Simo Hurttila

Verkonvalvontapalvelun testaus IPv6-ympäristössä

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Insinöörityö
29.11.2011

Tekijä Otsikko Sivumäärä Aika	Hurttila Simo Verkonvalvontapalvelun testaus IPv6-ympäristössä 49 sivua + 2 liitettä 29.11.2011
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoliikennetekniikka
Ohjaajat	tietoliikenneasiantuntija Jaakko Rautanen yliopettaja Matti Puska

Tämä työ tehtiin Cygate Oy:lle. IPv4:n (Internet-protokollan versio 4) loppuunkäytetty osoiteavaruus, ja muut lukuisat puutteet ovat aiheuttaneet sen, että yritysten on alettava varautua lähitulevaisuudessa tapahtuvaan IPv6:n (Internet-protokollan versio 6) käyttöönottoon. Kun tämä muutos tapahtuu, niin Cygaten on oltava valmis suoriutumaan verkonvalvonta- ja hallintatehtävistä myös IPv6-ympäristöissä.

Työn tavoitteena oli rakentaa perinteistä asiakasverkkoa vastaava IPv6:ta tukeva laboratorioympäristö, suorittaa suunnitelmien mukaiset testit, sekä kuvata testien aikana ilmenneet ongelmat ja rajoitukset. Työn alussa kuvattiin yleisimmät verkonvalvontaan ja –hallintaan käytetyt proseduurit ja protokollat (SNMP, ICMP, Syslog, MIB) mahdollisia rajoittuvuuksia samalla etsien IPv6:n näkökulmasta. Tämän jälkeen esiteltiin Cygaten nykyinen hallinta- ja valvonta-alustan kokoonpano ja toiminnallisuus.

Teoriaosuuden jälkeen suunniteltiin GNS3-virtuaaliympäristöön toteutettava perinteistä asiakasympäristöä vastaava tietoverkko, jonka laitteet toimivat työssä valvottavina kohteina. Suunnitteluosuus piti sisällään myös IPv6-osoitteistuksen ja aliverkkojen suunnittelun. Reititysprotokollaksi valittiin OSPFv3.

Lopuksi suunnitelmat toteutettiin suljetussa laboratorioympäristössä, ja konfiguroitiin laitteille työn alussa esitetyt tavallisimmat, myös tämänhetkisen Cygaten valvonta- ja hallinta-alustan käyttämät, verkonhallintaprotokollat, sekä selvitettiin ja tutkittiin niiden toimintaa yksityiskohtaisemmin. Työn viimeisessä osuudessa esitettiin arvio mahdollisuudesta ja aikataulusta siirtää palvelu tuotantoon. Testit osoittivat, että palvelu ei ole vielä valmis tuotantoon siirrettäväksi. Samalla esitettiin suositeltavat jatkotoimenpiteet.

Avainsanat	verkonvalvonta, verkonhallinta, IPv6, OSPFv3, ICMP, SNMP, Syslog, MIB, GNS3

Author Title Number of Pages Date	Simo Hurttila Testing network management service in IPv6 environment 49 pages + 2 appendices 29 November 2011
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructors	Jaakko Rautanen, Network Specialist Matti Puska, Principal Lecturer

This thesis was made for Cygate corporation. The driving force for this work was the exhausted IPv4 (Internet Protocol version 4) address space and the fact that companies will have to implement IPv6 (Internet Protocol version 6) networks in the near future. At that time Cygate needs to have a ready, secure and reliable solution to offer with an equal amount of features compared to the present system.

The main targets were to build a traditional and fully native IPv6 network in a virtualized environment and to run the planned tests using the same methods as the present network management system uses with IPv4. All the faced problems were documented carefully if they could not be solved during the project and if they were clearly out of the networking scope. The results were delivered to the network management system development team at Cygate who will initiate a sequel project and try to investigate and solve the emerged problems.

At the beginning, the thesis introduces traditional network management procedures and protocols from the IPv6 point of view. Cygate's existing network management platform is introduced followed by the plans to test it in an IPv6 environment. The plans also include addressing and subnetting the network with investigations for which dynamic routing protocol will be used. OSPFv3 was chosen as the routing protocol. After careful planning, the plan was excecuted in a closed network made for testing purposes only. After the basic network level connectivity with the dynamic routing was achieved, network monitoring specific configurations were executed and investigated in detail. All the tools, devices and addressing reflected the real customer networks indicating that the tests made would also be reliable in other environments.

The last part of the thesis discusses the possibility and schedule to move the IPv6 network management service into a production environment. Testing showed that the service is not completely ready for the production environment. Suggestions on how to proceed from here are given at the end.

Keywords	Network management, IPv6, OSPFv3, ICMP, SNMP, Syslog, MIB, GNS3

Sisällys

1 Johdanto

Tämän insinöörityön on tilannut Cygate Oy. Cygaten toimintaan kuuluu turvallisten IP-teknologiaan perustuvien tietoverkkojen suunnittelu, toimitus ja hallinta. Cygate-konsernissa työskentelee tällä hetkellä noin 500 työntekijää Suomessa ja Ruotsissa. Työ käsittelee Cygaten tarjoamaa verkonvalvontapalvelun testausta IPv6-ympäristössä laboratorio-olosuhteissa. Työn tavoitteena on rakentaa perinteistä asiakasverkkoa vastaava IPv6:ta tukeva laboratorioympäristö, suorittaa suunnitelmien mukaiset testit, sekä kuvata testien aikana ilmenneet ongelmat ja rajoitukset. Työn lopuksi esitetään arvio, onko järjestelmä mahdollista ottaa käyttöön tuotantoympäristössä, ja millä aikataululla. [1.]

IPv6 (Internet Protocol version six) on jatkojalostettu versio IPv4:stä (Internet Protocol version four). IPv4 on käytössä lähes kaikissa tietoverkoissa, mutta kyseisen protokollan rajoitukset ovat aiheuttaneet sen, että uutta protokollaversiota on alettu ottaa käyttöön ja siihen tullaan siirtymään vaiheittaisesti tulevaisuudessa. Muutos ei tule tapahtumaan lyhyessä ajassa, vaan siirtyminen tapahtuu vaiheittain siten, että nämä kaksi edellä mainittua protokollaa tulevat toimimaan samanaikaisesti toisiaan tukien. [2, s. 6–8.]

Yritysten ja organisaatioiden on varauduttava sekä valmistauduttava vaiheittaiseen muutokseen. Tästä syystä Cygaten on oltava valmis tuottamaan verkonvalvontapalvelua asiakkailleen myös IPv6-ympäristöissä. IPv6-ympäristöjen verkonvalvonnan mahdollistaminen tarjoaa yritykselle vahvan kilpailuvaltin. Tämä opinnäytetyö käsittelee ainoastaan verkonvalvontaa asiakkaiden paikallisverkoissa IPv6-ympäristöissä sekä valvontainformaation käsittelyä Cygaten toimesta. Työ ei ota kantaa siirtotekniikoihin tai protokolliin laajaverkoissa, vaan tarkoitus on tutkia IPv6:n yhteensopivuutta jo olemassa olevaan palveluun. IPv6:ta käytetään jo tuotantoympäristöissä laajaverkoissa jonkin verran, ja kyseiset laajaverkkojen siirtotekniikat tulevat olemaan standardeja tulevaisuudessa. Cygaten verkonvalvontapalvelun on tuolloin oltava yhteensopiva näiden kyseisten standardien kanssa. On selvää, että verkonvalvontapalveluun tullaan tekemään teknisiä muutoksia

IPv6:n valtaannousun myötä, ja tämän työn tarkoitus on kartoittaa juuri nämä muutosta vaativat kohdat.

2 Verkonvalvonnan ja -hallinnan toiminta

Tietoverkot ovat nykypäivänä elinehto useiden yritysten toiminnan kannalta. Tästä syystä niiden toiminnan ylläpitämiseen ja seuraamiseen käytetään verkonvalvontaa. Verkonvalvonnalla tarkoitetaan asiakkaan tietoverkossa sijaitsevien verkkolaitteiden, kuten reitittimien ja kytkimien, aktiivista seurantaa. Aktiivinen seuranta perustuu automatisoituihin kaksisuuntaisiin valvontakeinoihin. Verkonvalvontajärjestelmä tiedustelee aktiivisesti valvottavien laitteiden tilaa ennaltamääritetyin väliajoin.

Laite voi myös itsenäisesti raportoida verkonvalvontajärjestelmälle muuttuneesta tilasta. Tavoitteena on saada selville ei-toivotut tapahtumat verkossa, ja näin pienentää esimerkiksi laiterikkoutumisen sattuessa siitä aiheutuneita epäsuoria kuluja. Epäsuoria kuluja aiheutuu esimerkiksi silloin kun tietoverkko on laitevian takia käyttökelvoton, ja silloin kun yrityksen ydintoiminta on täysin riippuvainen toimivasta tietoverkosta. Pitkällä aikajaksolla ajateltuna verkonvalvonta määrittää myös tietoverkon toiminnalle niin sanotun normaalitilan. Tätä tilaa tavoitellaan, ja kaikki tuota tilaa alentavat tapahtumat ovat ei-toivottuja ja sellaisia jotka tulisi havaita ajoissa verkonvalvonnan kautta ylimääräisten kulujen minimoimiseksi. Tietoverkkojen moninaisuus on kuitenkin johtanut siihen, että jotkin verkonvalvontaan liittyvistä standardeista eivät enää päde koko verkossa, mikä lopulta on johtanut räätälöityihin ratkaisuihin ja täten kokonaiskustannusten nousuun. Laadukkaasti toteutettu verkonvalvonta ei siis ole yritykselle välttämättä kannattavaa, ellei koko liiketoiminta perustu toimivaan ja luotettavaan tietoverkkoon. [3; 4.]

2.1 Verkonvalvonnan ja -hallinnan eri osa-alueet

Verkonvalvonta ja -hallinta voidaan jakaa taulukossa 1 esitettyihin prosesseihin. [4; 5.]

Taulukko 1. Verkonvalvonnan ja -hallinnan prosessit.

Toiminto	Selite
Konfiguraatiohallinta	Konfiguraationhallinnalla määritellään muun muassa asiakkaan tietoliikenneverkon laitteet, niiden väliset relaatiot ja ominaisuudet yhtenäiseen tietojärjestelmään. Tällaista tietovarastoa kutsutaan nimellä Configuration Management Database (CMDB).
Vikatilanteiden hallinta	Palvelua häiritsevän vian havaitseminen, palvelun palauttaminen ja ennaltaehkäisevä toiminta.
Suorituskyvyn hallinta	Tietoverkon resurssien hallinta, seuranta ja raportointi. Tällä prosessilla voidaan ennaltaehkäistä siirtymistä vianhallintaprosessiin esimerkiksi kapasiteetin ylityksen aiheuttaman ongelman myötä.
Resurssien käytön hallinta	Asiakkaan käyttämien palveluiden ja resurssien hallinta. Tiedot ovat perustana asiakkaan laskutukselle.
Tietoturvan hallinta	Tietoverkon hallinta ulkoisia ja sisäisiä tietoturvauhkia vastaan. Esimerkiksi tietoverkon riskien analysointi.

2.2 Verkonvalvonnassa käytetyt yleisimmät menetelmät ja termit

2.2.1 ICMP – verkon kuljetuskerroksen hallintaprotokolla

ICMP eli Internet Control Message Protocol on IP-protokolla, jota käytetään verkkolaitteiden ja tarkemmin sanottuna myös käyttöjärjestelmien välillä liikenteen kontrollointiin. Protokolla sisältää useita sanomatyyppejä, joilla voidaan muun muassa tarkistaa onko yhteyden vastapäässä sijaitseva laite toiminnallinen IP-tasolla. ICMP sijoittuu OSI-mallissa kuljetustasolle (kerros 4) muun muassa TCP:n ja UDP:n kanssa. Tunnetuin ICMP-protokollaa hyödyntävä työkalu on Ping. Ping-työkalu lähettää ICMP echo -pyynnön (request) kohdelaitteelle, joka toimiessaan oletetulla tavalla lähettää ICMP echo -vastauksen (reply) takaisin. [7; 8; 9; 10.]

ICMP-protokollasta on kehitetty myös IPv6:ta tukeva versio. Se tunnetaan nimellä ICMPv6. Sen perustoiminnallisuus ei juurikaan eroa IPv4:n kanssa käytetystä alkuperäisestä ICMP-protokollasta. IPv6:n yhteydessä ICMPv6:ta käytetään naapurilaitteiden löytämiseen (neighbor discovery) sekä MTU:n (Maximum Transmission Unit) määrittämiseen. MTU:n arvo määrittelee paketille maksimikoon,

josta yhteyden kummassakin päässä sijaitsevien verkkolaitteiden on sovittava yhdessä. [6, s. 332–333.]

Verkonvalvonnassa Ping-työkalua käytetään tarkistamaan laitteen tavoitettavuus valvontapisteessä. Verkkolaitetta valvova järjestelmä lähettää ICMP echo -pyyntöjä laitteen verkko-osoitteeseen, yleisimmin hallintaosoitteeseen, tasaisin väliajoin, jolloin vastauksen tyypistä voidaan päätellä laitteen tila tai verkkolaitteiden välillä sijaitseva mahdollinen verkko- tai konfiguraatiovika. Lisäksi ICMP:n avulla voidaan määrittää vasteaika (Round Trip Time, RTT). RTT on kumulatiivinen aika, joka muodostuu, kun ICMP echo -pyyntö lähetetään valvottavalla laittelle, ja kun valvottavan laitteen ICMP echo -vastaus palautuu takaisin valvontapisteeseen.

2.2.2 SNMP – verkonvalvonta ja -hallinta sovellustasolla

SNMP eli Simple Network Management Protocol on verkon hallintaan ja valvontaan suunniteltu protokolla. SNMP sijoittuu OSI-mallin sovelluskerrokselle (Application layer, kerros 7), ja tarkemmin sanottuna se käyttää siirtoprotokollana UDP:ta, joka sijoittuu vastaavasti OSI-mallissa kuljetuskerrokselle (kerros 4). Useimmissa tapauksissa SNMP:tä hyödyntää verkonhallintajärjestelmä (NMS, Network Management System), joka voi olla palvelimelle asennettu graafinen sovellus. Tällaista sovellusta kutsutaan SNMP-manageriksi. SNMP-manageri keskustelee verkkolaitteiden kanssa, jotka ovat SNMP-agentteja. Useimmat verkkolaitteet tukevat SNMP:n eri versioita. Tällä hetkellä SNMP:n toinen versio (SNMPv2) on yleisin.

Koska SNMP on itsenäisesti sovelluskerroksella toimiva protokolla, sillä ei ole suoraa vaatimusta Internet protokollan versiolle. Täten SNMP on siis IPv6-yhteensopiva, ja varsinaiset yhteensopivuusongelmat liittyvätkin laitteiden valvottaviin IPv6-hallintaobjekteihin, jotka on selitetty tarkemmin seuraavassa luvussa. SNMP:n tyypillinen käyttötarkoitus on lukea (GET) verkkolaitteelta tietoja, mutta sillä voidaan myös tehdä (SET) muun muassa konfiguraatiomuutoksia suoraan verkonhallintajärjestelmästä. Laite voi myös itsenäisesti raportoida muuttunesta tilastaan verkonhallintajärjestelmälle. Tähän suuntaan tapahtuvaa SNMP-sanomaa kutsutaan nimellä Trap. Jokainen SNMP:tä tukeva verkkolaite sisältää hierarkkisen tietokannan tyypillisimmistä valvottavista tiedoista laitteella, kuten prosessorikuormasta, laitteen mallista ja versiosta. Tällaista tietokantaa kutsutaan

nimellä MIB (Management Information Base), ja se selitetään tarkemmin seuraavassa luvussa. [9; 11; 12.]

2.2.3 MIB – verkkolaitteen hallintaobjektit

MIB (Management Information Base) on hierarkkinen tietorakenne verkkolaitteella olemassa olevista hallintaobjekteista. Tätä tietorakenteen kokonaisuutta kutsutaan verkkolaitteella suoritettavaksi agentiksi, koska se on käytännössä erillinen ohjelmistokomponentti. Tietorakenteen, tai tietokannan, jokaista tietuetta, objektia, voidaan osoittaa yksilöllisellä tunnisteella, joka tunnetaan nimellä OID (Object Identifier). Tunniste osoittaa siis etsittävän objektin paikan hallintatietokannassa. Yksi tällainen objekti (MO, Managed Object) saattaa sisältää tiedon esimerkiksi verkkolaitteen prosessorin käyttöasteesta. Objektin sisältämä tieto kommunikoi suoraan laitteen prosessorin kanssa. Hallittavat objektit (MO:t) yhdessä muodostavat MIB:n, joka edustaa puolestaan edustaa koko fyysisen verkkolaitteen hallinta- ja valvontaominaisuuksia. [6, s. 308–312.]

MIB:n tietoja hyödynnetään useimmiten verkon hallinta- ja valvontasovelluksella (NMS, Network Management System), joka osaa lukea ja mahdollisesti myös muokata SNMP-protokollan avulla verkkolaitteen MIB:n tietoja. Tämä edellyttää sitä, että verkon hallinta- ja valvontasovellus on tietoinen verkkolaitteella käytettävästä MIB:n versiosta, jotta se osaa osoittaa OID:lla laitteen MIB:n oikeaa hallittavaa objektia. [6, s. 308–312.]

Aluksi IETF (Internet Engineering Task Force) julkaisi IPv6-yhteensopivan standardin (RFC 2465, 2452 ja 2454) MIB:stä IPv4:ää tukevan MIB:n rinnalle. Jälkeen päin muodostui kuitenkin tarve protokollariippumattomalle MIB-standardille, koska useat verkkototeutukset olivat jo vaiheittain siirtyneet osittain tukemaan IPv6:ta, mutta suurin osa liikenteestä kulki edelleenkin IPv4:n muodossa. Lopulta IETF julkaisi neljä protokollariippumatonta MIB-suunnitelmaa, jotka ovat lyhyesti esitetty taulukossa 2. [6, s. 308–312.]

Taulukko 2. IETF:n julkaisemat RFC:t protokollariippumattomista MIB:stä.

RFC:n numero	MIB:n kuvaus
RFC 4292	IP Forwarding Table MIB. Kuvailee IPv4:n ja IPv6:n MIB:n yleisellä tasolla.
RFC 4293	Internet protokollan (IP) MIB. Yhdistää IPv6-kohtaisia RFC:itä (RFC 2465, 2466 ja 2011) paremman IPv6-tuen saavuttamiseksi. On kuitenkin muiden MIB:ien tapaan Internet protokollan versiosta riippumaton.
RFC 4022	Kuljetustason kontrolliprotokollan (TCP) MIB.
RFC 4113	UDP:n (User Datagram Protocol) MIB.

Vaikka MIB:t ovat standardisoituja IETF:n toimesta, niin valmistajat ovat kuitenkin tehneet omia muunnelmia jo olemassaolevista MIB:stä. Verkkolaitteella voi siis olla useampi MIB, kuten esimerkiksi laitteen alkuperäiset Internet protokollaan liittyvät MIB:t, ja sen lisäksi valmistajakohtainen MIB, jolla voidaan esimerkiksi SNMP:llä kopioida Cisco IOS-reitittimen konfiguraatio talteen. [6, s. 308–312.]

2.2.4 Syslog – keskitetty lokitietojen varastointi

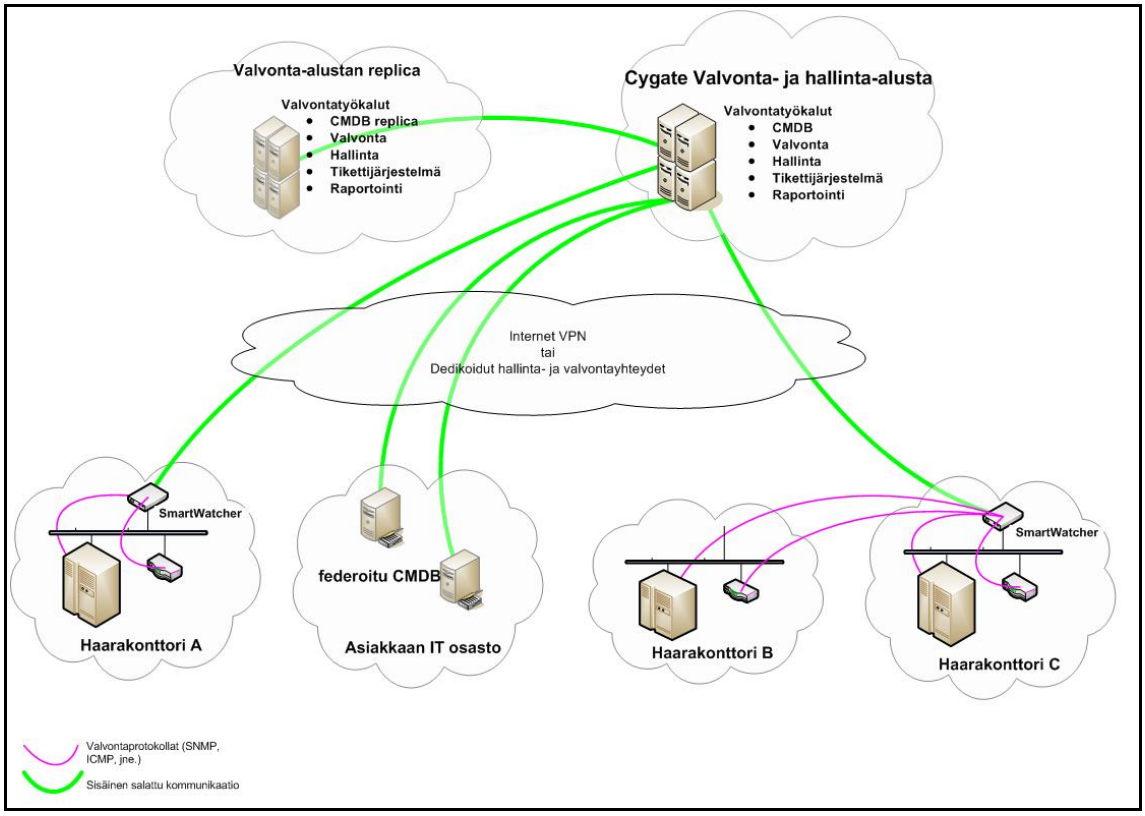
Syslog-protokollalla voidaan siirtää verkkolaitteen, jossa suoritetaan Syslog-taustaprosessia (daemon), lokitietoja keskitettyyn lokien varastointijärjestelmään. Varastointijärjestelmänä voi toimia normaali palvelin, jossa suoritetaan Syslog-palvelinsovellusta. Syslog-taustaprosessia suorittavat verkkolaitteet lähettävät itse ennalta konfiguroitujen sääntöjen perusteella lokitietoja Syslog-palvelimelle. Syslog-palvelin voi toimia keskitettynä lokitietojen varastointipisteenä usealle verkkolaitteelle. Näin laitteiden tapahtumia voidaan tallentaa muualle kuin verkkolaitteiden omaan muistiin, jolloin säästetään itse verkkolaitteiden resursseja ja varmistetaan, että lokitiedot ovat tallessa myös laiterikon sattuessa. Syslog käyttää kuljetuskerroksen siirtoprotokollana UDP:ta. Itse Syslog on SNMP:n tavoin sovelluskerroksen (kerros 7) sovellus. [13; 14.]

