LAUREA AMMATTIKORKEAKOULU Uuden edellä

IPv4-verkosta siirtyminen IPv6-verkkoon organisaatioissa

Kneckt Henri, Leppänen Konstantin

2012 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

IPv4-verkosta siirtyminen IPv6-verkkoon organisaatioissa

Kneckt Henri, Leppänen Konstantin
Tietojenkäsittely
Opinnäytetyö
Kesäkuu 2012

Laurea Ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittely

Kneckt Henri, Leppänen Konstantin

IPv4-verkosta siirtyminen IPv6-verkkoon organisaatioissa

Vuosi 2012 Sivumäärä 70

Tässä opinnäytetyössä käsitellään organisaatioiden siirtymistä IPv4-verkon käytöstä IPv6-verkon käyttöön. IPv6 on uusi verkkoprotokolla, jonka on tarkoitus korvata vanha IPv4-protokolla. Työ jakautuu kolmeen osaan: IP-protokollia käsittävään teoriaosuuteen, IPv6:n tilanteeseen yleisesti sekä organisaatio-caseihin.

Työn tarkoitus oli selvittää eri organisaatioiden IPv6:n käyttöönoton valmiuksia ja tietoisuutta sekä ylipäätään IPv6:n tilannetta Suomessa ja maailmanlaajuisesti. Tavoitteena oli laatia erityyppisille organisaatioille yleispätevä ohjeistus asioista, joita tulee huomioida IPv6:n siirryttäessä.

Opinnäytetyötä varten haastateltiin erityyppisiä organisaatioita. Esimerkkicaseina olivat valtion virasto, Louhi Net Oy ja Yritys X. Haastatteluilla pyrittiin selvittämään missä vaiheessa organisaatiot menevät IPv6:n käyttöönotossa ja miten he ovat siihen valmistautuneet. Lisäksi oli tärkeää saada selville miten IPv6:n käyttöönotto vaikuttaa organisaatioiden toimintaan ja miten organisaatio mahdollisesti hyötyisi IPv6:n käytöstä.

Työn lopuksi tehtiin yhteenveto IPv6:n tämän hetkisestä tilasta ja tulevaisuudesta organisaatioissa. Tuloksena saatiin kokonaiskuva IPv6:n käyttöönotosta organisaatioissa verrattuna kokonaiskuvaan Suomessa ja mahdollistaa jatkotutkimus asian tiimoilta.

Asiasanat: IPv4, IPv6, Internet, protokollat, organisaatio, siirtymävaihe

Laurea University of Applied Sciences **Abstract**
Leppävaara Leppävaara
Bachelor's Degree Programme in Business Information Technology

Kneckt Henri, Leppänen Konstantin

Migrating from IPv4-networks to IPv6-networks in organizations

Year 2012 Pages 70

The objective of this thesis was to research migration from the old IPv4 protocol to the new IPv6 protocol in different organizations. IPv6 is a new network protocol, which is going to replace the old IPv4 protocol. This thesis was divided in three parts: the IP-protocol theory section, the overall situation of IPv6 and different organization cases.

The purpose was to find out how different organizations are prepared for IPv6 deployment and IPv6 knowledge and examine the overall situation of IPv6 in Finland and worldwide. Another purpose was to create a guideline for organizations about aspects that need to be taken into consideration when migrating to IPv6.

Different organizations were interviewed for the thesis. These organizations were government's agency, Louhi Net Oy and company X. The purpose of interviews was to discover how organizations have taken IPv6 to use and how they have prepared for it. Also, it was crucial to discover how IPv6 deployment would affect the organization's function and how it could benefit from IPv6.

Finally, the current situation and the future of IPv6 in organizations were summarized. The result was a general view of IPv6 deployment in researched organizations compared to the overall IPv6 deployment in Finland. Also it allows further research on the issues involved.

Keywords: IPv4, IPv6, Internet, protocols, organization, migration

SISÄLLYS

1. Johdanto 8
1.1 Työn tarkoitus, tausta ja tavoitteet 8
1.2 Työn rakenne ja rajaus 8
2. Internet-protokollat 9
2.1 TCP/IP 9
2.2 TCP/IP:n viitemalli 10
2.2.1 Peruskerros / siirto- ja fyysinenkerros (Network Access Layer) 11
2.2.2 Verkkokerros (Internet Layer) 11
2.2.3 Kuljetuskerros (Transport Layer) 12
2.2.4 Sovelluskerros (Application Layer) 12
2.3 Standardit 12
2.4 IP eli Internet Protocol 12
2.6 Standardointi ja versiot 13
2.7 OSI-malli 14
2.8 OSI-mallin rakenne 14
2.9 OSI-mallin kerrosten tehtävät 15
3. IPv4 16
3.1 IPv4-osoitteet ja osoiteluokat 17
3.1.1 A-luokan osoitteet 17
3.1.2 B-luokan osoitteet 17
3.1.3 C-luokan osoitteet 17
3.1.4 Varatut osoitteet 17
3.2 NAT (Network Address Translation) 18
3.2.1 NAT:in toiminta 18
3.2.2 Dynaaminen NAT 18
3.2.3 Staattinen NAT 19
3.3 IPv4 otsikkokenttä (header) 20
3.4 IPv4:n otsikkokentän rakenne 21
4. IPv6 23
4.1 IPv6:n tietoturva 23
4.2 IPv6-osoitteen muoto ja varatut osoitteet 24
4.3 Aliverkotus (subnetting) ja CIDR 24
4.4 IPv6 Unicast-osoite 25
4.4.1 Linkkikohtainen osoite (link local) 25
4.4.2 Aluekohtainen osoite (site local) 25
4.4.3 Globaali osoite (global) 26
4.4.4 Ryhmälähetys (multicast) 26
4.4.5 Anycast-lähetykset 27

4.4.6 Naapurin tunnistus (neighbor discovery) 28
4.4.7 Autokonfigurointi (autoconfiguration) 28
4.4.8 Palvelun laatu eli QoS (Quality of Service) 28
4.5 Otsikkokenttä (header) 29
4.5.1 Pakollinen otsikko 29
4.5.2 Hyppyoptio-otsikko (hop-by-hop options) 30
4.5.3 Kohdeoptio-otsikko (destination options header) 30
4.5.4 Reititysotsikko (routing header) 30
4.5.5 Fragmentointiotsikko eli lohkomisotsikko (fragment header) 31
4.5.6 Todennusotsikko (authentication header) 31
4.5.7 Salausotsikko (encrypted security payload header) 31
4.6.1 IPv4-osoitteen mappaus IPv6-osoitteeksi 32
4.6.2 Dual Stack 32
4.6.3 Tunnelointi: Tunnel broker 32
4.6.4 Tunnelointi: 6to4 ja 6rd 33
4.6.5 Tunnelointi: Teredo 33
4.6.6 6bone 34
5. IPv6 Suomessa ja muualla maailmalla 34
5.1 IPv6-tappajasovellus (killer application). 34
5.2 IPv6 Suomessa 35
5.2.1 IPv6-seminaari ja sen tulokset 35
5.2.2 Viestintäviraston IPv6-toimet 36
5.2.3 Operaattoreiden IPv6-palveluiden tarjonta Suomessa 36
5.2.4 IPv6-liikenne Suomessa 36
5.3 IPv6 muualla maailmalla 37
5.3.1 IPv6-osoitteiden jako maailmalla 38
5.3.2 Maailmanlaajuinen IPv6-päivä 2011 ja Maailmanlaajuinen IPv6-julkaisupäivä 2012 38
5.3.3 IPv6-liikenne maailmalla 39
6 IPv6:n käyttöönotto ja huomioon otettavat asiat organisaatioissa 40
6.1 Syitä IPv6:seen siirtymistä vastaan 40
6.2 Syitä IPv6:seen siirtymisen puolesta 41
6.2.1 Tekniset syyt 41
6.2.2 Taloudelliset syyt 42
6.3 IPv6-verkon käyttöönotossa huomioitavat asiat 42
6.3.1 Aloituspiste ja eri arviot 43
6.3.2 Aika ja resurssit 44
6.3.3 Organisointi ja koordinointi 44
6.3.4 Koulutus 44

6.3.5 Pilottihanke 45
6.3.6 Ongelmat laitteissa ja ohjelmistoissa 45
6.3.7 Ongelmat IPv6-verkon käytössä 46
6.3.8 Yhteistyö organisaation ja valmistajien välillä 46
7. IPv6 organisaatio-caset 46
7.1 Case Louhi Net Oy 47
7.1.1 Louhen perustiedot 47
7.1.2 Louhen palveluiden määrittely 47
7.1.3 IPv6:n vaikutus Louhen palveluihin ja asiakkaisiin 47
7.1.4 IPv6:n lisäarvo Louhelle 48
7.1.5 IPv6 tulevaisuudessa osana Louhen palveluita ja tuotteita 48
7.2 Case yritys X 48
7.2.1 Yritys X:n perustiedot 48
7.2.2 Yritys X:n IPv6-tilanne 49
7.3 Case valtionvirasto Y 49
7.3.1 Valtionvirasto Y:n perustiedot 49
7.3.2 Valtionvirasto Y:n IPv6-tilanne 49
7.4 Yhteenveto caseista ja haastattelutuloksista 50
8. Yhteenveto ja pohdinta 51
LÄHTEET 53
KUVAT JA TAULUKOT 56
LIITTEET 57
Liite 1: Louhi Net Oy haastattelu 21.3.2012 58
Liite 2: Yritys X, haastattelu 9.5.2012 62
Liite 3: Valtion virasto Y:n haastattelu 21.5.2012 64
Liite 4: Kysely Ficoran IPv6-liikenteestä 4.5.2012 66

1. Johdanto

1.1 Työn tarkoitus, tausta ja tavoitteet

Tämän opinnäytetyön tarkoituksena on tutkia, mitä asioita täytyy ottaa huomioon siirryttäessä IPv4-verkosta IPv6-verkon käyttöön. Tarkoituksena on selvittää, mitä toimia organisaatioiden tulisi tehdä IPv6:n käyttöönottoprosessin aikana. Työn tarkoitus on selvittää ja analysoida IPv6:n käyttöönoton vaikutuksia eri organisaatioiden näkökulmasta ja miten siihen on valmistauduttu. Tarkoitus on tutkia IPv6:n vaikutusta eri organisaatioissa. Kohdeorganisaatiot ovat valtion virasto Y (joka ei halunnut nimeään mainittavan opinnäytetyössä), sekä yrityksistä internet hostingpalveluita tarjoavaa Louhi Net Oy ja kosmetiikka- ja muita kulutustuotteita tarjoava yritys X (joka ei myöskään halunnut nimeään mainittavan opinnäytetyössä).

Tavoitteena on luoda edellytykset IPv6:n laajempaa käyttöä varten ja mahdollistaa jatkotutkimukset aiheen tiimoilta. Työssä selvitetään organisaatioiden IPv6-valmiutta ja sen käyttömahdollisuuksia tulevaisuudessa. Tarkoitus on selvittää organisaatioiden IPv6-tilannetta ja IPv6-tietoisuutta, sekä mitä siirtyminen IPv6:sen käyttöön merkitsee organisaatiolle ja millä aikataululla sekä keinoilla organisaatiot ovat siirtymään valmistautumassa. Tavoitteena on tehdä yleisluontoinen ohjeistus asioista, mistä organisaatioiden kannattaa ottaa huomioon IPv6-verkon käyttöön siirryttäessä.

Lisäksi työssä yritetään saada hahmoteltua kuva IPv6:n tämänhetkisestä tilanteesta Suomessa ja myös maailmalla. Tarkoitus on selvittää, miten yritykset ja muut organisaatiot ovat ottaneet IPv6:n käyttöön ja miten paljon IPv6-liikenne on lisääntynyt viime vuosien aikana. Tarkoitus olisi myös hieman pohtia IPv6:n tulevaisuutta Suomessa.

1.2 Työn rakenne ja rajaus

Opinnäytetyö koostuu neljästä pääosiosta: internet-protokollia sekä IPv4- ja IPv6-verkkoja käsittelevästä teoriaosuudesta, yleisestä IPv6-tilanteesta Suomessa ja maailmalla, IPv6:n käyttöönoton ohjeistuksesta organisaatioille ja kohdecaseorganisaatioiden IPv6-siirtymisestä. Lisäksi työ sisältää asiaan kuuluvat johtopäätökset ja yhteenvedot.

Organisaatioiden haastatteluilla pyritään saamaan tietoa kyseisten organisaatioiden IPv6-tilanteesta ja tämän pohjalta tehdä arvioita heidän IPv6-tarpeesta. Näitä saatuja tuloksia myös verrataan yleisiin tilastoihin ja tietoihin Suomessa tapahtuvasta IPv6-migraatiosta ja selvitetään millainen kohdeorganisaatioiden tilanne on verrattuna yleiseen

tilaan. Jokaisen caseorganisaation edustajaa tullaan haastattelemaan. Haastattelukysymykset eroavat hieman toisistaan, riippuen siitä millainen organisaatio on kyseessä. Lopuksi haastatteluiden tulokset tullaan analysoimaan. Lopuksi tehdään johtopäätökset opinnäytetyön teon aikana tehdyistä havainnoista, jotta saadaan kokonaiskuva IPv6:n vaikutuksesta.

Opinnäytetyössä on pyritty rajaamaan tutkittava asia tarkasti. Tässä työssä ei perehdytä eri teknisiin ratkaisuihin organisaatiolle, eikä sen syvällisemmin pohdita tai esitetä näitä vaihtoehtoja, vaan opinnäytetyön pääpainona on tekniikoiden tutkimista teoriatasolla organisaatioilta saatujen tietojen pohjalta. Erilaisista organisaatiocaseista huolimatta, on etenkin IPv6-ohjeistus haluttu pitää mahdollisimman yleispätevänä, jotta se voisi soveltua monien erityyppisten organisaatioiden käytettäväksi. Tästä syystä eri caseorganisaatioille ei ole tehty erikseen tarkkoja suunnitelmia IPv6:seen siirtymisestä.

Lisäksi opinnäytetyöhön sisältyvä tilastollinen analyysi eri maiden IPv6-liikenteestä on rajattu melko pintapuoliseksi, eikä sen suhteen ole tehty syvempää tutkimusta pidemmältä aikaväliltä vaan saadut tiedot painottuvat lähivuosiin.

2. Internet-protokollat

Tässä luvussa käsitellään internetprotokollia, pääasiassa TCP/IP:tä. IPv4- ja IPv6-protokollaversiolle on tässä työssä varattuna omat lukunsa.

2.1 TCP/IP

TCP/IP on verkkolaitteiden kommunikointiin tarkoitettu protokollajärjestelmä, jonka tehtävänä on mahdollistaa eri verkkolaitteiden välinen kommunikointi. TCP/IP koostuu kahdesta eri protokollasta, IP:stä (Internet Protocol) joka toimii verkkokerroksessa ja TCP:stä (Transmission Control Protocol) joka toimii kuljetuskerroksessa. TCP/IP tarjoaa maailmanlaajuisen IP-osoiteavaruuden, joka mahdollistaa eri verkkolaitteiden toiminnan riippumatta näiden fyysisestä sijainnista tai käytettävästä tekniikasta. Tästä syystä TCP/IP:stä on tullut standardi puhuttaessa verkkolaitteiden kommunikointitekniikoista. (Kaario 2002, 15.)

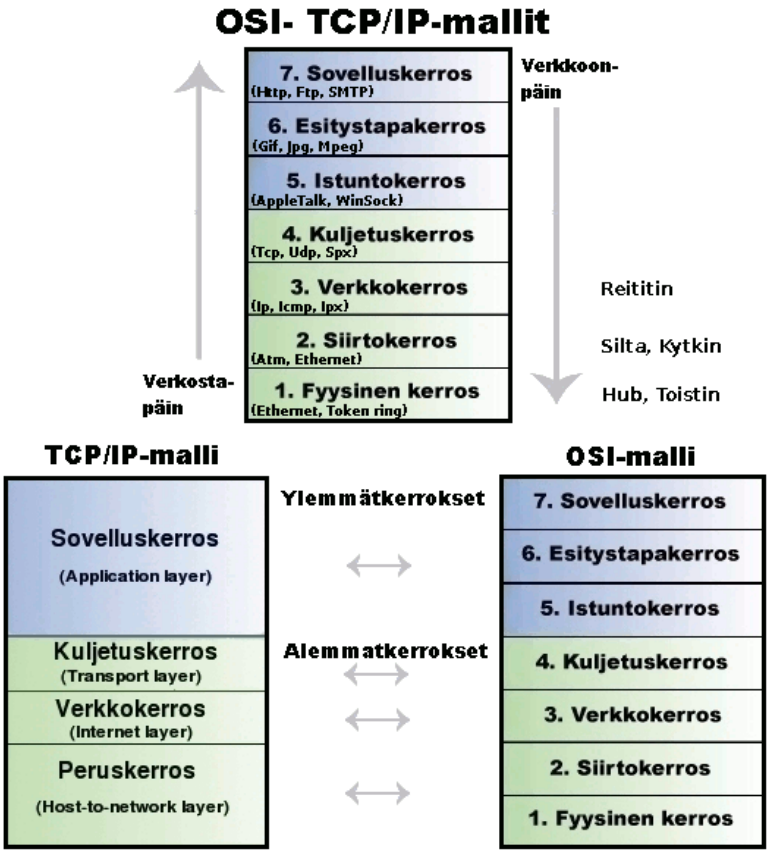
TCP/IP malli poikkeaa OSI-mallista siten, että kerrokset on jaettu 5 eri kerrokseen: fyysiseen kerrokseen, siirtokerrokseen, verkkokerrokseen, kuljetuskerrokseen ja sovelluskerrokseen joka kattaa OSI-mallin istunto-, esitystapa-, ja sovelluskerrokset. Fyysisen kerroksen ja siirtokerroksen protokollia ei ole erikseen määritelty TCP/IP mallin standardeissa, vaan näissä voidaan käyttää erilaisia protokollia. (Kaario 2002, 21-23.)

TCP/IP-verkoilla yhdistetään monenlaisilla käyttöjärjestelmillä toimivia ja erilaisiin tarkoituksiin suunniteltuja laitteita joustavasti toisiinsa. TCP/IP:tä voidaan käyttää monissa eri muodoissa, tavallisten kiinteiden lähiverkkojen lisäksi langattomassa ympäristössä, automaatioverkoissa – ja oikeastaan missä vain, mihin yleensä on mahdollista toteuttaa TCP/IP protokollaohjelmisto eli protokollapino. Mikään muu tietoliikenteen verkkoteknologia ei ole saavuttanut samanlaista monikäyttöisyyttä. (Kaario 2002, 14.)

TCP/IP tarkoittaa yhtä prokollaperhettä, joka rakentuu verkkokerroksen protokollan ympärille. TCP/IP:n verkkokerroksen nimenä on Internet Protocol (IP). Toinen TCP/IP-protokollaperheen nimeen päässeistä protokollista on Transmission Control Protocol (TCP), joka on IP-protokollan yläpuolella kuljetuskerroksella toimiva luotettavan palvelun takaava protokolla. Muita TCP/IP-protokollaperheeseen kuuluvia protokollia ovat esimerkiksi User Datagram protocol (UDP), verkkohallintaprotokolla Simple Network Management Protocol (VRRP) ja reititysprotokolla Open Shortest Path First (OSPF). Tämän päivän IP ja sitä kautta koko TCP/IP-protokollaperhe on 1960-luvun loppupuolella alkunsa saaneen ARPANET:in jälkeläinen. (Kaario 2002, 14–15.)

2.2 TCP/IP:n viitemalli

TCP/IP on viitemalli, jota käytetään kuvaamaan internetin tietoliikenneverkkojen arkkitehtuuria (kuva 1). TCP/IP muodostuu kahdesta pääprotokollasta, TCP:stä ja IP:stä. Kun TCP/IP:tä kehitettiin, oli OSI-malli jo olemassa mutta TCP/IP:n malli ei noudattanut sitä. Kuitenkin molemmissa malleissa on monia yhtäläisyyksiä. Eniten mallit muistuttavat toisiaan tärkeissä Kuljetus ja Internet kerroksisssa. TCP/IP koostuu neljästä kerroksesta: peruskerroksesta, verkkokerroksesta, kuljetuskerroksesta ja sovelluskerroksesta. (Casad 2011, 26-28.)



Kuva 1: TCP/IP - malli ylimmästä alimpaan (Krimaka)

2.2.1 Peruskerros / siirto- ja fyysinenkerros (Network Access Layer)

Peruskerros muuntaa datan sähköiseksi tai analogiseksi pulssiksi fyysiseen verkkoon. Peruskerroksen käyttämää protokollaa ei ole määritelty IETF:n RFC-dokumenteissa, vaan näissä voidaan käyttää monia erilaisia protokollia. Periatteessa tässä voidaan käyttää mitä tahansa verkkotekniikkaa, yleisin käytettävä tekniikka on Ethernet. TCP/IP pinossa alimmat kerrokset voivat kuitenkin koostua useammista eri protokollista, ei pelkästään yhdestä. (Casad 2011, 27; Kaario 2002, 21-22.)

2.2.2 Verkkokerros (Internet Layer)

Verkkokerroksen tehtävänä on reitittää datapaketteja verkon läpi oikeaan kohteeseen. Verkkokerroksella voi olla myös muita tehtäviä, kuten vuonvalvonta ja laatuvaatimusten tarkkailu. Jokainen datapaketti reititetään itsenäisesti parasta mahdollista reittiä pitkin, eikä yhteyden osapuolten välillä ole olemassa erillistä sopimusta yhteyden olemassaolosta, vaan puhutaan yhteydettömästä tiedonsiirrosta. (Kaario 2002, 20.)

2.2.3 Kuljetuskerros (Transport Layer)

Kuljetuskerroksen tehtävän on huolehtia suoran yhteyden muodostamisesta lähde- ja kohdekoneiden välille. Tätä hoitavat mm. TCP ja UDP protokollat. Kuljetuskerros toimii alempien datakerrosten ja ylempien sovellusprosessien välillä. Yksi kuljetuskerroksen protokollan tehtävä on myös huolehtia pakettien vastaanottojärjestyksestä ja uudelleenlähetyksistä. (Kaario 2002, 21.)

