TEKNIIKKA JA LIIKENNE

Tietotekniikka

Ohjelmistotekniikka

INSINÖÖRITYÖ

IPv6:N KÄYTTÖÖNOTTO TAIDETEOLLISESSA KORKEAKOULUSSA

Työn tekijä: Keijo Rantasalmi
Työn valvoja: Janne Salonen
Työn ohjaaja: Mika Niemi

Työ hyväksytty: __. __. 2009

Janne Salonen
yliopettaja

Metropolia

INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä: Keijo Rantasalmi	
Työn nimi: IPv6:n käyttöönotto Taideteollisessa korkeakoulussa	
Päivämäärä: 4.3.2009	Sivumäärä: 29 s. + 1 liitettä
Koulutusohjelma: Tietotekniikka	Suuntautumisvaihtoehto: Ohjelmistotekniikka
Työn ohjaaja: yliopettaja Janne Salonen Työn ohjaaja: Mika Niemi	
Työn tarkoituksena oli tutustua uuteen Internet-protokollaan ja samalla tutkia IPv6:een siirtymisen tuomia etuja tietoverkon toiminnalle sekä protokollan käyttöön siirtymisen helppoutta. Tarkoituksena oli myös saada aikaan prosessi, joka helpottaa organisaation siirtymistä uuden protokollan käyttöön. Työn aikana tutustuttiin uuden protokollan rakenteeseen ja toimintaan sekä vertailtiin vanhan ja uuden protokollan ominaisuuksia. Työssä tarkasteltiin myös hieman DHCPv6:tta, joka on tarkoitettu toimimaan IPv6-verkoissa. Samaten tutustuttiin jossain määrin protokollan tarjoamiin tietoturvaominaisuuksiin sekä nimipalvelimien tarjoamiin palveluihin uudelle protokollalle. Käytännössä IPv6-protokollan toimintaa tarkasteltiin muutaman tietokoneen ja reitittimen laboratorioverkossa.	
Avainsanat: IPv6, DHCPv6	

Metropolia

ABSTRACT

Name: Keijo Rantasalmi

Title: Implementing IPv6 in University of Art and Design Helsinki

Date: 4.3.2009 Number of pages: 29 + 1 appendix

Department: Information Technology Study Programme: Software Engineering

Instructor: Janne Salonen

Supervisor: Mika Niemi

The purpose of this study was to become acquainted with the new Internet protocol and investigate the advantages for the network when transferring to IPv6 protocol. One purpose was also to create a process to implement easily the new protocol.

During the study the structure and functions of the new protocol were examined and the properties of the old and the new protocol were compared. During the study DHCPv6 protocol was also studied. The security properties of the protocol were also studied. In practice the new IPv6 protocol was tested in a network consisting of a few computers and routers.

Keywords: IPv6, DHCPv6

SISÄLLYS

TERMIEN SELITYKSET

AAA	Authentication, Authorization and Accounting: tunnistaminen, valtuutus ja kirjaaminen.
AH	Authentication Header: menetelmä, jota käyttämällä sanoman lähettäjä voidaan luotettavasti tunnistaa.
BIND	Berkeley Internet Name Domain: Alkujaan Berkeleyn yliopiston kehittämä nimipalvelinohjelmisto, jonka kehityksestä ja ylläpidosta vastaa nykyään Internet Systems Consortium ISC.
CIDR	Classless Inter-Domain Routing: protokolla, jonka avulla pystytään yli- ja aliverkottamaan luokallisia verkkoja sekä esittämään reitit yhdistettyinä reititystauluissa.
DDNS	Dynamic DNS: mekanismi, jonka avulla pystytään automatisoimaan dynaamisesti jaettujen verkko-osoitteiden ylläpito nimipalvelimilla.
DHCP	Dynamic Host Configuration Protocol: protokolla, jonka avulla tietokoneille pystytään jakamaan tietoliikenneasetukset keskitetysti.
DNS	Domain Name System: hierarkkinen järjestelmä, jonka avulla IP-osoitteet yhdistetään konenimiin tai päinvastoin. Esim. www.ipv6.funet.fi nimeä vastaa osoite 2001:708:10:f::c1a6:301.
ESP	Encapsulating Security Payload: protokolla, joka salaa lähetettävän tiedon.
EUI-64	Extended Unique Identifier: 64-bittinen globaali yksilöllinen tunniste.
IANA	Internet Assigned Numbers Authority: organisaatio, joka vastaa Internetin osoitteiden jakamisesta.
IETF	Internet Engineering Task Force: avoin kansainvälinen yhteisö, joka muodostuu verkkosuunnittelijoista, operaattoreista, valmistajista ja tutkijoista, jotka ovat kiinnostuneet kehittämään Internetin arkkitehtuuria. Yhteisö on avoin kaikille IETF:n tehtävästä (RFC3935) kiinnostuneille.
IKE	Internet Key Exchange: protokolla, jonka avulla pystytään automaattisesti vaihtamaan IPsec-salausavaimia koneiden välillä.
IPsec	Internet Protocol security: salaukseen perustuva ryhmä turvallisuuspalveluita ja protokollia IP-kerroksen liikennettä varten. IPsec tarjoaa pääsyn valvonnan, eheyden, lähteen autentikoinnin, toiston havaitsemisen ja hylkäyksen sekä luottamuksellisuuden.
LAN	Local Area Network: lähiverkko, yleensä maantieteellisesti hyvin pienellä alueella oleva tietoverkko.

LIR	Local Internet Registry: paikallinen Internet-rekisteri, vastaa Internet-osoitteiden jakamisesta ja ylläpidosta paikallisella tasolla, usein Internet-operaattoreita tai suuria yrityksiä.
MTU	Maximum Transfer Unit: verkossa lähetettävän tietosähkeen suurin mahdollinen koko.
RADIUS	Remote Access Dial-In User Service: protokolla, jonka avulla voidaan suorittaa turvallinen kirjautuminen verkkoresursseihin. Radius voi myös suorittaa autorisoinnin ja kirjaamisen.
RFC	Request for Comments: IETF:n ylläpitämä avoin asiakirjakokoelma, joka on vapaasti kaikkien kiinnostuneiden muokattavissa.
RIPE	Réseaux IP Européens: organisaatio, joka vastaa ip-osoitteiden jakamisesta ja niiden ylläpidosta Euroopassa, Lähi-Idässä sekä Keski-Aasiassa.
RIR	Regional Internet Registry: alueellinen Internet-rekisteri, vastaa alueensa Internet-osoitteiden ylläpidosta, esim. RIPE.
RR	Resource Record: resurssitietue, nimipalvelun tietokannan tietue, joita on useaa tyyppiä, esim. AAAA, joka tarkoittaa IPv6-osoitetta ja MX, joka on postipalvelin.
SA	Security Association: määrittää yhteydessä käytettävät tiiviste- ja salausalgoritmit.
SPI	Security Parameter Index: määrittää yhteydessä käytettävän SA:n.
TACACS+	Terminal Access Controller Access Control System Plus: Cisco Systemsin käyttäjän tunnistamisprotokolla, joka toimii AAA-palvelimena.
VLAN	Virtual LAN: virtuaalinen lähiverkko. Fyysisesti samassa segmentissä olevat tietokoneet on jaettu eri loogisiin verkkoihin. Eri VLANien väliseen liikennöintiin tarvitaan reititintä.
VPN	Virtual Private Network: virtuaalinen yksityinen verkko, menetelmä, jonka avulla luodaan julkista verkkoa käyttäen verkko, joka toimii kuten yksityinen verkko.
WAN	Wide Area Network: maantieteellisesti laajalle alueelle levinnyt tietoverkko.

1 JOHDANTO

Tässä työssä tutustuttiin Internetprotokollan versio kuuteen (IPv6). Ensin työssä tarkasteltiin uuden protokollan rakennetta ja vertailtiin sitä vanhaan IPv4-protokollaan. Tämän jälkeen protokollan toimintaan tutustuttiin testaamalla erilaisia konfigurointeja laboratorioverkossa.

Työ tehtiin Taideteolliselle korkeakoululle, jotta selvitettäisiin IPv6-protokollan käyttöön siirtymisen helppoutta ja mahdollisia ongelmia. Työn tarkoituksena oli myös määrittää prosessi, jonka avulla tulevaisuudessa IPv6:n käyttöönotto helpottuisi.

Luvussa kaksi selvitetään Internetin laajenemista ja keinoja, joilla on pystytty jatkamaan IPv4:n käyttöä, vaikka osoitteiden määrä on rajallinen. Luvussa esitetään myös IPv6:n kehityksen pääpiirteet. Kolmannessa luvussa tutustutaan tarkemmin uuteen protokollaan ja vertaillaan sen ominaisuuksia ja rakennetta vanhaan versioon.

Luvuissa neljä ja viisi tarkastellaan eri mahdollisuuksia verkon solmun konfigurointia varten sekä nimipalvelun konfigurointia. Tässä selvitetään autokonfiguraation ja dynaamisen konfiguroinnin ominaisuuksia sekä niiden etuja ja haittoja. Luvussa tarkastellaan myös nimipalvelun toimintaa sekä selvitetään suositun BIND-nimipalvelimen IPv6-ominaisuuksia. Kuudes luku käsittelee IPv6-protokollaan liittyvää tietoturvaa sekä siihen liittyviä protokollia.