Esimerkiksi Cisco-merkkisissä IOS-käyttöjärjestelmällä varustetuissa reitittimissä Syslog-viestit näyttävät samoilta kuin konsoli- tai etäistunnon aikana käyttäjälle näytettävät lokiviestit. Myös komennolla ”show logging” nähdään koko istunnon aikana kertyneet lokit. Syslog-viestien lähetystä voidaan erikseen määritellä siten, että tietyn

kriittisyyden täyttävät tai ylittävät tapahtumat lähetetään Syslog-palvelimelle. Syslog on IPv6-tuettu Cisco IOS:llä versiosta 12.4(4)T lähtien. [6, s. 332.]

3 Cygaten tuottama verkonvalvontapalvelu

Kuvassa 1 on esitetty ylemmän tason verkkokuva yksittäisen monitoimipaikkaisen asiakkaan verkonvalvonnasta. Salattu verkonvalvontaliikenne siirretään dedikoitujen valvontayhteyksien tai vaihtoehtoisesti VPN-tunnelissa Internetin läpi valvonta- ja hallinta-alustalle. VPN:ää hyödynnettäessä ei erillisiä dedikoituja valvontayhteyksitä tarvita. Valvonta- ja hallinta-alustassa käsitellään verkonvalvontatietoa, luodaan raportteja, sekä etähallitaan laitteita. Verkonvalvontiedon käsittelyn yhtenä mahdollisena tuloksena on hälytys. [15, s. 1.]



Kuva 1. Ylemmän tason verkkokuva yksittäisen asiakkaan eri toimipisteiden verkonvalvonnasta.

CMDB (engl. Configuration Management Database) on tietokanta ja se sisältää tietoa asiakkaan valvottavista laitteista. Tietokanta voi sijaita valvonta- ja hallinta-alustalla, tai vaihtoehtoisesti laitetiedot voidaan lukea ennaltamääritetyin väliajoin (federoitu laitetietokanta) asiakkaan omasta tietojärjestelmästä. [16.]

3.1 SmartWatcher

SmartWatcher on asiakkaan verkossa sijaitseva Linux-pohjainen palvelin. Sen tehtävä on valvoa asiakkaan verkon laitteita, kuten reitittimiä, kytkimiä, palvelimia ja palomuureja. SmartWatcher suorittaa laitteiden valvontaa muun muassa seuraavassa taulukossa esitetyin menetelmin. [17.]

Taulukko 3. Yleisimmät valvonta- ja hallintamenetelmät SmartWatcherilla. [17.]

Menetelmä	Protokolla	Esimerkki
– Tavoitettavuus – Viive – Pakettihävikki	ICMP	Ping. SmartWatcher lähettää ICMP echo –pyyntöjä valvottavan laitteen IP-osoitteeseen.
– Vikailmoitukset – Konfiguraatioiden varmuuskopiointi – Statistiikka	SNMP	Trap. Valvottava laite raportoi itse muuttuneesta tilanteesta SmartWatcherille.
– Tapahtumien tallennus keskitetysti	Syslog	Lokien keräys laitteilta.

SmartWatcher on yhteydessä valvonta- ja hallinta-alustaan kuvassa 2 esitetyllä tavalla. [17.]

SmartWatcher voi olla myös virtuaalinen, kuten tässä työssä osoitetaan. SmartWatcherin toiminnallisuus on sijoitettu virtuaaliseen VMware-koneeseen, joka vastaavasti sijaitsee valvonta- ja hallinta-alustan blade-kehikossa. Blade-kehikolla tarkoitetaan tässä tapauksessa modulaarista palvelinympistöä. Kyseinen virtuaalikone sijaitsee eri verkossa kuin valvonta- ja hallinta-alustan muut toiminnallisuudet, joten se toimii tällaisenaankin kuvassa 2 esitetyllä tavalla, eli toisin sanoen se on eristetty loogisesti (VLAN:ien avulla, Virtual Local Area Network, virtuaalinen lähiverkko) muusta verkosta. Valvonta- ja hallinta-alustan reititystä selitetään tarkemmin jäljempänä. [17.]

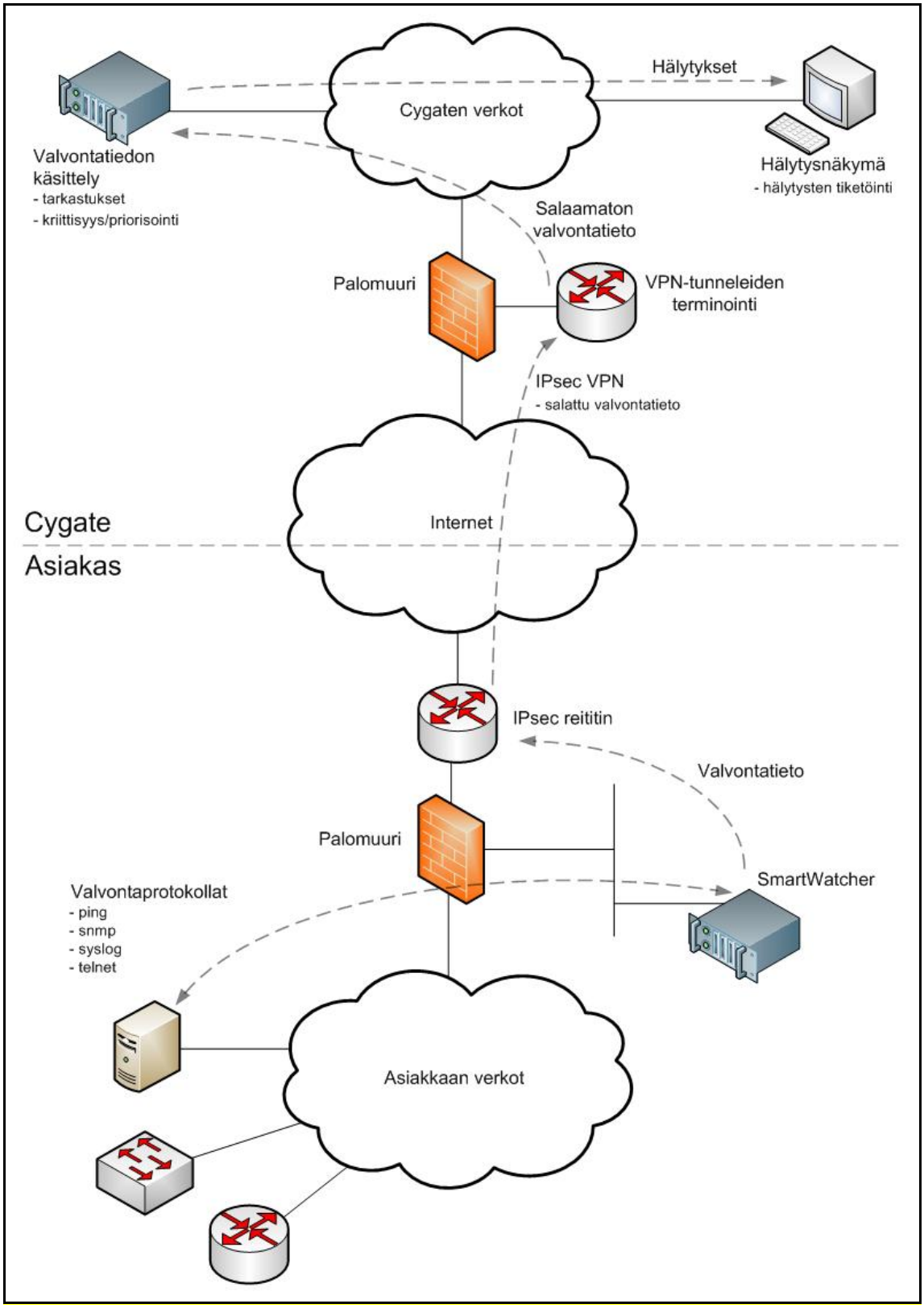
3.2 Verkonvalvontatiedon kulku

Kuvassa 2 on esitetty yksityiskohtaisemmin verkonvalvontatiedon kulku asiakkaan verkosta valvonta- ja hallinta-alustalle. SmartWatcher on sijoitettu asiakkaan sisäverkkoon siten, että se on omassa verkkosegmentissään, ja liikennöinti asiakasverkoissa sijaitsevien laitteiden ja SmartWatcherin välillä tapahtuu palomuurin

kautta. IPsec on IPv4:n tapauksessa valinnainen lajitelma protokollia, joilla tietoverkossa liikkuva data voidaan salata, todentaa sekä varmistaa sen eheys. Käytännössä nykyään kaikki Internetin yli liikennöitävä yritysten toimipisteiden välinen liikenne salataan IPsec:llä. IPsec on IPv6:n tapauksessa ottanut suurehkon kehitysaskeleen, koska RFC:n mukainen IPv6-toteutus vaatii IPsec:n käytön. IPsec ei kuitenkaan ole oletusarvoisesti käytössä IPv6:ssa, joten kuvitelma, että IPv6 on lähtökohtaisesti tietoturvaltaan parempi kuin IPv4, on väärä. RFC:t (Request for Comments) ovat IETF-organisaation (Internet Engineer Task Force) julkaisemia dokumenttejä verkkoarkkitehtuureihin liittyvistä standardeista. [6, s. 10; 18; 19.]

Verkonvalvontaan liittyvä liikenne reititetään IPsec-reitittimen kautta Cygaten verkkoon, jossa VPN-tunneli terminoidaan. Verkonvalvontatieto kulkee siis turvallisesti salattuna Internetissä. Liikenteen salaus asiakkaan sekä Cygaten paikallisverkoissa jätetään sovelluskerroksen protokollien vastuulle. Toisin sanoen muun muassa SNMPv3 ja SSH-yhteydet (Secure Shell, salatun tietoliikenteen protokolla) ovat tällaisessa tapauksessa salattua liikennettä. [15, s. 2.]

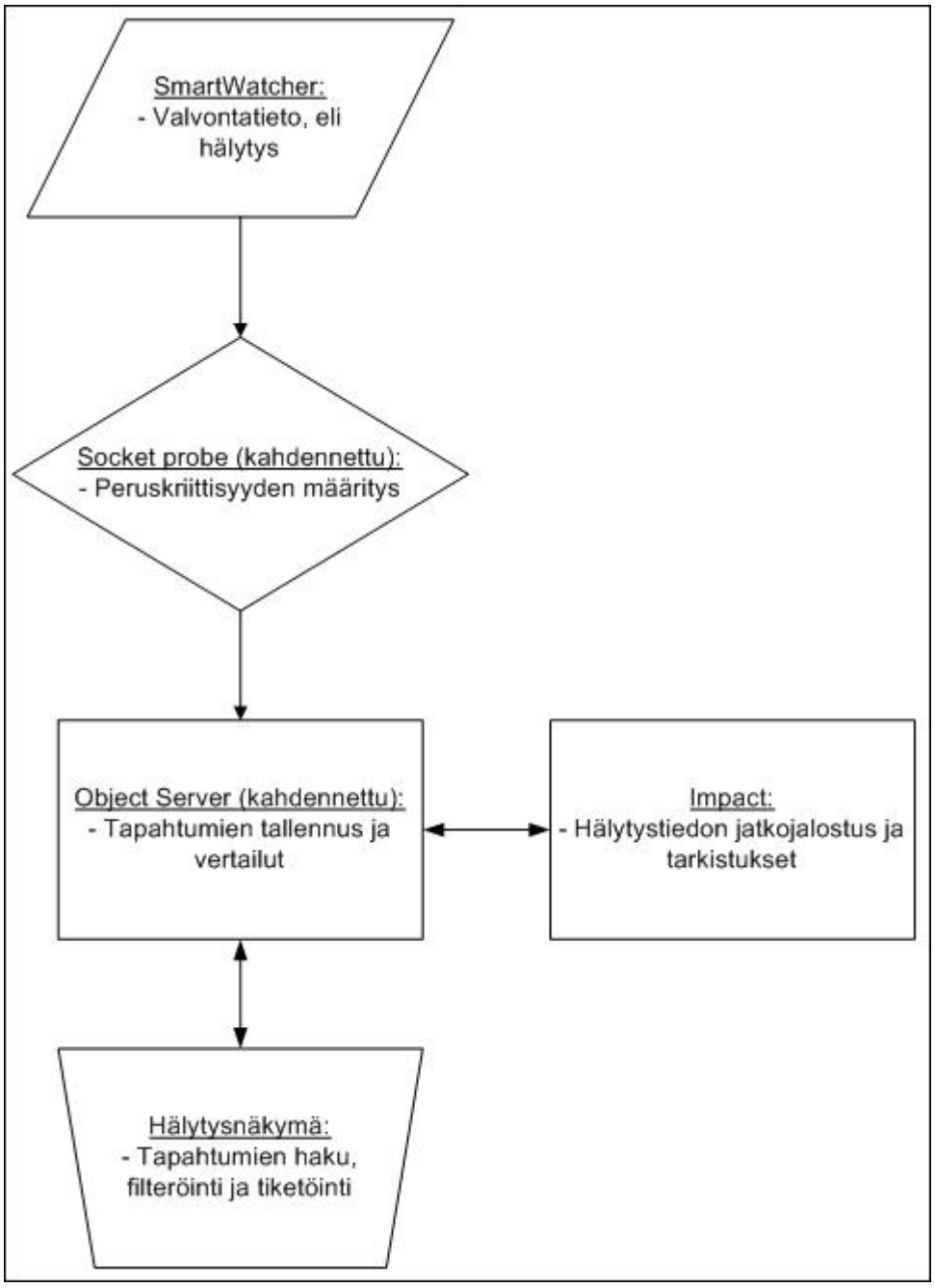
SmartWatcher valvoo asiakkaan verkkojen laitteita muun muassa ICMP- ja SNMP-protokollilla. Myös verkon laitteet lähettävät itse SNMP-trapeja jos niiden tila muuttuu ja hälytykselle asetettu raja-arvo ylittyy. Tällöin SmartWatcher lähettää verkonvalvontatiedon kohti valvonta- ja hallinta-alustaa, tieto salataan IPsec-reitittimellä, reititetään Internetin läpi ja palautetaan selkokieliseksi Cygaten VPN-tunnelien terminointipisteessä. Tästä tieto jatkaa matkaansa käsiteltäväksi valvonta- ja hallinta-alustalle. Lopuksi siitä generoidaan hälytys, joka toimitetaan hälytysnäkymään. [15, s. 2; 17.]



Kuva 2. Yksittäisen toimipisteen verkonvalvonnan toteutus ja verkonvalvontatiedon kulku.

3.3 Verkonvalvontatiedon käsittely

Kuva 3 havainnollistaa verkonvalvontapalvelussa läpikäytävät prosessit aina SmartWatcher:lta hälytysnäkymälle asti.



Kuva 3. Verkonvaltontatiedon käsittely valvonta- ja hallinta-alustassa [20].

SmartWatcherin lähettämä valvontatieto eli hälytys vastaanotetaan hallinta-alustalla virtuaalikoneilla (kahdennettu) nimeltä Socket probe 1 ja 2. Kummatkin koneista

suorittavat samaa toimintoa ja ovat identtiset, eli koneiden jatkuva saatavuus on varmistettu kahdennuksella. Socket probet pitävät sisällään socket-, trap- ja syslog-nimiset prosessit (kutsutaan nimellä probe), jotka määrittelevät muun muassa hälytyksen peruskriittisyyden. Valvontaa tehdään siis huomattavasti laajemmissa määrin, sillä vain murto-osa valvontadatasta päätyy SmartWatcherin generoimasta hälytyksestä valvontanäkymään. Hälytysdataa priorisoidaan ja suodatetaan ennen hälytyksen toimittamista valvontanäkymään. Socket-, trap- ja syslog-probet ovat toteutettu skriptikielellä. [20.]

Socket probet kommunikoivat Object serverin kanssa. Object Server on Socket probejen tapaan kahdennettu. Object server on tietokanta, johon tallennetaan hälytystapahtumia. Tietokannasta myös poistetaan hälytystapahtumia, mikäli kyseinen tapahtuma ei ole enää voimassa. Tällä tarkoitetaan muun muassa sitä, että valvottava verkkolaite käynnistyy uudelleen, jolloin se ei ole enää hetkellisesti saavutettavissa. Tästä tapahtumasta syntyy hälytys, joka tallennetaan Object serverille. Kun laite taas pian käynnistyttyään on saavutettavissa, uutta hälytystä verrataan Object serverin tietoihin, ja huomataan, että siellä on jo aktiivinen hälytys, joka voidaan nyt siis poistaa. Myös lukuisat muut järjestelmät, kuten raportointityökalut, käyttävät Object serverin tietoja hyväkseen. Lisäksi Object server kommunikoi Impact nimisen palvelimen kanssa, jonka tehtävä on rikastaa SmartWatcherin alun perin toimittamaa hälytystä. Impact siis muun muassa tarkistaa, onko laite tuotantolaite, löytyykö se laitetietokannasta (CMDB), millä asiakkaan toimipisteistä se sijaitsee, mitkä ovat laitekohtaiset tiedot, kuten laitteen malli ja käyttöjärjestelmän versio, sekä kuka on laitteelle määritetty asiakkaan yhteyshenkilö. Lopuksi hälytystieto toimitetaan valvontanäkymään, jossa käytetään vielä lisäksi käyttäjäkohtaisia suotimia näyttämään haluttuja hälytyksiä. [20.]

4 Siirtyminen IPv6:een

IETF:n (The Internet Engineering Task Force) ennusteiden mukaan julkiset IPv4-osoitteet on jaettu loppuun vuoteen 2011 mennessä. IPv4-osoiteavaruus pitää sisällään noin 4,3 miljardia osoitetta, kun taas IPv6 tarjoaa käytännössä rajoittamattoman määrän osoitteita. IPv4-osoiteavaruuden epäkäytännöllinen jaottelu luokkiin on myös

kasvattanut Internetin runkoreitittimien reititystaulujen kokoa huomattavasti. Reititystaulun pituus vaikuttaa alentavasti reitityspäätöksien nopeuteen. [6, s. 2; 21.]

IPv4-osoiteavaruuden rajoittuvuus ja ehtyminen ovat aiheuttaneet sen, että IP-protokollan päälle on jatkokehitetty uusia IPv4:n elinikää lisääviä tekniikoita, koska siirtyminen IPv6:een tulee tapahtumaan hitaasti ja vaiheittain. Tällaisia tekniikoita ovat muun muassa osoitteenmuunnos (NAT, Network Address Translation). NAT:lla on saavutettu julkisten IP-osoitteiden käytön parempi tehokkuus, mutta toisaalta se on myös monimutkaistanut ja hankaloittanut verkon infrastruktuuria sekä tehnyt jopa mahdottomaksi käyttöönottaa joitakin sovelluksia. NAT häiritsee IP-protokollalle ominaista kaksisuuntaista tiedonsiirtoa, eli toisin sanoen piilottaa tai muokkaa ainakin osittain kahden päätelaitteen (palvelin, tietokone, mobiililaite) välisen suoran liikennöinnin (engl. peer-to-peer). Tästä johtuen palomuurit ja reitittimet sisältävät monimutkaisiakin ratkaisuja hoitamaan osoitteenmuunnokset, jotka vaativat myös ylimääräistä prosessoritehoa. IPv6-osoitteiden määrä mahdollistaa suoran kaksisuuntaisen liikennöinnin ilman osoitteenmuunnoksia. Tämä yksinkertaistaa verkon rakennetta sekä mahdollistaa myös sellaisten ohjelmistojen käytön, joita ei aiemmin olla tehokkaasti, tai ollenkaan, saatu käyttöön osoitteenmuunnosten kanssa. [6, s. 2.]

