/IPv4- tunneli. Ennenkuin reititys toimisi oikein myös reititin 2 tarvitsi vastaavanlaisen konfiguroinnin. Kytkimet tarvitsivat myös peruskonfiguroinnin. Reitin 2 –ja kytkinkonfiguroinnit löytyvät liitteistä. Yhteydet reitittimien välillä testattiin ping –ja ping6 komennoilla.

3.2 Windows Server 2008R2

Windows Server 2008R2 on uusi Microsoftin tarjoama palvelinohjelma. Se julkaistiin helmikuussa 2008. R2 on päivitetty versio Server 2008 ohjelmasta. Se sisältää jonkin verran uusia toimintoja verrattuna aiempaan versioon. Näistä uusia toimintoja ovat esimerkiksi paranneltu etäkäyttö ja tietoturva ominaisuudet. Windows Server 2008R2 pohjautuu Windows Vistan ohjelmakoodiin sekä sisältää samat arkkitehtuuriset uudistukset ja toiminnalliset parannukset kuin Vistalla [4].

R2 olikin hyvä vaihtoehto käyttää tässä opinnäytetyössä palvelinohjelmana. Se oli asennettuna fyysiselle palvelinkoneelle. Palvelinohjelmaa hallinnoitiin palvelinkoneelta

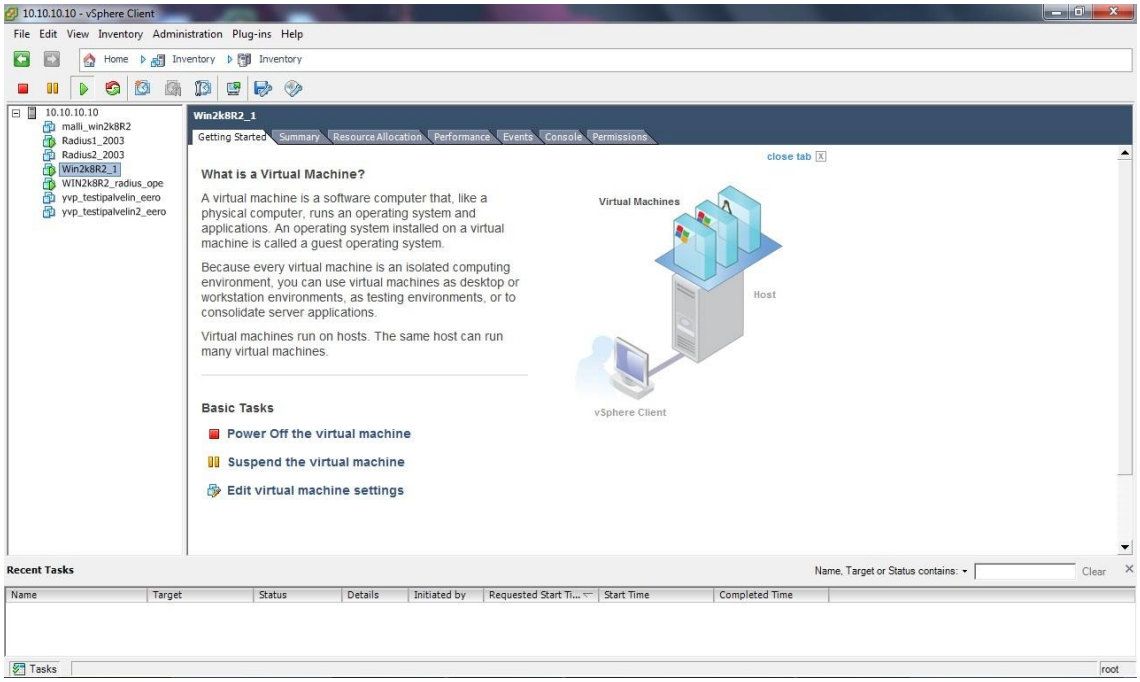
erillisellä kannettavalla tietokoneella, Vmware vSphere client ohjelmaa apuna käyttäen. Vmware vSphere clientillä pystyi muodostamaan virtuaalisen yhteyden fyysiselle palvelimelle, koska palvelin sijaitsi erillisessä huoneessa. Windows Server 2008R2:n avulla täytyi luoda DHCPv6 -ja DNS6-roolit palvelimelle. Tämä tapahtui helposti palvelinohjelmiston oman velhon avulla.

3.3 Tietoliikenneverkko

Verkkolaitteiden konfiguroimisen jälkeen täytyi HP DL360G5 palvelimelle asentaa DNS –ja DHCP-roolit. Laboratoriossa joutui käyttämään koulun runkoverkkoa apuna, jotta päästiin käsiksi palvelinhuoneessa sijaitsevaan fyysiseen palvelinkoneeseen. Tämä kytkettiin Ciscon Catalyst 3560G kytkimen GigabitEthernet 0/24 porttiin. Palvelimeen otettiin virtuaaliyhteys Vmware vSphere Client ohjelman avulla, joka oli valmiiksi asennettuna kannettavalle tietokoneelle (kuva 2).

Kannettavalle tietokoneelle asetettiin 10.10.10.100 IP-osoite hallintayhteyttä varten. Kuvasta 3 näkee Vmware ohjelman ja sen käyttöliittymän. Nähtävillä on 10.10.10.10 osoite, johon yhdistymällä päästään käsiksi W2008R2 palvelimelle. Käyttäjänimi oli root sekä salasana password.

Kuva 2. Vmware vSphere Clientiin yhdistyminen.



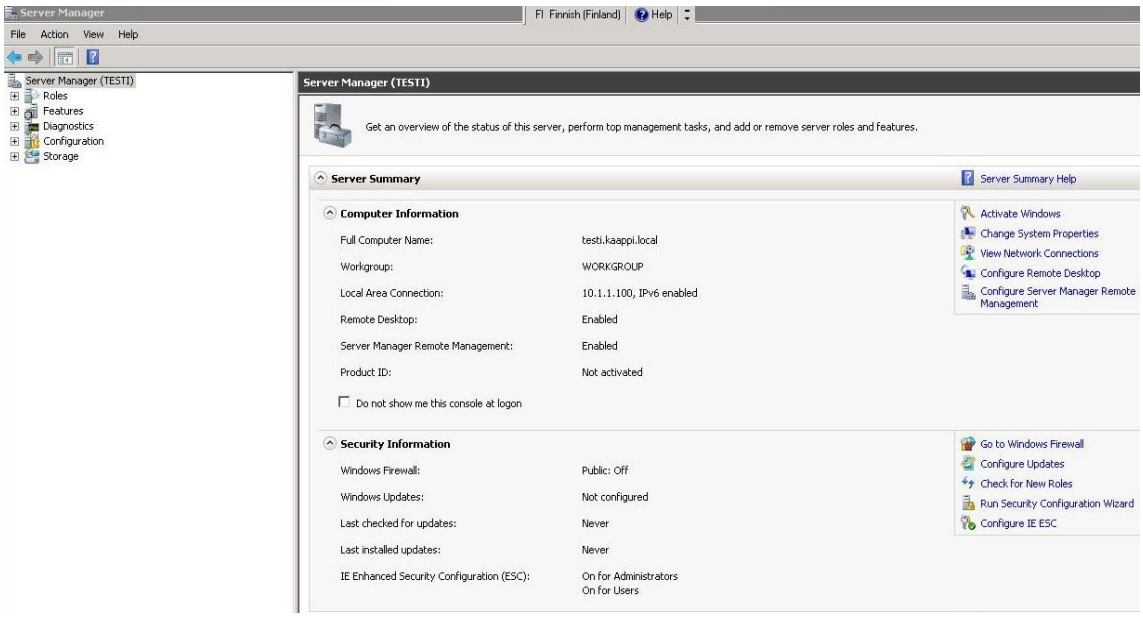
Kuva 3. Vmware vSphere Clientin ulkoasu.

