Ali Al-Rifai

IPv6-palveluntarjonta siirtymävaiheessa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

26.4.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Ali Al-Rifai IPv6 palveluntarjonta siirtymävaiheessa. 35 sivua + 1 liite 26.4.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	tietoverkkoasiantuntija Tomi Raittinen yliopettaja Janne Salonen

Tämä insinöörityö tehtiin Cygate Oy:lle. Työn tavoitteena oli tutkia, miten IPv4-verkossa sijaitsevilla (Internet-protokolla versio 4) web-palvelimilla voidaan tuoda samat palvelut IPv6-verkosta (Internet-protokolla versio 6) liittyville asiakkaille käyttämällä F5 Big-IP -laitetta Local Traffic Manager -moduulilla. IPv4:n osoiteavaruuden loppuminen on luonut maailmanlaajuisen tarpeen siirtyä käyttämään IPv6:sta tulevaisuudessa. Ennen siirtymistä kokonaan IPv6-verkkoihin Cygate pystyy tarjoamaan asiakkailleen mahdollisuuden tarjota IPv6-palveluita muuttamatta koko verkkoinfrastruktuurian tai sovelluksen päivittämistä tukemaan IPv6:ta.

Työssä toteutettiin yksinkertainen IPv4-ympäristö, jossa sijaitsee erilaisia web-palveluita kuvaamaan nykyistä tilannetta yrityksissä. Työssä käytettiin Cygaten laboratorioympäristön IPv4- ja IPv6-verkkoa. Yhteyksien toimivuutta ja tiedon häviämistä selvitettiin matkalla IPv6-verkosta IPv4-verkon BIG-IP LTM:n läpi taustalla sijaitseviin palveluihin. Työssä haluttiin selvittää mahdollisesti yhteensopimattomat palvelut.

Teoriaosuudessa käydään läpi IPv6-protokollan uusia toiminnallisuuksia ja tärkeimpiä muutoksia vanhaan protokollaan verrattuna sekä tutkitaan muita mahdollisuuksia tarjota palveluita IPv6:lla. Samalla pohditaan syitä vielä toistaiseksi vähäiseen IPv6-käyttöönottoon sekä palveluntarjoajan että palveluita käyttävien asiakkaiden näkökulmasta.

Lopuksi arvioitiin toteutuksen tuloksia ja käytännöllisyyttä toteuttaa palveluita IPv6-verkon asiakkaille. Web-palvelimien tuominen IPv6-verkon tavoitettavaksi onnistui vaivatta, lukuunottamatta muutamia ongelmia. Yhteyden muodostaminen pelkällä IPv6-osoitteella aiheutti myös ongelmia, sillä IPv6-tukemattomat sovellukset saattavat sallia vain IPv4-osoitteita. Ongelmia tuotti myös yksittäinen sovellus, joka ei tukenut IPv6:tta. Lokitus IPv6-verkosta keskitettiin kuormanjakajalta yhdelle syslog-palvelimelle, josta pystyttiin selvittämään pyynnön alkuperäinen osoite.

Työn tuloksena eräs Cygaten asiakas otti toteutuksen käyttöön ja tarjoaa asiakkailleen palveluita IPv6:lla.

Avainsanat	BIG-IP, IPv6, Local Traffic Manager

Author(s) Title Number of Pages Date	Ali Al-Rifai IPv6 Service Providing during The Transition Phase 35 pages + 1 appendix 26 April 2013
Degree	Bachelor of Engineering
Degree Programme	Computer Science
Specialisation option	Data Networks
Instructor(s)	Tomi Raittinen, Network Specialist Janne Salonen, Principal Lecturer

This Bachelor's Thesis was conducted for Cygate corporation. The objective for this thesis was to examine how IPv4 (Internet Protocol version 4) enabled web servers could provide services to IPv6 (Internet Protocol version 6) enabled clients with F5 Networks' BIG-IP appliance. The exhaustion of the public IPv4 address space has created a global need to implement IPv6 in the future. Before companies completely adapt to IPv6 networks, Cygate has an opportunity to offer a solution for companies to provide IPv6 services without having the need to update the whole network infrastructure or to update the provided application to support IPv6.

A simplified IPv4 network containing various web services was set up to simulate the current state in a customer network. The test environment was set up in Cygate's Lab which had IPv6 and IPv4 networks established. The connections from IPv6 to IPv4 services via the BIG-IP LTM were examined, to identify incompatible services which would not support the transition. Solutions to access logging were looked into, as some information would be lost in the transition for the end service. BIG-IP works as a proxy between the client and server connections.

The theoretical section of this study, focuses on the new features of IPv6 and significant changes to the previous protocol. It also reviews alternative solutions to provide IPv6 services. The theoretical section also evaluates the possible factors affecting the slow adaptation to IPv6 from both the service provider´s and client´s point of view.

The results of this study were analyzed and reviewed whether the implementation is a practical solution to provide services to IPv6 clients. The implementation proved to be effortless with minor issues. Establishing a connection to a web site with an IP address and not the DNS name caused problems as the application did not identify the IPv6 address. Problems emerged with a particular client side application which did not support IPv6. The connections were logged into a centralized syslog server to preserve the original address of the client.

As a result of this study one of Cygate's customers implemented the solution to their production web servers to provide access to IPv6 clients.

Keywords	BIG-IP, IPv6, Local Traffic Manager

Sisällys

Lyhenteet

HTTP	Hypertext Transfer Protocol. WWW-palvelinten ja selainten käyttämä protokolla tiedonsiirtoon.
HTTPS	Hypertext Transfer Protocol Secure. SSL-suojattu HTTP-protokolla.
IANA	Internet Assigned Numbers Authority. Jakaa ja hallinnoi globaalisti IPv6-osoitteiden jakamista.
IETF	Internet Engineering Task Force. Internet-protokollien standardoinnista vastaava organisaatio.
OSI	Open System Interconnection -malli. Jakaa tiedonsiirtoprotokollat seitsemään eri kerrokseen.
RDP	Remote Desktop Protocol. Microsoftin protokolla, jolla käyttäjä voi ottaa yhteyden graafisesti etätyöasemaan.
RSPV	Resource Preservation Protocol. Protokolla, jota käytetään resurssien varaukseen tietovuossa.
SSL	Secure Sockets Layer. Salausprotokolla, jolla voidaan salata esimerkiksi HTTPS- tai sähköpostiliikennettä Internetin yli.
SSL VPN	Secure Socket Layer Virtual Private Network. Tekniikka, jolla HTTPS-protokollan yli päästään käsiksi sisäverkon resursseihin.
TCP	Transmission Control Protocol. Kuljetuskerroksen tietoliikenneprotokolla, joka varmistaa pakettien saapumisen perille.
UDP	User Datagram Protocol. Kuljetuskerroksen tietoliikenneprotokolla, joka ei varmista paketin saapumista perille.

1 Johdanto

Internet -osoitteita jakava järjestö IANA (Internet Assigned Numbers Authority) on jakanut viimeisen IPv4-osoiteavaruuden [30]. IPv4-osoitteiden rajallisuus on luonut tarpeen uudelle IPv6-protokollalle, joka kasvattaa osoiteavaruutta huomattavasti. Euroopassa siirtyminen IPv6:een on kuitenkin alkanut hitaasti useiden maiden kohdalla. Euroopan edelläkävijät 5.4.2013 Googlen hakukoneen läpi kulkevan IPv6 -liikenteen osalta ovat Ranska 5,21 % ja Romania 8,83 %. [3.]

Insinöörityö tehtiin Cygate Oy:lle. Cygate on TeliaSoneran tytäryhtiö, joka suunnittelee, hallitsee ja ylläpitää turvallisia tietoverkkoratkaisuja yrityksille. Toimipisteitä Cygatella on Ruotsissa ja Suomessa. Työntekijöitä konsernilla on tällä hetkellä noin 500. Työ käsittelee IPv6-palveluntarjontaa palveluntarjoajan näkökulmasta ja käsittelee eri vaihtoehtoja palvelujen tuomista uuden protokollan tavoitettavaksi. Työn tavoitteena on testata, miten kuormantasaajalla voidaan tarjota IPv4-ympäristöllä palveluita IPv6-loppukäyttäjille ennen ympäristön siirtämistä kokonaan IPv6:een. Työssä tutkitaan, miten palveluntarjonta onnistuu pystytetyllä ympäristöllä.

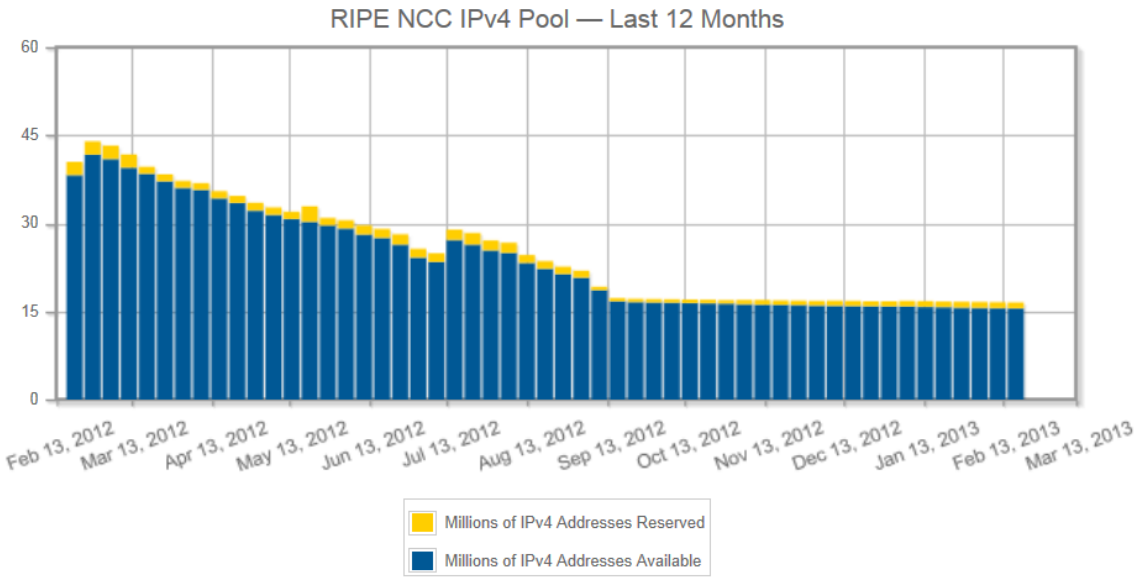
Käytännön toteutuksessa käytetään Apachen web-palvelinta ja Juniperin SA 2500 -laitetta IPv4-osoitteilla, johon liikennettä ohjataan IPv6-osoitteista F5 BIG-IP Local Traffic Managerilla. Tarkoituksena on selvittää, mitä tulee ottaa huomioon jo käytössä olevien ulkoisten palveluiden tuomista IPv6-internetin saataville.

Insinöörityö koostuu neljästä osasta. Ensimmäisessä osassa käydään läpi IPv6-teoriaa, sen tuomia uusia ominaisuuksia ja osoitteistusta. Toisessa osiossa käydään lyhyesti läpi eri tapoja tuoda palveluita IPv6-protokollalla ja niiden tuomia haasteita. Osiossa pohditaan myös syitä vielä toistaiseksi hitaaseen IPv6:n käyttöönottoon. Kolmannessa tutustutaan laitteisiin ja osiossa toteutetaan BIG-IP Local Traffic Managerilla IPv6-palveluntarjonta IPv4-ympäristöllä. Neljäs osio keskittyy pohdintaan ja yhteenvetoon työstä.

2 IPv6-protokolla

Internetin käyttäjämäärä lähti räjähdysmäiseen kasvuun 90-luvun lopulla. Erityisesti Kiinan ja Intian potentiaaliset käyttäjämäärät loivat tarpeen korvata yhä nopeammin ehtyvän IPv4-osoiteavaruuden. IETF (The Internet Engineering Task Force) tiedosti tulevan ongelman ja aloitti IPv6-protokollan kehittämisen jo 90-luvun alkupuolella. Protokollan tarkoituksena oli tuoda ratkaisu IPv4-protokollan rajoitettuun osoiteavaruuteen, joka on noin 4,3 miljardia osoitetta [1, s. 3.]. Yhä useammat laitteet aina tietokoneista puhelimiin ja tabletteihin käyttävät nykypäivänä IP-protokollaa viestintään. IPv6-kehityksessä on otettu tämä huomioon ja osoiteavaruutta on kasvatettu 128 bittiin, joka riittää kattamaan maapallon asukkaat, ja tulevaisuuden kasvun, useampaan kertaan. [2.]

Internet-osoitteita jakava Internet Assigned Numbers Authority (IANA) vastaa sekä IPv4- että IPv6-osoitteiden jakamisesta globaalisti. Osoitteet jaetaan hierarkisesti eri tahoille. IANA jakaa osoitteet maantieteelliselle rekisterille eli Region Internet Registry (RIR), joka taas jakaa osoitteita paikallisrekistereille eli Local Internet Registery (LIR). LIR:t jakavat osoitteita paikallisoperaattoreille. Paikallisoperaattori vastaavat osoitteiden luovuttamisesta loppukäyttäjille [32]. Euroopan osoitteista vastaava rekisteri RIPE NCC on aloittanut jakamaan viimeistä IPv4-osoiteavaruutta. IANA jakaa RIR:lle /8-prefiksillä verkkoja, joista jokainen sisältää yhteensä 16 777 216 osoitetta. [15.]

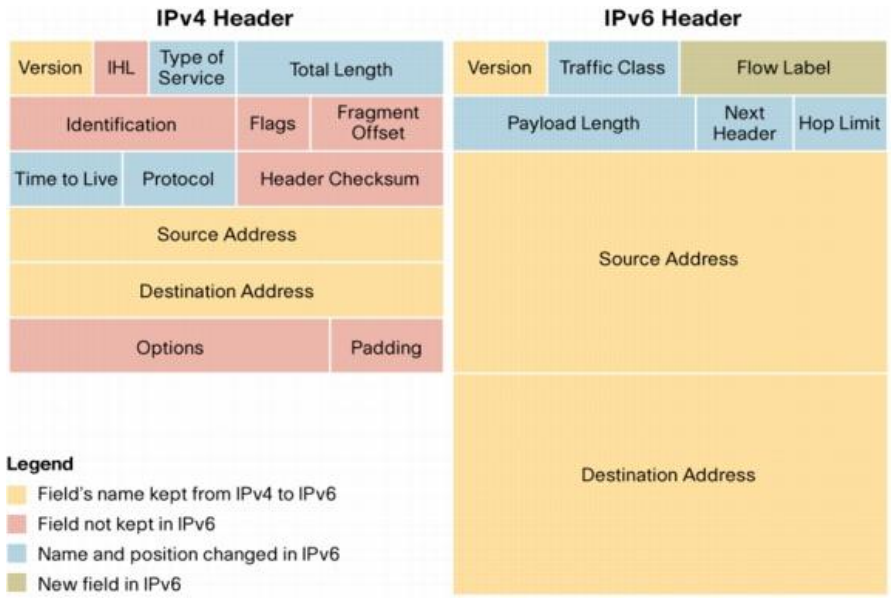


Kuva 1. RIPE NCC:n viimeisen IPv4-osoiteavaruuden tilanne 13.2.2012 – 13.2.2013. Jäljellä olevia osoitteita tullaan jakamaan rajoitetusti. [14.]

2.1 Uusittu kehysrakenne

IPv6-kehysrakenne on kooltaan kiinteät 40 tavua ja koostuu 32 tavun lähde- ja kohdeosoitekentästä, sekä 8 tavun yleisille attribuuteille varatuista kentistä. IPv6:ssa on voitu jättää IPv4:sta tuttu pituuden määrittelevä kenttä pois sen kiinteän koon ansiosta [1, s. 4]. Vertailuna IPv4-pääkehyksen koko voi olla 20 - 60 tavua käytettäessä eri optioita, joilla voidaan määritellä esimerkiksi turvallisuusominaisuudet (Security Options), lähdereititys (Source Routing) tai aikaleimat (Time Stamps). IPv4:ssa reitittimet joutuvat selvittämään optioiden sisällön, kun taas IPv6:ssa tämä tehtävä on siirretty lähes kokonaan päätelaitteille. [1, s. 10.]

Merkittävin uudistus IPv4:n verrattuna on laajennuskehysten käyttö, jotka yksinkertaistavat paketteja kuljettavien laitteiden, kuten reitittimien, työkuormaa. Paketin supistetun rakenteen ja kiinteän koon ansiosta reitittimet voivat välittää paketteja nopeammin puuttumatta jokaiseen optioon, toisin kuin IPv4:ssa. [8.]