Ennen IPv6:een siirtymistä on suotavaa käyttää runsaasti aikaa siirtymisessä huomioitaviin seikkoihin ja kartoittaa ja dokumentoida verkosta mahdolliset siirtymistä vaikeuttavat tai kokonaan estävät tekijät. Aluksi on syytä asettaa tavoite, eli mitkä palvelut ja laitteet viedään IPv6-toiminnallisuuden piiriin ensimmäisessä vaiheessa. Jokainen verkkolaite ja verkkoa käyttävä sovellus on tutkittava perinpohjaisesti, jotta saadaan selville, onko kyseinen laite tai sovellus mahdollista ottaa mukaan ensimmäiseen vaiheeseen. Lisäksi on kartoitettava riskit ja mahdollinen palautussuunnitelma, jos jonkin laitteen tai sovelluksen kanssa tulee ongelmia. Tavoitteen asettaminen vaatii laitteiden ja sovellusten kartoituksen. Kartoitus on syytä tehdä kerralla kattavasti, jotta mikään tärkeä osa ei jää epähuomiossa ulkopuolelle. [22, s. 17–18.]

Useimmat verkkolaitteet ja käyttöjärjestelmät tukevat jo hyvin IPv6:ta, mutta joidenkin ohjelmistojen kehitys on voinut päättyä, jolloin ne on korvattava uusilla IPv6:ta tukevilla ohjelmistoilla, tai vaihtoehtoisesti ne on jätettävä käyttämään IPv4-verkkoa,

kunnes vaihtoehtoinen ratkaisu löytyy. Useat verkon laitteet tulevat pitkäänkin tukemaan sekä IPv4:ää että IPv6:ta, joten laitteen resurssit on otettava huomioon. Kahden eri protokollaversion tukeminen vaatii usein laitteelta enemmän muistia sekä prosessoritehoa, joten siirtymän aikana on valmistauduttava hankkimaan kokonaan uusia verkkolaitteita tai päivitettävä jo olemassa olevia, jos se on mahdollista. [22, s. 18–19.]

Tavoitteen asettamisen ja laite- sekä ohjelmistokartoituksen jälkeen voidaan siirtyä IPv6-osoitteistuksen suunnitteluun. Tämän jälkeen seuraava askel on siirtymän toteutus sekä totetutuksen jälkeinen testaus ja seuranta, jolla määritellään, missä määrin tavoite on saavutettu. Toteutus pitää sisällään laitteisiin ja ohjelmistoihin tarvittavien muutosten toteutuksen, kuten reitittimien ohjelmistopäivitykset, muistin lisäyksen ja IPv6-konfiguraatiot. [22, s. 25–30.]

IPv6:n vaatimukset tämän työn osalta rajoittuvat ainoastaan verkkolaitteiden käyttöjärjestelmiin ja niissä ajettavien ominaisuuksien versioihin. Esimeriksi Ciscon IOS:a käyttävät verkkolaitteet ovat IPv6-tuettuja käyttöjärjestelmän versiosta 12.x(T) lähtien. On kuitenkin syytä muistaa, että vaikka IPv6 olisikin laitteen valmistajan mukaan tuettu, niin se ei silti välttämättä tue sen kaikkia ominaisuuksia. Kaikki tämän työn verkkolaitteet käytiin läpi, ja ne tukevat kaikkia tässä työssä vaadittuja toiminnallisuuksia myös IPv6:n kanssa. Muun muassa virtuaalisessa asiakasverkossa, joka esitellään myöhemmin, on käytössä Ciscon IOS-versio 15.1(4)M. Työn tarkoitus on kartoittaa myös valvonta- ja hallinta-alustaan tarvittavat mahdolliset päivitykset ja muutokset, jotta IPv6-tuki täyttyy. Työn aikana on myös varmistettu ja tutkittu yleisimpien verkon valvontaan ja hallitaan käytettyjen protokollien (ICMP, Syslog, SNMP) IPv6-tukea.

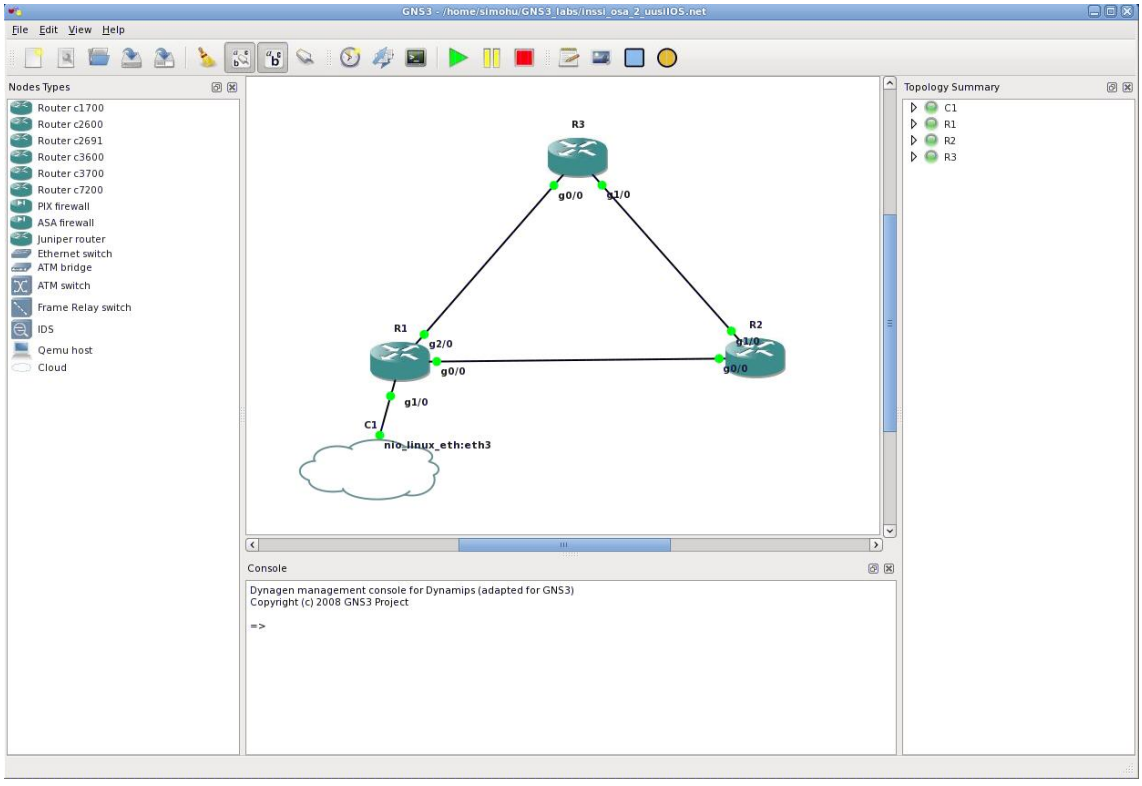
5 Testiympäristön suunnittelu ja toteutus

5.1 Testiympäristön suunnittelu

Tyypillistä asiakasympäristöä vastaava verkko toteutetaan GNS3-virtuaaliympäristössä. Tätä työkalua käsitellään tarkemmin luvussa 5.1.1. Verkonvalvontapalvelun fyysinen hallinta-alusta (blade-kehikko) sijoitetaan laboratorioverkkoon, johon myös GNS3-virtuaaliympäristö liitetään osaksi fyysistä verkkoa.

5.1.1 GNS3-virtuaaliympäristö

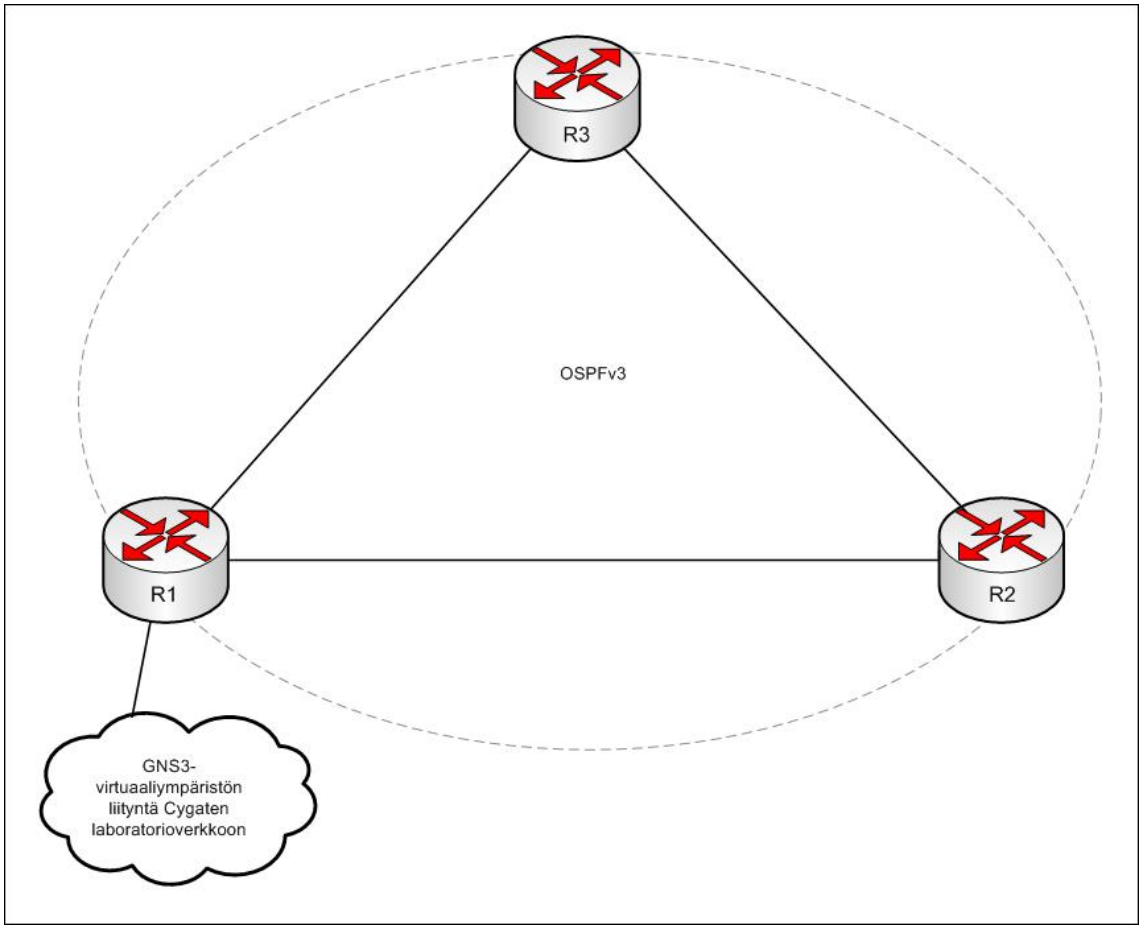
GNS3 (Graphical Network Simulator version 3) on graafinen verkkosimulaattori, jolla voidaan graafisesti emuloida monimutkaisiakin verkkoja. Työkalulla voidaan ajaa muun muassa seuraavien fyysisten laitteiden käyttöjärjestelmiä täysin virtuaalisesti: Cisco IOS, Cisco PIX, Cisco ASA ja JunOS. Graafinen verkkosimulaattori mahdollistaa laitteiden välisten linkkien luomisen, joten sillä saa rakennettua vaativimpiakin verkkotopologioita, jotka voidaan sitten testauksen jälkeen siirtää turvallisemmin suoraan tuotantoympäristöön. GNS3 emuloi edellä mainittujen valmistajien verkkolaitteita ja suorittaa niissä virallisia fyysisille laitteille tarkoitettuja käyttöjärjestelmiä, joten verkot käyttäytyvät virtuaalisina samoin kuten vastaavat fyysisillä laitteilla rakennetut verkot. GNS3:een on myös sisäänrakennettu laajalti käytössä oleva pakettianalysaattori, Wireshark. Tällä työkalulla voidaan tutkia verkkoliikennettä pakettikohtaisesi yksityiskohtaisella tasolla, jolloin saadaan todennettua helposti ja nopeasti verkon tapahtumia. [23; 24.]



Kuva 4. GNS3-verkkosimulaattorin käyttöliittymä.

Cygaten konesaliin on asennettu Linux-pohjainen (Fedora 13) palvelin, jossa GNS3-virtuaaliympäristöä ajetaan. Kuvassa 4 on kuvakaappaus GNS3:n käyttöliittymästä. Palvelimelle otetaan yhteys NoMachine NX -etäkäyttöohjelmistolla. GNS3 tukee useita yhtäaikaisia käyttäjiä. Jokainen GNS3:lla emuloitu verkkolaite vaatii itselleen tietyn määrän resursseja, joka riippuu emoloidun laitteen ominaisuuksista, siihen lisättävistä moduuleista, käyttöjärjestelmästä ja laitteen konfiguraatiosta. Monimutkaisemmissa verkkotopologioissa palvelimelta vaaditaankin jo huomattavia resurssivaroja. Palvelimelta löytyy fyysisiä verkkoliitäntöjä, joista yksi on varattu tälle työlle ja kytketty laboratorioverkkoon. Fyysisiä verkkoliityntöjä voidaan hyödyntää GNS3:ssa, jolloin virtuaaliympäristön saa kytkettyä tässä tapauksessa osaksi fyysistä laboratorioverkkoa. Edellä mainittu kytkentä selitetään yksityiskohtaisemmin kohdassa 5.1.3. [23.]

5.1.2 Asiakkaan verkon mallinnus virtuaaliympäristössä



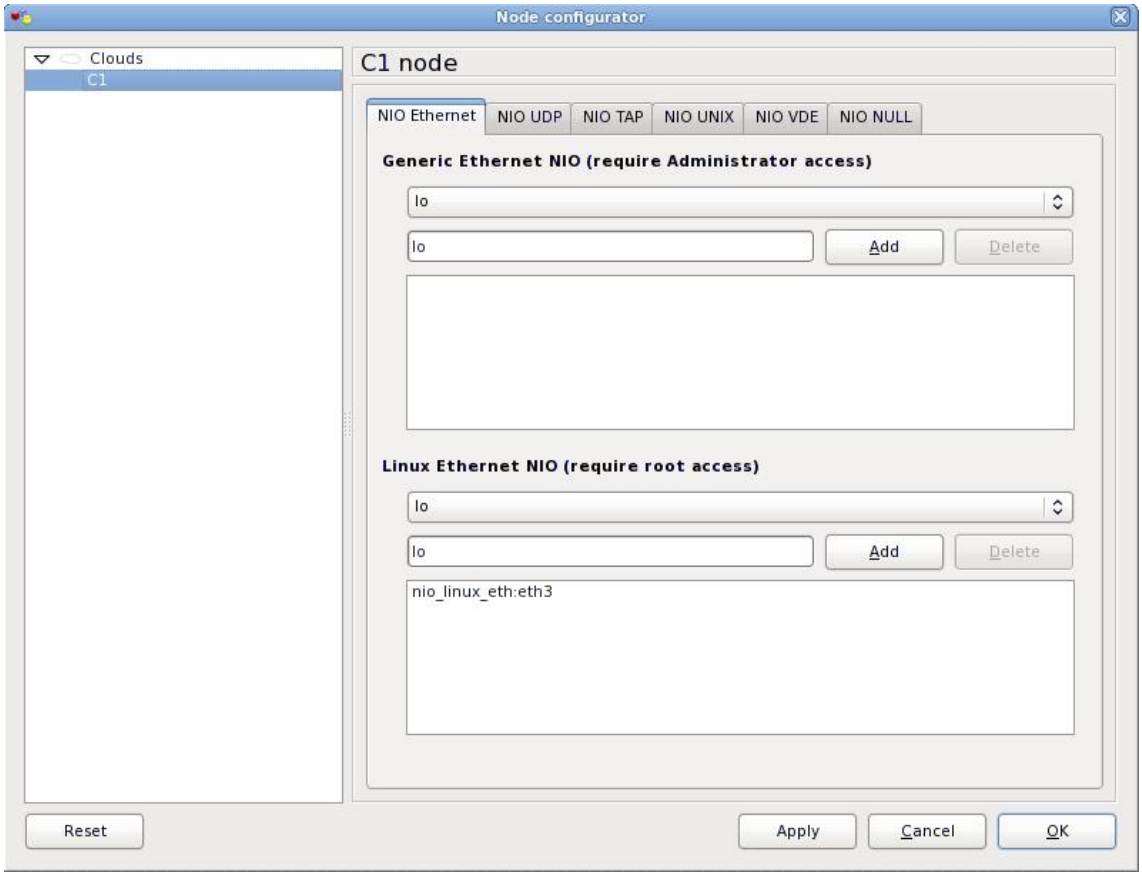
Kuva 5. Suunnitteluvaiheen verkkotopologia GNS3-virtuaaliympäristössä.

Asiakkaan verkko koostuu kolmesta Cisco 7200-sarjalaisesta reitittimestä kuvan 5 osoittamalla tavalla. Cisco 7200 on modulaarinen verkon palveluita keskittävä reititin. Sen avulla voidaan integroida verkon eri palveluita, kuten VoIP ja VPN, yhdelle laitteelle. Tämän työn kaikki kolme reititintä osallistuvat OSPFv3 reitityksprotokollan reititysprosessiin, jotta työssä voidaan todentaa myös reitityksprotokollan käyttäytymistä verkonvalvonnan näkökulmasta. Myöhemmässä vaiheessa pohditaan, konfiguroidaanko reitittimille vielä erilliset loogiset liitännät (Loopback Interface).

Reitittimeen R1 on lisätty kolme Gigabit Ethernet (nopeus 1 Gbps) moduulia, jotta liitäntöjä olisi tarpeeksi. Reitittimillä R2 ja R2 näitä samoja moduuleita on kaksi kappaletta kummassakin.

5.1.3 Virtuaaliympäristön liittäminen laboratorioverkkoon

GNS3-virtuaaliympäristön palvelimen yksi verkkoliitännöistä (Linux Ethernet, liitäntä 3) liitetään fyysiseen laboratorioverkkoon.



Kuva 6. GNS3:n virtuaaliympäristön liittäminen laboratorioverkkoon.

GNS3:ssa on erityinen objekti tätä tarkoitusta varten (C1 node kuvassa 6) ja sitä kuvataan pilven symbolilla. Kuvassa 6 on esitetty kuvakaappaus objektin konfiguraatiosta. Sille ei siis konfiguroida omaa IP-osoitetta GNS3:n kautta, vaan ainoa parametri on palvelimen fyysisen verkkokortin yksilöivä nimi. Objekti voidaan konfiguroida siten, että se muodostaa liitännän sovellustasolla suoraan palvelimen verkkokortin kanssa. Seuraavassa on esitetty GNS3-virtuaaliympäristön liitännän eth3 konfiguraatio.

```
eth3 Link encap:Ethernet  HWaddr 00:1E:68:86:53:BB
inet6 addr: 2001:67c:110:3003:21e:68ff:fe86:53bb/64
Scope:Global
inet6 addr: fe80::21e:68ff:fe86:53bb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:151729 errors:0 dropped:0 overruns:0 frame:0
TX packets:16298 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:12338241 (11.7 MiB)  TX bytes:1882732 (1.7 MiB)
Interrupt:30 Base address:0xa000
```

Liitännän konfiguraatiosta nähdään, että julkisesti reitittyvä (Scope: Global) osoite on muodostettu automaattisesti yhdistämällä se linkin paikalliseen osoitteeseen (Scope: Link), mutta osoite ei ole tässä tapauksessa merkittävä, koska liitäntä eth3 ainoastaan laajentaa fyysistä yhteyttä virtuaalilaboratorion sisään. [2, s. 34.]

Swi1-kytkimen liitäntä Fast Ethernet 3/18 kuuluu VLAN:iin 500. Swi1:llä on määritelty VLAN-liitännälle 500 IPv6-osoite 2001:67c:110:3003::1/64. Alla näkyy GNS3-virtuaaliympäristön reitittimen R1 liitännän Gigabit Ethernet 1/0 ja siihen liittyvä osittainen Swi1-kytkimen konfiguraatio.

```
Swi1#show ipv6 interface vlan 500
Vlan500 is up, line protocol is up
  IPv6     is     enabled,     link-local     address     is
FE80::209:E8FF:FE99:45BF
  Description: GNS3-virtual-lab
  Global unicast address(es):
    2001:67C:110:3003::1, subnet is 2001:67C:110:3003::/64


Swi1#show configuration
interface FastEthernet3/18
 description Link to GNS3 virtual lab
 switchport access vlan 500
 switchport mode access
```

```
R1#show configuration
interface GigabitEthernet1/0
 no ip address
 negotiation auto
 ipv6 address 2001:67C:110:3003::2/64
```

Konfiguraatiossa on määritelty VLAN-liitännälle 500 IPv6-osoite 2001:67C:110:3003::1, joka on siis peräisin verkosta 2001:67C:110:3003::0/64. Samasta verkosta on otettu osoite myös reitittimen R1 liitännälle Gigabit Ethernet 1/0. Kytkimellä Swi1 liitäntä Fast Ethernet 3/18 kuuluu ainoastaan VLAN:iin 500. VLAN 500 ei ole käytössä missään muualla laboratorioverkossa, joten tähän työhön liittyvä liikenne pysyy eristettynä muusta verkon liikenteestä.

```
R1#ping ipv6 2001:67c:110:3003::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:67C:110:3003::1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/4/8 ms
```

Ping-tulosteesta nähdään, että GNS3-virtuaaliympäristön ja laboratorioverkon välinen yhteys toimii IP-tasolla. Vaikka kytkentä ja arkkitehtuuri on yksinkertainen, testi osoittaa sen, että virtuaaliympäristön, sekä laboratorioverkon laitteet tukevat IPv6:ta silloinkin, kun IPv4-osoitteita ei ole laitteille konfiguroitu ollenkaan. Ympäristö on siis natiivisti IPv6:ta tukeva. Tällä pyritään käytännössä osoittamaan se, että nykyisin ei välttämättä ole enää tarve siirtyä vaiheittain kohti IPv6:tta, vaikkakin se on suotavaa monimutkaisemmissa verkoissa, joissa suoritetaan monimutkaisempia ohjelmistoja. Vaiheittaisella siirtymisellä tarkoitetaan tässä tapauksessa IPv4:n ja IPv6:n samanaikaista olemassaoloa verkkolaitteella. Tätä kutsutaan nimellä dual-stack. [25.]