2.2.4 Sovelluskerros (Application Layer)

TCP/IP:n ylin kerros on sovelluskerros. Sovelluskerros koostuu eri verkkomenetelmistä ja palveluista, jotka kommunikoivat alemman kerroksen TCP ja UDP porttien kautta. Sovelluskerroksen osat voivat vaihdella monen eri käyttötarkoituksen mukaan. Tunnetuimpia sovelluskerroksen protokollia ovat mm. FTP, SMTP, DNS, RIP ja HTTP. (Casad 2011, 114; Microsoft TCP/IP Protocol Architecture.)

2.3 Standardit

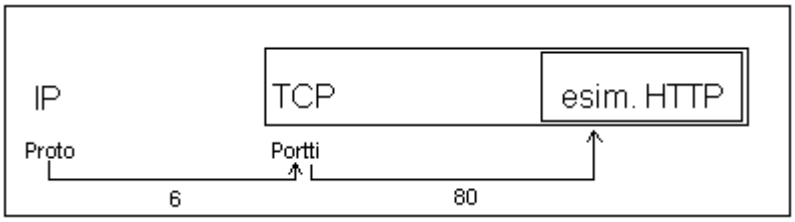
Internetin ja TCP/IP-protokollaperheen kehityksestä vastaa ja ohjaa joukko organisaatiota, kuten IETF-standardointiorganisaatio, ISOC – Internetin katto-organisaatio, W3C – www-organisaatio, IEEE – kansainvälinen tekniikan alan järjestö ja joukko muita organisaatioita. TCP/IP:n määritykset määritellään ja julkaistaan IETF:n hyväksymissä RFC-sarjan dokumenteissa. Ennen määritystä varsinaiseksi RFC-sarjan dokumentiksi, siitä tehdään ensin luonnos eli Internet draft, josta se kehittyy eri vaihdeiden kautta lopulta virallinen standardi. (Kaario 2002, 16-17.)

2.4 IP eli Internet Protocol

Verkkokerroksessa sijaitseva IP-protokolla on TCP/IP:n keskeisin protokolla. Vaikka TCP/IP-rakenteessa on monia eri protokollia, on IP niistä tärkein sillä verkko rakentuu sen ympärille. Ehkä tärkein IP:n pohjalta rakentunut verkko on Internet. Verkossa data reititetään IP-osoitteiden avulla, verkossa sijaitsevia ethernet- tai muulla verkkotekniikalla toimivia kokonaisuuksia voidaan niputtaa IP-aliverkoiksi. Reitittimet välittävät verkossa vain IP-paketteja, eikä reitittimiä kiinnosta alemman tai ylemmän tason protokollat. (Kaario 2002, 45-46, 53.)

2.5 IP-protokollat

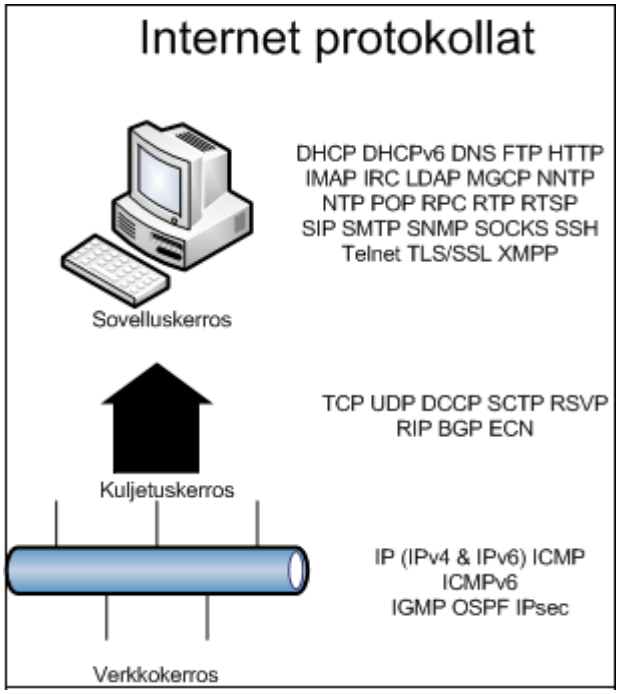
Verkossa kulkevassa IP-paketissa kuljetettavat eri protokollat on numeroitu. Protokollan numerosta vastaanottaja tietää, mitä IP-paketiti sisältää (kuva 2). IP-paketissa kuljetettavia protokollia ovat mm. ICMP, TCP, UDP, IPv6, GRE, ESP, AH ja OSPF. (IANA, protocol numbers.)



Kuva 2: IP-paketti

2.6 Standardointi ja versiot

Yleisein käytössä oleva versio IP:stä on IPv4. Sen seuraajaksi on kaavailtu IPv6:sta, jonka pitäisi korvata IPv4 tulevaisuudessa. Suurimpana syynä IPv6:n käyttöönottoon on käyttökelpoisten IPv4-osoitteiden loppuminen. Tarvetta IPv6:n siirtymiseen on vähentänyt NAT ja CIDR, joiden avulla on paikattu IPv4-osoitepulaa. IPv6:n etuna verrattuna IPv4:n on osoiteavaruuden koko, joka mahdollistaa suuremman tietokoneiden ja laitteiden määrän verkossa. IPv4:n ja IPv6:n yhteiskäyttöä heikentää se, että ne eivät ole suoraan yhteensopivia vaan erilaisia tekniikoita tarvitaan niiden yhteensovittamiseksi. (Casad 2011, 54, 282-283.)



Kuva 3: Internet protokollat

2.7 OSI-malli

OSI-malli on kansainvälisen standardointijärjestö ISO:n (International Standards Organization) kehittämä tietojärjestelmien viitemalli laitevalmistajille ja verkkojenkäyttäjille. OSI-malli perustuu kerrosajatteluun, jossa eri toiminnot pilkotaan eri kerroksiin. OSI-malli jakautuu seitsemään eri protokollakerrokseen. Jokainen näistä kerroksista on riippumaton toisistaan, mutta kuitenkin tukeutuu alla olevaan kerrokseen. (Kaario 2002, 18; Ratol.fi OSI-malli.)

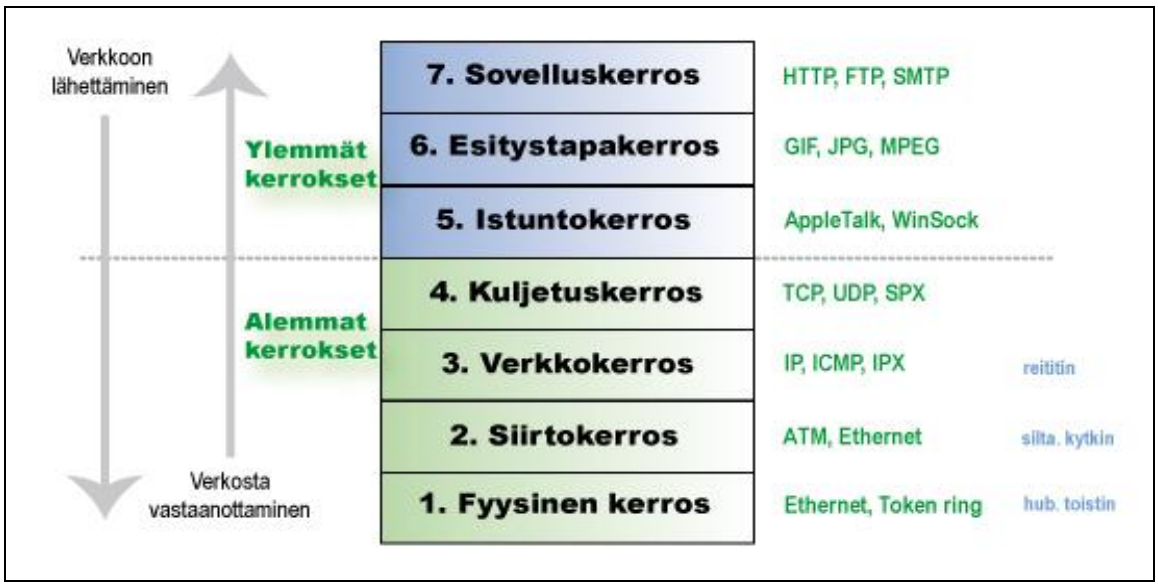
2.8 OSI-mallin rakenne

OSI-malli rakentuu seitsemästä kerroksesta joita ovat: fyysinen kerros, siirtokerros, verkkokerros, kuljetuskerros, istuntokerros, esitystapakerros ja sovelluskerros. Kerrosrakenne toimii hierarkisesti, jolloin kerros voi vastaanottaa ylemmältä kerrokselta yhteydenmuodostuskäskyn. Tämän jälkeen kerros käskee alempana olevaa kerrosta muodostamaan yhteyden ja lähettämään dataa. Eri kerrosten tehtävät on määritelty, mutta niiden toteutustapa on jätetty vapaaksi. Jokainen kerros liikennöi toiseen koneeseen vain samalla kerroksella olevan ohjelman kanssa. Tarpeen mukaan liikennöinnissä käytetty protokolla voidaan myös korvata vastaavalla protokollalla. (Kaario 2002, 18-19; Ratol.fi OSI-malli.)

OSI-malli ei ole protokolla tai tuote, vaan se suunniteltiin avoimeksi standardimalliksi sovelluskehittäjille. OSI-mallin laadinta alkoi jo 1970-luvulla ja jatkuu edelleen. OSI-mallissa määritellään raamit tietoliikenteen standardointityölle ja protokollien suunnittelulle. Se tarjoaa peruskäsitteistön, jonka avulla tietoliikennejärjestelmiä rakennetaan. OSI-malli onkin ollut vaikuttajana eri protokollien suunnittelussa ja toteutuksessa. OSI-malli onkin osa standardointia, jonka tarkoitus on avointen järjestelmien yhteenliittäminen. Tämä mahdollistaa esimerkiksi yhteistoiminnan eri valmistajien tietoliikennelaitteiden, siirtopalveluiden ja verkkojen välillä. Seuraavat organisaatiot huolehtivat standardoinnista, mm. ISO ja ITU (International Telecommunication Union). (Casad 2011, 26-27; Ratol.fi OSI-malli.)

2.9 OSI-mallin kerrosten tehtävät

Jokaisella OSI-mallin kerroksella on omat tehtävänsä (kuva 4). OSI-mallin alkuperäinen malli ei pidä nykypäivänä enää täysin paikkaansa, vaan se on ajan saatossa muuttunut. OSI-mallissa oli alun perin seitsemän kerrosta, mutta alimpia kerroksia on jaettu eri alikerroksiin ja samalla myös eri kerrosten työnjako on muuttunut. (Ratol.fi OSI-malli.)



Kuva 4: OSI-malli (Wikipedia OSI-malli. 2012.)

- Sovelluskerros (Application layer)

Jota käyttäjälle näkyvät sovellukset käyttävät viestintään.

- Esitystapakerros (Presentation layer)

Vastaa muun muassa eri merkistökoodauksien yhteensovittamisesta.

- Istuntokerros (yhteysjakso, Session layer)

Huolehtii useiden yhdessä yhteydessä kulkevien istuntojen multipleksoinnista.

- Kuljetuskerros (Transport layer)

Huolehtii siitä, että paketit tulevat perille ja että ne järjestetään oikeaan järjestykseen.

- Verkkokerros (Network layer)

Välittää ylempien kerrosten tietoliikennepaketteja tietokoneiden välillä, tarjoten päästä päähän yhteyden erilaisten verkkoratkaisujen ylitse.

- Siirtokerros (Data link layer)

Kehystää ylempien kerrosten tietoliikennepaketin fyysisen kerroksen siirtoa varten.

- Fyysinen kerros (Physical layer)

Määrittelee tiedonsiirron fyysisen median, joka voi esimerkiksi olla esimerkiksi sähkökaapeli, valokuitu tai radioaalto.

3. IPv4

Internet Protocol version 4 eli IPv4 perustuu 32-bittiseen osoitejärjestelmään, joka pystyy teoriassa kattamaan kokonaisuudessaan 4 miljardia, tarkalleen 4 294 967 296, verkkoasemaa koko Internetissä. Todellisuudessa osoitejärjestelmä pystyy kattamaan vain 3,2 – 3,3 miljardia verkkoasemaa koko Internetissä johtuen IP-osoitteiden luokittelusta. (Cisco Systems 2006.)

IPv4 on yhteydetön pakettien kuljetusprotokolla. Protokolla on epäluotettava, sillä se ei sisällä minkäänlaista mekanismia, jolla se varmistaisi pakettien perille pääsyn. Paketit kulkevat Internetin läpi reitittimien kautta. Jokainen reititin toimii itsenäisesti ohjaten paketteja reititystaulun mukaisesti. Reititystaulu voi olla dynaamisesti muodostettu, jonkun reititysprotokollan muodostamana. Reititystauluun voi myös käsin kiinteästi määrätä kohde IP-osoitteen perusteella, minne paketti seuraavaksi kuuluisi lähettää. Samasta päätelaitteesta samaan kohteeseen lähteneet paketit voivat siis mennä eri reittiä kohteeseen. Tämä aiheuttaa sen, että osa paketeista saattaa viipyä reitillä pidempään, jolloin ensimmäiseksi lähetetty paketti tuleekin myöhemmin perille kuin myöhemmin lähetetyt paketit. Paketteja saattaa myös hävitä matkalla esimerkiksi verkon ruuhkaisuuden takia. (Douglas 2002, 97.)

IPv4 on nykypäivänä verkkokerroksen hallitseva protokolla. IPv4 on hyvin toimiva protokolla, jonka suurimpana heikkoutena pidetään IP-osoitteiden loppumista. Tästä syystä rinnalle on kehitelty IPv6–protokolla jolla on monikertainen osoiteavaruus IPv4-verkkoon verrattuna.

3.1 IPv4-osoitteet ja osoiteluokat

Tämä 32-bittinen järjestelmä jaettiin alun perin viiteen hierarkkiseen luokkaan, jota johtaa IANA. Kolme ensimmäistä luokkaa, A, B ja C luokka, ovat käytettävissä globaaleina ainutlaatuisina unicast IP -osoitteina. Nämä luokat asetettiin käyttäjille, joilla on erimittaisia verkkomaskeja. Verkkomaski on sarja 1 bittejä, jotka muodostavat IP-osoitteen verkko-osan. (Desmeules 2007, 6.) Kaksi viimeistä luokkaa ovat D ja E-luokka. Näiden luokkien osoitteet on varattu kokeellisiin ja multicast tarkoituksiin (Desmeules 2007, 7).

3.1.1 A-luokan osoitteet

A-luokka varaa IP-osoiteavaruudesta suurimman osan. Siihen kuuluvat osoitteet väliltä 1.0.0.0->126.0.0.0 pois lukien 10.0.0.0, joka kuuluu varattuihin verkkoihin. Luokasta on käytettävissä 124 osoiteryhmää, joihin jokaiseen kuuluu 16 777 216 osoitetta. A-luokan aliverkolle käytetään maskia 255.0.0.0 ja vastaava lyhenne on /8. Joitain A-luokan osoitteista on jaettu uudelleen B ja C luokkina, jotta osoiteavaruus ei loppuisi kesken.

3.1.2 B-luokan osoitteet

B-luokat ovat välillä 128.0.0.0->192.167.255.255. Luokasta on käytettävissä 16487 verkkoa, johon voi kuulua maksimissaan 65535 osoitetta. B-luokan aliverkko on muotoa 255.255.0.0, vastaava lyhenne on /16.

3.1.3 C-luokan osoitteet

C-luokan osoitteet ovat välillä 193.0.0.0->239.255.255.0. Kuhunkin verkkoon kuuluu 255 osoitetta. C-luokan aliverkko on muotoa 255.255.255.0, vastaava lyhenne on /24.

3.1.4 Varatut osoitteet

Osoitteita on varattu myös tietty määrä yksityiseen käyttöön, verkkolaitteiden suorituskykytestaukseen, loopback osoitteeksi, dokumentointi ja esimerkkikäyttöön, multicastingiin sekä tulevaisuuden käyttöön (kuva 5).

Verkon luokka	Verkon peitto (netmask)	Verkon osoite
A	255.0.0.0	1.0.0.0 - 126.255.255.255
B	255.255.0.0	128.0.0.0 - 191.255.255.255
C	255.255.255.0	192.0.0.0 - 223.255.255.255
D (Multicast)	255.255.255.0	224.0.0.0 - 239.255.255.255
E (Varattu)	—	240.0.0.0 - 255.255.255.255

Kuva 5: Osoiteluokat

3.2 NAT (Network Address Translation)

NAT syntyi, kun huomattiin IP-osoitteiden olevan loppumassa maailmasta, jossa Internet kasvoi yhtäkkiä odottamattoman paljon. Tarkkaa lukumäärää verkossa oleville verkkolaitteille ei tiedetä mutta arviolta se on 100 miljoonaa isäntälaitetta ja yli 350 miljoonaa käyttäjää koko Internetissä. Kasvuvauhti on ollut niin kova, että Internet kaksinkertaistaa kokonsa joka vuosi. (Cisco Systems 2006.)

3.2.1 NAT:in toiminta

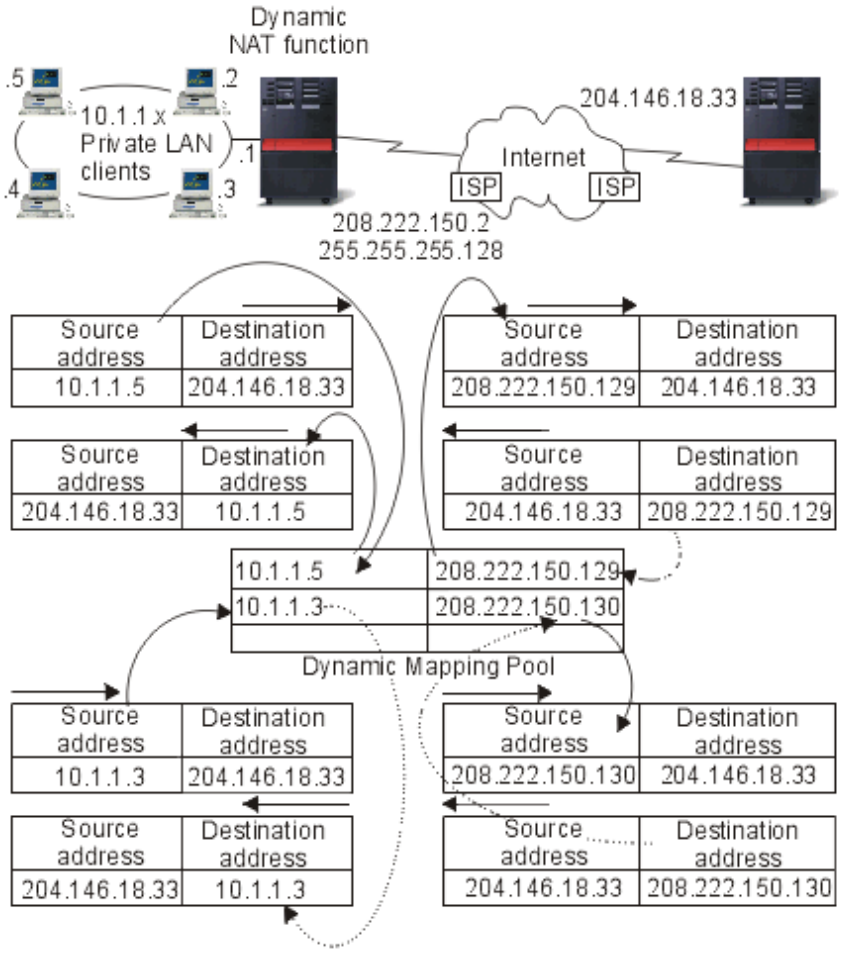
NAT-tekniikka mahdollistaa reitittimen olon ”agenttina” Internetin ja paikallisen verkon välissä. Tämä tarkoittaa sitä, että riittää vain yksi julkinen IP-osoite monelle sisäverkon yksityiselle osoitteelle eli monta yksityistä sisäverkon konetta pystyy liikennöimään Internetissä yhdellä julkisella IP-osoitteella. Lisäksi NAT lisää turvallisuutta ja hallittavuutta. (Cisco Systems 2006.)

3.2.2 Dynaaminen NAT

Dynaamisen NAT tekniikan avulla voidaan muodostaa yhteys ainoastaan yksityisestä verkosta julkiseen verkkoon. Yhteyttä muodostaessa jokaiselle yhteydelle noudetaan julkinen IP-osoite osoitealtaasta. Jokainen yhteys saa oman uniikin julkisen osoitteen. Yhtäaikaisia yhteyksiä on mahdollista muodostaa niin monta kuin on IP-osoitteita osoitealtaassa. Dynaaminen NAT mahdollistaa yhteyden muodostamisen Internetiin dynaamisen NAT-osoitteen kautta (kuva 6). (Dynamic NAT 2012.)

