



DHCPv6-palvelun suunnittelu ja käyttöönotto operaattoriympäristössä

Petri Hätönen

2021 Laurea



Laurea-ammattikorkeakoulu

DHCPv6-palvelun suunnittelu ja käyttöönotto operaattoriympäristössä

Petri Hätönen
Tietojenkäsittelyn koulutus
Opinnäytetyö
Toukokuu, 2021

Petri Hätönen

DHCPv6-palvelun suunnittelu ja käyttöönotto operaattoriympäristössä

Vuosi

2021

Sivumäärä 43

Tämän opinnäytetyön toimeksiantajana toimi työnantaja. Työn tavoitteena oli suunnitella, asentaa ja ottaa käyttöön uusi DHCPv6-palvelin, sekä siirtää palvelu uusille verkkolaitteille. Näillä verkkoon tehtävillä uudistuksilla työn toimeksiantaja saa tulevaisuudessa kustannussäästöjä, pienentää hiilijalanjälkeä ja parantaa palvelun toimintavarmuutta. Uudet ohjelmistoversiot lisäävät palveluun myös uusia ominaisuuksia.

Työssä tutustuttiin erilaisiin DHCPv6-palvelun toteutustapoihin sekä verkkoarkkitehtuureihin ja pyrittiin löytämään paras ratkaisu palvelun toteuttamiseksi. Apuna työssä käytettiin sisäisiä- sekä ulkoisia sidosryhmiä parhaan konfiguraation ja parhaiden käytäntöjen löytämiseksi.

Kun sopivaan ratkaisuun päädyttiin, niin palvelin suunniteltiin sekä asennettiin. Lopuksi järjestelmiä testattiin ja verrattiin rinnakkain. Testauksessa käytettiin erillistä DHCPv6-palvelimen testaukseen tarkoitettua testausohjelmistoa. Järjestelmien väliset erot analysoitiin sekä niistä tehtiin johtopäätökset. Lopuksi uusi järjestelmä todettiin toimivaksi.

Opinnäytetyön ohessa selville tulleiden seikkojen vuoksi uutta DHCPv6-ratkaisua ei vielä otettu käyttöön. Palvelun kehittämistä ja suunnittelua päätettiin jatkaa vielä pidemmälle, jotta päästäisiin toivottuihin lopputuloksiin.

Tämä jatkokehitys mahdollistaa, että palvelusta saadaan mahdollisimman kattava. Tulevaisuudessa reitittimet sekä palvelimet on tarkoitus kahdentaa IPv4 DHCP- sekä IPv6 DHCPv6-palvelujen osalta. Tämä kahdentaminen mahdollistaa, että uusista palvelimista sekä reitittimistä saadaan täysi hyöty ja päästään palveluiden laadussa vähintään Traficomien määrittelemien suositusten tasolle.

Asiasanat: tietoliikenne, internet operaattori, DHCPv6, IPv6

Petri Hätönen

Planning and Implementing DHCPv6 Service in Operator Network

Year 2021 Pages 43

This thesis was ordered by employer. The scope of the thesis was to plan, implement and bring the new DHCPv6 server into use. Scope also included moving service to new network devices. Employer profits from these operations by cost savings, smaller carbon footprint and better network reliability. New software versions also add numerous new features to the services.

Work with this thesis taught different ways to build a DHCPv6 service. Different network architectures were studied and used to find the best practices. Internal and external stakeholders also helped in developing the solution.

When adequate solutions were found for the server, it was planned and implemented. After implementation, systems were compared by side-to-side measurement. These indicated that the new service was working as planned.

During the thesis, it became apparent that the new DHCPv6 service should not yet be used in the network. There was a need to continue planning and development of the service, so it could meet the needed requirements.

Servers and routers should be duplicated for both IPv4 and IPv6 DHCP services so they would be comprehensive enough. This also ensures that the service meets the minimum Traficom requirements in the future.

Keywords: Telecommunications, Internet operator, DHCPv6, IPv6

Sisällys

1	Johdanto.....	6
2	Opinnäytetyön taustat sekä tavoitteet.....	6
2.1	Aihealueen rajaus	7
2.2	Opinnäytetyön tutkimuskysymykset	8
2.3	Opinnäytetyön kehitys- ja tutkimusmenetelmät	8
3	Keskeiset käsitteet	8
4	Internet Engineering Task Force	10
5	Internet Protokolla	10
5.1	Internet protokolla versio 4	10
5.2	Internet protokolla versio 6	11
6	Parhaat käytännöt ja suositukset DHCPv6-palveluissa	11
7	Verkoarkkitehtuuri.....	12
7.1	Modulaarinen arkkitehtuuri	12
8	Nykyinen DHCPv6-palvelu	13
8.1	Uuden DHCPv6-palvelun suunnitelma	14
8.2	Tulevien muiden muutoksien huomioiminen	15
9	Palvelinohjelmisto	16
10	Testaus kotilaboratoriossa	17
10.1	Kea DHCP-ohjelmiston asennus	18
10.2	Konfiguraation konvertoiminen	20
10.3	KeaMA:lla konvertoidun konfiguraatitiedoston sisältö	21
10.4	Toimivuuden testaus.....	24
11	Tuotantopalvelimen käyttöjärjestelmän valinta.....	25
11.1	Kea DHCP-ohjelmiston asennus tuotantopalvelimelle	26
12	IPv6-osoitteiden välityspalvelun testaus uudella reitittimellä.....	26
13	Palvelinten suorituskyvyn tutkiminen	27
13.1	Suorituskykymittausten analyysi	28
14	Uuden DHCPv6-palvelimen käyttöönotto	32
15	Johtopäätökset ja yhteenveto.....	32
16	Jatkokehitysehdotukset	33
17	Oman oppimisen arviointi	34
	Lähteet.....	35
	Kuviot	38
	Taulukot	39
	Liitteet	40

1 Johdanto

Vuonna 1965 Intelin yksi perustajista Gordon Moore esitti että ”prosessorien tehokkuus tuplaantuu aina kahden vuoden välein”. Tästä on luotu mikropiirien kehitysvauhtia kuvaileva Mooren laki. Vaikka väittämä ei välttämättä pitäisikään enää nykyään täysin paikkaansa, niin kehitys on kuitenkin ollut tähän päivään asti todella nopeaa. Tästä syystä tekniikan alalla toimivien yritysten on pysyttävä mukana uusien teknologioiden käyttöönotossa pysyäkseen kilpailukykyisinä. (Shein 2020.)

Edellä mainittu nopea teknologioiden kehitys pakottaa myös tietoliikenneoperaattorit uusimaan ja päivittämään palveluitaan sekä laitteistojaan jatkuvasti. Uusin teknologia takaa, että tietoliikenneoperaattorin asiakkaille pystytään tarjoamaan monipuolisimmat- sekä parhaat mahdolliset palvelut. Uudet teknologiat myös tuovat parannuksia laitteisiin sekä säästöjä sähkönkulutuksen pienenemisen muodossa. Ne myös säästävät henkilöstöltä aikaa palveluiden ylläpidossa vanhaan tekniikkaan verrattuna. (router-switch.com 2013.)

2 Opinnäytetyön taustat sekä tavoitteet

Tämä opinnäytetyö sai alkunsa tarpeesta uusia internetoperaattorin DHCPv6-palvelin ja sen tarvitsemat tietoliikennelaitteet. Uusi palvelin tulisi suunnitella niin että se integroituisi nykyiseen verkon topologiaan paremmin ja olisi toteutettavissa jo nykyisin käytössä olevilla uudemmilla verkkolaitteilla. Palvelimen toteuttamiseen tulisi löytää myös paras ratkaisumalli, joka mahdollistaa tulevat muutokset, skaalautuvuuden, helpon ylläpidon sekä palveluiden mahdollisimman korkean saatavuuden.

Työssä tulee ottaa huomioon myös ennakoimattomat kehitysmahdollisuudet, joita saattaa ilmetä työn edetessä. Samalla tulee miettiä olisiko jokin palveluun liittyvä muu osa-alue kehitettävissä ja paranneltavissa tulevaisuudessa. Näitä mahdollisia kehitysmahdollisuuksia ovat esimerkiksi erilaiset ratkaisut, joilla palvelusta saataisiin varmatoimisempi.

DHCPv6-palvelu on ennen opinnäytetyön muutoksia toteutettu melko ikääntyneellä Cisco Systems laitevalmistajan reitittimellä, joka toimii DHCPv6-osoite pyyntöjen välittäjänä erilliselle virtuaaliympäristössä sijaitsevalle palvelimelle. Tämä nykyinen Ciscon reititin palvelee ainoastaan IPv6 DHCPv6-pyyntöjen välitystä, jonka vuoksi tämä toiminto tulisi siirtää jollekin muulle verkossa jo valmiiksi olevalle uudemmalle laitteelle. Myös DHCPv6-palvelinohjelmisto tulisi uusia, sekä samalla päivittää palvelimen käyttöjärjestelmä uudempaan.

Vanhat tietoliikennelaitteet ovat fyysisesti isompia kuin uudemmat laitteet ja vievät näin ollen tarpeettomasti tilaa tietoliikennekeskuksien laitekaapeissa. Uudet verkkolaitteet ovat myös tehokkaampia, jolloin niissä voidaan ajaa samaan aikaan useampia verkon palveluita. Yksittäisen laitteen suoran sähkönkulutuksen lisäksi palveluiden siirto toiselle laitteelle vähentää myös ilmastonin sähkönkulutusta. Opinnäytetyön toimeksiantajan yhtenä tärkeänä arvona onkin tuottaa palvelut ekologisesti kestäväällä ja yhteiskuntavastuullisella tavalla.

Palveluun muutoksia suunnitellessa tulee selvittää myös, minkälaisia vaihtoehtoja palvelun kahdentamiseen uusi DHCPv6-palvelinohjelmisto tukee. Huomioon tulee ottaa myös uusien päivitettyjen ohjelmistoversioiden tarjoamat mahdollisuudet verkon toiminnan ja vikasietoisuuden kannalta.

Opinnäytetyössä selvitän ensin nykyistä verkon topologiaa DHCPv6-palvelun osalta sekä pyrin hahmottamaan kokonaiskuvan palvelimen nykytilanteesta. Seuraavassa vaiheessa tutustun teorian kautta erilaisiin mahdollisuuksiin palvelun toteuttamiseksi. Selvitan myös, miten palvelu tulisi rakentaa parhaiden verkkoarkkitehtuuristen ominaisuuksien hyödyntämiseksi. Tarvittaessa käytän apuna sisäisiä- sekä ulkoisia sidosryhmiä parhaiden ratkaisujen sekä käytänteiden löytämiseksi.

Tarkoituksena on testata palvelun toiminta ensin hallituissa olosuhteissa omassa palvelin- ja verkkolaboratoriossani. Mikäli totean palvelun toimivaksi, niin asennan sen varsinaiselle tuotantoverkon virtuaalipalvelimelle koekäyttöön ja testattavaksi.

Uusi palvelu on tarkoitus rakentaa vanhan järjestelmän rinnalle. Tällöin palveluja voi verrata helposti keskenään. Työn edetessä tulee selvittää miten palvelinten suorituskykyä sekä laatua voi mitata. Näiden mittauksien tulokset tulee analysoida tarkasti, jotta uuden palvelimen toimivuus ja suorituskyky voidaan varmistaa testituloksien perusteella.

Toiminta tulee testata ennen käyttöönottoa riittävästi aidossa tuotantoverkkoympäristössä. Lopuksi tarkoituksena on siirtää kaikkien kuluttaja asiakkaiden IPv6 DHCPv6-palvelut uudelle DHCPv6-osoitteiden pyyntöjen välittämiseen tarkoitettulle reitittimelle sekä uudelle DHCPv6-palvelimelle

2.1 Aihealueen rajaus

Opinnäytetyö on rajattu uuden DHCPv6-palvelimen, DHCP-ohjelmiston sekä sen konfiguraation tutkimiseen ja suunnitteluun. Työssä tutkitaan ja suunnitellaan myös palvelimen tarvitsema topologia DHCPv6-viestien välitykseen osallistuvan reitittimen osalta, sekä sen verkkoarkkitehtuuri, näiden liittyessä oleellisesti uuteen palvelimeen.

Opinnäytetyössä ei oteta huomioon uuden palvelimen käyttöjärjestelmän tai verkon tietoturva ominaisuuksia, eikä palvelimelle varattuja resursseja. Työssä ei myöskään

perehdytä operaattorin sisäiseen runkoverkkoon tai asiakasverkon osa-alueisiin, eikä asiakkaiden käyttämiin päätelaitteisiin.

2.2 Opinnäytetyön tutkimuskysymykset

Opinnäytetyössä tutkitaan mikä on paras tapa toteuttaa DHCPv6-palvelu operaattoriverkossa. Palveluun liittyy oleellisesti myös siihen sidottu verkkoarkkitehtuuri sekä palvelun topologia. Työssä tuleekin tämän vuoksi tutkia verkkoarkkitehtuureja sekä topologioita ja saada luotettava kuva siitä minkälainen ratkaisu sopii tähän tapaukseen parhaiten.