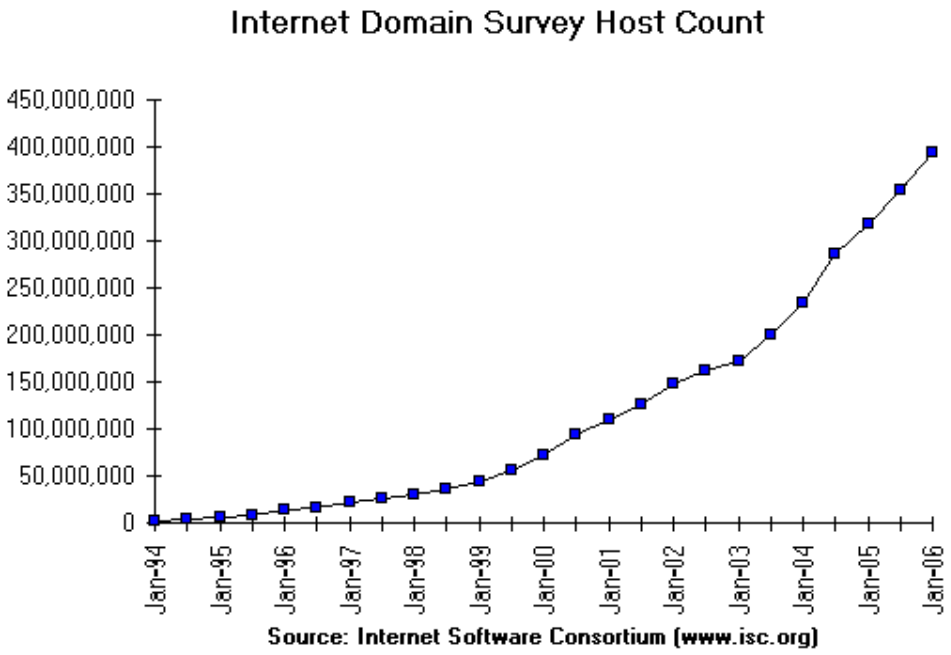
Luku seitsemän esittää Taideteollisen korkeakoulun tietoliikenneverkon rakenteen. Siinä esitetään myös protokollaa testattaessa käytetty laboratorioverkko.

Kahdeksannessa luvussa tutkitaan testien tuloksia sekä niiden perusteella tehtyjä johtopäätöksiä. Luku yhdeksän on yhteenveto lopputyöstä.

2 INTERNET-PROTOKOLLA

Internet-protokolla versio 6:n kehittäminen alkoi 1990-luvun puolivälissä. Tähän ajoi ensisijaisesti pelko käytössä olevan versio 4:n osoitteiden loppu-

misesta Internetin räjähdysmäisen kasvun seurauksena. Elokuussa 1981 Internetissä oli 213 tietokonetta [12 s. 4]. Vuoden 1986 puolivälissä verkkoon oli rekisteröity 3100 konetta, 1990 koneita oli noin 137 000 ja vuonna 2000 60 miljoonaa [1 s. 462]. Kuva 1 esittää Internetiin liitettyjen laitteiden määrän kasvun vuodesta 1994 tammikuuhun 2006. Huiteman mukaan ip-osoitteiden määrässä saavutetaan teoreettinen yli neljän miljardin maksimimäärä vuosien 2005 ja 2015 välillä [2 s. 3].



Kuva 1: Internetiin liitettyjen koneiden lukumäärän kehitys

IPv4 on jo lähes kaksikymmentä vuotta vanha. Se on vuosien aikana osoittautunut toimivaksi ja joustavaksi protokollaksi. Mutta silläkin on puutteensa, joista suurin lienee osoitteiden luokat. Nämä rajoittavat osoitteiden tehokasta käyttöä. Koska osoitteilla ei ole hierarkiaa, peräkkäiset verkot saattavat sijaita missä päin maailmaa tahansa Tämä vaikeuttaa ja hidastaa reititystä, koska reititystaulut muodostuvat suuriksi.

Alkujaan osoiteavaruus on jaettu viiteen luokkaan: A-, B-, C-, D- ja E-luokkaan [3 s. 7]. A-luokan verkkoja on vain 126 kappaletta ja kussakin voi olla yli 16,7 miljoonaa päätelaitetta. B-luokan verkkoja on runsaat 16000 kappaletta ja kussakin verkossa voi olla 65534 laitetta. C-luokan verkkoja on yli 2

miljoonaa mutta niissä kussakin voi olla vain 254 konetta. D-luokan osoitteet ovat monilähetysosoitteita ja E-luokka on varattu kokeilukäyttöön.

Classless Inter-Domain Routing

IPv4-osoitteita on vielä riittänyt, koska on kehitetty eri tapoja kiertää osoitteiden vähyyttä. Koska IPv4 perustuu osoiteluokkiin, kehitettiin Classless Inter-Domain Routing CIDR. Tämän menetelmän avulla ei olla riippuvaisia osoitteiden luokkarajoista, vaan niitä pystytään aliverkottamaan eli jakamaan pienemmiksi verkoiksi, joiden aliverkon peite (subnet mask) ei rajoitu alkuperäisiin 8, 16 tai 24 bittiin vaan voi olla periaatteessa miten monta bittiä tahansa. Käytännössä pisin mahdollinen peite on 30 bittiä, jolloin aliverkossa on neljä osoitetta ja siinä voi olla kaksi konetta. CIDR:in avulla käytettävät verkot voidaan jakaa sopivan kokoisiksi verkoiksi, jolloin osoitteita ei mene hukkaan. CIDR mahdollistaa myös useiden peräkkäisten verkkojen yhdistämisen reitityksen kannalta yhdeksi suuremmaksi (aggregointi). Tällöin reitittimien osoitetaulut pysyvät pienempinä ja reititys tapahtuu nopeasti.

Yksityiset verkko-osoitteet

Internetin osoitepulaa helpottamaan RFC 1918:ssa määritellään osoiteavaruudet, joita kuka tahansa saa käyttää. Ainoa rajoitus on se, ettei niitä saa reitittää Internetiin. Julkisia osoitteita tarvitaan vain laitteille, joihin tarvitaan pääsyä Internetistä, esim. www- ja postipalvelimet. Omassa lähiverkossa voidaan käyttää RFC 1918:n määrittämiä osoitteita. Tällöin lähiverkon osoitteet käännetään julkisiksi osoitteiksi NAT-laitteessa. Tämä on yleensä reititin tai palomuurilaite, joka sijaitsee lähiverkon ja Internetin rajalla.

Uusi protokolla

Tammikuussa 1995 S Bradner ja A Mankin saivat valmiiksi suosituksen uuden protokollan ominaisuuksista (RFC 1752). Ensimmäinen versio määrittelystä valmistui joulukuussa 1995 (RFC 1883). Sen jälkeen protokollaa on kehitetty ja siihen on tullut useita muutoksia, tätä kirjoitettaessa viimeisimmät huhtikuussa 2006.

Protokolla on ollut testikäytössä laajasti jo vuosia. Muun muassa eurooppalainen 6net-projekti toteutti natiivin IPv6-verkon 16 maan välille. Tämän kolmivuotisen projektin tarkoituksena oli demonstroida, että uuden IPv6-teknologian avulla pystytään kohtaamaan Internetin jatkuva kasvu. Projekti on nyt päättynyt ja verkko lakkautettiin. Natiivien IPv6-yhteyksien hallinta luovutettiin Géantille. Géant-projekti tarjoaa useiden gigabittien yhteyksiä kansallisten tutkimus- ja oppilaitosten käyttöön. [4 s. 5] Suomalainen Funet osallistui myös 6net-projektiin ja tarjoaa asiakkailleen myös IPv6-yhteyksiä.

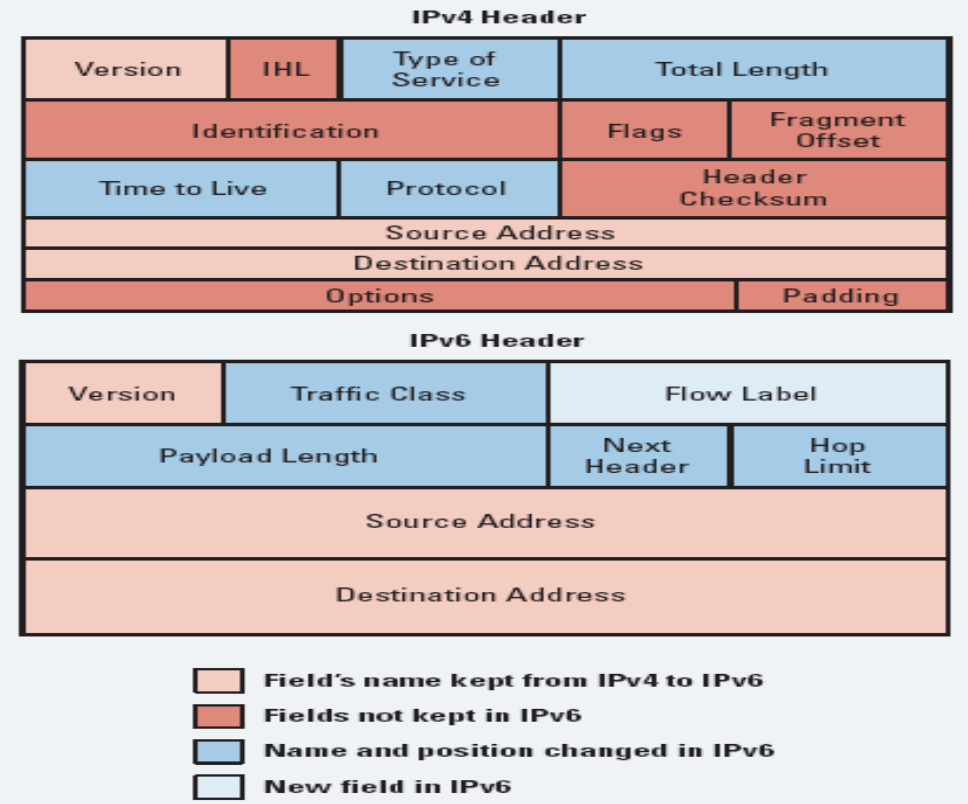
Uusi protokolla on erityisen runsaasti käytössä Aasiassa, koska siellä tietokoneiden määrä on lisääntynyt räjähdysmäisesti, mutta IPv4-osoiteavaruuksia ei ole ollut jakaa riittävästi.

Kesäkuun 6. päivä 2006 oli tärkeä merkkipaalu IPv6:n kehityksessä. Tällöin lakkautettiin kymmenen vuotta toiminut maailmanlaajuinen IPv6-verkko, 6bone, joka toimi testialustana protokollalle. Tämän myötä IPv6:sta tuli tuotantovalmis protokolla, jolle on tuki lähes kaikkien valmistajien tuotteissa. Lisäksi ainakin eräät suuret asiakkaat alkavat vaatia ostamiltaan laitteilta tukea IPv6:lle. Esimerkiksi Yhdysvaltain puolustusministeriö on ilmoittanut ostavansa lokakuusta 2003 lähtien vain IPv6:tta tukevia laitteita [5 s. xxii] ja valtion hallinnon tavoitteena oli täysi IPv6-implementaatio vuonna 2008.