5.2 Testiympäristön osoitteistuksen suunnittelu

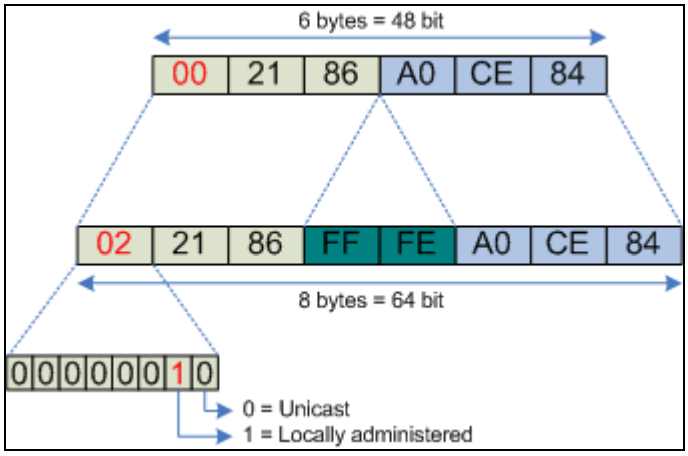
5.2.1 IPv6-osoitteet

IPv6-osoiteavaruus on 128-bittinen, joten se tarjoaa tarpeisiin nähden lähes loputtoman määrän yksilöllisiä verkko-osoitteita. IPv6-osoitteet voidaan jakaa kolmeen pääkategoriaan, jotka ovat unicast-osoitteet, multicast-osoitteet ja anycast-osoitteet. Tässä työssä keskitytään oikeastaan ainoastaan unicast-osoitteisiin, jolla tarkoitetaan siis osoitetta, joka yksilöi yhden ainoan fyysisen verkkoliitännän jollakin tietyllä verkkolaitteella. Kommunikointi tapahtuu siis kahden pisteen välillä. Tällaista kutsutaan

termillä point-to-point-yhteys. Kaksi edellä mainittua osoitetyyppiä, unicast ja multicast, ovat käytössä myös IPv4:n yhteydessä. Globaalilla tasolla reititettävät unicast-osoitteet koostuvat 48-bittisestä Global Prefix -osuudesta, 16-bittisestä aliverkon tunnisteesta, sekä 64-bittisestä verkkokortin tunnisteesta. Osoitteet jaetaan hierarkkisesti, jotta saavutetaan tehokkaampi osoitteiden ja verkkojen aggregointi Internetin runkoreitittimillä. Global Prefix -verkot jaetaan IANA:n (Internet Assigned Numbers Authority) toimesta eteenpäin eri maanosien rekistereille. Euroopan rekisteri (RIR, Regional Internet Registries) on nimeltään RIPE, joka jakaa Global Prefix -verkkoja Internet-palveluja tarjoaville yrityksille (ISP, Internet Service Provider), jotka vastaavasti jakavat näitä Global Prefix -verkkoja yrityksille. [2, s. 26–27, s.34–35; 26.]

Kuten IPv4:n yhteydessä, myös IPv6-osoite koostuu kahdesta osasta: verkon osoitteesta (Global Prefix ja Subnet ID) ja verkkokortin tunnisteesta. Aiemmin IPv4:n yhteydessä edellä mainitusta verkkokortin tunnisteesta puhuttiin nimellä host-osoite, mutta nykyään nimityksestä on luovuttu, koska tietokoneet voivat sisältää useita verkkokortteja ja kuulua useisiin verkkoihin. Tästä syystä nimitys host-osoite ei ole enää oikea tai tarpeeksi kattava, joten IPv6:n yhteydessä puhutaan jatkossa verkkokortin yksilöivästä tunnisteesta. Tällainen verkkokortin yksilöivä IPv6-osoite voidaan generoida usealla tapaa. Näitä tapoja ovat esimerkiksi DHCPv6 ja EUI-64, joista jälkimmäinen on esitetty seuraavassa kappaleessa yksityiskohtaisemmin. Osoite voidaan myös konfiguroida verkkokortille manuaalisesti. [2, s. 28.]

Verkkokortin tunniste voidaan muodostaa yhdistämällä verkon osoite ja EUI-64-muotoinen osoite. EUI-64 on IEEE:n (Institute of Electrical and Electronics Engineers) määrittelemä. Osoite saadaan generoitua verkkokortin 48-bittisestä MAC-osoitteesta. Se muodostetaan kuvan 7 osoittamalla tavalla.



Kuva 7. EUI-64-osoitteen muodostus MAC-osoitteesta [27].

Kuvassa 7 on 48-bittinen MAC-osoite. MAC-osoitteesta otetaan ensiksi 24 ensimmäistä bittiä, jonka jälkeen sijoitetaan arvo FFFE heksadesimaalisena, tai bittijonona kirjoitettuna 1111111111111110. Tämän perään sijoitetaan alkuperäisen MAC-osoitteen 24 viimeistä bittiä. Lopuksi saadaan 64-bittinen osoite, josta vasemmalta katsottuna asetetaan seitsemäs bitti arvolle 1, koska osoite on paikallisesti generoitu EUI-64-osoite. Tämä 64-bittinen osoite sijoitetaan lopuksi 64-bittisen verkko-osoitteen perään, jolloin saadaan yksittäisen verkkokortin yksilöivä 128-bittinen osoite. Koska EUI-64-muotoisesta osoitteesta saadaan koottua täysin validi globaalisti reitittyvä osoite, ja kun kokonainen IPv6-osoite on 128 bittiä pitkä, tästä voidaan päätellä, että EUI-64:ää voidaan käyttää ainoastaan vain verkko-osan ollessa 64-bittinen tai lyhyempi. [2, s. 45–46; 27.]

IPv6 unicast-osoite voi olla merkittävä kolmella eri tasolla. Link-local-osoite on linkin paikallinen osoite, eikä sillä ole merkitystä linkin ulkopuolella. IETF:n RFC:n 4291 mukaan jokaisella liitännällä on oltava vähintään yksi link-local-unicast-osoite. Tällainen osoite ei ole reitittyvä, vaan sitä käytetään yksittäisessä linkissä automaattiseen osoitteistukseen ja naapurilaitteiden löytämiseen. Jotkin reititysprotokollat käyttävät hyväkseen linkin paikallisia osoitteita. Link-local-osoitteet generoidaan dynaamisesti käyttämällä arvoa FE80::/10 ja yhdistämällä siihen esimerkiksi EUI-64:llä generoidun verkkokortin 64-bittinen tunniste. Unique-local-osoite (ULA, Unique Local Address) on paikallisesti merkittävä. Se tarkoittaa pitkälti samaa kuin privaatti LAN-osoite IPv4:n yhteydessä, joten tällaista osoitetta ei reititetä Internetiin sellaisenaan. Unique-local-osoite alkaa arvolla FC00::/7. Sitä täydennetään 40-bittisellä Global ID:llä, joka valitaan

satunnaisesti, eikä se saa olla jatkuva. Global ID:n valinnan algoritmi on selitetty tarkemmin RFC:ssä 4193. Kolmas unicast-osoitteen tyyppi on merkittävä globaalilla tasolla. Tällainen osoite reititetään oletuksena Internetiin. [2, s. 29, 33; 22, s. 9; 53; 54.]

5.2.2 Osoitteistuksen ja aliverkkojen toteutus

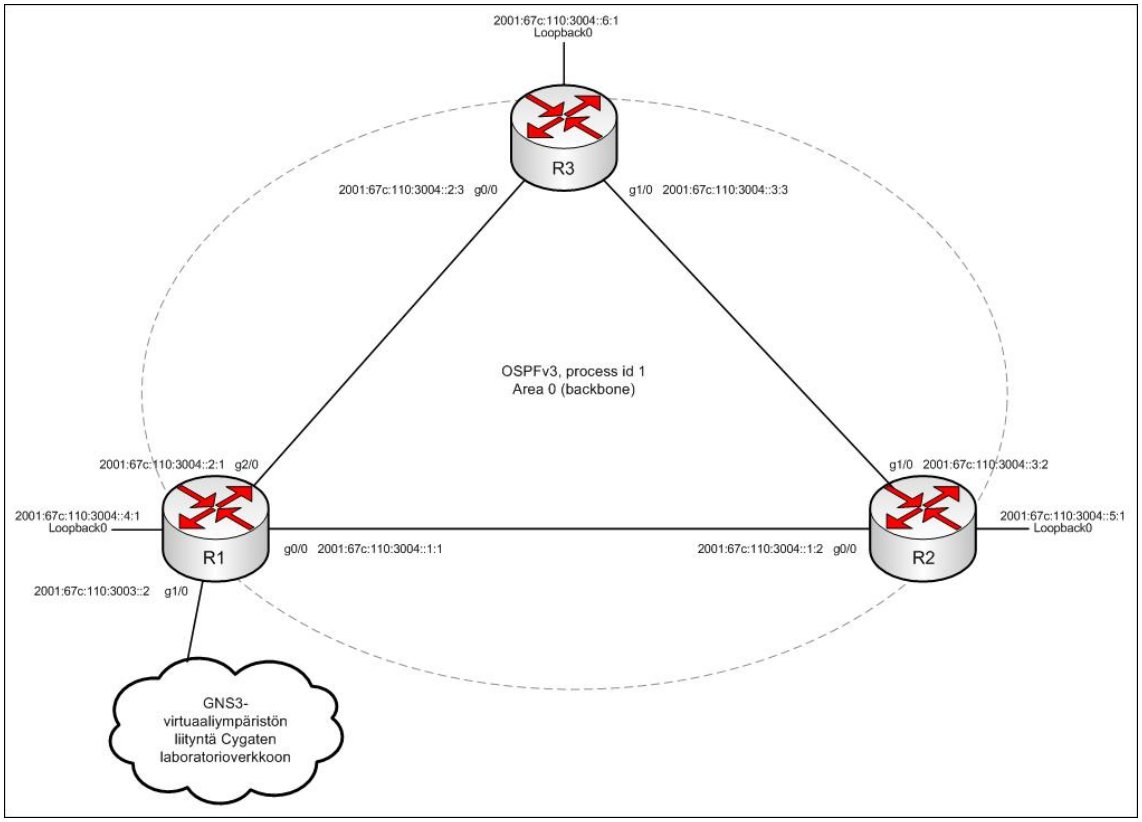
Testiympäristölle on varattu IPv6-osoiteavaruudet 2001:67c:110:3003::/64 ja 2001:67c:110:3004::/64, jotka ovat allokoitu verkosta 2001:67c:110:3000::/56. Nämä kaksi /54-verkosta allokoitua /64-verkkoa ovat siis globaalilla tasolla merkittäviä verkkoja, joten ne ovat Internetin ylitse reitittyviä. Verkko 2001:67c:110:3003::/64 tarjoaa siis noin 2^64 IPv6-osoitetta, mutta tässä työssä siitä käytetään ainoastaan kaksi osoitetta GNS3-virtuaaliympäristön ja fyysisen laboratorioympäristön välisen linkin osoitteistukseen. Huomattavaa on se, että IPv4 osoitteita on olemassa yhteensä ainoastaan 2^32 kappaletta, kun pelkästään tälle työlle allokoitu verkko 2001:67c:110:3003::/64 tarjoaa monin verroin enemmän. Verkkoa 2001:67c:110:3004::/64 käytetään kuvitteellisen asiakkaan toimipisteen verkkojen osoitteistukseen ja sitä tullaan aliverkottamaan, jotta asiakasverkosta saadaan tarpeeksi monipuolinen. Tällöin voidaan testata muun muassa myös reititysprotokollien toimintaa verkonvalvonnan näkökulmasta.

Taulukko 4. Työssä käytettävät verkot, aliverkot sekä host-osoitteet

IPv6-verkko tai -osoite	Selite
2001:67c:110:3003::/64	GNS3-virtuaaliympäristön ja fyysisen laboratorioverkon välisen linkin verkko.
2001:67c:110:3003::2	GNS3-virtuaaliympäristön palvelimen fyysisen portin osoite.
2001:67c:110:3003::1	Laboratorioverkon Swi1 kytkimen portin Fast Ethernet 3/18 osoite.
2001:67c:110:3004::/64	Asiakkaan toimipisteen osoiteavaruus. Jaettu aliverkkoihin, joissa käytetty maskina /112. Katso liite 1.
2001:67c:110:3001::3	SmartWatcher

Taulukossa 4 on esitetty kaikki työssä käytetyt ja aliverkotetut IPv6-verkot ja -osoitteet. IPv6-verkko 2001:67c:110:3004::/64 on jaettu maskin /112 aliverkkoihin. Tarkempi jaottelu löytyy liitteen 1 taulukosta. Edellä mainittu maskin /64 verkko on siis jaettu tasaisesti maskin /112 aliverkkoihin siitä syystä, että tässä työssä ei käytännössä tarvita paljon eri määrän host-osoitteita sisältäviä verkkoja, vaan kaikki maskin /112 verkot käytetään reitittimien välisien linkkien ja mahdollisesi myös loopback-liitäntöjen osoitteistukseen. Maskin /112 verkosta tarvitaan siis kahden reitittimen välisen linkin osoitteistuksen tapauksessa ainoastaan kaksi osoitetta. Toinen tälle työlle annettu IPv6-verkko, 2001:67c:110:3004::/64, ei ole siis jaettu aliverkkoihin parhaalla mahdollisella ja tehokkaalla tavalla, mutta tässä työssä on päätetty laittaa selkeys etusijalle. Todellisen asiakasympäristön tapauksessa maskin /64 IPv6-verkko olisi jaettu useisiin erikokoisiin aliverkkoihin (engl. VSLM, Variable Length Subnet Masking). Tällöin verkkojen koot olisivat määräytyneet tarvittavien host-osoitteiden ja aliverkkojen määrän mukaan. [28; 29.]

Liitteessä 1 esitetyllä verkon 2001:67c:110:3004::/64 jaottelulla saavutetaan maskilla /112 yhteensä 2^(112-64) aliverkkoa. Näistä jokainen aliverkko antaa käyttöön yhteensä 2^16 host-osoitetta eli noin 65500. Esimerkiksi verkosta 2001:67c:110:3004::/64 maskilla /112 saatu aliverkko 2001:67c:110:3004:0:0:5:0/112 sallii host-osoitteet välillä 2001:67c:110:3004:0:0:5:0/112 ja 2001:67c:110:3004:0:0:5:ffff/112. Tällaiset aliverkot riittävät siis mainiosti tämän työn osoitetarpeisiin ja pitävät samalla verkkotopologian selkeänä ainakin reitityksen, reittien mahdollisen aggregoinnin ja vianetsinnän osalta. Kuva 8 on alustava suunnitelma GNS3-virtuaaliympäristön osoitteistuksesta. Verkon reititys käydään läpi jäljempänä. [28; 29.]



Kuva 8. Alustava suunnitelma virtuaaliympäristön osoitteistuksen toteutuksesta.

5.3 GNS3-virtuaaliympäristön reitittimien IPv6-peruskonfiguraatiot

Cisco IOS ei ole oletusarvoisesti asetettu käsittelemään IPv6-paketteja. Tästä syystä seuraavat konfiguraatiot syötetään GNS3-virtuaaliympäristön reitittimiin R1, R2 ja R3.

```
R1(config)#ipv6 unicast-routing
```

Komento käynnistää IPv6-unicast-pakettien reitityksen reitittimien liitäntöjen välillä. Tämän komennon lisäksi reitittimien liitäntöihin konfiguroidaan globaalisti reititettävät IPv6-osoitteet liitteen 1 mukaisesti. Seuraavilla komennoilla asetetaan reitittimen liitäntä käyttämään IPv6-osoitetta. [30.]

```
R1(config-if)#ipv6 address 2001:67c:110:3004::2:3/112
R1(config-if)#ipv6 enable
```

Ylempi komento asettaa reitittimen R1 liitäntään globaalisti reititettävän IPv6-osoitteen. Alempi komento ei ole pakollinen, eikä sillä ole tässä tapauksessa vaikutusta. Jos globaalisti reititettävää osoitetta ei syötettäisi, alempi komento käynnistäisi

liitäntäkohtaisen IPv6-tuen, ja konfiguroisi automaattisesti link-local-IPv6-osoitteen liitännälle. Tällaista osoitetta ei reititetä globaalisti, vaan sitä käytetään ainoastaan linkin paikalliseen kommunikointiin. [30.]

5.4 Reitityksen suunnittelu

Reititys virtuaaliympäristössä (asiakkaan verkossa) toteutetaan OSPFv3-reititysprotokollaa käyttäen. Näin taataan yhteensopivuus nyt ja jatkossa muidenkin kuin Cisco-merkkisten laitteiden kanssa. EIGRP on myös yhteensopiva IPv6:n kanssa, mutta se on Ciscon omistama kaupallinen reititysprotokolla, minkä vuoksi tuki rajoittuu lähinnä ainoastaan Ciscon valmistamiin verkkolaitteisiin. Syy, miksi reititysprotokollana ei käytetä muun muassa IS-IS:ää, on se, että kyseinen protokolla on käytössä laajemmin operaattoreilla eikä niinkään asiakkaiden paikallisissa verkoissa ja toimipisteiden välisissä reitityksissä. Käytössä on lähes poikkeuksetta OSPF sisäverkkojen reitityksessä, ja Internetin yli reititetään BGP:n avulla. Asiakasverkon OSPFv3-reitityksen toteutuksesta kerrotaan yksityiskohtaisemmin kappaleessa 5.4.2. [31.]

Valvonta- ja hallinta-alusta on blade-kehikko, jossa suoritetaan useita virtuaalikoneita. Virtuaalikoneet sijaitsevat loogisesti eri verkoissa (VLAN), ja niiden välistä liikennettä reititetään yhdellä VMware-virtuaalikoneista suoritettavalla Linux-pohjaisella käyttöjärjestelmällä nimeltä Vyatta. Vyatta on ilmainen avoimen lähdekoodin Debianiin perustuva käyttöjärjestelmä, joka tukee IPv4:ää ja IPv6:ta. Käyttöjärjestelmä sisältää muun muassa reitittimen ja palomuurin ominaisuudet, jotka ovat ominaisuuksiltaan ja käytettävyydeltään verrattavissa esimerkiksi moneen Ciscon ja Juniperin toimittamaan laitteistopohjaiseen reitittimeen tai palomuuriin. Vyatta on otettu käyttöön ainoastaan tätä työtä varten. Se ei ole käytössä tuotantoympäristöissä. Se on kuitenkin riittävä ratkaisu käytettäväksi tämän työn yhteydessä. [32; 33.]

5.4.1 GNS3-virtuaaliympäristön ja laboratorioympäristön välinen reititys

Asiakasverkon reitittimille R1, R2 ja R3 levitetään reitittimen R1 toimesta OSPFv3:n avulla oletusreitti. Oletusreitti reitittää kaiken liikenteen, jonka kohdeosoite tai -verkko ei ole tunnettu, ulos R1-reitittimen liitännästä Gigabit Ethernet 1/0. Kyseinen liitäntä on sovellustasolla loogisesti liitetty ja reititetty GNS3-palvelimen fyysiseen liitäntään

Ethernet3, joka vastaavasti on fyysisesti kiinni laboratorioverkon L3-kytkimessä Swi1 liitännässä Fast Ethernet 3/18.

Laboratorioverkon kytkimet osallistuvat omaan OSPF-prosessiin, eikä asiakasverkon OSPF-prosessin haluta levittää reittejä laboratorioverkon kytkimille, joten GNS3-ympäristön ja laboratorioverkon välisen linkin liitännät asetetaan passiivisiksi. Tällöin ne eivät mainosta reittejä määriteltyjen liitäntöjen kautta. Näin kaksi OSPF-prosessia toimivat itsenäisesti sekaantumatta toisiinsa, vaikka niillä sattumoisin olisikin identtiset globaalillakin tasolla merkittävät asetukset, kuten reititysprosessiin osallistuvien liitäntöjen alue (area). Tämä käsite esitellään jäljempänä reitityksen toteutusvaiheessa.