Uutta palvelinta ja siihen liittyvää topologiaa tulee mitata sekä analysoida asennuksen jälkeen. Tuloksia tulee verrata vanhan palvelimen suorituskykyyn ja pohtia onko uudella palvelimella päästy toivottuun lopputulokseen suorituskyvyn ja toiminnallisuuden osalta.

2.3 Opinnäytetyön kehitys- ja tutkimusmenetelmät

Opinnäytetyö on tutkimuksellinen kehitystyö. Opinnäytetyössä kehitetään operaattorin verkossa toimivaa palvelua. Tutkimusmenetelmänä käytetään aluksi dokumenttianalyysiä. Analyysissä perehdytään IPv4-, IPv6 sekä DHCP ja DHCPv6-prokollien teoriaan sekä DHCPv6-palvelun suosituksiin. Tästä teoriasta muodostetaan työn tietoperusta.

Tutkimustyötä tehdään myös tutkimalla ohjelmiston käyttäytymistä sekä kokeilemalla erilaisia vaihtoehtoja ohjelmiston konfiguraatiossa. Tästä empiirisestä tutkimustyöstä pyritään löytämään tarvittavat tekniset ratkaisut palvelun toteuttamiseksi.

Opinnäytetyössä käytetään apuna ulkoisia- ja sisäisiä sidosryhmiä. Tätä yhteisöllistä ideointia tehdään tarpeen mukaan, mikäli työssä tulee vastaan asioita, joihin tarvitaan erilaista näkökulmaa. Sidosryhmiä käytetään apuna myös kysymyksissä, joihin ei löydy tietoperustasta tarvittavaa ratkaisua.

Työn tuloksia mitataan ja analysoidaan mahdollisuuksien mukaan määrällisillä sekä laadullisilla menetelmillä. Työn tulokset pyritään mittaamaan numeerisesti. Palvelun laatua arvioidaan vertaamalla sen suorituskykyä ja ominaisuuksia vanhaan palveluun sekä peilaamalla tuloksia tietoperustaan.

3 Keskeiset käsitteet

DHCP RELAY Reitittimeen konfiguroitu ominaisuus. Reititin välittää verkossa asiakaslaitteen DHCP-pyyntöä eteenpäin varsinaiselle DHCP-palvelimelle.

DHCP	Dynamic Host Configuration Protocol jakaa päätelaitteen pyynnöstä tälle IPv4-osoitteen, oletusyhdykäytävän osoitteen sekä nimipalvelinten osoitteet dynaamisesti.
DHCPv6	Dynamic Host Configuration Protocol version 6. DHCP-palvelu jakaa päätelaitteen pyynnöstä tälle IPv6-osoitteen sekä muita verkossa liikennöintiin sekä lisäpalveluihin tarvittavia tietoja.
DHCPv6 PD	Dynamic Host Configuration Protocol version 6 - Prefix Delegation. DHCPv6-palvelun asiakkaalle jaetaan palvelimelta kokonainen IPv6-aliverkko yksittäisen osoitteen sijasta.
HA	High availability tarkoittaa korkean saatavuuden järjestelmää. Järjestelmän tarkoitus on maksimoida aika, jolloin se on käyttäjälle käytettävissä.
ISC DHCP	Vuonna 1998 julkaistu ISC:n kehittämä ja ylläpitämä avoimen lähdekoodin DHCP-palvelin ohjelmisto.
IETF	Internet Engineering Task Force on voittoa tavoittelematon organisaatio, joka vastaa Internet-protokollien standardoinnista.
IP	Internet Protocol on verkkotason protokolla, joka mahdollistaa verkkoon kytkettyjen laitteiden kommunikoinnin keskenään.
IPv4	Vanhempi 4. versio Internet Protokollasta. Osoitteen pituus on 32 bittiä.
IPv6	Uudempi 6. versio Internet Protokollasta. Osoitteen pituus on 128 bittiä.
ISC	Internet Systems Consortium on yleishyödyllinen yhdistys. Se kehittää Internetin infrastruktuuria ylläpitäviä vapaan lähdekoodin ohjelmia.
Kea DHCP	Vuonna 2014 julkaistu ISC:n kehittämä ja ylläpitämä modulaarinen avoimen lähdekoodin DHCP-palvelin ohjelmisto.
LINUX	Linux-käyttöjärjestelmät ovat Unixin kaltainen käyttöjärjestelmäperhe. Linux on avoimen lähdekoodin ohjelmisto mutta jotkut yritykset myyvät omiin julkaisuihinsa tukipalveluita sekä lisäohjelmistoja.
NAT	Name Address Translation on tekniikka, jolla pystytään ylikuormittamaan yhden julkisen IP-osoitteen taakse useita laitteita, joissa käytetään yksityisiä IP-osoitteita.

RFC	Request for Comments on dokumentti, jossa kuvaillaan muun muassa erilaisten Internetin järjestelmien toimintaa, tutkimusta ja innovaatioita. Osasta näitä dokumentteja muodostuu Internetiä koskevia standardeja.
UDP	User Datagram Protocol on yhteydetön tietoliikenneprotokolla, täten UDP ei muodosta aktiivista yhteyttä liikennöivien laitteiden välille. UDP protokollassa tiedon lähettäjä ei saa tietoa onko vastapää vastaanottanut viestin.

4 Internet Engineering Task Force

Internet Engineering Task Force kertoo verkkosivuillaan olevansa suuri avoin organisaatio, johon kuuluu verkkosuunnittelijoita, operaattoreita, laitevalmistajia ja tutkijoita. IETF koostuu työryhmistä, jotka tuottavat pääosin postituslistojen avulla Internetin toiminnan kannalta tärkeää sekä oleellista tietoa. (IETF 2021a.)

IETF:n tuottamat dokumentit ovat nimeltään RFC-dokumentteja. Kaikki IETF:n työ julkaistaan RFC-dokumentteina ja osasta näistä muodostuu koko Internetiä koskevia standardeja. (IETF 2021b.)

5 Internet Protokolla

Jokaisen Internetiin kytketyn laitteen on liikennöitävä verkkoon yksilöllisellä IP-osoitteella. Blank (2002, 80) vertaa IP-osoitetta katuosoitteeseen. Mikäli kahdella talolla olisi sama osoite niin postinkantajalle tuottaisi suuria vaikeuksia tuoda kirje oikeaan osoitteeseen. Samalla tavalla yksilöllinen IP-osoite varmistaa, että Internetiin lähetetyt paketit löytävät perille useiden Internetin reitittimien läpi täsmälleen oikeaan kohteeseen. (IETF 1981, 1.)

5.1 Internet protokolla versio 4

IPv4-osoitteet otettiin käyttöön 1980-luvun alussa ja näitä Yksilöllisiä IPv4-osoitteita on noin 4.3 miljardia kappaletta. Vapaat IPv4-osoitteet ovat nykyisin loppuneet niitä jakavilta tahoilta. IPv4-osoitteita voikin enää saada vain jonottamalla erityisillä jonotuslistoilla. Toinen mahdollisuus on vuokrata tai ostaa vapaita osoitealueita niitä välittäviltä ja myyvilä yrityksiltä. (RIPE NCC 2019, 2021.)

Syy IPv4-osoitteiden loppumiseen 90-luvulla oli Internetiin kytkeytyvien laitteiden määrän räjähdys Internetin yleistymisen ja sen valtavan suosion myötä. Tällöin lisäajan hankkimiseksi alettiin käyttämään NAT-tekniikka. Tällä tekniikalla yksittäisiä IPv4-osoitteita voitiin ylikuormittaa. Ylikuormitus mahdollistaa usean laitteen yhdistämisen Internetiin yhden

julkisen IP-osoitteen takaa. Tämä tekniikka mahdollistaakin että 4.3 miljardia IPv4-osoitetta on riittänyt näihin päiviin asti. Ilman tätä tekniikkaa IPv4-osoitteiden loppuminen olisi aiheuttanut suuria ongelmia. (Zhang 2007.)

IPv4-osoite voidaan määrittää päätelaitteeseen joko staattisesti käsin tai osoite voidaan jakaa laitteelle automaattisesti DHCP-palvelulla. DHCP-palvelu poistaa tarpeen konfiguroida päätelaite manuaalisesti ja näin ollen helpottaa päätelaitteiden yhdistämistä verkkoon. Päätelaite saa myös muita tärkeitä tietoja DHCP-palvelusta. Näitä ovat esimerkiksi nimipalvelimien osoitteet sekä oletusyhdyksikäytävän IP-osoite. (IETF. 1997, 6-8.)

5.2 Internet protokolla versio 6

IPv6-protokollaa alettiin kehittämään heti 1990-luvun alussa, kun huomattiin että vapaat IPv4-protokollan osoitteet tulisivat jossain vaiheessa loppumaan. IPv6-protokolla pitää sisällään useita tärkeitä uudistuksia. Laittevalmistaja Juniper Networksin mukaan IPv6-protokollan tärkeimmät ominaisuudet IPv4-protokollaan verrattuna ovat tehokkaampi reititys, parempi liikenteen luokittelu ja priorisointi, uudet tietoturvaominaisuudet sekä varsinkin valtava yksilöllisten osoitteiden määrä. (Juniper Networks 2021.)

IPv4-osoitteen pituus on vain 32 bittiä kun taas IPv6-osoite on 128bittinen. Hyvän kuvan tästä osoitteiden määrästä antaa Goralskin (2014, 2) Juniper Networksille laatima dokumentti, jonka mukaan jokaiselle aurinkokunnan molekyylille riittäisi oma yksilöllinen IPv6 osoite.

Kuten IPv4-osoite, myös IPv6-osoite voidaan jakaa päätelaitteelle DHCPv6-palvelulla, määritellä staattisesti tai käyttää muita uusia IPv6-protokollaan suunniteltuja osoitteen hankkimiseen tarkoitettuja tekniikoita. Tässä opinnäytetyössä keskitytään DHCPv6-palveluun. (IETF 2018, 18-22.)

6 Parhaat käytännöt ja suositukset DHCPv6-palveluissa

Liikenne- ja viestintävirasto Traficom toimii suomessa liikenteen sekä viestinnän lupa-, rekisteröinti- ja hyväksyntä- sekä turvallisuusviranomaisena. Traficom in yhtenä tehtävänä on antaa sääntöjä, määräyksiä ja suosituksia internetoperaattoreille. Traficom on julkaissut ohjeistuksen ja suositukset IPv6-palvelujen tarjoamisesta asiakkaille. (Traficom 2020.)

Tässä Traficom in dokumentissa tärkeimmät kohdat DHCPv6-palvelun suunnittelun kannalta ovat tarve liittymän loppukäyttäjän tunnistamiseen, DHCPv6 Prefix Delegation-palvelun käyttöönotto, käänteisnimipalvelu, DHCP Prefix Delegation-ominaisuudella jaettavan verkkoalueen pituus ja asiakkaalle jaetun verkon määritelty voimassaoloaika. (Nieminen 2019.)

Näitä Traficomien ohjeita ja suosituksia seuraamalla voidaan varmistaa työn eettisyys, kun pidetään huoli, että DHCPv6-palvelu sisältää suositellut sekä tarvittavat ominaisuudet ja toiminnallisuudet. On mahdollista, ettei kaikkia suositusten mukaisia ominaisuuksia voida ottaa heti käyttöön vaan palveluun sekä verkkoon vaaditaan myöhemmin lisää muutoksia. Silti nämä suositellut ominaisuudet tulee ottaa huomioon palvelun suunnittelun ja uudistamisen yhteydessä, jotta niiden käyttöönotto helpottuu tulevaisuudessa.

7 Verkkoarkkitehtuuri

Verkkoarkkitehtuuri määrittelee miten verkon reitittimet, kytkimet sekä muut laitteet ja palvelut rakentuvat yhdeksi kokonaisuudeksi. Arkkitehtuuri määrittää myös, miten verkon tehtävät ja prosessit on jaettu eri verkkolaitteille. (Cisco Systems 2021.)

7.1 Modulaarinen arkkitehtuuri

Pohdin erilaisia ratkaisuja uuden DHCP-palvelimen topologian kannalta ja tutustuin verkossa tietoliikenneverkkojen arkkitehtuureihin sekä toteutusratkaisuihin. Näiden lähteiden sekä kokemuksieni pohjalta tulin siihen johtopäätökseen, että järkevästi suunniteltu modulaarisuus tietoliikenneverkossa sekä sen laitteissa lisää verkon selvyyttä sekä helpottaa ongelmatilanteiden selvittämistä. Cisco Press (2014, 1.2.1.1) listaa julkaisussaan Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design, että modulaarisella verkkosuunnittelulla saadaan useita oleellisia hyötyjä.

- ”Yksittäisessä verkon moduulissa tapahtuva ongelma voidaan rajata ja eristää muusta verkosta. Tällöin ongelman rajaamisesta tulee yksinkertaisempaa ja nopeampaa.”
- ”Verkon muutokset ja päivitykset sekä uusien palveluiden luominen on hallitumpaa.”
- ”Moduulin kapasiteetin tai ominaisuuksien loppuessa kesken sen voi päivittää tai korvata uudella moduulilla.”
- ”Turvallisuusominaisuudet voidaan suunnitella moduulikohtaisesti.”

