Teppo Wahlman

MIKSEI VIELÄKÄÄN IPV6?

Opinnäytetyö

Tietotekniikka

Joulukuu 2016

KYAMK
University of Applied Sciences

KYAMK
University of Applied Sciences

Tekijä/Tekijät	Tutkinto	Aika
Teppo Wahlman	Insinööri (AMK)	Joulukuu 2016

Opinnäytetyön nimi

Miksei vieläkään IPv6?

23 sivua

Toimeksiantaja

Kymenlaakson Ammattikorkeakoulu

Ohjaaja

Yliopettaja Martti Kettunen

Tiivistelmä

IPv4-verkkoprotokollan korvaajaksi suunniteltu IPv6 on tehnyt tuloaan jo kaksi vuosikymmentä. Protokollan uudistusta on ajettu ennen kaikkea IPv4:n niukan osoiteavaruuden takia, joka ei enää pysty nykypäivänä vastaamaan räjähdysmäisesti kasvaneen internetin tarpeisiin. Suurin osa vapaana olevista, julkisista IPv4-osoitteista on käytännössä jo jaeltu palveluntarjoajille. IPv4 on kuitenkin heikkouksistaan huolimatta säilyttänyt asemansa pääasiallisena IP-verkkoprotokollana.

Opinnäytetyössä käydään lyhyesti läpi sekä IPv4-protokollan jatkuvalle tukemiselle rajoitteeksi muodostuneet seikat, että IPv6-protokollan tuomat tärkeimmät uudistukset. IPv4:n elinikää on pidennetty keinotekoisesti NAT-osoitteenmuunnostekniikoilla ja verkko-osoitteiden säännöstelyllä. Siirtymävaihetta silmällä pitäen on kehitetty erityisiä siirtymätekniikoita, joiden avulla IPv4- ja IPv6-laitteet voivat kommunikoida keskenään todellisen yhteensopivuuden puuttuessa protokollien väliltä.

Työn loppupuolella tarkastellaan syitä IPv6:n hitaalle käyttöönotolle. Monista eduistaan huolimatta se ei ole ollut riittävän houkutteleva vaihtoehto yrityksille saati kuluttajille, eikä sen kasvu ole ollut merkittävää kuin vasta muutaman vuoden ajan. Uuteen protokollaan siirtymistä ovat viivyttäneet niin taloudellisen kannattavuuden puute, kuin suunnittelun ja käytännön toteuttamisen haasteet.

IPv6 on viimein alkanut saada merkittävää jalansijaa IPv4:n rinnalla. Kehitystä ovat ajaneet protokollaa tukevien laitteiden ja ohjelmistojen yleistyminen, internet-sisällön- ja palveluntarjoajien kasvava tuki, sekä mobiiliverkkojen räjähdysmäinen kasvu. IPv4 ja IPv6 tulevat elämään rinnakkain vielä vuosia, mutta suuntaus on lupaava ja muutos vain ajan kysymys, nyt paljon konkreettisemmin kuin siirtymävaiheen alkutaipaleella. Verkottuneiden laitteiden ja internet-palveluiden määrän jatkuva kasvu takaa sen, että yhä useammat muodostavat internet-yhteyden IPv6:n avulla.

Asiasanat
IPv6, IPv4, IPv6 siirtymä, Internet

KYAMK
University of Applied Sciences

Author (authors)	Degree	Time
Teppo Wahlman	Bachelor of Engineering	December 2016

Thesis Title

Why Still No IPv6?

23 pages

Commissioned by

Kymenlaakso University of Applied Sciences

Supervisor

Martti Kettunen, Senior Lecturer

Abstract

The IPv6 network protocol was designed to replace the old IPv4 version, but the transition has taken more than two decades. The foremost impetus behind the change was the shrinking pool of IPv4 addresses, which was unable to meet the demands of the exponential growth of the internet. A majority of the available public IPv4 address space has already been distributed to local ISPs. Despite its shortcomings, IPv4 has managed to maintain its place as the dominant IP network protocol.

The purpose of this thesis was to go over the factors limiting the appeal of continued support of IPv4, as well as the primary advancements and benefits of IPv6 deployment. IPv4 has enjoyed extended lifespan via techniques such as NAT address translation and carefully regulated address allocation. Several transition protocols were created to enable communications between IPv4 and IPv6, as the two lack real backwards compatibility.

The various reasons for the slow adaption rate of IPv6 were examined in the latter half of the thesis. Despite its many benefits, IPv6 has lacked real appeal to both enterprises and consumers. The growth of IPv6 networks has been unsubstantial until very recently. The transition has been delayed by both a lack of profitability, as well as the challenges that come with the design and implementation process.

IPv6 has finally started to gain notable foothold beside its predecessor. The increases in compatible hardware and software, online content and service provider support, as well as the rapid growth of mobile networks, have been instrumental to its success. IPv4 and IPv6 will continue to coexist for years to come, however the year that we move away from the old protocol is closer by the day. The continued increase in networked devices and internet services guarantee that more and more internet connections will be established using IPv6.

Keywords

IPv6, IPv4, IPv6 transition, Internet

SISÄLLYS

LYHENNELUETTELO

6TO4	IPv4-IPv6 tunnelointimetodi.
AH	Authentication Header. Pakettien todennukseen ja eheyden tarkistamiseen suunniteltu protokolla.
ARIN	American Registry for Internet Numbers. Amerikassa IP-osoitteita hallinnoiva RIR.
ARPANET	The Advanced Research Projects Agency Network. USA:n puolustusministeriön alulle panema verkkohanke, josta syntyi internet.
DHCP	Dynamic Host Configuration Protocol. Verkon laitteille IP-osoitteita jakeleva protokolla.
DHCPV6	DHCP:n IPv6 versio.
DNS	Domain Name System. Nimipalvelin, yhdistää IP-osoitteet niitä vastaaviin verkkosivujen nimiin.
DNS64	DNS IPv6 versio.
ESP	Encapsulating Security Payload. Pakettivirtojen salaamiseen käytetty protokolla.
IANA	The Internet Assigned Numbers Authority. Internet-resurssien jakelusta vastaava maailmanlaajuinen järjestö.
IETF	Internet Engineering Task Force. Internet-protokollien standardoinnista ja kehityksestä vastaava organisaatio.
IOT	Internet of Things. Esineiden internet, jolla kuvataan verkon yli ohjattavien laitteiden yleistymistä.
IPNG	Internet Protocol Next Generation. Alkuperäinen suunnitelma IPv4:lle, josta tuli lopulta IPv6.
IPSEC	Internet Protocol Security. TCP/IP yhteyksien turvaamiseen tarkoitettu protokollaperhe.