Reitittimille R1, R2 ja R3 konfiguroidaan loopback-liitännät ja jokaiselle näistä liitännöistä annetaan IPv6-osoite. Syy on reitittimien hallinnassa. Asiakkaan verkko on niin sanottu full-mesh-verkko, eli jokaiselta reitittimeltä on fyysisellä tasolla yhteys verkon jokaiseen reittimeen. Yksinkertaisemmin sanottuna, reitittimeltä R1 pääsee reitittimelle R3 kahta eri reittiä: suoraan reitittimelle R3 tai vaihtoehtoisesti reitittimen R2 kautta. Loogiset loopback-liitännät ovat reitittimen käyttöjärjestelmässä ohjelmistolla toteutettuja liitäntöjä. Niiden toimintaa eivät häiritse muun muassa ulkoiset kaapeliviat tai reitittimien verkkokorttien fyysiset rikkoutumiset. Looginen liitäntä toimii aina, kun reittimen käyttöjärjestelmä on toiminnassa. Tästä syystä loopback-liitäntöjen IPv6-osoitteita käytetään reitittimien hallintaan. Esimerkiksi kaapelin katketessa reitittimien R1 ja R3 välillä pääsy reitittimelle R3 ei esty, koska loopback-liitäntä on toiminnassa, ja reitittimelle R3 on pääsy myös reitittimen R2 kautta. Ilman loopback-liitäntöjä reitittimien hallinta (SSH- tai Telnet-yhteyden muodostus etänä) tapahtuisi reitittimien Gigabit Ethernet –liitännöille annettuja osoitteita käyttäen, mutta koskaan ei voisi olla varma, onko kyseinen liitäntä toimimattomassa tilassa, jolloin pääsy laitteelle estyy. Kun etäyhteys otetaan käyttäen loopback-liitännän osoitetta, reitittimien reititysprosessi osaa etsiä toisen reitin kohteeseen, jos kohteen jokin fyysisistä liitännöistä ei ole toiminnallinen.

Reitittimelle R1 on konfiguroitu staattinen reitti, joka reitittää kaiken liikenteen, jonka kohdeosoite tai -verkko ei ole tunnettu, ulos R1-reitittimen liitännästä Gigabit Ethernet 1/0. Tätä reittiä mainostetaan asiakasverkon OSPFv3-reititysprosessiin luvussa 5.4.2 esitetyllä tavalla. Samassa luvussa on myös esitetty konfiguraation liitännän Gigabit

Ethernet 1/0:n asettamisesta passiiviseksi asiakasverkon OSPFv3-reititysprosessissa. Seuraavaksi on esitetty reitittimen R1 oletusreitin konfiguraatio.

```
R1#show configuration | include ::/0
ipv6 route ::/0 GigabitEthernet1/0 2001:67C:110:3003::1
```

IPv6-reitti osoittaa siis reitittimellä R1 ulos liitännästä Gigabit Ethernet 1/0 ja next-hop-osoitteeksi on annettu Swi1-kytkimen VLAN500-liitännän osoite 2001:67C:110:3003::1.

5.4.2 Asiakasverkon reititys

Asiakasverkon reititys toteutetaan OSPFv3-reititysprotokollalla. OSPFv3 on IPv6:ta tukeva reititysprotokolla. GNS3-virtuaaliympäristössä uusin saatavilla oleva Ciscon käyttöjärjestelmä on IOS 15.0(1)M. IOS-version tulee olla vähintään 15.1(3)S tai 15.2(1)T, jotta OSPFv3 on täysin tuettu. GNS3-virtuaaliympäristö päivitettiin siten, että virtuaalireitittimillä on mahdollista ajaa myös näitä uudempia OSPFv3:a tukevia käyttöjärjestelmiä. [34; 35.]

Seuraavassa on esitetty reitittimien R1, R2 ja R3 OSPFv3-reititysprosessin konfiguraatiot. IPv6:n myötä OSPFv3-reititysprosessiin mukaan otettavia verkkoja ei konfiguroida enää prosessin yhteydessä, kuten aiemmin OSPFv2:n tapauksessa, vaan liitännän yhteydessä. Nämä liitäntäkohtaiset konfiguraatiot esitetään jäljempänä. [36; 37; 38.]

```
R1#show configuration | begin router
ipv6 router ospf 1
 router-id 1.1.1.1
 default-information originate
 passive-interface GigabitEthernet1/0


R2#show configuration | begin router
ipv6 router ospf 1
 router-id 2.2.2.2


R3#show configuration | begin router
ipv6 router ospf 1
 router-id 3.3.3.3
```

Reitittimien reititysprosessien konfiguraatioissa on yhtenäisesti ensiksi konfiguroitu reititysprosessi, joka on on kaikilla reitittimillä numero yksi. Prosessin numerollinen arvo ei ole globaalisti merkittävä, joten se on vain selkeyssyistä konfiguroitu kaikilla

laitteilla samalla arvolla. Laitteilla voi pyöriä useita prosesseja, mutta tässä tapauksessa on tarve vain yhdelle reititysprosessille. Router-id identifioi laitteen reititysprosessissa, ja kyseisen arvon mukaan määräytyy reitittimen rooli OSPF-topologiassa. Tässä työssä näillä arvoilla ei kuitenkaan ole merkitystä, koska reitittimien väliset linkit ovat point-to-point-linkkejä, sekä verkko on itsessään full-mesh-tyylinen. Vaikka IPv6 on osoitteistukseltaan 128-bittinen, reitittimet identifioidaan yhä käyttäen 32 bittiä, eli IPv4-osoitteen muodossa. Ciscon IOS-käyttöjärjestelmät vielä nykyisinkin pyrkivät konfiguroimaan reitittimen id:n automaattisesti korkeimmasta mahdollisesta saatavilla olevasta IPv4-osoitteesta laitteella. Tässä tapauksessa kun yhtään IPv4-osoitetta ei ole konfiguroitu laitteelle, reititysprosessi ei käynnisty, vaan palauttaa konsoliin virheen ja pyytää konfiguroimaan reitittimelle router-id:n manuaalisesti. Seuraavaksi on esitetty esimerkki edellä kuvatusta tapahtumasta. [36; 37; 38.]

```
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a
router-id, please configure manually
```

Tämän jälkeen laitteille voidaan konfiguroida router-id:t manuaalisesti, jonka jälkeen reititysprosessit käynnistyvät.

Lisäksi reitittimellä R1 liitäntä Gigabit Ethernet 1/0 on asetettu passiiviseksi, joten reititin ei levitä OSPFv3:n reitityssanomia ulos tästä portista. Tämä komento siis varmistaa sen, että reititysprosessit laboratorioverkossa ja asiakasverkossa eivät häiritse toistensa toimintaa.

Reitittimen R1 komento ”default-information originate” tarkoittaa sitä, että reitittimelle konfiguroidut oletusreitit mainostetaan toisille reitittimille reititysprosessin reitityssanomissa. Tällöin myös reitittimet R2 ja R3 saavat reititystauluunsa oletusreitin ja näin ollen tietävät lähettää paketteja kohti reititintä R1, kun kohdeosoite tai -verkko ei ole tiedossa.

Kuten aiemmin mainittiin, OSPFv3:n kanssa reititysprosessiin mukaan otettavat verkot konfiguroidaan liitäntätasolla, ei reititysprosessissa, niin kuin aiemmin oli käytäntönä IPv4:n ja OSPFv2:n kanssa. Seuraavaksi on esitetty reitittimen R1 OSPFv3-reititysprosessiin 1 kuuluvien liitäntöjen konfiguraatiot.

```
R1#show configuration | begin interface
interface Loopback0
 no ip address
 ipv6 address 2001:67C:110:3004::4:1/112
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0
 no ip address
 no ip route-cache
 ipv6 address 2001:67C:110:3004::1:1/112
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1/0
 no ip address
 no ip route-cache
 negotiation auto
 ipv6 address 2001:67C:110:3003::2/64
 ipv6 enable
!
interface GigabitEthernet2/0
 no ip address
 no ip route-cache
 ipv6 address 2001:67C:110:3004::2:1/112
 ipv6 enable
 ipv6 ospf 1 area 0
```

Reitittimellä R1 kaikki liitännät, lukuun ottamatta liitäntää Gigabit Ethernet 1/0, osallistuvat OSPFv3:n reititysprosessiin 1. Komennossa näkyvä ”area 0” tarkoittaa sitä, että kyseinen liitäntä kuuluu alueeseen 0, eli OSPF:n tapauksessa arvo 0 tarkoittaa runkoverkkoa (engl. backbone). Runkoverkon alue hoitaa reitityksen muiden OSPF:n alueiden kesken. Jos tämän työn virtuaalinen asiakasverkko toteutettaisiin oikeassa asiakasympäristössä, reitittimien R1, R2 ja R3 loopback0-liitännät voisivat kuulua muuhun kuin alueeseen 0, ja silloin reititys näiden verkkojen kesken liikennöitäisiin runkoveron alueen 0 kautta. Syy, miksi liitäntä Gigabit Ethernet 1/0 ei kuulu reititysprosessiin, on vain varotoimenpide. Kyseinen liitäntä on liitetty laboratorioverkkoon, eikä reittejä haluta mainostaa tuohon verkkoon. Reitittimien R2 ja R3 liitäntöjen konfiguraatiot ovat samankaltaiset reitittimen R1 konfiguraation kanssa. Näillä reitittimillä kaikki liitännät osallistuvat OSPF-reititysprosessiin 1 ja alueeseen 0. [39.]

Seuraavaksi on esitetty kahden reitittimen välisen OSPFv3-naapuruuden todentaminen. Kun reitittimelle R1 ja R2 on syötetty liitäntöihin konfiguraatiot, jotka määrittelevät kyseenomaisen liitännän kuuluvaksi prosessiin 1 ja alueeseen 0, muodostuu OSPF-naapuruus, joka voidaan todentaa seuraavalla tavalla:

```
*Oct  29  23:06:28.987:  %OSPFv3-5-ADJCHG:  Process  1,  Nbr
3.3.3.3 on GigabitEthernet2/0 from LOADING to FULL, Loading
Done


R1#show ipv6 ospf neighbor

Neighbor ID   State       Dead Time    Interface
3.3.3.3       FULL/DR     00:00:38     GigabitEthernet2/0
2.2.2.2       FULL/DR     00:00:31     GigabitEthernet0/0
```

Ylempi terminaaliin tulostunut Syslog-viesti osoittaa, että IPv6-naapuruus on onnistuneesti muodostettu reitittimen R1 ja R3 välillä. Naapuruuslistasta nähdään, että reititin R1 on muodostanut OSPF-naapuruuden myös reitittimen R2 kanssa.

Seuraavaksi tarkastellaan reitittimen R1 IPv6-reititystaulua. Ainoastaan reittien lyhenteiden selitykset on poistettu reititystaulun yläosasta tilan säästämiseksi.

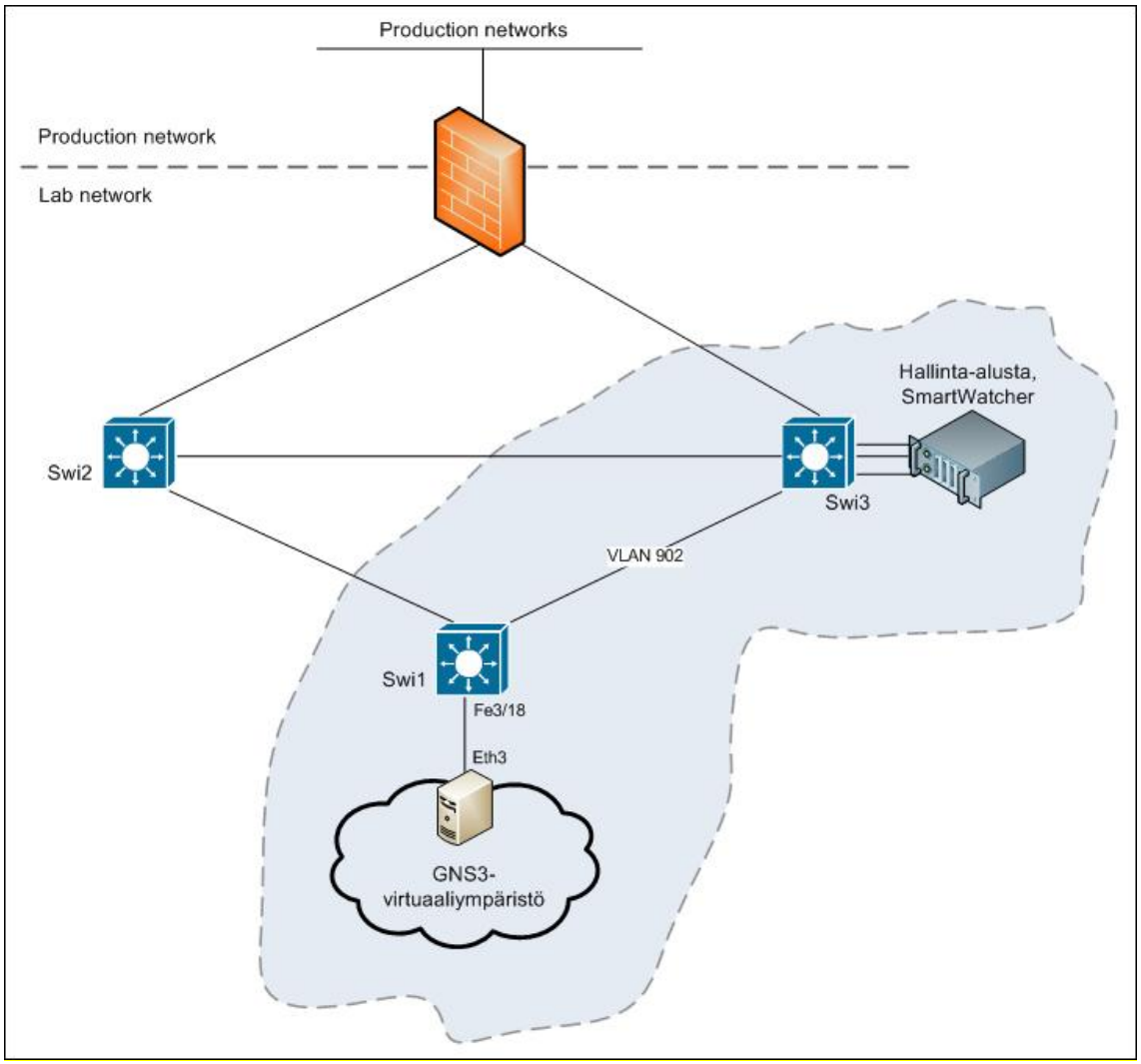
```
R1#show ipv6 route
IPv6 Routing Table - default - 13 entries
S   ::/0 [1/0]
     via 2001:67C:110:3003::1, GigabitEthernet1/0
C   2001:67C:110:3003::/64 [0/0]
     via GigabitEthernet1/0, directly connected
L   2001:67C:110:3003::2/128 [0/0]
     via GigabitEthernet1/0, receive
C   2001:67C:110:3004::1:0/112 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:67C:110:3004::1:1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:67C:110:3004::2:0/112 [0/0]
     via GigabitEthernet2/0, directly connected
L   2001:67C:110:3004::2:1/128 [0/0]
     via GigabitEthernet2/0, receive
O   2001:67C:110:3004::3:0/112 [110/2]
     via FE80::C801:41FF:FED2:8, GigabitEthernet0/0
     via FE80::C802:41FF:FEE1:8, GigabitEthernet2/0
C   2001:67C:110:3004::4:0/112 [0/0]
     via Loopback0, directly connected
L   2001:67C:110:3004::4:1/128 [0/0]
     via Loopback0, receive
O   2001:67C:110:3004::5:1/128 [110/1]
     via FE80::C801:41FF:FED2:8, GigabitEthernet0/0
O   2001:67C:110:3004::6:1/128 [110/1]
     via FE80::C802:41FF:FEE1:8, GigabitEthernet2/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Reititystaulusta nähdään, että OSPFv3-reititysprosessissa (O, eli OSPF Intra) mainostetut reitit käyttävät next-hop-osoitteena liitäntöjen link-local-osoitteita

(FE80::/10). Link-local-osoitteet ovat linkkien kesken paikallisia osoitteita ja niitä käytetään ainoastaan linkin keskinäiseen kommunikointiin. Link-local-osoitteita ei reititetä linkin ulkopuolelle ollenkaan. [2, s. 30.]

5.4.3 Tarvittavat reititysmuutokset laboratorioverkossa

Kuvassa 9 on esitetty laboratorioverkon verkkokuva. Katkoviivalla rajattu alue koskee tätä työtä, eivätkä alueen ulkopuolella sijaitsevat verkkolaitteet liity työhön.



Kuva 9. Laboratorioverkon pelkistetty verkkokuva.

Swi1 on Cisco Catalyst 4000 -sarjan L3-kytkin. Se siis sisältää sekä kytkimen, että reitittimen ominaisuudet. Swi3 on myös saman tyyppinen L3-kytkin, mutta se on Cisco Calatyst 6000 -sarjasta. Swi1-kytkimelle on konfiguroitu OSPFv3-reititysprosessi IPv6:ta varten. Laboratorioverkon runko tukee sekä IPv4:ää että IPv6:ta. Rungon muodostavat

verkkolaitteet toimivat siis niin sanotusti dual-stack moodissa, eli niillä on muun muassa omat reititystaulut kummallekin protokollaversiolle. Swi1-kytkimelle on konfiguroitu tätä työtä varten staattinen reitti kohti GNS3-virtuaaliympäristön verkkoja seuraavalla komennolla, joka levitetään laboratorioverkon reititysprotokollalla muille runkoverkon laitteille.

```
Swi1(config)#ipv6 route 2001:67C:110:3004::/64
2001:67C:110:3003::2
```

Komennossa on siis käytetty next-hop osoitteena GNS3-virtuaaliympäristön reitittimen R1 liitännän Gigabit Ethernet 1/0 osoitetta. Koska kytkimellä Swi1 liitäntä VLAN 500 on konfiguroitu kuulumaan laboratorioverkon OSPFv3-reititysprosessiin, staattinen reitti saadaan levitettyä kaikille samaan prosessiin kuuluville runkoverkon laitteille. Seuraavassa on esitetty komennot, joilla reitti levitetään reititysprosessiin.

