TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

IIRO KAISLA

TIETOTURVALLISUUS JA PALOMUURAUS IPV6-PROTOKOLLAN SIIRTYMÄVAIHEESSA

Diplomityö

Tarkastaja: Marko Helenius
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan tiedekunta-
neuvoston kokouksessa 02.05.2018

TIIVISTELMÄ

Iiro Kaisla: Tietoturvallisuus ja palomuuraus IPv6-protokollan siirtymävaiheessa
Tampereen teknillinen yliopisto
Diplomityö, 47 sivua
Marraskuu 2018
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tietoliikennetekniikka
Tarkastaja: Marko Helenius

Avainsanat: IPv6, IPv4, palomuuri, tietoturva, siirtymävaihe, siirtymätekniikka

Tässä työssä käydään läpi IPv6-protokollaan siirtymistä, ja miten tässä prosessissa pitää ottaa huomioon tietoturva ja palomuuraus. IPv6-siirtymässä käytetään erilaisia menetelmiä ja tekniikoita, jotta kaikkien palveluiden saatavuus on taattu molemmilla IP-protokollan versioilla. Tämä toteutetaan erilaisilla tunneleilla ja protokollan muutoksilla, joihin liittyy tietysti omat haasteensa ja ongelmansa, kuten haasteet näiden menetelmien palomuuraukselle.

Tietoturva ja palomuuraus ovat myös asioita, jotka tarvitsee ottaa huomioon IPv6:een siirryttäessä. Miten IPv6-palomuuri eroaa IPv4-muurista? Entä millaisia IPv6-hyökkäyksiä on olemassa? Työ vastaa muun muassa näihin kysymyksiin. IPv6 tuottaa myös tietoturvauhkia IPv4-verkoille ja -muureille, varsinkin erilaisten tunnelointiratkaisujen vuoksi.

Työssä havaittiin, että IPv6-protokollaan siirtymisessä voi ilmetä paljon ongelmia sekä itse verkon toteutuksessa että verkon tietoturvan ja palomuurauksen toteutuksessa. IPv6:een siirtymisen suunnittelu kannattaakin toteuttaa huolella ja miettiä asioita myös IPv4-verkon sekä sen tietoturvan kannalta.

ABSTRACT

Iiro Kaisla: Information security and firewalling in transition to IPv6
Tampere University of Technology
Master of Science Thesis, 47 pages
November 2018
Master's Degree Programme in Information Technology
Major: Communication Systems and Networks
Examiner: Marko Helenius

Keywords: IPv6, IPv4, firewall, information security, transition period, transition technology

This thesis work reviews transition to IPv6-protocol and how to consider information security and firewalling during this transition. Many different methods and techniques are used in transition to IPv6 to achieve reliable availability of services with both IP-protocol versions. This is achieved by use of different kind of tunnels and protocol translations, which introduce also their own problems and challenges such as firewalling these methods.

Information security and firewalling should also be considered, when you are switching over to use IPv6. How IPv6 firewall differs from IPv4 firewall? What kind of attacks against IPv6 exists? The thesis answers also these questions. Using IPv6 cause security threats also for IPv4 networks, especially when using tunnels.

In this thesis work is noticed, that when transition to IPv6-protocol, many problems can appear in implementation of IPv6 network, it's security and firewalls. That is why planning of the transition should execute carefully and take IPv4 network and it's security also into account.

ALKUSANAT

Haluan kiittää kaikkia työn tekemiseen osallistuneita ja siinä auttaneita henkilöitä. Vaikka kirjoitus prosessissa kesti kauan, silti ihmiset luottivat minuun ja joustivat tarvittaessa. Kiitän työn nykyistä tarkastajaa Marko Heleniusta ja työn aloituksessa mukana ollutta Jarmo Harjua.

Erityiskiitokset kuuluvat vaimolleni Tarulle, joka jaksoi koko tämän pitkän prosessin ajan uskoa ja patistaa minua tekemään työn loppuun. Lopuksi kiitos pojalleni Jooalle, joka minut lopulta patisti työn tekoon ja osallistui välillä neuvovasti työn katselmointiin määrätietoisella vauvan huudollaan.

Espoossa, 11.11.2018

Iiro Kaisla

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

6rd	IPv6 rabid deployment
ARP	Address resolution protocol
BGP	Border gateway protocol
DAD	Duplicate address detection
DAD-DOS	Duplicate address detection denial of service
DHCP	Dynamic host configuration protocol
DHCPv6	DHCP version 6
DMZ	Demilitarized zone
DOS	Denial of service
DS-Lite	Dual stack lite
IANA	Internet Assigned Numbers Authority
ICMPv6	Internet control message protocol version 6
IDS	Intrusion detection system
IPS	Intrusion protection system
IPsec	IP security architecture
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ISATAP	Intra-Site Automatic TuMTUnel Addressing
MAC	Media access control
MLD	Multicast listener discovery
MTU	Maximum transmission unit
NA	Neighbor advertisement
NAT	Network address translation
ND	Neighbor discovery
NGFW	Next-generation firewall
NS	Neighbor solicitation
OSI-malli	Open systems interconnection reference model
OSPF	Open shortest path first
OSPFv3	Open shortest path first version 3
RA	Router advertisement
RIR	Regional internet registry
RS	Router solicitation
SEND	Secure neighbor discovery
SIIT	Stateless IP/ICMP translation
SLAAC	Stateless address autoconfiguration
TCP	Transmission control protocol
TSP	Tunnel setup protocol
UDP	User datagram protocol
ULA	Unique local address

1. JOHDANTO

Internet protocol version 6 (IPv6) on IP version 4:n (IPv4) tilalle kehitetty open systems interconnection reference model (OSI) -mallin siirtokerroksen protokolla, jolla vastataan IPv4-osoiteavaruuden ehtymiseen. Tästä johtuen, lähes jokaiselle internetiä tai muita tietoliikenneverkkoja käyttävälle tulee IPv6-protokolla jossain vaiheessa vastaan, jos ei ole jo tullut tähän mennessä.

Työn tavoitteena oli selvittää IPv6-protokollaan siirtymiseen liittyviä ongelmia. Samalla saataisiin vastaus, miksi protokollan käyttöönotto on vienyt niin kauan aikaa. Työllä haluttiin selvittää tietoturvan ja palomuurin toteutus IPv6:ssa.

Tutkimusongelmaksi työhön muodostui kysymykset: mikä on IPv6-protokollan siirtymävaihe, miten tietoturva sekä palomuurausliittyvät tähän ja mitä tulee ottaa huomioon IPv6-protokollaan siirryttäessä. Näihin vastausta lähdettiin hakemaan tutustumalla aiheisiin liittyviin teoksiin ja tekniikkoihin. Tutkimuksen tueksi rakennettiin testiverkko, jolla saatiin kokeiltua sekä testattua joitakin työssä käsiteltäviä aiheita. Testiverkosta ja yleisestä verkonhallinta kokemuksesta saatiin lisää tietämystä aiheen käsittelyyn.

IPv6:sta on tehty paljon tutkimusta ja erilaisia teoksia. Siihen liittyy myös paljon eri standardeja sekä avustavia protokollia. Siirtymisestä IPv6-protokollaan on myös tehty tutkimusta, kuten esimerkiksi Zamanin ja Zubairn ”Deploying IPv6: Security and Future” [1] tai Arkkon & co:n ”Securing IPv6 Neighbor and Router Discovery” [2]. Ei kuitenkaan löytynyt tutkimuksia, jotka painottaisivat tämän työn näkökantaa eli tietoturvaa ja palomuureja siirtymävaiheessa samalla laajuudella. Työn tulokset osoittavat, että siirtymisessä IPv6-protokollaan kannattaa panostaa tietoturvan ja palomuurin toteutukseen sekä niiden suunnitteluun, sillä mahdollisia ongelmia saattaa tulla useita ja vielä yllättävistä syistä. IPv6:ta vastaan on myös tehty paljon erilaisia hyökkäyksiä, joista osa on aivan IPv6:n perusominaisuuksia vastaan. Myös itse IPv6:n käyttöönotossa on omat vaikeutensa, jotka ovat kuitenkin selvitettävissä.

Työn kannalta oleelliset perustiedot IPv6-protokollan toiminnasta sekä verkon tietoturvasta ja palomuureista käydään läpi toisessa luvussa. Kolmannessa luvussa taasen käydään läpi siirtymävaiheen tekniikoita ja menetelmiä. Luvussa esitellään myös käytetty testiverkko ja käydään tästä sekä yleisesti IPv6-verkoista esiin tulleita seikkoja.

Neljännessä luvussa ovat IPv6-hyökkäykset käsiteltävänä. Esiteltävänä on erilaisia hyökkäyksiä, jotka käyttävät IPv6:n ominaisuuksia tai hyökkäävät näitä vastaan. Luvussa käydään myös mahdollisia suojautumiskeinoja ja estämistapoja kyseisiä hyökkäyksiä vastaan.

Palomuureja käsitellään taasen luvussa viisi. Näitä vertaillaan IPv4:n ja IPv6:n välillä sekä käsitellään testiympäristössä olevien muurien eroja. Kuudennessa luvussa pohditaan IPv6:n tietoturva- ja palomuurausongelmia syvällisemmin ja mietitään, mitä pitää ottaa huomioon IPv6-protokollaan siirryttäessä. Viimeiseksi seitsemännessä luvussa kootaan työn tulokset ja ajatukset yhteenvedoksi.

2. YLEISTÄ TIETOTURVASTA, PALOMUURAUKSESTA JA IPV6:STA

Tässä kappaleessa käydään läpi työnkannalta tärkeitä perustietoja tietoturvasta, palomuurauksesta ja IPv6-protokollasta. Kuinka IPv6-protokolla toimii sekä millaisia palomuureja on olemassa? Mitä verkon tietoturva on ja miksi sitä tarvitaan?

2.1 Yleistä verkon tietoturvasta ja palomuureista

Verkon tietoturvaa ei aina tule miettineeksi. Mutta mitä verkon tietoturva oikeasti on? Tätä voisi lähteä ratkaisemaan siltä kannalta, mitä tapahtuisi ilman verkontietoturvaa. Tällöin hyökkääjät pääsisivät vapaasti valloilleen ja verkon käyttö voisi tuntua turvattomalta sekä pelottavalta. Verkkoon ei uskaltaisi lähettää mitään tietoja tai edes kytkeä laitteita verkkoihin. Voisi myös olla, että verkot olisivat käyttökelvottomia palvelunestohyökkäysten vuoksi ja laitteen kytkeydyttyä verkkoon, sekin lakkaisi toimimasta estohyökkäyksen tai haitallisen ohjelman vuoksi.

Tästä pääsemme lähemmäksi vastausta, mitä verkon tietoturva on. Se voitaisiin määritellä niin, että verkot olisivat luotettavia, sieltä saatu tieto olisi eheää ja se olisi saavutettavissa. Tämä saavutetaan erilaisilla menetelmillä, jotka kokonaisuutena toteuttavat tietoturvallisen verkon. Verkossa olisi pääsynvalvontaa käytössä tiedon saannille sekä käytölle. Organisaation sisäverkkoon ei pääsisi fyysisesti liittymään valtuuttamattomat henkilöt omilla laitteillaan fyysisen pääsynvalvonnan avulla, esimerkiksi toimiston ovet olisivat lukittuja. Pääsynvalvonnan lisäksi tarvitsisi olla käyttäjät todennettuja, jotta he ovat todella henkilöitä joita väittävät ja pääsynvalvonta olisi helpompaa. Nämä saavutetaan pitämällä verkon laitteet ja ohjelmat ajan tasalla sekä käyttämällä uusimpia päivityksiä. Lisäksi käytettäisiin verkkoliikenteen valvontaa ja tämän suodatusta, esimerkiksi palomuurien avulla. Verkon tietoturvassa kannattaa aina varautua pahimpaan ja ajaa verkossa hyökkäyksen tunnistus ja esto -työkaluja.

Tästä päästään palomuureihin: mitä ne ovat ja millaisia niitä on. Palomuuri on vähän niin kuin verkon vartija, sillä se päättää, kuka kulkee muurin ovelta sisään ja kuka ulos tiettyjen sääntöjen perusteella. Palomuuri on yksi tärkeimmistä verkon tietoturvan työkaluista, muttei todellakaan ainut. Palomuurin tehtävänä on suodattaa ja sallia liikennettä niin, että se toimii näkymättömästi verkonkäyttäjille, joilla on oikeus käyttää verkkoa ja sen palveluita. Tämä onnistuu suodattamalla pois kaikki haitallinen ja määrittelemätön liikenne pois sekä jakamalla verkko turvalliseen sisäverkkoon ja turvattomaan internetiin. Näin palomuuri turvaa verkon palvelut ja käyttäjät haitallisilta hyökkäyksiltä sekä mahdollistaa palveluiden saannin estämällä palvelunestohyökkäyksiä.

Tämä olisi ideaali tilanne, jossa yksittäinen palomuuri pystyisi kaikkeen, mutta niitä on eri tasoisia ja toimintatavoiltaan erilaisia. Yksinkertaisin palomuurin tyyppi on pakettisuodatin, joka suodattaa liikennettä vain IP-otsikon ja kuljetuskerroksen otsikoiden perusteella. Hieman kehittyneempi palomuuri toimii tilallisena muurina, joka pakettisuodattimen tapaan suodattaa liikennettä samojen otsikoiden perusteella, mutta se pitää yllä myös tietoa yhteyksien tiloista eli esimerkiksi sallii sisäverkosta lähetetyn paketin vastauksen läpi. Viimeisenä tyyppinä on sovelluskerroksen huomioon ottava muuri eli se pystyy analysoimaan sovelluskerroksen sisältöä ja päättämään tämän perusteella sallitaanko liikenne. [3]

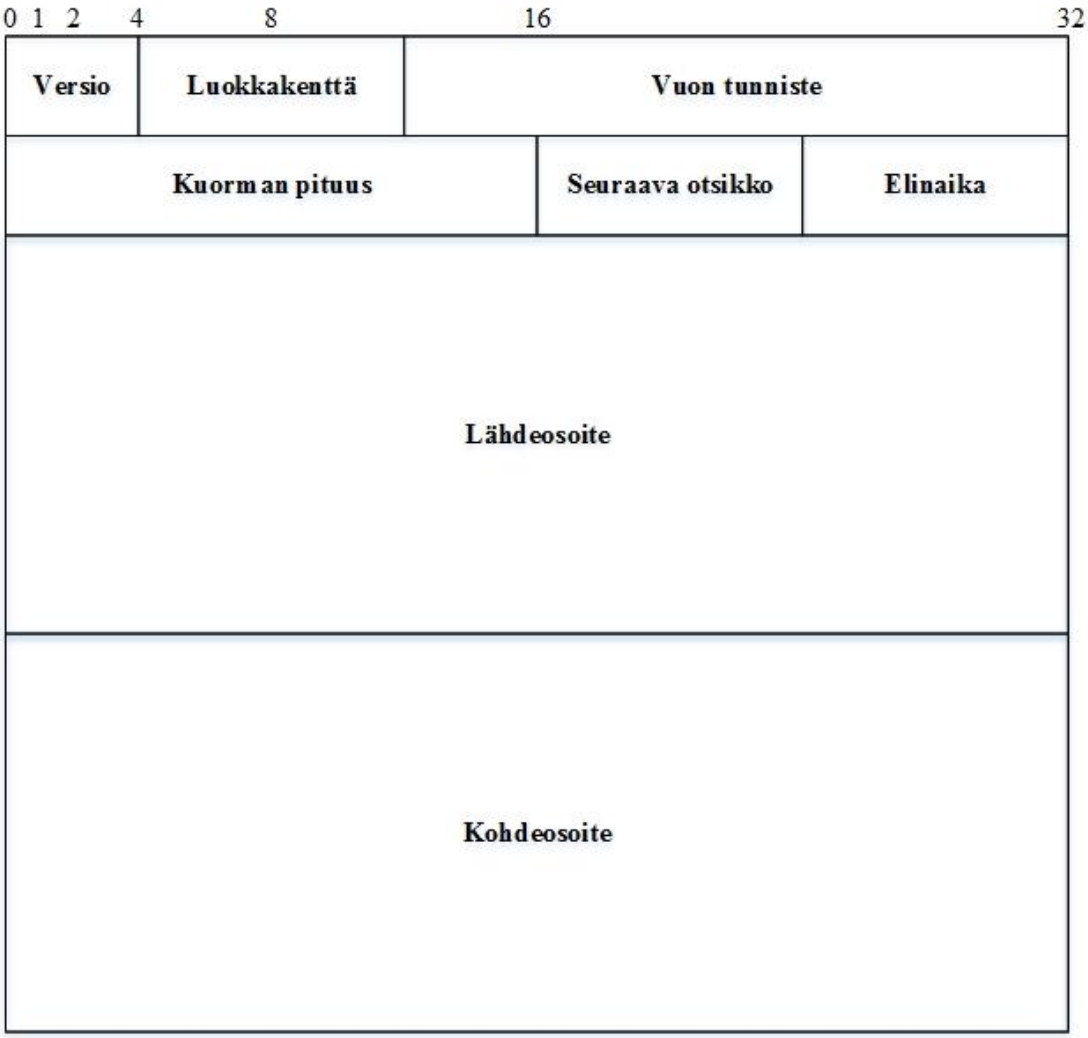
Nykyään monet uudet ja kehittyneimmät palomuurit käyttävät näitä kaikkia tyyppejä yhdessä suodattaakseen ja salliakseen paketteja verkossa. Näissä on usein myös lisää ominaisuuksia kuten hyökkäysten havaitsemis-, torjunta- ja esto-ominaisuuksia. Tällaisia palomuureja kutsutaan usein seuraavan sukupolven palomuureiksi (next-generation firewall, NGFW).

2.2 IPv6:n perustoiminta ja tietoturvaominaisuudet

IPv6-protokolla kehitettiin, koska IPv4-osoitteet alkoivat ehtymään ja tämä piti ratkaista muullakin kuin network address translation (NAT) avulla [4]. IPv6:ssa on isommat 128 bittiä pitkät osoitteet sekä uusi otsikkorakenne. Siihen on sisäänrakennettuna uusia ominaisuuksia, kuten automaattinen osoitteiden autokonfiguraatio ja sisäänrakennettu IP security architecture (IPsec). IPv6 tarvitsee toimiakseen muita tukevia protokollia, kuten Internet control message protocol version 6 (ICMPv6). Termistössä IPv6:ta käyttävää laitetta kutsutaan solmuksi (node) ja IPv6:tta reitittävää laitetta reitittimeksi (router). IPv6-solmulla on yleensä kaksi osoitetta: paikallinen ja globaali, joita se käyttää keskusteluun lähiverkossa ja IPv6-internetin kanssa.

2.2.1 Otsikko

Jokainen IPv6-paketti sisältää otsikko- (header) ja data-osion eli hyötykuorman. Jokaiselle otsikko-osiolle on määrätty pakolliset otsikkotiedot, jotka näkyvät Kuva 1. Pakollisten otsikkotietojen kokonaispituus ja täten IPv6-otsikon vähimmäispituus on 320 bittiä. Tämän lisäksi voi varsinaisen IPv6-otsikon jälkeen tulla valinnaisia lisäotsikoita, joilla saadaan kasvatettua perusotsikon lisäksi paketin ominaisuuksia tarvittaessa.



Kuva 1. *IPv6-otsikon rakenne [5]*

Versio (Version) 4-bit: kertoo mitä Internet protokollan versiota käytetään. Tässä tapauksessa käytetään numeroa kuusi.

Luokkakenttä (Traffic Class) 8-bit: kertoo paketin luokan

Vuon tunniste (Flow Label) 20-bit: kertoo mihin vuohon eli lähetykseen paketti kuuluu. Käytetään lähinnä reaaliaikaisiin lähetyksiin, jotta paketit eivät kulkisi eri reittejä pitkin, vaan jokainen vuon paketti reitittyisivät samalla tavalla, jotta vältyttäisiin pakettien saapuminen väärässä järjestyksessä.

Kuorman pituus (Payload Length) 16-bit: kertoo, kuinka suuri on paketin hyötykuorma tavuina. Hyötykuormaksi lasketaan kaikki tämän otsikon jälkeinen data.

Seuraava otsikko (Next Header) 8-bit: kertoo, seuraavan otsikon tyypin, joka on tässä samassa paketissa. Se voi olla joko mahdollinen lisäotsikko tai ylemmän kerroksen otsikko.

Elinaika (Hop Limit) 8-bit: kertoo, paketin sallimat siirtymät reitittimien välillä. Jokainen reititin vähentää tätä lukua yhdellä ja sen saavuttaessa nollan, tiputetaan se pois liikennöinnistä.

