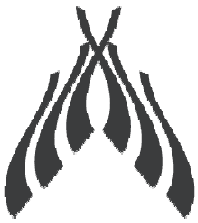
OPINNÄYTETYÖ

ARTTU SALONEN 2011

IPv6:N KÄYTTÖÖNOTTO PK-YRITYKSESSÄ



Rovaniemen
ammattikorkeakoulu
University of Applied Sciences

TIETOTEKNIIKAN KOULUTUSOHJELMA

Rovaniemen
ammattikorkeakoulu
University of Applied Sciences

ROVANIEMEN AMMATTIKORKEAKOULU

TEKNIIKKA JA LIIKENNE

Tietotekniikan koulutusohjelma

Opinnäytetyö

IPv6:N KÄYTTÖÖNOTTO PK-YRITYKSESSÄ

Arttu Salonen

2011

Ohjaaja Kenneth Karlsson

Rovaniemen ammattikorkeakoulu
University of Applied Sciences

Tekniikka ja liikenne
Tietotekniikan koulutusohjelma

Opinnäytetyön tiivistelmä

Tekijä	Arttu Salonen	Vuosi	2011
Toimeksiantaja			
Työn nimi	IPv6:n käyttöönotto PK-yrityksessä		
Sivu- ja liitemäärä	73		

Tämän opinnäytetyön tarkoituksena on selvittää, kuinka IPv6-yhteydet otetaan käyttöön PK-yrityksessä. Työssä selvitetään minkälaiset vaatimukset IPv6 asettaa laitteistolle ja minkälaisia käytännön asioita yrityksen täytyy huomioida IPv6:n käyttöönotossa. Lisäksi työssä on laboratoriosimulaation avulla havainnollistettu eri käyttöjärjestelmien tukea IPv6:lle ja käyttöönottoon liittyviä reititin- ja osoitekonfiguraatioita.

Käyttöönoton lisäksi opinnäytetyössä esitellään IPv6-protokollan rakenne ja ominaisuudet sekä esitellään syyt, miksi uusi protokollaversio on tarpeellinen. Työssä on myös selvitetty, miten IPv6:een siirtyminen on Suomessa ja maailmalla edennyt.

Opinnäytetyössä on myös esitelty Internetin kehityshistoriaa, tietoliikenteen ja TCP/IP-protokollapinon teoreettista taustaa sekä kaksi tärkeää protokollaa: TCP ja IPv4.

Työn tutkimusaineistona on käytetty aiheeseen liittyvää kirjallisuutta sekä Internet-aineistoa. Lisäksi Käyttöönotto-osiota varten on suoritettu kyselyjä kahdelle suurelle Internet-operaattorille Suomessa.

Tämän opinnäytetyön pohjalta voidaan sanoa, että IPv6 on kokonaisvaltainen ja pitkäkestoinen ratkaisu, jolla voidaan suurelta osin korjata vanhaan IPv4-versioon liittyvät ongelmat. IPv6 tarjoaa käyttöön uusia ominaisuuksia, mutta on samalla dynaaminen ja kevyt käyttää.

IPv6:een siirtyminen on tähän mennessä sujunut hitaasti vaikka toimia maailmanlaajuisen siirtymisen eteen on tehty ja ollaan tekemässä. Siirtyminen on selvästi myöhässä ja vanhan version rajoitukset ovat tulossa vastaan nopealla tahdilla. Siirtymiseen liittyvien ongelmien ratkaisu vaatii sekä resurssien lisäämistä osaavien työntekijöiden koulutukseen että rahallista panostusta.

PK-yrityksen näkökulmasta siirtyminen IPv6:een voidaan laitteiston puolesta hoitaa helposti. Suurimmaksi ongelmaksi muodostuukin operaattoreiden IPv6-yhteyksien tarjonnan vähäisyys sekä osaavan henkilökunnan puute. Siirtymisessä tullaan myös noudattamaan useita erilaisia tapoja, jotka saattavat vaihdella operaattorista toiseen. PK-yritysten siirtymistä helpottaa ajoissa suoritettu IPv6-käyttöönotto, jotta saadaan aikaa testauksella ja ongelmakohtien selvittämiselle.

Asiasanat: IPv6, Internet, IPv4, TCP/IP, tietoliikenne

Rovaniemen ammattikorkeakoulu
University of Applied Sciences

School of Technology
Information Technology Programme

Abstract of Thesis

Author Arttu Salonen Year 2011

Commissioned by
Subject of thesis Deploying IPv6 in a Small Business Network
Number of pages 73

The aim of this thesis was to find out how IPv6 is deployed in a small business network. The goal was to find out what hardware and operating system requirements IPv6 sets and what other issues have to be considered when implementing IPv6 in a small business. Network laboratory simulation was included to demonstrate the router and address configurations.

In addition to the deployment guidelines the thesis includes an inclusive description of IPv6. The description includes the development history, the datagram structure, the new features, the reasons why IPv6 is deployed and the information on the state of the deployment in Finland and globally.

The material of this thesis consists of literature on the subject and Internet material. Inquiries to two major Internet service providers in Finland were made to acquire additional information.

Based on this thesis IPv6 can be considered as a well planned update to the older IP version. IPv6 is a comprehensive solution to the problems of the IPv4 and it also provides new features that make it a long lasting standard in network communications.

The global deployment of IPv6 has not developed as fast as it should have. The solutions to the problems in IPv6 deployment demand more resources on education as well as financial investments.

The most difficult problem in a small business deployment is the lack of supply of the IPv6 connections from the Internet service providers in Finland. Despite the lack of support from the ISPs the deployment of IPv6 in small businesses should be started in time. Thus, there would be time for finding the problem areas and testing the connections.

Key words IPv6, Internet, IPv4, TCP/IP

SISÄLTÖ

TAULUKKOLUETTELO

KUVIOLUETTELO

LYHENNELUETTELO

ACK-bitti	*Acknowledgement*-bitti on yksi TCP-lipuista, jota käytetään muun muassa virtuaalisen TCP-yhteyden muodostamisessa.
ANSNET	*Advanced Networks and Services* oli tietoverkko, jonka oli määrä toimia Internetin selkärankana.
ARPA	*Advanced Research Projects Agency* oli Yhdysvaltain asevoimien tutkimusorganisaatio, jonka nimi vaihtui 1972 *Defense Advanced Research Projects Agency*:ksi. Organisaatio vastasi ARPANET:in kehittämisestä.
ARPANET	*Advanced Research Projects Agency Network* oli Yhdysvalloissa kehitetty TCP/IP-protokollaa käyttänyt tietoverkko, jonka pohjalta kehitettiin Internet.
CATNIP	*Common Architecture for Next Generation IP* oli yksi ratkaisuesityksistä IPv4:n korvaavaksi protokollaksi, jonka pohjalta IPv6 myöhemmin kehitettiin.
CIDR	*Classless Inter-Domain Routing* tarkoittaa luokatonta reititystä, jonka avulla IPv4-osoiteluokkia on mahdollista jakaa aliverkkoihin.
CSNET	*Computer Science Network* oli tieteellisten instituutioiden käyttämä tietoverkko, jota voidaan pitää Internetin esiasteena.
DCA	*Defence Communication Agency* on USA:n puolustusvoimien tiedusteluvirasto.
DHCP	*Dynamic Host Configuration Protocol* on verkkoprotokolla, jonka tehtävänä on jakaa IP-osoitteita niitä tarvitseville laitteille.
DNS	*Domain Name System* on nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi.
EIGRP	*Enhanced Interior Gateway Routing Protocol* on CISCOn suljettu reititysprotokolla.
ESP	*Encapsulating Security Payload* on IPsecin käyttämä protokolla, joka mahdollistaa salakirjoitusominaisuuksien käyttöönoton.
FTP	*File Transfer Protocol* on TCP/IP-protokollapinoon kuuluva tiedonsiirtoprotokolla, jonka avulla on mahdollista kopioida tiedostoja isäntälaitteesta toiseen verkon yli.
HTTP	*Hypertext Transfer Protocol* on TCP/IP-protokollapinoon kuuluva protokolla, jota selaimet ja palvelimet käyttävät tiedonsiirtoon.

IAB	*Internet Architecture Board* on yksi Internetin teknisestä kehityksestä vastaavista organisaatioista.
IANA	*Internet Assigned Numbers Authority* on organisaatio, joka vastaa IP-osoitteiden jakamisesta.
IETF	*The Internet Engineering Task Force* on Internetiin liittyvien protokollien standardisoimisesta vastaava organisaatio.
IGP	*Interior Gateway Protocol* on autonomisen järjestelmän sisällä käytettävä reititysprotokolla.
IKE	*Internet Key Exchange* on IPsec:in käyttämä protokolla, jonka avulla voidaan turvallisesti välittää salausavaimia.
IP	*Internet Protocol* on yksi TCP/IP-protokollapinon tärkeimpiä protokollia. IP toimii Internet-kerroksella ja vastaa IP-pakettien reitityksestä.
IPsec	*IP Security Architecture* on protokollakokoelma, joka mahdollistaa tietoturvaominaisuuksien käyttöönoton.
IPv4	*Internet Protocol version 4* on nykyisin eniten käytetty IP-protokollan versio, joka on vanhentumassa.
IPv6	*Internet Protocol version 6* on uusin IP-protokollan versio, jonka on määrä korvata IPv4.
NAT	*Network Address Translation* on osoitteenmuunnostekniikka, jolla säästetään julkiseen liikennöintiin käytettäviä IP-osoitteita. Menetelmä mahdollistaa yksityisten IP-osoitteiden käyttämisen sisäverkoissa.
NSFNET	*National Science Foundation Network* oli tietoverkko, jota voidaan pitää yhtenä Internetin esiasteena.
OSI	*Open Systems Interconnection Reference Model* on ISO-organisaation kehittämä verkkoliikennemalli, jossa verkkoliikenne on jaettu seitsemään kerrokseen. Malli on nykyisellään käytössä vain teoreettisena viitekehyksenä.
PAT	*Port Address Translation* on osoitteenmuunnostekniikka, jolla säästetään julkiseen liikennöintiin käytettäviä IP-osoitteita. Menetelmä käyttää yhteyksien tunnistamiseen porttinumeroita ja mahdollistaa useamman yhteysprosessin saman IP-osoitteen alla.
RFC	*Request for Comments* on sarja IETF:n julkaisemia Internetin toimintaan liittyviä standardeja.

RIPE *Réseaux IP Européens* on avoin foorumi, joka keskittyy Internetin kehittämiseen. Foorumi toimii yhteistyössä RIPE NCC:n kanssa mutta ei tuota standardeja tai osallistu IP-osoitteiden jakamiseen.

RIPE NCC *Réseaux IP Européens Network Coordination Centre* on Euroopan, Lähi-idän ja Keski-Aasian IP-osoitteiden jakamisesta vastaava organisaatio.

RIPng *Routing Information Protocol next generation* on IPv6-tuettu versio RIP-protokollasta.

RIR *Regional Internet Registry* on alueellisesta IP-osoitteiden jakamisesta vastaava organisaatio.

SIPP *Simple Internet Protocol Plus* oli yksi ratkaisuesityksistä IPv4:n korvaavaksi protokollaksi, jonka pohjalta IPv6 myöhemmin kehitettiin.

SYN-bitti Synchronisation-bitti on yksi TCP-lipuista, jota käytetään muun muassa TCP-yhteyden muodostamisessa.

TCP *Transmission Control Protocol* on yksi TCP/IP-protokollapinon tärkeimpiä protokollia. Protokolla huolehtii muun muassa luotettavasta tiedonsiirrosta sekä virtuaalisen yhteyden muodostamisesta päätelaitteiden välillä.

TCP/IP-malli *Transmission Control Protocol / Internet Protocol*-malli on protokollakokoelma, joka on nykyisin tietotoliikenteessä käytetty standardi.

TOS *Type Of Service*

UDP *User Datagram Protocol* on TCP/IP-protokollapinoon kuuluva protokolla, joka toimii Kuljetuskerroksella.

VLSM *Variable-Length Subnet Masking* on aliverkotustapa, jossa aliverkko-osuus voidaan joustavasti määritellä.

WWW *World Wide Web* on Internet-verkossa toimiva hypertekstijärjestelmä, jossa selaimen avulla voidaan näyttää palvelimelta ladattuja hypertekstidokumentteja.

1 JOHDANTO

Nykyisen globaalin tietoyhteiskunnan kulmakivenä voidaan perustellusti pitää lukuisista toistensa kanssa kommunikoivista tietoverkoista koostuvaa Internetiä. Internet mahdollistaa rajattoman tiedonsiirron, globaalin palvelutarjonnan ja nykyisellään myös globaalin kommunikaation mobiilien tietoliikenneyhteyksien avulla. Internetin käyttäjämäärät ovat kasvaneet räjähdysmäisesti erityisesti mobiililaitteiden kautta, mutta myös siksi, että esimerkiksi Aasiassa on yhä enemmän loppukäyttäjiä. Käyttäjämäärät ovat suurin syy siihen, miksi Internetin perustana käytettävä teknologia on vanhentumassa. Erityisesti nykyisellään käytössä oleva IPv4-protokolla täytyy tulevaisuudessa korvata, koska sen tarjoama IP-osoiteavaruus on täyttymässä. Kun osoiteavaruus täyttyy, ei IP-osoitteita ja tätä myöten yhteyksiä voida enää tarjota uusille asiakkaille.

IPv4-osoiteavaruuden täyttymistä on pyritty hidastamaan erilaisin keinoin muun muassa käyttämällä NAT-osoitteenmuunnosta ja kehittämällä protokollan aliverkotusta. Nämä ratkaisut ovat kuitenkin parhaimmillaankin vain hidastavia toimenpiteitä. IPv6 on uusi protokolla, jonka tavoitteena on ratkaista vanhan protokollaversion ongelmat sekä tarjota käyttöön myös uusia ominaisuuksia. Uuden protokollan on määrä olla kestävä ja pitkäikäinen ratkaisu, joten sen kehittämisessä on huomioitu myös tulevaisuuden kasvavat tietoliikennetarpeet. IPv6:sta voidaan yleisesti sanoa, että se on joustavampi ja monipuolisempi protokolla kuin edeltäjänsä ja sillä on kyetty myös ratkaisemaan erityisesti osoitteistukseen liittyvät ongelmat. Protokolla sisältää myös tärkeitä tietoturvaominaisuuksia, jotka entisestä protokollasta puuttuvat.

Tämän opinnäytetyön tavoitteena on selvittää, kuinka IPv6-yhteydet otetaan käyttöön PK-yrityksen mittakaavassa. Opinnäytetyöni kuvaa myös yleisesti tietoliikenteen toimintaa ja IPv6:ta. Työn teoreettinen osuus keskittyy esittelemään tietoliikenteen yleistä rakennetta, TCP/IP-protokollapinoa ja IPv6:ta. Käytännönosuuteen keskittyvä osa puolestaan kuvaa IPv6:n käyttöönottoon liittyvät asiat ja käytännön toimet sekä havainnollistaa simulaation avulla käyttöönoton vaiheita, kongifuraatioita ja ongelmakohtia.

Työn toinen luku käsittelee Internetin historiaa ja yleistä teoreettista taustaa. Luku esittelee ne rakennusosat, joista tietoliikenne rakentuu ja antaa lukijalle käsityksen tietoliikenteen toimintaan liittyvistä peruskäsitteistä ja ilmiöistä.

Kolmas luku esittelee TCP/IP-protokollapinon teoreettista taustaa. Lisäksi luvussa on kuvattu protokollapinon kaksi tärkeintä protokollaa TCP ja IP. TCP-protokollasta esitellään kehysrakenne ja ominaisuudet. IPv4-protokollasta esitellään rakenteen ja ominaisuuksien lisäksi myös protokollaan liittyvät ongelmat.

Neljäs luku keskittyy uuden IPv6-protokollan kehityshistorian, ominaisuuksien, kehysrakenteen, osoitteistuksen ja tietoturvaominaisuuksien esittelyyn. Luku antaa kuvauksen IPv6:sta ja sen toiminnasta sekä vertailee vanhaa ja uutta protokollaversiota toisiinsa.

Viidennessä luvussa selvitetään IPv6:een siirtymisen tilannetta Suomessa ja maailmalla. Luvussa kerrotaan, minkälainen käyttöönoton tilanne on tällä hetkellä ja mitä toimia siirtymisen edistämiseksi on tehty. Luvussa tuodaan myös esille siirtymisen ongelmakohdat ja haasteet.

Kuudennessa luvussa keskitytään IPv6:n käyttöönottoon PK-yrityksessä ja kerrotaan, minkälaisia asioita yrityksessä on otettava huomioon, kun IPv6 otetaan käyttöön. Luku sisältää myös selvityksen suomalaisten Internet-palveluntarjoajien kyvystä tarjota IPv6-yhteyksiä tällä hetkellä. Lisäksi luku sisältää reititysesimerkin, jossa simuloidaan PK-yrityksen mittakaavassa tapahtuvaa IPv6-käyttöönottoa. Simulointi havainnollistaa myös käyttöjärjestelmien ja laitteiden tukea IPv6:lle ja mahdollisia ongelmia.

Yhteenveto-osiossa kerrataan työn tärkeimmät osat sekä kerrotaan, kuinka hyvin työ onnistui täyttämään tarkoituksensa ja mitkä ovat tärkeimmät työstä tehtävät johtopäätökset. Luvussa kuvataan myös työn tekemiseen liittyvää prosessia ja esitetään mahdollisia jatkotutkimusaiheita.

2 PERUSKÄSITTEITÄ

2.1 Internet

TCP/IP-protokollaperheen käyttötarkoituksen, luonteen ja ongelmien ymmärtämiseksi on syytä selventää sitä kokonaisuutta, jonka rakenneosina ovat muun muassa World Wide Web (WWW), muut tietoverkot, reitittimet, päätelaitteet sekä tiedonsiirrossa käytettävät protokollat. Nykyinen globaalitietoyhteiskuntamme perustuu pitkälti tietoverkkojen tarjoaman vapaan ja nopean tiedonkulun tuomiin mahdollisuuksiin. Erilaisten laitteiden ja verkkojen liittyminen toisiinsa on saanut aikaan nopeasti kasvavan palvelutarjonnan sekä kasvattanut päätelaitteiden ja käyttäjien määrää räjähdysmäisen nopeasti. Käyttäjinä toimivat yksityiset henkilöt, organisaatiot, yritykset sekä valtiot. Kannettavien tietokoneiden, matkapuhelimien ja langattomien verkkojen myötä tietoyhteiskunnasta on tullut yksilön kannalta olennainen osa päivittäistä toimintaa. Globaalit ja liikkuvat tietoliikenneyhteydet mahdollistavat tietoliikenteen läsnäolon kaikkialla. Internet ja TCP/IP-protokollaperhe perustuu vanhentuneelle tekniikalle, ja sitä ei alun perin ole tarkoitettu nykyisen kaltaiselle käyttäjämäärälle. Tämä onkin yksi syy ongelmiin, joita yritetään ja on yritetty korjata erilaisin tavoin.

Internet on nykyisellään organisoitu tietoverkkojen yhdistymä, jonka kautta käyttäjät kytkeytyvät globaaliin tietoverkkoon. Internet tarjoaa mahdollisuuden rajattomaan tiedonhakuun ja palveluiden tarjoamiseen yrityksille, organisaatioille ja valtioille. Internetin historia alkaa vuodesta 1969, jolloin alkujaan muutaman tietokoneen välinen tietoverkko ARPANET esiteltiin (Forouzan 2006, 2).

1960-luvulla tutkimusorganisaatioiden käyttämät tietokoneet olivat itsenäisiä päätelaitteita, jotka eivät esimerkiksi kyenneet kommunikoimaan toisen valmistajan laitteiden kanssa. The Advanced Research Projects Agency (ARPA) alkoi kehittää järjestelmää, jossa tietoa eri tutkimuksista voitaisiin lähettää kustannustehokkaasti ja nopeasti toisiinsa kytkettyjen tietokoneiden välillä (Forouzan 2006, 2). Ensimmäisen vaiheen ARPANET julkaistiin vuonna 1969, ja se yhdisti vain muutamia laitteita vaatimattoman kilobittiluokan ver-

kolla. Päätelaitteiden välisestä kommunikaatiosta huolehti Network Control Protocol (NCP). (Forouzan 2006, 2; Kaario 2002, 15.)

ARPANET:in kehitystyössä mukana olleet V. Cerf ja B. Kahn aloittivat ARPANET:in idean jatkokehityksen vuonna 1972. Heidän tavoitteenaan oli päätelaitteiden yhdistämisen sijaan yhdistää itsenäiset verkot toisiinsa, jolloin päätelaite toisessa verkossa voisi kommunikoida toisen verkon päätelaitteen kanssa. Yhteistyötä kutsuttiin nimellä ”*Internetting Project*” ja sen tuloksena julkaistiin vuonna 1973 raportti, jossa määriteltiin uusi versio NCP-protokollasta eli Transmission Control Protocol (TCP). Tämän lisäksi raportissa määriteltiin useita nykyisen tietoverkkotekniikan kannalta tärkeitä käsitteitä kuten kapselointi, paketti ja yhdyskäytävän (gateway) periaate. *ARPANET Internetin* kehitystyöstä vastasi Defence Communication Agency (DCA), joka julkaisi toimivan kolmen yhdistetyn verkon kokonaisuuden vuonna 1977. Tämän jälkeen myös tehtiin päätös erottaa TCP kahteen osaan: TCP sekä Internetworking Protocol (IP). (Forouzan 2006, 2–3.)

1980-luvulla julkaistiin ARPANETin korvaavat CSNET ja NSFNET, jotka hyödynsivät TCP/IP-protokollia kommunikoidakseen keskenään. Internet laajeni valtion ylläpitämistä tietoverkoista TCP/IP-protokollien avulla toimiviksi laajoiksi yhdistyneiksi verkoiksi. Internetin kasvaessa julkaistiin vielä 1991 ANSNET, jonka oli määrä toimia Internetin selkärankana. (Forouzan 2006, 4.) Internetin lopullisena läpimurtona voidaan pitää hypertekstiin pohjautuvaa 1991 julkaistua sovellusta Gopher, jonka myötä syntyi World Wide Web, sekä ensimmäistä graafista käyttöliittymää hyödyntävää Mosaic-selainta (1992) (Kaario 2002, 15).

Nykyisellään Internet koostuu lukuisista eri palvelujentarjoajien ylläpitämistä verkoista, joiden avulla käyttäjät voivat kommunikoida toisissa verkoissa olevien käyttäjien kanssa. Internetin toimintaa määrittelevät useat eri järjestöt sekä standardit. Taulukossa 1 on joitakin Internetin toimintaan liittyviä organisaatioita.

Taulukko 1. Internetin hallinnoinnista vastaavia organisaatioita (ks. Kaario 2002, 16)

Organisaatio	Tehtävä
Internet Society (ISOC)	Kattojärjestö, joka avustaa standardoinnissa ja ylläpitää valvovia järjestöjä
Internet Architecture Board (IAB)	Toimii Internetin teknisen kehityksen parissa.
Internet Research Force (IRTF)	Tutkimusorganisaatio. Internetin kehitys, protokollat, sovellukset
Internet Engineering Task Force (IETF)	Ongelmanratkaisu, standardointi mm. protokollat ja sovellukset
Network Information Center (NIC)	Kerää ja jakaa tietoa TCP/IP-protokollista
Internet Assigned Numbers Authority (IANA)	Domain-nimien hallinnointi ja numerointi, IP-osoitteiden jakaminen
Internet Corporation for Assigned Names and Numbers (ICANN)	IANA:a hallinnoiva järjestö

Erityisen tärkeänä voidaan pitää IETF:n toimintaa ongelmanratkaisussa ja Internetin avoimessa kehittämisessä. IETF julkaisee Internetiin liittyviä standardeja Request For Comments- sarjassa (RFC). RFC-dokumentit sisältävät uusinta tietoa käytössä olevista Internet-standardeista ja niiden muutoksista sekä muuan muassa TCP/IP-protokollaperheestä. RFC-dokumentit ovat saatavilla IETF:n kotisivuilta (Kaario 2002, 17).

2.2 OSI-malli

Tietoliikennejärjestelmien monimuotoisuus asettaa haasteita luotettavalle tiedon välittämiselle ja vastaanottamiselle. Näiden ongelmien ratkaiseminen helpottuu, kun tietoliikenteen ajatellaan koostuvan eri kerroksilla tapahtuvasta toiminnasta. Näiden kerroksien välillä toimivat yhteysprotokollat, jotka takaavat luotettavan kommunikaation kerrosten välillä. (Kaario 2002, 18.)

Myös TCP/IP-protokollaperheen toiminnan perustana on tiedonsiirron jakaminen eri kerroksiin. Tämän kerrosmallisen ajattelun lähtökohtana voidaan pitää International Standard Organisationin (ISO) tuottamaa OSI-kerrosmallia, joka esiteltiin 1970-luvun lopulla (Forouzan 2006, 17). OSI-mallin oli tarkoitus tarjota laitevalmistajien käyttöön standardeja, joiden avulla eri valmistajat pystyisivät rakentamaan paremmin yhteensopivia verkkolaitteita (Cisco Press 2002, 53). Vaikka OSI-mallista ei ole tullutkaan hallitsevaa standardia vaan se on lähinnä teoreettinen malli, on sen esittelemä ker-

rosajattelu edelleen nykyisen tietoliikenneajattelun pohjana (Kaario 2002, 18).

OSI-mallissa tietoliikenne jaetaan seitsemään eri kerrokseen, joiden läpi lähetettävän tai vastaanotettavan tiedon täytyy kulkea. Näiden kerrosten väliset rajapinnat huolehtivat tiedonsiirrosta kerrosten välillä. Rajapinnat määrittelevät sen, mitä tietoa seuraava kerros tarvitsee ja huolehtii sen lähettämisestä. Rajapinnat mahdollistavat kerroksen sisäisen muutoksen ilman, että muiden kerrosten toteutusta tarvitsee muuttaa.(Forouzan 2006, 18–19.) Kuvio 1. kuvaa OSI-mallin seitsemän kerrosta.