3 IPV6-PROTOKOLLA

Uuden protokollan huomattavin ero vanhaan on osoitteen kasvaminen 32 bitistä 128 bittiin. Teoriassa osoitteita on nyt siis 2^{128} eli $3{,}4*10^{38}$ kappaletta. Osoiteavaruuden voidaan katsoa olevan vähintäänkin riittävä. Maapallon ikä on noin 4,5 miljardia vuotta ja jos sinä aikana olisi otettu käyttöön miljardi osoitetta sekunnissa, nyt olisi kulutettu biljoonasosa osoitteista [6]. IPv6-protokollassa on pyritty säilyttämään vanhan version hyvät ominaisuudet, kuten yksinkertaisuus, skaalautuvuus, joustavuus ja laajennettavuus. Siitä on jätetty pois IPv4:ssä olevia turhiksi osoittautuneita ominaisuuksia ja muutettu toisia ja lisätty joitain IPv4:stä puuttuneita ja kaivattuja ominaisuuksia. Sen lisäksi protokollaa on pyritty yksinkertaistamaan ja reititystä nopeuttamaan.

3.1 Otsikoiden rakenne



Kuva 2: IP-otsikoiden rakenne

Kuvassa 2 on esitetty eri versioiden otsikoiden rakenne sekä kenttien nimet. Kenttien määrä on vähentynyt kahdeksaan pakolliseen kenttään ja niiden selitykset lyhyesti ovat seuraavat:

Versio 4

- Version: 4 bittiä ja arvona 4
- Internet Header Length, 4 bittiä, otsikon pituus, koska pituus voi vaihdella options-kentän sisällöstä riippuen
- Type of Service, 8 bittiä, palvelun laatu
- Total Length, 16 bittiä, datagrammin pituus
- Identification, 16 bittiä, tunniste pirstoutuneiden datagrammien kokoamiseksi
- Flags, 3 bittiä, ensimmäinen varattu, aina 0, toinen bitti 0= May Fragment 1=Don't Fragment, kolmas bitti 0=Last Fragment 1=More Fragments

- Fragment Offset, 13 bittiä, osoittaa fragmentin ensimmäiseen oktettiin
- Time to Live, 8 bittiä, datagrammin elinaika sekunteina, jokainen reitillä oleva reititin pienentää arvoa paketin käsittelyyn kuluneella ajalla tai vähintään yhdellä
- Protocol, 8 bittiä, ilmoittaa ylemmän tason protokollan, (TCP, UDP)
- Header Checksum, 16 bittiä, otsikon tarkastussumma, lasketaan joka reitittimessä uudestaan
- Source Address, 32 bittiä
- Destination Address, 32 bittiä
- Options, n bittiä, eri optiot
- Padding, n bittiä, täytebitit, joilla otsikon pituus saadaan m*32-bittiseksi.

IPv4-otsikko on aina vähintään 20 oktettia pitkä.

Versio 6

- Version, 4 bittiä, arvo 6
- Traffic Class, 8 bittiä, liikenteen luokka, käytetään palvelun laadun toteuttamisessa
- Flow Label, 20 bittiä, vuon tunnus, lähinnä reaaliaikaisen liikenteen siirtoon, reitittimet tarjoavat vuolle tiettyä palvelua
- Payload Length, 16 bittiä, hyötykuorman pituus, otsikon jälkeen paketissa olevien oktettien määrä, sisältää myös seuraavat otsikot
- Next Header, 8 bittiä, seuraava otsikko, joko valinnainen otsikko tai ylemmän kerroksen (TCP, UDP) otsikko
- Hop Limit, 8 bittiä, rajoittaa paketin eliniän, jokainen välittävä reititin pienentää arvoa yhdellä

- Source Address, 128 bittiä, lähdeosoite
- Destination Address, 128 bittiä, kohdeosoite.

Uudessa versiossa perusotsikon (base header) pituus on aina 40 oktettia. Tämä helpottaa reitittimien muistinhallintaa, koska otsikkoa varten pystytään varaamaan aina saman suuruinen muistialue ja tällä tavoin reititys nopeutuu.

3.2 Lisäotsikot

IPv4:n Options-kentän toiminnot on siirretty lisäotsikoihin. Näitä käytetään vain, jos on tarvetta erilaisiin lisätoimintoihin. Lisäotsikko sijoitetaan perusotsikon ja datan väliin ja perusotsikon Next Header -kenttä ilmoittaa seuraavan lisäotsikon tyypin. Otsikon tyyppeinä käytetään RFC 1700 ja sen seuraajien määrittämiä tyyppejä, jotka ovat samat kuin IPv4:ssä. Kuvassa 3 esitetään, kuinka lisäotsikoita voidaan ketjuttaa useita peräkkäin.

IPv6 header Next Header = TCP	TCP header + Data		
IPv6 header Next Header = Routing	Routing header Next Header = TCP	TCP header + data	
IPv6 header Next Header = Routing	Routing header Next Header = Fragment	Fragment header Next Header = TCP	fragment of TCP header + data

Kuva 3: IPv6-otsikoiden ketjutus

IPv6:ssa on mahdollista liittää mielivaltainen määrä lisäotsikoita ip-otsikon ja hyötykuorman väliin. Kukin otsikko sisältää otsikkotyypin ja ketjun seuraavan otsikon tyypin tai viimeisen lisäotsikon ollessa kyseessä hyötykuorman otsikon.

Jos ip-paketissa on useampia otsikoita, niiden järjestykseksi suositellaan seuraavaa [7 s. 7-8]:

- IPv6

- Hop-by-Hop, jokainen matkalla oleva solmu käsittelee nämä
- Destination Options, jokaiselle matkalla olevalle solmulle tarkoitetut optiot
- Routing, lähde käyttää tätä listatakseen solmut, joiden kautta reitin pitää kulkea
- Fragment, lähde lähettää paketin, joka on suurempi kuin polun MTU
- Authentication, lähteen tunnistus ja tiedon muuttumattomuuden varmistus
- Encapsulating Security Payload, takaa tiedon luottamuksellisuuden, lähteen tunnistamisen, koskemattomuuden ja toistamattomuuden
- Destination Options, vastaanottajalle tarkoitetut optiot
- upper layer, ylemmän kerroksen protokolla.

Tätä järjestystä suositellaan siksi, ettei matkalla olevien reitittimien tarvitse käydä läpi kaikkia otsikoita, vaan että se pystyy mahdollisimman nopeasti lähettämään paketin edelleen.

IPv4:n Fragment Offset -kenttä on jätetty pois, koska tietosähkettä ei pirstota matkan varrella olevissa reitittimissä, vaan se tehdään ainoastaan lähettävässä solmussa. Protokollassa on määritelty, että reitittimien tulee välittää vähintään 1280 oktettia pitkä datagrammi. Lisäksi lähettävä solmu voi selvittää itsensä ja kohteen välisen reitin pienimmän MTU:n. Protokollassa suositellaan käytettäväksi aina mahdollisimman suurta datagrammia, jolloin hyötysuhde on paras.

3.3 IPv6-osoitteet

IPv6-osoite on 128 bitin pituinen. Se jakautuu 64-bittiseen verkko-osaan ja 64-bittiseen sovitinosaan. IPv4-osoitteista poiketen osoite yhdistetään verkkosovittimeen eikä verkon solmuun. Koska yhdellä solmulla voi olla useita sovittimia, solmuun voidaan viitata minkä tahansa sen sovittimen osoitteella.

[8 s. 3] Osoite esitetään kahdeksana 16 bitin ryhmänä heksadesimaalilukuina. Ryhmien välissä käytetään erottimena kaksoispistettä, esim.

FEDC:BA98:0000:0076:0000:1234:5678:9ABC.

Jos osoitteessa on kokonaisia 16 nolla-bitin ryhmiä, ne voidaan korvata kahdella kaksoispisteellä. Tätä merkintää voidaan käyttää vain kerran osoitteessa, koska muutoin osoite ei ole enää yksiselitteinen. Myöskään alkunollia ei tarvitse merkitä. Edellä oleva osoite voidaan tällöin esittää seuraavilla tavoilla:

FEDC:BA98::76:0:1234:5678:9ABC tai

FEDC:BA98:0:76::1234:5678:9ABC.

Osoite muodostuu etuliitteestä, prefix, ja sovittimen tunnisteesta. Etuliitteen merkinnässä käytetään vastaavaa tapaa kuin IPv4:n CIDR aliverkon peitto. Osoitteesta merkitään verkon tunniste ja peiton bittimäärä.

3.4 Osoitetyypit ja näkyvyys

Osoitteet on jaettu eri alueisiin, joilla on kiinteä merkitys:

- määrittelemätön osoite (unspecified) ::/128
- silmukkaosoite (loopback) ::1/128
- monilähetys (multicast) FF00::/8
- link-local FE80::/10
- site-local FEC0::/10
- globaali yksilähetys kaikki muut.

Lisäksi on olemassa anycast-osoitteet, jotka ovat osa yksilähetysosoitteita. Anycast-osoitteelle ei ole vastinetta IPv4:ssä. Sama anycast-osoite on usealla sovittimella, yleensä eri koneissa. Jos ip-paketin kohdeosoite on anycast-

osoite, se lähetetään yhdelle, reititysprotokollan mukaan lähimmälle, koneelle. Verkossa voi olla esimerkiksi useita samaa tehtävää hoitavia palvelimia, jolloin asiakkaan pyyntö lähetetään vain yhdelle niistä.

Osoitteen näkyvyys (scope) voi olla yksilähetysosoitteilla linkki (link-local) tai globaali. Alkuperäisessä määrityksessä oli myös site-local-näkyvyys, joka on poistettu käytöstä. Syyt sen poistamiseen olivat osoitteiden moniselitteisyys ja käsitteen ”site” epäselvyys. Nämä tekijät aiheuttivat ongelmia sovellusten kehittäjille, verkon ylläpitäjille sekä reitittimille. Uudet IPv6-toteutukset eivät saa tukea site-local-osoitteita, mutta jo olemassa olevat voivat käyttää sitä edelleen. [9 s. 2-7.]

