

Vesa Ävist

# Junos-harjoitteluympäristöt opetuksen kehittämistarkoituksiin

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinööriytyö

29.5.2013

Tekijä(t) Otsikko	Vesa Ävist Junos-harjoitteluympäristöt opetuksen kehittämistarkoituksiin
Sivumäärä Aika	43 sivua + 2 liitettä 29.5.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	projekti-insinööri Heikki Rahkonen
<p>Insinööriytyössä tutkittiin erilaisia menetelmiä, joita voitaisiin ottaa käyttöön Junos-verkkokäyttäjärjestelmän harjoittelussa Metropolia Ammattikorkeakoulussa Leppävaaran toimipisteessä. Tutkimuksesta saatuja tuloksia voidaan käyttää Juniperin laitteita hyödyntävien kurssien suunnittelussa ja toteutuksessa.</p> <p>Tutkimuksen aikana koulun laboratoriotiloissa ei ollut Juniperin laitteita. Laitteita oli kuitenkin palvelinhuoneessa Juniverse-varausjärjestelmän käytössä. Juniverse-järjestelmä ei kuitenkaan ollut vielä valmis, joten sen laitteet otettiin harjoittelukäyttöön terminaalipalvelimen avulla. Laitteita oli kuitenkin rajallisesti, joten ne riittivät vain pienille oppilasryhmille. Terminaalipalvelinta ja Juniversea voidaan hyödyntää Junos-harjoitteluun ainakin yksinkertaisilla kolmen laitteen verkoilla.</p> <p>Fyysisten laitteiden tuomien rajoitusten takia työssä tutkittiin myös virtuaalisia keinoja Junos-harjoitteluun. Junosphere-pilvipalvelua voidaan käyttää harjoitteluympäristönä virtualisoiduilla Juniperin laitteilla. Palvelun käyttöön tarvitsee vain tietokoneen ja toimivan internetyhteyden. Todettiin, että palvelu sopisi hyvin Junos-harjoitteluun sen saatavuuden, helppokäyttöisyyden ja harjoitusverkkojen laajuuden vuoksi. Palvelun hinta on kuitenkin suurin este sen käyttöönotolle. Palvelun soveltuvuutta Junos-harjoitteluun arvioitiin verkkolähteistä saatujen tietojen pohjalta.</p> <p>Myös ilmaisessa GNS3-verkkosimulaattorissa pystytään käyttämään virtuaalisia verkkolaitteita. GNS3-ympäristöön voidaan niin ikään toteuttaa laajoja verkkoja. Lisenssioikeudellisista syistä GNS3:ssa ei voida kuitenkaan käyttää Junosin levykuvia. GNS3:ssa testattiin kokeellisesti ilmaista Vyatta-käyttäjärjestelmää, jonka käyttöliittymä on hyvin samankaltainen Junosin kanssa. Vyatta todettiin toimivaksi ratkaisuksi GNS3:ssa. Testeissä havaittiin kuitenkin eroja Junosiin sen verran, että Junos-opetukseen sitä ei voi varauksetta suositella.</p>	
Avainsanat	GNS3, Junos, Junosphere, terminaalipalvelin, virtuaalikone, Vyatta

Author(s) Title	Vesa Ävist Junos practicing environments for developing teaching
Number of Pages Date	43 pages + 2 appendices 29 May 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Computer Networks
Instructor(s)	Heikki Rahkonen, Project Engineer
<p>This study explains various methods that can be used for practicing the Junos network operating system at the Metropolia University of Applied Sciences in Leppävaara. The results are used in the planning and implementing of courses which use Juniper Networks' devices.</p> <p>At the time of the study, the school had devices only in the server room and they were reserved for an unfinished Juniverse application. They were put into operation by implementing a terminal server. The amount of devices was limited to small student groups. The terminal server and Juniverse could be used for Junos training with simple three device networks.</p> <p>Virtual methods were also explored for Junos training. Firstly, it was observed that the Junosphere cloud service enables practicing with virtualized Juniper devices and only requires a computer and internet access. Consequently, Junosphere would be very suitable for Junos training because of its availability, ease of use and support for large scale networks. The applicability was evaluated by analyzing information gathered from various internet sources. However, the price of the service is its biggest drawback.</p> <p>Secondly, the GNS3 network simulator also uses virtualized network devices and supports large scale networks. However, the Junos license agreement does not allow using Junos images in GNS3. In addition, a free Vyatta network operating system was experimented in GNS3. Vyatta was a working solution for GNS3. Nevertheless, some noticeable differences to Junos were discovered, so Vyatta cannot be recommended for Junos training without reservations.</p>	
Keywords	GNS3, Junos, Junosphere, terminal server, virtual machine, Vyatta

## Sisällys

### Lyhenteet ja käsitteet

1	Johdanto	1
2	Junos-opetus Metropoliasa	2
3	Juniper Networks	3
3.1	Tietoa yrityksestä	3
3.2	Junos-käyttöjärjestelmä	4
3.3	Koulutustarjonta	5
4	Junosphere	8
4.1	Palvelukuvaus	8
4.2	Palvelun käyttö	9
4.3	Palvelun käyttö laboratorioharjoitteluun	11
5	Laboratorioverkko ja harjoittelu	13
5.1	Juniverse	13
5.2	Terminaalipalvelin	14
5.3	Esimerkkiharjoitus	20
6	Graafinen verkkosimulaattori	21
6.1	Ohjelman kuvaus	21
6.2	Lisenssiongelmat	22
7	Vyatta-käyttöjärjestelmä	23
7.1	Vyatta Network OS	23
7.2	Vyatta graafisessa verkkosimulaattorissa	24
7.3	Vertailua Junosiin ja arviointi	31
8	Yhteenveto	37
	Lähteet	39
	Liitteet	
	Liite 1. Terminaalipalvelimen konfiguraatio	
	Liite 2. Esimerkkiharjoitus	

## Lyhenteet ja käsitteet

BGP	<i>Border Gateway Protocol</i> . Reititysprotokolla, jota käytetään autonomisten järjestelmien välillä. BGP on polkuvektoriprotokolla, jonka reititys tehdään polun, sekä erilaisten verkkopolitiikkojen ja sääntöasetusten mukaan.
CLI	<i>Command-Line Interface</i> . Tekstipohjainen käyttöliittymä ihmisen ja tietokoneen väliseen kommunikointiin.
Daemon	<i>Disk And Execution Monitor</i> . Moniajojärjestelmissä, kuten Unixissa, taustaprosessina suoritettava ohjelma, jota käyttäjä ei suoraan hallitse. Daemonit käynnistyvät yleensä käyttöjärjestelmän käynnistyessä ja ne palvevat verkosta tulevia pyyntöjä, laitteiston toimintaa tai muita ohjelmia suorittamalla erilaisia tehtäviä.
DTE	<i>Data terminal equipment</i> . DTE eli päätelaite on tietoliikenneyhteyden päässä oleva laite, joka muuttaa käyttäjätiedon signaaleiksi tai muuttaa signaalit dataksi. DTE pystyy kommunikoimaan DCE laitteen kanssa.
GNS3	<i>Graphical Network Simulator version 3</i> . Graafinen verkkosimulaattori, jolla voidaan simuloida kompleksisia IP-verkkoja.
GPL	<i>GNU General Public License</i> . Laajasti käytössä oleva vapaan ohjelmiston julkaisuun tarkoitettu lisenssi. Kenellä tahansa on oikeus käyttää, kopioida, muuttaa ja jakaa GPL-lisenssin alaisuudessa olevia ohjelmia ja niiden lähdekoodia.
GUI	<i>Graphical User Interface</i> . Graafinen käyttöliittymä koostuu tekstin lisäksi kuvista ja muista graafisista elementeistä joiden avulla tietokonetta tai tietokoneohjattua laitetta voidaan käyttää.
Host	Tietokone, joka on kytketty tietoverkkoon.
IOS	<i>Internetwork Operating System</i> . Cisco Systemsin verkkolaitteiden käyttöjärjestelmä.

