Suvi Kemppainen

Runkoverkon monitorointi ilmaisohjelmalla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

2.5.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Suvi Kemppainen Runkoverkon monitorointi ilmaisohjelmalla 68 sivua + 25 liitettä 2.5.2014
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Tietoverkkojen suuntautumisvaihtoehto
Ohjaaja(t)	Lehtori Marko Uusitalo

Insinöörityön tavoitteena oli monitoroida Metropolia Ammattikorkeakoulun Helsingin toimipisteen tietoverkkolaboratorion opetusrunkoverkkoa käyttötarkoitukseen parhaiten soveltuvalla ilmaisohjelmalla. Päätettyjen valintakriteereiden mukaan ohjelman tuli tuottaa hälytyksiä ja ilmoituksia erilaisin laukaisutekijöin, havaita verkkolaitteet automaattisesti ja luoda niistä looginen ryhmittely, käyttää hyväksi SNMP-, Syslog- ja NetFlow-protokollia sekä tuottaa keräämästään aineistosta selkeitä raportteja. Vertailun ulkopuolelle jätettiin ilmaiseksi käytettävät, useammasta erityisohjelmasta koostuvat ohjelmapaketit.

Ohjelmavertailuun valittiin lopulta seitsemän kriteerit täyttävää ilmaisohjelmaa. Ohjelmat asennettiin yksitellen testikoneelle ohjelman kokeilemiseksi. Valinta suoritettiin vertailemalla ohjelmien asennus- ja käyttökokemusta, ominaisuuksia ja rajoituksia, skaalautuvuutta ja monitoroinnin laajennuskustannuksia. Vertailun perusteella opetusrunkoverkon monitorointiin valittiin op5 Monitor -ohjelma.

Runkoverkon monitorointi toteutettiin asentamalla Metropolian verkossa olevalle palvelimelle op5 Monitor ja konfiguroimalla runkoverkon reitittimet ja kytkimet lähettämään sekä SNMP- että NetFlow-tietoa. op5 Monitor konfiguroitiin havaitsemaan verkkolaitteet ja niiden lähettämä SNMP-tieto. Ohjelman piti pystyä vastaanottamaan NetFlow-tietoa automaattisesti.

op5 Monitor monitoroi opetusrunkoverkkoa kahden viikon ajan, minkä jälkeen kerätty tieto ja ohjelman toiminta tarkistettiin. Ohjelma oli onnistuneesti monitoroinut verkkolaitteiden rajapintoja ja tietoliikenteen määrää, mutta NetFlow-tiedolle ei löydetty raportteja tai konfiguroitavia komentoja.

op5 Monitorin todettiin olevan vasta-alkajalle hankalakäyttöinen ja epäonnistunut valinta NetFlow-tiedon monitorointiin, mutta ohjelmassa oli muuten laajat, muokattavat monitorointimahdollisuudet, joita Metropolia pystyisi halutessaan hyödyntämään opetusrunkoverkkonsa monitoroinnissa ohjelmaan ja Linux-käyttöjärjestelmään syvemmin perehtyneen verkonvalvojan johdolla.

Avainsanat	juniper, monitorointi, ilmaisohjelma, runkoverkko, cisco

Author(s) Title Number of Pages Date	Suvi Kemppainen Monitoring a Backbone Network Using Free-of-Charge Software 68 pages + 25 appendices 2 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Marko Uusitalo, Senior Lecturer

The purpose of this graduate study was to monitor the teaching backbone network of the network laboratory in Metropolia University of Applied Sciences' Helsinki branch with free-of-charge software that would best suit the school's monitoring needs. By the chosen criteria, the aim was to find a program that would be able to perform a number of tasks, i.e. use varying triggers to produce alerts, automatically discover network devices and group them together logically, use SNMP, Syslog and NetFlow protocols, and produce reports of the data collected. Free-of-charge software consisting of various smaller programs was disregarded.

Seven programs that fit the criteria were finally selected for software comparison. The programs were installed on a test computer one by one to try out the program. The choice was made by comparing how easy it was to install and use a program, what the program's features, limitations and scalability were, and how much additional device monitoring would cost. Based on the comparison, the software chosen for the installation was op5 Monitor.

The monitoring of the backbone network was implemented by installing op5 Monitor on a server in Metropolia's teaching backbone network. Routers and switches in the backbone network were configured to send SNMP and NetFlow data to the program. op5 Monitor was configured to discover the devices and receive the SNMP data sent by them. In addition, op5 Monitor would supposedly automatically receive NetFlow information.

op5 Monitor monitored the backbone network for two weeks after which the data collected and the functionality of the program were checked. The program had been successful in monitoring the interfaces and the amount of data that had passed through them, but no reports or commands could be found or configured for the NetFlow data.

The results indicate that op5 Monitor is too complicated for a beginner and a poor choice to monitor NetFlow data but otherwise its range of customizable monitoring options could be utilized by Metropolia in monitoring its teaching backbone network with the help of a network administrator better versed in Linux and op5 Monitor.

Keywords	juniper, backbone, network, free-of-charge, monitoring, cisco

Sisällys

Lyhenteet

AD	*Active Directory.* Microsoftin Windows-käyttöjärjestelmän komponentti, jolla suoritetaan käyttäjähallintaa ja todennusta.
API	*Application Programming Interface.* Ohjelmointirajapinta. Protokollien, työkalujen ja aliohjelmien joukko, joka määrittelee, miten ohjelmat vaihtavat tietoa keskenään.
BIOS	*Basic Input/Output System.* Tietokoneohjelma, joka esimerkiksi lataa käyttöjärjestelmän tietokoneen käynnistyessä.
BMC	*Baseboard Management Controller.* Tietokoneen emolevyssä oleva mikrokontrolleri, joka hallitsee rajapintaa järjestelmänhallintasovelluksen ja tietokonelaitteiston välillä.
BYOD	*Bring-your-own-device*. Teknologia, joka sallii työntekijöiden henkilökohtaisten IT-laitteiden käytön yritysverkossa.
CIM	*Common Information Model.* Tapa määritellä järjestelmien, tietoverkkojen, applikaatioiden ja palvelinten hallintatietoja.
DHCP	*Dynamic Host Control Protocol.* Protokolla, joka jakaa IP-osoitteita niitä tarvitseville verkkolaitteille määritellyistä IP-osoiteryhmistä.
DNS	*Domain Name System.* Nimipalvelujärjestelmä. Tietokanta, jonka avulla Internetin verkkotunnukset muunnetaan IP-osoitteiksi.
FTP	*File Transfer Protocol.* Protokolla, jolla voidaan lähettää tiedostoja Internetissä olevien tietokoneiden välillä.
HTTP	*Hypertext Transfer Protocol.* Protokolla, joka määrittää viestien formatointitavan ja lähetystavan sekä miten Web-palvelimet ja selaimet reagoivat eri komentoihin Internetissä.
ICMP	*Internet Control Message Protocol.* Protokolla, jota käytetään Internet-kyselyjen ja -virheviestien lähetykseen

IETF	*Internet Engineering Task Force.* Internet-protokollien standardointiorganisaatio.
IP	*Internet Protocol.* Protokolla, jonka avulla tietoliikennepaketit kuljetetaan vastaanottajalle Internetissä.
IPFIX	*IP Flow Information Export*. Protokolla, jolla reitittimeltä voidaan viedä informaatiota tietoliikennepaketteja sisältävistä verkkoliikennevoista tietoa keräävälle laitteille ja hallintajärjestelmille.
IPMI	*Intelligent Platform Management Interface.* Palvelimen tietokonelaitteiston kunnon etämonitorointi- ja etähallintajärjestelmä.
IPTV	*Internet Protocol TV*. Tekniikka, jolla televisio-ohjelma siirretään digitaalisessa muodossa paketteina IP-protokollaa käyttävän verkon yli.
LAN	*Local Area Network*. Lähiverkko. Tietoverkko, joka kattaa pienen alueen, esimerkiksi yhden rakennuksen alan.
MIB	*Management Information Base.* SNMP-protokollan käyttämä tietokanta, joka hallitsee laiteinformaation sisältäviä tietoverkkokokonaisuuksia
MX	*Mail Exchanger.* DNS:n rekisteri, jolta sähköpostipalvelimet saavat tarvittavat tiedot sähköpostin välittämiseen vastaanottajan sähköpostipalvelimelle.
OID	*Object Identifier.* Kansainvälinen verkkolaitteen yksilöintitunnus.
QoS	*Quality of Service*. Palvelunlaatu. Erityisesti käyttäjien hahmottama puhelin- tai tietoverkon suorituskyky.
RAM	*Random Access Memory.* Tietokoneen keskusmuisti. RAM-muistissa ovat tietokoneella kullakin hetkellä suoritettavat sovellukset sekä sovellusten tarvitsemat tiedot.

SIP *Session Initiation Protocol.* Protokolla, jota käytetään istuntojen luomiseen, muokkaamiseen ja päättämiseen. Istunto on yhteys protokollaan tai yhteys käyttäjän tai käyttäjän selaimen ja palvelimen välillä.

SNMP *Simple Network Management Protocol.* Protokolla, jota käytetään verkkolaitteiden automaattiseen havaitsemiseen.

SSH *Secure Socket Shell.* Teknologia, jota käytetään turvalliseen etäkirjautumiseen.

SSL *Secure Sockets Layer.* Salausprotokolla, jota käytetään turvaamaan Internetin yli tapahtuva viestintä.

SVC *Service.* DNS:n rekisteri, jolta Microsoft Active Directory saa tiedot verkkopalvelujen paikallistamiseen.

TCP *Transfer Control Protocol.* Protokolla, jonka avulla asiakasohjelmat voivat muodostaa luotettavan yhteyden verkon yli ja vaihtaa keskenään informaatiota.

TLS *Transport Layer Security.* Salausprotokolla, jota käytetään turvaamaan Internetin yli tapahtuva viestintä. TLS on SSL-protokollaan perustuva SSL-protokollaa turvallisempi protokolla.

UDP *User Datagram Protocol.* Protokolla, jonka avulla asiakasohjelmat voivat vaihtaa keskenään informaatiota.

UNIX UNIX-käyttöjärjestelmä.

VoIP *Voice over Internet Protocol*. IP-puhe. Tekniikka, jolla puhe muutetaan digitaaliseen muotoon ja siirretään paketteina reaaliaikaisesti IP-protokollaa käyttävän verkon yli.

VPN *Virtual Private Network*. Virtuaalinen erillisverkko. Tapa, jolla useita yrityksen tietoverkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen tietoverkon. Myös työaseman liittämistä yrityksen verkkoon etäyhteyden kautta kutsutaan VPN:ksi.

WAN *Wide Area Network*. Laajaverkko. Tietoverkko, joka toimii laajalla, esimerkiksi usean kaupungin kattavalla, alueella.

WMI *Windows Management Instrumentation.* Windows-käyttöjärjestelmässä toimiva ohjelmointirajapinta, joka mahdollistaa verkkolaitteiden ja verkossa olevien järjestelmien hallitsemisen.

WWW *World Wide Web.* Internetissä toimiva Web-sivujen eli dokumenttien linkkejä sisältävä järjestelmä, jota luetaan selaimella.

1 Johdanto

Metropolia Ammattikorkeakoulu on vuodesta 2008 pääkaupunkiseudulla toiminut hakijamäärältään suurin ammattikorkeakoulu Suomessa. Metropolialla on toimipisteitä Espoossa, Helsingissä ja Vantaalla. Metropoliassa voi opiskella kulttuuria, liiketaloutta, sosiaali- ja terveysalaa sekä tekniikkaa. Tässä insinöörityössä käsitellään Metropolian Helsingin toimipisteen opetusrunkoverkon monitorointia. Työ toteutetaan tietotekniikan koulutusohjelman opetuskäytössä olevassa tietoverkkolaboratoriossa, joka sijaitsee Metropolian Bulevardin toimipisteessä Helsingissä.

Tämän insinöörityön tavoitteena on vertailla olemassa olevia verkon monitorointiin tarkoitettuja ilmaisohjelmia, valita näistä Metropolia Ammattikorkeakoulun kannalta monitorointiin parhaiten soveltuva ohjelma ja toteuttaa alustava opetusrunkoverkon monitorointi. Työssä on tarkoitus monitoroida Metropolian verkkoliikennettä opetusrunkoverkossa sekä opetusrunkoverkon ja tietoverkkolaboratorion välillä.

2 Verkon monitorointi

Verkon monitorointi tarkoittaa tietoverkon tarkkailua verkon sisäisten muutosten havaitsemiseksi. Se on osa verkon hallintaa, mutta rajoittuu tarkkailuun, vikojen havaitsemiseen ja raportointiin eikä itsessään niiden korjaamiseen tai tietoturvaan. Monitorointi voidaan toteuttaa eri käyttöjärjestelmillä ja laitteilla yksittäisten komentojen tai monitorointiohjelmiston avulla tai monitorointiohjelmiston ja avustavan laitteiston yhdistelmällä. Verkon monitorointiin on käytettävissä maksullisia ohjelmia ja räätälöityjä palveluja, mutta myös avoimen lähdekoodin (open source) ilmaisohjelmia, kaupallisten ohjelmien ilmaisversioita sekä ilmaistyökaluja löytyy useita. [1.] Tässä työssä keskitymme verkon monitorointiin ilmaisohjelmien avulla.

2.1 Tärkeys

Verkkoa monitoroimalla voidaan havaita tietoverkossa piilevät ongelmat, kuten hitaus, tietojen katoaminen tai muu verkon epäoptimaalinen toimivuus. Monitoroinnilla voidaan havaita myös mahdolliset säästökohteet, kuten tarpeettoman suuri määrä verkkolaittei-

ta. Muita havaittavia asioita ovat muun muassa palveluntoimittajien kanssa sovittujen vasteaikojen toteutuminen, palvelunlaatu (QoS, quality of service), ylikuormitetut laitteet ja yhteydet tai tietoturvauhkiin viittaava epäilyttävä tietoliikenne. Näiden taustalla ovat usein jonkun verkon osan tai laitteen vikatila, verkon huono suunnittelu tai tahattomat ja tahalliset käyttäjätoimet. [1.]

Verkon ympärivuorokautinen monitorointi on tärkeää verkon toiminnan ja saatavuuden säilyttämiseksi ja sen suorituskyvyn parantamiseksi. Tarkkailun alla ovat yleensä kaistan käyttö, tietoliikenneyhteyksien toimivuus sekä ohjelmien ja palvelinten suorituskyky ja saatavuus. Tietoverkossa oleva hitaus tai vika ei aiheuta ongelmia vain tietoverkossa itsessään, vaan se vaikuttaa loppukäyttäjien tyytyväisyyteen ja työtehokkuuteen ja täten yrityksen tehokkuuteen, tulokseen ja maineeseen negatiivisesti. [1; 2.]

2.2 Toiminta

Periaatteessa mitä tahansa verkkoa voidaan monitoroida, olipa kyse langattomasta tai langallisesta verkosta, lähiverkosta eli LAN:sta (Local Area Network), virtuaalisesta erillisverkosta eli VPN:stä (Virtual Private Network) tai palveluntarjoajan laajaverkosta eli WAN:sta (Wide Area Network). LAN on tietoverkko, joka yhdistää ryhmän toisiaan lähellä sijaitsevia tietokoneita esimerkiksi yhden rakennuksen sisällä [3]. WAN puolestaan on tietoverkko, joka kattaa suuren maantieteellisen alueen, kuten koko valtion. WAN-verkkojen kautta voidaan yhdistää eri LAN-verkkoja toisiinsa. Internet on yksi esimerkki WAN-verkosta. VPN taas mahdollistaa näennäisesti yksityisen verkon luomisen Internetin yli esimerkiksi yrityksen LAN-verkkojen yhdistämiseksi. [4; 5.]

Yksinkertaisimmillaan monitorointia on esimerkiksi ping-komento, joka lähettää Internet-protokollaa käyttäen testiviestejä kahden laiteisännän (host) välillä. Ping-komentoa käyttäen voidaan täten selvittää, toimiiko tietoliikenneyhteys näiden kahden pisteen välillä, onko yhteydessä hitautta ja hukkaako yhteys lähetettyjä paketteja matkan varrelle. Yleensä ping-testaus on nykyään sisällytetty laajempaan kokonaisuuteen komentoja ja tehtäviä eli verkonmonitorointijärjestelmään. [1.]

Verkonmonitorointijärjestelmiä on useita ja niissä on monia eroavaisuuksia, mutta järjestelmien toiminta on pääpiirteiltään sama. Ensin käyttäjä määrittelee monitoroitavan IP-osoiteavaruuden. Tämä kertoo ohjelmalle, mistä verkko-osoitteista ohjelman tulee

etsiä monitoroitavat fyysiset, virtuaaliset tai pilvessä sijaitsevat laitteet, applikaatiot ja palvelut, jos ohjelmasta löytyy automaattisen verkkolaitteiden havaitsemisen toiminto (automatic discovery). Seuraavaksi käyttäjän tulee määritellä, mitä havaituista laitteista, applikaatioista ja palveluista tulee monitoroida. Laitteista voidaan monitoroida esimerkiksi komponenttien toimintaa, suorituskykyä, kovalevytilan käyttöä, lämpötilaa, muistia, käytettyjä portteja tai kaistan käyttöä. Applikaatioista voidaan monitoroida esimerkiksi niiden toimivuutta ja palveluista muun muassa saatavuutta. Näiden kahden määrittelyvaiheen jälkeen monitorointi on konfiguroitu käyttöön.

Alkukonfiguroinnin jälkeen monitorointijärjestelmä voidaan määritellä tuottamaan kirjallisia ja kaaviollisia raportteja verkon sen hetkisestä tilasta erilaisin mittarein tuotettuna. Raportit voivat sisältää tietoa esimerkiksi tietoliikenteen siirtomäärästä (throughput), virheprosenteista, laitteen tai verkon osan pois päältä ja päällä olosta (downtime/uptime), käyttöajoista, sekä automatisoitujen ja manuaalisten syötteiden tai pyyntöjen vasteajoista. [6; 7.]

Monitorointijärjestelmä ilmoittaa havaitsemistaan vioista tai muutoksista ohjelmaikkunassa näkyvin hälytyksin ja ilmoituksin (alert). Järjestelmään voidaan itse konfiguroida hälytyksiä määrittelemällä laukaisutekijöitä (trigger). Laukaisutekijät ovat ehtoja, joiden täyttyessä ohjelma aktivoi käyttäjän määrittelemän hälytyksen. Järjestelmä voidaan myös konfiguroida ilmoittamaan hälytyksistä järjestelmästä vastaavalle henkilölle tekstiviestillä, sähköpostilla tai muulla tavalla.

2.3 Ongelmat

Verkon monitoroinnissa on omat huonot puolensa ja ongelmansa. Tietoliikenteen saatavuuden ja laadun vaatimusten muuttuessa ja kasvaessa myös verkon monitoroinnin pitää pystyä huomaamaan näistä johtuvat ongelmat. Joillain yrityksillä on tapana ottaa monitorointi käyttöön ja unohtaa se jälkikäteen, mikä on huono ajatus tietoturvan kannalta. Tekniikan kehittyessä uusimmat tekniikat asentamishetkellä kattava ohjelma jää jälkeen, jos sitä ei päivitetä. Esimerkiksi tarve lähettää häviötöntä (lossless) tietoa reaaliajassa ei onnistu vanhentuneella, dokumenttien välittämiseen soveltuvalla discard-and-resend-paketinlähetystavalla, joka tietyn paketin estyessä pudottaa tämän paketin lähetysjonosta ja yrittää uudelleen myöhemmin. Häviötöntä reaaliaikaista tiedonsiirtoa tarvitsevat esimerkiksi IP-puhe eli VoIP (Voice over Internet Protocol) ja Internetin väli-

tyksellä tapahtuva televisio- tai videolähetys eli IPTV (Internet Protocol TV). Reaaliaikaisen tiedonsiirron tarve myös kuormittaa verkkoa, joka huonontaa palvelujen ja tiedon saatavuutta. [10; 11.]

Nykyaikainen liikenteen tai pakettien priorisointi ja säännöstely aiheuttaa väistämättä viivettä tietoliikenteeseen. Viiveiden takia verkon monitorointijärjestelmän on mahdotonta arvioida, täyttääkö tietty applikaatio ajallisesti sille asetetun hyväksyttävän palvelutason kriteerit. Tästä johtuva mahdollinen palvelutason huonontuminen puolestaan vaikuttaa suoraan asiakastyytyväisyyteen. Taustalla on myös ongelmaksi muodostunut päätöksenteko siitä, mikä verkkoliikenne priorisoidaan asiakastyytyväisyyden takaamiseksi. Tällä hetkellä kaikki verkon monitorointitekniikat eivät ylipäätään pysty vastaamaan uusimpiin haasteisiin, joita tiedon tarpeen reaaliaikaisuus, nopeus ja kaistankulutus asettavat esimerkiksi virtuaalisissa palvelinkeskuksissa (data center), pilvipalveluja tuottavissa ympäristöissä (cloud application delivery environments) ja työntekijöiden henkilökohtaisten IT-laitteiden käytön yritysverkossa sallivassa BYOD-teknologiassa (bring-your-own-device). Tämän lisäksi tietopaketin matkalla pisteestä pisteeseen yhä monimutkaisemmissa tietoverkoissa saattaa olla useampi palveluntarjoaja; Yksi palveluntarjoaja ei voi taata nopeutta, saatavuutta, luotettavuutta ja laatua toisen puolesta. [8; 9; 10; 11.]

Ongelmaksi ja hidasteeksi muodostuvat myös resursseja vievät monitorointijärjestelmät, jotka saattavat olla hyvinkin monimutkaisia. Esimerkiksi yksinkertaisemmat monitorointiohjelmien käyttöliittymät sallisivat verkkoasiantuntijoiden keskittyä verkon ongelmien ratkomiseen ja verkon optimointiin useiden eri monitorointijärjestelmien konfiguroinnin ja hallinnan sijaan. Ohjelmat ovat kuitenkin muuttumassa helppokäyttöisemmiksi rutiinitoimenpiteiden automatisoinnin, suodatuksen parantamisen ja ongelmien ennakoimisen myötä. [12.]

Yksi huono puoli on myös rahanmeno; Suurissa yrityksissä verkon monitorointi voi maksaa satoja tuhansia. Monitoroinnin rahareikiä ovat ohjelmisto, laitteet, monitoroinnin käyttöönottoon ja ylläpitoon käytetty työvoima ja mahdollinen toimittajan maksullinen ohjelmistotuki. Vaikka rahoituksen saaminen verkon ja täten yrityksen turvaamiseksi ei yleensä ole vaikeaa, hankitut varat voivat valua hukkaan huonosti valitulla tai käyttämättömäksi jäävällä ratkaisulla. Kustannukset lisääntyvät, jos verkon monitorointijärjestelmä on epäoptimaalisesti konfiguroitu. [13.] Tässä työssä kustannukset eivät muodostu ongelmaksi valittavan ohjelman ilmaisuuden ansiosta.

3 Käytetyt teknologiat

3.1 DNS

DNS-nimipalvelujärjestelmä (Domain Name System) on Internet-protokollien standardointiorganisaation IETF:n (Internet Engineering Task Force) standardoima protokolla [14]. DNS on tärkeimmältä tehtävältään tietokanta, jonka avulla Internetin verkkotunnukset (domain) muunnetaan IP-osoitteiksi [15]. Verkkolaitteet käyttävät Internetissä kommunikoidakseen näitä numeerisia osoitteita, joten haluttuun sivustoon voidaan yhdistää vasta DNS-protokollan selvitettyä verkkotunnusta vastaavan IP-osoitteen. Kun käyttäjä esimerkiksi kirjoittaa selaimeen verkkotunnuksen www.google.com, DNS löytää tietokannastaan sitä vastaavan IP-osoitteen ja yhdistäminen sivustoon onnistuu. DNS-protokollalla on myös kaksi muuta tehtävää; Sähköpostipalvelimet saavat DNS:n erilliseltä MX-rekisteriltä (Mail Exchanger) tarvittavat tiedot sähköpostin välittämiseen vastaanottajan sähköpostipalvelimelle, ja Microsoft Active Directory eli AD saa DNS:n erilliseltä SVC-rekisteriltä (service) tiedot verkkopalvelujen paikallistamiseen. AD on Windows-käyttöjärjestelmän komponentti, jolla suoritetaan käyttäjähallintaa ja todennusta. Verkonmonitorointijärjestelmä käyttää DNS-protokollaa hyväkseen kaikilla kolmella mainitulla tavalla. [16; 17.]

3.2 FTP

FTP (File Transfer Protocol) on IETF:n standardoima protokolla, jolla voidaan lähettää tiedostoja Internetissä olevien tietokoneiden välillä. FTP-protokollaa voidaan käyttää esimerkiksi Web-sivutiedostojen siirtämiseen kyseisen sivuston käyttämälle palvelimelle tai ohjelmien ja tiedostojen lataamiseen palvelimilta henkilökohtaiselle tietokoneelle. Verkonmonitorointijärjestelmä voi monitoroida verkossa käytettyjä FTP-palveluja. [18; 19.]

3.3 HTTP

HTTP (Hypertext Transfer Protocol) on IETF:n standardoima protokolla, joka määrittää viestien formatointi- ja lähetystavan sekä miten Web-palvelimet ja selaimet reagoivat eri komentoihin Internetissä. Esimerkiksi Internet-sivuston osoitteen kirjoittaminen se-

laimeen lähettää HTTP-käskyn Web-palvelimelle halutun sivuston hakemiseksi ja lähettämiseksi. [20; 21.] Verkonmonitorointijärjestelmä voi käyttää HTTP-protokollaa monitoroimaan esimerkiksi tietyn Internet-sivuston tilaa havaiten, milloin sivusto on kaatunut. Järjestelmä voi monitoroida HTTP-protokollan kautta myös Internet-sivuston toimimista havaiten Web-palvelimen osoitteiden perusteella, milloin sivuston osa toimii väärin. Web-palvelimesta voidaan lisäksi tarkkailla prosessorin käyttöä, levytilan määrää ja muita sen tuottamia sisäisiä arvoja. [22.]

3.4 ICMP

ICMP (Internet Control Message Protocol) on IETF:n standardoima, toiminnaltaan yksinkertainen protokolla, jota käytetään kyselyjen ja virheviestien lähetykseen. ICMP-viesti voi ilmoittaa esimerkiksi siitä, kun lähetetty data ei pääse päämääräänsä. [23.] ICMP on myös luvun alussa mainitun ping-komennon toiminnan takana. Verkonmonitorointijärjestelmissä ICMP-protokollaa käytetään verkkolaitteen olemassa olon selvittämiseen lähettämällä kysely ICMP echo request -pakettina, johon verkossa oleva laite vastaa ICMP echo reply -paketilla. [1.]

3.5 IPMI

IPMI (Intelligent Platform Management Interface) on Cisco Systemsin, Dell Inc.:in, Hewlett-Packardin, Intel Corporationin ja NEC Corporationin kehittämä palvelimen tietokonelaitteiston (hardware) kunnon etämonitorointi- ja etähallintajärjestelmä. IPMI on standardoitu rajapinta, joka toimii tietokoneen emolevyssä olevalla mikrokontrollerilla, BMC:llä (Baseboard Management Controller). BMC hallitsee rajapintaa järjestelmänhallintasovelluksen ja tietokonelaitteiston välillä. Se monitoroi tietokonejärjestelmässä olevia sensoreita, jotka välittävät BMC-mikrokontrollerille järjestelmäinformaatiota. BMC viestittää informaation perusteella hälytyksiä järjestelmänvalvojalle. IPMI-rajapinnan kautta verkon ylläpitäjä ja verkonmonitorointijärjestelmä voi täten esimerkiksi seurata järjestelmän lämpötiloja, tuulettimien toimintaa tai virtalähteen kuntoa ja päästä käsiksi tietokoneen BIOS:iin (Basic Input/Output System). BIOS on tietokoneohjelma, joka esimerkiksi lataa käyttöjärjestelmän tietokoneen käynnistyessä. [24; 25; 26; 27.]

IPMI-rajapinnan kautta verkkoyhteys otetaan suoraan tietokonelaitteistoon käyttöjärjestelmän tai kirjautumiskomentotulkin (login shell) sijaan, joten sen kautta voidaan monitoroida ja hallita myös tietokonetta, joka on pois päältä tai ei virhetilan seurauksena vastaa. IPMI:n kautta voidaan esimerkiksi käynnistää kone uudelleen. Jotta sammuksissa olevaa tietokonetta voidaan hallita, laitteen täytyy kuitenkin saada virtaa pistorasiasta ja laitteella on oltava esimerkiksi lähiverkkoyhteys. [27.] Koska IPMI-rajapinnan kautta otetussa yhteydessä ohitetaan käyttöjärjestelmä, jossa olisi palomuuri ja muut turvallisuusjärjestelmät, IPMI:n käytössä on omat turvallisuusriskinsä. Tunkeutujalla on mahdollisuus löytää avoinna oleva hallintarajapinta ja aiheuttaa sitä hyväkseen käyttäen ongelmia tietoverkossa, sillä rajapinnat ovat harvoin hyvin suojattuja. Tästä syystä suositellaan IPMI:n rajoittamista sisäisiin verkkoihin sekä rajapintojen, laitteiden ja tarvittavan verkkoliikenteen salaamista ja suojaamista vahvoin salasanoin. [28.]

3.6 NetFlow ja IPFIX

NetFlow on Cisco Systemsin kehittämä protokolla, jolla reitittimeltä voidaan viedä informaatiota verkkoliikennevirtauksista eli verkkovoista (network flow) dataa kerääville laitteille ja verkon hallintajärjestelmille. Virtaus eli vuo on tietty joukko paketteja lähetettynä lähteestä määränpäähän tietoverkossa. Vuodataa analysoimalla voidaan selvittää esimerkiksi verkkoliikenteen tarkka lähde ja määränpää, käytetyt IP-osoitteet, portit ja protokollat sekä generoituneen verkkoliikenteen määrä ja verkon käytön ruuhka-ajat. Analyysilla voidaan saada tietoa myös verkon käyttäjistä ja applikaatioista. [29; 30; 31.]

NetFlow-dataa voidaan kerätä ja analysoida Netflow-datan kerääjällä (NetFlow collector), joka voi olla joko fyysinen laite tai ohjelmiston osa. NetFlow’n toiminta on käytännössä yksinkertaista; reitittimet keräävät verkostaan tietoja NetFlow-käyttöön valjastetuilta rajapinnoiltaan ja kirjaavat tiedot NetFlow-tietueiksi, jotka lähetetään luvussa 3.11 käsiteltävän UDP-tiedonsiirtoprotokollan avulla NetFlow-datan kerääjän sisältävälle laitteelle. NetFlow’n kannalta tärkeimmät paketin sisältämät tiedot ovat vuon sisääntulo- ja ulosmeno-rajapinnan numero, pakettimäärä, tavumäärä ja ajankohta. NetFlow-datan kerääjä prosessoi saamansa tiedot ja ilmoittaa verkkoliikenneanalyysin tulokset käyttäjälle ymmärrettävässä muodossa. Verkonmonitorointijärjestelmissä kerättyä vuodataa käytetään kaistan monitorointiin ja verkkoliikenteen analyysiin, esimerkiksi sen määrittämiseen, minkä tiettyjen IP-osoitteiden tai verkkolaitteen porttien kautta eri data kulkee.

NetFlow toimii vain NetFlow-protokollaa tukevilla reitittimillä ja kytkimillä, mikä alun perin tarkoitti toiminnan rajoittumista vain Ciscon omille verkkolaitteille. NetFlow on kuitenkin muotoutunut epävirallisesti standardiksi tietoverkkoalalla, ja suurin osa eri yritysten verkkolaitteista tukee protokollaa. Monilla yrityksillä on myös oma vastaava protokollansa, kuten Jflow Juniper Networksillä ja sFlow Hewlett-Packardilla. [30; 31; 32.]

NetFlow'n uusin versio on NetFlow 9. IPFIX (IP Flow Information Export) on IETF:n standardoima protokolla, joka perustuu tähän NetFlow 9 -protokollaan. NetFlow-protokollan tapaan myös IPFIX on kehitetty verkkovoiden monitorointiin ja vuodatan keräämiseen. Koska IPFIX on IETF:n standardoima, se toimii kaikilla sitä tukevilla reitittimillä ja hallintaohjelmistoilla toimittajasta riippumatta. Tästä syystä IPFIXin käyttö on saamassa vähitellen lisää kannatusta NetFlow'n dominoimalla tietoverkkoalalla. [33.]

3.7 SIP

SIP (Session Initiation Protocol) on IETF:n standardoima protokolla istuntojen (session) luomiseen, muokkaamiseen ja päättämiseen [34]. Istunto on yhteys protokollaan tai yhteys käyttäjän tai käyttäjän selaimen ja palvelimen välillä. Istunnossa voi olla yksi tai useampi osallistuja. [35.] Istuntoja ovat esimerkiksi tekstin, puheen tai videokuvan jakaminen, Internet-puhelut tai tekstiä, puhetta ja videota käyttävät kokousapplikaatiot. SIP-protokollaa käytetään esimerkiksi pikaviestimissä, IP-puheessa ja verkkopelaamisessa (online gaming). Verkonmonitorointijärjestelmä voi monitoroida verkossa olevien SIP-protokollaa käyttävien palveluiden tilaa ja saatavuutta lähettämällä itse SIP-viestejä laitetta tai selainta matkien ja odottamalla palvelun vastausta. Yleisimmin tällä tavalla monitoroidaan IP-puhetta. [36; 37; 38.]

3.8 SNMP

SNMP (Simple Network Management Protocol) on IETF:n standardoima verkonhallintaprotokolla, joka on yleisin automaattiseen verkkolaitteiden havaitsemiseen käytetty protokolla. SNMP-protokollaa käytetään sekä tiedon keräämiseen verkkolaitteista että niiden konfigurointiin. Suurin osa verkkolaitteista ja monitorointiohjelmistoista tukee sitä. [39.]

Laitetta, jolle on asennettu SNMP-protokollan hallintaohjelmisto, kutsutaan SNMP-hallinta-asemaksi (SNMP manager). Hallinta-asema lähettää SNMP-kyselyjä (SNMP query) laitteille, joilta halutaan informaatiota. Näitä hallittuja laitteita kutsutaan SNMP-agenteiksi (SNMP agent). SNMP-agentteja voivat olla muun muassa reitittimet, verkkotulostimet ja tietokoneet. Jotta agentti ja hallinta-asema voivat vaihtaa viestejä keskenään, niille täytyy konfiguroida yhteinen SNMP-yhteisötunnus (SNMP community). Yhteisötunnus toimii salasanan tavoin laitteiden välisessä viestinnässä. SNMP-agentin keräämä laiteinformaatio on kunkin verkkolaitteen omassa tietoverkon kokonaisuuksia hallitsevassa MIB-tietokannassa (Management Information Base) kansainvälisenä OID-yksilöintitunnuksena (Object Identifier). SNMP-agentti hakee MIB-tietokannastaan kysytyn objektin ja välittää sen SNMP-hallinta-asemalle. Hallinta-aseman lähettämillä kyselyillä voidaan selvittää käytetty verkkoprotokolla, laitteiston ja ohjelmiston konfiguraatiotiedot, laitteen suorituskyky- ja käyttö- sekä virhe- ja tapahtumatiedot, ohjelmien ja applikaatioiden käyttötiedot sekä havaita verkossa olevia laitteita. SNMP-agentit voidaan konfiguroida itse lähettämään erillisiä SNMP-ilmoituksia (SNMP trap) hallinta-asemalle, jolloin agentti voi vaihtaa tiettyä informaatiota hallinta-aseman kanssa ilman hallinta-aseman lähettämää kyselyä. Tällaisilla viesteillä voidaan informoida hallinta-asemaa esimerkiksi agentin verkkosovittimen tilamuutoksista tai agentin ja hallintajärjestelmän välisistä todennusvirheistä. [40; 41.]