Kuva 2. IP–pakettien kehysrakenteiden erot. [7.]

IPv6-kehyksen kentät avattuna.

- **Versio (Version):** Protokollan versionumeron tunnistekenttä.
- **Luokka (Traffic Class):** Määrittelee paketin luokan ja prioriteetti. Korvaa IPv4 Type of Service –kentän.

- **Vuon tunniste (Flow Label):** Voidaan käyttää pakettien jaksotukseen, mikäli reitittimet tätä vaativat. Mikäli päätelaite tai reititin ei tue vuon tunnistetta, tulee lähettäjän asettaa arvo nollaan, välittävien laitteiden muuttamatta arvoa ja vastaanottavan laitteen olla välittämättä kentästä.

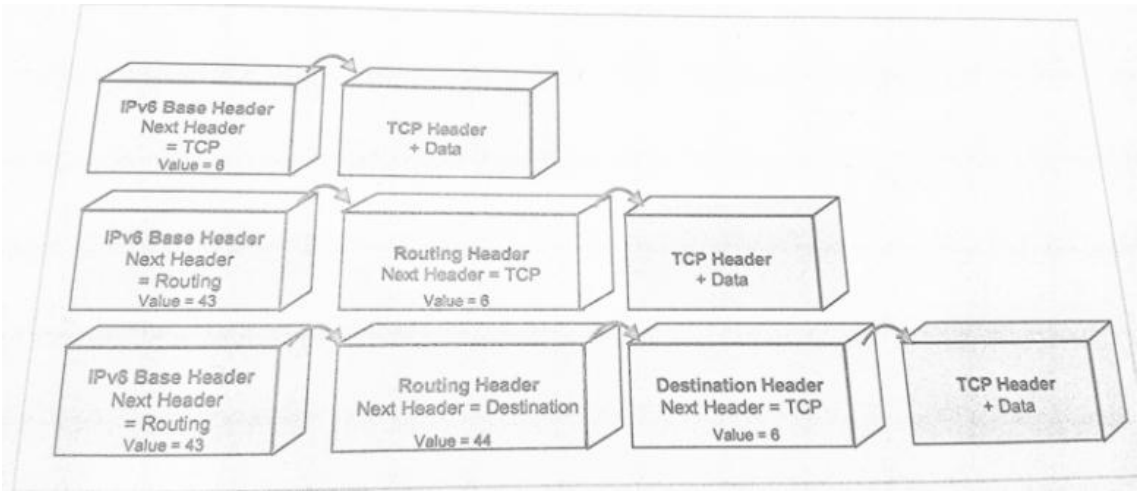
- **Kuorman pituus (Payload Length):** Ilmaisee kuljetettavan paketin koon, eli laajennuskehykset ja kuljetettavan datan. Pääkehystä ei tarvitse mainita, sillä se on kiinteät 40 tavua.

- **Seuraava kehys (Next header):** Ilmaisee seuraavan kentän tyypin. Mikäli laajennuskehykset ovat käytössä, pääkehyksen kentässä määritellään laajennuskehyksen tyyppi. Jokainen laajennuskehys sisältää kentän. Kentällä ilmaistaan kuljetettavan datan tyyppi esim. TCP/UDP.

- **Elinaika (Hop limit):** Korvaa IPv4 TTL –kentän (Time to Live). Määrittelee paketin elinajan hyppyjen määrällä. Voidaan myös käyttää reitittimien lukumäärän selvittämiseen paketin matkalla.

2.2 Laajennuskehykset

IPv6-kehyksen arkkitehtuuria on muutettu ottamalla IPv4-kehykseen sisältyneet optiot pois pääkehyksestä ja otettu käyttöön laajennuskehykset, joilla voidaan halutessa lisätä tarvittavat optiot. Laajennuskehykset sijoittuvat IPv6-pääkehyksen ja OSI-mallin neljännen kerroksen, eli kuljetuskerroksen (Transport Layer) väliin [1, s. 4]. Kuvasta 3 voidaan todeta, miten laajennuskehykset sijaitsevat IPv6-kehyksen ja TCP-kehyksen välissä.



Kuva 3. Laajennuskehysten esiintyminen IPv6-kehyksen jälkeen.

Laajennuskehykset nopeuttavat pakettien välittämistä, sillä kuljettavat reitittimet eivät oletuksena tutki laajennuskehysten sisältöä. Poikkeuksena on kuitenkin Hop-by-Hop–optio, jonka jokainen paketin matkalla oleva laite joutuu selvittämään, mukaan lukien lähde- ja kohdelaitteet [6, s. 6-7]. Laajennuskehyksiä voidaan tarpeen mukaan tutkia reitittimissä ACL:llä (Access Control List), mikä kuitenkin vaikuttaa huomattavasti laitteen suorituskykyyn. Hop-by-Hop on laajennuskehyskentistä raskain, sillä se joudutaan käymään prosessoritasolla systemaattisesti läpi. Tästä syystä se sijaitsee välittömästi pääkehyksen jälkeen IPv6-paketissa [7].

Pakettien pirstalointi (fragmentation) IPv6:ssa on siirretty reitittimiltä päätelaitteille. IPv6-linkin läpi menevälle liikenteelle MTU (Maximum Transmission Unit) on oltava vähintään 1280 tavua. Lähettäessä pirstaloidun paketin päätelaite lisää pirstalointilaajennuskehyksen IPv6-pakettiin [1, s.10; 6]. Päätelaitteet päättelevät linkin MTU:n käyttämällä Path MTU Discovery (PTMU) ominaisuutta. Laitteet selvittävät dynaamisesti linkin MTU:n käyttämällä PTMU:ta. Päätelaite lähettää paketin ensimmäiselle reitittävälle laitteelle, joka ilmoittaa välillä käytettävän MTU:n. Laite olettaa koko matkan kohteeseen käyttävän samaa MTU:ta ja aloittaa lähetyksen saadulla MTU-arvolla. Matkan varrella reitittävät linkit saattavat kuitenkin tukea pienempää MTU-arvoa eivätkä suostu välittämään paketteja eteenpäin. Tällöin reititin ilmoittaa ”Packet Too Big” -viestin päätelaitteelle. Näin lähettäjä tunnustelee linkin pienimmän MTU:n ja käyttää sitä pirstaloitujen pakettien kokona kohteeseen. [33, s. 3-4.]

Taulukko 1. Laajennuskehysten selitteet.

Järjestys	**Laajennuskehys**	**Tehtävä**	**NH**
1.	Hop-by-Hop-kehys (Hop-by-hop header)	IPv6 jumbogram -optiolla voidaan lähettää yli 64 kilotavun paketteja. Router Alert -optiolla reitittimille voidaan kertoa tärkeää tietoa, jota protokollat, kuten RSVP käyttävät. Jokaisen pakettia välittävän laitteen on käytävä Hop-by-Hop-kehys läpi.	0
2.	Reitityskehys (Routing header)	Kehyksellä voidaan määritellä haluttu polku, jota paketti kulkee kohteeseensa. Vastaa IPv4 loose routingia.	43
3.	Pirstalointikehys (Fragmentation header)	Käytetään, mikäli lähetetään suurempia paketteja, kuin mitä linkin MTU tukee. Kehyksen M-lippu viittaa fragmentoinnin jatkuvuuteen. Asetus 1 viittaan seuraavien pakettien sisältävän fragmentteja, kun taas 0 viittaa paketin olevan viimeinen pirstale.	44

4.	Autentikointikehys (Authentication header)	Käytetään tuomaan yhteydetöntä eheyttä sekä datan alkuperän autentikoimista. Estää myös uudelleenlähetyshyökkäystä vastaan.	51
5.	Kapselointikehys (Encapsulation header)	Liikenteen kryptaamiseen käytetty kehys, jolla voidaan estää myös uudelleenlähteys-hyökkäykset.	50
6.	Kohdeoptiokehys (Destination header)	Sisältää valinnaista tietoa paketin kohteelle. Käytetään esimerkiksi Mobiili IPv6:ssa.	60
7.	Mobiilikehys (Mobility header)	Verkkojen välillä liikkuvat mobiililaitteet käyttävät mobiilikehystä.	135

Laajennuskehyksille on RFC 2460:n mukaan määritelty suositeltu esiintymisjärjestys IPv6-paketissa. Taulukko 1 havainnolistaa järjestyksen [6, s. 7; 8]. NH eli Next Header on laajennuskehyksen tunniste.

2.3 ICMPv6-verkkokerroksen hallintaprotokolla

Verkkolaitteet viestittävät ICMPv6-protokollalla pakettien prosessoinnissa tapahtuneista virheistä. ICMPv6 sisältää IPv4:stä tutut ”ping”- ja ”traceroute6” -verkkokerroksen diagnostiikkatyökalut. ICMPv6 määritellään tarkemmin IEEE:n dokumentissa RFC 4443 [1, s. 27]. ICMPv6:n lisätty uusi ominaisuus, naapurintunnistus (Neighbor Discovery), joka koostuu viidestä eri ICMP-pakettityypistä.

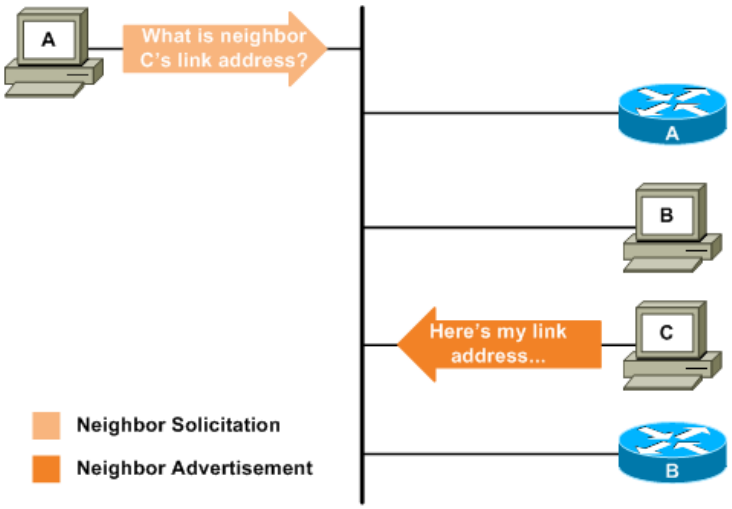
- Reititinkyselyt (Router Solicitation)
- Reititinmainostukset (Router Advertisement)
- Naapurikyselyt (Neighbor Solicitation)
- Naapurimainostukset (Neighbor Advertisements)
- Uudelleenojaus (ICMP Redirect).

ND:llä samassa verkkosegmentissä sijaitsevat laitteet voivat tunnistaa toisensa ja toistensa linkkiosoitteet. ND korvaa myös IPv4:n ARP-protokollan (Address Resolution Protocol). Verkkolaitteet löytävät ND:n avulla myös paketteja reitittävät laitteet sekä pitävät yllä tietoa verkon tavoitettavista laitteista (Neigbor Cache, NC) [29, s. 10,12]. Uusina ominaisuuksina ovat myös tavoittamattomien naapurien tunnistus (Neighbor Unreachability Detection, NUD) sekä päällekkäisten osoitteiden tunnistus (Duplicate IP

Address Detection, DAD). DAD:n tarkoitus on estää saman osoitteen jakamista usealle laitteelle. [1, s. 31.]

2.3.1 Naapurikysely ja naapurimainostus

Nodet, eli reitittimet ja päätelaitteet käyttävät naapurin tunnistusta selvittämään link-local-osoitetta, eli saman paikallisen verkkosegmentin osoitteita. Verkon laitteet lähettävät naapurimainostuksia (Neighbor Advertisement, NA) ja naapurin kyselyitä (Neighbor Solicitation, NS) verkon laitteiden selvittämiseksi. Verkkolaite, joka haluaa keskustella toisen verkossa sijaitsevan laitteen kanssa, lähettää NS-kyselyn multicastina osoitteeseen FF02::1, eli kaikille verkon laitteille, joissa se tarjoaa oman osoitteensa. Kyselyn kohde ymmärtää, että kyseessä on sen osoite, ja vastaa NA-viestillä, jossa se ilmoittaa oman linkkiosoitteensa kyselyn aloittaneelle laitteelle. [53, s. 9-10.]



Kuva 4. Naapurikyselyn ja naapurimainostuksen toimintaperiaate. [54.]

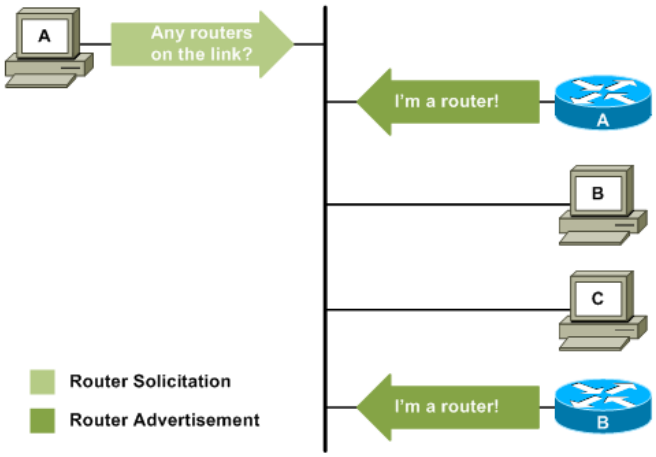
Verkon kaikki laitteet pitävät yllä kahta erillistä taulua tavoitettavista yhteyksistä ND:n avulla. Tavoitettavista naapureista pidetään tietoa Neighbor Cachessa. NC:ssa säilytetään laitteiden unicast-osoitteita, jonne verkkolaite on aikaisemmin lähettänyt paketteja. Jokainen merkintä sisältää myös linkkiosoitteen sekä onko laite reititin vai päätelaite. Toinen tauluista, Destination Cache (DC), sisältää tiedon kohteista, jonne paketteja on viimeksi lähetetty. DC pitää tiedossaan verkkosegmentin sekä paikalliset että etäosoitteet ja sitoo paikallisen osoitteen etäosoitteeseen, jos se ei sijaitse samassa verkkosegmentissä. [1, s. 43-44.]

NUD eli Neighbor Unreachability Detectionilla selvitetään verkkolaitteen tavoitettavuus. NC pitää yllä taulua laitteista, jotka on tavoitettu tai yritetty tavoittaa. Lähettäessä pakettia laite tarkastaa NC:n ja selvittää, onko verkkolaite tai pakettia kuljettava laite tavoitettavissa ja lähettää paketin, mikäli se todetaan tavoitettavaksi. Jos laite ei vastaa tai sitä ei löydy NC:stä, lähetetään NS-viesti laitteen tavoittamiseksi. [1, s. 43.]

DAD eli Duplicate Address Detection tarkastaa, että laitteelle konfiguroitu osoite on uniikki. DAD suoritetaan niin manuaalisesti kuin autokonfiguroiduille osoitteille. Konfiguroitua osoitetta ei voida käyttää ennen kuin DAD on onnistunut osoitteelle. DAD:n selvittämiseksi verkkoon liittynyt laite lähettää NS-viestin. Jos viestiin ei tule vastausta, voidaan osoite ottaa käyttöön. Mikäli verkossa on samalla osoitteella konfiguroitu laite, se vastaa NA-viestillä kaikille laittelle kyseessä olevan duplikaatti osoite. [1, s. 45.]

2.3.2 Reititinpyynnöt ja -mainostukset

Reitittimen havaitseminen IPv6-verkossa tapahtuu reititinkyselyillä (Router solicitation, RS) sekä reititinmainostuksilla (Router advertisement, RA). Reitittimet lähettävät tietyin aikavälein reititinmainostuksia multicast-osoitteeseen FF02::1, jota muut verkon laitteet kuuntelevat. Verkkoon liitetyt päätelaitteet voivat myös lähettää RS-kyselyn, johon reititin vastaa välittömästi RA-mainostuksella. Kuva 5 havainnollistaa, miten verkkolaitteet käyttävät RA- ja RS-viestejä. [1; 6.]



Kuva 5. Reititinpyyntöjen ja reititinmainostusten toimintaperiaate. [54.]