IP	<i>Internet Protocol</i> . Internet protokollapinin pääprotokolla, joka huolehtii IP-pakettien toimittamisesta perille pakettikytkentäisessä verkossa, erityisesti internetissä.
OSPF	<i>Open Shortest Path First</i> . OSPF on reititysprotokolla TCP/IP-verkoissa. OSPF käyttää reittien laskemiseen linkkilallista algoritmia, joka laskee reitit reitittimien määrän, tiedonsiirtonopeuden, viiveiden ja reitin hinnan mukaan.
POD	<i>Point of Delivery</i> . Podi on Verkkolaite, tietokone, tallennus ja/tai ohjelmisto komponenteista muodostuva kokonaisuus, joka tarjoaa verkkopalveluita.
SSH	<i>Secure Shell</i> . Salattuun tietoliikenteeseen tarkoitettu verkkoprotokolla.
TCP	<i>Transmission Control Protocol</i> . Tietoliikenneprotokolla, joka mahdollistaa luotettavien, järjestettyjen ja virheiltä tarkistettujen datavirtojen kuljettamisen IP-verkossa olevien tietokoneiden välillä. TCP on internet-protokollapinin keskeisimpiä protokollia.
TCP-/UDP-portti	Portti täydentää tiedonvälityksessä kohteen IP-osoitetta. Portti määrittää sovelluksen tai prosessin, jonka käsiteltäväksi datapaketti annetaan.
telnet	Telnet on yhteysprotokolla kaksisuuntaisiin pääteyhteyksiin TCP-protokollan päällä.
TTY	<i>Terminal Type tai Teletype line</i> . TTY-linjat ovat fyysisiä laitteistopohjaisia asynkronisia yhteyksiä. Niitä käytetään terminaaliyhteyksiin joissa suoritetaan tekstipohjaisia sovelluksia.
UDP	<i>User Datagram Protocol</i> . UDP on yksi internet-protokollapinin ydinprotokollista ja mahdollistaa TCP:n tapaan tiedonsiirron IP-verkossa olevien tietokoneiden välillä. UDP:ssä ei kuitenkaan suoriteta alkukättelyä, kuittau- lua eikä kolmivaiheista kättelyä.

- VM *Virtual Machine*. Virtuaalikone on tietokone, joka on toteutettu ohjelmallisesti ja jossa voidaan ajaa ohjelmia kuten aidossa tietokoneessa.
- VM-yksikkö *Virtual Machine* -yksikkö. Junosphen tilaukseen ja kulutukseen liittyvä termi. Yksi VM-yksikkö mahdollistaa virtuaalikoneen ajamisen Junosphe-  
ressä 24 tunnin ajan.
- VTY *Virtual Teletype* tai *Terminal line*. VTY-linjat ovat virtuaalisia TTY-linjoja. Niitä käytetään, kun reitittimeen yhdistetään telnetillä tai SSH:lla.

## 1 Johdanto

Juniper Networks on yksi maailman suurimmista IP-verkkolaittevalmistajista ja yksi Cisco Systemsin vahvimista kilpailijoista. Erityisesti palveluntarjoajien runkoreitinmarkkinoilla sillä on menestyksekkäs historia. Kaikissa Juniper Networksin verkkolaitteissa on käytössä Junos-käyttöjärjestelmä. (1.)

Metropolia Ammattikorkeakoulussa järjestetään kattavasti opetusta Ciscon IOS-käyttöjärjestelmälle. Tietoverkko-opiskelijoilla olisi kuitenkin hyvä olla opiskelujen kautta tuntumaa muidenkin valmistajien käyttöjärjestelmiin. Monipuolisempi osaaminen valmentaa opiskelijaa työelämän vaihteleviin tehtäviin ja haasteisiin. Junos-osaaminen on arvokas valtti työmarkkinoilla.

Perinteisesti IP-verkkotekniikoita harjoitellaan laboratorioissa oikeilla laitteilla. Metropolian Leppävaaran toimipisteen IP-laboratorioissa ei kuitenkaan ole Juniperin verkkolaitteita. Laitteita on muutama käyttämättömänä palvelinhuoneessa. Ne voidaan ottaa käyttöön Junos-harjoittelussa etäyhteyksien avulla. Virtualisoinnin ja pilvipalvelujen yleistymisen myötä on tullut uusia keinoja tehdä harjoituksia, myös ilman fyysisiä laitteita. Juniperin oma Junosphere pilvipalvelu mahdollistaa virtualisoidun harjoitteluympäristön esimerkiksi opiskelijan omalla tietokoneella. Myös avoimen lähdekoodin graafinen verkkosimulaattori, GNS3, hyödyntää virtualisointia verkon simuloinnissa.

Insinöörityön tavoitteena on selvittää Junospheren, etäyhteyksien ja verkkosimulaattorin käyttöä Junos-harjoitteluun ja pohtia esimerkein niiden soveltuvuutta opetuskäyttöön. Lisäksi tutkitaan Vyatta nimistä avoimen lähdekoodin verkkokäyttöjärjestelmää, jonka käyttöliittymä on hyvin samankaltainen Junosin kanssa. Vyattan käyttämistä harjoitteluun ja eroja Junos-käyttöjärjestelmään selvitetään kokeellisesti. Työn tuloksia voidaan hyödyntää mahdollisten tulevien Junos-kurssien suunnitteluun. Lisäksi esimerkiksi opiskelijat voivat hyödyntää verkkosimulaattorin käytöstä saatuja tuloksia itsenäiseen harjoitteluun.

## 2 Junos-opetus Metropoliaassa

Metropolian Leppävaaran toimipisteessä Espoossa tietotekniikan koulutusohjelmassa ei järjestetä varsinaista Junos-opetusta. Kolmannen tai neljännen vuoden opiskelijoilla on kuitenkin mahdollisuus osallistua koko kevätlukukauden kestäväan laajahkoon tietoverkkoprojektiin. Projektin verkossa käytetään Juniperin reitittimiä ja kytkimiä. Junosin käyttö tulee tutuksi projektin edetessä. Aiempi kokemus tosin helpottaisi ja nopeuttaisi projektin etenemistä, kun opiskelijan ei tarvitsisi käyttää aikaa Junosin perusteiden opetteluun.

Kaikilla tietoverkko-opiskelijoilla on hyvä kokemus Ciscon laitteista ja niiden IOS-käyttöjärjestelmästä. Ciscon kurssit alkavat jo ensimmäisenä opiskeluvuotena. Ciscon kursseilta opiskelijat saavat vahvat pohjatiedot verkkotekniikoista ja -protokollista. Junos-opetus sopisikin parhaiten opetettavaksi myöhempinä vuosina, jolloin opiskelija pääsee hyödyntämään aiemmin oppimaansa.

Helsingissä, Metropolian Bulevardin toimipisteessä järjestetään kerran vuodessa Junos-perusteet kurssi. Opettajana toimii lehtori Marko Uusitalo. Kurssi sisältää teoriaopetusta ja laboratorioharjoituksia koulun IP-laboratoriossa. Luentomateriaali pohjautuu pääasiassa JNCIA-Junos opiskelu oppaaseen, joka löytyy Juniperin sivuston opintoportaalista Fast Track -ohjelman alta. Materiaaliin pääsy vaatii rekisteröitymisen. Laboratorioharjoitukset Uusitalo on kehittänyt kokonaan itse ja niissä käytetään sekä Ciscon että Juniperin laitteita. Bulevardin IP-laboratoriossa on kuusi laiteräkkiä, joissa on usean Ciscon reitittimen ja kytkimen lisäksi kaksi kappaletta Juniper SRX210 Services Gateway -laitetta. (2; 3.)

### 3 Juniper Networks

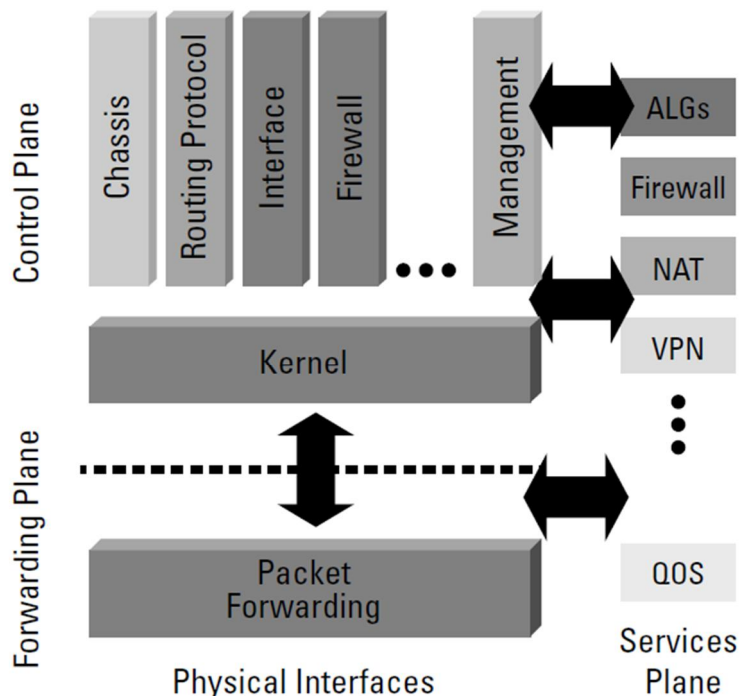
#### 3.1 Tietoa yrityksestä

Juniper Networks on yhdysvaltalainen verkkolaitteiden valmistaja. Yrityksen perusti vuonna 1996 tiedemies Pradeep Sindhu, joka toimii nykyään yrityksen teknologiajohtajana. Internet kasvoi räjähdysmäisesti 1990-luvulla, joten palveluntarjoajilla oli kasvava tarve nopeammista reitittimistä. Sindhun idea oli vastata kysyntään kehittämällä lukuisien yhteistyökumppaneiden kanssa yhtiön ensimmäinen ja markkinoiden nopein runko-reititin. Juniper M40-reititin oli myös markkinoiden ensimmäinen reititin, jonka paketin edelleenlähetys oli toteutettu laitteessa omalle sirulle. Reititin oli jättimenestys mullistavan arkkitehtuurinsa ansiosta. Menestys mahdollisti Juniper Networksin nopean laajenemisen ja kasvamisen yhdeksi merkittävimmistä verkkolaittevalmistajista. Yritys listautui pörssiin vuonna 1999. (1.)