Verkonmonitorointijärjestelmä käyttää SNMP-protokollaa palveluiden, kuten IP-osoitteita verkkolaitteille jakelevan DHCP-protokollan (Dynamic Host Configuration Protocol), ja verkkolaitteiden, kuten tietokoneiden, reitittimien ja kytkimien, havaitsemiseen ja monitorointiin. SNMP-agentti ja SNMP-hallinta-asema vaihtavat keskenään MIB-tietokannasta haetun objektin verkkolaitteen tunnistamiseksi. [41.] SNMP käyttää hyväkseen UDP-kyselyjä (User Datagram Protocol), joihin verkossa olevat muut laitteet lähettävät vastauksen. Luvussa 3.11 käsiteltävä UDP-protokolla ei muodosta monivaiheista yhteyttä laitteiden välille eikä varmistele paketin välittymistä ja on täten verkkoliikenteellisesti kevyempi ratkaisu kuin TCP-kyselyt (Transmission Control Protocol); luvussa 3.11 myös käsiteltävän TCP-protokollan virhetarkistukset (error checking) ja paketin saapumisvahvistukset (delivery validation) olisivat tarpeettomia tässä käyttötarkoituksessa. [42; 43.]

3.9 SSL ja TLS

SSL (Secure Sockets Layer) ja TLS (Transport Layer Security) ovat salausprotokollia, joita käytetään turvaamaan Internetin yli tapahtuva viestintä. SSL kehitettiin alun perin Netscape Communicationsin toimesta yksityisten dokumenttien lähettämiseen Internetin yli, mutta nykyään se on osa laajempaa, SSL-protokollan 3.0-versioon perustuvaa TLS-turvallisuusprotokollaa. SSL käyttää hyväkseen julkisen ja yksityisen avaimen salausjärjestelmää (public-and-private key encryption system). Julkinen avain on avoin kaikille ja yksityinen tai salattu avain on vain viestin vastaanottajan tiedossa. [44.] Salauksen saa purettua vain kummankin avaimen tiedossa ollessa. TLS taas koostuu TLS Record Protocol -tietueprotokollasta, joka turvaa yhteyden joko salauksella tai ilman salausta, sekä TLS Handshake Protocol -kättelyprotokollasta, jonka avulla palvelin ja asiakasohjelma (client) todentavat toisensa ja sopivat salaustavasta ja -avaimista ennen informaation vaihtoa. [45; 46.] Internet-selaimet ja Web-palvelimet käyttävät hyväkseen SSL- ja TLS-protokollaa. Selaimessa salausprotokollan aktivoitumisen näkee osoitteen "http"-alun muuttumisesta "https"-muotoon osoiterivillä siirryttäessä salatulle sivustolle. SSL- ja TLS-protokolla eivät ole yhteensopivia, mutta SSL-protokollaa käyttävä asiakasohjelma voi käsitellä TLS-protokollalla lähetetyn viestin. [47; 48.] Verkonmonitorointijärjestelmä voi seurata SSL- ja TLS-protokollan luomaa liikennettä ja näin monitoroida verkossa tapahtuvan viestinnän turvallisuuden tilaa.

3.10 Syslog

Syslog on IETF:n standardoima protokolla, jolla verkkolaitteet voivat lähettää viestejä eri tapahtumista lokitietoja ylläpitävälle palvelimelle, jota usein kutsutaan Syslog-palvelimeksi. Suurin osa eri käyttöjärjestelmillä toimivista verkkolaitteista palomuureista ja Web-palvelimista verkkotulostimiin pystyy lähettämään Syslog-viestejä, joten Syslogilla voidaan keskittää lokitiedot kätevästi esimerkiksi yhdelle palvelimelle. Windows-palvelimet eivät sinänsä tue Syslogia, mutta näiltäkin palvelimilta saadaan lähetettyä tiedot esimerkiksi Windows-tapahtumalokista (Windows Event Log) kolmannen osapuolen ohjelmalla tai muulla työkalulla Syslog-palvelimelle. Tietojen keräys useammista järjestelmistä on kuitenkin myös yksi Syslogin haittapuolista; Puuttumatta tapahtumaviestien formaattiin millään tavalla, Syslog-palvelimelle kerääntyy sekalaisia viestejä, joista osa on suoraan verkonvalvojan luettavissa, mutta osa ei. Verkonmonitorointijär-

jestelmä käyttää Syslogia keräämään monitorointia varten tarvittavaa tietoa monitoroitavasta tietoverkosta. [49; 50.]

3.11 TCP ja UDP

TCP (Transmission Control Protocol) on IETF:n standardoima protokolla, jonka avulla asiakasohjelmat voivat muodostaa luotettavan yhteyden verkon yli ja vaihtaa keskenään informaatiota [51, s.1; 52]. TCP jakaa lähetetyn tiedon numeroiduiksi datapaketeiksi ja lähettää ne yksitellen päätepistettä kohti. Paketit saattavat kulkea verkon läpi eri reittejä, mutta TCP yhdistää paketit järjestyksessä takaisin lähetetyksi tiedoksi päätepisteessä ja lähettää näin alkuperäisen tiedon vastaanottajalle. [53.] TCP takaa tiedon saapumisen vastaanottajalle lähetysjärjestyksessä ja luotettavasti paketin numeroinnin ja virheen tarkistuksen kautta. TCP-protokollaa käytetään esimerkiksi Internet-selainten yhdistäessä WWW-palvelimiin, sähköpostin lähetykseen ja tiedostojen siirtoon. Myös useat toiset protokollat, kuten SIP ja FTP, käyttävät toimintaansa TCP-protokollaa. [54; 55.] Verkonmonitorointijärjestelmä voi käyttää TCP-protokollaa yhteyksien muodostamiseen monitoroinnissa, paketin jäljitykseen verkossa ja järjestelmä voi luonnollisesti monitoroida myös itse TCP-liikennettä.

Kun lähettäjä ei tarvitse vahvistusta vastaanottajalle onnistuneesti saapuneista paketeista tai paketin virheentarkistusta tai nämä toimenpiteet voidaan tehdä itse asiakasohjelmassa, voidaan käyttää UDP-protokollaa. UDP (User Datagram Protocol) on TCP-protokollan tapaan IETF:n standardoima protokolla, jota asiakasohjelmat käyttävät viestien vaihtoon keskenään. TCP-protokollasta poiketen UDP-protokollassa ei ole virheentarkistusta tai paketin lähetysjärjestyksen säilyttävää tarkistusta, sillä UDP ei jaottele dataa numeroituihin paketteihin. UDP ei myöskään takaa lähetyksen saapumista päätepisteeseen. UDP takaa vain paketin sisäisen datan luotettavuuden. [56; 57.] UDP-protokollaa voidaan käyttää myös multicast-ominaisuudessa paketin lähettämiseen monelle vastaanottajalle samaan aikaan, jolloin siirtoon tarvitaan vähemmän kaistaa. UDP on täten verkkoliikenteellisesti kevyempi ratkaisu kuin TCP. UDP-protokollaa käyttävät esimerkiksi asiakasohjelmat, joille nopea tai reaaliaikainen tiedonsiirto on tärkeämpää kuin pakettikato tai joilla on tarvetta lähettää vain pieniä määriä dataa kerralla, sekä toiset protokollat, kuten SNMP ja SIP. Verkonmonitorointijärjestelmä voi monitoroida UDP-liikennettä tai esimerkiksi käyttää UDP-protokollaa multicast-ominaisuuden myötä palvelinten havaitsemiseen verkossa. [58; 54; 43.]

3.12 Telnet ja SSH

Telnet on IETF:n standardoima protokolla ja tekstipohjainen applikaatio, jonka kautta tietokoneiden välille voidaan muodostaa kaksisuuntainen yhteys verkon yli [59]. Telnetiä käytetään pääasiassa komentojen syöttämistarkoituksessa etäyhteyden muodostamiseen palvelimelle tai muulle verkkolaitteelle, jolla Telnet-palvelu on toiminnassa. Telnet on alunperin suunniteltu käyttöön vain yksityisessä verkossa, eikä siihen täten ole sisällytetty salausta, todennusta tai muita turvallisuusominaisuuksia. Komennot ja salasanat ovat suoraan luettavissa. Telnetin onkin nykyään laajalti korvannut turvallisempi protokolla, SSH. Telnetiä käytetään nykyään lähinnä viihde-, testaus- ja vianselvitystarkoituksessa. Verkonmonitorointijärjestelmä voi käyttää Telnetiä esimerkiksi käyttämään etänä Web-palvelimia tai eri palvelujen toiminnan testaamiseen ottamalla yhteyden palvelimelle ja syöttämällä testattavan palvelun käyttämän protokollan toiminnan tarkistukseen tarvittavat komennot. [60; 61.]

SSH (Secure Shell, Secure Socket Shell) on IETF:n standardoima UNIX-käyttöjärjestelmäpohjainen teknologia, jota käytetään turvalliseen etäkirjautumiseen [62]. SSH kehitettiin korvaamaan tietoturvassaan puutteelliset protokollat kuten Telnet. SSH-protokollalla voidaan muodostaa salattu ja todennettu komentoriviyhteys kahden tietokoneen välille ja siirtää tiedostoja koneiden välillä. SSH-protokollalla voidaan myös muodostaa VPN-tunneli tarvitulle fyysiselle tai virtuaaliselle laitteelle. [63, s.1; 64.] Verkonmonitorointijärjestelmä käyttää SSH-protokollaa muodostamaan turvallisen yhteyden monitoroitavalle verkkolaitteelle sekä UNIX- ja Linux-laitteiden tunnistamiseen. SSH käyttää julkisen avaimen salausta (public key cryptography) verkkolaitteen todentamiseen, josta vastauksen saadessaan monitorointiohjelma tunnistaa verkossa olevan laitteen. [65; 66; 67.]

3.13 WMI

WMI (Windows Management Instrumentation) on Windows-käyttöjärjestelmässä toimiva API (Application Programming Interface) eli ohjelmointirajapinta. Ohjelmointirajapinta on protokollien, työkalujen ja aliohjelmien joukko, joka määrittelee miten ohjelmat vaihtavat tietoja keskenään. WMI käyttää toimintaansa CIM-tekniikkaa (Common Information Model). [68; 69; 70.] CIM on yleinen tapa määritellä järjestelmien, tietoverkkojen, applikaatioiden ja palvelinten hallintatietoja [71]. CIM mahdollistaa laitteiden ja

applikaatioiden hallinnan valmistajasta tai lähteestä riippumatta. WMI mahdollistaa verkkolaitteiden ja verkossa olevien järjestelmien hallitsemisen esimerkiksi järjestelmäasetusten ja pääsyoikeuksien muuttamiseksi, prosessien tai tehtävien aloittamiseksi ja ajoittamiseksi etätietokoneella, ja etätietokoneen käynnistämiseksi. WMI-rajapinnan kautta voidaan myös kerätä tietoa sekä paikallisista tietokoneista että etäjärjestelmistä. Verkonmonitorointijärjestelmä voi käyttää WMI-rajapintaa tietojen keräämiseen tietoverkosta WMI-rajapintaa käyttävistä järjestelmistä eli Windows-järjestelmistä. [72; 73.]

4 Ilmaisohjelmat tietoverkon monitorointiin

Vertailuun valittiin seitsemän ilmaiseksi käytettävää Windows- tai Linux-ympäristössä toimivaa ohjelmaa, jotka pystyivät käyttämään erilaisia laukaisutekijöitä, tuottamaan hälytyksiä ja ilmoituksia, mahdollisesti havaitsemaan kehityssuuntia (trending) ja myös ennustamaan niitä (trend prediction), havaitsemaan verkkoon liitetyt laitteet automaattisesti ja luomaan niistä loogisen ryhmittelyn ja mahdollisesti selkeän visuaalisen topologian, käyttämään hyväkseen SNMP-protokollaa, Syslogia ja NetFlow'ta tai vastaavaa protokollaa, sekä tuottamaan keräämästään aineistosta selkeitä raportteja. Vertailun ulkopuolelle jätettiin ilmaiseksi käytettävät monista erityisohjelmista koostuvat ohjelmapaketit.

Alla on listattu pääpiirteittäin tässä ohjelmavertailuosiossa käytetyn tietokoneen kokoonpano:

- neliydinprosessori
- 6 GB RAM-muistia
- 80 GB kovalevytilaa
- Windows 7 Home Premium SP1.

Windows-käyttöjärjestelmää käyttävät ohjelmat asennettiin koneelle suoraan yksitellen jokainen vuorollaan. Poikkeuksellisesti kohdan 4.2 ohjelma asennettiin Windows Server 2012 R2 -käyttöjärjestelmälle, joka oli ensin itse asennettu VMware Workstation 10.0.1 -virtualisointiohjelmaan luodulle virtuaalikoneelle. Näiden ohjelmien testauksen jälkeen koneelle VMware Workstation 10.0.1 -virtualisointiohjelmaan luotiin toinen virtuaalikone, jonka käyttöjärjestelmäksi asennettiin CentOS 6.5. Tällä virtuaalikoneella

testattiin ohjelmavertailun Linux-käyttöjärjestelmää käyttävät ohjelmat yksitellen jokainen vuorollaan. Seuraavissa alaluvuissa luodaan nopea katsaus kaikkiin vertailuun valittuihin ohjelmiin aakkosjärjestyksessä ja käsitellään ohjelmavertailun tulokset. Alaluvuissa ohjelmien havainnollistamista varten ohjelmista otetut kuvakaappaukset on rajattu näyttämään ohjelmista vain tekstissä käsitelty olennaisin osa.

4.1 CA Nimsoft Monitor Snap

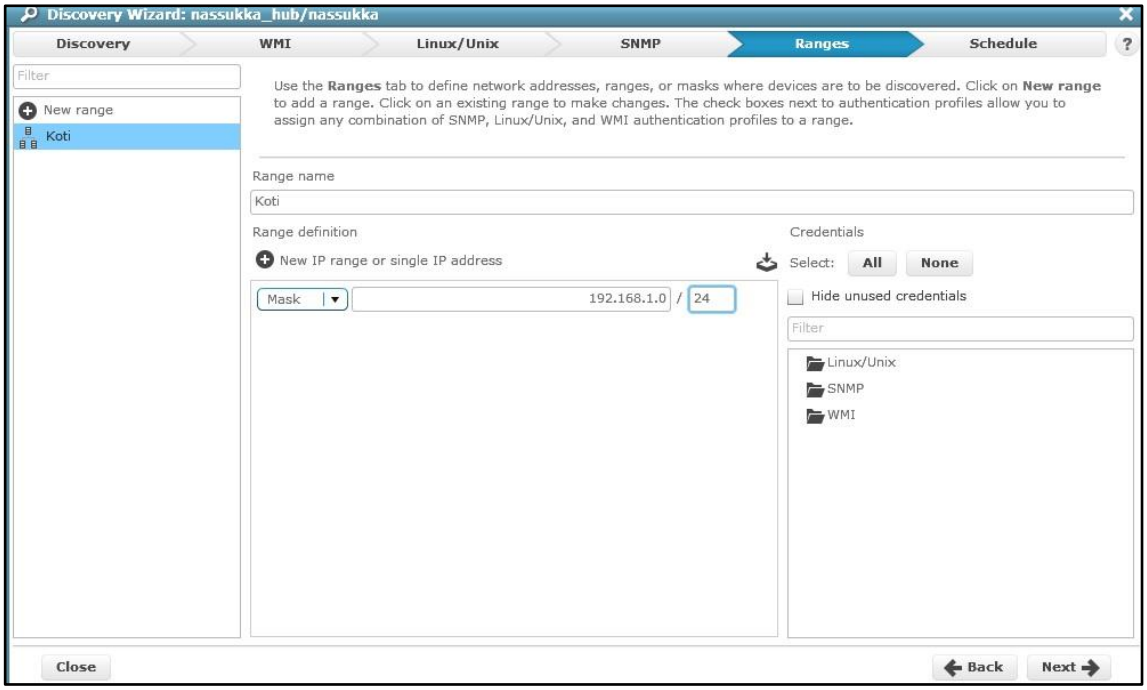
CA Technologies on vuonna 1976 perustettu yhdysvaltalainen yhtiö. Se myy yrityksille IT-hallintaohjelmistoja ja -ratkaisuja [74]. Näistä CA Nimsoft Monitor Snap on ilmainen versio yrityksen laajemmasta CA Nimsoft Monitor -ohjelmasta. Ohjelmalla voidaan monitoroida fyysisiä ja virtuaalipalvelimia, ohjelmia, tietoverkkoja ja -laitteita, tietokantoja, levyjärjestelmiä, kaistanleveyttä (bandwidth) tai Internet-sivuja. Ohjelma on rajoitettu enimmillään 30 laitteen monitorointiin ja monitoroinnin tietovarasto (data storage) 10GB:uun. [75; 76.]

CA Nimsoft Monitor Snap -ohjelman vähimmäisjärjestelmävaatimukset on listattu alla:

- 3 GB ohjelmalle varattua RAM-keskusmuistia
- 1,6 GHz tuplaydinprosessori
- 15 GB kovalevytilaa
- 64-bittinen Windows 7 SP1 / Windows Server 2008 R2 SP1 / Windows Server 2012. [77.]

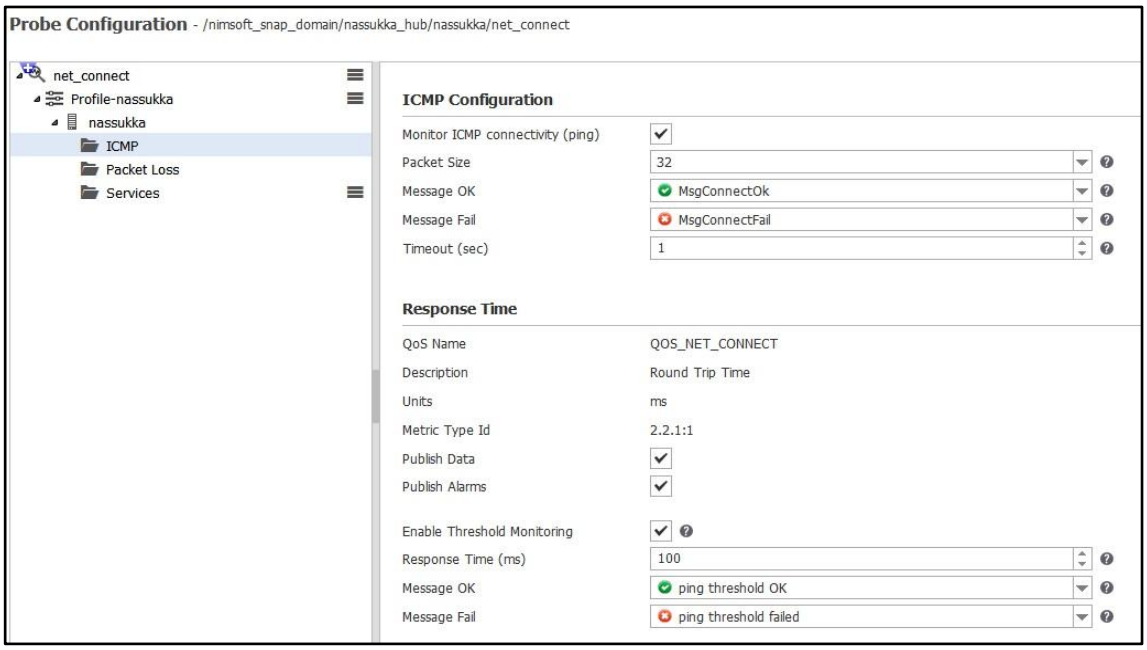
Testausta varten asennettiin ohjelman uusin 7.1-versio [78]. Ohjelman 1,11 GB:n asennustiedoston lataaminen oli kohtuullisen nopea toimenpide, mutta ohjelman asentuminen kesti yli tunnin.

CA Nimsoft Monitor Snap -ohjelmassa on selainpohjainen käyttöliittymä. Ohjelman ensimmäisellä käynnistyskerralla avautuu niin kutsuttu ”wizard” eli ohjattu käyttöönotto (kuva 1). Ohjatun käyttöönoton ponnahdusikkunasta valitaan määritteet verkkolaitteiden automaattiselle havaitsemiselle, kuten IP-osoiteavaruus, josta laitteita tulee etsiä. Tämän automaattisen havaitsemistoiminnon pystyy myös ajastamaan.



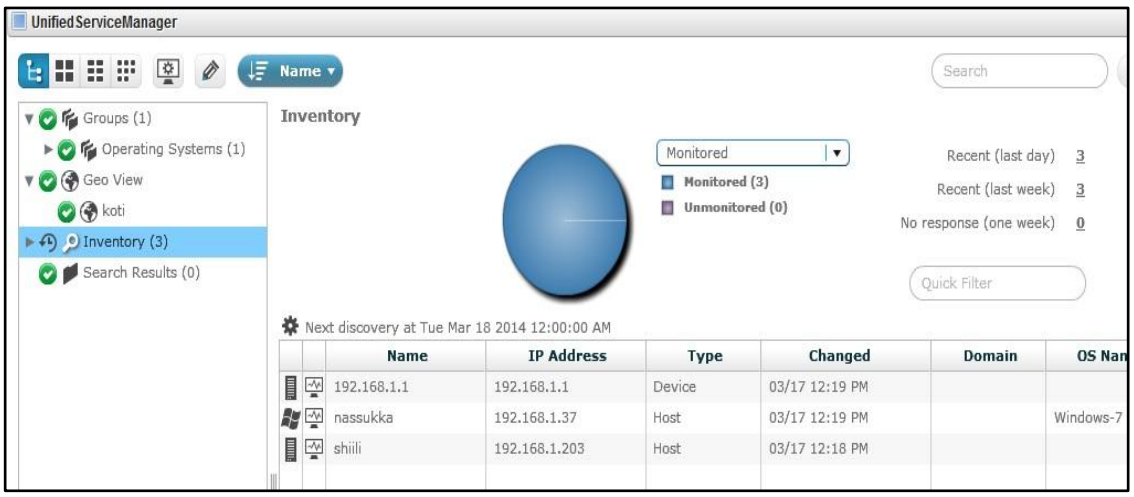
Kuva 1. CA Nimsoft Monitor Snap -ohjelman ohjattu käyttöönotto.

Ohjatussa käyttöönotossa määritetään myös muun muassa, mitä löydettyjä laitteita sekä näiden palveluja ja applikaatioita monitoroidaan. Myös ohjatun käyttöönoton jälkeen voidaan myöhemmin asettaa niin kutsuttuja antureita (probe) monitorointikohteiden valitsemiseksi (kuva 2).



Kuva 2. Esimerkki monitorointianturin määrittämisestä CA Nimsoft Monitor Snap -ohjelmassa.

Ohjelmassa voidaan määrittää tiettyjä laukaisutekijöitä hälytyksille, kuten laitteen häiriön, ja ajastaa raportteja. Ajastetut sekä manuaalisesti ajetut raportit voidaan listata sisältöineen Reports-välilehdeltä. Ohjelman Inventory-yleisnäkymässä on tiedot monitoroiduista laitteista ja mitä kyseisestä laitteesta monitoroidaan (kuva 3).



Kuva 3. Yksityiskohta CA Nimsoft Monitor Snap -ohjelman Inventory-näkymästä.

CA Nimsoft Monitor Snap oli tietokoneelle raskas ohjelma suorittaa. Tämä näkyi esimerkiksi hiiren liikkeen takkuamisessa ruudulla ja viiveessä reagoida painikkeiden painalluksiin. Ohjelmassa jäi myös kaipaamaan visuaalista topologiaa, jotta verkosta ja sen sisällöstä olisi saanut selkeän käsityksen. Tämä ominaisuus on vain ohjelman maksullissa versiossa.

4.2 Heroix Longitude Community Edition

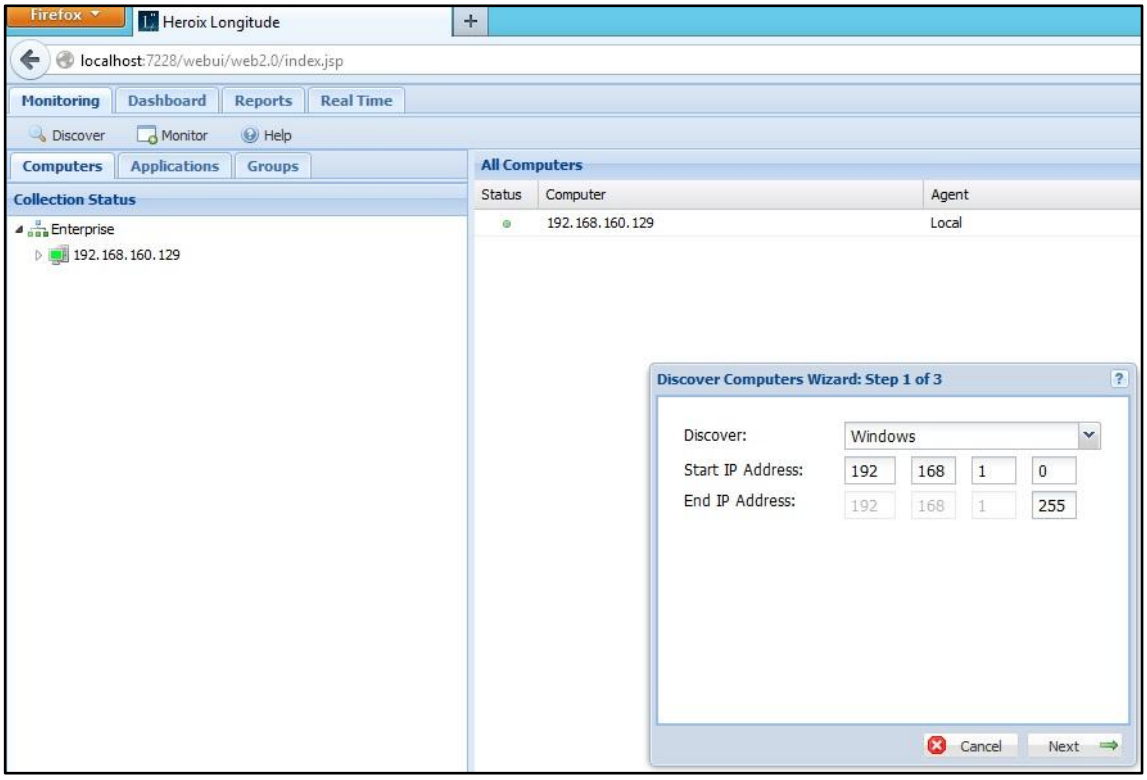
Heroix on vuonna 1975 perustettu IT-hallintaohjelmia tarjoava yhdysvaltalainen yritys [79; 80]. Yrityksen Heroix Longitude Community Edition on lisäominaisuuksilla höystetyn Heroix Longitude Enterprise Editionin ilmaisversio. Ohjelmalla voidaan monitoroida verkkolaitteita, palvelimia, applikaatioita ja virtuaaliympäristöjä. Ohjelman käyttö on rajoitettu viiden laitteen ja kahden Vmware-virtuaalikoneen monitorointiin. [81.]

Heroix Longitude Community Edition -ohjelman vähimmäisjärjestelmävaatimukset on listattu alla:

- 2,4 GHz:n prosessori
- 2 GB RAM-muistia
- 30 GB kovalevytilaa
- Windows Server 2003 (Windows XP etc. vain evaluointi). [82.]

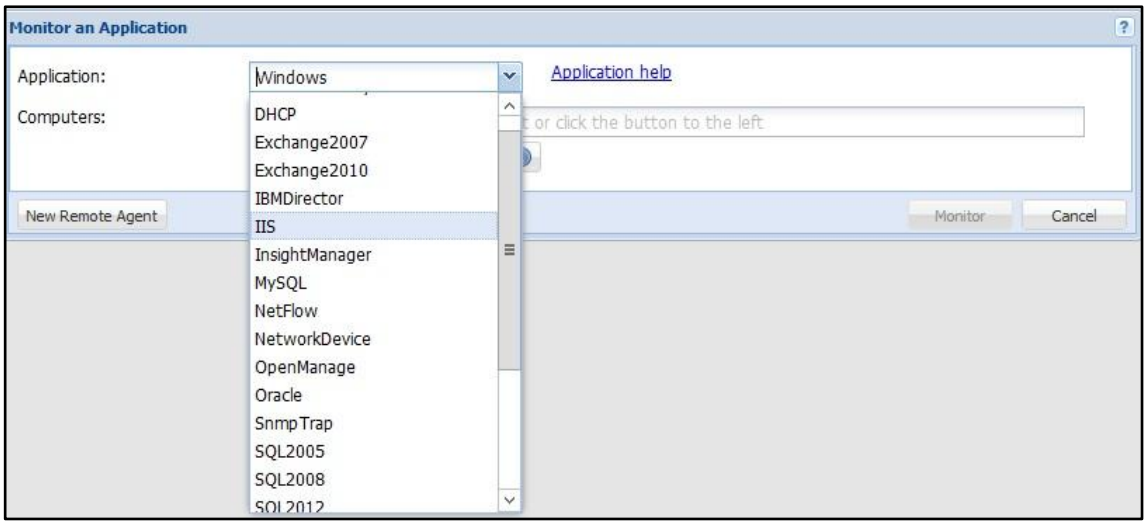
Testausta varten asennettiin ohjelman V8.2-versio [83]. Järjestelmävaatimuksista kertovassa kohdassa valmistajan Internet-sivuilla sanottiin, että ohjelma voidaan evaluointitarkoituksessa asentaa myös esimerkiksi Windows 7 -käyttöjärjestelmälle, mutta ohjelman asentuminen päättyi virheilmoitukseen sekä 32- että 64-bittisessä ympäristössä tällä käyttöjärjestelmällä kokeiltaessa. Ohjelma asennettiin onnistuneesti lopulta VMware Workstation 10.0.1 -virtualisointiohjelmaan luodulle virtuaalikoneelle, jossa oli Windows Server 2012 R2 -käyttöjärjestelmä. Heroixin asennustiedosto oli kooltaan 459 MB ja asentui muutamassa minuutissa.

Heroix Longitude toimii selainkäyttöliittymällä. Heroix Longitudessa ei ole ohjattua käyttöönottoa, vaan ohjelmassa aukeaa ensimmäiseksi listaus verkkolaitteista. Listalla on aluksi vain tietokone, jolle ohjelma on asennettu. Ohjelmassa painetaan erikseen Discover-nappia, joka aukaisee automaattisen verkkolaitteiden havaitsemistoiminnon ikkunan (kuva 4). Ponnahdusikkunassa tulee valita halutaanko etsiä Windows-, Unix- vai verkkolaitteita ja syöttää IP-osoiteavaruus, josta laitteita etsitään. Jotta Heroix Longitude voi ottaa yhteyden verkossa olevaan laitteeseen, tulee laitteelle olla asennettu Heroix Longitude -agentti eli niin kutsuttu välittäjäohjelma.



Kuva 4. Automaattinen verkkolaitteiden havaitseminen Heroix Longitude -ohjelmassa.

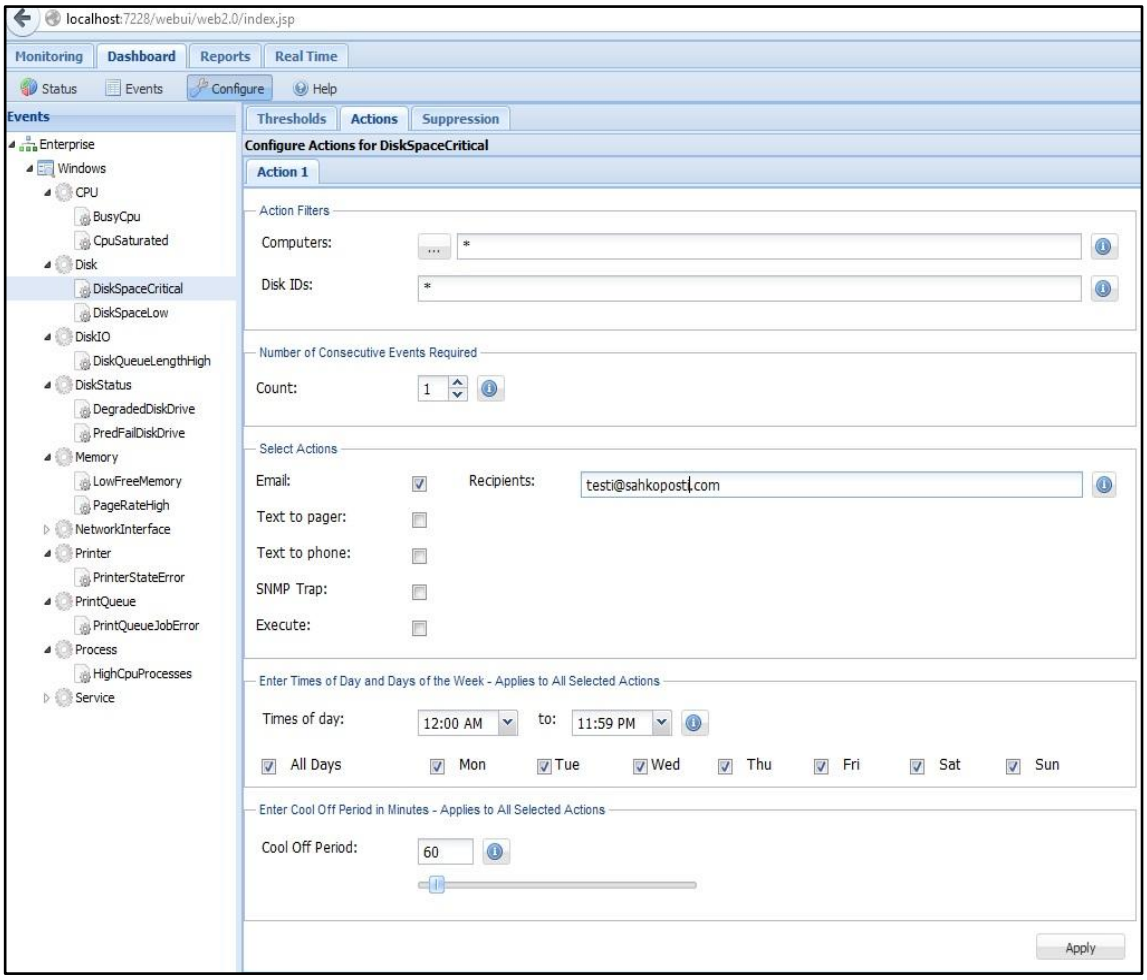
Heroix Longitudessa voidaan määrittää monitoroitavaksi eri applikaatioita, kuten käyttöjärjestelmiä, NetFlow-verkkovoista ja verkkolaitteita (kuva 5).



Kuva 5. Applikaatioiden monitorointi Heroix Longitude -ohjelmassa.

Heroix Longitudessa voidaan myös asettaa hälytyksiä esimerkiksi silloin, kun haluttu palvelu ei vastaa sille lähetettyihin kyselyihin. Ohjelma luo hälytyksistä raportin ja dia-

grammin, joihin pääsee käsiksi Reports-kohdasta. Heroix Longitude voi tuottaa raportteja myös reaaliaikaisena. Ohjelmassa voidaan myös konfiguroida toimintoja, joita ohjelman tulee kunkin hälytyksen tai muun tapahtuman yhteydessä suorittaa. Kuvassa 6 toiminnoksi määritellään sähköpostin lähettäminen määritettyyn osoitteeseen tietyllä aikavälillä.



Kuva 6. Suoritettavan toiminnon määrittäminen Heroix Longitude -ohjelmassa.

Heroix Longitude vaikutti alkuvaikeuksien jälkeen selkeältä ja helppokäyttöiseltä ohjelmalta. Ohjelmasta puuttuu kuitenkin visuaalinen topologia, joka havainnollistaisi monitoroitavaa verkkoa ja sen laitteita paremmin kuin tämän hetkinen listaus IP-osoitteista, laitenimistä ja kirjallisesta kuvauksesta.