Kuvassa 3 on esitettynä Vmware vSphere Client ohjelman käyttöliittymää. Palvelinhuoneen HP DL360GS verkkokortti täytyi liittää virtuaaliseen verkkokorttiin vmWaren avulla. Samalla verkkokortti liitettiin Vlan 10:een. Vlan 10 luotiin konsoliyhteyden kautta Tera Term ohjelmaa apuna käyttäen kytkimelle. Tarkemmat konfiguraatiot löytyvät lähteistä [5, 6, 7].

3.4 DNS -ja DHCP-palvelujen asentaminen

Palvelimelle täytyi asentaa rooleja. Tässä työssä tarvittavat roolit olivat DNS ja DHCP. Niiden asentaminen onnistui yksinkertaisesti Windows Server 2008R2:en omalla sisäänrakennetulla velholla.

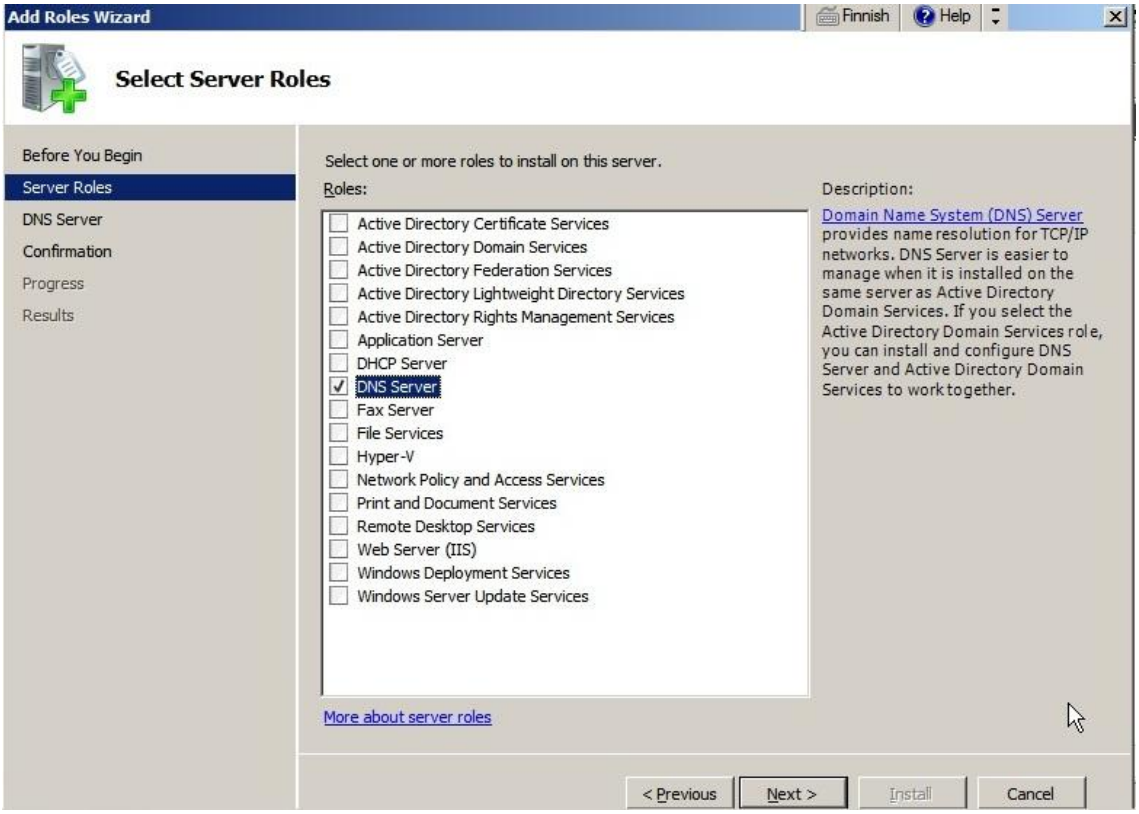
DNS-palvelun asentaminen tapahtui helposti Server Manager ohjelmalla. Server Manager ohjelmalla, pystyy luomaan, poistamaan ja navigoimaan helposti palvelinta. Kuvassa 4 on kuvattuna tässä työssä käytetyn palvelimen hallintasivu.



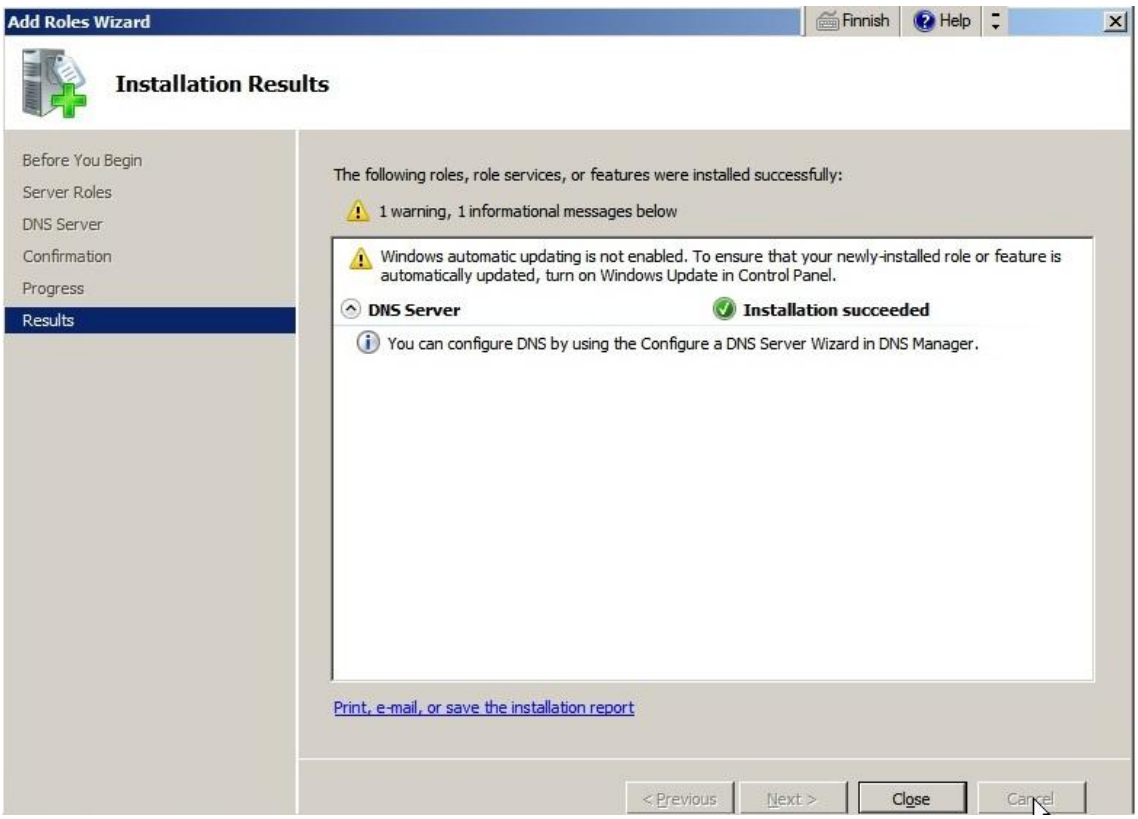
Kuva 4. Server Manager.