```
Swi1(config)#route-map IPv6-Static-to-GNS permit 10
Swi1(config-route-map)#match ipv6 address prefix-list IPv6-
Static-Prefixes

Swi1(config)#ipv6 prefix-list IPv6-Static-Prefixes permit
2001:67c:110:3004::/64

Swi1(config)#ipv6 router ospf 65000
Swi1(config-rtr)#redistribute static route-map IPv6-Static-
to-GNS
```

Ratkaisussa on käytetty hyväksi reitti- ja osoitelistoja (route-map ja prefix-list). Tähän päädyttiin selkeyden takia, jotta reititystaulua on helpompi lukea vianselvitystilanteessa, koska reititysprosessiin levitettävät reitit on nimetty selkeästi reitti- ja osoitelistojen avulla. Lisäksi reitti- ja osoitelistoilla estetään se, että mitään muita reittejä ei vahingossakaan levitetä laboratorioverkon reititysprosessiin. Tarvittaessa staattisia reittejä voidaan lisätä suoraan reittilistaan, jolloin ne levittyvät automaattisesti reittilistan kautta reititysprosessiin.

5.5 Verkonvalvontaan liittyvät konfiguraatiot

5.5.1 ICMP-konfiguraatio

SmartWatcher lähettää laitteelle ICMP echo -pyynnön, johon laite vastaa ICMP echo -vastauksella. ICMP echo -vastauksen kohdeosoitteina käytetään reitittimien R1, R2 ja R3 Loopback0-liitäntöjä. SmartWatcherin toimintatapa Ping:iin liittyen on lähettää

ennalta määritetyin väliajoin ICMP echo -pyyntöjä CMDB:stä löytyvien laitteiden hallintaosoitteisiin. Smartwatcher lähettää siis ICMP echo -pyynnön kohti CMDB:stä löytyvää laitetta, jonka jälkeen se toistaa saman toiminnon tietokannasta löytyvällä seuraavalle laitteelle. Smartwatcher ei jää odottamaan laitteen vastausta, vaan jatkaa CMDB:n läpikäyntiä edellä mainitulla tavalla. Normaalisti tämä toistetaan aina viiden minuutin välein, mutta kyseinen aika voidaan määrittää myös pidemmäksi tai lyhyemmäksi tilanteen mukaan. Smartwatcherilla on tällaisessa tapauksessa noin 75 % aikaa viidestä minuutista (225 sekuntia) todeta jokin tietokannan laitteista tavoittamattomaksi. Kun laitetietokannassa on runsaasti laitteita, niin silloin ICMP echo -vastauksen time-out-arvoa saatetaan dynaamisesti muuttaa pienemmäksi, jotta pysytään määritellyssä aikaikkunassa. Lisäksi ICMP echo -pyyntö voidaan toistaa määrityksestä riippuen noin 1–3 kertaa kyselykierroksen aikana. Jos laite ei kierroksen aikana lähetä vastausta Smartwatcherille, niin normaalitapauksessa tällaisesta tapahtumasta generoidaan hälytys valvontanäkymään. Järjestelmä on jatkuvasti aktiivinen aina valvontanäkymään asti, joten jos hälyttävä laite vastaa toisella ICMP echo -pyyntökierroksella, niin aiemmin valvontanäkymään tuotu hälytysrivi poistetaan. [32.]

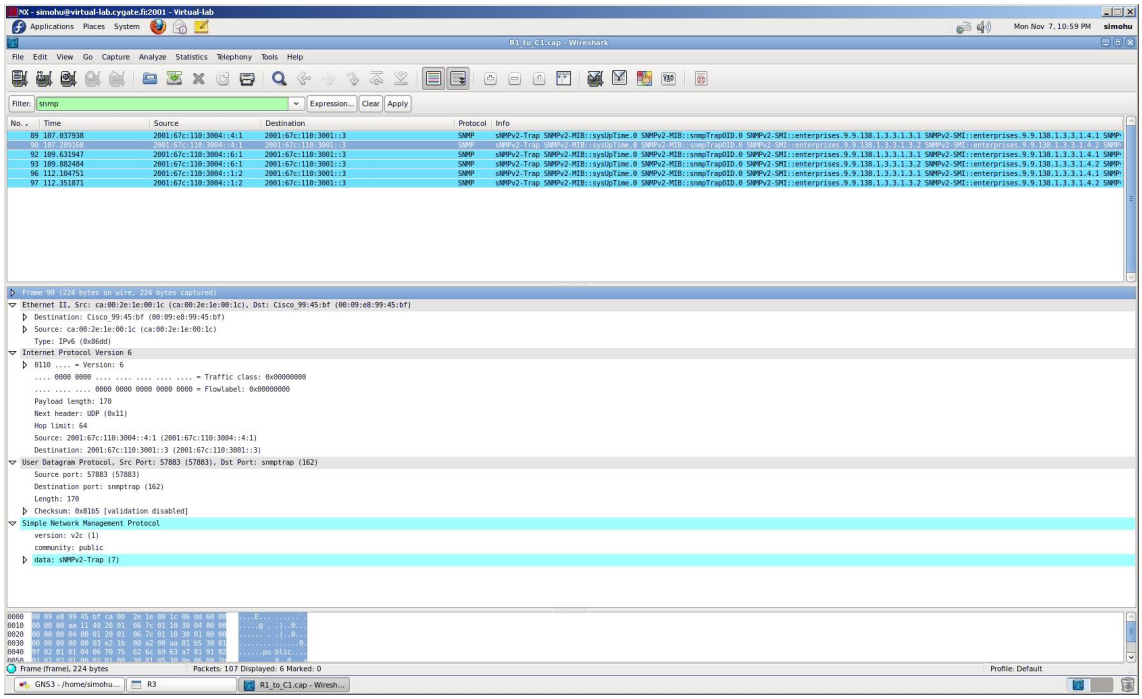
5.5.2 SNMP-konfiguraatio

Reitittimille konfiguroidaan seuraavanlaiset SNMP-asetukset:

```
R1#show configuration | begin snmp
snmp-server community public RW
snmp-server trap-source Loopback0
snmp-server enable traps ospf state-change
snmp-server enable traps alarms informational
snmp-server host 2001:67C:110:3001::3 version 2c public
```

Konfiguraatiossa on asetettu SNMP-trapien vastaanottajaksi SmartWatcherin osoite sekä valittu versioksi 2c. Komennon lopussa sana ”public” on SNMP-yhteisön tunnus. Sen tarkoitus on käytännössä sama kuin salasanalla. Yhteisötunnuksen pitää olla sekä SNMP-isännän ja SNMP-managerin tiedossa, jotta SNMP-yhteys voidaan muodostaa. Yhteisötunnuksilla voidaan myös jakaa hallittava verkko useisiin loogisiin alueisiin. Kommuunille on lisäksi annettu kirjoitus- ja lukuoikeudet (RW), joten SNMP-manageri voi tarvittaessa suorittaa laitteelle sekä luku- että kirjoitustoimintoja. Lukutoiminto (GET) tarkoittaa laitteen tietojen lukemista SNMP-managerin suuntaan. Kirjoitustoiminnolla (SET) tarkoitetaan esimerkiksi SNMP-managerin toimesta tehtyjä

konfiguraatiomuutoksia. SNMP-manageri voi olla esimerkiksi palvelimelle asennettu verkonhallintasovellus (NMS, Network Management System). Yleensä laitteille konfiguroidaan tietoturvasyistä vain lukuoikeus, mutta tässä tapauksessa voidaan lisätä myös kirjoitusoikeus, jotta testejä pystytään suorittamaan mahdollisimman laajasti. SNMP-trapit lähetetään siten, että trapin lähdeosoitteeksi tulee tässä tapauksessa reitittimen R1 loopback0-liitännän osoite. Lisäksi konfiguraatiossa on määritelty, että OSPF-naapuruuksien tilojen muutokset, sekä tason 4 ja siitä kriittisemmät hälytykset, aiheuttavat SNMP-trapin lähetyksen. [6, s. 331; 40; 41.]



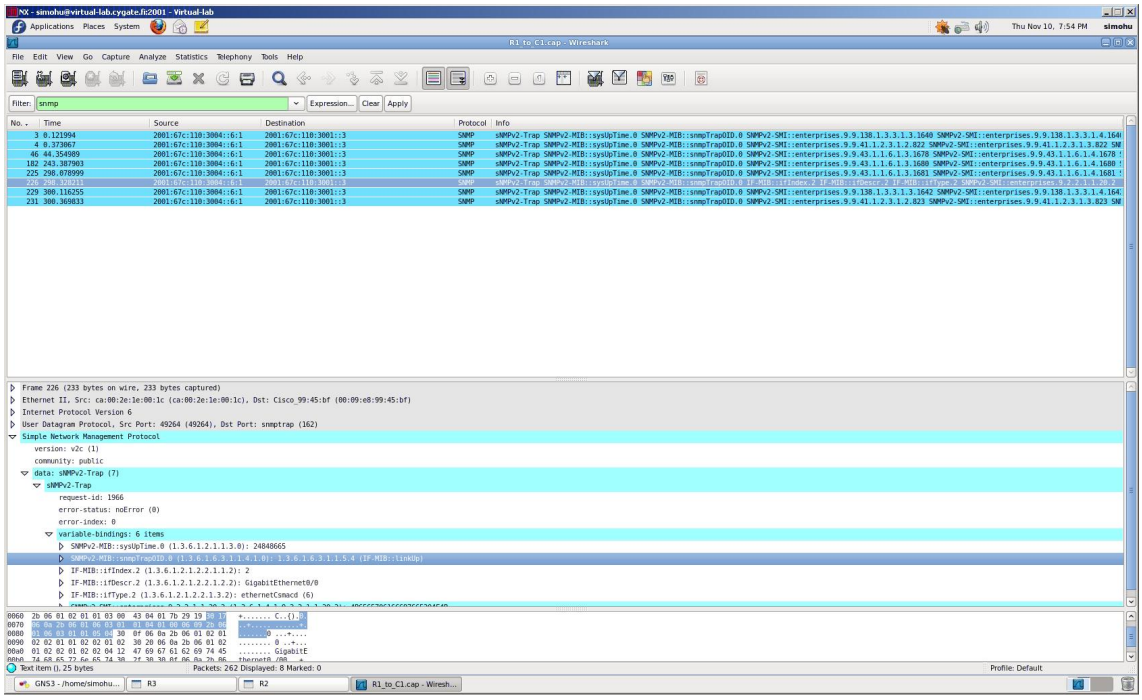
Kuva 10. Wireshark-kaappaus SNMP-liikenteestä reitittimeltä R1.

Kuva 10 on Wireshark-kaappaus SNMP-liikenteestä reitittimen R1 liitännästä Gigabit Ethernet 1/0. Reitittimien konfiguraatioita täytyy tutkia tarkemmin, koska kaappauksessa ei näy ollenkaan OSPF-reititysprosessin naapuruuksien tilojen muutoksia. Liikenteen kaappauksen aikana nimittäin laitettiin manuaalisesti reitittimen R1 ja R3 välinen linkki alas, joten tästä olisi pitänyt generoitua useita SNMP-trapeja. Kuvassa näkyvät paketit ovat kaikki laitekohtaisia yleisiä SNMP-trapeja, jotka muun muassa kertovat laitteen päälläoloajan (sysUpTime).

Vianetsintä aloitetaan laittamalla aluksi kaikki SNMP-trapit päälle. Aiemmin laitteille lisätty SNMP-konfiguraatio sallii ainoastaan OSPF-reititysprosessin naapuruuksien tilamuutokset.

```
R3(config)#snmp-server enable traps
```

Edellä esitelty komento kytkee päälle kaikki mahdolliset SNMP-trapit. Kuvasta 11 nähdään, että nyt myös linkin ja OSPF-reititysprosessin naapuruuksien tilamuutoksista generoituu trap. Kuvassa 11 liikennettä on kaapattu reitittimen R1 liitännästä Gigabit Ethernet 1/0, ja reitittimen R3 liitäntä Gigabit Ethernet 0/0 on laitettu kaappauksen aikana testimielessä ensiksi toimimattomaan tilaan ja sitten laitettu heti takaisin toiminnalliseksi. [42.]



Kuva 11. Wireshark-kaappaus SNMP-liikenteestä reitittimen R1 liitännästä Gigabit Ethernet 1/0 nähtynä.

Wireshark-kaappauksesta nähdään, että tässä toistuu sama ongelma kuin Syslog-viestien kanssa. Tilanne on tarkemmin kuvattuna kohdassa 4.5.3. Ainoastaan linkin palauttamisesta takaisin toiminnalliseksi nähdään SNMP-trap. Tätä ongelmaa tutkitaan syvällisemmin kohdassa 5.5.3. Kun SNMP-trap-pakettia tarkastellaan tarkemmin, nähdään, että paketin lähdeosoitteena on reitittimen R3 loopback0-liitäntä ja

kohdeosoitteena Smartwatcherin osoite. Tiedoista nähdään myös, että liitännän tyyppi on Ethernet, liitännän nimi Gigabit Ethernet 0/0 ja liitännän indeksinumero 2. Nämä tiedot SNMP-agentti (reititin R3) on löytänyt IF-MIB-nimisestä MIB:stä. Esimerkiksi liitännän indeksinumeron Object ID (OID) on tässä tapauksessa 1.3.6.1.2.1.2.2.1.1.2.

5.5.3 Syslog-konfiguraatio

Asiakasverkon jokaiselle reitittimille on konfiguroitu Syslog-sanomia varten seuraavat asetukset:

```
R3#show configuration | begin logging
logging trap notifications
logging source-interface Loopback0
logging host ipv6 2001:67C:110:3001::3
```

Konfiguraatiossa on Syslog-viestien vastaanottajaksi asetettu SmartWatcherin IPv6-osoite 2001:67C:110:3001::3. Syslog-viestien lähettäjäksi voidaan määritellä myös Loopback-liitäntä, eli viestien lähetysosoitteeksi merkitään tässä tapauksessa reitittimen R3 Loopback0 liitännän osoite 2001:67c:110:3004::6:1. Tällöin varmistetaan, että viestit menevät perille silloinkin, kun jompi kumpi reitittimien välisistä linkeistä on toimimattomassa tilassa. Ratkaisulla saadaan myös viestien lähdeosoite pysymään samana, vaikka reititys muuttuisikin toisen linkin mennessä alas. Syslog-viesteille on lisäksi määritelty tietty raja-arvo, jolla määritellään minkä vakavuusasteen tapahtumista lähetetään Syslog-viesti. Tässä tapauksessa raja-arvoksi on annettu melko alhainen ”notifications”, joka on Cisco:n IOS:ssä numeroarvo 5. Arvo voi sijoittua välille 0–7. Mitä pienempi arvo, sitä kriittisempi tapahtuma. Esimerkiksi arvo 0 tarkoittaa erittäin vakavaa laitteen ydintoimintaa haittaavaa tai estävää tapahtumaa. Tässä työssä on valittu arvo 5, koska laitteita on vähän, ja kriittisimpiä tapahtumia ei voida kunnolla simuloida laboratorio-olosuhteissa. Arvon ollessa 5 saadaan Syslog-viestejä generoitua muun muassa reitittimien välisten linkkien mennessä toimimattomaan tilaan.

Syslog-viestejä testattaessa huomattiin, että OSPF-naapurien tilojen muutokset eivät aiheuta lähetettävää Syslog-tapahtumaa. Ratkaisu oli konfiguroida tämä ominaisuus päälle jokaisen reitittimen IPv6:n OSPF-reititysprosessissa seuraavalla tavalla:

```
R3(config)#ipv6 router ospf 1
```

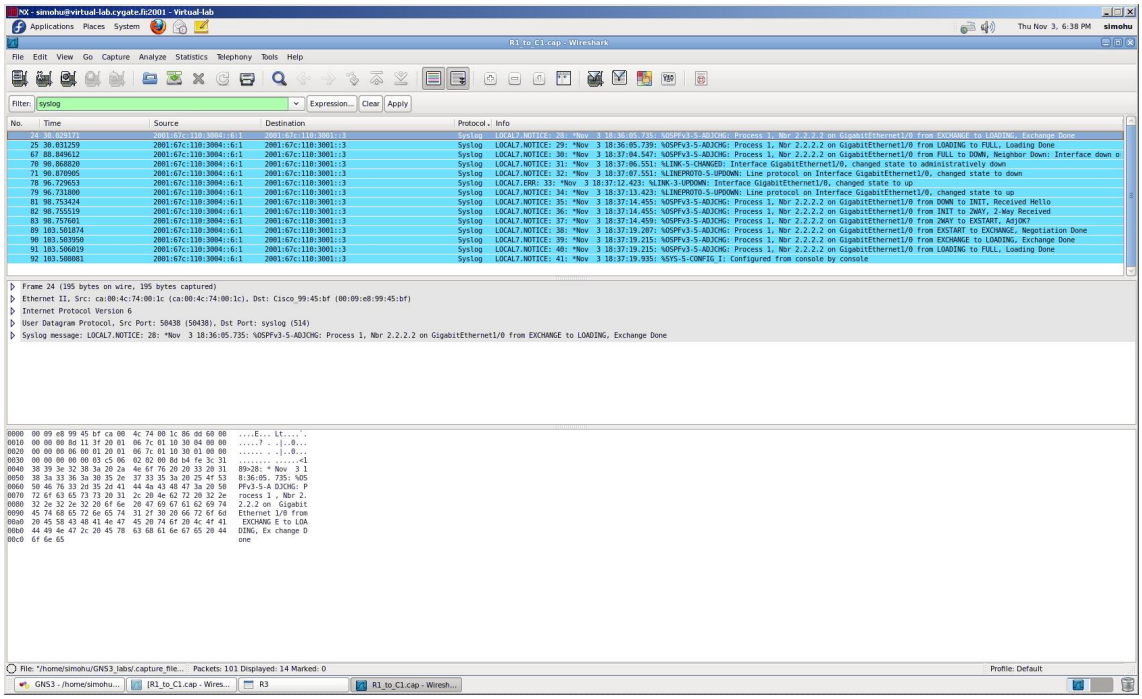
```
R3(config-rtr)#log-adjacency-changes detail
```

Tämän jälkeen tutkittiin liikennettä Wiresharkiilla, ja huomattiin, että ainoastaan linkin nousu takaisin toiminnalliseen tilaan aiheuttaa Syslog-viestin. Toisin sanoen, esimerkiksi reitittimen R3 ja R1 välisen linkin konfiguroiminen administrative down -tilaan ei generoinut Syslog-viestiä, vaikka liikennettä tarkasteltiin reitittimen R1 liitännässä Gigabit Ethernet 1/0. Tässä liitännässä pitäisi näkyä kaikki Syslog-liikenne, eli UDP-liikenne kohdeporttiin 514 kohti SmartWatcherin osoitetta. Ongelman selvittelyä jatkettiin ja todettiin, että Syslog-viestit eivät välity, jos esimerkiksi reitittimen R1 ja R3 välinen linkki on alhaalla. Syslog-viestit eivät osaa ottaa toista reittiä reitittimen R2 kautta, vaikka muu liikenne toimiikin juuri odotetulla tavalla ja reitittyy uudelleen toista kautta, jos ensisijainen reitti on poikki. Tämä vahvistettiin sillä, että generoitiin Syslog-viestejä epästabiilista linkistä reitittimen R3 ja R2 välillä, ja seurattiin liikennettä reitittimen R3 portista Gigabit Ethernet 0/0. Tällöin huomattiin, että Wiresharkissa näkyy myös viestit linkin mennessä toimimattomaan tilaan.

Ongelma on siis tiivistettynä se, että esimeriksi reitittimellä R3 tapahtuvat OSPF-naapuruuksien muutokset ottavat oletuksena reitin reitittimen R3 liitännän Gigabit Ethernet 0/0 kautta, vaikka tuo kyseinen liitäntä olisikin toimimattomassa tilassa. Syslog-liikenne ei siis reitity liitännän Gigabit Ethernet 0/0 ollessa toimimattomassa tilassa toista reittiä, eli kohti reititintä R2 liitännän Gigabit Ethernet 1/0 kautta. Tämä ei kuitenkaan ole tavanomainen reititysongelma, koska muu verkkoliikenne uudelleenreitittyy OSPF:n toimesta, jos liitäntä Gigabit Ethernet 0/0 pakotetaan toimimattomaan tilaan. Tämä todennettiin vielä tarkastelemalla reititystaulua liitännän Gigabit Ethernet 0/0 ollessa toiminnallinen, ja sen jälkeen kun liitäntä on pakotettu toimimattomaan tilaan. Tämä testi osoittaa, että oletusreitin ::/0 next-hop muuttui liitännän Gigabit Ethernet 0/0 ollessa toimimattomassa tilassa siten, että liikenne kulkee ulospäin reititystaulunkin mukaan reitittimen R3 liitännästä Gigabit Ethernet 1/0. Reititys siis toimii kuten pitääkin, joten ongelmaa on etsittävä muualta.

Kuvasta 12 nähdään Wireshark-pakettianalysaattorilla tietoa Syslog-viesteistä. Liikennettä seurattiin reitittimen R1 liitännästä Gigabit Ethernet 1/0, ja sitten pakotettiin reitittimen R1 liitäntä Gigabit Ethernet 1/0 toimimattomaan tilaan komennolla ”shutdown” ja takaisin toiminnalliseksi komennolla ”no shutdown”. Näin

saatiin generoitua tarpeeksi Syslog-viestejä, josta voidaan todentaa reitittimen R3 ja R2 välisen linkin olleen hetken aikaa poikki.



Kuva 12. Wireshark-pakettianalysaattorin kaappaus Syslog-liikenteestä reitittimellä R1.

Kuvasta nähdään, että lähdeosoite (source) on reitittimen R3 loopback0-liitännän osoite 2001:67c:110:3004::6:1, ja kohdeosoite (Destination) hallinta-alustan virtuaalisen SmartWatcherin osoite 2001:67c:110:3001::3.

5.5.4 Reititysongelman vianetsintä

GNS3-virtuaaliympäristön verkon reititys toimii oletetulla tavalla. Linkin mennessä alas reititys kääntyy käyttämään toista linkkiä. Vianselvityksen tuloksena voidaan päätellä, että SNMP- ja Syslog-viestit lähetetään linkin mennessä alas ennen kuin reititysprotokolla on ehtinyt reagoida tapahtumaan, ja kääntämään liikennettä toiselle reitille. Tämä voidaan todentaa muun muassa seuraamalla reitittimellä R3 SNMP-trapien lähettämistä samanaikaisesti kun tarkastellaan reaaliaikaisesti reititysprotokollan reaktiota toimimattomaan tilaan menneelle linkille.

```
R3#
*Nov 10 21:34:32.214: %OSPFv3-5-ADJCHG: Process 1, Nbr
1.1.1.1 on GigabitEthernet0/0 from FULL to DOWN, Neighbor
Down: Interface down or detached
```

```
*Nov 10 21:34:34.218: %LINK-5-CHANGED: Interface
GigabitEthernet0/0, changed state to administratively down
*Nov 10 21:34:35.218: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to down
*Nov 10 21:34:35.222: SNMP: Queuing packet to
2001:67C:110:3001::3
*Nov 10 21:34:35.222: SNMP: V2 Trap, reqid 2112, errstat 0,
erridx 0
 sysUpTime.0 = 25457221
 snmpTrapOID.0 = snmpTraps.3
 ifIndex.2 = 2
 ifDescr.2 = GigabitEthernet0/0
 ifType.2 = 6
 lifEntry.20.2 = administratively down
*Nov 10 21:34:35.474: SNMP: Packet sent via UDP to
2001:67C:110:3001::3
*Nov 10 21:34:37.278: [OSPFv3-1 Router]IPv6RT[default]:
ospf 1, Route add ::/0 [owner]
*Nov 10 21:34:37.278: [OSPFv3-1 Router]IPv6RT[default]:
ospf 1, Added path
FE80::C801:2EFF:FE1E:1C/GigabitEthernet1/0
*Nov 10 21:34:37.278: [OSPFv3-1 Router]IPv6RT[default]:
ospf 1, Delete next-hop FE80::C800:2EFF:FE1E:38,
GigabitEthernet0/0 for ::/0
```

Loki on saatu aikaiseksi seuraamalla IOS:n terminaalilta reitityksen ja SNMP-liikenteen toimintaa. Lokin keräystä ennen laitettiin reitittimen R3 liitäntä Gigabit Ethernet 0/0 manuaalisesti administratively down -tilaan. Seuraavat debug-komennot kytkettiin päälle reitittimellä R3, jotta voitaisiin nähdä yllä näkyvää yksityiskohtaisempaa tietoa reititysprosessissa tapahtuvista muutoksista sekä SNMP-paketeista.