Kuvio 1. OSI-malli (ks. Kaario 2002, 18; Loshin 1997, 14)

Fyysisen kerroksen tehtävänä on fyysisesti siirtää bittivirta, jonka se saa käsittelyynsä ylemmältä kerrokselta. Muiden kerrosten ollessa lähestulkoon pelkästään ohjelmallisia fyysisen kerroksen täytyy ottaa huomioon myös fysikaaliset ilmiöt. (Kaario 2002, 19–20.) Fyysinen kerros määrittelee käytännöt ja toiminnot fyysisten laitteiden ja rajapintojen välille, jotta sähköimpulssien (bittivirta) lähetys onnistuu (Forouzan 2006, 21–22 ; Loshin 1997, 13–14).

Siirtokerroksen tehtäviä ovat muun muassa fyysinen osoitteistus ja bittivirran luotettava siirtäminen siirtotiellä. Kerroksen toteutuksesta vastaa yhteyskäytäntö, jolla voidaan ottaa signaalista dataa, tarkistaa sen oikeellisuus ja lähettää sitä tietynlaisina paketteina. Siirtokerroksen tehtäviin kuuluu myös tarjota ylemmälle kerrokselle eli verkkokerrokselle yhteys kahden verkkoelementin välillä. Erona datan kuljetuksessa siirto- ja verkkokerroksen välillä on se, että siirtokerros vastaa datapaketin kuljetuksesta saman verkon (linkki) sisällä. Kerros huolehtii myös siitä, että pääsyä siirtokerroksen palveluille jaetaan käyttäjien kesken. (Forouzan 2006, 22–23; Kaario 2002, 20; Loshin 1997, 14.)

Verkkokerros vastaa datapakettien siirtämisestä lähtöpisteestä päämääräänsä. Kerros huolehtii loogisesta osoitteistuksesta sekä reitityksestä. Verkkokerros mahdollistaa reitittimien toiminnan ja polun valinnan eri solmulaitteiden välisessä tiedonsiirrossa. Näiden tehtävien lisäksi verkkokerros osallistuu myös laatuvaatimusten täyttämiseen. (Cisco Press 2002, 57; Kaario 2002, 20.) Verkkokerroksen alapuoliset kerrokset eivät ota kantaa varsinaisten pakettien sisältöön (dataan), vaan niiden toiminnan keskiössä on datapakettien lähettäminen solmulaitteiden välillä. Verkkokerroksen yläpuoliset kerrokset eivät puolestaan osallistu datapakettien kuljetukseen solmulaitteiden välillä vaan dataa lähetetään päätelaitteilla käytettävien ohjelmien tai prosessien välillä. (Loshin 1997, 15.)

Kuljetuskerroksen tehtävänä on prosessien välisestä datasiirrosta ja kommunikaatiosta huolehtiminen. Kerros segmentoi isännästä lähtevän datan, joka kootaan määränpäässä uudestaan kokonaisuudeksi. Prosessien välillä tapahtuvan datasiirron vuoksi kuljetuskerros määrittelee, mihin prosessiin tietoa lähetetään niin sanottujen porttinumeroiden avulla. Kerros myös takaa datan luotettavan kuljetuksen, johon se pyrkii virhetunnistuksen ja virhekorjauksen avulla. (Forouzan 2006, 24–26; Kaario 2002, 21.)

Kuljetuskerroksen yläpuolisten kerrosten toiminta liittyy pitkälti sovelluksiin (Cisco Press 2002, 57). Istuntokerroksen tehtäviin kuuluu muun muassa yhteyden solmiminen ja ylläpitäminen kahden järjestelmän välillä. Esitystapakerros puolestaan vastaa käyttävästä esitystavasta ja sen sopimisesta. So-

velluskerros toimii käyttäjän ja tietoverkon välisenä rajapintana, joka tarjoaa sovellusten kautta käyttäjälle mahdollisuuden käyttää erilaisia palveluja. Näiden palvelujen kautta käyttäjän on mahdollista lähettää tietoa toisille käyttäjille tai isäntälaitteille tietoverkossa. (Kaario 2002, 21.)

OSI-malli tarjoaa siis kattavan kuvauksen jokaisen kerroksen toimintaan ja vastuualueisiin. Kun tietoliikenne jaetaan kerroksiin, on sen hallinta helpompaa ja eri tehtäviin tarkoitettujen protokollien määritteleminen yksinkertaisempaa. Kerrostamalla tietoliikennettä myös virheiden löytäminen ja korjaaminen onnistuu helpommin. OSI-mallissa tapahtuvan tiedonsiirron periaatteeseen kuuluu myös tiedon kapselointi, jolla tarkoitetaan prosessia, jossa eri kerroksilla käytettävät protokollat lisäävät datapakettiin määrättyjä osoite- tai lopukekenttiä. Kun datapaketti siirtyy alas OSI-mallin kerroksia, pakettia kasvatetaan kunkin kerroksen vaatimilla laajennuksilla. Vastaanottopäässä puolestaan datapaketista puretaan jokaisella kerroksella vaadittu osa, jonka jälkeen datapaketti siirtyy ylemmäs kerrosmallissa. OSI-malli on varsin hyvä teoreettinen tietoliikennemalli. Sen vahvuus on kunkin kerroksen itsenäisyys. Näin kerroksen toteutusta voidaan muuttaa ilman, että muutokset vaikuttavat kokonaisuuteen. Tiedonsiirto kerrosten välillä tapahtuu rajapintojen avulla. OSI-mallin pohjalta voidaan tarkastella TCP/IP-protokollapinoa, jonka toteutus vastaa melko hyvin OSI-mallin teoreettista kehystä, vaikka onkin kehitetty ennen varsinaista OSI-standardia.

3 TCP/IP-PROTOKOLLAPINO

3.1 TCP/IP-malli

TCP/IP-protokollapinon kehityksen alkuperäisenä tarkoituksena oli luoda yhtenäinen tiedonsiirtoprotokolla, jonka toiminta ei riippuisi siitä, minkälainen verkkotekniikka sen alapuolella on. Verkkotekniikasta huolimatta TCP:n tehtävänä on tarjota luotettava yhteys eri isäntälaitteiden välillä riippumatta siitä, ovatko yksittäiset verkot tai solmut käytössä. Alkujaan sotilaskäyttöön kehitetty protokolla on myös nykyään hallitseva avoin standardi tietoliikenteessä. (Cisco Press 2002, 64.) TCP/IP-mallissa verkon ja sen isäntälaitteiden tiedonsiirron ongelmat on ratkaistu OSI-mallin tavoin jakamalla tietoliikenne eri kerroksiin. TCP/IP-protokollapinon tärkeimmät protokollat ovat Transmission Control Protocol sekä Internet Protocol.

Tässä työssä erityisesti IPv4-protokollan ongelmat ovat keskeisiä. Nämä ongelmat johtuvat pääosin siitä, että protokollat edustavat vanhentunutta teknologiaa, jonka alkuperäistarkoitus ei ollut kattaa nykyisen tietoyhteiskunnan edellyttämiä käyttäjämääriä. Tämän vuoksi pitkään käytettyä IPv4-protokollaa ollaan korvaamassa IPv6-protokollalla, jolla on määrä muun muassa ratkaista IPv4-protokollan akuutti osoiteavaruuden loppuminen

OSI-mallin tavoin TCP/IP-mallissa tietoliikenne nähdään eri kerroksista muodostuvana kokonaisuutena. Koska se on kehitetty ennen OSI-mallia, sen kerrosjako on erilainen. Mallin tunteminen on protokollien ja kokonaisuuden hahmottamisen vuoksi välttämätöntä. TCP/IP-malli eroaa OSI-mallista myös siinä, että se on muotoutunut verkkoliikenneammattilaisten käytännön työn kautta (Comer 2002, 183). TCP/IP-malli on osoittautunut tähän asti toimivaksi tietoliikenteen organisoimistavaksi. Kuvio 2 esittelee OSI-mallin ja TCP/IP-mallin eroja ja vastaavuuksia.

Kuvio 2. OSI-malli ja TCP/IP-malli (ks. Kaario 2002, 22)

Edellä olevasta kuviosta 2 voidaan tarkastella TCP/IP-mallin ja OSI-mallin kerrosrakenteen vastaavuuksia. TCP/IP-mallissa tietoliikenne on jaettu neljään osaan: sovelluskerros, kuljetuskerros, Internet-kerros ja verkkoyhteyskerros (Cisco Press 2002, 65). Mallista on olemassa myös sellaisia tulkintoja, joissa viimeinen kerros on jaettu OSI-mallin mukaisesti kahteen osaan: siirtokerrokseen ja fyysiseen kerrokseen (vrt. Forouzan 2006, 30). On myös huomattava, että kerrosten nimitykset sekä suomeksi että englanniksi vaihtelevat hieman lähteestä riippuen.

TCP/IP-malli on hierarkkinen protokollakokoelma, joka koostuu itsenäisistä moduuleista. Nämä moduulit tarjoavat tiettyjä tarkoin määriteltyjä interaktiivisia palveluita. OSI-mallista poiketen tietyt toiminnallisuudet eivät ole sidottuja ainoastaan tietyille kerroksille, vaan yksittäiset itsenäiset protokollat voidaan ottaa käyttöön järjestelmän vaatimalla tavalla. Hierarkkisuus näyttäytyy siinä, että ylemmän tason protokollat on tuettu yhdellä tai useammalla alemman tason protokollalla. (Forouzan 2006, 30.) TCP/IP-mallissakin voidaan kuitenkin tarkastella kerrosten tehtäviä ja vastuualueita sekä niitä protokollia, jotka muodostavat kyseisen kerroksen. Mallin yksi perusajatus on se, että sen alla voisi toimia mikä tahansa verkkotekniikka. Tämän vuoksi mallissa ei ole var-

sinaista fyysistä verkkokerrosta eikä sille määriteltyjä protokollia vaan ylemmät kerrokset huolehtivat verkossa tapahtuvasta kommunikaatiosta ja fyysiset verkot vastaavat toiminnastaan TCP/IP-mallin ulkopuolella. (Loshin 1997, 16.)

Verkkoyhteyskerros (*engl. link layer, data-link layer*) vastaa niistä toiminnoista ja tekijöistä, joilla IP-paketti todella siirtyy fyysisen yhteyden kautta. Kerroksen toimintaan liittyvät muun muassa verkkoadapterit ja laiteajurit, jotka kommunikoivat verkon kanssa. (Cisco Press 2002, 65; Stevens 1999, 2.)

Internet-kerros (*engl. network layer*) huolehtii datapakettien liikkumisesta verkossa. Se huolehtii reitityksestä eli parhaan polun määrityksestä, pakettien kytkennästä ja siitä, että lähetetyt paketit tulevat perille riippumatta käytetystä polusta ja verkoista. Internet Protocol (IP), Internet Control Message Protocol (ICMP) ja Internet Group Management Protocol (IGMP) muodostavat tämän kerroksen toiminnot. (Cisco Press 2002, 65; Stevens 1999, 2.)

Kuljetuskerroksen (*engl. transport layer*) tehtävänä on tarjota kahden isäntälaitteen välille luotettava tietoliikenneyhteys, jota sovelluskerros voi käyttää datan lähetykseen. Lisäksi kerros huolehtii vuonohjauksesta sekä uudelleen lähettämisestä. Kuljetuskerroksen tärkeimpiä protokollia on Transmission Control Protocol (TCP), joka tarjoaa luotettavan datasiirtoyhteyden. Toinen tärkeä kuljetuskerroksen protokolla on User Datagram Protocol (UDP). Suurin ero näiden kahden protokollan välillä on se, että UDP ei tarjoa luotettavaa yhteyttä vaan sitä käytettäessä yhteyden luotettavuutta täytyy erikseen valvoa sovelluskerroksella. (Stevens 1999, 2.)

Sovelluskerroksella (*engl. application layer*) TCP/IP-mallissa tapahtuu kaikki se toiminta, joka on OSI-mallissa määritelty kolmen päällimmäisen kerroksen toimintoihin. Kerroksen protokollat vastaavat istunto- ja esitystapoihin liittyvistä toiminnoista sekä koodauksesta ja keskustelusta kahden järjestelmän välillä. Useita TCP/IP-sovelluskerroksen protokollia käytetään laajasti nykyisissä tietoliikennejärjestelmissä. Kerroksessa käytettäviä protokollia ovat muun muassa Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) ja Domain Name Server (DNS). (Forouzan 2006, 32; Stevens 1999, 3.)

3.2 Transmission Control Protocol (TCP)

Transmission Control Protocol eli TCP on TCP/IP-mallin kuljetuskerroksen yksi protokolla. Kuljetuskerroksen tehtäviin kuuluu tarjota tietoliikenneyhteys kahden isäntälaitteen välillä ja erityisesti kahden isäntälaitteella pyörivän prosessin välillä. TCP on yhteydellinen *process-to-process*-protokolla, joka tarjoaa luotettavan prosessien välisen datasiirtotavan. Se sopii käytettäväksi silloin, kun datalähetystä tapahtuu sellaisten sovellusten välillä, joiden toiminta häiriintyy vähäisestäkin määrästä hävinneitä datakehyksiä. Luotettavuudella tarkoitetaan sitä, että TCP valvoo lähettämiensä datapakettien perillemenoa sekä järjestystä ja tarvittaessa lähettää tietoa uudestaan jos virheitä syntyy. Sovellusten ei siis tarvitse huolehtia virheentarkistuksesta. (Forouzan 2006, 275–276; Kaario 2002, 166–167.) Yhteydellisyys puolestaan tarkoittaa sitä, että protokolla luo kahden päätepisteen välille virtuaalisen yhteyden, joka muodostetaan neuvottelemalla ennen varsinaista datansiirtoa. Yhteys myös lopetetaan neuvottelemalla päätepistelaitteiden protokollien välillä. (Stevens 1999, 224.)

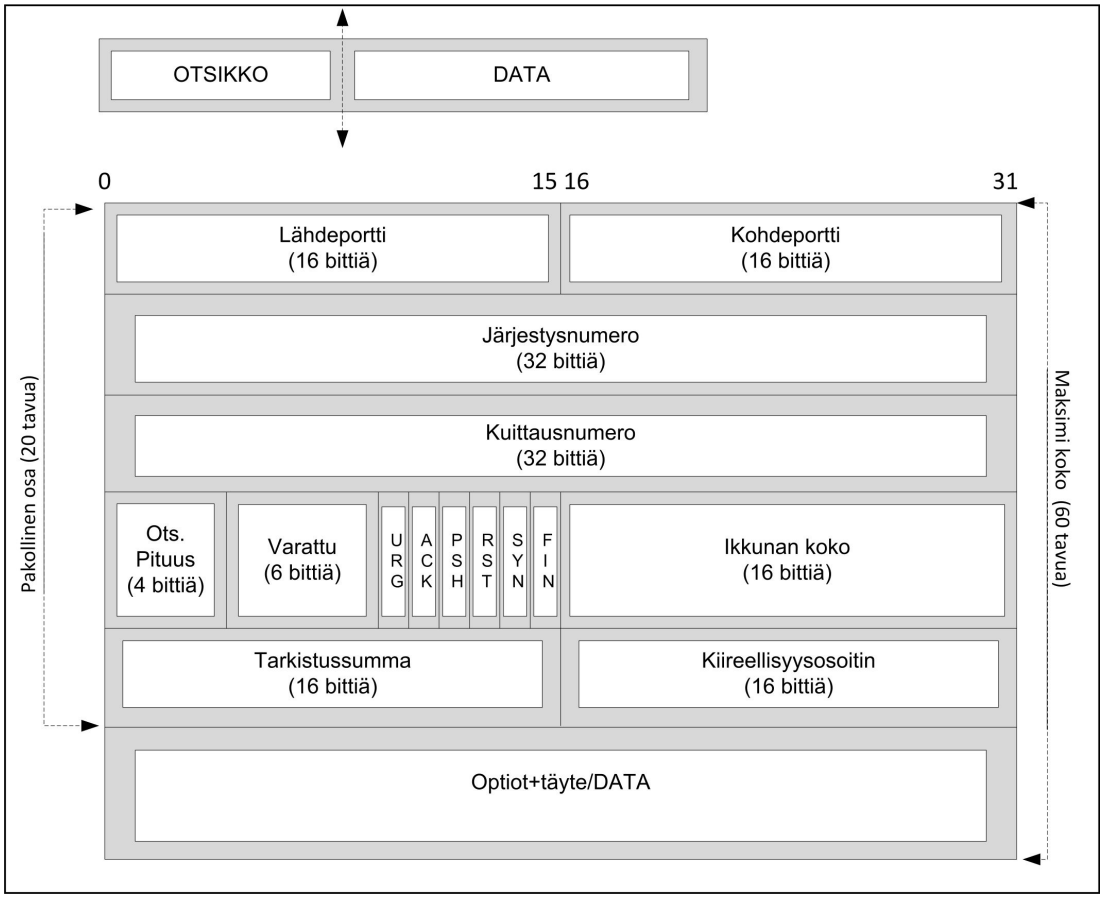
TCP on kuljetuskerroksen protokolla, joten sen tehtävänä on lähettää ylempien kerrosten sovelluksilta saatua dataa vastaanottopään sovelluksiin. Tämän vuoksi TCP määrittelee sovelluksille porttinumeroita, joilla se erottaa yläpuolella toimivat sovellukset toisistaan. Tämä mahdollistaa myös useamman sovelluksen yhtäaikaisen palvelemisen. (Kaario 2002, 166.) Taulukko 2. esittelee porttien numeroinnin periaatteet sekä esimerkkejä tunnetuista ja varatuista porttinumeroista. Tunnetut ja varatut porttinumerot muun muassa helpottavat ylläpitäjän työtä virhetilanteissa, ja ne ovat myös tärkeitä palomuurien ja virustorjuntaohjelmien toiminnan säätämisessä. Edellä mainittujen porttityyppien lisäksi osoitteita on myös varattu väliaikaisia portteja varten.

Taulukko 2. Sovelluksien porttiosoitteita (ks. Forouzan 2006, 276)

Tunnetut portit 0-1023	**Nimi/Protokolla**	**Kuvaus**
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
53	DNS	Domain Name Server
80	HTTP	Hypertext Transfer Protocol
Rekisteröidyt portit 1024-49151	**Nimi/Protokolla**	**Kuvaus**
1293	IPSec	Internet Protocol Security
1723	PPTP	Microsoft Point-to-Point Tunneling Protocol
33434	tracerout	Tracerout-työkaluohjelma
Dynaamiset, yksityiset ja lyhytikäiset portit	**49152–65535**	**Tarkoitettu väliaikaiseen käyttöön tietyissä tapauksissa**

TCP saa ylemmässä kerroksessa toimivista sovelluksista käyttöönsä tavuvirtaa, jota sen tulee lähettää eteenpäin. Protokolla ei kuitenkaan lähetä saamaansa dataa sellaisenaan eteenpäin vaan tarjoaa alemmille kerroksille sovelluksilta saamaansa ja varastoimaansa dataa kehyksissä. Näitä kehyksiä kutsutaan segmenteiksi. TCP pystyy määrittelemään eteenpäin lähettämänsä segmentin koon, joten se voi lähettää erikokoisia segmenttejä kuin sovelluksen lähettämät alkuperäiset datapalaset. Tällä tavoin TCP pystyy optimoimaan lähetykset yhteyden nopeuden ja kapasiteetin mukaan. Segmentoimalla dataa TCP myös hoitaa vuonvalvontaa ja uudelleenlähettämistä. (Kaario 2002, 166–167.)

TCP-kehysrakenteessa otsikkokenttä on 20–60 tavua pitkä, ja sen pituus riippuu siitä, kuinka paljon valinnaisia kenttiä on käytössä. Kehyksen pakollinen osa on 20 tavua. (Forouzan 2006, 282.) Kehysrakenne esitellään kuviossa 3.



Kuvio 3. TCP-kehysrakenne ja otsikko (Forouzan 2006, 282)

Lähdeportti (16 bittiä) tarkoittaa porttia, josta data lähetetään. Tietyt porttinumerot ovat varattuja tietyille sovelluksille, jolloin yleensä käytetään kyseistä varattua porttia. Jos sovellukselle ei ole varattu tiettyä porttia, otetaan käyttöön lyhytikäinen porttinumero, joka toimii prosessin lähtöosoitteena. Kohdeportti puolestaan toimii vastaanottajaprosessin tunnuksena, ja siihen pätevät samat ominaisuudet kuin lähtöporttiin. (Kaario 2002, 167–168.)

Järjestysnumerolla (32 bittiä) TCP ilmoittaa segmentissä olevan ensimmäisen dataoktetin järjestysluvun. Tämän avulla protokolla suorittaa virheentarkistusta ja tarvittaessa lähettää segmentit uudestaan. Järjestysnumero takaa TCP:n luotettavuuden. Kuittausnumero puolestaan ilmoittaa, mitä dataoktettia vastaanottaja seuraavaksi odottaa. Kuittausnumeroksi tulee siis viimeisen dataoktetin järjestysluku + 1. TCP käyttää kaksisuuntaista yhteyttä, ja molempiin suuntaan tapahtuva liikenne numeroidaan. Järjestys- ja kuittausnumerolla vahvistetaan edelleen yhteyden luotettavuutta ja datasegmenttien oikeaa lähetysjärjestystä. (Forouzan 2006, 282: Kaario 2002, 168.)

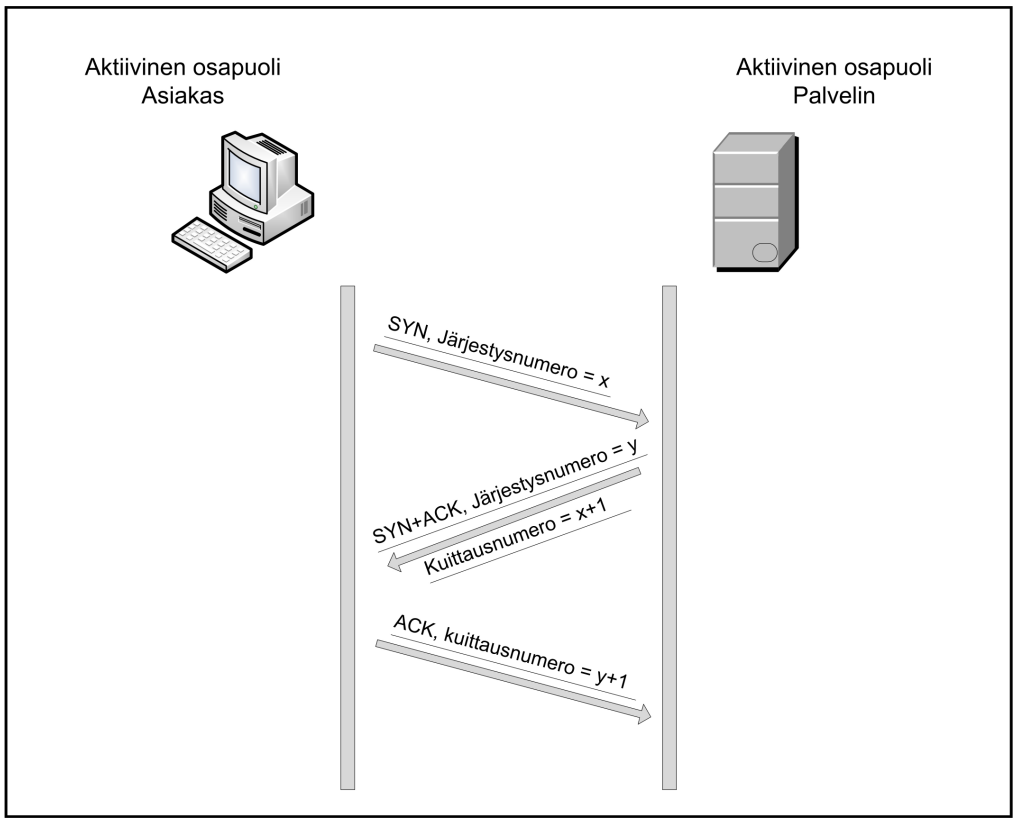
Otsikon pituudessa (4 bittiä) ilmoitetaan TCP-otsikon pituus (20–60 tavua). Seuraavat kuusi bittiä on varattu myöhempään käyttöön, ja sen jälkeen tulevat kuusi bittiä ilmoittavat lippuja. (Kaario 2002, 169.) Taulukossa 3 on selitetty lippujen tarkoitukset.

Taulukko 3. TCP-liput (Forouzan 2006, 283)

Lippu	**Kuvaus**
URG	Kiireellisyysosoitin-kentän arvo on validi
ACK	Kuittausnumero-kentän arvo on validi
PSH	Työnnä dataa
RST	Yhteys täytyy nollata
SYN	Synkronoi sekvenssinumerot yhteyden aikana
FIN	Lopeta yhteys

Lippujen jälkeen määritellään ikkunan koko (16 bittiä). Ikkunan koolla TCP määrittelee, mikä on optimaalinen lähetyskoko, jonka vastaanottaja pystyy ilman ongelmia käsittelemään. Ikkunan kokoa muuttamalla protokolla pystyy vastaamaan järjestelmän ja prosessien kuormituksen vaihteluun. Ikkunan koon jälkeinen kenttä on Tarkistussumma-kenttä (16 bittiä), jolla pystytään tarkistamaan, että segmentti on menossa oikean protokollan käsittelyyn. Kiireellisyysosoitin (16 bittiä) puolestaan kertoo vastaanottajalle, mikä osa datasta on kiireellistä. Lopuksi kehyksessä jätetään tilaa myös valinnaisille kehyksenosille eli optioille sekä datalle. Näistä optioista vain harvoilla on todellisuudessa käyttöä. Huomattavaa on myös se, että data ei ole pakollinen TCP-kehyksen osa. (Kaario 2002, 169; Stevens 1999, 227.)

Yksi merkittävä TCP:n ominaisuus on yhteydellisyys. Tällä tarkoitetaan tapaa, jolla protokolla luo virtuaalisen yhteyden kahden isännän prosessien välille. Tämä yhteys synnytetään niin sanotun kolmitiekättelyn (*engl. Three-Way Handshaking*) kautta. Kuvio 4 esittelee kolmitiekättelyn normaalitilanteessa.