Lähdeosoite (Source Address) 128-bit: ilmoittaa lähettäneen solmun IPv6-osoitteen.

Kohdeosoite (Destination Address) 128-bit: ilmoittaa halutun vastaanottajan IPv6-osoitteen, joka voi olla myös ryhmälähetysosoite.

Tämän lisäksi voi otsikko-osio sisältää lisäotsikoita, jotka ovat: hyppyoptio- (Hop-by-Hop Options), kohdeoptio- (Destination Options), reititys- (Routing (Type 0)), lohkomis- (Fragment), todennus- (Authentication) ja salausotsikko (Encapsulating Security Payload). Nämä tulevat paketin hyötykuormassa ja niin, että aina seuraavan lisäotsikon tyyppi ilmoitetaan edellisessä otsikossa, eli jos paketti sisältää yhdenkin lisäotsikon, ensimmäisen lisäotsikon tyyppi ilmoitetaan perusotsikon seuraava otsikko -kentässä, ja seuraavan lisäotsikon tyyppi ensimmäisen lisäotsikon seuraava otsikko -kentässä ja niin edelleen. [5]

2.2.2 Osoitteen muoto

IPv6-osoite on 128 bittiä pitkä ja se esitetään heksadesimaaleilla kahdeksana neljän numeron ryhmänä, jotka on eroteltuna kaksioispisteillä toisistaan, esimerkiksi 2001:0db8:0000:0000:0000:1337:0000:cafe. Osoitteen esitystä voidaan lyhentää lukemisen helpottamiseksi poistamalla kunkin ryhmän etunollat pois ja peräkkäiset vain nollia sisältävät ryhmät voidaan lyhentää kahdella kaksoispisteellä yhdessä kohtaa osoitetta. Edellä oleva esimerkkiosoite muuntuu tällä säännöllä aluksi muotoon 2001:db8:0:0:0:1337:0:cafe ja edelleen poistamalla peräkkäiset nollaryhmät muotoon 2001:db8::1337:0:cafe.

IPv6:ssa kerrotaan aliverkon peite eli etuliitteen pituus osoitteen jälkeen kauttamerkillä eroteltuna normaalilla kymmenjärjestelmän numerolla, esim. /64. Tämä ilmaisee, kuinka monta bittiä osoitteen alusta on verkon etuliiteosaa. Pienin etuliitteen pituus on yksittäinen osoite peitteellä /128 ja suurin on koko IPv6-osoiteavaruus peitteellä /0. Hyvänä tapana on pidetty, että pienin peite olisi /64, koska tällöin kaikki IPv6:n ominaisuudet toimivat oikein. Kuitenkin kahden laitteen välinen siirtoverkko pisteestä pisteeseen voi olla /127 peitteellä ja yksittäisen laitteen yksilöinti loopback-osoite peitteellä /128. [4]

IPv6-osoiteavaruus on jaettu Internet Assigned Numbers Authorityn (IANA) toimesta tiettyihin ennalta määriteltyihin alueisiin, joita käytetään erilaisissa tarkoituksissa. Kuitenkin vain murto-osa koko IPv6-avaruudesta on tällä hetkellä allokoituna. Allokoimattomat IPv6-osoiteavaruudet odottavat tulevaisuutta ja mahdollisia uusia käyttötarkoituksia. Taulukko 1 on listattuna yleisimmin käytetyt IPv6-osoitealueet. Päivittyvä luettelo löytyy IANA:n tietokannasta. [6]

Taulukko 1. *Luettelo yleisemmistä IPv6-osoitealueista [7]*

IPv6-osoitealue	Selitys	Esimerkkiosoite
::1/128	Loopback-osoite	
fc00::/7	Unique local adress (ULA) -osoitteet	fc00:1a2b:3f::5c
fe80::/10	Paikalliset osoitteet	fe80::445e:e339:b4aa:89cf
2001:0000::/32	Teredo-osoitteet	2001:0000:0a0a:5005:3843:d8da:3fff:f505
2001:0002::/48	Suorituskykytesti-osoitteet	2001:0002:20::15
2002::/16	6to4-osoitteet	2002:c633:6401::
2001:db8::/32	Dokumentaatio-osoitteet	2001:db8::1
2000::/3	Globaalit osoitteet	2001:4860:4860::8888
ff00::/8	Ryhmälähetysosoitteet	ff02::1

Kuten Taulukko 1 havaitaan, on osoite ::1/128 varttu loopback-osoitteelle, eli kun kone haluaa ottaa yhteyden itseensä, käytetään tätä osoitetta, esim. koneella olevan web-palvelun selaamiseen. Vastaava osoite IPv4-maailmassa on 127.0.0.1. Toinen paljon käytetty alue on Unique local adress (ULA)-osoitteet, joita voidaan käyttää lähiverkossa osoitteina, joilla ei pääse kiinni IPv6-internetiin, esim. IPv4-osoitealue 192.168.0.0/16 vastaa tätä.

Teredo-osoitteita käytetään siirtymävaiheen tunnelointiprotokolla Teredo:ssa. Näille on oma muodostumisperusteensa IPv4-osoitteen ja yhteyden tietojen perusteella. Toinen siirtymävaiheen osoitealue on 6to4-osoitteet. Näitä käytetään 6to4-tunneleita varten ja nämäkin muodostuvat IPv4-osoitteen perusteella.

Dokumentaatiossa voidaan käyttää esimerkkiosoitteina dokumentaatio-osoitteita tai suorituskykytesti osoitteita. Näiden osoitteiden avulla ei tarvitse esimerkki dokumentaatioissa käyttää mahdollisesti käytössä olevia aitoja IPv6 osoitteita. [7]

Kuitenkin tärkeimmät IPv6-osoitealueet ovat paikalliset osoitteet (link-local), globaalit osoitteet (global unicast) ja ryhmälähetysosoitteet. IPv6:n toiminta perustuu näihin kolmeen osoitealueeseen.

Paikallisia osoitteita käytetään lähiverkossa viestittelyyn ja nämä muodostuvat yleensä laitteen portille automaattisesti portin media access control (MAC) -osoitteen perusteella. Tämä osoite näkyy usein laitteen verkkoasetuksissa valmiina, jos se on IPv6-kykenevä.

Globaalit eli julkiset osoitteet ovat reititettäviä osoitteita, joilla laite viestittelee IPv6-internetin tai lähiverkon ulkopuolisen laitteen kanssa. Nämä osoitteet tarvitsee määritellä jollain tavalla laitteelle, johon on useita eri tapoja. Näistä tavoista kerrotaan lisää kappaleessa 2.3.4. Mitä tahansa tämän alueen osoitteita ei voi ottaa käyttöön, vaan organisaation tms. tarvitsee lunastaa itselleen oma IPv6-etuliite palveluntarjoajalta tai muulta taholta. Tästä alueesta voi sitten määritellä osoitteita haluamallaan tavalla. [4]

Ryhmälähetysosoitteilla saadaan lähiverkossa tavoitettua useita laitteita saman aikaisesti. Nämä korvaavat IPv4:n yleislähetykset. Esimerkiksi osoitteella ff02::1 voidaan lähettää

kaikille paikallisverkon laitteille viesti, kun taas ff05::2-osoitteella saadaan viesti välitettyä kaikille lähiverkon reitittimille. [4] Ryhmälähetysosoitteiden huonona puolena voidaan pitää niiden helppoa käyttöä verkkohyökkäyksissä. Toisaalta niiden hyväksikäyttö hyökkäyksessä vaatii hyökkääjän olemista itse verkossa kiinni.

Laitteen portilla voi IPv6-protokollassa olla useampi IPv6-osoite, mikä on aivan normaalia. Tämä eroaa IPv4-protokollaan, jossa portilla voi olla vain yksi osoite. Jos portista on yhteys IPv6-internetiin, on sillä ainakin kaksi osoitetta: globaali osoite lähiverkon ulkopuolelle viestittelyyn ja lokaali lähiverkossa liikennöintiin. Portilla voi olla myös useampia globaaleja osoitteita, jotka kaikki toimivat. Tämä voi johtua virheellisistä asetuksista tai olla aivan tarkoituksenmukaista.

2.2.3 ICMPv6

ICMPv6 on ehdottomasti tärkein IPv6:n toimintaa tukeva protokolla ja on pakollinen IPv6:n oikean toimimisen kannalta. Sen viestit ovat kahden tyyppisiä, joko ne ovat virheviestejä, joilla ilmaistaan paketin välityksen tai toimituksen virhetilanteista, tai informatiivisia viestejä.

Virheviestejä on neljää erityyppiä. Ensimmäinen on kohdetta ei saavutettu, jonka lähettää jokin paketin reitin laitteista. Sillä ilmaistaan, että pakettia ei voitu toimittaa vastaanottajalle. Virheessä myös ilmaistaan miksi näin ei voitu tehdä, esim. ei reittiä vastaanottajalle tai osoite saavuttamattomissa. Toinen virhetyyppi on paketti liian suuri, mikä lähetetään, kun linkin maximum transmission unit (MTU) eli suurin sallittu paketin koko on liian pieni paketin kokoon nähden. Tämä johtuu siitä, että vain lähettäjä voi pilkkoa paketin pienemmäksi. Kolmas virhetyyppi on aika ylitetty, joka lähetetään, kun IPv6-otsikon elinaika on nolla eli paketti ei ole saavuttanut määränpäätään liian monen hypyn vuoksi. Viimeinen virhetyyppi on parametri ongelma. Tämä lähetetään, jos IPv6-otsikossa tai -lisäotsikossa on virhe, joka estää paketin tai otsikon oikean käsittelyn.

Paketti liian suuri -virhetyyppiä voidaan käyttää paketin maksimaalisen koon selvittämiseen tiettyjen laitteiden välillä, jotta voidaan viestiä mahdollisimman tehokkaasti. Tässä selvitetään paketin reitin pienin MTU-arvo. Aluksi laite lähettää oman yhteytensä MTU-arvon mittaisen paketin. Tämä matkaa reitillä, kunnes jokin MTU on pienempi kuin lähetetty paketti, jolloin lähetetään paketti liian suuri -virhe, jossa on tämän linkin MTU-arvo. Nyt lähettävä laite luo paketin, jonka koko on tämä virheviestistä saatu MTU. Paketti joko pääsee nyt määränpäähänsä tai matkalle tulee vielä pienempi MTU-arvo, jolloin prosessi vain toistetaan. Kun vastaanottaja on saanut paketin, tiedetään reitin suurin sallittu MTU.

Informatiivisia viestityyppejä on myös neljä erilaista. Ensimmäiset kaksi ovat perinteiset ping-viestit eli echo request ja reply. Näitä voidaan käyttää samalla tavalla kuin IPv4:ssä eli laite lähettää echo request -viestin, mihin vastaanottaja vastaa echo reply -viestillä.

Kolmas informatiivinen viestityyppi on multicast listener discovery (MLD). Näitä viestejä käytetään ryhmälähetysryhmien hallintaan ja niihin liittymiseen.

Viimeinen informatiivinen viestityyppi on naapurin havaitsemiseen käytettävä neighbor discovery (ND). Tämä sisältää viisi erilaista viesti tyyppiä: router solicitation (RS) eli reitittimen pyyntö, router advertisement (RA) eli reitittimen mainsotus, neighbor solicitation (ns) eli naapurin pyyntö, neighbor advertisement (NA) eli naapurin mainostus ja redirect eli uudelleen ohjaus. Näiden viestien avulla laite voi myös saada määriteltyä itselleen IPv6-osoitteen ja muutkin tiedot verkossa viestittelyyn.

Uudelleen ohjaus -viestin lähettää aina reititin. Näiden viestien avulla se saa kerrottua verkon laitteelle paremman ensimmäisen hypyn osoitteen, kun ollaan yhteydessä tiettyyn osoitteeseen. Nämä viestit lähetetään aina vastaukseksi laitteen yrittäessä ottaa yhteyttä reitittimen läpi toiselle laitteella ja aina laitteen omaan osoitteeseen.

RS-viestin lähettää IPv6-laite, kun se haluaa saada verkon tiedot reitittimeltä. Tämä tapahtuu esimerkiksi aina kun laite liittyy verkkoon. Viesti lähetetään IPv6-ryhmälähetys MAC-osoitteeseen 33:33:00:00:00:02 ja IPv6-vastaanottaja on kaikki reitittimet -osoite ff02::2,lähettäjän IPv6-osoitteen ollessa laitteen oma osoite tai nolla osoite eli ::, jos laitteella ei vielä ole osoitetta. Tähän verkon reitittimet vastaavat RA-viestillä.

RA-viestin lähettää aina reititin joko ajastetusti tai vastauksena RS-viestiin. Tämän avulla reititin pystyy mainostamaan itseään aliverkon laitteille. Viesti sisältää tarvittavat tiedot, jotta verkkoon liittyvä laite voi alkaa viestimään verkossa. Välitetyt tiedot ovat verkon IPv6-etuliite, yhteyden MTU, tietyt reitit, tieto siitä, käytetäänkö osoitteiden autokonfiguraatiota, ja osoitteiden voimassaoloaika. Viesti lähetetään myös IPv6-ryhmälähetys MAC-osoitteeseen ja IPv6-vastaanottaja on kaikki laitteet -osoite ff02::1. Paketin lähettäjän IPv6-osoite asetetaan reitittimen lähettävän portin paikallisosoitteeksi.

NS-viestin lähettää verkon laite halutessaan selvittää toisen laitteen MAC-osoitteen tai tarkistaakseen MAC-osoitteen paikkansapitävyyden. Sitä voidaan käyttää myös tarkastukseen, onko IPv6-osoite jo käytössä tai onko laite tietyllä osoitteella vielä saavutettavissa. NS-viesti lähetetään yleensä kaikki laitteet -ryhmälähetysosoitteeseen tai tarkistettaessa tiettyä laitetta, niin suoraan tällä.

NA-viestillä vastataan NS-viestiin tai laitteen tilan muuttuessa. NA-viesti sisältää tiedot viestin tyypistä, lähettäjän roolista verkossa ja normaalisti myös lähettäjän MAC-osoitteen. Paketti lähetetään aina sisältäen tiedon myös lähettävän portin IPv6-osoitteesta.

Uuden laitteen liittyessä verkkoon se tarkistaa, onko hänen osoitteensa käytössä verkossa. Tätä mekanismia kutsutaan duplicate address detection:ksi (DAD) eli osoitteiden kaksoiskappaleiden havaitsemiseksi. Se vastaa IPv4-maailman address resolution prtocol -protokollaa (ARP). DAD-mekanismi toimii niin, että tarkistava laite lähettää NS-viestin, jonka vastaanottajana on tarkistettava IPv6-osoite. Lähettäjän osoitteena on taasen ::-

osoite. Jos osoite on jo käytössä, osoitteen haltija lähettää NA-viestin kaikki laitteet -osoitteella ja omalla osoitteellaan, jolloin osoitteen kyselijä ei voi ottaa osoitetta käyttöönsä. Jos NS-viestiin ei tule vastausta, ottaa laite tämän osoitteen itselleen käyttöön.

NS-viestillä voidaan myös varmistaa, onko tietyn osoitteen haltija vielä saavutettavissa. Tässä lähetettään NS-viesti suoraan testattavaan osoitteeseen. Jos laite saa NA-vastauksen osoitteesta, tulkitaan, että laite on vielä saavutettavissa. NA-viestin lähettäjä ei voi kuitenkaan olettaa, että NS-viestin lähettäjä olisi saavutettavissa, koska se ei tiedä, vastaanottiko tämä hänen NA-viestin. [4]

2.2.4 Osoitteen määrittyminen

IPv6-verkossa osoite voi määrittyä neljällä erilaisella tavalla: staattisesti kiinteillä osoitteilla, stateless address autoconfigurationin (SLAAC) eli tilattoman osoitteen autokonfiguraation avulla, tilattomalla tai tilallisella dynamic host configuration protocol version 6:lla (DHCPv6). Näitä kaikkia tapoja käytetään yleisesti ja niitä usein käytetään rinnan samassa organisaatioissa, esimerkiksi organisaation palvelinverkossa käytetään staattisia osoitteita sekä kaikille verkon aktiivilaitteille on syötetty staattiset IPv6-osoitteet, mutta työasemaverkossa on käytössä tilallinen DHCPv6, vierailijaverkossa SLAAC ja kehitysverkossa tilaton DHCPv6.

Kun IPv6-laitteiden osoitteet määritetään staattisesti, tarvitsee jokaiselle verkon laitteelle erikseen syöttää kiinteät globaalit osoitteet sekä oletusreitit. Tämän lisäksi laitteille tarvitsee syöttää muutkin tiedot, kuten nimipalvelimen osoite. Tämä voi olla melko työlästä, varsinkin suurella määrällä laitteita, mutta joillekin laitteille se voi olla kannattavaa, kuten reitittimet ja muut aktiivilaitteet sekä palvelimet. Näin saadaan helposti otettua yhteyttä laitteisiin, kun niiden osoitteet eivät muutu automaattisesti ajan kuluessa. Muuten näille joutuisi käyttämään nimipalvelimia, jotka voivat muotoutua nopeasti monimutkaisiksi toteuttaa.

IPv6:n mukana tullut sisäänrakennettu osoitteiden automaattinen konfiguraatio SLAAC on uusi tapa osoitteiden määrittämiseen. Siinä ICMPv6 ND-viestityyppien avulla verkkoon liittyvä laite saa luotua itselleen uniikin, oikealla etuliitteellä olevan IPv6-osoitteen sekä määrittämään itselleen oletusreitin. Tämä on mahdollista reitittimen RA-mainostuksesta saadulla etuliitteellä, josta laite tekee itselleen IPv6-osoitteen, esim. MAC-osoitteensa perusteella, mikäli tämä on sallittu RA-viestissä. Tämä luotu osoite joudutaan tarkistuttamaan verkolta DAD-menetelmällä, jotta kukaan ei käytä jo tätä osoitetta. Lisäksi RA-viestistä saa oletusyhdyskäytävän osoitteen sekä elinajan kaikille saaduille arvoille. SLAAC:n avulla laite ei saa kylläkään kaikkia tarvitsemia tietojaan, kuten nimipalvelimen osoitetta, vaan nämä tarvitsee oppia jollain muulla menetelmällä.

Tähän ongelmaan voi käyttää tilatonta DHCPv6-palvelinta. Tässä laite oppii SLAAC:n avulla edellä mainitut tiedot, mutta esim. DNS-osoitteen DHCPv6-palvelimen viesteistä.

Tämä on hyvä tapa määrittää osoitteita, koska DHCPv6-osoitepalvelimen tai muunkaan laitteen ei tarvitse pitää kirjaa käytetyistä osoitteista. Tämä vähentää osoitepalvelimen kuormaa ja yksinkertaistaa verkkoa, kun se käyttää IPv6:n sisäänrakennettua osoitteen määrittämisominaisuutta.

Tilallisella DHCPv6:lla taasen kaikki tiedot tulevat osoitepalvelimelta. Reititin edelleen lähettää RA-viestejä, mutta niissä kielletään SLAAC:n käyttö. Tilallinen DHCPv6-palvelin lähettää liittyvälle laitteelle kaikki viestintään tarvittavat tiedot sekä laitteella käytettäväksi tarkoitetun IPv6-osoitteen. Palvelin pitää listaa määritellyistä osoite/laite-pareista, joka voi muodostua melko suureksi tietokannaksi. Tilallinen DHCPv6 soveltuu hyvin verkkoihin, jotka tarvitsevat tarkkaa osoitteenhallinnan keskittämistä. Sillä voidaan jakaa myös staattiseksi määrättyjä osoitteita tietyille laitteille, esim. tietyllä MAC-osoitteella oleva laite saa aina osoitteen 2001:db8:1000::dad. Tämä voi olla hyvä esimerkiksi kehitysverkossa, jossa laitteiden osoitteiden tulisi pysyä lähes samoina, mutta verkon etuliite vaihtuu usein ja näin staattiset osoitteet olisivat hankalia. [4]

Kun määritettäviä osoitteita aletaan suunnittelemaan, kannattaa ottaa huomioon myös tietoturva sekä mahdolliset hyökkäykset. Osoitteista kannattaa tehdä sellaisia, ettei hyökkääjä arvaa niitä helposti. Esimerkiksi hyökkääjä saa tietää, että verkossa on laite, jonka IPv6-osoite on 2001:db8:3000::6. Tästä on melko helppo päätellä, että verkossa on käytössä joko staattiset osoitteet tai tilallinen DHCPv6. Seuraavaksi hyökkääjä alkaa testaamaan löydetyn osoitteen viereisiä osoitteita numerojärjestyksessä ja löytää todennäköisesti lisää verkon laitteita. Tämän vuoksi kannattaa osoitteiden valinnassa käyttää mielikuvitusta eikä aloittaa aina tasaluvuista. Esimerkiksi staattisilla osoitteilla voidaan määrittää verkon palomuurien osoitteet päättymään DEF1, DEF2 jne. tai kahvitilan langaton reititin olisi CAFE-loppuinen osoite. Näissä on hyvä käyttää osoitteita, jotka on helppo muistaa. DHCPv6-palvelin voidaan määrittää aloittamaan osoitteet jostain muualta kuin perinteisestä tasasadasta, esim. osoitteesta 2001:db8:b00::1337 eteenpäin. Osoitepalvelin voidaan myös määrittää jakamaan satunnaisia osoitteita tietystä osoiteavaruudesta.