Yksi NAT:in muoto on Overloading, jota kutsutaan myös PAT-tekniikaksi. PAT-tekniikan toimii niin, että se tarvitsee vain yhden tai muutaman julkisen IP-osoitteen eikä paljon julkisia IP-

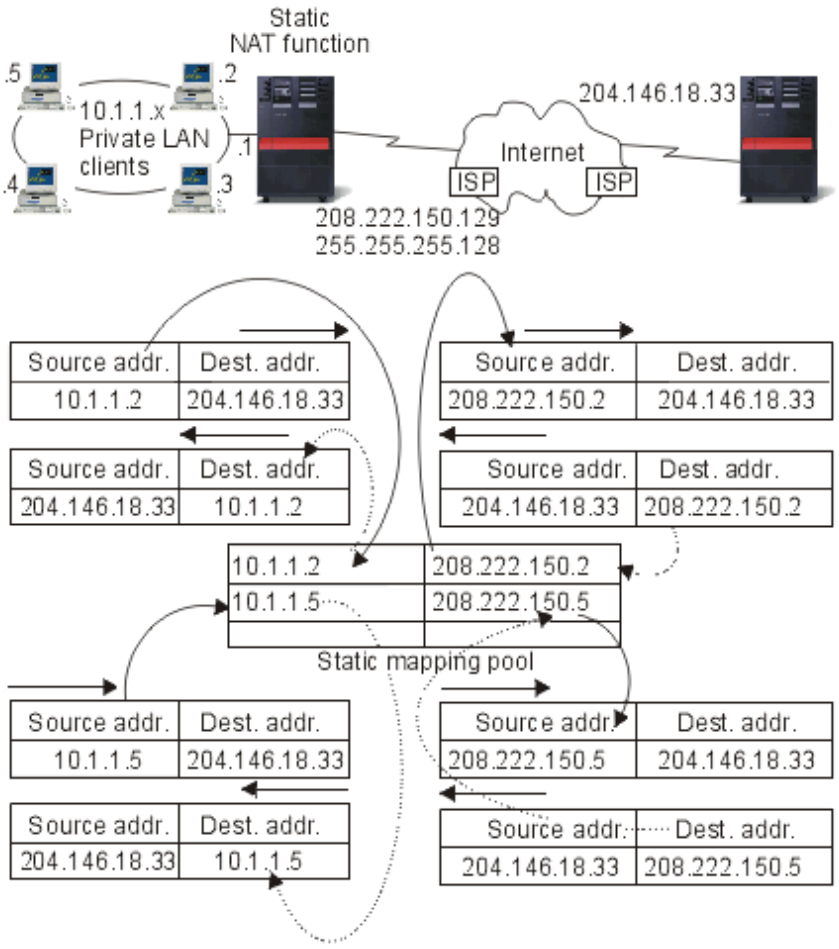
osoitteita. Tähän on syynä se, että PAT erottelee eri istuntoja verkossa porttinumeron perusteella. Mikäli käyttäjä haluaa päästä Internetiin sisäisestä verkosta, käyttäjä lähettää pyynnön reitittimelle, jossa NAT-protokolla on käytössä. Tämän jälkeen reititin kääntää paketin IP-osoitteen ja porttinumeron käyttämään reitittimen julkista IP-osoitetta ja samaa porttinumeroa, jos porttinumeroa ei ole varattu jonkun muun käyttäjän toimesta julkisessa verkossa. Tämän muunnoksen jälkeen reititin välittää paketin kohteeseen. Kaikki NAT-porttikartoitukset ovat tallennettuna reitittimen NAT-tauluun.



Kuva 6: Dynaaminen NAT-toiminta. (Dynamic NAT)

3.2.3 Staattinen NAT

Staattinen NAT tekniikan avulla voidaan toteuttaa yhden yksityisen osoitteen ja yhden julkisen osoitteen yhdistäminen (kuva 7). Yhdellä yksityisellä/sisäisellä IP-osoitteella on koko ajan yksi ja sama julkinen/ulkoinen IP-osoite käytössä. Staattisesta NAT-tekniikasta on erityisesti hyötyä silloin, kun yksityisen verkon laitteeseen täytyy päästä käsiksi julkisesta verkosta päin. (Static NAT 2012.)



Kuva 7: Staattinen NAT-toiminta. (Static NAT.)

3.3 IPv4 otsikkokenttä (header)

IP-paketit kulkeutuvat verkossa erilaisten linkkikerrosten yli, jotka voivat olla esimerkiksi Ethernet (10 Mbps), Fastethernet (100 Mbps), Gigabit Ethernet (1000 Mbps), ja monien muiden linkkikerroksen teknologioiden kautta. Kaikilla linkkikerrosteknologialla on omanlaisensa linkkikerroskehys, joka kuljettaa IP-paketteja. IP-paketti koostuu kahdesta olennaisesta osasta, IP-otsikkokentästä sekä Payload-osasta.

IP:n otsikkokenttä sisältää kaikki reitittimen tarvitsemat lähetys- ja vastaanottotiedot. Otsikkokenttä sisältää tiedot kuten lähettäjän, vastaanottajan, kuljetusprotokollan ja monia muita tietoja. Otsikkokentän pituus voi vaihdella 20 ja 60 tavun välillä. Enintään se voi kuitenkin olla 65 535 tavua. Kaikki järjestelmät eivät osaa käsitellä näin suurta otsikkokenttää, joten suurin mahdollinen toimiva koko voi olla 576 tavua. (Young 2006; Desmeules 2007, 41.)

Payload tarkoittaa lähetettyä informaatiota eli dataa. (Young 2006; Desmeules 2007, 41.)

3.4 IPv4:n otsikkokentän rakenne

IP-paketti koostuu pakollisista otsikkotiedoista ja data-osioista (kuva 8).

+	0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	versio	otsikon pituus	palveluluokka	kokonaispituus	
32	fragmenttitunnus			liput	fragmentin paikka
64	elinaika		protokollan numero	otsikon tarkistussumma	
96	lähdeosoite				
128	kohdeosoite				
160	Optiot				
192	Data				

Kuva 8: IPv4:n otsikkokentän rakenne (Wikipedia IP-paketti. 2012.)

- Versio (Version)

Versiokenttä identifioi mitä versiota käytetään. Tässä tapauksessa se on IPv4. Kentän pituus on 4 tavua.

- Otsikon pituus (IHL Header Length)

Tämä kenttä ilmaisee IP-paketin otsikon pituuden 32 bittinä. Kentän pituus on 4 tavua.

- Palveluluokka eli TOS (Type of Service)

Tämä kenttä ilmaisee paketin prioriteetin joka voi olla: todella kiireellinen, kiireellinen, tai normaali toimitus. Prioriteetti määräytyy toimituksen tärkeyden, viiveen tai luotettavuuden mukaan.

- Kokonaispituus (Total Length)

Tavuina ilmoitettu IP-paketin pituus, johon sisältyy otsikkokenttä ja itse data. Tämä osa sallii IP-paketin pituudeksi enintään 65 535 tavua. Suurimmat osat verkoista ja niiden laitteista eivät tue enintään kun 576 tavua suuria IP-paketteja. (TCP/IP Suite 2012.)

- Tunniste (Identifier)

Tämän kentän avulla kasataan IP-paketin osat yhteen.

- Liput (Flags)

Tavuina ilmoitettu IP-paketin pituus, johon sisältyy internet-header ja itse data. Tämä osa sallii IP-paketin pituudeksi enintään 65 535 tavua. Suurimmat osat verkoista ja niiden laitteista eivät tue enintään kun 576 tavua suuria IP-paketteja. (TCP/IP Suite 2012.)

- Fragmenttitunnus (Fragment Offset)

Tämän kentän avulla on mahdollista päätellä mihin mikäkin osa kuuluu IP-paketissa.

- Paketin elinaika (TTL, Time to live)

Tämä kenttä ilmaisee ajan kuinka kauan IP-paketti saa olla Internetissä. Mikäli tämän kentän arvo on nolla, niin IP-paketti on tuhottava.

- Protokolla (Protocol)

Tämä kenttä ilmaisee seuraavan kerroksen protokollan IP-paketille.

- Tarkistussumma (Header checksum)

Tavuina ilmoitettu IP-paketin pituus, johon sisältyy otsikkokenttä ja itse data. Tämä osa sallii IP-paketin pituudeksi enintään 65 535 tavua. Suurimmat osat verkoista ja niiden laitteista eivät tue enintään kun 576 tavua suuria IP-paketteja. (TCP/IP Suite 2012.)

- Lähde- ja kohdeosoite (Source and Destination Address)

Lähettäjän- ja vastaanottajan IP-osoite.

- Optiot (Options)

Tämä kenttä on vapaasti valittava. Sen koko määräytyy käyttötarkoituksen mukaan.

- Tieto (Data)

Tämä kenttä sisältää IP-paketin varsinaisen datan, joka yleensä alkaa seuraavan tason protokollan otsikolla.

4. IPv6

IPv6 on IPv4 seuraaja, jonka tarkoituksena on tulevaisuudessa korvata IPv4 kokonaan. Suurimpana syynä siirtymiseen IPv6-osoitteisiin on kasvava laitekanta ja osoitetarve. Tämä on aiheuttanut sen, ettei IPv4-osoitteita riitä enää kaikille. IPv4-osoitteiden ja myös IPv6-osoitteiden jakamisesta vastaa Internetin katto-organisaatio, joka edelleen jakaa osoitteita eri ISP:lle eli palveluntarjoajille. IPv6 syntyi käytännössä vuonna 1991, silloin tehtiin ensimmäiset merkittävät päätökset uuden IP-protokollan kehittämiseksi. Vuonna 1998 tehtiin merkittävät IPv6-standardoinnit.

IPv6:n suurimpana etuna suhteessa sen edeltäjään IPv4:n, on suurempi osoiteavaruus, eli 128 bittisenä käyttökelpoisia osoitteita on yhteensä tarjolla 2^128 kappaletta. Käytännössä IPv6-osoitteita on loputon määrä nykysukupolville. 32-bittisessä IPv4:ssä osoitteita on ”vain” 3 miljardia, kuitenkin IPv4-osoiterakenteen takia suurin osa osoitteista jää käyttämättä.

IPv6:n etuna ei pelkästään ole vain suurempi osoiteavaruus, vaan myös monia teknisiä parannuksia on tehty, jotka mm. lisäävät ominaisuuksia ja parantavat tietoturvaa. Yksi suurimmista muutoksista mitä IPv6 tuo, on paranneltu ja yksinkertaistettu kehysrakenne ja otsikkokentät. Verrattuna IPv4:n, on IPv6:ssa pakollisten kenttien määrä pudonnut kahdestatoista kahdeksaan ja samalla optiokenttien määrä on lisääntynyt. IPv6:n otsikkokenttien jatkoksi voidaan ketjuttaa lisää otsikkokenttiä tarpeen mukaan, tämä tekee IPv6:sta erittäin joustavan ja monipuolisen protokollan joka mahdollistaa tehokkaan jatkokehityksen.

Muita paranneltuja ominaisuuksia IPv6:ssa on pakettien pilkkominen verkossa. Vanha IPv4 sallii pakettien pilkkomisen reitittimessä, IPv6:ssa tämä on kiellettyä. IPv6-pakettien pilkkominen tapahtuu jo verkon reunalla paketin alkuperäisen lähettäjän toimesta. Tämä on myös johtanut siihen, että IP-pakettien välityksen koko verkossa on kasvanut IPv4:n 68 tavun mittaisesta IPv6:n 1280 tavun mittaiseksi. (Kaario 2002, 108-109.)

4.1 IPv6:n tietoturva

IPv4:n verrattuna IPv6:ssa tietoturvaominaisuudet ovat aivan toista luokkaa. IPv4:n tietoturva on protokollassa lisäominaisuutena, on se jo IPv6-protokollan suunnittelussa otettu huomioon ja tehty kiinteäksi ominaisuudeksi osana protokollaa. IPv6-protkollassa kehysrakenteen lisäoptio-otsikot mahdollistavat erilaisia tietoturvaominaisuuksia myös ylemmissä protokollakerroksissa. Näin tietoturvaominaisuudet ulottuvat, ei pelkästään perinteisen sovellukselta sovellukselle tasolle, vaan myös reitittimeltä reitittimelle. IPv6:ssa on myös parannettu palvelun laatua eli QoS (Quality of Service) vuontunnisteilla ja luokkakentällä,

näillä ominaisuuksilla IPv6:n pakettien priorisointi ja jakaminen verkossa onnistuu entistä paremmin. (Kaario 2002, 126.)

4.2 IPv6-osoitteen muoto ja varatut osoitteet

IPv6-osoite eroaa jo ulkonäöllisesti IPv4-osoitteesta merkittävästi. IPv6-osoite esitetään heksadesimaalilukuna esim. 1F80:BAD8:3120:0:0:0:FF01:800. Yksi ongelma IPv6-osoitteissa on juurikin pituus ja vaikea muoto, joka tekee sen hankalaksi ulkoa muistettavaksi. IPv6-osoite voidaan kuitenkin lyhentää käyttämällä kahta peräkkäistä kaksoispistettä, jos osoitteessa esiintyy riittävästi nollia. Esim. osoite 0:0:0:0:0:0:0:0 voidaan esittää muodossa :: tai edellä mainittu 1F80:BAD8:3120:0:0:0:FF01:800 muodossa 1F80:BAD8:3120::FF01:800. IPv4-osoite voidaan myös esittää IPv6-muodossa 0:0:0:0:0:0:x:x:x:x missä x.x.x.x on IPv4-osoitteen normaalimuoto. (Kaario 2002, 111.)

IPv4-osoitteiden tavoin myös IPv6-osoiteavaruudessa on tiettyjä osoitteita, jotka on varattu erityiskäyttöön. Näitä ovat esim. 0...00 eli koko osoite pelkkiä nollia, joka kuvastaa osoitteen puuttumista. 0...01 (127 kpl nollia) on varattu loopbackiin, eli paketin lähettämiselle itselle. 0...0:FFFF (80 kpl nollia) on varattu nykyisille IPv4-osoiteavaruudelle muutettavaksi IPv6-muotoon. Muista osoitteista 11111111 on varattu multicastiin ja 1111111010 link-local unicastiin automaattiseen osoitteen konfigurointiin. (Casad 2011, 287–288.)

4.3 Aliverkotus (subnetting) ja CIDR

IPv4:n tavoin myös IPv6:ssa onnistuu aliverkotus. IPv6 käyttää myös CIDR:iä (classless interdomain routing), joka tuli yleiseksi tavaksi aliverkotukselle IPv4:ssä, kun vanhasta luokkapohjaisesta jaosta luovuttiin. CIDR muodossa IP-osoite esitetään lisäämällä IP-osoitteen perään /x jossa x on numero, joka kertoo bittien määrän verkossa ja aliverkossa. Esimerkkinä IPv4-osoite 205.123.196.183/25. IPv6-osoitteessa tämä toimii samalla tavalla. (Casad 2011, 289.)

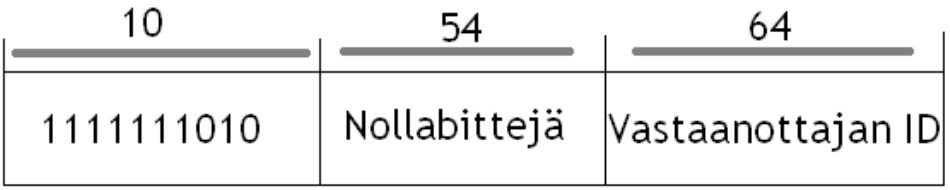
IPv6-osoiteavaruus eroaa aliverkotuksessa paljon IPv4:n vastaavasta. IPv6 on kooltaan 128 bittiä, joista aliverkotus vie ensimmäiset 64 bittiä ja jälkimmäinen 64 bittiä on varattu host ID:lle. Koska käytettäviä host ID:tä on miljoonia, ei aliverkotukselle sinänsä ole tarvetta pelkästään IP-osoitteiden säästämisen takia. Tämmöinen määrä hosteja pitäisi riittää suurempaankin määrään verkkoja. Kuitenkin verkon ylläpitäjä voi tarvittaessa haluta rajata verkkoa aliverkkoihin esim. verkon liikenteen hallitsemiseksi. Tällöin osoitteen ensimmäiset 64 bittiä mahdollistavat riittävästi tilaa verkon ja aliverkon osille. Esim. jos halutaan jakaa verkko /48 osoitelaajuuden mukaisesti, se jättää 16 bittiä aliverkoille ja 64 bittiä host ID:lle. (Casad 2011, 289.)

4.4 IPv6 Unicast-osoite

IPv6-protokollassa ei ole erikseen määritelty erillistä luokkajakoa kuten IPv4:n A-, B-, ja C-luokat, vaan osoitteet ovat unicasteja. Osoitteet ovat kuitenkin jaettu eri tasolle aliverkotuksen mukaan. Nämä tasot ovat globaali, aluekohtainen ja linkkikohtainen taso. (Kaario 2002, 112.)

4.4.1 Linkkikohtainen osoite (link local)

Link local eli linkkikohtainen osoite on IPv6-osoite, joka on määritelty vain yhdelle linkkivälille ja reitittimen ei tule välittää sitä muualle. Link local vastaa IPv4-protokollan yksityisiä IPv4-osoitteita. Link local osoitetta on tarkoitus käyttää lähiverkossa mm. naapureiden määrittelyssä ja laitteiden automaattisessa konfiguroinnissa. Tämä mahdollistaa sen, että tietokoneet pystyvät kommunikoimaan lähiverkossa ilman manuaalista konfigurointia tai automaattista konfigurointia DHCP:n kautta. Link local osoitteessa ensimmäiset 10 bittiä kuvastavat linkkikohtaista osoitetta, tämän jälkeen tulee 54 nollabittiä ja sen jälkeen 64 bittiä, jotka kertovat vastaanottajan ID:n. (Casad 2011, 290; Kaario 2002, 112–113.)



Kuva 9: Link Local osoite

4.4.2 Aluekohtainen osoite (site local)

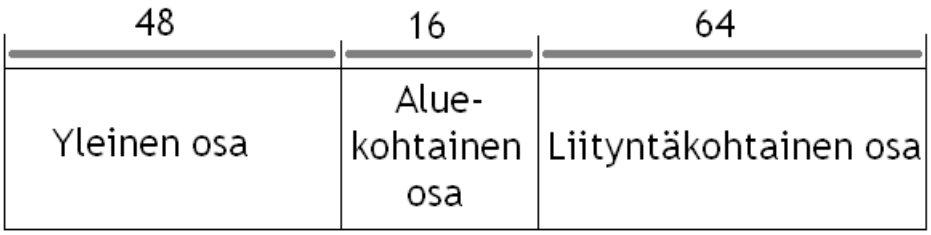
Site local eli aluekohtaiset osoitteet ovat tarkoitettu käytettäväksi yhden yhtenäisen alueen sisällä, esimerkiksi yrityksen sisäverkossa. Aluekohtaiset osoitteet ovat määritelty tietylle alueelle, jolloin reitittimet eivät saa välittää aluekohtaisia osoitteita kyseisen alueen ulkopuolelle. Site local osoitteessa osoite alkaa 10 bitillä, jonka jälkeen tulee 38 nollabittiä. Seuraavana on 16 bitin osuus, joka kertoo aliverkkotunnuksen. Viimeiset 64 bittiä kertovat Link local osoitteen tavoin vastaanottajan ID:n. (Kaario 2002, 112–113.)

Kuva 10: Site local osoite

4.4.3 Globaali osoite (global)

Tärkein kolmesta eri osoitetyypistä on Global eli globaali IPv6-osoite. Globaali osoite muodostuu kolmesta eri osasta: yleisestä osasta, alueellisesta osasta ja vastaanottajan ID osasta.

Yleinen osa on tarkoitettu palveluntarjoajia ja internetoperaattoreita varten, tämä estää sen, että aluekohtaisen osoitteen haltijat tarjoaisivat datasiirtopalveluita oman verkkonsa ulkopuolelle. Yleinen osa on kooltaan 48 bittiä, joka jakautuu vielä ylimmän tason tunnukseksi (13 bittiä) ja seuraavan tason tunnukseksi (24 bittiä). Mitä korkeampi tason tunnus on, sitä korkeampi taho huolehtii kyseisten tunnusten jakamisesta. Seuraavana on alueellinen osa (16 bittiä), joka on hierarkian alin taso. Viimeiset 64 bittiä kertovat Link Local ja Site Local osoitteiden tavoin vastaanottajan ID:n. (Kaario 2002, 113–114.)



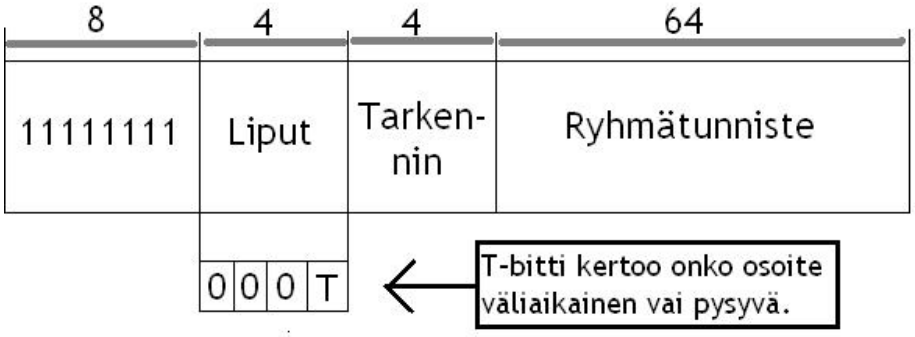
Kuva 11: Globaali osoite

4.4.4 Ryhmälähetys (multicast)

IPv6-version multicastin on tarkoitus korvata IPv4-version broadcast ominaisuus. Tarkoituksena oli kehittää IPv6:n ominaisuus joka vastaisi IPv4:n broadcastia, mutta kohdennetulle ryhmälle. IPv4:n broadcastissa viesti lähetetään jokaiselle saman verkon alla olevalle osoitteelle, joka johtaa turhaan liikenteeseen verkossa, kun kaikki vastaanottajat eivät välttämättä tarvitse kyseistä viestiä. Multicastissa hostit jakavat yhteisen multicast-

osoitteen johon viestit lähetetään, näin hostit jotka eivät kuulu kyseisen multicastryhmän piiriin eivät myöskään saa kyseistä viestiä.

Multicast osoitteessa ensimmäiset 8 bittiä ovat kaikki ykkösiä eli 11111111. Seuraavat 4 bittiä ovat lippubittejä, jotka kertovat ryhmälähetysosoitteen pysyvyydestä. Lippubiteissä ensimmäiset 3 bittiä ovat arvoltaan kaikki nollia ja neljäs bitti arvoltaan joko 0 tai 1. Jos arvo on nolla, niin kyseessä on tunnettu ja pysyvä osoite, jos taas yksi niin kyseessä on väliaikainen osoite. Lippubittejä seuraa tarkennin joka on kooltaan 4 bittiä, sen tehtävänä on tarkentaa ja kertoa lisätietoa osoitteesta. Tarkentimen arvo on väliltä 0000 – 1111, jolla jokaisella väliarvolla on oma merkitys, esim. arvo 0001 on solmukohtainen ryhmä, arvo 0010 linkkikohtainen ryhmä, 0101 aluekohtainen ryhmä ja niin edelleen. Viimeiset 64 bittiä ovat ryhmätunniste. (Casad 2011, 289–290; Kaario 2002, 59–60.)



Kuva 12: Multicast osoite

Multicastin hyötynä on sen monikäyttöisyys esim. eri taustaprosesseissa IPv6-verkossa, sekä mahdollistaa ohjelmien tehokas viestintä eri hosteille IPv6-verkossa.

4.4.5 Anycast-lähetykset

Anycast-osoitteet ovat samankaltaisia kuin muut unicast osoitteet, mutta se mahdollistaa saman IPv6-osoitteen käytön useassa eri koneessa. Anycast on tarkoitettu pääasiassa käytettäväksi palvelin – asiakas tilanteissa, joissa asiakas muodostaa kyselyn palvelimeen tai palvelinryhmään jossa on useampi palvelin. Jos palvelimet ovat yhteisessä anycast-ryhmässä, niin reititin osoittaa asiakkaalle asiakkaan kannalta lähimmän olemassa olevan palvelimen, jolloin asiakkaan ei tarvitse tietää koko ryhmästä kuin yksi osoite.