Yllä olevassa kuvassa on Windows Server 2008R2 Server Manager ohjelman ulkoasu. Täältä voidaan hallinnoida helppokäyttöisesti serveriä. Kuvassa on näkyvillä esimerkiksi IP-osoite.

Roles välilehdellä luodaan ja poistetaan rooleja. Tältä sivulta DNS -ja DHCP-roolien asentaminen tapahtui helposti. Kuvassa 5 on kuvattuna avautunut ikkuna, jossa on mahdollista asentaa palvelimelle erilaisia rooleja. Aluksi asennettiin DNS-rooli valitsemalla se listalta ja menemällä eteenpäin.



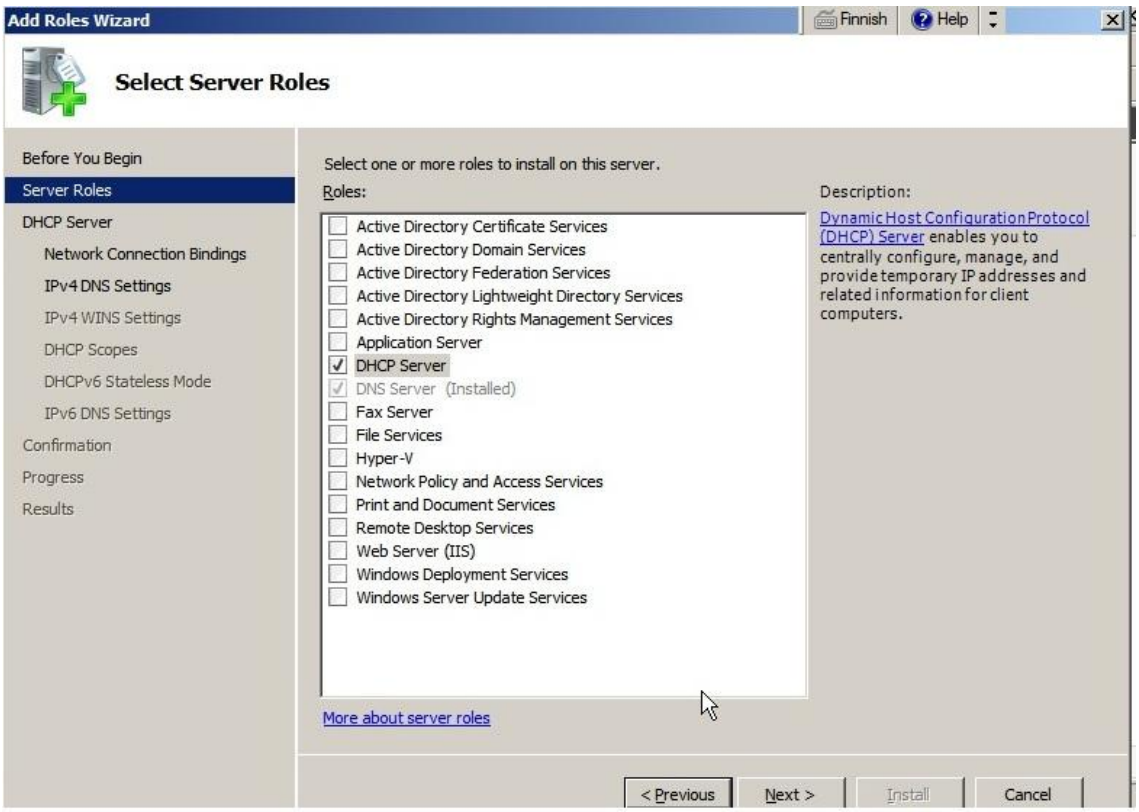
Kuva 5. Roolit.



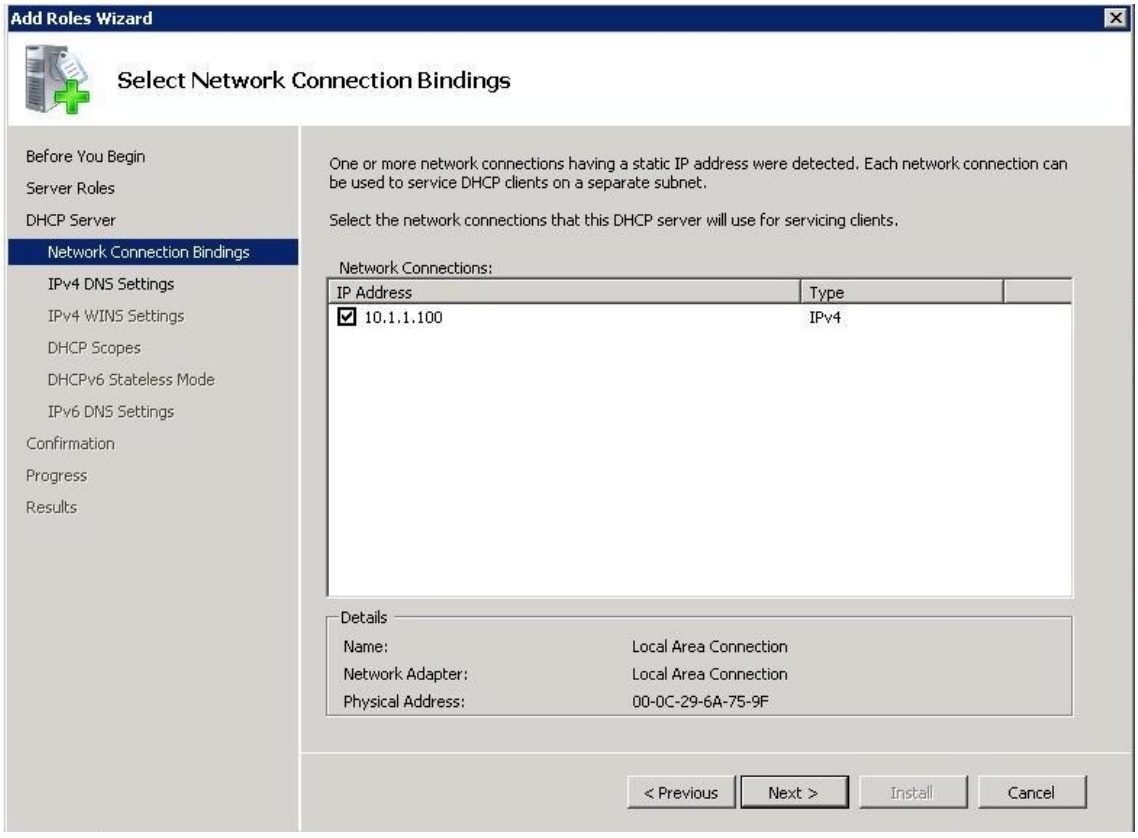
Kuva 6. DNS asennus.