2.2.5 Tietoturvaominaisuudet

Vaikka yleisesti väitetään, että IPv6-protokollaan on tietoturva sisäänrakennettuna, ei tämä pidä paikkaansa. Ainut sisäänrakennettu tietoturvaominaisuus IPv6:ssa on oikeastaan IPsec, jota ei enää nykyään edes tarvitse IPv6-laitteiden tukea, vaikka ennen kaikkien IPv6-laitteiden tuli tukea IPsec-ominaisuutta. Yksi mahdollinen syy protokollan pakollisuuden poistamiseen oli vähäinen käyttöaste, vaikka ominaisuus oli sisäänrakennettuna.

IPsec:n avula pystytään luomaan salattu tunneli, joka turvaa IP-liikenteen sisällään. Paketin reitillä vain tunnelin päätepisteiden tarvitsee käyttää IPsec-protokollaa ja muiden vain välittää paketti eteenpäin. IPsec tunnelin muodostuksella on kaksi vaihtoehtoa: tunnelimalli ja kuljetusmalli. Nämä eroavat sillä, että kuljetusmalli suojaa vain IP-liikenteen hyötykuorman, kun taas tunnelimalli koko IP-liikenteen eli myös IP-otsikon. [4]

Tämä ei kuitenkaan turvaa IPv6-protokollaa, jos sitä ei aktiivisesti käytetä kaikkiin yhteyksiin, mikä ei ole mahdollista tukemattomuuden vuoksi. Silti sisäänrakennetusta IPsec-ominaisuudesta on noussut turvallisuuden tunne ja olettamus, että IPv6 on turvallisempi kuin IPv4.

3. SIIRTYMÄVAIHE IPV4:STÄ IPV6:EEN SEKÄ TESTIYMPÄRISTÖ

Tässä kappaleessa kerrotaan, mikä on siirtymävaihe, mitä tekniikoita ja protokollia siinä käytetään sekä esitellään testiympäristö. Testiverkkoa on käytetty joidenkin työn asioiden testaamiseen. Lopuksi käydään läpi huomioita, mitä testiympäristöstä ja sen käytöstä ilmeni sekä mitä muita huomioita on IPv6:den käytöstä ilmennyt.

3.1 Siirtymävaihe

Siirtymävaiheella tarkoitetaan aikaväliä, jonka aikana siirrytään täydellisestä IPv4-verkosta käyttämään täydellistä IPv6-verkkoa, jossa ei enää ole IPv4-osoitteita käytössä. Siirtymä vaiheessa kestää melko kauan, koska kaikkien Internetin laitteiden on käytettävä lopuksi pelkästään IPv6. Tämän mahdollistamiseksi tarvitaan eri tekniikoita, jotta kaikki palvelut ja laitteet ovat saavutettavissa protokolla versiosta riippumatta.

Kun IPv6-protokolla julkaistiin, verkkolaitteiden tuki tälle oli vähäistä. Pikkuhiljaa laitteet alkoivat tukemaan IPv6-osoitteita ja -viestintää. Nykyään lähestulkoon poikkeuksetta jokainen uusi verkkoon kytkettävä laite tukee IPv6-protokollaa viestinnässään. Vanhoihin laitteisiin on tullut myös IPv6-ominaisuuksia ohjelmistopäivitysten kautta, mutta ei silti välttämättä kaikkia IPv6-ominaisuuksia tai kaikkia laitteen tukemia ominaisuuksia myös IPv6:lla, esim. kytkimen tai reitittimen palomuuraus ei tue IPv6-protokollaa.

IPv6-protokolla ei tuo muutoksia OSI-mallin kerroksella kaksi toimiviin laitteisiin eli esimerkiksi WIFI-tukiasemaan, koska IPv6 toimii OSI-mallin kerroksella kolme. Osa käyttöjärjestelmistä tukee suoraan myös siirtymätekniikoita ja -protokollia, esimerkiksi Windows pitää sisällään Teredo-asiakkaan. [4]

IPv6-protokollan käyttöönottamista kannattaa edeltää hyvä suunnitteluvaihe. Tässä selvitetään, mitä laitteita ja palveluita halutaan yhdistää IPv6-verkkoon. Suunnittelussa tarvitsee ottaa huomioon myös se, tukevatko kaikki nämä laitteet ja palvelut IPv6-protokollaa tarvittavalla tasolla. Lisäksi tarvitsee päättää, käytetäänkö IPv4:a ja IPv6:a rinnakkain samoissa laitteissa eli dual stack. Jos jokin palveluista ei tue IPv6:ta ja sitä tarvitaan myös IPv6-laitteilla, tarvitsee tämän edessä käyttää jotain muuta siirtymätekniikkaa esim. osoitteen muutosta tai NAT64:sta. Osoitteiden jako aliverkkoihin on myös tärkeä suunnittelun vaihe, johon liittyy myös laitteiden osoitteiden saamistapa. Käytetäänkö staattisia IPv6-osoitteita, SLAAC:a, tilatonta tai tilallista DHCPv6:ta. Myös verkon tietoturvaa ja palomuurausta tarvitsee pohtia, kuten myös palomuurien sijainteja verkossa, jotta saavutetaan molemmilla IP-protokollilla riittävä ja samantasoinen suojaus.

Siirtymävaiheessa tarvitaan tukena tekniikoita ja protokollia, joiden avulla saadaan tarvittava yhteensopivuus IPv4:n ja IPv6:n välillä. Yksi tällainen tekniikka on tunnelointi, jonka avulla saadaan toisen protokollaversion liikenne kulkemaan toisen sisällä, esim. IPv6-liikenne tunneloituna IPv4-verkon lävitse IPv4-kehyksen sisällä. Tähän löytyy monia tapoja sekä protokollia, joita käydään kappaleessa 3.1.2 paremmin lävitse. Toinen siirtymävaiheen avustava tekniikka on NAT64, jossa tehdään yhden IPv4-osoitteen alle IPv6-verkko ja liikenteelle tehdään tarvittavat osoitteen muutokset. Suosituin siirtymävaiheen tekniikka on dual stack eli käytetään molempia IP-protokollia rinnakkain samoissa porteissa. Viimeisenä tekniikkana on osoitteen muutos, jonka avulla erilliset IPv4-verkko ja IPv6-verkko voivat keskustella keskenään yhdyskäytävän läpi, joka muuttaa käytetyt osoitteet sopivaksi molemmille verkoille liikenteen läpi kulkiessa. [4]

IPv6:een siirtymistä helpottamaan on luotu palveluita, jotka voivat päättää asiakkaiden luomia tunneleita käyttääkseen IPv6-protokollaa. Tällaisia palveluita kutsutaan tunnel broker-nimellä ja yksi tällainen on Hurricane Electric:n palvelu [8]. Palvelua käytetään, kun halutaan käyttää IPv6:a, mutta internetpalveluntarjoajalla on vain IPv4-liityntäverkko asiakkaalle. Tällöin asiakas luo IPv6-liikenteelle tunnelin operaattorin IPv4-verkon läpi tunnel broker-palveluun, josta IPv6-liikenne pääsee IPv6-internetiin. Tämä mahdollistaa myös liikenteen kulkea toiseen suuntaan, sillä tunnelin rekisteröityessä annetaan oman verkon tiedot, kuten IPv6-osoiteavaruus ja tunnelin alkupisteen IPv4-osoite. [8]

IPv6 on tuonut mukanaan myös uusia muokattuja protokollia vanhoista vastaavista IPv4-protokollaa käyttävistä. Yksi tällainen on dynamic host configuration protocol (DHCP), josta tuli IPv6:ta tukeva uusi versio DHCP version 6 (DHCPv6). Nämä ovat perusperiaatteeltaan hyvin samanlaisia eli tarjoavat verkon laitteille osoitteen ja verkon tiedot. Toisen yleisesti käytetyn protokollan päivitys on open shortest path first version 3 (OSPFv3), joka oikeastaan muuttaa protokollaa vain salliakseen pitkien IPv6-osoitteiden käytön verrattuna IPv4-osoitteisiin. DNS palveluun on tullut myös lisäys IPv6-palveluille eli tuki AAAA-tietueille. [4]

3.1.1 Dual stack

Dual stack tarkoittaa, että rakennetaan jo olevassa olevaan IPv4-verkkoon loogisesti rinnalle IPv6-verkko. Tällöin jokaisella dual stack -verkon portilla on sekä IPv4- että IPv6-osoite ja kaikki verkon palvelut ovat saatavilla molempia protokollia käyttäen joko suoraan tai muita siirtymätekniikoita hyväksi käyttäen. Fyysisessä verkkokuvassa verkot ovat samoissa kaapeleissa ja laitteissa, mutta loogisesti ne ovat täysin eri verkot, jotka voidaan kuitenkin piirtää samaan verkkokuvaan.

Dual stack:ssa vaikka portti on sama, on molemmilla protokollan versiolla eri käsittely pino. Tämä tarkoittaa sitä, että OSI-mallin verkko- ja kuljetuskerrokset ovat omansa eri protokollan versioilla, eli esimerkiksi IPv6:lla on oma erillinen transmission control protocol (TCP) käsittelijä IPv4:ään verrattuna.[4]

Esimerkkinä dual stack-verkosta on se, että verkossa on tietokone, reititin ja palvelin, joilla jokaisella on sekä IPv4- että IPv6-osoitteet. Reitittimeltä on yhteys internettiin käyttäen molempia protokollia. Palvelimella on useita palveluita, jotka ovat myös saatavilla käyttäen molempia protokolla versioita, mutta palvelu x tukee vain IPv4:ää. Jotta palveluun x saataisiin tietokoneelta yhteys käyttäen IPv6:tta, on palvelun eteen tehtävä joillain muulla siirtymävaiheen protokollalla muutos IPv6:sta IPv4:ään, esim. köyttäen NAT64. Näin saadaan koko verkko saavutettavaksi molemmilla protokollilla ja dual stackin periaate toteutuu.

Dual stackista on olemassa myös toinen versio: dual stack lite (DS-Lite). Se on tarkoitettu verkontarjoajille IPv4-osoitteiden säästämiseksi. Siinä runkoverkko toteutetaan asiakkaan reunalle asti IPv6:lla, josta asiakas voi käyttää IPv6-liikennettä normaalisti. Mutta jos asiakas haluaa käyttää IPv4-liikennettä, käytetään tässä tilanteessa NAT-osoitteen muutosta ja 4in6-tunnelointia eli tunneloidaan asiakkaan IPv4-liikenne IPv6:n sisällä asiakkaan reunalla, ja kun paketit saavuttavat IPv4-internetin reunan, terminoidaan tunneli sekä tehdään osoitteille NAT. [9] Operaattorilta säästyy näin julkisia IPv4 osoitteita, kerran kaikki osoitteet ennen IPv4-internetin reunaa ovat yksityisiä. Kuitenkin asiakkaalla on saavutettavissa sekä IPv4- että IPv6-internetit.

3.1.2 Tunnelointiprotokollat

Tunnelointiprotokollat ovat siirtymävaiheessa käytettäviä erilaisia menetelmiä tunneloida liikennettä toisen IP-version verkon yli, niin että vastaanottaja pystyy tunnistamaan lähettäjän ja vastaamaan tälle, esim. IPv4-laite juttelee IPv4-palvelimelle IPv6-runkoverkon yli. Tunnelointimenetelmät voidaan jakaa usealla eri tavalla ryhmiin riippuen niiden toimintatavasta, tunnelin päistä, konfigurointi tavasta ja siirtoverkosta. Helpoin tapa erotella tunnelit, on jakaa ne kahteen riippuen siirtoverkon IP-versiosta ja täten myös tunneloitavasta versiosta. Tunnelit voivat olla IPv6 liikennettä IPv4 verkon yli tai toisin päin. Toinen tapa on jakaa konfigurointi tavan mukaan, eli onko tunnelit automaattisesti konfiguroituvia vai tarvitseeko ne konfiguroida kokonaan käsin. Seuraava tapa erotella tunneleita on niiden päätepisteiden sijainti eli ovatko ne käyttäjältä käyttäjälle -tunneleita (host-to-host), käyttäjän ja reitittimen välillä (host-to-router/router-to-host) vai reitittimien välisiä (router-to-router). Osaa tunneliprotokollista voi käyttää useammalla näistä tavoista, joten ne eivät ole tarkasti rajoittavia ryhmiä.

Ensimmäiseksi käsitellään tunnelointi tavat, jotka käyttävät verkkokerroksenaan IPv6:ta. Nämä eivät ole, ainakaan vielä, aivan niin yleisiä kuin tunnelit, joiden verkkokerroksena käytetään IPv4:ää. Tämä johtuu siitä, että IPv6-verkot eivät ole vielä niin yleisiä kuin IPv4-verkot. Joten näitä tunnelointi menetelmiä tullaan käyttämään enemmissä määrin vasta myöhemmin siirtymävaiheessa, kun IPv6 on yleistynyt laajemmin. Toki näitä voidaan käyttää erikoistapauksissa jo nyt, kuten esimerkiksi operaattoreiden siirtoverkoissa. Yleisimmät tämän tyyliset tunnelointitavat ovat 4in6 ja 4over6.

4in6 käyttää hyväkseen IPv6:n geneeristä tunnelointi ominaisuutta. Siinä konfiguroidaan manuaalisesti tunneli IPv6-verkon läpi, jonka sisään sijoitetaan IPv4-liikenne. Tätä tunnelointimekanismia voitaisiin käyttää kaikenlaiseen liikenteeseen protokollasta riippumatta. Konfiguroitu tunneli on yksisuuntainen. Jotta siitä saataisiin kaksisuuntainen, tarvitsee tunneli konfiguroida myös paluusuuntaan. Ennen tunnelin muodostusta tarvitsee tunnelin aloituspäällä ja lopetuspäällä olla reitit toisiinsa IPv6-verkon yli. Tämän jälkeen kerrotaan tunnelin molempien päiden laitteille vastapäiden osoitteet tunnelin muodostamista varten sekä mikä IPv4-verkko vastapäästä löytyy reititystä varten. [10] Näin saadaan pelkästään IPv4:ää käyttävän verkon paketit liikennöityä IPv6-verkon yli tunnelia pitkin toisen pään IPv4-verkkoon. 4in6-tunneli on mahdollista toteuttaa myös automaattisesti muodostuvana erilaisia tunnelinmuodostusprotokollia käyttäen, esim. Tunnel setup protocol (TSP), mutta tämä ei ole kuitenkaan niin yleistä.

TSP:tä käytetään kahden halutun tunnelin päätepisteen välillä välittämään tunnelin asetukset toisilleen. Toinen tunnelin päistä on TSP-palvelin ja toinen TSP-asiakas, mutta toki TSP-asiakkaita voi olla useampi yhdellä TSP-palvelimella, jolloin jokaiselle muodostuu oma tunnelinsa. Kun tunnelia aletaan muodostamaan, neuvottelevat päätepisteet vähintään seuraavat parametrit keskenään: käyttäjän autentikointitapa, joka voi olla myös anonyymi, tunnelin kapselointi (IPv6 IPv4:n yli, IPv4 IPv6:n yli vai IPv6 UDP-IPv4:n yli NAT:a varten), IP-osoitteistus tunnelin päille ja DNS-rekisteröinti näille osoitteille. Lisäksi TSP:llä voidaan neuvotella tunnelin elinaika ja yhteyden toimivuuden testaus. Jos asiakas on reititin, voivat päätepisteet neuvotella myös käytettävät reititysprotokollat ja IPv6-etuliitteen asiakkaalle. TSP:n etuina on staattiset tunnelit sekä IP-osoitteet ja -etuliitteet, mobiliteetti eli tunneli muodostuu automaattisesti uudelleen, jos asiakas vaihtaa verkkoa, protokollan joustavuus sekä kapseloinnin monet mahdollisuudet. [11]

4over6 on taasen suunnattua lähinnä verkontarjoajille, jotka voivat tämän avulla saada IPv4-asiakkaat liikennöimään operaattorin IPv6-runkoverkon yli IPv4-internetiin automaattisesti muodostuvia tunneleita pitkin. 4over6 käytetään, kun operaattorilla on vain IPv6:a käyttävä runkoverkko ja sen tarvitsee välittää asiakkaiden IPv4-liikenne ylitse. Asiakkaan IPv6-liikenne toimii aivan normaalisti, mutta IPv4-liikenne kulkee operaattorin verkon läpi tunnelia pitkin. Tunnelina 4over6 käyttää hyväkseen 4in6:a eli IPv6:n geneeristä kapselointi mekanismia. 4over6-mekanismia ei kuitenkaan enää suositella käytettäväksi uusissa tapauksissa, vaan tämän uudempaa DS-Liten laajennosta lightweight 4over6:ä. [12] Lightweight 4over6 eroaa DS-Litestä niin, että NAT osoitteen muutos tehdään asiakkaan päässä eikä operaattorin tunnelin päätepisteessä.[13]

Seuraavaksi käydään läpi tunnelointimenetelmät, jotka kapseloivat IPv6-liikenteen IPv4-verkon yli. Näitä on monenlaisia ja ne käyttäytyvät osa melkein samalla tavalla, mutta tässä esitellään vain yleisimmät. Tunnelointi menetelmiä on kahden tyyppisiä: ne jotka käyttävät protokolla 41 kapselointia eli IPv6-paketti suoraan IPv4-paketin sisällä ilman lisäotsikoita ja IPv4-otsikon protokollakentässä on numero 41, ja niitä jotka eivät tätä käytä. [14] Esitellyistä tekniikoista vain Teredo ei käytä protokolla 41 kapselointia. Muut

esitellyt menetelmät ovat 6in4, 6to4, 6over4, IPv6 rapid deployment (6rd) ja Intra-Site Automatic Tunnel Addressing (ISATAP).

6in4-tunnelit konfiguroidaan manuaalisesti samalla tapaa kuin 4in6, mutta muodostunut tunneli on yleensä molemmin suuntainen. Tunnelin päätepiste voi olla organisaation sisäinen, mutta yleensä se on ulkopuolinen Tunnel broker -palvelu, joka mahdollistaa IPv4-asiakkaiden käyttää IPv6-internetiä. Muodostunut tunneli on aina staattinen, jos sitä ei laajenneta muilla protokollilla tai menetelmillä, kuten Heartbeat protokollalla jolloin tunnelinpää voi vaihtua ja yhteys muuttuu dynaamiseksi. 6in4-menetelmää kutsutaan myös nimillä manuaalinen tunneli, konfiguroitu tunneli, staattinen tunneli ja protokolla 41 tunneli. [14] 6in4-tunnelit ovat työläämpiä toteuttaa kuin automaattisesti konfiguroitavat tai automaattitunnelit, mutta niiden toimintaa on helpompi ennustaa sekä testata staattisten päätepisteiden ja reitin vuoksi.