```
R3#debug ipv6 routing
R3#debug snmp packets
```

Loki osoittaa selvästi, että SNMP-trap lähetetään kohti Smartwatcherin osoitetta aikaleimalla *Nov 10 21:34:35.474. Tällöin reititystaulu osoittaa next-hop:ksi toimimattomaan tilaan menneen liitännän Gigabit Ethernet 0/0. Reititystaulun muutos next-hop:in osalta tapahtuu vasta lokin viimeisellä rivillä, aikaleimalla *Nov 10 21:34:37.278. SNMP-trap lähetetään siis ennen reititystaulussa tapahtuvaa muutosta, ja paketti lähetetään liitännästä loopback0 kohti administratively down -tilassa olevaa liitäntää Gigabit Ethernet 0/0, vaikka ainoa reitti reitittimelle R1 olisi tässä vaiheessa reitittimen R2 kautta. SNMP käyttää kuljetuskerroksella UDP:ta, joka on ominaisuuksiltaan yhteydetön protokolla eikä se myöskään odota lähetetylle paketille minkäänlaista vahvistusta perillemenosta. Tästä syystä virheilmoitusta ei nähdä, kun SNMP-trap lähetetään kohti administratively down -tilassa olevaa liitäntää. Kun liitäntä

laitetaan manuaalisesti takaisin toiminnalliseksi, niin SNMP-trap lähtee nyt muuttuneen reititystaulun mukaisesti ulos reitittimen R3 liitännästä Gigabit Ethernet 1/0. SNMP-trap ehtii lähteä siis tässäkin tapauksessa ennen kuin reititysprotokolla on kääntänyt liikenteen takaisin alkuperäiselle linkille, liitännän Gigabit Ethernet 0/0 kautta kohti reititintä R1. Tästä syystä nähdään Wireshark-pakettianalysaattorissa ainoastaan SNMP-trapeja ja Syslog-viestejä, kun liitännät palautetaan takaisin toiminnalliseen tilaan. [43.]

Ongelmaa ei luonnollisesti ole olemassa jos reitittimen R3 liitäntä Gigabit Ethernet 1/0 laitetaan ensin administratively down -tilaan, koska reittiä liitännän Gigabit Ethernet 0/0 kautta suositaan sen reititysarvon paremmuuden takia. Tämä johtuu siitä, että vaikka kaikki liitännät ovat nopeudeltaan samanarvoiset (1 Gbps), reitittimeltä R3 reitittimelle R1 reitittimen R2 kautta liikennöitäessä joudutaan kiertämään yhden ylimääräisen reitittimen kautta. Suora reitti reitittimeltä R3 reitittimelle R1 valitaan ensisijaisesti reititysprotokollan toimesta, vasta sen jälkeen käytetään vaihtoehtoisia reittejä.

Seuraavaksi on syytä etsiä ongelmaa OSPFv3-reititysprotokollan ajastimista. Reititysprotokollan ajastimilla määrätään, kuinka taajaan reititysmuutoksiin reagoidaan, eli kuinka usein jokainen reititin kyselee linkin toisessa päässä sijaitsevalta reitittimeltä sen tilaa ja reittitopologiaa. Jonkin liitännän epästabiilius yhdessä liian lyhyiksi konfiguroitujen ajastimien kanssa saattaa aiheuttaa runsaasti ylimääräistä reititysprotokollaan liittyvää liikennettä, ja reitittimillä SPF-algoritmin taajempaa laskentaa. Isommissa verkoissa SPF-algoritmin laskenta vaatii usein huomattavan paljon prosessorin laskentatehoa, ja saattaa täten heikentää reitittimen toimintaa muilla osa-aluille. Tätä on osaltaan pyritty estämään sillä, että OSPF-naapuruudet on perustettu stabiilien loopback-liitäntöjen välille, joten fyysisistä kaapeli- ja verkkokorttiongelmista aiheutuvat epästabiiliudet on saatu rajattua pois. Toisaalta liian pitkiksi konfiguroidut ajastimet saattavat aiheuttaa tässäkin työssä vastaantulleen ongelman, eli reititysprotokollalla kestää liian kauan päivittää reititystaulu vastaamaan todellista tilannetta. GNS3-virtuaaliympäristö ei osaa emuloida fyysisiä linkkejä niin hyvin, kuin se osaa emuloida fyysisiä verkkolaitteita. Reititykseen liittyvä ongelma saattaa liittyä siihen tai reititysprotokollan ajastimiin. Seuraavassa on esitetty komennot, joilla virtuaaliympäristön reitittimet konfiguroidaan reagoimaan nopeammin

tapahtuviin reititystopologian muutoksiin. Ensiksi on kuitenkin esitelty reitittimen R1 oletusarvot OSPF-ajastimille. [44.]

```
R1#show ipv6 ospf
 Routing Process "ospfv3 1" with ID 1.1.1.1
 Event-log enabled, Maximum number of events: 1000, Mode:
cyclic
 It is an autonomous system boundary router
 Originate Default Route
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x006580
 Number of areas in this router is 1. 1 normal 0 stub 0
nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        SPF algorithm executed 5942 times
        Number of LSA 16. Checksum Sum 0x069F34
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 1
```

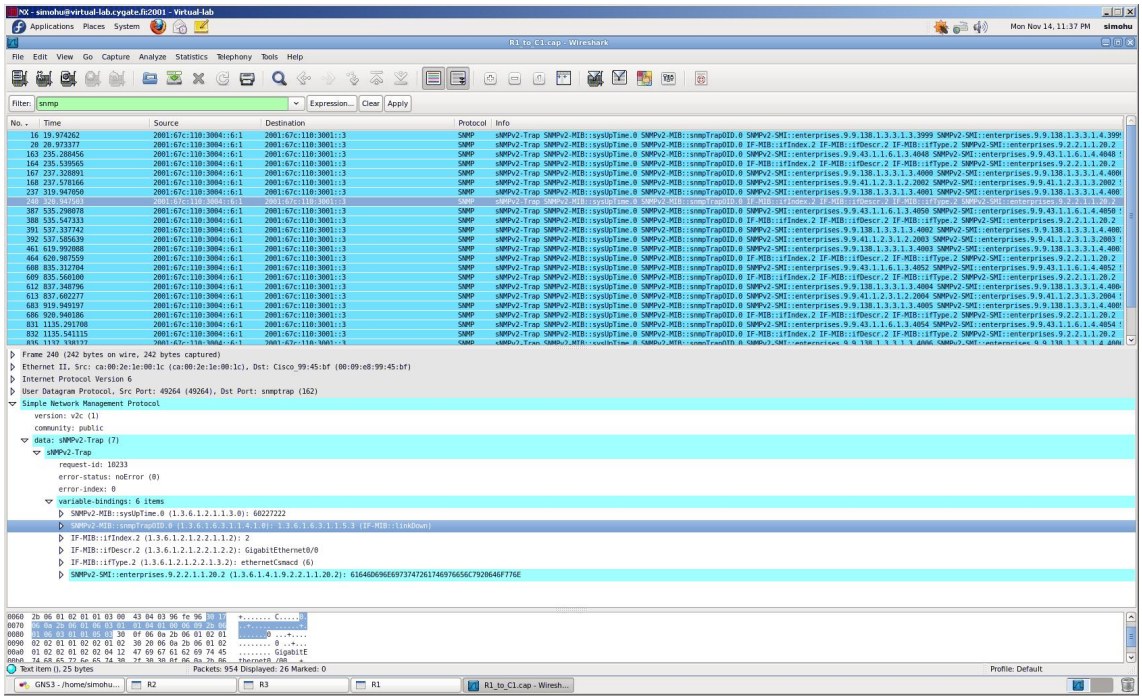
OSPF on niin sanottu Link State -protokolla. Verkkotopologia rakennetaan perustuen linkkien kesken lähetettäviin Link State -viesteihin (LSA, Link State Advertisement).

Konfiguroidaan virtuaaliympäristön jokaiselle reitittimelle seuraavat ajastimien (timers) arvot.

```
R3#show running-config | section router
ipv6 router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes detail
 timers throttle spf 200 200 200
 timers throttle lsa 300 300 300
 timers lsa arrival 300
 timers pacing lsa-group 300
 timers pacing flood 30
 timers pacing retransmission 100
```

Ratkaisevimmat arvot ovat komennoissa ”timers throttle spf” ja ”timers throttle lsa”. Oletusajastimien mukaan SPF-algoritmi (Shortest Path First) suoritetaan 5000

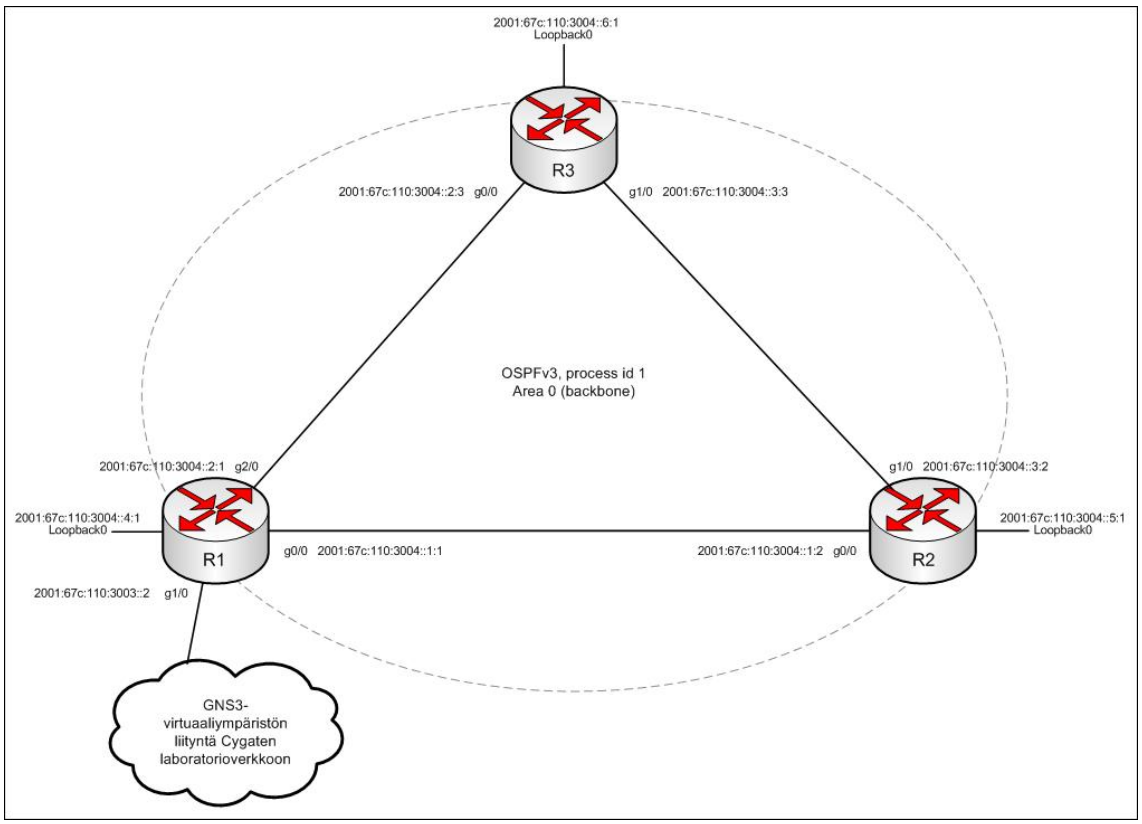
millisekunnin viiveellä, jotta mahdolliset lyhet katkokset linkissä eivät aina aiheuttaisi SPF-algoritmin uudelleenlaskentaa. Tämä on liian pitkä viive, koska kyseessä on virtuaaliympäristö, ja GNS3 käsittelee laitteiden välisiä linkkejä sovellustasolla eri prioriteetilla kuin simuloituja laitteita. Arvoksi on nyt muutettu SPF-algoritmin suorittamiselle 200 millisekuntia, ja Link State -viestit lähetetään 300 millisekunnin viiveellä SPF-algoritmin laskennasta. Tällä saavutetaan se, että OSPF ehtii päivittää reititystaulun ennen SNMP-trapin lähetystä. Näin ollen SNMP-trap lähtee nyt aina liitännästä, joka on toiminnallisessa tilassa. Tilanne voidaan todeta seuraavasta Wireshark-kuvakaappauksesta (kuva 13), jossa näkyy nyt siis myös SNMP-viestejä liitännän menosta toimimattomaan tilaan. Kuvassa näkyvät paketit on kaapattu reitittimen R1 liitännästä Gigabit Ethernet 1/0, ja testaustilanteessa reitittimen R3 liitäntä Gigabit Ethernet 0/0 on laitettu toimimattomaan tilaan ja takaisin toiminnalliseksi noin viiden minuutin välein. [44.]



Kuva 13. Wireshark-pakettianalysaattorin kaappaus SNMP-liikenteestä OSPFv3-reititysprotokollan laskurien hienosäädön jälkeen.

6 Testausten suunnittelu ja suorittaminen

6.1 Toteutunut testiympäristö



Kuva 14. Toteutunut verkkotopologia GNS3-virtuaaliympäristössä.

Kuva 14 on lopullinen toteutunut asiakkaan verkko GNS3-virtuaaliympäristössä. Kuvassa on esitetty myös liitännät sekä niiden osoitteet. Laitteita hallitaan (Ping, SNMP, Syslog, etäyhteydet) loopback0-liitäntöjen kautta. Reitittimen R1 lopullinen konfiguraatio löytyy liitteestä 2. Reitittimien R2 ja R3 konfiguraatiot ovat hyvin samankaltaisia reitittimen R1 kanssa, joten niiden konfiguraatiot on jätetty pois liitteistä.

6.2 Testitilanteiden suunnittelu

Työssä testataan yleisimpiä valvontamenetelmiä. Asiakasverkko koostuu reitittimistä ja niiden välisistä linkeistä, joten valvonta rajoittuu ainoastaan näihin mainittuihin kohteisiin. Reitittimien tavoitettavuutta voidaan valvoa ensisijaisesti Ping:llä, eli Smartwatcher lähettää ICMP echo -pyyntöjä reitittimien loopback0-liitäntöjen osoitteisiin tietyin väliajoin. Lisäksi Syslogilla ja SNMP:llä voidaan valvoa reitittimien

välisiä linkkejä ja OSPF-reititysprosessia. Seuraavassa kappaleessa on esitetty ratkaisu, jolla saadaan automaattisesti luotua ei-toivottuja tapahtumia linkeissä ja OSPF-reititysprosessissa. Tätä hyödynnetään testien suorittamisen yhteydessä, jotta saadaan tasaisesti lähetettyä Syslog- ja SNMP-viestejä Smartwatcherille. Näin vältytään siltä, että palvelimista vastaavat ja niiden lokitietoihin käsiksi pääsevät henkilöt eivät joudu odottamaan kun joku manuaalisesti laittaa esimerkiksi kahden reitittimen välisen linkin toimimattomaan tilaan (administratively down).

Cisco EEM (Embedded Event Manager) on Cisco IOS:ään sisäänrakennettu tapahtumien hallintaohjelmisto. Se on käytännössä skriptikieltä, jolla voidaan määrätä ehtoja ja näiden ehtojen täyttyessä suoritetaan jokin toiminto. Suoritettavalla toiminnolla voidaan muun muassa käynnistää reititin uudelleen, kun huomataan, että prosessorin ja muistin käyttöaste ovat ylittäneet tietyn raja-arvon. Reitittimelle R3 on konfiguroitu seuraavanlaiset kaksi EEM-skriptiä. Vastoin normaalia EEM:n käyttötarkoitusta tässä työssä halutaan tietyn ehdon täyttyessä laittaa reitittimen fyysinen liitäntä toimimattomaan tilaan ja takaisin toiminnalliseksi, jolloin saadaan automaattisesti generoitua hälytysdataa tasaisin väliajoin. [45; 46.]

```
 R3#show configuration | begin event
event manager applet FLAP-UP
 event timer watchdog time 300
 action 1.0 cli command "enable"
 action 2.0 cli command "conf t"
 action 3.0 cli command "interface g0/0"
 action 4.0 cli command "no shutdown"


event manager applet FLAP-DOWN
 event timer watchdog time 300
 action 1.0 cli command "enable"
 action 2.0 cli command "conf t"
 action 3.0 cli command "interface g0/0"
 action 4.0 cli command "shutdown"
```

Ensimmäinen FLAP-UP-niminen skripti laittaa fyysisen liitännän Gigabit Ethernet 0/0 “no shutdown” -tilaan, jolloin siis liitäntä on päällä ja toiminnallinen. Tapahtumalle on annettu ajastimeksi 300 sekuntia, eli 5 minuuttia, ja laskurin mennessä nollaan, sen alla olevat komennot suoritetaan laitteella. Komennot siis vastaavat täysin Cisco IOS:n komentoja. Toinen skripti on nimeltään FLAP-DOWN ja se on muuten vastaava FLAP-UP skriptin kanssa, mutta tässä tapauksessa skripti sammuttaa kyseisen liitännän. Näin saadaan aikaan se, että liitäntä Gigabit Ethernet 0/0 menee pois päältä, ja takaisin

päälle noin 5 minuutin välein, ja jokaisesta tällaisesta tapahtumasta lähetetään Syslog- sekä SNNP-viestit Smartwatcherille. Seuraava komento näyttää EEM-tapahtumien historian. [45; 46.]

```
R3#show event manager history events
No.  Job Id Proc Status   Time of Event            Event
Type         Name
1    466    Actv success  Tue Nov 8 18:54:32 2011  timer
watchdog     applet: FLAP-DOWN
2    467    Actv success  Tue Nov 8 18:58:09 2011  timer
watchdog     applet: FLAP-UP
3    468    Actv success  Tue Nov 8 18:59:32 2011  timer
watchdog     applet: FLAP-DOWN
4    469    Actv success  Tue Nov 8 19:03:09 2011  timer
watchdog     applet: FLAP-UP
```

Tulosteesta nähdään, että tapahtuman tyyppi on “watchdog” eli aikalaskuri, ja aikaleimoista nähdään tapahtumien vuorottelevan noin viiden minuutin välein.

6.3 Testien suoritus ja tulokset

6.3.1 Syslog-testit ja -tulokset

Syslog ei itsessään vaadi erityisiä muutoksia valvonta- ja hallinta-alustaan tukeakseen IPv6-tuetuilta laitteilta lähetettyjä Syslog-viestejä. Viestit ovat rakenteeltaan pitkiä merkkijonoja, ja ne kuljetetaan UDP:ta käyttäen, joka siis sijoittuu verkkotason (OSI-mallin kolmas kerros, IPv4 ja IPv6) päälle. Näin ollen Syslog-viestien perillemeno voidaan varmentaa seuraamalla Smartwatcherilla liikennettä kohdistuen UDP:n porttiin 514. [47.]

Seuraavassa on esitetty tcpdump-nimisellä Unix-työkalulla kaapattua Syslog-liikennettä Smartwatcherilla. Lähettävä laite on siis reititin R3 ja lähdeosoitteena laitteen loopback0-liitännän osoite. Wiresharkilla voidaan lisäksi tarkastella Syslog-viestien sisältöä. [48.]

```
16:24:46.846678 IP6 2001:67c:110:3004::6:1.57391 >
2001:67c:110:3001::3.syslog: SYSLOG local7.error, length:
96
16:24:46.848508 IP6 2001:67c:110:3004::6:1.57391 >
2001:67c:110:3001::3.syslog: SYSLOG local7.notice, length:
118
16:24:53.742902 IP6 2001:67c:110:3004::6:1.57391 >
2001:67c:110:3001::3.syslog: SYSLOG local7.notice, length:
128
```

Smartwatcherilla oli aluksi ongelmia Syslog-viestien vastaanotossa. Syslog-viestit lähtivät reitittimeltä oikein, mutta eivät koskaan tallentuneet Smartwatcherille. Syy oli yksinkertaisesti Linuxin ip6tables-niminen ohjelmallinen palomuuri, ja ratkaisu oli sallia sisään päin tulevat yhteydet Syslogille kyseisellä palomuurilla. Kyseessä on vastaava palomuuri, jota käytetään Linuxissa IPv4:n yhteydessä, mutta IPv6:lle on omat palomuurisääntönsä. Koska IPv6:ta ei ollut aiemmin käytetty tällä Smartwatcherilla, niin kyseisen IPv6-palomuurin säännöt eivät oletusarvoisesti sallineet Syslog-liikennettä. [49]

Lisäksi käytettävään Syslog-ng-taustaprosessiin tuli tehdä konfiguraatiomuutos IPv6-tuen päälle kytkemiseksi. Samassa Syslog-ng päivitettiin uusimpaan versioon (3.2). [50.]

6.3.2 SNMP-testit ja -tulokset

SNMP-testissä todettiin, että IPv6-muotoiset SNMP-trapit vastaanotetaan ja käsitellään Smartwatcherin toimesta ilman ongelmia. Testit kuitenkin osoittivat myös, että Smartwatcherin yrittäessä lukea laitteiden tietoja (GET) tapahtui kuljetuskerroksen (OSI-mallin neljäs kerros, tässä tapauksessa tarkemmin ottaen UDP) virhe, jonka syy ei ole toistaiseksi tiedossa. Kyseinen Smartwatcherilla käytössä oleva SNMP-kirjasto on oletusarvoisesti IPv6-tuettu, joten ongelmaa täytyy tutkia laajemmin. IPv6-tuen käyttöönotto vaatii palvelusta vastaavien asiantuntijoiden mukaan muutoksia lähdekoodiin. [51.]

SNMP-trapien käsittely Smartwatcherilla onnistuu ongelmitta. Alla ote vastaanotetusta SNMP-trapista reitittimeltä R3.