Lopulta tullaan kohtaan, jossa velho kertoo asennuksen onnistuneen (kuva 6). Tämän jälkeen oli vuorossa DHCP-roolin asentaminen.

DHCP-roolin asennus tapahtuu samalta sivulta, kuin DNS-palvelunkin. Valitaan listasta DHCP-server ja painetaan seuraavaa (kuva 7). DNS-palvelu on näkyvillä harmaalla, joka merkitsee että se on asennettuna.

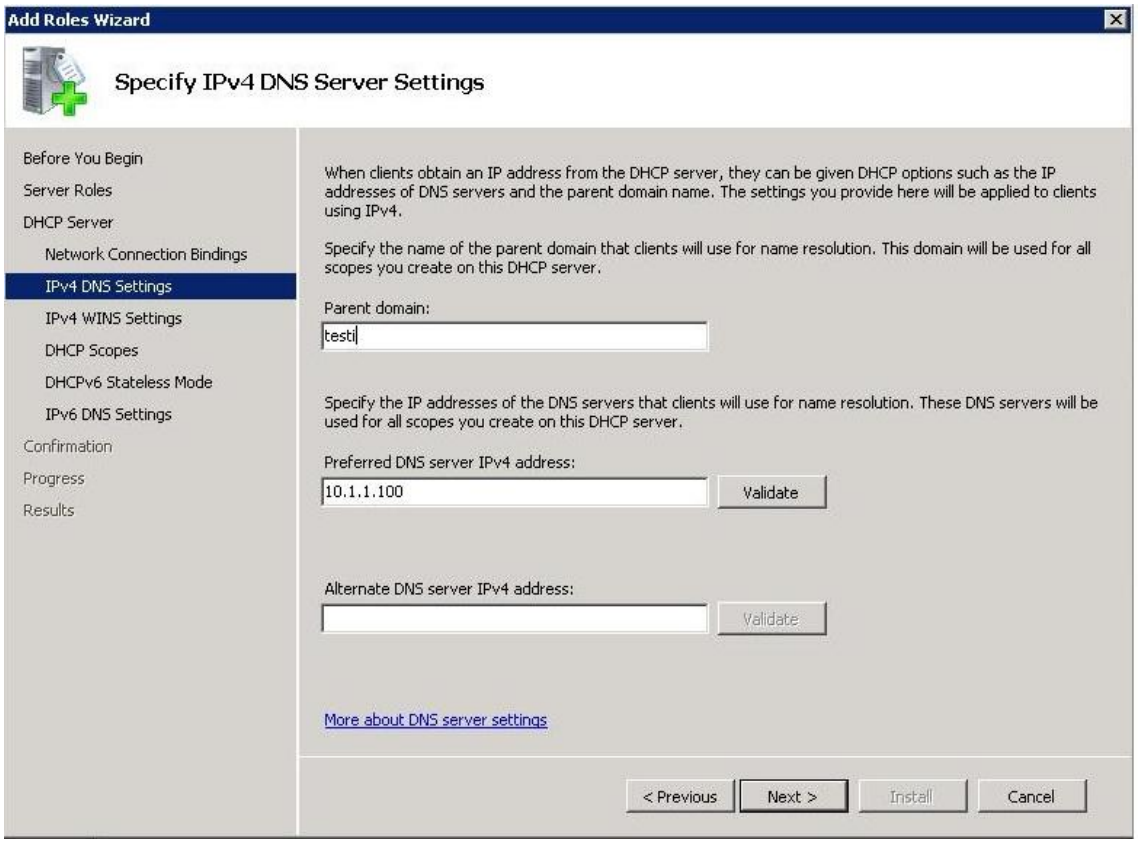


Kuva 7. DHCP-serverin valinta.



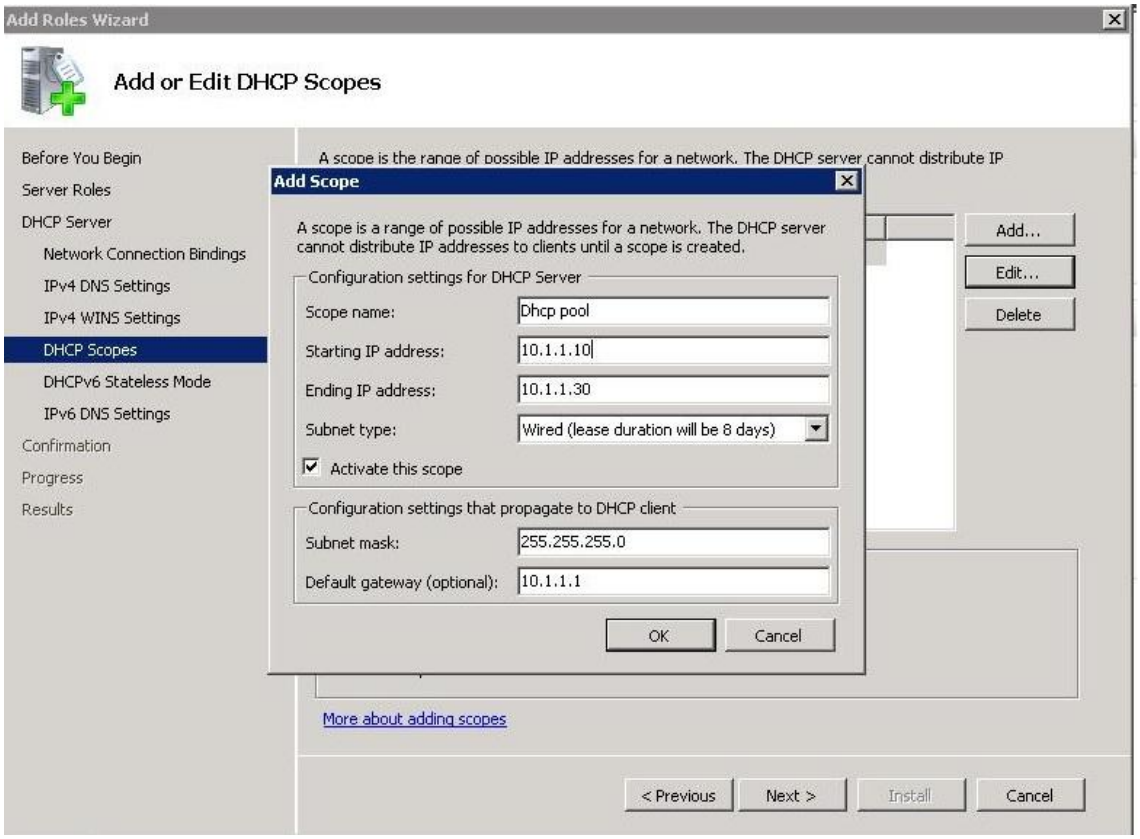
Kuva 8. DHCP-liitos.