Juniper Networks on kovasta kilpailusta huolimatta 90-luvun lopusta lähtien pitänyt pintansa reititinmarkkinoilla. Ensimmäisen kytkimen yhtiö julkaisi vasta vuonna 2008. Nykyään yhtiön tuotevalikoima on laaja ja siihen kuuluu mm. reitittimiä, ethernet-kytkimiä ja tietoturvalaitteita moneen eri tarpeeseen. Lisäksi yhtiö tarjoaa asiakkailleen konsultointi-, asennus- ja ylläpitopalveluita. Asiakkaina on satoja tunnettuja verkko-operaattoreita, yrityksiä ja julkisen sektorin organisaatioita. Yhtiön pääkonttori sijaitsee Sunnyvalessa, Kaliforniassa. Työntekijöitä yhtiössä on yli 9000 ja sillä on toimistoja 46:ssa eri maassa. Yhtiön liikevaihto vuonna 2012 oli noin 4,365 miljardia dollaria. (1; 4.)

### 3.2 Junos-käyttöjärjestelmä

Junos-käyttöjärjestelmä on käytössä lähes kaikissa Juniperin julkaisemissa verkkolaitteissa. Sen ensimmäinen versio julkaistiin M40-reitittimen mukana vuonna 1998. Käyttöjärjestelmä vastaa pakettien hallinnoinnista ja edelleenlähetyksestä sekä verkon erilaisten palvelujen toteutumisesta. Junosin arkkitehtuurissa nämä tehtävät ovat selkeästi erotettu omiin toimintatasoihinsa: hallinta-, edelleenlähetys- ja palvelutasoon. Tämä jako mahdollistaa Junosin skaalautuvuuden erilaisille alustoille. Kuva 1 esittää Junosin arkkitehtuuria sekä esimerkkiprosesseja, joita hallinta- ja palvelutasoilla voidaan ajaa. (5, s. 9–12.)



Kuva 1. Junosin arkkitehtuuri (5, s. 12).

Kaikkia hallintatason prosesseja suorittaa verkkolaitteen *reititysmoottori* (RE). Hallintatasolla on jokaisella prosessilla oma moduulinsa ja rajapinnat moduulien välille. Käyttöjärjestelmän ydin eli kerneli ohjaa moduuleita ja vastaa tiedonvälityksestä kaikkien osien välillä. Ydin pohjautuu Unix-tyyppisen avoimen lähdekoodin käyttöjärjestelmän, FreeBSD:n kerneliin. FreeBSD:n kerneli on Junosissa perusteellisesti muokattu verkkotyöskentelyn tarpeisiin. Laitteeseen tulevien pakettien vastaanottoa ja lähetystä suorittaa edelleenlähetystasolla *paketin edelleenlähetysmoottori* (PFE). Se sisältää oman

edelleenlähetystaulun, jossa on reititysmoottorilta (RE) saadut tiedot, kuinka paketteja tulee käsitellä. Näin PFE pystyy toimimaan itsenäisesti hallintatason tilasta riippumatta. Palvelutasolla palvelujen prosessointi on niin ikään eristetty muusta toiminnasta, mikä mahdollistaa laajan yhteensopivuuden eri tyyppisten palvelujen kanssa alustasta riippumatta. (5, s. 12–14.)

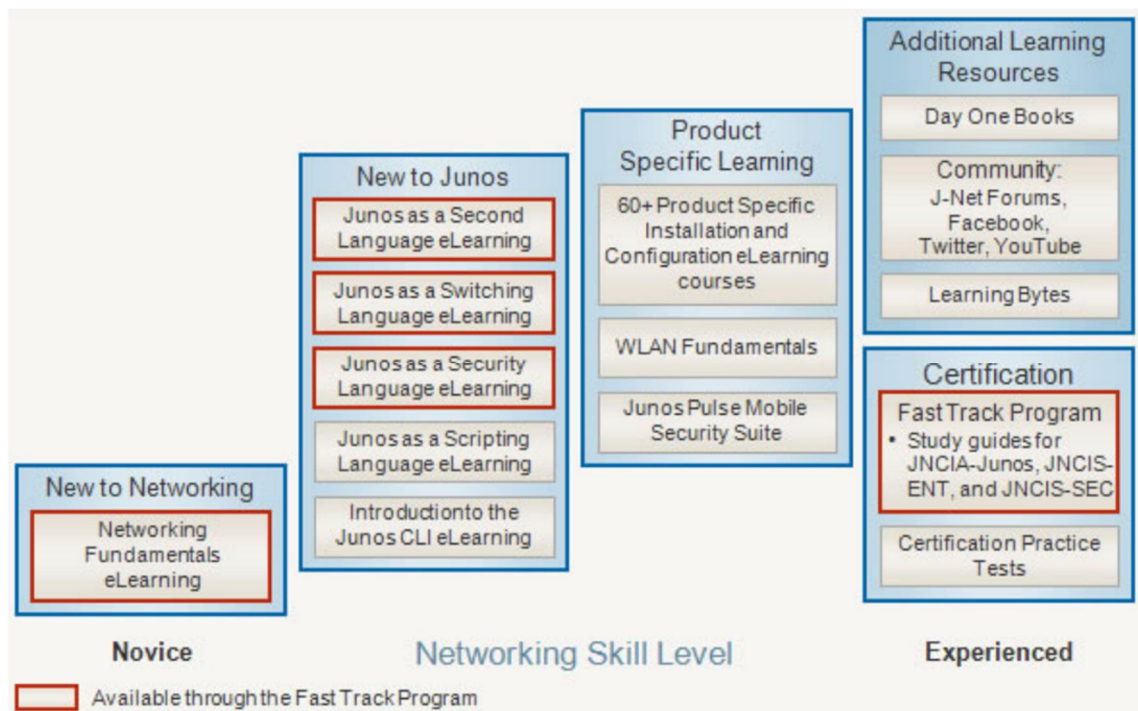
Junos on modulaarisen arkkitehtuurinsa ansiosta vakaa käyttöjärjestelmä. Jokainen hallintatason moduuli (Unixeissa daemon) suoritetaan omassa muistiavaruudessaan ja sen käytössä on tietyt resurssit. Jos yksi moduuli aiheuttaa virheen tai kaatuu, muut moduulit ja järjestelmä pystyvät jatkamaan toimintaansa normaalisti. Virheen paikantaminen ja korjaaminen on myös helpompaa. Modulaarisuus helpottaa myös uusien ominaisuuksien ja palvelujen tuomista järjestelmään. Junosin päivittäminen uuteen versioon on siten turvallista, eikä tuo mukanaan uusia ongelmia. Uudet versiot toimivat kaikissa alustoissa, joissa Junos on asennettuna. Juniper Networks julkaisee päivityksen neljästi vuodessa. (5, s. 14–16.)

Junosia käytetään yleensä komentoliittymän (CLI) kautta. Joillakin alustoilla on tarjolla myös web-pohjainen graafinen käyttöliittymä (GUI) J-Web. Komentoliittymä on kuitenkin totuttelun jälkeen paljon nopeampi ja helpompi käyttää. Komentoliittymässä kaksi komentotilaa: toiminnallinen tila ja konfigurointitila. Toiminnallisessa tilassa voidaan hallita ja valvoa laitteistoa ja ohjelmistoa sekä tarkkailla verkon toimintaa. Konfigurointitilassa määritetään laitteen käyttäytyminen, kuten mitä protokollia, turvallisuusasetuksia ja liitäntöjä käytetään. Kaikki komennot ja toiminnot on järjestetty hierarkkisesti. Tämä ryhmittää loogisesti toisiinsa liittyvät lisäkomennot niitä edeltävän komentosan alle. (6, s. 8; 7, s. 1–2.)