IPV4	Internet Protocol version 4.
IPV6	Internet Protocol version 6.
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol. Tunnelointimetodi sisäverkkoihin.
ISP	Internet Service Provider. Internet-palveluntarjoaja.
NAT	Network Address Translation. Osoitteenmuunnos, mahdollistaa IP-osoitteiden vaihtamisen toisiksi osoitteiksi.
NAT64	Osoitteenmuunnos IPv4- ja IPv6-osoitteiden välillä.
NDP	Neighbor Discovery Protocol. Käytetään naapuruussuhteiden muodostamisessa IPv6-verkoissa.
OSI	Open Systems Interconnection. Tiedonsiirtoprotokollien kuvaamiseen kehitetty viitemalli.
PAT	Port Address Translation. Dynaamisen NAT:n muoto, joka tarjoaa myös porttimuunnoksen.
QOS	Quality of Service. Tietoliikenteen luokittelu ja priorisointi.
RFC	Request for Comments. Internetstandardeja käsittelevä dokumentti.
RIPE NCC	The Réseaux IP Européens Network Coordination Centre. Euroopassa IP-osoitteita hallinnoiva RIR.
RIR	Regional Internet Registry. Internet-resurssien jakelusta vastaava alueellinen järjestö.
SLAAC	Stateless Address Autoconfiguration. Tilaton autokonfiguraatio, jonka avulla IPv6-laite voi konfiguroida itselleen osoitteen automaattisesti.

TCP	Transmission Control Protocol. Protokolla yhteyksien luomiseksi internet-laitteiden välillä.
TEREDO	Tunnelointimetodi, joka mahdollistaa IPv6-IPv4 yhteydet NAT:n takaa.
UDP	User Datagram Protocol. Yhteydetön tiedonsiirtoprotokolla.
VPN	Virtual Private Network. Menetelmä, jossa yksityisiä verkkoja yhdistetään julkisen verkon yli.

1 JOHDANTO

IPv6 vietti tämän vuoden alussa 20-vuotisjuhliaan. Tämä edeltäjästään uudistettu verkkoprotokollaperhe suunniteltiin korvaamaan nopeasti ominaisuuksiltaan rajalliseksi todettu IPv4, jota ei oltu suunniteltu vastaamaan räjähdysmäiseen kasvuun kääntyneen internetin haasteisiin. IPv6 luotiin silmälläpitäen tehokkaampaa, turvallisempaa ja automatisoidumpaa tiedonsiirtoa. Ennen kaikkea sen oli tarkoitus korvata IPv4:n rajallinen, kovaa vauhtia hupenemassa ollut 32-bittinen osoiteavaruus uusilla 128-bittisillä osoitteillaan.

Euroopan internet-rekisteriä ylläpitävä Ripe NCC ilmoitti osoitteidensa käytännössä loppuneen jo 2012 (Vänskä 2012). Vain pieniä määriä on saatavilla, osa niistä takaisin käyttöön palautuneita, toiminnasta poistuneilta operaattoreilta perittyjä osoitteita. Niin ikään Pohjois-Amerikan osoitejakelusta vastaava Arin ilmoitti oman varastonsa ehtyneen viime vuonna, ja nyt viimeistään palveluntarjoajia kehotetaan siirtymään IPv6-protokollaan (Darrow 2015). Vuosikymmenten jälkeenkin IPv4 kuitenkin osoittaa sitkeytensä. Vaikka sen käytössä olevat osoitealueet ovat käytännössä jaettu pois, on sen elinikää pidennetty ja pidennetään yhä monin eri tavoin. Säännöstely ja esimerkiksi osoitteenmuunnoksen kaltaiset tekniikat ovat kuitenkin ainoastaan hidastaneet vääjäämätöntä muutosta.

Internet jatkaa kasvuaan. Sen käyttökohteet ja kattavuus tulee vain laajenemaan erilaisten verkkolaitteiden hintojen ja saatavuuden kohdatessa paremmin kuluttajien vaatimukset. IPv6-osoitteisiin siirtyminen on siksi käytännössä pakollista. Suomessa IPv6-palveluita tarjoaa esimerkiksi DNA, Elisa, KaseNet, MPY, Ålcom, Sonera, SuomiCom ja Verkko-osuuskunta Kajo (Tivi 2016).

Tässä työssä käydään lyhyesti läpi vanhan IPv4-protokollan heikkoudet, IPv6:n tuomat uudistukset ja sen käyttöönoton edut, protokollien yhteensopivuus, sekä miten IPv4:n elinikää on pidennetty erilaisin keinoin. Lopuksi tarkastellaan, miksi siirtyminen uudempaan verkkotekniikkaan on ollut verrattain hidasta, miten tilanne on kehittynyt viime vuosina ja miltä tulevaisuus näyttää.

2 IPV4-PROTOKOLLA LYHYESTI

Nykyverkkoja yhä hallitseva protokolla IPv4 ei ole muuttunut merkittävästi vuonna 1981 julkaistusta Request for Comments (RFC) 791 standardista. Internetin kasvaessa nykymittoihinsa yliopistojen välisestä verkosta maailmanlaajuiseksi, IPv4 on osoittanut sitkeytensä ja helppokäyttöisyytensä. On kuitenkin useita asioita, joita sen alkuperäisessä suunnittelussa ei otettu tai osattu ottaa huomioon.

2.1 IPv4-protokollan rajoitukset

Internetin eksponentiaalinen kasvu ja IPv4-osoiteavaruuden hupeneminen

IPv4:n 32-bittinen osoiteavaruus mahdollistaa periaatteessa noin 4,3 miljardia osoitetta, joita säätelee Internet Assigned Numbers Authority (IANA). Osittain johtuen tavoista, joilla varhaisia osoitteita jaettiin, julkisten saatavilla olevien osoitteiden määrä on verrattain pieni. Osoitteiden jakelua on säädelty erilaisin tavoin jo 90-luvulta internetin kääntyessä voimakkaaseen kasvuun, tärkeimpänä NAT (Network Address Translation) jolla muunnetaan yksi julkinen osoite useiksi yksityisiksi osoitteiksi. Osoitteenmuunnokset pidentävät IPv4:n elinikää, mutta myös raskauttavat liikennettä ja hankaloittavat suoria vertaisverkkoyhteyksiä, koska kaikilla verkon solmuilla ei ole omaa uniikkia osoitettaan. Internetiin kytkettyjen laitteiden kasvava määrä tarkoittaa, että osoitteet tulevat loppumaan kesken viivytysyrityksistä huolimatta. (Davies 2012, 1.)