Pohdin modulaarista arkkitehtuuria käytännön kannalta ja mielestäni arkkitehtuurissa pitää ottaa huomioon myös taloudelliset seikat, kuten esimerkiksi yksittäisten laitteiden kustannukset. Mikäli jokaiseen verkon toimintoon tai palveluun hankittaisiin oma laitteensa, kustannukset nousevat huomattavasti ja liian moni yksittäinen laite saattaa jopa hankaloittaa verkon operointia.

Laitteet tarvitsevat myös jatkuvia päivityksiä. Tällöin useamman verkkolaitteen päivitys lisää työkuormaa, sekä aiheuttaa enemmän katkoksia asiakasliikenteelle. Myös laitteiden tarvitsema energia tulee ottaa huomioon suunnittelussa.

Edellä mainittujen syiden vuoksi tuleekin harkita tarkasti, miten verkko jaetaan eri moduuleihin. Toiminnoista ja verkon sisäisistä palveluista tulisikin mielestäni saada kustannustehokkaita, yksinkertaisia sekä helposti ylläpidettäviä.

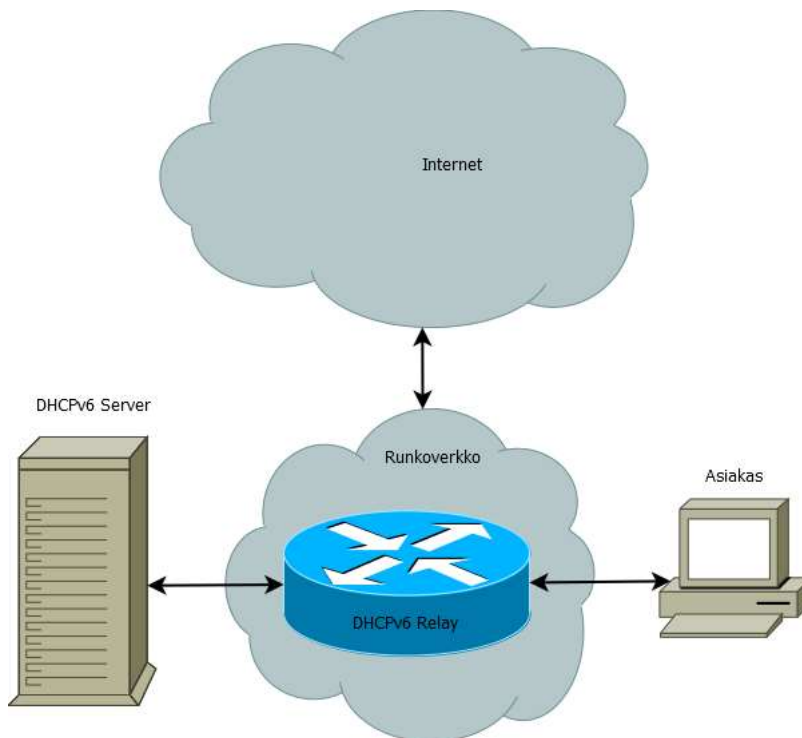
8 Nykyinen DHCPv6-palvelu

Nykyinen konfiguraatio koostuu IPv6-osoitteiden jakoon tarkoitettusta erillisestä virtuaalialustalla toimivasta DHCPv6-palvelimesta sekä IPv6-osoitepyyntöjä DHCPv6-palvelimelle välittävästä reitittimestä. Palvelimen topologia ei tällä hetkellä ole vikasetoinen, koska yhden laitteen vikaantuminen keskeyttäisi koko palvelun toiminnan.

Tällä hetkellä kuluttaja asiakkaat eivät käytä IPv6-osoitteita kovinkaan laajasti verrattuna IPv4-osoitteisiin. Nykyisestä palvelimesta oli 26.3.2021 jaettu 42 Prefix Delegation verkkoa ja 57 yksittäistä osoitetta.

IPv4 DHCP-palvelu on täysin eriytetty IPv6 DHCPv6-palvelusta, joten se toimii koko ajan, vaikka DHCPv6-palvelimessa tapahtuisi häiriö. Tämän vuoksi katkos palveluun ei juurikaan vaikuttaisi asiakkaiden Internetliikenteen toimivuuteen. Myöskään IPv6-toiminnallisuus ei lakkaisi, koska palvelin käsittelee vain DHCPv6-protokollalla tehtyjä IPv6-osoitteiden pyyntöjä, eikä osallistu yhteyksien reititykseen. Mahdollisen häiriön aikana ainoa tapahtuva asia olisi, että uusia IPv6-osoitteita ei enää kyettäisiin jakamaan asiakkaille.

Viankorjausajat ovat verkossa hyvin lyhyet, mutta on mahdollista, että joidenkin asiakkaiden laitteet pyrkisivät uusimaan tai hakisivat uutta IPv6-osoitetta juuri vian ajankohtana. Edellä mainituista syistä, sekä IPv6 DHCPv6-palvelimen käyttöasteen huomioon ottaen, palvelun kahdennus ei ole ollut aiemmin verkon toiminnan kannalta oleellista.



Kuvio 1: Nykyinen topologia

Nykyisessä topologiassa asiakkaan päätelaite lähettää pyynnön IPv6-osoitteesta operaattorin verkkoon. Tämä pyyntö päättyy runkoverkossa nykyiselle Cisco Systemsin reitittimelle, joka välittää pyynnön erilliselle virtualisoidulle DHCPv6-palvelimelle. DHCPv6-palvelin vastaa pyyntöön ja lähettää asiakkaan laitteelle sen pyytämän IPv6-osoitteen tai kokonaisen IPv6-aliverkon Prefix Delegation ominaisuudella. Asiakkaalle lähetetään IPv6 osoitteen ohella myös muut sen tarvitsemat ja pyytämät tiedot.

8.1 Uuden DHCPv6-palvelun suunnitelma

Mietimme parasta toteutustapaa DHCPv6-palvelimelle palaverissa yhdessä tekniikkaosastomme henkilöstön kanssa. Olimme kaikki samaa mieltä siitä, että uusi DHCPv6-palvelin tulisi toteuttaa samankaltaisella topologialla kuin nykyinen palvelinkin. Nykyinen DHCPv6-palvelu toimii tällä hetkellä omalla palvelimellaan ja on täten eriytetty täysin varsinaisista tietoliikennelaitteista.

Nykyään lähes kaikissa reitittimissä on DHCP-, DHCPv6-, sekä kokonaisen IPv6-aliverkon asiakkaalle lähetävä DHCPv6 Prefix Delegation-ominaisuus. Vaikka tämäkin palvelu voitaisiin suunnitella sekä toteuttaa jollakin verkossa olevalla reitittimellä, niin mielestäni on kuitenkin järkevää jakaa toiminnallisuuksia harkitusti eri laitteille. Tämä toteutustapa tuo modulaarisen arkkitehtuurin hyödyistä johtuen palveluun monia etuja.

Päätimme tekniikkaosaston kesken, että vanha Ciscon reititin tulisi purkaa muutoksen jälkeen pois verkosta. Minä selvittäisin työssäni myös, miten DHCPv6-viestien välityspalvelu voitaisiin siirtää uudempaan, monikäyttöisempään ja tehokkaampaan Nokian valmistamaan runkoverkon palvelureitittimeen.

8.2 Tulevien muiden muutoksien huomioiminen

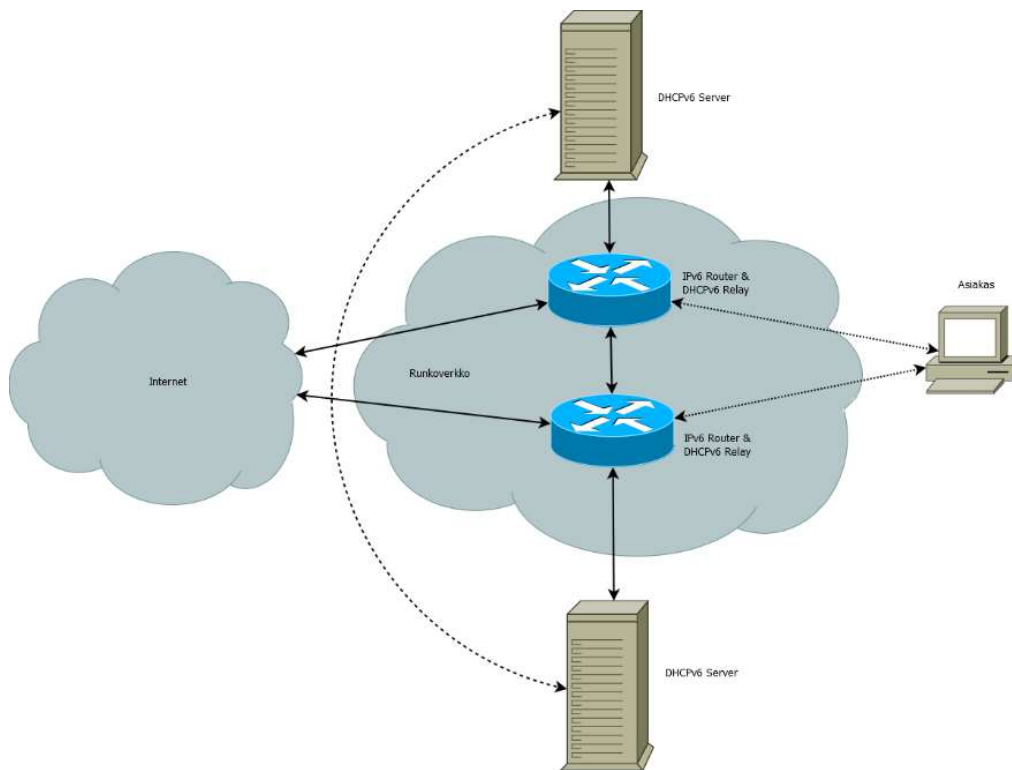
Mietimme palaverin jälkeen palveluiden tulevaa kehitystä yhdessä yrityksen vanhemman verkkoinsinöörin kanssa, jolla on eniten kokemusta verkosta ja sen palveluista. Saimme ajatuksen, että myös IPv4 DHCP-palvelut voisi tulevaisuudessa uudistaa ja siirtää myös ne uudelle palvelimelle. Tätä vaihtoehtoa minun tulisikin myös selvittää tarkemmin työn edetessä.

IPv4-osoitteita on jaettu DHCP-palvelusta huomattavasti enemmän asiakkaiden käyttöön kuin IPv6-osoitteita. Tämä tekee IPv4 DHCP-palvelusta huomattavasti tärkeämmän sekä kriittisen verkon ja asiakasliikenteen toiminnan kannalta. Tämän vuoksi olisikin hyvä, että uutta reititintä sekä palvelinta voitaisiin testata ensin IPv6-käytössä.

Mikäli IPv4 DHCP-palvelut päätetään siirtää niin palvelimet sekä reitittimet tulisi myös samalla kahdentaa IPv4-palveluiden tärkeyden vuoksi. Tällöin sekä DHCP- että DHCPv6-palveluista saataisiin korkean saatavuuden palveluita.

Korkea saatavuus tarkoittaa, että palvelun tulisi olla käytettävissä lähes koko ajan. Tätä käytettävyyttä voidaan mitata esimerkiksi vuositasolla. 99 % käytettävyys tarkoittaisi, että palvelu olisi vuoden aikana vialla 3,65 päivää. (Heidi 2016.)

Mielestäni yli kolmen päivän katkos internetpalveluissa kuulostaa kohtuuttoman pitkältä ajalta vuositasolla ja korkean palvelun tulisikin tähdätä sataan prosenttiin. Korkean saatavuuden järjestelmässä ei saisi olla yksittäistä pistettä, jonka toimintahäiriö keskeyttäisi koko palvelun toiminnan. Mikäli yksi laite verkossa vikaantuu niin toisen laitteen tulisi automaattisesti ottaa sen tehtävät hoidettavakseen. (Heidi 2016.)



Kuvio 2: Korkean saatavuuden palvelussa reitittimet sekä palvelimet on kahdennettu

Yllä olevassa kuviossa on esimerkki korkean saatavuuden DHCPv6-palveluista. Asiakkaan DHCPv6-osoitepyynnöt menevät runkoverkossa kahdelle erilliselle reitittimelle. Nämä molemmat reitittimet välittävät pyynnöt eteenpäin kahdelle DHCPv6-palvelimelle. Näillä palvelimilla on yhteinen tietokanta asiakkaille annetuista osoitteista. Mikäli toinen palvelin ei jostain syystä pystyisi antamaan asiakkaalle osoitetta niin toinen palvelin alkaisi hoitamaan sen tehtäviä automaattisesti. Myös reitittimet kahdentavat toisiaan samankaltaisesti.

9 Palvelinohjelmisto

Nykyisessä DHCPv6-palvelimessa käytetään Internet Systems Consortium, Inc. julkaisemaa Linux-käyttöjärjestelmälle tarkoitettua ISC DHCP-ohjelmistoa. ISC on voittoa tavoittelematon yksityinen osakeyhtiö, joka on perustettu vuonna 1994 Yhdysvalloissa. ISC tuottaa ja kehittää kolmea avoimen lähdekoodin ohjelmistoa, jotka ovat BIND 9, ISC DHCP sekä Kea DHCP. Useimmista ohjelmistoista on saatavilla myös maksullinen versio, joka sisältää enemmän ominaisuuksia ja mahdollisuuden ISC:n tuottamaan käyttötukeen. (Isc.org 2021a.)