Anycastin käyttö ja hyödyntäminen on vasta kehitysasteella. Siihen liittyy paljon kysymysmerkkejä ja selvitettäviä asioita mm. sovelluskäytettävyyden ja tietoturvan osalta. Yksittäisissä kyselyissä anycast on vahva, mutta jatkuvaan yhteydenpitoon se ei tällä hetkellä

sovellu mm. sen takia koska sen käyttö TCP-protokollalla on lähes mahdotonta. (Kaario 2002, 122–123; IETF RFC2526.)

4.4.6 Naapurin tunnistus (neighbor discovery)

Neighbor discovery, eli naapurin tunnistus on palvelu joka kartoittaa laitteen ympäröivän verkon muita laitteita ja reitittimiä etsimällä näiden linkkitason osoitteita ja näin luoden aktiivisen naapuriverkon. Naapurin tunnistuksen tarkoituksena on kartoittaa aktiivisia reitittimiä ja laitteita, sekä pitää huolen että osoitteet ovat vielä aktiivisia ja samalla yrittää löytää vaihtoehtoisia reittejä epäaktiivisille reiteille.

Selvittääkseen lähiverkossa sijaitsevan IP-osoitteen, laite lähettää lähiverkkoon osoitepyynnön, joka sisältää IPv6-osoitteen jonka lähettäjä haluaa selvittää. Laite lähettää samalla myös oman fyysisen osoitteensa paluuosoitteeksi vastaanottajalle. IPv6-osoitteen omistaja lähettää laitteelle vastauksena oman fyysisen osoitteen sekä linkkitason osoitteen. (Casad 2011, 290-291; IETF RFC 4861.)

4.4.7 Autokonfigurointi (autoconfiguration)

Autokonfigurointi tarkoittaa tapaa jolla IPv6-protokollan osoite asennetaan laitteistoon, tämä voidaan hoitaa joko tilattomasti (stetaless autoconfiguration) tai tilallisesti (stateful autoconfiguration). Tilattomassa tilassa laite itse generoi automaattisesti oman osoitteensa ilman kontrolloitua hallintaa. Tilallisessa tilassa konfigurointiin käytetään erityistä palvelua esim. DHCP joka vastaa DHCP:llä suoritettua osoitteen asennusta IPv4:ssä.

Tilattomalla vaihtoehdolla varmistetaan että laite saa osoitteen, vaikka sille ei ole manuaalisesti määritelty osoitetta eikä DHCP pysty tarjoamaan sille sellaista. Tällä varmistetaan laitteen toiminta verkossa, jolloin laite saa yhteyden esim. paikallisiin tulostimiin tai pystyy paikallistamaan lähiverkon laitteita DNS:n kautta. Tilattomassa vaihtoehdossa laite määrittelee link local osoitteen joka perustuu laitteen fyysiseen MAC-osoitteeseen, 48-bittinen fyysinen osoite muunnetaan 64-bittiseksi link-local osoitteeksi. Tilallisessa tilassa menetelmä itse määrittelee koko 128-bittisen osoitteen, mutta tilattomassa tilassa vain ylintä 64-bittiä. (Kaario 2002, 123–125.)

4.4.8 Palvelun laatu eli QoS (Quality of Service)

Lisääntynyt ja monipuolistunut liikenne IPv4-verkossa toi tarpeen myös kontrolloida ja luokitella liikennettä IPv6-verkossa. Eri IP-paketeilla on eri tarpeet. Osa paketeista, kuten

esim. video ja internetpuheluiden paketit tulee olla mahdollisimman nopeasti perillä aiheuttamatta katkoja tai turhaa viivettä liikenteeseen.

QoS eli Quality of Service määrittelee datan priorisoinnin liikenteessä ja eri pakettien tärkeystason. IPv6:ssa paketin luokkakenttä ja vuontunniste mahdollistavat eri IP-pakettien tyypin määrittämisen ja priorisoinnin verkossa. (Casad 2011, 291-292.)

4.5 Otsikkokenttä (header)

IPv6-paketti koostuu otsikkokentistä, joita ovat pakollinen varsinainen otsikko, sekä eri lisäotsikoista joiden määrä on valinnainen. Osa otsikkokentistä ja niiden sisältämästä datasta on tarkoitettu matkanvarrella oleviin reitittimiin ja muihin kohteisiin ja osa vain lopulliselle vastaanottajalle. Lisäotsikoita saa olla kussakin paketissa vain yksi kappale lukuun ottamatta kohdeoptio-otsikkoa, joita saa olla kaksi kappaletta. (Casad 2011, 284; Kaario 2002, 115.)

4.5.1 Pakollinen otsikko

IPv6-paketin tärkein otsikko on pakollinen otsikko, joka jo nimensä puolesta ilmaisee kyseessä olevan pakollinen. Jos IPv6-paketissa ei ole muita otsikoita kuin pakollinen otsikko, tulee sen pituudeksi 320 bittiä eli 40 oktettia.

Pakollisen otsikon otsikkokentistä ensimmäinen on versionumero, joka kertoo mikä IP-versio on kyseessä, tässä tapauksessa IPv6. Versionumerolle on varattu IP-paketista 4 bittiä.

Seuraavana otsikkokenttänä on luokkakenttä jolle on varattu 8 bittiä. Luokkakentän tarkoituksena on luokitella paketteja eri ryhmiin niiden tärkeysasteen perusteella. Luokkakentän antaman arvon paketille perusteella reitittimet ja muut verkon laitteet tekevät päätöksen paketin priorisoinnista liikenteessä.

Otsikkokentän jälkeen tulee vuon tunnistekenttä, joka on kooltaan 20 bittiä. Vuon tunnistekenttä käsittelee eri vuoita jotka kertovat saman lähettäjän samaan kohteeseen lähettämiä IPv6-paketteja joilla on sama vuonotsikko. Eri IPv6-paketeilla voi olla sama vuo, eri vuo, tai ei lainkaan vuota jolloin vuontunnisteen arvo on nolla. Vuojärjestelmän tarkoituksena on mahdollistaa samankaltainen kohtelu samalla vuotunnisteella oleville paketeille. Vuon kohtelu IP-verkossa voidaan kuvata hyppyoptio-otsikon avulla.

Kuorman pituus kertoo datan pituuden pakollisen otsikon jälkeen IPv6-paketissa. Kuorman pituutta mitataan okteteissa ja raja on 65575 oktettia. Rajan ylittyessä jumbopaketissa kentän arvoksi tulee nolla. Kuorman pituus kenttä on kooltaan 16 bittiä.

Seuraava otsikko kentässä ilmoitetaan otsikkokentästä, joka seuraa tavallista IPv6-otsikkoa, kyseessä voi olla ylemmän tason otsikkokentän tyyppi kuten TCP tai UDP tai lisäotsikon tyyppi. Seuraava otsikko kentän koko on 8 bittiä ja jos siinä ei ole dataa sen arvoksi tulee 59.

Elinikäkenttä määrittelee IPv6-paketin eliniän, eli kuinka monen reitittimen kautta IPv6-paketti voi kulkea ennen kuin se tuhotaan. Kun elinikäkenttä saa arvoksi 0, täytyy se tuhota. Elinikäkentällä estetään pakettien ”ikuinen” kierto verkossa.

Lähdeosoite on kooltaan 128 bittiä ja se määrittelee tietokoneen IPv6-osoitteen joka lähettää paketin. Kohdeosoite on kooltaan myös 128 bittiä ja se määrittelee tietokoneen IPv6-osoitteen joka vastaanottaa paketin. (Casad 2011, 284-285; Kaario 2002, 116-117.)

4.5.2 Hyppyoptio-otsikko (hop-by-hop options)

Hyppyotsikko on kolmesta osasta muodostuva IPv6-paketin osa, jonka tarkoitus on jakaa tietoa matkan varrella oleviin reitittimiin. IPv6-paketti ei aina sisällä hyppyotsikkoa, vaan kyseinen osa on optio. Hyppyotsikon kolme osaa ovat tyyppikenttä (8 bit), lisäotsikon pituuden ilmaiseva kenttä (8 bit) ja hyppyoptio-otsikon datasta eli optiosta. Optiot kuvataan TLV-koodausta (Type-Lenght-Value) käyttäen jossa ensimmäinen kenttä kertoo option tyypin, toinen datan pituuden ja kolmas sisältää datan. Tyyppikentän kaksi enimmäistä bittiä kertoo miten reitittimen tulee käsitellä pakettia. 00 bittikuviolla se jatkaa käsittelyä hyppäämällä option yli, 01 hylkää paketin, 10 hylkää paketin ja lähettää ICMP-paketin lähettäjälle, 11 hylkää paketin ja jos kohdeosoite on ryhmälähetysosoite, niin myös ICMP-paketti lähetetään. Tyyppikentän kolmas bitti kertoo datan muuttumisesta matkalla, arvolla 0 data ei muutu ja arvolla 1 data voi muuttua. (Casad 2011, 285; Kaario 2002, 117-118.)

4.5.3 Kohdeoptio-otsikko (destination options header)

Kohdeoptio-otsikko on rakenteeltaan samanlainen kuin hyppyoptio-otsikko sisältäen myös tyyppikentän, lisäotsikon pituuskentän ja datan. Kohdeoptio-otsikko eroaa hyppyoptio-otsikosta sillä että sen sisältämää dataa käytetään vain paketin saavuttua kohteeseensa. (Casad 2011, 286; Kaario 2002, 118.)

4.5.4 Reititysotsikko (routing header)

Reititysotsikko on osa IPv6-pakettia, jolla se voidaan ohjata kulkemaan tiettyjen verkon reitittimien tai solmukohtien läpi. Reititysotsikko koostuu 5 eri datakentästä: seuraavasta otsikosta, lisäotsikon pituudesta, reititystyypistä, solmuja jäljellä ja datasta. Ensimmäiset 8

bittiä ovat seuraava otsikkokenttä, joka kertoo seuraavan lisäotsikon tyypin. Seuraavat 8 bittiä kertovat lisäotsikon pituuden. Reititystyyppi määrittää reititysotsikkotyypin joka voi vaihdella eri tilanteissa. Reititystyyppikentän poikkeava arvo määrittää reitittimille että tämän on hylättävä koko IPv6-paketti ja lisäksi lähetettävä ICMP-viesti lähettäjälle. Solmuja jäljellä kentän 8 bittiä kertovat jäljellä olevien solmujen määrän ennen kohdetta. Viimeinen otsikkokenttä on varattu reititystyypille ominaiselle datalle. (Casad 2011, 286 ; Kaario 2002 118–119.)

4.5.5 Fragmentointiotsikko eli lohkomisotsikko (fragment header)

Lohkomisotsikko hoitaa IPv6-paketin lohkomista ja sisältää tarpeellisen tiedon pilkottujen lohkojen kokoamisesta. Toisin kuin IPv4-protokollassa, IPv6-protokollassa ei voida pilkkoa IPv6-pakettia matkan varrella reitittimillä vaan pilkkominen täytyy tapahtua IPv6-paketin lähetyksen yhteydessä joka myös nopeuttaa pakettien käsittelyä reitittimissä. IPv6-protokolla määrittelee paketin maksimipituuden jokaiselle yhteydelle ICMP-protokollan avulla. ICMP lähettää varoitusviestin jos paketti on liian iso ja samalla kertoo tiedon paketin suurimmasta sallitusta koosta. (Casad 2011, 286; Kaario 2002, 121.)

4.5.6 Todennusotsikko (authentication header)

Todennusotsikko hoitaa IPv6-paketin tietoturvaominaisuuksia yhdessä salausotsikon kanssa. Todennusotsikko kertoo paketin vastaanottajalle lähettäjän olevan oikea eikä paketti ole matkalla muuttunut. Todennusotsikossa olevan todennusdatan tarkistussumma kertoo vastaanottajalle paketin eheyden. Tarkistussumma lasketaan eri parametreja käyttämällä joista yksi on salainen avain. Vastaanottaja generoi datakentästä saman tarkistussumman ja jos kyseinen summa on identtinen, on paketti aito. (Casad 2011, 287; Kaario 2002, 121.)

4.5.7 Salausotsikko (encrypted security payload header)

Salausotsikon tehtävänä on salata IPv6-paketti ja siinä lähetettävä data. Salausotsikko salaa tarpeen mukaan IPv6-paketin, joko kokonaan tai vain osittain. IPv6-paketin viimeinen selväkielinen lisäkenttä on salausotsikko, jonka jälkeen kaikki muut lisäkentät ovat salattuja. Myös salausotsikko on salattu lukuun ottamatta kahta ensimmäistä osaa, turvallisuusindeksiä ja järjestysnumeroa. ESP-tunneloinnissa taas koko IPv6-paketti salataan ja sijoitetaan ylemmän suojaamattoman paketin sisään. (Casad 2011, 287; Kaario 2002, 122.)

4.6 IPv4:n & IPv6:n käyttö eri tekniikoilla

Siirtyminen maailmanlaajuisesta IPv4-verkosta IPv6-verkkoon ei ole yhden yön juttu, vaan siirtyminen tapahtuu pikkuhiljaa sitä mukaa kun IPv4-osoitteet loppuvat ja isot operaattorit alkavat aktiivisesti myöntämään IPv6-osoitteita asiakkaille. Teknisesti IPv4- ja IPv6-verkot eivät ole suoraan yhteensopivia, vaan on kehitetty eri tekniikoita joilla mahdollistetaan mm. IPv6:n käyttö IPv4-verkon sisällä. Tällaisia tekniikoita ovat mm. mappaus (IPv4-osoitteen kääntäminen IPv6:n), Dual Stack ja eri tunnelointimenetelmät joissa IP-paketti paketoidaan toisen IP-paketin sisään. (Casad 2011, 292.)

4.6.1 IPv4-osoitteen mappaus IPv6-osoitteeksi

Ensimmäinen askel yhteiskäyttöön tehtiin jo IPv6:n kehitysvaiheessa, kun IPv6:n varattiin mahdollisuus muuntaa olemassa oleva IPv4-osoite IPv6-osoitteeksi. Tätä kutsutaan mappaukseksi. Alun perin tämä piti tapahtua lisäämällä jokaiseen muutettuun IPv6-osoitteeseen 96 nollabittiä 32 bittisen IPv4-osoitteen eteen. Tämä tekniikka ei kuitenkaan tullut viralliseksi standardiksi, vaan tilalle tuli vaihtoehtoinen ratkaisu jossa 32 bittisen IPv4-osoitteen eteen lisätään 80 nollabittiä ja tämän perään 16 ykkösbittiä. Näin esimerkiksi IPv4-osoitteesta 169.219.13.133 muodostuu IPv6-muodossa seuraavanlainen osoite: 0000:0000:0000:0000:0000:FFFF:A9DB:0D85 tai lyhennettynä ::FFFF:A9DB:0D85. Osoite voidaan esittää myös muodossa ::FFFF:169.219.13.133. (Casad 2011, 292–293.)

4.6.2 Dual Stack

Dual Stack on menetelmä jossa tietokone tukee molempia protokollia, sekä IPv4:sta että IPv6.sta. Dual Stackissa tietokone valitsee kumpaa yhteyttä se käyttää tai se voi tarvittaessa käyttää molempia hybridinä. Suurimmassa osassa nykyisistä käyttöjärjestelmistä on tämä hybridiominaisuus. Kun tietokone käyttää hybriditilassa IPv4-protokollaa, se esittää osoitteen mapattuna eli muunnettuna IPv6-protokolla muodosta niin kuin edellisessä kappaleessa on kerrottu. (IETF RFC 4213)

4.6.3 Tunnelointi: Tunnel broker

Tunnel brokerit ovat yksi tapa tarjota IPv6-yhteys IPv4-käyttäjälle. Tunnel Brokerit ovat eri palveluntarjoajien mahdollisuuksia päästä IPv6-verkkoon. Käyttäjä valitsee eri tunnetuista palveluntarjoajista itselleen lähimmän ja parhaan vaihtoehdon. Tunnel brokerissa käyttäjä ottaa yhteyden IPv4-verkon läpi tunnel brokeriin, joka tarjoaa yhteyden IPv6-verkkoon. Käyttäjällä tulee olla dual stack valmius joka tukee sekä IPv4- että IPv6-liikennettä. Tunnel broker yhteydessä IPv6-paketti paketoidaan IPv4-paketin sisään.

Tunnel broker menetelmään liittyy useita ongelmia osoitteiston ja tietoturvan kannalta ja näin ollen se ei ole paras eikä pysyvä ratkaisu IPv6-verkon käyttöön. Se ei esimerkiksi tuo ratkaisua IPv4-osoitteiden loppumisongelmaan. (IETF RFC 3053; Casad 2011, 293–294.)

4.6.4 Tunnelointi: 6to4 ja 6rd

6to4 on tunnelointitekniikka, joka käyttää hyväkseen mappausta. 6to4 mappaus eroaa aikaisemmin selitetystä mappauksesta siten, että 6to4 varaa IPv6-osoitteesta tietyn osoiteosion luoden IPv6-osoitteen jonka verkko tunnistaa automaattisesti 6to4-osoitteeksi. 6to4 menetelmä tarjoaa väylän IPv4-verkossa IPv6-paketeille vaikka IPv6-verkolla ei ole tunnelointipalvelua tai palveluntarjoajan IPv6 tukea.

6to4 menetelmässä IPv4-osoite paketoidaan IPv6-osoitteeseen. 6to4 palvelimessa IPv6-paketti puretaan ja sen sisällä olevasta IPv4-osoitteesta luodaan IPv4-paketti joka sisältää alkuperäisen IPv6-paketin, joka edelleen lähetetään IPv4-verkkoon. IPv6-osoitteet 2002::/16 etuliitteellä ovat varattuja 6to4 menetelmälle. (Casad 2011, 294–295.)

6rd on Ranskassa kehitetty muunnos 6to4:stä, jossa palveluntarjoaja hoitaa IP-pakettien muunnoksen eikä välipalvelimia tarvita. 6rd mallissa käytetään palveluntarjoajan omaa etuliitettä 6to4 menetelmässä käytetyn 2002::/16 sijaan. Tämä malli takaa sen, että palvelu on tavoitettavissa kaikista natiiveista IPv6-osoitteista jolloin pystytään takaamaan palvelun laatu kaikissa tilanteissa. Tämä myös vähentää kolmannen osapuolen palveluihin liittyviä tietoturvauhkia ja mahdollisia toimimattomuusongelmia joita 6to4 menetelmässä voi ilmetä. (IETF RFC 5569, 5969.)

4.6.5 Tunnelointi: Teredo

6to4 on tunnelointimenetelmänä erittäin hyvä, mutta siinä on yksi suuri heikkous, se ei toimi jos lähettäjä on NAT:in takana. Teredo kehitettiin vastaamaan tähän ongelmaan. Teredo käyttää kuljetusprotokollana UDP:tä TCP:n sijaan, koska se toimii paremmin NAT:in läpi. Teredossa palvelin pitää yllä listaa NAT:in takana toimivista käyttäjistä.

Teredossa IPv6-osoitteeseen tulee ensin Teredopaketin oma etuliite (3FFE:831F::/32) ja tämän jälkeen Teredopalvelimen 32-bittinen IPv4-osoite. Näiden lisäksi IPv6-pakettiin tulee NAT-laitteen IPv4-osoite sekä NAT:in takana olevan paketin vastaanottajan UDP-portin numero.

Teredo on jo käytössä osassa verkkoja, mutta se on vielä kehitysasteella. Tällä hetkellä kaikki tunnelointimenetelmät ovat enemmän tai vähemmän väliaikaisia ja kun tulevaisuudessa

internet saavuttaa täyden IPv6-kattavuuden, ei toivottavasti tunnelointimenetelmiä enää tarvita. (Casad 2011, 295–296.)

4.6.6 6bone

6bone oli vuonna 1996 perustettu kokeellinen ja tutkimuksellinen IPv6-verkko. 6bonessa tutkittiin ja testattiin uutta IPv6-protokollaa ja sen tuomia uusia teknisiä mahdollisuuksia. 6bone aloitti aluksi virtuaaliverkkona IPv4-verkossa ja lisäsi hitaasti natiiveja IPv6-osoitteita. Aluksi 6bonen päämäärä keskittyi enemmän eri standardien ja sovellutusten kokeilemiseen, mutta myöhemmin enemmän ja enemmän eri liikennöinnin, verkon käytön ja operatiivisten proseduurien testaamiseen.

6bone testiverkon etuliite on 3FFE::/16. Vuonna 2003 6bone saavutti käyttöhuippunsa jolloin siihen oli reititettynä yli 150 korkean tason 6bone 3FFE::/16 etuliitettä yhdistäen yli 1000 sivustoa yli 50 eri maasta. Kun tuli selväksi 6bonen tehokkuus ja toimintakyky määritellä tällainen määrä etuliitteitä joita julkiset ja yksityiset IPv6-verkot käyttivät 6bone ulkopuolella, niin aloitettiin 6bonen alasajo. 6bonen virallinen käyttö päättyi vuonna 2006 ja IANA:n päätöksellä siihen liittyviä osoite-etuliitteitä ei tulisi enää käyttää. (IETF RFC3701; Kaario 2002, 109.)

5. IPv6 Suomessa ja muualla maailmalla

Tässä luvussa käsitellään IPv6:n tilannetta ja liikennemääriä Suomessa ja muualla maailmassa.

5.1 IPv6-tappajasovellus (killer application).

Yksi syy mistä mahdollisesti toivottiin maailmanlaajuista IPv6-vauhdittajaa, olisi tappajasovellus. Tappajasovelluksella tarkoitetaan sovellusta tai muuta vastaavaa ohjelmaa joka toimii pelkästään IPv6-verkossa ja joka jollain tavalla mullistaisi IPv6:n käytön. Tällainen sovellus pakottaisi yritykset siirtymään vanhasta IPv4-versiosta uuteen IPv6-version käyttöön. Vaikka asia on ollut pitkään esillä, ei vielä tällaista sovellusta ole saatu kehitettyä.