Kuvio 4. TCP-yhteydenmuodostus eli kolmitiekättely (Kaario 2002, 175)

TCP-otsikossa on yhteydenmuodostamisen kannalta merkittäviä kenttiä: SYN- ja ACK-bitit sekä järjestys- ja kuittausnumerot (Kaario 2002, 174). Ensimmäiseksi yhteyden avaava osapuoli lähettää haluamaansa kohteeseen viestin, joka sisältää aktiivisen SYN-bitin sekä satunnaisesti muodostetun järjestysnumeron. Vastapuoli lähettää vastauksen, jossa SYN- ja ACK-bitit ovat aktiivisia. Kolmannessa vaiheessa yhteyden avaava puoli vastaa vielä viestillä, jossa ACK-bitti on aktiivinen. (Kaario 2002, 174.) On huomioitava, että yhteyden muodostaminen ja lopettaminen voivat tapahtua monimutkaisemminkin riippuen tilanteesta ja yhteydenmuodostuksen tarkoituksesta. Oleellista on kuitenkin se, että TCP käyttää yhteyden muodostamiseen ja lopettamiseen isäntälaitteiden välisiä sanomia.

TCP on myös paljon monimutkaisempi protokolla kuin edellä on esitelty. Sen toimintaan liittyy paljon hienovaraisia ominaisuuksia, jotka tekevät protokollasta hyvin moneen tarkoitukseen soveltuvan. TCP on myös monitasoinen protokolla, jonka toiminnan kuvaaminen ei ole yksinkertaista ja onnistuisi parhaiten erilaisten tilakoneiden avulla. Tilakone on järjestelmän tilojen, tilasiirtymisten ja erilaisten herätteiden muodostama määrittely. Näistä määrittelyistä muodostetaan graafinen kuva, joka on helpompi tulkita. Tämän työn

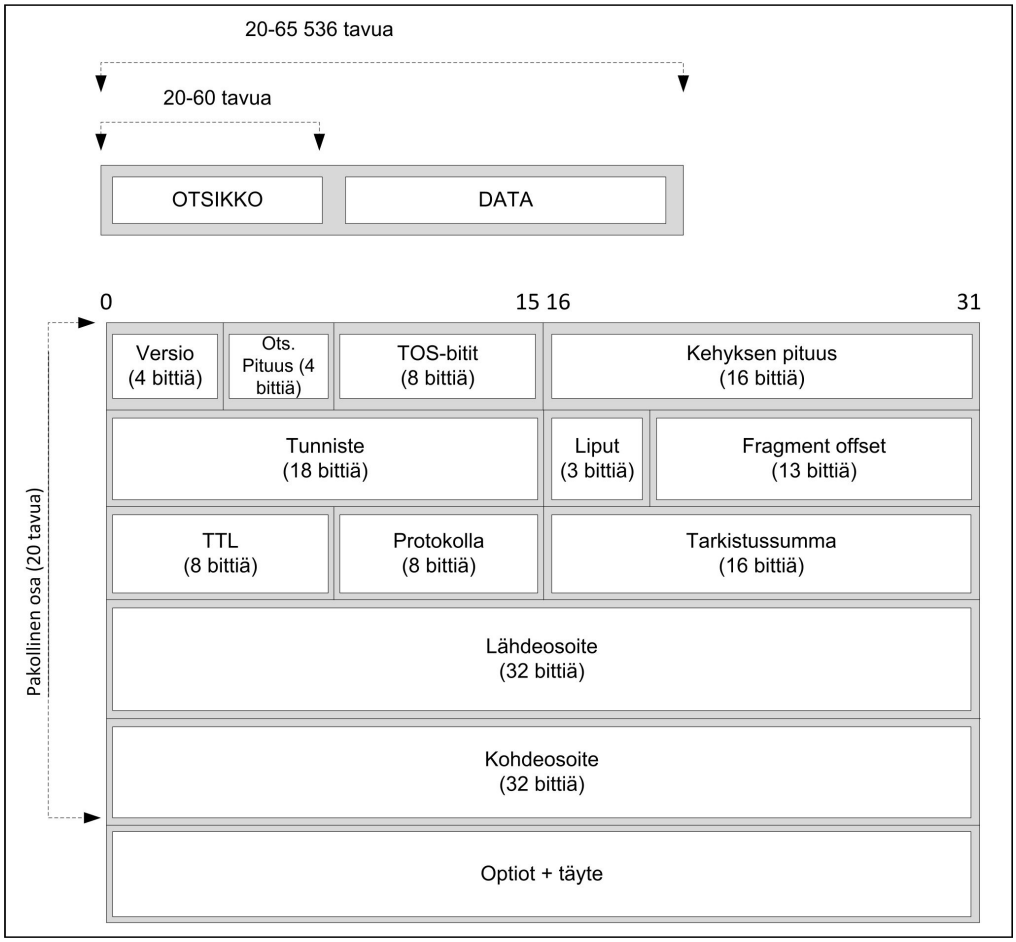
puitteissa kuitenkin riittää protokollan keskeisempien ominaisuuksien ja toiminnallisuuksien esittely.

3.3 Internet Protocol (IPv4)

IPv4 on TCP/IP-protokollaperheen tärkein protokolla. Se toimii Internet-kerroksella ja kaikki sovellukset tai prosessit, jotka haluavat toimia IP-verkoissa, joutuvat käyttämään IP-kerroksen tuottamia palveluja. IPv4 on kuitenkin kehitetty aikana, jolloin nykyisiä käyttäjämääriä ei osattu kuvitella, joten sen rakenteessa ja toiminnassa on pahoja puutteita. Isoin puute on protokollan käyttämä Osoite-kenttä. Osoite-kenttä on 32 bittiä pitkä, ja tästä syntyvä osoiteavaruus on teoreettisesti 4 294 967 296 (2^{32}) ainutlaatuista osoitetta. Käytännössä osia osoiteavaruudesta on kuitenkin varattu erilaisiin tarkoituksiin, joten tietoliikenteen käyttöön ei jää näin suurta määrää ainutkertaisia osoitteita. Osoiteavaruuden nykyiseen suureen varaukseen vaikuttaa myös se tosiasia, että osoitteita jaettiin alkuaikoina varsin epäloogisesti ja vailla tarkempaa suunnitelmaa. Osoitekapasiteetin täyttymisestä on erilaisia arvioita, mutta suuri osa arvioista sijoittaa loppumispäivämäärän parin vuoden sisälle, jopa aiemmin (Hain 2005; Hain 2010; Huston 2010). IPv4 on siis vanhentunutta teknologiaa, ja sitä ollaan korvaamassa uudella IPv6-protokollalla. Uudistuksen käyttöönotto on kuitenkin hidasta, ja senkin jälkeen IPv4 on edelleen olemassa ainakin siirtymävaiheen ajan. Tämän vuoksi on tärkeää esitellä myös vanhan IP-version ominaisuuksia. Ominaisuuksien esittely helpottaa myös vertailua uuteen versioon.

IPv4 on epäluotettava ja yhteydetön protokolla, joka toimii niin sanotulla *best-effort* -periaatteella. Epäluotettavuus tarkoittaa sitä, että IPv4 ei ota kantaa lähetyksen perillemenoon eikä virhetarkistukseen vaan olettaa toimivansa luotettavan yhteyden päällä. Luotettavan yhteyden hallinta täytyy näin ollen hoitaa muilla kerroksilla toimivilla protokollilla, esimerkiksi TCP:llä. Yhteydettömyys tarkoittaa sitä, että IPv4 toimittaa eteenpäin IP-paketteja (*engl. datagram*) niin, että paketit toimitetaan perille toisistaan riippumatta, jopa eri reittejä ja alkuperäisestä järjestyksestä poiketen. Tämän vuoksi myös yhteydellisyys täytyy hoitaa muilla protokollilla. (Forouzan 2006, 179–180; Loshin 1997, 104.)

IPv4:n ominaisuuksia on helpointa lähteä tarkastelemaan IP-paketin kehysrakenteen ja erityisesti sen otsikko-osan avulla. Kuten TCP-segmentti myös IP-paketti (datagram) sisältää osoitetietoja ja määrityksiä varsinaisen datan lisäksi. Kuvio 5 kuvaa IP-paketin kehysrakenteen.



Kuvio 5. IPv4-kehysrakenne ja otsikko (ks. Kaario 2002, 46)

Kehysrakenteesta voidaan nähdä, että IP-otsikon minimipituus on 20 tavua, jonka jälkeen tulevat mahdolliset optiot sekä paketin varsinainen dataosuus. Optioiden käyttö IPv4:ssä on suhteellisen harvinaista. IP-paketin otsikossa on monia kenttiä, joiden avulla paketti muun muassa reititetään tai jaetaan osiin.

Versio (4 bittiä) kertoo, mikä IP-versio on käytössä. IPv4:n ollessa käytössä kenttä saa arvon 4 ja uusi IP-versio saa puolestaan arvon 6. Otsikon pituus puolestaan kertoo, kuinka monta 32 bitin sanaa otsikossa on ja saa siis usein arvon 5. TOS-bitit (Type of Service) eli kahdeksan seuraavaa bittiä käytetään IP-pakettien ryhmittelyssä niiden tarvitseman palvelun mukaan. Vain yksi bitti kerrallaan voi olla aktiivinen. TOS-arvoja voivat olla viive, läpäisy, hinta ja

luotettavuus. Kehyksen kokonaispituus on seuraava 16 bitin kenttä. Kenttä ilmoittaa, kuinka pitkä kehys, otsikko mukaan lukien, on. IP-paketin koko voi näin ollen olla 2^{16}-1 eli 65 535 tavua pitkä. Kokonais- ja otsikonpituuden avulla voidaan myös ilmoittaa datan alkamis- ja päättymiskohdat paketissa, koska näille ei ole varsinaista merkkiä järjestelmässä. Tunnistekenttä (16 bittiä) identifioi vastaanottopäälle ne IP-paketit, jotka on pilkottu samasta ylemmänkerroksen datasta. Liput-kenttäkin (3 bittiä) osallistuu datan pilkkomiseen muun muassa ilmoittamalla, onko IP-paketin pilkkominen mahdollista. M-bitti ilmoittaa, että pakettiin kuuluu vielä osia ja D-bitti ilmoittaa, että pakettia ei tule pilkkoa pienempiin osiin. Fragment Offset -kenttä kertoo pilkottujen datapakettien järjestyksen. Nämä kolme kenttää osallistuvat menetelmään, jota kutsutaan kehysten fragmentoinniksi. Se tarkoittaa yksinkertaistettuna IPv4:n kykyä pilkkoa kehyksiä pienempiin osiin, jos esimerkiksi verkon alemmat protokollat sitä vaativat. (Kaario 2002, 46–49; Loshin 1997, 106–107.)

Otsikkorakenteessa seuraavat kahdeksan bittiä muodostavat Time to Live-kentän, jolla IPv4 ilmoittaa, kuinka monen reitittimen kautta paketti voi kulkea ennen kuin se tuhotaan. Time to Live-kentän avulla vältetään tilanne, jossa paketti jäisi ikuisesti kiertämään verkossa. Protokolla-kenttä (8 bittiä) kertoo, mistä protokollasta data on IP-kerrokseen tullut. Tarkistussumma (8 bittiä) on kehyksen tarkistussumma. Reitityksen ja IP-pakettien lähettämisen kannalta merkittävät kentät ovat 32 bittiset lähde- ja kohdeosoitekentät, joissa määritellään vastaanottajan ja lähettäjän IP-osoitteet. Loppuosan otsikosta muodostavat optiot ja täyte, jolloin otsikon koko voi olla 20–60 tavua. (Kaario 2002, 49–50; Loshin 1997, 107–108.)

IPv4:n ongelmallisin ominaisuus on sen käyttämä 32-bittinen IP-osoite. IP-osoite on yksilöllinen looginen osoite jokaiselle laitteelle, joka haluaa kommunikoida toisten Internet-verkossa olevien laitteiden kanssa. IPv4-osoite muodostuu neljästä kahdeksan bitin tuottamasta kokonaisluvusta. Yleisin osoitteen kirjoitusmuoto on *n.n.n.n*, missä jokainen n edustaa 8 bitin muodostamaa kokonaislukua. IP-osoitteesta voidaan erotella myös verkko-osa sekä laiteosa. (Forouzan 2006, 81–82.) Esimerkiksi 192.168.1.32 on desimaalimuotoinen IP-osoite, jonka binäärimuotoinen vastine olisi 11000000

10101000 00000001 00100000. IPv4-osoitteen muoto on varsin erilainen verrattuna IPv6-notaatioon, joka esitellään myöhemmin.

Alkujaan nykyistä paljon pienemmille käyttäjämäärille suunniteltu IP-osoiteavaruus on jäämässä pieneksi muun muassa kannettavien tietokoneiden, mobiililaitteiden sekä jatkuvasti päällä olevien laitteiden, esimerkiksi reitittimien, takia. Nykyisellään IP-osoitteiden jakamista valvovat IANA sekä alueelliset organisaatiot kuten Euroopassa RIPE NCC. Yleisesti voidaan sanoa, että osoiteavaruuksia jaetaan operaattoreille, jotka puolestaan jakavat osoiteavaruutta asiakkailleen.

IP-osoiteavaruuden varaukseen on merkittävästi vaikuttanut myös se, että alun perin IP-osoitteita käsiteltiin luokiteltuina. Luokat sisälsivät tietyn määrän osoitteita, ja osoitteita jaettiin luokkien koon mukaan niitä tarvitseville. IP-osoiteluokkia tarkasteltaessa huomataan merkittäviä suunnitteluvirheitä, joiden vuoksi nykyisellään ollaan tilanteessa, jossa osoiteavaruus on täyttymässä huolimatta siitä, että IP-osoitteita vaativat laitteet eivät välttämättä vielä tarvitsisi teoreettista yli neljää miljardia osoitetta. (Forouzan 2006, 95.) Taulukko 4 kuvaa IP-osoitteiden luokkajakoa, osoitemääriä sekä luokkien viemää tilaa osoiteavaruudesta. Taulukosta on myös helppo nähdä suunnitteluvirheet luokkajaossa.

Taulukko 4. IP-osoiteluokat ja osoitemäärät (Forouzan 2006, 85)

Luokka	Luokan tunnusbitit	Osoitemäärä	Osuus
A	0	2^{31} = 2 147 483 648	50 %
B	10	2^{30} = 1 073 741 824	25 %
C	110	2^{29} = 536 870 912	12,50 %
D	1110	2^{28} = 268 435 456	6,25 %
E	1111	2^{28} = 268 435 456	6,25 %

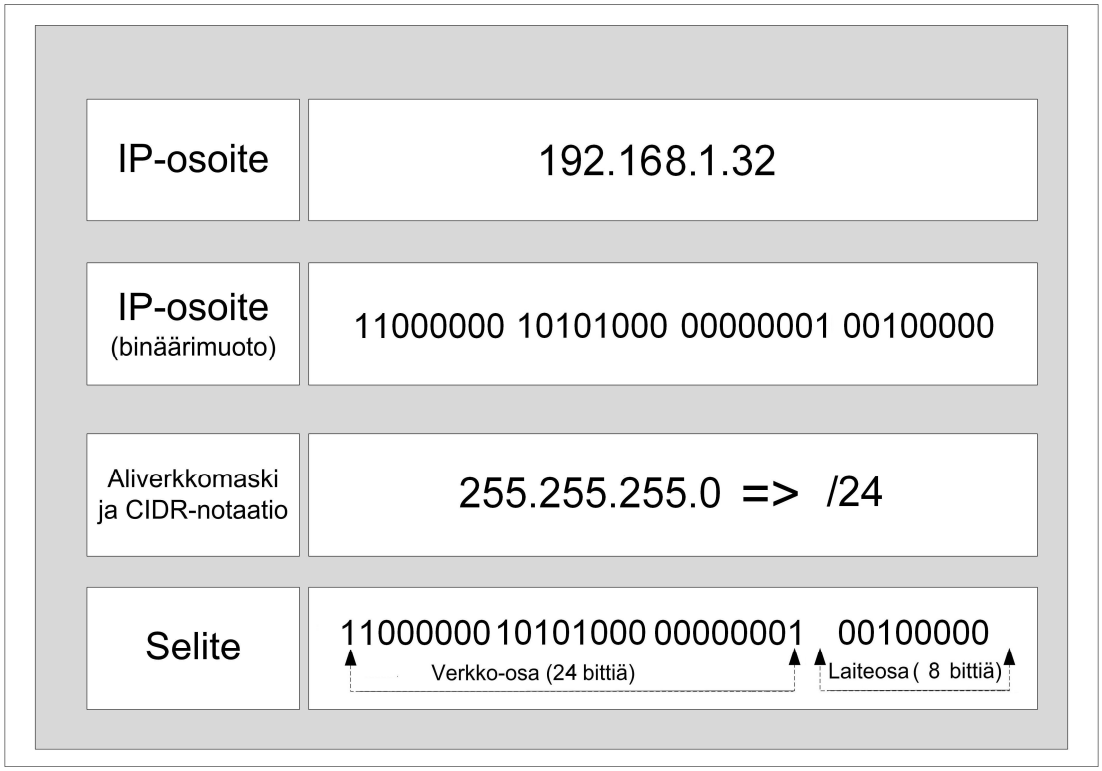
Taulukosta huomaamme, että A-luokan osoitteet vievät IPv4-osoiteavaruudesta merkittävän osan, noin puolet. Tämä on huomionarvoista siitä syystä, että alkujaan tällaisia A-luokan osoitteita jaettiin jopa yrityksille. A-luokan osoitteesta voidaan todeta, että se muodostuu luokan tunnusbitistä,

seitsemän bitin verkko osasta ja 24 bitin laiteosasta. Koska IP-osoitteilla on tiettyjä varauksia, kuten multicast- ja broadcast-osoitteet ja koska tiettyjä osoitevälejä on varattu yksityisiin verkkoihin, jää A-luokan verkko-osoitteita jäljelle 125. Edellä mainittujen rajoituksien jälkeen 125 organisaatiota voi saada A-luokan osoitteen. Tämä tarkoittaa kuitenkin sitä, että jokainen verkko voi sisältää 16 777 216 osoitetta, joka tarkoittaisi suurta lähes valtiotason kokoista yritystä tai organisaatiota. Jakamalla A-osoitteita organisaatioille, hukattiin miljoonia IP-osoitteita. (Forouzan 2006, 84–91.)

Sama osoitteiden katoamisen ongelma koskee myös B-luokan osoitteita, joista syntyy 16 368 verkko-osoitetta, joissa on 65 536 osoitetta kussakin. Tämäkin osoiteluokka vaatisi isoja organisaatioita, jotta kaikki osoitteet tulisivat käyttöön. Myös B-luokan osoitteita on suuressa määrin hukattu. C-luokan osoitteet puolestaan muodostavat käänteisen ongelman, koska luokan tuottamia verkko-osoitteita on runsaasti eli noin kaksi miljoonaa, mutta jokaisessa verkossa voi olla vain 256 osoitetta. Määrä on liian pieni useimmille organisaatioille. (Forouzan 2006, 84–91.)

Luokallisen IP-osoitteistuksen ongelmallisuuden vuoksi siirryttiin, nykyisenkaltaisen Internetin synnyttyä, 1990-luvun puolivälissä käyttämään luokatonta IP-osoitteistusta. Luokattomat IP-osoitteet ovat käytössä oleva standardi, ja muun muassa lähes kaikki reititinprotokollat tukevat ja suosivat luokatonta osoitteistusta. Huomattavaa on kuitenkin se, että vaikka luokaton IP-osoitteistus on laajalti käytössä, ei kaikkia aikaisemmin jaettuja luokallisia osoiteavaruuksia ole saatu käyttöön. Myös luokattomassa osoitteistuksessa IP-osoite jaetaan verkko-osaan ja laiteosaan. Luokallisen IP-osoitteen pääasiallinen ero on se, että osoiteavaruutta ei tarvitse enää jakaa epäkäytännöllisten luokkien mukaan vaan jokaiselle IP-osoiteavaruutta tarvitsevalle yritykselle tai organisaatiolle pystytään varamaan juuri sopiva määrä verkko- ja laiteosoitteita käsittävä pala osoiteavaruudesta. Tällöin vältetään turhien osoitteiden jakaminen. Luokaton IP-osoitteistus myös mahdollistaa paremmin useamman tason hierarkian ja samassa fyysisessä verkossa voi olla monia eri loogisen tason verkkoja. Nykyisellään kaikki verkot käyttävät vähintään kolmen tason hierarkiaa ja aliverkotusta tietoverkkojen reitityksessä ja osoitteistuksessa. (Cisco Press 2002, 394; Forouzan 2006, 92–108.)

Luokaton IP-osoitteistus perustuu aliverkkomaskin käyttöön. Yksinkertaistettuna aliverkkomaski ilmoittaa, mikä osuus IP-osoitteesta kuuluu verkko-osalle ja mikä on laiteosoitteen osuus (Kaario 2002, 58.) Kuvio 6 selventää aliverkkomaskin ja IP-osoitteen välistä suhdetta.



Kuvio 6. IP-osoite ja aliverkkomaski

Aliverkkomaski ja erityisesti 1993 tehty Classless Interdomain Routing (CIDR) lisäys IPv4:ään toimivat nykyisellään perustana IP-osoitteille. CIDR mahdollistaa aliverkkomaskin, joka ilmoittaa verkko-osan olevan minkä tahansa pituinen osa IP-osoitteesta. Näin mahdollistetaan entistä tehokkaampi IP-osoitteiden jako niitä tarvitseville. CIDR notaatiossa aliverkkomaskin pituus ilmoitetaan IP-osoitteen jälkeen tulevalla /n merkinnällä, jossa n merkitsee, kuinka monta bittiä IP-osoitteesta on käytössä verkko-osalle ja mikä osa osoitteesta jää laiteosalle (Kaario 2002, 58.) CIDR:ää käyttämällä voidaan jakaa esimerkiksi osoiteavaruus 10.10.10.32/27. Notaatio tarkoittaa sitä, että IP-osoitteesta 27 bittiä on käytetty verkko-osaan ja jäljelle jäävät 5 bittiä muodostavat laiteosan. Tämän jaon avulla saadaan käyttöön osoiteavaruus, joka olisi välillä 10.10.10.32–10.10.10.63 ja tarjoaisi näin 30 mahdollista laiteosoitetta ja vapauttaisi seuraavan osoiteavaruuden muuhun käyttöön. CIDR perustuu vaihtuvanmittaiseen aliverkkomaskiin (*engl. Variable Lenght*

Subnet Mask), jossa verkko-osan pituus voidaan joustavasti määritellä. Esimerkiksi edellä mainittu osoiteavaruus 10.10.10.32/27, voitaisiin vaihtuvanmittaista aliverkkomaskia käyttäen jakaa pienempien osoiteblokkien kesken taulukon 5 osoittamalla tavalla.

Taulukko 5. Osoiteavaruuden jakaminen (VLSM)

Aliverkon nimi	Verkkotunnus	Laite-osoitteet	Osoiteblokin pituus
Alkuperäinen	***10.10.10.32 /27***	***30***	***10.10.10.32–10.10.10.63***
Aliverkko 1	10.10.10.32 /28	14	10.10.10.32–10.10.10.47
Aliverkko 2	10.10.10.48 /29	6	10.10.10.48–10.10.10.55
Aliverkko 3	10.10.10.56 /30	2	10.10.10.56–10.10.10.59
Aliverkko 4	10.10.10.60 /30	2	10.10.10.60–10.10.10.63

CIDR ei ole ainoa menetelmä, jolla IPv4-osoiteavaruuden loppumista on pyritty hillitsemään. Network Address Translation (NAT) eli osoitteenkäännös tarkoittaa menetelmää, jossa IP-osoite vaihdetaan toiseen esimerkiksi reitittimessä. Tällä tavoin yksityisiä IP-osoitteita käyttävät laitteet voivat kommunikoida ulospäin verkostaan. Yksityiset osoitteet löytyvät taulukosta 6.

Taulukko 6. Yksityiset IP-osoiteavaruudet (ks. IETF 1996)

Luokka	Verkkotunnus	Blokit
A	10.0.0.0–10.255.255.255	1
B	172.16.0.0–172.31.255.255	16
C	192.168.0.0–192.168.255.255	256

Osoitteenkäännössä yksityisen IP-osoitteen omistava isäntälaite lähettää NAT-laitteelle ulkoverkkoon tarkoitetun IP-paketin. NAT-laite, yleensä reititin, toimii tynkäverkon rajalla eli tarjoaa ainoan yhteyden tynkäverkosta ulkoverkkoihin. Otettuaan vastaan IP-paketin NAT-laite tarkastaa siinä olevan IP-otsikon ja vaihtaa paketissa olevan yksityisen osoitteen globaalisti ainutkertaisella IP-osoitteella. Tämän jälkeen NAT-laite lähettää paketin eteenpäin vastaanottajalle. Vastauksen saadessaan NAT-laite katsoo käännöstaulukosta, mikä yksityinen osoite vastaa vastaanotetun paketin yleistä IP-osoitetta ja toimittaa sen perusteella paketin yksityiseen osoitteeseen. (Cisco Press 2002, 414.) NATin hyötynä IP-osoiteavaruuden loppumisen ehkäisemiseksi

on se, että sitä käyttämällä organisaatio tarvitsee vähemmän varsinaisia IP-osoitteita käyttöönsä. Oletuksena on, että organisaation kaikki koneet eivät ole yhtä aikaa yhteydessä ulkoverkkoihin, jolloin vähempi määrä ainutkertaisia IP-osoitteita riittää yhteyden säilyttämiseksi. NAT auttaa myös tilanteessa, jossa organisaatio kasvaessaan on ylittänyt varatun osoiteavaruuden ja tarvitsee lisää IP-osoitteita. NAT:in avulla yksityisiä osoitteita voi ottaa käyttöön eikä varsinaisia IP-osoitteita näin ollen tarvitse lisätä. NAT lisää myös tietoturvaa piilottamalla verkon sisäisen rakenteen ulkopuolisilta verkoilta. (Cisco Press 2002, 414–417.)