6to4 tarkoituksena on mahdollistaa IPv4-verkon takana eristyksissä olevan IPv6-laitteen tai -domainin yhdistyä IPv6-verkkoon mahdollisimman helposti ja vähällä konfiguraatiolla. Laite, joka käyttää tai reitittää muille laitteille 6to4-menetelmää, tarvitsee globaalisti reitittyvän IPv4-osoitteen, jotta menetelmä toimii oikein, eli menetelmä ei ole käytettävissä suoraan NAT-verkon sisällä, vaan tällaisen verkon reititin täytyy hoitaa 6to4 tunnelointi tai on käytettävä muuta menetelmää. 6to4 käyttää hyväkseen protokolla 41 -menetelmää ja tämän lisäksi osoitteenmuutosta IPv4-osoitteesta IPv6-osoitteeseen. 6to4-osoitteille on globaalisti varattuna oma alueensa 2002::/16. Osoitteenmuutos tapahtuu seuraavasti: 6to4 IPv6 -osoite alkaa aina 2002: ja tämän jälkeen IPv4-osoite muutettuna heksadesimaalimuotoon, esimerkiksi 198.51.100.1 on 6to4-osoitteena 2002:c633:6401:: eli 198 on c6 heksadesimaalimuodossa, 51 on 33, 100 on 64 ja 1 on 01. Tätä osoitetta käytetään vain tunnelinpäänä, josta voidaan muodostaa tunneliyhteys useampaan toiseen tunnelinpäähän. Näin muodostetut tunnelin päät voidaan reitittää organisaation sisällä ja laitteet voivat keskustella IPv6:lla keskenään IPv4-verkon yli käyttäen tunnelia hyväkseen. Jotta tunnelia voidaan käyttää globaaliin viestintään, tarvitsee tunneli yhdistää 6to4-välityspalveluun (6to4-relay) tai rekisteröidä oma 6to4-tunnelinpää osoitteineen palveluntarjoajan avulla Regional internet registryn (RIR) tietokantaan. [15] Koska 6to4 ei tue NAT-verkon takana olevia laitteita, jota operaattorit ovat alkaneet käyttämään siirtoverkoissaan asiakkaille julkisten IPv4-osoitteiden sijaan, protokolla alkaa jäämään historiaan tulevaisuudessa toimintaperiaatteensa vuoksi.[4]

6over4 on tarkoitettu organisaation sisäiseen IPv4-verkoon, käyttäen tätä IPv4-verkkoa virtuaalisena Ethernet-kerroksena IPv6-liikenteelle. IPv4-ryhmälähetystä hyväksi käyttäen pystyy 6over4-mekanismi lähettämään IPv6-ryhmälähetyksiä ja täten ICMPv6:n ominaisuudet, kuten ND on mahdollinen sekä näitä viestipaketteja käyttävät ominaisuudet mm. tilaton osoitteiden autokonfiguraatio. 6over4 käyttää protokolla 41-kapselointia, joka tehdään aina asiakaslaitteella tai reitittimellä paluuviestille. Siinä myös luodaan IPv6 paikallinen osoite laitteen IPv4-osoitteesta niin, että IPv4-osoite muutetaan heksadesimaalimuotoon ja laitetaan tämä fe80:: alkuisen osoitteen loppuun, esim. 10.0.2.1 on

muutettuna fe80::0a00:0201. 6over4 etuina on minimaalinen konfiguraatio ja ICMPv6-protokollan toimiminen. Tällä menetelmällä saadaan 6over4:ta käyttävä laite yhdistettyä IPv6-internetiin, kunhan yhdyskäytävä on tuohon yhteydessä. Tämä kuitenkin vaatii sen, että laitteella on globaali IPv4-osoite. Kuitenkin organisaatio, joka käyttää NAT-verkkoa yhdistävällä laitteella, voi luoda yhteydet organisaation sisällä paikallisilla IPv6-osoitteilla ja näin saavuttaa organisaation sisäiset IPv6-palvelut. [14]

6rd on luotu internetpalveluntarjoajille nopeaksi sekä halvaksi vaihtoehdoksi IPv6-yhteyden tarjoamiseksi asiakkaillensa IPv4-liityntäverkkonsa yli tunneloimalla. 6rd on muokattu versio 6to4-menetelmästä, sillä erotuksella että tässä käytetään palveluntarjoajan omaa IPv6-osoiteavaruutta 2002::-avaruuden sijaan. Lisäksi tunnelointi tapahtuu pelkästään operaattorin omassa verkossa, joten tunnelin hallinta ja virheiden etsintä on helppoa. Halvan toteutuksen protokollasta tekee minimaaliset laitehankinnat, koska 6rd:tä tukevia laitteita tarvitaan vain asiakkaan verkon reunalle sekä internetpalveluntarjoajan IPv6-verkon reunalle, joiden välille tunneli muodostetaan olemassa olevan IPv4-verkon yli. 6rd:ssä asiakas käyttää joko dual stack-verkkoa tai pelkästään IPv6-verkkoa. Asiakkaan verkon reunalla oleva laite tunneloi IPv6-liikenteen 6to4-menetelmällä, niin että lähettäjän IPv6-osoite on generoitu operaattorin reitittyvästä 6rd:lle varatusta osoiteavaruudesta ja asiakkaanreunan laitteen IPv4-osoittesta samalla tavoin kuin 6to4:ssä. Tätä generoitua osoitetta voidaan käyttää myös asiakkaan verkon globaalina IPv6-alueena. Näin ollen generoitu IPv6-osoite on globaalisti reitittyvä toisin kuin 6to4:ssa, jossa jouduttiin käyttämään ulkopuolista välityspalvelua globaaliin reititykseen. 6rd:ssä tunnelin terminoinnin hoitaa palveluntarjoajan IPv6-verkon reunalla oleva reititin, joten tunnelin hallinnointi ei päädy kolmannelle osapuolelle ja täten se on hieman tietoturvallisempi sekä palvelu on vakaammalla pohjalla. [16]

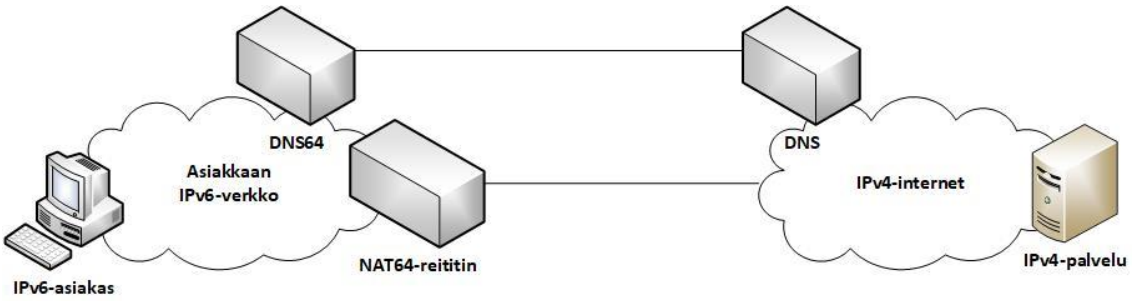
ISATAP, niin kuin nimikin sanoo, on tarkoitettu organisaation sisäverkossa eli intra-verkkossa käytettäväksi tunnelointi protokollaksi, joka käyttää protokolla 41-kapselointia viestiäkseen IPv6-liikennettä IPv4-verkon yli. Kuitenkin nykyään ainakin Microsoft suosittelee, ettei ISATAP-menetelmää käytetä kuin testaus tarkoituksissa, eikä ollenkaan tuotantoverkoissa. [4] ISATAP on samantapainen kuin 6over4, mutta ISATAP ei käytä IPv4-ryhmälähetyksiä viestintäänsä. Saadakseen IPv6-osoitteen, ISATAP-verkkoon yhdistyvän laiteen on lähetettävä organisaationsa ISATAP-reitittimelle router solicitation-viesti. Reitittimen osoite on opittu joko käsin syöttämällä, DHCP:lla tai DNS:llä. Jokaisen ISATAP-verkkoon liittyvän laitteen on itse ajettava ISATAP-protokollaa, jotta voivat yhdistää ISATAP-reitittimen takana olevaan IPv6-verkkoon. ISATAP-menetelmää voidaan käyttää laitteen yhdistämiseksi reitittimeen ja toisinpäin sekä reitittimien välillä. Tässä menetelmässä luodaan myös verkkoon yhdistyvälle laitteelle osoite, joka voi olla globaali tai lokaali laitteen IPv4-osoitteen perusteella. Jos laitteen IPv4-osoite on privaattialueelta, niin muodostuva osoite on lokaali, ja jos taas julkiselta alueelta, niin sitten globaali. Globaaliosoite on muotoa ::0200:5efe:… ja lokaali muotoa ::0000:5efe:…, esim. 10.2.192.1-

osoite on globaalissa muodossa ::0200:5efe:10.2.192.1 tai ::0200:5efe:0a02:c001 ja lokaali ::0200:5efe:10.21.192.1. Osoitteen alkuun on mahdollista lisätä organisaation oma IPv6-etuliite. [14]

Teredo on hyvin samanlainen 6to4-menetelmän kanssa, mutta se ratkaisee tämän suurimman ongelman eli NAT-verkot. Teredo mahdollistaa myös NAT-verkon laitteiden yhdistää IPv6-internetiin, vaikka niillä ei olisikaan globaalia IPv4-osoitetta. Tämän se mahdollistaa käyttämällä liikennöintiinsä kuljetuskerroksella ja kapseloinnissa user datagram protocol-protokollaa (UDP), erityistä generoitua IPv6-osoitetta, jolla pystyy yksilöimään myös NAT-verkon sisällä olevan laitteen ja on täten globaalisti uniikki sekä reitittyvä, sekä erillisiä Teredo-palvelimia yhteyden muodostukseen. Teredo-tunnelin muodostus aloitetaan ottamalla yhteys Teredo-palvelimeen, esim. teredo.trex.fi, jolta asiakas vastaanottaa tarvittavat parametrit mm. asiakkaalle generoitu IPv6-osoite, joiden avulla Teredo-tunneli muodostuu automaattisesti. Generoituva IPv6-osoite on aina osoiteavaruudesta 2001:0000::/32 ja se muodostuu seuraavalla tavalla. Alussa olevan 2001:0000: perään tulee käytetyn Teredo-palvelimen IPv4-osoite heksadesimaalimuodossa, jonka jälkeen 16 bittiä erilaisia lippuja. Ensimmäinen lippujen bitti kertoo, onko asiakas tietyntyylisessä NAT-verkossa. Kuitenkin tämä suositellaan nykyään asettamaan nollaksi tietoturvasyistä. Seuraava bitti on varattu tulevaisuuden laajennoksia varten ja asetetaan nollaksi, jonka jälkeen neljä satunnaista bittiä, joita seuraa kaksi nolla bittiä, jotka olivat varattuna tietoturvasyistä poistetuille universaali/lokaali-bitille ja yksilö/ryhmä-bitille. Viimeiset kahdeksan lippubittiä ovat satunnaisia, jotka olivat edellä olevien satunnaisbittien lisäksi aikaisemmin nollia, mutta ne muutettiin satunnaisiksi tietoturvasyistä, ettei osoitteesta saisi ylimääräistä tietoa tietoturvahyökkäyksen toteutukseen. Seuraavaksi osoitteessa on 16 bittinen NAT-verkon UDP-portti asiakkaan yhteydelle käänteisillä biteillä ja asiakkaan julkinen IPv4-osoite myös käänteisillä biteillä. Esimerkiksi asiakas yhdistää NAT-verkosta Teredo-palvelin 10.10.80.5 (0a0a5005), lippubittien ollessa tietoturvasyistä 0, 0, satunnaiset neljä 1110, 0,0 ja satunnaiset kahdeksan 10100011, joka on heksadesimaalina 38A3, UDP porttina käytetään 10021 (d8da) ja asiakkaan reitittimen julkinen IPv4-osoite on 192.0.10.250 (3fff f505), josta muodostuu kokonainen IPv6-osoite 2001:0000:0a0a:5005:3843:d8da:3fff:f505. Teredo-asiakas pitää yllä yhteyttään Teredo-palvelimelle ja kun asiakas haluaa ottaa yhteyttä julkiseen IPv6-osoitteeseen, se lähettää ICMPv6 ping-paketin osoitteeseen palvelimen välityksellä, jonka jälkeen ping-paluupaketin avulla neuvotellaan yhteydelle paras Teredo-välityspalvelin hoitamaan lopullinen tiedonsiirto asiakkaan ja kohteen kesken. Teredon etuina voidaan pitää sitä, ettei internet-palveluntarjoajan tarvitse tehdä muutoksia omaan verkkoonsa, yhteys IPv6-internetiin onnistuu NAT-verkosta, sekä Teredo on sisäänrakennettuna Windows-käyttöjärjestelmän koneissa. Kuitenkin Teredo ei toimi kaikkien NAT-toteutusten kanssa, sen toiminta on useimmiten hidasta Teredo-välityspalvelimien etsinnän vuoksi ja näillä julkisilla välityspalvelimilla saattaa olla suuria kuormia, mikä aiheuttaa usein epästabiileja yhteyksiä näiden lävitse.[4; 14]

3.1.3 NAT64

IPv6:en siirtymisessä voidaan käyttää myös hyväksi IPv4-verkoista tuttua NAT-menetelmää, jossa yhden IPv4-osoitteen alle voidaan luoda verkko, josta voidaan muodostaa yhteyksiä myös ulkopuoliseen verkkoon vähentäen käytettävien julkisten IPv4-osoitteiden määrää. NAT64 on osoitteenmuutosprotokolla, jonka avulla pelkästään IPv6:a käyttävä laite pystyy viestimään pelkästään IPv4:a käyttävän laitteen kanssa. Toimiakseen oikein, NAT64 tarvitsee tuekseen DNS64-protokollan, jonka avulla muutetaan nimipalvelimen IPv4:n A-tietue IPv6:n käyttämään AAAA-tietueeksi. Kuva 2 on esitelty pelkistetty esimerkkikuva tapauksesta, jossa voidaan käyttää NAT64:ta. Kuvasta löytyy NAT64-menetelmän tärkeimmät elementit eli NAT64-reititin ja DNS64, jotka voivat olla myös samassa laitteessa.



Kuva 2. *NAT64-verkon yksinkertainen toteutus*

Kun IPv6-asiakas haluaa ottaa yhteyttä IPv4-palveluun, se tekee aluksi DNS-kyselyn DNS64-palvelimelle, joka välittää kyselyn eteenpäin IPv4-palvelun vastaavalle DNS-palvelimelle. Tällä on tarjota vain IPv4-palvelun A-tietue eli palvelun IPv4-osoite, jota IPv6-asiakas ei voi suoraan käyttää vaan se tarvitsee muuttaa IPv6-muotoon. Tämän muutoksen toteuttaa DNS64, siten että IPv4-osoite muutetaan heksadesimaali muotoon ja liitetään asiakkaan määrittämän IPv6-etuliitteen perään. Muutettu osoite lähetetään asiakkaalle. Nyt asiakas voi lähettää kyselynsä IPv4-palvelun suuntaan NAT64-reititimen läpi. Kun paketti saapuu reitittimelle, sille tehdään muutos riisumalla IPv6-kehys pois paketin ympäriltä ja liittämällä IPv4-kehys tämän tilalle vastaanottajanosoitteen IPv4:ksi palautuksen jälkeen. Lähettäjän IPv4-osoitteeksi merkataan reitittimen IPv4-osoite ja lähettäjän portiksi erikseen valikoitunut porttinumero. Reititin pitää kirjaa näistä portti-IPv6-osoite pareista, joiden avuilla se pystyy välittämään paluupaketit oikeille vastaanottajille ja tekemään paketille saman kehyksen muutoksen kuin aikaisemmin mutta päinvastaisesti. [4]

NAT64-verkoissa voidaan käyttää joko verkonhaltijan omaa IPv6-etuliitettä tai geneeristä NAT64:lle varattua osoite avaruutta 64:ff9b::/96. Tähän käyttöön voidaan myös ottaa Unique local addresses-avaruuden (ULA) eli fc00::/7 osoitteita, jotka eivät ole reitittyviä organisaation ulkopuolella. Valittava osoiteavaruus riippuu täysin toteutuksesta, sillä jos ei käytetä globaalia IPv6-etuliitettä IPv6-verkossa, ei myöskään IPv6-internet ole

saavutettavissa. DNS64:n muutokseen valittava etuliite on myös tärkeä, ettei muutettu osoite mene päällekkäin jo olemassa olevan osoitteen kanssa. Esimerkiksi voidaan käyttää organisaation omaa IPv6-etuliitettä verkon laitteille ja DNS64 käyttää 64:ff/96 -etuliitettä, jolloin NAT64-reitittimen on helppo tunnistaa IPv4-osoitteet, jotka on muutettu IPv6-muotoon.

Yksi mahdollinen NAT64-toteutus voisi olla esimerkiksi organisaatiolla, joka on toteuttanut koko verkkoympäristönsä IPv6:lla. Kuitenkin yksi palvelu ei tue kuin IPv4-protokollaa. Tällöin organisaatio voi toteuttaa NAT64-palvelun IPv4-palvelimen eteen. Tällöin IPv4-palvelu on saavutettavissa myös IPv6-asiakkaille. Toinen hyvä käyttökohde on mobiilioperaattorilla, niin että NAT64:n takana on puhelimet IPv6-verkossa, koska tähän tarvitaan paljon osoitteita ja IPv6-osoitteita on huomattavasti enemmän operaattoreilla kuin IPv4-osoitteita. Näin saadaan useampi mobiililaite yhden IPv4-osoitteen taakse. Tämä kuitenkin vaatii puhelimilta IPv6:lle tuen.

NAT64 voi toteuttaa kahdella tavalla. Edellä kuvatulla tavalla, jossa osoitteet ja portit luovat automaattisesti parin. Tätä kutsutaan tilalliseksi NAT64:ksi. Sitten on myös tilaton NAT64, jossa määritetään käsin IPv4/IPv6-osoiteparit. Tämä on huomattavasti työläämpi eikä sillä saavuteta samaa IPv4-osoitteiden säästöä kuin tilallisessa versiossa. Siksi tilatonta NAT64:ta käytetään harvemmin. Se soveltuu kuitenkin esimerkiksi IPv6-palvelun eteen, sillä sen avulla voidaan ottaa yhteyttä NAT64-reititimen takana olevaan IPv6-palveluun IPv4-verkosta, toisin kuin tilallisesti NAT64:ssa, jossa yhteydet eivät voi aueta IPv6-verkkoon IPv4-verkosta. [17]

Keskustelu NAT64-protokollan käänteisestä protokollasta NAT46:stä on noussut aika ajoin esille, mutta siitä ei ole ainakaan vielä tullut virallista protokollaa tai standardia. Siinä olisi samanlaiset ominaisuudet kuin NAT64:ssa, mutta päinvastaisesti, mukaan lukien DNS46. Jotkin laitevalmistajat ovat tuoneet tämäntyyppisiä ominaisuuksia laitteisiinsa, mutta näillä ei vaikuttaisi olevan mitään vakiintunutta toteutustapaa. Tämän protokollan standardointi tulee todennäköisesti eteen tulevaisuudessa, kun siirtymävaihe on edennyt ja IPv4-verkot alkavat olemaan harvemmassa, kun palvelut ja laitteet ovat siirtyneet pelkästään käyttämään IPv6:a ja vain vanhemmat laitteet sekä verkot käyttäisivät enää IPv4:a. Tällöin näiden IPv4-laitteiden tulisi pystyä yhdistymään IPv6-palveluihin. Tähän on jo nyt muitakin tapoja, joten ehkä siksi keskustelu NAT46:sta ei ole tuottanut siitä protokollaa.

464XLAT on oikeastaan NAT64 laajennos, jossa ei välttämättä tarvita ollenkaan DNS64:ta. Se on kehitetty, koska kaikki palvelut eivät toimi IPv6:lla vaan tarvitsevat IPv4-osoitteen. 464XLAT yhdistää sekä tilattoman ja tilallisen osoitteenmuutoksen. Siinä käytetään NAT64-verkkoa ja asiakkaan laitteella olevaa CLAT-toimintoa, jonka avulla laitteen sisällä IPv4-osoitetta käyttävä palvelu keskustelee IPv4:lla, mutta fyysiseen IPv6-verkkoon siirryttäessä, tapahtuu osoitteen muutos IPv6:ksi. Näin palvelu toimii IPv6-ver-

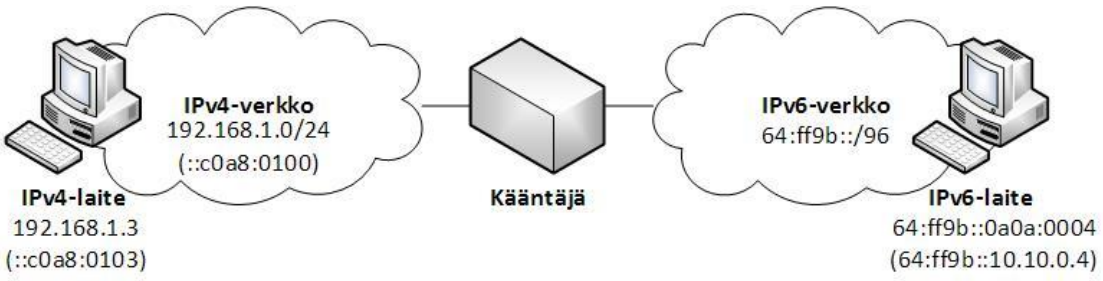
kossa ja yhdistyy NAT64:n avulla IPv4-internetiin. Koska palvelu keskustelee itse pelkästään IPv4:lla, ei tarvitse DNS-kyselyn A-tietuetta muuttaa DNS64:n avulla AAAA-tietueeksi. 464XLAT nimi on melko kuvaava, sillä aluksi IPv4-osoite muutetaan IPv6-muotoon ja tämä taas takaisin IPv4-osoitteeksi. Tästä johtuen vain viimeisen IPv4-osoiteen tarvitsee olla globaali, joka säästää huomattavasti IP-osoitteita. Tämä protokolla on myös suosittu mobiiliverkoissa, sillä vieläkin moni puhelinsovellus ei tue kuin IPv4-vistintää.[18]

3.1.4 Tilaton osoitteenmuutos

Stateless IP/ICMP translation (SIIT) eli tilaton IP/ICMP-muutos on siirtymätekniikka, jolla saadaan osoitteenmuutoksella yhdistettyä IPv4- ja IPv6-verkot. Jotta tämän tyyppinen muutos on mahdollista, täytyy laiteiden osoitteiden ja IP-verkkoavaruuksien olla tähän sopivat, varsinkin IPv6-osoitteden osalta, jotta IPv6-osoite saadaan muutettua IPv4-osoitteeksi. Tämän takia kannattaa jo verkon suunnitteluvaiheessa ottaa huomioon, jos aiotaan käyttää SIIT-menetelmää.