Reititinmainostuksen kehyksessä merkittäviä osoitteen konfigurointiin liittyviä bittejä ovat M- (Managed) ja O-bitit (Other). Näistä M-bitti määrittelee, käyttääkö laite tilallista

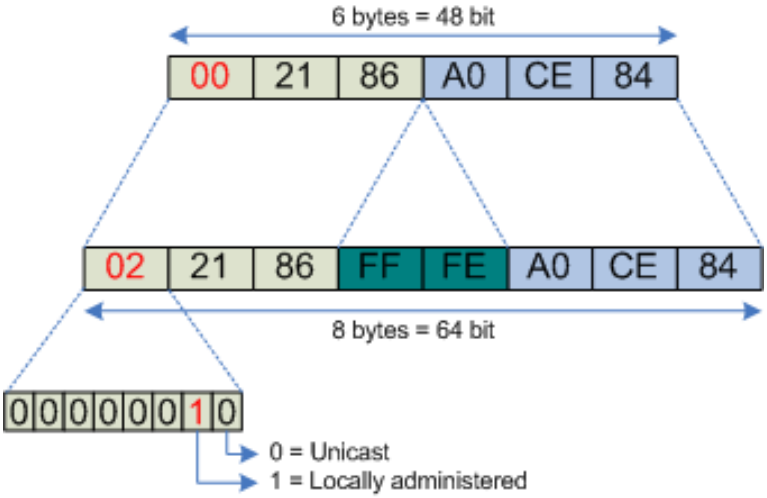
osoitteenkonfigurointia eli DHCPv6:tä. M-bitin ollessa päällä käytetään DHCPv6-osoitteen konfiguroimiseen, ja O-bitti määrittelee, otetaanko DHCP-palvelimelta vastaan muita asetuksia esimerkiksi DNS-asetukset. M-bitin ollessa pois päältä ei O-bittiä tarvitse tutkia ja tällöin käytetään tilatonta osoitteenkonfigurointia. [1, s. 35.]

2.4 Autokonfigurointi (Auto-configuration)

IPv6 tarjoaa kaksi menetelmää osoitteen konfigurointiin dynaamisesti. Osoite voidaan saada verkkolaitteelle tutulla DHCP-protkollalla sekä käyttämällä tilatonta osoitteenkonfigurointia eli Stateless Address Autoconfigurointia (SLAAC). SLAAC ei vaadi päätelaitteiden manuaalista osoitteenkonfigurointia. Verkkoon liitetty päätelaite lähettää RS-viestin multicastina reitittimelle, joka vastaa RA-viestillä sisältäen verkkoprefiksin, josta laitteet päättelevät linkin aliverkon. Päätelaite vastaanottaa verkkoprefiksin ja muodostaa 48-bittisestä fyysisestä MAC-osoitteesta itselleen IEEE:n (Institute of electrical and Electronics Engineers) määrittelemän EUI 64-bittisen verkontunnisteen. Verkkolaite liittää osoitteet yhteen ja muodostaa itselleen 128-bittisen IPv6-osoitteen. SLAAC ei tue DNS-asetuksien konfigurointia. [1, s. 50-51.]

Uusittu DHCPv6-protkolla toimii kutakuinkin samoin kuin IPv4:ssa käytetty DHCP. DHCPv6 voidaan ottaa käyttöön joko tilallisena (Stateful) tai tilattomana (Stateless). Nämä eroavat toisistaan niin, että tilallinen säilyttää jaetuista osoitteista rekisteriä omassa kannassaan, kun taas tilaton vain jakaa osoitteita kirjaamatta niitä ylös. Tilatonta DHCP:ta käytetään silloin, kun käyttäjät ovat saaneet omat osoitteensa käyttämällä SLAAC:ta. Tilaton DHCP ei siis määritä laitteelle osoitetta vaan tarjoaa tarvittavat DNS-palvelimet nimien muuttamiseen. SLAAC tukee ainoastaa osoitteen konfigurointia, joten DNS-asetukset tulee määritellä laitteille tilattomalla DHCP:llä. [55.]

IPv6-verkkoliitännän tunnisteella (Interface Identifier) viitataan entiseen hostnimitykseen, sillä yhdellä hostilla voi olla useampia verkkoliitäntöjä. IPv6-verkkoliitännän tunnisteet ovat pituudeltaan 64 bittiä ja ne ovat EUI-64-muotoa. Verkkoliitännän IEEE 802 MAC-osoitteesta voidaan muodostaa EUI-64-osoite. [1, s. 14.]



Kuva 6. EUI-64-osoitteen muodostaminen MAC-osoitteesta. [56.]

Kuva 6 havainnollistaa, miten 48-bittisestä MAC-osoitteesta muodostetaan 64-bittinen EUI-64-verkkoliitännän tunniste. MAC-osoitteen vasemmasta laidasta invertoidaan seitsemäs bitti, joka määrittelee osoitteen toimialueen paikalliseksi tai globaaliksi. MAC-osoitteen ensimmäisten 24 bitin jälkeen osoitteen perään sijoitetaan 16 bitin FFFE-arvo heksadesimaalisena. Perään lisätään alkuperäisen MAC-osoitteen viimeiset 24 bittiä. 128-bittinen IPv6-osoite muodostuu siis verkon 64-bittisestä prefiksistä sekä sen perään liitetystä 64-bittisestä EUI-64-tunnisteesta [1, s. 14]. FFFE-arvo lisätään MAC-osoitteeseen, jotta EUI-64-tunnisteesta saadaan kooltaan 64 bittiä.

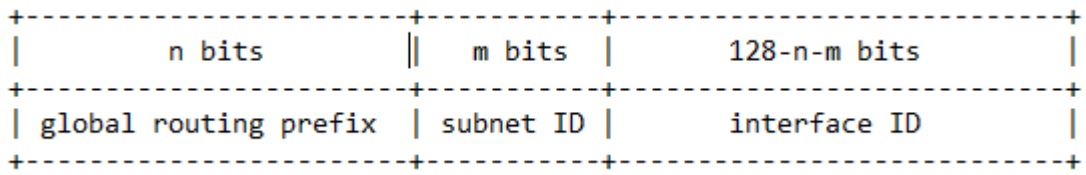
2.5 Osoitearkkitehtuuri

IPv6-osoiteen pituuden myötä osoite esitetään heksadesimaalisena. Pitkien osoitteiden esittämiseen on erilaisia keinoja esittää osoite. Osoite koostuu kahdeksasta kuudentoista bitin kentästä x:x:x:x:x:x:x:x, jossa x on yksi kenttä. Mikäli osoitteessa on paljon nollia välissä, voidaan ne antaa muodossa ”::” , kuten esimerkkinä käytetyssä osoitteessa 2001:db8:af45:4231::10, joka näyttää avattuna seuraavalta: 2001:0db8:af45:4231:0000:0000:0000:10. Esimerkistä näkyy myös, että db8 edessä oleva nolla voidaan myös jättää ilmaisematta. Lyhennystä ”::” voidaan käyttää vain kerran osoitteessa. Yksittäistä 16-bittisen kentän lyhentämiseen ei voida käyttää "::" lyhennettä. IPv4:sta tuttu nollareitti, 0.0.0.0/0 voidaankin IPv6:lla ilmaista seuraavasti ::/0. [1, s. 4.]

IPv6-osoitteet koostuvat 128 bitistä, joita jaetaan verkkoliitännälle itse laitteen sijaan. IPv6 unicast -osoite viittaa siis yhteen verkkoliitännälle määriteltyyn osoitteeseen. Laitteella voi olla useampi liitäntä unicast-osoitteella, joita voidaan käyttää laitteen tunnistamiseen. Jokaisella verkkoliitännällä tulee olla vähintään yksi unicast-osoite. Yksittäisellä IPv6-verkkoliitännällä voi olla useampi erityyppinen osoite, kuten unicast, multicast tai anycast [1, s. 3]. Unicast-osoitteita on useampaa tyyppiä, niistä merkittävimmät käydään läpi tarkemmin seuraavissa osioissa.

2.5.1 Globaali unicast-osoite (Global Unicast Address)

IPv6 globaalit unicast-osoitteet ovat globaalisti reititettäviä osoitteita ja niitä voidaan verrata julkisiin IPv4-osoitteisiin. Arkkitehtuuriltaan IPv6-osoitteet on jaettu hierarkkisesti niin, että globaaliprefiksi muodostuu 48 bitistä, aliverkko 16 bitistä ja 64 bitin verkkokortintunnisteesta. Kuva 7 havainnollistaa globaalin unicast-osoitteen rakennetta. [19, s. 1.]



Kuva 7. Globaalin unicast-osoitteen esitystapa. [10.]

IANA (Internet Assigned Numbers Authority) vastaa IPv6-osoitteiden jakamisesta globaalisti. IANA jakaa globaalilla prefiksillä verkkoja maantieteellisille internet rekistereille (RIR, Regional Internet Registries) /23-prefiksillä osoitteita [17]. Euroopan alueen IP-allokaatioista vastaa RIPE NCC, joka jakaa lokaaleille Internet rekistereille (LIR, Local Internet Registry), eli paikallisoperaattoreille osoitteet /32-prefiksillä [18]. RIPE NCC:n ohjeistaa operaattoreita jakamaan aliverkkoja loppukäyttäjille minimissään /48-prefiksillä ja maksimissaan /64-prefiksillä [20]. Aliverkon hierarkkisesta määrittelystä vastaavat aliverkon lunastaneet tahot. [19, s. 1.]

2.5.2 Linkkiosoite (Link-Local Address)

Linkkiosoitetta (Link-Local) käytetään ainoastaan verkkosegmentin sisällä. Osoitteita ei myöskään reititetä julkiseen internetiin. Linkkisoitteita käytetäänkin naapuritunnistuk-

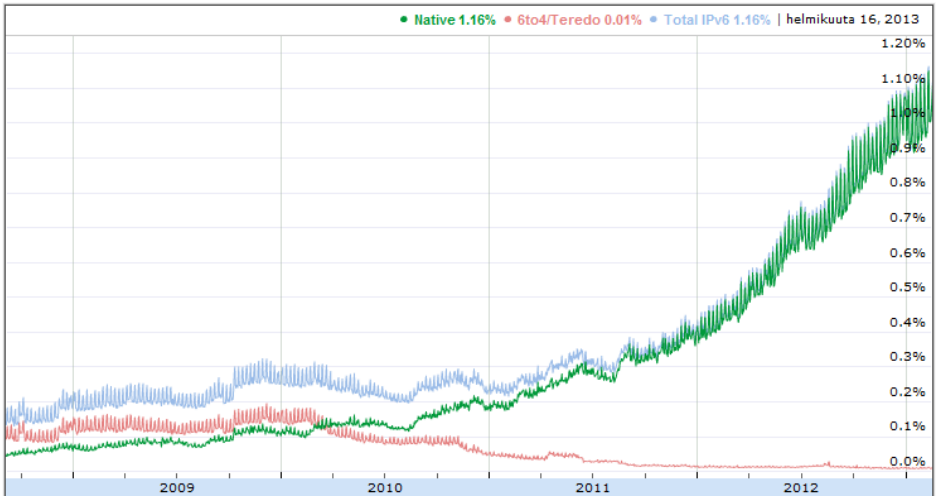
seen, automaattiseen osoitteen konfigurointiin, tai kun reitittimiä ei ole tavoitettavissa. Keskenään kytketyt laitteet voivat kommunikoida linkkiosoitteilla ilman osoitteenkonfigurointia. Linkkiosoitteet kuuluvat FE80::/10 verkkoon. [1, s. 24.]

2.5.3 Uniikkilokaaliosoite (Unique-Local Address)

Uniikkilokaaliosoitteilla (Unique-Local) on globaalisti uniikki prefiksi, jota ei reititetä julkiseen internetiin. Uniikkilokaaliosoitteet ovat tarkoitettu etäkonttoreille ja etäkonttorien välisten VPN-tunneleiden osoitteiden määrittelemiseen. ULA-osoitteita voidaan käyttää, mikäli uutta globaalisti reititettyä aliverkkoa ei haluta anoa operaattorilta. Uniikkilokaaliosoitteet määritellään dokumentissa RFC 4193. [51.]

3 Palveluntarjonta IPv6-protokollalla

Suomessa tunnetuimmista web-palveluntarjoajista IPv6:lla tarjoaa palveluita MTV3 ja Iltalehti [27]. Googlen mukaan maailmanlaajuisesti (16.2.2013) sen käyttäjistä 1,16% käyttää sen palveluita IPv6:lla. Kuvasta 8 voi seurata tilannetta Googlen IPv6-käyttäjämäärää aina vuoden 2008 lopusta lähtien. [3.]



Kuva 8. Googlen käyttäjämäärät IPv6-verkoista [3.]

Alhaisista käyttäjäluvuista johtuen IPv6:n siirtyminen ei ole vielä ollut ajankohtaista tai houkuttelevaa yrityksille, jotka tarjoavat esimerkiksi web-palveluita. Suurin osa asia-

kaskunnasta on edelleen tavoitettavissa vanhalla protokollalla, joten akuuttia tarvetta ei ole lähteä välittömästi tuottamaan palveluita IPv6:lla.

Kneckt & Leppänen työssään ”IPv4-verkosta siirtyminen IPv6-verkkoon organisaatiossa” ovat selvittäneet muutamien yrityksien halukkuutta siirtyä IPv6-verkkoihin. Työssä suoritettuun haastatteluun osallistui Hosting-palveluita yksityis- ja yritysasiakkaille tarjoava Louhi Net Oy. Louhen asiakaskunta koostuu noin 14 000 asiakkaasta, joista kotimaisia asiakkaita on 99 %. Yritys ei näe ajankohtaiseksi siirtyä IPv6:een, sillä työn aikana operaattorit eivät pystyneet tarjoamaan yritykselle IPv6-palveluita. Myöskään asiakaskunnan suunnalta ei ole tullut pakottavaa tarvetta saada IPv6-osoitteita käyttöön. [25, s. 46-48,58.]

Suurimpien suomalaisten kuluttajaliittymien palveluntarjoajien IPv6-tuki on vielä toistaiseksi tuloillaan. Operaattoreiden mukaan IPv6:een siirtyminen kuluttajapuolella vaatii muutoksia siltauksiin ja reitityksiin. Soneralta todetaan, että kuluttajalaitteet voidaan joutua vaihtamaan IPv6-yhteensopiviin laitteisiin. Elisalla IPv4-osoitepulaa korvataan käyttämällä yksityisiä osoitteita mobiiliverkon asiakkaille, eli yksittäisen julkisen osoitteen taakse piilotetaan useampi käyttäjä käyttämällä NAT:a (Network Address Translation) [28]. Suomen näkökulmasta tilanne on vielä toistaiseksi hyvä, sillä osoitteita väkilukuun nähden on varmasti enemmän kuin mitä esimerkiksi Aasiassa tulee olemaan lähitulevaisuudessa. Suurella web-kaupalla saattaa kuitenkin olla asiakkaita useammalla eri mantereella, tai yrityksellä etäkäyttäjiä maissa, joissa julkisen IPv4-osoitteen saaminen ei enää ole mahdollista. Jos yrityksen palvelut ovat tässä vaiheessa tavoitettavissa vain IPv4:llä, eivät käyttäjät pääse käyttämään palveluita.

Aasian osoitteista vastaava internetrekisteri APNIC jakaa tällä hetkellä sille jaettua viimeistä IPv4-osoiteavaruutta. APNIC on myös luovuttanut jo merkittävän määrän /32-prefiksin IPv6-verkkoja. Aasian jaetuista IPv6-verkoista kärkeä pitävät seuraavat maat. [35; 36.]

- Kiina 14 595
- Japani 11 229
- Korea 5 230
- Taiwan 2 338.

Aasia tulee olemaan maailmanlaajuisen IPv6-käyttöönoton merkittävä tekijä, joka tulee ennen pitkää pakottamaan lännen siirtymistä käyttämään IPv6:sta. Älypuhelimien ja tablettien yleistyminen Kiinan keskiluokan keskuudessa tulee varmastikin vauhdittamaan kiinalaisten operaattorien IPv6-käyttöönottoa julkisten osoitteiden piilottamisen sijaan. IP-protokollaa tukevien laitteiden määrä tulee kasvamaan entisestään ja yhtä henkilöä kohden tulee olemaan useampi osoite.

Operaattorien näkökulmasta välitöntä tarvetta tuoda IPv6-osoitteita asiakkaille ei ole, sillä vanhoja osoitteita on vielä tarjolla, joskin rajoitetusti. Ajan ja rahoituksen löytäminen ovatkin todennäköisesti IPv6-projekteille suurimmat haasteet niin yrityksissä kuin operaattoreilla. Yrityksien johdon ja tietohallinnon on kuitenkin syytä aloittaa jo alustavat keskustelut tulevaisuuden varalta ja punnita riskejä, miten IPv6:n puutteellisuudella saattaa olla vaikutusta yrityksen tuottavuudelle. Palveluntarjonnan näkökulmasta merkittävä haaste IPv6:lle on tällä hetkellä sille löytyvä tuki ja yrityksissä käytettävät vanhat tietojärjestelmät. Nämä järjestelmät eivät välttämättä tule ikinä tukemaan uutta protokollaa. IPv6:n 128-bittinen osoitejärjestelmä tai uudet ominaisuudet saattavat olla arkkitehtuurillisesti mahdotonta toteuttaa tai niiden toteuttaminen vaatii liian suuria investointeja. Kun lähtökohtana on IPv4-verkko, ei muutos uuteen protokollaan tapahdu hetkessä. Toisaalta yrityksen verkon edustalla olevien palveluiden IPv6-käyttöönotto ei vaadi koko yritysverkon kääntämistä IPv6:lle.