### 3.3 Koulutustarjonta

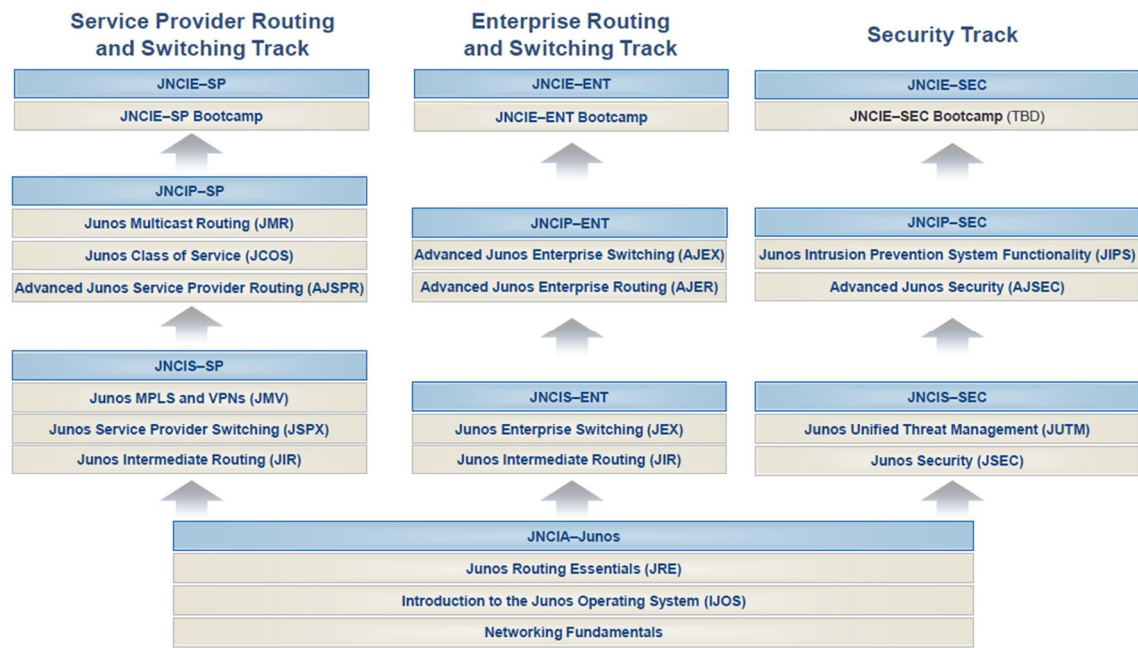
Juniper Networks tarjoaa paljon erilaisia opiskeluvaihtoehtoja. Maksullisia ohjattuja kursseja on saatavilla verkossa sekä Juniper Networksin koulutuskeskuksissa ja valtuutetuilta koulutuspartnereilla ympäri maailmaa. Oman alueen kurssitarjonnan voi tarkistaa osoitteessa [www.juniper.net/courses](http://www.juniper.net/courses). Samalta sivulta voi hakea myös verkkokursseja, jotka ovat ilmaisia. Verkkokursseihin ja Juniper Learning Bytes -opetusvideoihin pääsee käsiksi rekisteröitymällä ensin opintoportaaliin osoitteessa [learningportal.juniper.net/](http://learningportal.juniper.net/). Lisäksi osoitteesta [forums.juniper.net/](http://forums.juniper.net/) löytyy J-Net-yhteisö,

jonne voi rekisteröityä jos on yhtiön partneri tai asiakas. Rekisteröitymiseen tarvitsee auktorisointikoodin tai Juniperin tuotteen sarjanumeron. J-Net-jäsenet voivat foorumin käytön lisäksi ladata ilmaiseksi mitä tahansa kirjoja Day One -kirjastosta osoitteessa [www.juniper.net/us/en/training/jnbooks/day-one/](http://www.juniper.net/us/en/training/jnbooks/day-one/). Kuvasta 2 käy ilmi kaikki ilmaiseksi saatavilla oleva opetusmateriaali.



Kuva 2. Ilmaiset opiskelumateriaalit verkossa (8).

Sertifikaatit ovat työelämässä arvostettu osaamisen mittari. Juniper Networksilla on Junos-käyttöjärjestelmään liittyviä sertifikaatteja yhteensä kymmenen erilaista. Lisäksi E-sarjan laitteille, palomuureille ja VPN:lle, Junos Pulselle ja QFabricille löytyvät omat sertifikaattinsa. Alimman (Associate) tason Junos-sertifikaatin (JNCIA-Junos) suorituksen jälkeen valittavissa on kolme eri sertifiointipolkua: palveluntarjoajan reititys ja kytkentä (SP), yritysten reititys ja kytkentä (ENT) sekä tietoturvapolku (SEC). Jokaiseen polkuun kuuluu kolme eritasoista sertifikaattia: spesialisti (S), ammattilainen (P) ja asiantuntija (E). Kuva 3 esittää sertifiointipolut sekä sertifiointiin valmistavat kurssit. Kirjainyhdistelmä JNCI tulee sanoista Juniper Networks Certified. Juniper opintoportaalin Fast Track -ohjelma tarjoaa ilmaiset itseopiskelumateriaalit JNCIA-Junos-, JNCIS-ENT- ja JNCIS-SEC-sertifikaateille. Ohjelmasta saa alennuskupongit sertifikaattikokeisiin, jos läpäisee verkossa olevan esiarviointikokeen. (9.)



Kuva 3. Sertifiointipolut (9, s. 5).

Akateemisille yhteisöille, kuten yliopistoille, yhtiöllä on tarjolla Juniper Networks Academic Alliance (JNAA) -ohjelma. Ohjelman tarkoitus on yhteistyösuhteen muodostaminen yhtiön ja yliopiston välille. JNAA-jäsenyyden sisältö rakennetaan modulaarisesti. Moduuleja on viisi erilaista, joista korkeakoulu voi valita haluamansa omien tarpeidensa mukaan. Riippuen valituista moduuleista tarjolla on muun muassa kurssi- ja koulutusmateriaalia, alennuksia yhtiön tuotteista ja Junosphere-virtuaalilaboratorioympäristöstä, sekä alennuskuponkeja sertifikaattikokeisiin. Lisäksi on mahdollisuus myös jäsenyyksiin, joissa yliopisto pääsee tekemään tutkimus- ja kehitysyhteistyötä Juniper Networksin kanssa. (10.)

## 4 Junosphere

### 4.1 Palvelukuvaus

Junosphere on pilvilaskentaan pohjautuva palvelu ja virtuaaliympäristö, johon voidaan rakentaa verkkotopologioita virtualisoiduilla verkkolaitteilla. Junosphere on kehitetty verkkosuunnitteluun, testaukseen ja harjoitteluun Juniperin laitteilla. Virtuaalisissa laitteissa on sama Junos-käyttöjärjestelmä kuin oikeissa fyysisissä laitteissa. Lisäksi laitteet käyttäytyvät samalla tavalla ja tukevat kaikkia samoja protokollia kuin fyysisetkin laitteet. Tämä tarkoittaa myös sitä, että jos Junosin versiossa on jotain ohjelmointivirheitä, joita ei ole vielä korjattu, virheet ovat mukana myös virtuaalisessa käyttöjärjestelmässä. (11, s. 1–2.)

Koska palvelu sijaitsee internetissä, sen käyttöön ei tarvitse tietokoneen lisäksi kuin toimivan internet-yhteyden ja verkkoselaimen. Junosphere luokitellaan kuuluvaksi niin kutsuttuun ohjelmisto palveluna eli SaaS (Software as a Service) -pilvipalveluluokkaan. Pilven käyttäjät eivät pääse käsiksi pilven sisäiseen rakenteeseen tai ohjelmistoalustaan. Palvelun tarjoaja vastaa sovelluksen hallinnasta. Palvelu pystyy skaalautumaan lisääntyvään kuormitukseen ajon aikana jakamalla työtaakkaa usean virtuaalikoneen kesken. (12.)

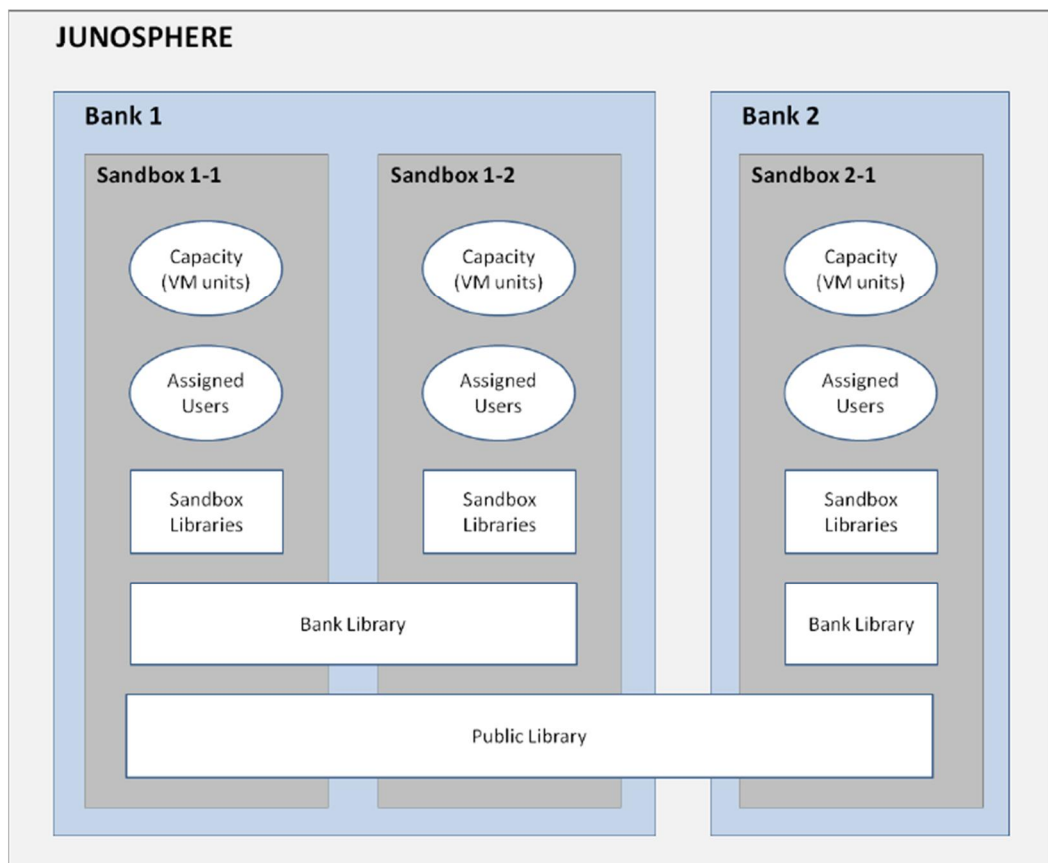
Junosphenen käyttöliittymään pääsee kirjautumaan osoitteessa [www.junosphere.net](http://www.junosphere.net). Palvelu on maksullinen ja on käytössä ympäri vuorokauden. Käyttäjätunnukset Junosphereen palvelun tilaaja saa ilmoittamaansa sähköpostiosoitteeseen. Palvelun graafinen käyttöliittymä on selkeä ja yksinkertainen käyttää.