Kääntäjä tekee tarvittavat osoitteen ja paketin kehyksen muutokset, jotta saa yhdistettyä kahden eri IP-protokollan version verkot toisiinsa. Kääntäjä pystyy muokkaamaan myös muitakin kuin IP-kehyksiä. Se pystyy muuttamaan ICMP-protokollan versiota neljän ja kuuden välillä sekä tekemään tästä johtuvat kenttien muutokset, esim. tarkistussumman uudelleen laskeminen.

Kuva 3 on esimerkki verkosta, jossa käytetään SIIT-menetelmää. Tässä verkossa tarvitsee olla oikeastaan kolme osoiteavaruutta: yksi IPv4-avaruus IPv4-verkolle ja sen laitteille, tässä 192.168.1.0/24; yksi IPv6-osoite avaruus, joka voi olla vain /32, /40, /48, /56, /64 tai /96, tässä 64:ff9b::/96; ja yksi IPv4-avaruus IPv6-laitteiden osoitteiksi mahdollistamaan helppo osoitteen muutos, tässä 10.10.0.0/24. Tämä viimeinen IPv4-osoiteavaruus muutetaan tietysti heksadesimaali muotoon eli ::0a0a:0000, josta viimeiset kaksi merkkiä on varattu IPv6-laitteiden identifiointiin, esim. tässä verkossa IPv6-laitteen osoite on 64:ff9b:0a0a:0004. Kohta johon tämä IPv4-etuliite sijoitetaan IPv6-etuliitteessä, riippuu IPv6-etuliitteen pituudesta: IPv6-osoitteesta on varattu bitit 64-71 yhteensopivuudeksi laitteiden tunnistamismenetelmän kanssa, alussa on verkon etuliite osa sekä niin paljon IPv4-etuliitteestä kuin mahtuu ennen bittiä numero 64 ja loppu etuliitteen osa heti bitin 71 jälkeen, jos tämä katkennut. /96 etuliite on tästä poikkeus, sillä siinä on vain IPv6- ja IPv4-etuliitteet. IPv6-etuliitteinä voisi tässä käyttää esimerkiksi ::ffff:0:0/96 tai ::ffff:0:0:0/96, jotka ovat nimenomaan tarkoitettu IPv4-muunnokseen. Myös kuvassa käytetty 64:ff9b::/96 on hyväksytty tähän tarkoitukseen. Tietysti organisaatio voi käyttää omaa etuliitettään ylläolevat rajoitukset huomioiden. [19]

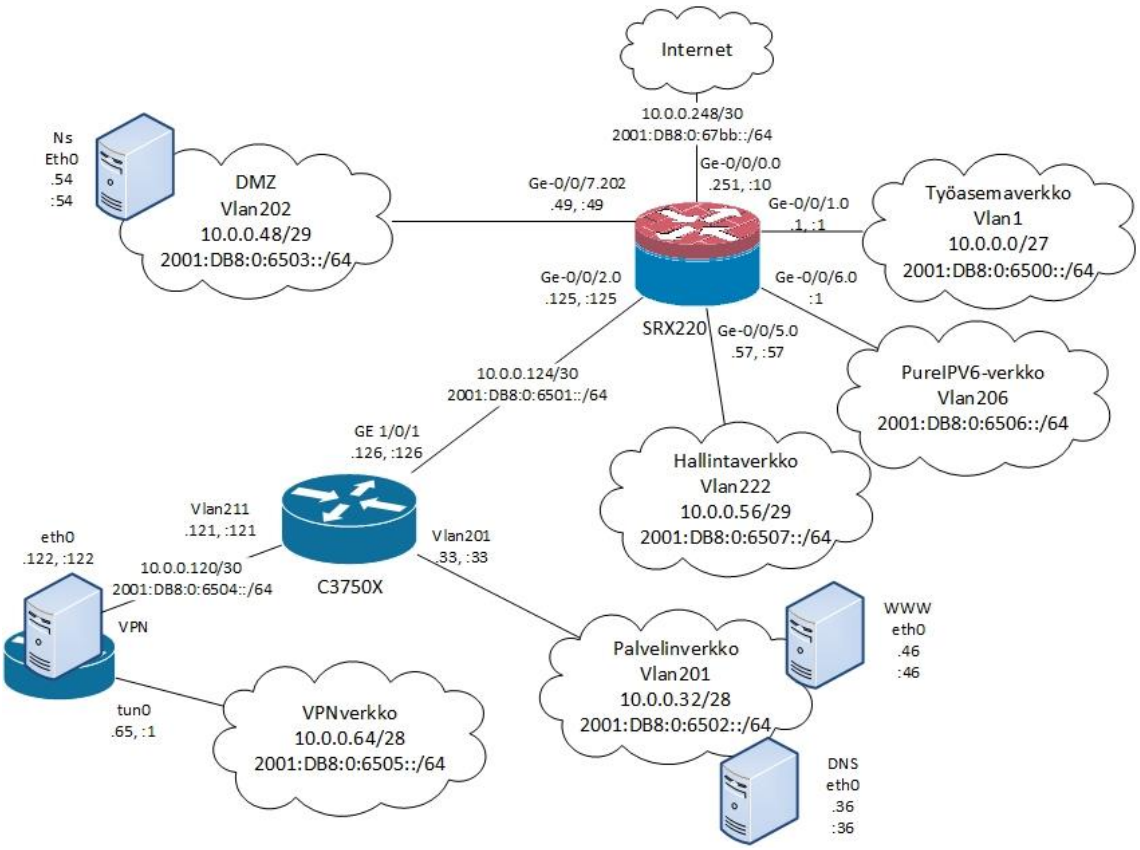


Kuva 3. *Yksinkertainen toteutus SIIT-verkosta*

Kun kuvan 3 IPv6-laite haluaa lähettää viestin IPv4-laitteeseen, se muuttaa kohdelaitteen IPv4-osoitteen IPv6-muotoon eli 192.168.1.3 aluksi heksadesimaaliksi ::c0a8:0103 ja liitetään tämä IPv6-etuliitteensä, jolloin lopullinen kohdeosoite on 64:ff9b::c0a8:0103. IPv6-laite lähettää paketin eteenpäin ja se päätyy kääntäjälle, joka purkaa paketin IPv6-kehyksen, muuttaa lähettäjän IPv6-osoitteen IPv4-osoitteeksi, eli osoitteesta 64:ff9b::0a0a:0004 poistetaan etuliite, jolloin jää ::0a0a:0004, ja tämä desimaali muodossa on 10.10.0.4, sekä vastaanottajan osoite takaisin IPv4-muotoon, ja lisätään uusi, käännetyillä osoitteilla muodostunut IPv4-kehys. Samalla kääntäjä muuttaa kehyksen muitakin arvoja, jotta ne olisivat oikein uudella paketilla, esim. tarkastussumma lasketaan uudelleen tarvittaessa. Tämän jälkeen paketti matkaa vastaanottajalleen, joka tietysti lähettää vastauspaketin IPv6-laitteille. Tämä matkaa samalla tavalla kääntäjän kautta, mutta muutokset pakettiin tapahtuvat käänteisesti. Jos taas yhteyden avaa IPv4-laite, tapahtuvat samat vaiheet kuin edelläkin, mutta kohteen osoite muutetaan IPv6-muodosta IPv4-muotoon. Tämä tapahtuu poistamalla kohteen IPv6-osoitteesta verkon etuliite eli 64:ff9b:0a0a:0004 muuttuu muotoon ::0a0a:0004, joka taasen on desimaalimuodossa 10.10.0.4. Näin on saatu viestille IPv4-kohdeosoite. Tämän jälkeen viestintä tapahtuu samoin kuin yllä eli paketti siirtyy kääntäjälle, joka tekee IPv4/IPv6-muutoksen ja välittää paketin vastaanottajalle, minkä jälkeen paluupaketti tekee kaiken tämän käänteisenä. [20]

3.2 Testiympäristön esittely

Tätä työtä varten rakennettiin testiverkko, jossa pystyttiin testaamaan joitakin työn tekniikoita ja yleisesti IPv6:n toimintaperiaatteita. Samalla testattiin reitittimien ja asennettujen palvelujen eri IPv6-ominaisuuksia sekä palomuurausta, josta on enemmän kappaleessa 5.2. Verkko toteutettiin dual stack-tekniikalla, eli verkon laitteilla ja palveluilla oli sekä IPv6- että IPv4-osoite. Verkossa oli myös pelkästään IPv6:ta käyttävä alue. Verkon looginen rakenne löytyy Kuva 4. Verkon IP-alueet on tietoturvallisuussyistä muutettu dokumentaarisiin alueisiin 10.0.0.0/25 ja 2001:DB8:0:6500::/56 alkuperäisistä julkisista osoiteavaruuksista.



Kuva 4. *Labraverkon looginen kuva*

Verkko koostui kolmesta aktiivilaitteesta: Juniper SRX220 -palomuurireititin, Cisco C3750X ja C3750-kytkimet, jotka pystyivät käsittelemään myös OSI-mallin kolmannen tason protokollia ja reitittämään. Kuitenkin C3750 toimi vain perinteisenä OSI-kerroksen kaksi kytkimenä, joten se ei näy Kuva 4. SRX220 käytti ohjelmistoversiota 12.1X46-D15.3 ja C3750X versiota 12.2(44)SE laajimmalla IP services -lisenssillä, missä oli tuki IPv6:lle. Käytössä oli myös työasemia, jotka sai kytkettyä haluttuihin aktiivilaitteiden portteihin. Nämä käyttivät BackBox-linux käyttöjärjestelmää, joka on tarkoitettu tietoturvatestaukseen ja pohjautuu Ubuntu-linux käyttöjärjestelmään. Näiden avulla saatiin testattua verkon toimivuutta eri verkkoalueista.

Verkkoon oli kytkettynä ristikytkennän kautta VMware vSphere -virtuaalikonepalvelin, jossa oli asennettuna Ubuntu server 14.04 -käyttöjärjestelmän palvelimia. Palvelimet olivat seuraavat: autoritäärinen nimipalvelin Ns, joka käytti Bind-ohjelmaa palvelun tuottamiseen; Unbound-ohjelmalla toimiva resolveri nimipalvelin DNS; Apache-webpalvelin WWW; OpenVPN-ohjelmalla toimiva virtual private network -palvelin (vpn) VPN.

SRX220 toimi verkon pääreitittimenä, pääpalomuurina sekä yhteytenä ulkomaailmaan. Se hoiti hallintaverkon, työasemaverkon, pureIPv6-verkon sekä DMZ-alueen eli demilitarized zone (DMZ) reitityksen. C3750 oli yhdistettynä SRX:ään kahdella kaapelilla ja se toimi työasemaverkon sekä pureIPv6-verkon liityntäkytkimenä jakaen puolella porteis-

taan työasemaverkkoa ja toisella puolella pureIPv6-verkkoa. C3750X toimi palvelinverkon reitittimenä ja yhteytenä VPN-palvelimelle. Ciscon laitteille tarvitsi antaa komento *sdm prefer dual-ipv4-and-ipv6 default*, jotta nämä ymmärsivät IPv4:n lisäksi IPv6:ta. Juniper toimi jo oletuksena dual stack -tilassa.

Juniper SRX220 ja Cisco C3750X käyttivät keskenään reittien vaihtamiseen OSPF- ja OSPFv3-protokollia. Nämä toimivat moitteettomasti ja olivat helppo asettaa. SRX:lle oli asetettu staattiset reitit ulos verkosta ja tämän vastalaitteelle myös staattisesti paluureitit testiverkkoon. Työasemaverkossa testattiin myös SLAAC:n toimivuutta, mikä onnistui hyvin, laitteet osasivat luoda itselleen osoitteet ja saivat reitittimen osoitteen itselleen. Nimipalvelimen osoitetta ei SLAAC:lla saa työasemille automaattisesti vaan tämä piti syöttää käsin.

Molemmilla reitittimillä ajettiin myös DHCP- ja DHCPv6-palvelinta, mutta täydellinen tilallinen DHCPv6-palvelin ei ollut tuettuna kummallakaan laitteella. DHCPv6-palvelimet jakoivat IPv6-osoitteita ja nimipalvelimen osoitetta sekä RA-viestin avulla reitittimen osoitetta. Vaikka molemmille sai DHCP- ja DHCPv6-palvelimet toimimaan, ne eivät kuitenkaan olleet luotettavia, sillä kun reitittimet olivat olleet pitkään käynnissä ne eivät enää jakaneetkaan vastauspaketteja tai vastasivat vasta kymmenenteen pyyntöön ja tällöinkin todennäköisesti vain toisen IP-protokollan version -osoitteella. Lisäksi kumpikaan DHCPv6-palvelimista ei tukenut staattisia IPv6-osoitteita asiakkaille, vaan nämä määräytyivät aina numerojärjestyksestä seuraavana vapaana olevaksi.

Käytetyt nimipalvelut kuten muutkin palvelut oli konfiguroitu molemmilla osoitteilla eli IPv4- sekä IPv6-osoitteella. Nimipalvelut toimivat hieman vaihtelevasti, välillä toimien moitteettomasti molemmilla IP-versioilla, mutta välillä ei kummallakaan tai vain toisella. Autoritäärinen nimipalvelin vaikutti toimivan hieman luotettavammin kuin resolveri. Web-palvelu toimi taas aivan toisin eli oli koko ajan saatavissa molemmilla versioilla ja se oli vielä helppo konfiguroida toimivaksi molemmilla IP-protokollan versioilla.

Samaa ei voi sanoa OpenVPN-palvelimesta. IPv4-vpn-palvelin toimi hienosti ja asiakkaan päässä kaikki liikenne kulki tunneliin. IPv6-liikenne kulki myös tähän tunneliin ja toimi oikein. Vaikeudet alkoivat, kun yhdistettiin IPv6-vpn-palvelimeen. Asetuksia muuttamalla saatiin kaikki liikenne kulkemaan muodostuneeseen vpn-putkeen, mutta mitään ei mennyt perille asti. Toisilla asetuksilla saatiin IPv4-liikenne toimimaan IPv6-putkessa ja testiverkon IPv6-osoitealueen liikenne, mutta muualle kohdistunut liikenne kulki putken ohitse. Tämä vaikutti selvästi reititys ja asetusongelmista, mitä ei saatu ratkaistua verkon testijakson aikana.

Lopuksi testattiin verkon palomuurausta molemmilla reitittimillä. Juniper SRX220 toimi alueisiin perustuvana palomuurina, jossa oli kaksi aluetta: sisäverkko ja ulkoverkko. Ulkoverkko oli testiverkon ulkopuolinen verkko eli internet ja sisäverkko koko muu testi-

verkko. Näitä alueita olisi voinut tehdä enemmänkin, mutta tämä oli riittävä ominaisuuksien testaamiseen ja näin vältyttiin monimutkaisilta palomuuraussäännöiltä. Suodatuksen pääperiaatteena oli, että sisäverkossa sai liikennöidä vapaasti, mutta ulkoverkosta sisäverkkoon vain WWW-, Ns- ja VPN-palvelimille. Ciscon C3750X käytti pääsylistoja suodattaakseen liikennettä. Tämä oli hankalaa kerran laite ei tukenut refleksiivisiä listoja IPv6:lle. Lisää testiverkon palomuureista käydään kappaleessa 5.2, jossa verrataan näitä kahta muuria ja Palo Alton palomuuria keskenään.

3.3 Yleisiä havaintoja dual stack -verkoista ja testiverkosta

Yleisesti dual stack-verkkoa pidetään helpoimpana vaihtoehtona ottaa IPv6-protokolla käyttöön. Sen käyttöönotossa on kuitenkin omat hankaluutensa, kuten huomattiin testiverkossa. Kaikki näytti toimivan aluksi, mutta tarkemmin tarkasteltuna tai hetken ajankuluttua ongelmia alkoi ilmenemään. DNS-nimipalvelut olivat epävakaita eivätkä aina vastanneet kyselyihin molemmilla IP-protokollan versioilla. DHCP-palvelimissa oli myös ongelmia, varsinkin pitkän päällä olon jälkeen. Ne eivät enää vastanneet kyselyihin tai vastauksessa kesti kauan.

Nämä voivat johtua vanhemmista laitteista ja vanhemmista ohjelmistoversioista tai verkon konfiguraatioista. Uudemmilla laitteilla ja ohjelmistoilla ei välttämättä samanlaisia ongelmia olisi ilmennyt tai jos verkko olisi rakennettu hieman toisin tai uudelleen.

Testiverkon työasemat halusivat välttämättä IPv4-osoitteen ja yhteyden IPv4-verkkoon, tai muuten ilmoittivat, ettei yhteyttä verkkoon. Työasemalle ei riittänyt, että sillä oli toimiva IPv6-osoite ja yhteys IPv6-internetiin. Tämä saattoi olla kyseisen linux-käyttöjärjestelmän ominaisuus tai mahdollisesti myös muissa käyttöjärjestelmissä olisi ollut samoja ongelmia.

Työasemilla saattoi olla myös useita IPv6-osoitteita yhdellä portilla. Pahimmassa tapauksessa portilla oli kahdeksan eri IPv6-osoitetta, joista seitsemän oli julkisia osoitteita, mistä osa oli saatu DHCPv6 kautta ja osa vanhoja SLAAC:lla muodostuneita osoitteita, jotka eivät olleet poistuneet uudelleenkäynnistyksen yhteydessä. Tässä huomattiin, että DHCP ja RA-mainostusten kanssa tarvitsee olla tarkkana. Testiverkon ulkopuolella on havaittu yleisesti samaa, että laitteella saattaa portissa olla useampi IPv6-osoite, jotka ovat muodostuneet SLAAC:n avulla.

Testiverkonkin ulkopuolella on havaittu, että monissa verkoissa on IPv6-protokolla oletuksena päällä, mutta sitä ei ole mitenkään palomuureilla rajattu. Tällöin pystyy lokaaleja IPv6-osoitteita käyttämään lähiverkon laitteisiin yhdistämiseen vaikka tämä ei olisi aina sallittua IPv4-osoitteilla.

Yleisesti on havaittu dual stack -verkoissa, että kaikkia palveluja ei aina ole saatavilla sekä IPv4- että IPv6-protokollalla. Usein on käynyt niin, että IPv6-palvelu on jäänyt epähuomioissa tai jopa tarkoituksella konfiguroimatta. On tullut myös vastaan dual stack -verkkoja, joista vain IPv4:llä on päässyt sisäverkon ulkopuolelle. Tämä on johtunut usein siitä, ettei internetpalveluntarjoaja ole tarjonnut IPv6-yhteyttä organisaatiolle. Tällöin on myös usein muutkin siirtymätekniikoiden suomat mahdollisuudet jätetty käyttämättä ja käytetty IPv6:ta vain sisäisten palvelujen tarjoamiseen.

Testiverkkoa käyttämään ja konfiguroimaan päästettiin myös muita opiskelijoita, jotta saataisiin pieni otanta, miten verkonhaltijat käsittelisivät IPv6-protokollaa. Opiskelijoita oli 18 kappaletta ja he muodostivat kolmen hengen ryhmiä, joista jokainen muokkasi ja käytti verkkoa halutulla tavallaan. Tämä oli osa verkon tietoturva -kurssia.

Opiskelijat eivät löytäneet aluksi ollenkaan pelkästään IPv6:ta käyttävää verkkoa ja he eivät dokumentoineet IPv6-osoitteita eivätkä IPv6-verkkoja. Kun he tekivät verkkoon muutoksia, suurimmalla osalla IPv6 unohdettiin kokonaan. Uudet palvelut eivät saaneet IPv6-vastinetta IPv4-palvelulle ja palomuuraussääntöjen lisäyksiä ei tehty IPv6:lle. Yhdessä tapauksessa IPv6 estettiin kokonaan verkossa palomuurilla ja IPv6-osoitteet poistettiin. Jos joitain muutoksia tehtiin IPv6-verkkoihin, näiden reititys unohdettiin useimmiten kokonaan.