4.3 Network Management Information System

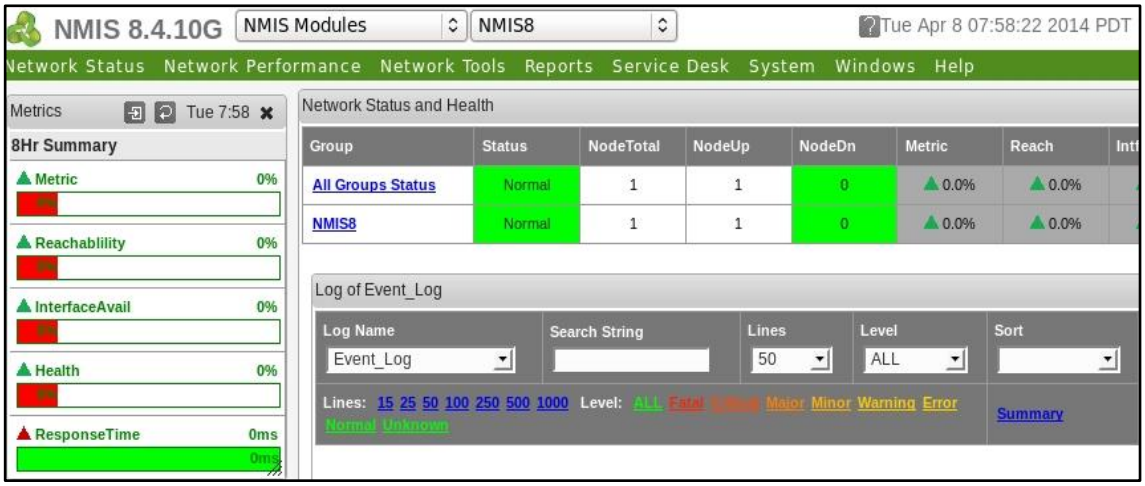
Opmantek on avoimen lähdekoodin verkonhallintajärjestelmiä kehittävä australialainen yritys. Yrityksen lippulaiva Network Management Information System, lyhyemmin NMIS, on ilmainen avoimen lähdekoodin monitorointiohjelma. Vuonna 1998 julkaistu NMIS oli ensimmäinen avointa lähdekoodia käyttävä verkonmonitorointiohjelma. [84.] Ohjelmalla voidaan monitoroida esimerkiksi verkkolaitteita, palvelimia, palveluita, ja protokollia. [85.]

NMIS-ohjelman järjestelmävaatimukset on poikkeuksellisesti lueteltu valmistajan sivulla 1000 monitoroitua laitetta kohden:

- 2 GB RAM-muistia
- 20 GB kovalevytilaa
- 64-bittinen Red Hat Enterprise Linux / CentOS 5.4. [86.]

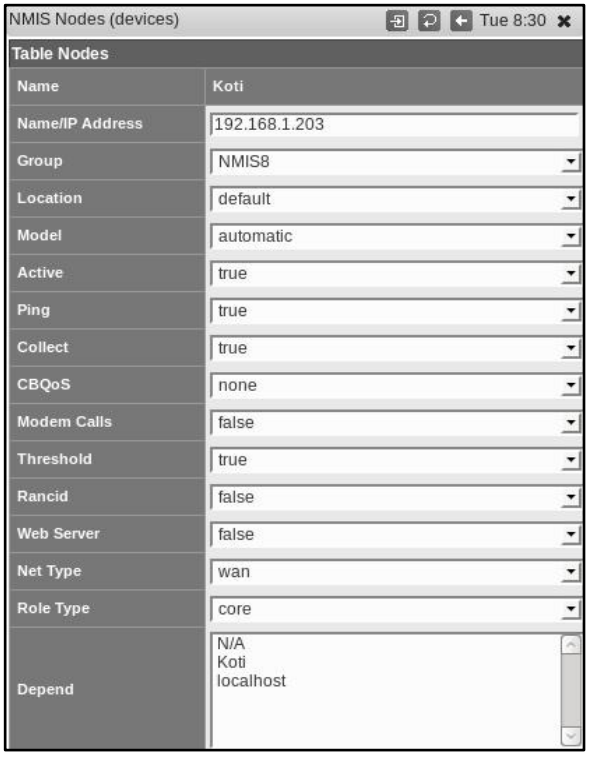
Testausta varten asennettiin ohjelman 8.4.10-versio [87]. Asennustiedosto oli kooltaan 2,2 MB. Asennus kesti reilun tunnin, koska asennusohjelma tarvitsee toimiakseen käyttöjärjestelmän päivitystä tietyin paketein, esimerkiksi RRDTool-asennuksen, eikä testauksessa käytetty CentOS-käyttöjärjestelmä sisältänyt suurinta osaa tarvituista päivityksistä. Lopulta asennukset tehtiin yksitellen manuaalisesti automatiikan epäonnistuessa. Opmantekin asennusohjesivusto tarjoaa tarkat komennot päivitysten tekemiseksi. [88.]

NMIS-ohjelmassa on selainkäyttöliittymä. Kirjautuminen tapahtuu oletustunnuksella ja -salasanalla, jotka ovat Opmantekin sivuston ohjeistuksen mukaisesti ”nmis” ja ”nm1888” [89]. Network Status -aloitusnäkymässä on katsaus verkon tapahtumiin, verkosta tehtyihin mittauksiin ja verkon tämän hetkiseen tilaan (kuva 7).



Kuva 7. Yksityiskohta NMIS-ohjelman Network Status -aloitusnäkymästä.

NMIS-ohjelmassa monitoroitavia laitteita voidaan lisätä verkosta napsauttamalla Add-lisäyslinkkiä NMIS Nodes -ikkunassa. Ikkunan kenttiin tulee määrittää vähintään laitteen IP-osoite ja nimi, mutta tarjolla on myös useita vaihtoehtoisia määritteitä, kuten laitteen rooli verkossa ja laitteen käyttämät palvelut (kuva 8). NMIS-ohjelmassa laitteita voidaan etsiä myös automaattisesti, mutta sitä varten täytyy ohjelmaan ladata erillinen Open-AudIT-moduuli [90].



Kuva 8. Monitoroitavan laitteen lisäys NMIS-ohjelmassa.

NMIS-ohjelma voidaan määrittää ilmoittamaan tapahtumista tiettyyn sähköpostiosoitteeseen määrittämällä tämän Contacts-ikkunassa. Ohjelmassa voidaan myös tarkastella esimerkiksi sen luomia raportteja Reports-ikkunassa ja sen monitoroimia palveluita Services-ikkunassa. Monet NMIS-ohjelman määritysten muutoksista tehdään itse käyttöjärjestelmässä konfigurointitiedostoja muokkaamalla.

NMIS on laaja, mutta ei kovinkaan selkeä monitorointiohjelma. Opmantekin sivustolla olevat asennusohjeet ja tarkat komennot olivat asennusvaiheessa tarpeen, mutta Linux-käyttöjärjestelmään perinpohjaisesti perehtymättömälle henkilölle komennot sekä niiden ja asennuspakettien tarkoitus jäivät epäselviksi. Myös itse ohjelman monitorointimääritteiden asettaminen ja monitorointidatan havainnoiminen oli hidasta ja vaikeaselkoista.

4.4 Observer Infrastructure

Network Instruments on vuonna 1994 perustettu yhdysvaltalainen tietoverkko- ja ohjelmahallintaratkaisuja kehittävä yritys. Nykyään yrityksen omistaa yhdysvaltalainen JDSU. JDSU on markkinajohtaja optisissa tietoliikenneverkoissa (optical communications networks), tietoliikenteen testaus- ja mittauslaitteissa, lasereissa ja muissa mukautetuissa optisissa laitteissa. Network Instruments toimii JDSU:n Performance Management -yksikkönä. [91.]

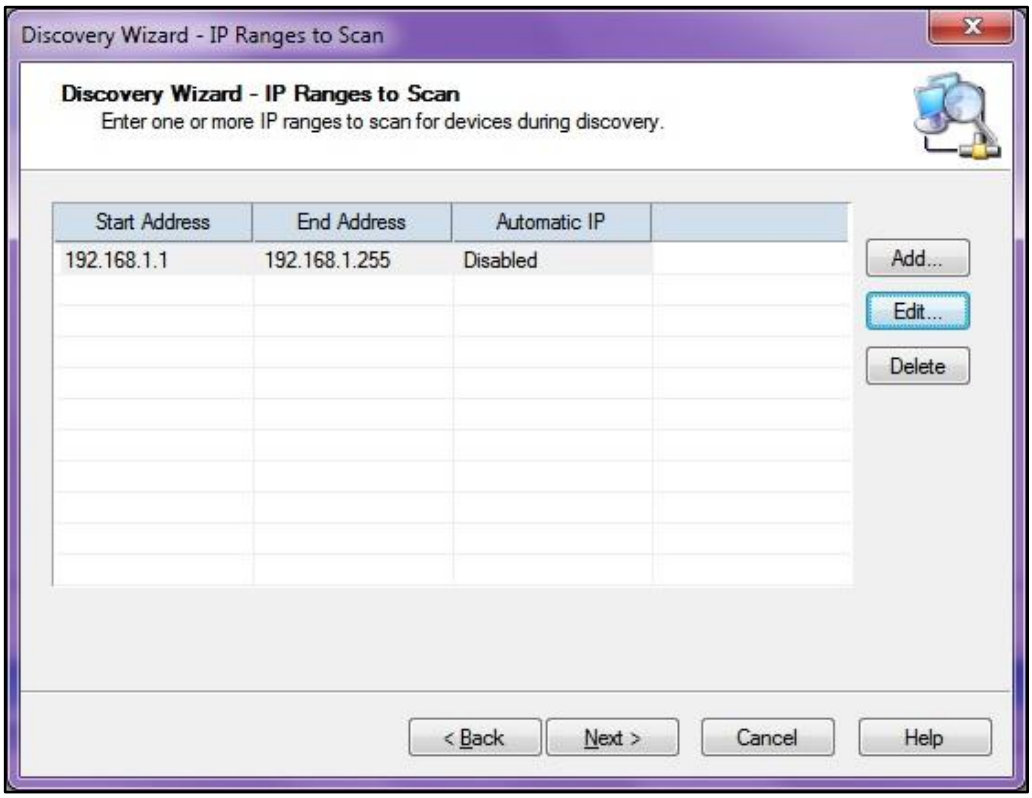
Observer Infrastructure -ohjelma, lyhyemmin OI, on Network Instrumentsin lippulaiva. OI:lla voidaan monitoroida verkkolaitteita, palvelimia, pilveä, palveluita ja applikaatioita. Ohjelman ilmainen käyttö on rajoitettu 10 laitteen monitorointiin. [92.]

Observer Infrastructure -ohjelman vähimmäisjärjestelmävaatimukset on listattu alla:

- tuplaydinprosessori tai neliydinprosessori
- 2 GB tai 4 GB RAM-muistia
- 250 GB tai 500 GB kovalevytilaa
- Windows XP. [93.]

Testausta varten asennettiin ohjelman 3.1-versio, sillä uudesta 4.0-versiosta oli testaushetkellä saatavilla vain demoversio [94]. Ohjelman asennustiedosto oli vain 60 MB, ja sen nopea asennus vei odotetusti vain muutaman minuutin. Epätavallista ohjelmalle oli se, että asennus ei luonut minkäänlaisia pikakuvakkeita tietokoneelle. Testikoneen virusohjelma piti kytkeä pois päältä ohjelman asennuksen ajaksi, koska se luokitteli asennustiedoston liian epäilyttäväksi ja näin esti Observer Infrastructuren asentumisen.

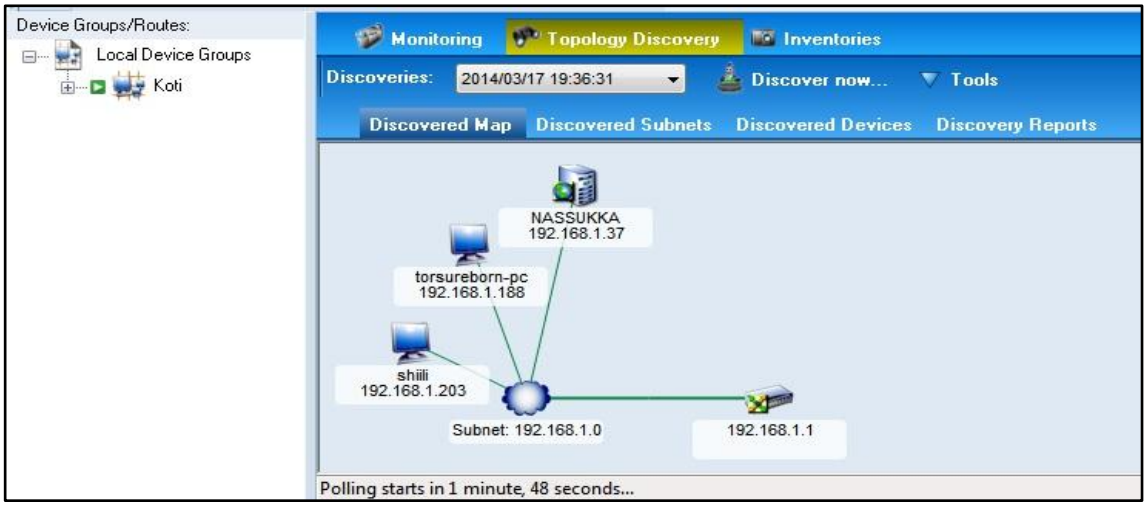
Observer Infrastructure avaa ensimmäiseksi verkkolaitteiden havaitsemisen ohjatun käyttöönoton toiminnon (kuva 9).



Kuva 9. Automaattinen verkkolaitteiden havaitseminen Observer Infrastructure -ohjelmassa.

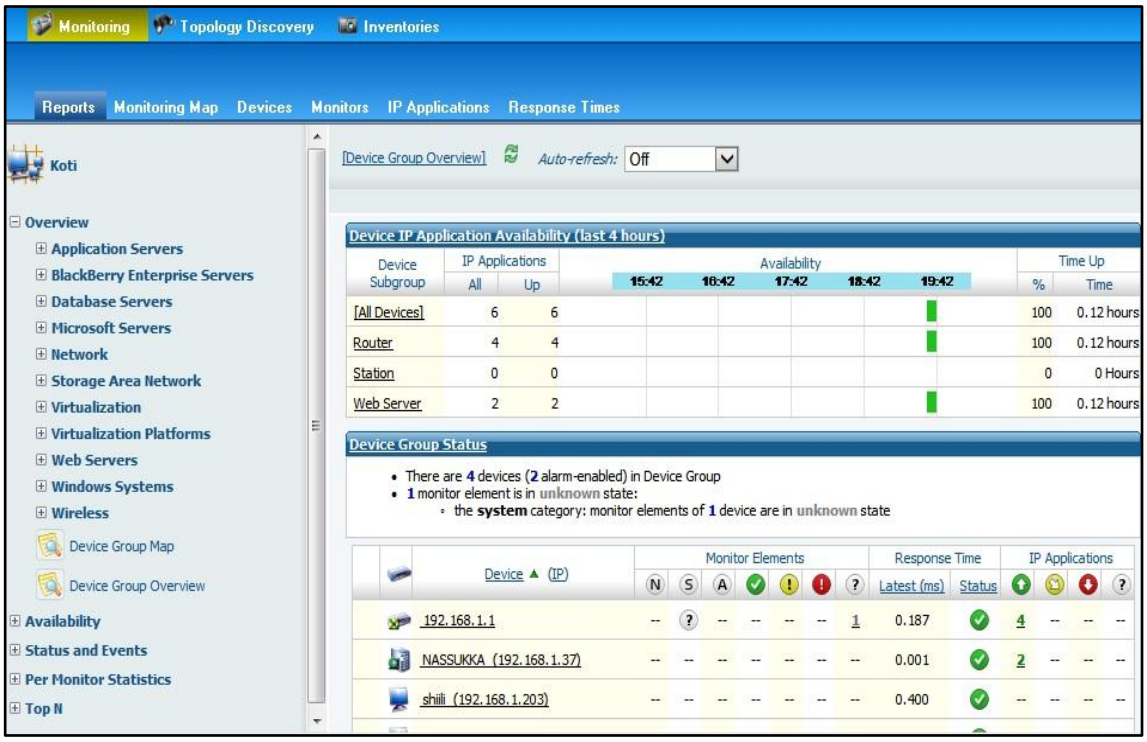
Ikkunassa tulee määrittää IP-osoiteavaruus, josta verkkolaitteita sekä monitoroitavia applikaatioita ja protokollia etsitään. IP-osoiteavaruuden määrittelykentässä on oletuksena aliverkko, johon ohjelman asennuksen sisältävä tietokone kuuluu.

Observer Infrastructuressa on listaus löydetyistä verkkolaitteista tietoineen, ja selkeä visuaalinen kartta verkon rakenteesta (kuva 10). Ohjelma rakentaa kartan verkkolaitteiden automaattisen havaitsemistoiminnon perusteella.



Kuva 10. Topologia Observer Infrastructure -ohjelmassa.

Ohjelmassa voidaan myös ajastaa määriteltyihin laiteryhmiin laitelistan päivitys (device group inventory). Ohjelma voi luoda raportteja esimerkiksi laitteiden saatavuudesta (device availability), hälytyslokitiedoista (alarm logs), porttien käytöstä (port usage) ja pakettien kulusta verkossa (kuva 11). Vaikka Observer Infrastructure toimii erillisenä ohjelmana, esimerkiksi raportteja voidaan näyttää myös Internet-selaimessa.



Kuva 11. Esimerkki raportoinnista Observer Infrastructure -ohjelmassa.

Observer Infrastructuren käyttöliittymä on selkeä, ja ohjelma toimii sujuvasti. Observer Infrastructure on myös yksi harvoista vertailuosion ohjelmista, joka tuottaa monitoroidusta verkosta helposti selkeän visuaalisen topologian.

4.5 op5 Monitor

op5 on vuonna 2004 perustettu ruotsalainen yritys, joka kehittää avoimen lähdekoodin hallintaratkaisuja. op5 on alansa markkinajohtaja [95]. Yrityksen lippulaiva on avoimen lähdekoodin monitorointiohjelma op5 Monitor, joka perustuu yhdysvaltalaisen Nagios Enterprises -yhtiön vuonna 1999 julkaistuun avoimen lähdekoodin Nagios-ohjelmaan (alkuperäisnimeltään NetSaint). [96; 97.] op5 Monitorilla voidaan monitoroida fyysisiä ja virtuaalisia palvelimia, verkkolaitteita, ohjelmia, palveluja, tietoverkkoja, pilveä ja suorituskykyä [98]. op5 Monitoria voidaan käyttää ilmaiseksi enintään 20 laitteen monitorointiin [99].

op5 monitor -ohjelman vähimmäisjärjestelmävaatimukset on listattu alla:

- Xeon E3-1220v2 neliydinprosessori
- 8 GB RAM-muistia
- 500 GB kovalevytilaa
- 64-bittinen Red Hat Enterprise Linux 6 / CentOS 6 / op5 APS. [100; 101.]

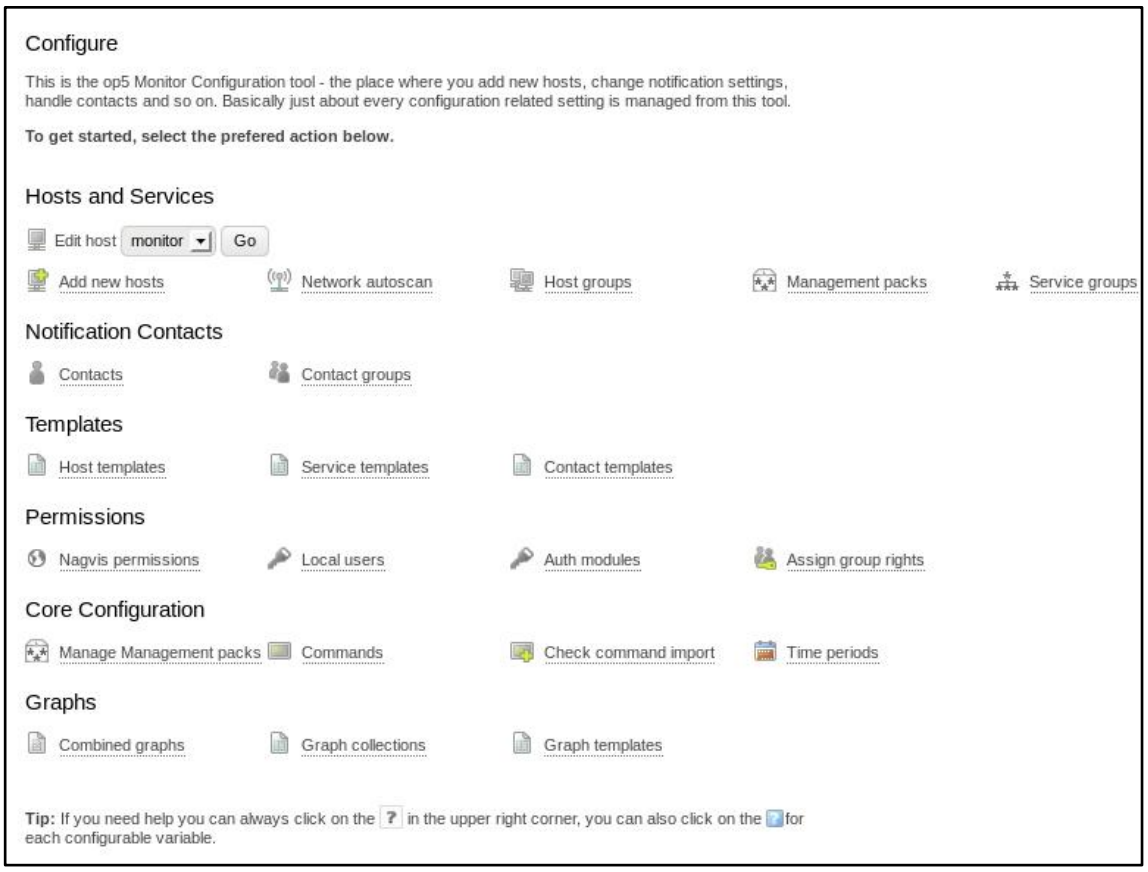
Testausta varten asennettiin ohjelman 6.2.1-versio [99]. Ohjelman asennustiedosto oli kooltaan 218,5 MB. Ohjelman asennus täytyi ajaa Linux-käyttöjärjestelmässä root-käyttäjänä eli järjestelmänvalvojaoikeuksin.

op5 Monitorissa on selainkäyttöliittymä. Ohjelmaan pääsee käsiksi syöttämällä Internet-selaimen osoitekenttään asennuksen sisältävän tietokoneen IP-osoitteen. Login-kirjautumisruudussa syötetään käyttäjänimi- ja salasanakenttiin molempiin sekä oletuskäyttäjäksi että oletussalasanaksi op5-yrityksen määrittelemä ”monitor” [102].

Kirjautumisen jälkeen op5 Monitorissa käynnistyy ohjattu käyttöönotto. Ikkunasta voidaan valita halutaanko ohjatun käyttöönoton avautuvan joka kirjautumiskerralla vai vain tämän kerran. Ensimmäinen vaihe ohjatussa käyttöönotossa on laitetyyppi (device ty-

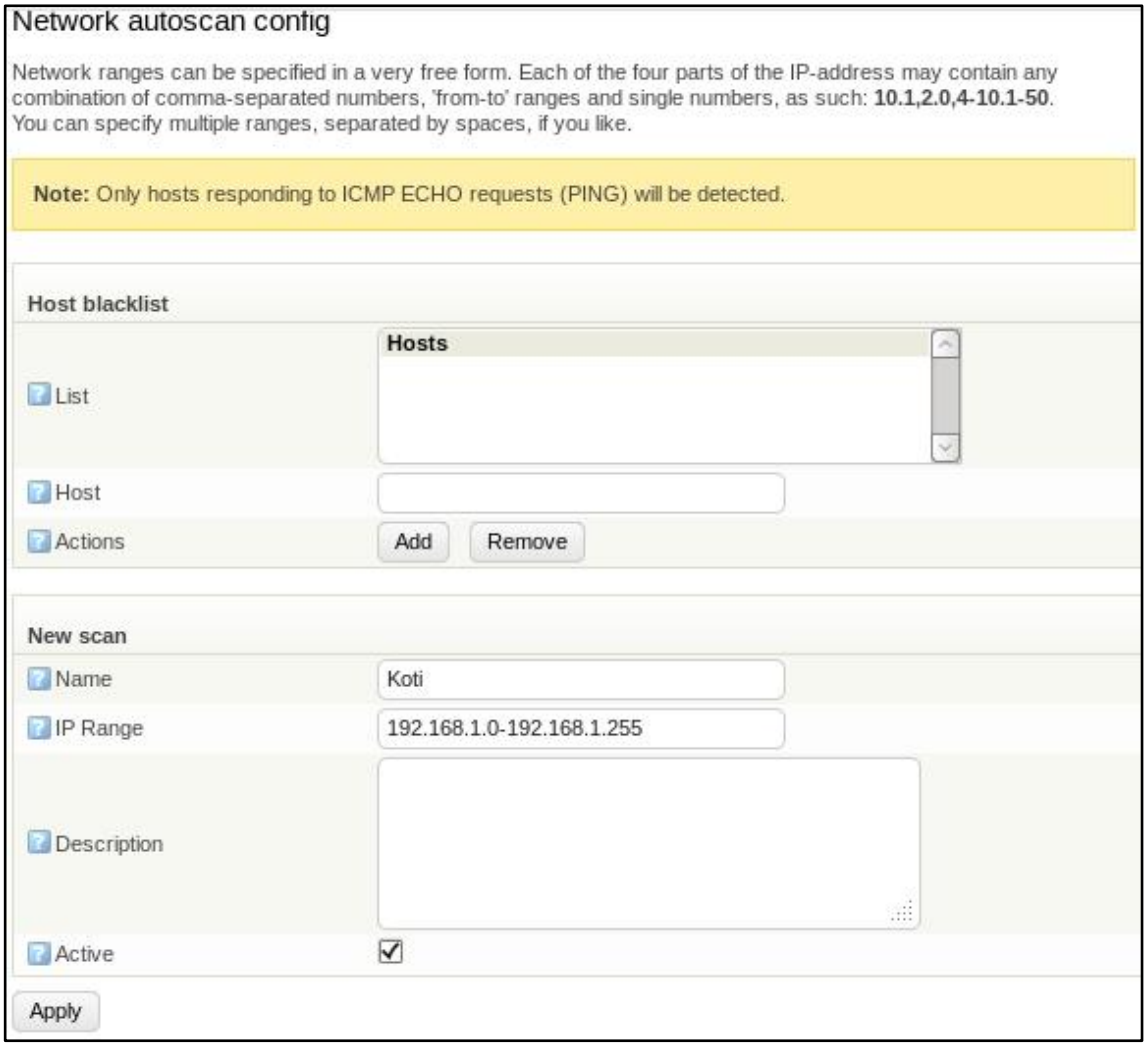
pe). Tässä vaiheessa tulee määritellä yksi tai useampi hallintapaketti (management pack), joka kuvaa monitoroitavaksi haluttavia laitteita. Vaihtoehtoja ovat DNS-palvelin, yleinen palvelin, erillinen Vmware-virtuaalikone, Web-palvelin, HTTPS-protokollaa käyttävä Web-palvelin, ja Windows-palvelin. Toisessa ohjatun käyttöönoton vaiheessa voidaan määritellä nimet ja IP-osoitteet laitteille, joita halutaan monitoroida. Ohjatun käyttöönoton lopuksi määritetyt asetukset tallennetaan.

op5 Monitorin asetuksia voidaan muuttaa Configuration-valikosta valitsemalla vaihtoehdon ”Configure”. Avautuvasta näkymästä voidaan määrittää esimerkiksi oikeuksia, diagrammeja, lisää monitoroitavia verkkolaitteita sekä määritellä ohjelmalle automaattisen verkkolaitteiden havaitsemistoiminnon (kuva 12).



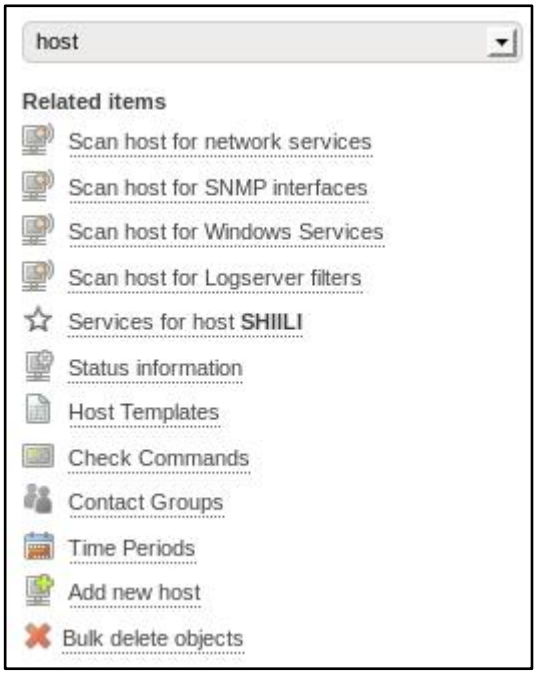
Kuva 12. Configure-näkymä op5 Monitor -ohjelmassa.

Automaattisessa verkkolaitteiden havaitsemistoiminnossa määritellään tallennettaville havaitsemisasetuksille nimi ja IP-osoiteavaruus, josta laitteita tulee etsiä, kohdassa "Network autoscan" (kuva 13). Ohjelma suorittaa havaitsemisen taustalla ja ilmoittaa löytyneistä laitteista.



Kuva 13. Automaattinen verkkolaitteiden havaitseminen op5 Monitor -ohjelmassa.

Monitoroitavista laitteista voidaan erikseen etsiä esimerkiksi palveluita valitsemalla Configure-kohdasta alasvetovalikosta laitteen ja napsauttamalla Edit-nappia. Aukeavassa näkymässä voidaan valita erilaisia toimenpiteitä tehtäväksi laitteelle, kuten edellä mainittu palvelujen etsiminen valitsemalla "Scan host for network services" (kuva 14).



Kuva 14. Esimerkki suoritettavista toiminnoista op5 Monitor -ohjelmassa.

op5 Monitorilla voidaan listata monitoroitavat laitteet, palvelut ja näiden ongelmat. Ohjelmalla voidaan tarkastella ja ajastaa raportteja, tarkastella verkon rakennetta ohjelman perustamasta kartasta ja määrittää esimerkiksi, missä vaiheessa ohjelma lähettää hälytyksiä ja mitä kautta se ilmoittaa näistä järjestelmänvalvojalle.

op5 Monitorissa on laaja kirjo asetuksia, mutta ne eivät ole helposti löydettävissä. Tästä syystä op5 Monitorin käyttö vaatii enemmän opettelua kuin tähän asti vertailussa käsitellyt muut ohjelmat.

4.6 Pandora Flexible Monitoring System

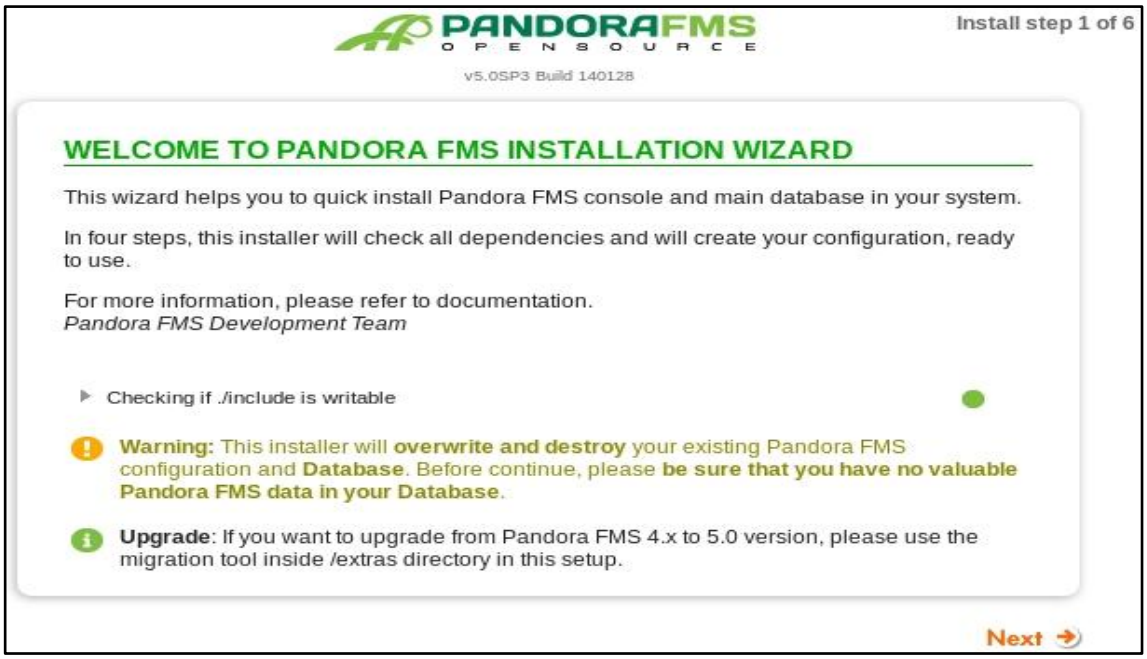
Ártica Soluciones Technológicas on vuonna 2005 perustettu espanjalainen yritys, joka on erikoistunut ohjelmakehitykseen, IT-hallintaan, tietoturvaan ja tietoverkkoihin [103]. Yrityksen omistamaa avoimen lähdekoodin Pandora Flexible Monitoring System -ohjelmaa, lyhyemmin Pandora FMS, alettiin ohjelmoida jo vuonna 2003 ohjelman alkuperäisen kehittäjän Sancho Lerenan toimesta [104]. Pandora FMS:llä voidaan monitoroida tietoverkkoja, ohjelmia, palvelimia, suorituskykyä, Internet-ympäristöä ja virtuaalista infrastruktuuria [105]. Pandora FMS:n ilmaisversiolla monitoroitavaa laitemäärää ei ole rajoitettu, mutta ohjelmasta puuttuu esimerkiksi palvelujen monitorointi, joka löytyy

maksullisista versioista. Ilmaisversion ominaisuudet ovat kuitenkin lukuisat ja hyvin tähän työhön riittävät. [106.]

Pandora FMS -ohjelman vähimmäisjärjestelmävaatimukset on listattu alla:

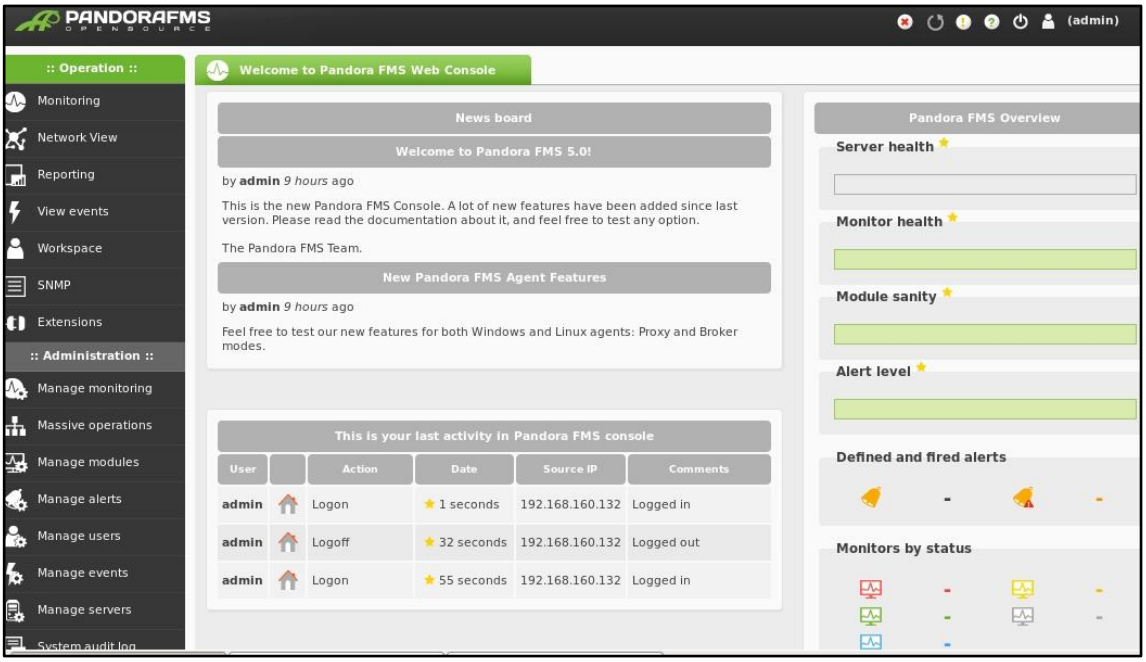
- 2,5 GHz:n prosessori
- 3 GB RAM-muistia
- 15 GB kovalevytilaa
- Red Hat Enterprise 6 / CentOS 6 / SLES 11 SP1 / OpenSUSE 11 SP1 / Debian 5 / Ubuntu 11. [107.]