ISC suosittelee, että kaikissa uusissa asennuksissa sekä vanhojen järjestelmien päivityksissä käytetään uudempaa avoimen lähdekoodin Kea DHCP-palvelinohjelmistoa. ISC kertoo uuden

Kea DHCP-ohjelmiston eduiksi useita ominaisuuksia. Näistä mielestäni tärkeimmät on lueteltu alla. (Internet Systems Consortium 2020.)

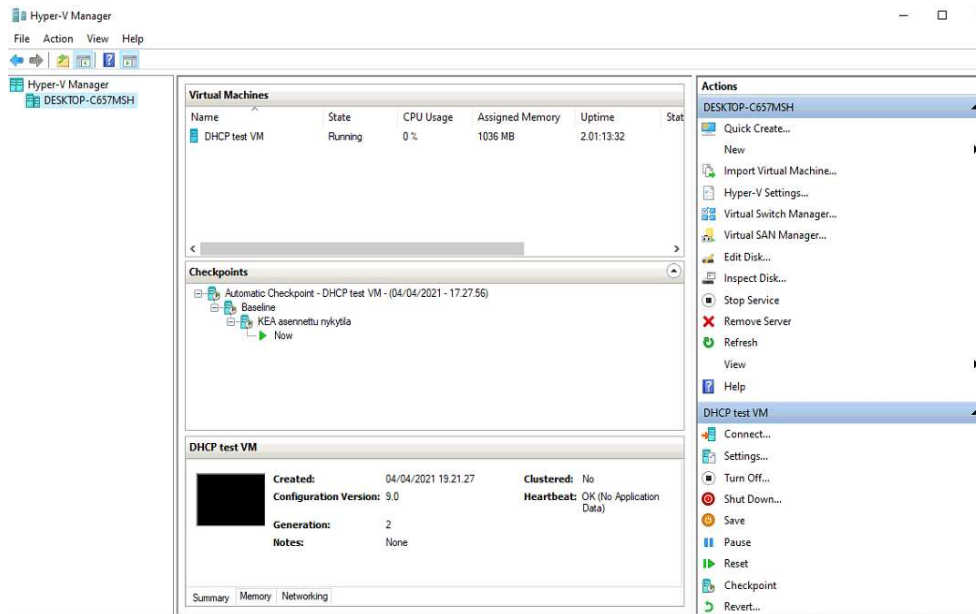
- ”Kea koostuu modulaarisista osista. esimerkiksi DHCPv4- ja DHCPv6-palvelimet on erotettu omiksi komponenteiksi.”
- ”JSON konfiguraatio, jota pystyy muuttamaan sammuttamatta ohjelmistoa.”
- ”Helppo integroiminen muihin järjestelmiin.”
- ”Web pohjainen graafinen käyttöliittymä.”
- ”Kea DHCP on kokonaisuutena modernimpi ja pitää sisällään paljon uusia ominaisuuksia.”

Vertailin Kea DHCP- sekä ISC DHCP-pääkäyttäjän manuaaleja ja näistä oli huomattavissa, että konfiguraatitiedoston muoto, sekä ohjelman muut parametrit olivat muuttuneet hyvin paljon. Tämän vuoksi arvelin Kea DHCP-ohjelmiston käyttämisen lisäävän huomattavasti enemmän tarvittavaa tutkimus- ja selvitystyötä siihen verrattuna, että käyttäisin vanhempaa ISC DHCP-ohjelmistoa. Tein kuitenkin päätöksen käyttää uudempaa ohjelmistoa uudessa palvelimessa ISC:n antamien suositusten mukaisesti.

10 Testaus kotilaboratoriossa

Kotilaboratorioni koostuu pienikokoisesta DELL poweredge T40 tornipalvelimesta, jossa on Windows 10 Pro käyttöjärjestelmä. Käyttöjärjestelmässä on Microsoftin oma Hyper-V virtualisointi alusta käytössä ja kokoonpanossa olen testaillut erilaisia käyttöjärjestelmiä sekä ohjelmistoja. Palvelimessa toimii myös omat pilvipalveluni sekä muutamia verkkosivustojani.

Hyper-V on mielestäni loistava alusta varsinkin ohjelmien testaamiseen ja sen paras ominaisuus onkin palautuspisteiden luominen sekä näiden palauttaminen. Palvelimeen voi tehdä perusasennuksen ja alkaa rohkeasti kokeilemaan erilaisia ohjelmistoja ja asetuksia. Mikäli asennuksessa tapahtuu virhe tai jostain muusta syystä haluaa palata takaisin, niin koneen voi saattaa alkuperäiseen tilaan muutamissa sekunneissa. Microsoft sivuillaan kertookin Hyper-V:n eduksi varsinkin erilaisten käyttöjärjestelmien ja ohjelmien testausmahdollisuuden. (Microsoft 2018.)



Kuvio 3: Hyper-V ohjelman graafinen käyttöliittymä on selvä ja helppokäyttöinen

Yllä olevassa kuviossa näkyy, että Hyper-V ohjelman käyttöliittymä on hyvin selkeä. Keskellä ruutua ylhäällä on listattuna alustalle luodut virtuaalikoneet. Keskimmäinen osio näyttää koneesta luodut manuaaliset sekä automaattiset palautuspisteet. Alimmissä ikkunoissa kerrotaan tarkemmin koneen tilasta ja ominaisuuksista. Oikeanpuoleisessa toiminto ikkunassa voidaan virtuaalikoneelle tehdä erilaisia toimenpiteitä.

10.1 Kea DHCP-ohjelmiston asennus

Päätin suunnitelmiani mukaan testata ohjelmistoa omissa kotilaboratoriossani ennen asennusta tuotantokäyttöön suunnitellulle palvelimelle. Yleensä Linux-ohjelmissa on riippuvuuksia muista ohjelmista, joten asennus ei ole aina välttämättä yksinkertainen prosessi. Jokaiseen Linux-jakeluun on myös omat asennuspakettinsa, jotka eivät käy ristiin jakeluiden välillä. (Hess 2020.)

Olen aiemmin käyttänyt koulu- sekä työtehtävissäni Red Hat Linux-jakeluun perustuvaa CentOS 7 julkaisua. Myös omaan käyttöön luomani palvelut toimivat tällä käyttöjärjestelmällä, joten sen käyttö on itselleni hyvin tuttua. Aloitin ensimmäiseksi selvittämään miten CentOS 7 käyttöjärjestelmään saa Kea DHCP-ohjelmiston asennettua.

Löysin ISC:n verkkosivustolta tiedon, että ISC julkaisee DHCP-ohjelmistonsa avoimena lähdekoodina sekä myös eri Linux-käyttöjärjestelmille valmiiksi koottuina asennus paketteina. Nämä asennuspaketit on julkaistu cloudsmith.io sivustolla. Mielestäni valmiiden asennuspakettien toimittaminen on ISC:ltä hyvä ratkaisu, koska lähdekoodista ohjelmien kääntäminen on mielestäni työläs sekä aikaa vievä turha vaihe. ISC ilmoittaa suoraan

sivuillaan, että se haluaa tehdä käyttäjien elämän helpommaksi julkaisemalla valmiit asennuspaketit verkossa. (Isc.org 2021c.)

Cloudsmith.io ja isc.org sivustolla oli asennuksen helpottamiseksi myös suorat ohjeet, miten sivuston osoite lisätään Linuxin pakettilähteeksi. Tämän jälkeen Linuxin pakettienhallintaohjelmisto löytää ohjelmiston ja pystyy lataamaan sen suoraan sivustolta. Ainut asia mikä pakettilähdettä valittaessa tulee tietää, on käytetty Linux-jakelu. Tässä tapauksessa asensin RPM pakettilähteen koska käytössäni oli Red Hat Enterprise Linux-pohjainen CentOS jakelu. (Linuxise.com 2021.)

RPM Repositories

To install RPM packages, you can quickly setup the repository automatically (recommended):



```
Bash Copy
curl -sLf \
  'https://dl.cloudsmith.io/public/isc/kea-1-8/cfg/setup/bash.rpm.sh' \
  | sudo bash
```

Kuvio 4: Ohje cloudsmith.io RPM pakettilähteen asennuksesta CentOS 7 käyttöjärjestelmään

Yllä olevassa kuvassa näkyy komento sivustolla oleva ohje. Ohjeen alla on komento, jolla Kean versio 1.8 lisää pakettilähteiden joukkoon. Kuvan komennon pystyi kopioimaan suoraan sivustolta Linuxin komentokehoteeseen asennuksen helpottamiseksi.

Kun aloin asentamaan Kea DHCP-ohjelmistoa niin huomasin että se ei suostunut asentumaan suoraan Centos 7 käyttöjärjestelmään. Tämä johtui siitä, että asennusta varten ei löytynyt muutamaa tarvittavaa pakettia, joista Kea DHCP-ohjelmisto on riippuvainen. Asennan yleensä koneisiin vanhasta kokemuksesta EPEL pakettilähteen heti asennuksen aluksi, mutta nyt en ollut sitä tehnyt. Arvelin että nämä puuttuvat Kea DHCP:n tarvitsemat paketit olisivat saatavilla tuosta pakettilähteestä, joten asensin sen seuraavaksi.

```
[root@DHCP ~]# yum install epel-release.noarch
```

Kuvio 5: Komento EPEL pakettilähteen asentamiseksi

Syötin yllä olevan kuvion komennon Linuxin komentokehoteeseen. Tällä komennolla Linux asentaa yum ohjelmaa käyttäen EPEL pakettilähteen pakettilähteiden listalle. EPEL-pakettilähteen asentamisen jälkeen Linuxin asennusohjelma löysi Kea DHCP:n tarvitsemat ohjelmapaketit ja Kea DHCP asentuikin ongelmitta.

10.2 Konfiguraation konvertoiminen

Ennen ohjelmiston testausta tulisi suunnitella ja rakentaa DHCP-palvelinohjelmiston tarvitsema konfiguraatio. Päätin käyttää pohjana vanhaa konfiguraatiota ja aloin tutkimaan Kea DHCP-ylläpitäjän manuaalista ohjeita Kea DHCP:n tarvitseman konfiguraation rakentamiseen.

Löysin manuaalista tiedon, että ISC on tehnyt ohjelmistojen välillä siirtymistä helpottamaan erillisen KeaMA-työkalun (Kea Migration Assistant), jolla voi muuntaa vanhan ISC DHCP-konfiguraation Kea DHCP ohjelmistoon sopivaksi. Myös tämän ohjelman sai asennettua cloudsmith.io sivustolta helposti lisäämällä cloudsmith.io KeaMA-hakemiston Linuxin pakettivarastojen joukkoon. (isc.org 2021c.)

```
[root@DHCP ~]# curl -lsLf \  
> 'https://dl.cloudsmith.io/public/isc/keama/setup.rpm.sh' \  
> | sudo -E bash  
Executing the setup script for the 'isc/keama' repository ...
```

Kuvio 6: Komento KeaMA ohjelman sisältävän pakettivaraston asentamiseksi

Yllä olevassa kuviossa asennan palvelimeen pakettilähteen samalla tavalla kuin varsinaisen DHCP-ohjelmiston pakettivaraston. Komento on ohjeessa jaettu useille riveille selvyiden vuoksi. Jotta Linux osaa lukea komennon yhdeksi lauseeksi niin rivit on jaettu \ merkeillä.

Pakettilähteen lisäämisen jälkeen asennus olikin helppoa. Nyt paketinhallintaohjelmisto löysi ohjelman suoraan pakettivarastosta ja osasi lisätä automaattisesti ohjelmiston tarvitsemat muut ohjelmat joista se on riippuvainen.

```
[root@DHCP ~]# yum install isc-dhcp-keama.x86_64
```

Kuvio 7: Komento KeaMA ohjelman asentamiseksi

Yllä olevassa kuviossa näkyy Linuxin komentokehotteeseen syötetty rivi ISC:n KeaMA ohjelman asentamiseksi. Asennus suoritettiin Centos käyttöjärjestelmän pakettienhallintaan tarkoitetulla yum ohjelmalla.

Yritin seuraavaksi konvertoida konfiguraation KeaMA työkalulla mutta jostain syystä se kommentoi konfiguraatiossa olleen DHCP Prefix Delegation-osuuden ulos konfiguraatiosta eikä muokannut sitä Keaan sopivaan syntaksiin. Ilman Prefix Delegation konfiguraatiota asiakkaille ei pystyittäisi jakamaan kokonaisia IPv6-aliverkkoja palvelimelta. Konfiguraatitiedostosta puuttui myös Keassa pakolliseksi tullut interface konfiguraatio, jossa ohjelmalle määritetään sen käyttämä verkkoadapteri.

Näiden konfiguraatioiden puutteet sekä syntaksi piti selvittää Kean ylläpitäjän manuaalista. Konfiguraatioon piti lisätä myös tarvittavien logien tallennus sekä annettujen IPv6-osoitteiden tietokannan sijainti. Keassa pystyy tallentamaan loki tietoja usealla eri tarkkuudella ja arvelin että testien aluksi olisi hyvä tallentaa debug tasoiset lokit, jotta mahdolliset ongelmat selviäisivät nopeammin. Debug tasolla Kea tallentaa kaiken ohjelmistoon käyttöön liittyvän tiedon lokeihin.