Erilaisia vaihtoehtoja tappajasovelluksesta on esitetty: VOIP ja muut kuvan sekä äänen siirtoon liittyvät vaihtoehdot, erilaiset maksu-tv sovellutukset, langattomien laitteiden mahdollisuudet, elektroniset maksusovellukset, IP-pohjaiset datavarastot ja pelkästään IP-liikenteen jatkuvuus yritystoiminnassa. Mikään näistä vaihtoehdoista ei vielä ole kuitenkaan lyönyt itseään läpi IPv6:n tulevaisuuden takaajana. (Searchnetworking.techtarget 2002; Network world 2012.)

IPv6 mahdollistaisi monia eri uusia ominaisuuksia, mitä ei IPv4:llä pysty tekemään. Tällaisen mullistavan tappajasovelluksen tulo todennäköisesti pakottaisi yritykset tekemään ratkaisun IPv6:seen siirtymisestä nopealla aikataululla. On oletettavaa että kyseinen sovellus syntyisi Itä-Aasian suunnalla, jossa IPv6:n käyttöönotto on ollut ripeämpää, sillä siellä ei IPv4-osoitteita ole riittävästi. Pahimmillaan tämä johtaisin Euroopan kannalta sellaiseen tilanteeseen, jossa Aasiassa käytössä oleva huipputason sovellus (esim. Facebook ym. vastaavan tason keksintö) olisi jo käytössä. Tämä voisi johtaa eurooppalaisten ja muiden länsimaalaisten käyttäjien paitsiotilanteeseen, koska he eivät sitä pystyisi välttämättä ottamaan heti käyttöön, sillä IPv6-valmius puuttuisi. Tämä johtuisi siitä, koska länsimaalaisilla yrityksillä ei välttämättä olisi sovelluksen vaatimaa IPv6-infraa vielä käytössä.

5.2 IPv6 Suomessa

IPv6:n käyttöönotto Suomessa on lähtenyt hitaasti liikkeelle. Suomessa yritykset ja organisaatiot eivät ole osoittaneet suurta kiinnostusta IPv6:n käyttöönottoa kohtaan. Suurimpana syynä tähän on se, ettei IPv6:n käyttöönotto ole vielä pakollista. Organisaatiot odottavat syitä minkä takia heidän pitäisi siirtyä IPv6:n käyttöön ja tällaista pakottavaa syytä ei ole vielä löytynyt. IPv4-osoitteiden loppuminen pakottaa yritykset miettimään jatkossa siirtymistä IPv6:n käyttöön. Tällä hetkellä se ei ole yksin vielä riittävän pakottava syy siirtyä IPv4:n käytöstä IPv6:n käyttöön, sillä yrityksillä on vielä riittävästi IPv4-osoitteita käytössä. Näiden lisäksi henkilö- tai yksityiskäyttäjillä ei ole vielä IPv6-yhteyksiä käytössä kovinkaan paljon, joten organisaatiolle ei tule vaatimuksia saada palveluita tarjottavan myös IPv6-muodossa.

5.2.1 IPv6-seminaari ja sen tulokset

Huhtikuussa 2011 järjestettiin Espoon Dipolissa Viestintäviraston ja Suomen Internet-yhdistyksen toimesta tärkeä IPv6-seminaari, jonka tavoitteena oli antaa osallistujille kuva siitä, miksi IPv6:n käyttöönotto on välttämätöntä tulevaisuudessa. Seminaariin osallistui useita eri tietoliikennetahojen edustajia mm. operaattorin edustajana Sonera ja tietojärjestelmien näkökantaa asiaan toi Fujitsu. (Ficora 2011.)

Yksi osallistujista oli Suomessa IPv6-edelläkävijä, eli AYY eli Aalto-yliopiston ylioppilaskunta, joka pitää yllä Trinet tietoliikenneverkkoa. AYY:n edustaja esitteli Trinetin toimintaa ja heidän kokemuksia IPv6:sen käyttöönotosta. AYY on yksi ensimmäisistä suuren luokan toimijoista jotka ovat ottaneet IPv6:n kokonaan käyttöön heidän järjestelmissä ja palveluissa. (Ficora 2011.)

Jatkossa tulevaisuudessa vastaavia seminaareja tullaan järjestämään muutamien vuosien välein, sitä mukaan kun IPv6:n käyttöönotto etenee. Tällaiset seminaarit ovat hyviä tilaisuuksia eri toimijoille jakaa ja päivittää IPv6-tietoutta ja tilannetta niin operaattoreiden, laitevalmistajien kuin muidenki asiasta kiinnostuneiden kesken. Näin edistetään entisestään IPv6:n käyttöönottoa tulevaisuudessa.

5.2.2 Viestintäviraston IPv6-toimet

Viestintävirasto eli Ficora joka hallitsee ja myöntää suomalaisia internetin .fi päätteitä ja hallinnoi fi-juuren nimipalvelimia, on omalta osaltaan edesauttanut Suomessa tapahtuvaa IPv6-siirtymää ottamalla IPv6-nimipalvelimet käyttöön. Ficoran ensimmäinen fi-juuren IPv6-nimipalvelin otettiin käyttöön vuonna 2006 Tukholmassa. Vuonna 2008 Ficora otti käyttöön IPv6-osoitteen fi-juuren ensisijaisessa juurinimipalvelimessa. Tällä Ficora haluaa varmistaa tuen IPv6-liikenteelle, jonka se uskoo lisääntyvän rajusti lähitulevaisuudessa IPv4-osoitteiden loppumisen vuoksi. (Ficora 2008.)

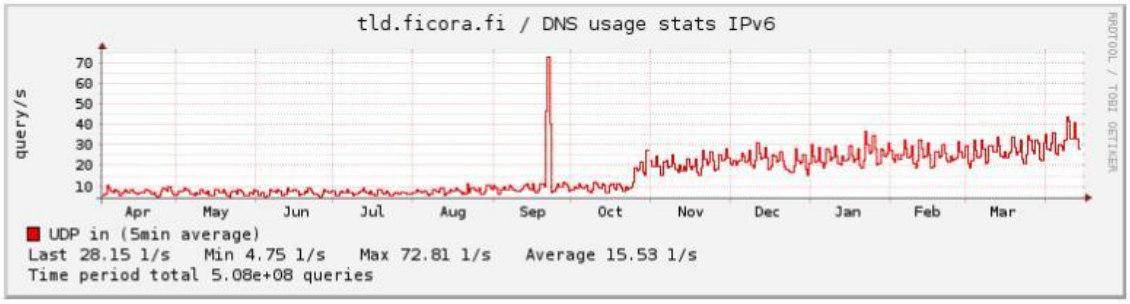
5.2.3 Operaattoreiden IPv6-palveluiden tarjonta Suomessa

Yksi suurimmista syistä miksi IPv6:n käyttöönotto on myös hidastellut Suomessa, on internetoperaattorit. Tällä hetkellä harva Suomessa toimiva operaattori tarjoaa IPv6-yhteyksiä yritys- tai henkilöasiakkaille. Yrityspuolella tilanne on parempi kuin henkilöasiakaspuolella. Henkilöasiakkaan on tällä hetkellä melkeinpä mahdotonta saada käyttöön IPv6-liittymää ja natiivia IPv6-osoitetta. Operaattoreilla ei ole välttämättä edes aikataulua, koska mahdollisesti IPv6-osoitteet ja liittymät tulevat kaupalliseen myyntiin. Esimerkiksi Sonera on ilmoittanut henkilöasiakkaiden IPv6-liittymien tulevan saataville aikaisintaan vuonna 2013. Tämä on huono asia, sillä kiinnostusta IPv6-liittymiin olisi ja tällä hetkellä osa joutuu turvautumaan vaihtoehtoisiin tunnelointi ym. menetelmiin päästäkseen IPv6-verkkoon. Näihin vaihtoehtoisiin liityntätapoihin liittyy aina riskejä, sillä niiden toimintavarmuus ja tietoturva eivät välttämättä ole parhaalla mahdollisella tasolla. (ape3000.com/ipv6 2011.)

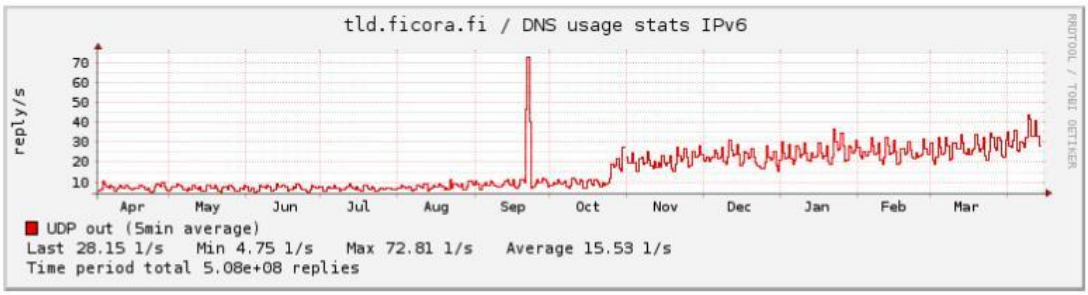
5.2.4 IPv6-liikenne Suomessa

IPv6-liikenne on Suomessa pikkuhiljaa kasvamassa sitä mukaan kun operaattorit tarjoavat IPv6-yhteyksiä asiakkaille ja IPv6-liittymät yleistyvät. Samalla koko verkkoliikenteenmääristä IPv6-liikenteen osuus on kasvanut kokoajan. Ficoran vuoden 2005 raportissa todetaan, että yhden operaattorin tilastointi osoitti IPv6-liikenteen määrän FICIX:in (Finnish Communication and Internet Exchange - FICIX ry) kautta oli n. 1 % koko IP-liikenteen määrästä. Tällä hetkellä FICIX:in mukaan sen A.fi:n nimipalvelimen IPv6-liikenne on n. 1/8 osa IPv4-liikenteestä.

FICIX:in tilastot osoittavat IPv6-liikenteen kyselyiden olleen melko vähäistä ennen loppuvuotta 2011, jolloin IPv6-kyselyiden määrä moninkertaistui (kuva 13, 14). FICIX on vuonna 1993 aloittanut yhdistys, joka toimii internetin solmupisteenä Suomessa. FICIX:in jäseninä ovat mm. kaikki Suomen merkittävimmät internet-palveluntarjoajat ja kansainväliset toimijat. (Ficora 2005; FICIX.fi 2011.)



Kuva 13: IPv6 kyselyt per sekunti 2.4.2011 – 16.4.2012 välisenä aikana



Kuva 14: IPv6 vastaukset per sekunti 2.4 – 16.4.2012 välisenä aikana

5.3 IPv6 muualla maailmalla

Kuten jo aikaisemmin todettiin, niin suurimmat IPv6:n käyttöönottoalueet sijaitsevat tällä hetkellä Aasiassa, jossa pula IPv4-osoitteista on pakottanut etsimään uusia vaihtoehtoisia ratkaisuja eli käytännössä ottamaan IPv6:n käyttöön. Ylipäätään koko IPv6:n käyttöönotto on lähtenyt maailmalla hitaammin liikkeelle mitä 10–15 vuotta sitten arvioitiin. Tällöin uskottiin IPv4-osoitteiden loppumisesta, lisääntyvästä laite- ja käyttäjäkannasta ja muista syistä että IPv6-käyttäjien määrä tulee räjähdysmäisesti kasvamaan lähitulevaisuudessa. Tätä nopeaa kasvua ei ole ainakaan vielä tapahtunut, vaan uusien IPv6-käyttöönottojen määrä on ollut hitaassa kasvussa.

IPv6 on kuitenkin saanut uusia käyttäjiä varsin merkittäviltä tahoilta, kun suuret yritykset ja organisaatiot ovat pikkuhiljaa alkaneet ottamaan IPv6:sta käyttöön. Myös palveluntarjoajat ovat aloittaneet tarjota niin yritys- kuin yksityisasiakkaille uusia IPv6-liittymiä. Myös

kansalliset tutkimus- ja koulutusverkot (NREN) ovat eri maissa alkaneet ottamaan IPv6:sta käyttöön, näin on käynyt esim. Afrikassa Egyptissä ja Etelä-Afrikassa sekä monessa maailman muussa maassa. (Isoc.org 2009.)

5.3.1 IPv6-osoitteiden jako maailmalla

RIPE (Réseaux IP Européens = European IP Networks) on yksi viidestä RIR:stä (Regional Internet registries), jonka yhtenä tehtävänä on jakaa ja myöntää julkisia IPv6-osoitteita eri palveluntarjoajille ja yrityksille. Yksi hyvä keino seurata IPv6-osoitteiden määrän kasvua, on seurata näiden osoitteiden lukumääriä ja alueellisen jakamisen määriä. Myönnettävien osoitteiden määrä on kasvussa, vuonna 2010 uusia osoitteita myönnettiin 834 kpl kun vuonna 2009 luku oli 554. (Fix6 2011.)

Seuraavassa on lista suurimmista ja kappalemäärällisesti tärkeimmistä maista ja niille myönnetyistä osoitemääristä maa per kappaletta:
USA yli 2000, Saksa n.600, Iso-Britannia n.500, Australia n. 500, Japani n.400, Venäjä n. 350, Ranska n.300, Kanada n.250, Italia n. 200, Espanja n. 150, Indonesia, Intia ja Kiina jokaiselle n.170. Erityishuomiona pohjoismaat: Ruotsi n. 250, Norja n. 150, Tanska ja Suomi molemmat n.100. Lopuilla maista on osoitteita keskimäärin 0-100 kpl. (IPv6actnow 2012.)

5.3.2 Maailmanlaajuinen IPv6-päivä 2011 ja Maailmanlaajuinen IPv6-julkaisupäivä 2012

Heinäkuussa 2011 suuret internetsivustot kuten Google, Yahoo, Facebook ym. ja internetpalveluntarjoajat yhdistivät voimansa ja pitivät suuren IPv6-markkinointitapahtuman, johon osallistui yli 1000 eri internetsivua. Tapahtuman tarkoitus oli markkinoida ja tuoda suurelle yleisölle esille IPv6-tietoisuutta. Tapahtumassa yritykset testasivat ensikerran globaalisti IPv6-valmiuksia ja -liikennettä suuressa mittakaavassa julkaisemalla sivustot IPv6-verkossa 24 tunnin ajan. Tapahtumalla yritykset halusivat todistaa olevansa valmiita siirtymään IPv6:n käyttöön tulevaisuudessa. (World IPv6 Day 2012.)

Toinen vastaava tapahtuma eli maailmanlaajuinen IPv6-julkaisupäivä tulee heinäkuussa 2012. Tässä tapahtumassa eri osallistujayritykset ottavat virallisesti sivustonsa ja palvelunsa pysyvästi käyttöön IPv6-verkossa. Osalla sivustoista IPv6-vaihtoehto toimii jo nyt. Tällä hetkellä tapahtumaan on ilmoittautunut globaalisti yli 1000 eri yritystä ja organisaatiota. Suomalaisia osallistujia on tähän mennessä ilmoittautunut varsin vähän, n. parikymmentä organisaatiota. Koko tapahtuma on Suomessa jäänyt varsin vähälle huomiolle. (World IPv6 launch 2012.)

Muita pienempiä IPv6:n käyttöönotto- ja markkinointitapahtumia on järjestetty eri puolilla maailmaa, esim. Saksassa saksalainen heise.de sivusto järjesti 2010 tapahtuman jonka tarkoitus oli testata IPv6:n käyttöönottoa heidän palveluissaan ja sivustolla. Toinen tapahtuma oli Norjassa vuonna 2010, jolloin kaksi Norjan suurimmista websivustoista, A-pressen Digitale Medier ja VG Multimedia julkaisivat sivustonsa IPv6-verkossa 24 tunnin ajan. Vastaavanlaisia tapahtumia tullaan varmasti järjestämään jatkossa lisää eri puolilla maailmaa. Tämä toivottavasti auttaa yrityksiä siirtämään IPv6-verkon käyttöön ja myös jakaa käyttäjille IPv6-tietoutta.
(World IPv6 Day 2012.)

5.3.3 IPv6-liikenne maailmalla

IPv6-liikennettä on ollut verkossa siitä lähtien kun ensimmäiset IPv6-verkot otettiin käyttöön. Tämän jälkeen liikenteen määrä suhteessa IPv4-liikenteeseen ja muuhun verkkoliikenteeseen on ollut hitaassa kasvussa sitä mukaan kun uusia IPv6-käyttäjiä on ilmestynyt verkkoon. IPv6:n hidasta käyttöönottoa on yritetty vauhdittaa useiden eri tahojen toimesta, mm. Yhdysvaltain hallinto vaatii vuodesta 2008 lähtien jokaiselta siviili- ja puolustustarvikkeiden myyjältä laitteiden ja ohjelmistojen IPv6-yhteensopivuutta. Japanissa valtiohallinto tukee vahvasti siirtymistä IPv6:n käyttöön. Myös Kiinassa valtiohallinto on vahvasti mukana IPv6 käyttöönotossa. Vuonna 2008 Pekingin olympialaisissa Kiina esitteli sen IPv6-verkon käyttöönottoa, kun kaikki verkkoliikenne valvontakameroista internet streameihin oli toteutettu IPv6:lla. Ranskassa France Telecom on ollut vahvasti mukana IPv6-verkkojen rakentamisessa ja yhteyksien tarjoamisessa yhteistyössä IPv6 Task Forcen kanssa. Koreassa on käynnissä hanke, jonka tavoitteena on tarjota yrityksille ja yksityisille asiakkaille IPv6-liittymiä sekä palveluita. Korean hallituksen tavoitteena on saada koko julkinen sektori käyttämään IPv6:sta lähitulevaisuudessa. (ipv6.com.)

Maaliskuussa 2012 IETF (Internet Engineering Task Force) julkaisi dokumentin jossa mitattiin IPv6-liikenteen määrä BitTorrent verkossa. Aikavälillä 2011- 2012 tehdyissä mittauksissa tutkittiin P2P (Peer-to-peer) verkoissa tapahtuvasta IPv6-liikenteestä, sen eri laaduista ja määristä. Tutkimuksessa mitattiin P2P-liikennettä, koska se on tärkeässä roolissa koko internetliikenteen määrässä ja koska sen avulla on helppo löytää IPv6-käyttäjiä koska nämä eivät ole NAT:in takana niin kuin on useimmat IPv4-käyttäjät. Uusimmassa mittauksessa 12.4.2012 koko IPv6-liikenteestä 47 % oli Teredo-liikennettä, 43 % 6to4-liikennettä ja 9,9 % natiivia liikennettä, loput liikenteestä on muilla tavoin toteutettu. (IETF draft 2012.)

Maantieteellisesti mitattuna suurimmat natiivi IPv6:n käyttäjämäärät suhteessa IPv4-käyttäjiin olivat Ranskassa, USA:ssa, Kiinassa ja Japanissa. Vuoden 2011 mittauksessa löydettiin yhteensä 197 natiivia IPv6-osoitetta yli 25 maassa, joista yli 40 % sijaitsi Ranskassa.

Vuoden 2012 mittauksessa löydettiin 1466 natiivia IPv6-osoitetta, joista Ranskalla oli suurin määrä kaikista maista natiivien IPv6-osoitteden määrässä suhteessa kaikkiin IP-osoitteisiin, 2,10 % lukemalla. Seuraavana perässä tulivat Kiina (0,65 %) ja Japani (0,59 %). (IETF Draft 2012.)

6 IPv6:n käyttöönotto ja huomioon otettavat asiat organisaatioissa

Miksi IPv6:n käyttöön tulisi sitten siirtyä? IPv4 ei näillä näkymin ole häviämässä vielä hetkeen ja jos yhteydet ja järjestelmät toimivat nykyisillä IPv4-ratkaisuilla hyvin niin miksi siirtyä?

6.1 Syitä IPv6:seen siirtymistä vastaan

- Vanhan teknologian toimivuus, jos IPv4 toimii vielä ja NAT:in avulla pystyy verkon kapasiteettiongelman paikkaamaan eli verkkoon kytkemään enemmän laitteita.
- Vanhat ominaisuudet ja sovellukset toimivat vielä IPv4-verkossa, esim. mobiili IP, tietoturva (IPsec) ja palvelunlaatu (QoS).
- Verkkojen ja prosessien toiminta tehostuu ja nopeutuu IPv6:sta huolimatta, kun uusia tehokkaampia laitteita otetaan käyttöön, joten IPv6:n käyttö ei tällä saralla ole välttämättä perusteltua.
- Hinta. Siirtyminen IPv6:n käyttöön on kallista. Vaikka yrityksen laite- ja ohjelmistokanta olisikin jo valmiiksi suoraan IPv6-yhteensopivia, niin henkilöstön koulutus ja IPv6:n käyttöönotto sekä mahdolliset ongelmat IPv6:n käyttöönotossa voivat aiheuttaa ylimääräisiä kustannuksia.
- Ei tarjoa suoraa hyötyä. IPv6 ei tarjoa tällä hetkellä suurimmalle osalle yrityksistä mitään konkreettista hyötyä tai parannusta mitä IPv4 jo ei tarjoaisi. Näin ollen ei ole syytä ottaa sitä käyttöön ennen kuin on pakko.
- Laite- ja ohjelmisto-ongelmat. Vaikka yrityksellä olisi IPv6-valmiit laitteet ja ohjelmat, voi silti ongelmia esiintyä käyttöönotossa, koska kaikkia IPv6:seen liittyviä asioita ei ole ratkaistu. Etenkin normaalikäytöstä poikkeavien laitteiden tai ohjelmistojen käyttötarkoitukset ja reititysratkaisut voivat aiheuttaa ongelmia. Näiden korjaaminen vaatisi yhteydenottoa ohjelmisto- tai laitevalmistajiin uusien ohjelmistoversioiden saamiseksi.
- IPv6-tuen puutuminen laitteista ja ohjelmistoista. Jos yrityksen ohjelmistot eivät ole yhteensopivia IPv6:n kanssa eikä valmistajilta ole saatavissa uusia päivitysversioita, ei siirtyminen IPv6:seen ole välttämättä vielä kannattavaa.

- IPv6:n tulevaisuus, IPv6 on ollut tuloillaan vuosia eikä sitä vieläkään ole saatu suuren yleisön käyttöön täysipainoisesti. Todennäköisesti tähän menee vielä vuosia, jopa vuosikymmeniä ja asiat ehtivät muuttua siinä ajassa radikaalisti. Sitä paitsi uusi teknologia voi tehdä siirtymisen IPv6:seen turhaksi, jos kehitetään uusi ja parempi vaihtoehto joka korvaa sekä IPv6:n että IPv4:n.