Verkkolaitteiden konfigurointi

Useimmat IPv4 ratkaisut vaativat joko manuaalista konfigurointia, tai tilallisen konfigurointiprotokollan, kuten Dynamic Host Configuration Protocol (DHCP), käyttöä. IP-kytkettyjen laitteiden määrän kasvaessa nousee myös tarve automaattisemmille, vähemmän hallintaa vaativille ratkaisuille.

Tietoturva

Tietoturvan tarve korostuu, kun lähetetään yksityistä tietoa julkisen verkon, kuten internet, yli. Tiedon suojaamiseksi ja sen muokkaamisen estämiseksi

IPv4 tukee Internet Protocol Security (IPsec) standardia, mutta se ei ole pakollinen, ja sen rinnalla on käytössä useita muita tekniikoita.

Tietoliikenteen luokittelu ja priorisointi

Quality of Service (QoS) nimellä usein tunnettuun datan lähetyksen priorisointiin on olemassa standardit IPv4-ympäristössä. Liikenteenhallinta kuitenkin perustuu vanhentuneeseen IPv4-kehyksen Type of Service (ToS) kenttään ja datatyypin tunnistamiseen, tyypillisesti User Datagram Protocol (UDP) tai Transmission Control Protocol (TCP) portin kautta. TOS-kentän rajoitusten vuoksi se on määritelty uudelleen useaan kertaan, mutta nykystandardin mukaan datan prioriteetti luetaan siihen merkittävästä arvosta, jonka datan lähettäjä merkitsee ja välittävät reitittimet tulkitsevat. Toisena rajoituksena salauksen käyttö ei ole mahdollista, jos käytetään UDP- tai TCP-porttia. (Davies 2012, 2.)

2.2 Network Address Translation (NAT)

NAT on osoitteenmuunnostekniikka, joka on ollut merkittävä tekijä IPv4-protokollan eliniän pidentämisessä. NAT mahdollistaa yksityisen, sisäverkon IP-osoitteen piilottamisen julkisen, internetissä käytettävän osoitteen taakse. NAT-tekniikasta riippuen yhteen ulkoverkon osoitteeseen voidaan sitoa yksi tai useampia sisäverkon osoitteita. NAT kehitettiin alun perin lähinnä eri verkkojen välillä liikkumiseen, mutta IPv4-osoitteiden vähentyessä se on tullut tunnetuksi parhaiten juuri sisäverkon IP-osoitteiden kätkijänä.

Tyypillisesti NAT asetetaan internet-rajapinnan tuntumaan, esimerkiksi reunareitittimeen tai palomuuriin. NAT toimii samalla verkkokerroksella kuten reitittimetkin. Yksityiset sisäverkon osoitteet muutetaan NAT-laitteessa julkisiksi liikennöitäessä internetiin. Laite merkitsee tietokantaansa muunnetun osoitteen, johon se lähettää datapaketit saadessaan vastauksen, näin tehden osoitteenmuunnoksen toiseen suuntaan. Sisäverkon topologia pysyy ulkomaailmalle näkymättömänä. NAT-tekniikkaa voidaan soveltaa monin eri tavoin, esimerkiksi staattinen NAT muuntaa tietyn osoitteen aina samaan osoitteeseen, kun taas dynaaminen NAT valitsee ennalta säädetystä osoiteavaruudesta. Jälkimmäisen yleinen variaatio on NAT overload, eli PAT (Port Address Translation), joka voi jaella saman julkisen osoitteen usealle

yksityiselle osoitteelle lisäämällä perään tiedon lähdeportista. (Comer 2002, 394 - 397.)

NAT on ollut hyödyllinen työkalu IPv4-osoitteiden säännöstelyssä, mutta se tuo mukanaan myös ongelmia. Verkon tehokkaan toiminnan ja yleisen suorituskyvyn kannalta jokainen NAT-käännös syö omalta osaltaan verkkoresursseja. Portti- ja osoitemuunnosten lisäksi se joutuu tekemään IPv4-protokollan vaatimia laskutoimituksia, päivittämään tietokantaa sekä julkisen että yksityisen puolen osoitteista ja pitämään kirjaa yhteyksien sen hetkisistä tiloista. Mitä monimutkaisemmaksi verkon solmujen väliset yhteydet muodostuvat, sitä suurempaa kapasiteettia vaaditaan. NAT-laitteen pitää käytännössä ymmärtää kaikkien ohjelmistojen protokollia, joiden liikenne kulkee sen kautta (Blanchet 2007, 6-7). Kapasiteettia tarvitaan aina vain lisää, kun laitteet, yhteyksien määrä ja internet-kaistan nopeus kasvaa. Toisena merkittävänä ongelmana osoitteenmuunnokset yhteysvälillä sotivat ideaalisen, suoran päästä-päähän yhteyden ajatusta vastaan, joka on IPv6-maailman yksi kulmakiviä.

3 IPV6-PROTOKOLLA LYHYESTI

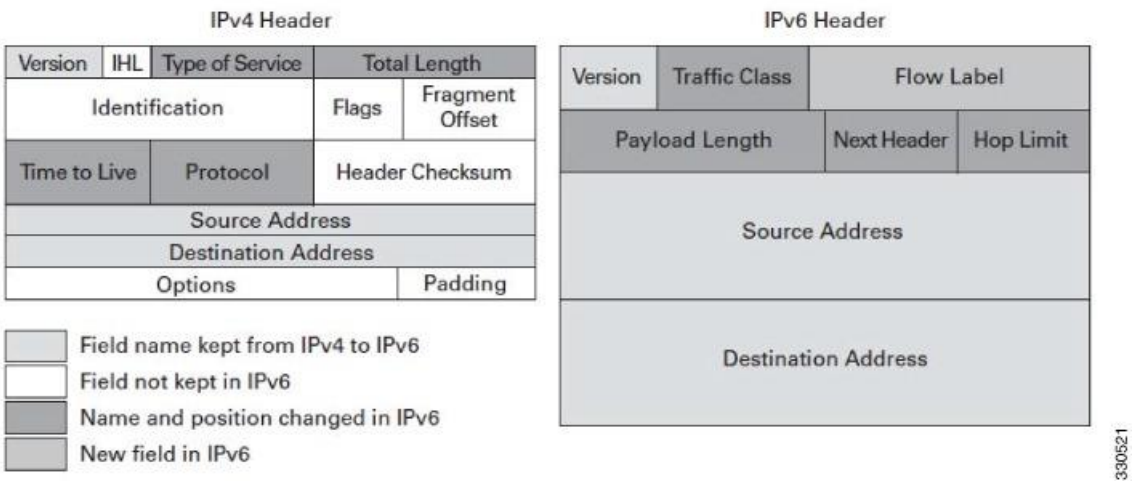
Internetin edeltäjä on ARPANET (Advanced Research Projects Agency Network), Yhdysvaltojen puolustusministeriön hanke, jonka tarkoitus oli luoda pakettikytkentäinen verkko vuonna 1969. Verkon laajantuessa ympäri maailmaa ja sen siirtyessä puhtaasta tutkimuskäytöstä myös kaupallisiin tarkoituksiin alettiin puhua internetistä. Internetin nopea kasvu ja muun kuin tekstityyppisen datan lisääntyminen osoitti nopeasti IPv4-protokollan rajallisuuden. (Kessler 1997.)