Palvelu voidaan ostaa joko käyttötarpeen mukaan tai vuotuisena kiinteänä pakettina. Hinta määräytyy tarvittavan ajan ja virtuaalikoneiden määrän mukaan. Palvelupaketit koostuvat niin kutsutuista VM-yksiköistä, jotka maksavat viisi dollaria kappale. Yhdellä VM-yksiköllä voidaan ajaa yhden verkkolaitteen levykuvaa virtuaalisesti yhden vuorokauden ajan. Vuotuinen paketti on tarpeen silloin, kun kapasiteetti on jatkuvassa käytössä. Tällöin käytössä on aina tietty määrä VM-yksiköitä joka päivä ympäri vuorokauden. Jos taas ostetaan käytön mukaan maksettavia VM-yksiköitä, niin ne kuluvat vain silloin kun ajetaan aktiivinen verkkotopologia. Junosphere laskee vain vuorokaudet eli 24 tuntia, eikä sitä voi pilkkoa pienempiin osiin ja käyttää myöhemmin. Esimerkiksi ajat-

taessa kolmesta virtuaalisesta verkkolaitteesta koostuvaa verkkotopologiaa kahtena eri 24 tunnin ajanjaksona kuluu yhteensä kuusi VM-yksikköä. Käyttämätön kapasiteetti on voimassa vuoden ajan ostopäivästä. (11, s. 4.)

#### 4.2 Palvelun käyttö

Ostettu kapasiteetti tallentuu asiakkaan Junospheressä niin kutsuttuun pankkiin. Junospheressä on kahdenlaisia käyttäjätilejä: Pankin ylläpitäjä ja tavallinen käyttäjä. Pankin ylläpitäjän tehtävä on hallita Junospheren käyttöä. Hän voi muun muassa lisätä pankille uusia käyttäjiä, luoda uusia työtiloja (Sandbox) ja määrittää niiden kapasiteetin (VM-yksiköitä) ja käyttäjät sekä hallita käyttäjien käyttöoikeuksia. Lisäksi pankin ylläpitäjä voi luoda uusia topologioita ja tallentaa niitä pankin kirjastoon tai työtilojen kirjastoihin. Kuvasta 4 näkyy pankin kaikki komponentit ja eri topologiakirjastojen näkyvyys työtiloihin. (13, s. 4–6.)



Kuva 4. Junosphere-pankin rakenne (13, s. 5).



ja/tai työtilan topologiakirjastoon. Pankin kirjastoon tallennetut topologiat ovat käytettävissä kaikissa työtiloissa. (16, s. 5–9.)

Topologiassa voidaan käyttää virtuaalisia laitteita VXJ, VSRX ja VPTX. Uusia virtuaalilaitteita kehitetään koko ajan lisää. Tulossa on virtuaaliset vastineet ainakin MX-sarjan reunareitittimille ja EX-sarjan ethernet-kytkimille. (17, s. 11; 18, s. 4–8.) Lisäksi topologiaan voi lisätä virtuaalikoneita Juniper-partnereiden tarjoamista levykuvista. VXJ vastaa ominaisuuksiltaan Juniperin J-sarjan fyysisiä reitittimiä. VSRX vastaa sivukonttoreille tarkoitettuja SRX-sarjan fyysisiä laitteita. VPTX laitteet vastaavat palveluntarjoajien PTX-runkoverkkoreitittimiä. (19.) Lisäksi Junosphereen voidaan ostaa VM-yksiköiden tapaan vuorokausiluontoisesti Junosphere Connector, joka mahdollistaa topologioiden yhdistämisen pilvestä fyysiseen verkkoon. Yhteys toimii maksimissaan 1 Mbps:n nopeudella. (20.)

Topologioiden käynnistys tapahtuu ensin varaamalla työtilaan topologian vaatiman määrän VM-yksiköitä. Kun topologia on käynnistetty, siihen tulee liittyä, jotta virtuaalikoneisiin saadaan omalta koneelta yhteys. (14, s. 31–32.) Yhteys muodostuu Junospheren käyttöliittymästä SSL-VPN -yhteyttä käyttäen. Tämän jälkeen virtuaalikoneisiin voidaan yhdistää terminaaliohjelmalla ja päästään käyttämään Junosia. (14, s. 39–41.)

#### 4.3 Palvelun käyttö laboratorioharjoitteluun

Junosphere soveltuisi hyvin Junos-harjoitteluun. Palvelu on opetus ja tutkimus käytössä ainakin Georgia Institute of Technology, Princeton University ja Queen Mary, University of London korkeakouluissa (21).

Harjoitusverkon koolla eivät tule rajoitukset, kuten tilanpuute ja korkea hinta, niin nopeasti vastaan kuin fyysisillä laitteilla. Lisäksi aikaa ei kulu kaapeleiden kytkemiseen tai mahdollisten vikatilanteiden selvittämiseen. Sähkönkulutus pienenee huomattavasti. Jokaiselle opiskelijalle on mahdollisuus tarjota omat virtuaaliset verkkolaitteet, eikä työtilaa tarvitse näin ollen jakaa muiden oppilaiden kanssa. Tämä tosin voi tulla pidemmällä tähtäimellä kalliiksi, jos opiskelijoita on paljon, mutta johtaisi varmasti parempaan oppimistulokseen.

Opiskelijoille ei tulisi antaa topologioiden hallintaoikeutta, koska muuten he pystyvät käynnistämään topologian turhaan ja tuhlaamaan näin maksetut VM-yksiköt. Vaikka opiskelijoille ei olisi annettu mitään oikeuksia, he voivat silti liittyä aktiiviseen topologiaan ja tehdä näin ollen laboratorioharjoituksia.

Ohjaajat tai opettajat toimisivat pankin ylläpitäjinä. Heidän tehtävänään olisi luoda opiskelijoille käyttäjätilit ja laittaa heidät oikeisiin työtiloihin. Lisäksi opettajat vastaisivat harjoitustopologioiden tekemisestä topologiavelholla. VM-yksiköiden tilaus tarpeen mukaan olisi myös heidän vastuullaan. Tarve määräytyy tehtyjen harjoitustopologioiden laajuuden mukaan.

On kuitenkin huomioitava, että Junosphere voi tulla pitkällä aikavälillä melko kalliiksi, varsinkin jos harjoitusverkoista tehdään laajoja ja niissä käytetään paljon virtuaalikoneita. Tosin Juniper Networks saattaa antaa palvelusta alennusta korkeakouluille, esimerkiksi JNAA-jäsenyyden kautta (Juniper Networks Academic Alliance).