Testausta varten asennettiin ohjelman 5.0-versio. Ohjelman asennustiedosto on helpointa hakea suoraan Linux-käyttöjärjestelmässä pakettivaraston (software repository) kautta Pandora FMS:n sivuilla olevien asennusohjeiden mukaisesti. [107.] Asennuspaketin hakemisessa ja tiedostojen asentamisessa kului aikaa lähinnä käyttöjärjestelmän päivittämiseen Pandora FMS:n tarvitsemin palvelupaketein ja lopulta asennuksen tähän vaiheeseen kului aikaa lähes kaksi tuntia. Tämän jälkeen Internet-selaimen kautta suoritettiin ohjelman ohjattu asennuksen niin kutsuttu viimeistely (kuva 15). Tähän selainkonsolin ja päätietokannan asentamiseen kului vain muutama minuutti. Asennuksen jälkeen asennuksen php-tiedosto tuli tuhota.



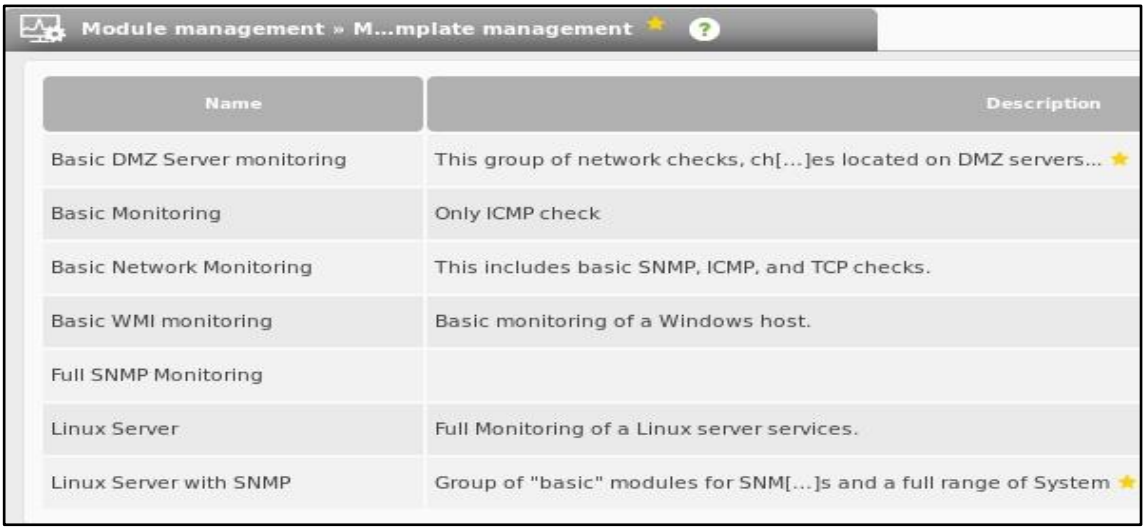
Kuva 15. Pandora FMS -ohjelman asennuksen viimeistely.

Pandora FMS-ohjelmassa on selainkäyttöliittymä. Kirjautuminen tapahtuu oletuskäyttäjänimellä ja -salasanalla, jotka ovat ”admin” ja ”pandora”, ohjelman asennuksen lopussa ilmoitetusti. Kirjautumisen jälkeen ohjelmasta avautuu Web-konsolisivu, josta löytyvät kaikki tarvittavat valikot ja tiedot monitoroinnin tilasta (kuva 16).



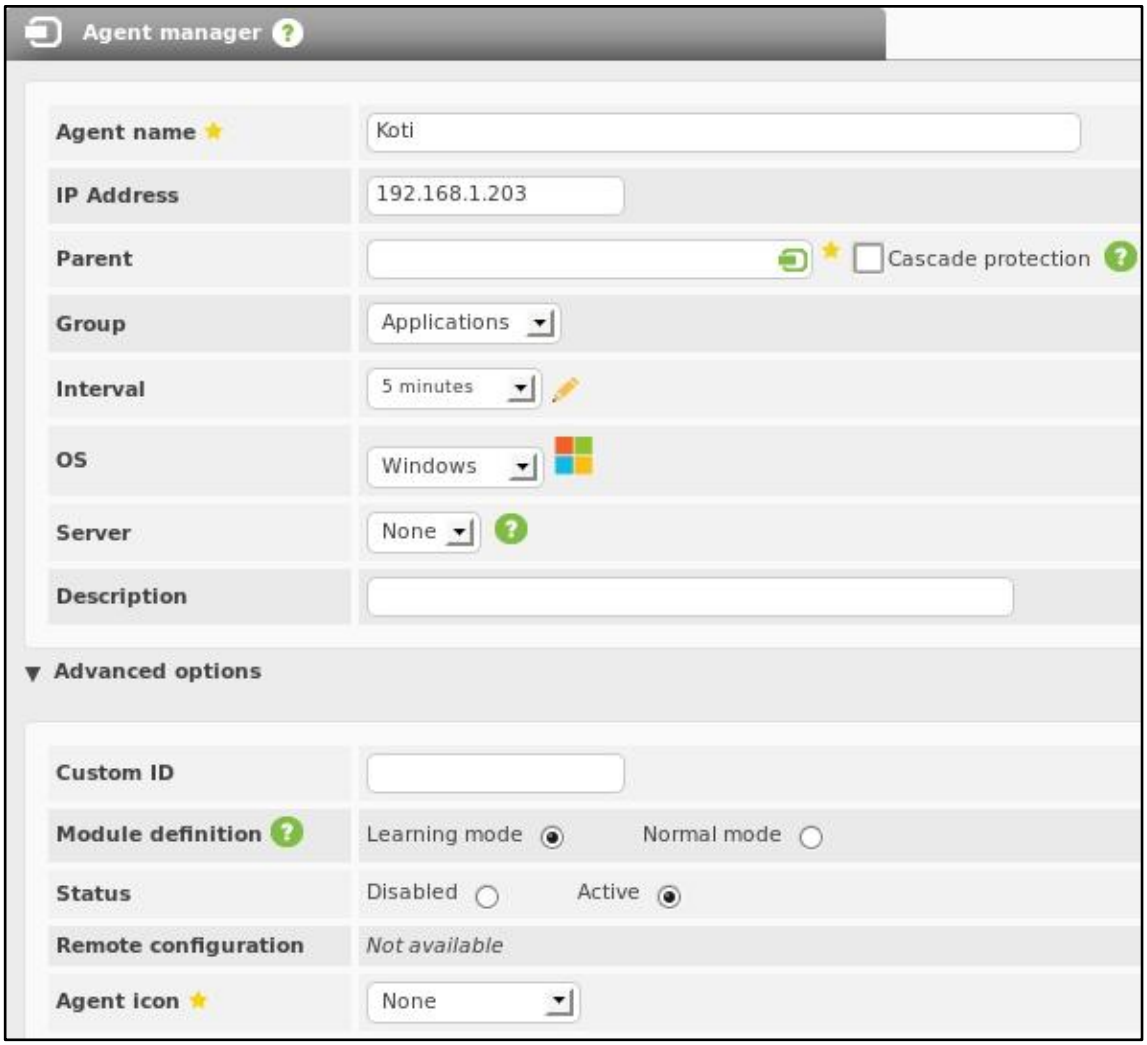
Kuva 16. Pandora FMS -ohjelman pääsivu.

Administration-sarakkeesta voidaan valita minkälaisia moduuleja monitoroidaan, esimerkiksi verkon perusmonitorointi (kuva 17).



Kuva 17. Monitorointimoduulien valinta Pandora FMS -ohjelmassa.

Administration-sarakkeesta voidaan määritellä myös verkossa monitoroitava laite. Löydettyjen laitteiden monitorointia hallitaan ohjelman Administration-sarakkeen Manage monitoring -valinnan kautta Agent manager -toiminnossa (kuva 18).



Kuva 18. Esimerkki laitemonitoroinnin hallinnasta Pandora FMS -ohjelmassa.

Ohjelma voi muodostaa monitoroiduista laitteista visuaalisen rakennekartan. Ohjelmassa voidaan myös määritellä eri hälytyksiä ja ne voidaan määrittää esimerkiksi lähettämään järjestelmänvalvojalle sähköpostia hälytyksen sattuessa.

Pandora FMS:n monitoroinnin määrittäminen ei ole niin suoraviivaista kuin testatuissa Windows-käyttöjärjestelmälle rakennetuissa monitorointiohjelmissa, mutta sen tarjoamat monitorointimahdollisuudet ovat kohtuulliset. Ohjelman suurin kompastuskivi on asennusvaihe, joka tuottaa vaikeuksia Linux-käyttöjärjestelmään laajemmin perehtymättömälle järjestelmänvalvojalle.

4.7 PRTG Network Monitor

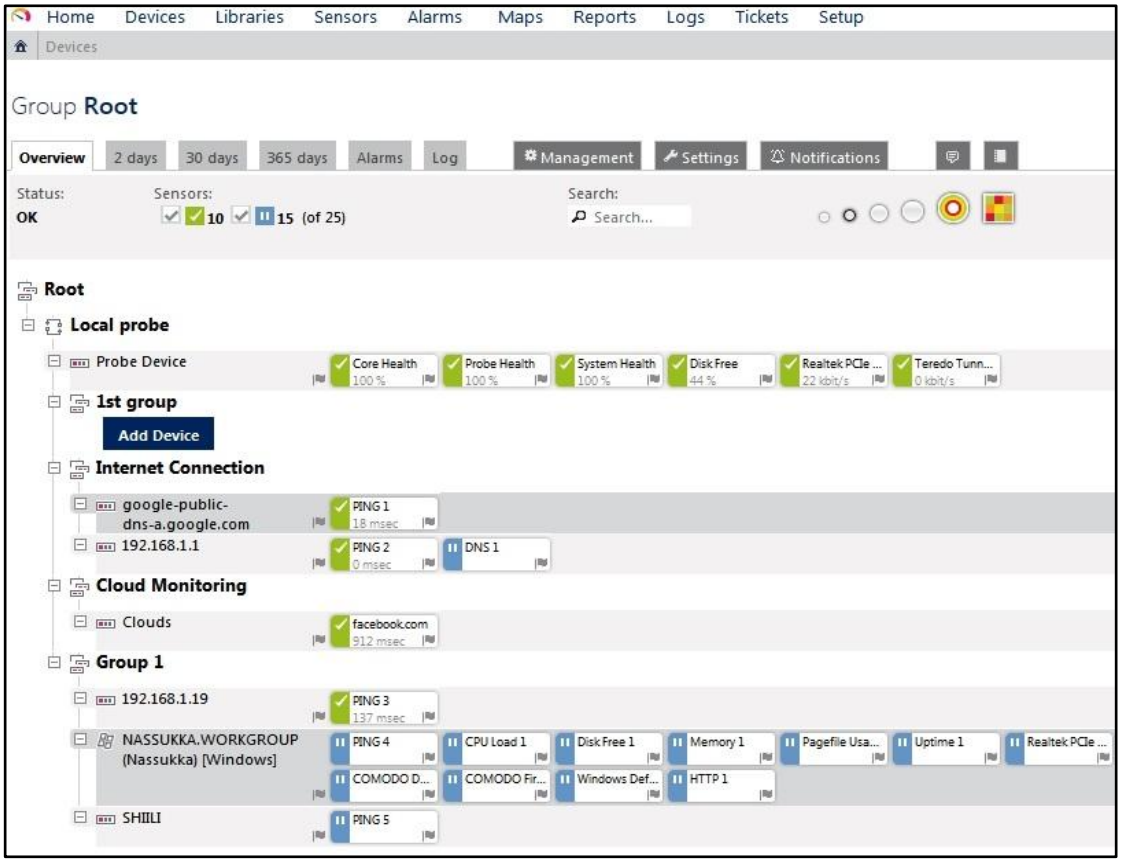
Paessler AG on vuonna 1997 perustettu saksalainen verkkomonitorointi- ja testausratkaisuja tarjoava yritys [108]. Yrityksen PRTG Network Monitor -ohjelmalla voidaan monitoroida tietoverkkoja, ohjelmia, virtuaalipalvelimia, kaistanleveyttä ja palvelutasosopimuksia (SLA, Service Level Agreement) [109]. Ohjelmaa voidaan käyttää ilmaiseksi monitorointiin enintään 10 sensorilla [110]. Paessler määrittää yhdeksi sensoriksi yhden yksittäisen monitorointikokonaisuuden (monitoring entity) eli yksi sensori vastaa esimerkiksi yhtä URL-osoitetta, yhtä tietoliikenneyhteyttä tai yhtä kytkimen porttia [111].

PRTG Network Monitor -ohjelman vähimmäisjärjestelmävaatimukset on listattu alla:

- keskimääräisen, vuoden 2007 jälkeen rakennetun PC:n prosessorin teho
- 1024 MB RAM-muistia, 150 KB RAM per sensori
- 200 KB kovalevytilaa per sensori
- Windows XP SP2 / Windows Server 2003 SP1 / Windows Server 2008 R2. [112.]

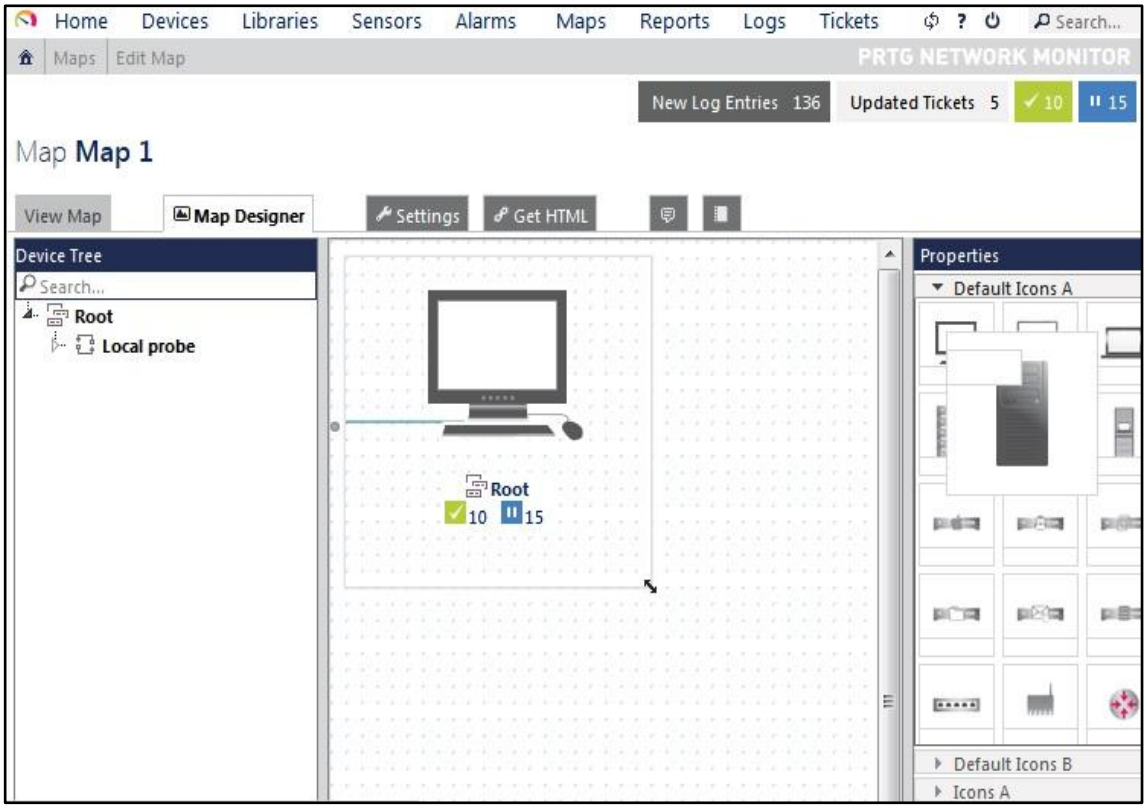
Testausta varten asennettiin ohjelman 14.1-versio [113]. Ohjelman asennustiedosto oli kooltaan 124 MB, ja asennus vei vain muutaman minuutin.

PRTG Network Monitor toimii selainkäyttöliittymällä. Ensimmäisellä käynnistyskerralla ohjelmassa aukeaa ”Guru” eli ohjattu käyttöönotto. Gurussa tulee ensimmäiseksi määritellä järjestelmänvalvojan käyttäjätili monitoroitaville laitteille. Gurussa määritellään myös IP-osoiteavaruus automaattista verkkolaitteiden havaitsemista varten sekä mitä palvelimia ja palveluita verkossa tulee monitoroida. IP-kenttään ohjelma kirjaa oletukseksi ohjelman asennuksen sisältävän koneen aliverkon. PRTG Network Monitorin automaattinen verkkolaitteiden havaitsemisvaihe on huomattavan hidas toimenpide verrattuna muihin testattuihin monitorointiohjelmiin (kuva 19).



Kuva 19. Automaattinen verkkolaitteiden havaitseminen PRTG Network Monitor -ohjelmassa.

PRTG Network Monitorissa saadaan asetettua lukuisia eri laukaisutekijöitä hälytyksiä varten, esimerkiksi monitoroitavan kokonaisuuden nopeuden vaihtelut (speed), määritetyn kynnyksen ylitys (threshold) ja tilan muutos (change). Hälytykset voidaan määritellä esimerkiksi lähettämään järjestelmänvalvojalle sähköpostia hälytyksen tapahtuessa. Ohjelma voi myös tuottaa hälytyksistä ja monitorointitiedoista erilaisia raportteja. Ohjelmassa ei ole selkeää visuaalista karttaa monitoroidusta verkosta ja sen rakenteesta, jos sitä ei rakenna itse ohjelman Map Designer -osiossa (kuva 20).



Kuva 20. PRTG Network Monitor -ohjelman monitoroidun verkon rakennekartan muodostus.

PRTG Network Monitorin ilmainen versio on todella rajoitettu, sillä kymmenen sallitun sensorin raja rikkoutuu jo normaaleista ping-komennoista. Kaikista havaituista verkkolaitteista ei täten saanut edes varmistettua laitteen saatavuutta muuttelematta sensoreita jatkuvasti (kuva 19). Tästä syystä ilmaisesta versiosta ei saanut kunnollista käsitystä ohjelman mahdollisuuksista. Myös Map Designer -osion manuaalisen rakennekartan muodostaminen on käytännössä työlästä, joten PRTG Network Monitorilta jäi kaipaamaan automaattisesti verkon rakennekartan muodostavaa ominaisuutta.

4.8 Ohjelmavertailu

Työhön valittuja ohjelmia vertailtaessa kiinnitettiin huomiota ohjelman testiasennus- ja -käyttökokemukseen, ominaisuuksiin ja rajoituksiin. Tärkeimmät vertailutiedot on koottu taulukkoon 1.

Taulukko 1. Valittujen ohjelmien vertailu testauksen ja ominaisuuksien mukaan.

Ohjelma	**Asennus**	**Käyttö**	**Topologia**	**Rajoitukset**
CA Nimsoft Monitor Snap	hidas	hidas	vain maksullisessa versiossa	30 laitetta
Heroix Longitude	helppo	helppo	ei	5 laitetta ja 2 virtuaalikonetta
NMIS	vaikea	vaikea	ei	ei
OI	helppo	helppo	kyllä	10 laitetta
op5 Monitor	helppo	vaikea	kyllä	20 laitetta
Pandora FMS	vaikea	kohtuullinen	kyllä	rajoitetut ominaisuudet
PRTG Network Monitor	helppo	helppo	manuaalinen	10 sensoria

Lisäksi huomioitiin se, että monitoroitavien laitteiden määrä saattaisi tulevaisuudessa kasvaa. Täten myös skaalautuvuus ja laitemäärän kasvusta mahdollisesti koituvat kustannukset otettiin mukaan vertailuun. Nämä vertailutiedot on koottu taulukkoon 2.

Taulukko 2. Valittujen ohjelmien vertailu tulevaisuuden lisälaitetarpeen mukaan.

Ohjelma	**Skaalautuvuus**	**Laitteiden lisäys**	**Lisäyksen hinta**
CA Nimsoft Monitor Snap	hyvä	maksullinen versio	tarjouksen mukaan
Heroix Longitude	hyvä	maksullinen versio	10 laitetta 290 e/vuosi - 1 000 laitetta 4 340 e/vuosi [114]
NMIS	hyvä	kyllä	ilmainen [86]
OI	hyvä	maksullinen versio	tarjouksen mukaan [115]
op5 Monitor	hyvä	maksullinen versio	25 laitetta 45 e/kk (540 e/vuosi) -tarjouksen mukaan [116]
Pandora FMS	hyvä	ei rajoitettu, lisäominaisuudet maksullisessa versiossa	ilmainen, ominaisuuksienlisäys tarjouksen mukaan [106]
PRTG Network Monitor	hyvä	maksullinen versio	100 sensoria 330 e - Corporate 5 Core Global 35 000 e [117]

Taulukon 1 Asennus- ja Käyttö-sarakkeiden perusteella helppokäyttöisimpiä ja selkeimpiä ohjelmia tämän työn käyttötarkoitukseen olivat Heroix Longitude, OI, op5 Monitor ja PRTG Network Monitoring. Näistä topologian puolesta jatkoon pääsivät OI ja op5 Monitor. Viimeisen sarakkeen rajoituksien perusteella op5 Monitor on 20 laitteellaan parempi kuin 10 laitteen OI. Taulukon 1 perusteella vertailluista ohjelmista paras olisi siis op5 Monitor.

Jokainen vertailtu ohjelma skaalautuu hyvin, joten taulukossa 2 Skaalautuvuus-sarakkeesta voidaan suoraan hypätä Laitteiden lisäys -sarakkeeseen. Jos taulukon 1 alkuvertailussa helppokäyttöisimmiksi ja selkeimmiksi valittujen ohjelmien Heroix Longitude, OI, op5 Monitor ja PRTG Network Monitoring lisälaitemahdollisuutta ja lisäyksen hintaa tarkastellaan, näissä kaikissa ohjelmissa lisälaitteita voidaan monitoroida vasta maksullisessa versiossa. Taulukon 2 tärkein sarake on täten ”Lisäyksen hinta”. Heroix Longitude -ohjelman laitemäärän lisäyksen hinta on vähintään 290 e/vuosi 10 laitteelta. OI:sta ei löydy tietoja, koska hinnat määräytyvät yrityksille räätälöityjen tarjoushintojen perusteella. op5 Monitorin lisälaitteiden hinta on vähintään 45 e/kk 25 laitteelta. Kuten alla olevasta yhtälöstä näkyy, kertomalla summan kahdellatoista tämä tekisi vuodessa 540e samalta määrältä laitteita:

$$45e/kk * 12 = 540e$$

PRTG Network Monitoring laskee laitelisäykset sensoreittain eli tosiasiassa tarvittava lisälaitemäärä olisi sensoreittain laskettuna paljon suurempi ja täten kalliimpi, kuin sama laitemäärä muilla ohjelmilla. PRTG:n hintatietoja ei pysty tämän takia rinnastamaan toisten ohjelmien hintatietojen kanssa, koska hinta riippuu paljolti, kuinka montaa eri asiaa laitteilla monitoroidaan.

Annettujen tietojen perusteella Taulukon 2 pohjalta ovat vertailtavissa Heroix Longitude ja op5 Monitor. Jotta vertailu voidaan tehdä saman laitemäärän hinnasta, lasketaan op5 Monitorin 25 laitteen 45 e/kk hinnasta ensin yksikköhinta alla olevan yhtälön mukaan:

$$\frac{45e/kk}{25} = 1{,}80e/kk$$

Yhtälöstä saatiin yksikköhinta 1,80 e/kk. Seuraavaksi lasketaan 10 laitteen kuukausihinta kertomalla yksikköhinta laitemäärällä seuraavassa yhtälössä:

$$1{,}80e/kk * 10 = 18e/kk$$

Yhtälöstä saatiin op5 Monitor -ohjelman 10 laitteen kuukausihinnaksi 18 e/kk. Viimeisessä yhtälössä lasketaan ohjelman 10 laitteen hinta vuodessa kertomalla kuukausihinta kahdellatoista:

$$18e/kk * 12kk = 216e$$

Lopulliseksi op5 Monitorin 10 laitteen hinnaksi vuodessa saadaan siis 216 euroa. Verrattaessa tätä 10 laitteen hintaa 216 e/vuosi Heroix Longituden saman laitemäärän hintaan 290 e/vuosi, op5 Monitor nousee jälleen vertailuvoittajaksi. op5 Monitor on täten vertailun paras ohjelma sekä taulukon 1 että taulukon 2 perusteella.

5 Metropolia Ammattikorkeakoulun monitorointiratkaisu

Metropolia Ammattikorkeakoulun Bulevardin toimipisteessä Helsingissä haluttiin ottaa käyttöön verkonmonitorointijärjestelmä tietoverkkolaboratorion opetusrunkoverkon monitorointia varten. Järjestelmän haluttiin monitoroivan verkkolaitteista pääasiassa reitittimiä ja kytkimiä. Ohjelman tuli olla ilmainen ja tarvittaessa laajennettavissa kattamaan suuremman verkon monitoroinnin. Ohjelman tuli myös pystyä käyttämään hyväkseen verkkolaitteiden tuottamaa NetFlow-tietoa.

Luvun 4 vertailun perusteella ohjelmaksi valittiin op5 Monitor. Se tarjosi monitorointimahdollisuuden ilmaiseksi suurimmillaan kahdelle kymmenelle verkkolaitteelle, joka oli riittävä haluttujen operaattorirunkoverkon laitteiden seurantaan. Monitoroinnin mahdollinen laajentaminen tulevaisuudessa tulisi kustantamaan vähintään 216 euroa vuodessa, joka oli hyväksyttävä määrä. op5 Monitor tarjosi myös avoimen lähdekoodin ohjelmana muokkaamismahdollisuutta Metropolian mahdollisiin lisätarpeisiin.

5.1 op5 Monitorin asennus ja konfigurointi

Metropolian verkossa olevalle palvelimelle oli valmiiksi asennettu käyttöjärjestelmäksi CentOS 6. Bulevardin toimipisteen verkkolaboratoriossa palvelimeen otettiin SSH-yhteys verkon yli Putty-etäyhteysohjelmalla ja kirjauduttiin sisään root-pääkäyttäjänä. Palvelimelle vaihdettiin kiinteä IP-osoite 10.95.250.76 ja tarvittavat DNS-palvelin- ja yhdyskäytävätiedot. Tämä tehtiin muokkaamalla ifcfg-eth0-tiedostoa, joka sijaitsee

käyttöjärjestelmän /etc/sysconfig/network-scripts-kansiossa. Muokkaus tehtiin Linux-pohjaisilla käyttöjärjestelmillä käytössä olevalla nano-tekstieditorilla:

nano /etc/sysconfig/network-scripts/ifcfg-eth0

ifcfg-eth0-tiedosto sisältää Ethernet-verkkorajapinnan tiedot. Tiedoston muokkauksen jälkeiset tiedot ovat liitteessä 1.

Palvelimelle kopioitiin pakattu op5 Monitor -ohjelman 6.2.1-version asennustiedosto, joka purettiin Unix-järjestelmien tar-tiedostonkäsittelykomennolla seuraavasti:

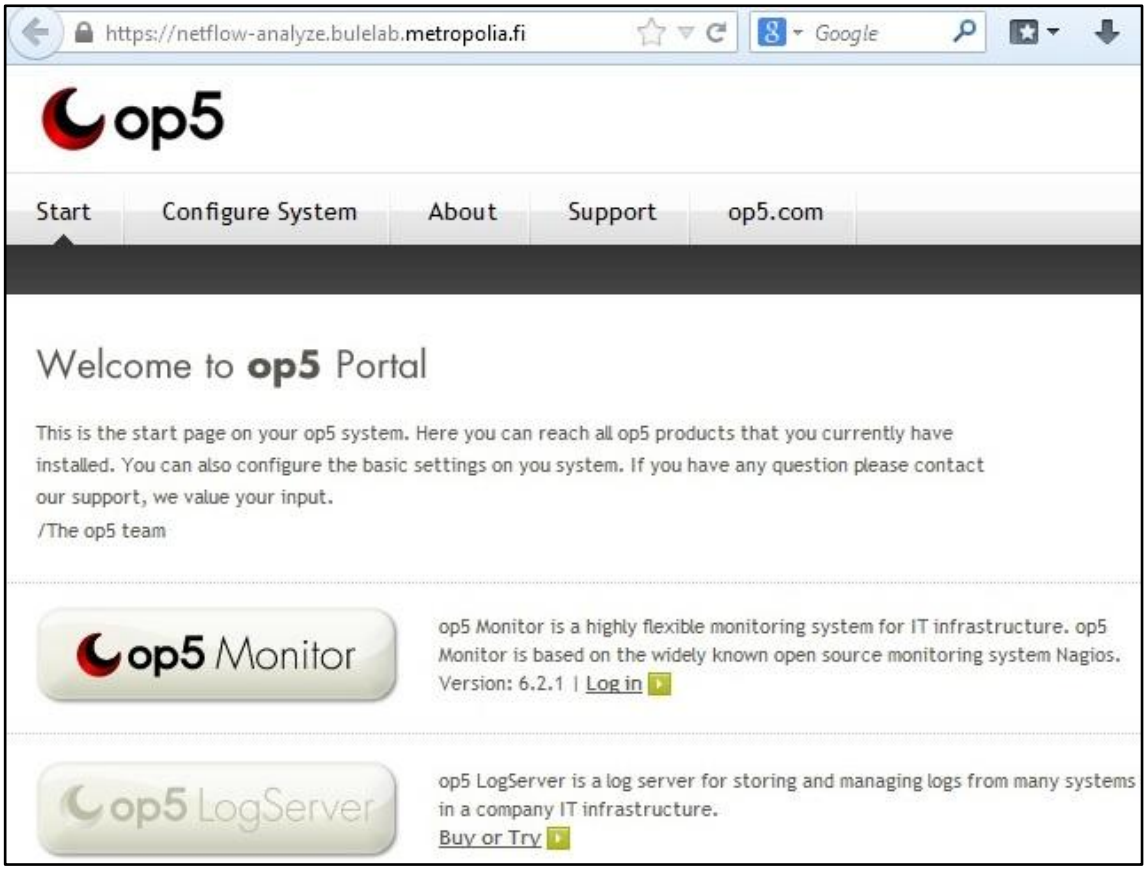
tar zxfv op5-monitor-6.2.1-20131220.tar.gz

Tar-komennon z-valinta tarvitaan, jotta tar pystyy käsittelemään gz-loppuisia pakattuja tiedostoja. Komennon x-valinta (extract) tarvitaan, kun pakattu tiedosto tulee purkaa. Valinta ”f” (file) mahdollistaa arkistotiedoston käytön, ja valinnalla ”v” (verbose) saadaan purkutoimenpiteestä näkyviin yksityiskohtaiset tiedot komentoriville.

Tar-paketista puretusta kansiosta ajettiin install-komennolla install.sh-skripti, joka aloitti ohjelman asennuksen:

install install.sh

Asennus onnistui ongelmitta, minkä jälkeen SSH-yhteys palvelimeen suljettiin. Palvelimen osoitteelle oli valmiiksi asetettu DNS-nimi ”netflow-analyze.bulelab.metropolia.fi”, joten op5 Monitor -ohjelmaan päästiin käsiksi avaamalla selain ja kirjoittamalla osoitekenttään palvelimen nimi. Aloitussivu näkyy kuvassa 21 alla.



Kuva 21. op5 Monitor -ohjelman kirjautumissivu.

op5 Monitoriin kirjauduttiin oletustunnuksella ja oletussalasanalla ”monitor”. Onnistuneen kirjautumisen jälkeen ilmestyvästä ohjelman esittelyikkunasta valittiin ”Skip this introduction in the future”-vaihtoehto, jotta ikkuna ei enää ilmestyisi kirjautumisen yhteydessä. Seuraavaksi ohjelmassa avautui Management pack -valintaikkuna. Vaikka Metropolian ei ollut tarkoitus monitoroida palvelimia, annetuista palvelinmonitorointivaihtoehdoista oli pakko valita vähintään yksi. Vaihtoehdoista valittiin ”generic server” eli yleinen palvelin. Palvelimen nimi- ja IP-tietokenttiin syötettiin op5 Monitor -ohjelman asennuksen sisältävän palvelimen tiedot.

Jotta op5 Monitor pystyisi monitoroimaan haluttuja verkkolaitteita, verkkolaitteiden IP-osoitteet tai IP-osoiteavaruudet piti syöttää ohjelmaan. Verkon monitoroitavaksi haluttujen Juniper-laitteiden IP-osoitetiedot saatiin selville Metropolia Ammattikorkeakoululle tehdyn projektityön ”Operaattorirunkoverkon rakentaminen Metropolian laboratoriokäyttöön” dokumentaatiosta ja Cisco-laitteiden tiedot tämän päättötyön ohjaajalta [118]. Näiden laitteiden lisäksi haluttiin monitoroida verkkoliikennettä opetusrunkoverkon ja tietoverkkolaboratorion välillä. Nämä laitteet oli valmiiksi konfiguroitu, ja laitteiden IP-

osoitetiedot selvitettiin työn ohjaajalta. op5 Monitorissa valittiin ohjelman Configurations-välilehdeltä kohta ”Add new hosts” eli uusien laitteiden lisäys. Tältä uudelta sivulta napsautettiin verkon tutkimislinkkiä ”Network scan”. Kenttiin syötettiin Juniper-laitteiden testikäyttöön tarkoitettujen Loopback-rajapintojen eli silmukkaliitäntöjen IP-osoitteet, Cisco-laitteiden GigabitEthernet-rajapintojen IP-osoitteet ja laboratorioverkkoon kytkettyjen laitteiden IP-osoitteet sekä nämä IP-osoitteet käsittävät aliverkot ja lopuksi napsautettiin ”Scan ranges”-etsinnänaloituspainiketta (kuva 22).

Kuva 22. Uusien verkkolaitteiden lisäys op5 Monitor -ohjelmassa.

op5 Monitor löysi kaikki halutut verkkolaitteet osoitetietojen perusteella, joten kaikki laitteet määriteltiin monitoroitavaksi. op5 Monitor tutki verkkolaitteet automaattisesti palvelujen varalta ja löysi laitteilta ping- ja SSH-palvelut, jotka otettiin mukaan monitorointiin. Jotta op5 Monitor pystyisi monitoroimaan verkkolaitteiden portteja ja rajapintoja, verkkolaitteet piti konfiguroida lähettämään op5 Monitorille SNMP- sekä NetFlow-dataa tarkempia tietoja varten. Nämä laitekonfiguroinnit on selitetty seuraavissa alaluvuissa 5.2 sekä 5.3. Juniper-laitteiden tarkat konfiguraatiotiedostot löytyvät liitteistä 2-9 ja tarkistuskomennot liitteistä 10-17. Cisco-laitteiden tarkat konfiguraatiotiedostot löytyvät liitteistä 18 ja 19 sekä tarkistuskomennot liitteistä 20-22.