```
Customer CYGATEIPV6LAB
Node 2001:67c:110:3004:0:0:6:1
NodeAlias 2001:67c:110:3004:0:0:6:1
Summary Physical Entity Alarm Cleared (
ceAlarmHistEntPhysicalIndex = 30, ceAlarmHistAlarmType = 1
) Severity 1 AlertGroup Entity Alarm Type 2 Agent Cisco-
Entity Alarm Manager Smartwatcher trap probe on lab-ipv6-
wa1 AlertKey 30 Clazz 40057 Identifier
2001:67c:110:3004:0:0:6:1 30 Entity Alarm 2 Cisco-Entity
Alarm Smartwatcher trap probe on lab-ipv6-wa1 2 watcherid
CYGATEIPV6LAB(1451a4e7) alarmtype watcher_trap
```

Yllä näkyvän SNMP-trapin tietoja käytetään hallinta- ja valvonta-alustan Socket probe:lla hälytyksen jatkokäsittelyyn. [51.]

6.3.3 Ping-testit ja -tulokset

Ping-valvonta Smartwatcherilla toimii odotetulla tavalla. Smartwatcherilla tarvittu ainoa muutos on vaihtaa Ping-työkalun (fping) versio ICMPv6:ta tukevaan. [51; 52.]

6.4 Testitulosten dokumentointi

Taulukossa 5 on tiivistetty Smartwatcherin valvontamenetelmien (Syslog, SNMP, Ping) testitilanteet, ja kuvattu tarvittavat jatkotoimenpiteet.

Taulukko 5. Hallinta- ja valvonta-alustan testien lopputulokset tiivistettynä.

Valvonta- tai hallintamenetelmä	Selite
Ping	Toiminta testattu. Todettu toimivaksi. Ei jatkotoimenpiteitä tässä vaiheessa.
Syslog	Toiminta testattu. Todettu toimivaksi. Ei jatkotoimenpiteitä tässä vaiheessa.
SNMP	SNMP-trap ja SNMP-get testattu. SNMP-trap todettu toimivaksi. Ei jatkotoimenpiteitä tässä vaiheessa. Tietojen lukeminen laitteella SNMP:llä (GET) ei toimi. Vaatii lisätutkimuksia Smartwatcherilla.

7 Johtopäätökset

7.1 Tuotantoonoton aikataulu

IPv6-pohjainen verkon hallinta- ja valvontapalvelu ei tällä hetkellä ole vielä valmis tuotantoympäristöön. Ongelmat on dokumentoitu, ja ne on ratkaistavissa. Palvelu on mahdollista ottaa aluksi testikäyttöön muun muassa hallintaverkon puolella, jotta pystytään mahdollisimman hyvin todeta palvelun puutteet ja muutoskohteet aidossa verkkoympäristössä. Virtuaalinen ympäristö ei takaa aivan täyttä näkyvyyttä, koska verkkolaitteiden valmistajien ja eri mallien kirjo ei ole virtuaaliympäristössä tarpeeksi kattava. Ennen palvelun testausta esimerkiksi hallintaverkon puolella on muun muassa ratkaista SNMP:hen liittyvät ongelmat, koska se on näistä kolmesta aiemmin luetellusta

valvonta- ja hallinta-menetelmästä kaikista merkittävin. Työn kirjoitushetkellä ei ole täysin varmaa tietoa tuotantoon siirtymisen aikataulusta, koska välitöntä tarvetta ei vielä toistaiseksi ole olemassa. Tulosten perusteella voidaan kuitenkin arvioida, että myös SNMP on mahdollista saada lukemaan IPv6:en pohjautuvia MIB:ejä hyvinkin lyhyellä aikataululla.

IPv6-verkonvalvonnan ja -hallintapalvelun täysimittainen tuotantoon siirto edellyttää tarvetta asiakkaan suunnalta, joka tulee esille vasta sitten kun IPv4:n rajoittuvuudet alkavat huomattavasti heikentää yritysten tietoverkkojen tehokkuutta ja kun tämä vähentynyt tehokkuus heijastuu suoraan menetettyihin voittoihin. Tämä sama ilmiö koskee tällä hetkellä koko IPv6-verkkoinfrastruktuuria. Siihen siirtymiseen ei ole välitöntä tarvetta, mutta tarpeeseen on vastattava lyhyellä viiveellä sitten, kun huomataan, että IPv4:n rajoittuvuuksista aiheutuneet haitat ovat merkittävämmät kuin IPv6:en siirtymisestä aiheutuvat lisäkustannukset.

7.2 Tulosten käsittely tavoitteen näkökulmasta

Työlle asetettu tavoite on saavutettu, koska työssä on onnistuttu tietyin rajoituksin toteuttamaan ja kuvaamaan toimiva verkonvalvonta- ja hallintapalvelu IPv6-ympäristössä. Nämä edellä mainitut rajoitukset ovat avainasemassa tässä työssä ja niiden ratkaiseminen muodostaa seuraavan kehitysvaiheen projektissa. Suurin osa työpanoksesta painottui valvontamenetelmien toiminnallisuuksien tutkimiseen IPv6-ympäristössä, joten työ antaa hyvän pohjan projektin seuraavalle vaiheelle. Ympäristö voidaan milloin tahansa toteuttaa alusta asti uudestaan, koska suurin osa kokonaisuudesta on toteutettu avoimesti saatavilla olevista virtuaalisista komponeista, ja muun muassa tässä työssä käsiteltyyn reititysprotokollan toimintaan verkonvalvonnan ja -hallinnan kannalta on käytetty huomattavan paljon aikaa, jotta itse verkonvalvonnan ja -hallinnan ydintoiminnoille on saatu mahdollisimman varma ja hyvin dokumentoitu perusta. IPv6-muotoisen hälytystiedon, statistiikan ja raportoinnin käsittely hallinta-alustassa vaatii kuitenkin vielä paljon selvitystyötä, ja on selvää, että näihin tullaan tekemään muutoksia jatkotutkimusten pohjalta, jotta koko verkonvalvontapalvelun ydin, valvonta- ja hallinta-alusta, voidaan kokonaan ja luotettavasti siirtää mahdollisimman valmiina tuotantoon. Työssä on kuitenkin onnistuttu osoittamaan, että asiakasverkkoon, ja siihen sijoitettavaan Smartwatcheriin ei tarvitse tehdä erityisen vaativia tai mittavia muutoksia.

7.3 Yhteenveto

Työn tavoitteet saavutettiin alkuperäisten suunnitelmien mukaisesti. Valvonta- ja hallinta-palvelun siirto IPv6-tuettuun tuotantoverkkoon ei ole vielä suositeltavaa. Työssä saatiin kuitenkin selvitettyä merkittävimmät ongelmakohdat. Työ osoittaa myös, että IPv6:n, laboratorioverkon ja virtuaaliympäristön yhteistoiminnassakin kohdattiin ennalta odottamattomia tilanteita. Nämä seikat tulee ottaa huomioon myös jatkoprojekteissa, jotta vältytään mahdollisilta suuremmilta yllätyksiltä tuotantoon siirron aikana. Työssä kohdatut verkkotason ongelmat saatiin ratkaistua työn kirjoituksen aikana, mutta hallinta-alustan ohjelmistokomponenttien monimutkaisuuden takia niiden tutkiminen ja muutosten suunnittelu ottaa oman aikansa. Niihin myös tarvitaan enemmän kyseiseen järjestelmään paneutuneiden asiantuntijoiden työpanosta. Kokonaisvaltainen IPv6-projekti, johon tämäkin työ tullaan sisällyttämään, käynnistänee lähitulevaisuudessa projektin, joka käsittelee ja pyrkii ratkaisemaan tässä työssä havaittuja ongelmakohtia.

Lähteet

1 Yritys. Verkkodokumentti. Cygate Oy. <http://www.cygategroup.com/cy_templates/Page.aspx?id=304>. Luettu 8.11.2011.

2 Popoviciu, Ciprian, CCIE. 2006. Deploying IPv6 Networks. Cisco Press.

3 Why Use Network Management. Verkkodokumentti. Infocollections Learning. <http://learning.infocollections.com/ebook%202/Computer/Networking/Network%20Design%20&%20Architecture/Network.Management.MIBs.and.MPLS/0131011138_ch01lev1sec2.html>. Luettu 8.11.2011.

4 Kahani Moshen. Network Management. Principles and Protocols. Verkkodokumentti (PowerPoint-esitys). Ferdowsi University of Mashhad. <http://www.google.fi/url?sa=t&rct=j&q=network%20management%20principles&source=web&cd=2&ved=0CEoQFjAB&url=http%3A%2F%2Fprofsite.um.ac.ir%2F~kahani%2Fppt%2Fnetworkman.ppt&ei=AYa5TpT5N-j-4QScp72vCA&usg=AFQjCNHGLRJJSepQjSBdAoomItWGQoq7yw>. Luettu 8.11.2011.

5 Aidarous Salah. Principles of Network Management. Verkkodokumentti (PDF). <http://www.google.fi/url?sa=t&rct=j&q=network%20management%20principles&source=web&cd=1&ved=0CEEQFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.125.3183%26rep%3Drep1%26type%3Dpdf&ei=AYa5TpT5N-j-4QScp72vCA&usg=AFQjCNFNQIRWBTqkmOUxXOFcEEVF3Zps1w>. Luettu 8.11.2011.

6 McFarland, Shannon, CCIE. 2011. IPv6 for Enterprise Networks. Cisco Press.

7 Internet Control Message Protocol. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol>. Luettu 3.11.2011.

8 Ping. Verkkodokumentti. Wikipedia. < http://en.wikipedia.org/wiki/Ping>. Luettu 3.11.2011.

9 OSI-model. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/OSI_model>. Luettu 3.11.2011.

10 RFC 792 (Internet Control Message Protocol). Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc792>. Luettu 3.11.2011.

11 SNMP. Verkkodokumentti. Javvin Network Management and Security. <http://www.javvin.com/protocolSNMP.html>. Luettu 3.11.2011.

12 SNMP messages. Verkkodokumentti. Tech-Faq. <http://www.tech-faq.com/snmp.html>. Luettu 3.11.2011.

13 Syslog. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/tech/tk648/tk362/tk790/tsd_technology_support_sub-protocol_home.html>. Luettu 4.11.2011.

14 RFC 5242. The Syslog Protocol. Verkkodokumentti. RFC-Editor. <http://www.rfc-editor.org/rfc/rfc5424.txt>. Luettu 14.11.2011.

15 Hyvönen, Timo. 2011. Cygate Oy Management and Monitoring Connection Build-out Principles. Cygate Oy.

16 Toivanen, Heikki. 2011. Hallintajärjestelmät, Cygate Oy, Espoo. Keskustelu 19.5.2011.

17 Jakobsson, Jussi. 2011. Hallintajärjestelmät, Cygate Oy, Espoo. Keskustelu 19.5.2011.

18 Request For Comments. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Request_for_Comments>. Luettu 2.11.2011.

19 IPsec. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/IPsec>. Luettu 2.11.2011.

20 Harjunen, Timo. 2011. Hallintajärjestelmät, Cygate Oy, Espoo. Keskustelu 31.10.2011.

21 IPv4 address report. Verkkodokumentti. Potaroo.net. <http://www.potaroo.net/tools/ipv4/index.html>. Luettu 21.8.2011.

22 Raittinen, Tomi. 2010. Transition to IPv6. Opinnäytetyö. Metropolia Ammattikorkeakoulu.

23 Graphical Network Simulator. Verkkodokumentti. GNS 3. <http://www.gns3.net>. Luettu 20.5.2011.

24 Introduction to Wireshark network packet analyzer. Verkkodokumentti. Wireshark. <http://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs>. Luettu 20.5.2011.

25 IPv6 Dual IP Stack Implementation. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/IPv6#Dual_IP_stack_implementation>. Luettu 25.10.2011.

26 Regional Internet Registries. Verkkodokumentti. RIPE NCC. <http://www.ripe.net>. Luettu 9.11.2011.

27 EUI-64. Verkkodokumentti. Tekkom. <http://mars.tekkom.dk/mediawiki/index.php/EUI-64>. Luettu 9.11.2011.

28 Hurttila, Simo. 2011. IPv6-osoitetaulukko. Liite 1.

29 Variable Lengt Subnet Masking. Verkkodokumentti. TCP IP Guide. <http://www.tcpipguide.com/free/t_IPVariableLengthSubnetMaskingVLSM.htm>. Luettu 18.10.2011.

30 Implementin Cisco IPv6 Networks. Verkkodokumentti. Cisco Press. <http://www.ciscopress.com/articles/article.asp?p=31948&seqNum=4>. Luettu 8.11.2011.

31 Hurttila, Simo. 2009-2010. Cisco CCNA- ja CCNP-kurssimuistiinpanot. Metropolia Ammattikorkeakoulu.

32 Jakobsson, Jussi. 2011. Hallintajärjestelmät, Cygate Oy, Espoo. Keskustelu 4.11.2011.

33 Vyatta Network OS. Verkkodokumentti. PDF. Vyatta. <http://www.vyatta.com/sites/vyatta.com/files/pdfs/vyatta_software_datasheet.pdf>. Luettu 7.11.2011.

34 Implementin OSPF for IPv6. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf_ps6922_TSD_Products_Configuration_Guide_Chapter.html#wp1087678>. Luettu 18.10.2011.

35 Sample Configuration for OSPFv3. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/tech/tk872/technologies_configuration_example09186a0080b40d8a.shtml>. Luettu 26.10.2011.

36 Pepelnjak, Ivan, CCIE. Blogi. Verkkodokumentti. NIL Data Communications. <http://blog.ioshints.info/2008/04/ipv4-forever.html>. Luettu 3.11.2011

37 OSPF – Frequently Asked Questions. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/tech/tk365/technologies_q_and_a_item09186a0080094704.shtml#q36>. Luettu 3.11.2011.

38 OSPF Design Guide. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml>. Luettu 3.11.2011.

39 OSPF Backbone Area. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Open_Shortest_Path_First#Backbone_area>. Luettu 29.10.2011.

40 SNMP. Verkkodokumentti. Tech-faq. <http://www.tech-faq.com/snmp.html>. Luettu 3.11.2011.

41 IOS SNMP Traps Supported and How to Configure Them. Cisco. Verkkodokumentti. <http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a05.shtml>. Luettu 3.11.2011.

42 Rautanen, Jaakko. 2011. Asiantuntijapalvelut, Cygate Oy, Espoo. Keskustelu 19.11.2011.

43 User Datagram Protocol. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/User_Datagram_Protocol>. Luettu 10.11.2011.

44 Tuning LSA and SPF Timers for OSPFv3 Fast Convergence. Cisco. Verkkodokumentti. <http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1112761>. Luettu 15.11.2011.

45 Cisco IOS Embedded Event Manager. Verkkodokumentti. Expert Study Notes. <http://expertstudynotes.com/index.php?title=Cisco_IOS_Embedded_Event_Manager>. Luettu 7.11.2011.

46 Embedded Event Manager Overview. Verkkodokumentti. Cisco. <http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview_ps6441_TSD_Products_Configuration_Guide_Chapter.html>. Luettu 7.11.2011.

47 Logging via Syslog. Verkkodokumentti. Practically Networked. <http://www.practicallynetworked.com/support/syslog.htm>. Luettu 14.11.2011.

48 Tcpdump manual pages. Verkkodokumentti. Tcpdump. <http://www.tcpdump.org/tcpdump_man.html>. Luettu 14.11.2011.

49 IPv6 Firewall for Linux. Verkkodokumentti. Cyberciti. <http://www.cyberciti.biz/faq/ip6tables-ipv6-firewall-for-linux/>. Luettu 14.11.2011.

50 Syslog-ng. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Syslog-ng>. Luettu 14.11.2011.

51 Jakobsson, Jussi. 2011. Hallintajärjestelmät, Cygate Oy, Espoo. Keskustelu 14.11.2011.

52 Fping6. Verkkodokumentti. Linux.die.net. <http://linux.die.net/man/8/fping6>. Luettu 14.11.2011.

53 RFC 4291. IP Version 6 Addressing Architecture. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc4291>. Luettu 17.11.2011.

54 RFC 4193. Unique Local IPv6 Unicast Addresses. Verkkodokumentti. IETF. <http://tools.ietf.org/html/rfc4193>. Luettu 17.11.2011.

IPv6-osoitetaulukko

/64 verkot	Mahdollinen aliverkotus	Host-osoitteet	Kuvaus
2001:67c:110:3003::/64			**Virtual-labbing environment**
		2001:67c:110:3003::1	Swi vlan 500
		2001:67c:110:3003::2	Virtual router - gw to virtual lab inside GNS3, Gigabit Ethernet 1/0 on R1
2001:67c:110:3004::/64			**Virtual-labbing environment2**
	2001:67c:110:3004:0:0:0:0/112	Free	
	2001:67c:110:3004:0:0:1:0/112		**R1 <-> R2 link**
		2001:67c:110:3004::1:1	Interface Gigabit Ethernet 0/0 on R1
		2001:67c:110:3004::1:2	Interface Gigabit Ethernet 0/0 on R2
	2001:67c:110:3004:0:0:2:0/112		**R1 <-> R3 link**
		2001:67c:110:3004::2:1	Interface Gigabit Ethernet 2/0 on R1
		2001:67c:110:3004::2:3	Interface Gigabit Ethernet 0/0 on R3
	2001:67c:110:3004:0:0:3:0/112		**R2 <-> R3 link**
		2001:67c:110:3004::3:2	Interface Gigabit Ethernet 1/0 on R2
		2001:67c:110:3004::3:3	Interface Gigabit Ethernet 1/0 on R3
	2001:67c:110:3004:0:0:4:0/112		**R1 Loopback**
		2001:67c:110:3004::4:1	Interface loopback 0
	2001:67c:110:3004:0:0:5:0/112		**R2 Loopback**
		2001:67c:110:3004::5:1	Interface loopback 0
	2001:67c:110:3004:0:0:6:0/112		**R3 Loopback**
		2001:67c:110:3004::6:1	Interface loopback 0
	2001:67c:110:3004:0:0:7:0/112	Free	
	2001:67c:110:3004:0:0:8:0/112	Free	
	2001:67c:110:3004:0:0:9:0/112	Free	
	2001:67c:110:3004:0:0:a:0/112	Free	
	2001:67c:110:3004:0:0:b:0/112	Free	

Reitittimen R1 konfiguraatio

```
! Last configuration change at 21:18:36 UTC Mon Nov 14 2011
upgrade fpd auto
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip source-route
no ip routing
no ip cef
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
redundancy
!
interface Loopback0
 no ip address
 ipv6 address 2001:67C:110:3004::4:1/112
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Ethernet0/0
 no ip address
 no ip route-cache
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 no ip address
 no ip route-cache
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 ipv6 address 2001:67C:110:3004::1:1/112
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet1/0
 no ip address
 no ip route-cache
 negotiation auto
 ipv6 address 2001:67C:110:3003::2/64
```

```
 ipv6 enable
!
interface GigabitEthernet2/0
 no ip address
 no ip route-cache
 negotiation auto
 ipv6 address 2001:67C:110:3004::2:1/112
 ipv6 enable
 ipv6 ospf 1 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ipv6 route ::/0 GigabitEthernet1/0 2001:67C:110:3003::1
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes detail
 default-information originate
 passive-interface GigabitEthernet1/0
 timers throttle spf 200 200 200
 timers throttle lsa 300 300 300
 timers lsa arrival 300
 timers pacing lsa-group 300
 timers pacing flood 30
 timers pacing retransmission 100
!
snmp-server community public RW
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown
linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps flowmon
snmp-server enable traps ds1
snmp-server enable traps call-home message-send-fail
server-fail
snmp-server enable traps tty
snmp-server enable traps gatekeeper
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change
nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change
shamlink interface
snmp-server enable traps ospf cisco-specific state-change
shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps xgcp
snmp-server enable traps ethernet cfm cc mep-up mep-down
cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-
missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps srp
```

```
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ima
snmp-server enable traps diameter
snmp-server enable traps channel
snmp-server enable traps ip local pool
snmp-server enable traps rf
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps bfd
snmp-server enable traps bgp
snmp-server enable traps bstun
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps cef resource-failure peer-state-
change peer-fib-state-change inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dial
snmp-server enable traps dlsw
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps frame-relay multilink bundle-
mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmobile
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-
change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps stun
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
```

```
snmp-server enable traps pw vc
snmp-server enable traps event-manager
snmp-server enable traps firewall serverstatus
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps alarms informational
snmp-server enable traps ccme
snmp-server enable traps srst
snmp-server enable traps mpls vpn
snmp-server enable traps voice
snmp-server enable traps dnis
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-
up vnet-trunk-down
snmp-server host 2001:67C:110:3001::3 version 2c public
!
control-plane
!
mgcp profile default
!
gatekeeper
 shutdown
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
 transport input all
!
end
```