Link-local-osoitteen etuliite on fe80::/10. Sama osoite voi periaatteessa olla usealla eri sovittimella, kunhan ne ovat eri fyysisessä linkissä. Tämä osoite on vastaava kuin IPv4:n 169.254.0.0/16-osoite. Nämä osoitteet ovat merkityksellisiä vain yhdessä linkissä. Tällaisessa tapauksessa tietenkin linkin jokaisella koneella täytyy olla yksilöllinen osoite. Samassa linkissä olevat koneet pystyvät kommunikoimaan keskenään ilman reitititintä. Globaalit osoitteet vastaavat IPv4:n julkisia osoitteita.

Osoitehierarkia

IPv4-osoitteissa peräkkäiset verkot saattavat sijaita maantieteellisesti hyvinkin etäällä toisistaan. Esimerkiksi 192.5.2.0/24-verkko kuuluu Floridan yliopistolle Gainesvillessä, kun taas seuraava verkko, 192.5.3.0/24, on Beverly Hillsin kaupungin verkko Kaliforniassa. Tämän hajanaisuuden takia reittien summaaminen eli usean pienen verkon mainostaminen yhdellä osoitteella ei ole mahdollista ja runkoreitittimien reititystaulut kasvavat suuriksi. Tämä hidastaa reititystä, koska reitityksessä käytetään pisimmän vastaavuuden periaatetta. Tällöin jos reititystaulussa on samalla etuliitteellä useita merkintöjä, liikenne ohjataan sinne, jonka aliverkon peite on pisin.

IPv6-protokollan osoitteistoa suunniteltaessa on otettu huomioon hierarkkisuus, joka helpottaa hallintaa. Globaalin yksilähetysosoitteen määrittää sen etuliitteen kaksi ensimmäistä oktettia: 2001::/16 on tavallinen IPv6-osoite ja

2002::/16 6to4-osoite, joka mahdollistaa IPv6:n automaattisen tunneloinnin IPv4-verkon yli.

Kuva 4 esittää IPv6-osoitteen etuliitteen muodostumisen.

16	16	16	16
2001	Assigned by RIR	Assigned by LIR	Subnet ID

Kuva 4: IPv6-etuliitteen rakenne.

Kaksi ensimmäistä oktettia (2001) määrittää osoitteen globaaliksi yksilähetysosoitteeksi. Alueellisen Internet-rekisterin, RIR (esim. RIPE), ylläpitäjä määrittää asiakkaalleen kolmannen ja neljännen oktetin. Nämä asiakkaat ovat paikallisia Internet-rekisterin, LIR, ylläpitäjiä, useimmiten Internet-palveluntarjoajia. Joskus kyseessä voi olla suuri yritys tai muu organisaatio. LIR jakaa hallitsemastaan osoiteavaruudesta palasia omille asiakkailleen määrittämällä viidennen ja kuudennen oktetin. Pääperiaatteena on, että kaikille asiakkaille annettavan verkon peite on 48 bittiä. Tällöin asiakkaalle jää vielä omia aliverkkojaan varten 16 bittiä eli 65 536 aliverkkoa.

3.5 Muita toimintoja

ICMP-nimiselvitys

Pääasiallinen tapa yhdistää ip-osoitteet ja nimet toisiinsa on DNS-nimipalvelu. IPv6:een on suositeltu mekanismia nimiselvitykseen ICMPv6-protokollan avulla. Tällä tavalla pystytään yhdistämään nimet ja osoitteet myös palvelimettomissa verkoissa. Selvityksessä käytetään Node Information Query - ja Node Information Reply -viestejä. Kysely voidaan osoittaa mille tahansa koneelle mutta kohde voi jättää vastaamatta kyselyyn. [5 s. 41.]

Uudelleennumerointi

Organisaation ip-osoitteet saattavat muuttua useasta syystä, esim. verkon topologiaa muutetaan tai palveluntarjoaja vaihtuu. Tällöin koneiden osoitteet täytyy saada muutettua. Tämä käy helposti, jos kyseessä on autokonfiguraatiolla osoitteensa määrittävät koneet, reitittimien mainostamien etuliitteiden muutos riittää. Mutta suuressa organisaatiossa voi olla useita kymmeniä rei-

tittimiä maantieteellisesti laajalla alueella. Näiden osoitteen muuttamiseen voidaan käyttää ICMPv6-protokollan Router Renumbering -viestejä, joiden avulla pystytään muuttamaan reitittimen osoitteen etuliitteet. Manuaalisesti konfiguroidut osoitteet joudutaan tietenkin muuttamaan yksitellen. [5 s. 42.]

4 AUTOKONFIGURAATIO JA DHCP

IPv6 määrittelee sekä tilattoman että tilallisen osoitteiden automaattisen konfiguroinnin. Nämä voivat olla käytössä sekä erikseen että yhtäaikaisesti, ja ne täydentävät toisiaan.

4.1 Tilaton autokonfiguraatio

IPv6:n tilaton autokonfiguraatio määritetään dokumentissa RFC 2462. Tilattomassa konfiguroinnissa (Stateless Autoconfiguration) tietokoneen asetuksia ei tarvitse asettaa manuaalisesti ja reitittimeenkin tarvitaan hyvin vähän asetuksia. Tämä mahdollistaa osoitteen luomisen jopa ilman reititintä. Jos reititin tai DHCP-palvelin ei anna etuliitettä, päätelaite pystyy luomaan itselleen vain link-local-osoitteen, jota voidaan käyttää vain samassa linkissä olevien koneiden välisessä liikenteessä.

Yleensä kuitenkin päätelaite saa ainakin ip-osoitteen etuliitteen DHCP-palvelimelta tai reitittimeltä. Tällöin päätelaite käyttää 64-bittistä tunnistetta, joka on EUI-64-tunniste tai luomaansa modified EUI-64 -tunnistetta, joka perustuu IEEE:n EUI-64-määritykseen. Määrityksen mukaan ensimmäisen oktetin toiseksi vähiten merkitsevän bitin arvo on yksi, jos tunniste on globaalisti ainutkertainen. Päätelaite luo itselleen tunnisteen, joka perustuu verkkosovittimen 48-bittiseen MAC-osoitteeseen. Tämä tapahtuu siten, että MAC-osoitteen seitsemäs bitti asetetaan ykköseksi. Lisäksi valmistajan tunnisteen kolmen oktetin ja sovittimen tunnisteen kolmen oktetin väliin lisätään kaksi oktettia, joiden arvo on fffe. Esimerkiksi jos verkkokortin fyysinen eli MAC-osoite on

00:d0:b7:84:47:a9,

siitä muodostuu seuraavanlainen modifioitu EUI-64:

02d0:b7ff:fe84:47a9.

Tämä liitetään 64-bittiseen joko verkon tunnisteeseen, joka on esimerkiksi 2001:db8:0:1001::/64, tai link-local -tunnisteeseen fe80::/10. Tällöin sovittimen tunniste on esimerkiksi

2001:db8:0:1001:2d0:b7ff:fe84:47a9,

joka on ainutkertainen globaali tunniste, jota voidaan käyttää kaikessa liikenteessä tai jos päätelaite ei saa reitittimeltä osoitteen etuliitettä,

fe80::2d0:b7ff:fe84:47a9, joka taas on link-local-osoite.

Asiakkaan täytyy myös varmistaa osoitteensa ainutlaatuisuus ennen sen yhdistämistä sovittimeen. Tämä tapahtuu siten, että asiakas suorittaa Duplicate Address Detection -proseduurin. Tämä suoritetaan kaikille yksittäislähetysosoitteille riippumatta siitä, onko osoite saatu tilattoman vai tilallisen autokonfiguraation avulla. Duplicate Address Detection on suoritettava kaikille yksittäislähetysosoitteille, paitsi seuraavissa tapauksissa:

- Osoite on anycast-osoite.
- Käytetään tilatonta autokonfiguraatiota, osoitteen ainutlaatuisuus päätetään ainoastaan sovittimen tunnisteen perusteella olettaen, että aliverkon liite on määritelty oikein. Siis jos samalla sovittimen tunnisteella määritetään useampia osoitteita, joissa verkon tunnisteet eroavat toisistaan, riittää, että tarkistetaan link-local-osoitteen ainutkertaisuus.

Kun päätelaite määrittää itselleen osoitteen, se asetetaan ensin testattavaan (tentative) tilaan. Osoitetta ei ole silloin yhdistetty sovittimeen perinteisessä mielessä. Sovittimen tulee hyväksyä Neighbor Solicitation- ja Neighbor Advertisement -viestit, joiden kohdeosoitteena on testattava osoite mutta käsiteltävä ne eri tavalla kuin paketit, jotka on osoitettu sovittimelle liitettyyn osoit-

teeseen. Lisäksi tämä sama osoitteen tunnistus tulee suorittaa ennen osoitteen yhdistämistä sovittimeen.

Tilaton DHCP

Tilaton DHCP-palvelu määritetään RFC 3736:ssa. Tilaton DHCP täydentää autokonfiguraatiota ja sitä käytetään, kun asiakkaat tarvitsevat sellaista tietoa, joka ei edellytä yksittäisen asiakkaan tilan seurantaa. Koneen, joka käyttää tilatonta DHCP:tä, täytyy määrittää osoitteensa jollain muulla tavalla, yleensä tilattomalla autokonfiguraatiolla. Tällöin solmu liittää oman sovittimen tunnisteensa reitittimeltä saatavaan etuliitteeseen, jolloin saadaan globaali yksikäsitteinen osoite, jota voidaan käyttää kaikessa liikenteessä. Reitittimeltä voidaan saada lisäksi ohje, että tarvitaan ylimääräisiä asetuksia, jolloin kone pyytää tiedot DHCP-palvelimelta. Tällä tavoin voidaan asiakkaalle asettaa esimerkiksi DNS- ja NTP-palvelimien tiedot.