Kea DHCP käyttää konfiguraatiossaan JSON-muotoa, joten konfiguraatio vaatii tarkkaavaisuutta koska konfiguraatiossa on useita kaari ja hakasulkuja. Syntaksin on oltava täysin oikein muuten ohjelma ei suostu käynnistymään.

Minulla oli suuria vaikeuksia saada aluksi syntaksia oikein, kunnes keksin etsiä verkosta JSON syntaksin validointi työkaluja. Tämä tuli mieleeni suorittamistani ohjelmointikursseista, joissa koodia validoitiin verkkopalveluissa. Näillä työkaluilla konfiguraation oikeamuotoisuus olikin helppo tarkistaa ja lopulta sain palvelun käyntiin.

```
[root@DHCP DHCP]# keama -6 -i vanha-dhcp.conf -o uusi-dhcp.conf
```

Kuvio 8: Komento konfiguraation konvertoimiseksi KeaMA ohjelmalla

Yllä olevassa kuviossa näkyy KeaMA ohjelman komento Linuxin komentokehotteessa. Selvyyden vuoksi konfiguraatitiedostot on nimetty vanhaksi ja uudeksi .conf päätteiseksi tiedostoksi. Työkalu sopii myös IPv4 DHCP-konfiguraation konvertoimiseen ja tämän vuoksi komentoon lisätään -6 optio, joka kertoo työkalulle, että konfiguraatio on DHCPv6-ohjelmistosta.

10.3 KeaMA:lla konvertoidun konfiguraatitiedoston sisältö

Alla käyn läpi vanhasta konfiguraatiosta konvertoidun uuden konfiguraation. Konfiguraatiosta on poistettu työnantajani verkkojen oikeat IPv6-osoitteet tietoturvan vuoksi.

```
{
    "Dhcp6": {
        "lease-database": {
            "type": "memfile",
            "persist": true,
            "name": "/var/log/kea-leases6.csv",
            "lfc-interval": 1800,
            "max-row-errors": 100
        },
```

Kuvio 9: IP-tietokannan konfiguraatio

Yllä olevassa kuviossa näkyy, että tiedosto alkaa palvelimen IP-tietokannan määrittelyllä. Tässä on määritelty, että tietokanta tallennetaan muistin lisäksi levyllä /var/log/kea-leases6.csv tiedostoon. Lfc-interval määrittelee sekunneissa, kuinka usein tietokanta käydään läpi ja puhdistetaan vanhentuneista osoitteista. Max-row-errors määrittelee kuinka monta virheellistä riviä tietokannassa voi olla palvelun käynnistyessä. Mikäli määritelty rivimäärä ylittyy niin ohjelma ei käynnisty ja antaa virheilmoituksen.

```
"loggers": [{
  "name": "kea-dhcp6",
  "output_options": [{
    "output": "/var/log/kea-debug.log",
    "maxver": 8,
    "maxsize": 204800,
    "flush": true,
    "pattern": "%d{%j} %H:%M:%S.%q} %c %m\n"
  }],
  "severity": "DEBUG",
  "debuglevel": 99
}],
```

Kuvio 10: Lokien konfiguraatio

Yllä olevassa kuviossa näkyy konfiguraatitiedoston loki osio. Tässä määritellään miten ja mitä tietoa Kea tallentaa lokitiedostoihinsa. Tässä konfiguraatiossa ohjelman lokit tallennetaan DEBUG tasolla 99, joka on kaikista tarkin taso. Lokitiedostoja tehdään 8 kappaletta ja yhden tiedoston koko on maksimissaan 2 megatavua. Pattern rivi antaa mahdollisuuden muotoilla lokirivien muotoa mieleiseseen esimerkiksi lisäämällä siihen päivämäärät sekä kellonajat ylläpitäjän parhaaksi näkemässä formaatissa.

```
"interfaces-config": {
  "interfaces": ["ens3/XXXX:XXXX:XXX:X::XX"]
},
```

Kuvio 11: Interface konfiguraatio

Loggers osiota seuraa yllä olevan kuvion interface konfiguraatio, jossa määritellään mistä paikallisesta verkkokortista kuunnellaan IPv6-pyyntöjä. Konfiguraatiossa voidaan määritellä myös verkkokortin IPv6-osoite.

```
"min-valid-lifetime": 14400,
"valid-lifetime": 43200,
"max-valid-lifetime": 86400,
```

Kuvio 12: Osoitteiden voimassaoloaika

Seuraavaksi yllä olevassa kuviossa osoitteille määritellään voimassaoloaika. Nämä arvot määritellään sekunneissa. Yksi Traficomien suosituksista oli, että verkkoalueen tulisi olla pitkäaikainen. Tämä tuleekin ottaa huomioon lopullisessa konfiguraatiossa.

```
"subnet6": [{
  "id": 1,
  "subnet": "XXXX:XXXX:XXX:X::/64"
},
{
  "id": 2,
  "subnet": "XXXX:XXXX:XXXX::/36",
  "option-data": [{
    "space": "dhcp6",
    "name": "dns-servers",
    "code": 23,
    "data": "XXXX:XXXX:XXX:X::X, XXXX:XXXX:XXX:X::X"
  },
  {
    "space": "dhcp6",
    "name": "domain-search",
    "code": 24,
    "data": "XXXXX.dhcp6.fi"
  }
],
"pools": [{
  "pool": "XXXX:XXXX:XXXX:XX:X::1-XXXX:XXXX:XXXX:XX:ffff:ffff:ffff:ffff"
}],
}
```

Kuvio 13: Verkot ja jaettavien osoitteiden IPv6-Alueet

Yllä olevassa konfiguraation osassa määritellään aliverkkojen ja jaettavien osoitteiden alueen lisäksi, mitä lisätietoja asiakkaalle annetaan. Asiakkaan päätelaitteeseen voidaan yleensä määritellä minkälaista lisätietoa se pyytää palvelimelta. Tässä konfiguraatioesimerkissä asiakkaalle annettavaksi lisätiedoksi on määriteltä nimipalvelinten osoite sekä domain hakunimi.

Lopuksi määritellään vielä DHCPv6 Prefix Delegation-ominaisuuden jakama verkkoalue sekä sen aliverkon pituus. Prefix Delegation mahdollistaa kokonaisen aliverkon luovuttamisen asiakkaan käyttöön.

```
"pd-pools": [{
  "prefix": "XXXX:XXXX:XXXX::",
  "prefix-len": 48,
  "delegated-len": 56
}]}} }
```

Kuvio 14: Prefix delegaation konfiguraatio

Yllä olevassa kuviossa näkyy miten Prefix Delegation määritellään konfiguraatioon. Mielestäni Prefix Delegation on DHCPv6-palvelun hienoimpia ja monimutkaisimpia ominaisuuksia. Yllätyksekseni se oli silti todella helppo määritellä konfiguraatitiedostoon.

10.4 Toimivuuden testaus

Kun sain konfiguraation valmiiksi käynnistin ohjelmiston palvelimessa. Ohjelmisto käynnistyi saman tien ja sen lokitiedostoon ei tullut mitään virheilmoituksia.

```

■ kea-dhcp6.service - Kea DHCPv6 Server
  Loaded: loaded (/usr/lib/systemd/system/kea-dhcp6.service; disabled; vendor preset: disabled)
  Active: active (running) since Fri 2021-04-09 22:57:50 EEST; 1 weeks 1 days ago
  Docs: man:kea-dhcp6(8)
  Main PID: 5959 (kea-dhcp6)
  CGroup: /system.slice/kea-dhcp6.service
          └─5959 /usr/sbin/kea-dhcp6 -c /etc/kea/kea-dhcp6.conf

```

Kuvio 15: Kean prosessi aktiivisena palvelimessa

Yllä olevassa kuvassa on Linuxin komentokehotteessa syötetty komento `systemctl status kea-dhcp6`. Tällä komennolla saadaan näkyviin kyseisen palvelun tila Linux-käyttäjärjestelmässä. Tässä kuvassa näkyy vihreällä tekstillä, että prosessi on käynnissä ja aktiivinen.

Testikäyttöä varten otin palvelimen asiakkaaksi yhden kannettavistani, jossa on käyttäjärjestelmänä Windows 10 Pro. Kone ei aluksi saanut osoitetta palvelimelta mutta hetken tutkimisen jälkeen totesin, että tämä johtui palvelimen päässä DHCPv6-protokollan tarvitsemista tietoliikenneporteista, jotka olivat suljettu. Ongelman löytäminen oli helppoa. Sammutin Linux-palvelimen palomuurin kokonaan, jonka jälkeen kone saikin heti IPv6-osoitteen.

```

[root@DHCP-TEST ~]# systemctl status firewalld
■ firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: inactive (dead) since Fri 2021-04-09 18:03:40 EEST; 1 weeks 1 days ago
  Docs: man:firewalld(1)
  Process: 553 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/SUCCESS)
  Main PID: 553 (code=exited, status=0/SUCCESS)

```

Kuvio 16: Palomuri sammutettuna

Oheisessa kuvassa näkyy, että komentokehotteeseen on syötetty `systemctl status firewalld` komento. Ruudulle tulostettu tieto kertoo että palomuuripalvelu `firewalld.service` on ladattu mutta se ei ole aktiivinen.

Selvitin IETF RFC8415 dokumentista (IETF 2018, 27) että DHCPv6-palvelin sekä DHCPv6-pyyntöjä välittävä reititin kuuntelee viestejä UDP portista 547. Dokumentissa on kerrottu myös, että vastausviesti osoitteen pyytäjälle lähetetään UDP portin 546 kautta. Tuotantokäyttöön asennettavassa palvelimessa tulee ottaa huomioon, että edellä mainitut portit ovat avattuna. Tuotantokäytössä olevasta palvelimesta ei tietenkään voi sammuttaa palomuuria palvelimen tietoturvan vuoksi.

Kokeilin erilaisia konfiguraatio vaihtoehtoja palvelimella ja totesin että nämä vaikuttavat asiakaslaitteen saamiin tietoihin oletetusti. Tarkempaa testausta ei tässä vaiheessa enää tarvittaisi, koska palvelin voitaisiin säätää tuotantoverkossa testikäytössä Traficomien suositusten mukaisesti.

11 Tuotantopalvelimen käyttöjärjestelmän valinta

Pohdin sopivaa käyttöjärjestelmää tuotantopalvelimelle. Palvelimen käyttöjärjestelmän tulisi olla hyvin vakaatoiminen, sekä siihen tulisi saada päivityksiä mahdollisimman pitkään. Itselleni tuttu CentOS 7 käyttöjärjestelmä olisi muuten hyvä vaihtoehto mutta käyttöjärjestelmän tuki päättyy jo 30.6.2024. (CentOS 2020a.)

Uudempi versio CentOS 8 käyttöjärjestelmästä on muutettu Centos 8 Stream versioksi. CentOS Stream oli minulle tuntematon, joten aloin tutkia tämän käyttöjärjestelmän dokumentaatiota. Verkosta löytyneestä materiaalista päätelin, että uusi Stream versio olisi jonkinlainen testiympäristö Red Hat käyttöjärjestelmälle (Bharitya 2019). CentOS väittää tätä vastaan kuitenkin verkkosivuillaan ja kertoo että Stream ei olisi testialusta Red Hat julkaisulle. (Centos 2020b.)

Tulin lopulta lopputulokseen, että näin tärkeää keskeistä palvelua ei voi missään tapauksessa rakentaa kokeellisen käyttöjärjestelmän päälle. Pahin mahdollisuus on, että käyttöjärjestelmään tulee kehittäjän julkaisemien päivitysten mukana jokin nollapäivähaavoittuvuus, joka asettaa koko palvelun alttiiksi verkkohyökkäykselle.

Kysyin yrityksessä opinnäytetyön ohjaajaltani mielipidettä palvelinohjelmistosta. Hän kertoi minulle, että tärkeisiin palvelimiin on yrityksessä käytetty usein yhteistyökumppanimme omaa Linux-jakelua. Tällöin palvelimien ylläpitoon olisi ongelmatilanteissa saatavilla asiantuntevaa tukea. Myös palvelimien tietoturva sekä ohjelmisto pysyvät jatkuvasti ajan tasalla tällä Linux-jakelulla.

Otin yhteyttä yhteistyökumppaniimme ja keskustelimme puhelimitse palvelimesta, sekä sen tarpeellisista teknisistä ominaisuuksista. Yhteistyökumppanimme kertoi heidän järjestelmänsä pitävän kirjaa palvelimiin asennetuista ohjelmistopaketeista ja niiden versioista. Tällöin mahdollisten tietoturva-aukkojen ja haavoittuvuuksien paikkaus on helppoa sekä nopeaa.

Tulevaisuudessa palvelimen kahdennus on myös helpompaa, koska yhteistyökumppanillamme on laaja kokemus korkean saatavuuden palvelimista ja järjestelmistä. Päätimme yhdessä yrityksen tekniikkaosaston henkilökunnan kanssa, että käytämme palvelimessa tätä yhteistyökumppanimme Linux-jakelua sen tarjoaman lisäarvon vuoksi.