Vanhan järjestelmän heikkouksia korjatakseen Internet Engineering Task Force (IETF) kehitti uuden, alunperin IPng:nä (next generation) tunnetun, sittemmin IPv6:ksi nimetyn protokolla- ja standardikokoelman. Se sisältää paljon korjauksia ja uudistuksia aiempaan IPv4-protokollaan verrattuna. Protokollat eivät ole suoraan yhteensopivia, vaan vaativat erityisiä siirtymätekniikoita voidakseen kommunikoida keskenään. IPv6 suunniteltiin vaikuttamaan vain minimaalisesti ylemmän ja alemman tason kerrosten protokolliin. (Davies 2012, 2.)

3.1 IPv6 ominaisuudet

3.1.1 Uudenlainen header eli otsikko

IPv6-otsikon uusi formaatti on virtaviivaistettu IPv4:n vastaavasta, minkä tarkoituksena on vähentää sen aiheuttamaa prosessointia. Näin tiedon käsittely nopeutuu ja resurssien kulutus vähenee. Monet vähälle käytölle jääneet IPv4-otsikon kentät ovat kokonaan poistettu ja muut vaihtoehtoiset kentät on siirretty otsikon jälkeen (kuva 1). Monet lisätoiminnot, kuten esimerkiksi paketin eheyden tarkistaminen, jäävät loppupään laitteiden vastuulle. Tämä tekee reitittimien työstä nopeampaa. Myös protokollan jatkokehittäminen ja laajentaminen helpottuu, kun paketin pääotsikko pysyy ennallaan ja muutokset tehdään erillisten laajennusotsikoiden avulla, jotka sijoitetaan verkko- ja kuljetuskerrosten otsikoiden väliin. Näin IPv6 voidaan päivittää tarpeen mukaan lisäominaisuuksilla muuttamatta sen otsikon standardia. (RFC2460 Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998.)



Kuva 1. IPv4 ja IPv6 otsikot (Cisco 2013)

Koska IPv6-otsikko ja IPv4-otsikko ovat hyvin erilaisia, ne eivät voi kommunikoida suoraan keskenään. Toisin sanoen IPv6 ei ole taaksepäin yhteensopiva. Isäntäkoneen tai reitittimen tulee käyttää siirtymätekniikoita. Optimoidun sisältönsä ansiosta uusi IPv6-otsikko on vain kaksi kertaa IPv4-otsikon kokoinen, vaikka sen sisältämät osoitteet ovat neljä kertaa suurempia bittikooltaan. (Davies 2012, 6.)

3.1.2 Suuri osoiteavaruus

IPv6 käyttää osoitteidensa esittämiseen 128 bittiä, mikä nostaa osoitteiden määrän IPv4:n noin 4,3 miljardista aina 3,4x10^38 osoitteeseen. Valmiiksi suuri määrä on myös suunniteltu tukemaan useita kerroksia aliverkkoja, joita merkitään erityisillä IPv6-prefixeillä (Davies 2012, 60). Osoitteiden lukumäärä epäilemättä riittää kauas tulevaisuuteen, eikä NAT ole enää välttämätön.

3.1.3 Automatisoitu osoitteiden hallinta

Verkkoliikenteeseen vaadittavia osoitetietoja IPv4-verkoissa jakelee tyypillisesti siihen tarkoitukseen konfiguroitu DHCP-palvelin. Vastaavaa toiminnallisuutta IPv6-verkoissa toteuttaa DHCPv6, joka on edelleen tarpeellinen esimerkiksi palveluntarjoajan verkoissa. On kuitenkin mahdollista käyttää myös tilatonta automaattikonfigurointia (Stateless Address Autoconfiguraton, SLAAC), jonka avulla määritellään niin sanottu link-local-osoite automaattisesti IPv6-verkkolaitteen liittyessä verkkoon. Tilatonta ja tilallista konfigurointia voidaan käyttää samanaikaisesti. Esimerkiksi DNS-osoite (Domain Name System), jolla yhdistetään selaimeen kirjoitettava verkko-osoite sitä vastaavaan IP-osoitteeseen, voidaan jaella DHCPv6-palvelimella, vaikka muut tiedot tulevat SLAAC-toiminnon kautta.

SLAAC:in toiminta perustuu IPv6:n uuteen Neighbor Discovery -protokollaan (NDP), jonka avulla löydetään muita lähiverkon laitteita. Paitsi osoitetietojen löytämisen, se myös hoitaa esimerkiksi muiden verkon laitteiden tilan tai mahdollisten osoiteristiriitojen tarkistuksen. Link-local osoitteen avulla kukin verkkolaite, tai solmu, voi tehdä erillisen reititinkyselyn, jonka avulla se saa selville muiden lähireitittimien osoitteet ja muut tarvittavat parametrit verkkoliikennettä varten. (Davies 2012, 7, 205; RFC4862 IPv6 Stateless Address Autoconfiguration. S. Thomson, T. Narten, T. Jinmei. September 2007.)

3.1.4 Tietoturva

IPsec luotiin yhdessä IPv6-protokollan kanssa tuomaan parempaa suojausta vanhaan ARPANETin aikaiseen ratkaisuun. Sitä tukevat IPv6-otsakkeen laajennukset AH (Authentication Header) ja ESP (Encapsulating Security Payload), joilla salataan datapaketin sisältö ja varmistetaan sen eheys. IPsec-otsikoiden tukeminen ei varsinaisesti tee datan lähetyksestä turvallisempaa, vaan pikemminkin tuo sen mahdollistavat ominaisuudet integroidusti

saataville, toisin kuin IPv4:ssä johon IPsec piti sovittaa jälkikäteen. NAT:in poistuminen IPv6-verkoista mahdollistaa vertaisverkon, eli niin sanotun päästä–päähän-yhteyden salaamisen koko matkalta. IPseciä käytetäänkin usein VPN-etäverkkoyhteyksien (Virtual Private Network) salaamiseen. (Davies 2012, 7, 15.)