Kuvassa 8 on näytetty, mihin osoitteeseen DHCP-liitos tehdään. Kyseessä on IPv4-osoite ja se on fyysisen palvelimen verkkokortin IP-osoite. IPv6-osoitteet asetetaan myöhemmässä vaiheessa.

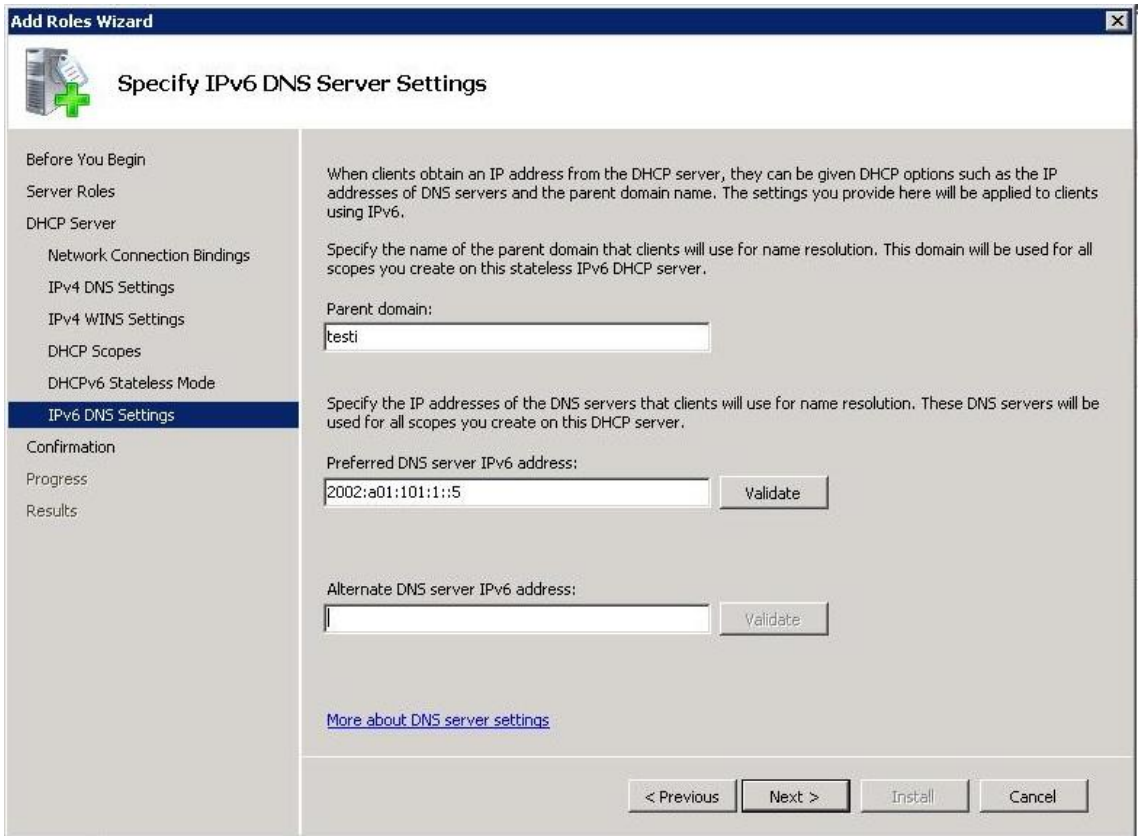


Kuva 9. IPv4 DNS.

Seuraavaksi täytyi asettaa domain nimi, joka on palvelimen nimi testi. Ensisijainen DNS-osoite on myös asetettava, jota halutaan käyttää nimipalvelussa. Tässä tapauksessa käytettiin verkkokortin osoitetta (kuva 9).



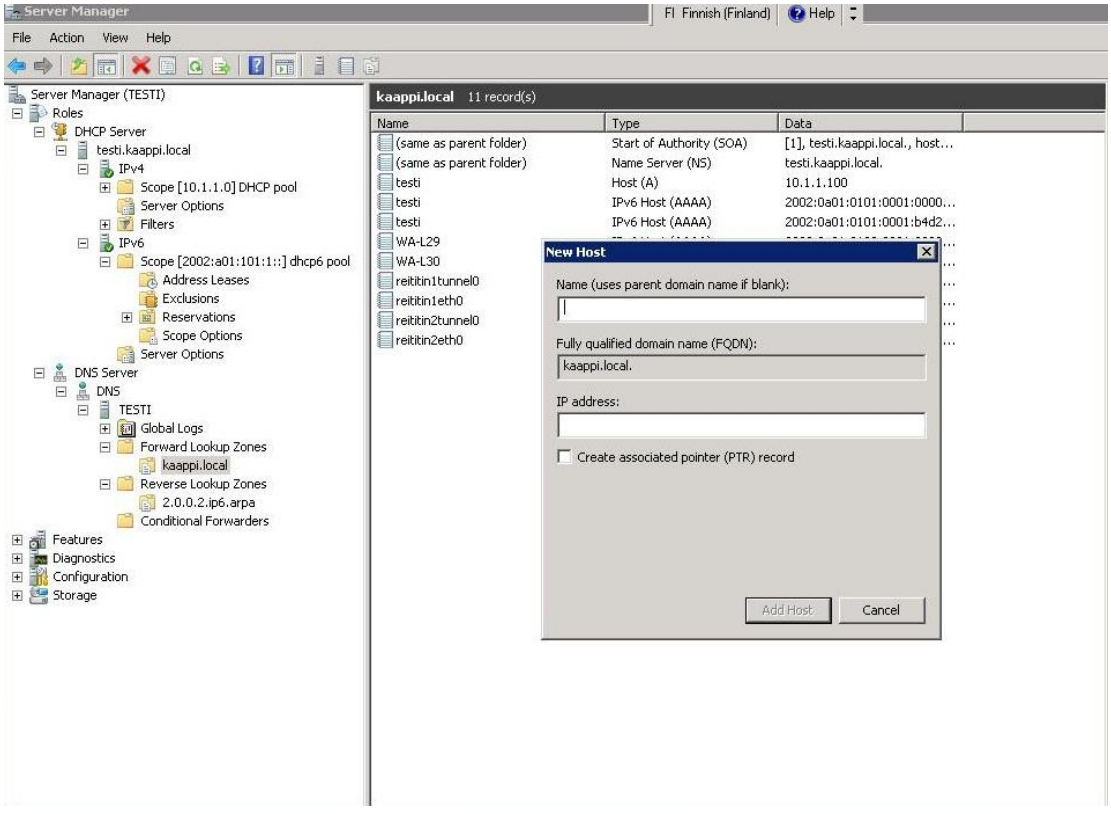
Kuva 10. DHCP pool.