5.2 Juniper-laitteet

Metropolian verkossa olevista Juniper-laitteista runkoverkon reitittimet olivat m20-mallisia ja Turun, Helsingin ja Tampereen kytkimet ex4200-24f-mallisia. Paikkakuntien Juniper-verkkojen topologiat on kuvattu liitteissä 23-25. Kaikki laitteet konfiguroitiin ottamalla laitteelle SSH-yhteys Putty-ohjelmalla. Ensimmäiseksi laitteet piti konfiguroida tuottamaan SNMP-tietoa. Tämä tehtiin editoimalla laitteen SNMP-palvelua:

root@turku-bbrtr01#edit snmp

Laitteelle tuli asettaa SNMP-yhteisötunnus sekä oikeudet yhteisö-tietoihin. Yhteisönimeksi valittiin ”junipersnmp” ja yhteisötietoihin annettiin sekä luku- että kirjoitusoikeudet:

root@turku-bbrtr01#set community “junipersnmp” authorization read-write

Laitteelle määritettiin SNMP-ilmoitusryhmä (SNMP trap group) laitteen nimellä:

root@turku-bbrtr01#set trap-group "turku-bbrtr01"

Tämän jälkeen määritetyt asetukset tallennettiin commit-komennolla ja SNMP-editoinnista poistuttiin:

root@turku-bbrtr01#commit

root@turku-bbrtr01#exit

Määritellyn SNMP-toiminnan sai vahvistettua seuraavilla komennoilla:

root@turku-bbrtr01#show snmp

root@turku-bbrtr01>show snmp statistics [119.]

Seuraavaksi siirryttiin NetFlow'n konfigurointiin. Tämä voitiin konfiguroida vain reitittimillä, sillä kytkimet eivät tukeneet tätä ominaisuutta. Ensimmäiseksi reitittimillä otettiin käyttöön NetFlow'n otanta (sampling) halutuilla laitteiden välisillä porteilla sekä sisään että ulos:

root@turku-bbrtr01# set interfaces ge-2/0/0 unit 0 family inet sampling input output

root@turku-bbrtr01# set interfaces ge-2/1/0 unit 0 family inet sampling input output

root@turku-bbrtr01# set interfaces ge-2/2/0 unit 0 family inet sampling input output

Tämän jälkeen asetettiin otantatiheys (sampling rate) ja määriteltiin, minne vuotieto tuli lähettää eli op5 Monitorin sisältävän palvelimen IP-osoite ja NetFlow-tietoa vastaanottava oletusportti 2055:

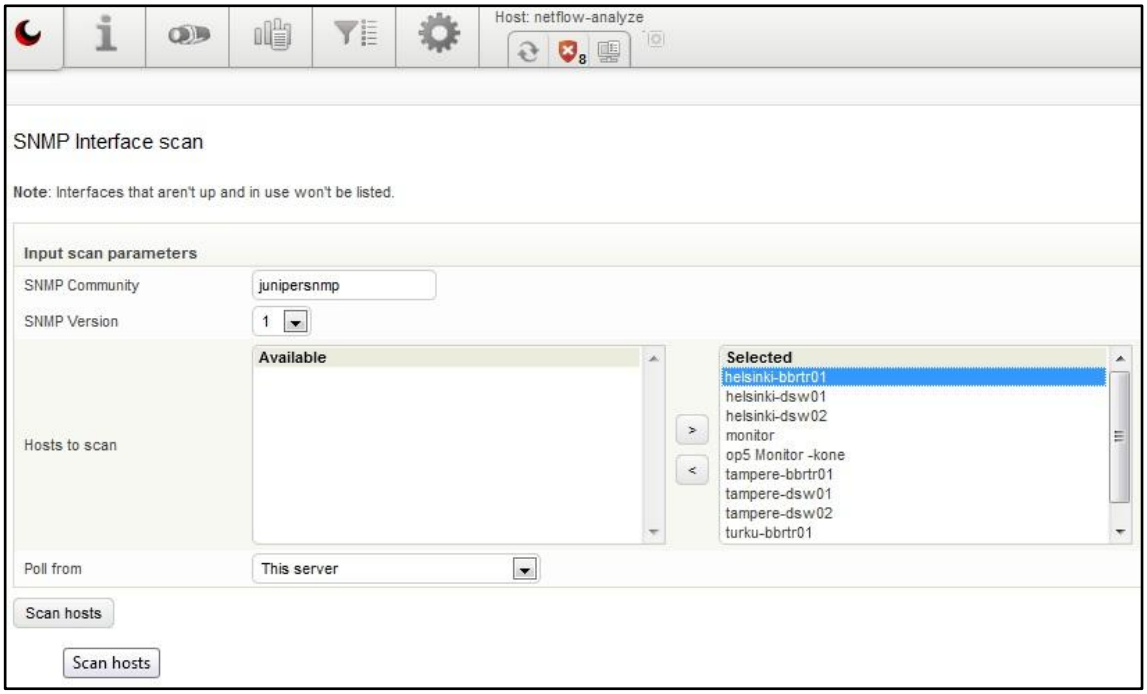
root@turku-bbrtr01# set forwarding-options sampling input family inet rate 100

root@turku-bbrtr01# set forwarding-options sampling output cflowd 10.95.250.76 port 2055 version 5 [120.]

Käytettäväksi NetFlow-versioksi yllä olevassa komennossa määriteltiin versio 5 parhaimman yhteensopivuuden varmistamiseksi. Viimeiseksi asetukset tallennettiin jälleen commit-komennolla:

root@turku-bbrtr01# commit

Kaikkien Juniper-laitteiden konfiguroinnin jälkeen op5 Monitorissa valittiin muokattavaksi verkkolaite ja napsautettiin ”SNMP Interface scan”-linkkiä. Tällä SNMP:tä käyttävien rajapintojen etsimissivulla valittiin tutkittaviksi kaikki verkon Juniper-laitteet, syötettiin Juniper-laitteissa käytetty SNMP-yhteisötunnus ja napsautettiin ”Scan hosts”-painiketta (kuva 23).



Kuva 23. SNMP:tä käyttävien rajapintojen havaitseminen op5 Monitor -ohjelmassa.

Sama tehtiin myös valmiiksi konfiguroiduille tietoverkkolaboratorion laitteille niille määritettyä SNMP-yhteisötunnusta käyttäen. op5 Monitor löysi kaikki laitteille konfiguroidut SNMP-protokollaa käyttävät portit ja näistä määritettiin monitoroitavaksi laitteiden välisten linkkien portit. op5 Monitor -ohjelman sanotaan vastaanottavan NetFlow-tietoa automaattisesti, joten tämän tiedon vastaanottamiseksi ei ohjelmassa tehty erillistä etsintäprosessia.

5.3 Cisco-laitteet

Metropolian Ammattikorkeakoulun opetusrunkoverkossa olevista Cisco-laitteista valittiin monitoroitaviksi opetusrunkoverkon reititin ja laboratorioympäristön opetusrunkoverkkoon yhdistävä reititin. Reitittimet olivat Cisco 2911 -mallisia. Opetusrunkoverkon reititin konfiguroitiin ottamalla laitteelle Putty-ohjelmalla SSH-yhteys ja toinen reititin ottamalla laitteelle Telnet-yhteys, koska SSH-yhteys ei ollut mahdollinen tällä laitteella. Reitittimelle asetettiin ensin SNMP-yhteisötunnus ja oikeudet yhteisötietoihin. Nimeksi valittiin ”ciscosnmp” ja yhteisötietoihin annettiin sekä luku- että kirjoitusoikeudet:

core-rtr1# configure terminal

core-rtr1(config)#snmp-server community ciscosnmp rw

Laitteille määritettiin minne vuotiedot tuli lähettää eli op5 Monitorin sisältävän palvelimen IP-osoite ja SNMP-versio, jota laitteen tuli käyttää määritellyssä yhteisötunnuksessa:

core-rtr1(config)#snmp-server host 10.95.250.76 version 2c ciscosnmp

Laitteille aktivoitiin lisäksi SNMP-ilmoitukset, jonka jälkeen tehdyt asetusmuutokset tallennettiin kopioimalla laitteen tämän hetkinen konfiguraatio aloituskonfiguraatioksi:

core-rtr1(config)#snmp-server enable traps snmp [121.]

core-rtr1(config)#exit

core-rtr1#copy running-configuration starting-configuration

Seuraavaksi siirryttiin NetFlow'n konfigurointiin. Ensimmäiseksi reitittimillä aktivoitiin verkon toimintaa optimoiva Cisco CEF-teknologia (Cisco Express Forwarding):

core-rtr1# configure terminal

core-rtr1(config)#ip cef

NetFlow tulee ottaa käyttöön kaikilla fyysisillä rajapinnoilla eli porteilla, joiden kautta monitoroitavaksi haluttu liikenne kulkee. NetFlow aktivoitiin täten käyttöön verkkolaitteiden välisten linkkien porteissa:

core-rtr1(config)#interface g0/0

core-rtr1(config-if)#ip route-cache flow

core-rtr1(config-if)#exit

Laitteille määritettiin käytettävä NetFlow-versio ja minne vuotieto tuli lähettää eli op5 Monitorin sisältävän palvelimen IP-osoite ja NetFlow-tietoa vastaanottava oletusportti 2055:

core-rtr1(config)#ip flow-export version 5

core-rtr1(config)#ip flow-export destination 10.95.250.76 2055

Lisäksi määriteltiin NetFlow-tietoa laitteelta lähettävä rajapinta. Täksi rajapinnaksi tulee valita portti, joka todennäköisimmin pysyy ylhäällä, sillä NetFlow-tietoa ei voida viedä laitteesta alhaalla olevasta rajapinnasta. Suositeltu vientirajapinta on Loopback-silmukkaliitäntä tai vakaa Ethernet-portti. Laitteille määritettiin täten vientirajapinnaksi Loopback0:

core-rtr1(config)#ip flow-export Lo0 [122.]

Tämän jälkeen asetukset jälleen tallennettiin kuten edellä. Reitittimillä varmistettiin vuodatan tuotto seuraavilla komennoilla:

core-rtr1#show ip cache flow

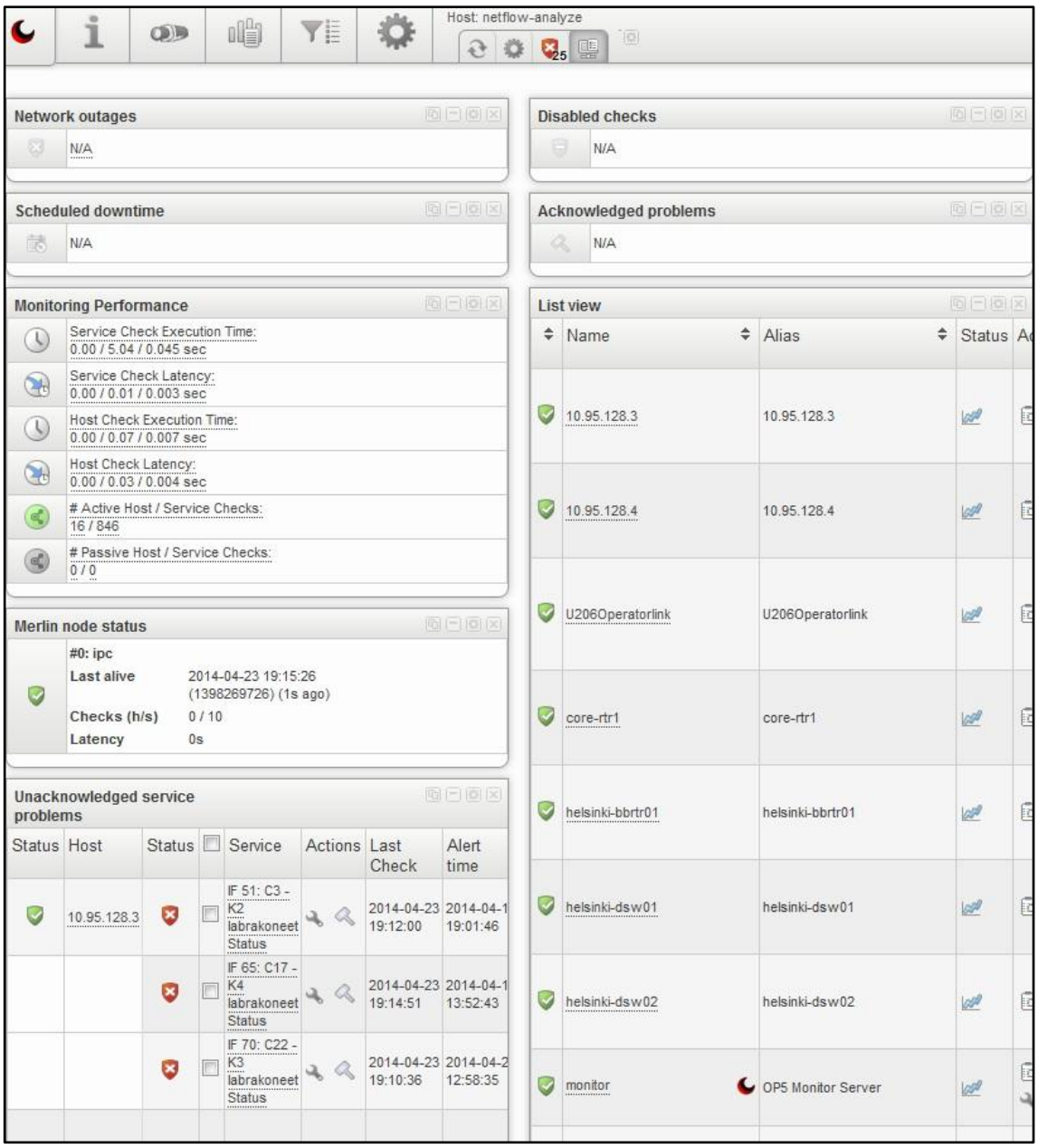
core-rtr1#show ip cache verbose flow

Cisco-laitteiden konfiguroinnin jälkeen op5 Monitorissa valittiin muokattavaksi verkkolaite ja etsittiin SNMP-protokollaa käyttävät rajapinnat ”SNMP Interface scan”-linkin kautta (kuva 23). op5 Monitor löysi kaikki laitteille konfiguroidut SNMP-protokollaa käyttävät portit ja näistä määritettiin Juniper-laitteiden tapaan monitoroitavaksi laitteiden välisten linkkien portit. NetFlow-tiedon vastaanottamiseksi ohjelmaa ei erikseen konfiguroitu.

5.4 Monitorointitulokset

op5 Monitor -ohjelma keräsi monitorointitietoa Metropolia Ammattikorkeakoulun Helsingin toimipisteen opetusrunkoverkossa ajalla 10.4.2014-23.4.2014. Ensimmäiseksi

op5 Monitorissa avautui Tactical Overview -yleisnäkymä. Kuvassa 24 näkyy yleisnäkymän raportoimaa informaatiota.

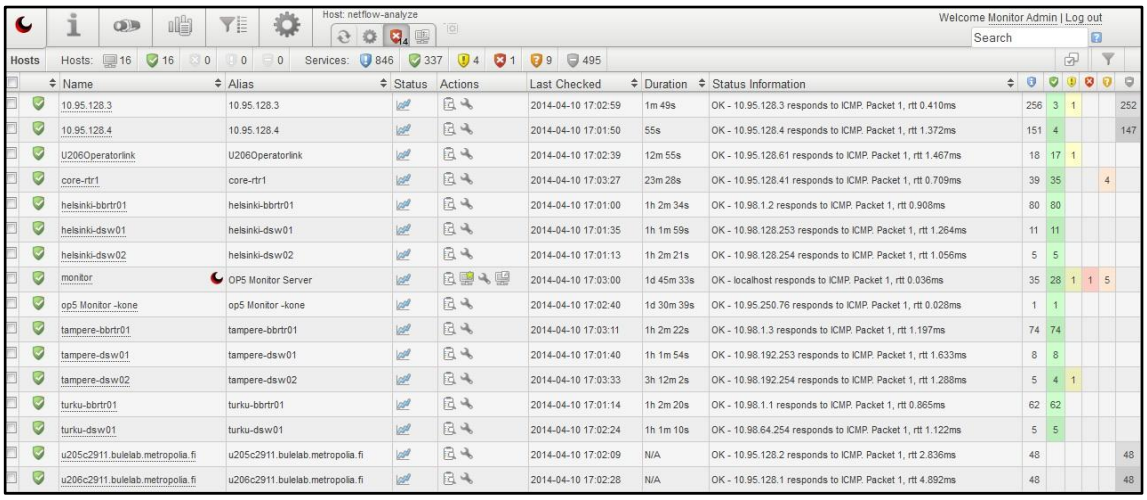


Kuva 24. Esimerkki yleisnäkymässä raportoidusta informaatiosta op5 Monitor -ohjelmassa.

Yleisnäkymässä on myös Network health -ikkuna, josta järjestelmänvalvojan on helppo nähdä, missä kunnossa laitteet ja palvelut ovat. Kuvassa 25 nähdään, miltä Metropolian Helsingin toimipisteen opetusrunverkon tila näytti 23.4.2014.

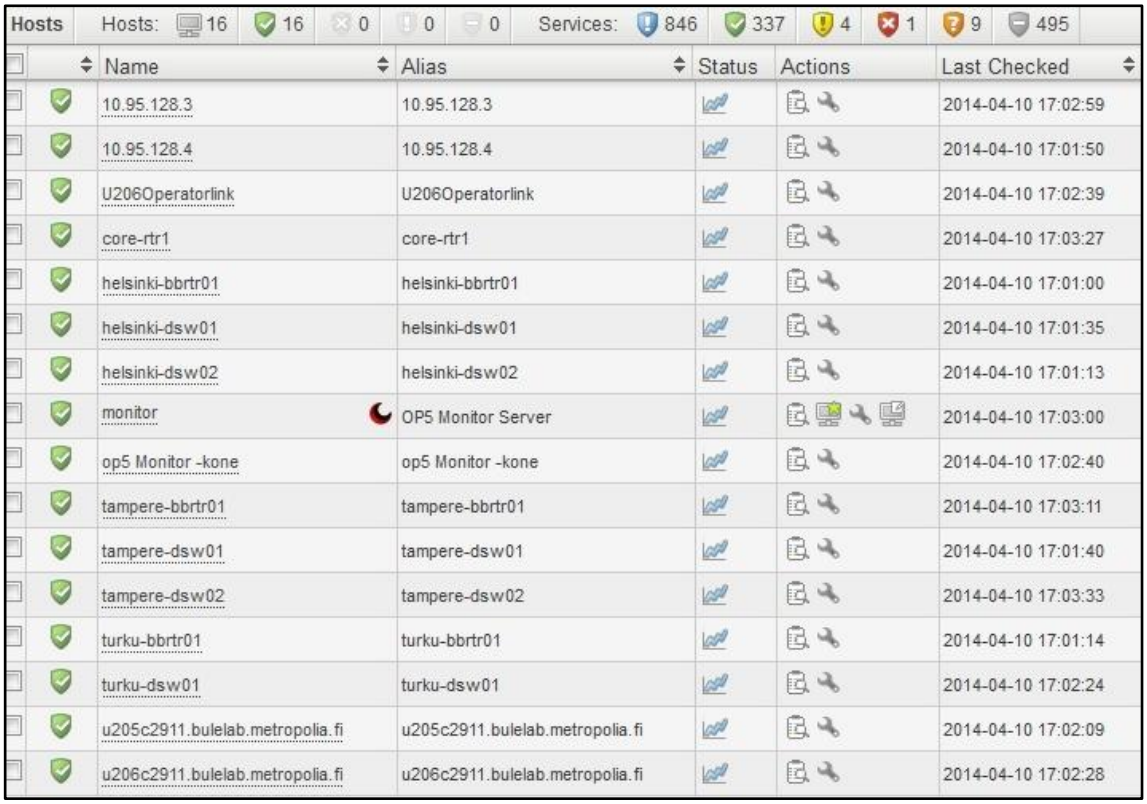
Kuva 25. Verkon tila -ikkuna op5 Monitor -ohjelman yleisnäkymässä.

Metropolian monitoroidut laitteet näkyivät laite- eli Hosts-näkymässä (kuva 26).



Kuva 26. Laitenäkymä op5 Monitor -ohjelmassa.

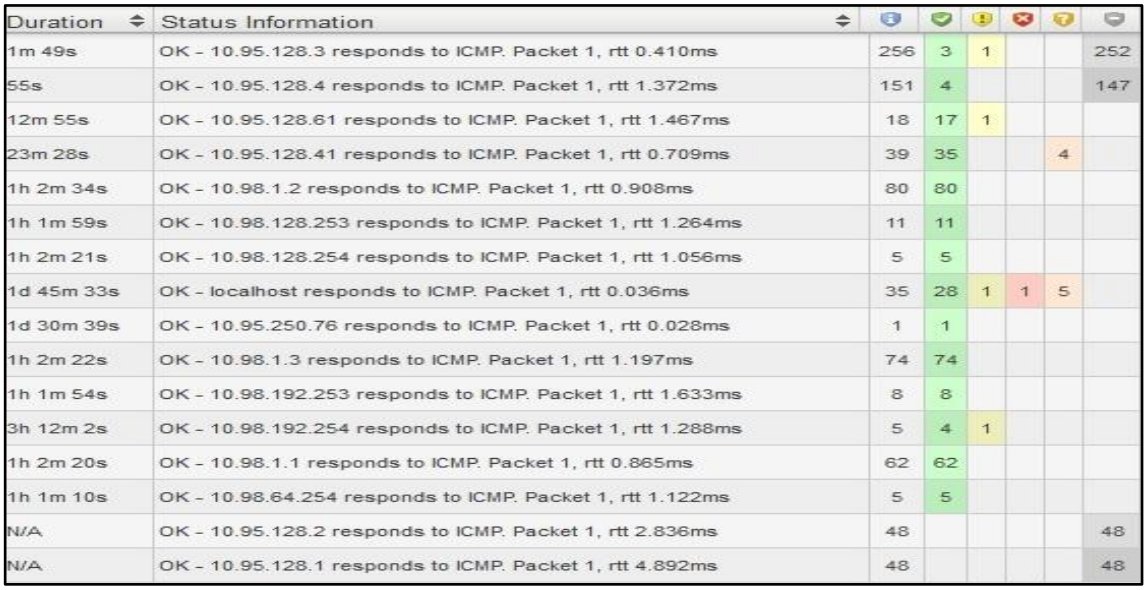
Jos tätä näkymää tarkastellaan lähemmin, näkymän vasemmalla puolella on tiedot laitteen verkkonimestä tai IP-osoitteesta ja siitä, milloin laite on viimeksi tarkistettu (kuva 27).



Hosts	Hosts: 16	16	0	0	0	Services: 846	337	4	1	9	495	
		Name	Alias	Status	Actions	Last Checked						
		10.95.128.3	10.95.128.3			2014-04-10 17:02:59						
		10.95.128.4	10.95.128.4			2014-04-10 17:01:50						
		U206Operatorlink	U206Operatorlink			2014-04-10 17:02:39						
		core-rtr1	core-rtr1			2014-04-10 17:03:27						
		helsinki-bbrtr01	helsinki-bbrtr01			2014-04-10 17:01:00						
		helsinki-dsw01	helsinki-dsw01			2014-04-10 17:01:35						
		helsinki-dsw02	helsinki-dsw02			2014-04-10 17:01:13						
		monitor	OP5 Monitor Server			2014-04-10 17:03:00						
		op5 Monitor -kone	op5 Monitor -kone			2014-04-10 17:02:40						
		tampere-bbrtr01	tampere-bbrtr01			2014-04-10 17:03:11						
		tampere-dsw01	tampere-dsw01			2014-04-10 17:01:40						
		tampere-dsw02	tampere-dsw02			2014-04-10 17:03:33						
		turku-bbrtr01	turku-bbrtr01			2014-04-10 17:01:14						
		turku-dsw01	turku-dsw01			2014-04-10 17:02:24						
		u205c2911.bulelab.metropolia.fi	u205c2911.bulelab.metropolia.fi			2014-04-10 17:02:09						
		u206c2911.bulelab.metropolia.fi	u206c2911.bulelab.metropolia.fi			2014-04-10 17:02:28						

Kuva 27. Laitteen verkkonimen ja tarkistusajan näyttävä yksityiskohta op5 Monitor -ohjelman laitenäkymästä.

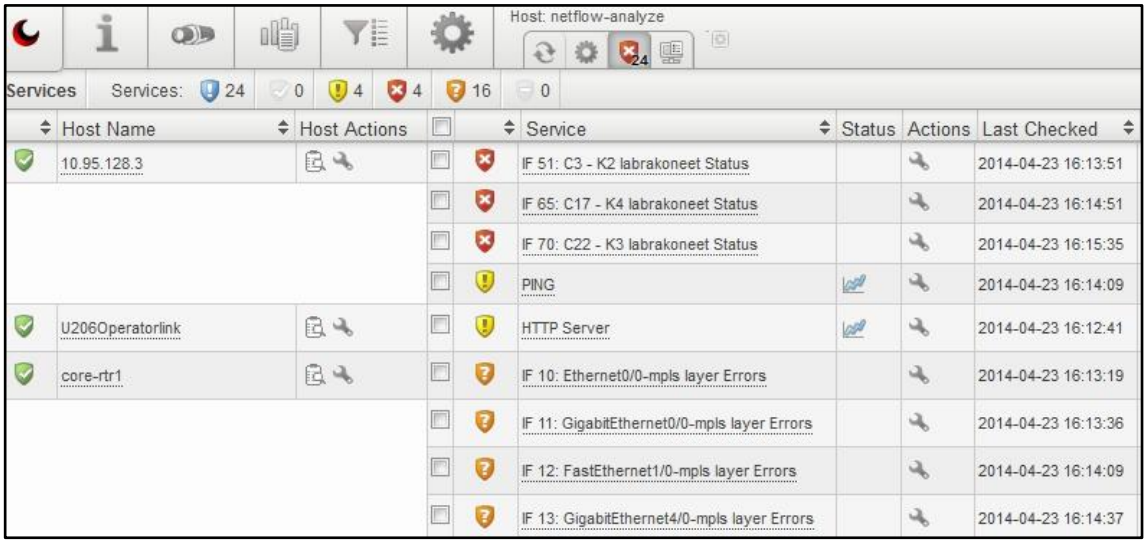
Laitenäkymän tiedot jatkuvat ilmoittamalla laitteen tilan ja esimerkiksi laitteesta monitoroidut palvelut, ongelmat ja muutokset (kuva 28).



Duration	Status Information						
1m 49s	OK - 10.95.128.3 responds to ICMP. Packet 1, rtt 0.410ms	256	3	1			252
55s	OK - 10.95.128.4 responds to ICMP. Packet 1, rtt 1.372ms	151	4				147
12m 55s	OK - 10.95.128.61 responds to ICMP. Packet 1, rtt 1.467ms	18	17	1			
23m 28s	OK - 10.95.128.41 responds to ICMP. Packet 1, rtt 0.709ms	39	35			4	
1h 2m 34s	OK - 10.98.1.2 responds to ICMP. Packet 1, rtt 0.908ms	80	80				
1h 1m 59s	OK - 10.98.128.253 responds to ICMP. Packet 1, rtt 1.264ms	11	11				
1h 2m 21s	OK - 10.98.128.254 responds to ICMP. Packet 1, rtt 1.056ms	5	5				
1d 45m 33s	OK - localhost responds to ICMP. Packet 1, rtt 0.036ms	35	28	1	1	5	
1d 30m 39s	OK - 10.95.250.76 responds to ICMP. Packet 1, rtt 0.028ms	1	1				
1h 2m 22s	OK - 10.98.1.3 responds to ICMP. Packet 1, rtt 1.197ms	74	74				
1h 1m 54s	OK - 10.98.192.253 responds to ICMP. Packet 1, rtt 1.633ms	8	8				
3h 12m 2s	OK - 10.98.192.254 responds to ICMP. Packet 1, rtt 1.288ms	5	4	1			
1h 2m 20s	OK - 10.98.1.1 responds to ICMP. Packet 1, rtt 0.865ms	62	62				
1h 1m 10s	OK - 10.98.64.254 responds to ICMP. Packet 1, rtt 1.122ms	5	5				
N/A	OK - 10.95.128.2 responds to ICMP. Packet 1, rtt 2.836ms	48					48
N/A	OK - 10.95.128.1 responds to ICMP. Packet 1, rtt 4.892ms	48					48

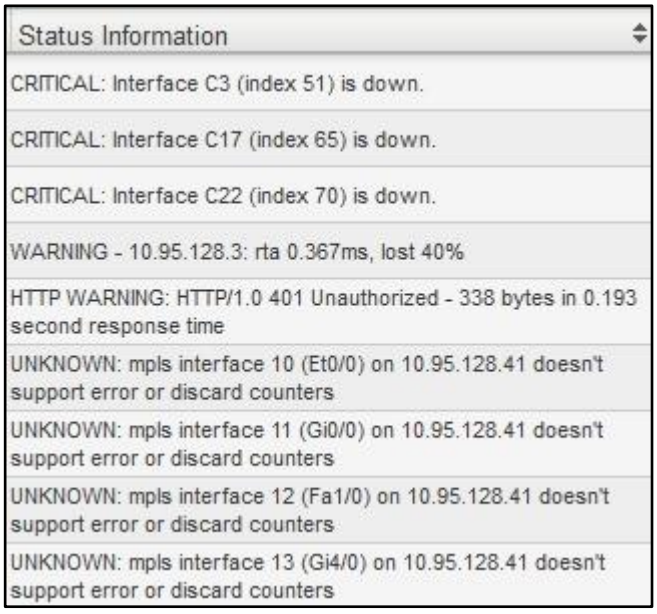
Kuva 28. Laitteen nimen ja monitoroidut asiat listaava yksityiskohta op5 Monitor -ohjelman laitenäkymästä.

Kuten kuvista 27 ja 28 näkyy, opetusrunkoverkon monitoroidut laitteet olivat tarkasteluhetkellä kaikki verkossa ICMP-protokollan vastauksen mukaan. Kuvissa näkyy myös kuvake, jossa on punainen kilpi valkoisella ristillä. Tämä kuvake tarkoittaa kriittistä ongelmaa, johon järjestelmänvalvojan tulisi heti tarttua. Kriittisessä tilassa olevia palveluita pääsee tarkastelemaan painamalla tätä kuvaketta op5 Monitorin yläriviltä. Tästä palvelunäkymästä saatiin selville, että opetusrunkoverkossa oli tarkasteluhetkellä monitoroituja palveluita kriittisessä tilassa esimerkiksi laboratorioverkossa kiinni olevalla reitittimellä 10.95.128.3 (kuva 29).



Kuva 29. Yksityiskohta palvelunäkymän kriittisessä tilassa olevia palveluita sisältävistä laitteista op5 Monitor -ohjelmassa.

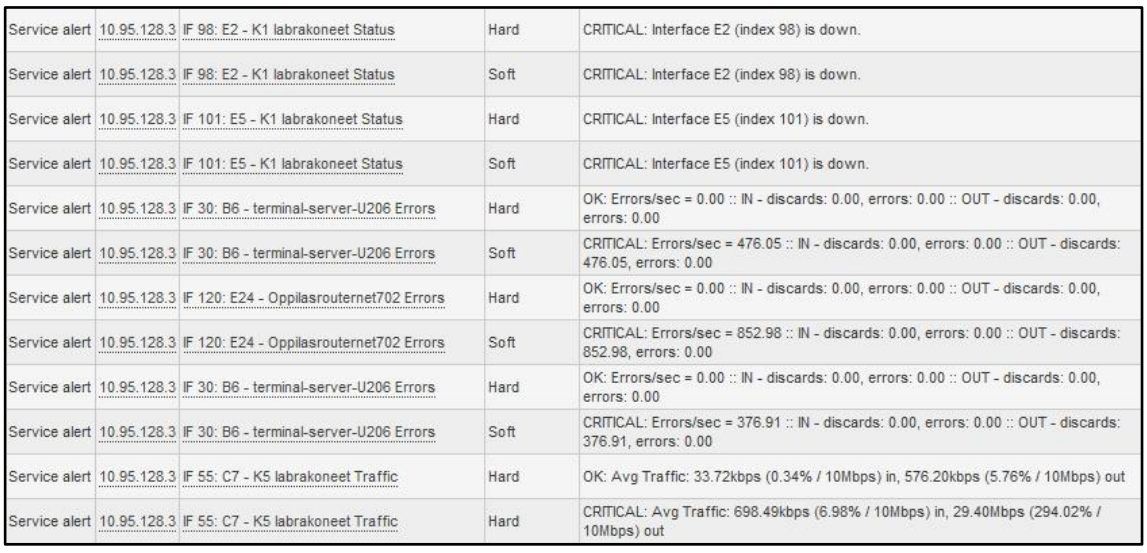
Palvelu- eli Service-sarakkeen palvelunimestä näkyy, että kyseessä on esimerkiksi ”IF” ”C3” eli rajapintaa C3 seuraava palvelu ja ”Status” eli tilaa seuraava palvelu. Kriittisessä tilassa oleva palvelu oli tarkasteluhetkellä siis muun muassa rajapinnan C3 tilaa seuraava palvelu. Lisäinformaatiota palvelun tilasta saadaan rivin lopussa olevasta Status Information -sarakkeesta. Tätä kuvassa 30 näkyvää saraketta tarkastelemalla saadaan selville, että reitittimen rajapinta C3 oli tarkasteluhetkellä alhaalla eikä täten reitittänyt informaatiota.



Status Information
CRITICAL: Interface C3 (index 51) is down.
CRITICAL: Interface C17 (index 65) is down.
CRITICAL: Interface C22 (index 70) is down.
WARNING - 10.95.128.3: rta 0.367ms, lost 40%
HTTP WARNING: HTTP/1.0 401 Unauthorized - 338 bytes in 0.193 second response time
UNKNOWN: mpls interface 10 (Et0/0) on 10.95.128.41 doesn't support error or discard counters
UNKNOWN: mpls interface 11 (Gi0/0) on 10.95.128.41 doesn't support error or discard counters
UNKNOWN: mpls interface 12 (Fa1/0) on 10.95.128.41 doesn't support error or discard counters
UNKNOWN: mpls interface 13 (Gi4/0) on 10.95.128.41 doesn't support error or discard counters

Kuva 30. Yksityiskohta palvelunäkymän kriittisessä tilassa olevia palveluita sisältävien laitteiden tilan lisäinformaatiosta op5 Monitor -ohjelmassa.

op5 Monitorissa laitteista saadaan listattua myös täysi hälytyshistoria. Yllä tarkastellun reitittimen 10.95.128.3 kuvassa 29 näkyvää jakoavainkuvaketta napauttamalla avautui laitteen konfiguraatiosivu. Konfiguraatiosivun ylälaidasta löytyvästä Alert history -painikkeesta saatiin listattua laitteesta aiheutuneet ilmoitukset monitoroinnin aloituksesta tarkasteluhetkeen. Esimerkkejä reitittimestä 10.95.128.3 aiheutuneista ilmoituksista on kuvassa 31. Muun muassa reitittimen rajapintoja oli alhaalla, paketteja oli jäänyt matkan varrelle ja liikenne oli epätasaisesti jakautunutta.