Suomessa operaattorit ovat keskeisessä asemassa siinä, milloin IPv6-käyttöönoton tulee ajankohtaiseksi. Vasta kun suurimmat operaattorit alkavat jakaa liittymille IPv6-osoitteita, alkavat yritykset todella kiinnostua IPv6-käyttöönotosta. Erilaisia ratkaisuja palveluntarjontaan IPv6:lla käydään läpi seuraavissa kappaleissa.

3.1 Natiivi IPv6

Web-palvelimelle määritellään ainoastaan IPv6-osoite. Yleisimmät web-palvelimet, kuten IIS ja Apache, ovat tukeneet IPv6:ta jo useamman vuoden. Päivittämällä palvelimet vanhasta protokollasta uuteen on nopeasti katsottuna edullinen ratkaisu. Mikäli palvelimen ohjelma ei käytä, muokkaa tai säilö asiakkaiden osoitteita, ei investointeja ohjelmiston muokkaamiseen tarvitse juurikaan tehdä. Vaihtoehtona on myös pystyttää erilliset IPv6-palvelimet julkisten IPv4-palvelinten rinnalle [16, s. 5] Mikäli IPv4-

palvelinten rinnalle pystytetään erilliset IPv6-palvelimet, tulee polku yrityksen internetistä reittimeltä DMZ:lle (Demilitarized Zone) päivittää käyttämään IPv6:tta.

3.2 Dual Stack

Dual Stack-toteutuksessa käytetään samanaikaisesti sekä IPv4- että IPv6 toiminnallisuutta. Loppukäyttäjälaitteille, reunakytkimille, runkokytkimille ja reitittimille määritellään kummankin protokollan toiminnallisuus. Tarvittaessa toinen protokolla voidaan ottaa pois käytöstä, jolloin laite toimii kuten IPv4- tai IPv6-laite riippuen poistetusta protokollasta. DNS-palvelusta tulee myös löytyä IPv6:n käyttämä AAAA-tietue ja IPv4:n käyttämä A-tietue, jotta kummallakin protokollalla voidaan muuttaa nimiä osoitteiksi [11, s. 4-5].

Palveluntarjonnan näkökulmasta tarjottavien palveluiden ohjelmien tulee tukea kumpaakin protokollaa, mikäli halutaan tuottaa palveluita uudella, että vanhalla protokollalla. Toteutuksessa uusien verkkojen lisääminen tai palomuuriavaukset joudutaan tekemään kahteen kertaan kummallekin protokollalle.

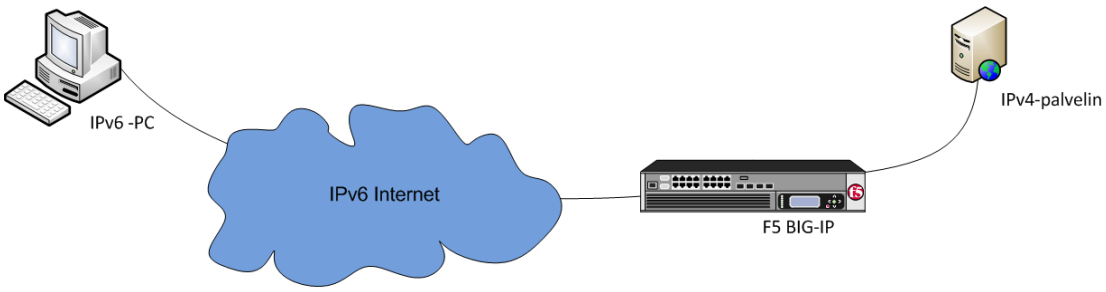
3.3 Välityspalvelin

Välityspalvelin eli proxy näkyy asiakkaille tavallisena web-palvelimena, joka ohjaa pyynnön taustalla oleville palvelimille ja palauttaa pyydetyn sivun. Asiakas näkee välityspalvelimen palauttavan sivun. Tyypillisesti välityspalvelimia käytetään Internetistä liikennöivien asiakkaiden pyyntöjen välittämistä palvelimille, jotka sijaitsevat palomuurin takana. Pyynnöt voidaan jakaa taustalla oleville palvelimille ja yksittäisen palvelimen kuormaan voidaan jakaa useammalle palvelimelle. Välityspalvelin toimiikin kuormanjakajana esimerkiksi yksittäiselle URL:lle. Tämän tyylinen välityspalvelin tunnetaan reverse proxyna. Kun asiakas hakee Internetistä sivun proxyn kautta, toimii proxy silloin forwarding proxynä. [47.]

4 Toteutus ja laitteet

Työssä haluttiin selvittää, miten palveluita voidaan tuoda IPv6-internetin saataville mahdollisimman vaivattomasti kuormanjakajalla. Asiakasympäristö, jonne toteutusta tultaisiin mahdollisesti käyttämään, olisi todennäköisesti toteutettu IPv4:lla.

Ympäristö toteutettiin käyttämällä F5-kuormanjakajaa kääntämää IPv4-verkosta palveluiden osoitteet IPv6-verkolle tavoitettavaksi. F5 toimii toteutuksessa välityspalvelimena pyynnöille. Ympäristön toimintaa testataan IPv6-osoitteella varustetuilla koneilla, joiden on tarkoitus ilmentää IPv6-internetistä yhteyttä ottavaa asiakasta. Palveluiden tarjontaa työssä simuloidaan Linuxin Apache web-palvelimella ja etäkäyttöpalvelua Juniperin SA 2500 -laitteella. Kuva 9 havainnollistaa ympäristöä.



Kuva 9. Yksinkertainen havainnekuva ratkaisusta.

Työssä toteutettiin kaksi toteutusta. Ensimmäisessä toteutuksessa käytettiin yksinkertaista web-palvelinta, joka ei parsi http-kehystä tarkemmin vaan palauttaa vain pyydetyn sivun. Toisessa toteutuksessa olisi palvelu, joka ei myöskään tue uutta protokollaa ja jossa ohjelma tunnistaa käyttäjän osoitteen ja saattaa tämän perusteella tehdä rajoituksia tai lokitusta. Työssä haluttiin tutkia ja selvittää mahdollisia ongelmatapauksia, joita IPv6-tukemattomat sovellukset saattaisivat aiheuttaa toteutuksissa.

Ensimmäisessä toteutuksessa päädyttiin käyttämään Apachen web-palvelinta, joka otettaisiin käyttöön mahdollisimman vähäisellä konfiguroinnilla. Tällä simuloitaisiin tavanomaista yrityksen sivua, jossa esitellään yritys. Toisessa ratkaisussa tuli ottaa huomioon järjestelmän tuki IPv6-osoitteille ja mahdolliset ongelmatilanteet, jossa ohjelman tuki on vain IPv4-osoitteelle. Työssä testattiin web-palvelimelle pääsy selaimesta sekä IP-osoitteella että FQDN-osoitteella (Fully Qualified Domain Name).

IPv4-ohjelmalle on osoitekentälle saatettu ohjelmoitaessa varata vain 32 bittiä, kun taas IPv6-ohjelmalle osoitekentän tulee tukea 128 bittiä. Tämä aiheuttaa ongelmia ja ohjelmiston päivittäminen IPv6-tukeen saattaa olla edessä, mikäli välityspalvelinmalliin ei päädytä.

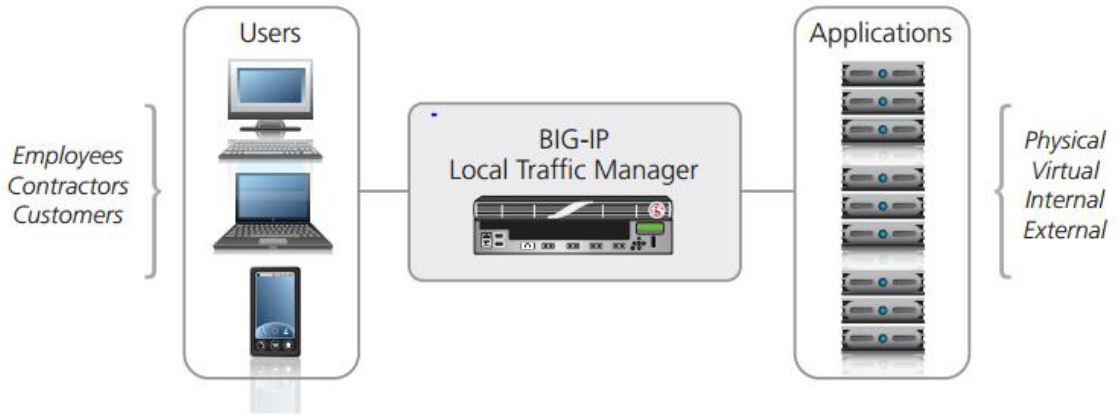
Käytössä olevan välityspalvelin tekniikan johdosta lokitukseen tuli kiinnittää huomiota. Asiakkaan IPv6-osoite ei tulisi toteutuksen takia koskaan näkymään pyynnön prosessoivalle palvelulle. Lokituksen kohdalla tutkittiin myös erilaisia ratkaisuja toteuttaa asiakkaiden pääsylokitus järkevästi.

4.1 F5 Big-IP Virtual Edition

F5 Big-IP on F5 Networksin tuote, jolla voidaan toteuttaa kuormanjakoa, skaalautuvuutta, korkeaa käytettävyyttä ja suorityskyvyn optimointia. Big-IP on niin sanottu ADC eli Application Delivery Controller, joka sijaitsee useimmiten palveluiden edessä palvelinsaleissa, verkkoarkkitehtuurin näkökulmasta DMZ:lla [38]. Big-IP-laitteet ovat modulaarisia ja niihin voidaan lisätä tarvittaessa eri ominaisuuksia lisensseillä. Työssä keskitytään BIG-IP:n Local Traffic Manager (LTM) -lisenssin kuormanjako-ominaisuuksiin. Joitakin BIG-IP:n moduuleja ja niiden tukemia ominaisuuksia käydään läpi alla. [39, s. 1-3.]

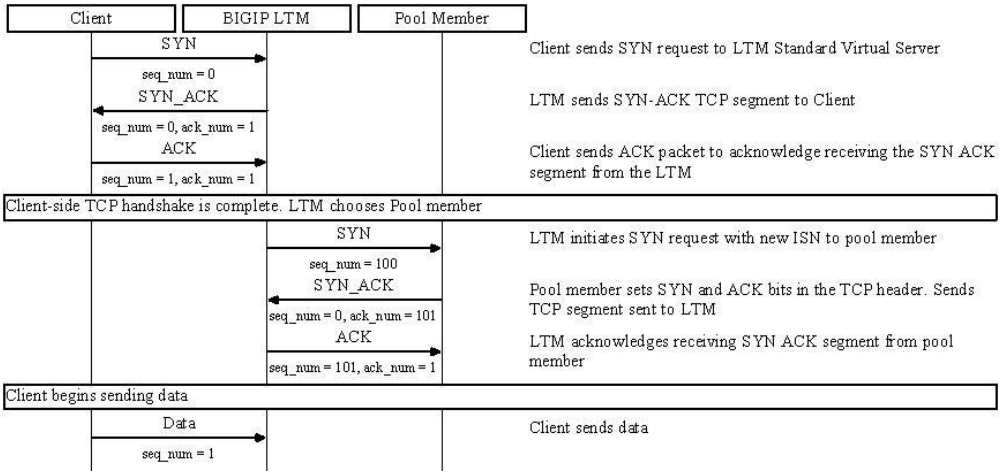
- **Local Traffic Manager:** Kuormanjako, DDoS-suojaus sekä palomuuriominaisuudet.
- **Application Security Manager**: Web-sovelluksien palomuuri, jolla voidaan suojata sovelluksia fyysisissä, virtuaalisissa ja pilviympäristöissä
- **Global Traffic Manager:** Jakaa DNS-kyselyt esimerkiksi yrityksien, asiakkaiden maantieteellisen sijainnin tai taustalla olevan sovelluksen toiminnallisuuden perusteella.

Kuormanjakajalla voidaan nopeuttaa yrityksen kriittisiä ohjelmia jakamalla kuormaa useammalle palvelimelle yhdenaikaisesti. Laite pystyy myös purkamaan raskasta SSL-protokollan käsittelyä [40]. Työssä käytettiin fyysisen laitteen sijasta virtuaalista Big-IP Virtual Edition -laitetta, joka toimii VMWare-virtualisointialustalla. Ohjelmistoversio työssä käytetyssä laitteessa oli BIG-IP V11.3.0.



Kuva 10. BIG-IP Local Traffic Managerin toimintaperiaate

Tavallisen kuormanjakan läpi pyydetty sivu muodostaa suoran yhteyden taustalla sijaitsevaan palvelimeen. Big-IP ohjaa liikennettä välityspalvelimen tavoin, jolloin laite luo erilliset ja toisistaan riippumattomat yhteydet asiakkaalta kuormanjakajalle ja kuormanjakalata palvelimelle. Tämä tunnetaan paremmin F5:n nimeämänä Full Proxy -arkkitehtuurina, jonka perustana on eri protokollien syvällinen ymmärtäminen [37, s. 4]. LTM:llä voidaan luoda jokaiselle palvelulle oma virtuaalipalvelin, jonka kautta liikenne ohjautuu taustalla tarjottaviin palveluihin. TCP-yhteyttä käytettäessä Standard-virtuaalipalvelin toimii Full Proxy -arkkitehtuurin mukaisesti. Big-IP avaa palvelinpuolelle oman TCP-yhteyden ja välittää tiedon asiakkaalle. TCP-kättely tapahtuu asiakkaan ja kuormanjakajan välillä, ennen kuin yhteys avataan kuormanjakajalta farmin palvelimelle. Kun yhteys on muodostettu asiakkaalta kuormanjakajalle, toteutetaan sama kättely kuormanjakajalta palvelimen suuntaan ennen datan siirtoa. Kuvassa 11 havainnollistetaan yhteyden muodostus. [41.]



Kuva 11. Standard-virtuaalipalvelimen TCP-kättely. [41.]

iRule on F5:n tarjoama skriptikieli, jolla voidaan muokata manuaalisesti kuormanjakoa palvelinfarmilta toiselle HTTP-kehyksen datan mukaan. iRuleja voidaan käyttää LTM-ominaisuudella ja F5 tarjoaakin kattavat ohjeet iRulejen kirjoittamiseen DevCentral-tukiportaalissaan. iRuleilla voidaan muokata kuormanjakajan läpi menevän liikenteen HTTP-kehyksen arvoja eri yhteysvaiheissa [42]. Laitteella voidaan suorittaa tilallista liikenteen tutkintaa palomuurin tavoin. iRuleilla voidaan muokata, sallia, lokittaa tai pudottaa liikennettä aina OSI-mallin 2. tasolta 7. tasolle. [37, s. 7.]

4.2 Juniper Secure Access 2500 SSL VPN

Juniperin Networksin SA 2500 SSL VPN -laitteella käyttäjät voivat etänä käyttää yrityksen resursseja julkisen internetin yli HTTPS-protokollalla ilman erillisiä asennettuja ohjelmistoja [47]. SSL VPN -käsittellä (Secure Sockets Layer Virtual Private Network) viitataan käytäntöön, jossa kuljetetaan yksityistä tietoa julkisen Internetin yli käyttäen HTTPS-protokollaa joka käyttää SSL-salausta. [23, s. 2.]