Edellä esitelty osoitteenmuunnostekniikka ei todellisuudessa säästä kovinkaan montaa julkista IP-osoitetta, mutta NAT:iin perustuvan porttimuunnoksen (*engl. Port Address Translation, PAT*) avulla on mahdollista merkittävästi vähentää IP-osoitteiden tarvetta. Porttimuunnoksessa on teoriassa mahdollista nimetä organisaatiolle vain yksi julkinen IP-osoite, joka toimii kaiken ulospäin toimivan liikenteen osoitteena. Päätelaitteilta lähtevä ja tuleva liikennöinti identifioidaan porttinumerolla, jonka PAT-laite määrittelee jokaiselle sille saapuvalla yhteyspyynnölle. Porttinumeroita on teoreettisesti olemassa 65 536 kappaletta, joten yhden julkisen IP-osoitteen alla voisi liikennöidä tuhansia päätelaitteita. Päätelaitteiden tunnistaminen tapahtuisi porttinumeroiden perusteella NAT-menetelmän periaatteiden mukaista yhteyksien tunnistamisprosessia noudattaen. (Cisco Press 2003, 373.)

Osoitteenmuunnoksista on olemassa muunlaisiakin sovelluksia, mutta niiden perusperiaate on samankaltainen. Erilaiset osoitemuunnostekniikat ovatkin nykyisellään yleisesti käytetty menetelmä, joka toisaalta on vähentänyt julkisten IP-osoitteiden tarvetta organisaatioissa, mutta myös lisännyt tietoturvaa ja helpottanut verkkojen suunnittelua.

4 IPv6

4.1 Kehitys ja ominaisuudet

IPv6 on uusi versio IP-protokollasta, jonka on määrä ratkaista vanhaan IPv4:ään liittyvät ongelmat. IPv4 on nykyisellään vanhentumassa erityisesti sen tuottaman IP-osoiteavaruuden loppumisen vuoksi. Erilaisten arvioitten mukaan IP-osoitteet, joita hallinnoivat esimerkiksi IANA ja Euroopassa RIPE NCC, ovat loppumassa seuraavien kahden vuoden kuluessa, jopa aikaisemmin. Tilannetta pahentaa erityisesti se, että Internetin käyttäjiä tulee jatkuvasti enemmän muun muassa Afrikan ja Aasian maista sekä uusien mobiilipäätelaitteiden kautta. IP-osoitteiden loppumisesta on esitetty arvioita jo 1980-luvulta lähtien, kun nykyinen Internet sai alkunsa ja tilanteeseen on ehditty varautua jo useampi vuosikymmen. Väliaikaisena ratkaisuna IPv4-osoiteavaruuden loppumista on pyritty hillitsemään muun muassa NAT-menetelmää käyttämällä, sekä kehittämällä protokollan aliverkotustapaa. Nämä menetelmät ovatkin hidastaneet osoiteavaruuden varaamisen tahtia. Osoiteavaruuden loppuminen on hidastumisesta huolimatta vääjäämättömästi edessä, ja uuteen versioon siirtyminen on tulevaisuudessa välttämätöntä ja väistämätöntä.

Uuden protokollan käyttöönottoon liittyy kuitenkin monenlaisia vaikeuksia ja kustannuksia, joiden vuoksi nykyisellään IPv6 ei ole vielä käytössä kovinkaan laajalti. Tilanne on huolestuttava, koska isot palveluntarjoajat eivät ole vielä ilmoittaneet, kuinka ja millä aikataululla IPv6 otetaan käyttöön. IPv6 tarjoaa uuden osoitteistuksen ja mobiili-IP-ominaisuuksien lisäksi parannuksia muun muassa tietoturvaan verrattuna aikaisempaan versioon ja sen avulla on mahdollista tarjota aivan uudenlaisia palveluita käyttäjille. Erityisesti reaaliaikaiset audio- ja videopalvelut, jotka vaativat resurssien varaamista verkosta, on huomioitu IPv6:ssa toisin kuin aikaisemmassa versiossa.

IPv6:n pohjana voidaan pitää useita erilaisia ratkaisumalleja, joita kehitettiin 1991 pidetyssä Internet Activities Boardin kokouksessa esitettyihin Internetin ongelmiin. Jo 1990-luvun alkupuolella oli selvää, että Internet tulisi kohtaamaan ongelmia, jotka vaatisivat muutoksia protokollatasolla tai jopa muutoksia koko Internetin hierarkiaan ja toteutukseen. Erityisenä ongelmana pidettiin sitä, että Internetin rakenne monimutkaistuu käyttäjämäärien ja verkkojen

lisääntyessä samalla, kun yhteys Internetiin voitaisiin saavuttaa lukuisten palveluntarjoajien ja yksityisverkkojen kautta. Selvää oli, että erityisesti IP-protokolla vaatisi päivityksiä. Lukuisiin tulevaisuuden uhkakuviin ehdotettiin monia eri ratkaisumalleja. Osassa ratkaisumalleista olisi hylätty koko TCP/IP-mallin ja siirrytty OSI-mallin mukaiseen protokollaperheeseen. Toisaalta myös TCP/IP-mallia haluttiin päivittää lisäämällä kerroksia käytettyyn malliin. Konkreettisista ratkaisumalleista tärkeinä voidaan pitää esitystä IPv7-protokollasta, joka esiteltiin vuonna 1993 RFC 1475:ssä ja CATNIP (RFC 1707) sekä SIPP-protokollaa (RFC 1710). Edellä mainituissa parannusehdotuksissa on lähdetty erilaisin menetelmin ratkaisemaan IPv4:n ongelmia muuan muassa laajentamalla osoitekenttää 64 bittiin, yksinkertaistamalla IP-kehysrakennetta, parantamalla optioiden käyttöä ja selkeyttämällä reititystä. On perusteltua sanoa, että näitä ratkaisumalleja yhdistämällä alettiin kehittää IPv6-protokollaa ja lopulta vuonna 1998 hyväksytty versio uudesta IPv6-protokollasta ja sen apuprotokollista julkaistiin. IPv6 on kuvattu muun muassa RFC:ssä numero 2373. (Loshin 1999, 57–68.) IPv6-protokolla on siis ratkaisumallina yli kymmenen vuotta vanha, joten voidaan pitää hämmästyttävänä sitä tosiasiaa, että IPv4 on yhä, ongelmistaan huolimatta, vallitseva standardi. Huomioitavaa on myös se, että Microsoft- ja Linux-käyttöjärjestelmät ovat jo pitkään tukeneet IPv6:n käyttöä samoin kuin suuri osa reititinmalleista.

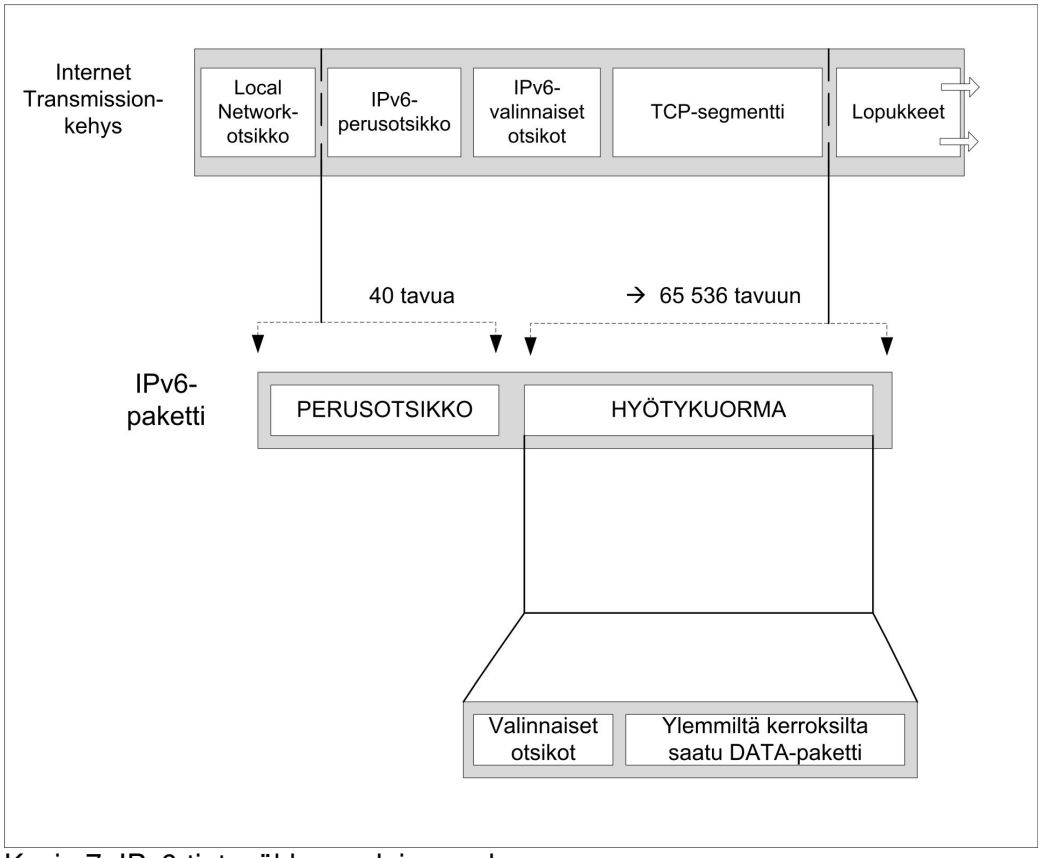
IPv6 on edeltäjänsä tavoin yhteydetön ja epäluotettava protokolla, eli se toimittaa IP-paketteja eteenpäin toisistaan riippumatta ja vailla virtuaalista yhteyttä vastaanottopäähän. IPv6:ssa on kuitenkin tehty merkittäviä parannuksia verrattuna IPv4:ään. Uudistukset voidaan jakaa viiteen eri osaan: laajennettu osoitteistus, joustava ja yksinkertaistettu otsikkorakenne, paranneltu optioiden ja laajennusten käyttö, vuontunnistus sekä identifiointi ja tietoturva. IPv6 tarjoaa myös ratkaisun Internetin laajentumisen myötä kasvaneiden reititystaulujen pienentämiseen sekä lisää automaattisen asetusmäärityksen ja uudelleennumeroinnin mahdollisuuksia. (Loshin 1999, 70–71.) Lisäksi IPv6 mahdollistaa entistä paremmin mobiilien tietoliikenneyhteyksien käyttämisen.

Uutta protokollaversiota voidaankin pitää maltillisena ratkaisuna, joka poistaa monia vanhan version ongelmia luoden samalla uuden joustavan protokollan, jonka käyttöiällä ei ole merkittäviä rajoitteita. Tässä työssä kuvataan ensin

IPv6-protokollan kehys- ja otsikkorakenne sekä siihen liittyvät uudistukset, jonka jälkeen esitellään uusi osoitteistus. Tietoturvanäkökulmat käsitellään näiden jälkeen. Kehysrakennetta tarkkailemalla ja vertailemalla sitä vanhaan IPv4-versioon, on helppo huomata uudistukset ja se, millä tavalla ne on tehty. Tämän vuoksi kehysrakenteen tarkastelu on perusteltua suorittaa ensimmäisenä.

4.2 Kehysrakenne ja otsikko

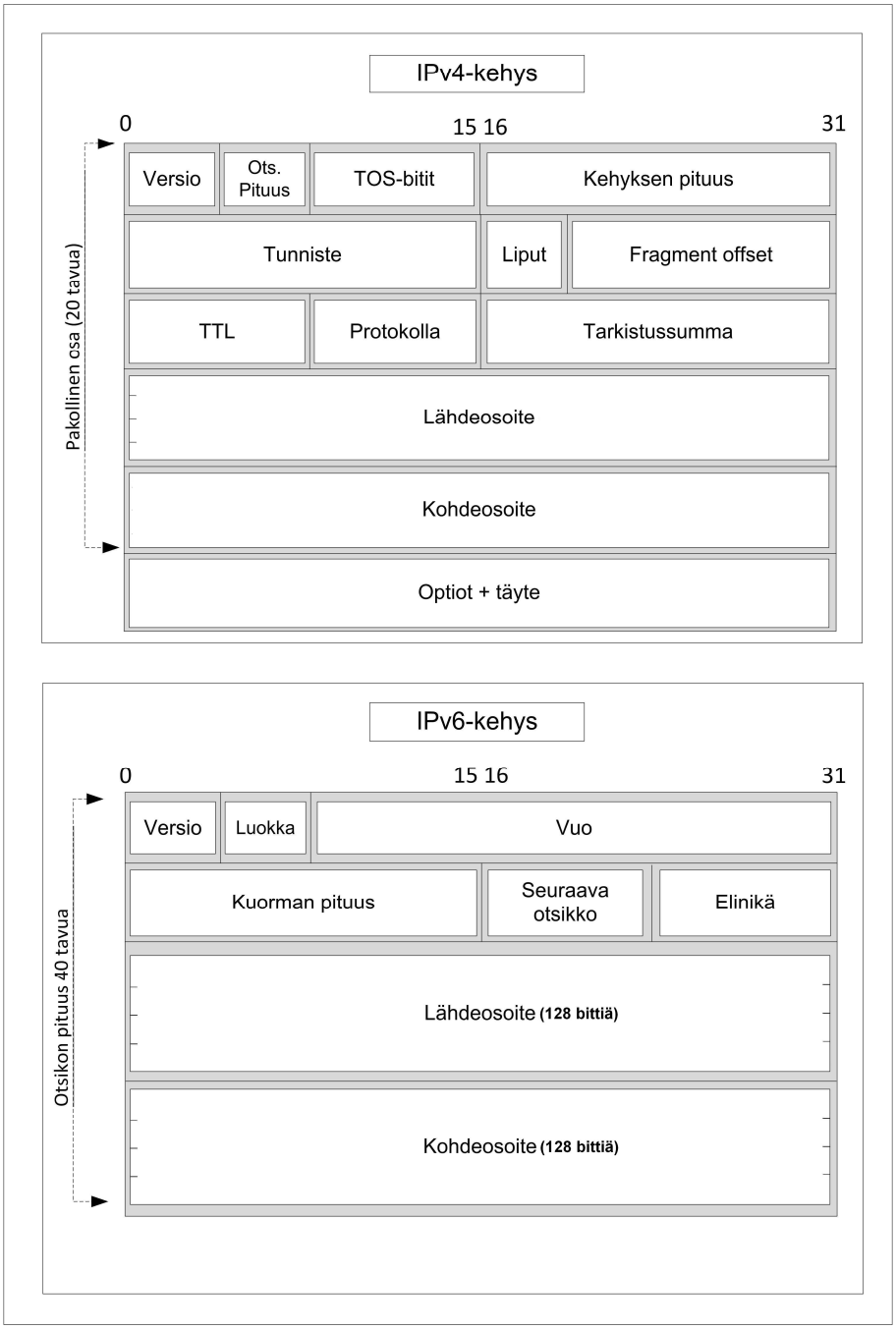
IPv6-kehysrakenteessa voidaan nähdä merkittäviä muutoksia ja parannuksia verrattuna IPv4-kehysrakenteeseen. Kehysrakenteessa otsikkoa on pyritty yksinkertaistamaan mutta tästä huolimatta on mahdollistettu uusien ominaisuuksien käyttöönotto. Lisäksi IPv6 muuttaa koko kehysrakennetta lisäämällä kehykseen perusotsikon lisäksi valinnaiset otsikot (Miller 2000, 30.) Kuvio 7 esittelee IPv6-tietosähkeen yleisen rakenteen.



Kuvio 7. IPv6-tietosähkeen yleinen rakenne

Jakamalla otsikkorakenne kahteen osaan on mahdollistettu toisaalta peruspakettien kohdalla yksinkertainen otsikkorakenne ja toisaalta valinnaisten otsikoiden avulla monimutkaisempien pakettien vaatimat ominaisuudet. Rakenteessa ainoastaan perusotsikko on pakollinen. Perusotsikon yksinkertais-

taminen näkyy jo otsikon pituudesta, joka on määritelty kiinteästi 40 tavuun. Vanha IPv4-otsikko on 20–60 tavua pitkä, jolloin vaihteleva pituus vaatii ylemmän tason protokollilta ylimääräisiä toimia, esimerkiksi otsikon ja data-osuuden pituuden selvittämiseksi. Uudessa versiossa kiinteästi määritelty otsikon pituus poistaa turhat tarkistukset ja niitä varten asetetut otsikkokentät. (Loshin 1999, 71–72.) Muutos tarkoittaa myös sitä, että IPv6 toimii 64-bittisen arkkitehtuurin sisällä, jolloin käyttö 64-bittisessä ympäristössä on optimaalinen (Kaario 2002, 109). IPv4-otsikko ja IPv6-otsikko kuvataan kuviossa 8, josta voidaan huomata otsikkokenttien muutokset.



Kuvio 8. IPv4-otsikko ja IPv6-otsikko (ks. Kaario 2002, 110)

IPv6-otsikossa on käytössä vain kahdeksan kenttää. Muutos IPv4-otsikkoon on merkittävä, koska vanhan version kahdestatoista kentästä on näin pystytty poistamaan neljä kenttää. Kenttien vähäisempi määrä helpottaa ja nopeuttaa IP-pakettien reitittämistä, koska läpikäytäviä kenttiä on vähemmän. Syyt kenttien poistamiseen ja tehokkuuden parantamiseen ovat yksinkertaiset. Koska IPv6-otsikon pituus on määritelty kiinteästi 40 tavuun, ei otsikon ja dataosuuden erottamiseksi enää tarvita Otsikon pituus -kenttää. Toinen muutos liittyy IP-pakettien fragmentointiin. IPv4 mahdollisti pakettien fragmentoinnin, missä tahansa verkon solmupisteessä. Fragmentointi on mahdollista IPv6:ssa vain verkon reunalla ja ainoastaan lähettäjän toimesta. Välittävät solmupisteet eivät siis enää voi fragmentoida pakettia. Tämän ominaisuuden ansiosta otsikosta voidaan poistaa useita kenttiä. Lisäksi otsikosta on poistettu Tarkistussumma-kenttä, jonka merkitys luotettavuuden kannalta todettu turhaksi, koska luotettavuuden takaavat ylemmissä kerroksissa toimivat protokollat kuten TCP ja UDP. (Loshin 1999, 71–72.) Näillä muutoksilla IPv6-otsikkorakenne muodostuu siis kahdeksasta pakollisesta kentästä.

Neljän bitin pituinen Versio-kenttä ilmoittaa käytetyn protokollaversion numeron ja saa arvon 6. Versionumeron avulla paketti ohjautuu oikeaan protokollan prosessoitavaksi. Seuraava kenttä on kahdeksan bitin pituinen Luokka-kenttä, ja sen avulla päätelaitteet ja välittävät reitittimet tunnistavat ja erottelevat luokkia ja prioriteetteja IPv6-paketeista. Luokka-kentän voidaan katsoa vastaavan IPv4-otsikon TOS-kenttää, mutta sen toimintaa on paranneltu ja tarkennettu. Kentän avulla voitaisiin esimerkiksi organisaation sisällä priorisoida jostakin sovelluksesta tai lähdepisteestä lähtöisin oleva liikenne ja taata näin paras mahdollinen yhteys halutulle liikenteelle. (Loshin 1999, 83–84; Miller 2000, 37–51.)

Vuo-kenttä liittyy myös erikoisia palveluja vaativien pakettien reitittämiseen ja erityisesti verkkoresurssien varaamiseen näille paketeille. Kentän avulla on mahdollista tunnistaa ja eriyttää tietoliikenteestä tietty vuo sellaiselle liikenteelle, joka vaatii tiettyjä erityisiä välityspalveluja. Vuo toimii ikään kuin takuuna tietystä palvelutasosta verkon läpi. Vuon tunnistus tapahtuu Vuo-kentän tietojen ja kohdeosoitteen avulla. Esimerkkinä vuon käytöstä voitaisiin pitää videokuvan lähettämistä verkossa kahden päätelaitteen välillä. Nämä kaksi

päätelaitetta voisivat muodostaa välilleen vuon, joka täyttää esimerkiksi viive- ja kaistanleveysvaatimukset. Toisaalta organisaatiossa voitaisiin varata vuo tietyille tiedonsiirtoa vaativille sovelluksille, joiden toimintaa määrittelevät tietyt reunaehdot. Luokka- ja Vuo-kenttä toimivat esimerkkinä siitä, kuinka IPv6 mahdollistaa entistä paremmin mahdollisuudet tarkentaa IP-paketteihin kohdistuvaa palvelua. Erityisesti Vuo-kenttä mahdollistaa reaaliaikaiset audio- ja videopalvelut, jotka vaativat verkkoresurssien varaamista. Näillä muutoksilla on myös korvattu osa IPv4:n käyttämistä optiokentistä, joiden käyttö ei ollut kovinkaan yleistä. (Comer 2002, 603–605; Miller 2000, 31–35; Wegner–Rockell, 2000, 420–421.)

Seuraava kenttä IPv6-otsikossa on Kuorman pituus -kenttä, jossa ilmoitetaan, kuinka monta oktettia kuormaa sähkeessä on. Kuorman maksimimäärä paketissa on yleisesti 65 535 oktettia dataa ja tähän dataan lasketaan mukaan mahdolliset valinnaiset otsikot ja ylemmän tason protokolla-paketit. Kuorman määrä voi myös ylittää edellä mainitun maksimimäärän jolloin datan määrä määritellään valinnaisessa otsikossa. Seuraava otsikko -kentälle on varattu seuraavat kahdeksan bittiä. Kenttä ilmoittaa, minkä tyyppinen otsikko on IP-paketissa välittömästi perusotsikon jälkeen. IPv6 mahdollistaa valinnaisten otsikoiden ketjuttamisen, jolloin Seuraava otsikko -kenttä ilmoittaa aina ketjussa seuraavana olevan otsikon tyypin. Valinnaisia otsikoita ketjuttamalla saadaan IP-pakettiin erityisiä ominaisuuksia, ja ne mahdollistavat muun muassa fragmentoinnin, välietappireitityksen sekä erilaiset tietoturvaominaisuudet. Valinnaiset otsikot takaavat siis sen, että erityisiä toimia vaativat paketit pystytään kuljettamaan kuten tavalliset paketit ja huolehtimaan samalla niiden erityistarpeista. Toisaalta ominaisuudet voidaan ottaa käyttöön vain tarvittaessa. Näin IPv6 toimii tehokkaammin ja tarkoituksenmukaisemmin. (Loshin 1999, 83–84; Miller 2000, 37–51.)

Valinnaisten osoitteiden järjestys on määrätty erikseen. Valinnaisia otsikoita ovat muun muassa Etappi-otsikko, jonka avulla voidaan ottaa käyttöön yli 65 535 oktettia dataa käsittävät IP-paketit, ja toisaalta ilmoittaa virhesanoma, jos verkko ei pysty tällaista eteenpäin toimittamaan. Toinen valinnainen otsikko on Reititys-otsikko, jonka avulla voidaan muun muassa määritellä erityisiä välietappeja IP-paketin kuljetukselle. Kolmas valinnainen otsikko on

Lohkomis-otsikko, joka puolestaan mahdollistaa pakettien fragmentoinnin eli IP-pakettien pilkkomisen pienempiin osiin verkon niin vaatiessa. Lisäksi valinnaisia otsikoita ovat esimerkiksi: Destination Options Header, Tunnistusotsikko, ESP-otsikko ja Destination Options Header. Lisäotsikoiden toiminnallisuuksia on käytössä suhteellisen vähän verrattuna niiden kykyyn määrittää erityisiä palveluja. Valinnaiset otsikot voidaankin nähdä erittäin potentiaalisena laajennusmahdollisuutena IPv6:een. (Loshin 1999, 83–84; Miller 2000, 37–51.)

IPv6-otsikossa seuraava kenttä on kahdeksan bitin Elinikä-kenttä, jolla on korvattu vanhan version Time To Live -kenttä. Periaate on edelleen sama eli kentän avulla pyritään rajaamaan IP-paketin elinikää verkossa ja välttämään verkossa ikuisesti kiertävät paketit. Elinikä-kenttä määrittää tietyn määrän siirtymiä reitittimestä toiseen ja jokaisen reitittimen jälkeen laskuri vähenee. Jos laskuri laskee nollaan, IP-paketti hylätään ja lähetetään virheviesti. Muutos edelliseen versioon on aikaan perustuvan laskurin hylkääminen. Viimeiset kentät IPv6-otsikossa ovat lähde- ja kohdeosoitekentät, jotka ovat 128-bittiä pitkiä ja joita voidaan pitää merkittävänä parannuksena vanhaan versioon. Lisäksi kohdeosoite ei enää yksiselitteisesti tarkoita lopullista päämäärää vaan lopullista osoitetta voidaan muuttaa valinnaisella Reititysotsikolla. (Miller 2002, 37–38) Laajennetut osoitekentät synnyttävät IPv6-osoiteavaruuden, jonka voidaan katsoa olevan riittävä tunnetussa tulevaisuudessa. Yhteenvetona voidaan sanoa, että IPv6-otsikkorakenne tarjoaa kasvatettujen osoitekenttien lisäksi myös muita parannuksia, joiden avulla protokolla on joustava ja suorituskykyinen, mutta silti kevyt toiminnaltaan.