3.1.5 Tehokkaampi reititys

IPv6 sisältää monia uudistuksia, jotka nopeuttavat pakettien prosessointia. Jo mainittu yksinkertaistettu otsikkomalli sisältää Flow Label -kentän, jolla yhdistetään tietyn lähteen tiettyyn kohteeseen lähettämiä paketteja niin sanotusti yhdeksi virraksi. Koska dataliikenne tunnistetaan paketin otsikosta, voidaan varsinainen tieto salata ja silti käyttää QoS-prioriteettia, mikä ei ollut mahdollista IPv4-paketeilla. (Davies 2012, 7.)

IPv6 myös korvaa kaikki Broadcast-osoitteet Multicast-osoitteilla. Tämä tarkoittaa, että paketteja ei lähetetä kaikille verkon koneille, vaan ainoastaan ennalta määritellylle multicast-ryhmälle. Verkon kuormitus vähenee, kun dataa ei enää kulje turhaan verkoille, joille sitä ei ollut tarkoitus lähettää. (Davies 2012, 70.)

3.2 IPv6 siirtymätekniikat

Koska IPv6 ei ole taaksepäin yhteensopiva, ei suora yhteys sen ja IPv4:n välillä ole mahdollinen. Käytännössä IPv6 suunniteltiin toimimaan siirtymävaiheen ajaksi rinnakkain IPv4:n kanssa. Tämä rinnakkaiselo tulee todennäköisesti jatkumaan vielä vuosia, varsinkin sillä palveluntarjoajien näkökulmasta loppukäyttäjälle lähes näkymätön siirtymä ei tuo välitöntä rahallista vastetta. Ennen kuin puhtaasti IPv6-pohjainen verkko saavutetaan, käytetään eri protokollien väliseen kommunikointiin erityisiä siirtymätekniikoita.

3.2.1 Dual Stack

Dual Stack eli kaksoispino tarkoittaa nimensä mukaisesti, että verkkolaite ajaa sekä IPv4- että IPv6-protokollapinoa samanaikaisesti. Tämä tarkoittaa, että molempia protokollia käyttävät järjestelmät ovat täysin tuettuja. Dual Stack on yksinkertainen tapa siirtyä vähitellen IPv6-verkkoon hylkäämättä heti vanhaa protokollaa.

Ratkaisun heikkoutena kahden protokollan rinnaikkaiselo vaatii myös enemmän resursseja verkkolaitteilta, sillä ne joutuvat pitämään kirjaa molempien tiedoista. Myös verkon ylläpidolliset prosessit, kuten verkon tilan tarkkailu, dokumentointi ja vianhallinta monimutkaistuvat, kun niissä pitää ottaa huomioon molempien protokollien vaatimukset. On myös huomioitavaa, että verkossa toimivan DNS-palvelimen tulee olla IPv6 yhteensopiva. (Blanchet 2007, 277-278.)

3.2.2 Tunnelointi

Kun ei ole mahdollista käyttää kaksoispinoa kaikissa verkon solmuissa esimerkiksi laitteiston rajoitusten takia, minkä johdosta verkkoon muodostuu toisistaan erotettuja IPv6-saarekkeita, voidaan käyttää tunnelointia. Tässä ratkaisussa IPv6-paketit kapseloidaan IPv4-pakettien sisään niin, että siirtotiellä olevat IPv4-laitteet käsittelevät paketin puhtaasti IPv4-otsikon perusteella. Kapselointi puretaan päätepisteessä, joka voi olla vastaanottava palvelin tai vaikkapa reunareititin. Tyypillinen esimerkki tunneloinnista on yrityksen eristyksiin joutuneiden IPv6-verkkojen yhdistäminen, samaan tapaan kuin VPN-etäverkoissa yhdistetään eri toimipisteiden sisäverkkoja internetin yli. Tunneloivat laitteet voivat olla joko reitittimiä tai päätelaitteita, joissa kaksoispino on käytössä. (Blanchet 2007, 278 - 279.)

IPv6-tunnelointi voidaan toteuttaa manuaalisesti, mutta tarjolla on myös useita automaattisia ratkaisuja. Tarkoitukseen parhaiten sopiva tunnelointimetodi riippuu siitä, millaisten laitteiden välillä ja minkä tyyppisellä siirtovälillä liikkennöidään, ja onko NAT käytössä kyseisellä siirtovälillä. 6to4 on tyypillisesti käytössä tapauksissa, joissa liikennöidään internetin yli. Se hyödyntää Dual Stack -reunareitittimen julkista IPv4-osoitetta. ISATAP on vastaava teknologia intranetiin eli sisäverkkoon. 6to4 ja ISATAP eivät toimi NAT:in läpi, eivätkä useat reititysprotokollat toimi niiden kanssa, koska ne eivät tue multicastia. Kun halutaan tunneloida IPv6-liikennettä IPv4 NAT-laitteiden läpi, käytetäänkin Teredo-tunnelointia, joka kapseloi datan UDP-viestinä. Teredo on raskaampi tunnelointiratkaisu kuin 6to4, mutta usein myös käytännöllisempi NAT-pohjaisten verkkojen yleisyyden takia. (Davies 2012, 295, 301, 323, 347.)