Service alert	10.95.128.3	IF 98: E2 - K1 labrakoneet Status	Hard	CRITICAL: Interface E2 (index 98) is down.
Service alert	10.95.128.3	IF 98: E2 - K1 labrakoneet Status	Soft	CRITICAL: Interface E2 (index 98) is down.
Service alert	10.95.128.3	IF 101: E5 - K1 labrakoneet Status	Hard	CRITICAL: Interface E5 (index 101) is down.
Service alert	10.95.128.3	IF 101: E5 - K1 labrakoneet Status	Soft	CRITICAL: Interface E5 (index 101) is down.
Service alert	10.95.128.3	IF 30: B6 - terminal-server-U206 Errors	Hard	OK: Errors/sec = 0.00 :: IN - discards: 0.00, errors: 0.00 :: OUT - discards: 0.00, errors: 0.00
Service alert	10.95.128.3	IF 30: B6 - terminal-server-U206 Errors	Soft	CRITICAL: Errors/sec = 476.05 :: IN - discards: 0.00, errors: 0.00 :: OUT - discards: 476.05, errors: 0.00
Service alert	10.95.128.3	IF 120: E24 - Oppilasrouternet702 Errors	Hard	OK: Errors/sec = 0.00 :: IN - discards: 0.00, errors: 0.00 :: OUT - discards: 0.00, errors: 0.00
Service alert	10.95.128.3	IF 120: E24 - Oppilasrouternet702 Errors	Soft	CRITICAL: Errors/sec = 852.98 :: IN - discards: 0.00, errors: 0.00 :: OUT - discards: 852.98, errors: 0.00
Service alert	10.95.128.3	IF 30: B6 - terminal-server-U206 Errors	Hard	OK: Errors/sec = 0.00 :: IN - discards: 0.00, errors: 0.00 :: OUT - discards: 0.00, errors: 0.00
Service alert	10.95.128.3	IF 30: B6 - terminal-server-U206 Errors	Soft	CRITICAL: Errors/sec = 376.91 :: IN - discards: 0.00, errors: 0.00 :: OUT - discards: 376.91, errors: 0.00
Service alert	10.95.128.3	IF 55: C7 - K5 labrakoneet Traffic	Hard	OK: Avg Traffic: 33.72kbps (0.34% / 10Mbps) in, 576.20kbps (5.76% / 10Mbps) out
Service alert	10.95.128.3	IF 55: C7 - K5 labrakoneet Traffic	Hard	CRITICAL: Avg Traffic: 698.49kbps (6.98% / 10Mbps) in, 29.40Mbps (294.02% / 10Mbps) out

Kuva 31. Esimerkki laitteen tuottamista ilmoituksista op5 Monitor -ohjelmassa.

op5 Monitorissa laitteista voidaan listata myös raportteja. Tarkastellen edelleen reititintä 10.95.128.3, kuvassa 32 on esimerkki reitittimen saatavuusraportin (availability report) palvelutiloista. Listauksesta nähdään, että tarkasteluhetkellä reitittimen E1- ja E2-rajapinnat olivat olleet alle sataprosenttisesti ylhäällä, joten Metropolian verkonvalvojan tulisi kiinnittää huomiota näihin rajapintoihin.

Selected services	Ok	Warning	Critical
Telnet	100 %	0 %	0 %
SSH Server	100 %	0 %	0 %
PING	0 %	100 %	0 %
IF 98: E2 - K1 labrakoneet Traffic	100 %	0 %	0 %
IF 98: E2 - K1 labrakoneet Status	99.355 %	0 %	0.645 %
IF 98: E2 - K1 labrakoneet Errors	100 %	0 %	0 %
IF 97: E1 - K1 labrakoneet Traffic	100 %	0 %	0 %
IF 97: E1 - K1 labrakoneet Status	99.851 %	0 %	0.149 %
IF 97: E1 - K1 labrakoneet Errors	100 %	0 %	0 %

Kuva 32. Yksityiskohta laitteen palvelujen saatavuudesta op5 Monitor -ohjelmassa.

Yksi verkon tilaa hyvin kuvaavista raporteista on verkon laitteiden ilmoitusmääriä listaavan Alert summary -osion Top alert producers -raportti. Tämä raportti listaa verkkolaitteet niiden palvelujen tuottaman ilmoitusmäärän mukaan. Opetusrunkoverkossa suurimmaksi ilmoitusten tuottajaksi paljastui kytkimen tampere-dsw02 Ping-palvelu 371 ilmoituksella (kuva 33).

Top alert producers

Reporting period: Last 7 days

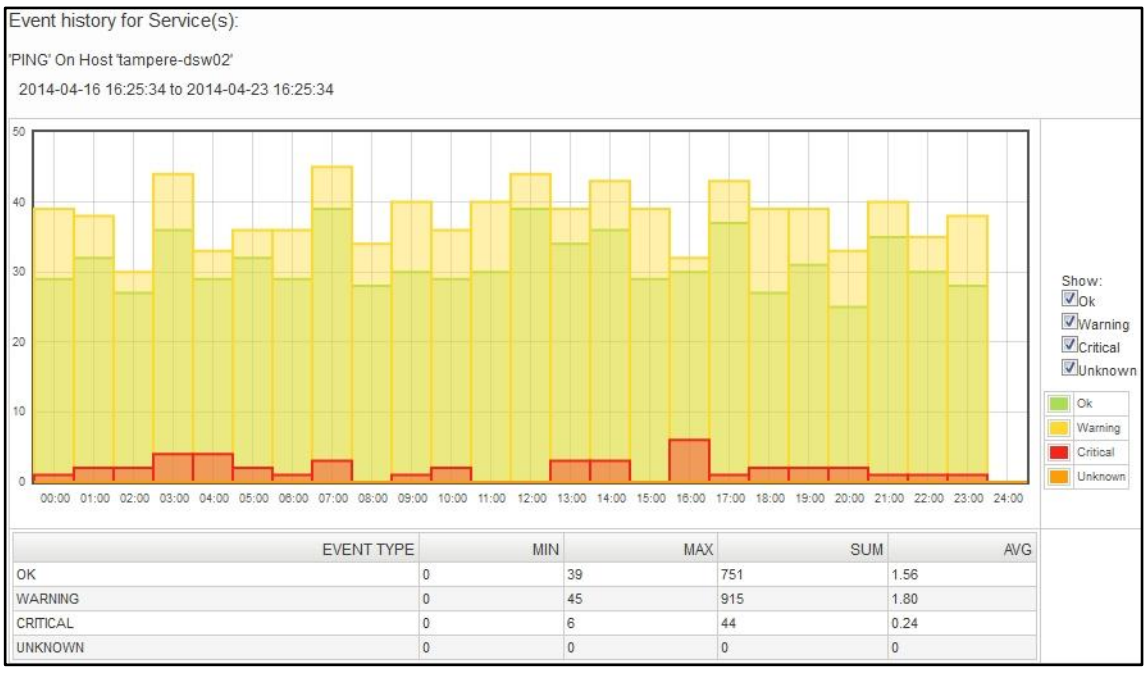
Assuming previous state during program downtime

Showing alerts for All service states, Hard states

Rank	Producer Type	Host	Service	Total Alerts
1	Service	tampere-dsw02	PING	371
2	Service	10.95.128.3	IF 55: C7 - K5 labrakoneet Traffic	4
3	Service	core-rtr1	IF 11: GigabitEthernet0/0-mpls layer Errors	3
4	Service	core-rtr1	IF 8: Null0 Traffic	3
5	Service	core-rtr1	IF 9: Loopback0 Status	3
6	Service	core-rtr1	IF 7: VoIP-Null0 Status	3

Kuva 33. Yksityiskohta monitoroitujen laitteiden suurimmat ilmoitusten tuottajat listaavasta raportista op5 Monitor -ohjelmassa.

Tampereen kytkimen tuottaessa huomattavan paljon Ping-palveluilmoituksia kytkimen rajapinnoissa voitiin päätellä olevan ongelmaa. Ping-palvelun käyttäytymistä laitteella tutkittiin lähemmin palvelun historiadiagrammilta. Kuvan 34 diagrammista nähdään, että palvelu oli tarkasteluhetkeen mennessä vaihdellut ok-tilan ja varoitustilojen välillä.



EVENT TYPE	MIN	MAX	SUM	AVG
OK	0	39	751	1.56
WARNING	0	45	915	1.80
CRITICAL	0	6	44	0.24
UNKNOWN	0	0	0	0

Kuva 34. Esimerkki palvelun tilasta historiadiagrammina op5 Monitor -ohjelmassa.

Ping-palvelua tarkasteltiin myös laitekohtaisella sivulla. Ping-palvelun laitekohtaisen sivun alalaidassa oli kommentti op5 Monitor prosessilta palveluilmoitusten väliaikaisesta lopettamisesta flapping-tilan tuottamien ilmoitusmäärien takia (kuva 33).

Author	Comment
(op5 Monitor Process)	Notifications for this service are being suppressed because it was detected as having been flapping between different states (22.5% change >= 20.0% threshold). When the service state stabilizes and the flapping stops, notifications will be re-enabled.

Kuva 35. Esimerkki op5 Monitor -prosessin kommenteista palveluihin liittyen op5 Monitor -ohjelmassa.

Kuvassa 36 näkyy myös vahvistus, että Ping-palvelun tila kytkimellä tampere-dsw02 vaihteli tarkistushetkellä ylös alas eli palvelu oli flapping-tilassa.

Kuva 36. Ping-palvelun tila laitteella op5 Monitor -ohjelmassa.

Palvelulistauksissa saattaa op5 Monitor -ohjelmassa näkyä myös oranssin värisiä kilpikuvakkeita kysymysmerkillä. Vaihtaen Tampereen kytkimestä tarkastelun kohteeksi reitittimen u205c2911.bulelab.metropolia.fi, laitteen palvelulistauksessa näkyi tarkasteluhetkellä ”IF 16: Port-channel1.2010 Errors”. Painamalla linkkiä op5 Monitorissa avautui sivu, jossa oli yksityiskohtaiset tiedot ilmoitetusta virheestä. Tältä kuvassa 37 näkyvältä sivulta saatiin selville, että op5 Monitor ei pystynyt määrittämään palvelun tilaa, koska tarkasteltu rajapinta ei tukenut määritystä.

IF 16: Port-channel1.2010 Errors

On host	u206c2911.bulelab.metropolia.fi (u206c2911.bulelab.metropolia.fi)
Address	10.95.128.1
Member of	No servicegroups
Contact groups	

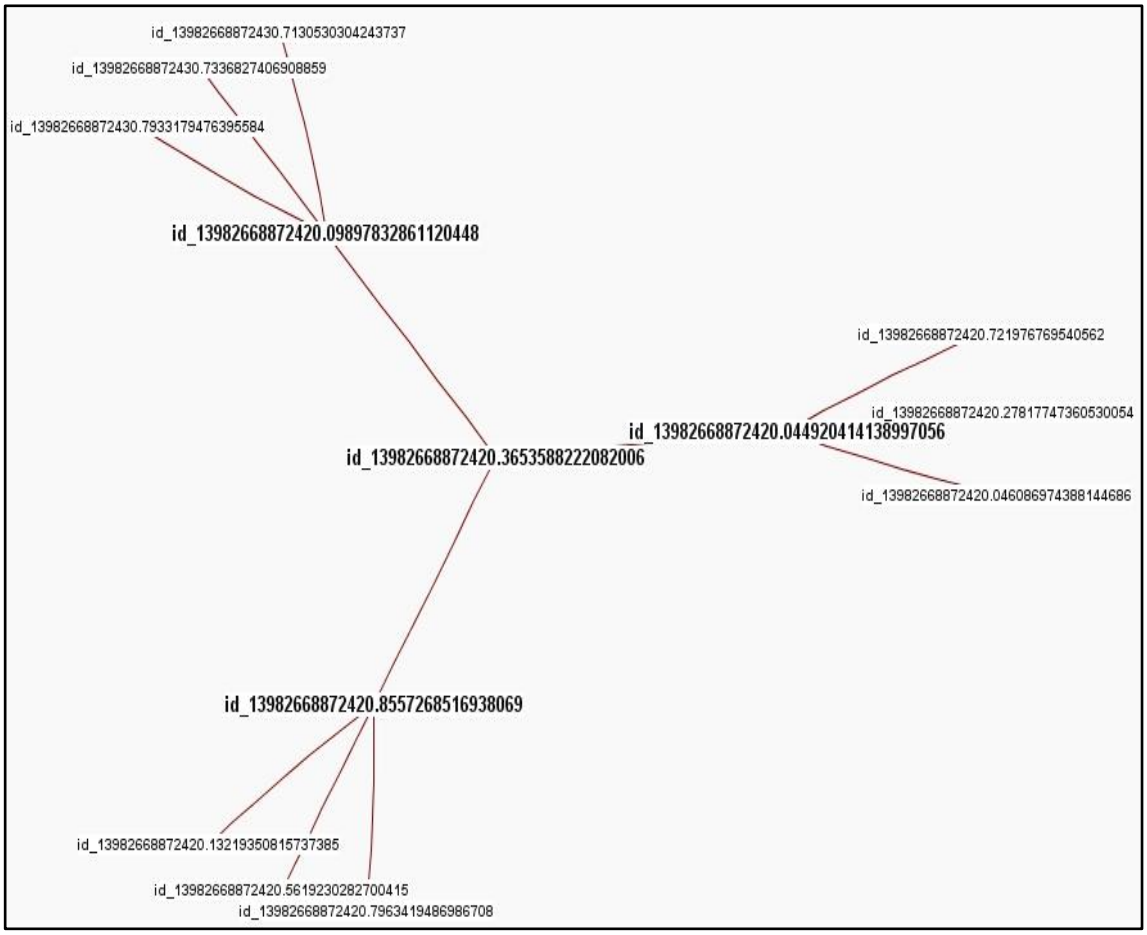
Configure

u206c2911.bulelab.metropolia.fi;IF 16: Port-channel1.2010 Errors

Current status	Unknown (for 12d 23h 10m 8s)
Status information	UNKNOWN: I2vlan interface 16 (Po1.2010) on 10.95.128.1 doesn't support error or discard counters
Performance data	
Current attempt	3/3 (hard)
Last check time	2014-04-23 16:13:57
Check source	netflow-analyze (local)
Check type	Active
Check latency / duration	0.003 / 0.009 seconds
Next scheduled active check	2014-04-23 16:18:57
Last state change	2014-04-10 17:06:52
Last notification	N/A (Notifications: 0)
Is this service flapping?	No (0.00% state change)
In scheduled downtime?	No
Active checks	Enabled
Passive checks	Enabled
Obsessing	Enabled
Notifications	Enabled
Event handler	Enabled
Flap detection	Enabled

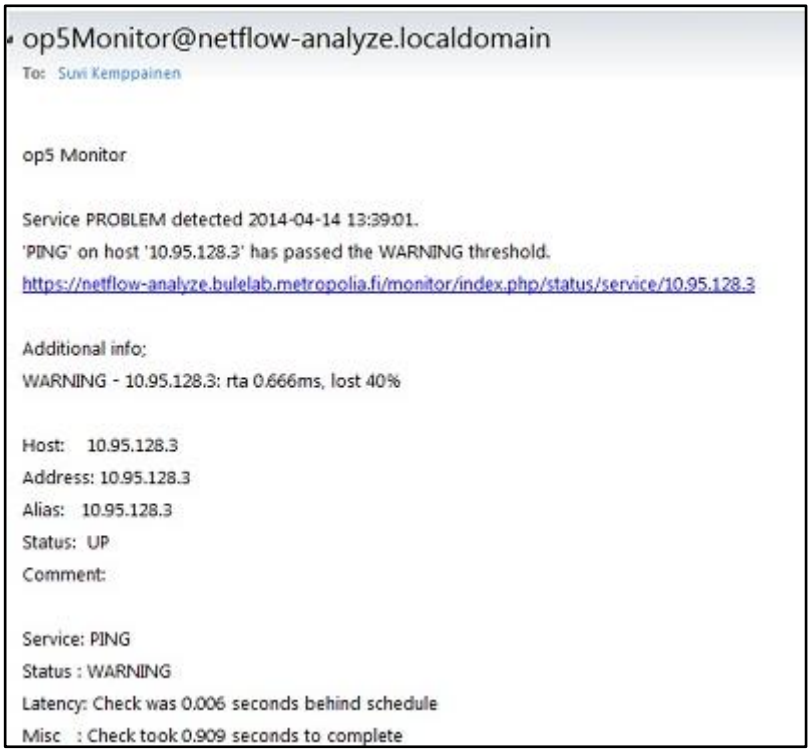
Kuva 37. Esimerkki palvelun virheinformaatiosta op5 Monitor -ohjelmassa.

Monitoroinnissa verkkolaitteiden keskinäisten suhteiden ja verkon rakenteen sen hetkistä hahmottamista helpottaa verkon topologiaa kuvaava kartta. op5 Monitorissa on automaattisen verkon topologian muodostava Hypermap-ominaisuus. Tarkastelu hetkellä Hypermapin koodissa oli vikaa eikä lopullista kuvaa voitu muodostaa tätä lopputyötä varten. Hypermap voitiin kuitenkin olettaa toimivaksi kartan muodostamisessa, sillä koodivikaisen ohjelman rakentamassa kuvassa näkyi yhteyksiä pisteiden välillä (kuva 38).



Kuva 38. Esimerkki verkon rakennekuvan muodostavasta Hypermap-ominaisuudesta op5 Monitor -ohjelmassa koodin ollessa viallinen.

Lopuksi op5 Monitor -ohjelmassa testattiin sen ominaisuutta lähettää hälytyksistä viestejä määritetylle henkilölle. Ohjelman Configure-näkymästä valittiin Add new contact -linkki, ja uudeksi kontaktiksi määritettiin ”monitoroija” halutulla sähköpostiosoitteella. Tämän jälkeen ”monitoroija” määritettiin laitteet yksi kerrallaan konfiguroiden laitteiden kontaktihenkilöksi. Määrittely todettiin toimivaksi, kun kontaktille määritettyyn sähköpostiosoitteeseen tulvi kuvan 39 kaltaisia viestejä.



Kuva 39. Esimerkki määritetylle kontaktihenkilölle lähettävistä ilmoitusviesteistä op5 Monitor -ohjelmassa.

Monitorointituloksien perusteella op5 Monitorin voidaan todeta toimineen määritellysti SNMP-tiedon avulla verkkolaitteiden rajapintoja ja niiden kautta kulkevaa tietoliikenteen määrää monitoroiden kahden viikon tarkkailujakson aikana. Määritellyistä vaatimuksista NetFlow'n käyttö jäi kuitenkin tuolloin varmistamattomaksi. Tarkasteluajankohtana ohjelmasta ei löytynyt sopivaa raporttia tai komentoa vuotiedon vastaanoton vahvistamiseksi. op5:n asiakaspalvelu vahvisti NetFlow-tuen puuttumisen insinöörityön viimeistelyvaiheessa. op5 Monitor -ohjelman valintaa voidaan siis pitää epäonnistuneena NetFlow-tiedon tarkastelutarkoituksessa. Ohjelma tarjoaa kuitenkin laajat ja hyvin vapaasti muokattavat monitorointimahdollisuudet, joten ohjelmaa voidaan pitää muutoin hyvänä valintana Metropolia Ammattikorkeakoulun tarpeisiin.

6 Yhteenveto

Insinöörityön tavoitteena oli vertailla ilmaisia verkonmonitorointiohjelmia ja valita näistä Metropolian kannalta monitorointiin parhaiten soveltuva ohjelma. Ilmaisohjelmien etsiminen ja valintakriteerien rajaaminen oli aluksi haastavaa ja aikaa vievää. Google-hakukoneen kautta löydetyistä ohjelmista suurin osa oli maksullisia, eikä ohjelmista

ollut ilmaiseksi tarjolla kuin 30 päivän kokeiluversioita. Runsaan tarjonnan ja ohjelmien ominaisuuslistauksien vajavaisuuksien vuoksi ohjelmia päätettiin alustavasti rajoittaa Wikipedia-artikkelin "Comparison of Network Monitoring Systems" pohjalta [123]. Artikkelissa listatuista ohjelmista etsittiin ne, joissa oli laajimmat ominaisuudet, ja näiden joukosta valittiin ilmaisohjelmat. Hakukoneita käyttämällä löytyi myös pari ohjelmaa listan ulkopuolelta, kuten Heroix Longitude.

Valituista ohjelmista pyrittiin varmistamaan Wikipedia-artikkelissa listattujen ominaisuuksien paikkansa pitävyys sekä artikkelista puuttuva NetFlow-tuki. Tiettyjen ohjelmien kohdalla tämä jäi vain pyrkimykseksi, sillä ohjelmista ei ollut tarjolla ominaisuustietoja. Kaikki ohjelmat, joista pystyttiin varmistamaan riittävät ominaisuudet, otettiin mukaan työhön. NetFlow-tuki osoittautui kaikista rajoittavimmaksi tekijäksi monitorointiohjelmien valinnassa, ja tuen puute karsi mahdollisten ohjelmien listalta monta nimeä. Oli yllättävää, että niinkin yleiset ohjelmat kuin OpenNMS, Zabbix tai Spiceworks eivät pystyneet käyttämään hyväkseen NetFlow-tietoa.

Työhön valituista ohjelmista jouduttiin karsimaan lisää ohjelmien testausvaiheessa. Alun perin mukana ollut Groundwork Monitor Core tarvitsikin yrityksen sähköpostiosoitteen ilmaisenkin lisenssin saamiseen, joten ohjelma poistettiin työstä. Zenoss Coren valinta taas kaatui asennusvaiheen ongelmiin. Asennusvaihe osoittautui ongelmalliseksi ja huomattavan aikaa vieväksi useammassakin ohjelmassa; Linux-käyttöjärjestelmää käyttävissä ohjelmissa helpoksi kuvattu asennusprosessi muuttui komentojen etsimiseksi hakukoneilta ja CentOS-käyttöjärjestelmän puuttuvien pakettien asentamiseksi, jotta monitorointiohjelman asennus oli ylipäätään mahdollista. Windows-käyttöjärjestelmää käyttävien ohjelmien kanssa ongelmaa ei ollut.

Testausvaiheen jälkeinen ohjelmavertailu oli työn helpoin vaihe. Ohjelmille sai helposti määriteltyä mittarit, ja vertailu oli suoraviivaista. Vertailutaulukon rakentaminen ja helppojen laskukaavojen käyttö niin kutsutun teknisesti oli hauskaakin. Ohjelmavertailun lopputulos ei valitettavasti ollut sataprosenttisen luotettava kolmen ohjelman hintatietojen puuttuessa, mutta vajailla tiedoilla op5 Monitorin voitosta ei voinut kiistellä.

Insinöörityössä oli tarkoitus monitoroida Metropolian Helsingin toimipisteen opetusrunkoverkon sisäistä sekä opetusrunkoverkon ja Metropolian tietoverkkolaboratorion välistä verkkoliikennettä. Verkkolaitteille syötettävät komennot olivat odotettua yksinkertaisempia, ja muutenkaan verkkolaitteiden kanssa ei esiintynyt ongelmia. Ongelmaksi

muodostui lopulta itse op5 Monitor -ohjelma sekä monitoroijan kokemattomuus. Verkkolaitteiden rajapintojen ja perusliikennemäärän monitorointi onnistui hyvin, mutta ohjelmasta ei löytynyt mitään NetFlow-tiedon seuraamiseen viittaavaa. op5 Monitor otettiin alunperin mukaan nimenomaan NetFlow-tuen vuoksi ja tuen olemassa olosta löytyi insinöörityön aloituksen aikana kaksi mainintaa, joita hakukoneetkaan eivät enää myöhemmin löytäneet. op5-yrityksen asiakastuki vahvisti NetFlow-tuen puuttumisen insinöörityön loppuvaiheessa. Tämä oli ikävä yllätys, ja tältä osin insinöörityön ohjelmavalinnan voidaan sanoa epäonnistuneen virheellisen lähdetiedon ja tästä juontuneen käsityksen takia. op5 Monitor -ohjelma kärsi seurantahetkellä myös koodiongelmasta, minkä takia opetusrunkoverkosta ei saatu edes kunnollista topologiakuvaa. op5 Monitor osoittautui kuitenkin ongelmistaan huolimatta muilta osin hämmästyttävän monipuoliseksi verkonmonitorointiohjelmaksi. Käytännössä tämä tarkoitti sitä, että insinöörityön tekemisen aikana ohjelmasta ei saanut vasta-alkajana täyttä hyötyä irti.

Opetusrunkoverkon op5 Monitorin tämän hetkiseen konfiguraatioon voidaan tehdä parannuksia esimerkiksi laitteiden jakamisella laiteryhmiin. Tällöin asetukset voidaan määritellä ryhmille yksittäisten laitteiden sijaan, säästäen konfiguraatioon käytettyä aikaa. Laitteiden välille voidaan myös lisätä vanhempi-lapsi-suhteet (parent-child relationship), joka takaa, että ohjelma osaa muodostaa topologian oikein.

op5 Monitorin Internet-sivujen huvittava väite ohjelman helppokäyttöisyydestä tarkoittaa todellisuudessa sitä, että ohjelman kanssa pärjää parhaiten Linux-käyttöjärjestelmään syvemmin perehtynyt skriptitaitoinen verkonvalvoja [124]. Avoimen lähdekoodin ohjelmana op5 Monitoriin saa lisättyä omia komentojaan, joka tarkoittanee myös mahdollisuutta rakentaa tietyn asteen korvaaja puuttuvalle NetFlow-tiedon kerääjälle. Täten on suuri todennäköisyys, että Metropolia Ammattikorkeakoulu voi hyödyntää asennettua op5 Monitoria asiaan perehtyneen monitoroijan käsissä. Mikäli ohjelmaan ei kuitenkaan ole tarvetta tai halua tehdä omia muutoksia eikä Metropolialla ole ohjelman valvomiseen resursseja, ammattikorkeakoulun kannattanee harkita ohjelman vaihtamista helppokäyttöisempään.

Lähteet

1 Behr, Alyson & Nash, Kim S. 2009. Network Monitoring Definitions and Solutions. Verkkodokumentti. <http://www.cio.com/article/133700/Network_Monitoring_Definition_and_Solutions>. Päivitetty 5.6.2009. Luettu 12.2.2014.

2 The Value of Network Monitoring. Verkkodokumentti. Ipswitch, Inc. <http://www.draware.dk/fileadmin/Ipswitch/wug/Value_of_Network_Monitoring.pdf>. Luettu 14.2.2014.

3 Mitchell, Bradley. LAN - Local Area Network. Verkkodokumentti. <http://compnetworking.about.com/cs/lanvlanwan/g/bldef_lan.htm>. Luettu 24.3.2014.

4 Mitchell, Bradley. WAN - Wide Area Network. Verkkodokumentti. <http://compnetworking.about.com/cs/lanvlanwan/g/bldef_wan.htm>. Luettu 24.3.2014.

5 Mitchell, Bradley. VPN - Virtual Private Network. Verkkodokumentti. <http://compnetworking.about.com/od/vpn/g/bldef_vpn.htm>. Luettu 24.3.2014.

6 Throughput. Verkkodokumentti. <http://en.wikipedia.org/wiki/Throughput>. Päivitetty 1.3.2014. Luettu 26.3.2014.

7 Janssen, Cory. Network Monitoring. Verkkodokumentti. <http://www.techopedia.com/definition/24149/network-monitoring>. Luettu 5.3.2014.

8 BYOD: Bring your own device. Verkkodokumentti. IBM Corporation. <http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html>. Luettu 27.2.2014.

9 McLellan, Charles. 2013. Consumerization, BYOD and MDM: What you need to know. Verkkodokumentti. <http://www.zdnet.com/consumerization-byod-and-mdm-what-you-need-to-know-7000010205/>. 1.2.2013. Luettu 27.2.2014.

10 Galbraith, Craig. 2013. Is Network Monitoring Dead?. Verkkodokumentti. <http://www.billingworld.com/news/2013/05/is-network-monitoring-dead.aspx>. 3.5.2013. Luettu 27.2.2014.

11 Palmer, Julian. 2012. Is Network Traffic Failing - Customer Complaints Remain Number 1 Problem. Verkkodokumentti. <http://networking.onestopclick.com/topic/200/529/is-network-traffic-monitoring-failing-%E2%80%93-customer-complaints-remain-number-1-problem.html>. 5.1.2012. Luettu 26.2.2014.

12 Echols, Jason. 2013. The next revolution in network monitoring: Simplicity. Verkkodokumentti. <http://www.techrepublic.com/blog/data-center/the-next-revolution-in-network-monitoring-simplicity/#>. 30.7.2013. Luettu 27.2.2014.

13 Blacharski, Dan. 2012. Network Monitoring - Why we need it, and why it doesn't work. Verkkodokumentti. <http://networking.onestopclick.com/topic/201/531/network-monitoring-why-we-need-it-and-why-it-doesnt-work.html>. 10.1.2012. Luettu 26.2.2014.

14 About the IETF. Verkkodokumentti. IETF. <http://www.ietf.org/about/>. Luettu 27.3.2014.

15 Verkkotunnus. Verkkodokumentti. <http://fi.wikipedia.org/wiki/Verkkotunnus>. Päivitetty 10.3.2014. Luettu 28.3.2014.

16 Domain Name System. Verkkodokumentti. Microsoft Corporation. <http://technet.microsoft.com/en-us/network/bb629410.aspx>. Luettu 28.3.2014.

17 Dalan, David & Rampling, Blair. DNS: What It Is and What It Does. Verkkodokumentti. <http://www.dummies.com/how-to/content/dns-what-it-is-and-what-it-does.html>. Luettu 28.3.2014.

18 Rouse, Margaret. File Transfer Protocol (FTP). Verkkodokumentti. <http://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol>. Päivitetty 4/2007. Luettu 28.3.2014.

19 Postel, J. & Reynolds, J. 1985. File Transfer Protocol (FTP). Verkkodokumentti. <http://tools.ietf.org/html/rfc959>. 10/1985. Luettu 28.3.2014.

20 HTTP - HyperText Transfer Protocol. Verkkodokumentti. <http://www.webopedia.com/TERM/H/HTTP.html>. Luettu 30.3.2014.

21 Berners-Lee, T. & Fielding, R. & Frystyk, H. & Gettys, J. & Leach, P. & Masinter, L. & Mogul, J. 1999. Hypertext Transfer Protocol -- HTTP/1.1. Verkkodokumentti. <http://tools.ietf.org/html/rfc2616>. 6/1999. Luettu 30.3.2014.

22 Website Monitoring. Verkkodokumentti. Paessler AG. <http://www.paessler.com/network_monitoring/website_monitoring>. Luettu 30.3.2014.

23 Postel, J. 1981. Internet Control Message Protocol. Verkkodokumentti. <https://tools.ietf.org/html/rfc792>. 9/1981. Luettu 27.3.2014.

24 Rouse, Margaret. 2007. baseboard management controller (BMC). Verkkodokumentti. <http://searchnetworking.techtarget.com/definition/baseboard-management-controller>. Päivitetty 5/2007. Luettu 30.3.2014.

25 Intelligent Platform Management Interface. Verkkodokumentti. <http://www.webopedia.com/TERM/I/Intelligent_Platform_Management_Interface_IPMI.html>. Luettu 30.3.2014.

26 Tyson, Jeff. How BIOS Works. Verkkodokumentti. <http://computer.howstuffworks.com/bios1.htm>. Luettu 30.3.2014.

27 Intelligent Platform Management Interface. Verkkodokumentti. <http://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface>. Päivitetty 26.2.2014. Luettu 30.3.2014.

28 Risks of Using the Intelligent Platform Management Interface (IPMI). 2013. Verkkodokumentti. US-CERT. <https://www.us-cert.gov/ncas/alerts/TA13-207A>. 26.7.2013. Päivitetty 4.10.2013. Luettu 30.3.2014.

29 Carpenter, B. & Conta, A. & Deering, S. & Rajahalme, J. 2004. IPv6 Flow Label Specification. Verkkodokumentti. <http://www.ietf.org/rfc/rfc3697.txt>. 3/2004. Luettu 27.3.2014.

30 Rouse, Margaret. NetFlow (Cisco). Verkkodokumentti. <http://whatis.techtarget.com/definition/NetFlow-Cisco>. Päivitetty 1/2013. Luettu 27.3.2014.

31 What is NetFlow? Verkkodokumentti. SolarWinds Inc. <http://www.solarwinds.com/what-is-netflow.aspx>. Luettu 27.3.2014.

32 About Cisco NetFlow. Verkkodokumentti. Zoho Corporation. <http://www.manageengine.com/products/netflow/cisco-netflow.html>. Luettu 27.3.2014.

33 Claise, Benoit & Kohler, Paul. 2003. IPFIX fine-tunes traffic analysis. Verkkodokumentti. <http://www.networkworld.com/news/tech/2003/0811techupdate.html>. 11.8.2003. Luettu 27.3.2014.

34 Camarillo, G. & Handley, M. & Johnston, A. & Peterson, J. & Rosenberg, J. & Schooler, E. & Schulzrinne, H. & Sparks, R. 2002. SIP: Session Initiation Protocol. Verkkodokumentti. <http://www.ietf.org/rfc/rfc3261.txt>. 6/2002. Luettu 30.3.2014.

35 Istunto (tietotekniikka). Verkkodokumentti. <http://fi.wikipedia.org/wiki/Istunto_%28tietotekniikka%29>. Päivitetty 11.3.2014. Luettu 30.3.2014.

36 SIP. Verkkodokumentti. <http://www.voip-info.org/wiki/view/SIP>. Luettu 30.3.2014.

37 SIP Technology. Verkkodokumentti. <http://www.sipforum.org/content/view/19/72/>. Luettu 30.3.2014.

38 SIP Monitoring - Voice Over IP (VoIP) Monitoring. Verkkodokumentti. Dotcom-Monitor. <https://www.dotcom-monitor.com/server-monitor/voip-monitoring-sip.aspx>. Luettu 30.3.2014.

39 What Is SNMP? Verkkodokukentti. Microsoft Corporation. <http://technet.microsoft.com/en-us/library/cc776379%28v=ws.10%29.aspx>. Päivitetty 28.3.2003. Luettu 30.3.2014.

40 OID. Verkkodokumentti. <http://fi.wikipedia.org/wiki/OID>. Päivitetty 13.8.2013. Luettu 24.3.2014.

41 How SNMP Works. Verkkodokumentti. Microsoft Corporation. <http://technet.microsoft.com/en-us/library/cc783142%28v=ws.10%29.aspx>. Päivitetty 28.3.2003. Luettu 30.3.2014.

42 Automatic Discovery. Verkkodokumentti. Ipswitch, Inc. <http://www.whatsupgold.com/glossary/network-discovery-tool/automatic-discovery.aspx>. Luettu 24.3.2014.

43 Pessach, Yaniv. 2006. Take Total Control Of Your Networking With .NET And UDP. Verkkodokumentti. <http://msdn.microsoft.com/en-us/magazine/cc163648.aspx#S1>. 2/2006. Luettu 24.3.2014.

44 SSl Secure Socket Layer. Verkkodokumentti. <http://www.webopedia.com/TERM/S/SSL.html>. Luettu 31.3.2014.

45 Rouse, Margaret. Transport Layer Security (TLS). Verkkodokumentti. <http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS>. Päivitetty 7/2006. Luettu 31.3.2014.

46 TLS. Verkkodokumentti. <http://www.webopedia.com/TERM/T/TLS.html>. Luettu 31.3.2014.

47 Tyson, Jeff. How Encryption Works. Verkkodokumentti. <http://computer.howstuffworks.com/encryption4.htm>. Luettu 31.3.2014.

48 Rouse, Margaret. Secure Sockets Layer (SSL). Verkkodokumentti. <http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL>. Päivitetty 3/2007. Luettu 31.3.2014.

49 Gerhards, R. 2009. The Syslog Protocol. Verkkodokumentti. <http://tools.ietf.org/html/rfc5424>. 3/2009. Luettu 31.3.2014.

50 Leskiw, Aaron. Understanding Syslog: Servers, Messages & Security. Verkkodokumentti. <http://www.networkmanagementsoftware.com/what-is-syslog>. Luettu 31.3.2014.

51 Transmission Control Protocol. 1981. Verkkodokumentti. <https://tools.ietf.org/html/rfc793>. 9/1981. Luettu 1.4.2014.

52 TCP - Tranmission Control Protocol. Verkkodokumentti. <http://www.webopedia.com/TERM/T/TCP.html>. Luettu 1.4.2014.

53 Rouse, Margaret. TCP (Transmission Control Protocol). Verkkodokumentti. <http://searchnetworking.techtarget.com/definition/TCP>. Päivitetty 8/2006. Luettu 1.4.2014.