4. IPV6-HYÖKKÄYKSIÄ JA NIIDEN TORJUNTA

IPv6-protokolla toi mukanaan uusia mahdollisuuksia tehdä erilaisia hyökkäyksiä. Tässä kappaleessa käydään läpi näitä uusia ja tunnettuja IPv6-hyökkäyksiä sekä mahdollisuuksia torjua niitä. Lisäksi käydään läpi kunkin hyökkäyksen kohteet sekä toimintaperiaatteet. Monen näiden hyökkäysten torjunta haittaa normaalia IPv6:n toimintaa tai osaa sen ominaisuuksista kuten esimerkiksi SLAAC:n toimintaa. Lähes jokainen hyökkäyksistä on mahdollinen vain hyökkääjän laitteen ollessa kohdeverkossa eli tehokkaimmat tällaisen hyökkäyksen estokeinot ovat tilojen hyvä pääsynhallinta sekä verkon yleinen tietoturvallisuus ja palomuuraus.

4.1 Ryhmälähetyshyökkäykset

Ryhmälähetyksiä voidaan käyttää hyökkäystarkoituksessa helposti tai niiden avulla voi löytää verkosta mahdollisia hyökkäyskohteita. Ryhmälähetyshyökkäyksissä hyökkääjän tulee olla itse verkossa, jotta nämä onnistuisivat, koska ryhmälähetyksiä ei reititetä. Näiden hyökkäysten kohteena voivat olla yksitäiset laitteet, verkon reititin tai koko aliverkko. Hyökkäykset ovat palvelunestohyökkäyksiä lukuun ottamatta laitteiden nuuskintaa.

Hyökkääjä pystyy löytämään verkosta laitteita yksinkertaisella ryhmälähetys ping-komennolla. Ping-kysely lähetetään tässä IPv6:n kaikki solmut -ryhmälähetysosoitteeseen eli ff02::1. Tähän vastaavat kaikki laitteet omalla lokaalilla IPv6-osoitteellaan, jos tätä ei ole estetty laitteen asetuksissa. Näin hyökkääjä saa listaa verkkoon kytketyistä laitteista. Hyökkääjä voi käyttää tässä myös kaikki reitittimet- tai kaikki DHCP-palvelimet -ryhmälähetysosoitteita. [21]

Smurf-hyökkäyksessä käytetään ryhmälähetystä niin, että lähetetään echo request -paketteja hyökkäyksen kohteen osoitteen ollessa lähettäjänosoite. Vastaanottajaksi näihin paketteihin laitetaan kaikki solmut -osoite. Kun tämä paketti lähetetään verkkoon, kaikki laitteet vastaavat kohteelle. Mitä enemmän aliverkossa on laitteita, sitä enemmän paluupaketteja hyökkäyksen kohde vastaanottaa. Kun hyökkääjä lähettää näitä paketteja suurella taajuudella myös paluupakettien määrä lisääntyy. Jossain vaiheessa verkon tai vastaanottajan kapasiteetti ei enää riitä ja syntyy palvelunesto. Hyökkäys voi ilmentyä myös merkittävänä verkkoyhteyden hitautena kaikilla aliverkon laitteilla. Hyökkäystä voidaan tehostaa kasvattamalla lähetettyjen pakettien kokoa. [6] Hyökkäys on melko helppo estää kieltämällä verkossa echo request -paketit ryhmälähetysosoitteilla, näihin vastaamisen kieltäminen laitteilla tai kokonaan echo request -kyselyihin vastaamisen kieltäminen.

Smurf-hyökkäyksestä on olemassa myös käänteinen versio, jossa lähetetään myös echo request-paketteja. Tässä lähettäjänosoitteena on ff02::1-ryhmälähetysosoite ja vastaanottajana hyökkäyksen kohde. Tässä hyökätään lähinnä verkkoa vastaan, koska paketteja

tulee helposti paljon. Hyökkääjän lähetettyihin paketteihin kohde vastaa ja lähettää nämä vastauspaketit ryhmälähetysosoitteeseen. Näihin paketteihin kaikki verkon laitteet vastaavat virheviestillä. Kun hyökkääjä lähettää paketteja tarpeeksi nopeasti, on kohde verkko nopeasti täysin tukossa. Tämä käänteinen smurf -hyökkäys on nykyisin hankala toteuttaa, koska laiteille ja ohjelmistoille on jo valmiiksi asetettu, että jos lähettäjänä on ryhmälähetysosoite ei viestiin vastata tai välitetä eteenpäin, jos kyseessä verkon aktiivilaite. [21] Muuten tämän hyökkäyksen torjunta toimisi samoin kuin normaalinkin smurf-hyökkäyksen.

Viimeinen ryhmälähetyshyökkäys on tulvahyökkäys, jossa lähetetään ping-paketteja ryhmälähetysosoitteen ollessa sekä lähettäjänä että vastaanottajana. Tällöin kaikki laitteet vastaisivat ryhmälähetysosoitteelle, joihin kaikki vastaisivat toisilleen virheviesteillä. Tämä tuottaa todella paljon viestejä, ja jo pienellä määrällä hyökkääjän lähetyksiä verkkoon tulee suuri kuorma. Tämä ei nykyisin ole enää oikeastaan mahdollista samasta syystä kuin käänteinen smurf-hyökkäys eli ryhmälähetysosoitetta ei hyväksytä lähettäjänosoitteeksi.

4.2 ICMPv6-spooffaukset

ICMPv6-spooffaus eli ICMPv6-viestien väärentäminen on hyökkäystapa suurelle joukolle erilaisia hyökkäyksiä. Tässä käytyjen hyökkäysten yhdistävänä tekijänä on SLAAC:n toimintaan tarvittavat viestityypit eli RA, RS, NA ja NS sekä se, että hyökkäävän laitteen tarvitsee olla kohdeverkossa.

RA-spooffausta on kolmea erilaista. Ensimmäisessä hyökkääjä lähettää virheellisiä RA-viestejä. Jos verkon laite kuuntelee näitä viestejä ja käyttää SLAAC:a osoitteensaamiseksi, vaihtaa se osoitteensa tai oletusyhdyskäytävänsä osoitteen. Tällöin hyökkääjä voi toimia miehenä välissä tai estämään IPv6-internetiin pääsyn. Tämän hyökkäyksen kohteena on nimenomaan verkossa olevat tietokoneet ja laitteet.

Toisessa RA-hyökkäyksessä kopioidaan verkon reitittimen RA-viesti ja muutetaan sitä hieman. Muutettava kenttä on voimassaoloaika ja tämä muutetaan nollaksi tai muuksi pieneksi luvuksi. Tällainen muutettu viesti lähetetään aina heti, kun hyökkääjä havaitsee reitittimen lähettävän vastaavanlaisen viestin. Tällöin verkon laitteet päivittävät oman reititystaulunsa virheellisellä eliniällä, joka umpeutuu lähes välittömästi. Tämän vuoksi laitteet eivät voi viestiä IPv6-internetiin.

Kolmas RA-spooffaus on RA-tulva, jolla saadaan kaikille verkon solmuille tehtyä nopeasti palvelunestohyökkäys. Tässä lähetetään muokattuja ja toisistaan poikkeavia RA-viestejä nopealla tahdilla verkkoon. Jokainen vastaanotettu RA-viesti pakottaa laitteen luomaan itselleen uuden osoitteen ja päivittämään reititystaulua. Kun paketteja on lähetetty jonkin aikaa, on hyökkäyksen kohteilla todella paljon eri IPv6-osoitteita ja reititystaulut ovat kasvaneet valtaviksi. Osoitteiden luominen ja reititystaulun päivittäminen käyttää

yllättävän paljon prosessoria, mikä alkaa hidastamaan laitteita tai ainakin näiden verkon käyttöä, ja lopulta laite ei pysty enää toimimaan. [21]

RA-hyökkäysten estona voidaan käyttää staattisia osoitteita tai käytetään tilallista DHCPv6-palvelinta. Tietysti verkon kytkimellä tai laitteilla voidaan sallia vain RA-viestit tietyiltä tunnetuilta lähteiltä.

ND-spooffaus käyttävät hyväkseen NA-viestejä, jonka avulla saadaan toteutettua palvelunestohyökkäys tai mies välissä -tilanne. Hyökkäyksen kohteena on yleensä verkon laite, mutta voi olla myös reititin. Hyökkääjä kuuntelee verkon liikennettä ja kun havaitsee NS-viestin, vastaa tähän välittömästi virheellisiä tietoja sisältävällä NA-paketilla, jossa MAC-osoitteena on hyökkääjän oma MAC-osoite. Tämä vastauksen tarvitsee olla perillä ennen oikeaa NA-vastausta, jotta hyökkäyksen kohde hyväksyy hyökkääjän paketin oikean sijaan. Näin saadaan kohteen osoitetauluun hyökkääjän syöttämät tiedot. Tässä tilanteessa kaikki tiettyyn osoitteeseen tarkoitetut paketit tulevatkin hyökkääjälle. Jos hyökkääjä saa vielä viestinnän toisenkin osapuolen osoitetauluun omat tietonsa, liikennöinti kahden kohteen välillä saadaan kulkemaan hyökkääjän kautta. Tässä tilanteessa hyökkääjä voi välittää viestit ja toimia miehenä välissä tai tuhota viestit sitä mukaan, kun ne saapuvat, jolloin tapahtuu palvelunesto. [21]

Tämän hyökkäyksen kohteena reititin on hankalampi tapaus, koska reititin säilyttää IPv6-/MAC-osoite -pareja kauemmin omassa taulussaan. Tällöin hyökkääjän tietojen soluttaminen vie pidemmän aikaa, koska hyökkäystä ei voi käyttää ennen kuin osoiteparien voimassaoloaika on mennyt umpeen tai lista on täyttynyt ja vanhimmat merkinnät poistetaan uusien tieltä. Tätä voidaan nopeuttaa jollain muulla hyökkäyksellä tai yksinkertaisesti vain odottaa. Kun hyökkääjä on saanut kaikki aliverkon laitteiden MAC-osoitteet muutettua itselleen, voidaan jäädä tähän ja tehdä vain palvelunesto. Toisaalta viestit reitittimeltä laitteille kulkevat jo hyökkääjän kautta, joten jos tehdään vielä RA-hyökkäys, niin saadaan täydellinen mies välissä-hyökkäys aliverkkoon eli kaikki liikenne kulkisi hyökkääjän laitteen kautta. [21]

NA-spooffaus voidaan toteuttaa myös niin, että annetaan NA-vastauksessa keksitty MAC-osoite. Tällöin kohde ei voi viestiä ollenkaan haluamalleen laitteelle tällä IPv6-osoitteella.

Duplicate address detection denial of service (DAD-DOS) eli duplikaatti osoitteiden havaitsemista hyväksikäyttävä palvelunestohyökkäys on kohdistettu verkkoon liittyville uusille laitteille. Jotta hyökkäys toimisi, tulee verkossa olla käytössä SLAAC osoitteiden jakamista varten sekä hyökkääjän olla läsnä verkossa. Kun uusi laite liittyy IPv6-verkkoon ja luo itselleen IPv6-osoitteen SLAAC:n avulle, se kysyy, onko osoite jo käytössä. Tähän kyselyyn hyökkääjä lähettää aina vastauksen. Hyökkääjällä on kaksi vaihtoehtoa vastaukselle, joko NS-viesti, jolloin hyökkääjä olisi luomassa myös mukamas itselleen

samaa osoitetta kuin hyökkäyksen kohteella, tai NA-viestillä, jolloin hyökkääjä vain ilmoittaa, että osoite jo käytössä. Kun tämä suoritetaan jokaiselle DAD-kyselylle, ei verkkoon liittynyt laite saa itselleen koskaan IPv6-osoitetta ja hänen IPv6-palvelu on estetty. [22] DAD-DOS voidaan mahdollisesti estää käyttämällä kiinteitä osoitteita tai DHCPv6:a osoitteiden jakamiseen.

DAD-DOS:a voidaan käyttää myös yrityksenä sammuttaa verkon aktiivilaitteen jokin tietty portti tai IPv6-osoite. Tässä hyökkääjä ilmoittaa DAD-viestillä, että hänellä on käytössä aktiivilaitteen portin IPv6-osoite. Aktiivilaitteen osoite on staattisesti asetettu, joten sille ei jää muuta vaihtoehtoa kuin sammuttaa porttinsa väliaikaisesti. Tämä on kylläkin helppo torjua estämällä tämä sammuminen ja DAD-menetelmän käyttö aktiivilaitteessa. [6]

Kaikkien ICMPv6-hyökkäysten täydellinen torjuminen on todella hankalaa, jollei halua konfiguroida kaikkea käsin IPv6-osoitteista aina naapuruuslistan tekemiseen asti. Tämä johtuu siitä, että IPv6 nojaa niin vahvasti ICMPv6:n ominaisuuksiin. Osan hyökkäyksistä pystyy torjumaan kytkimelle sijoitetulla palomuurilla ja vielä suuremman osan, jos siellä pyörii hyökkäyksen tunnistus ja torjunta -palvelu. ICMPv6-viestittelyn turvaamiseen voidaan käyttää myös ehdotettua Secure neighbor discovery (SEND) -menetelmää, jossa laitteet eivät hyväksy ND-protokollan viestejä kuin tietyn sertifikaatin omaavilta laitteilta. [21]

4.3 Etä-ND-DOS

Etä-ND-DOS on etäältä tehtävä ND-mekanismia käyttävä palvelunestohyökkäys. Tämän hyökkäyksen kohteena on tietyn osoiteavaruuden reititin, jonka toiminta ja muiden asiakkaiden palvelu yritetään estää. Esimerkkinä kohteesta on 2001:db8:10::/64-etuliitteen reititin.

Hyökkääjä luo ja lähettää paketteja, joiden vastaanottajina on kohdeverkon keksittyjä osoitteita, esim. 2001:db8:10::cafe ja 2001:db8:10::1337. Tällaisia paketteja ja osoitteita luodaan suurella tahdilla. Kun paketti saapuu kohdeverkon reitittimelle, reititin joutuu lähettämään verkkoon NS-viestin, jotta se saisi selville vastaanottajan laitteen. Koska osoitteet ovat keksittyjä, ei vastausta tähän kyselyyn tule. Reititin joutuu odottamaan vaaditun ajan ennen kuin toteaa, ettei vastaanottajaa ole olemassa. Hyökkäyksessä tällaisia paketteja saapuu reitittimelle nopealla tahdilla, mikä aiheuttaa sen, ettei normaali yhteydenmuodostaja pääse muodostamaan yhteyttä omaan kohteeseensa. [22]

Tämän hyökkäyksen torjunta on melko hankalaa. Yksi torjunta tapa olisi sallia vain tiettymäärä aktiivisia NS-viestejä, jotka odottavat vastausta, ja hylätä tämän ylittävät viestit. Toinen tapa olisi sallia yhteydet vain tiettyihin osoitteisiin ja jos kohdeosoite olisi muu, niin se hylättäisiin eikä NS-viestejä muodostuisi.[22]

4.4 Lisäotsikkohyökkäykset

IPv6 toi mukanaan uuden ominaisuuden, lisäotsikot. Protokollan spesifikaatio ei rajoita näiden käyttöä eli ne ovat oiva työkalu hyökkääjälle. Yksi hyökkäystapa lisäotsikoilla on tehdä todella pitkä ketju lisäotsikoita yhteen lähetettävään pakettiin, mikä on täysin sallittua protokollan näkökulmasta. Tämän paketin käsittelevälaite voi tukahtua käsitellessään sitä, varsinkin jos laite on vanhempi tai vähemmän tehoja omaava. Tällainen paketti voi toimia jo itsenään palvelunestävänä, mutta suuret määrät näitä viimeistään.

Pitkillä lisäotsikkoketjuilla voidaan huijata myös palomuureja päästämään paketit suojauksen sisälle virheellisesti. Tämä onnistuu varsinkin, kun paketti lähetetään pilkottuna, jolloin palomuuri käsittelee vain ensimmäisen ilmentymän paketista ja sallii tämän, koska ei löydä mitään virheellistä tai vaarallista paketista. Kun ensimmäinen paketinosa on mennyt onnistuneesti palomuurin lävitse, toinen paketinosa päästetään tarkistamatta läpi, koska kuuluu samaan viestiketjuun. Tämä toimii varsinkin yksinkertaisemmilla palomuureilla, jotka voivat jo hämmentyä pelkästä lisäotsikoiden pituudesta.

Tällaiset hyökkäykset voidaan torjua suodattamalla palomuurissa kaikki ei toivotut lisäotsikot pois tai sallitaan vain yksi esiintyminen jokaista lisäotsikkotyyppiä. Suodattaminen voidaan toteuttaa myös jokaisessa pakettia käsittelevässä laitteessa matkalla, joka aiheuttaa paketin verkon läpäisyyn ylimääräistä viivettä. Jos tätä suodatusta ei tehdä, voi paketin vastaanottajan verkkoportti tai käyttöjärjestelmä mennä vastaamattomaan tilaan pitkän lisäotsikkoketjun käsittelystä tai jopa otsikko on voinut sisältää haitallista koodia. [6]

Lisäotsikoita voidaan vielä käyttää moniin erilaisiin hyökkäyksiin ja uusia hyökkäyksiä tulee myös lisää. Erilaisilla lisäotsikkohyökkäyksillä saadaan ohitettu palomuureja sekä tehtyä palvelunestoja. Lähes jokaista lisäotsikkoa voidaan käyttää myös yksistään hyökkäystyökaluna. [21]

4.5 DHCPv6-hyökkäykset

DHCPv6-palvelinta vastaan on myös hyökkäyksiä. Ensimmäinen on DHCPv6-palvelimen jaettavan osoiteavaruuden ehtyminen. Se saavutetaan hyökkääjän lähettämällä palvelimelle todella suuren määrän osoitepyyntöjä ja lopulta DHCPv6:lle varattu osoiteavaruus loppuu tai palvelimen muisti loppuu suuren osoitteiden ylläpitolistan vuoksi. Hyökkäys lopulta aiheuttaa palvelun eston eli toimii palvelunestohyökkäyksenä. Tätä on todella vaikea torjua ja oikeastaan ainut vaihtoehto on rajoittaa verkossa DHCPv6-pyyntöjen määrää tai käyttää tilatonta DHCPv6-palvelinta SLAAC:n tukena. [6]

Toinen hyökkäys tapa on huijari DHCPv6-palvelin. Tässä hyökkääjä on asentanut oman DHCPv6-palvelimensa hyökättävään verkkoon ja lähettää verkkoon liittyville asiakkaille

virheellistä tietoja sisältäviä paketteja, esim. virheelliset osoitteet mm. oletusyhdyskäytävälle ja nimipalvelimelle. Hyökkäys voi aiheuttaa asiakkaalle palveluneston, jos annetut osoitteet virheellisiä, tai mies keskellä -tilan, jolloin kaikki viestit kulkevat hyökkääjän kautta. Virheellisellä nimipalvelimen osoitteella, hyökkääjä voi ohjata uhrin haitallisille sivustoille, josta mahdollisesti latautuu haittaohjelmia asiakkaan koneelle. Tämä hyökkäys voidaan torjua käyttämällä DHCPv6:n autentikointi ominaisuutta tai palomuurilla sallia DHCPv6-vastaukset vain oikealta verkon osoitepalvelimelta. [6]

Viimeinen DHCPv6-hyökkäys on ennemminkin tiedonkeruuta hyökkääjälle. Tässä hyökkääjä löytää yhden DHCPv6:lla saadun IPv6-osoitteen. Tätä tutkimalla huomataan, että osoitepalvelin jakaa osoitteita numerojärjestyksessä, koska löydetyn osoitteen tunnistin osa on todella lyhyt, esim. osoite on 2001:db8:1337::60. Näin hyökkääjä saa mahdollisia uusia uhreja itselleen käyttämällä viereisiä osoitteita sekä numerojärjestyksessä seuraavia osoitteita. Tämä saadaan estetty konfiguroimalla DHCPv6-palvelin antamaan satunnaisia tunnisteosia asiakkaille. [6]

4.6 Hyökkäykset siirtymätekniikoita vastaan

IPv6:n siirtymävaiheessa käytetään hyväksi muun muassa tunneleita IPv6-liikenteelle IPv4-verkon lävitse. Nämä tunnelit ovat usein salaamattomia, joten tässä on hyökkääjälle hyvä hyökkäyspinta. Ensimmäinen siirtymävaiheen tunneleita koskeva hyökkäys on tunnelin nuuskinta. Tässä hyökkääjällä on hallussaan jokin tunnelin matkalla oleva reititin, josta hän voi analysoida tunnelin liikennettä. Tällainen tilanne on vaarallinen myös IPv4-liikenteelle. Tässä hyökkäyksessä paljastuu tunnelin sisäinen liikenne ja pahimmassa tapauksessa voi tapahtua mies välissä-hyökkäys, jolloin liikenne voidaan ohjata myös muualle tai palvelun käyttö voidaan estää.