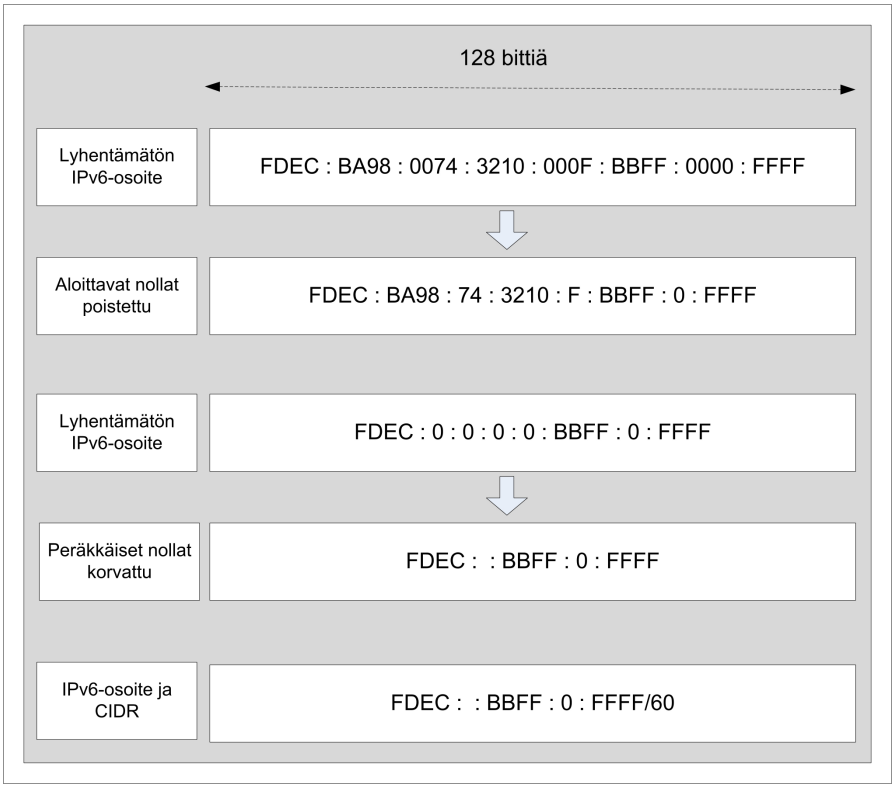
4.3 Osoitteistus

IPv6 tarjoaa 128 bittisen osoitteistuksen, jota voidaan pitää merkittävänä laajennuksena aikaisempaan 32-bittiseen osoitteistukseen. Uusittu osoiterakenne antaa osoiteavaruuden, jonka teoreettinen koko on 2^{128} ainutkertaista osoitetta. Voidaan todeta, että osoitteiden määrä on sellainen, että se täyttää nykyisenkaltaisen Internetin tarpeet tulevaisuudessakin moninkertaisesti. Osoiteavaruuden kasvattamisessa ei ole kuitenkaan ollut itsetarkoituksena ainoastaan ainutkertaisten osoitteiden määrän maksimoiminen vaan IPv6-osoitteistus mahdollistaa myös uudenlaisen osoitehierarkian, joka helpottaa

osoitteiden jakamista, reititysprosesseja ja myös mahdollistaa uudenlaisen tyyppiluokittelun.

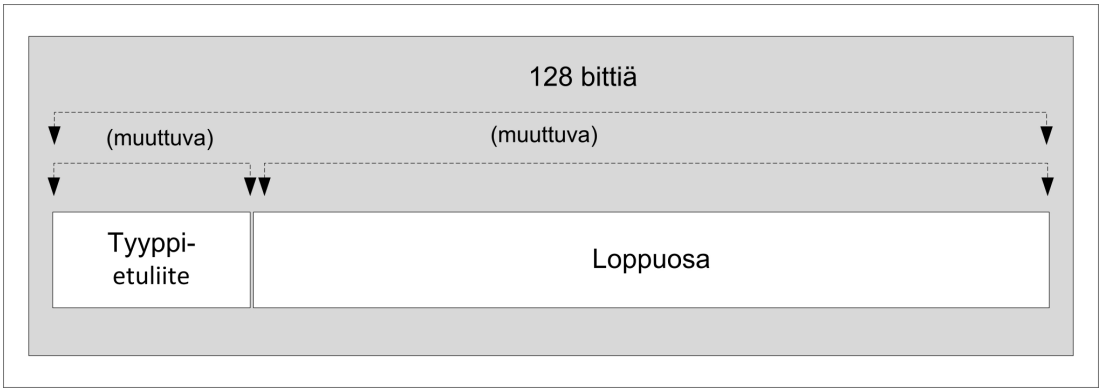
Aikaisempaan verrattuna voidaan sanoa IPv4-osoitteistuksen toimivan kahdella tasolla: verkkotasolla ja laitetasolla. IPv6 puolestaan mahdollistaa hierarkian, jossa osoitetyypit, rekisteröintivirasto, operaattori, tilaaja, verkko ja laitteet luovat monitasoisen kokonaisuuden. Tällä saavutetaan parempi osoiteavaruuden hallinta ja osoitteiden tunnistus kuin vanhassa IP-versiossa. Uusittu osoiterakenne tarjoaa siis kasvaneen osoitemäärän lisäksi myös uusittua toiminnallisuutta ja on täten kokonaisvaltainen ratkaisu.

IPv6-osoitteiden muoto on myös uudistunut. IPv4:ssä 32-bittinen IP-osoite ilmaistiin neljällä kahdeksan bitin muodostamalla kokonaisluvulla. Nämä luvut erotetaan toisistaan pisteellä, jolloin osoitteet saavat muodon n.n.n.n, missä n edustaa kokonaislukua. IPv6-osoitteet ovat 128-bittiä pitkiä ja ne jaetaan kahdeksaan 16 bitin heksadesimaalilukuun. Nämä heksadesimaaliluvut erotetaan toisistaan kaksoispisteellä. Osoite saa tällöin muodon x:x:x:x:x:x:x:x, jossa jokainen x edustaa heksadesimaalilukua. Koska osoite on jaettu kahdeksaan osaan, ja jokainen osa on 2 tavua pitkä, muodostuu lopullinen osoite 32 erillisestä heksadesimaaliluvusta. Verrattuna aikaisempaan muotoonsa IPv6-osoitteet näyttävät monimutkaisemmilta ja ovat vaikeasti muistettavampia. Notaatioon on kuitenkin olemassa tiettyjä helpotuksia. Koska osoitteet ovat pitkiä ja monet luvut ovat nollia, on sovittu, että osoitetta voidaan lyhentää. Kaksoispisteen jälkeen luvusta voidaan poistaa kaikki nollat, jotka sijaitsevat ennen muita numeroita. Tämän lisäksi IPv6-osoitteissa olevat pitkät nollasarjat voidaan merkitä kahdella peräkkäisellä kaksoispisteellä. Tätä kaksoispiste-merkintää saa käyttää kuitenkin vain kerran. (Forouzan 2006, 690–691; Kaario 2002, 111–112; Miller 2000, 69–70.) Näiden lyhennysten jälkeen IPv6-osoitteet saavat hieman selkeämmän muodon. Kuvio 9 esittelee IPv6-osoitteen alkuperäisen muodon ja siihen tehtävät mahdolliset lyhennykset.



Kuvio 9. IPv6-osoitenotaatiot

IPv6-osoitteen rakenne on tekijä, joka mahdollistaa uudenlaisen, moniulotteisemman hierarkiarakenteen kuin IPv4:ssä. Siinä missä IPv4-osoite muodostui verkko- ja laiteosasta, IPv6-osoite muodostuu Tyyppi-etuliitteestä ja loppuosasta. Tyyppi-etuliite on vaihtuvanpituinen ja määrittelee osoitteen käyttötarkoituksen. Etuliitteen muodostavat koodit (bittijonot) on määritelty ja osoiteavaruus on jaoteltu näiden koodien ja käyttötarkoituksien mukaan. Tyyppikoodit ovat ainutlaatuisia ja näin ollen etuliitteestä on helppo nähdä osoitteen käyttötarkoitus. (Forouzan 2006, 692–693.) Kuvio 10 esittelee IPv6-osoitteen perusrakenteen.



Kuvio 10. IPv6-osoitteen perusrakenne (ks. Forouzan 2006, 692)

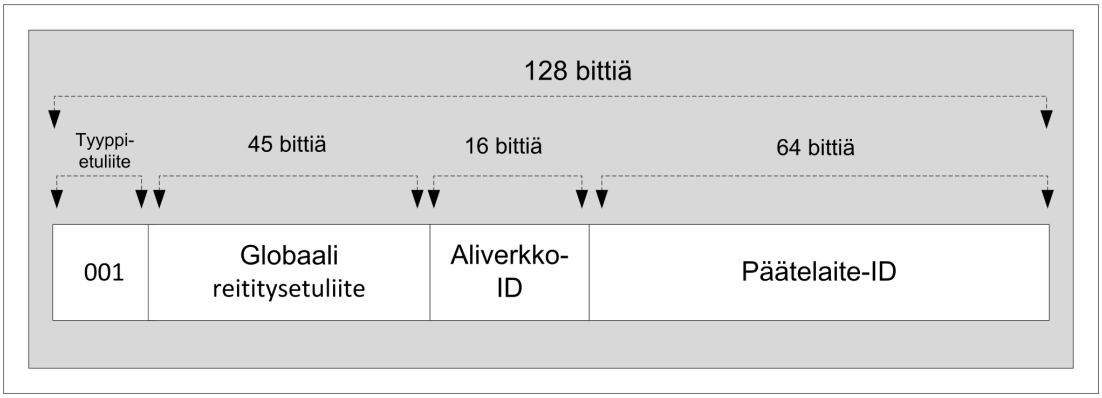
IPv6-osoitteista voidaan erotella kolme pääosoitetyyppiä: Unicast, Anycast ja Multicast. Unicast-osoitteella määritellään yksittäinen päätelaite, ja Unicast-osoitteella varustettu paketti toimitetaan aina kyseisellä osoitteella varustettuun päätelaitteeseen. Anycast-osoitteella määritellään tietty ryhmä solmulaitteita tai päätelaitteita, joiden osoitteessa on sama osoite-etuliite. Esimerkkinä voitaisiin nähdä joukko tietyn palveluntarjoajan reitittimiä, jotka ovat samassa fyysisessä verkossa ja joilla on sama osoite-etuliite. Anycast-osoitteella varustettu paketti toimitetaan vain yhteen reitittimeen, yleensä lähimpänä olevaan. Käyttökohteena Anycast-osoitteille voitaisiin myös nähdä tiettyyn aliverkkoon kuuluvat reitittimet tai tiettyyn reititysalueeseen kulkuväylän tarjoavat reitittimet. Multicast-osoite määrittelee tietyn ryhmän ja tähän osoitteeseen lähetetyt paketit toimitetaan kaikille ryhmän jäsenille. Edellä esitettyjen osoitetyyppien lisäksi on määritelty joukko erikoisempia osoitteita, joiden käyttötarkoitukset esitellään myöhemmin. (Forouzan 2006, 690–694; Wegner-Rockwell 2000 370–376.)

Taulukko 7 esittelee IPv6-osoitteiden tyypit ja Tyyppi-etuliitteet sekä määrittelee, mikä osuus osoiteavaruudesta on varattu tietylle osoitetyypille tai käyttötarkoitukselle. Huomattavaa on, että varsin suuri osa osoiteavaruudesta on varattu tulevaisuudelle ja uusille, vielä määrittelemättömille, käyttötarkoituksille.

Taulukko 7. IPv6-osoiteavaruuden jako (IANA 2010)

IPv6-etuliite	Allokointi	IPv6-etuliite	Allokointi
0000::/8	Varattu IETF	A000::/3	Varattu IETF
0100::/8	Varattu IETF	C000::/3	Varattu IETF
0200::/7	Varattu IETF	E000::/4	Varattu IETF
0400::/6	Varattu IETF	F000::/5	Varattu IETF
0800::/5	Varattu IETF	F800::/6	Varattu IETF
1000::/4	Varattu IETF	FC00::/7	Unique Local Unicast -osoitteet
2000::/3	Globaali Unicast -osoitteet	FE00::/9	Varattu IETF
4000::/3	Varattu IETF	FE80::/10	Link Local Unicast -osoitteet
6000::/3	Varattu IETF	FEC0::/10	Varattu IETF
8000::/3	Varattu IETF	FF00::/8	Multicast-osoitteet

Globaali Unicast -osoitteiden voidaan katsoa olevan peruskäyttäjien ja palveluntarjoajien kannalta tärkeimpiä osoitetyyppejä. Käytännössä nämä osoitteet edustavat myös IPv6-osoitteistuksen uudenlaista hierarkiaa, koska osoitteesta voidaan erotella myös eri tasot: tyyppi, globaali reititysetuliite, aliverkko ja päätelaite-ID. Globaali reititysetuliite on tyypillisesti hierarkkisesti rakentuva etuliite, joka muodostuu rekisteröintiviraston, palveluntarjoajan ja tilaajan toimesta (RFC 4291, 8). Päätelaite-ID voidaan määritellä eri tavoin riippuen onko käytössä esimerkiksi DHCP-palvelin. Globaali Unicast -osoitteen rakenne on esitelty kuviossa 11.



Kuvio 11. Globaali Unicast -osoitteen rakenne (RFC 3587)

Globaalin Unicast -osoitteen rakennetta tarkkailemalla voidaan siis varsin nopeasti erotella erilaiset hierarkkiset ulottuvuudet. Reititys puolestaan helpottuu ja reititystaulujen koko ei kasva tarpeettomasti, koska paketin toimittamiseen tarvittavat tiedot voidaan tarkemman hierarkiarakenteen avulla määritellä paremmin. Globaali Unicast -osoitteille on varattu IPv6-osoiteavaruudesta heksadesimaali-etuliitteellä 2000::/3 merkitty osoiteavaruus (IANA 2010). Tämä osoiteavaruus puolestaan on jaettu kansallisten osoitevirastojen hallintaan, joista esimerkiksi palveluntarjoajat voivat hakea käyttöönsä osoiteavaruuksia (IANA 2008). Myös Anycast-osoitteet sijaitsevat tämän osoiteavaruuden sisällä, koska Anycast-osoitteita ei ole määritelty erillisellä Tyyppi-etuliitteellä. Anycast-paketit tunnistetaan yleisesti etsimällä pienin yhteinen tekijä määritellyistä osoitteista. Multicast-osoitteille on varattu oma osoiteavaruutensa, joka saa arvon FF00/8 (IANA 2010). Erikseen määritellyllä Multicast-osoiteavaruudella nopeutetaan tällaisia osoitteita sisältävien pakettien toimitus ja erotellaan ne Unicast-paketeista. IPv6-osoiterakenne siis mahdollistaa entistä nopeamman reitityksen lisäksi myös paremman

osoitteiden jakamisen, jolloin osoitteiden määrä saadaan entistä paremmin vastaamaan tarvetta, ja erilaisten virastojen toiminta osoitteidenjaossa helpottuu.

Unicast, Anycast ja Multicast-osoitteiden lisäksi IPv6 sisältää myös muita osoitteellisia toiminnallisuuksia. Osoiteavaruudesta on erikseen määrätty osa niin sanotuille Unique Local Unicast -osoitteille, jotka toiminnaltaan muistuttavat yksityisiä IPv4-osoitteita. Yleisesti voidaan sanoa, että Unique Local Unicast -osoitteita voitaisiin käyttää esimerkiksi yritysten sisäverkoissa tapahtuvan tietoliikenteen reititykseen. Näin ollen voitaisiin edelleen yksinkertaistaa ja nopeuttaa globaalin tietoliikenteen reititysprosesseja. Local Unicast -osoitteille on varattu IPv6-osoiteavaruudesta FC00/7-etuliitteellä koodattu osoiteavaruus (IANA 2010). Unique Local Unicast -osoitteiden rakenne poikkeaa normaaleista Unicast-osoitteista eikä niitä tämän vuoksi voida reitittää globaalisti. Sovellukset kuitenkin käsittelevät näitä osoitteita muiden IPv6-osoitteiden tavoin. Paikallisten Unicast-osoitteiden käytön etuna voidaan pitää sitä, että sisäisen verkon rakennetta voidaan muuttaa huolimatta siitä, minkälainen on ulospäin näkyvä rakenne. Tämä säästää osaltaan kustannuksia ja toisaalta tekee reititysrakenteesta yksinkertaisemman ylläpitää. Haittapuolena voidaan pitää globaalin reititysmahdollisuuden puutetta ja tiettyjä suunnitelmallisia ratkaisuja Unique Local Unicast -osoitteen rakenteessa.

Toinen osoitteellinen ja toiminnallinen uusi ominaisuus IPv6-osoitteistuksessa on niin sanottu Link-Local Unicast -osoite, jolle on määritelty osoiteavaruudesta FE80/10-etuliitttellä koodattu osoitetila. Tämän osoiteryhmän on tarkoitus olla nimensä mukaisesti linkkikohtainen osoite, jota käytetään lähinnä automaattiseen asetustenmäärittelyyn, naapurireitittimien välisen yhteyden solmimiseen sekä silloin, kun reitittimiä ei ole käytössä. (Miller 2000, 82.) Edellä mainittujen osoitteiden lisäksi IPv6:ssa on määrittelyt myös Unspesified address - ja Loopback adress -osoitteille sekä IPv4-yhteensopiville osoitteille. Ensin mainittujen osoitteiden toiminnallisuus liittyy lähinnä testaukseen ja automaattiseen asetustenmäärittelyyn. IPv4-yhteensopivat osoitteet puolestaan on suunniteltu käytettäväksi siirtymävaiheen ajan. (Forouzan 2006,694.)

Kokonaisuutena IPv6-osoitteistus ja uusittu osoiterakenne tarjoaa joustavan ratkaisun, joka verrattuna aikaisempaan järjestelmään antaa käyttöön aivan uudenlaisia toiminnallisuuksia ja käyttötapoja kuitenkin niin, että perustoiminnot ja erityisesti reititys tapahtuvat nopeasti. IPv6-osoitteistuksen lisäarvona voidaan myös pitää sitä, että sen kapasiteetista on käytetty vasta hyvin pieni osa. Tämä tarjoaa mahdollisuuden laajentaa käyttötapoja ja osoitteistusta vielä entisestään, kun tarvetta ilmenee.

4.4 Tietoturva

IPv6:een siirtymiseen on useita syitä, ja sen uudet ominaisuudet tekevät siitä varsin monipuolisen ja kestävän protokollan. Yksi nykyajan tietoliikenteen isoimpia haasteita ovat erilaiset tietoturvaan liittyvät kysymykset. IPv6 tarjoaa edeltäjäänsä verrattuna myös tällä osa-alueella muutoksia ja tiettyjä parannuksia, joiden katsotaan paremmin vastaavan nykyisen kaltaisen tietoliikenteen haasteisiin. On kuitenkin syytä huomata, että IPv6 ei ole myöskään täysin aukoton tai turvallinen protokolla vaan sisältää uusia uhkia ja ongelmia, joiden ratkaisemiseksi vaaditaan protokollan jatkokehittelyä tai muunlaisia tietoturvatoimia. Tietoturvaan liittyy olennaisena osana erilaisten salausalgoritmien toiminta, ja niiden matemaattinen perusta. Tämän työn puitteissa ei kuitenkaan käsitellä salauksen teoreettista taustaa vaan lähinnä erilaisia käytännön toteutuksia ja tapoja, joita IPv6:ssa käytetään.

IPv4 on tietoturvan kannalta monella tapaa ongelmallinen. Peruslähtökohdiltaan IPv4 ei ota kantaa salaukseen, koska se katsoo, että ylemmillä kerroksella toimivat sovellukset esimerkiksi sähköposti, vastaavat itse datan salauksesta ja käyttäjätunnistuksesta. Tämä toimintamalli liittyy IPv4 *end-to-end*-malliseen historialliseen ajatteluun, jossa verkossa olevat käyttäjämäärät olivat pieniä ja käyttäjät tiedettiin turvallisiksi. Turvallisuus voitiin näin ollen jättää vain päätelaitteilla toimivien sovelluksien huolehdittavaksi. Nykyisen kaltaisessa Internetissä ja tietoverkoissa yleensä tällainen malli ei enää toimi, vaan tietoturvasta täytyy huolehtia myös IP-pakettien osalta. (Sotillo 2006, 1.)

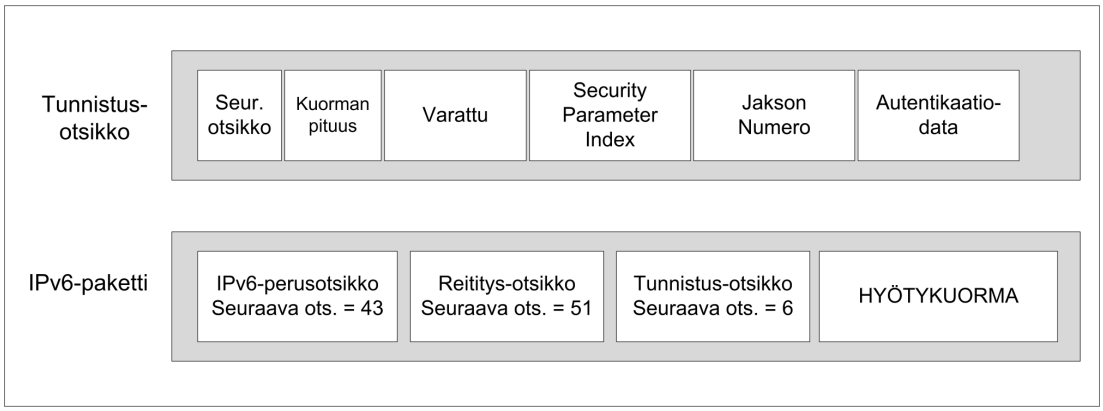
IPv4:n rakenne mahdollistaa myös itsessään tietynlaiset väärinkäytökset. Erityisen ongelmallisena voidaan pitää IPv4-osoitetta, jonka koko mahdollistaa tietoliikenneporttien kuuntelun ja haavoittuvien kohtien selvittämisen mel-

ko nopeasti. Esimerkiksi normaalin IPv4-aliverkon ja sen osoiteavaruuden läpikäyminen kestää vain muutamia sekunteja. Vastaava toiminto IPv6-osoitteilla ja niiden luomilla osoiteavaruuksilla voi olla useita vuosia. (Cisco Systems Inc. 2006, 8-9; Sotillo 2006, 6.) IPv4:ssä on edellä mainittujen ongelmien lisäksi myös muita tietoturvaan liittyviä näkökulmia, joiden vuoksi sitä voidaan pitää vanhentuneena ja jopa lähtökohtaisesti soveltumattomana nykyisenkaltaiseen tietoliikenteeseen.

IPv6:n suunnittelussa on otettu huomioon myös tietoturvaominaisuudet. Tehdyt muutokset ovat osaksi rakenteellisia ja liittyvät erityisesti osoitteiden kokoon ja kehysrakenteeseen. Yksi lähtökohtainen parannus IPv4:ään verrattuna on se, että IPv6 vaatii IPsec-protokollan käyttöönoton jokaisessa solmupisteessä. IPv4:ssä kyseessä olevan protokollan käyttö oli valinnainen toiminto. IPv6:n tietoturvaominaisuudet lepäävätkin pitkälti IPsec-protokollan varassa. IPsec ei ole yksittäinen tiukasti määritelty protokolla vaan erilaisia määrityksiä sisältävä protokollakokoelma, joka antaa käyttöön eri suojausprotokollia ja niiden joustavia käyttöönottotapoja. IPsec:in avulla voidaan helposti määritellä sopiva suojaustaso ja -tapa käyttökohteen mukaan. IPsecin avulla voidaan ottaa käyttöön kaksi tietoturvaominaisuutta: laillisuustarkistus (engl. authentication) ja salakirjoitus (engl. encryption). Nämä ominaisuudet otetaan käyttöön erikseen määritellyillä otsikoilla, jotka lisätään IPv6-tietosähkeeseen. IPsec:in toiminta mahdollistaa sovelluskohtaisen ja epäsymmetrisen käytön, jolloin sovellus voi määritellä kumpaa toimintoa käyttää ja vaaditaanko kummaltakin osapuolelta samojen toiminnallisuuksien käyttämistä. (Comer 2002, 584; Loshin 1999, 156–157.)

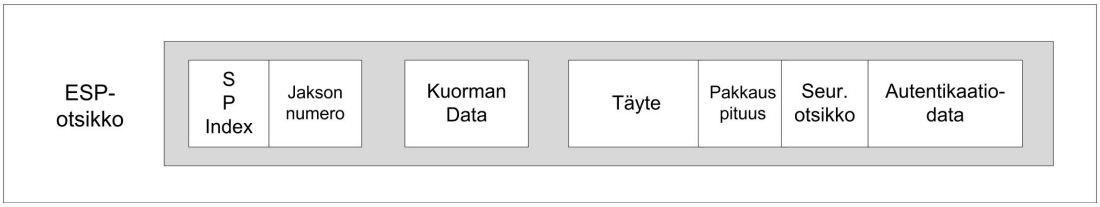
IPsec suorittaa laillisuustarkistuksen niin sanotun Tunnistus-otsikon avulla (*engl. Authentication Header*). Pääpiirteittäin laillisuustarkistuksen avulla on mahdollista estää IP-paketin sisältöön kajoaminen tai sen muuttaminen matkalla päätelaitteesta toiseen. Lisäksi Tunnistus-otsikon avulla on mahdollista estää pakettien uudelleenlähettämiseen perustuvat *replay*-hyökkäykset. IPv6:n myötä jouduttiin Tunnistus-otsikon toimintaa päivittämään, koska IPv6-paketti sisältää tietoja, jotka saattavat muuttua matkalla. Tämän vuoksi Tunnistus-otsikko tarkistaa vain ne kentät, jotka on lähtökohtaisesti määritelty muuttumattomiksi. IPv6:n joustava otsikkorakenne mahdollistaa Tunnistus-

otsikon liittämisen suoraan IP-pakettiin. (Comer 2002, 584–586; Sotillo 2006, 3–4.) Kuvio 12 esittelee Tunnistus-otsikon rakenteen ja liittämisen IPv6-pakettiin.



Kuvio 12. Tunnistus-otsikon rakenne ja Tunnistus-otsikko IPv6-paketissa (Sotillo 2006, 4)

Salakirjoitus otetaan käyttöön Encapsulating Security Payload-protokollalla (ESP), joka on toiminnaltaan monimutkaisempi kuin Tunnistus-otsikko. ESP tarjoaa osin samat toiminnallisuudet kuin Tunnistus-otsikko, mutta huolehtii lisäksi myös IP-pakettien luotettavuudesta salauksen yhteydessä ja datan alkuperän todentamisesta julkiseen avaimeen perustuvan salaamisen avulla. Toiminnallisuus toteutetaan Tunnistus-otsikon tavoin erillisellä ESP-otsikolla, joka liitetään IP-pakettiin. Tunnistus-otsikosta poiketen ESP-otsikon avulla on mahdollista suojata vain ne otsikkokentät, jotka tulevat sen jälkeen IP-paketissa. (Loshin 1999, 161–163; Sotillo 2006, 3-4.) Kuvio 13 kuvaa ESP-otsikon rakenteen.