54 Service Name and Transport Protocol Port Number Registry. Verkkodokumentti. <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>. Luettu 1.4.2014.

55 Transmission Control Protocol. Verkkodokumentti. <http://en.wikipedia.org/wiki/Transmission_Control_Protocol>. Päivitetty 24.3.2013. Luettu 1.4.2014.

56 Postel, J. 1980. User Datagram Protocol. Verkkodokumentti. <http://www.ietf.org/rfc/rfc768.txt>. 28.8.1980. Luettu 1.4.2014.

57 User Datagram Protocol. Verkkodokumentti. <http://en.wikipedia.org/wiki/User_Datagram_Protocol>. Päivitetty 11.3.2014. Luettu 1.4.2014.

58 Rouse, Margaret. UDP (User Datagram Protocol). Verkkodokumentti. <http://searchsoa.techtarget.com/definition/UDP>. Päivitetty 9/2005. Luettu 1.4.2014.

59 Telnet. Verkkodokumentti. <http://en.wikipedia.org/wiki/Telnet>. Päivitetty 25.2.2014. Luettu 1.4.2014.

60 Difference Between Telnet and SSH. Verkkodokumentti. <http://www.differencebetween.net/technology/internet/difference-between-telnet-and-ssh/>. Luettu 1.4.2014.

61 Telnet FAQ. Verkkodokumentti. <http://www.telnet.org/htm/faq.htm>. Luettu 1.4.2014.

62 Gil, Paul. What Is 'SSL'? What Is 'SSH'? Verkkodokumentti. <http://netforbeginners.about.com/od/technoglossary/f/whatis_SSL.htm>. Luettu 30.3.2014.

63 Lonvick, C. & Ylonen, T. 2006. The Secure Shell (SSH) Transport Layer Protocol. Verkkodokumentti. <http://tools.ietf.org/html/rfc4253>. 1/2006. Luettu 1.4.2014.

64 Mitchell, Bradley. SSH. Verkkodokumentti. <http://compnetworking.about.com/od/softwareapplicationstools/g/bldef_ssh.htm> . Luettu 30.3.2014.

65 SSH Protocol. Verkkodokumentti. Ipswitch, Inc. <http://www.whatsupgold.com/glossary/network-discovery-tool/ssh-protocol.aspx>. Luettu 25.4.2014.

66 Rouse, Margaret. Secure Shell (SSH). Verkkodokumentti. <http://searchsecurity.techtarget.com/definition/Secure-Shell>. Päivitetty 7/2005. Luettu 30.3.2014.

67 Secure Shell. Verkkodokumentti. <http://en.wikipedia.org/wiki/Secure_Shell>. Päivitetty 14.4.2014. Luettu 25.4.2014.

68 Ohjelmointirajapinta. Verkkodokumentti. <http://fi.wikipedia.org/wiki/Ohjelmointirajapinta>. Päivitetty 3.7.2013. Luettu 1.4.2014.

69 API - application program interface. Verkkodokumentti. <http://www.webopedia.com/TERM/A/API.html>. Luettu 1.4.2014.

70 WMI. Verkkodokumentti. <http://www.webopedia.com/TERM/W/WMI.html>. Luettu 1.4.2014.

71 Common Information Model. Verkkodokumentti. Distributed Management Task Force, Inc. <http://www.dmtf.org/standards/cim>. Luettu 1.4.2014.

72 Rouse, Margaret. Windows Management Instrumentation (WMI). Verkkodokumentti. <http://searchwindowsserver.techtarget.com/definition/Windows-Management-Instrumentation>. Päivitetty 9/2005. Luettu 1.4.2014.

73 Barry, Sean. 2009. Just What is WMI? Verkkodokumentti. <http://www.whatsupgold.com/blog/2009/05/12/just-what-is-wmi/>. 12.5.2009. Luettu 1.4.2014.

74 About Us. Verkkodokumentti. CA Technologies. <http://www.ca.com/se/en/about-us.aspx>. Luettu 7.3.2014.

75 CA Nimsoft Monitor Snap. Verkkodokumentti. CA Technologies. <http://www.ca.com/us/opscenter/ca-nimsoft-monitor-snap/product-details.aspx>. Luettu 7.3.2014.

76 CA Nimsoft Monitor Snap Comparison chart. Verkkodokumentti. CA Technologies. <http://www.ca.com/se/en/~/media/Files/TechnicalDocuments/CA-Nimsoft-Monitor-Snap-Comparison-chart.PDF>. Luettu 7.3.2014.

77 CA Nimsoft Monitor Snap. 2013. Verkkodokumentti. CA Technologies. <http://www.ca.com/se/en/~/media/Files/DataSheets/ca-nimsoft-monitor-snap.PDF>. Luettu 7.3.2014.

78 Download CA Nimsoft Monitor Snap. Verkkodokumentti. CA Technologies. <http://www.ca.com/us/lpg/nimsoft-monitor-snap/register.aspx>. Luettu 16.3.2014.

79 Company Overview of Heroix Corporation. Verkkodokumentti. <http://investing.businessweek.com/research/stocks/private/person.asp?personId=69377455&privcapId=7959677>. Luettu 18.3.2014.

80 Heroix Company Information. Verkkodokumentti. Heroix. <http://www.heroix.com/company_info.html>. Luettu 18.3.2014.

81 Longitude - Application & Server Monitoring Software Packages Comparison. Verkkodokumentti. Heroix. <http://www.heroix.com/packages_compare.html>. Luettu 18.3.2014.

82 Heroix Longitude V8.2 Quick Start Guide. Verkkodokumentti. Heroix. <http://www.heroix.com/longitude/8.2/longitude_quick_start_guide.htm>. Luettu 18.3.2014.

83 Longitude V8.2 Community Edition - Free. Verkkodokumentti. Heroix. <http://www.heroix.com/aspscript/demo_longitude_community.asp>. Luettu 18.3.2014.

84 About. Verkkodokumentti. Opmantek. <https://opmantek.com/about/>. Luettu 7.3.2014.

85 Sinclair, Keith. 2013. Verkkodokumentti. <https://community.opmantek.com/display/NMIS/NMIS8+Vendor+and+Device+Support>. 22.5.2013. Luettu 25.4.2014.

86 Network Management Information System - What uou need. Verkkodokumentti. Opmantek. <https://opmantek.com/network-management-system-nmis/>. Luettu 7.3.2014.

87 Download. Verkkodokumentti. Opmantek. <https://opmantek.com/network-tools-download/>. Luettu 7.4.2014.

88 Dueck, Mark. NMIS8 Installation Guide. Verkkodokumentti. <https://community.opmantek.com/display/NMIS/NMIS+8+Installation+Guide#NMIS8InstallationGuide-AdditionalPackages>. Päivitetty 28.1.2014. Luettu 7.4.2014.

89 Sinclair, Keith. 2013. Default Credentials (Passwords) for NMIS8 VM. Verkkodokumentti. <https://community.opmantek.com/display/NMIS/Default+Credentials+%28Passwords%29+for+NMIS8+VM>. 6.12.2013. Luettu 8.4.2014.

90 Unwin, Mark. 2014. How to use Open-AudIT Discovery on a Subnet. Verkkodokumentti. <https://community.opmantek.com/display/OA/How+to+use+Open-AudIT+Discovery+on+a+Subnet>. 11.3.2014. Luettu 8.4.2014.

91 About us.. Verkkodokumentti. JDSU. <http://www.networkinstruments.com/about/index.php>. Luettu 7.3.2014.

92 Observer Infrastructure. Verkkodokumentti. JDSU. <http://www.networkinstruments.com/products/observer-infrastructure/index.php>. Luettu 7.3.2014.

93 Observer Infrastructure System Requirements. Verkkodokumentti. JDSU. <http://www.networkinstruments.com/includes/popups/oi/requirements-compare.php>. Luettu 7.3.2014.

94 Support. Verkkodokumentti. JDSU. <https://networkinstruments.com/support/previous-versions.php>. Luettu 17.3.2014.

95 About op5. Verkkodokumentti. op5 AB. <https://www.op5.com/about/>. Luettu 7.3.2014.

96 History. Verkkodokumentti. op5 AB. <https://www.op5.com/about/history/>. Luettu 7.3.2014.

97 Nagios History. Verkkodokumentti. Nagios Enterprises. <http://www.nagios.org/about/history>. Luettu 7.3.2014.

98 Features. Verkkodokumentti. op5 AB. <https://www.op5.com/explore-op5-monitor/features/>. Luettu 7.3.2014.

99 Download op5 Monitor. Verkkodokumentti. op5 AB. <https://www.op5.com/download-op5-monitor/>. Luettu 7.3.2014.

100 Hardware Requirements. Verkkodokumentti. op5 AB. <http://www.op5.com/support/documentation/hardware-requirements/>. Luettu 7.3.2014.

101 op5 Monitor - Systems Management Software. Verkkodokumentti. <http://systems-management.findthebest.com/l/58/op5-Monitor>. Luettu 7.3.2014.

102 op5 Monitor User Manual. Verkkodokumentti. op5 AB. <https://www.op5.com/manuals/index.html#page/op5_Monitor_User_Manual/03_The_GUI.3.1.html>. Luettu 17.3.2014.

103 About us. Verkkodokumentti. Ártica Soluciones Tecnológicas. <http://artica.es/Company/quienessomos/en>. Luettu 7.3.2014.

104 Pandora FMS team. Verkkodokumentti. Ártica Soluciones Tecnológicas. <http://pandorafms.com/Community/pandora_team/en>. Luettu 7.3.2014.

105 Pandora FMS Enterprise. Verkkodokumentti. Ártica Soluciones Tecnológicas. <http://pandorafms.com/downloads/presentacion_pandora_2014-EN.pdf>. Luettu 7.3.2014.

106 Pandora FMS prices. Verkkodokumentti. Ártica Soluciones Tecnológicas. <http://pandorafms.com/Soporte/pricing/en>. Luettu 7.3.2014.

107 Pandora FMS Installation. Verkkodokumentti. Ártica Soluciones Tecnológicas. <http://wiki.pandorafms.com/index.php?title=Pandora:Documentation_en:Installing>. Luettu 7.3.2014.

108 Paessler AG. Verkkodokumentti. Paessler AG. <http://www.paessler.com/company>. Luettu 7.3.2014.

109 PRTG Network Monitor Feature Overview. Verkkodokumentti. Paessler AG. <http://www.paessler.com/prtg/features>. Luettu 7.3.2014.

110 Verkkodokumentti. Paessler AG. <http://www.paessler.com/prtg>. Luettu 7.3.2014.

111 Frequently Asked Questions (FAQs). Verkkodokumentti. Paessler AG. <http://www.paessler.com/support/faqs>. Luettu 7.3.2014.

112 Detailed System Requirements for PRTG Network Monitor. Verkkodokumentti. Paessler AG. <http://www.paessler.com/prtg/detailed-requirements>. Luettu 7.3.2014.

113 Verkkodokumentti. Paessler AG. <https://shop.paessler.com/shop/standalone_free_license/>. Luettu 17.3.2014.

114 Longitude Application Performance Monitoring Software - Enterprise Edition Pricing. Verkkodokumentti. Heroix. <http://www.heroix.com/packages_enterprise.html>. Luettu 27.4.

115 Observer Infrastructure - Upgrade Anytime. Verkkodokumentti. Heroix. <https://networkinstruments.com/products/observer-infrastructure/index.php?tab=upgrade-anytime>. Luettu 27.4.

116 Price and comparison. Verkkodokumentti. op5 AB. <https://www.op5.com/explore-op5-monitor/price-and-comparison/>. Luettu 27.4.

117 Price List of PRTG Network Monitor. Verkkodokumentti. Paessler AG. <http://www.paessler.com/prtg/price_list>. Luettu 27.4.

118 Hokkanen, Raimo & Kurillo, Kim & Moilanen, Ilkka & Päivinen, Jerry. 2013. Operaattorirunkoverkon rakentaminen Metropolian laboratoriokäyttöön. Verkkodokumentti. <https://moodle.metropolia.fi/mod/wiki/files.php?pageid=9361>. Päivitetty 13.12.2013. Luettu 10.4.2014.

119 Kangas, Justine & Shaw, Helen & Simmons, Brian Wesley & Taillon, Michael. 2002. ERX Edge Routers System Basics Configuration Guide. Verkkodokumentti. Juniper Networks, Inc. <http://www.juniper.net/techpubs/software/erx/erx402/bookpdfs/swconfig-system-basics.pdf>. Päivitetty 11/2002. Luettu 10.4.2014.

120 Dale. 2010. Juniper SRX series Gateway supports J-Flow. Verkkodokumentti. <http://www.plixer.com/blog/scrutinizer/juniper-srx-series-gateway-supports-j-flow/>. 13.8.2010. Luettu 9.4.2014.

121 Davis, David. 2007. Configure SNMP on a Cisco router or switch. Verkkodokumentti. <http://www.techrepublic.com/blog/data-center/configure-snmp-on-a-cisco-router-or-switch/283/#>. 28.6.2007. Luettu 10.4.2014.

122 Configuring NetFlow, IPFIX & sFlow. Verkkodokumentti. <http://www.plixer.com/Scrutinizer-Netflow-Sflow/configuring-netflow-ipfix-sflow.html>. Luettu 9.4.2014.

123 Comparison of Network Monitoring Systems. Verkkodokumentti. <http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems>. Päivitetty 10.2.2014. Luettu 12.2.2014.

124 Explore op5 Monitor. Verkkodokumentti. op5 AB. <https://www.op5.com/explore-op5-monitor/>. Luettu 27.4.2014.

CentOS 6 -käyttöjärjestelmän ifcfg-eth0-tiedosto

DEVICE='eth0'
STARTMODE='auto'
BOOTPROTO='none'
IPV6INIT='yes'
IPV6_AUTOCONF='yes'
IPADDR=10.95.250.76
NETMASK=255.255.254.0
GATEWAY=10.95.251.254
DNS1=10.95.254.252
DNS2=10.95.254.253

turku-bbrtr01 Juniper-reitittimen konfiguraatio

```
root@turku-bbrtr01#show
## Last changed: 2014-04-22 11:24:49 UTC
version 9.3R4.4;
system {
    host-name turku-bbrtr01;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password "$1$H2AiZ/8O$pxsqjhedMZC8SJXwVnzT81"; ## SECRET-
DATA
    }
    radius-server {
        10.95.250.75 secret "$9$/EtG90IyrvL7VKMVY4Zkqz369uOIEclvW"; ## SECRET-
DATA
    }
    login {
        user remote {
            full-name ispradius.bulelab.metropolia.fi;
            uid 2001;
            class super-user;
        }
    }
    services {
        ssh;
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
```

```
            interactive-commands any;
        }
    }
}
interfaces {
    ge-2/0/0 {
        description "Backbone connection to Tampere (tampere-bbrtr01)";
        unit 0 {
            family inet {
                sampling {
                    input;
                    output;
                }
                address 10.98.0.10/30;
            }
            family iso;
            family inet6 {
                address 2001:0708:0130:f803::/64 {
                    eui-64;
                }
            }
            family mpls;
        }
    }
    ge-2/1/0 {
        description "Backbone connection to Helsinki (helsinki-bbrtr01)";
        unit 0 {
            family inet {
                sampling {
                    input;
                    output;
                }
                address 10.98.0.1/30;
            }
            family iso;
```

```
        family inet6 {
            address 2001:0708:0130:f801::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
ge-2/2/0 {
    description "Connection to turku distribution network (turku-dsw01)";
    unit 0 {
        family inet {
            sampling {
                input;
                output;
            }
            address 10.98.64.1/30;
        }
        family iso;
        family inet6 {
            address 2001:0708:0130:f804::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
lo0 {
    description Router-id;
    unit 0 {
        family inet {
            address 10.98.1.1/32;
        }
        family iso {
            address 49.0010.0098.0001.0001.00;
```

```
            }
            family inet6 {
                address 2001:0708:0130:f800::1/128;
            }
        }
    }
}
forwarding-options {
    sampling {
        input {
            family inet {
                rate 100;
            }
        }
        output {
            cflowd 10.95.250.76 {
                port 2055;
                version 5;
            }
        }
    }
}
snmp {
    community junipersnmp {
        authorization read-write;
    }
    trap-group turku-bbrtr01;
}
routing-options {
    router-id 10.98.1.1;
    autonomous-system 65001;
}
protocols {
    rsvp {
        interface ge-2/0/0.0;
```

```
        interface ge-2/1/0.0;
        interface ge-2/2/0.0;
        interface lo0.0;
    }
    mpls {
        interface ge-2/0/0.0;
        interface ge-2/1/0.0;
        interface ge-2/2/0.0;
    }
    bgp {
        group internal-peers {
            type internal;
            multihop;
            local-address 10.98.1.1;
            neighbor 10.98.64.254;
            neighbor 10.98.1.2;
            neighbor 10.98.1.3;
            neighbor 10.98.128.253;
            neighbor 10.98.128.254;
            neighbor 10.98.192.253;
            neighbor 10.98.192.254;
        }
    }
    isis {
        topologies ipv6-unicast;
        interface ge-2/0/0.0;
        interface ge-2/1/0.0;
        interface ge-2/2/0.0;
        interface lo0.0;
    }
}
```

helsinki-bbrtr01 Juniper-reitittimen konfiguraatio

```
root@helsinki-bbrtr01# show
## Last changed: 2014-04-22 11:28:09 UTC
version 9.3R4.4;
system {
    host-name helsinki-bbrtr01;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password "$1$zXdHjlgw$bykoIFVjxFcg19jTaMg4f0"; ## SECRET-
DATA
    }
    radius-server {
        10.95.250.75 secret "$9$/EtG90IyrvL7VKMVY4Zkqz369uOIEclvW"; ## SECRET-
DATA
    }
    login {
        message "Tietoverkkoprojekti - Juniper MPLS-runkoverkko";
        user remote {
            full-name ispradius.bulelab.metropolia.fi;
            uid 2001;
            class super-user;
        }
    }
    services {
        ssh;
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
```

```
            interactive-commands any;
        }
    }
}
interfaces {
    ge-1/0/0 {
        description "Peering with Cisco ISP (link 1)";
        unit 0 {
            family inet {
                sampling {
                    input;
                    output;
                }
                address 10.97.11.2/30;
            }
        }
    }
    ge-1/1/0 {
        description "Peering with Cisco ISP (link 2)";
        unit 0 {
            family inet {
                sampling {
                    input;
                    output;
                }
            }
        }
    }
    ge-2/0/0 {
        description "Backbone connection to Tampere (tampere-bbrtr01)";
        unit 0 {
            family inet {
                sampling {
                    input;
                    output;
```

```
            }
            address 10.98.0.5/30;
        }
        family iso;
        family inet6 {
            address 2001:0708:0130:f802::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
ge-2/1/0 {
    description "Backbone connection to Turku (turku-bbrtr01)";
    unit 0 {
        family inet {
            sampling {
                input;
                output;
            }
            address 10.98.0.2/30;
        }
        family iso;
        family inet6 {
            address 2001:0708:0130:f801::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
ge-2/2/0 {
    description "Connection to helsinki distribution network (helsinki-dsw01)";
    unit 0 {
        family inet {
```

```
            sampling {
                input;
                output;
            }
            address 10.98.128.1/30;
        }
        family iso;
        family inet6 {
            address 2001:0708:0130:f805::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
ge-2/3/0 {
    description "Connection to helsinki distribution network (helsinki-dsw02)";
    unit 0 {
        family inet {
            sampling {
                input;
                output;
            }
            address 10.98.128.5/30;
        }
        family iso;
        family inet6 {
            address 2001:0708:0130:f806::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
lo0 {
```

```
        description Router-id;
        unit 0 {
            family inet {
                address 10.98.1.2/32;
            }
            family iso {
                address 49.0010.0098.0001.0002.00;
            }
            family inet6 {
                address 2001:0708:0130:f800::2/128;
            }
        }
    }
}
forwarding-options {
    sampling {
        input {
            family inet {
                rate 100;
            }
        }
        output {
            cflowd 10.95.250.76 {
                port 2055;
                version 5;
            }
        }
    }
}
snmp {
    community junipersnmp {
        authorization read-write;
    }
    trap-group helsinki-bbrtr01;
}
```

```
routing-options {
    static {
        route 192.168.1.2/32 next-hop 10.97.11.1;
    }
    generate {
        route 10.98.0.0/16 discard;
    }
    router-id 10.98.1.2;
    autonomous-system 65001;
}
protocols {
    rsvp {
        interface ge-2/0/0.0;
        interface ge-2/1/0.0;
        interface ge-2/2/0.0;
        interface ge-2/3/0.0;
        interface lo0.0;
    }
    mpls {
        interface ge-2/0/0.0;
        interface ge-2/1/0.0;
        interface ge-2/3/0.0;
        interface ge-2/2/0.0;
    }
    bgp {
        group internal-peers {
            type internal;
            multihop;
            local-address 10.98.1.2;
            neighbor 10.98.64.254;
            neighbor 10.98.1.1;
            neighbor 10.98.1.3;
            neighbor 10.98.128.253;
            neighbor 10.98.128.254;
            neighbor 10.98.192.253;
```

```
            neighbor 10.98.192.254;
        }
        group cisco-peering {
            type external;
            multihop;
            local-address 10.98.1.2;
            export export-bgp;
            neighbor 192.168.1.2 {
                peer-as 65007;
            }
        }
    }
    isis {
        topologies ipv6-unicast;
        interface ge-2/0/0.0;
        interface ge-2/1/0.0;
        interface ge-2/2/0.0;
        interface ge-2/3/0.0;
        interface lo0.0;
    }
}
policy-options {
    policy-statement export-bgp {
        term 1 {
            from {
                route-filter 10.98.0.0/16 exact;
            }
            then accept;
        }
        term END {
            then reject;
        }
    }
}
```

tampere-bbrtr01 Juniper-reitittimen konfiguraatio

```
root@tampere-bbrtr01# show
## Last changed: 2014-04-15 18:24:15 UTC
version 9.3R4.4;
system {
    host-name tampere-bbrtr01;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password "$1$3mfJHOHS$hF6h6XsRC4DXHL1CtPI3X0"; ## SE-
CRET-DATA
    }
    radius-server {
        10.95.250.75 secret "$9$/EtG90IyrvL7VKMVY4Zkqz369uOIEclvW"; ## SECRET-
DATA
    }
    login {
        user cisco1 {
            uid 2000;
            class super-user;
            authentication {
                encrypted-password "$1$DvfH2go.$V1ni80H8yi7EYTaE3975i/"; ## SE-
CRET-DATA
            }
        }
        user remote {
            full-name ispradius.bulelab.metropolia.fi;
            uid 2001;
            class super-user;
        }
    }
    services {
        ssh;
    }
    syslog {
        user * {
```

```
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
    }
}
interfaces {
    ge-1/0/0 {
        unit 0 {
            family inet {
                sampling {
                    input;
                    output;
                }
                address 10.95.128.37/27;
            }
            family inet6 {
                address 2001:708:130:FFFE::37/64;
            }
        }
    }
    ge-2/0/0 {
        description "Backbone connection to Turku (turku-bbrtr01)";
        unit 0 {
            family inet {
                sampling {
                    input;
                    output;
                }
                address 10.98.0.9/30;
            }
            family iso;
            family inet6 {
```

```
            address 2001:0708:0130:f803::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
ge-2/1/0 {
    description "Backbone connection to Helsinki (helsinki-bbrtr01)";
    unit 0 {
        family inet {
            sampling {
                input;
                output;
            }
            address 10.98.0.6/30;
        }
        family iso;
        family inet6 {
            address 2001:0708:0130:f802::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
ge-2/2/0 {
    description "Connection to Tampere distribution network (tampere-dsw01)";
    unit 0 {
        family inet {
            sampling {
                input;
                output;
            }
            address 10.98.192.1/30;
```

```
        }
        family iso;
        family inet6 {
            address 2001:0708:0130:f807::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
ge-2/3/0 {
    description "Connection to Tampere distribution network (tampere-dsw02)";
    unit 0 {
        family inet {
            sampling {
                input;
                output;
            }
            address 10.98.192.5/30;
        }
        family iso;
        family inet6 {
            address 2001:0708:0130:f808::/64 {
                eui-64;
            }
        }
        family mpls;
    }
}
ge-3/2/0 {
    unit 0 {
        family inet {
            sampling {
                input;
                output;
```

```
            }
            address 10.98.0.18/29;
        }
    }
}
ge-3/3/0 {
    description "To U205";
    unit 0 {
        family inet {
            sampling {
                input;
                output;
            }
            address 10.98.0.17/29;
        }
    }
}
lo0 {
    description Router-id;
    unit 0 {
        family inet {
            address 127.0.0.1/32;
            address 10.98.1.3/32;
        }
        family iso {
            address 49.0010.0098.0001.0003.00;
        }
        family inet6 {
            address 2001:0708:0130:f800::3/128;
        }
    }
}
}
forwarding-options {
    sampling {
```

```
        input {
            family inet {
                rate 100;
            }
        }
        output {
            cflowd 10.95.250.76 {
                port 2055;
                version 5;
            }
        }
    }
}
snmp {
    community junipersnmp {
        authorization read-write;
    }
    trap-group tampere-bbrtr01;
}
routing-options {
    rib inet6.0 {
        aggregate {
            route 2001:708:130:f800::/55;
        }
    }
    aggregate {
        route 10.98.0.0/16;
    }
    router-id 10.98.1.3;
    autonomous-system 65001;
}
protocols {
    igmp;
    rsvp {
        interface ge-2/0/0.0;
```

```
    interface ge-2/1/0.0;
    interface ge-2/2/0.0;
    interface ge-2/3/0.0;
    interface lo0.0;
}
mpls {
    interface ge-2/0/0.0;
    interface ge-2/1/0.0;
    interface ge-2/2/0.0;
    interface ge-2/3/0.0;
}
bgp {
    group internal-peers {
        type internal;
        multihop;
        local-address 10.98.1.3;
        advertise-external;
        neighbor 10.98.64.254;
        neighbor 10.98.1.2;
        neighbor 10.98.1.1;
        neighbor 10.98.128.253;
        neighbor 10.98.128.254;
        neighbor 10.98.192.253;
        neighbor 10.98.192.254;
    }
    group external-peers {
        type external;
        export [ BGP-EXPORT BGP-IPV6-EXPORT ];
        multipath;
        neighbor 10.95.128.33 {
            family inet {
                unicast;
            }
            family inet6 {
                unicast;
```

```
            }
            peer-as 65300;
        }
        neighbor 2001:708:130:fffe::abba {
            family inet6 {
                unicast;
            }
            peer-as 65300;
        }
        neighbor 10.95.128.34 {
            family inet {
                unicast;
            }
            family inet6 {
                unicast;
            }
            peer-as 65300;
        }
        neighbor 2001:708:130:fffe::face {
            family inet6 {
                unicast;
            }
            peer-as 65300;
        }
    }
}
isis {
    export ISISexportPolicy;
    topologies ipv6-unicast;
    interface ge-2/0/0.0;
    interface ge-2/1/0.0;
    interface ge-2/2/0.0;
    interface ge-2/3/0.0;
    interface lo0.0;
}
```

```
    ospf3 {
        area 0.0.0.0 {
            interface ge-3/3/0.0;
        }
    }
    pim {
        rp {
            local {
                family inet {
                    address 10.95.1.254;
                }
            }
        }
        interface ge-1/0/0.0 {
            mode sparse;
            version 2;
        }
        interface lo0.0 {
            mode sparse;
            version 2;
        }
        interface ge-2/3/0.0 {
            mode sparse;
            version 2;
        }
    }
}
policy-options {
    policy-statement BGP-EXPORT {
        term export {
            from {
                protocol aggregate;
                route-filter 10.98.0.0/16 exact;
            }
            then accept;
```

```
        }
    }
    policy-statement BGP-IPV6-EXPORT {
        term export {
            from {
                protocol aggregate;
                rib inet6.0;
                route-filter 2001:708:130:f800::/55 exact;
            }
            then accept;
        }
    }
    policy-statement ISISexportPolicy {
        term 1 {
            from {
                protocol bgp;
                route-filter 0.0.0.0/0 exact;
            }
            then accept;
        }
    }
}
```

turku-dsw01 Juniper-kytkimen konfiguraatio

```
root@turku-dsw01# show
## Last changed: 2013-11-21 00:19:12 EET
version 13.2X50-D10.2;
system {
    host-name turku-dsw01;
    auto-snapshot;
    time-zone Europe/Helsinki;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password "$1$wQ0gg1qM$KKmbbEBwobQRc/OQ7S0z80"; ## SE-
CRET-DATA
    }
    radius-server {
        10.95.250.75 secret "$9$/EtG90IyrvL7VKMVY4Zkqz369uOIEclvW"; ## SECRET-
DATA
    }
    login {
        user remote {
            full-name ispradius.bulelab.metropolia.fi;
            uid 2001;
            class super-user;
        }
    }
    services {
        ssh;
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
```

```
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    ge-0/0/0 {
        description "Link to backbone (turku-bbrtr01)";
        unit 0 {
            family inet {
                address 10.98.64.2/30;
            }
            family iso;
            family inet6 {
                address 2001:0708:0130:f804::/64 {
                    eui-64;
                }
            }
            family mpls;
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-0/0/3 {
        unit 0 {
            family ethernet-switching;
        }
```

```
}
ge-0/0/4 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/5 {
    description "Customer link (customerX-turku1)";
    unit 0 {
        family inet;
    }
}
ge-0/0/7 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/8 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/9 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/10 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching;
```

```
    }
}
ge-0/0/12 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/13 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/14 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/15 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/16 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/17 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/18 {
    unit 0 {
        family ethernet-switching;
```

```
    }
}
ge-0/0/19 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/20 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/21 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/22 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/23 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/0 {
    unit 0 {
        family ethernet-switching;
```

```
    }
}
ge-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/3 {
    unit 0 {
        family ethernet-switching;
    }
}
lo0 {
    description Router-id;
    unit 0 {
        family inet {
            address 10.98.64.254/32;
        }
        family iso {
            address 49.0010.0098.0064.0254.00;
        }
        family inet6 {
            address 2001:0708:0130:f800::4/128;
        }
    }
```

```
    }
    vlan {
        unit 0 {
            family inet;
        }
    }
    vme {
        unit 0 {
            family inet;
        }
    }
}
snmp {
    community junipersnmp {
        authorization read-write;
    }
    trap-group turku-dsw01;
}
routing-options {
    router-id 10.98.64.254;
    autonomous-system 65001;
}
protocols {
    rsvp {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
    mpls {
        interface ge-0/0/0.0;
    }
    bgp {
        group internal-peers {
            type internal;
            multihop;
            local-address 10.98.64.254;
```

```
            neighbor 10.98.1.1;
            neighbor 10.98.1.2;
            neighbor 10.98.1.3;
            neighbor 10.98.128.253;
            neighbor 10.98.128.254;
            neighbor 10.98.192.253;
            neighbor 10.98.192.254;
        }
    }
    isis {
        topologies ipv6-unicast;
        interface ge-0/0/0.0;
        interface lo0.0;
    }
}
ethernet-switching-options {
    storm-control {
        interface all;
    }
}
vlans {
    default {
        l3-interface vlan.0;
    }
}
poe {
    interface all;
}
```