4.2 Tilallinen autokonfiguraatio

Tilallisessa autokonfiguraatiossa (Stateful Autoconfiguration) tietokone saa tarvitsemansa tiedot DHCP-palvelimelta. Tietokoneella on DHCP-asiakasohjelma, joka suorittaa konfigurointitietojen pyytämisen palvelimelta. Asiakasohjelma voi pyytää useita eri tietoja yhdellä pyynnöllä.

Tilallisessa autokonfiguraatiossa asiakas saa palvelimelta IP-osoitteen sekä muut asetustiedot kuten esimerkiksi nimipalvelimien osoitteet. DHCP-palvelin voi myös asettaa osoitteille eliniän (preferred ja valid lifetime). Palvelin pitää yllä tietoa myöntämiensä osoitteiden tilasta, tästä syystä tätä konfigurointitapaa sanotaan tilalliseksi.

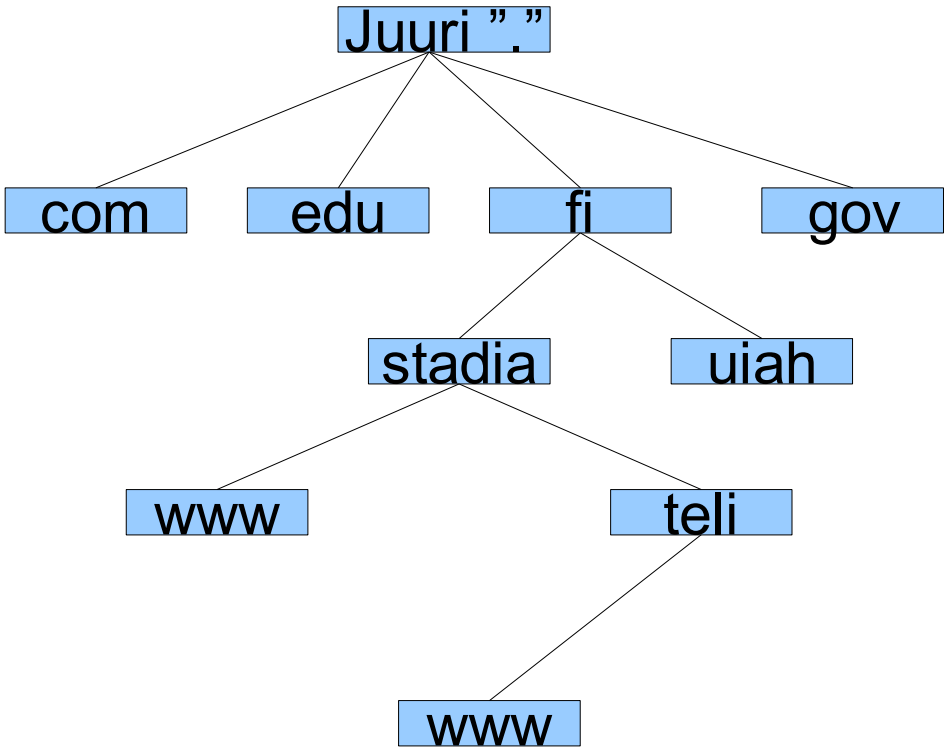
5 NIMIPALVELU

Internetin, tai oikeammin ARPAnetin, alkuaikoina nimipalvelu perustui Stanford Research Instituten Network Information Centerin, SRI-NIC, ylläpitä-

mään HOSTS.TXT-tiedostoon. Tässä tiedostossa oli kaikkien verkkoon liitettyjen koneiden nimi- ja osoitetiedot. ARPAnetin ylläpitäjät lähettivät muutokset sähköpostilla NICille, jossa muutokset lisättiin tiedostoon pari kertaa viikossa. Verkon kasvun myötä tällainen malli kävi ylivoimaiseksi ylläpitää ja päädyttiin kehittämään hierarkkinen nimipalvelumalli, joka nykyään on käytössä. [10 s. 3-4]

Nykyinen nimipalvelu, Domain Name System DNS, on hajautettu tietokanta. Nimiavaruus jakautuu toimialueisiin (domain). Toimialue voi muodostua useista alitoimialueista tai olla yksittäinen tietokone. Kukin toimialue toimii itsenäisesti ja alueen ylläpitäjä voi lisätä toimialueelleen alitoimialueita ja koneita vapaasti. Puumainen rakenne mahdollistaa myös sen, että toimialueilla voi olla saman nimisiä alitoimialueita, esim. on olemassa cs-niminen toimialue sekä Helsingin yliopistolla että Teknillisellä korkeakoululla. Alkuperäisen ARPAnetin aikana jokaisella koneella piti olla yksilöllinen nimi, joten tämä ei olisi ollut mahdollista. DNS:n rakenteen takia kumpikin kone voidaan yksilöidä, koska ne kuuluvat eri toimialueisiin.

Kuvassa 5 esitetään nimipalvelujärjestelmän puumainen rakenne.



Kuva 5: DNS nimipalvelun rakenne

Hierarkkisen rakenteen ansiosta ylemmän tason nimipalvelimien ei tarvitse tietää alemman tason toimialueistaan muuta kuin nimipalvelin. Kun esimerkiksi selainohjelman osoiteriville kirjoitetaan www.metropolia.fi, DNS-asiakasohjelma tarkastaa välimuistin. Jos osoitetta ei ole muistissa, kysytään omalta nimipalvelimelta, esim. ns.example.com. Jos tämä ei tiedä osoitetta, se suorittaa kyselyn juuripalvelimelle. Kysely ohjautuu satunnaisesti yhdelle Internetin kolmestatoista juuripalvelimesta. Tämä tietää vain seuraavan alemman tason eli fi-toimialueen nimipalvelimen osoitteen, jonka se palauttaa. Yksi fi-toimialueen palvelimista palauttaa osoitteen Metropolian nimipalvelimeen, joka tietääkin, että www.metropolia.fi löytyy osoitteesta 195.148.144.15, jonka se palauttaa kysyjälle.

5.1 Berkeley Internet Name Domain

Berkeley Internet Name Domain BIND on tunnetuin ja myös käytetyin Internetin nimipalvelin. Sen versio BIND 8 sisältää osittaisen IPv6-tuen käsittäen AAAA-tietueet ja käänteiset toimialueet IP6.INT ja IP6.ARPA. Versiosta 8.4 lähtien on tuettu myös IPv6-liikennöintiä. BIND 9 on itse asiassa tarjonnut täyttä IPv6-tukea kauemmin, mutta se on hitaampi kuin BIND 8, joten 8.4-versiolla on otettu huomioon raskaasti kuormitetut palvelimet, jotka haluavat kuitenkin tarjota palvelua IPv6-protokollaa käyttäen.

5.2 BINDin konfigurointi

Nimipalvelussa käytetään toimialueesta nimitystä vyöhyke (zone). Vyöhyke sisältää toimialueeseen kuuluvien koneiden osoitteet, aliakset sekä nimipalvelimen ylläpidosta vastaavan henkilön sähköpostiosoitteen. Vyöhyketiedot säilytetään tekstitiedostossa, jonka palvelin lukee käynnistyessään.

```
;
; BIND forward data file for ipv6.example.com
$TTL    14400
@       IN      SOA     ns.ipv6.example.com.  root.ipv6.example.com. (
```

```
                        2006060905     ; serial
                        3600           ; refresh
                        1800           ; retry
                        864000          ; expire
                        14400  )       ; negative cache TTL
;
       IN      NS      ns.ipv6.example.com.
ipv6.example.com. IN      AAAA    2001:db8:0:1::1
ns              IN      AAAA    2001:db8:0:1::3
                IN      A       10.5.1.180
www             IN      AAAA    2001:db8:0:1::2
mail            IN      MX      10 2001:db8:0:1::a
ntp             IN      AAAA    2001:db8 :0:1::4
ssh             IN      CNAME   ipv6.example.com.
router1         IN      AAAA    2001:db8:0:1::11
router2         IN      AAAA    2001:db8:0:1::12
client1001      IN      AAAA    2001:db8:0:1:1001::11
client1002      IN      AAAA    2001:db8:0:1:1002::22
```

Edellä oleva tiedosto sisältää ipv6.example.com-vyöhykkeen tiedot. Tietueet ovat seuraavat:

SOA	Start of Authority, osoittaa valtuutuksen tähän vyöhykkeeseen
NS	Name Server, nimipalvelimen osoite
A	IPv4-osoite
AAAA	IPv6-osoite (quad A)
MX	Mail eXchange, sähköpostipalvelimen prioriteetti ja osoite
CNAME	Canonical Name, aliasnimi

Tämän tiedoston avulla selvitetään koneen IP-osoite sen nimen perusteella. Lisäksi on olemassa erityiset vyöhykkeet, IN-ADDR.ARPA, IP6.ARPA sekä IP6.INT, jonka käyttöä ei suositella uusissa ohjelmistoimplementoinneissa. IPv4-version käänteinen nimiselvitys tapahtuu IN-ADDR.ARPA -vyöhykkeen avulla. Pääosin ohjelmat käyttävät nykyään IP6.ARPAa mutta ARPA-kyselyn epäonnistuessa ne saattavat käyttää IP6.INT-vyöhykettä käänteiseen

nimiselvitykseen. IP6.INT-vyöhykettä ei tosin enää suositella käytettäväksi. Näiden vyöhykkeiden avulla selvitetään nimen perusteella koneen osoite. Niiden muoto on seuraavanlainen.

```
;
; BIND reverse data file for ipv6.example.com
;
$TTL    604800
@       IN      SOA     ipv6.example.com.  root.ipv6.example.com. (
                        2006060901      ; serial
                        604800          ; refresh
                        86400           ; retry
                        2419200         ; expire
                        604800 )        ; negative cache TTL
;
        IN      NS      ns.ipv6.example.com.

$ORIGIN 0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0 IN      PTR     ipv6.example.com.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN      PTR     ns.ipv6.example.com.
$ORIGIN 1.5.10.in-addr.arpa
180                 PTR                 ns.ipv6.example.com.
```

$ORIGIN osoittaa vyöhykkeen, joka esitetään siten, että vyöhykkeen ip-osoitteen verkko-osuus merkitään käännetyssä järjestyksessä. IPv6-osoitteet merkitään käännettyinä puolitavuittain (reverse nibble). Lisäksi on huomattava, että myös nolla-tavut on merkittävä.