Toinen tunneleihin kohdistunut hyökkäys on tunkeutuminen. Siinä hyökkääjä löytää tunneli yhteyden ja hän lähettää tekaistuja paketteja tähän tunneliin. Tämä onnistuu, kun hyökkääjä syöttää oikean tunnelin päätepisteiden osoitteet näille varattuihin kenttiin ja lähettää paketin uhrin tunnelinpäätepisteelle. Jos tunnelin päätepiste hyväksyy paketin, voi hyökkääjä lähettää kohde verkkoon mitä vain IPv6-liikennettä. Hyökkääjä ei kylläkään saa paluupaketteja itselleen, mutta saatua yhteyttä voidaan käyttää palvelunesto-hyökkäykseen.

Näiden hyökkäysten torjumiseen tarvitaan erilaisia toimia. Yksi on suojata tunnelin IPv6-yhteys palomuurilla. Toinen on käyttää vain luotettuja tunnelintarjoajia tai luoda oma tunnelinpäätepiste IPv6-internetin reunalle. Kolmantena tapana voidaan käyttää tunnelille jotain salausta, esimerkiksi IPsec, jolloin hyökkääjä ei pysty lukemaan liikennettä tai lähettämään omia pakettejaan tunneliin. [21]

NAT64:lle ja DNS64:lle on myös olemassa hyökkäyksiä. Yksi NAT64:n ongelma on, ettei se salli IPsec:n käyttöä liikenteen salaamiseen. Yksi NAT64: palvelunestohyökkäys

on sisäverkosta lähettää niin paljon viestejä ulkoverkkoon, että NAT64-reititin ei pysty käsittelemään kaikkia yhteyksiä tai IPv4-osoitteet ja porttinumerot loppuvat NAT64-reitittimeltä. [21] Suuri määrä kyselyitä rasittaa myös DNS64-palvelinta, koska tämä joutuu tekemään osoitemuutokset jokaiselle kyselylle. Tämä voi lamaannuttaa myös DNS64-palvelimen ja näin syntyy palvelunestohyökkäys.

Tällainen hyökkäys on vaikea torjua, koska hyökkäjä on päässyt sisäverkkoon. Ainut keino tämän estämiseen on todennäköisesti rajoittamalla liikenteen ja yhtäaikaisten yhteyksien määrää, mitkä kulkevat NAT64-reitittimen läpi. Myös nimipalvelulle esitettävien kyselyjen määrää voidaan rajoittaa. Nämä toimet voivat myös hieman helpottaa hyökkäysten toteutuksia, mutta laitteet eivät ainakaan joudu vastaamattomaan tilaan niin helposti.

5. PALOMUURIEN VERTAILUA

Kun aletaan käyttämään vanhan IPv4-verkon rinnalla IPv6-verkkoa eli dual stack -verkkoa, tarvitsee toteuttaa molemmille versiolle samanlaiset palomuurit. Kuitenkin molemmilla protokollan versioilla on muurausta ajatellen omat erikoisuutensa ja mahdollisesti tarvitsee ottaa huomioon erilaisia seikkoja jo nykyisissä toteutuksissa, kun toinen tulee rinnalle. Yksinkertaistettuna kaikki suojaus ominaisuudet sekä suodatus- ja sallimissäännöt täytyy toteuttaa molemmille identtisinä vaihtaen vain osoitteet. Toki joitain sääntöjä ei voi toteuttaa ollenkaan toisella. Tässä kappaleessa käsitellään, miten IPv6-muuraus eroaa IPv4-palomuurauksesta ja mitä eroja testiverkon palomuureilla oli.

5.1 IPv6-palomuuri verrattuna IPv4-palomuuriin

Palomuuraus on perusperiaatteiltaan samanlaista molemmilla IP-protokollan versioilla. Liikennettä rajoitetaan ja sallitaan riippuen otsikkokentissä olevien arvojen perusteella. Tutkittavat tasot vaihtelevat palomuurin tyypin perusteella siirtokerroksesta aina sovelluskerrokselle asti. IPv6 tuo omat haasteensa palomuurauksen toteutukseen, koska vanhan IPv4-muurin lisäksi tarvitsee toteuttaa IPv6-muuraus. Tämän suunnittelu täytyy tehdä huolella ja ottaa huomioon IPv6:n tuomat muutokset sekä eroavaisuudet IPv4-palomuuriin. Muuraukset voidaan toteuttaa samassa laitteessa, mutta varsinkin vanhemmat laitteet eivät tue kaikki IPv6-muurauksen ominaisuuksia tai eivät pysty tekemään kaikki tarvittavia suodatuksia mitä IPv4-muurilla pystyy.

IPv4- ja IPv6-muureissa on paljon samaa. Molemmat voivat suodattaa paketteja kohde- tai lähdeosoitteiden, käytettyjen porttien sekä sovellusten perusteilla. Refleksiiviset listat ja tilallinen muuraus, eli yhteyksiin perustuva suodatus, ovat myös mahdollisia. Kumpikin palomuuri voidaan toteuttaa staattisena paketti suodattimena, tilallisena paketin tarkastajana tai sovelluskerroksen suodattimena. [23]

Molempien protokollien muureissa pystytään jakamaan verkko samoin perustein. On DMZ-alue ulos tarjottaviin palveluihin, kuten webpalvelu yrityksen kotisivuja varten. Jako intraverkon ja internetin välillä suoritetaan niin, että internet on ei luotettu -verkko ja intra taas luotettuverkko palomuurausta ajatellen eli sallitaan yhteyksiä intraverkosta internetiin, mutta ei toisin päin. Näiden kaikkien eri verkon alueiden välille voidaan asettaa suodatuksia ja tarkistuksia erikseen, jolloin molemmissa saadaan samanlainen aluejako helpottamaan tietoturvaa.

IPv4- sekä IPv6-palomuurit joutuvat molemmat käsittelemään sisäverkon ei julkisia -osoitteita, joita ei saa päästää yleiseen internetiin sellaisenaan, esim. 10.0.0.0/8-alueen IPv4-osoitteet tai IPv6 puolella ULA-osoitteet eli fc00::/7. Jos organisaation ulkorajalla

eli internetiä vastaan olevalle muurille tulee paketti kummalle tahansa sisä- tai ulkoverkon puolelle yrittäen kulkea muurin läpi toiselle puolelle lähettäjän tai vastaanottajan osoitteen ollessa jokin ei julkinen-osoite, molempien protokollaversion muurien tulisi suodattaa tällainen paketti. IPv6-puolella tästä tekee hankalan IPv6:n lokaalit- ja ryhmälähetysosoitteet, jotka voivat sisältää palomuurille tärkeitä tietoja reitittimistä, osoitteista tai lähilaitteista, tai jos organisaation sisäisten verkkojen välissä oleva muuri suodattaa ryhmälähetyksiä, jotka suunnattu koko organisaation tai alueen verkolle, esim. ff05::2 kaikki alueen reitittimet. Molemmat muurit joutuvat käsittelemään myös keksittyjä, virheellisiä ja allokoimattomia osoitteita, jotka tulisi myös pystyä erottamaan ja suodattamaan pois, koska nämä ovat mitä todennäköisemmin hyökkäysyrityksiä. [23]

Erilaisten tunneleiden käsittely on mahdollista molemmilla versioiden muureilla, joilla on kuitenkin erilaiset haasteet toisiinsa nähden. Tästä käydään lisää myöhempänä molempien versioiden käsittelyssä erikseen. Erityisesti IPsec-tunnelit tuottavat molemmille muurityypeille päänvaivaa, koska salauksen takia hyötykuormaa ja ylempien protokollien kehyksiä voi olla hankala tai jopa mahdotonta analysoida suodatusta varten. Tämä tietysti on hyvä asiakkaan liikenteelle internetissä kulkiessa, mutta se mahdollistaa myös hyökkääjän piilottaa liikennettään. Tästä johtuen tarvitsee IPsec-liikennettä koskevien sääntöjen luonnissa olla tarkkana, sillä hyvää, tarkoituksenmukaista liikennettä ei haluta estää, mutta haitallinen liikenne halutaan estää kokonaan. Oman mausteensa tähän tuo IPv6:een sisäänrakennettu IPsec-ominaisuus, joka ei kuitenkaan aina ole käytössä ja eikä enää edes pakollista tukea IPv6-laitteilla. [6]

Pirstaloituneet paketit aiheuttavat sekä IPv4- että IPv6-palomuurille hankaluuksia. Pirstoutumisesta johtuen, ei välttämättä kaikki paketin suodattamiseen tarvittavat tiedot ole ensimmäisessä paketissa, joka saapuu muurille. Tästä johtuen paketti voikin päästä väärin perustein läpi muurista. Molemmilla protokollilla pirstoutuminen tapahtuu hieman eri tavoilla ja paikoissa. [6] Tämä aiheuttaa hieman eroavaisuutta IPv4- ja IPv6-muurin välillä.

IPv6-palomuuri joutuu käsittelemään IPv6:een tullutta uutta ominaisuutta eli lisäotsikoita, joita voi periaatteessa olla rajoittamaton määrä peräkkäin ketjutettuna. Kun taas IPv4-muurissa ei tällaisia tarvitse käsitellä. Samoja lisäotsikoita voi olla yhdessä paketissa useita ja niitä voidaan tulevaisuudessa kehittää lisää, mikä aiheuttaa sen, että IPv6-paketin IPv6-otsikoiden pituus voi vaihdella paljon. Vaihteleva otsikon pituus hankaloittaa muurausta, sillä kaikki otsikkokentät täytyy analysoida ja käydä läpi, jotta päästään muurista riippuen tarvittaessa ylempiin kerroksiin kiinni ja niitä analysoimaan, esim. käytettyyn TCP-portin numeroon. Tämä pitkien otsikoiden käsittely vie enemmän aikaa ja samalla muurin prosessoritehoa, mikä mahdollisesti helpottaa DOS-hyökkäyksen toteutusta muurille. Tästä johtuen jotkut heikommat muurit eivät käsittele lisäotsikoita ollenkaan tai vain ensimmäisiä tai ensimmäistä esiintymistä per lisäotsikkotyyppi. Pirstoutuminen on lisäotsikoilla paha, sillä kaikki lisäotsikkokentät eivät välttämättä mahdu samaan pakettiin tai ylempien tasojen otsikot eivät mahdu ensimmäiseen pakettiin IPv6-

lisäotsikoiden vuoksi. [24] Kuinka tällöin pitäisi paketteja käsitellä? Suodattaa heti pois, kun ei pystytä tarpeeksi luotettavasti analysoimaan paketin sisältöä ja tarkoitusta?

IPv6-osoitteet tuovat eroa muuraukseen versioiden kuusi ja neljä välillä. Toisaalta IPv6-osoitteita on paljon ja monia erityyppejä, mikä hankaloittaa muurausta, mutta taas toisaalta allokoituja osoiteavaruuksia on vain murto-osa koko IPv6-osoiteavaruudesta ja ne on hyvin määritelty ylempien tahojen toimesta. Verrattuna IPv4:än, jonka koko osoiteavaruus on allokoitu ja erikoisosoitetyypit ovat pirstoutuneet laajalle alueelle osoiteavaruutta. IPv6:sta muuraus mielessä tekee hankalan myös se, että periaatteessa jokaisella IPv6-laitteella on globaali IPv6-osoite, joka on reitittyvä internetiin. Verrattuna IPv4-maailmaan, jossa on käytössä yleensä NAT ja näin julkinen osoite on vain NAT-verkon reitittimellä. [6]

IPv6-muurausta hankaloittaa myös SLAAC:n avulla automaattisesti muodostuvat osoitteet, sillä laitteen osoite saattaa muuttua käynnistyskerrasta riippuen. Muurauksessa on myös otettava huomioon kaikki muutkin osoitteiden saanti tavat eli staattiset sekä tilattomat ja tilalliset DHCPv6:t. IPv6:lla pitää ottaa huomioon myös se että portilla saattaa olla useampi globaali IPv6-osoite. Joka tapauksessa IPv6-portilla on kaksi osoitetta: lokaali- ja globaaliosoite. Näitten eri osoitteiden käsittely hankaloittaa IPv6-muurausta verrattuna IPv4-muuraukseen. [6] Lokaali osoitteiden käsittelyn hankaluus IPv6-muurilla on hyvin havaittavissa, esimerkiksi jos border gateway protogol (BGP) on konfiguroitu käyttämään naapureille viestittelyyn lokaaleja osoitteita, niin tällöin jos lokaaliosoitteita ei sallita muurin ulkorajalla, eivät BGPviestit välttämättä päädy perille.

ICMP-protokollan käsittely on myös erilaista IPv6- kuin IPv4-palomuurauksessa, koska IPv6-protokollan toiminta nojaa paljon ICMPv6-viesteihin. Tämän vuoksi IPv6-muurissa tarvitsee sallia hieman enemmän erilaisia ICMP-viestityyppejä kuin IPv4-muurissa. Esimerkiksi RA, RS, NS ja NA -tyyppiset viestit tulee mahdollisesti sallia palomuurille itselleen sekä sisäverkosta että ulkoverkosta ja lisäksi mahdollisesti myös palomuurilta itseltään molempiin suuntiin. Tämä on erityisen tärkeää varsinkin näkymättömällä palomuurilla, joka toimii OSI-mallin tasolla kaksi, sillä muuten yhteydet eivät välttämättä toimi IPv6-protokollalla ollenkaan. Tällöin tarvitsee ainakin sallia naapuruuksien tutkimiseen käytettävät paketit eli NA ja NS sekä duplikaatti osoitteiden tunnistus DAD. Myös IPv6-ryhmälähetykset MAC-osoitteilla 33:33:00:00:00:00-33:33:FF:FF:FF:FF tulee sallia ainakin näkymättämässä IPv6-muurissa, jotta NA- ja NS-viestit pääsevät kulkemaan muurin lävitse. MTU:n selvitys ICMPv6 viesteillä on myös tärkeä IPv6-viestin lähetyksen kannalta, sillä sen avulla tiedetään, mikä on paketin maksimikoko matkatakseen verkon läpi. Tämän vuoksi nämä paketit tulisi sallia IPv6-palomuurissa ainakin sisäverkon alueille, joille on yhteydenmuodostus sallittua. [6]

Tunnelit aiheuttavat päänvaivaa IPv6-palomuurille kuten myös IPv4-muurille mutta eri tavalla. Tunneli voi nimittäin sisältää mitä tahansa liikennettä ja ne ovat yleensä salattuja,

joten itse kuljetettavaan sisältöön on vaikea päästä käsiksi. Erityisen haasteen IPv6-muurille tuo siirtymävaiheen tunnelointi protokollat, jotka kuljettavat sisällään IPv4-liikennettä. Miten tämä liikenne käsitellään, jos IPv6-muurissa ei olekaan IPv4:lle tukea? IPv4-muurilla on samanlainen ongelma, mutta päin vastainen eli IPv4-paketteja, joiden sisässä on IPv6-liikennettä. Toki nämä tunneloidut paketit voidaan suodattaa vasta tunnelinpääte pisteessä, mutta tämä ei välttämättä aina ole mahdollista. [1]

IPv6:lla pakettien pirstoutuminen on erilaista kuin IPv4:lla, joten muurauksessakin on eroa. IPv6-paketti voi pirstoutua vain lähettävällä laitteella, koska reitin MTU on selvitetty aiemmin, kun taas IPv4-paketti voi pirstoutua missä vain reitin varrella. Tämän vuoksi IPv4-muuri joutuu aina käsittelemään otsikkokentän pirstoutumis-ID:n, kun taas IPv6:ssa tätä varten on lisäotsikko. Tämä helpottaa hieman IPv6-muurin toimintaa verrattuna IPv4-muuriin, jos paketti ei ole pirstoutunut. Mutta jos paketti on pirstoutunut, joutuu IPv6-palomuuri tekemään enemmän töitä käsitellessään ylimääräistä otsikkoa. [1]

IPv4-muuri tekee myös asioita mitä IPv6-muuri ei. Protokollan neljännen version muurin tarvitsee laskea käsiteltyään IPv4-pakettia otsikossa oleva tarkistussumma uudelleen, mikäli se ei ole OSI-tasolla kaksi toimiva näkymätönmuuri. NAT-menetelmän tuoma yhden osoitteen takana monta laitetta -tapaus on myös ongelma, joka löytyy vain IPv4 muurista. [24]

Siirtymävaihe on tuonut varsinkin IPv4-muuraukseen lisää huomioitavia asioita, joita kaikkia ei löydy IPv6-muurauksesta. NAT64 on yksi näistä, koska normaalin NAT:n tapaan NAT64:ssa yhden IPv4-osoitteen alle tulee useampi laite kiinni. Tästä hankalan tekee se, että liitetyt laitteet ovat IPv6-osoitetta käyttäviä, mutta toisaalta näiden yhteydet ovat IPv4-laitteisiin ja -palveluihin. Myös protokolla 41 -kapselointia käyttävät tekniikat ovat ongelmana vain IPv4-muureilla, vähän niin kuin oli IPv6-muureilla IPv4-liikenteen tunnelointi IPv6-pakettien sisällä. Pystyykö IPv4-muuri käsittelemään ja suodattamaan tarvittavalla tasolla IPv6-liikennettä, vai tarvitseeko tunneloitu IPv6-liikenne analysoida ja suodattaa muualla? [23]

5.2 Testiympäristön muurien vertailu

Testiympäristössä oli kaksi laitetta, joita käytettiin muuraukseen: Juniper SRX220 -palomuurireititin ja Cisco C3750X -tason 3 kytkin. Näiden lisäksi päästiin myös tutustumaan nopeasti Palo Alto PA-200 -NGFW-palomuuriin, jota ei toteutettu testiverkkoon. Ciscon laite pystyi lähinnä toimimaan vain paketti suodattimena pääsylistojen avulla, kun taas Juniperin SRX pystyy jo paljon monimutkaisempiin analysointeihin. Palo Alton laite on taasen suunniteltu kokonaisvaltaiseen palomuuraukseen uusimmilla palomuurausteknii-koilla. Palomuurien testauksen aikaan C3750X käytti ohjelmistoversiota 12.2(44)SE ja SRX220 versioita 12.1X46-D15.3. Tämän jälkeen näihin on tullut uusia ominaisuuksia ja korjauksia, mutta vertailu toteutetaan edellä mainittujen versioiden perusteella.

Testiympäristön laitteiden muurausominaisuudet olivat hyvin erilaiset. Tämä johtuu vahvasti siitä, että Ciscon laite oli puhtaasti kytkin, johon on yhdistetty vain hieman palomuurausominaisuuksia, kun taas Juniperin laite oli suunniteltu varta vasten palomuuriksi. Palo Alton laite oli taas melko samanlainen Juniperin SRX-sarjalaisen reitittimen kanssa, sillä se oli tarkoitettu vain palomuuriksi. Taulukko 2 on vertailtu laitteiden eri ominaisuuksia. Siitä havaitaan, että SRX220 ja PA-200 olivat monipuolisimmat laitteet. Käyttökokemuksen perusteella Palo Alton laite oli hieman monipuolisempi palomuurausominaisuuksiltaan, mutta Juniper oli hieman nopeampi käyttäjille. Toisaalta SRX220 toimi hyvin myös pelkkänä reitittimenä huomattavasti paremmin kuin PA-200. C3750X on suunniteltu organisaation sisäverkkoon toimimaan esim. talokytkimenä tai kerroskytkimenä toimien VLAN-yhteyksien reitittimenä sekä yhteytenä organisaation kokoavaan reitittimeen.