11.1 Kea DHCP-ohjelmiston asennus tuotantopalvelimelle

Asennus sujui yhteistyökumppanin Linux-jakeluun sujuvammin kuin laboratoriossani olevalle palvelimelle. Heidän julkaisustaan löytyi suoraan valmiiksi kaikki tarvittavat paketit Kea DHCP-ohjelmiston asentamiseksi. Asennuksen ja konfiguroinnin jälkeen palvelimelle piti enää avata DHCPv6-portti käyttöjärjestelmän palomuurissa.

Testasimme aluksi uutta palvelinta vanhan DHCPv6-pyyntöjä välittävän reitittimen kanssa, jotta saisimme varmuuden palvelimen toimimisesta. Palvelimeen määritettiin rinnakkainen IPv6-osoitealue, jotta uuden palvelimen toiminnan voisi selvästi erottaa vanhan palvelimen toiminnasta. Testattaessa uusi palvelin alkoi heti jakamaan IPv6-osoitteita DHCPv6-pyyntöjä välittävän reitittimen yli ja totesimme palvelimen konfiguraation toimivaksi.

12 IPv6-osoitteiden välityspalvelun testaus uudella reitittimellä

En ollut aiemmin tehnyt Nokia merkkiseen palvelureitittimeemme DHCPv6-pyyntöjen välitykseen tarvittavaa konfiguraatiota. Lähdin tutkimaan laitteen valmistajan julkaisemaa konfiguraatiomanuaalia, mutta en löytänyt sieltä selvää vastausta siihen, miten tällainen konfiguraatio olisi paras suunnitella. Mietimme tilannetta yhdessä osastollamme ja päätimme että käännyimme asiassa yhteistyökumppanimme puoleen, jolla on syvä kokemus erilaisista laitteen konfiguraatioista.

Saamme tältä yhteistyökumppanilta tarvittaessa tukea laitteiden käytössä ja konfiguroimisessa. He vastasivat todella nopeasti kysymykseen ja lähettivät esimerkki konfiguraation, jolla perustoimivuuden voisi testata.

```

*A:NOKIA-SR>config>router>router-advert# info
-----
interface "dhcp6-testi"
  no shutdown
  exit
-----
*A:NOKIA-SR>config>service>ies# info
-----
interface "dhcp6-testi" create
  ipv6
  address XXXX:XXXX:XXXX:XXXX::1/56
  dhcp6-relay
  lease-populate 100 route-populate pd
  source-address XXXX:XXXX:XXXX:XXXX::1
  link-address XXXX:XXXX:XXXX:XXXX::1
  server XXXX:XXXX:XXXX:X::1
  no shutdown
  exit
exit
sap pw-XXXX:0 create|
exit
exit
no shutdown
-----

```

Kuvio 17: Palvelureitittimen konfiguraatioesimerkki

Yllä olevasta konfiguraatiossa määritellään ensin, että reititin mainostaa välittämiään IPv6-osoitteita verkkoon. Tämän jälkeen konfiguraatiossa määritellään laitteen oman IPv6-rajapinnan osoite sekä DHCPv6-palvelimen osoite. Esimerkistä on poistettu IPv6-osoitteet sekä palvelun tunnus tietoturvan vuoksi.

Konfiguraatioiden tekemisen jälkeen testasimme palvelua yhdessä osastomme vanhemman verkkoinsinöörin kanssa tuotantoverkossa. Testien jälkeen tulimme johtopäätökseen, että DHCPv6-palvelin sekä uusi DHCPv6-pyynnöjä välittävä reititin toimivat suunnitellusti.

13 Palvelinten suorituskyvyn tutkiminen

Olin huomannut Kea DHCP-ohjelmiston dokumentaation tutkimisen yhteydessä, että ISC on kehittänyt myös DHCP-palvelinten testaamiseen tarkoitettun PerfDHCP-työkalun. Tutustuin tähän ohjelmaan nyt tarkemmin, kun molemmat palvelimet olivat rinnakkain asennettuina tuotantoverkossa. Molempia palvelimia olisi mahdollista testata tuotantoverkon yli ja saada niiden suorituskyvystä statistiikkaa. (isc.org 2021b.)

Verkosta löysin Torchinskyn (2017) laatiman hyvän artikkelin. Tässä artikkelissa kerrotaan miten DHCP-testin tuloksia kannattaisi tulkita ja mitä asioita pitäisi ottaa huomioon testauksessa sekä tulosten analysoinnissa.

Tutustuin ensin PerfDHCP-ohjelman käyttämään syntaksiin ja tein muutamia kokeiluja ohjelmalla. Ohjelmaan suoritukseen voi määritellä useita erilaisia ominaisuuksia, mutta päätin pitää testin hyvin yksinkertaisena. Säädin kuitenkin kokeilemalla testin pituuden sopivaksi -p valinnalla sekä lähetettävien osoitepyyntöjen määrän -r valinnalla hieman palvelinten suorituskyvyn yli, jotta testi todella kuormittaisi palvelimia ja näistä saisi keskenään vertailtavaa tietoa. Päädyin testaamaan palvelimia 650 osoitepyynnöllä sekunnissa.

Testissä tehdään automaattisesti sekä Solicit-Advertise sekä Request-Reply testit. Nämä testit eroavat toisistaan tavassa, jolla testin simuloima päätelaite pyytää osoitetta palvelimelta. (IETF 2018.)

13.1 Suorituskykymittauksien analyysi

Pudonneista paketeista oli selvästi nähtävillä, että uusi palvelin vastaa DHCP-kyselyihin huomattavasti varmemmin kuin vanha palvelin. Tämä oli odotettua, koska uusi palvelin oli toteutettu uudemmalla käyttöjärjestelmällä sekä palvelinohjelmistolla.

Odottamaton löydös oli, että uuden palvelimen pakettien viiveet olivat huomattavasti korkeammat kuin vanhan palvelimen. Pohdin mistä ero syntyy ja mielestäni viiveen lisääntyminen johtuu DHCPv6-pyyntöjen välitystehtävän siirrosta Nokian palvelureitittimelle. Vanha Ciscon reititin hoiti pelkästään osoitteiden välittämistä, mutta uudella reitittimellä on tämän lisäksi huomattavasti enemmän tehtäviä.

SOLICIT-ADVERTISE TESTI	Uusi palvelin	Vanha palvelin
Lähetetyt paketit	6498	6499
Vastaanotetut paketit	6063	4965
Pudotetut paketit	435	1534
Pudotettujen pakettien prosenttimäärä	6,69 %	23,60 %
Alin viive	2,944ms	1,336ms
Keskimääräinen viive	47,967ms	1,817ms
Ylin viive	90,636ms	13,476ms
Viiveen keskihajonta	26,005ms	0,38ms

Taulukko 1: Solicit-advertise testitulokset.

REQUEST-REPLY TESTI	Uusi palvelin	Vanha palvelin
Lähetetyt paketit	6063	4965
Vastaanotetut paketit	5759	4397
Pudotetut paketit	304	568
Pudotettujen pakettien prosenttimäärä	5,01 %	11,44 %
Alin viive	2,944ms	1,336ms
Keskimääräinen viive	47,967ms	1,817ms
Ylin viive	90,636ms	13,476ms
Viiveen keskihajonta	26,005ms	0,38ms

Taulukko 2: Request-reply testitulokset.

Yllä olevissa taulukoissa näkyy selvästi väreillä erotettuna testissä esiin tulleet tulokset. Uuden palvelimen Solicit-Advertise testin pakettihävikki on vain 6,69 % kun vanhassa palvelimessa sama hävikki on 23,6 %. Fortinetin verkkosivuilla olevan tiedon mukaan pakettihäviötä voi tapahtua, kun palvelin on liian kuormittunut. Testi suoritettiin palvelinten suorituskyvyn rajoilla, jotta mittaus tuloksista nähtäisiin selvästi palvelinten välinen ero. (Fortinet 2021.)

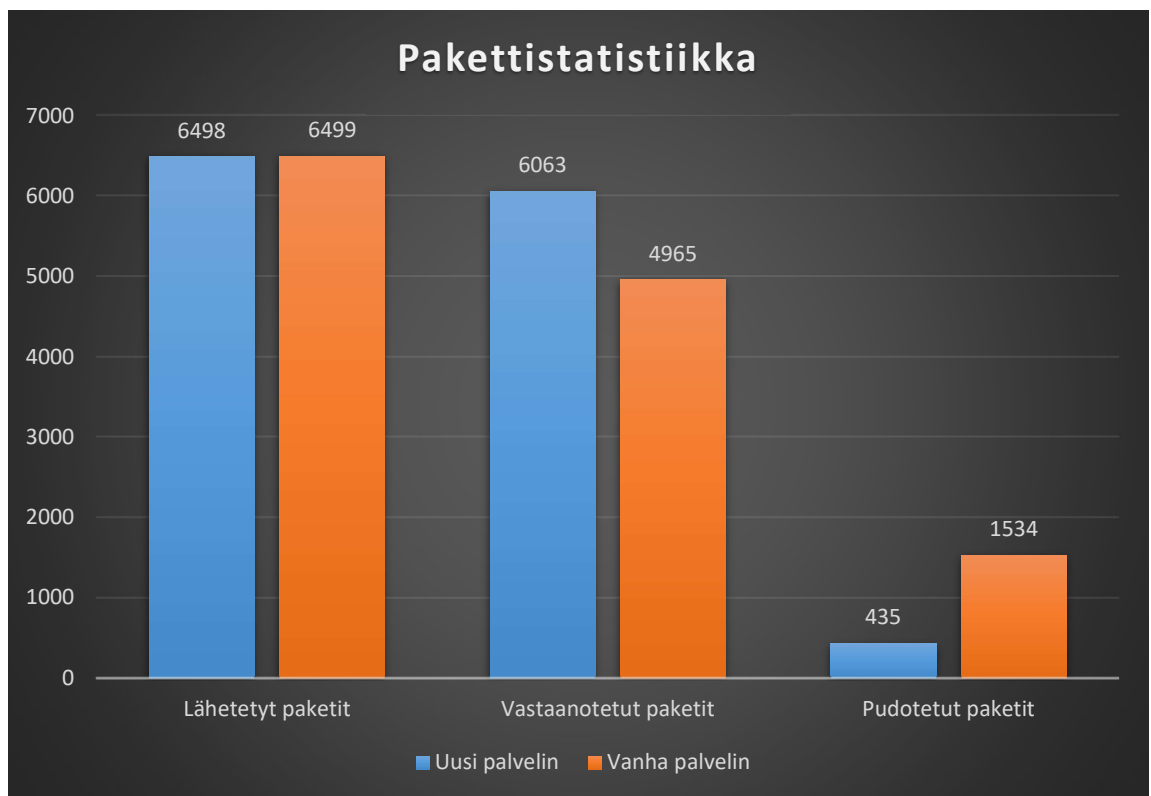
Pudotettujen pakettien määrästä voidaan päätellä, että testiin valitut pakettimäärien mittauseräparametrit olivat hyvin valittu. Testi tuotti selkeän lopputuloksen, josta pystyy helposti toteamaan palvelinten suorituskyvyn eron.

Viiveellä tarkoitetaan aikaa, joka paketin lähettämisestä kuluu vastauksen vastaanottamiseen. Viiveellä on suuri merkitys, kun kyse tiedonsiirron tulisi olla mahdollisimman reaaliaikaista tai kun verkkoon liikennöivän ohjelman toiminnan kannalta viiveiden tulisi olla mahdollisimman pienet. (SAS Global Communications Ltd 2021.)

Pakettien viiveet ovat uudella palvelimella ja uuden palvelureitittimen läpi yllättäen huomattavasti suuremmat. Epäilen että uudessa reitittimessä on sisäisesti jaettu tehtäviä eri kiireellisyysluokkiin ja IPv6-osoitteiden välitys DHCPv6 protokollalla ei ole näistä tehtävistä kaikkein tärkein. Tämän vuoksi sille ei luultavasti anneta laitteella juurikaan prosessoriaikaa. Etsin tietoa eri liikennetyyppien sisäisestä priorisoinnista laitteen manuaalista, mutta tästä ei löytynyt tarkkaa kuvausta.