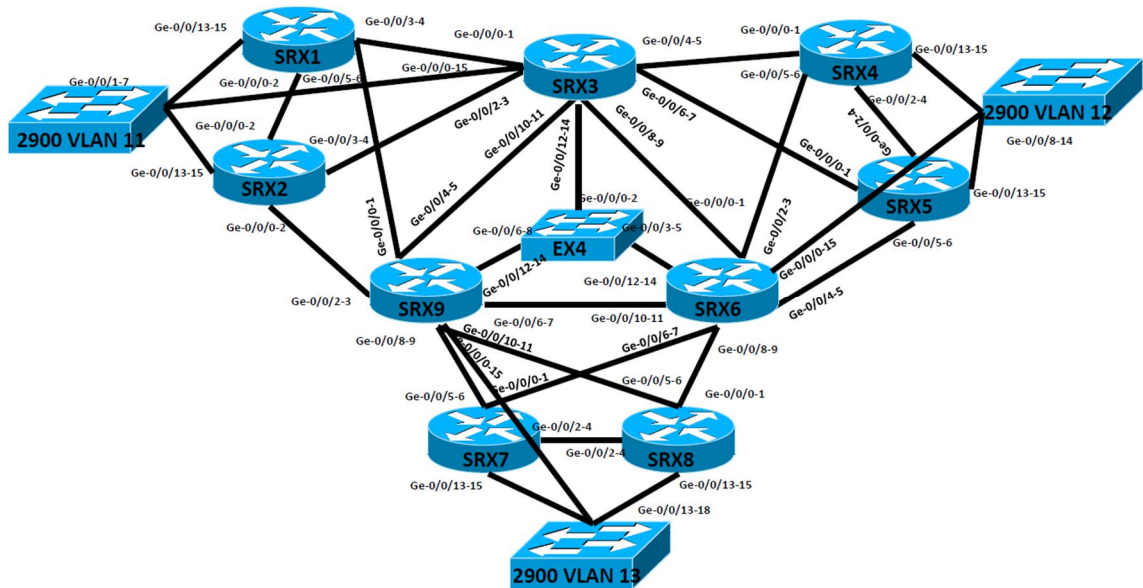
Esimerkkinä käytettäköön harjoitteluympäristöä, jossa on viisi työtilaa ja jokaisessa työtilassa pankin ylläpitäjän lisäksi neljä käyttäjää. Opiskelijoita olisi esimerkiksi 20, he jaettaisiin neljän hengen ryhmiin ja jokaiselle ryhmän jäsenelle annettaisiin tunnukset omaan työtilaansa. Jokaisessa työtilassa olisi varattuna neljä VM-yksikköä, mikä mahdollistaa neljän virtuaalikoneen ajamisen vuorokauden ajan. Jokaisen ryhmän opiskelijalle tulisi tässä tapauksessa siis konfiguroitavaksi yksi virtuaalinen verkkolaite. Tämä maksaisi kaiken kaikkiaan 100 dollaria vuorokautta kohden (24 tuntia). Tosin kuluja voisi vähentää pitämällä samana päivänä saman harjoituksen eri 20 hengen opiskelijaryhmille. Jos taas jokaiselle opiskelijalle annettaisiin oma työtila samalla VM-yksikkömäärällä, hintaa tulisi 400 dollaria vuorokautta tai harjoituskertaa kohden.

## 5 Laboratorioverkko ja harjoittelu

### 5.1 Juniverse

Metropolia Ammattikorkeakoulun Leppävaaran toimipisteessä on opetuskäyttöön varattu yhteensä 26 Juniperin verkkolaitetta. Joukossa on 18 kappaletta SRX240 Services Gateway -laitteita, viisi kappaletta EX3200 Ethernet -kytkimiä ja kolme kappaletta MX80-reitittimiä. Näistä yhdeksän SRX240-laitetta on tarkoitettu kehitteillä olevan Juniverse-sovelluksen käyttöön. Loput laitteet on varattu kevään tietoverkkoprojektia varten. Laitteet ovat kaikki palvelinhuoneessa, tietoverkkoprojektin laitteet omassa räkissä ja Juniversen laitteet omassaan. Laitteita ei tulla siirtämään laboratoriotiloihin kuten Bulevardin toimipisteessä. Ciscon kurssija suorittaneille opiskelijoille kaapeleiden jatkuva edestakaisin kytkeminen, jota joutuu tekemään paljon fyysisillä laitteilla, olisi muutenkin ajan haaskausta.

Juniverse-sovellus on ohjelmistotekniikan harjoittelijaopiskelijoiden vuonna 2012 aloittama projekti. Projektin ideana on kehittää NDG:n Netlabia vastaava selaimen kautta toimiva web-sovellus. Netlab-sovellus mahdollistaa koulun Cisco-kurssien laboratorioharjoitusten tekemisen etänä. Tunnuksella sovelluksen käyttöön opiskelija saa opettajalta. Opiskelija pystyy varaamaan web-käyttöliittymän kautta käyttöönsä valmiiksi yhteen kytketyistä oikeista verkkolaitteista koostuvia laiteryhmiä eli podeja. Käyttöliittymästä voidaan vapaasti hallita ja konfiguroida laitteita varatun ajan puitteissa. Kun harjoitus lopetetaan tai varattu aika loppuu, laitteet sammuvat ja vapautuvat muiden opiskelijoiden käyttöön. (22.)



Kuva 6. Juniverse-verkon topologia (23).

Juniverse-sovellus pyrkii samankaltaiseen varausjärjestelmään ja verkkolaitteiden etäkäyttöön. Sovellus ei ole niin kehittynyt ja monipuolinen kuin kaupallinen Netlab, mutta olisi silti hyvä harjoitteluväline. Riippuu tietysti siitä miten pitkälle sitä ollaan valmiita kehittämään. Sovellus tallentaa varaukset palvelimen tietokantaan. Kun opiskelija käynnistää tekemänsä varauksen, laitteisiin muodostuu SSH-yhteys. SSH-protokollan salaus takaa turvallisen etäyhteyden laitteisiin, käytettiinpä sovellusta missä tahansa. (24.) Järjestelmän verkkotopologia on esitettyä kuvassa 6. Podit muodostuvat kolmen SRX240-laitteen ryhmistä. Esimerkiksi ensimmäiseen podiin kuuluu SRX1, SRX2 ja SRX3, toiseen SRX4, SRX5 ja SRX6 ja niin edelleen. Sovellus ei kuitenkaan ollut tämän insinööriyön tekemisen aikana vielä valmis, eikä sen jatkokehityksestä ollut vielä varmaa tietoa, joten Junos-harjoitteluun oli etsittävä muita vaihtoehtoja.

## 5.2 Terminaalipalvelin

Telnet on kaksisuuntainen sovelluserroksella toimiva yhteysprotokolla. Telnet mahdollistaa asiakaskoneen ja palvelimen välisen merkkipohjaisen kommunikoinnin kuljetuserroksen TCP-protokollan päällä. Palvelinpään telnetd-taustaprosessi (daemon) kuuntelee TCP-porttia 23, johon asiakaspään aloittama yhteys muodostuu. Telnetiä käytetään yleensä etäyhteyden muodostamiseen palvelinpään käyttöjärjestelmän komentoliittymään (CLI). Telnetin asiakaspään ohjelma löytyy lähes kaikista tietokonealustoista. Telnet ei ole turvallinen protokolla, koska se ei salaa etäyhteyden läpi kulkevaa dataa.

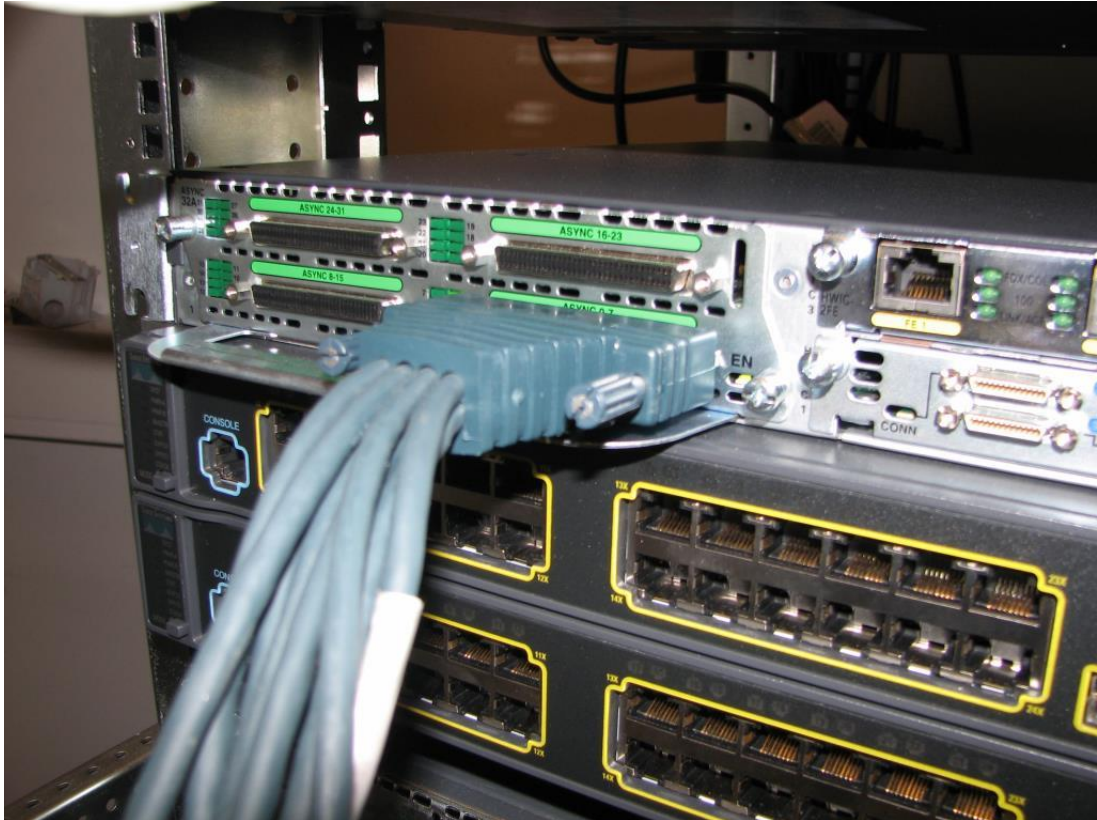
Data on kaapattavissa esimerkiksi verkkolaitteen kautta, joka sijaitsee Telnet-asiakaskoneen ja -palvelimen välissä. Kaapattu data voidaan lukea pakettianalysointilaitteilla, esimerkiksi WireSharkilla. Tästä syystä telnetiä ei juurikaan käytetä enää pääteyhteyksiin tuotantoverkoissa. Laboratorioympäristössä sen käyttö ei ole kuitenkaan vaarallista. (25.)