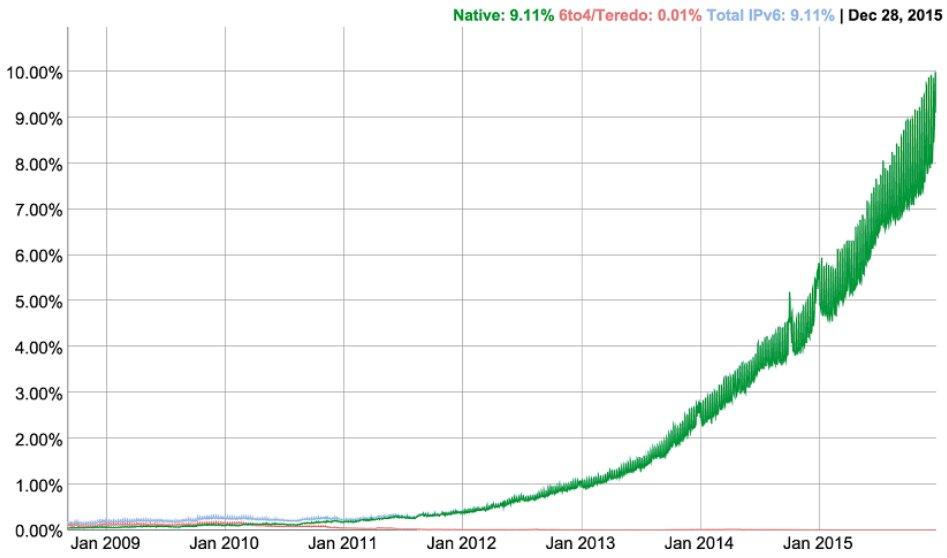
3.2.3 NAT64

NAT64 on siirtymätekniikka, joka vastaa IPv4-verkkojen osoitteenmuunnosta. Erotuksena aiempaan versioon NAT64 myös vaihtaa protokollaa, muuntaen IPv6-osoitteet IPv4-osoitteiksi. Tyypillisesti osoitteenmuunnos on käytössä verkkojen välillä yhdyskäytävänä toimivassa reitittimessä. NAT64 on suunniteltu nimenomaan IPv6-laitteesta IPv4-verkkoon suuntautuvalle liikenteelle. Tilallisesti konfiguroituna yhdessä DNS64-palvelimen kanssa se toimii tekemättä muutoksia yhteyden aloittavaan IPv6-laitteeseen tai kohteena olevaan IPv4-palvelimeen. Tilallinen NAT64 vaatii laitetehoja pitääkseen kirjaa yhteyksien tiloista, mutta se mahdollistaa myös useiden IPv6-lähdeosoitteiden kääntämiseen yhteen julkiseen IPv4-osoitteeseen. Osoitteenmuunnoksen avulla puhtaasti IPv6-pohjaiset verkkolaitteet pääsevät käsiksi IPv4 internetiin ilman Dual Stack asennusta. (RFC6146 Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. M. Bagnulo, P. Matthews, I. van Beijnum. April 2011.)

4 IPV6-SIIRTYMÄ JA SEN VAIKEUDET

IPv6-protokollan uudistukset ja parannukset tarjoavat monia hyviä syitä sen suosimiseen IPv4:n sijaan. Ilmeisin korjaus on osoiteavaruuden laajennus, joka on entistä tärkeämpää mobiililaitteiden määrän kasvaessa huikeaa tahtia, sekä etäohjattavan elektroniikan yleistyessä niin sanotussa esineiden internetissä (Internet of Things, IoT). IPv6-protokolla tarjoaa tehokkaampaa ja turvallisempaa, aidosti päästä–päähän-tiedonsiirtoa, ja siinä on sisäänrakennettu tuki salaukselle ja verkoista toiseen siirtymiselle. Se ei tuki verkkoa broadcast-lähetyksiin, vaan korvaa ne järkevämmillä multicasteilla.

Kaikista hyödyistä huolimatta siirtyminen IPv6-protokollaan on ollut hidasta. 20 vuotta julkaisunsa jälkeen se saavutti viimein 10 % käyttöönoton Googlen mittausten mukaan (kuva 2). Rajapyykki on merkittävä ja kasvu aiempia vuosia parempaa, mutta kehitys on ollut selvästi odotettua verkkaisempaa. Alla tarkastellaan joitakin pitkäksi venyneen siirtymäkauden todennäköisiä aiheuttajia.



Kuva 2. IPv6 maailmanlaajuinen käyttöönotto tammikuu (Google 2016)

4.1 Taloudelliset syyt

Ehkä ilmeisin hidaste minkä tahansa uuden teknologian tai menettelytavan käyttöönotolle on raha. IPv6:n omaksuminen pitää perustella käyttäjä- tai yrityiskohtaisesti liiketoiminnan kannalta, ja sen omaksuminen vaatii paitsi laitteistoa myös henkilökuntaa ja osaamista. Verkkoratkaisun uudistaminen edellyttää suunnittelutyötä, ei vain itse IPv6-verkon vaan myös IPv4-laitteiden kanssa yhteistoiminnan kannalta, puhumattakaan verkon ylläpidosta ja varsinaisesta asennustyöstä. Kaikki vaadittava laitteisto, ohjelmisto, henkilöstö ja tietenkin aika vaativat merkittävää investointia.

IPv6-kehityksen kannalta ongelmallista on ollut, ettei yrityksillä ole juurikaan ollut painavia syitä uuden protokollan käyttöönottoon. Siirtyminen ei ole tuonut välitöntä rahallista vastinetta, varsinkaan jos mahdolliset muut investoinnit ovat ajaneet sen edelle, eli raha on mennyt muihin projekteihin uuden tekniikan sijaan. Vasta viime vuosina asiakaskunnan ja internetin palvelujen hitaasti mutta varmasti siirtyessä IPv6:n käyttöön on yritystenkin ollut ajankohtaisempaa investoida siihen.

Edes IPv4-osoitteiden loppuminen ei ole ollut ehkä niin kriittistä kuin ennustettiin. Päinvastoin ISP:t ja operaattorit myös hyötyvät, sillä ne voivat pyytää korkeampaa hintaa kuluttajilta harvinaisista, kiinteistä osoitteista. On myös huomioitavaa, että vaikka IANA on jaellut suurimman osan osoitteista palveluntarjoajille, ei se tarkoita että ne olisivat vielä kaikki käytössä. Jos

verkon käyttäjäkunnan koko on suunnilleen vakio, kierrätetään vanhat osoitteet poistuvilta asiakkailta uusille, toisin sanoen ongelmia syntyy lähinnä kasvavissa verkoissa. Operaattorit voivat myös ostaa osoitteistoja toisiltaan, tosin tämä on tarkasti RIR-organisaatioiden kuten RIPE ja ARIN säätelemää (Arin 2016).

4.2 Tekniset syyt

Yksi suuri hidaste IPv4-verkoista pois siirtymiselle on IPv4-protokolla itse. Koska IPv6 ei ole taaksepäin yhteensopiva, tai pikemminkin IPv4:ää ei suunniteltu eteenpäin yhteensopivaksi, on vähän kerrallaan uuteen protokollaan siirtyminen hyvin hankalaa. Ongelmana on IPv4:n kankea kehysrakenne, jolle jo yhden bitin lisääminen osoitteisiin olisi taannut taaksepäin yhteensopimattomuuden. Alun perin IPv4:n korvaajaksi suunniteltiinkin pituudeltaan vaihtelevia osoitteita tukevaa CLNP-tekniikkaa. Se kuitenkin jäi IETF:n ajaman TCP/IP-ratkaisun jalkoihin, todennäköisesti ei vähiten kustannussyistä. Sama kohtalo oli OSI-mallilla, jota kuitenkin käytetään laajalti opetuskäytössä. (Van Beijnum 2016.)