6.2 Syitä IPv6:seen siirtymisen puolesta

- IPv6 tulee joka tapauksessa, kyseessä on vain ajankysymys joten miksi ei aloittaisi jo nyt.
- IPv4-osoiteavaruus on loppumassa tai jo loppunut, uusia osoitteita ei välttämättä saa kohta ollenkaan joten IPv6-siirtymä on pakko toteuttaa.
- IPv6 mahdollistaa uusia käyttötapoja ja sovellutuksia ja se on muutenkin monipuolisempi kuin vanha IPv4. Tämä voi tarjota esim. ohjelmisto- tai laitekehittäjille uusia mahdollisuuksia tuotekehityksen saralla.
- IPv6-edelläkävijä, uuden teknologian käyttöönotto ja lanseeraus voi olla merkittävä brändi ja kilpailuvaltti etenkin tiukasti kilpailuilla aloilla.
- IPv6 tarjoaa isomman osoiteavaruuden ja paremman aliverkotuksen sisäverkkoon. Tämä voi olla ratkaiseva tekijä isoissa organisaatioissa joissa on paljon laitteita ja käyttäjiä.

Jos edellisen kappaleen perusteella IPv6:n käyttöä vastaan on suurempi määrä syitä kuin sen puolesta, niin miksi organisaation pitäisi sitten lähteä näin hankalaan prosessiin mukaan? Jos ei ole teknistä, rahallista, markkinoinnillista tai muutakaan pätevää syytä tai motivaatiota lähteä IPv6-kelkkaan juuri nyt, niin mitkä voisivat olla sellaisia syitä miksi ottaa IPv6 käyttöön. Tällaisia syitä löytyy muutamia, joista yleensä tärkeimmät ovat tekniset ja/tai taloudelliset syyt, jotka pakottavat muutokseen. Kuitenkin nämä kaikki syyt eivät pelkästään ole aina yksittäisen syyn, esim. teknisen siirtymän aiheuttamia, vaan yleensä nämä kaikki syyt ovat enemmän tai vähemmän vaikuttamassa koko prosessissa.

6.2.1 Tekniset syyt

Tekniset syyt ovat tilanteita, joissa organisaatio erinäisistä teknisistä syistä johtuen joutuu uudistamaan olemassa olevia verkkoratkaisuja tai luomaan kokonaan uuden verkon. Yleensä taustalla on jokin tarve tai syy, jossa olemassa oleva tai rakenteilla oleva verkko ei pysty tarjoamaan yrityksen tarvitsemia toimintavalmiuksia. Tällaisten syiden aiheuttajia voi löytyä hyvin monenlaisia, kuitenkin lähes aina kyseessä on tilanne jossa on pakko etsiä uusia toimintakykyisiä verkkoratkaisuja vanhojen ratkaisuiden tilalle. Tällaisissa tilanteissa

siirtyminen IPv6-verkon käyttöön olisi vaihtoehto sen sijaan että uusi verkko toteutettaisiin vanhalla IPv4:llä.

Yksi syy olisi tarve yhdistää eri verkkoja (esim. yhdistää kaksi IPv4-verkkoa). Esimerkkinä tilanteesta jossa kaksi yritystä/organisaatiota yhdistyy ja niiden verkkotoiminnot halutaan yhdistää. Tällöin ei välttämättä ole kannattavaa lähteä isoon ja hankalaan IPv4-verkkojen yhdistämisprojektiin, jossa mahdollisesti tulee verkon rajat ja kapasiteetti vastaan ja joudutaan tekemään hankalia aliverkotus tai osoitteensiirtoratkaisuja, vaan voisi miettiä samalla vaivalla toimintojen siirtämistä kokonaan uuteen IPv6-verkkoon.

Toinen syy olisi tilanne jossa joudutaan luomaan kokonaan uusi lähiverkko yrityksen tarpeisiin. On kannattavampaa lähteä rakentamaan puhtaalta pöydältä uutta IPv6-verkkoa joka todennäköisesti kestää pitkään tulevaisuudessa, kuin vanhaa IPv4-verkkoa vaikka IPv6-verkko ehkä vaatiikin enemmän työtä laitteiden ja ohjelmistojen sovittamiseksi toimintakuntoon.

6.2.2 Taloudelliset syyt

Teknisten syiden tapaan myös taloudellisia syitä on monenlaisia, joista johtuen organisaation tulisi siirtyä, tai ainakin harkita siirtymistä IPv6:n käyttöön. Yleensä taloudellisissa syissä on jokin tarve tai paine joko organisaation sisältä tai ulkoa lähtöisin, joka pakottaa organisaation tekemään muutoksia. Esimerkkinä tällaisista syistä voisi olla esimerkiksi yrityksen asiakkaat vaativat yrityksen palveluja saatavaksi IPv6-verkkoon. Tämä voi olla kotimaasta tai ulkomailta tulevaa painetta. Esimerkki voisi olla tilanteesta jossa yritys toimii alueella missä siirtyminen IPv6-verkon käyttöön on nopeampaa (esim. Kiina, Intia ym. kehittyvät maat) ja sen on pakko siirtyä IPv6:n käyttöön pystyäkseen kilpailemaan markkinoilla.

Olivatpa taloudelliset syyt mitkä tahansa mietittäessä siirtymistä IPv6:n käyttöön, niin tulee organisaatiossa tarkkaan laskea siirtymisestä aiheutuvat kustannukset sekä siitä saatavat taloudelliset hyödyt. Isojen investointien tekeminen IPv6-tekniikkaan nyt muutaman asiakkaan toivomuksen vuoksi ei yleensä ole kannattavaa, elleivät asiat tulevaisuudessa muutu.

6.3 IPv6-verkon käyttöönotossa huomioitavat asiat

Jos halutaan lähteä toteuttamaan siirtoa IPv6-verkkoon, niin on joukko asioita mitä tulisi huomioida ja mihin varautua ennen toteutusta ja toteutuksen aikana. Tähän lukuun on koottu lista asioita mitä organisaatioissa tulisi huomioida, jos suunnitellaan siirtymistä IPv6:n käyttöön. Näiden ohjeiden lisäksi on hyvä varautua mahdollisiin yllätyksiin, mitä voi tapahtua

projektin aikana. Nämä ovat yleisiä asioita, mitä IPv6:n siirtyminen vaatii organisaatiolta, eikä tässä käsitellä syvällisiä teknisiä ratkaisuja. Organisaation tulisi käsitellä IPv6-siirtymää isona prosessina, jossa on useita eri vaiheita ennen varsinaista käyttöönottoa.

6.3.1 Aloituspiste ja eri arviot

Ensimmäinen asia mitä organisaatiossa tulee ottaa huomioon IPv6-siirtymän aloittamisessa, on aloituspiste. Aloituspisteessä organisaation tulisi määritellä ne syyt miksi se haluaa IPv6:seen siirtyä. Organisaation tulisi käsitellä asioita etenkin liiketoimintanäkökulmasta, mitkä ovat ne taloudelliset intressit ja vaatimukset mitä IPv6 sille tuo. Organisaation tulisi tehdä hyötyanalyysi, jossa käsitellä mm. miten IPv6 mahdollisesti lisää tai ylläpitää organisaation taloudellista tuottoa. (McFarland, Sambi, Sharma, Hooda 2011, 91-92.)

Organisaation tulisi määritellä se lähestyminen ja taktiikka millä IPv6 lähdetään ottamaan käyttöön ja syitä sen takana. Yleensä lähestyminen on joko hyökkäävä tai puolustava. Puolustavassa lähestymisessä organisaatio ei välttämättä näe suoria taloudellista hyötyä nyt IPv6:n siirtymisessä, vaan halutaan rakentaa mahdollisuudet ja tekniset ratkaisut jos tulevaisuudessa jokin uusi liikeidea tai tekninen innovaatio mahdollistaa IPv6-verkon hyödyntämisen. Hyökkäävässä lähestymisessä taustalla on yleensä jokin suora hyöty millä halutaan saada suoraa taloudellista hyötyä IPv6:n käyttöönotosta, esimerkiksi uudet IPv6-pohjaiset palvelut asiakkaille. (McFarland 2011, 92.)

Edellisten selvitysten lisäksi organisaation tulisi tehdä kustannusarvio IPv6:n käyttöönotosta. Selvityksessä tulisi ottaa mitä kustannuksia IPv6 aiheuttaa käyttöönottovaiheessa ja sen jälkeen. Kustannusarviossa tulisi arvioida ainakin seuraavien kulujen määrä:

- Suunnittelu ja toteutus (sisältävät suunnittelun, järjestelmän rakennuksen, testauksen, käyttöönoton)
- Infrastruktuurin muutokset ja päivitykset (laitteistot, ohjelmistot, sovellukset, kaikki IT-välineet)
- Henkilöstön koulutus (uuden IPv6-tekniikan käyttöönotto, IPv4:n ja IPv6:n välisen tekniikan käyttö ym.)
- Operatiivisesta käytöstä aiheutuvat kulut järjestelmän käyttöönoton jälkeen

Näiden lisäksi organisaatiossa kannattaa huomioida etenkin infrastruktuurin osalta laitteiston ja ohjelmistojen elämänkaari. IPv6-siirtymä kannattaa toteuttaa siinä vaiheessa, kun infrastruktuuri vaatii muutenkin päivittämistä tai vähintään ottaa uusissa infrastruktuuri-hankinnoissa IPv6-vaatimukset huomioon. Näin organisaatio voi säästää ison summan jos koko

laite- ja ohjelmistokantaa ei tarvitse kerralla uusia IPv6-yhteensopivaksi. (McFarland 2011, 93-94.)

Viimeinen seikka mitä aloituspisteessä tulee suunnitella, on riskianalyysi. Tämä sisältää riskianalyysit taloudellisiin-, teknisiin- ja juridisiin-riskeihin. Tunnistamalla riskit ajoissa organisaatio voi välttyä suurilta ongelmilta, tai ainakin pienentää niiden haittavaikutuksia tulevaisuudessa. (McFarland 2011, 94.)

6.3.2 Aika ja resurssit

Yksi tärkeimmistä asioista missä tahansa uusien asioiden käyttöönotossa organisaatiossa on varata niille riittävästi aikaa ja resursseja. Ei pidä kuvitella siirtymisen menevän heittämällä ilman minkäänlaisia ongelmia, vaan on varauduttava siihen että ongelmia tulee ja niiden selvittämiseen kuluu aikaa ja rahaa.

Toinen tärkeä asia on osaaminen. IPv6 vaatii tietotaitoa henkilöstöltä, niin sen suunnittelu, käyttöönotto kuin päivittäinen käyttökin. Tuli osaaminen sitten organisaation sisältä tai ulkopuolelta, tulee pitää huoli että henkilöstö osaa tarvittavat asiat ja osaa myös ongelmatilanteissa toimia oikein, jotta vältytään järjestelmien käyttökatkoilta sekä muilta ongelmatilanteilta.

6.3.3 Organisointi ja koordinointi

Organisointi ja koordinointi, kaikilla vaativilla projekteilla tulee olla vastuuhenkilö tai -henkilöt jotka vastaavat projektin viemisestä eteenpäin. Tämän henkilön tulee olla linkkinä organisaation henkilöstön ja mahdollisten ulkopuolisten tahojen kanssa ja koordinoida projektin aikataulua ja toimintaa. Vastuuhenkilö hallitsee projektin kustannuksia, koulutuksia, henkilöstöä ja muita projektiin liittyviä asioita. (McFarland 2011, 95.)

6.3.4 Koulutus

Etenkin suurissa organisaatioissa on tärkeää varata riittävästi aikaa ja resursseja henkilöstön koulutukseen. Hyvällä koulutuksella varmistetaan se että kaikki asiat toimivat, sekä liiketoiminnalliset ja tekniset näkökulmat IPv6:n käyttöönotossa otetaan huomioon. Tärkeää olisi saada koko organisaation tuki mukaan projektiin. Kuitenkaan kaikkien ihmisten ei tarvitse tietää, eikä pidäkään tietää kaikkea, vaan eri rooleissa toimivat henkilöt tulisi kategorisoida omiin ryhmiinsä sen perusteella minkälaista IPv6-koulutusta he vaativat. Nämä voidaan jakaa erilaisiin kategorioihin, joista esimerkkeinä voivat olla seuraavat.

- Tietoisuuskoulutus, jossa opetetaan IPv6:n tekniset ja liiketoiminnalliset perusteet.
- Arkkitehtuurinen koulutus, missä opetetaan IPv6:n arkkitehtuurista, suunnittelusta ja käyttöönotosta.
- Operatiivinen koulutus, missä opetetaan IPv6:n operatiivista käyttöä verkossa.
- Erikoiskoulutus, missä keskitytään tiettyyn tekniseen alueeseen (esim. tietoturva, mobiilitekniikat ym.)

Organisaatiosta ja tilanteesta riippuen eri koulutuskategorioita voi yhdistellä tai muunnella tarpeen mukaan. (McFarland 2011, 95-96.)

6.3.5 Pilottihanke

Etenkin suurissa organisaatioissa siirryttäessä IPv6:n käyttöönottoon on lähes aina tehtävä pilottitestaus, missä erillisessä kontrolloidussa ympäristössä simuloidaan IPv6:n käyttöönottoa organisaation järjestelmissä. Pilottihankkeella on tarkoitus hankkia tietoa miten organisaation järjestelmä käyttäytyy IPv6:n siirryttäessä ja mitä mahdollisia ongelmia tai vaikutuksia siitä aiheutuu. Pilottihanke voidaan toteuttaa useassa eri vaiheessa, aluksi esim. ottamalla vain osa verkosta kokeiluun ja laajentamalla sitä lopuksi koskemaan koko verkkoa ja vaikka suoraan siirtyä varsinaiseen käyttöönottoon. (McFarland 2011, 96.)

6.3.6 Ongelmat laitteissa ja ohjelmistoissa

Vaikka organisaatiossa olisi otettu huomioon IPv6 laite- ja ohjelmistohankinnoissa tai jo olemassa olevissa laitteissa ja ohjelmistoissa, niin näin ei välttämättä ole. Jos laite- ja ohjelmistokanta olisi muuten IPv6-yhteensopivia, niin tämä ei silti välttämättä pidä paikkaansa. Periaatteessa IPv6-yhteensopiva laite voi pitää sisällään ongelmia ja siitä voi puuttua pakollisia ominaisuuksia, mitä voidaan tarvita verkon käytössä. Välttämättä edes uusimista ohjelmistopäivityksistä ei ole apua ongelmien korjaamiseen jolloin pahimmassa tapauksessa joudutaan hankkimaan kokonaan uudet laitteet tai ohjelmat.

IPv6 voi aiheuttaa ongelmia myös aikaisemmin toimiville ohjelmille, esim. jos aikaisemmin toimiva virustorjuntaohjelma oletuksena blokkaa kaiken IPv6-liikenteen, eikä sitä saa kytkettyä toimimaan IPv6-verkossa, niin voi joutua pakostakin etsimään vaihtoehtoisia ratkaisuja näille ohjelmille.

6.3.7 Ongelmat IPv6-verkon käytössä

IPv6 voi tuoda ja todennäköisesti myös tuo uusia ongelmia, joita IT-tuki joutuu korjaamaan. Nämä ongelmat voivat olla sellaisia mitä ei esiinny IPv4-verkossa. Ongelmia voi tuoda esim. DHCP-palvelu, selaimet, päätelaitteet, periaatteessa ihan mikä tahansa järjestelmän osa. Näiden ongelmien huomioiminen jo käyttöönottovaiheessa on tärkeää, sillä pahimmassa tapauksessa ne voivat estää tai kaataa koko verkon käytön.

6.3.8 Yhteistyö organisaation ja valmistajien välillä

Varsinkin näin IPv6:n käyttöönoton alkuvaiheessa, jolloin vasta ohjelmistojen ja laitteiden valmistajat suunnittelevat ja tutkivat uusia versioita, voi ongelmia ilmetä yllättäviltä tahoilta. Yrityksen laitteet tai ohjelmat voivat käyttää ominaisuuksia joita valmistajat eivät ole osanneet ottaa vielä huomioon, joten välttämättä uusin ohjelmistopäivityskään ei tuo ratkaisua ongelmaan. Tällöin organisaatiolla tulee olla hyvät yhteydet valmistajiin ongelmien ratkaisemiseksi. Tähän pitää varata kuitenkin reilusti aikaa ja energiaa sillä valmistajat eivät välttämättä ymmärrä ongelmaa tai organisaation käytössä olevaa ohjelmaa. Näin ollen ongelman ratkaisemiseen voi kulua paljonkin aikaa, jos ei vikaa osata paikantaa tai sen korjaamiseen löydetä sopivaa ratkaisua.

7. IPv6 organisaatio-caset

Selvitimme muutamasta yrityksestä ja muusta organisaatiosta mikä heidän IPv6-tilanteensa on ja miten he ovat IPv6:n saapumiseen varautuneet. Tarkoituksena oli selvittää nykytilanne, millaiset IPv6-käyttöönottosuunnitelmat heillä on IPv6:n suhteen ja miten IPv6 vaikuttaa heidän palveluihinsa, tuotteisiin, toimintaan ym.

Kohdeorganisaatioita oli kolme kappaletta, joista 2 oli liikeyrityksiä ja yksi valtion virasto. Liikeyrityksistä toinen oli Louhi Net Oy, joka tarjoaa internet hosting-palveluita. Louhelta haastateltavana oli online-palveluiden liiketoimintapäällikkö Lassi Virtanen. Toinen liikeyrityksistä oli yritys X (joka ei halunnut nimeään mainittavan opinnäytetyössä), josta haastattelimme yrityksen tietohallintopäällikköä. Kolmantena organisaationa oli valtionvirasto Y (joka ei halunnut nimeään mainittavan opinnäytetyössä), josta haastattelimme viraston kehityspäällikköä. Tarkoituksena oli valita kohdeorganisaatiot erityyppisiltä toimialoilta, jotta saisimme kattavamman näkökulman IPv6-tilanteesta.

Pyysimme jokaiselta näiden organisaatioiden edustajilta haastattelun, haastatteluiden vastaukset löytyvät liite-osiosta. Analysoimme haastatteluista saadut tiedot ja lopuksi

vertasimme saatuja tietoja yleiseen tilanteeseen yrityksissä ja muissa organisaatioissa Suomessa. Kaikissa haastateltavissa organisaatioissa oli IPv6-siirtymä vasta harkinnan alla tai vasta tulossa tulevaisuudessa. Emme saaneet pyynnöistä huolimatta haastateltavaksi yritystä tai organisaatiota jossa olisi IPv6-siirtymä käynnissä tai jo tehty.

7.1 Case Louhi Net Oy

Tämä luku käsittelee yrityscase Louhi Net Oy:tä. Opinnäytetyötä varten haastateltiin yrityksen online-palveluiden liiketoimintapäällikkö Lassi Virtasta. Haastattelu löytyy tämän opinnäytetyön liitteistä.

7.1.1 Louhen perustiedot

Louhi Net Oy on Suomessa toimiva internet Hosting-palveluita tarjoava yritys. Yrityksellä on toimipiste Espoon Perkkaalla ja se työllistää 25 henkeä. Yrityksen liikevaihto on n. 3 miljoona euroa. Asiakkaita Louhella on n. 14 000. Asiakkaista 99 % on kotimaisia.

7.1.2 Louhen palveluiden määrittely

Louhi Net Oy tarjoaa yksityis- ja yritysasiakkaille erilaisia Webhotel ja Domain palveluita, tiedon tallennus ja roskapostinsuodatuspalveluita sekä virtuaali- ja OnDemand-palveluita. Tällä hetkellä kaikki Louhen palvelut toimivat IPv4-verkossa ja tulevat todennäköisesti säilymään vielä pitkään, koska akuuttia tarvetta IPv6:n käyttöönotolle ei vielä ole. Esimerkiksi IPv4-osoitteita on vielä runsaasti jäljellä Louhella käytössä.

7.1.3 IPv6:n vaikutus Louhen palveluihin ja asiakkaisiin

IPv6:n tuleminen koskettaa myös Louhen palveluita, tulevaisuudessa myös Louhi tulee siirtymään IPv6-pohjaisiin verkkoratkaisuihin kun IPv6:n käyttö yleistyy. Tällä hetkellä Louhella ei ole suurta kiinnostusta IPv6:sta kohtaan, sillä asiakkaiden kiinnostus IPv6:sta kohtaan on ollut hyvin vähäistä. Kysynnän vähäisyyden vuoksi IPv6-muunnos tulisi liian kalliiksi. Tulevaisuutta silmällä pitäen Louhen laitteistoissa ja infrastruktuurissa on jo nyt IPv6-tuki olemassa ja sen käyttöönotto on mahdollista tarvittaessa. Mitään palveluita ei kuitenkaan ole vielä siirretty IPv6-verkkoon. Ensimmäisenä tullaan päivittämään nimipalvelun palvelut IPv6-verkkoon, mutta siihen menee vielä pitkä aika ennen kuin Louhi tarjoaa nimipalvelimille pelkästään pelkkiä IPv6-osoitteita.

IPv6-verkon yleistyessä Louhen vanhoille asiakkaille tullaan tarjoamaan rinnakkain palvelut palvelimilla myös IPv6:n puolella jolloin loppuasiakkaille ei tule näkymään näkyviä muutoksia.

Tässä vaiheessa IPv6:n mahdollisesti tuomat uudet palvelut tai ominaisuudet voidaan siirtää Louhen palveluihin.

7.1.4 IPv6:n lisäarvo Louhelle

Tällä hetkellä Louhella ollaan melko pessimistisiä IPv6:n suhteen, Louhella odotetaan IPv6:n läpimurtoa ja mitään suuria rahallisia tai teknisiä panostuksia ei vielä haluta tehdä. Louhi näkee IPv6:seen siirtymisen lähinnä teknisenä asiana josta ei oleteta saavan isompaa hyötyä. Ainut hyöty mikä IPv6:seen siirtymisessä olisi, on markkinointihyöty IPv6-edelläkävijänä. Kuitenkaan suurinta osaa asiakaskunnasta ei kiinnosta käytössä oleva tekniikka, niin sen hyödyt jäisivät vähäisiksi. Asiakkaan kannalta tärkeintä on palveluiden toimivuus ja luotettavuus, Louhelta todetaan. Osa Louhen kilpailijoista tarjoaa jo nyt IPv6-tukea, mutta Louhelta tämä nähdään enemmän markkinointikikkana, kuin todellisena IPv6-tekniikan päänavauksena.