Kuvio 13. ESP-otsikon rakenne (Sotillo 2006, 4)

IPsecin toimintaan kuuluu myös Internet Key Exchange-protokolla (IKE), jonka toiminta liittyy salausavainten lähettämiseen sekä eri salausalgoritmien sopimiseen ja neuvottelemiseen osapuolten välillä. IPsec:in tietoturva ominaisuuksia on kehitetty osin yhdessä IPv6:n kanssa, ja sen liittäminen uuteen

protokollaversioon onnistuu aikaisempaa paremmin. IPsecin lisäksi IPv6 version Neighbour Discovery -toiminnot ja automaattinen asetusten määrittely tekevät siitä edeltävää versiota turvallisemman. (Sotillo 2006, 4-5). IPv6 tuo kuitenkin mukanaan uusia mahdollisia tietoturvauhkia, joita pelkkä IPsec:in käyttöönotto ei välttämättä ratkaise.

IPv6:n uudet ominaisuudet vaativat erityistä tarkkuutta järjestelmänvalvojilta. Erityisesti asetusten määrittely tulee tehdä huolella ja niin, että tietoturva-aukkoja ei jää. Vaikka IPv6-osoitteiden koko estää tehokkaasti porttien ja osoitteiden skannauksen, ovat erilaiset *Flooding*-tyyppiset solmukohtien ylikuormittamiseen perustuvat väärinkäytökset mahdollisia. Erityisesti IPv6 Multicast -osoitteiden toiminnassa täytyy varmistaa, että niiden kautta tapahtuva liikenne rajoittuu vain tiettyihin verkkoihin tai niiden osiin. Julkisista verkoista tuleva Multicast-osoitteisiin tarkoitettu liikenne tulisi estää. Lisäksi IPv6-otsikkorakenne mahdollistaa uudella tavalla otsikoiden väärinkäytön. Väärinkäytösten avulla voitaisiin mahdollisesti ylikuormittaa tiettyjä verkon solmukohtia. Myös uusi mobiili-IP ominaisuus tuo tietoturvan kannalta uusia uhkia, joiden ratkaiseminen vaatii erityistä tarkkuutta järjestelmänvalvojilta. (Cisco Systems 2006; 1-30; Sotillo 2006, 5-6.)

Edellä mainittujen ongelmien lisäksi IPv6:n käyttöönotossa joudutaan kahden järjestelmän tilaan, jossa kaksi olemassa olevaa protokollaa, IPv6 ja IPv4, ovat käytössä samaan aikaan. Tämän siirtymäajan tietoturvaongelmat ovat erityisen suuria, koska tunnelointimenetelmät ovat alttiita hyökkäyksille. Kokonaisuutena IPv6 on tietoturvan kannalta vähintään yhtä haastava kuin vanhakin versio. Uuden protokollan käyttöönotto vaati uudenlaisia järjestelmänvalvontatoimia ja tuottaa erityisesti alussa haasteita. Uuden protokollan käyttöönotossa ei näin ollen voida täysin tuudittautua sen turvallisuuteen vaan tietoturvan ylläpitämiseksi täytyy tehdä vähintään samanlaisia tai jopa vahvempia toimia kuin IPv4:n kanssa.

5 IPv6:EEN SIIRTYMINEN

5.1 Tilanne Suomessa ja maailmalla

IPv4-osoiteavaruuden loppuminen on useimpien arvioiden mukaan käsillä muutaman vuoden sisällä (Hain 2010; Huston 2010). Korvaava protokolla IPv6 on ollut olemassa varovaisten arvioidenkin mukaan lähes kymmenen vuotta. Tämän lisäksi useimmat käyttöjärjestelmät, reitittimet, muut solmulaitteet ja reititysprotokollat ovat tukeneet IPv6:n käyttöä jo pitkään. Lukuisat laitevalmistajat ovat implementoineet laitteisiinsa IPv6-valmiuden ja ovat ilmoittaneet olevansa valmiit siirtymään tältä osin uuden protokollan käyttöön. Useat Internet-palveluntarjoajat puolestaan ovat varanneet IPv6-osoiteavaruuksia muun muassa RIPE NCC:ltä ja ilmoittavat tarjoavansa IPv6-palveluita. Näistä lähtökohdista voitaisiin sanoa, että siirtyminen IPv6-pohjaisiin verkkoihin vaikuttaisi olevan organisoitua ja tapahtuisi hyvissä ajoin ennen kuin IPv4-osoiteavaruus loppuu. Todellisuudessa tilanne on kuitenkin toinen ja voidaan jopa varauksellisesti sanoa, että IPv6-käyttöönotto on suurilta osin pahasti myöhässä.

Vaikka IPv6 on hiljalleen otettu käyttöön useissakin maissa, ovat sen käyttäjämäärät niin alhaiset, että varsinaisesta massasiirtymisestä on liian aikaista puhua. IPv6-valmiutta ja käyttöönottoastetta voidaan seurata usealla tavalla. Yksi tapa on seurata, kuinka monta toimijaa on hakenut osoiteblokkeja eri maiden RIR-rekistereistä. Määrien voidaan sanoa toistaiseksi olevan vähäisiä. USA:ssa osoiteblokkeja on haettu käyttöön n.1373, joka on vertailun suurin määrä. Euroopassa suurin määrä osoiteblokkeja on haettu Saksaan eli 363 kappaletta. Suomessa vastaava luku on 50. Ongelmallisin tilanne näyttäisi olevan erityisesti Aasiassa, jonka kasvaneet tietoverkkotarpeet voidaan ratkaista vain IPv6:n käyttöönotolla. Aasian alueella IPv6-osoiteblokkien varaus on toistaiseksi erittäin vähäinen. (IPv6 ACT NOW 2010.) Pelkkä osoiteblokkien varaaminen ei kuitenkaan ole suoraan verrannollinen siihen, kuinka paljon IPv6 on käytössä Internetissä. IPv6:n osuus Euroopan verkkoliikenteestä on arviolta yksi prosentti (CSC 2010). Vuonna 2009 tehdyssä ”IPv6 Deployment Monitoring Survey” –tutkimuksessa kartoitettiin IPv6-käyttöönoton todellista tilannetta RIPE:n alueella. Tutkimuksen mukaan valtaosa vastaajista kokee, että IPv6-verkkoliikenne on IPV4:ään verrattuna

merkityksetöntä (Botterman 2009). Todellisuudessa käyttöönotetut IPv6-osoitemäärät ovat siis vielä pienemmät kuin blokkien varaus antaa ymmärtää (IPv6 ACT NOW 2010). Tämä ilmiö näkyy myös Suomessa, jossa osoiteavaruuksia on varattu, mutta todellisten käyttäjien määrä on erittäin pieni.

Todellista käyttöönoton määrää voidaan tarkastella myös maakohtaisten suosituimpien Internet-sivustojen kautta. RIPE-alueen vuoden 2009 tutkimuksen mukaan vain yksi sivusto 27 maan 30 suosituimmasta sivustosta tuki IPv6:ta. (Botterman 2009.) Samalla tavalla tarkkailtuna tilanne näyttää huonolta myös Aasiassa, jossa vain pieni prosenttimäärä suosituimmasta sivustoista tukee IPv6:tta. Aasian tilanne on nurinkurinen, koska juuri Aasian alue tarvitsee eniten IPv6-käyttöönottoa kasvavana tietoliikennealueena. (Vyncke 2010.) IPv6:ta tukevien web-sivujen määrä kuitenkin kasvaa kaikkialla tasaisesti.

Viestintäviraston vuonna 2008 teettämän tutkimuksen mukaan vain pieni osa Suomen operaattoreista tarjoaa asiakkailleen IPv6-yhteyksiä. Valmiudet uuteen protokollaan siirtymiseen ovat kuitenkin olemassa usealla operaattorilla. Vaikka Viestintäviraston viimeisin kysely on vuodelta 2008, ei tilanteessa ole kuitenkaan nähty suurta muutosta viime vuosien aikana. Kyselystä käy ilmi, että osan operaattoreista on määrä siirtyä tarjoamaan IPv6-palveluita vuosien 2008–2010 aikana. (Viestintävirasto 2008.) Linjauksen toteutumisesta ei kuitenkaan ole varmuutta. Viestintävirasto teettää ajoittain tarkistuksia Suomen IPv6-tilanteesta ja viimeisimmän tarkistuksen mukaan tilanteessa ei ole tapahtunut merkittäviä muutoksia (Leppänen 2010).

IPv6:n käyttöönoton nopeuttamiseksi on kuitenkin tehty joitakin merkittäviä toimia. Euroopassa Euroopan Komissio on tehnyt linjauksia, joiden mukaan IPv6-käyttöönottoa pitää tukea muun muassa lisäämällä IPv6-koulutusta tekniikan alan koulutusohjelmissa sekä tietoliikennekurssein. Lisäksi suositellaan, että yritykset huomioisivat IPv6-asiat laitehankinnoissaan ja päivityksissä. Euroopan Komission linjauksen mukaan IPv6 tulisi olla käytössä 2011 mennessä, jolloin noin 25 % loppukäyttäjistä käyttäisi uutta protokollaa. Myös käytetyimpien web-sivustojen tulisi tarjota palvelujaan IPv6:n kautta. Komissio näkee IPv6:ssa myös uusien tietoteknisten innovaatioiden mahdollisuu-

den ja että sen nopea käyttöönotto edistäisi Euroopan alueen asemaa johtavana internetin kehittäjänä. Samanlaisia linjauksia on tehty myös OECD:n ministerineuvostossa ja Yhdysvalloissa. (CSC 2010.) Yhdysvalloissa liittovaltio on hiljattain antanut määräyksen, jonka mukaan kaikki liittovaltion Internettiin näkyvät palvelut, esimerkiksi sähköposti ja DNS, tulee päivittää IPv6-pohjaisiksi vuoteen 2012 mennessä. Seuraavassa vaiheessa kaikki virastojen verkoissa toimivat tietokoneet tulevat käyttämään IPv6:ta. Toinen vaihe on määrä olla valmis vuonna 2014. (Executive Office Of The President 2010)

5.2 Ongelmat

Kuten edellä on todettu, IPv6:een siirtyminen ei etene odotetun nopeasti vaan pikemminkin asenne on kauttaaltaan odottava. Vaikka käynnistäviä toimia on tehty aina valtiotasolta asti, tuntuvat operaattorit, laitevalmistajat ja muut alan toimijat yhä olevan epätietoisia siitä, miten IPv6-käyttöönotto todella aloitetaan. Mitkä ovat suurimmat syyt siihen käyttöönoton hitaaseen edistymiseen?

Viestintäviraston kysely suomalaisille Internet-operaattoreille keskittyy osaltaan näiden syiden selvittämiseen. Kyselyn yhteenvedon pohjalta voidaan todeta, että operaattorit eivät näe IPv6:ssa erityisiä tietoturvauhkia, jotka estäisivät käyttöönoton. Osa vastanneista korostaa kuitenkin, että uuden protokollan käyttöönotto edellyttää tarkkuutta tietoturva-asioissa. Käyttöönottoon ei siis näyttäisi liittyvän lisääntyneiden tietoturvauhkien pelko. Suurin osa kyselyyn vastanneista myös kokevat, että IPv6:sta on ollut saatavilla riittävästi tietoa vaikka muutama vastanneista ilmoittaakin, että kaipaisi tietoa muun muassa tarkasta IPv6-markkinatilanteesta operaattoreiden osalta. Kyselyn mukaan IPv6-käyttöönottoa pitäisi edistää muun muassa laitevalmistajien aktiivisemmalla toiminnalla, lisäämällä IPv6-kykyisten laitteiden tarjontaa ja henkilöstökoulutusta, operaattorien keskinäisellä aikataulutuksella, investointituilla ja IPv6-palveluiden kehittämisellä. (Viestintävirasto 2008.) Kyselyn tuloksista voitaisiin päätellä, että operaattorit ovat varsin odottavalla kannalla ja peräänkuuluttavat kannustavia toimia käyttöönoton edistämiseksi.

Vastaavanlainen kysely on suoritettu myös vuonna 2010 globaalisti RIR-alueiden palveluntarjoajille ja muille Internet-palveluja tarjoaville tai niitä tarvitseville organisaatioille. Kyselyn avulla on pyritty selvittämään IPv6:n käyttöönoton tasoa ja ongelmia globaalisti. Vuoden 2010 kyselyssä organisaatioista, jotka eivät vielä käytä IPv6:ta, yli 60 prosenttia kokee suurimmaksi esteeksi IPv6-käyttöönotolle siitä aiheutuvat kustannukset. Toiseksi suurin syy on osaavan henkilökunnan puute. Osaavan henkilökunnan puute koetaan isoksi ongelmaksi myös niissä organisaatioissa, joissa IPv6 on jo käytössä tai sitä harkitaan. Näissä organisaatioissa myös kauppiaiden tuen puute nähdään ongelmana. Vuoden 2010 kyselyssä suurimmaksi ongelmaksi IPv6-tuotteiden ja -palvelujen tuottamisessa nähdään kuluttajakysynnän puute sekä kokemuksen puute. Kun vuoden 2010 globaalia kyselyä verrataan vuonna 2009 tehtyyn RIPE-alueen kyselyyn, todetaan että asiakaskysyntä on hieman kasvanut vuoden aikana. Myös tietoisuus IPv6:n välttämättömyydestä on kasvanut samoin kuin käyttöönottojen ja suunnitelmien määrä. IPv6-liikenne ei kuitenkaan ole kasvanut. (Botterman 2010.)

Suurin IPv6-palvelujen lisääntymistä jarruttava tekijä tuntuu olevan niin sanottu kysynnän ja tarjonnan laki. IPv6-palveluille ei ole kysyntää, joten palveluntarjoajat eivät näe siinä mahdollisuutta kannattavaan liiketoimintaan. Tämän vuoksi palvelujen määrä on pieni. Kuluttajatietouden lisääminen IPv6-asioista saattaisi olla ratkaiseva tekijä, jolla käyttöönotto saataisiin todella liikkeelle. Monet tahot korostavat myös niin sanotun läpimurtosovelluksen merkitystä IPv6-implementoinnissa (CSC 2010; Botterman 2009). Tällaisen sovelluksen ilmaantuminen olisi varmasti tekijä, jonka myötä IPv6-palvelujen tarjonta lisääntyisi. Toisaalta IPv6:een siirtymisen ongelmina yritykset näkevät juuri palvelujentarjoajien ja kokemusten puuttumisen. Lisäksi IPv6-käyttöönottoa hidastaa osaavan henkilökunnan puute. Yksi jarruttava tekijä on IPv6:een siirtymisestä aiheutuvat kustannukset ja samalla se, että pakottavaa tarvetta ei koeta olevan niin kauan kuin IPv4-osoitteita on saatavilla.

IPv6-käyttöönottoon liittyvien ongelmien ratkaisemiseksi tehdään monia eri toimia. Tilanne vaatii kuitenkin sekä kuluttajatietouden lisäämistä ja ammattiosaajien kouluttamista, että tietoisia valtiotason toimia, joilla palveluntarjoajat saadaan siirtymään IPv6:een. Tulevaisuus näyttää, millä aikataululla

IPv6-käyttöönotto etenee eri puolella maailmaa. Ennakoiva siirtyminen helpottaisi käyttöönottoa monin tavoin ja äkkinäisesti tehtävät massasiirtymiset puolestaan pahentaisivat ongelmia.

6 IPv6:N KÄYTTÖÖNOTTO PK-YRITYKSESSÄ

6.1 Lähtökohdat

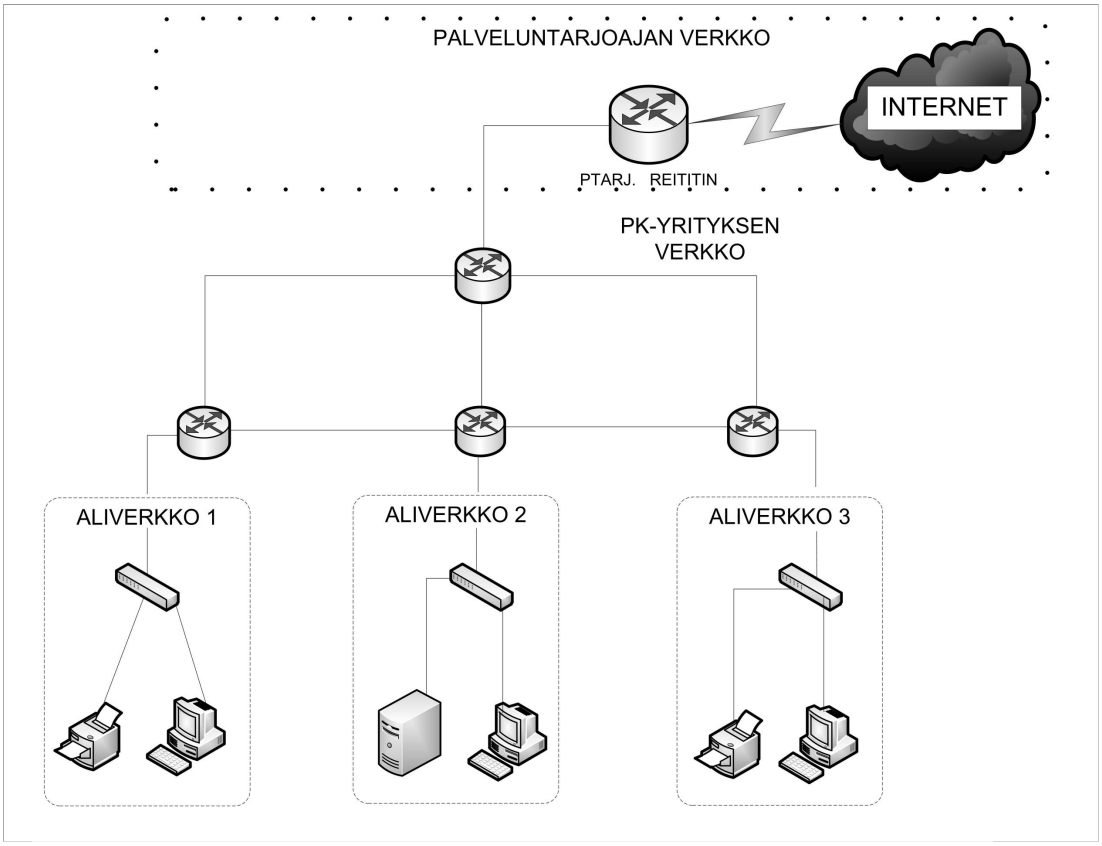
Kuten edellä on todettu, IPv6:een siirtyminen tapahtuu globaalissa mittakaavassa hitaasti ja on selvää, että uusi protokolla ja vanha IPv4-versio tulevat olemaan käytössä rinnan usean vuoden ajan. On kuitenkin syytä selvittää, minkälaisia käytännön toimenpiteitä IPv6:n käyttöönottoon liittyy. Tämän opinnäytetyön tarkoituksena on selvittää, kuinka IPv6 otetaan käyttöön PK-yritystä vastaavassa ympäristössä ja mitkä ovat käyttöönoton peruselementit sekä mahdolliset ongelmat. Olen valinnut PK-yrityksen käyttöönottoympäristöksi, koska mielestäni juuri PK-yrityksille siirtyminen voi tuottaa ongelmia muun muassa osaavan henkilökunnan puutteen ja pienten resurssien vuoksi. Koen myös, että tässäkin mittakaavassa voidaan huomata käyttöönottoon liittyvät erikoispiirteet ja vaatimukset. Haasteita uuden protokollan implementointiin asettavat myös edellisessä luvussa mainitut IPv6:een siirtymisen yleiset ongelmat, joista johtuen tällä hetkellä palveluntarjoajien palvelut uudelle protokollalle ovat vaillinaiset.

Käyttöönotto-osan tarkoituksena on selvittää, minkälaiset vaatimukset IPv6 asettaa reitittimille, käyttöjärjestelmille ja muulle laitteistolle. Lisäksi selvitetään, mitkä ovat ne käytännön toimet, jotka PK-yrityksessä tulee ottaa huomioon palveluntarjoajien suhteen, jotta IPv6:tta tukevat tietoliikenneyhteydet saadaan käyttöön. Käyttöönoton vaiheita ja uuden protokollan toimivuutta on tarkoitus havainnollistaa verkkolaboratoriossa suoritettavalla reitityssimulaatiolla, jonka on tarkoitus havainnollistaa PK-yrityksen mittakaavan ja resurssien mukaista käyttöönottoa. Simuloitu esimerkki on tarkoituksella yksinkertaistettu, tiettyjen piirteiden ja vaatimusten selvittämiseksi, mutta se on laajennettavissa isompaan kontekstiin.

Käyttöönoton esimerkkiyrityksen koko on 50–70 henkilöä, ja sisäisessä tietoverkossa oletetaan olevan kolme aliverkkoa. Yrityksen oletetaan toimivan sellaisella alalla, jossa päätelaite tarvitaan lähes jokaista henkilöä kohden. Esimerkkiyritys vastaa mielestäni varsin hyvin todellista PK-yritystä, jossa voi olla erikseen määritellyt aliverkot erilaisille osastoille ja jonka tietoliikennetarpeita voidaan pitää kohtuullisina. Esimerkkiyrityksen vaatimukset voidaan

skaalata myös isompaan ja pienempään yritykseen, jolloin määritykset hieman muuttuvat. Esimerkkitapausta ei myöskään rakenneta Unique Local Unicast -osoitteille NAT-menetelmää käyttäen vaan Globaali Unicast-osotteiden varaan. Tätä tapaa voidaan tulevaisuudessa pitää suositumpana, koska IPv6-osoiteavaruuden laajuus poistaa NAT-menetelmän tarpeellisuuden. Kuvio 14 esittelee loogisen verkkotopologian, joka voisi edustaa myös PK-yrityksen sisäistä verkkoa. Esimerkkiä on syytä pitää yksinkertaistettuna verrattuna reaalimaailman verkkorakenteeseen.

Kuvio 14. Esimerkkiyrityksen looginen topologia



Kuvan mukaisesti PK-yrityksen verkko olisi jaettu aliverkkoihin. Päätelaitteet yhdistyisivät kytkimien ja reitittimien kautta palveluntarjoajan reitittimeen, joka puolestaan tarjoaa yhteyden Internetiin. Kuvan esimerkissä myös palomuurit sijaitsevat palveluntarjoajan reitittimellä.

IPv6:ta tukevan sisäverkon rakenneosat ovat pitkälti samoja kuin IPv4-verkossa. Käytännössä palveluntarjoajista riippuen tullaan tulevaisuudessa tilanteeseen, jossa käytössä on monenlaisia erilaisia tietoliikennetoteutuksia, joissa IPv6:n käyttöönotto on hoidettu eri tavalla. PK-yrityksessä mahdollisia IPv6-toteutuksia ovat erilaiset tunnelointimenetelmät (*IPv6 to IPv4*),

dual-stack-toteutukset (IPv6 ja IPv4) tai puhdas IPv6-toteutus. Jokaisessa toteutustavassa on etuja ja hyötyjä. Oma näkemykseni on, että käyttöönotto jonkinlaisen *dual-stack* -toteutuksen kautta on PK-yrityksen kannalta paras ratkaisu. *Dual-stack*:illa tarkoitetaan tilannetta, jossa laitteet tukevat kumpaakin IP-protokollan versiota. Tämän järjestelmän etuna voidaan pitää muun muassa sitä, että näin saadaan siirtymäaikana pidettyä yllä toimivat tietoliikenneyhteydet IPv4: n avulla, mutta toisaalta voidaan koekäyttää ja testata IPv6-yhteydet. Näin mahdolliset ongelmat voidaan korjata välttäen liian suuret haitat. *Dual-Stack* takaa myös yhteydet IPv4:än kautta, jos palveluntarjoajalta tilattu tietoliikenneyhteys ei heti olekaan IPv6-yhteensopiva. Järjestelmä vaatii kuitenkin hieman enemmän ylläpitotoimia, koska hallinnoitavana on kaksi erillistä järjestelmää. Hyödyt tässä menetelmässä ovat kuitenkin merkittävät verrattuna suoraan IPv6-verkkoon siirtymiseen tai IPv4-verkolla jatkamiseen. Todennäköisesti palveluntarjoajat muuttavat käytäntöjään ajan kuluessa ja päällekkäisistä järjestelmistä siirrytään pikkuhiljaa puhtaaseen IPv6:n käyttöön.

Taulukko 8 esittelee perusvaatimukset IPv6-tietoverkolle, joka voitaisiin ottaa käyttöön PK-yrityksessä. Vaatimuksissa on otettu huomioon, että PK-yritys käyttää *dual-stack*-menetelmää ja varsinainen Internet-yhteys hoidetaan palveluntarjoajan kautta.

Taulukko 8. IPv6-tietoverkon perusvaatimukset ja esimerkkilaitteita.