Kuva 12. Juniper Networks Secure Access 2500 SSL VPN -laite

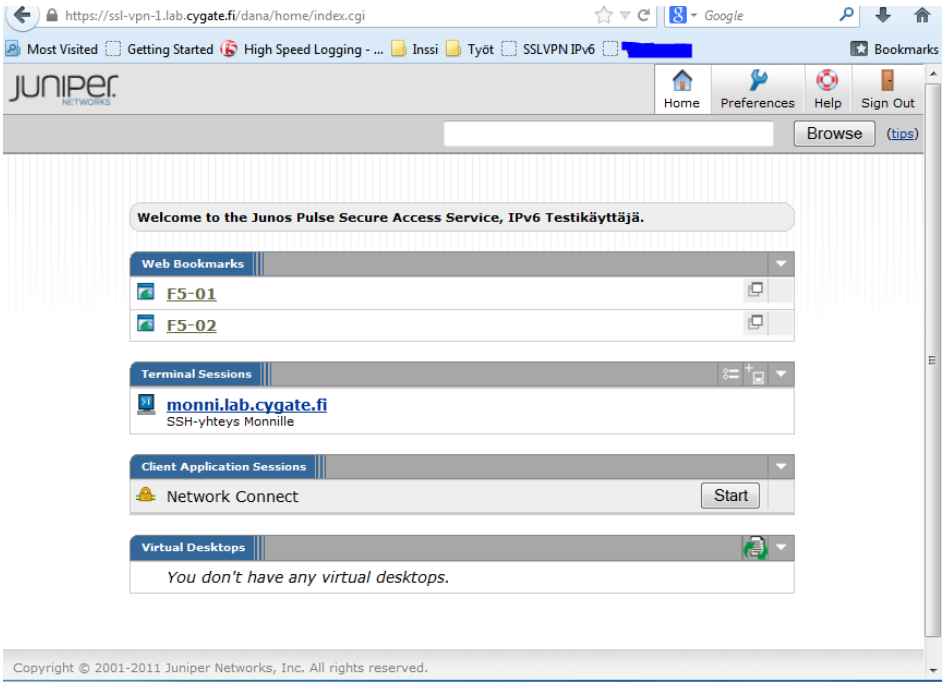
SSL VPN -laitteella voidaan tarjotaan resursseja Secure Access Service -portaalin (SAS) kautta. Resursseiksi määritellään palvelimet tai tiedostot, joihin voidaan päästä

SAS:n kautta. Laitteella voidaan määritellä säännöt käyttäjäkohtaisesti resursseihin. Seuraavat on SAS:n tukemia resursseja. [48.]

- TELNET/SSH
- RDP
- Tiedostojaot
- VPN-tunnelointi.

Tavanomaista VPN-tunnelointia SA SSL VPN tukee Network Connect-soveluksella (NC). NC on toteutettu Javalla. Käyttäjän liikenne tunneloidaan SSL VPN -laitteelle SSL-liikenteenä. Käyttäjä pystyy suojatun tunnelin kautta pääsemään esimerkiksi yritysensä verkkoon ja se sille osoitetaan sisäverkon osoite. [49; 50.]

Työssä ei keskitytä SSL VPN:n konfigurointiin. Laitteen tarjoamaan portaaliin on luotu yksinkertaiset resurssit, joita testataan työssä. SAS -portaalin on havainnollistettu kuvassa 13.



Kuva 13. Secure Access Service -portaalinäkymä.

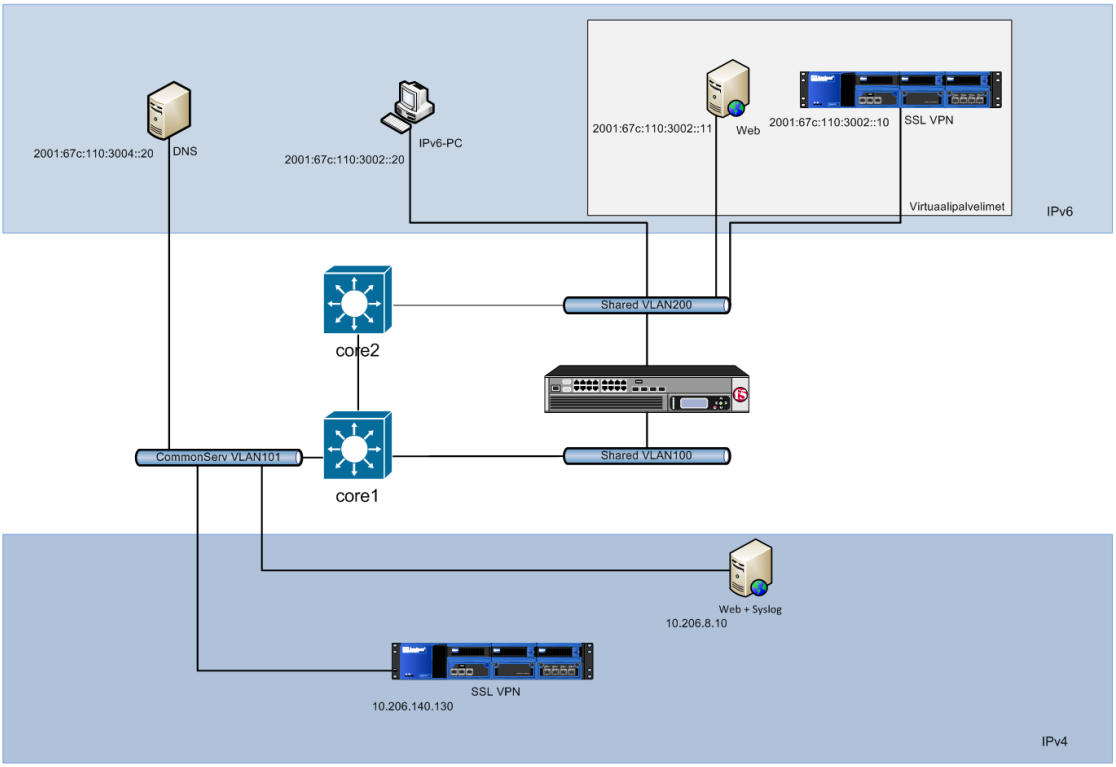
4.3 Testiympäristön pystyttäminen

Testiympäristön pystyttäminen aloitettiin IPv6-osoitteiden määrittelystä. Työssä käytettiin Cygaten olemassa olevaa laboratorioverkko, jossa oli jo varatut IPv4- ja IPv6-verkot. Kuormanjakajalle jouduttiin määrittelemään IPv6-osoite ja selvittämään aliverkolle osoitettu IPv6-verkko. Palveluiden testausta varten luotiin yksi IPv6-osoitteella määritelty testi-PC.

Taulukko 2. Ympäristössä käytettävät osoitteet ja verkot

IPv6-verkko/osoite	**DNS-nimi**	**IPv4-osoite**	**Selitys**
2001:67c:110:3002::/64	-	-	IPv6-verkko virtuaalipalvelimille ja testi-PC:lle.
2001:67c:110:3002::9	hki-per-f5ve0x.lab.cygate.fi	10.206.4.9	BIG-IP:n IPv6-osoite on ulkoinen liityntä ja IPv4-osoite sisäinen liityntä
2001:67c:110:3002::10	ssl-vpn-1.lab.cygate.fi	10.206.140.131	SSL VPN virtuaalipalvelimelle varattu osoite.
2001:67c:110:3002::11	monni.lab.cygate.fi	10.206.8.10	Web-palvelimen virtuaalipalvelimen osoite
2001:67c:110:3002::20	-	-	IPv6-PC
2001:67c:110:3004::/64	-	-	Palvelimille varattu IPv6-verkko
2001:67c:110:3004::20	ns-monni.lab.cygate.fi	10.206.8.10	DNS-palvelin

Käytössä olevat IPv6- ja IPv4-osoitteet ja verkot on kuvattu taulukossa 2. Käytössä oleva SSL VPN:n ja F5 löytyivät jo valmiiksi asennettuna Cygaten laboratoriosta IPv4-osoitteilla. Kuva 14 havainnollistaa toteutettua testiympäristöä.

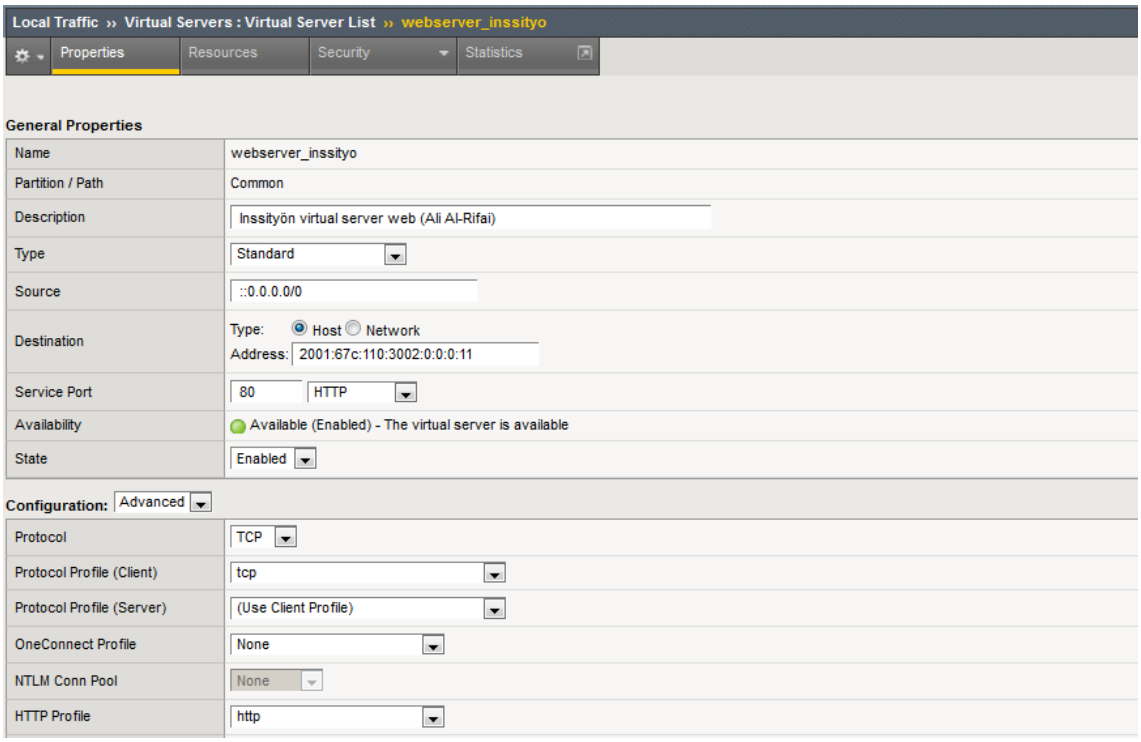


Kuva 14. Testiympäristö jaettuna IPv4- ja IPv6-alueisiin. Virtuaalipalvelimet on sijoitettu eri VLAN:in, kuin missä itse fyysiset laitteet sijaitsevat. VLAN101 on määritelty sekä IPv4- että IPv6-verkko.

Asiakasympäristössä, jossa ei ole otettu IPv6:sta käyttöön, tulisi operaattorilta varata oma IPv6-osoiteavaruus ja konfiguroida yrityksen edustareittimet tukemaan IPv6:ta. Tämän jälkeen DMZ:lta, missä BIG-IP LTM sijaitsee, tulee reitittää edustareittimien kautta Internettiin jotta BIG-IP:lle luodut virtuaalipalvelimet ja laite pystyvät tavoittamaan julkisen IPv6-internetin.

4.4 Toteutus 1: Web-palvelimen IPv6-käyttöönotto

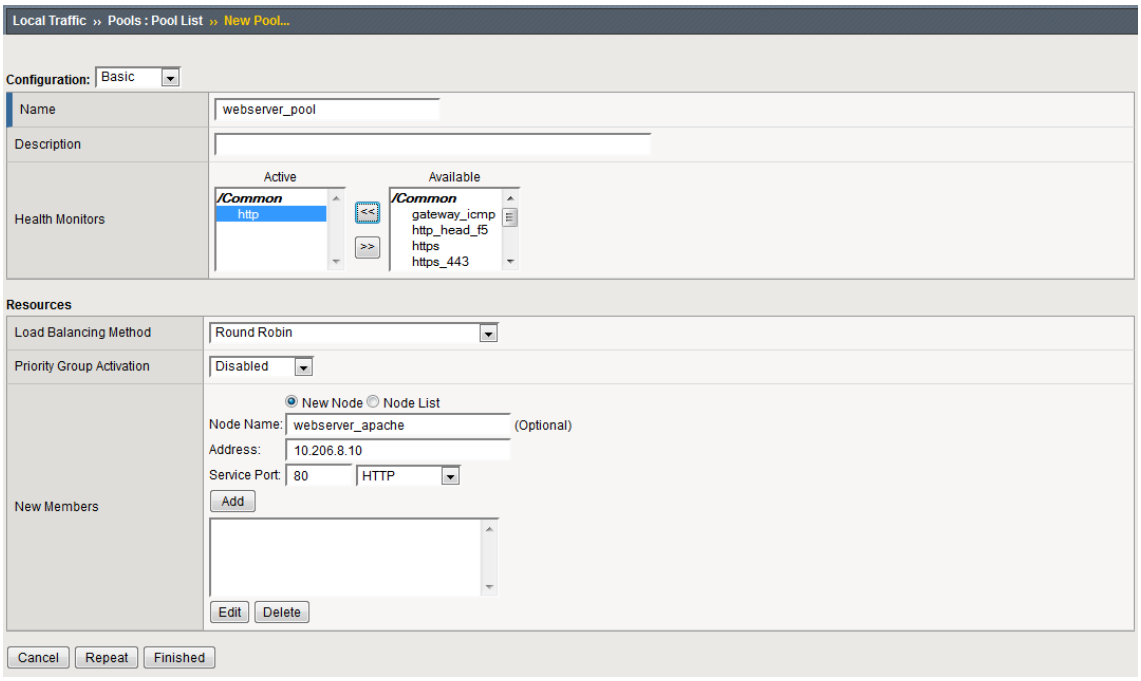
Toteutuksessa käytettiin LTM:n standardivirtuaalipalvelinta, jolloin kuormanjakaja toimii välityspalvelimena yhteyksille. Kun yhteys otetaan IPv6-osoitteesta, kuormanjakaja ottaa yhteyden vastaan ja avaa IPv4-osoitteella yhteyden palvelimelle omalla IPv4-osoitteellaan. Toteutus aloitettiin määrittelemällä virtuaaliserverin IPv6-osoite ja virtuaaliserverin portti 80. Protocol Profile -asetuksella määritellään protokolla, jolla virtuaalipalvelin vastaa kyselyihin. Kuva 15 havainnollistaa webserver_inssityö-virtuaalipalvelimen käyttöönottoa.



Kuva 15. Web-pavelimen IPv6-virtuaalipalvelin.

Virtuaalipalvelimelle on määriteltävä palvelin tai palvelinfarmi, jonne yhteydet ohjataan virtuaalipalvelimelle tulleille kyselyille. Kuormaa voidaan jakaa farmin palvelimille eri ehdoilla. Työssä webserver_pool -farmissa on käytettynä vain yksi palvelin, joten kuormanjakoon valittiin Round Robin. Tällöin kuormaa jaetaan vuorotellen farmin palvelimille. Farmiin lisättiin palvelin webserver_apache ja palvelimelle määriteltiin palveluportiksi portti 80.

Palvelimien tilaa voidaan valvoa Health Monitoreilla. Monitoreita voidaan määrittää useampia, esimerkkinä ping tai http-kysely. Jos palvelimelle määritellään useampi monitori, on sen pystyttävä vastaamaan kaikkiin kyselyihin tai palvelin todetaan tavoittamattomaksi ja se poistetaan farmista. Jos web-palvelimelle määritellään vain yksi monitori, on suositeltavaa määritellä vain http-monitori. Mikäli http-prosessi on palvelimella jumissa, mutta palvelin vastaa pingiin aiheutetaan asiakkaille katkoksia palvelussa, sillä viallinen palvelin pidetään farmissa. Palvelinfarmin luomisen jälkeen se liitetään virtuaaliserverin käyttämäksi farmiksi.



Kuva 16. Palvelinfarmin luonti ja määrittely.

Kuormantasaaja käyttäytyy välityspalvelimen tavoin sen ohjatessa liikennettä itsensä läpi. Läpi menevän liikenteen alkuperän selvittämiseksi HTTP-kehykseen on lisätty x-forwarded-for-kenttä, jota voidaan käyttää välityspalvelimen läpi menevän liikenteen alkuperän selvittämiseksi kohteena olevalle web-palvelimelle [17]. Välityspalvelin, eli tässä tapauksessa BIG-IP, sijoittaa kenttään asiakkaan lähdeosoitteen.