6 TIETOTURVA

Internetin käytön ja myös väärinkäytön lisääntyessä tietoturvan merkitys on yhä tärkeämpää. Yritysten tiedosta yhä suurempi osa on saatavilla Internetin kautta. Yritysten toiminta on myös hajaantunut maantieteellisesti laajalle alueelle: toimipisteitä on useassa kaupungissa ja maassa. On välttämätöntä, että työntekijät pääsevät tarpeellisiin tietoihin yrityksen tietojärjestelmässä riippumatta sijainnista. Tällöin kyse on yrityksen intranetistä. Lisäksi yrityk-

set tarjoavat yhteistyökumppaneilleen pääsyn verkkoonsa ja haluttuihin tietoihin niin sanotun extranetin kautta. Kummassakin tapauksessa tarvitaan mahdollisuutta rajoittaa pääsyä tietoon, suojata tieto sekä varmistaa, että tiedon lähde on oikea ja myös estää siirrettävän tiedon väärinkäyttöä. Tähän IPsec eli IP security tarjoaa keinot.

IP security on ryhmä eri protokollia, jotka tarjoavat lähteen tunnistuksen, tiedon koskemattomuuden ja salauksen. AH (Authentication Header) mahdollistaa tunnistuksen ja tiedon koskemattomuuden varmistamisen. ESP:n (Encapsulating Security Protocol) avulla pystytään tieto lisäksi salaamaan. IKE (Internet Key Exchange) mahdollistaa automaattisen salausavainten hallinnan.

Authentication Header

AH:ta käytetään varmistamaan yhteydetön eheys ja tiedon alkuperän tunnistukseen sekä estämään tiedon toisto, joka edellyttää turvayhteyden luomista.. AH-toteutuksen täytyy tukea HMAC-SHA1-96 -algoritmia sekä suosituksena on myös AES-XCBC-MAC-96 [12 s. 5]. Tiedon varmentaminen ja allekirjoitus tapahtuu käyttämällä yhteisesti turvayhteydessä sovittua avainta ja algoritmia.

Encapsulating Security Protocol

ESP-protokolla tarjoaa turvallisuuspalveluita IPv4:lle ja IPv6:lle. Sitä voidaan käyttää yksin tai yhdessä Authentication Headerin kanssa. Sen avulla voidaan suojata kahden yksittäisen tietokoneen, kahden turvallisuusyhdyskäytävän tai tietokoneen ja yhdyskäytävän välinen liikenne. ESP:tä voidaan käyttää kuljetusmuodossa jolloin vain paketin sisältämä data salataan tai tunnelimuodossa jolloin myös otsikkotiedot salataan. Sillä voidaan autentikoida tiedon lähde sekä taata tiedon luottamuksellisuus ja eheys sekä estää tiedon toistaminen.

Security Association

Turvayhteys SA (Security Association) on välttämätön IPsecille. Sekä AH että ESP käyttävät hyväkseen turvayhteyttä. Lisäksi IKE:n tärkein tehtävä on luoda ja ylläpitää turvayhteyttä. Turvayhteys on yksisuuntainen ”yhteys”, joka määrittää yhteydessä käytettävän suojauksen. SA voi sisältää vain yhden protokollan, joko AH:n tai ESP:n. Jos liikenteessä käytetään sekä tunnistusta että salausta, tarvitaan kummallekin protokollalle oma SA:nsa. [11 s. 11-12.]

IPsecia voidaan käyttää kuljetus- tai tunnelimoodissa. Kuljetusmoodissa AH- ja ESP-protokollat suojaavat ylemmän tason protokollia (TCP, UDP), kun taas tunnelimoodissa suojataan IP-paketit, jolloin koko lähetettävä paketti enkapsuloidaan ja siihen lisätään uudet lähde- ja kohdeosoitteet. Kuljetusmoodia käytetään yleensä kahden yksittäisen koneen välillä. Jos SA:n kumpi tahansa päätepiste on turvallisuusyhdyskäytävä, esim. VPN-laite, täytyy kahta poikkeusta lukuun ottamatta käyttää tunnelimoodia.

1. Jos turvallisuusyhdyskäytävä toimii viestin päätepisteenä, esim. SNMP-viestin kohteena.
2. Jos yhdyskäytävä toimii vain välittäjänä kahden verkon välillä. [11 s. 15.]

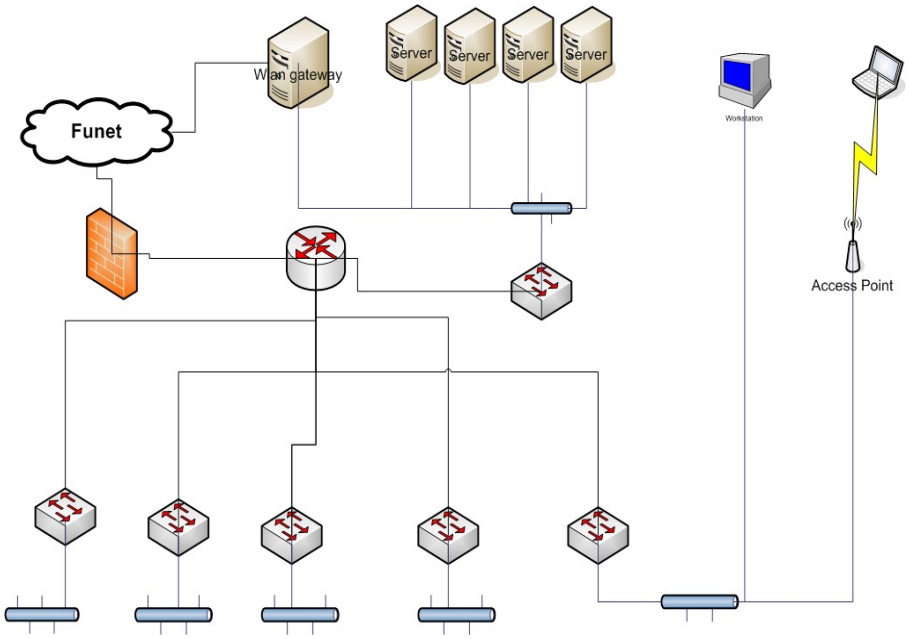
IPv6-protokollaa suunniteltaessa on otettu huomioon tietoturva ja sen määrityksessä vaaditaan, että kaikissa toteutuksissa on implementoitu IPsec. Lisäksi määrityksessä vaaditaan, että IPsec-implementoinnissa käytetään ainakin MD5-algoritmia tunnistukseen ja koskemattomuuden varmistamiseen ja DES-CBC-algoritmia salaukseen. Näillä vähimmäisvaatimuksilla varmistetaan eri toteutusten keskinäinen yhteensopivuus.

7 TAIDETEOLLINEN KORKEAKOULU

7.1 Tuotantoverkko

Taideteollisen korkeakoulun verkko on virtuaalisiin lähiverkkoihin (VLAN) perustuva kytkentäinen verkko. Jokainen hallinnollinen yksikkö on erotettu omaan VLANiinsa, esim. hallinto, graafinen suunnittelu ja Medialaboratorio. Kuvassa 6 esitetään Taideteollisen korkeakoulun verkon rakenne. Koulun

verkon topologia on tähtimäinen (Hub and Spoke). Hierarkia on kaksitasoinen ja tyypillinen pienehkölle organisaatiolle. Se muodostuu kerroskytkimistä (Access Layer) ja reitittävästä runkokytkimestä (Backbone).



Kuva 6: Taideteollisen korkeakoulun verkon topologia

Korkeakoulun verkko on rakennettu Cisco Systemsin laitteilla. Kerroskytkimet ovat pääosin 2950-sarjan ja 3500-sarjan Layer 2 -kytkimiä ilman reititysominaisuuksia. Runkokytkin on 6000-sarjan modulaarinen kytkin, jossa on reititysmoduuli. Kerroskytkimet on kytketty runkoon optisella kuidulla. Kerroskaapelointi on pääosin toteutettu Cat 6 -kaapelilla, ainoastaan vanhin kaapelointi on Cat 5e -kaapelia. Työasemat liittyvät verkkoon 100 Mbps:n nopeudella. Kerroskytkinten ja rungon välinen liikenne kulkee 1000 Mbps:n nopeudella. Samoin yhteys Funetin verkkoon on gigabitin yhteys. Kaikki liikenne lukuun ottamatta langatonta kulkee PIX-palomuurilaitteen kautta. Langaton liikenne ohjataan suoraan palomuurin ulkopuolelle, koska koulu tarjoaa Internet-yhteyttä myös vierailijoille. Lisäksi etätyötä varten tarjotaan turvallisia vpn-yhteyksiä 3000-sarjan VPN-keskittimellä.

Kerroskytkimet toimivat puhtaasti OSI-mallin 2. kerroksella, joten ne eivät käytä ip-osoitteita muuhun kuin hallintaan. Runkokytkimessä ja palomuurissa on tuki IPv6:lle. VPN-laite ei tue uutta ip-versiota.