IPv6-VERKON VAATIMUS	VALMISTAJA JA LAITE
Käyttöjärjestelmä, joka tukee IPv6:tta	**Apple:**Apple Mac OS x 10.4.7 **Linux:** Red Hat Enterprise Linux WS **Microsoft Windows:** XP/Vista/ Windows 7
Reititin IPv6/IPv4 dual-stack -tuella	**Allied Telesis:** Rapier Series (Layer 3 -kytkin) tai AR410/AR410S **Cisco: ISR Router 2800/3800** **D-Link**: xStack DGS 3612G (Layer 3 -kytkin) **Extreme Networks**: Black Diamond 2890 tai Summit 8450-24p (Layer 3 -kytkimet)
LAN-kytkin MLD-tuella	**Allied Telesis:** Rapier Series (Layer 3 -kytkin) tai AR410/AR410S **Cisco:** Catalyst 3750 **D-Link:** xStack DGS 3612G (Layer 3 -kytkin) **Extreme Networks:** Black Diamond 2890 tai Summit 8450-24p (Layer 3 -kytkimet)
Palomuurit	Useita vaihtoehtoja

Lähemmin tarkasteltuna vaatimukset täyttävä laitteisto ei juuri eroa IPv4-tietoverkon vastaavista. Tämä johtuu pitkälti siitä, että reititinvalmistajat ja päätelaitevalmistajat ovat implementoineet IPv6-tuen useimpiin tuotteisiinsa hyvissä ajoin. Tämän vuoksi markkinoilla on saatavia useita tuotteita, joilla edellä mainitun kaltainen IPv6-tietoverkko voidaan toteuttaa. Tuotteita löytyy useammalta laitevalmistajalta ja lukuisilla erilaisilla määrityksillä, jolloin hinta-vertailun kautta on mahdollista valita omiin resursseihin ja tarpeisiin sopiva laitteisto. Edellä mainitut laitteet eivät ole tarkoitettu suoraan PK-yrityksen tarpeisiin sopiviksi vaan toimivat vain esimerkkeinä. Laitteiden lisäksi IPv6 ei ole sidottu vain tiettyihin käyttöjärjestelmiin vaan useista Windows-, Mac- ja Linux-käyttöjärjestelmistä löytyy IPv6-tuki. Käytännön kannalta rakennusosat ovat siis olemassa ja valmiita käyttöönottoon.

Mikä on sitten suomalaisten Internet-palvelujentarjoajien todellinen IPv6-palvelutarjonta kuluttajalle? Lähestyin kahta suurta operaattoria, Elisaa ja Soneraa, sekä puhelimitse että sähköpostilla kysyäkseni, minkälaisia tietoliikenneratkaisuja ne tarjoavat PK-yrityksille. Määrittelin esimerkkiyrityksen mukaisen yrityskoon ja sen tarpeet sekä kysyin erityisesti IPv6-tuen omaavista tietoliikenneyhteyksistä. Puhelinhaastattelun kohdistin yritysten asiakaspalveluun ja tämän lisäksi tein sähköpostikyselyt Pohjois-Suomen aluepäälliköille.

Soneralta ilmoitettiin, että se tarjoaa esimerkkiyritykseni kaltaisille yrityksille kattavia ja erikseen räätälöitäviä tietoliikenneratkaisuja, mutta IPv6:ta tukevia yhteyksiä ei ole saatavilla. Myös Elisalla on tarjolla yrityksille räätälöityjä tietoliikenneratkaisuja, mutta Soneran tapaan IPv6-yhteyksiä ei ole vielä tarjolla asiakkaille. Elisan puolelta kuitenkin ilmoitettiin, että IPv6-yhteyksiä testataan parasta aikaa muutamien yritysten kanssa ja testauksen jälkeen IPv6-yhteydet myös tuotteistetaan. Tuotteistamisen aikataulua ei kuitenkaan osattu kertoa. Elisalta kerrottiin myös, että IPv6-yhteydet ovat hinnaltaan samansuuruisia kuin IPv4-yhteydet ja niiden toteutus tapahtuu samoilla reitittimellä kuin tähänkin asti. Tästä voidaan huomioida, että Elisa toteuttaa IPv6-yhteydet jonkinlaisella *dual-stack*-menetelmällä.

Kahdelle suurelle operaattorille kohdistetun käytännönläheisen tiedustelun pohjalta voidaan mielestäni todeta seuraavaa: suomalaiset operaattorit eivät olleet vielä tämän opinnäytetyön tekohetkellä valmiita tarjoamaan IPv6-tuettuja yhteyksiä, vaikka ne tarjoavatkin kattavasti vanhaan protokollaan tukeutuvia tietoliikenneratkaisuja. Huomioitavaa on kuitenkin, että kysely on suoritettu Pohjois-Suomen alueella vastaamaan rovaniemeläisen PK-yrityksen tarpeita, ja tarjonnassa voi olla alueellisia vaihteluita.

Operaattoreiden tilanne voi olla vaikea sellaisten IPv6-yhteyksiä haluavien yritysten kannalta, jotka ovat ajoissa investoineet IPv6-yhteensopiviin laitteistoihin. Elisan testauskäytäntö tarjoaa kuitenkin jonkinlaisen mahdollisuuden IPv6-yhteyksien käyttöönottoon, joten mielestäni on perusteltua suositella yrityksille hakeutumista tällaisen testauksen piiriin. Sen etuna on hallittu käyttöönotto ja ongelmakohtien löytäminen sekä korjaaminen. Myös varsinaisten yhteyksien hankkiminen testauksen jälkeen sujuu näin ollen sujuvasti samalta operaattorilta. Todennäköisesti IPv6:een siirtyminen tulee aluksi tapahtumaan myös suomalaisten operaattorien toimesta erilaisten tunnelointi ja *dual-stack*-menetelmien kautta. Tätä päätelmää tukevat erityisesti Elisan antamat tiedot sekä arviot operaattoreiden nykyisestä IPv6-valmiudesta. Puhtaaseen IPv6-liikennöintiin siirrytään siis hiljalleen.

Mainitsin jo aikaisemmin, että PK-yrityksen mittakaavassa suoritettava IPv6-käyttöönotto on mielestäni syytä suorittaa niin, että verkko tukee molemmilla protokollaversioilla tapahtuvaa tietoliikennettä. Näin vältetään mahdolliset ongelmat erityisesti uuden protokollaversion käyttöönotossa. On myös perusteltua sanoa, että koska IPv6:een siirtyminen vaatii aikaa ja resursseja, on käyttöönotto syytä aloittaa ajoissa. *Dual-stack*-menetelmän ansiosta uuden protokollan käyttöönotto voidaan aloittaa, vaikka palveluntarjoajien tukea uudelle protokollalle ei olekaan. Mielestäni tilanne on PK-yrityksen kannalta otollinen, koska näin saadaan aikaa testaukseen ja henkilökunnan koulutukseen, jotta siirtyminen puhtaaseen IPv6:een hoituu vaivattomasti. Tämän käyttöönottomuodon etuna pidän myös sitä, että näin yritys voi päättää asteittain, mitä palveluja tarjoaa IPv6-tuettuina ja mitä ei. Näin voidaan taata tärkeiden palvelujen saatavuus vanhalla protokollalla, mutta myös IPv6:lla.

6.2 Käyttöönoton simulointi

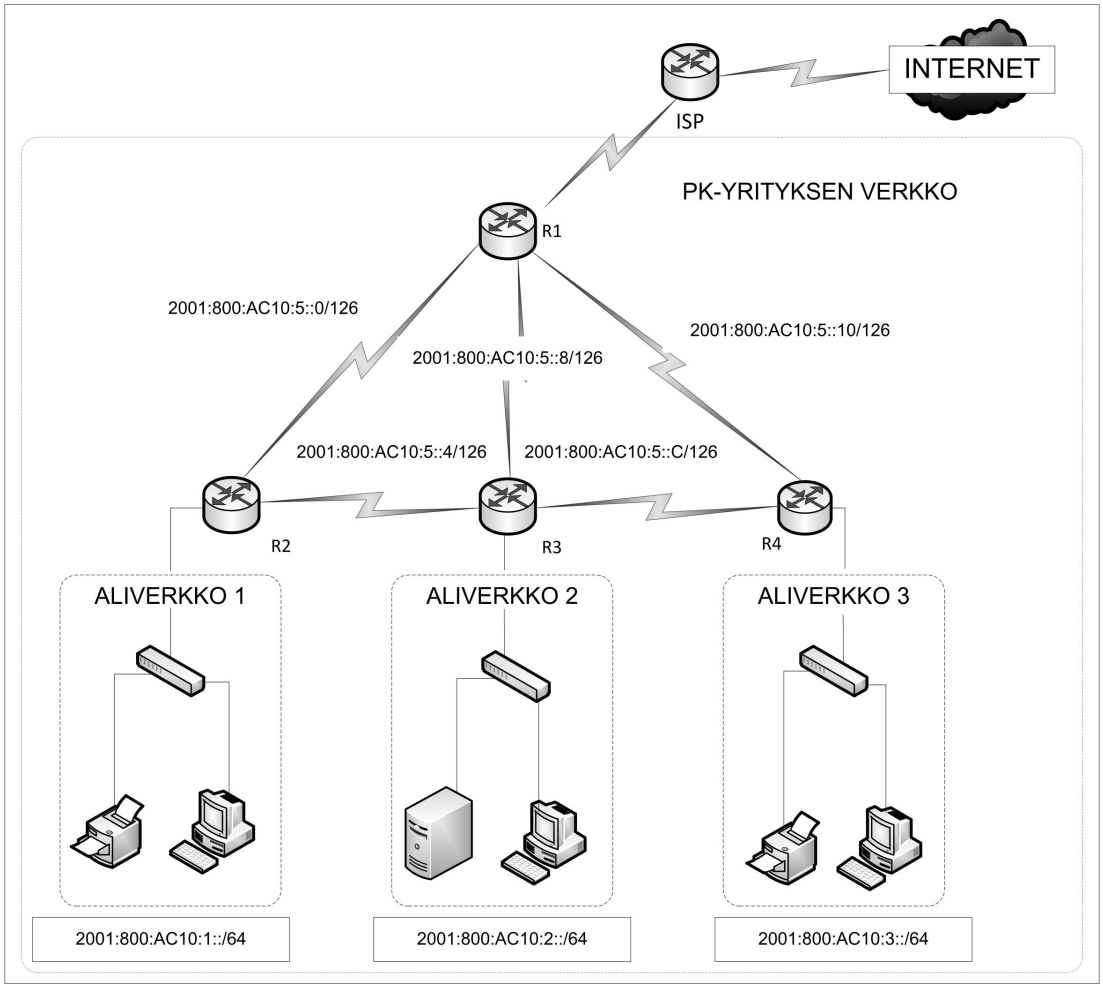
6.2.1 Simulaation määrittelyt

Koska ensikäden tietoa siitä, miten palveluntarjoajat todella Suomessa alkavat IPv6-yhteyksiä toteuttaa ei ole saatavilla, olen simulointiosuutta varten tehnyt itse tiettyjä määrityksiä. Palveluntarjoajat tulevat todennäköisesti tarjoamaan IPv6-yhteyksiä PK-yrityksille tietynlaisina pakettiratkaisuina, joissa tietoliikenneyhteyden lisäksi mukana tulee muun muassa palveluntarjoajan hallinnoima reititin sekä tarvittavat IP-osoitteet. Tällä hetkellä IPv4-ratkaisuissakin on mahdollista saada perustellusti julkisiin osoitteisiin perustuva osoitteistus yrityksen käyttöön. IPv6:n myötä julkisten osoitteiden jakaminen todennäköisesti entisestään helpottuu niiden suuren määrän vuoksi.

Lähtökohtani simulointiin on, että palveluntarjoaja tarjoaa tietoliikenneyhteyden, gateway-reitittimen ja osoiteavaruuden yrityksen käyttöön. Sisäistä verkkoa PK-yritys hallinnoi itse. Tässä tapauksessa email-palvelimet ja palomuurit ovat palveluntarjoajan hallinnoimia, joten niitä ei simuloidussa esimerkissä ole. Todellisuudessa myös sisäisessä verkossa on syytä käyttää jonkinlaista palomuuria. Myös DNS-nimipalvelimet ovat todennäköisesti palveluntarjoajien ja IPv6 voidaan nykyisellääänkin implementoida olemassa oleviin laitteisiin. PK-yrityksen täytyy kuitenkin rekisteröidä omat IPv6-osoitteet näille palvelimille.

Simuloinnin osoitteistuksen pääpiirteet perustan kuvauksiin käytännöistä koskien palveluntarjoajien osoitteiden jakamisesta (Cisco 2002; Cisco 2010). Palveluntarjoajat tulevat todennäköisesti jakamaan asiakkailleen käyttöön kiinteämittaisia osoiteavaruuksia, joita asiakas saa hallinnoida itse. Jaettavat osoiteavaruudet sijaitsevat Globaali Unicast -osoitteiden, 2000::/3-etuliitteellä määritellyssä osoiteavaruudessa ja niiden pituus on merkitty /48-aliverkkomaskilla. Tämä tarkoittaa sitä, että yritykselle jaetaan osoiteavaruus, jossa 3 ensimmäistä bittiä muodostavat tyyppi-etuliitteen ja seuraavat 45 bittiä globaalin reititysetuliitteen. Jäljelle jäävästä 80 bitistä 16 käytetään aliverkkojen jakamiseen ja loput 64 bittiä jäävät päätelaiteosoitteiksi (host-osoitteet). Annetusta osoiteavaruudesta voidaan huomata IPv6-osoitteistuksen laajuus. 16 bittiä antaa mahdollisuuden 65 536 aliverkkoon

(2^{16}). Host-osoitteita puolestaan saadaan käyttöön 2^{64} kappaletta. Kuviossa 15 esitellään laboratoriosimulaation looginen topologia sekä IPv6-osoitteistus.

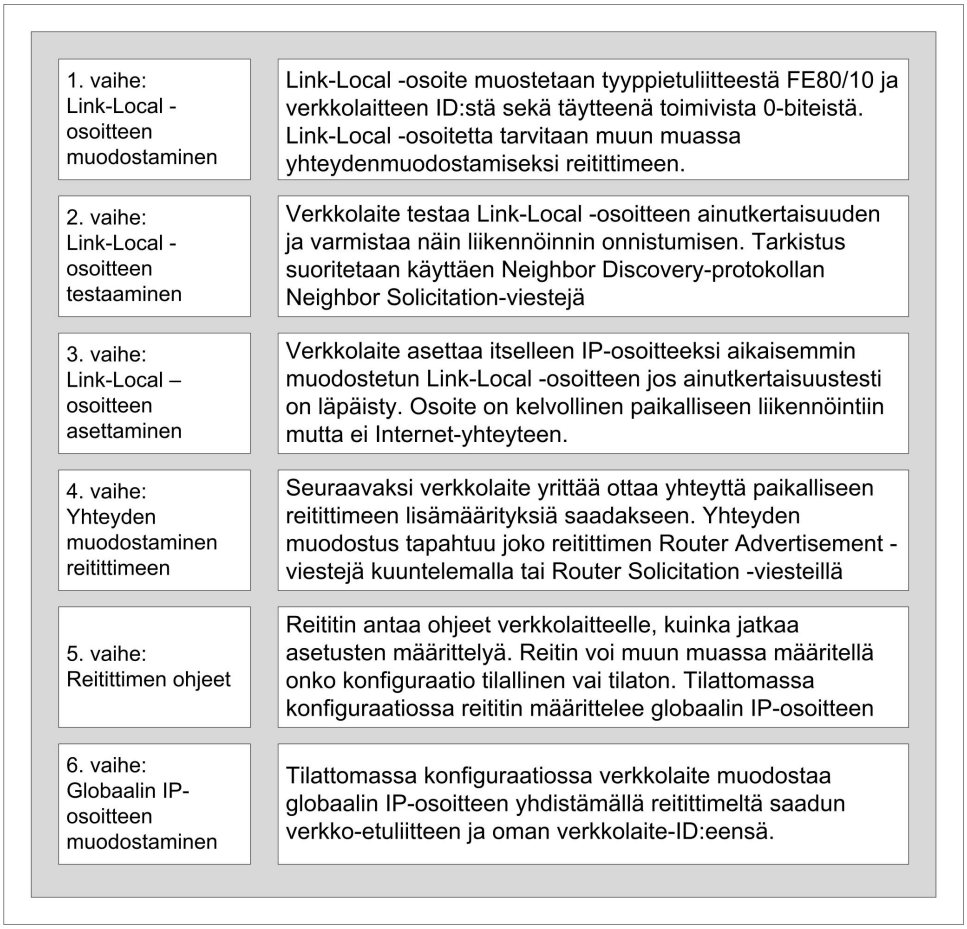


Kuvio 15. Laboratoriosimulaation looginen topologia ja IPv6-osoitteistus

Simulaatiossa aliverkkojen osoitteina on käytetty Globaali Unicast -osoitteita, jotka sijaitsevat RIPE:n varaamassa osoiteavaruudessa. Osa globaalista reititysetuliitteestä on kuitenkin keksitty, koska palveluntarjoajilta ei saatu käytännön tietoa jaettavien osoitteiden muodosta. Osoitteistus noudattaa kuitenkin edellä esiteltyjä palvelutarjoajien mahdollisia käytäntöjä. Tämän lisäksi reitittimien välisille aliverkoille on määritelty aliverkkomaskilla /126 merkityt aliverkot. Käytäntöä voidaan verrata IPv4:n /30-aliverkkomaskiin, jolla säästetään turhien osoitteiden allokointi, jos päätelaitteita on vain kaksi.

Päätelaitteiden osoitteiden osalta simulaatiossa käytetään IPv6:n uutta tilatonta autokonfiguraatio-ominaisuutta (*engl. Stateless Autoconfiguration*). Tilattomassa autokonfiguraatiossa päätelaitteet hakevat automaattisesti osoit-

teen, kun ne kytketään tietoverkkoon. Yksinkertaistettuna prosessissa päätelaite ottaa yhteyttä reitittimeen, joka puolestaan lähettää päätelaitteelle sen aliverkkoliitännän IP-osoitteen, jossa päätelaite on kytkettynä. Tämän jälkeen päätelaite muodostaa itselleen IP-osoitteen yhdistämällä reitittimeltä saadun aliverkko-osoitteen ja oman verkkolaitteensa MAC-osoitteen. Näin jokaisella päätelaitteelle muodostuu ainutkertainen IP-osoite, joka täyttää myös Globaali Unicast -osoitteiden vaatimukset. (Miller 2000, 153–155) Kuvio 16 selventää tilattoman autokonfiguraation vaiheita sekä siinä käytettäviä protokollia ja IP-osoitteita.



Kuvio 16. Tilattoman autokonfiguraation vaiheet

Tilatonta autokonfiguraatiota voidaan pitää merkittävänä parannuksena verrattuna vanhan protokollaversion ominaisuuksiin, koska se vähentää merkittävästi manuaalisen konfiguraation tarvetta ja poistaa osaksi ylimääräisten laitteiden, kuten DHCP-palvelimien implementaatiotarpeen verkkoihin. Lisäksi ominaisuus mahdollistaa laitteiden *hot-plugging*-kytkennät ilman manuaalista osoitteiden asettelua. Tilaton autokonfiguraatio sopii erityisen hyvin lan-

gattomiin tietoliikenneyhteyksiin, joissa osoitteiden jakaminen uusiin laitteisiin onnistuu vaivattomasti.

6.2.2 Simulaation toteutus

Reitityssimulaatio toteutettiin Rovaniemen Ammattikorkeakoulun Järjestelmien hallinnan-, tietoverkkojen- ja tietoturvankehityslaboratoriossa edellä esiteltyjen määrityksien ja loogisen topologian mukaisesti. Simulaatiota varten laboratorioon luotiin suljettu verkko. Käytössä ollut laitteisto on eritelty taulukossa 9.

Taulukko 9. Reitityssimulaatiossa käytetty laitteisto

Laite	Laitteen tiedot
Reitittimet (4)	Cisco 2811 Integrated Services Router IOS Version: 15.1(1)T Advanced IP Services 1 x WIC-2T 2-Port Serial WAN Interface Card
Kytkimet (2)	Cisco 3560-24PS IOS Version: 12.2(53)SE2 IP Services
Kytkimet (2)	Cisco 2960-24TT-L IOS Version: 12.2(53)SE2 Lan Base

Edellä esitettyjen laitteiden lisäksi käytössä oli päätelaitteina iMac-tietokoneet, joissa käyttöjärjestelmänä oli *Mac OS X version 10.6.5*. Reitittimet pyrittiin yhdistämään toisiinsa käyttämällä sarjaportteja ja asianmukaista kaapelointia. Jos reitittimessä ei ollut yhteyksien vaatimaa määrää sarjaportteja, käytettiin lisäksi FastEthernet-portteja. Päätelaitteet ja kytkimet yhdistettiin FastEthernet-portteja käyttäen. Myös reitittimet yhdistettiin kytkimiin FastEthernet-portteja käyttäen.

Fyysisen yhteydenmuodostamisen eli kaapeloinnin jälkeen reitittimistä poistettiin niissä mahdollisesti olleet asetukset ja niihin konfiguroitiin perusasetukset. Tämän jälkeen reitittimien porteille määriteltiin loogisen topologian mukaiset IP-osoitteet. Päätelaitteiden osalta IP-osoitteet muodostuvat automaattisesti. Reititinporttien IP-osoitteet on esitelty taulukossa 10.

Taulukko 10. Reititinporttien IP-osoitteet

Laite	Host-nimi	Portti (*Interface*)	IP-osoite	Aliverkko/CIDR
Reititin 1	R1	Serial 0/0/0	2001:800:AC10:5::1	2001:800:AC10:5::0 / 126
		Serial 0/0/1	2001:800:AC10:5::11	2001:800:AC10:5::10 / 126
		FastEthernet 0/0	2001:800:AC10:5::9	2001:800:AC10:5::8 /126
Reititin 2	R2	Serial 0/0/0	2001:800:AC10:5::2	2001:800:AC10:5::0 / 126
		Serial 0/0/1	2001:800:AC10:5::5	2001:800:AC10:5::4 / 126
		FastEthernet 0/0	2001:800:AC10:1::1	2001:800:AC10:1:: / 64
Reititin 3	R3	Serial 0/0/0	2001:800:AC10:5::D	2001:800:AC10:5::C / 126
		Serial 0/0/1	2001:800:AC10:5::6	2001:800:AC10:5::4 / 126
		FastEthernet 0/0	2001:800:AC10:5::A	2001:800:AC10:5::8 /126
		FastEthernet 0/1	2001:800:AC10:2::1	2001:800:AC10:2:: / 64
Reititin 4	R4	Serial 0/0/0	2001:800:AC10:5::E	2001:800:AC10:5::C / 126
		Serial 0/0/1	2001:800:AC10:5::12	2001:800:AC10:5::10 / 126
		FastEthernet 0/0	2001:800:AC10:3::1	2001:800:AC10:3:: / 64

Porttien osoitteiden konfiguroinnin jälkeen pystyttiin varmistamaan yhteys toisiinsa kytkettyinä olevien laitteiden välillä reitittimien ping-komentoa käyttäen. Reitittimien peruskonfiguraatiossa ja porttien IP-osoitteiden asettamisessa käytetyt käskyt on esitelty taulukossa 11.

Taulukko 11. Reitittimien konfiguraatioissa käytetyt käskyt

Komento	Kuvaus	Esimerkki
enable	siirtyy privileged-tilaan ja mahdollistaa reitittimen konfiguroimisen	
config t	siirtyy config-tilaan ja mahdollistaa mm. IP-osoitteiden määrittelyn	
hostname	asettaa laitteelle Host-nimen.	hostname *R1*
enable secret	asettaa privileged-tilalle salakirjoitetun login-tunnuksen	enable secret *class*
no IP domain-lookup	poistaa käytöstä DNS:än	
clock rate	asettaa kellotusajan yhteydelle, käytetään jos järjestelmässä ei ole DCE-laitetta	
line console 0	sirtyy line configuration-tilaan (konsoli)	
login	asettaa sisäänkirjautumisen käyttöön	
password	asettaa salasanan	password *cisco*
line vty 0-4	siirtyy line vty-tilaan (telnet)	
interface *tyyppi/nro*	siirtyy annetun portin konfigurointi tilaan	interface *FastEthernet 0/1*
ipv6 address *osoite/etuliite*	asettaa annetun IPv6-osoitteen	ipv6 address *2001:0DB8:0:1::/64*
ipv6 enable	ottaa käyttöön IPv6:n	
no shutdown	käynnistää portin	
ipv6 unicast-routing	mahdollistaa IPv6-reitityksen	

Perusasetusten ja porttien IP-osoitteiden asettamisen jälkeen vain toisiinsa suoraan kytketyt laitteet voivat kommunikoida keskenään. Jotta järjestelmän kaikki laitteet voivat kommunikoida toistensa kanssa, on reitittimiin luotava reititystaulut järjestelmässä olevista aliverkoista ja laitteista. Simulaatiossa reititystietojen luominen toteutettiin reititysprotokollia käyttäen.

Toinen mahdollisuus reititystaulujen luomiseen olisi luoda staattisia reittejä eli manuaalisesti konfiguroida kaikki halutut reitit. Staattisia reittejä käytettäessä järjestelmän muutokset joudutaan päivittämään manuaalisesti, joten todellisuudessa reititysprotokollan käyttö on suositeltavaa. Reititysprotokollaa käytettäessä järjestelmän muutokset päivittyvät automaattisesti, kun konfiguroinnit tehdään muutoksen alaiseen reitittimeen. Protokollaa käyttämällä on myös

helpompi muuttaa osoitteistusta ja välttää mahdolliset osoitteistusvirheet. Simulaatiossa käytettiin RIPng- ja EIGRP-reititysprotokollia, jotka tukevat IPv6:ta.

RIPng (*engl. Routing Information Protocol next generation*) on uusin versio vanhasta RIP-protokollasta. Se on suunniteltu vastaamaan IPv6:n vaatimuksiin. RIPng on autonomisen systeemin sisällä käytettävä IGP (*Interior Gateway Protocol*)-tyyppinen protokolla, joka soveltuu hyvin käytettäväksi pienissä verkoissa. RIP käyttää parhaan reitin laskemiseen *etäisyys vektori* -algoritmia. Etäisyysarvona (*engl. metric*) toimii *hop count*. RIPng-protokollan käyttöönottamiseksi vaadittavat käskyt on esitelty taulukossa 12.