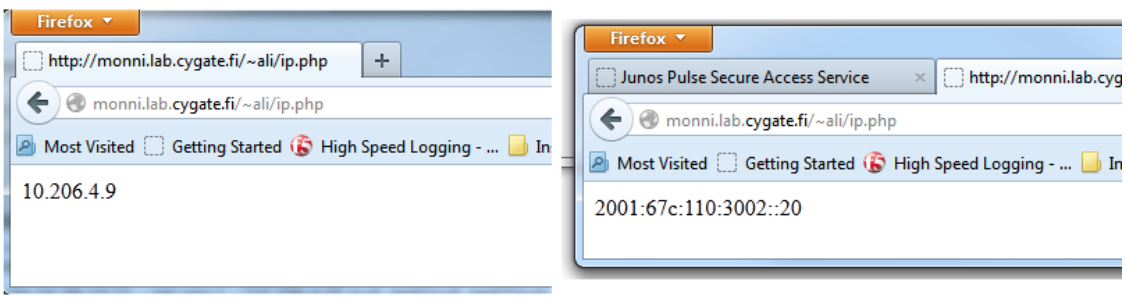
Apache-palvelimelle luotiin PHP-skripti, jolla x-forwarded-for-kenttä kaapattiin näkyviin web-sivulla. Mikäli PHP-skripti toteaa HTTP_X_FORWARDED_FOR-kentän tyhjäksi, palautetaan REMOTE_ADDR -kentän osoite, josta pyyntö on tullut, eli kuormanjakajan osoite.

```
 GNU nano 2.2.4                                File: ip.php

<?php
function getRealIpAddr()
{
    if (!empty($_SERVER['HTTP_CLIENT_IP']))   //check ip from share internet
    {
      $ip=$_SERVER['HTTP_CLIENT_IP'];
    }
    elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR']))   //to check ip is pass from proxy
    {
      $ip=$_SERVER['HTTP_X_FORWARDED_FOR'];
    }
    else
    {
      $ip=$_SERVER['REMOTE_ADDR'];
    }
    return $ip;
}

print getRealIpAddr();
?>
```

Kuva 17. X-forwarded-for-kentän kaappaaminen PHP-skriptillä. [23.]

F5 tukee x-forwarded-for-arvon lisäämistä HTTP-profiiliin. HTTP-profiileilla voidaan muokata iRulen tavoin HTTP-kehyksen arvoja, mutta rajoitetummin [4; 43]. Seuraavaksi luotiin uusi HTTP-profiili "x-forwarded-for", joka lisää x-forwarded-for arvon HTTP-kehykseen. Luotu x-forwarded-for -profiili liitettiin kuvan 15 web-virtuaalipavelimen "http"-profiilin tilalle. Myös iRuleilla voidaan lisätä läpi meneviin HTTP-kehyksiin x-forwarded-for-arvo. iRulet tulee määrittää erikseen käytettäväksi virtuaalipalvelimessa.

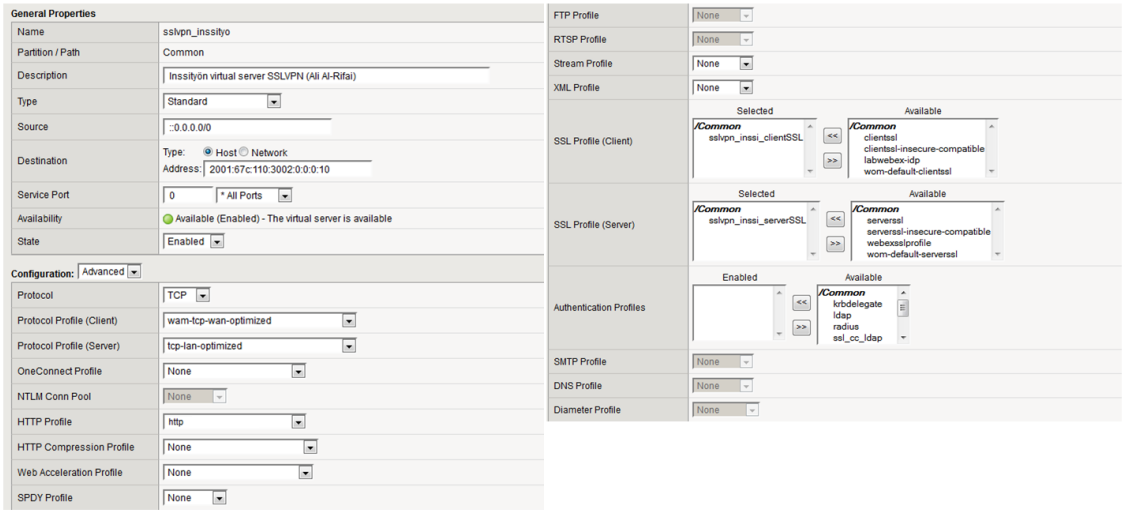
Onnistunut yhteydenmuodostus ja todellinen lähdeosoite voidaan todeta php-skriptin ansiosta suoraan ottamalla yhteyttä web-selaimella palvelimeen. Kuvassa 18 näkyy onnistunut yhteys, jossa osoite näytetään sivulla. Oikeanpuoleinen kuva esittää tilannetta, jossa virtuaalipalvelin on lisännyt x-forwarded-for-arvon HTTP-kehykseen.



Kuva 18. Oikeanpuoleinen kuva esittää PHP-skritpin ajoa, kun x-forwarded-for iRule on käytössä.

4.5 Toteutus 2: Juniper SSL VPN -palvelun IPv6-käyttöönotto

SSL VPN -toteutus aloitettiin luomalla virtuaalipalvelin ja palvelinfarmin. SSL VPN lisättiin sslvpn_inssi-farmiin. Toteutuksessa oli otettava huomioon muutamia seikkoja taustalla olevan palvelun vaatimuksista, jotka saattaisivat aiheuttaa ongelmia. Juniper SSL VPN lokittaa käyttäjän lähdeosoitteen omaan lokiinsa. Lokitus ei välttämättä tue IPv6-osoitteita kentässään ja tästä saattaa koitua ongelmia. SSL VPN ei myöskään tue yhteydenottoa HTTP:n yli, vaan yhteys luodaan turvallisesti HTTPS:n yli. Kuormanjakajan tulee purkaa SSL-salaus ja salata se uudelleen lähettäessään HTTPS-pyyntöä eteenpäin, jotta HTTP-kehyksen arvoja voidaan tutkia tai muokata. SSL-sertifikaatti ja purkuavain luotiin käyttämällä Linuxin OpenSSL-ohjelmaa. Liitteessä 1 käydään läpi sertifikaatin luonti.



Kuva 19. SSL VPN virtuaalipalvelimen luonti, jossa määritelty SSL-sertifikaatti asiakas- ja palvelinpuolelle.

Virtuaalipalvelimen ja SSL-sertifikaatin ja avaimen luonnin jälkeen sertifikaatti liitetään virtuaalipalvelimen profiiliin. BIG-IP LTM pystyy purkamaan HTTPS-pyynnön, kun sille määritellään SSL-profiili, jossa annetaan sekä sertifikaatti että sertifikaatin purkuavain. ClientsideSSL:llä määritellään asiakkaalle lähetettävä sertifikaatti. Laitteen avatessa yhteyttä taustalla olevalle palvelulle, se käyttää ServersideSSL-profiilia ja käyttää sertifikaattia palvelimelle keskustellessaan. Sertifikaatti ja avain täytyy antaa samalla nimellä laitteelle, jotta ne pystytään tunnistamaan toistensa vastineiksi. Sertifikaatti tunnistetaan .crt päätteestä ja purkuavain .key päätteestä. [44; 45.]

Yhteyden muodostaminen IPv6-osoitteeseen kohdattiin ensimmäinen vastoinkäyminen, kun HTTP-kehyksen host-kenttä sisälsi IPv6-osoitteen eikä SSL VPN päästänyt pyyntöä eteenpäin. Kuva 20 havainnollistaa virheviestin.

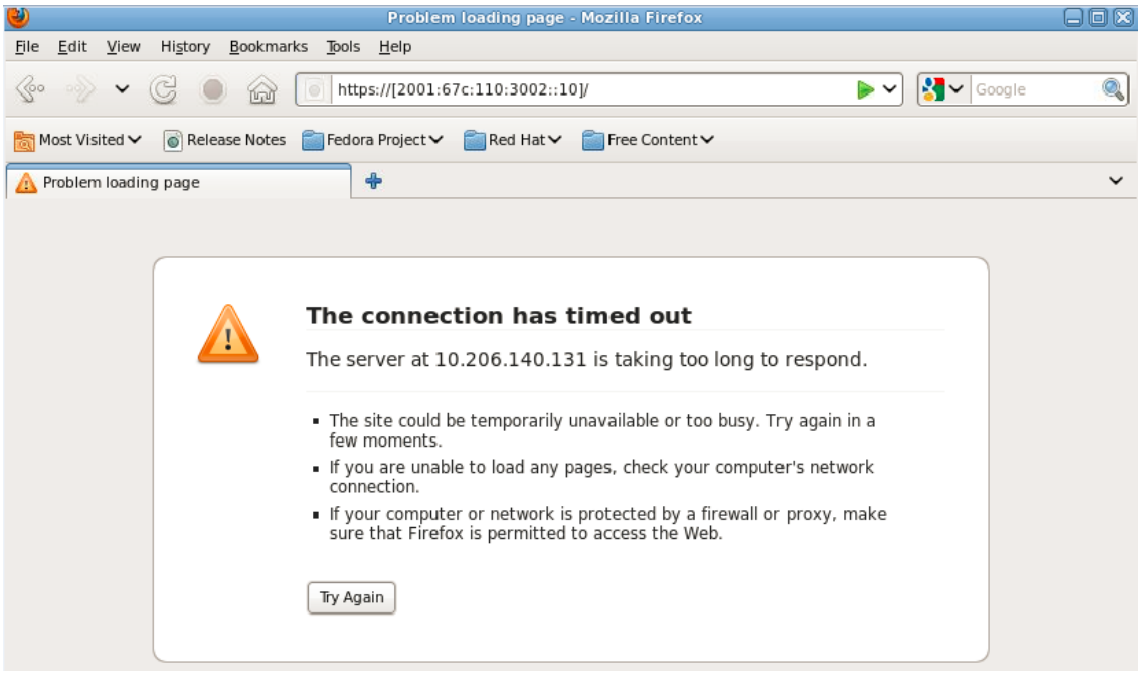
Kuva 20. SSL VPN -virtuaalipalvelimen IPv6-osoitteeseen kohdistettu HTTP-pyyntö ja virheviesti.

HTTP-kehyksen host-kenttä sisältää tiedon HTTP-pyynnön kohteesta, sekä pyynnön porttinumeron ”host:portti” -muodossa. Kenttä voi sisältää joko IP-osoitteen tai DNS-nimen. [52, s. 6.]

Ongelman selvittämiseksi tutkittiin mahdollisuutta muuttaa HTTP-pyynnön host-kenttää kuormanjakajalla iRuleja käyttämällä. Kappaleessa 5 viitattiin mahdollisuuteen muokata HTTP-kehyksen arvoja eri yhteysvaiheissa, joita päädyttiin tutkimaan tarkemmin. Host-kentän muokkaamista pystytään toteuttamaan kahdessa eri vaiheessa, asiakkaan ottaessa yhteyttä web-palvelimen virtuaalipalvelimeen ja kun kuormanjakaja ottaa yhteyttä itse palvelimeen. iRuleja tutkittiin F5-tukisivustoilta ongelman selvittämiseksi. Ohjeistuksen perusteella kenttää ei saada muokattua, kun yhteys muodostetaan kuormantasaajalta palvelimelle. iRulejen yhteystapahtumat (Events) HTTP_REQUEST eli asiakkaan HTTP-pyyntö ja HTTP_REQUEST_SEND eli kuormantasaajan lähettämä HTTP-pyyntö palvelimelle tukee vain asiakaspuolen parametrien muuttamista [58]. Testiksi toteutettiin iRule, jolla muutettiin käsin host-kenttä IPv4-osoitteeksi.

```
when HTTP_REQUEST_SEND {
clientside {
            HTTP::header replace Host "10.206.140.131:443"
}
}
```

Kuva 21 havainnollistaa ongelman, kun asiakkaalla ei ole pääsyä IPv4-verkon osoitteisiin.



Kuva 21. Host-kentän manipulointi IPv6-osoitteesta IPv4-osoitteeksi.

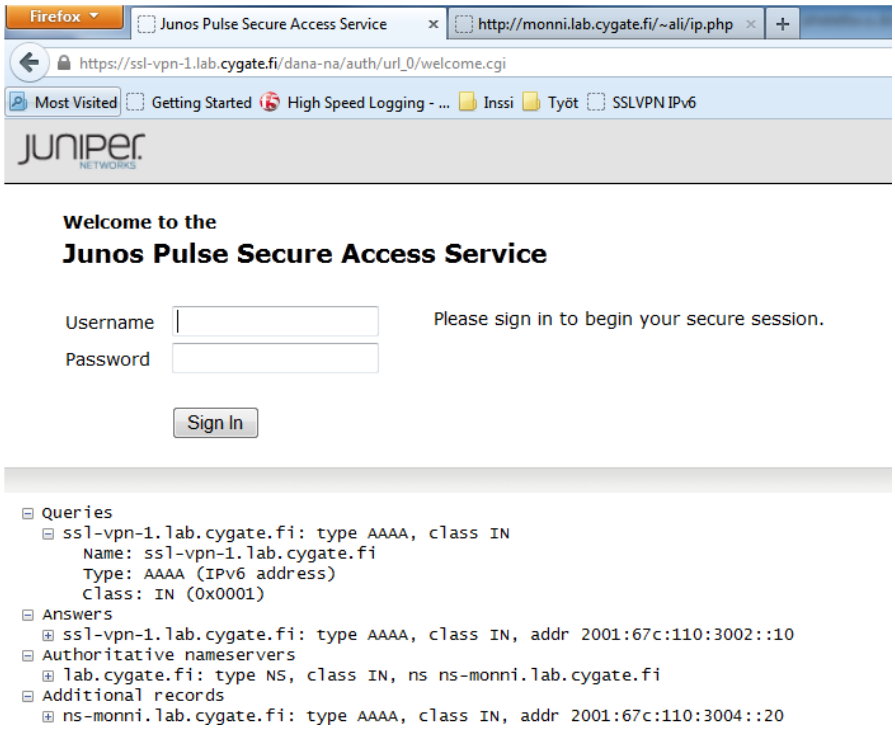
Tästä voitiinkin todeta, että annetuilla työkaluilla ei ole mahdollista ottaa yhteyttä taustalla olevaan palveluun ilman DNS-nimeä. Seuraavaksi lähdettiinkin tutkimaan eri mahdollisuuksia toteuttaa DNS-palvelin palvelun toteuttamiseksi. Yksinkertaisin toteutus oli luoda Linuxin BIND-nimipalvelin (Berkley Internet Name Domain), jonne luotaisiin IPv6-tietue osoittamaan SSL VPN:n virtuaalipalvelimen osoitteeseen.

Työssä käytetyn web-palvelimelle asennettiin DNS-palvelu Linuxin ohjelmistokirjastosta Tässä vaiheessa myös palvelimelle tuli määritellä IPv6-osoite, jonne DNS-kyselyt ohjattaisiin. Palvelimelle määriteltiin myös IPv6-osoite 2001:67c:110:3004::20.

```
root@m0nni:~# cat /etc/bind/db.lab.cygate.fi
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns-monni.lab.cygate.fi. monni.cygate.fi. (
                         2013011104     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;Nameservers
                           IN      NS          ns-monni.lab.cygate.fi.

$ORIGIN lab.cygate.fi.

;Hosts
ssl-vpn-1                  IN      AAAA        2001:67c:110:3002::10
monni                      IN      AAAA        2001:67c:110:3002::11
ns-monni                   IN      AAAA        2001:67c:110:3004::20
```

Kuva 22. Bind-nimipalvelimen IPv6-tietueiden konfigurointi.

Nimipalvelun asennuksen ja tietueiden lisäämisen jälkeen yhteyttä yritettiin jälleen. IPv6-koneelle määriteltiin muodostettu nimipalvelin ensisijaisesti käytettäväksi nimipalvelimeksi. Yhteyden muodostus selaimella osoitteeseen https://ssl-vpn-1.lab.cygate.fi saatiin muodostettua, sillä HTTP-kehyksen host-kentässä ei ole IPv6-osoitetta, josta SSL VPN antoi virheilmoituksen. Kuvassa 23 kuvataan onnistunut yhteyden muodostus DNS-nimellä käyttäen AAAA-tietuetta.