Taulukko 2. *Testiverkon palomuurien vertailu*

	C3750X	**SRX220**	**PA-200**
Pääasiallinen konfigurointi liittymä	komentorivi	komentorivi	graafinen webliittymä
Voi toimia reitittimenä	kyllä (ei tue kaikkia protokollia)	kyllä	kyllä, virtuaalireitittimillä
Voi toimia näkymätömänä muuri	ei	kyllä	kyllä
Pääsylista omianisuus	kyllä	kyllä	kyllä
Alueisiin jako	ei	kyllä	kyllä
Sovellukseen pohjautuva suodatus	ei	kyllä	kyllä
IDS ja/tai IPS	ei/ei	kyllä/kyllä	kyllä/kyllä
Tilallinen muuraus IPv4	kyllä, refleksiiviset listat	kyllä	kyllä
Tilallinen muuraus IPv6	ei, uudemmissa ohjelmistoissa tuettu	kyllä	kyllä
IPv6 yhteensopiva	kyllä	kyllä	kyllä

Kaikkia kolmea verrattavaa laitetta voitiin konfiguroida sekä webpohjaisen graafisenympäristön avulla tai komentoriviltä. Kuitenkin Palo Alto oli ainut, jolla voi webympäristössä asettaa kaikki samat käskyt ja vielä mielekkäämmin kuin komentoriviltä. Kun taas Juniperilla ja Ciscolla komentorivi oli oikeastaan ainut toimiva konfigurointi mahdollisuus. Kuitenkin PA-200:n graafinen ympäristö oli paikoitellen hieman sekava ja vaati hieman totuttelua, jotta halutut ominaisuudet sai päälle tai ylipäänsä löysi kohdan, josta pääsi asetukseen vaikuttamaan. Toisaalta tämä osoittaa, että Palo Altoon oli pakattu todella suuri määrä ominaisuuksia.

Jokaisessa näistä kolmesta laitteesta löytyi reititysominaisuudet. Juniperin laitteessa nämä olivat laajimmat, kun taas Ciscon laiteessa suppeimmat. Kaikki laitteet sai käyttämään IPv4-osoitteiden lisäksi IPv6-osoitteita sekä reitittämään IPv6-liikennettä. Kuitenkin kaikki IPv6-ominaisuudet eivät olleet tuettuja kaikilla laitteilla.

Ciscon C3750X-kytkimen pääasiallinen palomuurausominaisuus oli pääsylistat. Näillä listoilla sai sallittua tai suodatettua liikennettä osoitteiden ja porttien perusteella. Sekä SRX220:stä että PA-200:sta ei suoranaisesti ollut pääsylistoja, mutta tämä saatiin toteutettua muiden ominaisuuksien avulla. Juniperin pääasiallinen muuraustapa oli alueisiin

jako ja näiden välisen liikenteen salliminen ja suodattaminen. Tämä suodatus ja salliminen voitiin toteuttaa osoitteiden, porttien tai sovellusten perusteella tilallisesti ja riippuen kumpaan suuntaan liikenne oli menossa. Palo Alton PA-200 perustui myös alueisiin ja sillä pystyi suodattamaan ja sallimaan liikennettä monilla eritavoilla.

C3750X oli ainut, joka ei pystynyt toimimaan näkymättömänä muurina eli OSI-mallin toisella tasolla piilottaen itsensä IP-tasolla. Se oli myös ainoa, jossa ei ollut todellista tunkeilijan havaitsemisjärjestelmää (Intrucion detection system, IDS) tai murron estämisjärjestelmää (Intrusion protection system, IPS). Juniper hidastui huomattavasti ja oli lähes käyttökelvoton, kun nämä ominaisuudet kytkettiin päälle. SRX220:en kytkettyjen laitteiden väliset yhteydet hidastuivat merkittävästi, varsinkin Juniperin oman päivittyvän IDS-listan kanssa. Palo Altosta löytyi tämä ominaisuus, mutta sitä ei testattu.

Niin Ciscon kytkin kuin myös kaksi muuta kehittyneempää laitetta kykenivät IPv4-protokollan tilallisen muuraukseen, mutta C3750X vain refleksiivisillä listoilla, eli se ei ollut virallisesti tilallinen palomuuri. IPv6-protokollan kohdalla Ciscon laite ei enää tukenutkaan silloisella ohjelmistoversiolla refleksiivisiä listoja, kun taas Juniper ja Palo Alto toimivat samoin kuin IPv4-protokollan kanssa. Cisco oli myös ainut, jossa dual stack ei ollut oletuksena päällä vaan se tarvitsi erikseen aktivoida.

6. IPV6 TIETOTURVA- JA PALOMUURAUSONGELMAT

IPv6:n tietoturvassa on yksi suuri heikkous, nimittäin ihmisten asenne ja olettamukset. Yleisesti on olettamus, että IPv6-protokollaan on tietoturva sisäänrakennettuna ja tuudittaudutaan tähän olettamukseen. Tämä ei pidä paikkansa, vaikka protokolassa on sisäinen IPsec-ominaisuus, jota laitteiden ei tarvitse enää edes tukea. Tästä ilmeisesti luullaan, että se ratkaisee kaikki tietoturvaongelmat. Vakavan tästä tekee vielä se, että tuota IPsec-tunnelointi ominaisuutta ei edes käytetä kovinkaan usein.

Toinen yleinen IPv6-ongelma ja samalla tietoturvauhka on se, että IPv6:ta ei oteta huomioon uusissa ja vanhoissa verkoissa. Nykyään kuitenkin laitteilla on IPv6 oletuksena käytössä SLAAC-ominaisuuden kanssa. Vaikka verkossa ei olisi yhtään IPv6-reititintä, voivat laitteet viestiä keskenään IPv6-protokollalla paikallisilla osoitteilla kytkinten yli. Tämä on erittäin vakava ongelma yksityishenkilöillä, jotka asentavat verkkoonsa modeemin tai reitittimen, joka saa operaattorilta globaalin IPv6-etuliitteen, jonka se jakaa liitetyille aliverkon laitteille. Nyt laitteella on IPv6-internetiin reitittyvä osoite. Vielä pahemman tästä tekee se, että mahdollisesti reitittimen IPv6-palomuuri ei ole oletuksena päällä, jolloin hyökkääjällä on suora reitti aliverkkoon.

Vielä vain IPv4-verkkoja käyttävien organisaatioiden tarvitsee ottaa tietoturvassaan ja palomuurauksessa huomioon myös IPv6. Tämä johtuu siitä, että käyttäjät voivat luoda siirtymävaiheen tekniikoilla itselleen yhteyden IPv6-internetiin, esimerkiksi käyttäen 6to4-tunnelia, Teredoa tai muuta vastaavaa. Kun laitteella on suodattamaton yhteys IPv6-internetiin, voi liikenteen mukana olla myös haitallisia paketteja. Tätä tekniikkaa voi myös hyökkääjä käyttää saadakseen oman paluuliikenteensä piilotettua palomuurilta. Tällainen tunneli voi myös muodostua vahingossa käyttöjärjestelmän sisäisten tunnelointimekanismien vuoksi, esim. Teredon avulla. Tämä on nykyään hieman epätodennäköisempää Microsoftin suljettua omat Teredo-palvelimensa, joiden osoitteet olivat sisäänrakennettuna Windows-käyttöjärjestelmissä.

IPv6-protokollan perustoiminnallisuuksia vastaan ja niitä käyttäviä hyökkäyksiä on myös paljon, esim. ICMPv6-protokollaa hyväksi käyttävät hyökkäykset. Näitä käytiin melko laajasti läpi kappaleessa 4. Osa ICMPv6-ominaisuuksista vaikuttivat siltä, kuin ne olisi luotu hyökkäyksen tekemiseen. Ihmeellisen tästä tekee se, että nämä ominaisuudet ovat niin tärkeä osa koko IPv6-protokollan toimintaa, kuten NA- ja NS- viestit. Toisaalta hyökkääjän näitä käyttääkseen tarvitsee itse sijaita kohde verkossa. Tämä asettaa paineita myös verkon fyysiseen pääsynhallintaan, eli hyökkääjä ei saa päästä asentamaan verkkoon fyysisesti omaa laitettaan vaan tämä täytyy rajoittaa rakennusten ja tilojen oikeaoppisella pääsynhallinnalla.

Tästä pääsemme ICMPv6-viestien rajoittamiseen ja osoitteiden määräytymiseen. Rajoitetaanko verkossa ICMPv6-viestejä, joka aiheuttaa osan IPv6:n ominaisuuksien toimimattomuuden? Jos näin tehdään niin, miten osoitteet määritellään verkonlaitteille? Kaikkea ei voi tehdä staattisilla osoitteilla, varsinkin suuremmissa verkoissa. Entä DHCPv6-palvelu? Jaetaanko osoitteet ja muut tiedot sillä. DHCPv6:ta vastaan on myös omat hyökkäyksensä. Näistä kysymyksistä muodostuu nopeasti kaksiteräinen miekka, rajoittamalla ja suodattamalla jotain, niin toinen asia hankaloituu.

IPv6:lle muodostuu ongelmaksi myös vanhat laitteet, joilla ei ole täyttä IPv6-protokollan ja tätä tukevien protokollien tukea, esim. vanha reititin ei tue OSPFv3-reititysprotokollaa. Tämä voi aiheuttaa palveluiden puutoksia IPv6-protokollalle. Myös vanhempi IPv4:lle suunniteltu palomuuri voi olla ongelman aiheuttaja, kun se otetaan käyttöön dual stack -verkossa myös IPv6:lla. Siinä ei välttämättä ole kaikkia samoja ominaisuuksia molemmille protokollille. Koska laite joutuu nyt käsittelemään molempia protokollia, voi sen suorituskyky olla heikkoa varsinkin IPv6:n pitkiä osoitteita käsiteltäessä.

Tämä voi aiheuttaa sen, että IPv6:ta varten otetaan toinen erillinen muuri käyttöön. Tällöin protokollien käsittely eriytyy ja helposti käy niin, että vain toinen protokolla saa tietyn säännön muurilleen. Protokollien tietoturva on verrattaessa tällöin epätasapainossa ja toisesta protokollasta voi tulla haavoittuvampi hyökkäyksille.

IPv6:n lisääminen olemassa olevaan IPv4-verkkoon voi monimutkaistaa muurin sääntöjä. Lisätyt säännöt kasvattavat sääntölistaa ja mitä enemmän listassa on rivejä, sitä todennäköisempää on virhe jossain vaiheessa. Dual stack pakottaa periaatteessa tekemään kaikki suojaukset kahteen kertaan, molemmille protokollille erikseen. Jotkin asiat voidaan joutua tekemään eritavoilla, koska kyseistä tehtävää ei tueta toisella protokollalla ollenkaan tai käytettävä protokolla on eri. Tästä esimerkkinä on OSPFv3 verrattuna OSPF tai ICMP verrattuna ICMPv6 ja näiden suodattaminen.

Siirtymävaiheen protokollat ja tekniikat aiheuttavat myös ongelmia, koska myös toisen IP version liikenne on otettava huomioon. Myös muutkin tunnelointi menetelmät aiheuttavat hankaluuksia palomuureille. Tähän voi joutua toteuttamaan hajautettuja muureja eli tunneleiden päätepisteisiin sijoitetaan muureja, jotka suodattavat tätä tunnelista tulevaa liikennettä. Voi olla myös tilanne, missä helpointa on soudattaa toisen IP-protokollan liikenne kokonaan pois verkosta. Tämä voi yksinkertaistaa palomuurin sääntöjä, mutta palveluiden saatavuus voi huonontua. Myös tarpeettomat palvelut on hyvä suodattaa palomuurilla pois.

IPv6-palomuuri on vaikeampi toteuttaa pidempien osoitteiden ja muuttuvan pituisten otsikoiden vuoksi. IPv6-pakettia voi olla hankala analysoida tarkasti, koska sen lisäotsikot muuttavat otsikko kentän pituutta ja kokonaisjärjestystä eli lisäotsikot voivat vaihdella järjestystä ja niitä voi olla useampi samaa tyyppiä. Tämä voi tehdä IPv6-muurista hitaam-

man, jos sillä ei ole tarpeeksi resursseja kasvanutta kuormaa kompensoimassa. Lisäotsikot voiva myös aiheuttaa IPv6-paketin pirstaloitumisen. Tämä voi aiheuttaa lisää harmia palomuurille, koska kaikki suodattamiseen vaadittavat kentät eivät ole ensimmäisessä paketissa ja paketti pääsee virheellisesti sisälle verkkoon. Pirstaloituminen voi myös aiheuttaa palomuurille lisää laskentaa, joka hidastaa laitetta ennestään.

Yhtenä IPv6:n ongelmana on tiedon ja osaamisen osittainen puute toteuttavalla kentällä. Tämä johtuu varsinkin suomessa siitä, ettei IPv6 ole niin laajalti käytössä kuin oli kuviteltu. Tämä johtaa siihen, että henkilökunnan ei ole tarvinnut opetella IPv6:n käyttöä ja IPv6-verkkojen toteutusta. Ja koska asiaa ei ole opeteltu, ei myöskään tuotantoverkkoja ole käytössä. Tästä syntyy ongelma, joka junnaa osittain paikallaan. Tätä ei ole helpottanut se, että eri protokollia ja tekniikoita tulee jatkuvasti lisää ja vanhempia ei enää suositella käytettäväksi tai niihin tulee uusia korjaavia standardi muutoksia, joita taas kaikki laitteet eivät tue. Toisin sanoen IPv6:n ympärillä on osittainen tietotulva, jossa osa tiedoista on jo vanhentunut, kun käyttäjä on sen omaksunut.

7. YHTEENVETO

Tässä työssä käytiin läpi IPv6-protokollaan siirtymistä ja tämän vaiheen tietoturvaa sekä palomuureja. Lisäksi käytiin läpi yleisesti IPv6-palomuureja ja tietoturvauhkia hyökkäysten kautta. IPv6:lla on paljon samaa IPv4:n kanssa, mutta silti ne käyttäytyvät melko eri tavoin tämän työn kentässä.

IPv6:n siirtymävaiheesta ei todennäköisesti päästä koskaan eroon, vaan IPv4 jää rinnalle toimimaan. Kuitenkin IPv4:n käyttö vähenee jatkuvalla syötöllä, mutta siitä ei päästä koskaan kokonaan eroon. Joitain palveluita ja verkkoja jää toimintaa, koska kaikki vanhat menetelmät ja sovellukset eivät saa koskaan IPv6-tukea.

IPv6:a tukemaan ja siihen siirtymisen avuksi tulee todennäköisesti lisää uusia protokollia ja vanhoja jo käytössä olevia otetaan pois käytöstä niiden vanhentumisen sekä tehottomuuden johdosta. Osa siirtymävaiheentekniikoista eivät välttämättä toimi enää tulevaisuudessa muiden protokollien ja menetelmien muuttumisen vuoksi.

Työssä havaittiin, että IPv6:een siirtymisen viivästyminen voi johtua epävarmuudesta ja monesta tavasta toteuttaa sama asia. Myös tietoturva ja palomuuraus ongelmat sekä huolet ovat vaikeuttaneet siirtymisen aloittamista. IPv4-osoitteet ovatkin riittäneet odotettua pitempään, joka on myös viivyttänyt siirtymän aloittamista. Koska kaikki palvelut eivät ole vielä saatavissa molemmilla IP-protokollan versioilla, saattaisi IPv6:n implementointi tehdä verkoista liian monimutkaisia, mikä hankaloittaisi riittävän tietoturvaan ja palomuurauksen toteuttamista. Tässä tilanteessa tulisi kaksi rinnakkaista verkkoa, joiden tietoturva tulisi olla samalla tasolla, vaikka molemmille verkoille olisi omat hyökkäystapansa. IPv6:n toteutuksen ajattelutapa on myös hieman erilainen IPv4:ään verrattuna, sillä osoitteita on yhdellä portilla useita ja ne voivat olla erikäyttötarkoituksilla. Laitteet voivat oppia osoitteet myös automaattisesti. Siirtymämenetelmät ovat myös aiheuttaneet sen, että palomuurilla joutuu käsittelemään kummankin IP-version liikennettä, vaikka sisäinen verkko olisi toteutettu vain toisella, koska liikenne kulkee putkissa toisen protokolla version sisällä.

Työssä saavutettiin riittävä vastaus tutkimusongelmiin: mikä on IPv6:n siirtymävaihe ja miten tietoturva sekä palomuuraus liittyvät tähän. Lisäksi vastattiin myös toiseen kysymykseen, mitä pitää ottaa huomioon IPv6:een siirryttäessä. Tämä saavutettiin käsittelemällä työn aiheita tarpeeksi yksityiskohtaisesti ja monelta kantilta. Lisäksi toteuttamalla testiverkossa kokeilua ja havainnoimalla yleisesti IPv6-verkkojen toimintaa sekä mielipiteitä näistä, saatiin riittävän suuri kosketuspinta-ala aiheeseen.

Loppupäätelmänä voidaan todeta, että IPv6-protokollaan siirtyminen on mahdollista ja suotavaa. Siirtymisen tueksi on paljon erilaisia teknikoita ja menetelmiä sekä materiaali,

jotka helpottavan siirtymän toteutusta. Tietoturva ja palomuuraus eivät muodostu ongelmiksi, jos siirtymä suunnitellaan hyvin ja jokainen tietoturvauhka otetaan huomioon sen vaatimalla vakavuudella.

LÄHTEET

[1] Zamani, A T. & Zubair, S., Deploying IPv6: Security and Future, ternational Journal of advanced studies in Computer Science and Engineering IJASCSE, Vol. 3, No. 4, 2014, pp. 34.

[2] J. Arkko, T. Aura, J. Kempf, V. Mäntylä, P. Nikander, M. Roe, Securing IPv6 Neighbor and Router Discovery, Proceedings of the 1st ACM Workshop on Wireless Security, ACM, New York, NY, USA, pp. 77-86.

[3] I.S. Syngress Media, C. Amon, R.J. Shimonski, The Best Damn Firewall Book Period, William Andrew, Rockland, MA, 2003.

[4] J. Davies, Understanding IPv3, 3rd Edition, Microsoft Press, 2012, 716 p.

[5] Deering, S. & Hinden, R., Internet Protocol, Version 6 (IPv6) Specification, RFC 8200, Internet Engineering Task Force (IETF), 2017.

[6] Hogg, S. & Vyncke, E., IPv6 Security, Cisco Press, 2009, 561 p.

[7] IPv6 Address Types, the RIPE NCC in cooperation with ICANN, web page. Available (accessed 6.11.2018): www.ripe.net/ipv6-address-types.

[8] Hurricane Electric Free IPv6 Tunnel Broker, Hurricane Electric, web page. Available (accessed 6.11.20018): www.tunnelbroker.net.

[9] Black Book, IPv6 Transition Technologies, 10th edition ed. Ixia, 2014, 234 p.

[10] A.&.D. Conta S., Generic Packet Tunneling in IPv6 - Specification, RFC 2473, Network Working Group, 1998.

[11] Blanchet, M. & Parent, F., IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP), RFC 5572, Internet Engineering Task Force (IETF), 2010.

[12] Y. Cui, J. Wu, P. Wu, O. Vautrin, Y. Lee, Public IPv4-over-IPv6 Access Network, RFC 7040, Internet Engineering Task Force (IETF), 2013.

[13] Y. Cui, Q. Sun, M. Boucadair, T. Tsou, Y. Lee, I. Farrer, Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture, RFC 7596, Internet Engineering Task Force (IETF), 2015.

[14] S. Steffann, I. van Beijnum, R. van Rein, A Comparison of IPv6-over-IPv4 Tunnel Mechanisms, RFC 7059, Internet Engineering Task Force (IETF), 2013.

[15] Carpenter, B. & Moore, K., Connection of IPv6 Domains via IPv4 Clouds, RFC 3056, The Internet Society, 2001.

[16] Townsley, W. & Troan, O., IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) - Protocol Specification, RFC 5969, Internet Engineering Task Force (IETF), 2010.

[17] F. Baker, X. Li, C. Bao, K. Yin, Framework for IPv4/IPv6 Translation, RFC 6144, Internet Engineering Task Force (IETF), 2011.

[18] M. Mawatari, M. Kawashima, C. Byrne, 464XLAT: Combination of Stateful and Stateless Translation, RFC 6877, Internet Engineering Task Force (IETF), 2013.

[19] C. Bao, C. Huitema, M. Bagnulo, M. Boucadair, X. Li, IPv6 Addressing of IPv4/IPv6 Translators, RFC 6052, Internet Engineering Task Force (IETF), 2010.

[20] C. Bao, X. Li, F. Baker, T. Anderson, F. Gont, IP/ICMP Translation Algorithm, RFC 7915, Internet Engineering Task Force (IETF), 2016.

[21] J. Weber, IPv6 Security Test Laboratory, Master thesis, Ruhr-University Bochum, Saksa, 2013, 181 p. Available (accessed 1.11.2018): https://blog.webernetz.net/wp-content/uploads/2013/05/Master-Thesis-Johannes-Weber-IPv6-Security-Test-Laboratory.pdf.

[22] P. Nikander, J. Kempf, E. Nordmark, IPv6 Neighbor Discovery (ND) Trust Models and Threats, RFC 3756, The Internet Society, 2004.

[23] Convery, S. & Miller, D., IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0), 2004, 43 p.

[24] Minoli, D. & Kouns, J., Security in an IPv6 Environment, Taylor & Francis Group, LLC, 2009, 289 p.