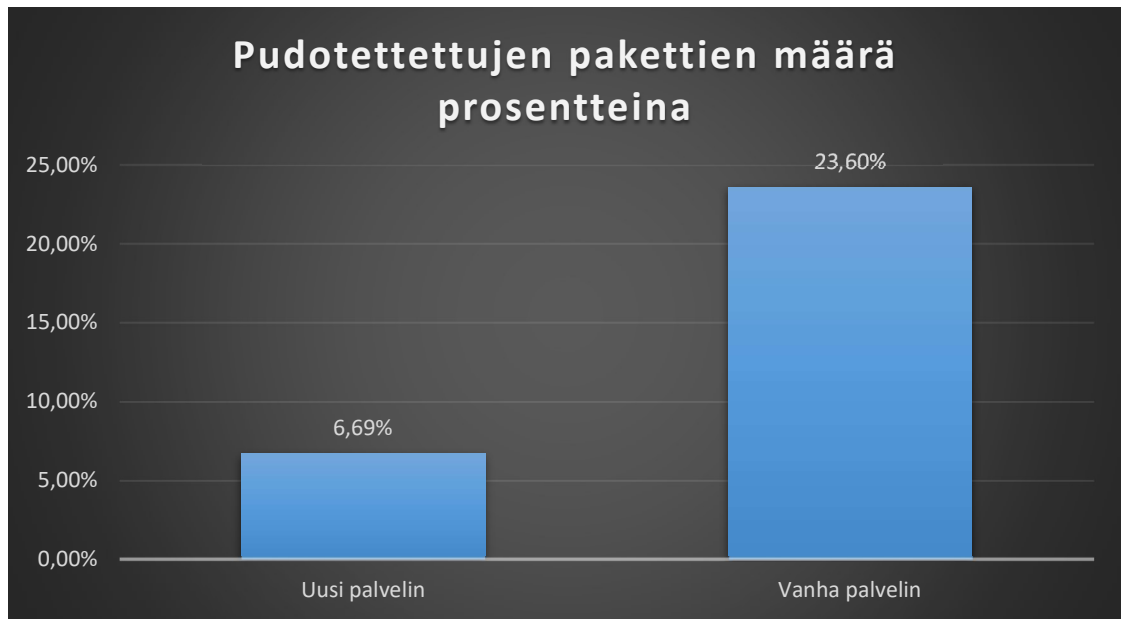
Viive pysyy mielestäni kuitenkin kohtuullisena koska testi tehtiin palvelimen suorituskyvyn rajoilla ja paketteja putosi uudella palvelimella sekä reitittimellä vähemmän kuin vanhalla palvelimella. Täten pakettien viive ei ole ainoa palvelun laatua kuvaava mittari vaan pudotettujen pakettien määrästä on selvästi nähtävillä, että uusi palvelin vastaa pyyntöihin huomattavasti luotettavammin, pyyntöjen mennessä uuden palvelureitittimen läpi.

Verkon asiakkaiden päätelaitteet eivät myöskään normaaleissa olosuhteissa hae osoitteita samalla hetkellä. Mikäli päätelaite ei saa osoitepyyntöön vastausta se lähettää hetken kuluttua uuden pyynnön. Ainoa tilanne milloin satoja tai tuhansia laitteita hakisi samaan aikaan osoitetta, olisi esimerkiksi isosta alueellisesta sähkökatkosta palautuminen. Tällöinkin laitteet käynnistyisivät hieman eri aikoihin, joten palvelin selviäisi osoitepyynnöistä ongelmitta, pystyessään käsittelemään ongelmitta yli 600 osoitepyyntöä sekunnissa. (Torchinsky 2017.)



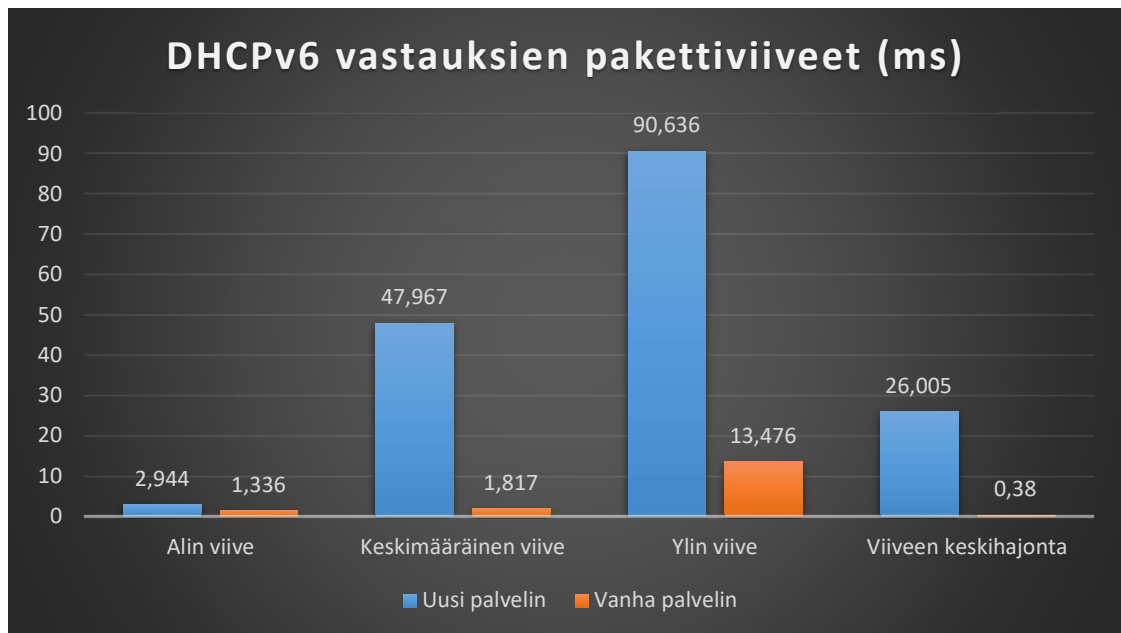
Kuvio 18: Solicit-advertise testin pakettistatistiikka.

Yllä olevassa kuviossa näkyy pakettistatistiikassa, että paketteja on lähetetty palvelimelle testauksen aikana melko tarkalleen sama määrä. Vanha palvelin on pudottanut samalla pakettimäärällä n. 1000 pakettia enemmän kuin uusi palvelin.



Kuvio 19: Solicit-advertise testissä pudonneet paketit.

Yllä olevassa kuviossa näkyy, että vanha palvelin pudotti lähes neljänneksen paketeista. Uuden palvelimen pakettihävikki jäi alle 7 prosenttiin.



Kuvio 20: Solicit-advertise testin pakettiviiveet.

Oheisessa kuviossa näkyy selvästi, että uuden palvelimen vastaanottamat, sekä Nokian palvelureitittimen läpi menneiden pakettien viiveet ovat huomattavasti isommat kuin vanhassa järjestelmässä. Uuden järjestelmän korkein viive on lähes sekunnin mittainen, vanhan järjestelmän ylimmän viiveen jäädessä 13 millisekuntiin.

14 Uuden DHCPv6-palvelimen käyttöönotto

Testasin asennuksen jälkeen kattavasti uutta palvelinta sekä kuormitin sitä PerfDHCP-testillä sen suorituskyvyn äärirajoille. Kun olin varmistunut, että DHCPv6-palvelin sekä palvelureitittimen DHCPv6-Relay toimivat vaaditulla tasolla niin kävimme tarkemman palaverin DHCPv6-palvelusta tekniikkaosastomme sekä palvelureitittimien konfiguraatioissa auttavan yhteistyökumppanimme kanssa. Tarkoituksemme oli selvittää mikä olisi paras käytäntö alkaa siirtämään asiakkaita uudelle palvelimelle.

Palaverissa meille selvisi, että IPv6-käyttäjän tunnistamista varten meidän tarvitsisi vielä siirtää myös IPv4-Relay toiminto palvelureitittimelle, jotta IPv4- sekä IPv6-tiedot voidaan liittää toisiinsa. Olimme ajatelleet tätä vaihtoehtoa jo aiemmin palvelua suunnitellessa ja teimmekin nyt päätöksen kahdentaa palvelimet sekä reitittimet. IPv4 DHCP-palvelut sekä DHCP4-Relay siirrettäisiin myös uusille palvelimille ja reitittimille.

Tämä tarkoittaa todella isoa muutosta verkossa ja päätimme DHCPv6-palvelimen käyttöönoton sijaan alkaa suunnittelemaa muutoksia verkkoon myös IPv4-toiminnallisuuksien osalta. Koska IPv4-palvelut ovat kriittisiä asiakasyhteyksien toimivuuden kannalta, niin asiakkaiden siirrot tulisi myös suunnitella erittäin tarkasti. Päätimme tässä vaiheessa ottaa projektiin mukaan lisää henkilöstöä työmäärän kasvaessa huomattavasti.

15 Johtopäätökset ja yhteenveto

Opinnäytetyön tekeminen oli hyvin mielenkiintoista, koska sen tekeminen liittyi vahvasti työtehtäviini. Työssä sain tutkia sekä kehittää tuotantoverkkoon käyttöön tulevaa aitoa järjestelmää. Tämä lisäsi motivaatiota työn tekemiseen. Opinnäytetyön tekeminen ja siihen liittyvä tutkimustyö lisäsi myös huomattavasti osaamistani.

Mielestäni opinnäytetyö eteni loogisesti alkaen aiheen teoriaan tutustumisesta. Kun olin saanut riittävän tietoperustan, niin etenin ensin suunnittelutyöhön. Suunnittelun jälkeen asensin palvelimen tuotantoverkkoon. Lopuksi palvelut testattiin johdonmukaisesti, sekä niitä verrattiin keskenään saatujen testitulosten varjossa.

Kertyneen kokemukseni mukaan palvelimen topologian sekä muiden ominaisuuksien suunnitteluun tulisi varata riittävästi aikaa ja suunnitelmiin tulisi kiinnittää hyvin paljon huomiota ennen työhön ryhtymistä. Tällä vältettäisiin mahdollisia virheitä prosessin edetessä. Vastaava kehitysprojekti voikin mielestäni kaatua myöhemmässä vaiheessa juuri heikon suunnittelun vuoksi.

Huomasin opinnäytetyötä tehdessäni, että tutkimus- ja kehitysprojektiä tehdessä on vaarana ajatella asioita hyvin yksipuoleisesti. Tällöin helposti ei tule otettua kaikkia tärkeitä asioita huomioon. Saadun kokemukseni perusteella näin laaja kehitysprojekti tulisi tehdä työryhmänä heti projektin suunnittelusta alkaen, jotta projektiin saataisiin tarpeeksi näkökulmia. Onnekseni minulla oli läpi opinnäytetyöhön hyvä tuki sisäisistä- sekä ulkoisista sidosryhmistä, joka mahdollisti näin laajan kokonaisuuden tutkimisen ja suunnittelun.

Työn edetessä huomasimme yhdessä sisäisien sidosryhmien kanssa, että tässä opinnäytetyössä kertyneen tiedon perusteella verkkoon tulee tehdä paljon aiottua suurempia muutoksia. Tämän vuoksi IPv6 DHCPv6-palvelun siirtäminen uudelle palvelimelle ei ollut tässä vaiheessa vielä kannattavaa. Tarkemmalla suunnittelulla heti työn alussa olisi voitu kartoittaa kokonaisuus paremmin ja varautua siihen, että kokonaisuus laajenee työn edetessä huomattavasti. Tämä olisi helpottanut työn suunnittelua ja siinä etenemistä.

Mielestäni työssä päästiin kuitenkin toivottuun lopputulokseen ja saatiin runsaasti kokemusta palvelimesta, sen konfiguraatiosta sekä DHCPv6-pyynnöjä välittävän reitittimien konfiguroimisesta. Palvelin toimi suunnitelmien mukaisesti ja antoi asiakaslaitteelle sen pyytämän IPv6-osoitteen tai Prefix Delegation-verkon.

Työn edetessä tutustuin myös korkean saatavuuden suunnitteluun, IPv4-ominaisuuksien liittämiseen järjestelmään sekä reitittimien kahdentamiseen. Nämä asiat toivat mielestäni työlle runsaasti lisäarvoa. Nämä kerääntyneet tiedot toimivat apuna myös palvelun jatkokehityksessä.

16 Jatkokehitysehdotukset

Jatkossa palvelua lähdetään rakentamaan suunnitteleamalla siihen myös IPv4-toiminnallisuus sekä reitittimien ja palvelinten kahdennus. Nämä ovat todella laajoja osa-alueita, joissa tarvitaan osaamista useasta eri tekniikasta ja laitteesta, sekä niiden yhteensovittamisesta.

Näihin jatkokehityssuunnitelmiin onkin perusteltua hankkia apua yrityksen ulkopuolisilta sidosryhmiltä. Jatkosta onkin jo sovittu ulkoisten sidosryhmien kanssa sekä hankittu yrityksen sisällä esimiehiltä lupa kehittämisprosessissa etenemiseen.

Palvelimen kahdentamisen dokumentaatioon tulee perehtyä ennen työn aloittamista ja palvelin tulee kahdentaa heti jatkokehityksen alkuvaiheessa. Myös palvelureitittimen kahdentaminen tarvitsee tarkkaa suunnittelua. Näin laajaa muutosta ei voi tehdä kerralla, vaan asiakasverkot tulee siirtää hallitusti yksi kerrallaan uusille palvelimille sekä reitittimille.

Palvelimille tulee lisäksi laatia päivitys suunnitelma sekä nimetä henkilö hoitamaan palvelimien ylläpito. Tämän lisäksi palvelimet tulee lisätä aktiivisen verkonvalvonnan piiriin, jotta mahdollisista virhetilanteista saadaan heti tieto päivystäjälle myös työajan ulkopuolella.

Tässä työssä ei keskitytty varsinaisesti Linux-palvelimen vaatimiin tietoturva ominaisuuksiin, joten nämä tulee vielä ennen palvelinten käyttöönottoa laittaa kuntoon.

Tietoturvaominaisuudet tulee suunnitella hyviä käytäntöjä seuraten. Yrityksessä onkin käytössä politiikka, että kaikki liikenne kielletään laitteiden palomuuereissa oletuksena ja sallitaan vain turvalliseksi tiedetty liikenne. Tämä onkin tärkein ohjenuora palomuurien konfiguroinnissa. (Contreras 2020.)