Reverse telnet on yksi tapa käyttää telnet protokollaa. Siinä palvelinpään laitteen komentoliittymään ei muodosteta yhteyttä vaan laite siirtää yhteyden eteenpäin päätelaiteliitäntään (DTE). Palvelinpään laite toimii siis niin sanottuna terminaali- tai konsoli palvelimena. (26; 27.)

Toteutin Juniversen SRX240-laitteisiin reverse telnet -yhteydet käyttäen Cisco 2811 Integrated Services -reititintä. Reverse telnet mahdollistaa konsoliyhteyksien muodostamisen SRX240-laitteisiin telnetin kautta koulun IP-laboratorioiden tietokoneilta. Näin käyttämättömät Juniperin laitteet saadaan tarvittaessa vaikka laboratorioharjoituskäyttöön. Konsoliyhteyksistä on hyötyä myös Juniversen kehittäjille ja ylläpitäjille. Jos laitteisiin menetetään etäyhteydet esimerkiksi konfigurointivirheen takia, virhettä ei tarvitse lähteä korjaamaan palvelinhuoneeseen vaan se voidaan tehdä laboratorioiden tietokoneilta.

Cisco 2811 -reitittimeen asennettiin 32-porttinen asynkroninen verkkomoduli Cisco NM-32A. Moduuli mahdollistaa laitteen toimimisen terminaali palvelimena useille konsoliyhteyksille SRX240-laitteeseen. Moduulissa on neljä 68-pinnistä porttia, joista jokainen tarjoaa kahdeksan päätelaiteliitäntää eli DTE-liitäntää (Data Terminal Equipment) asynkroniseen sarjaliikenteeseen. Cisco on tehnyt moduulin asennuksen helpoksi. Asennus sujui plug-and-play-tyylisesti. Lopuksi vain ruuvit kiristämällä moduuli oli käyttövalmis. (28, s. 6–8.)

EIA232 on Electronic Industries Associationin määrittelemä standardijoukko dataviestintään. DTE on määritelty EIA232-standardeissa sarjaliikennelinjojen toiseksi pääksi. Toinen pää tulisi olla verkkopääte eli DCE (Data Communication Equipment). SRX240-laitteiden konsoliportit ovat DTE-liitäntöjä. Jotta kahden DTE-liitäntän keskinäinen signaalointi voisi toimia, liitäntöjen lähetys ja vastaanottopinnit täytyy kytkeä ristiin. Tämän toteuttaa niin kutsuttu nollamodeemikaapeli. (29, s. 1; 30.)



Kuva 7. Cisco 2811 -reititin palvelinhuoneessa.

Cisco NM-32A verkkomoduulin porttiin kytkettiin CAB-OCTAL-ASYNC-kaapeli, joka haarautuu kahdeksaksi nollamodeemikaapeliksi, joissa on RJ45-tyyppiset liittimet. RJ45-liittimet sopivat suoraan SRX240-laitteiden konsoliporteihin, joten yksi CAB-OCTAL-ASYNC riittää kahdeksalle SRX-laitteelle. Cisco 2811 -reititin kytkettiin lopulta Cisco Catalyst 3560 -kytkimeen, joka pystyy myös reititykseen. Catalyst 3560 toimii yhdyskäytävänä laboratorioverkkoon. Kuvassa 7, joka on otettu palvelinhuoneesta, näkyy valmiiksi asennettuna Cisco 2811 -reititin, Cisco NM-32A-verkkomoduuli ja CAB-OCTAL-ASYNC-kaapeli. (31, s. 1–4.)

#### Reverse telnetin konfigurointi

Reverse telnetin konfigurointi on yksinkertainen, mutta testasin toiminnan kuitenkin ensiksi koulun IP-laboratoriossa ja konfiguroin laitteen mahdollisimman valmiiksi, ennen laitteen siirtämistä palvelinhuoneeseen Juniversen laitteille varattuun laiteräkkiin ja kytkemistä SRX240-laitteiden konsoliporteihin. Testasin laboratoriossa myös reverse SSH:n toiminnan, mutta päädyttiin siihen, että sen käyttö ei ole tarpeellista, kun laitteisiin ei oteta yhteyttä laboratorioiden ulkopuolelta. Reverse SSH ei myöskään suostunut

toimimaan ilman todennusta (autentikointia). SRX-laitessa on jo oma todennus, joten kaksinkertainen todennus koettiin turhaksi. Ohjaajalta sain IP-osoitteet joita sai käyttää loopback- ja fastethernet -liittymiin (interface).

Cisco 2811:n peruskonfiguraatioiden, kuten hostnimen, bannerin ja enable-salasanan jälkeen loin loopback-liittymän ja asetin sille IP-osoitteen.

```
Termserver(config)#interface Loopback0
Termserver(config-if)#ip address X.X.X.X 255.255.255.0
```

IOS käyttää kahdenlaisia rotaatiolukuja yhteyden muodostamiseen DTE-liittymiin: rotaatioryhmät ja rotaatiolinjat. Jokaista DTE-linjaa vastaa yksi linjarotaatio. Linjarotaatioluvut alkavat TCP-portista 2000. Reverse telnet yhteys muodostetaan siis porttiin 2000 + linjan numero. Terminaalilinjojen numerot vaihtelevat laitteistokohtaisesti, joten tarkistin luvut show line -komennolla. Komento näyttää laitteen kaikki mahdolliset terminaalilinjat, joita on neljää eri tyyppiä: konsoli (CTY), auxiliary (AUX), asynkroninen (TTY) ja virtuaalinen (VTY). Seuraavalla sivulla komennon tulostus kokonaisuudessaan. (32.)

```

Termserver#show line
Tty Line Typ Tx/Rx A Modem Roty Acco AccI Uses Noise Overruns Int
  0      0 CTY      - - - - - - 0      3 0/1322 -
  1      1 AUX 9600/9600 - - - - - - 0      0 0/0 -
1/0     66 TTY 9600/9600 - - - - - - 0      2 0/0 -
1/1     67 TTY 9600/9600 - - - - - - 0      2 0/0 -
1/2     68 TTY 9600/9600 - - - - - - 0      2 0/0 -
1/3     69 TTY 9600/9600 - - - - - - 0      2 0/0 -
1/4     70 TTY 9600/9600 - - - - - - 0      2 0/0 -
1/5     71 TTY 9600/9600 - - - - - - 0      2 0/0 -
1/6     72 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/7     73 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/8     74 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/9     75 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/10    76 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/11    77 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/12    78 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/13    79 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/14    80 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/15    81 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/16    82 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/17    83 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/18    84 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/19    85 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/20    86 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/21    87 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/22    88 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/23    89 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/24    90 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/25    91 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/26    92 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/27    93 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/28    94 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/29    95 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/30    96 TTY 9600/9600 - - - - - - 0      0 0/0 -
1/31    97 TTY 9600/9600 - - - - - - 0      0 0/0 -
* 514   514 VTY      - - - - - - 12     0 0/0 -
  515   515 VTY      - - - - - - 1      0 0/0 -
  516   516 VTY      - - - - - - 0      0 0/0 -
  517   517 VTY      - - - - - - 0      0 0/0 -
  518   518 VTY      - - - - - - 0      0 0/0 -

```

Line(s) not in async mode -or- with no hardware support:  
2-65, 98-513

Kuva 8. Show line -komennon tulostus.