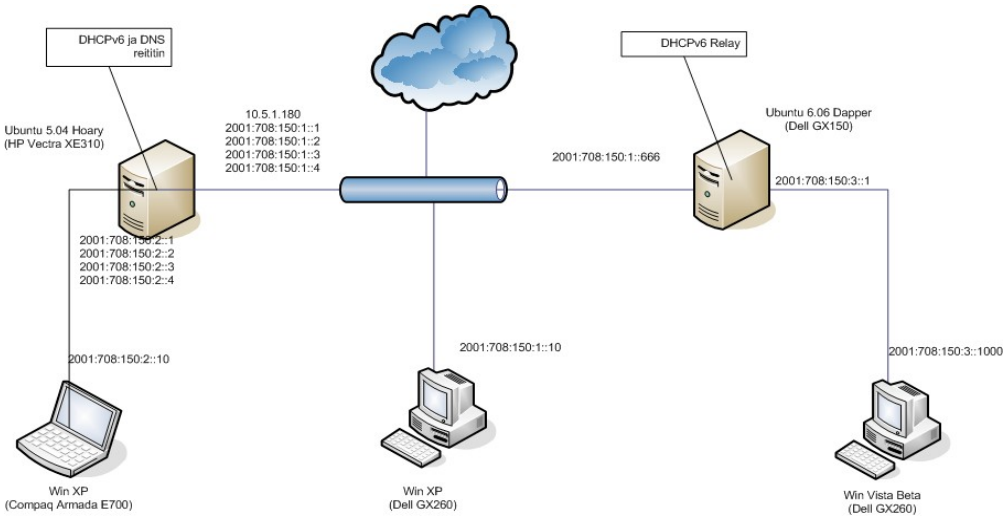
Palvelimet ja työasemat

Korkeakoulun verkossa on palvelimia noin kuusikymmentä. Niiden käyttöjärjestelminä on Novell NetWare, Sun Solaris, Red Hat Enterprise Linux, SUSE LINUX Enterprise Server, Mac OS X Server sekä Windows 2003 Server.

Työasemia verkossa on noin tuhat, joista Maceja on noin 300. Työasemissa käyttöjärjestelminä on Windows XP, jokunen Windows 2000 ja NT, Maceissa pääasiassa OS X sekä muutamassa työasemassa Linux. Näistä käyttöjärjestelmistä ainoastaan Windows NT:lle ei ole saatavissa IPv6-tukea.

7.2 Laboratorioverkko

Laboratorioverkko toteutettiin kolmena aliverkkona. Aliverkossa 1 on työasema sekä DHCPv6- että nimipalvelin ja lisäksi DHCPv6-välityspalvelin. Nimipalvelin ja DHCPv6-palvelin ovat samassa koneessa. Verkon etuliitteenä on 2001:708:150:1::/64. Aliverkko 2 toimii reitittimen Router1 ja työaseman välillä. Etuliitteenä verkossa käytetään 2001:708:150:2::/64. Aliverkko kolme on reitittimen Router2 ja työaseman välillä. Verkon etuliitteenä on 2001:708:150:3::/64. Router1 voi toimia myös yhdyskäytävänä tuotantoverkkoon. Aliverkot on kytketty toisiinsa kytkimellä tai keskittimellä. Kuvassa 7 esitetään suunnitellun laboratorioverkon looginen topologia.



Kuva 7: Laboratorioverkon topologia

Laitteisto

Käytössä oli Cisco 2950-48G -kytkin, johon kytkettiin aliverkot kaksi ja kolme. Aliverkko yksi oli kytketty tuotantoverkkoon Kaikki aliverkot kuuluivat omiin VLANeihinsa. Tietokoneet olivat pääasiassa käytöstä poistuvia PC-koneita. Koneiden käyttöjärjestelminä laboratoriossa käytettiin työasemissa Windows XP Professional SP2:ta ja yhdessä oli Windows Vista Beta. Windows Vistan kanssa samaan koneeseen oli asennettu myös SUSE Linux 10, jota myös testattiin hieman. Reitittimissä oli käytössä Ubuntu Linuxin kaksi versiota, reitittimessä yksi, nimipalvelussa *Ubuntu*, Hoary Hedgehog 5.04 ja reitittimessä kaksi, nimipalvelussa *Dapper*, Dapper Drake 6.06.

Ohjelmistot

Työasemissa oli käytössä Windows XP Professional, joihin oli asennettu kaikki viimeisimmät päivitykset ja yhdessä asemassa oli Windows Vista Beta. Windows XP:ssä on mahdollisuus käyttää IPv6-protokollaa. Tämä on tosin vielä testiasteella eikä sisällä kaikkia ominaisuuksia. Windows XP:ssä oli käytössä GPL-lisenssillä jaettava DHCPv6-asiakasohjelma Dibbler 0.41, koska Microsoftilla ei vielä tässä versiossa ollut asiakasohjelmaa. Windows Vis-

ta käyttää oletusarvoisesti kumpaakin versiota IP-protokollasta. Siinä on myös DHCPv6-asiakasohjelma natiivina.

DHCPv6-palvelimena ja välityspalvelimena käytettiin samoin dibbler 0.4.1:ä. Näiden palvelimien konfiguraatiot ovat liitteissä 1 ja 2. Nimipalvelimena käytettiin Internet Systems Consortiumin BIND9.2.4:ää.

8 TULOKSET JA YHTEENVETO

8.1 Tulokset

Testeissä keskityttiin tarkastelemaan eri konfigurointivaihtoehtojen toimintaa ja niiden helppoutta pääasiassa hallinnan kannalta. Lisäksi yhteyksien toimintaa testattiin ping- ja traceroute-komennoilla.

Autokonfiguraatio ilman DHCP-palvelinta

Tässä testissä ei ollut käytössä DHCP-palvelinta vaan koneet määrittivät osoitteensa automaattisesti. Reitittiminä toimivissa Linux-koneissa oli käynnissä radvd-ohjelma, Router Advertisement Daemon. Tämä ohjelma lähettää verkkoon Router Advertisement -paketteja, joiden sisältönä on tieto reitittimen osoitteesta sekä osoitteenmuodostuksessa käytettävästä etuliitteestä. Ubuntu ”Hoary Hedgehog” lähetti Router Advertisement -paketteja aliverkkoihin 2001:708:150:1:: ja 2001:708:150:2:: ja Dapper Drake kolmanteen aliverkkoon 2001:708:150:3::.

Kaikki koneet muodostivat itselleen link local -osoitteen ja globaalin osoitteen käyttäen reitittimen mainostamaa etuliitettä. Käytännössä tästä konfigurointitavasta ei juurikaan ole hyötyä, koska liikennöinti itse konfiguroidun IPv6-osoitteen perusteella on jokseenkin mahdotonta. Yhteydet toimivat mutta käyttö on erittäin hankalaa, koska kaikkien laitteiden ip-osoitteet pitäisi muistaa ulkoa.

Autokonfiguraatio DHCP-palvelimen avulla

Toisessa testissä Router Advertisement Daemonin konfiguraatiotiedostoon lisättiin rivi ”*OtherConfigFlag on*”, jonka perusteella autokonfiguraation suorittava tietokone osaa pyytää muita tietoja DHCP-palvelimelta, joten tämä edellyttää koneelta toimivaa DHCP-asiakasohjelmaa. Testissä asiakkaat saivat DHCP-palvelimelta nimipalvelimen osoitteen. Tämä malli on jo huomattavasti käyttökelpoisempi ja sopii normaaliin lähiverkkokäyttöön. Tätä konfigurointitapaa käytettäessä pystytään käyttämään tietokoneista nimiä.

Linuxeihin on tarjolla ainakin kaksi DHCPv6-asiakas- ja -palvelinohjelmistoa, alkujaan KAME-projektin osana kehitetty *WIDE-dhcpv6* sekä alkujaan Gdanskin teknillisen yliopiston lopputyönä alkanut *dibbler*. Wide-dhcpv6 on saatavana alustariippumattomana lähdekoodina ja se toimii ainakin unix-käyttöjärjestelmissä eli unixit, eri BSD:t sekä linux ja Mac OSX. Dibbler on saatavissa lähdekoodin lisäksi valmiina binäärinä Linux x86 -alustalle sekä portattuna Windows XP:lle ja Windows 2000:lle. Linuxit toimivat hyvin IPv6-verkossa, mutta haittana on se, että hyvin harvassa jakelupaketissa on valmiiksi tarvittavat ohjelmat uuden protokollan käyttämiseksi. Käyttäjän tai ylläpitäjän pitäisi asentaa kaikkiin työasemiin DHCPv6-asiakasohjelma, jotta käyttö olisi sujuvaa ja tästä aiheutuisi suuri ylimääräinen työ. Kokeilluista jakeluista ainoastaan Ubuntu Dapperissa oli jakeluun kuuluvana wide-dhcpv6-asiakasohjelma. Dibbler on saatavana Red Hatin rpm-pakettina, debianin apt-pakettina sekä Gentoon pakettina. Muihin ohjelma täytyy kääntää lähdekoodista.

Windows XP ei hallitse vielä yhtä hyvin uutta protokollaa, tosin sen IPv6-toteutuksen ohjeistuksessa mainitaankin, että sitä ei ole tarkoitettu tuotantokäyttöön vaan ainoastaan testaukseen. Windows XP tukee kuitenkin kohtalaisen hyvin IPv6:tta. Esimerkiksi Internet Explorer osaa käyttää IPv6-osoitteita ja ymmärtää myös, jos nimipalvelin palauttaa IPv6-osoitteen. Komentorivi (command prompt) osaa käyttää IPv6-osoitteita, jos ne kirjoitetaan riville, esim. ping 2001:708:150:1::1 mutta ei silloin, jos yritetään käyttää nimiä. Tämä johtuu siitä, että Windows XP:n DNS-asiakasohjelma ei osaa käyttää nimipalvelupyynnöissä IPv6-protokollaa. Edellä mainitut komennot toimivat, jos nimipalvelin käyttää IPv4-osoitetta.

Windows Vista vaikuttaisi beta-version perusteella tukevan hyvin myös IPv6-protokollaa. DHCP-asiakasohjelma osaa käyttää palvelimen tarjoaman tiedon ja luotuaan itselleen IPv6-osoitteen rekisteröi nimipalvelimien osoitteet.

Tilallinen autokonfiguraatio

Kolmantena testinä oli tilallinen konfiguraatio. Tässä DHCPv6-palvelin jakoi osoitteet asiakkaille. Tietokoneen käynnistyessä DHCP-asiakas pyytää palvelimelta itselleen IP-osoitteen ja yhdistää sen verkkosovittimeen. Sammutettaessa kone DHCP-asiakas lähettää vapautuspyynnön palvelimelle, jonka jälkeen sama osoite voidaan käyttää uudelleen. Kaikki asiakkaat ottivat käyttöön palvelimelta saamansa osoitteen ensisijaisena osoitteena. Tämän lisäksi ne määrittivät autokonfiguraatiolla itselleen toisen osoitteen reitittimen mainostaman etuliitteen perusteella.