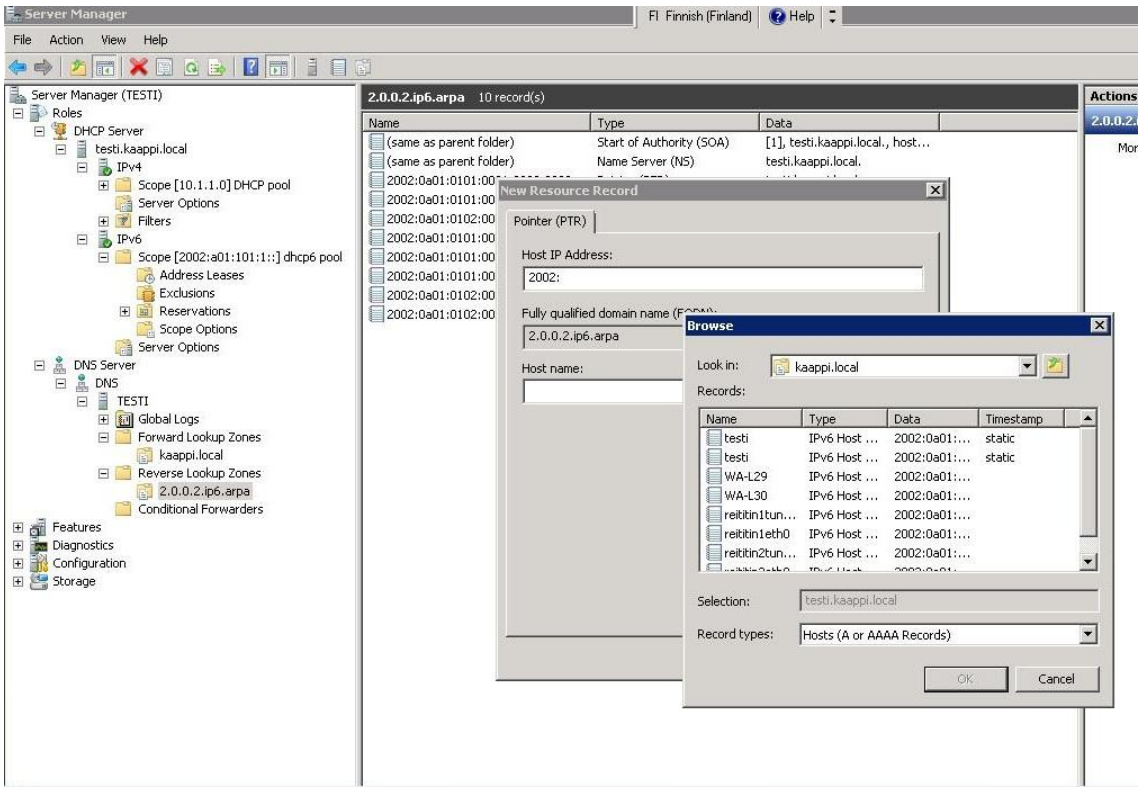
Kuva 11. DHCPv6.

Seuraavaksi oli vuorossa luoda DHCP-pooli, josta osoitteet jaetaan verkkoon. Yllä olevassa kuvassa on esitettynä osoitteiden alkamis- ja päättymisosoitteet (kuva 8). Kaikkien asetusten jälkeen painetaan ok ja next. Myös DHCPv6 saatiin luotua tämän velhon avulla. Kuvassa 11 on avautuneena samanlainen ikkuna, kuin IPv4-protokollallekin. Velho asentaa asetukset palvelimelle itsekseen ja DHCP rooli on luotu.

DHCP -ja DNS-palvelujen ollessa nyt asennettuna täytyi vielä asettaa erikseen IPv6 asetukset DNS-palveluun. Server Manager ohjelmaan oli nyt roolien alle tullut DHCP -ja DNS-server. DNS-roolia auki klikkaamalla löytyi Forward lookup zone kohta (kuva 12). Tänne täytyi tehdä uusi alue, jotta DNS-palvelu toimisi. Sieltä valittiin Primary zone ja asetettiin päälle dynaaminen päivittäminen. Tämä merkitsi sitä, että laitteiden kytkeytyessä verkkoon ne olivat suoraan yhteydessä nimipalveluun. Nimeämällä Primary zonen testiksi, saatiin kaikki asetukset automaattisesti asetettua. Kuvassa 12 nähdään kaappi.local osio, joka sisältää laitteiden nimiä. Hiiren oikealla valitsemalla new host saadaan lisättyä uusia laitteita (kuva 12).



Kuva 12. DNS laitteiden nimeäminen.



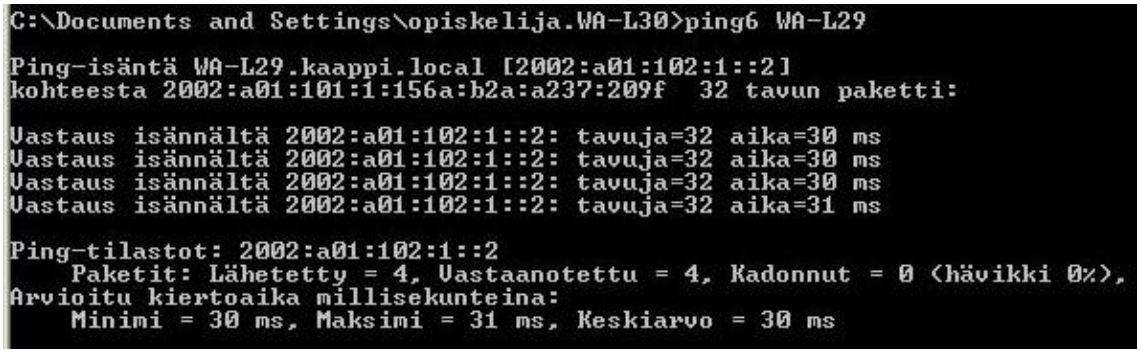
Kuva 13 Reverse Lookup Zone.

Seuraavaksi täytyi asettaa käänteisnimipalvelu, jolla haluttu IP-osoite lisätään nimeen (kuva 13). Tämä tapahtui forward lookup zonen alapuolelta reverse lookup zone kansiota hiiren oikealla klikkaamalla ja valitsemalla new zone. Reverse lookup zone luotiin samalla tavalla, kuin forward lookup zone. Muutoksina ainoastaan oli IPv6 DNS, joka asetettiin 2002::/16 verkon alle.

Reverse lookup zonea hiiren oikealla klikkaamalla ja valitsemalla new pointer kohdasta saadaan kuvan 13 mukainen ikkuna. Täällä pystytään liittämään halutut IP-osoitteet nimiin. Kaikille halutuille nimille tehtiin oma osoitin testaamista varten.