Helsingin helsinki-dsw01 Juniper-kytkimen konfiguraatio

```
root@helsinki-dsw01# show
## Last changed: 2013-11-20 22:19:51 UTC
version 12.3R3.4;
system {
    auto-snapshot;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password "$1$AIpwbGkH$iRQ1WQ3g4bZzP9nmaFwhq/"; ## SE-
CRET-DATA
    }
    radius-server {
        10.95.250.75 secret "$9$/EtG90IyrvL7VKMVY4Zkqz369uOIEclvW"; ## SECRET-
DATA
    }
    login {
        user remote {
            full-name ispradius.bulelab.metropolia.fi;
            uid 2001;
            class super-user;
        }
    }
    services {
        ssh;
        dhcp {
            traceoptions {
                file dhcp_logfile;
                level all;
                flag all;
            }
        }
    }
    syslog {
        user * {
            any emergency;
```

```
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
chassis {
    auto-image-upgrade;
}
interfaces {
    ge-0/0/0 {
        description "Link to backbone (helsinki-bbrtr01)";
        unit 0 {
            family inet {
                address 10.98.128.2/30;
            }
            family iso;
            family inet6 {
                address 2001:0708:0130:f805::/64 {
                    eui-64;
                }
            }
            family mpls;
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-0/0/2 {
```

```
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/3 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/4 {
    description "Customer WAN link";
    unit 0 {
        family inet {
            address 10.98.129.1/24;
        }
    }
}
ge-0/0/5 {
    description "Customer L2VPN link";
    vlan-tagging;
    unit 10 {
        vlan-id 10;
        family ccc;
    }
}
ge-0/0/6 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/7 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
ge-0/0/8 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/9 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/10 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/12 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/13 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/14 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
ge-0/0/15 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/16 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/17 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/18 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/19 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/20 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/21 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
ge-0/0/22 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/23 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/0 {
    unit 0 {
        description "Link to GPON";
        family inet {
            address 10.98.129.65/30;
        }
        family iso;
    }
}
ge-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/2 {
```

```
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/3 {
    unit 0 {
        family ethernet-switching;
    }
}
lo0 {
    description Router-id;
    unit 0 {
        family inet {
            address 10.98.128.253/32;
        }
        family iso {
            address 49.0010.0098.0128.0253.00;
        }
        family inet6 {
            address 2001:0708:0130:f800::5/128;
        }
    }
}
vlan {
    unit 0 {
        family inet {
            dhcp {
                vendor-id Juniper-ex4200-24f;
            }
        }
```

```
        }
    }
    vme {
        unit 0 {
            family inet {
                dhcp {
                    vendor-id Juniper-ex4200-24f;
                }
            }
        }
    }
}
snmp {
    community junipersnmp {
        authorization read-write;
    }
    trap-group helsinki-dsw01;
}
routing-options {
    static {
        route 192.168.0.1/32 next-hop 10.98.129.2;
        route 10.98.132.0/22 next-hop 10.98.129.66;
    }
    router-id 10.98.128.253;
    autonomous-system 65001;
}
protocols {
    rsvp {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
    ##
    ## Warning: requires 'mpls' license
    ##
    mpls {
```

```
    label-switched-path to_tamperedsw01 {
        to 10.98.192.253;
    }
    interface ge-0/0/0.0;
}
##
## Warning: requires 'bgp' license
##
bgp {
    group internal-peers {
        type internal;
        multihop;
        local-address 10.98.128.253;
        neighbor 10.98.1.1;
        neighbor 10.98.1.2;
        neighbor 10.98.1.3;
        neighbor 10.98.128.253;
        neighbor 10.98.64.254;
        neighbor 10.98.192.253;
        neighbor 10.98.192.254;
    }
    group external-peers {
        type external;
        multihop;
        local-address 10.98.128.253;
        export ebgp_default;
        neighbor 192.168.0.1 {
            peer-as 65003;
        }
    }
}
##
## Warning: requires 'isis' license
##
isis {
```

```
        topologies ipv6-unicast;
        interface ge-0/0/0.0;
        interface xe-0/1/0.0;
        interface lo0.0;
    }
    connections {
        remote-interface-switch vpn1 {
            interface ge-0/0/5.10;
            transmit-lsp to_tamperedsw01;
            receive-lsp to_helsinkidsw01;
        }
    }
    igmp-snooping {
        vlan all;
    }
    rstp;
    lldp {
        interface all;
    }
    lldp-med {
        interface all;
    }
}
policy-options {
    policy-statement ebgp_default {
        term 1 {
            from {
                route-filter 0.0.0.0/0 exact;
            }
            then accept;
        }
        term END {
            then reject;
        }
    }
```

```
}
ethernet-switching-options {
    storm-control {
        interface all;
    }
}
vlans {
    default {
        l3-interface vlan.0;
    }
}
poe {
    interface all;
}
```

helsinki-dsw02 Juniper-kytkimen konfiguraatio

```
root@helsinki-dsw02# show
## Last changed: 2013-11-20 22:22:41 UTC
version 13.2X50-D10.2;
system {
    auto-snapshot;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password "$1$lwYucTno$GQygOm4sDRloV2QXACtFv1"; ## SE-
CRET-DATA
    }
    radius-server {
        10.95.250.75 secret "$9$/EtG90IyrvL7VKMVY4Zkqz369uOIEclvW"; ## SECRET-
DATA
    }
    login {
        user remote {
            full-name ispradius.bulelab.metropolia.fi;
            uid 2001;
            class super-user;
        }
    }
    services {
        ssh;
        dhcp {
            traceoptions {
                file dhcp_logfile;
                level all;
                flag all;
            }
        }
    }
    syslog {
        user * {
            any emergency;
```

```
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
chassis {
    auto-image-upgrade;
}
interfaces {
    ge-0/0/0 {
        description "Link to backbone (helsinki-bbrtr01)";
        unit 0 {
            family inet {
                address 10.98.128.6/30;
            }
            family iso;
            family inet6 {
                address 2001:0708:0130:f806::/64 {
                    eui-64;
                }
            }
            family mpls;
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-0/0/2 {
```

```
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/3 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/4 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/5 {
    description "Link to radius / logging server";
    unit 0 {
        family inet {
            address 10.98.128.9/30;
        }
    }
}
ge-0/0/6 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/7 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/8 {
    unit 0 {
        family ethernet-switching;
```

```
    }
}
ge-0/0/9 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/10 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/12 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/13 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/14 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/15 {
    unit 0 {
        family ethernet-switching;
```

```
    }
}
ge-0/0/16 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/17 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/18 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/19 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/20 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/21 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/22 {
    unit 0 {
        family ethernet-switching;
```

```
    }
}
ge-0/0/23 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/2 {
    unit 0 {
        family ethernet-switching;
```

```
    }
}
ge-0/1/3 {
    unit 0 {
        family ethernet-switching;
    }
}
lo0 {
    description Router-id;
    unit 0 {
        family inet {
            address 10.98.128.254/32;
        }
        family iso {
            address 49.0010.0098.0128.0254.00;
        }
        family inet6 {
            address 2001:0708:0130:f800::6/128;
        }
    }
}
vlan {
    unit 0 {
        family inet {
            dhcp {
                vendor-id Juniper-ex4200-24f;
            }
        }
    }
}
vme {
    unit 0 {
        family inet {
            dhcp {
                vendor-id Juniper-ex4200-24f;
```

```
            }
        }
    }
  }
}
snmp {
    community junipersnmp {
        authorization read-write;
    }
    trap-group helsinki-dsw02;
}
routing-options {
    router-id 10.98.128.254;
    autonomous-system 65001;
}
protocols {
    rsvp {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
    ##
    ## Warning: requires 'mpls' license
    ##
    mpls {
        interface ge-0/0/0.0;
    }
    ##
    ## Warning: requires 'bgp' license
    ##
    bgp {
        group internal-peers {
            type internal;
            multihop;
            local-address 10.98.128.254;
            neighbor 10.98.64.254;
```

```
            neighbor 10.98.1.2;
            neighbor 10.98.1.3;
            neighbor 10.98.128.253;
            neighbor 10.98.1.1;
            neighbor 10.98.192.253;
            neighbor 10.98.192.254;
        }
    }
    ##
    ## Warning: requires 'isis' license
    ##
    isis {
        topologies ipv6-unicast;
        interface ge-0/0/0.0;
        interface lo0.0;
    }
    igmp-snooping {
        vlan all;
    }
    rstp;
    lldp {
        interface all;
    }
    lldp-med {
        interface all;
    }
}
ethernet-switching-options {
    storm-control {
        interface all;
    }
}
vlans {
    default {
        l3-interface vlan.0;
```

```
    }
}
poe {
    interface all;
}
```

tampere-dsw01 Juniper-kytkimen konfiguraatio

```
root@tampere-dsw01# show
## Last changed: 2013-07-20 13:10:25 UTC
version 13.2X50-D10.2;
system {
    host-name tampere-dsw01;
    auto-snapshot;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password "$1$iZNt44IF$p01VtbW8zzYloIhDIYkXW/"; ## SECRET-
DATA
    }
    radius-server {
        10.95.250.75 secret "$9$/EtG90IyrvL7VKMVY4Zkqz369uOIEclvW"; ## SECRET-
DATA
    }
    login {
        message "Tietoverkkoprojekti - Juniper MPLS-runkoverkko";
        user remote {
            full-name ispradius.bulelab.metropolia.fi;
            uid 2001;
            class super-user;
        }
    }
    services {
        ssh;
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
```

```
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    ge-0/0/0 {
        description "Link to backbone (tampere-bbrtr01)";
        unit 0 {
            family inet {
                address 10.98.192.2/30;
            }
            family iso;
            family inet6 {
                address 2001:0708:0130:f807::/64 {
                    eui-64;
                }
            }
            family mpls;
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-0/0/3 {
        unit 0 {
            family ethernet-switching;
        }
```

```
}
ge-0/0/4 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/5 {
    description "Customer link (customerX-tampere1)";
    vlan-tagging;
    unit 10 {
        vlan-id 10;
        family ccc;
    }
}
ge-0/0/6 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/7 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/8 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/9 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/10 {
```

```
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/12 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/13 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/14 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/15 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/16 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/17 {
```

```
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/18 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/19 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/20 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/21 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/22 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/23 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/0 {
```

```
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/3 {
    unit 0 {
        family ethernet-switching;
    }
}
lo0 {
```

```
        description Router-id;
        unit 0 {
            family inet {
                address 10.98.192.253/32;
            }
            family iso {
                address 49.0010.0098.0192.0253.00;
            }
            family inet6 {
                address 2001:0708:0130:f800::7/128;
            }
        }
    }
}
snmp {
    community junipersnmp {
        authorization read-write;
    }
    trap-group tampere-dsw01;
}
routing-options {
    router-id 10.98.192.253;
    autonomous-system 65001;
}
protocols {
    rsvp {
        interface ge-0/0/0.0;
        interface ge-0/0/5.0;
        interface lo0.0;
    }
    ##
    ## Warning: requires 'mpls' license
    ##
    mpls {
        label-switched-path to_helsinkidsw01 {
```

```
        to 10.98.128.253;
    }
    interface ge-0/0/0.0;
    interface ge-0/0/5.0;
}
##
## Warning: requires 'bgp' license
##
bgp {
    group internal-peers {
        type internal;
        multihop;
        local-address 10.98.192.253;
        neighbor 10.98.1.1;
        neighbor 10.98.1.2;
        neighbor 10.98.1.3;
        neighbor 10.98.128.253;
        neighbor 10.98.128.254;
        neighbor 10.98.64.254;
        neighbor 10.98.192.254;
    }
}
##
## Warning: requires 'isis' license
##
isis {
    topologies ipv6-unicast;
    interface ge-0/0/0.0;
    interface lo0.0;
}
connections {
    remote-interface-switch vpn1 {
        interface ge-0/0/5.10;
        transmit-lsp to_helsinkidsw01;
        receive-lsp to_tamperedsw01;
```

```
        }
    }
    igmp-snooping {
        vlan all;
    }
    rstp;
    lldp {
        interface all;
    }
    lldp-med {
        interface all;
    }
}
ethernet-switching-options {
    storm-control {
        interface all;
    }
}
poe {
    interface all;
}
```

tampere-dsw02 Juniper-kytkimen konfiguraatio

```
root@tampere-dsw02# show
## Last changed: 2013-07-20 13:11:33 UTC
version 13.2X50-D10.2;
system {
    host-name tampere-dsw02;
    auto-snapshot;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password "$1$zpupHnyr$6Kj1i9.ooLPhWoJhZ38hI/"; ## SECRET-
DATA
    }
    radius-server {
        10.95.250.75 secret "$9$/EtG90IyrvL7VKMVY4Zkqz369uOIEclvW"; ## SECRET-
DATA
    }
    login {
        user remote {
            full-name ispradius.bulelab.metropolia.fi;
            uid 2001;
            class super-user;
        }
    }
    services {
        ssh;
        dhcp {
            traceoptions {
                file dhcp_logfile;
                level all;
                flag all;
            }
        }
    }
    syslog {
        user * {
```

```
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
chassis {
    auto-image-upgrade;
}
interfaces {
    ge-0/0/0 {
        description "Link to backbone (tampere-bbrtr01)";
        unit 0 {
            family inet {
                address 10.98.192.6/30;
            }
            family iso;
            family inet6 {
                address 2001:0708:0130:f808::/64 {
                    eui-64;
                }
            }
            family mpls;
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching;
        }
    }
```

```
ge-0/0/2 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/3 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/4 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/6 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/7 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/8 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/9 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
ge-0/0/10 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/12 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/13 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/14 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/15 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/16 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
ge-0/0/17 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/18 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/19 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/20 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/21 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/22 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/23 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
ge-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/3 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
    lo0 {
        description Router-id;
        unit 0 {
            family inet {
                address 10.98.192.254/32;
            }
            family iso {
                address 49.0010.0098.0192.0254.00;
            }
            family inet6 {
                address 2001:0708:0130:f800::8/128;
            }
        }
    }
    vlan {
        unit 0 {
            family inet {
                dhcp {
                    vendor-id Juniper-ex4200-24f;
                }
            }
        }
    }
    vme {
        unit 0 {
            family inet {
                dhcp {
                    vendor-id Juniper-ex4200-24f;
                }
            }
        }
    }
}
snmp {
    community junipersnmp {
```

```
        authorization read-write;
    }
    trap-group tampere-dsw02;
}
routing-options {
    router-id 10.98.192.254;
    autonomous-system 65001;
}
protocols {
    rsvp {
        interface ge-0/0/0.0;
        interface lo0.0;
    }
    ##
    ## Warning: requires 'mpls' license
    ##
    mpls {
        interface ge-0/0/0.0;
    }
    ##
    ## Warning: requires 'bgp' license
    ##
    bgp {
        group internal-peers {
            type internal;
            multihop;
            local-address 10.98.192.254;
            neighbor 10.98.64.254;
            neighbor 10.98.1.2;
            neighbor 10.98.1.3;
            neighbor 10.98.128.253;
            neighbor 10.98.128.254;
            neighbor 10.98.192.253;
            neighbor 10.98.1.1;
        }
```

```
    }
    ##
    ## Warning: requires 'isis' license
    ##
    isis {
        topologies ipv6-unicast;
        interface ge-0/0/0.0;
        interface lo0.0;
    }
    igmp-snooping {
        vlan all;
    }
    rstp;
    lldp {
        interface all;
    }
    lldp-med {
        interface all;
    }
}
ethernet-switching-options {
    storm-control {
        interface all;
    }
}
vlans {
    default {
        l3-interface vlan.0;
    }
}
poe {
    interface all;
}
```

turku-bbrtr01 Juniper-reitittimen show snmp statistics -komento

```
root@turku-bbrtr01>show snmp statistics
SNMP statistics:
  Input:
    Packets: 225244, Bad versions: 0, Bad community names: 396,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 1573788, Total set varbinds: 0,
    Get requests: 224784, Get nexts: 46, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 224848, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 224848, Traps: 0
```

helsinki-bbrtr01 Juniper-reitittimen snmp show statistics -komento

```
root@helsinki-bbrtr01> show snmp statistics
SNMP statistics:
  Input:
    Packets: 292133, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 2044530, Total set varbinds: 0,
    Get requests: 292063, Get nexts: 64, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 292133, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 292133, Traps: 0
```

tampere-bbrtr01 Juniper-reitittimen show snmp statistics -komento

```
root@tampere-bbrtr01> show snmp statistics
SNMP statistics:
  Input:
    Packets: 269745, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 1887722, Total set varbinds: 0,
    Get requests: 269663, Get nexts: 76, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 269745, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 269745, Traps: 0
```

turku-dsw01 Juniper-kytkimen show snmp statistics -komento

```
root@turku-dsw01> show snmp statistics
SNMP statistics:
  Input:
    Packets: 11364, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 79149, Total set varbinds: 0,
    Get requests: 11294, Get nexts: 64, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 11364, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 11364, Traps: 0
```

helsinki-dsw01 Juniper-kytkimen show snmp statistics -komento

```
root@helsinki-dsw01> show snmp statistics
SNMP statistics:
  Input:
    Packets: 33840, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 236436, Total set varbinds: 0,
    Get requests: 33764, Get nexts: 70, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 33840, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 33840, Traps: 0
```

helsinki-dsw02 Juniper-kytkimen show snmp statistics -komento

```
root@helsinki-dsw02> show snmp statistics
SNMP statistics:
  Input:
    Packets: 11359, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 79144, Total set varbinds: 0,
    Get requests: 11293, Get nexts: 60, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 11359, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 11359, Traps: 0
```

tampere-dsw01 Juniper-kytkimen show snmp statistics -komento

```
root@tampere-dsw01> show snmp statistics
SNMP statistics:
  Input:
    Packets: 22598, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 157802, Total set varbinds: 0,
    Get requests: 22530, Get nexts: 62, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 22598, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 22598, Traps: 0
```

tampere-dsw02 Juniper-kytkimen show snmp statistics -komento

```
root@tampere-dsw02> show snmp statistics
SNMP statistics:
  Input:
    Packets: 11352, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 79091, Total set varbinds: 0,
    Get requests: 11286, Get nexts: 60, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 11352, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 11352, Traps: 0
```

core-rtr1 Cisco-reitittimen konfiguraatio

```
core-rtr1#show config
Using 8633 out of 129016 bytes
!
! Last configuration change at 02:06:23 EETS Wed Apr 23 2014 by cisco
! NVRAM config last updated at 02:09:19 EETS Wed Apr 23 2014 by cisco
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname core-rtr1
!
boot-start-marker
boot system disk0:c7200-advipservicesk9-mz.124-24.T8.bin
boot bootldr disk1:c7200-kboot-mz.124-24.T8.bin
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$YMb/$k7iXgQZk.1YjGNlmqjiXz.
!
aaa new-model
!
!
aaa authentication login default group radius local enable
!
!
aaa session-id common
clock timezone EET 2
clock summer-time EETS recurring last Sun Mar 3:00 last Sun Oct 4:00
ip source-route
ip cef
!
```

```
!
!
!
no ip domain lookup
ip domain name cisco.bulelab.metropolia.fi
ip multicast-routing
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
!
!
!
!
```

```
ip ssh time-out 60
!
!
!
!
interface Loopback0
 ip address 10.97.12.11 255.255.255.255
 ipv6 address 2001:708:130:FAFF::101/128
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Ethernet0/0
 description Core-rtr1 (U206) <-> Edge-rtr2 (U206)
 ip address 10.97.10.25 255.255.255.248
 ip pim sparse-mode
 duplex auto
 ipv6 address 2001:708:130:FA0B::1/64
 ipv6 ospf 1 area 0
 mpls ip
!
interface GigabitEthernet0/0
 description Core-rtr1 (U206) <-> Core-rtr2 (4g labra)
 ip address 10.97.10.1 255.255.255.248
 ip flow ingress
 ip pim sparse-mode
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 ipv6 address 2001:708:130:FA00::1/64
 ipv6 ospf 1 area 0
 mpls ip
!
interface FastEthernet1/0
 description Core-rtr1 (U206) <-> Edge-rtr1 (U206)
```

```
 ip address 10.97.10.17 255.255.255.248
 ip pim sparse-mode
 duplex half
 ipv6 address 2001:708:130:FA08::1/64
 ipv6 ospf 1 area 0
 mpls ip
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet3/0
 description Core-rtr1 (U206) <-> Labraverkko (pilvi)
 ip address 10.95.128.41 255.255.255.224
 ip flow ingress
 ip pim sparse-mode
 negotiation auto
 ipv6 address 2001:708:130:FFFE::41/64
 ipv6 enable
!
interface GigabitEthernet4/0
 description Core-rtr1 (U206) <-> Core-rtr3 (4g labra)
 ip address 10.97.10.90 255.255.255.248
 ip flow ingress
 ip pim sparse-mode
 negotiation auto
 ipv6 address 2001:708:130:FA01::1/64
 ipv6 ospf 1 area 0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet3/0
 network 10.95.128.32 0.0.0.31 area 0
```

```
 network 10.97.10.0 0.0.0.7 area 0
 network 10.97.10.16 0.0.0.7 area 0
 network 10.97.10.24 0.0.0.7 area 0
 network 10.97.10.88 0.0.0.7 area 0
 network 10.97.12.11 0.0.0.0 area 0
 default-information originate
!
router bgp 65007
 bgp cluster-id 1
 bgp log-neighbor-changes
 neighbor IBGP peer-group
 neighbor IBGP remote-as 65007
 neighbor IBGP update-source Loopback0
 neighbor 2001:708:130:FAFF::254/128 peer-group
 neighbor IBGPv6 peer-group
 neighbor 10.95.128.33 remote-as 65300
 neighbor 10.97.12.21 remote-as 65007
 neighbor 10.97.12.21 peer-group IBGP
 neighbor 10.97.12.22 remote-as 65007
 neighbor 10.97.12.22 peer-group IBGP
 neighbor 2001:708:130:FAFF::201 remote-as 65007
 neighbor 2001:708:130:FAFF::201 peer-group IBGPv6
 neighbor 2001:708:130:FAFF::202 remote-as 65007
 neighbor 2001:708:130:FAFF::202 peer-group IBGPv6
 neighbor 2001:708:130:FFFE::ABBA remote-as 65300
 !
 address-family ipv4
  neighbor IBGP route-reflector-client
  neighbor IBGPv6 route-reflector-client
  neighbor 10.95.128.33 activate
  neighbor 10.97.12.21 activate
  neighbor 10.97.12.22 activate
  neighbor 2001:708:130:FAFF::201 activate
  neighbor 2001:708:130:FAFF::202 activate
  neighbor 2001:708:130:FFFE::ABBA activate
```

```
 default-information originate
 no auto-summary
 no synchronization
 network 10.97.0.0 mask 255.255.0.0
exit-address-family
!
address-family ipv6
 neighbor 10.95.128.33 activate
 neighbor 2001:708:130:FAFF::201 activate
 neighbor 2001:708:130:FAFF::202 activate
 neighbor 2001:708:130:FFFE::ABBA activate
 network 2001:708:130:FA00::/55
 default-information originate
 no synchronization
exit-address-family
!
ip forward-protocol nd
ip route 10.97.0.0 255.255.0.0 Null0
no ip http server
no ip http secure-server
!
ip flow-export source Loopback0
ip flow-export version 5
ip flow-export destination 10.95.250.76 2055
!
ip pim rp-address 10.95.1.254
!
ipv6 route 2001:708:130:FA00::/55 Null0
ipv6 router ospf 1
 log-adjacency-changes
!
!
!
!
!
```

```
!
snmp-server community ciscosnmp RW
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
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 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 aaa_server
snmp-server enable traps atm subif
snmp-server enable traps bgp
snmp-server enable traps bulkstat collection transfer
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 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 event-manager
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 ipmulticast
snmp-server enable traps mpls ldp
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps msdp
snmp-server enable traps mvpn
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-old
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 pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
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 firewall serverstatus
snmp-server enable traps ipmobile

```
snmp-server enable traps rf
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 host 10.95.250.76 version 2c ciscosnmp
tftp-server disk1:/c7200-advipservicesk9-mz.122-33.SRC3.bin
tftp-server disk1:/c7200-advipservicesk9-mz.122-33.SRC3
radius-server host 10.95.250.75 auth-port 1812 acct-port 1812
radius-server key testing123
!
control-plane
!
!
!
!
!
dial-peer cor custom
!
!
!
!
```

```
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 666 0
 stopbits 1
line aux 0
 transport input telnet
 stopbits 1
line vty 0 4
 exec-timeout 30 0
 privilege level 15
 transport input telnet ssh
!
ntp server 10.95.254.252
ntp server 10.95.254.253 prefer
end
```

U206Operatorlink Cisco-kytkimen konfiguraatio

```
U206Operatorlink#show config
Using 1203 out of 32768 bytes
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname U206Operatorlink
!
enable secret 5 $1$/Wce$wYt/8gjAPwnOzZHj8egov0
!
!
!
!
!
!
ip subnet-zero
!
!
!
interface GigabitEthernet0/1
 description Juniper_Operaattoriverkko
 spanning-tree portfast
!
interface GigabitEthernet0/2
 spanning-tree portfast
!
interface GigabitEthernet0/3
 spanning-tree portfast
!
interface GigabitEthernet0/4
 description Cisco_operaattoriverkko_Core-rtr1_G3/0
```

```
 spanning-tree portfast
!
interface GigabitEthernet0/5
 spanning-tree portfast
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
 spanning-tree bpdufilter enable
!
interface VLAN1
 ip address 10.95.128.61 255.255.255.224
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 10.95.128.33
snmp-server engineID local 000000090200000AF4E69440
snmp-server community ciscosnmp RW
snmp-server enable traps snmp authentication linkdown linkup coldstart
snmp-server host 10.95.250.76 trap version 2c ciscosnmp
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

core-rtr1 Cisco-reitittimen show snmp -komento

```
core-rtr1#show snmp
Chassis: 21272449
10632 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    74432 Number of requested variables
    0 Number of altered variables
    10632 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
11407 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    10632 Response PDUs
    775 Trap PDUs
SNMP Dispatcher:
  queue 0/75 (current/max), 0 dropped
SNMP Engine:
  queue 0/1000 (current/max), 0 dropped
SNMP Trap Queue: 0 dropped due to resource failure.

SNMP logging: enabled
    Logging to 10.95.250.76.162, 0/10, 728 sent, 47 dropped.
```

U206Operatorlink Cisco-kytkimen show snmp -komento

U206Operatorlink#show snmp
Chassis: CAT0643X0YA
56048 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    56041 Get-request PDUs
    3 Get-next PDUs
    0 Set-request PDUs
63532 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    56048 Response PDUs
    7484 Trap PDUs
SNMP global trap: enabled

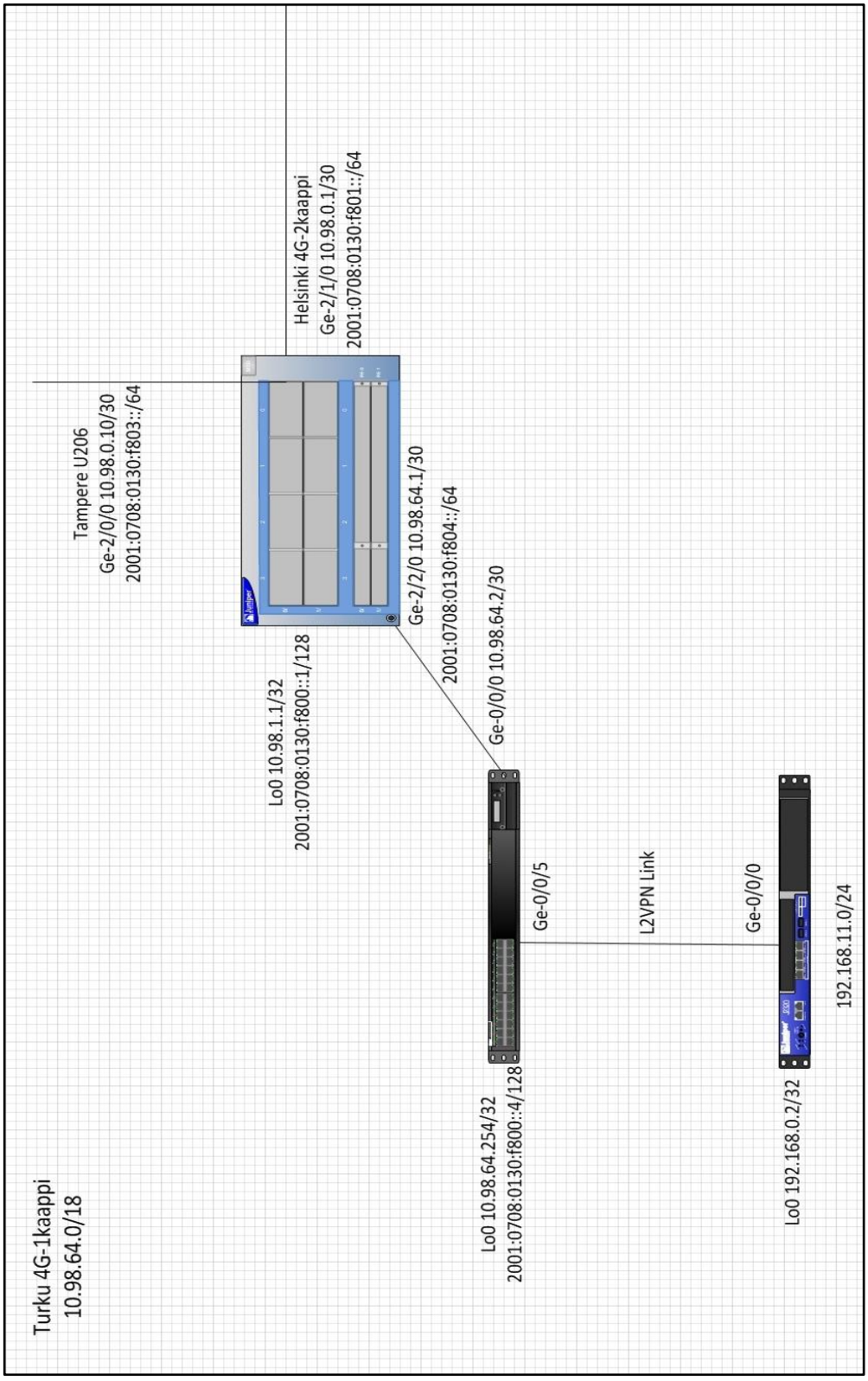
SNMP logging: enabled
    Logging to 10.95.250.76.162, 0/50, 7484 sent, 0 dropped.

core-rtr1 Cisco-reitittimen show ip cache flow -komento

```
core-rtr1#show ip cache flow
IP packet size distribution (168601 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .032 .649 .177 .026 .023 .022 .021 .000 .001 .006 .000 .004 .005 .000 .006

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .005 .000 .016 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  15 active, 65521 inactive, 59960 added
  1468946 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 533256 bytes
  15 active, 16369 inactive, 59911 added, 59911 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol        Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------        Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet        877      0.0         1    44      0.0       0.0       1.5
TCP-BGP         20587      0.2         1    45      0.2       0.3      15.4
TCP-other       10552      0.1         4    63      0.5       8.3      14.9
UDP-NTP           273      0.0         1    76      0.0       0.0      15.4
UDP-other       10695      0.1         4    86      0.5      16.2      15.3
ICMP             3102      0.0         3   352      0.1      23.8      15.3
IGMP             5449      0.0         1    29      0.0       0.0      15.5
IP-other         8411      0.0         3    71      0.3      21.6      15.3
Total:          59946      0.6         2    86      1.9       8.7      15.1

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi3/0         10.95.128.37    Null          224.0.0.13      67 0000 0000     1
Gi3/0         10.95.129.10    Local         10.95.128.41    06 0527 0016    26
Gi0/0         10.97.12.12     Local         10.97.12.11     06 2E41 0286     2
```

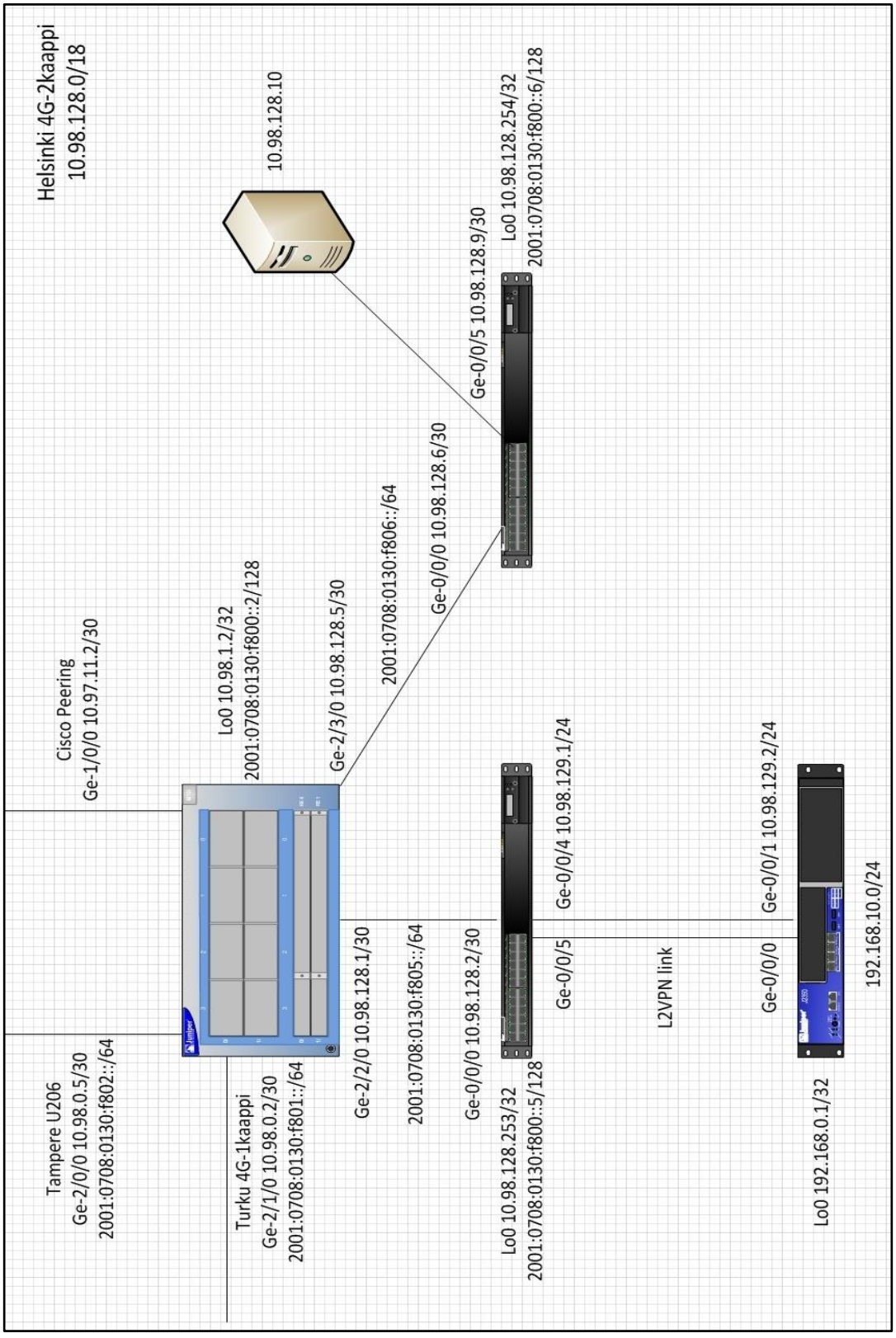
Gi4/0	10.97.10.89	Local	10.97.10.90	06 D00F 00B3	1
Gi0/0	10.97.10.2	Null	224.0.0.5	59 0000 0000	94
Gi4/0	10.97.10.89	Null	224.0.0.5	59 0000 0000	116
Gi0/0	10.97.10.2	Null	224.0.0.13	67 0000 0000	1
Gi4/0	10.97.12.13	Nu0	10.97.12.23	06 0286 E668	4
Gi0/0	10.97.10.2	Null	224.0.0.2	11 0286 0286	288
Gi4/0	10.97.10.89	Null	224.0.0.2	11 0286 0286	283
Gi4/0	10.97.12.13	Nu0	10.97.12.23	06 0286 850A	2
Gi3/0	10.95.250.76	Local	10.97.12.11	01 0000 0303	4
Gi3/0	10.95.128.34	Local	10.95.128.41	06 D9CC 00B3	1

Metropolia ammattikorkeakoulun Turun Juniper-verkon topologia



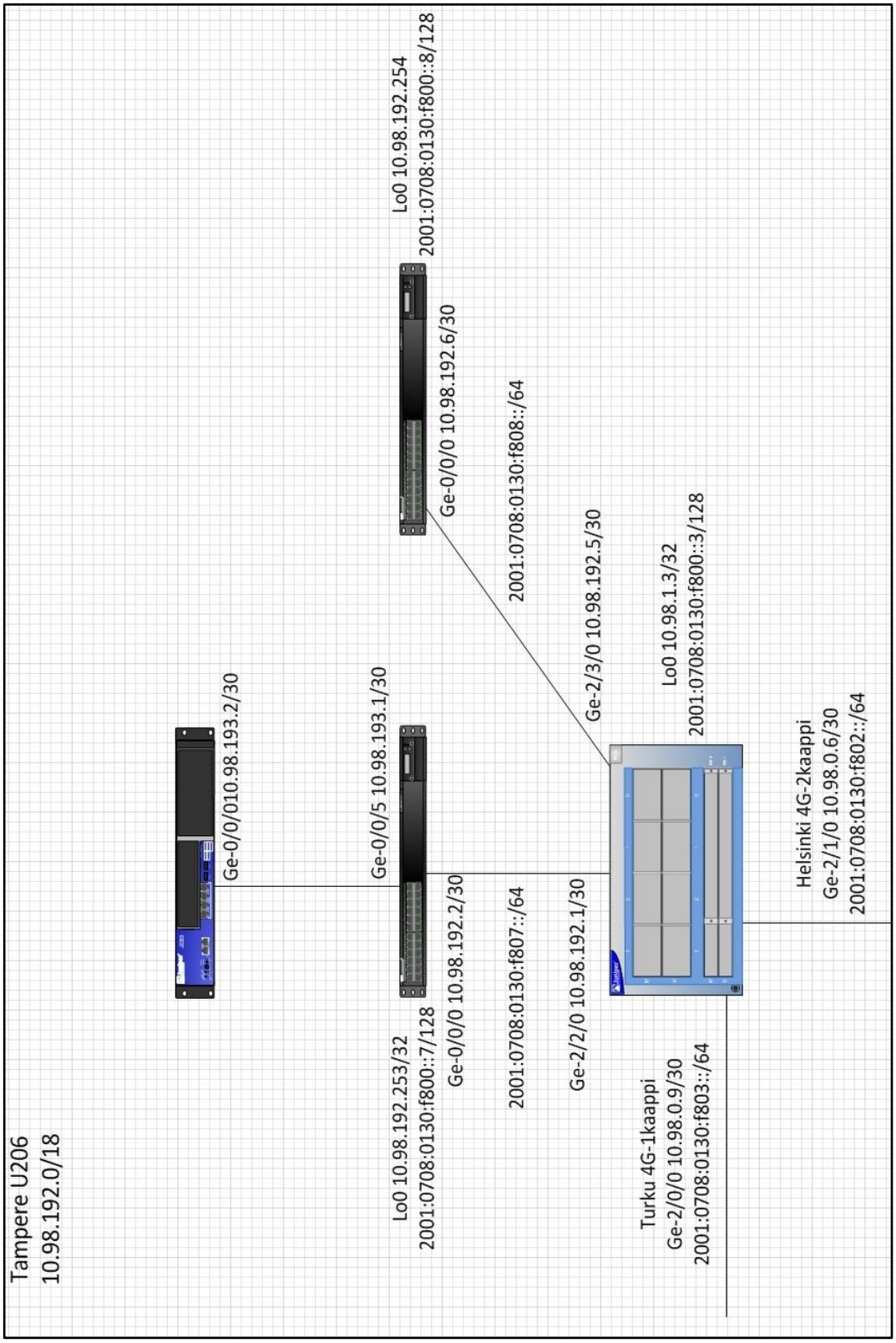
Kuva 1. Metropolia ammattikorkeakoulun Turun Juniper-verkon topologia [118]

Metropolia ammattikorkeakoulun Helsingin Juniper-verkon topologia



Kuva 2. Metropolia ammattikorkeakoulun Helsingin Juniper-verkon topologia [118]

Metropolia ammattikorkeakoulun Tampereen Juniper-verkon topologia



Kuva 3. Metropolia ammattikorkeakoulun Tampereen Juniper-verkon topologia [118]