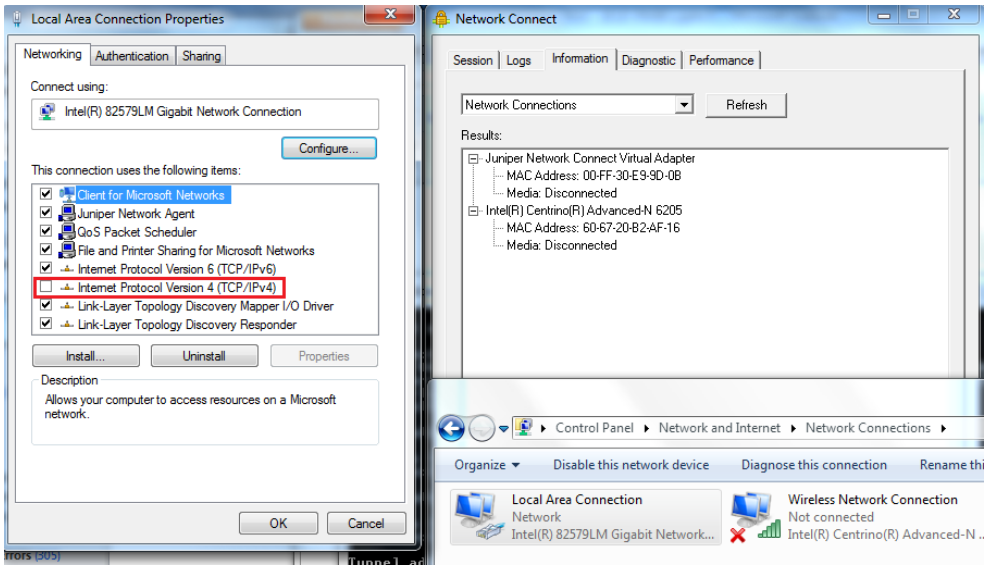
Kuva 23. Onnistunut yhteys SAS-portaaliin käyttämällä IPv6:n tukemaa AAAA-tietuetta.

Kun DNS-palvelin saatiin toimimaan, pystyttiin SSL VPN:n kanssa ilmenneet ongelmat yhteydenmuodostamisesta IP-osoitteilla kiertämään iRuleilla. Virtuaalipalvelimelle määriteltiin iRule, joka ohjaa IP-osoitteilla tulleet kyselyt käyttämään DNS-nimeä.

```
when HTTP_REQUEST {
            HTTP::header replace Host "ssl-vpn-1.lab.cygate.fi:443"
}
```

VPN-yhteyttä testattiin Network Connect (NC) -ohjelmalla, jota varten SSL VPN -laittellee luotiin profiili ja annettiin resurssiksi Network Connect. Käyttäjälle määriteltiin osoiteavaruudeksi 10.206.140.50 - 60. Avaruudesta varataan käyttäjälle osoite avattuun sessioon, jolla käyttäjä voi liikennöidä sisäverkossa sille sallittuihin osoitteisiin tai verkkoihin. Liikenne sallittiin työssä kaikkiin verkkoihin. Kun NC asentaa Java-komponentin Windows -työasemalle, se luo uuden virtuaaliverkkoliitännän, jonka kautta se tunneloi liikenteen yrityksen sisäverkkoon. Käyttäjän ottaessa yhteyttä palveluun virtuaaliliitännälle myönnetään osoite sille määritellystä osoiteavaruudesta.

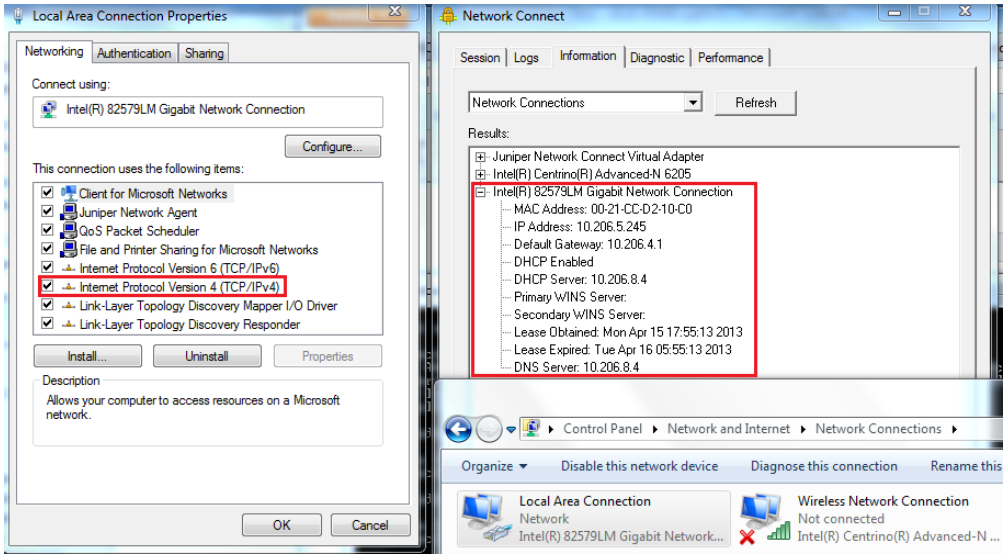
NC:n yhteyden muodostus ei onnistunut käytettäessä portaalia IPv6-verkosta. Kun verkkoliitännän IPv4 toiminnallisuus oli poistettu, ohjelma myös totesi fyysisen verkkoliitännän olevan alhaalla. Kuva 24 havainnollistaa tämän tilanteen.



Kuva 24. IPv4-toiminnallisuuden ollessa pois käytöstä Network Connect ei tunnistanut Gigabit Network -verkkoliitäntää.

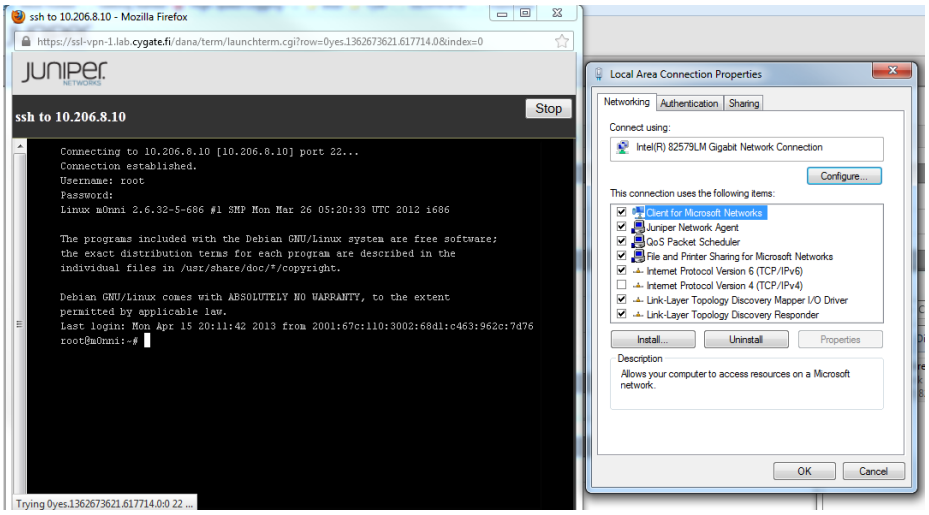
Kun fyysisen verkkoliitännän IPv4-toiminnallisuus otettiin takaisin käyttöön, NC saatin toimimaan, sillä laboratorion DHCP-palvelin jakoi IPv4-liitänälle osoitteen. Tästä voitiin

päätellä, että NC luo tunnelin ainoastaan IPv4-verkkoliitäntään. Mikäli Internetin yli yhteyttä ottavalla asiakkaalla on ainoastaan IPv6-osoite käytössä, ei NC voi tällä toteutuksella toimia. Asiakkaalla saattaa olla kuitenkin IPv4-toiminnallisuus päällä, mutta NC vaatii IPv4-verkon tavoittavan SSL VPN -sivuston, jotta tunneli voidaan luoda. Kuva 25 havainnollistaa tilanteen, kun IPv4-toiminnallisuus otettiin takaisin käyttöön. Saatu IPv4-osoite on testiympäristön DHCP:n jakama.



Kuva 25. Testi-PC:llä aktivoitiin IPv4-toiminnallisuus, jolloin NC tunnisti verkkoliitännän.

SSH-resursseja testattiin lisäämällä SAS-portaaliin linkki, joka avaa yhteyden sisäverkon *monni.lab.cygate.fi*-palvelimelle. Linkki avaa Java-sovelluksen, joka suoritetaan SSL VPN -laitteella. Yhteys saatiin toimimaan ilmaan mitään ongelmia. Kuva 26 havainnollistaa SSH-yhteyden muodostamisen, kun IPv4-toiminnallisuus on poistettu käytöstä testaamisen ajaksi.



Kuva 26. Onnistunut SSH-yhteys monni.lab.cygate.fi -palvelimelle SAS-portaalista.

4.6 Yhteyksien lokitus

Onnistuneiden testien jälkeen kummassakin tapauksessa palvelimien logit täyttyvät Big-IP:n sisäisen osoitteen yhteydenotoista. Tavallisen web-palvelimen tapauksessa tieto pystyttiin viemään x-forwarded-for-arvon perusteella aina itse palvelimelle asti, joka vaatii muutoksia palvelimen pääsylokituksen parametreihin. Mikäli taustalla olevan palvelun logitusparametrejä on hankala tai mahdotonta muokata, voidaan lokitus IPv6-yhteydenotoista keskittää yhteen paikkaan, jotta voidaan säilyttää lokitustiedot alkuperäisistä osoitteista.

F5-tukisivusto DevCentral on julkaissut lokitusohjeet x-forwarded-for-arvon säilyttämiseksi sekä Apache että Microsoft IIS (Internet Information Services) web-palvelimille. Ohjeessa Apachen httpd.conf-konfigurointitiedostoon luodaan uusi lokitusformaatti, sekä lokitustiedosto jonne otetaan talteen käyttäjän lähdeosoite. Seuraavilla asetuksilla voitaisiin ottaa käyttöön x-forwarded-for Apachessa. [26.]

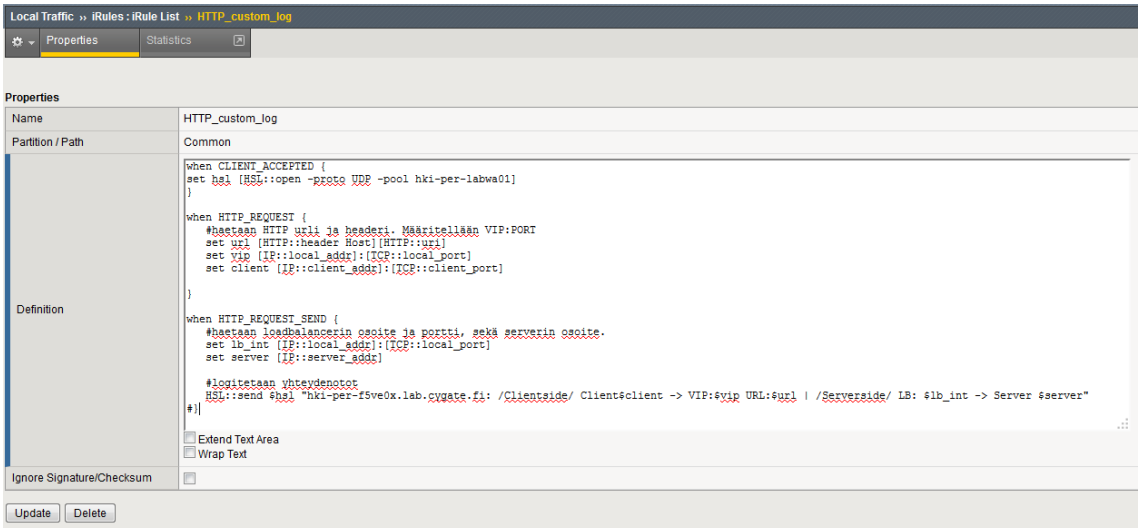
- LogFormat "%v %{X-Forwarded-For}i %l %u %t \"%r\" %>s %b" X-Forwarded-For

- CustomLog /var/log/apache/www.example.com-xforwarded.log X-Forwarded-For.

Big-IP:llä voidaan kerätä kootusti lokit myös keskeiselle lokipalvelimelle kaikista läpimenevistä yhteyksistä. Työssä käytettiin iRuleilla tuettua High Speed Logging (HSL) -ominaisuutta, jolla voidaan lähettää lokia palvelimille. HSL ei kuormita laitetta yhtä paljon kuin tavanomaisen lokin kerääminen ja muisti- ja prosessorikuorma saadaan pysymään alle 10 % laitteen resursseista. HSL tukee syslogin lähetystä TCP- ja UDP-protokollilla. [57.]

Syslog-palvelin otettiin käyttöön myös Linux-palvelimella, jonne lokit syötettäisiin. BIG-IP:llä luotiin uusi palvelinfarmi, jonne lisättiin syslog-viestejä vastaanottava palvelin syslogin käyttämällä portilla UDP 514. DevCentralin sivuilta löydetyillä HSL-ohjeilla luotiin iRulet kummallekin virtuaalipalvelimelle lokituksen saamiseksi keskitetylle syslog-palvelimelle. iRulessa määritellään asiakkaan avatessa yhteys CLIENT_ACCEPTED-tapahtumalla, jossa määritellään muuttuja ”hsl” -komennolla ”set hsl”, jossa määritellään HSL-yhteyden parametrit. Komennossa määritellään käytettäväksi protokollaksi UDP ja valitaan farmiksi Syslog. HTTP_REQUEST-tapahtumassa, asiakkaan lähettäessä HTTP-kyselyä kuormantasaajalle kaapataan HTTP-pyynnön URL- ja VIP-osoite, eli virtuaalipalvelimen osoite.

Client-muuttujalla saadaan asiakkaan osoite ja portti. Node-muuttujalla otetaan talteen virtuaalipalvelimen osoite ja portti. NodeResp-muuttujalla kaapataan HTTP-tilakoodi.



Kuva 27. Lokituksen määrittelevä iRule jossa käytetään High Speed Loggingia.

iRulen luonnin jälkeen se liitettiin kumpaankin virtuaalipalvelimeen, jotta yhteydenotto-lokit lähetetään syslog-palvelimelle. Yhteyden muodostamisen jälkeen virtuaalipalvelimille saatiin seuraavanlaisia lokeja muodostetuista yhteyksistä syslog-palvelimelle.

```
Apr 24 18:35:04 10.206.4.9 hki-per-f5ve0x.lab.cygate.fi: /Clientside/
Client2001:67c:110:3002::20:56368 -> VIP:2001:67c:110:3002::10:443
URL:ssl-vpn-1.lab.cygate.fi/dana-na/auth/welcome.cgi?p=rolelogo |
/Serverside/ LB: 10.206.4.9:56368 -> Server 10.206.140.131

Apr 24 18:35:09 10.206.4.9 hki-per-f5ve0x.lab.cygate.fi: /Clientside/
Client2001:67c:110:3002::20:56372 -> VIP:2001:67c:110:3002::11:80
URL:monni.lab.cygate.fi/~ali/ip.php | /Serverside/ LB: 10.206.4.9:56372 ->
Server 10.206.8.10
```

Lokituksesta voidaan seurata pyyntöjä lähettävien asiakkaiden alkuperäiset osoitteet sekä pyynnössä käytetty portti. BIG-IP:n sisäinen osoite sekä portti on hyvä lokittaa, sillä taustalla olevan palvelun lokitus saattaa täyttyä ainoastaan BIG-IP:n sisäisestä osoitteesta. Jotta kuormantasaajan ja taustalla olevan palvelun lokeja voidaan verrata toisiinsa, täytyy kummankin palvelimen käyttää samaan NTP-pavelinta (Network Time Protocol), jotta aikaleimat yhteyksistä täsmäävät.

5 Päätelmät

Työn tarkoituksena oli selvittää, miten IPv4-verkolla voidaan tuottaa IPv6-verkolla palveluita BIG-IP LTM tuotteella. Työssä päästiin osittain tavoitteisiin palvelun tuottamiseksi IPv6-osoitteilla. Tavanomaisten web-sivujen toteuttaminen laitteella luonnistui helposti ja niiden käyttöönotto ei vaatinut verkolta suuriakaan muutoksia. Haastavaksi työssä koitui kuitenkin SSL VPN toteutuksen Javaa käyttävä Network Connect VPN -tunnelointisovellus, jonka toimintaperiaatetta sovellustasolla ei pystytty arvioimaan. NC ei tunnistanut IPv6-verkkoliitäntää, kun IPv4-verkkoliitäntä oli poistettu käytöstä, eikä tunnelia pystytty luomaan. Laite antoi myös virheilmoituksen ottaessa palveluun yhteyttä pelkällä IPv6-osoitteella. Ongelma selvitettiin käyttämällä DNS-nimeä yhteydenotossa.