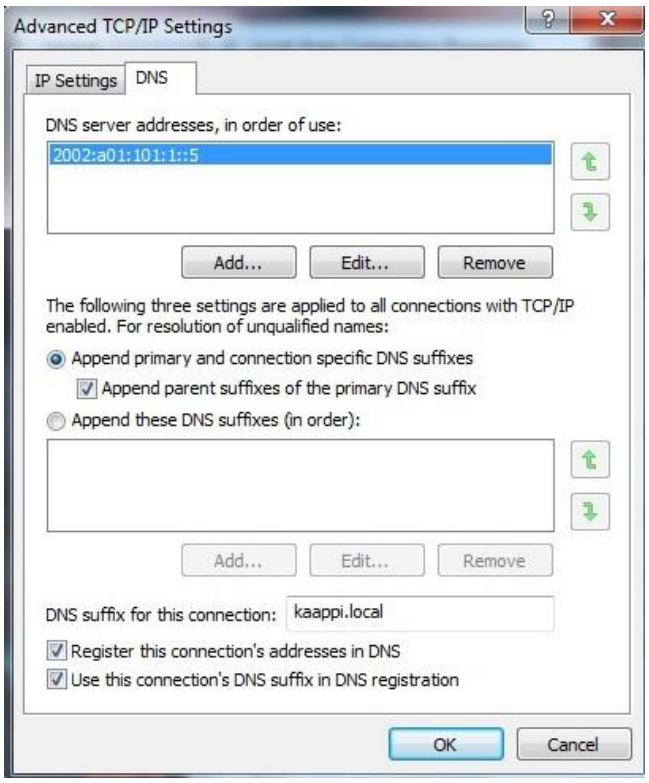
4 IPv6-opetusverkon testaus

Tietoliikenneverkkoa testattiin ping –ja ping6 komennoilla reitittimeltä toiselle, sekä reitittimeltä päätelaitteille ja päinvastoin. Nämä yhteydet olivat kunnossa. Tämän opinnäytetyön tärkeimpänä osana oli käyttää DNS-nimipalvelua verkossa, jotta IPv6-osoitteita ei tarvitse fyysisesti kirjoittaa. Nimipalvelu toimi moitteettomasti WA-L30 päätelaitteessa, jolta pystyttiin pingaamaan kaikkia haluttuja osoitteita. Kuvassa 14 on esimerkki pingaus päätelaitteelle WA-L29.



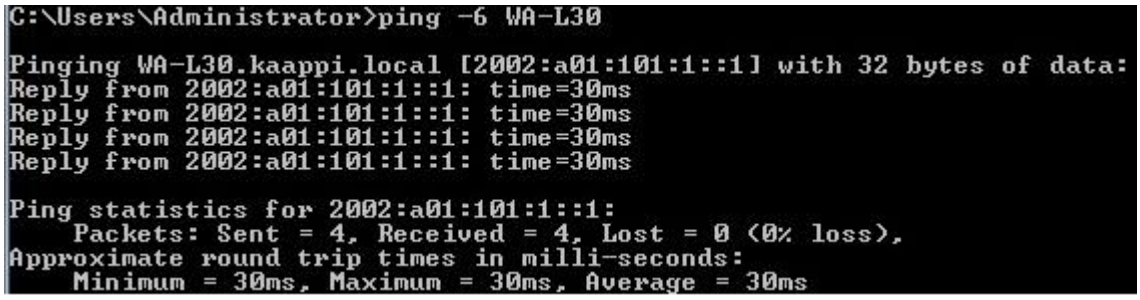
Kuva 14. Pingaus WA-L30 ja WA-L29 välillä.

Nimipalvelu ei näillä asetuksilla kuitenkaan vielä toiminut WA-L29 päätelaitteella, joten sen verkkoasetuksia täytyi vielä konfiguroida manuaalisesti.



Kuva 15. WA-L29 verkkoasetukset

Kuvassa 15 näytetään, kuinka DNS-palvelimen IP-osoite on asetettu sekä DNS-liitos kaappi.local:iin. Tämän jälkeen nimipalvelu toimi moitteettomasti myös päätelaite WA-L29:llä (kuva 15).



Kuva 16. Pingaus WA-L29 ja WA-L30 välillä.

Kuvassa 16 nähdään ping-komennon onnistuminen päätelaitteelta WA-L29 päätelaitteelle WA-L30. Pakettien lähettäminen siis onnistuu molempiin suuntiin.

5 Johtopäätökset

Opinnäytetyöni IPv6-opetusverkko on hyvä esimerkki siitä, minkälainen tavallinen IPv6 tietoliikenneverkko voi yrityksessä olla. Verkko oli yksinkertainen, mutta vaativa rakentaa ja suunnitella. En ollut aiemmin käsitellyt IPv6-protokollaa, joten taustatyötä täytyi tehdä paljon. Windows Server 2008R2 palvelinohjelma ei ollut minulle entuudestaan tuttu, joten jouduin käyttämään paljon aikaa sen tutkimiseen.

Suurena apuna palvelinohjelman oppimiselle oli opinnäytetyöni aikana käyty Uudet Verkkotekniikat kurssi. Tällä kurssilla käytiin Windows Server 2008R2 ohjelmaa läpi, jolloin sen käyttäminen helpottui kurssin edetessä. Pohjois-Karjalan ammattikorkeakoulun tarjoama opetusmateriaali verkossa toimi hyvin apuna sekä suunnittelu että toteutus vaiheessa. Kirjastosta lainaamani Windows Server 2008R2 ohjekirja antoi vinkkejä ja auttoi minua työssäni.

Suurimmat ongelmat kohtasin IPv6-protokollan tunneloinnissa sekä DNS-palvelun toiminnassa koko verkossa. Suunnittelemiseen olisi täytynyt panostaa paljon enemmän, koska siten olisin säästänyt aikaa. Lähdin aluksi kärsivällisesti tutkimaan mahdollisuuksia, joita kokeilin myös käytännössä. Suurinosa kokeiluistani osoittautui huonoksi vaihtoehdoksi tai ei ollenkaan toimivaksi. Lopulta sain tietoliikenneverkkoni kasattua hyväksi ja selkeäksi kokonaisuudeksi. Paremmalla suunnittelulla olisin säästynyt ylimääräiseltä työltä.

Tässä tietoliikenneverkossa on mahdollisia jatkokehitys mahdollisuuksia. Verkkoon voisi lisätä toiselle reitittimelle DHCPv6, jotta verkon toiset päätelaitteet saisivat dynaamisesti verkko-osoitteet, eikä niitä tarvitsisi staattisesti asettaa. Tässä työssä Cisco-1700 reitittimet eivät tukeneet tätä tekniikkaa. Verkkoa testatessani kokeilin tilatonta autokonfiguraatiota. Tilaton autokonfiguraatio toimi reitittimillä hyvin, jolloin reitittimet konfiguroituivat automaattisesti kytkeytyessään verkkoon. Tilatonta autokonfiguraatiota voisi käyttää enemmän seuraavassa versiossa työtäni.

Jatkokehitystä ajatellen verkkoon voisi liittää lisää aliverkkoja sekä palomuureja. Tulostimien testaaminen IPv6-protokollan kanssa olisi myös hyvä kokeilu, koska yritysmaailmassa niitä tullaan tarvitsemaan.

Tämä opinnäytetyö on hyvä pohja Pohjois-Karjalan ammattikorkeakoulun tietoliikenne kursseille, joissa käsitellään IPv6-protokollaa. Opinnäytetyötäni voi käyttää apuna opetusmateriaalina tulevaisuudessa. Tästä työstä opin erityisesti suunnittelemisen tärkeyden sekä uuden verkkoprotokollan toimintaperiaatteen. Tietoliikenneverkko valmisti minua työskentelemään yritysympäristössä, koska virtuaalipalvelimet sekä IPv6-protokolla alkavat olemaan nykypäivää monessa yrityksessä.