17 Oman oppimisen arviointi

Olen kiinnostunut palvelimista, tietotekniikasta sekä tietoliikenteestä ja työskentelen tietoliikennealalla. Tämän vuoksi opinnäytetyön tekeminen oli hyvin mielenkiintoista ja opettavaista. Opinnäytetyön tekeminen työnantajalle työtehtäviini liittyvästä aiheesta tuki myös omaa työssä kehittymistäni. Yrityksen saamien hyötyjen lisäksi tästä opinnäytetyöstä oli hyötyä myös minulle osaamiseni kehittymisen ja tietojeni lisääntymisen muodossa.

En ollut aiemmin ollut juurikaan tekemisissä IPv6-protokollan tai DHCPv6-palvelun kanssa. Opinnäytetyön ohessa opin näistä asioista valtavasti ja tunnen nyt molemmat erittäin hyvin. Lisäksi tutustuin palveluiden kahdentamiseen sekä verkkoarkkitehtuureihin. Pääsin myös soveltamaan oppimaani tietoa käytännössä ja rakentamaan toimivan palvelun verkkoon. Opin myös mittaamaan palveluiden ominaisuuksia ja analysoimaan mittauksien tuloksia.

Opinnäytetyöstä lähti eteenpäin isompi kehitystyö, jota jatketaan isommilla resursseilla. Täten asian tiimoilta oppiminen ei lopu tämän opinnäytetyön sisältöön vaan jatkuu projektin edetessä.

Opin työn aikana myös johdonmukaisen etenemisen merkityksen kehitys- ja tutkimustyössä sekä suunnittelun ja valmistelun tärkeyden kokonaisuuden kannalta. Nämä taidot auttavat minua varmasti myös tulevaisuudessa kehitystyön jatkuessa tässä projektissa sekä muussa työssäni.

Lähteet

Sähköiset

Bharitya, S. 2019. Red Hat Announces CentOS Stream. Viitattu 18.4.2021. <https://www.linux-magazine.com/Online/News/Red-Hat-Announces-CentOS-Stream>

Blank, A.G. 2002. TCP/IP JumpStart: Internet Protocol Basics. Viitattu 28.3.2021. New Jersey, USA: John Wiley & Sons, Incorporated.

CentOS. 2020a. CentOS Product Specifications. Viitattu 18.4.2021
<https://wiki.centos.org/About/Product>

Centos. 2020b. FAQ - CentOS Project shifts focus to CentOS Stream. Viitattu 28.3.2021.
<https://blog.centos.org/2020/12/future-is-centos-stream/>

Cisco Press. 2014. Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. Viitattu 31.3.2021.
<https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=5>

Cisco Systems. 2021. What Is Network Architecture? Viitattu 31.3.2021.
<https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-architecture.html>

Contreras, R. 2020. Best practices for firewall rules configuration. Viitattu 18.4.2021.
<https://docs.rackspace.com/support/how-to/best-practices-for-firewall-rules-configuration/>

Fortinet. 2021. What is Packet Loss? Viitattu 22.5.2021
<https://www.fortinet.com/resources/cyberglossary/what-is-packet-loss>

Heidi, E. 2016. What is High Availability? Viitattu 17.4.2021.
<https://www.digitalocean.com/community/tutorials/what-is-high-availability>

Hess, K. 2020. How to query files, packages, and repositories in Linux. Viitattu 13.4.2021
<https://www.redhat.com/sysadmin/package-queries>

IETF. 1981. RFC 791, Internet Protocol. Viitattu 28.3.2021. <https://tools.ietf.org/html/rfc791>

IETF. 1997. RFC 2131, Dynamic Host Configuration Protocol. Viitattu 28.3.2021.
<http://www.ietf.org/rfc/rfc2131.txt>

IETF. 2017. RFC 8200, Internet Protocol, Version 6 (IPv6) Specification. Viitattu 28.3.2021.
<https://tools.ietf.org/html/rfc8200>

IETF. 2018. RFC 8415, Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Viitattu 28.3.2021. <https://tools.ietf.org/html/rfc8415>

IETF. 2021a. About. Viitattu 22.5.2021. <https://www.ietf.org/about/>

IETF. 2021b. RFCs. Viitattu 22.5.2021 <https://www.ietf.org/standards/rfcs/>

Internet Systems Consortium. 2020. Kea Administrator Reference Manual. Viitattu 17.4.2021. <https://kea.readthedocs.io/en/kea-1.8.2/>

Isc.org. 2020. Kea DHCP. Viitattu 17.4.2021. <https://www.isc.org/kea/>

Isc.org. 2021a. About Us. Viitattu 17.4.2021. <https://www.isc.org/about/>

Isc.org. 2021b. perfdhcp - DHCP benchmarking tool. Viitattu 18.4.2021. <https://kea.readthedocs.io/en/latest/man/perfdhcp.8.html>

Isc.org. 2021c. Cloudsmith Repositories for BIND 9 and Kea DHCP. Viitattu 17.4.2021. <https://www.isc.org/blogs/cloudsmith-repos/>

Juniper Networks. 2021. What is the difference between IPv4 and IPv6. Viitattu 17.4.2021. <https://www.juniper.net/us/en/products-services/what-is/ipv4-vs-ipv6/>

Linuxise.com. 2019. How to Install RPM Files (Packages) on CentOS Linux. Viitattu 17.4.2021. <https://linuxize.com/post/how-to-install-rpm-packages-on-centos-linux/>

Microsoft. 2018. Introduction to Hyper-V on Windows 10. Viitattu 17.4.2021. <https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/>

Nieminen, K. 2019. Suositus IPv6:n käyttöönotosta kuluttajalaajakaistaliittymissä. Viitattu 28.3.2021. <https://www.traficom.fi/sites/default/files/media/regulation/Suositus-IPv6n-kayttoonotosta-kuluttajalaajakaistaliittymissa.pdf>

RIPE NCC. 2019. Understanding IP Addressing and CIDR Charts. Viitattu 28.3.2021. <https://www.ripe.net/about-us/press-centre/understanding-ip-addressing>

RIPE NCC. 2021. What is IPv4 Run Out? Viitattu 28.3.2021. <https://www.ripe.net/manage-ips-and-asns/ipv4/ipv4-run-out>

Router-switch.com. 2013. Networks in 2020: More Traffic, Less Energy. Viitattu 17.4.2021. <https://blog.router-switch.com/2013/05/networks-in-2020-more-traffic-less-energy/>

SAS Global Communications Ltd. 2021. What is network latency (and how do you use a latency calculator to calculate throughput)? Viitattu 22.5.2021. <https://www.sas.co.uk/blog/what-is-network-latency-how-do-you-use-a-latency-calculator-to-calculate-throughput>

Shein, E. 2020. Moore's Law turns 55: Is it still relevant? Viitattu 13.4.2021. <https://www.techrepublic.com/article/moores-law-turns-55-is-it-still-relevant/>

Torchinsky, M. 2017. Measuring DHCP Performance. Viitattu 18.4.2021. <https://www.intraway.com/blog/white-paper/measuring-dhcp-performance/>

Traficom. 2020. Tahto liikkua ja viestiä on meillä kaikilla. Sinun yhteytesi ovat meille sydämenasia. Viitattu 28.3.2021 <https://www.traficom.fi/fi/tahto-liikkua-ja-viestia>

Walter Goralski. 2014. Learn About Difference in Addressing Between IPv4 and IPv6. Viitattu 17.4.2021. https://www.juniper.net/documentation/en_US/learn-about/ipv4-ipv6-differences.pdf

Zhang, L. 2007. A Retrospective View of NAT. Viitattu 28.3.2021. <https://www.ietfjournal.org/a-retrospective-view-of-nat/>

Kuviot

Kuvio 1: Nykyinen topologia.....	14
Kuvio 2: Korkean saatavuuden palvelussa reitittimet sekä palvelimet on kahdennettu.....	16
Kuvio 3: Hyper-V ohjelman graafinen käyttöliittymä on selvä ja helppokäyttöinen	18
Kuvio 4: Ohje cloudsmith.io RPM pakettilähteen asennuksesta CentOS 7 käyttäjärjestelmään	19
Kuvio 5: Komento EPEL pakettilähteen asentamiseksi	19
Kuvio 6: Komento KeaMA ohjelman sisältävän pakettivaraston asentamiseksi	20
Kuvio 7: Komento KeaMA ohjelman asentamiseksi.....	20
Kuvio 8: Komento konfiguraation konvertoimiseksi KeaMA ohjelmalla	21
Kuvio 9: IP-tietokannan konfiguraatio	21
Kuvio 10: Lokien konfiguraatio	22
Kuvio 11: Interface konfiguraatio	22
Kuvio 12: Osoitteiden voimassaoloaika	22
Kuvio 13: Verkot ja jaettavien osoitteiden IPv6-Alueet.....	23
Kuvio 14: Prefix delegaation konfiguraatio	23
Kuvio 15: Kean prosessi aktiivisena palvelimessa	24
Kuvio 16: Palomuuuri sammutettuna.....	24
Kuvio 17: Palvelureitittimen konfiguraatioesimerkki.....	27
Kuvio 18: Solicit-advertise testin pakettistatistiikka.	30
Kuvio 19: Solicit-advertise testissä pudonneet paketit.....	31
Kuvio 20: Solicit-advertise testin pakettiviiveet.	31

Taulukot

Taulukko 1: Solicit-advertise testitulokset.....	28
Taulukko 2: Request-reply testitulokset.	29

Liitteet

Liite 1: KeaMA-ohjelmistolla muutettu valmis konfiguraatio.....	41
Liite 2: Uuden palvelimen PerfDHCP testin tulos	42
Liite 3: Vanhan palvelimen PerfDHCP testin tulos	43


```

{
  "Dhcp6": {
    "lease-database": {
      "type": "memfile",
      "persist": true,
      "name": "/var/log/kea-leases6.csv",
      "lfc-interval": 1800,
      "max-row-errors": 100
    },
    "loggers": [{
      "name": "kea-dhcp6",
      "output_options": [{
        "output": "/var/log/kea-debug.log",
        "maxver": 8,
        "maxsize": 204800,
        "flush": true,
        "pattern": "%d{%j} %H:%M:%S.%q} %c %m\n"
      }],
      "severity": "DEBUG",
      "debuglevel": 99
    }],
    "interfaces-config": {
      "interfaces": ["ens3/XXXX:XXXX:XXX:X::XX"]
    },
    "min-valid-lifetime": 14400,
    "valid-lifetime": 43200,
    "max-valid-lifetime": 86400,
    "subnet6": [{
      "id": 1,
      "subnet": "XXXX:XXXX:XXX:X::/64"
    },
    {
      "id": 2,
      "subnet": "XXXX:XXXX:XXXX::/36",
      "option-data": [{
        "space": "dhcp6",
        "name": "dns-servers",
        "code": 23,
        "data": "XXXX:XXXX:XXX:X::X, XXXX:XXXX:XXX:X::X"
      },
      {
        "space": "dhcp6",
        "name": "domain-search",
        "code": 24,
        "data": "XXXXX.dhcp6.fi"
      }
    ]
  },
    "pools": [{
      "pool": "XXXX:XXXX:XXXX:XX:X::1-XXXX:XXXX:XXXX:XX:ffff:ffff:ffff:ffff"
    }],
    "pd-pools": [
      {
        "prefix": "XXXX:XXXX:XXXX::",
        "prefix-len": 48,
        "delegated-len": 56
      }
    ]
  }
}

```

Liite 1: KeaMA-ohjelmistolla muutettu valmis konfiguraatio

```
Scenario: basic.
***Rate statistics***
Rate: 575.746 4-way exchanges/second, expected rate: 650

***Malformed Packets***
Malformed packets: 0
***Statistics for: SOLICIT-ADVERTISE***
sent packets: 6498
received packets: 6063
drops: 435
drops ratio: 6.69437 %
orphans: 0
rejected leases: 0
non unique addresses: 0

min delay: 2.944 ms
avg delay: 47.967 ms
max delay: 90.636 ms
std deviation: 26.005 ms
collected packets: 53

***Statistics for: REQUEST-REPLY***
sent packets: 6063
received packets: 5759
drops: 304
drops ratio: 5.014 %
orphans: 0
rejected leases: 5
non unique addresses: 0

min delay: 3.099 ms
avg delay: 47.106 ms
max delay: 90.922 ms
std deviation: 26.308 ms
collected packets: 31

[root@localhost ~]# s
```

Liite 2: Uuden palvelimen PerfDHCP testin tulos

```
Scenario: basic.
***Rate statistics***
Rate: 439.663 4-way exchanges/second, expected rate: 650

***Malformed Packets***
Malformed packets: 0
***Statistics for: SOLICIT-ADVERTISE***
sent packets: 6499
received packets: 4965
drops: 1534
drops ratio: 23.6036 %
orphans: 0
rejected leases: 0
non unique addresses: 0

min delay: 1.336 ms
avg delay: 1.817 ms
max delay: 13.476 ms
std deviation: 0.380 ms
collected packets: 880

***Statistics for: REQUEST-REPLY***
sent packets: 4965
received packets: 4397
drops: 568
drops ratio: 11.440 %
orphans: 0
rejected leases: 0
non unique addresses: 0

min delay: 1.374 ms
avg delay: 1.953 ms
max delay: 14.317 ms
std deviation: 0.451 ms
collected packets: 333

[root@localhost ~]# _
```

Liite 3: Vanhan palvelimen PerfDHCP testin tulos