Koska kaikkia vanhempia niin sanottuja legacy-laitteita tuskin päivitetään koskaan, hidastaa niiden vaatima tuki IPv6-verkkojen kehitystä, eikä täysin puhtaalta pöydältä aloittaminen verkkojen laajuuden vuoksi ole enää mielekästä. Tilanne on toinen kuin edellisen siirtymäkauden aikana, jolloin Arpanetin vanha NCP-protokolla vaihtui IPv4:ään internetin kasvun myötä, eikä laitteita ollut kuin satoja. Huomioitavaa on, että siihenkin prosessiin kului vuosi (Van Beijnum 2010). IPv4-verkoista ei käytännössä voida luopua niin kauan, kun IPv6 ei ole kaikkien saatavilla. Edellisessä kappaleessa mainitut taloudelliset syyt yhdessä teknisten hidasteiden kanssa ovat saaneet monet laitteistovalmistajat ja palveluntarjoajat odottamaan uuden protokollan laajempaa levikkiä.

IP-protokollan muutoksesta tekee osaltaan työlästä, että toisin kuin esimerkiksi sovelluskerroksen protokollat, joiden muutokset eivät vaikuta itse kuljetusväliin, IP täytyy olla tuettu jokaisessa laitteessa päästä päähän. Toisin sanoen kaikkien laitevalmistajien, liitäntäverkkojen, ohjelmistojen, sisällöntuottajien ja reunalaitteiden pitää tukea IPv6-protokollaa, jotta tiedonsiirto on mahdollista. Historiallisesti ongelmana on ollut myös osittainen tuki joillekin jälkikäteen implementoiduille IPv6-tekniikoille. Esimerkiksi

Windows XP ei tue DHCPv6-tekniikkaa, vain autokonfigurointia. Tämä ei ole enää ongelma myöhemmissä Windowsin versioissa (Davies 2012, 216).

4.3 Käytännönläheiset syyt

Puhtaasti rahallisten ja teknisten syiden rinnalta löytynee, jos ei aivan yhtä merkittävänä niin ainakin vaikuttavana tekijänä, ihmisten yleinen muutoksenhaluttomuus. Varsinkin peruskäyttäjän kohdalla ilmeisten hyötyjen puute on mahdollinen osasyy apatiaan IPv6-protokollaa kohtaan. Yritykset eivät ole välttämättä katsoneet IPv6:n käyttöönottoa mielekkääksi, jos ISP ei ole sitä vielä tukenut, eikä ISP ole sitä tehnyt edellä mainittujen taloudellisten ja teknisten syiden vuoksi. IPv6 ei yksinkertaisesti ole tarjonnut tarpeeksi polttavia syitä sen omaksumiseen, ei ainakaan samalla tavalla kuin IPv4 aikoinaan, joka oli käytännössä pakollinen jos halusit käyttää internetiä. IPv6-osoitteet eivät myöskään ole yhtä helposti ymmärrettävissä kuin edeltäjänsä, vaikka toki uusi tekniikka vaatii aina opettelua.

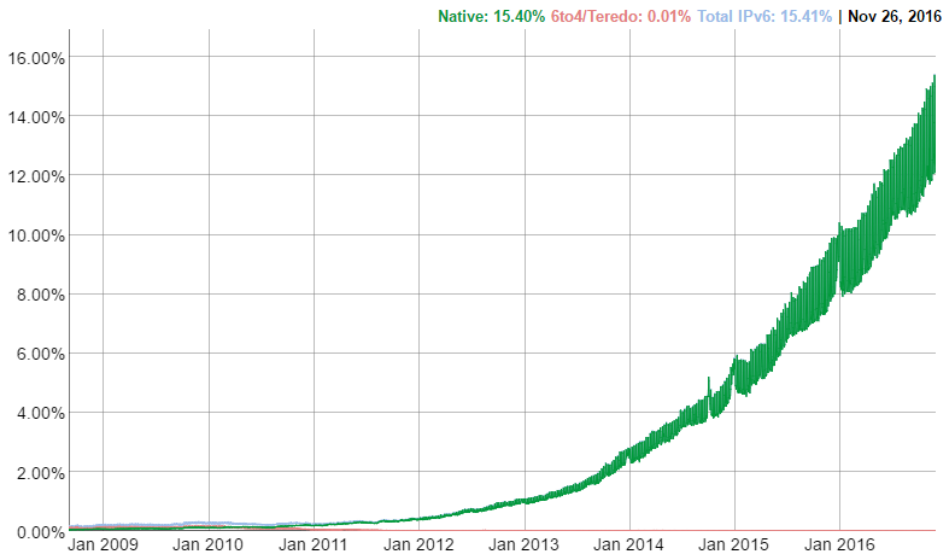
NAT on omalta osaltaan juurruttanut IPv4-ajattelun osaksi nykyistä internetiä, minkä takia kaikki konservatiivisemmat järjestelmänvalvojat eivät ole yhtä vakuuttuneita IPv6:n välttämättömyydestä. Jopa erillistä IPv6 NAT-ratkaisua on harkittu (Van Beijnum 2010). NAT on arvostettu osoitteenmuunnoksen ohella sen antamasta ylimääräisestä tietoturvasta, sillä se kätkee sisäverkon rakenteen ulkomaailmalta, mutta suorat päästä–päähän-yhteydetkin voidaan turvata oikeaoppisesti konfiguroiduilla palomuureilla ja pääsylistoilla.

IPv6-prokollan laajeneminen on laahannut suoran taloudellisen tai suoritustehollisen hyödyn puutteessa, minkä takia se on odottanut pitkään läpimurtoa kaukaa viisaiden yritysten ja innokkaiden harrastajien tukemana. Koska IPv4-osoitteiden loppumisesta on tiedetty jo pitkään, on syy hitaalle kehitykselle todennäköisemmin IANA:n, IETF:n ja muiden organisaatioiden kyvyttömyydessä vakuuttaa uuden protokollan muista eduista.