7.1.5 IPv6 tulevaisuudessa osana Louhen palveluita ja tuotteita

Louhella ollaan sitä mieltä, että siirtyminen toden teolla IPv6:n käyttöön tulee viemään vielä vuosia ja tarve IPv4:sta pois siirtymiseen ei ole vielä ajankohtainen. IPv4:n käyttö tulee jatkumaan vielä pitkään IPv6:n käyttöönoton jälkeenkin. Louhi aikoo siirtyä aktiivisesti IPv6:n käyttöön vasta, kun suurella määrällä asiakkaita on tarve siirtyä käyttämään IPv6:sta.

Yksi iso syy Louhen mukaan IPv6:n palveluiden käyttöönoton mahdollistajana ylipäätään on operaattorit. Niin kauan kun operaattoreilla ei ole isoa halua tai tahtoa tarjota IPv6-verkon käyttöä ja palveluita ei siirtymistä voi tehdä. Tällä hetkellä operaattorit eivät tarjoa Louhelle minkäänlaisia IPv6-palveluita. Louhella odotetaankin innokkaana koska operaattorit alkavat tarjota IPv6-palveluita yrityksille ja myös yksityisasiakkaille, mutta tähän voi mennä vielä tovi.

7.2 Case yritys X

Tämä case käsittelee yritys X:n casea. Opinnäytetyötä varten haastateltiin yrityksen tietohallintopäällikköä. Haastattelu löytyy opinnäytetyön liitteistä.

7.2.1 Yritys X:n perustiedot

Yritys X on suomalainen perheyritys joka tarjoaa erilaisia kosmetiikka- ja kulutustuotteita. Liikevaihtoa yritys X:llä on yli 100 miljoonaa euroa ja henkilöstöä yli 500 henkeä.

7.2.2 Yritys X:n IPv6-tilanne

Siirtyminen IPv6:n käyttöön yritys X:ssä ei tällä hetkellä ole ajankohtaista vaan asiaan perehdytään tarkemmin tulevaisuudessa. Yrityksessä on tiedostettu IPv6:n tuleminen, mutta toimenpiteisiin sen suhteen ei ole ryhdytty. Yrityksessä arvioidaan asian tulevan ajankohtaiseksi n. 3-5 vuoden sisällä. Yrityksen näkemyksen mukaan IPv6 ei tule ainakaan lähitulevaisuudessa vaikuttamaan heidän asiakkaisiinsa tai palveluihin, eikä heidän asiakkaillaan ole ollut kiinnostusta IPv6-palveluihin. Yrityksessä ei uskota IPv6-siirtymän tuovan tulevaisuudessa heille uusia asiakkaita tai palveluja.

Yrityksessä on kuitenkin kiinnostusta saada selville IPv6:n tarjoamia mahdollisuuksia, sekä sen antamaa lisäarvoa ja sen käytöstä ollaan kiinnostuneita mutta tietyllä varauksella. Esimerkiksi mahdollisia ongelmia voisi olla hyöty IPv6:sta suhteessa sen käyttöönottoon vaadittaviin kustannuksiin, on ymmärrettävää jos yrityksessä nähdään IPv6:sta saatavat hyödyt pienempinä mitä siihen käytetyt varat. Käyttöönottoon ei haluta ryhtyä viimeistään ennen kuin siihen on pakko.

7.3 Case valtionvirasto Y

Tämä luku käsittelee valtionvirasto Y:n casea. Opinnäytetyötä varten haastateltiin viraston kehityspäällikköä. Haastattelu löytyy opinnäytetyön liitteistä.

7.3.1 Valtionvirasto Y:n perustiedot

Yksi kohdecaseista on Suomen valtion virasto (joka ei halua nimeään mainittavan työssä), joka toiminta liittyy lääkealaan. Viraston toimipisteet sijaitsevat Helsingissä, Kuopiossa, Turussa sekä Oulussa ja sillä on henkilöstöä yli 200 henkeä. Viraston toimenkuvana on valvoa lääkkeitä, veri- ja kudostuotteita sekä kehittää lääkealaa. Asiakkaina ovat tavalliset kansalaiset sekä lääketeollisuus.

7.3.2 Valtionvirasto Y:n IPv6-tilanne

Siirtyminen IPv6:n käyttöön virasto Y:ssä ei ole vielä ajankohtainen. Ylipäätään koko IPv6 on melko tuntematonta aluetta virastolle, eikä suunnitelmia IPv6:n suhteen ole tehty tai suunnitteilla. Myöskään viraston asiakkailla tai sidosryhmillä ei ole ollut kiinnostusta IPv6-pohjaisten palveluiden käyttöön, eikä virasto ole tehnyt selvityksiä IPv6-palveluiden käyttöönotosta. Ylipäätään IPv6 ei pidetä kovin ajankohtaisena asiana, sillä heidän näkemyksen mukaan sen käyttöönotto voi viedä vielä vuosia.

Valtion virastojen IT-politiikka määritellään ylemmällä virkamiestasolla eli käytännössä ministeriötasolla, jolloin uudet tekniikat otetaan vasta viimeiseksi käyttöön kun muut yritykset ja organisaatiot ovat jo niihin siirtyneet. Tämä johtuu osittain myös siitä, että halutaan turvata palveluiden toimivuus joka tilanteessa, koska kyseessä on yhteiskunnan kannalta elintärkeät toiminnot. Näin ollen virastoissa ei voida ottaa käyttöön puolivalmiita tai teknisesti / muuten epätäydellisiä tekniikoita, jotka voivat aiheuttaa käyttökatkoksia tai ongelmia palveluiden saatavuuteen. Virasto Y:n ei vielä toukokuussa 2012 ollut tullut ylemmältä virkamiestasolta IPv6:n käyttöönottoon liittyviä määrityksiä.

7.4 Yhteenveto caseista ja haastattelutuloksista

Haastattelimme opinnäytetyötä varten kahta eri yritystä sekä kahta muuta organisaatiota ja kyselimme heidän IPv6-tilanteesta ja käyttöönottosuunnitelmista. Eri organisaatioilta kysyttiin hieman eri asioita, riippuen minkälaisesta organisaatiosta oli kyse ja mitä heidän toimintaansa kuului. Vastaukset olivat jokaisessa organisaatiossa melko yhtenevät vaikka organisaatioiden funktio ja toiminta yhteiskunnassa erosivat toisistaan. Saadut vastaukset eivät yllättäneet, vaan suurimmassa osassa organisaatioita IPv6:n käyttöön ei vielä ollut ryhdytty eikä suurempia suunnitelmia tehty. Osassa organisaatiossa oli tehty alustavia selvityksiä laitteiston ja muun infrastruktuurin suhteen miten ne toimivat IPv6 ympäristössä. Yhdessäkään organisaatiossa ei kuitenkaan ollut valmista suunnitelmaa IPv6:n suhteen, eikä tarkkaa aikataulua sen käyttöönottamiseksi. Tämä tukee hyvin sitä mielikuvaa, mitä opinnäytetyön aikana on saatu organisaatioiden ja yritysten IPv6-tilanteesta Suomessa.

Ilahduttavaa oli kuitenkin haastateltujen organisaatioiden IPv6-tietämys. Lähes jokaisessa organisaatiossa tiedettiin ainakin jollakin tasolla mikä IPv6 on ja mihin se liittyy. Myös jonkinlaisia arvioita esitettiin, koska mahdollisesti IPv6 tulisi yleisesti käyttöön. IT-maailmassa asiat kuitenkin muuttuvat nopeaan tahtiin. On ymmärrettävää ettei organisaatiossa ole varsinaisia konkreettisia ratkaisuja tehty, jos arviot IPv6:n käyttöönotosta vaihtelivat keskimäärin 2-5 vuoteen.

Vaikka haastatelluissa organisaatioissa oli hyvin tiedossa IPv6:n perusasiat, ei siitä kuitenkaan nähty saatavan hirveästi lisäarvoa tulevaisuudessa. IPv6:n vaikutusta organisaatioiden nykyisiin palveluihin ja tuotteisiin pidettiin epäoleellisena, eikä sen uskottu kasvattavan tai ainakaan positiivisesti lisäävän asiakaskuntaa. Yleinen mielipide oli sellainen, että koko IPv6:n käyttöönottoa pidettiin lähinnä teknisenä siirtymänä. Tätä varmasti osaltaan selittää se, ettei IPv6:n, tai sen tuomiin mahdollisuuksiin ole vielä perehdytty riittävästi organisaatioissa. Tämä toivottavasti tulee muuttumaan tulevaisuudessa, kun IPv6:n käyttöönotto lähenee organisaatioissa pakostakin.

Haastatteluista voi päätellä että tilanne on loppuen lopuksi melko samanlainen kaikkialla. Yleinen näkemys IPv6:sta oli, että se on tulevaisuuden tekniikka, joka pitää ottaa huomioon tulevaisuudessa. Kuitenkin IPv6:n käyttöönottoon organisaatioissa voi mennä vielä useita vuosia. Suurimpana syynä siihen miksei organisaatioissa ole vielä siirrytty IPv6:n käyttöön, on se, ettei siihen ole vielä pakottavaa tarvetta.

Osassa organisaatioissa on jo laadittu suunnitelmia ja tehty käytännön toimenpiteitä jo nyt IPv6:n käyttöönottoa varten, mutta osa organisaatioista ei ole vielä käyttänyt asiaan vielä yhtään aikaa tai energiaa. Osalla organisaatioista oli infrastruktuurissa IPv6-valmius laitteiston ja ohjelmistojen osalta ja suunnitelmia tehty mm. koulutuksen ja käyttöönoton osalta. Kaikkein huonoin tilanne oli valtion virastolla, jossa IPv6:n ei ole perehdytty kovin tarkasti. Toisaalta osittain tämä johtuu valtion virastojen harjoittamasta it-politiikasta.

8. Yhteenveto ja pohdinta

IPv6 tekee hitaasti tuloa, osittain vapaaehtoisesti, osittain pakon sanelemana. Asiantuntijat arvioivat 10–15 vuotta sitten IPv6:n tulevan täysipainoisesti käyttöön 5-10 vuoden sisällä. Tämä ei ole toteutunut, vaan nyt asiantuntija-arviot ovat edelleen sen samat 5-10 vuotta. Onneksi tilanne on tänään parempi, mitä se oli 5-10 vuotta sitten. Nyt on vihdoin tultu siihen pisteeseen, että IPv4:n tulevaisuus on kuljettu loppuun, kuitenkaan se ei tule häviämään verkoista vielä vuosikymmeniin vaikka IPv6 korvaisikin sen täysin.

IPv4:n osoiteavaruuden loppuminen ja muut tässä dokumentissa esitetyt syyt ovat pikkuhiljaa avanneet portit IPv6:lle ja myös pikkuhiljaa eri organisaatioiden olisi syytä siitä kiinnostua. Vielä ei ole liian myöhäistä aloittaa suunnitella IPv6-verkon käyttöönottoa tai palveluiden siirtämistä IPv6-puolelle organisaatiossa, mutta pikkuhiljaa se pitäisi ottaa huomioon. Ensimmäiset organisaatiot ovat maailmalla ja myös Suomessa jo täysillä siirtyneet IPv6:n käyttöön, sekä samalla opetelleet kantapään kautta kaikki lastentaudit ja ongelmat mitä se on tuonut. Jos organisaatio haluaa mainostaa itseään IPv6-edelläkävijänä, sekään ei ole vielä liian myöhäistä, jos IPv6:n käyttöönotto aloitetaan nyt.

Maailmalla ja myös Suomessa IPv6-liikenteen määrät ovat lisääntyneet, ei räjähdysmäisen nopeasti mitä odotettiin, vaan hitaasti tasaisesti kasvamalla. Tämä osoittaa sen, että organisaatiot sekä yksityiset käyttäjät ovat ottaneet ja ottavat jatkossakin IPv6-yhteyksiä käyttöön. Suurimpana vauhdittajana tässä on operaattorit, jotka toivottavasti tarjoavat jatkossa sekä yksityis- että yritysasiakkaille mahdollisimman monipuolisia IPv6-liittymiä.

Jokaisen organisaation tulee kuitenkin itse miettiä missä vaiheessa se haluaa IPv6:n siirtyä täysillä ja mitä hyötyä IPv6:n siirtyminen tarjoaa sille. IPv6:sta ei missään tapauksessa

kannata unohtaa, sillä tänään tehdyt ratkaisut voivat pahimmassa tapauksessa kostautua tulevaisuudessa. Päinvastoin nyt tehdyt panostukset IPv6-tekniikkaan voivat tulevaisuudessa IPv6-sovellusten kehittymisen ja käyttömäärien kasvun vuoksi tuoda organisaatiolle uusia potentiaalisia kasvun mahdollisuuksia, niin liiketoiminnassa kuin muissakin organisaatiota hyödyttävissä asioissa.

LÄHTEET

Casad, J. 2011. Sams Teach Yourself TCP/IP in 24 hours, Fifth Edition.5. painos. United States of America: Pearson Education.

CCNA 1: Networking Basics 3.1. 31.01.2005.
Module 9: TCP/IP Protocol Suite and IP Addressing

Comer, Douglas. 2000. Internetworking with TCP/IP:Principles, Protocols, and Architectures. 4. painos. Upper Saddle River, NJ: Prentice Hall.

Desmeules, R. Syyskuu 2007. Cisco Self-Study: Implementing IPv6 Networks (IPv6). 3. painos. United States of America: Cisco Press.

Douglas, E. C. 2002. TCP/IP. Jyväskylä: Gummerus.

Hakala, M. & Vainio, M. 2002. Tietoverkon rakentaminen. Jyväskylä: Docendo.

Kaario, K. 2002. TCP/IP-verkot. Porvoo: WSOY.

McFarland S, Sambi M, Sharma N, Hooda S. 2011. Cisco: IPv6 for Enterprise Networks. United States of America, Indianapolis: Cisco Press.

Ape3000.com 2011. IPv6-tuki suomalaisissa yksityishenkilöiden laajakaistaliittymissä. Viitattu 26.4.2012.
http://ape3000.com/ipv6/

BitTorrent Networks. Viitattu 2.5.2012.
http://tools.ietf.org/html/draft-vyncke-ipv6-traffic-in-p2p-networks-01

Cisco Systems. 24.01.2006. How NAT Works. [Pdf-julkaisu]. Cisco Systems [viitattu 23.5.2012].
http://www.cisco.com/image/gif/paws/6450/nat-cisco.pdf

FICIX 2011. Finnish Communication and Internet Exchange - FICIX ry. Viitattu 2.5.2012.
http://www.ficix.fi/

IPv6-tilanne Suomessa. Ficora 2005. Viitattu 2.5.2012.
http://www.ficora.fi/attachments/suomiry/1158858938733/TRaportti092005.pdf

Viestintävirasto parantaa fi-juuren IPv6-tukea. Ficora 2008. Viitattu 26.4.2012.
http://www.ficora.fi/index/viestintavirasto/uutiset/2008/P_140.html

IPv6-käyttöönotto AYY:n opiskelijaverkossa. Ficora 2011. Viitattu 26.4.2012.
http://www.ficora.fi/attachments/suomial/5xiWZV4lx/IPv611_Myyry.pdf
http://vimeo.com/21944823

IPv6-seminaarin 4.4.2011 esitykset. Ficora 2011. Viitattu 26.4.2012.
http://www.ficora.fi/index/viestintavirasto/asiakastiedotteet/verkotjaturvallisuus/2011/P_1.html

Fix6 2011. IPv6 address allocations. Viitattu 24.4.2012.
http://www.fix6.net/archives/2011/03/15/ipv6-address-allocations/

History of the Internet. Birth of TCP/IP Networking Protocol (Chapter 4 Excerpt).
Viitattu 14.5.2012
http://www.historyoftheinternet.com/chap4.html

IANA.org 2011. Protocol Numbers. Viitattu 1.6.2012.
http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml

Dynamic NAT. IBM. Viitattu 23.5.2012.
http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzajw%2Frzajwdynamic.htm

Static NAT. IBM. Viitattu 25.5.2012.
http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzajw%2Frzajwstatic.htm.

IETF The Internet Engineering Task Force 1999. Request for Comments (RFC) 2526, Reserved IPv6 Subnet Anycast Addresses. Viitattu 15.4.2012.
http://tools.ietf.org/html/rfc2526

IPv6 Tunnel Broker. Request for Comments (RFC) 3053. IETF The Internet Engineering Task Force 2011. Viitattu 15.4.2012.
http://www.ietf.org/rfc/rfc3053.txt

6bone (IPv6 testing address allocation) Phaseout. Request for Comments (RFC) 3701. IETF The Internet Engineering Task Force 2004, Viitattu 31.5.2012.
http://tools.ietf.org/html/rfc3701

Basic Transition mechanisms for IPv6 Hosts and Routers. Request for Comments (RFC) 4213. IETF The Internet Engineering Task Force 2005. Viitattu 31.5.2012
http://tools.ietf.org/html/rfc4213

Neighbor Discovery for IP version 6 (IPv6). Request for Comments (RFC) 4861. IETF The Internet Engineering Task Force 2007. Viitattu 15.4.2012.
http://tools.ietf.org/html/rfc4861

IPv6 Rapid Deployment on IPv4 Infrastructures (6rd). Request for Comments (RFC) 5569. IETF The Internet Engineering Task Force 2010. Viitattu 15.4.2012.
http://tools.ietf.org/html/rfc5569

IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification. Request for Comments (RFC) 5969. IETF The Internet Engineering Task Force 2010. Viitattu 15.4.2012.
http://tools.ietf.org/html/rfc5969

Measuring IPv6 Traffic in BitTorrent Networks. Draft. IETF The Internet Engineering Task Force 2012. Viitattu 15.4.2012.
http://tools.ietf.org/html/draft-defeche-ipv6-traffic-in-p2p-networks-00

Ipv6.com. IPv6 Deployment Around the World. Viitattu 1.5.2012
http://ipv6.com/articles/deployment/IPv6-Deployment-Status.htm

IPv6actnow 2012. Global IPv6 allocations & assigments. Viitattu 22.4.2012.
http://www.ipv6actnow.org/statistics/allocations-and-assignments/

Isoc 2009. IPv6 deployment in Africa. Viitattu 25.4.2012.
http://www.isoc.org/isoc/conferences/inet/09/docs/afrinic_20090518.pdf

Microsoft TechNet. 2012. TCP/IP Protocol Architecture. Viitattu 31.5.2012
http://technet.microsoft.com/en-us/library/cc958821.aspx

Networkworld. 2012. Business continuity emerges as latest IPv6 killer app. Viitattu 1.5.2012.
http://www.networkworld.com/news/2012/041112-business-continuity-ipv6-258166.html

Protocols.com. TCP/IP Suite. Viitattu 23.5.2012.
http://www.protocols.com/pbook/tcpip2.htm.

Ratol.fi OSI-malli. Viitattu 15.5.2012.
http://www.ratol.fi/opensource/lahiverkot/fin/yleista/osi_malli.htm

Search Networking. 2002. IPv6: Seven killer capabilities. Viitattu 1.5.2012.
http://searchnetworking.techtarget.com/news/851321/IPv6-Seven-killer-capabilities

Young, J. H. Helmikuu 2006. IP Packet Structure. Computer science Now. Viitattu 23.05.2012.
http://www.comsci.us/datacom/ippacket.html.

Vyncke 2012. IPv6-enabled BitTorrent Peers. Viitattu 2.5.2012.
http://www.vyncke.org/ipv6status/p2p.php?date=2012-04-12&region=world&ipv6=any

World IPv6 day 2012. Viitattu 22.4.2012.
http://www.worldipv6day.org/

World IPv6 launch 2012. Viitattu 22.4.2012.
http://www.worldipv6launch.org/

Kuvat:

Krimaka.net. 2012. TCP-IP malli. Viitattu 15.4.2012.
http://www.krimaka.net/tietotekniikka/verkko-ja-ethernet/kuvat/osi.gif

IP-paketti. Wikipedia 2012. Viitattu 15.4.2012.
http://fi.wikipedia.org/wiki/Tiedosto:IP-paketti.png

OSI-malli. Wikipedia 2011. Viitattu 15.4.2012.
http://fi.wikipedia.org/wiki/Tiedosto:OSI-malli.jpg

KUVAT JA TAULUKOT

Kuva 1: TCP/IP - malli ylimmästä alimpaan (Krimaka) 11
Kuva 2: IP-paketti 13
Kuva 3: Internet protokollat 14
Kuva 4: OSI-malli (Wikipedia OSI-malli) 15
Kuva 5: Osoiteluokat 18
Kuva 6: Dynaaminen NAT-toiminta. (Dynamic NAT [viitattu 23.05.2012].) 19
Kuva 7: Staattinen NAT-toiminta. (Static NAT [viitattu 23.05.2012].) 20
Kuva 8: IPv4:n otsikkokentän rakenne Kuva: http://fi.wikipedia.org/wiki/IP-paketti.. 21
Kuva 9: Link Local osoite 25
Kuva 10: Site local osoite 26
Kuva 11: Globaali osoite 26
Kuva 12: Multicast osoite 27
Kuva 13: IPv6 kyselyt per sekunti 2.4.2011 – 16.4.2012 välisenä aikana 37
Kuva 14: IPv6 vastaukset per sekunti 2.4 – 16.4.2012 välisenä aikana 37

LIITTEET

Liite 1 Louhi Net Oy haastattelu 21.3.2012 58

Liite 2 Yritys X:n haastattelu 9.5.2012 62

Liite 3 Valtion virasto Y:n haastattelu 21.5.2012 64

Liite 4 Kysely Ficoran IPv6-liikenteestä 4.5.2012 66

Liite 5 Tärkeimmät käsitteet 68

Liite 1: Louhi Net Oy haastattelu 21.3.2012

Haastattelu Louhi Net Oy, haastateltavana online-palveluiden liiketoimintapäällikkö Lassi Virtanen.