IPv6-läsnäolon toteuttaminen yritykselle ei vaadi Big-IP:llä suuriakaan ponnistuksia ja saattaa olla myös markkinoinnin kannalta hyödyllinen yrityksen imagolle. Laboratorioverkon IPv4-palvelimet saatiin hetkessä IPv6-verkon tavoitettavaksi. Tämän lisäksi julkisille DNS-palvelimille tulee lisätä AAAA-tietueet ja IPv6-osoite, mikäli asiakas on tavoitettavissa ainoastaan IPv6-verkolla, kuten työssä asetettiin olettamukseksi.

Erityisesti Hosting-palveluita tarjoavilla yrityksillä on tavanomaisesti jo kuormanjakaja käytössä eli laitteistoakin löytyy jo entuudestaan. Yleinen trendi yrityksissä vaikuttaa olevan, että protokollan käyttöönottoa ei nähdä vielä lähiaikoina tarpeelliseksi. Työssä tehdyllä toteutuksella ei aseteta koko yrityksen sisäistä verkkoa uudelle protokollalle "alttiiksi", mutta saadaan tärkeää kokemusta IPv6-käyttöönotosta.

Mikäli toteutusta harkitsee oman yrityksensä verkkoon, tulee web-sovellusten toimintaa tutkia ja testata tarkasti ennen tuotantoon ottamista. Sovellukset eivät välttämättä tunnista IPv6-osoitteita tai kuten Network Connect -tunnelointisovelluksen tapauksessa, vaativat IPv4-verkkoliitännän olevan kytkettynä päälle ja yhteydessä palveluun IPv4-verkon kautta. Näitä on vaikea lähteä tutkimaan, mikäli sovelluksen toimintaperiaatetta ei tunneta. Tässä työssä todettiinkin, että toteutusta ei voida soveltaa kaikkiin palveluihin. Työssä tehdyllä toteutuksella voidaan tulevaisuudessa mahdollisesti viivästyttää vanhojen järjestelmien, niin kutsuttujen legacy-järjestelmien, päivittämistä uudelle protokollalle. Legacy-järjestelmien "päivittäminen" voi vaatia koko sovelluksen uudelleen luomista. Lokituksen toteutusta täytyy myös harkita, pystytäänkö taustalla olevalle palvelulle välittämään x-forwarded-for-arvolla käyttäjän alkuperäinen lähdeosoite, vai kerätäänkö kaikki lokit keskitetysti yhdelle lokipalvelimelle.

Tämän työn tuloksena eräs Cygaten asiakas otti käyttöön IPv6-osoitteet heidän web-palvelimilleen työn toteutuksen tavalla.

Lähteet

1 Introduction to IPv6. tfk techonologies 2012.

2 Ipv6 – The History and Timeline. Verkkodokumentti. Luettu 16.9.2012. Saatavissa: http://www.ipv6.com/articles/general/timeline-of-ipv6.htm.

3 Statistics. Google IPv6. Verkkodokumentti. Luettu 5.4.2013. Saatavissa: http://www.google.com/ipv6/statistics.html#tab=ipv6-adoption.

4 Using "X-Forwarded-For" in Apache or PHP. Verkkodokumentti. luettu 5.4.2013. Saatavissa:https://devcentral.f5.com/weblogs/macvittie/archive/2008/06/02/3323.aspx.

5 Lokiohje. Valtivarainministeriö. Verkkodokumentti. Luettu 1.10.2012. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/name.jsp.

6 IPv6 header. Verkkodokumentti. Luettu 7.12.2012. Saatavissa: http://www.ietf.org/rfc/rfc2460.txt.

7 IPv6 Extension Header Review and Considerations. Luettu 2.1.2013. Saatavissa: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html.

8 IPv6 Header simplification. Verkkodokumentti. Luettu 10.1.2013. Saatavissa: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.commadmn/doc/commadmndita/tcpip_ipv6_headersimplif.htm.

9 IPv6 Jumbograms. Verkkodokumentti. Luettu 20.1.2013. Saatavissa: http://www.ietf.org/rfc/rfc2460.txt.

10 IP Version 6 Addressing Architecture. Verkkodokumentti. Luettu 27.1.2013. Saatavissa: http://tools.ietf.org/html/rfc4291.

11 Basic Transition Mechanisms for IPv6 Hosts and Routers. Verkkodokumentti. Luettu 19.2.2013. Saatavissa: http://tools.ietf.org/html/rfc4213.

12 Deploying IPv6 in the Internet Edge. Verkkodokumentti. Luettu 19.2.2013. Saatavissa: http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Internet_Edge/InternetEdgeIPv6.html#wp390518.

13 Framework for IPV4/IPV6 Translation. Luettu 19.2.2013. Saatavissa: http://tools.ietf.org/html/draft-ietf-behave-v6v4-framework-10#section-2.1.

14 RIPE NCC IPv4 Available Pool – Graph. Verkkodokumentti. Luettu 19.2.2013. Saatavissa: http://www.ripe.net/internet-coordination/ipv4-exhaustion/ipv4-available-pool-graph.

15 RIPE NCC Begins to Allocate IPv4 Address Space from the Last /8. Luettu 19.2.2013. Verkkodokumentti. Saatavissa: http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8.

16 What Enterprises Should Do About IPv6 in 2011. Verkkodokumentti. Luettu 18.3.2013. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper_c11-586154.pdf.

17 Forwarded HTTP Extension. Luettu 26.3.2013. Verkkodokumentti. Saatavissa: http://tools.ietf.org/html/draft-ietf-appsawg-http-forwarded-10#section-4.

18 IPv6 Global Unicast Address Assignments. Verkkodokumentti. Luettu 27.3.2013. Saatavissa: http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml.

19 IPv6 FAQ. Verkkodokumentti. Luettu 27.3.2013. Saatavissa: http://www.ripe.net/lir-services/resource-management/faq/faq-ipv6.

20 IPv6 Global Unicast Address Format. Verkkodokumentti. Luettu 27.3.2013. Saatavissa: http://www.ietf.org/rfc/rfc3587.txt.

21 IPv6 Address Allocation and Assignment Policy. Verkkodokumentti. Luettu 27.3.2013. Saatavissa: http://www.ripe.net/ripe/docs/ripe-552#lir.

22 What is TLS/SSL. Verkkodokumentti. Luettu 28.3.2013. Saatavissa: http://technet.microsoft.com/en-us/library/cc784450%28v=ws.10%29.aspx.

23 Juniper Networks VPN Decision Guide. Verkkodokumentti. Luettu 28.3.2013. Saatavissa: http://www.juniper.net/us/en/local/pdf/whitepapers/2000232-en.pdf.

24 How can I get the user's IP address in PHP. Verkkodokumentti. Luettu 28.3.2013. Saatavissa: http://stackoverflow.com/questions/848091/how-can-i-get-the-users-ip-address-in-php.

25 IPv4-verkosta siirtyminen IPv6-verkkoon organisaatiossa. Verkkodokumentti. Luettu 28.3.2013. Saatavissa: http://publications.theseus.fi/handle/10024/46221.

26 Using the X-Forwarded-For HTTP header to preserve the original client IP address for traffic translated by a SNAT. Verkkodokumentti. Luettu 2.4.2013. Saatavissa: http://support.f5.com/kb/en-us/solutions/public/4000/800/sol4816.html.

27 IPV6 Enabled Sites. Verkkodokumentti. Luettu 4.4.2013. Saatavissa: http://www.worldipv6day.org/ipv6-enabled-websites/.

28 Internetin suuri ipv6-muutos vaatii testaamista. Verkkodokumentti. Luettu 4.4.2013. Saatavissa: http://www.3t.fi/artikkeli/uutiset/teknologia/internetin_suuri_ipv6_muutos_vaatii_testaamista.

29 Neigbor Discovery for IPv6. Verkkodokumentti. Luettu 4.4.2013. Saatavissa: http://www.ietf.org/rfc/rfc2461.txt.

30 Protocol Complications with NAT. Verkkodokumentti. Luettu 4.4.2013. Saatavissa: http://www.ietf.org/rfc/rfc3027.txt.

31 IANA IPv4 Address Space Registry. Verkkodokumentti. Luettu 5.4.2013. Saatavissa: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml.

32 Number Resources. Verkkodokumentti. Luettu 7.4.2013. Saatavissa: http://www.iana.org/numbers.

33 RFC1981. Verkkodokumentti. Luettu 8.4.2013. Saatavissa: http://tools.ietf.org/html/rfc1981.

34 Transition Planning for Internet Protocol Version 6 (IPv6). Verkkodokumentti. Luettu. 8.4.2013. Saatavissa: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf.

35 APNIC's IPv4 pool usage. Verkkodokumentti. Luettu 8.4.2013. Saatavissa: http://www.apnic.net/community/ipv4-exhaustion/graphical-information.

36 IPv6 distribution within Eastern Asia. Verkkodokumentti. Luettu 8.4.2013. Saatavissa: http://www.apnic.net/publications/research-and-insights/stats/ipv6-eastern-asia.

37 TMOS: Redefining the Solution. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://www.f5.com/pdf/white-papers/tmos-wp.pdf.

38 Application Delivery Controller. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://support.f5.com/kb/en-us/solutions/public/8000/000/sol8082.html.

39 BIG-IP Modules. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://www.f5.com/pdf/products/big-ip-modules-ds.pdf.

40 Local Traffic Manager. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://www.f5.com/products/big-ip/big-ip-local-traffic-manager/specs/.

41 ASKF5 Knowledge Base: SOL8082. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://support.f5.com/kb/en-us/solutions/public/8000/000/sol8082.html.

42 iRules. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: https://devcentral.f5.com/wiki/iRules.HomePage.ashx.

43 Profiles for Managing HTTP Traffic. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-concepts-11-2-0/ltm_http_profiles.html#1226979.

44 Managing Client-side HTTPS Traffic using a CA-signed Certifiacate. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-11-2-0/16.html.

45 Overview of the Server SSL profile. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://support.f5.com/kb/en-us/solutions/public/11000/200/sol11220.html.

46 Forward and Reverse Proxies. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://httpd.apache.org/docs/2.0/mod/mod_proxy.html#forwardreverse.

47 SA Series: Features and Benefits. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://www.juniper.net/us/en/products-services/security/sa-series/#features.

48 Resource Policies. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://www.juniper.net/techpubs/en_US/sa7.1/topics/concept/secure-access-resource-policies-overview.html.

49 Network Connect. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://www.juniper.net/techpubs/software/ive/guides/howtos/How_To_NC_Config.pdf.

50 Juniper Knowledge Base:KB8619. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://kb.juniper.net/InfoCenter/index?page=content&id=KB8619.

51 Unique Local IPv6 Unicast Addresses. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://tools.ietf.org/html/rfc4193#section-5.2.

52 Hypertext Transfer Protocol. Verkkodokumentti. Luettu 19.4.2013. Saatavissa: http://tools.ietf.org/html/rfc2616#section-1.1.

53 Neighbor Discover for IPv6. Verkkodokumentti. Luettu 23.4.2013. Saatavissa: http://tools.ietf.org/html/rfc2461#section-1.

54 IPv6 neighbor discovery. Verkkodokumentti. Luettu 23.4.2013. Saatavissa: http://packetlife.net/blog/2008/aug/28/ipv6-neighbor-discovery/.

55 Cisco IPv6 Training Stateful or Stateless DHCP. Luettu 23.4.2013. Saatavissa: http://www.ciscoipv6ittechtips.com/differencebetweenstatefulandstatelessdhcp.html.

56 EUI-64. Verkkodokumentti. Luettu 23.4.2013. Saatavissa. http://mars.tekkom.dk/mediawiki/index.php/EUI-64.

57 High Speed Logging. Verkkodokumentti. Luettu 23.4.2013. Saatavissa: https://devcentral.f5.com/wiki/irules.hsl.ashx.

58 HTTP_REQUEST_SEND. Verkkodokumentti. Luettu 26.4.2013. Saatavissa: https://devcentral.f5.com/wiki/iRules.http_request_send.ashx.

SSL-sertifikaatin luonti

```
### Luodaan 1024 bitin RSA avain ###
debian:~$ openssl genrsa -des3 -out sslvpn1.lab.cygate.fi.orig.key 1024
Generating RSA private key, 1024 bit long modulus
.....................................++++++
.................++++++
e is 65537 (0x10001)
Enter pass phrase for sslvpn1.lab.cygate.fi.orig.key:
Verifying - Enter pass phrase for sslvpn1.lab.cygate.fi.orig.key:
###
debian:~$ openssl rsa -in sslvpn1.lab.cygate.fi.orig.key -out sslvpn1.lab.cygate.fi.key
Enter pass phrase for sslvpn1.lab.cygate.fi.orig.key:
writing RSA key

### Luodaan sertifikaattipyyntötiedosto .csr (Certificate Signing Request), joka lähete-
tään allekirjoitettavaksi ###
debian:~$ openssl req -new -key ssl-vpn-1.lab.cygate.fi.key -out ssl-vpn-
1.lab.cygate.fi.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:??
State or Province Name (full name) []:??
Locality Name (eg, city) [Default City]:??
Organization Name (eg, company) [Default Company Ltd]:Cygate
Organizational Unit Name (eg, section) []:??
Common Name (eg, your name or your server's hostname) []:ssl-vpn-1.lab.cygate.fi
Email Address []:??

### Allekirjoitetaan sertifikaattipyyntö ###
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
ali.al-rifai@hki-per-labwa01:~$ openssl x509 -req -days 1825 -in ssl-vpn-
1.lab.cygate.fi.csr -signkey ssl-vpn-1.lab.cygate.fi.key -out ssl-vpn-
1.lab.cygate.fi.crt
Signature ok
subject=/C=??/ST=??/L=??/O=Cygate/OU=??/CN=ssl-vpn-1.lab.cygate.fi/emailAddress=??
Getting Private key

debian:~$ ls -ll
```

```
total 24
*
-rw-r--r-- 1 ali.al-rifai nfsnobody 899 Feb 13 17:19 ssl-vpn-1.lab.cygate.fi.crt
-rw-r--r-- 1 ali.al-rifai nfsnobody 676 Feb 13 16:55 ssl-vpn-1.lab.cygate.fi.csr
-rw-r--r-- 1 ali.al-rifai nfsnobody 887 Feb 13 16:44 ssl-vpn-1.lab.cygate.fi.key
*

### Tarkastetaan luotu RSA-avain ###
debian:~$ cat ssl-vpn-1.lab.cygate.fi.key
-----BEGIN RSA PRIVATE KEY-----
### RSA avain piilotettu ###
-----END RSA PRIVATE KEY-----
### Tarkastetaan luotu sertifikaatti ###
debian:~$ cat ssl-vpn-1.lab.cygate.fi.crt
-----BEGIN CERTIFICATE-----
MIICazCCAdQCCQDcza0AOtm0cjANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwI/
PzELMAkGA1UECAwCPz8xCzAJBgNVBAcMAj8/MQ8wDQYDVQQKDAZDeWdhdGUxCzAJ
BgNVBAsMAj8/MSAwHgYDVQQDDBdzc2wtdnBuLTEubGFiLmN5Z2F0ZS5maTERMA8G
CSqGSIb3DQEJARYCPz8wHhcNMTMwMjEzMTUxOTIwWhcNMTgwMjEyMTUxOTIwWjB6
MQswCQYDVQQGEwI/PzELMAkGA1UECAwCPz8xCzAJBgNVBAcMAj8/MQ8wDQYDVQQK
DAZDeWdhdGUxCzAJBgNVBAsMAj8/MSAwHgYDVQQDDBdzc2wtdnBuLTEubGFiLmN5
Z2F0ZS5maTERMA8GCSqGSIb3DQEJARYCPz8wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMpR6NLvPQQ0ZDRf1iV6JjonrXVOZEwqfrRuRtycR0qt+rwgMswxZ8jD
NXKsytqGNA/P5U3F4kzR8wCsNZu+cGHhxLZyEyMX82B76LDUq6wxWyobr0ViDWpF
JZDj17CTYStvC52zc4YkxFZ2TkDMdovWCgB3mCiPhWbFhVnOF4rzAgMBAAEwDQYJ
KoZIhvcNAQEFBQADgYEAWpSYuNVoZcF7OR6RQByoTHieX4EWFmL3mz6j5xgDKaMs
tj40K0hqkz6rZiU9LBmKxHD4QzTwvUs1ohGtWAQbVPf7l6HODcp2fIsuD1YPuS1P
zFhPo/VcWYNdPwKEhfNKm3FnBhFShpoYLur/xgNEIxgChjdlkkp8xH2w9CcWYys=
-----END CERTIFICATE-----
```