Taulukko 12. RIPng:n käyttöönottoon liittyvät reititinkomennot

Komento	Kuvaus	Esimerkki
ipv6 router rip *word* (config-tilassa)	siirtyy RIP-protokollan määrittelytilaan Word tarkoittaa RIP-prosessin tunnusta	ipv6 router rip *prosessi1*
redistribute connected (rip-tilassa)	asetetaan jaettavaksi reitittimeen yhdistetyt yhteydet RIP-päivityksissä	
ipv6 rip *word* enable (interface config -tilassa)	otetaan käyttöön RIP-protokollan annetussa portissa	ipv6 rip *prosessi1* enable
show ipv6 rip database (privileged-tilassa)	näyttää RIP-protokollan määritykset ja mainostettavat reitit	
show ipv6 route (privileged-tilassa)	näyttää reitittimen reititystaulun. RIP-yhteydet merkitään R-kirjaimella	

RIP-protokollan käyttöönoton jälkeen yhteyttä toisiinsa suoraan kytkemättömien laitteiden kesken testattiin ping-komennolla. Lisäksi tarkistettiin, että reitittimien reititystaulut sisälsivät vaadittavat RIP-reitit ykset. Päätelaitteista varmistettiin, että IP-osoitteet määrittyivät oikein tilatonta autokonfiguraatiota käyttäen. Päätelaitteet edustavat yrityksen kolmea aliverkkoa, ja jokaiselle on määrittynyt IP-osoite oikeasta aliverkosta oletusreitittimen porttiosoitteen avulla. Tilattoman autokonfiguraation määrittelemät esimerkinomaiset IP-osoitteet on eritelty taulukossa 13. Osoitteista on eroteltu lihavoituna päätelaite-id.

Taulukko 13. Päätelaitteiden IP-osoitteet

Päätelaite	IP-osoite	Aliverkko
Host 1	2001:800:ac10:1:**5ab0:35ff:fef3:3f82**	2001:800:AC10:1::/ 64
Host 2	2001:800:ac10:2:**5ab0:35ff:fef3:3f5d**	2001:800:AC10:2::/ 64
Host 3	2001:800:ac10:3:**5ab0:35ff:fef0:5671**	2001:800:AC10:3::/ 64

Kun RIP-protokollan avulla tapahtuvan reitityksen toimivuus oli tarkastettu, lisättiin järjestelmään EIGRP-reititysprotokolla (*engl. Enhanced Interior Gateway Routing Protocol*). EIGRP on myös IGP-tyyppinen *etäisyys vektori*-protokolla. EIGRP sisältää RIP:iin verrattuna useita ominaisuuksia, jotka tekevät siitä tehokkaamman ja vakaamman käyttää. RIP:ia käytettäessä järjestelmän topologiamuutokset päivittyvät hitaasti toisin kuin EIGRP:ia käytettäessä. Tämä on mahdollista, koska protokolla varastoi tietoa koko verkon topologiasta pelkkien reititystietojen lisäksi. Nopean järjestelmän palautumisen lisäksi järjestelmän maksimikoko ei ole niin rajoitettu kuin RIP:ia käytettäessä.

EIGRP käyttää etäisyysarvona (metric) kaistanleveydestä, kuormasta, luotettavuudesta, viiveestä ja *hop countista* muodostunutta vertailulukua. Etäisyysarvon parametreihin voi myös vaikuttaa konfiguroimalla ne halutuiksi. Kaiken kaikkiaan EIGRP:ia voidaan pitää monipuolisempana protokollana kuin RIP:ia. Protokollan haittapuolena on se, että EIGRP toimii vain CISCO:n valmistamissa laitteissa.

EIGRP:in käyttöönotto tapahtui pitkälti samalla tavalla kuin RIP:in. Koska järjestelmän IP-osoitteet oli jo asetettu, määriteltiin vain EIGRP:n asetukset ja otettiin protokolla käyttöön halutuissa porteissa. Tämän jälkeen tarkastettiin reitittimistä reititystaulujen sisältö ja haluttujen yhteyksien toimivuus. EIGRP:n käyttöönotossa ja määrittelyissä käytetyt reititinkomennot on eritelty taulukossa 14.

Taulukko 14. EIGRP-komennot

Komento	Kuvaus	Esimerkki
ipv6 router eigrp *autonomous system number* (config-tilassa)	siirrytään EIGRP-tilaan. *Autonomous system number* arvo erottaa EIGRP-prosessit toisistaan	ipv6 router eigrp 1
redistribute connected (eigrp-tilassa)	asetetaan jaettavaksi reitittimeen yhdistetyt yhteydet EIGRP-päivityksissä	
eigrp router-id *ip-address* (eigrp-tilassa)	määritellään EIGRP:in toimintaan liittyvä reititin-id jos käytösssä ei ole IPv4 osoitteita	eigrp router-id *10.1.1.1*
ipv6 eigrp *autonomous system number* (interface config -tilassa)	otetaan eigrp käyttöön halutussa portissa	
show ivp6 eigrp (*autonomous system number)* interface	näyttää portit joissa EIGRP on aktiivinen	
show ivp6 eigrp (*autonomous system number)* topology	näyttää EIGRP-prosessin topologia taulun sisällön	

Kun järjestelmässä on käytössä useampia reititysprotokollia, täytyy reitittimien valita, miltä protokollalta saatuja reititystietoja reititykseen käytetään. CISCOn reitittimissä ongelma on ratkaistu asettamalla kullekin protokollalle *administrative distance* -arvo, jonka avulla reitin päättää, mikä reitti asetetaan reititystauluun. Mitä alhaisempi arvo on, sitä luotettavampana reititin pitää kyseessä olevaa reittiä. RIP:in *administrative distance*- arvo on 120 ja EIGRP:in 90. Tästä johtuen laboratoriosimulaation lopullisissa reititystauluissa dynaamisista reititystaulumerkinnöistä näkyvät vain EIGRP-protokollan reitit. RIP-reittien olemassaolo voidaan kuitenkin varmistaa *show ipv6 rip database* -käskyllä. Useamman reititysprotokollan käyttöä samassa järjestelmässä ei suositella, ja reitityssimulaatiossa kaksi protokollaa on otettu käyttöön vain esimerkin vuoksi. Kuviossa 17 on esitelty reitittimen R1 lopullinen reititystaulu sekä RIP-tiedot.

```
IPv6 Routing Table - default - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D   2001:800:AC10:1::/64 [90/2172416]
    via FE80::225:84FF:FE2C:90A0, Serial0/0/0
D   2001:800:AC10:2::/64 [90/30720]
    via FE80::225:45FF:FEEC:3A48, FastEthernet0/0
D   2001:800:AC10:3::/64 [90/2172416]
    via FE80::225:45FF:FEEC:3778, Serial0/0/1
C   2001:800:AC10:5::/126 [0/0]
    via Serial0/0/0, directly connected
L   2001:800:AC10:5::1/128 [0/0]
    via Serial0/0/0, receive
D   2001:800:AC10:5::4/126 [90/2172416]
    via FE80::225:45FF:FEEC:3A48, FastEthernet0/0
C   2001:800:AC10:5::8/126 [0/0]
    via FastEthernet0/0, directly connected
L   2001:800:AC10:5::9/128 [0/0]
    via FastEthernet0/0, receive
D   2001:800:AC10:5::C/126 [90/2172416]
    via FE80::225:45FF:FEEC:3A48, FastEthernet0/0
C   2001:800:AC10:5::10/126 [0/0]
    via Serial0/0/1, directly connected
L   2001:800:AC10:5::11/128 [0/0]
    via Serial0/0/1, receive
L   FF00::/8 [0/0]
    via Null0, receive
```

```
R1>show ipv6 rip database
RIP process "prosessi1", local RIB
2001:800:AC10:1::/64, metric 2, installed
    Serial0/0/0/FE80::225:84FF:FE2C:90A0, expires in 164 secs
 2001:800:AC10:2::/64, metric 2, installed
    FastEthernet0/0/FE80::225:45FF:FEEC:3A48, expires in 154 secs
 2001:800:AC10:3::/64, metric 2, installed
    Serial0/0/1/FE80::225:45FF:FEEC:3778, expires in 161 secs

2001:800:AC10:5::/126, metric 2
    Serial0/0/0/FE80::225:84FF:FE2C:90A0, expires in 164 secs
 2001:800:AC10:5::4/126, metric 2, installed
    Serial0/0/0/FE80::225:84FF:FE2C:90A0, expires in 164 secs
    FastEthernet0/0/FE80::225:45FF:FEEC:3A48, expires in 154 secs
 2001:800:AC10:5::8/126, metric 2
    FastEthernet0/0/FE80::225:45FF:FEEC:3A48, expires in 154 secs
 2001:800:AC10:5::C/126, metric 2, installed
    FastEthernet0/0/FE80::225:45FF:FEEC:3A48, expires in 154 secs
    Serial0/0/1/FE80::225:45FF:FEEC:3778, expires in 161 secs
 2001:800:AC10:5::10/126, metric 2
    Serial0/0/1/FE80::225:45FF:FEEC:3778, expires in 161 secs
```

Kuvio 17. Reitittimen R1 reititystaulu ja RIP-tiedot

R1-reitittimen reititystaulusta voidaan erottaa erityyppisiä yhteyksiä. D-kirjaimella merkityt reitit ovat EIGRP-protokollan kautta saatuja reititystietoja. C-kirjaimella merkityt reitit puolestaan ovat reitittimeen suoraan kytkettyjä reittejä. RIP-protokollan ominaisuuksista voidaan tarkastaa reittien yhtäläisyys. Huomionarvoinen asia reititystiedoissa on myös Link Local -osoitteiden käyttö Next Hop -osoitteina (FE80-tyyppietuliite).

Simulaation lopuksi järjestelmässä suoritettiin erilaisia yhteydentarkistuksia ja varmistuttiin, että yhteys on olemassa kaikkien päätelaitteiden kesken. Simu-

laatiossa olisi myös voitu asettaa palvelin johonkin aliverkkoon, jolloin esimerkiksi jonkin tiedoston noutaminen olisi toiminut konkreettisena esimerkkinä yhteyksien toimivuudesta. Ping-komennon käyttäminen kuitenkin riitti simulaation tarkoituksen täyttämiseen.

Yleisesti simulaatiosta voidaan todeta, että siinä kuvatun järjestelmän konfigurointi ei juuri eroa vanhan protokollaversion vastaavista toiminnoista. Osoitteiden asettaminen ja reititysprotokollien käyttöönotto tapahtuu lähes samalla tavalla kuin IPv4:ää käytettäessä. Suurimmat hankaluudet syntyivät uuden IP-osoitteen muodosta. IPv6-osoitteet ovat pitempiä ja vaikeammin luettavia kuin vanhan protokollaversion osoitteet. Näin ollen niiden käyttö edellyttää suurempaa huolellisuutta ja saattaa aiheuttaa osoitteistusvirheitä. Päätelaitteiden osalta voidaan sanoa, että *Mac OS X version 10.6.5* -käyttöjärjestelmässä on helposti löydettävissä IPv6-protokollan osoitteet, ja ominaisuudet on helppo ottaa käyttöön. Lisäksi tilaton autokonfiguraatio helpotti suuresti osoitteiden asettelua. Uuden ominaisuuden etu korostuu erityisesti silloin, kun järjestelmässä on paljon päätelaitteita.

Simulaation tarkoituksena oli selvittää ja kuvata IPv4 käyttöönottoon liittyviä komentoja ja ominaisuuksia. Näin ollen sitä ei tule pitää kattavana esittelynä reititinprotokollista tai IPv6:n ominaisuuksista yleensä. Tavoitteena oli testata, kuinka esimerkkiyrityksen kaltainen järjestelmä voitaisiin konfiguroida ja minkälainen on laitteiden ja käyttöjärjestelmien tuki uudelle protokollalle. Simulaation pohjalta voidaan todeta, että laitteiston puolelta IPv6-valmius on hyvä ja konfigurointi onnistuu suhteellisen helposti. Ongelmia syntyy erityisesti IPv6-osoitteiden uuden notaation kanssa. Laajempi IPv6-ominaisuuksien käyttöönotto voi luonnollisesti tuoda esille muitakin ongelma-alueita. Simulaation pohjalta voidaan todeta, että uusi protokolla on toimiva uudistus, mutta vaatii kouluttautumista ja rutiinia, jotta käyttöönotto ja järjestelmän ylläpito onnistuu hyvin.

7 JOHTOPÄÄTÖKSET

Internetillä ja tietoliikenteellä yleisesti on merkittävä osa nyky-yhteiskunnan toiminnassa. Siksi tietoliikenteessä ilmenevät ongelmat saattavat aiheuttaa merkittäviä haittoja, jotka hidastavat tai jopa pysäyttävät joitakin keskeisiä toimintoja. Nykyisellään käytettävä tekniikka, erityisesti IPv4-protokolla, on vanhentunutta, ja siihen on tehtävä merkittäviä päivityksiä. IPv4:ää ollaan korvaamassa uudella IPv6-protokollalla, jonka on määrä ratkaista erityisesti IP-osoitteiden loppumiseen liittyvät ongelmat.

IPv6 on huolellisesti suunniteltu uudistus, jonka merkittävin ominaisuus on sen 128-bittinen osoitekenttä. Tämä uudistus antaa käyttöön osoiteavaruuden, joka pystyy huolehtimaan tietoliikennetarpeista myös pitkälle tulevaisuuteen. Lisäksi protokolla on suunniteltu niin, että se tarjoaa käyttöön uusia ominaisuuksia, mutta on tästä huolimatta kevyt ja dynaaminen käyttää. Osoitteiden määrän kasvattamisen lisäksi uusittu osoitteistus mahdollistaa uudenlaisen osoitehierarkian, joka helpottaa osoitteiden jakamista ja reititysprosesseja.

Osoitteistukseen liittyvien uudistuksien lisäksi IPv6:n kehysrakennetta on yksinkertaistettu. Lisäksi on luotu täysin uudenlainen pääotsikosta ja valinnaisista otsikoista syntyvä dynaaminen rakenne. Tämä uudistus tekee kehysrakenteesta kevyen käyttää mutta mahdollistaa samalla kehittyneempien ominaisuuksien käyttöönoton sellaisten IP-pakettien kohdalla, jotka niitä tarvitsevat.

IPv6 mahdollistaa myös uudella tavalla reaaliaikaiset ääni- ja videopalvelut sekä mobiili-IP-ominaisuudet. Myös tietoturvaominaisuudet on IPv6:ssa huomioitu edeltäjäänsä paremmin. On kuitenkin syytä huomioida, että erityisesti tietoturvaominaisuuksien osalta IPv6 ei ole autuaaksi tekevä uudistus tietoliikenteessä. Uusi protokolla tuo mukanaan uusia tietoturvaongelmia, joiden ehkäiseminen vaatii uusia toimia. Lisäksi uusi protokolla vaatii yleisesti testausta ja lisää resursseja henkilökunnan koulutukseen. Yksi ongelma on myös siirtymisajan aikana vallitsevat päällekkäiset vanhaa ja uutta protokollaversiota käyttävät järjestelmät. Päällekkäiset järjestelmät saattavat pahimmillaan aiheuttaa vakavia ongelmia Internetin toiminnassa. IPv6:een tulee

siis jatkossakin suhtautua hyvänä, mutta lisätoimia vaativana protokollapäivityksenä.

IPv6:een siirtyminen ei uuden protokollan tarjoamista eduista ja uusista ominaisuuksista huolimatta ole edennyt toivotulla tavalla vaan toimijat ovat erittäin odottavalla kannalla. Tällä hetkellä vain erittäin pieni osa verkkoliikenteestä tapahtuu IPv6:ta käyttäen ja vain pieni osa suosituimmista sivustoista tukee uutta protokollaversiota. Käyttöönoton ongelmana pidetään IPv6-kysynnän pienuutta ja toisaalta osaavan henkilökunnan puutetta. Monella taholla myös koetaan, että varsinaista syytä protokollaan siirtymiseen ei vielä ole. IPv6-käyttöönotto kuitenkin etenee asteittain ja monen tasoisia toimia on tehty, jotta tilanne paranisi tulevaisuudessa. IPv4-osoiteavaruuden loppuminen on kuitenkin niin lähellä, että vaarana ovat kiireellä toteutetut massasiirtymiset, joista puolestaan voi aiheutua merkittäviä ongelmia ja kuluja.

IPv6:n käyttöönotto PK-yrityksessä on laitteiston puolesta helposti toteutettavissa. Yritys voi valita lukuisilta laitevalmistajilta resurssiensa mukaisen laitteiston. Myös lukuisat käyttöjärjestelmät tukevat uutta protokollaa. Uudesta protokollasta johtuvat investoinnit voivat myös olla vähäiset, koska yrityksissä käytettävät laitteet saattavat jo tukea IPv6:ta. PK-yrityksen kannalta paras käyttöönottotapa on *dual-stack*-järjestelmä, jolla tarkoitetaan järjestelmää, joka käyttää kumpaakin protokollaversiota. *Dual-stack*-järjestelmän ansiosta yritys voi tarjota kriittiset palvelut vanhaa protokollaversiota käyttäen, mutta myös käyttää uutta protokollaversiota haluamiensa palveluiden kohdalla. *Dual-stack*-järjestelmä antaa myös mahdollisuuden testata IPv6-yhteyksiä ja ratkaista mahdolliset ongelmakohdat ilman, että yrityksen tietoliikenne häiriintyy.

Reitityssimulaatiossa havainnollistettiin PK-yrityksen mittakaavassa tapahtuvaa käyttöönottoa. Simulaation pohjalta voidaan sanoa, että IPv6 käyttöönotto ja reititinkonfigurointi muistuttaa suurelta osin IPv4:ää. IPv6-tuettuja reititysprotokollia löytyy useita ja lisäksi tilaton autokonfiguraatio helpottaa päätelaitteiden osoitteenmäärittelyä. Simulaatiossa käytetystä käyttöjärjestelmästä löytyi myös tuki IPv6:lle ja IPv6-ominaisuuksien käyttöönotto tapahtui helposti. Varsinaisia ongelmia ei reitityssimulaation aikana IPv6:n käytössä ilmen-

nyt. Uusi protokolla vaatii kuitenkin perehtymistä vaadittuihin reititinkomentoihin ja reititysprotokolliin.

PK-yrityksen kannalta ongelmallisinta uuteen protokollaversioon siirtymisessä on se tosiasia, että ainakaan Suomessa, suurimmat palveluntarjoajat eivät tällä hetkellä tarjoa kuluttajille IPv6-yhteyksiä. Tämä vaikuttaa suoraan yritysten halukkuuteen investoida laitteisiin tai uuden protokollan käyttöönottoon. PK-yritysten kannattaa kuitenkin aloittaa IPv6:n käyttöönotto ajoissa. Näin saadaan aikaa testaukselle ja ongelma-alueiden selvittämiseen.

Opinnäytetyössäni käsitellään IPv6:n käyttöönottoa PK-yrityksessä. Mielestäni tehdyt huomiot voidaan kuitenkin yleistää laajemmassa mittakaavassa toteutettaviin käyttöönottoihin. IPv6:een siirtyminen on yksi lähitulevaisuuden suurimmista tietoliikenteen haasteista. Siirtyminen tarjoaa haasteita osaavan henkilökunnan kouluttamiseen ja vaatii myös investointeja uuteen laitteistoon. Selvää on myös se, että siirtyminen uuteen protokollaan tulee tapahtumaan asteittain, jolloin päällekkäiset järjestelmät aiheuttavat myös ongelmia tietoverkkoyhteyksien luotettavuudelle ja tietoturvalle.

Opinnäytteeni tekoprosessi oli hyvin suunniteltu ja toteutettu. Aloin suunnitella työtäni hyvissä ajoin ja keräsin alussa tarpeeksi aiheeseen liittyvää kirjallisuutta, jonka avulla oli helppoa päästä kiinni opinnäytetyön teoreettiseen taustaan ja erityisesti IPv6:n ominaisuuksiin ja rakenteeseen. Kirjoitustyö kesti heinäkuusta 2010 joulukuun alkuun 2010. Tänä aikana tein itselleni aikataulun, jonka mukaan suoritin kirjoitustyötä järjestelmällisesti osa-alue kerrallaan. Työmäärä ylitti lopulta alussa tehdyt työmääräarviot. Teoreettisen osan kirjoittaminen ja kirjallisuuden kokoaminen vaativat eniten työtä.

Koska IPv6 oli itselleni ennestään tuntematon aihe, tuli opinnäytetyöstäni myös erinomainen oppimisprosessi, jonka aikana tutustuin sekä uuteen protokollaversioon, että yleisesti tietoliikenteen teoreettiseen taustaan. Koen, että osaamiseni näillä alueilla on nyt paljon syvempää kuin ennen opinnäytetyötäni. Varsinaisia ongelmia en tekoprosessin aikana kohdannut. Työstäni tuli alkuperäissuunnitelmia laajempi mutta kirjoitustyö eteni nopeasti ja järjestelmällisesti. Opinnäytetyöni myös jäsentyi kirjoitusprosessin edetessä ja olen

tyytyväinen työn sisältöön ja rajauksiin. Koen myös, että sain työssäni vastattua asetettuihin tutkimusongelmiin ja, että työni rakenne on selkeä ja tarkoituksenmukainen. Kokonaisuutena opinnäytetyön tekeminen oli itselleni antoisa ja opettava kokemus.

IPv6:een liittyvänä jatkotutkimusaiheena näkisin muun muassa erilaiset tietoturvakysymykset. Tämän työn puitteissa tietoturvasta käsiteltiin vain perusominaisuudet, jotka ovat selkeitä parannuksia vanhaan protokollaversioon verrattuna, mutta eivät riitä ratkaisemaan kaikkia tietoturvaongelmia. Koen, että IPv6 asettaa haasteita erityisesti päätelaitteiden identifioitiin ja tietoliikenteen pääsynhallintaan. Järjestelmävalvojien osaaminen tietoturvaongelmien ratkaisemisessa ja ehkäisemisessä korostuu uuden protokollan myötä.

LÄHTEET

Botterman, M. 2009. IPv6 Deployment Survey. Based on the responses from the RIPE community during June 2009. Osoitteessa http://www.ripe.net/ripe/meetings/ripe-59/presentations/botterman-v6-survey.pdf. 6.10.2009.

Botterman, M. 2010. IPv6 Deployment Survey. Based on the responses from the global RIR community during June 2010. Osoitteessa http://www.nro.net/documents/GlobalIPv6SurveySummaryv2.pdf. 14.9.2010.

Cisco 2002. IPv6 Deployment Strategies. Osoitteessa http://www.ipv6-tf.com.pt/implementacoes/files/cisco/ipv6_DeploymentStrategies_Dec2002.pdf. 4.11.2010.

Cisco 2010. What Enterprises Should Do About IPv6 In 2010. Osoitteessa http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper_c11-586154.html. 4.11.2010.

Cisco Press 2002. Ciscon verkkoakatemia - 1. vuosi. Helsinki: Edita Publishing Oy.

Cisco Press 2003. Cisco Networking Academy Program. CCNA 3 and CCNA4 Companion Guide 3rd ed. Indianapolis: Cisco Press

Cisco Systems Inc. 2006. Cisco Networkers. Osoitteessa http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_presentation0900aecd8057a244.pdf. 8.9.2010.

Comer, D. E. 2002. TCP/IP. Helsinki: Edita Publishing Oy.

CSC. 2010. Tieteen tietotekniikan keskus. Tieteen tietotekniikka 1/2010. IPv6:n käyttöönotto etenee verkalleen. Osoitteessa http://www.csc.fi/csc/julkaisut/tieteentietotekniikka/2010/1/IPv6. 12.9.2010

Executive Office Of The President 2010. Memorandum for chief information officers of executive departments and agencies. Transition to IPv6 Osoitteessa http://www.cio.gov/Documents/IPv6MemoFINAL.pdf 28.9.2010.

Forouzan, B. A. 2006. TCP/IP Protocol Suite. 3rd ed. New York: McGraw-Hill.

Hain, T. 2005. A Pragmatic Report on IPv4 Address Space Consumption. The Internet Protocol Journal – Volume 8. Number 3. Osoitteessa http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html. 11.9.2010.

Hain, T. 2010. IPv4 Address Pool. IANA Policy -RIRs Allocated Pool for 12-24 Months Distribution Projections based on Jan 2000 to current. Osoitteessa http://www.tndh.net/~tony/ietf/ipv4-pool-combined-view.pdf. 11.9.2010.

Huston, G. 2010. IPv4 Address Report. Osoitteessa http://www.potaroo.net/tools/ipv4/index.html. 11.9.2010.

IANA. 2010. Internet Protocol Version 6 Address Space. Osoitteessa http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml. 11.9.2010.

IANA. 2008. IPv6 Global Unicast Address Assignments. Osoitteessa http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml. 11.9.2010.

IETF. 1996. Request for Comments: 1918. Address Allocation for Private Internets. Osoitteessa http://tools.ietf.org/html/rfc1918. 8.12.2010.

IPv6 ACT NOW. 2010. Osoitteessa http://www.ipv6actnow.org/info/statistics//. 12.9.2010.

Kaario, K. 2002. TCP/IP-verkot. Jyväskylä:Docendo.

Leppänen, T. 2010. Sähköpostivastaus tiedusteluun Viestintävirastosta 21.6.2010.

Loshin, P. 1997. TCP/IP Clearly explained. 2nd Ed. San Diego: Academic Press.

Loshin, P. 1999. IPv6 Clearly Explained. San Francisco: Morgan Kauffman Publishers Inc.

Miller, M. A. 2000. Implementing IPv6. Supporting the Next Generation Protocols. 2nd Ed. Foster City: M&T Books.

RFC 3587. IPv6 Global Unicast Address Format. Osoitteessa http://tools.ietf.org/html//rfc3587. 9.1.2011.

RFC 4291. IP version 6 Addressing Architecture. Osoitteessa http://tools.ietf.org/html/rfc4291#section-2.5. 11.9.2010.

Sotillo, S. 2006. IPv6 Security Issues. Osoitteessa http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf. 8.9.2010.

Stevens, W. R. 1994. TCP/IP Illustrated, Volume 1. The Protocols. Massachusetts: Corporate & Professional Publishing Group.

Viestintävirasto. 2008. IPv6-kyselyn yhteenveto. Osoitteessa http://www.ficora.fi/index/palvelut/palvelutaiheittain/standardointi/viestintahallinnonteknisettyoryhmat/ipv6.html. 18.3.2008.

Vyncke, E. 2010. IPv6 is being deployed but not in the expected places. Is IPv6 only deployed in Asia and in USA as the rumor says? Let's have a reality check. Osoitteessa http://www.networkworld.com/community/node/65476. 27.8.2010.

Wegner, J. D. – Rockell, R. 2000. IP Addressing and Subnetting including IPv6. Rockland MA: Syngress Media Inc.