5 IPV6-PROTOKOLLAN TILANNE JA TULEVAISUUS

2011 kesällä Internet Society, tukenaan satoja eri sisällöntarjoajia ja verkkoalan yrityksiä, järjesti World IPv6 Day -tapahtuman tarkoituksenaan testata IPv6-verkkojen toimintaa. Vuotta myöhemmin järjestetty World IPv6 Launch Day ei ollut enää vain kokeilua, vaan osallistuneet yritykset ottivat pysyvästi uuden protokollan käyttöön palveluissaan. Nyt neljä vuotta tuon

tapahtuman jälkeen alkavat vaikutukset viimein näkymään konkreettisesti, osoituksena siitä tämän vuoden IPv6 käyttöönottoasteen nousu alkuvuoden kymmenestä prosentista loppuvuoden viiteentoista prosenttiin (kuva 3). Internet-palveluiden kuten Googlen, Youtuben, Facebookin ja muiden suosittujen sisällöntarjoajien näyttäessä tietä ja käyttäjäkunnan hitaasti mutta varmasti kasvaessa, on viimein saavutettu kriittinen piste, jossa yritysten on mielekästä käyttää Dual Stack -ratkaisuja tai jopa puhtaasti IPv6-verkkoja. Operaattorien muutossuuntausta on lisäksi ajanut mobiiliverkkojen raju kasvu (Laitila 2015).



Kuva 3. IPv6 maailmanlaajuinen käyttöönotto marraskuu (Google 2016)

”Miksei vieläkään IPv6?” onkin oikeastaan tässä vaiheessa harhaanjohtava kysymys, sillä IPv6-siirtymä on tavallaan tapahtunut kulissien takana. Käyttäjän kannalta se halutaan mahdollisimman näkymättömänä ja saumattomana pitääkin (Laitila 2015). Kaikkien käyttöjärjestelmien ollessa käytännössä nykyään tilanteen tasalla, IoT-laitteiden yleistyessä, ja monien verkkopalvelujen hyötyessä yhä enemmän yksinkertaistetuista, suorista yhteyksistä kuluttajiin, oikeasti IPv6-pohjainen internet alkaa viimein tuntua uskottavalta ajatukselta. Esimerkiksi vaikkapa verkossa pelattavat videopelit, jotka usein perustuvat vertaisverkkoratkaisuihin kiinteiden palvelimien sijaan, hyötyvät NAT-laitteiden poistumisesta. Yleistyneet VPN-palvelut puolestaan käyttänevät suuren IPv6-osoitealueen hyödykseen (Lehto, 2016). IPv6 alkaa olla hyödyllinen niin yrityksille kuin peruskäyttäjille.

Globaalilla tasolla IPv6-koneiden levinneisyys on hyvin vaihtelevaa, suuri osa käyttäjistä on USA:ssa ja Euroopassa. IPv6-protokollaan siirtyminen, vaikka aina vain ajankohtaisempana, on yhä suuri investointi ja kehitystekninen haaste yrityksille ja palveluntarjoajille. IPv4 tuleekin todennäköisesti vaikuttamaan verkoissa vielä vuosia, 2016 alkuvuoden tahdilla kestää vähintäänkin vuoden 2020 kesään asti, ennen kuin IPv6 on kaikkien ulottuvilla. Historiallisesti siirtymän hidasteina olleet syyt menettävät kuitenkin jatkuvasti painoarvoaan saatavuuden ja ohjelmistojen yhteensopivuuden kasvaessa käyttäjämäärän kanssa. Siinä missä kukaan ei varhaisina kehitysvaiheina halunnut olla ensimmäinen, ei kukaan myöskään pyörän toden teolla pyörähdettyä liikkeelle halua olla viimeinen.

LÄHTEET

Arin, 2016. TRANSFER RESOURCES. Saatavilla: https://www.arin.net/resources/transfers/index.html [viitattu 2.12.2016].

Blanchet, M. 2007. Migrating to IPv6. John Wiley & Sons Ltd.

Cisco 2013. Routing and Bridging Guide vA5(1.0): Overview of IPv6. Saatavissa: http://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/configuration/rtg_brdg/guide/rtbrgdgd/ipv6.html [viitattu 29.11.2016].

Comer, D. 2002. TCP/IP. Jyväskylä: Gummerus.

Darrow, B. 2015. This time it's true: We're out of IPv4 addresses. Saatavilla: http://fortune.com/2015/09/24/we-are-out-of-ipv4-addresses/ [viitattu 29.11.2016].

Davies, J. 2012. Understanding IPv6. California: O'Reilly Media Inc, Microsoft.

Kessler, G. 1997. IPv6: The Next Generation Internet Protocol. Saatavissa: http://www.garykessler.net/library/ipv6_exp.html [viitattu 29.11.2016].

Laitila, T. MikroPC 18.6.2015 s.6 Nettiyhteydet nytkähtivät nykyaikaisemmiksi.

Lehto, T. Tekniikka&Talous 11.3.2016 s.28 Internet rikkoo sopimusrajat.

RFC2460 Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998. Saatavilla: tools.ietf.org/html/rfc2460 [viitattu 29.11.2016].

RFC4862 IPv6 Stateless Address Autoconfiguration. S. Thomson, T. Narten, T. Jinmei. September 2007. Saatavilla: tools.ietf.org/html/rfc4862 [viitattu 29.11.2016].

RFC6146 Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. M. Bagnulo, P. Matthews, I. van Beijnum. April 2011. Saatavilla: https://tools.ietf.org/html/rfc6146 [viitattu 2.12.2016].

Tivi, 2016. IPv6 juhlii merkkipäiväänsä - ja tärkeää merkkipaalua. Saatavilla: http://www.tivi.fi/Kaikki_uutiset/ipv6-juhlii-merkkipaivaansa-ja-tarkeaa-merkkipaalua-6242754 [viitattu 29.11.2016].

Van Beijnum, I. 2010. There is no Plan B: why the IPv4-to-IPv6 transition will be ugly. Saatavilla:http://arstechnica.com/business/2010/09/there-is-no-plan-b-why-the-ipv4-to-ipv6-transition-will-be-ugly/ [viitattu 2.12.2016].

Van Beijnum, I. 2016. IPv6 celebrates its 20th birthday. Saatavilla: http://arstechnica.com/business/2016/01/ipv6-celebrates-its-20th-birthday-by-reaching-10-percent-deployment/ [viitattu 29.11.2016].

Vänskä, O. 2012. Nyt se sitten kävi: ipv4-osoitteet loppuivat koko Euroopasta. Saatavilla: http://www.tivi.fi/Uutiset/2012-09-17/Nyt-se-sitten-k%C3%A4vi-ipv4-osoitteet-loppuivat-koko-Euroopasta-3194616.html [viitattu 29.11.2016].