Kun DHCP-palvelimen jakamille osoitteille ei määritelty erityisesti elinaikaa, osoitteiden elinaika on oletuksena ikuinen. Kun osoitteiden elinajaksi määriteltiin kohtuullisen lyhyt aika, osoittautui, että DHCP-asiakas ei vapauttanut osoitteita. Tämä ilmeni, kun käytössä oli pienehkö osoiteavaruus jokaiselle aliverkolle. Osoitteen muuttuessa vanhentuneeksi asiakas pyysi palvelimelta uuden osoitteen. Vanha osoite jäi kuitenkin varatuksi. Tämän tapahduttua tarpeeksi monta kertaa palvelimelta loppuivat jaettavat osoitteet, jonka jälkeen asiakaskoneiden liikennöinti loppui, koska niillä ei ollut voimassa olevaa osoitetta.

Testien perusteella ei Taideteollisen korkeakoulun siirtymistä IPv6-protokollan käyttöön voida pitää vielä ajankohtaisena, koska suurimmassa osassa koulun työasemia on käyttöjärjestelmänä Windows XP. Siirtyminen aiheuttaisi erittäin suuren ylimääräisen työn ylläpidolle tarpeellisten ohjelmien asentamisessa eikä IPv6 kuitenkaan tuota sellaista hyötyä, että se voitaisiin katsoa kannattavaksi. Uuden protokollan käyttöönotto kannattaa ottaa harkittavaksi, kun työasemien käyttöjärjestelmien päivitys Windows Vistaan tulee ajankohtaiseksi. Kaikki tämä pätee myös Maceihin, joiden kohdalla päivitys

tullee ajankohtaiseksi myös seuraavan suuremman käyttöjärjestelmäpäivityksen yhteydessä.

Tällä hetkellä voitaisiin harkita joidenkin palveluiden tarjoamista myös uutta protokollaa käyttäen. Senkin edut lienevät melko minimaaliset, koska useat julkiset palvelut, esimerkiksi intranet ja web-palvelut on ulkoistettu eikä palveluntarjoaja välttämättä tue IPv6-protokollaa. Mahdolliset tarjottavat palvelut olisivat oikeastaan opiskelijoiden ja henkilökunnan omat sivustot sekä etäyhteydet eräille palvelimille ssh:ta käyttäen. Lisäksi osassa palvelimia IPv6-palveluiden tarjoaminen saattaisi aiheuttaa ylimääräisiä ohjelmistopäivityksiä, jotka eivät muuten olisi ajankohtaisia.

VPN-yhteydet jäisivät kuitenkin vanhan protokollan varaan, koska käytössä oleva VPN-laitteisto ei tue uutta. Toisena vaihtoehtona olisi IPv6:n IPsecin käyttäminen. Tämä taas edellyttäisi, että käyttäjillä olisi käytössä IPv6, joten käytännössä tämä ei ole mikään vaihtoehto.

8.2 Yhteenveto

Tämä työ osoitti, että IPv6 on toimiva protokolla ja sinänsä tuotantokelpoinen. Tuotantokäyttöön ottamista hankaloittaa tarvittavien palvelinohjelmistojen puutteet sekä käyttöjärjestelmien vaillinaiset ominaisuudet. Kotikäytössä ja hyvin pienissä verkoissa protokollan käyttöä voi harkita mutta vähänkään suuremmissa organisaatioissa käyttöönotto kannattanee jättää myöhemmäksi.

IPv6 ja siihen liittyvät protokollat tarjoavat hyvät edellytykset verkon laajentumiselle ja hallinnalle. Protokollan osoitteisto on hyvin hierarkkinen, jonka vuoksi reititys tapahtuu tehokkaasti ja nopeasti runkoverkossa. Käyttöä helpottaa myös määritelty autokonfiguraatio, jonka avulla tietokone määrittää itselleen yksilöllisen ip-osoitteen.

Tällä hetkellä suurin hidastava tekijä IPv6:een siirtymisessä on vähäinen ja epätäydellinen protokollien toteutus. Toteutuksissa on keskitytty vain pakollisiin, kuten IPsec, ja tärkeimpiin ominaisuuksiin, joita ilman on käytännössä mahdotonta hyödyntää ohjelmaa. Tähän on tosin koko ajan tulossa parannus-

ta. Palvelinohjelmia kehitetään ja niihin lisätään puuttuvia ominaisuuksia sekä virheitä korjataan.

Toinen tärkeä hidastava tekijä on palveluntarjoajien haluttomuus tarjota IPv6-palveluita. Osittain tämä haluttomuus on ymmärrettävää, koska useille se merkitsisi suuria investointeja laitteistoon, koska vanhat laitteet eivät ymmärrä IPv6-protokollaa.

Työasemien osalta siirtymistä hankaloittaa myös se, että nykyään jo monet Internetin sekä myös intranetin palvelut edellyttävät nimipalvelimille myös reverse-tietuetta koneille. IPv4:ää käytettäessä tämä on helppo toteuttaa käyttämällä pieniä aliverkkoja ja generoimalla tiedot automaattisesti tai käyttämällä nimipalvelimen dynaamista päivitystä (DDNS). Tätä käytettäessä DHCP-palvelin päivittää muuttuneet tiedot nimipalvelimelle. Tätä ominaisuutta joudutaan vielä odottamaan DHCPv6-palvelimiin.

Protokollaan siirtymistä tai ainakin sen käyttöönottoa IPv4:n rinnalle kannattaa harkita ja aloittaa myös suunnittelu, jolloin siirtyminen pystytään toteuttamaan mahdollisimman helposti ja sujuvasti. Etenkin muutaman vuoden kuluessa, kun VoIP-puhelut lisääntyvät ja myös muita Internetin palveluita käytetään yhä enemmän mobiilipuhelimissa, tulee lisääntyvä tarve julkisille ip-osoitteille ja tällöin kauan uhkakuvana ollut osoitteiden loppuminen saattaa muuttua todellisuudeksi.

VIITELUETTELO

[1] Comer, Douglas E, *TCP/IP*. Helsinki: IT Press. 2002.

[2] Huitema, Christian, *IPv6 – the New Internet Protocol.* Upper Saddle River, NJ: Prentice Hall. 2. painos 1998(1997).

[3] Postel, J, *Internet Protocol – DARPA Internet Program Protocol Specification.* IETF Request for Comments 791. [verkkodokumentti] 9.1981 [viitattu 21.5.2006] Saatavissa: ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc791.txt.pdf.

[4] *6net – An IPv6 Deployment Guide*, toim. Dunmore, Martin. The 6NET Consortium. 2005.

[5] Murphy, Niall Richard – Malone, David, *IPv6 Network Administration*. Sebastopol, CA: O'Reilly Media. 2005.

[6] Kozierok, Charles M, *The TCP/IP Guide – IPv6 Addressing*. [verkkodokumentti] 20.9.2005 [viitattu 2.8.2006] Saatavissa: http://www.tcpipguide.com/free/t_IPv6AddressSizeandAddressSpace-2.htm.

[7] Deering, S – Hinden, R, *Internet Protocol, Version 6 (IPv6) Specification.* IETF Request for Comments 2460. [verkkodokumentti] 12.1998 [viitattu 21.5.2006] Saatavissa: ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc2460.txt.pdf.

[8] Hinden, R – Deering, S, *IP Version 6 Addressing Architecture.* IETF Request for Comments 4291 [verkkodokumentti] 2.2006 [viitattu 21.5.2006] Saatavissa: ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc4291.txt.pdf.

[9] Huitema, C – Carpenter, B, *Deprecating Site Local Addresses,* IETF Request for Comments 3879 [verkkodokumentti] 9.2004 [viitattu 21.5.2006] Saatavissa: ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc3879.txt.pdf.

[10] Albitz, Paul – Liu, Cricket, *DNS and BIND.* Sebastopol, CA: O'Reilly & Associates. Neljäs painos 2001(1992).

[11] Kent, S – Seo, K, *Security Architecture for the Internet Protocol.* IETF Request for Comments 4301 [verkkodokumentti] 12.2005 [viitattu 19.6.2006] Saatavissa: ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc4301.txt.pdf.

[12] Kent, S, *IP Encapsulating Security Payload (ESP)*, IETF Request for Comments 4303 [verkkodokumentti] 12.2005 [viitattu 19.6.2006] Saatavissa: ftp://ftp.rfc-editor.org/in-notes/pdfrfc/rfc4303.txt.pdf.

[13] Loshin, Pete, *IPv6: Theory, Protocol and Practice.* San Francisco, CA: Morgan Kaufmann Publishers. Toinen painos 2004(1999, IPv6 clearly Explained).

DHCPv6-palvelimen konfiguraatio

```
# server.conf

log-level 7
log-mode short
#stateless

iface "eth0" {
# clients should renew every 10 minutes
 T1 600
 T2 2000
 prefered-lifetime 3600
 valid-lifetime 7200
 option dns-server 2001:708:150:1::3
 option domain ipv6.uiah.fi
 class {
    pool 2001:708:150:1::10-2001:708:150:1::10
 }
}

iface "eth1" {
 T1 600
 T2 2000
 prefered-lifetime 3600
 valid-lifetime 7200
 option dns-server 2001:708:150:1::3
 option domain ipv6.uiah.fi
 class {
  pool 2001:708:150:2::10-2001:708:150:2::10
 }
}
iface relay1 {
 relay eth0
 interface-id 1000
 T1 600
 T2 2000
 option dns-server 2001:708:150:1::3
 option domain ipv6.uiah.fi
 class {
   pool 2001:708:150:3::10-2001:708:150:3::10
 }
}
```

DHCPv6-releen konfiguraatio

```
# relay.conf

log-level 8
log-mode short

# messages will be forwarded on this interface using multicast
iface eth0 {
  interface-id 100
  server multicast yes                  // relay messages on this inter-
face to ff05::1:3
#  server unicast 3ffe:8320:3:210::1:1  // relay messages on this inter-
face to this global address
}


# client can send messages to multicast
# (or specific link-local addr) on this link
iface eth1 {
  client multicast yes                    // bind ff02::1:2
#  client unicast fe80::2042:34ff:fe17:1353 // bind this address
  interface-id 1000
}
```