1) Louhi Net Oy:n perustiedot:
Nimi: Louhi Net Oy
Sijainti: Espoo, Perkkaa (konesalit Perkkaalla ja Katajanokalla)
Perustamisvuosi: 2004
Toimiala: Verkkopalvelut (hosting)
Omistus: Yksityinen suomalainen omistaja
Yrityskoko: Pk-yritys
Liikevaihto: Noin 3 miljoona euroa
Henkilöstö: 25
Toimipisteet: Espoo, Perkkaa
Valmistus: Suurin osa tuotteista myydään verkon kautta
Myyntipisteet: -
Asiakaskunta: 99 % asiakkaista on kotimaisia
Vienti: -
Tuonti: -

2) Louhi Net Oy:n tarjoamat palvelut:

- Webhotellit
- Domainit
- Jälleenmyynti
- Exchange, Sharepoint ja säilö
- Vartti
- Virtuaali- ja OnDemand-palvelimet
- Palvelinhotellit ja dedikoidut palvelimet
- Sähköposti
- Sovellukset

3) Oletteko yrityksessänne tutkineet palveluiden siirtämistä IPv6 verkkoon? Jos on niin miten?

V: Olemme tutkineet ja meidän verkkoinfra on IPv6 valmis. Meillä ei ole julkista IPv6 verkkoa, koska sille ei ole ollut kysyntää. Käytännössä sen käyttöönotto vaatisi, että hankkisimme julkisen IPv6 verkon. Laitteistot ja sovellusversiot tukevat jo tällä hetkellä siirtymistä IPv6 verkon käyttöön.

4) Mitä mahdollisia ongelmia palveluiden siirtämisestä IPv6 voisi tuoda? V: Yhtenä ongelma voi olla se, että juuri kukaan ei pysty muistamaan IPv6 osoitetta vaikean muodon vuoksi. IP osoite on sellainen mikä ei välttämättä pitäisi näkyä asiakkaalle ollenkaan.

5) Oletteko yrityksessänne testanneet IPv6 verkon valmiutta tekniseltä kannalta?

V: Emme ole mutta käytämme tunnettuja valmistajien laitteita joissa on olemassa IPv6 tuki ja mahdollisuus ottaa se tarvittaessa käyttöön. Mitään palveluita ei ole vielä siirretty fyysisesti tukemaan IPv6:sta.

5) Löytyykö yrityksessänne kiinnostusta saada selville IPv6 verkon tarjoamia mahdollisuuksia?

V: Meillä on tällä hetkellä riittävästi IPv4 osoitteita olemassa, joten meillä ei ole tarvetta IPv6 verkon käyttöönotolle tällä hetkellä. Totta kai jos joku keksii jonkun suuren liiketoimintamahdollisuuden IPv6, niin olemme kiinnostuneita mutta emme itse ole vielä keksineet mitään lisäarvoa mitä IPv6 toisi asiakkaalle.

6) Onko yrityksillä/asiakkailla ollut kiinnostusta siirtymisestä Ipv6-verkon käyttöön tai IPv6 pohjaisiin palveluihin?

V: Meille on tähän mennessä tullut alle 10 kyselyä koko IPv6 asiaan liittyen ja meillä on asiakkaita lähes 14 000. Ensimmäisenä tullaan päivittämään nimipalvelun palvelut IPv6 verkkoon, jotta voidaan nimipalveluita tarjota tarvittaessa tulevaisuudessa. Siihen menee varmasti vielä pitkä aika ennen kuin alamme tarjoamaan nimipalvelimille pelkkiä IPv6 osoitteita.

7) Mitä nykyisistä palveluistanne voisi tarjota IPv6 verkossa? Kuinka isoja investointeja tämä vaatisi?

V: Olemme hosting yritys joka tarjoaa verkkopalveluita, joten lähes kaikki meidän palvelut on mahdollista tarjota IPv6 verkossa. Laitehankintoja ei tarvitse tehdä, koska niissä on jo olemassa IPv6 tuki. Muuttuvat kustannukset koostuvat työmäärästä joka joudutaan käyttämään IPv6 käyttöönottoon ja kiinteät kustannukset hinnasta jonka operaattorit velottavat verkko-osoitteiden käytöstä.

8) Mitä lisäarvoa siirtyminen IPv6-verkkoon toisi yrityksellenne?

V: Lisäarvona olisi markkinointihyöty, jolloin asiakkaille voisi markkinoida yritystä edelläkävijänä IPv6 tarjoamissa palveluissa mutta tällä hetkellä asiakkaat eivät ymmärrä tai

eivät ole osoittaneet suurta kiinnostusta tai tietämystä kyseisistä palveluista. Asiakkaan kannalta ei ole väliä mitä teknologiaa palveluissa on käytetty kunhan palvelut toimivat ja palvelulupaukset täyttyvät ja kustannukset pysyvät kiinteänä.

9) Oletteko huomioineet IPv6 verkon mahdollisuudet uusien palveluiden kehityksessä ja uskotteko, että IPv6 voisi tuoda liiketoimintaanne uusia palveluita tai uusia tuotteita?

V: Tämänhetkisen tietämykseni mukaan IPv6 ei mahdollistaisi suoraan mitään uusia palveluita. Pitää muistaa, että yrityksemme ei suoranaisesti tarjoa verkko-osoitteita asiakkaiden päätelaitteille vaan verkko-osoitteet ovat yrityksemme omassa käytössä olevissa laitteissa ja meillä on vielä runsaasti IPv4 osoitteita jäljellä.

11) Miten IPv6 tuleminen vaikuttaa nykyisten asiakkaiden tai palveluiden käyttöön nyt tai tulevaisuudessa?

V: Kun tulevaisuudessa IPv6 verkko otetaan käyttöön tullaan asiakkaille tarjoamaan palvelut palvelimilla molemmissa verkoissa rinnakkain jolloin loppukäyttäjille ei tule muutoksia. Jos IPv6 mahdollisesti mahdollistaa jotain uusia palveluita tai ominaisuuksia niin näitä voidaan hyödyntää samalla. IPv4 tulee kuitenkin säilymää käytössä vielä pitkään ja todennäköisesti ennen IPv4 verkon loppumista tulee palvelut tai palveluiden tarve loppumaan.

12) Uskotteko että (asiakkaiden) IPv6 liittymien lisääntyminen ja kasvu mahdollistaa tulevaisuudessa myös asiakaskunnan kasvua?

V: Tällä hetkellä ei näkyvissä ole semmoista asiakasmäärän kasvua joka kattaisi IPv6 verkon ylläpidosta aiheutuvat kustannukset vaan taustalle tarvittaisiin huomattavasti suurempi asiakasmassa. Tulevaisuudessa muutos tulee joka tapauksessa tapahtumaan kun IPv6 on välttämätön mutta tähän voi mennä vielä vuosia ennen kuin muutokselle on tarvetta. Palveluiden tulee olla käyttäjille näkymättömiä jolloin asiakkaalle ei ole merkitystä onko käytössä IPv4 vai IPv6, korkeintaan molemmat verkot käytössä samaan aikaan jolloin palvelu toimii joka tapauksessa.

13) Osalla webhotelli ym. palveluja tarjoavista kilpailijoista on jo nyt tarjolla IPv6 tuki, onko teillä mahdollisesti jo olemassa tai tulossa vastaavaa palvelua/tukea?

V: Ei ole mainintaa nettisivuilla. Ei ole laajemmalti törmännyt muillakaan palveluntarjoajilla IPv6 tukeen. IPv6 mahdollisuus on kuitenkin laitteistoissa olemassa (webhotellit Redhat v6 joka tukee täysin IPv6) mutta sitä ei aktiivisesti mainosteta. IPv6 on tällä hetkellä lähinnä

mainoskeino. Louhi harkitsee aktiivisesti siirtymistä IPv6 versioon vasta kun suurella määrällä asiakkaita on jokin oikea tarve käyttää IPv6 IPv4 sijaan.

14) Sonera on ilmoittanut että se tarjoaa henkilöasiakkaille IPv6 yhteyksiä aikaisintaan vuonna 2013 ja nyt kesällä (World IPv6 launch) internetin suuret sivustot kuten facebook/google/bing ym. ovat siirtymässä myös IPv6 käyttöön. Miten Louhi näkee IPv6 noin yleisellä tasolla ja minkälaisella aikataululla saapuvan?

V: Suuret sivustot kuten facebook. ym. siirtyvät käyttämään IPv6 mutta jättävät myös IPv4 käyttöön. IPv6 on lähinnä markkinointikeino joilla luodaan kuva yrityksistä teknologisina edelläkävijöinä. IPv6 laajenemisen esteenä ovat tällä hetkellä suomalaiset operaattorit joiden tarpeesta ja halusta kasvu tapahtuu. Louhella ei ole omaa verkkoa vaan yritys ostaa yhteydet ulkopuolisilta palveluntarjoajilta. IPv6 yhteyksien laajempi käyttöönotto vaatisi operaattoreilta aktiivista IPv6 liittymien myyntiä tai tuomista nykyisten yhteyksien rinnalle. Tällä hetkellä operaattorit eivät tarjoa Louhelle minkäänlaisia IPv6 palveluita eikä niiden tulemisesta ole ollut mainintaa. Louhi näkee aktiivisemman muutoksen ja kehityksen kohti IPv6 verkkoa lähtevän operaattoreiden suunnalta. Louhella odotetaan innolla ensimmäisen operaattorin tarjoavan oletuksena asiakkaille IPv6 osoitteita jota ei kuitenkaan uskota tapahtuvan hetkeen.

Liite 2: Yritys X, haastattelu 9.5.2012

Haastattelu Yritys X, haastateltavana yrityksen tietohallintopäällikkö.

1) Yritys X:n perustiedot:
Nimi: -
Sijainti: Espoo
Toimiala: Päivittäistuotteet ja kosmetiikka
Omistus: -
Liikevaihto: yli 100 miljoonaa euroa
Henkilöstö: yli 500 henkeä
Toimipisteet: Espoo, Vantaa
Vienti: Globaali

2) Yritys X:n tarjoamat tuotteet:
V: Kosmetiikka- ja hygieniatuotteita, elintarvikkeet, itsehoitolääkkeet, karkotteet ja torjunta-aineet, kodinhoitotuotteet, puutarhanhoitotuotteet, teollisuustuotteet, ammattisiivous- ja hygienia.

3) Oletteko yrityksessänne tutkineet verkkopalveluiden tai nettisivujen siirtämistä IPv6-verkkoon? Jos on niin miten?
V: Asia on tiedostettu mutta ei ole nähty tarvetta välittömiin toimenpiteisiin.

4) Mitä luulette mitä mahdollisia ongelmia siirtyminen IPv6-verkkoon voisi tuoda?
V: Hyöty liiketoiminnalle suhteessa kustannuksiin.

5) Oletteko yrityksessänne testanneet IPv6-verkon valmiutta tekniseltä kannalta?
V: Ei

6) Löytyykö yrityksessänne kiinnostusta saada selville IPv6-verkon tarjoamia mahdollisuuksia?
V: Kyllä

7) Onko yrityksillä/asiakkailla ollut kiinnostusta siirtymisestä IPv6-pohjaisten sivujen tai palvelujen käyttöön?
V: Ei

8) Mitä nykyisistä palveluistanne voisi tarjota IPv6 verkossa? Kuinka isoja investointeja tämä vaatisi?
V: Asiaa ei ole tutkittu tarkemmin.

Liite 2

9) Mitä lisäarvoa siirtyminen IPv6-verkkoon toisi yrityksellenne?
V: Ei tiedossa

10) Luuletteko että IPv6-verkko lisäisi uusien tuotteiden ja palveluiden markkinointia ja uskotteko, että IPv6 voisi tuoda liiketoimintaanne uusia palveluita, tuotteita tai asiakkaita?
V: Ei

11) Miten luulette IPv6 tulemisen vaikuttavan nykyisten asiakkaiden tai palveluiden käyttöön nyt tai tulevaisuudessa?
V: Ei vaikutusta lähitulevaisuudessa

12) Uskotteko että (asiakkaiden) IPv6 liittymien lisääntyminen ja kasvu mahdollistaa tulevaisuudessa myös teidän asiakaskunnan kasvua?
V: Ei

13) Osaatteko sanoa onko teidän kilpailevilla yrityksillä jo sivuja IPv6-verkossa?
V: Ei

14) Sonera on ilmoittanut että se tarjoaa henkilöasiakkaille IPv6 yhteyksiä aikaisintaan vuonna 2013 ja nyt kesällä (World IPv6 launch) internetin suuret sivustot kuten facebook/google/bing ym. ovat siirtymässä myös IPv6 käyttöön. Onko yritys X:llä mitään näkemystä IPv6 noin yleisellä tasolla ja minkälaisella aikataululla saapuvan?
V: Ei näkemystä – asiaa arvioidaan uudelleen 3-5- vuoden kuluttua

Liite 3: Valtion virasto Y:n haastattelu 21.5.2012

Haastattelu valtionvirasto Y, haastateltavana viraston kehityspäällikkö.

1) Virasto perustiedot:
Nimi: -
Sijainti: Kuopio
Perustamisvuosi:
Toimiala / tehtävät: valtionvirasto
Henkilöstömäärä: 220
Toimipisteet: 2
Asiakaskunta: kansalaiset, lääketeollisuus
Asiakasmäärä: -

2) Viraston tehtävät ja toiminnot:
V: Virasto valvoo lääkkeitä, veri- ja kudostuotteita sekä kehittää lääkealaa

3) Oletteko virastossa tutkineet palveluiden siirtämistä IPv6 verkkoon? Jos on niin miten?
V: ei ole tutkittu

4) Mitä mahdollisia ongelmia palveluiden siirtämisestä IPv6 voisi tuoda?
V: ei ole selvitetty

5) Oletteko virastossa testanneet IPv6 verkon valmiutta tekniseltä kannalta?
V: ei ole testattu

5) Löytyykö virasto kiinnostusta saada selville IPv6 verkon tarjoamia mahdollisuuksia?
V: Ei erityisesti

6) Onko virastolla/asiakkailla ollut kiinnostusta siirtymisestä Ipv6-verkon käyttöön tai IPv6 pohjaisiin palveluihin?
V: Asiakkailta ei ole tullut aiheeseen liittyvää palautetta

7) Mitä nykyisistä palveluistanne voisi tarjota IPv6 verkossa? Kuinka isoja investointeja tämä vaatisi?
V: En tunne IPv6 niin hyvin, että osaisin ottaa kantaa tähän.

8) Mitä lisäarvoa siirtyminen IPv6-verkkoon toisi virastolle?
V: Ei ole tiedossa

Liite 3

9) Oletteko huomioineet IPv6 verkon mahdollisuudet uusien palveluiden kehityksessä ja uskotteko, että IPv6 voisi tuoda liiketoimintaanne uusia palveluita tai uusia tuotteita?
V: IPv6 ei ole esiintynyt edellytyksenä niille palveluilla, joita virastossa kehitetään

11) Miten IPv6 tuleminen vaikuttaa nykyisten asiakkaiden tai palveluiden käyttöön nyt tai tulevaisuudessa?
V: En tiedä onko asiakkaille näkyviä vaikutuksia

12) Osaatteko kertoa mikä on muiden virastojen aikataulu IPv6 suhteen ja onko esim. ministeriöstä tullut joitakin ylemmän tason linjauksia asian suhteen?
V: Ei ole tiedossa

13) Sonera on ilmoittanut että se tarjoaa henkilöasiakkaille IPv6-yhteyksiä aikaisintaan vuonna 2013 ja nyt kesällä (World IPv6 launch) internetin suuret sivustot kuten facebook/google/bing ym. ovat siirtymässä myös IPv6:n käyttöön. Miten virasto näkee IPv6:n noin yleisellä tasolla ja minkälaisella aikataululla saapuvan?
V: Ilmeisesti käyttöönotto viipyy vuosia, koska välittömiä tarpeita ole ja IP-osoitteiden pulaa on lievitetty NAT-osoitemuunnoksilla palomuureissa

Liite 4: Kysely Ficoran IPv6-liikenteestä 4.5.2012

Kysely Ficoran IPv6-liikenteestä

Hei

Pahoittelen että vastaus on viivästynyt.

laitoin liitteeksi primary fi-juurinimipalvelimen IPv6 statistiikkaa. Se kertoo kyselymääristä ainoastaan A.fi:n osalta, mutta kyselyt

jakaantuvat ~suunnilleen tasaisesti kaikille fi-juurinimipalvelimille joilla on IPv6 käytössä.

Statistiikan viimeisin kohta on oikeastaan mielenkiintoisin, se näyttää IPv6 kyselyt viimeisen 12 kuukauden ajalta. Siitä näkee että

kyselymäärät moninkertaistuivat loppuvuodesta viime vuonna. Siihen asti käyttö oli hyvin pientä.

Nyt IPv6 liikenne on noin ~1/8 osa IPv4 liikenteestä A.fi:llä.

Autan mielelläni jos asiasta tulee jotain kysyttävää.

Ystävällisin terveisin:

Sami Salmensuo as FI-DOM technical contact

Finnish Communications Regulatory Authority

tel +358 9 6966 700   fax +358 9 6966 590   fi-domain-tech@ficora.fi

https://domain.fi

Ke 25.huhti 2012 09:50:34 Marjo.Siren@ficora.fi kirjoitti:

>

>

> -----Original Message-----

> From: Konstantin Leppänen [mailto:Konstantin.Leppanen@laurea.fi]

> Sent: 24. huhtikuuta 2012 17:46

> To: Asiakaspalvelu

> Subject: IPv6 verkot Suomessa

>

> Hei,

>

> olen Laurean Ammattikorkeakoulun opiskelija ja teen opinnäytetyötä

Liite 4

> siirtymisestä IPv4 verkoista IPv6 verkon käyttöön. Kysyisinkin
> teiltä löytyykö teiltä mahdollisesti tilastoa tai tietoja kuinka
> paljon tulee nimipalvelukyselyitä IPv4 ja IPv6 verkon kautta
> Suomessa kuluneiden viimeisten vuosien aikana?
>
> Löysin sivuiltanne 4.4.2011 päivätyn IPv6 seminaariin liittyvät
> dokumentit. Myös muu ajankohtainen IPv6 verkkoon liittyvät tiedot
> ovat tervetulleita mikäli teillä on mahdollisuus niitä antaa/myydä
> tai ohjata oikealle sivustolle. Tiedot ja tilastot auttaisivat
> opinnäytetyössäni.
>
> Kiitos avusta!
>
> Ystävällisin terveisin
>
> Konsta Leppänen
>
> --
> Konstantin Leppänen
> Laurea University of Applied Sciences
> Leppävaara Unit
> Department: Business Information Technologies Student number: 0602780
> Group: NTA062
> Email: konstantin.leppanen@laurea.fi

Liite 5

Tärkeimmät käsitteet

- 6bone

IPv4 -> IPv6 kommunikointiin ja kehitykseen käytetty testiverkko josta on luovuttu teknisistä syistä. Siirtoliikenne tapahtuu tunneloimalla IPv6-paketti IPv4-paketin sisään tai natiivisti IPv6-protokollalla.

- 6to4

IPv4 -> IPv6 kommunikointiin käytetty siirtotekniikka jossa IPv6 paketit toimivat IPv4-verkossa ilman erillistä tunnelointia.

- ARPANET (Advanced Research Projects Agency Network)

1969 perustettu tietoverkko josta myöhemmin kehittyi nykyinen Internet.

- Dual Stack

IPv4 -> IP6 kommunikointiin käytetty siirtotekniikka jossa IPv4 ja IPv6 protokollat toimivat yhdessä tai erikseen.

- Ethernet

Pakettipohjainen lähiverkkoratkaisu (LAN), joka on yleisin ja ensimmäisenä laajasti hyväksytty lähiverkkotekniikka

- HTTP (Hypertext Transfer Protocol)

Protokolla jota selaimet ja www-palvelimet käyttävät tiedonsiirtoon.

- IEEE (Standardointiorganisaatio)

Kansainvälinen tekniikan alan järjestö.

- IETF (Standardointiorganisaatio)

Internet-protokollien standardoinnista vastaava organisaatio.

- ITU (International telecommunication Unit)

Kansainvälinen televiestintäliitto, televiestintäverkkoja ja -palveluja kansainvälisesti koordinoiva järjestö.

- IP-osoite

IPv4:n tai IPv6:n osoitesarja joka yksilöi verkkoon kytketyn laitteen.

- IPv4 (Internet protocol versio 4)

TCP/IP-mallin Internet-kerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta Internet-verkossa.

- IPv6 (Internet protocol versio 6)

TCP/IP-mallin Internet-kerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta Internet-verkossa. IPv4 protokollan seuraaja.

- IPv6-tappajasovellus (Killer application)

IPv6:lla toimiva sovellus tai toiminto joka pakottaa organisaatiot ottamaan IPv6:n käyttöön.

- ISO (International Standards organization)

Kansainvälinen standardisoimisjärjestö.

- Lähiverkko, LAN (Local Area Network)

Lähiverkko, rajoitetulla alueella toimiva tietoliikenneverkko.

- NAT (Network Address Translation)

IP-osoitteen osoitteenmuunnostekniikka.

- Otsikkokenttä (Header)

IP-paketin toinen osa joka sisältää IP-paketin tiedot. Toinen osa on datakenttä.

- OSI-malli (Open Systems Interconnection Reference Model)

Tietojärjestelmien liitäntämalli, joka määrittelee tietoliikennejärjestelmän kerrosteisen verkkorakenteen

- RFC-dokumentit (Request for Comments)

Internet Engineering Task Forcen (IETF) julkaisemia asiakirjoja jotka käsittelevät Internetin koskevia standardeja ja käytäntöjä.

- Reititin (Router)

Tietoverkkoja yhdistävä laite, jonka tehtävä on välittää tietoa tietoverkon eri osien välillä.

Liite 5

- TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP-protokolla vastaa päätelaitteiden osoitteistamisesta
ja pakettien reitittämisestä verkossa.

- Teredo

Siirtotekniikka joka mahdollistaa IPv6 yhteyden IPv4 verkossa ilman suoraa yhteyttä IPv6 verkkoon tunneloimalla IPv6 paketin IPv4 UDP pakettiin.

- Tunnel broker

IPv4 -> IPv6 kommunikointiin käytetty siirtotekniikka jossa IPv6-paketti tunneloidaan IPv4-paketin sisään.

- UDP (User Datagram protocol)

Yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedostojen siirron.

- Verkkopalvelut (Network Services)

Palvelimen verkkoon tarjoama palvelu, esim. multimedia- tai sisältökokonaisuus.

- W3C Standardointiorganisaatio (World Wide Web Consortium)

Kansainvälinen yritysten ja yhteisöjen yhteenliittymä, joka ylläpitää ja kehittää www:n standardeja tai suosituksia