6 Pohdinta

Internet on tänä päivänä tulossa yhä suurempaan osaan ihmisten jokapäiväistä elämää. Yritykset ja koulut pyrkivät kehittämään tekniikoita vähentääkseen paperin käyttöä. Paperiarkistoinnin vähentyessä se muuttuu sähköiseen muotoon. Tietojen arkistoinnin voi sijoittaa erilliselle palvelimelle, joka on ratkaisuna tietoturvallisesti parempi.

Internetin käytön lisääntyminen kuluttaa IP-osoitteet loppuun. Osoitteiden loppumista on pyritty estämään erilaisilla osoitteenmuunnostekniikoilla, kuten esimerkiksi NAT-tekniikka. Nämä tekniikat eivät pysty loputtomiin estämään IPv4-osoitteiden loppumista.

IPv6-protokolla on hyvä ratkaisu tähän IP-osoitteiden rajalliselle käytölle. Odotettavissa on ongelmia, kun uuteen protokollaan aletaan siirtyä. Päätelaitteet ja laitteisto on vaihdettava tai päivitettävä uuteen, jotta saadaan IPv6-protokollalle tuki. Suuressa osassa yrityksiä ja laitoksia on osattu jo ennalta varautua tähän siirtymävaiheeseen. Varsinkin kokemattomien käyttäjien kohdalla joudutaan todennäköisesti järjestämään IPv6-protokollan osaamista tukevia koulutuksia.

Tulevaisuudessa IPv6-protokollaa tullaan käyttämään IPv4-protokollan korvaajana. Muutos tulee olemaan väistämätön, koska laitteita liittyy Internetiin koko ajan lisää ja IPv4-osoiteavaruus ei riitä loputtomasti.

IPv6-protokolla turvaa sen, että osoitteet eivät tule vähään aikaan loppumaan. IPv6-protokollan osoiteavaruus on laajennettu edeltäjäänsä verrattuna suuremmaksi. Tämä

takaa sen että IP-osoitteita pystytään jakamaan laitteille, niin että osoitteet eivät tule ainakaan lähivuosina loppumaan.

Lähteet

1. Ahonen, Riku-Matti. Mobile IPv6 yhteensopivuus eri laiteympäristöissä. Tietotekniikan Pro Gradu –tutkielma 2007 [Viitattu 1.2.2011]. Saatavissa: http://research.jyu.fi/laila/Gradu_RA.pdf

2. Cisco Networking Academy Exploration 4.0. Chapter 7.3 IPv6 [Viitattu 3.2.2011]. Saatavissa: http://tekniikka.ncp.fi/Cisco/exploration/Exploration4_English/theme/cheetah.html?cid=1400000000&l1=en&l2=none&chapter=7

3. Vatilainen, Heikki. IPv6 tarkemmin. TLT-2600 Verkkotekniikan jatkokurssi [Viitattu 3.3.2011]. Saatavissa: http://www.cs.tut.fi/~hessu/ipv6-2006-2.pdf

4. Windows Server 2008R2. Overview. [Viitattu 23.4.2011]. Saatavissa: http://www.microsoft.com/windowsserver2008/en/us/overview.aspx

5. Baptista, Miguel. Lorga, Pedro. Muyal, Simon. Router configuration. South Africa Workshop WALC 2006 (Quito, Equador -26-28 July ’06) [Viitattu1.5.2011]. Saatavissa: http://www.6diss.org/workshops/sca/routers-1.pdf

6. Rantasalmi, Keijo. IPv6:n käyttöönotto taideteollisessa korkeakoulussa. Tietotekniikan insinöörityö 2009 [Viitattu 1.5.2011]. Saatavissa: https://publications.theseus.fi/bitstream/handle/10024/2957/RantasalmiKeijo%20Insinoorityo.pdf?sequence=1

7. Vincent NG. Technical consultant. IPv6 Router Desing and Configuration [Viitattu 1.5.2011]. Saatavissa: http://202.112.35.201/multicast/ipv6-5.pdf

Liite 1

IPv6-opetusverkko: Reititin 1 konfiguraatio

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
 hostname router1
!
 logging queue-limit 100
!
 ip subnet-zero
!
 ipv6 unicast-routing
!
 interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A01:101::1/64
 ipv6 rip koe enable
 tunnel source Serial1
 tunnel mode ipv6ip 6to4
 no shutdown
!
 interface FastEthernet0
 no ip address
 speed auto
 ipv6 address 2002:A01:101:1::1/64
 ipv6 enable
 ipv6 rip koe enable
 no shutdown
!
 interface Serial1
 ip address 10.1.1.1 255.255.255.0
 ipv6 enable
 ipv6 rip koe enable
 clockrate 64000
 no shutdown
!
ip classless
no ip http server
!
ipv6 route 2002::/16 Tunnel0
ipv6 router rip koe
!
end
```

Liite 2

IPv6-opetusverkko: Reititin 2 konfiguraatio

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
logging queue-limit 100
!
ip subnet-zero
!
no ip domain lookup
!
ipv6 unicast-routing
!
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A01:102::1/64
 ipv6 rip koe enable
 tunnel source Serial1
 tunnel mode ipv6ip 6to4
no shutdown
!
interface FastEthernet0
 ip address 10.1.2.2 255.255.255.0
 speed auto
 ipv6 address 2002:A01:102:1::1/64
 ipv6 enable
 no ipv6 redirects
 ipv6 rip koe enable
no shutdown
!
interface Serial1
 ip address 10.1.1.2 255.255.255.0
 ipv6 rip koe enable
no shutdown
!
router rip
!
ipv6 route 2002::/16 Tunnel0
ipv6 router rip koe
!
end
```

Liite 3

IPv6-opetusverkko: Kytkin 1 konfiguraatio

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname kytkin1
!
vlan internal allocation policy ascending
!
interface GigabitEthernet0/1
 switchport access vlan 10
!
interface GigabitEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/14
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan1
 no ip address
 ipv6 enable
!
interface Vlan10
 ip address 10.1.1.1 255.255.255.0
 ipv6 enable
!
end
```

Liite 4

IPv6-opetusverkko: Kytkin 2 konfiguraatio

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname kytkin2
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface Vlan1
 ip address 10.1.2.1 255.255.255.0
 no ip route-cache
!
ip http server
!
control-plane
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
end
```

Liite 5

IPv6-opetusverkon reititystaulut

router1#show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
S 2002::/16 [1/0]
via ::, Tunnel0
C 2002:A01:101::/64 [0/0]
via ::, Tunnel0
L 2002:A01:101::1/128 [0/0]
via ::, Tunnel0
C 2002:A01:101:1::/64 [0/0]
via ::, FastEthernet0
L 2002:A01:101:1::1/128 [0/0]
via ::, FastEthernet0
L FE80::/10 [0/0]
via ::, Null0
L FF00::/8 [0/0]
via ::, Null0

router2#show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
S 2002::/16 [1/0]
via ::, Tunnel0
C 2002:A01:102::/64 [0/0]
via ::, Tunnel0
L 2002:A01:102::1/128 [0/0]
via ::, Tunnel0
C 2002:A01:102:1::/64 [0/0]
via ::, FastEthernet0
L 2002:A01:102:1::1/128 [0/0]
via ::, FastEthernet0
L FE80::/10 [0/0]
via ::, Null0
L FF00::/8 [0/0]
via ::, Null0