Kuvasta 8 nähdään, että DTE-linjanumerot ovat väliltä 66–97. Näin ollen vastaavat TCP-portit ovat väliltä 2066–2097. Eli kaikenkaikkiaan 32 DTE-liitäntää, niin kuin pitääkin. Tulostuksesta nähdään myös muun muassa vastaavat TTY-luvut 1/0–1/31, lähetys- (Tx) ja vastaanottonopeudet (Rx) ja linjan käyttökerrat (Uses). \*-merkitetyt linjat ovat tällä hetkellä käytössä. Seuraavaksi konfiguroin DTE-linjat.

```

Termserver(config)#line 66 97
Termserver(config-line)#transport input telnet
Termserver(config-line)#session-timeout 60
Termserver(config-line)#absolute-timeout 300
Termserver(config-line)#no exec

```

Komento transport input-telnet varmistaa, että linjalle saa vain telnet-yhteyden. Session-timeout katkaisee yhteyden, jos se on käyttämättä 60 minuuttia. Absolute-timeout katkaisee yhteyden joka tapauksessa 300 minuutin päästä yhteyden avaamisesta. No-

exec varmistaa, ettei linjalle pääse laitteesta ei-toivottuja Exec-prosesseja estämään linjan käyttöä. Exec-prosessi vastaa TTY-linjojen kommunikoinnista. (33; 34.)

Terminaalipalvelin toimisi jo nyt, mutta asetin vielä ip host -komennolla jokaisen SRX-laitteen vastaaviin TCP-portteihin. Lisäksi asettamiseen tarvitaan aiemmin konfiguroitu loopback-osoite, koska se on virtuaalinen ja aina varmasti toiminnassa toisin kuin esimerkiksi FastEthernet. (33.)

```
Termserver(config)#ip host SRX1 2066 <loopback IP>
Termserver(config)#ip host SRX2 2067 <loopback IP>
Termserver(config)#ip host SRX3 2068 <loopback IP>
Termserver(config)#ip host SRX4 2069 <loopback IP>
Termserver(config)#ip host SRX5 2070 <loopback IP>
Termserver(config)#ip host SRX6 2071 <loopback IP>
Termserver(config)#ip host SRX7 2072 <loopback IP>
Termserver(config)#ip host SRX8 2073 <loopback IP>
Termserver(config)#ip host SRX9 2074 <loopback IP>
```

SRX9 ei ole vielä käytössä, mutta se saadaan helposti käyttöön toisella CAB-OCTAL-ASYNC-kaapelilla. Laitteita voi siis laittaa enemmänkin eikä konfiguraatioon tarvitse lisätä kuin vastaava ip host -rivi.

Konfiguroin oletusyhdyntäväksi FastEthernet0/0 -liitäntään kytketyn Catalyst 3650 -laitteen ja oletusreititin ulkoverkkoon komennoilla:

```
Termserver(config)#ip default-gateway <ip address>
Termserver(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
```

Tiukensin hieman laitteen tietoturvallisuutta, vaikka laboratorioympäristössä tämä ei niin tärkeää olisikaan. Loin kaksi eri käyttöoikeustasoa olevaa käyttäjää. Komennolla privilege exec level siirsin tietyt komennot pois alemmilta tasoilta. Käyttäjällä ops-clear on muutaman peruskomennon lisäksi oikeus tyhjentää linja komennolla clear line. Tästä voi olla hyötyä, jos terminaalilinja jostain syystä jumittaa, eikä yhteys suostu muulla tavoin katkeamaan. Käyttäjällä admin-metropolia on sen sijaan kaikki komennot käytössään ja oikeus myös konfiguroida laitetta. Tämän jälkeen lisäsin vielä lokaalin AAA-todennuksen kaikkiin muihin paitsi TTY-linjoin. SRX-laitteissa on jo oma todennus, niin kaksinkertainen todennus olisi ollut käyttäjille kiusallista.

Konfiguroin laitteeseen SSH versio 2:n ja laitoin VTY-linjoilla toimimaan vain SSH-yhteydet 60 minuutin aikakatkaisulla. Lopuksi kytin laitteen http-palvelimen väliaikai-

sesti toimintaan, jotta siihen voidaan muodostaa yhteys Cisco Configuration Professional -ohjelmalla (CCP). CCP:ssä käynnistin Configure-välilehdeltä Security/Security Audit -kansioista One-Step lockdownin. Tämä lisää laitteen turvallisuutta tekemällä automaattisesti konfiguraatiomuutoksia, jotka muun muassa poistavat turhia palveluita. Katsoin vielä konfiguraation kertaalleen läpi. Cisco 2811 -laitteen lopullinen konfiguraatio löytyy kokonaisuudessaan liitteestä 1.

Konfiguraation toimivuuden varmistin lopuksi laboratorion tietokoneella käyttäen Putty-pääteohjelmaa. Ensin avasin yhtäaikaiset telnet-yhteydet jokaiseen SRX-laitteeseen. Connection-typeksi valitaan Telnet, osoite-kenttään laitetaan Cisco 2811 -reitittimen FastEthernet 0/0 -liitännän IP-osoite ja portiksi valitaan haluttua SRX:ää vastaava TCP-portti.

### 5.3 Esimerkkiharjoitus

Terminaalipalvelinta voidaan käyttää hyväksi Junos-laboratorioharjoituksissa. Juniversen verkko muodostuu tällä hetkellä yhdeksästä SRX240-laitteesta, jotka voidaan jakaa kolmeen eri podiin. Mielestäni laitteet riittävät näin maksimissaan yhdeksälle opiskelijalle, jotka on jaettu kolmen hengen ryhmiin. Näin jokainen opiskelija voisi konfiguroida Putty-terminaaliohjelmaa käyttäen yhtä laitetta. Tämä ei siis ole optimaalisin oppimiskeino, jos oppilaita on paljon. Juniversen tuoma hyöty olisi erityisesti se, että jokainen opiskelija voisi tehdä harjoituksen omalla ajallaan ja konfiguroida kaikki laitteet yksin. Tämä olisi oppimisen kannalta paljon parempi vaihtoehto, kun laitteita ei ole tämän enempää. Ohjaavan opettajan mukaan verkkoa saatetaan kuitenkin laajentaa tilaamalla siihen lisää SRX-laitteita jos tarve vaatii.

Laboratorioharjoituksissa oppilaille annetaan kuva topologiasta ja kuvan SRX-laitteita vastaavat TCP-portit. Telnet-yhteyden muodostamiseen tulee käyttää Putty-ohjelmaa. Testasin Windowsin komentotulkkia (CMD) telnet yhteyden muodostamiseen eikä linja vapautunut, kun CMD:n lopetti. Terminaalipalvelinta hyödynnettäessä opettajilla tulisi olla ainakin aiemmin mainitut ops-clear-käyttäjätunnukset, jotta he pääsevät tarvittaessa vapauttamaan jumittuneita linjoja clear line -komennolla.

Liitteessä 2 on esimerkkiharjoitus, joka on suunniteltu tähän kolmen laitteen harjoitteluympäristöön. Se voidaan siis tehdä joko Juniverseä käyttäen sitten kun se on valmis tai

terminaalipalvelinta hyödyntäen. Harjoituksessa käydään läpi Junosin käyttöä sekä perusteet Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) ja staattisista reitityskonfiguraatioista. Harjoitteluympäristö mahdollistaisi myös esimerkiksi kytkentään, palomuuriasetuksiin ja VPN:ään liittyvät harjoitustehtävät.

## 6 Graafinen verkkosimulaattori

### 6.1 Ohjelman kuvaus

GNS3 (Graphical Network Simulator version 3) on graafinen verkon simulointiohjelma, jolla voidaan emuloida oikean verkon ja verkkolaitteiden toimintaa virtuaaliympäristössä. GNS3 on ensisijaisesti suunniteltu erilaisten Cisco Systemsin valmistamien laitteiden emulointiin, mutta sillä voidaan emuloida myös muiden valmistajan laitteita. Lisäksi voidaan useilla eri tavoilla emuloida isäntätietokoneita (host). Ohjelma on yleisesti käytössä harjoitteluvälineenä sertifiointikokeisiin valmistautuvilla sekä korkeakouluopiskelijoilla. Monet yritykset saattavat myös käyttää ohjelmaa verkkotopologioiden ja konfiguraatioiden testaamiseen ennen niiden toteuttamista oikeilla laitteilla. (35.)

GNS3:n asentaminen Windows PC:lle on helppoa, eikä vaadi mitään erityistietoja tai -osaamista. Asennusohjelman Windows ja Mac OS X (versiot 10.6 ja 10.7) käyttöjärjestelmiin voi ladata osoitteesta [www.gns3.net/download/](http://www.gns3.net/download/). All-in-one-asennusohjelma sisältää kaiken tarvittavan lisäksi Putty-pääteohjelman, Virtual PC Simulator -ohjelman ja Wireshark-pakettianalysointiohjelman. Lisäohjelmien asentaminen ei ole pakollista itse ohjelman toiminnan kannalta. Jos käyttää Linux Ubuntu, uusin GNS3 löytyy Ubuntu Software Centeristä. Muut Linux-käyttäjät saattavat joutua asentamaan ohjelman lähteistä. (35.)

GNS3:lla voidaan tehdä monimutkaisia topologioita. Toisin kuin useimmat muut reitintsimulaattorit, GNS3:n virtuaalilaitteissa toimii lähes kaikki konfigurointikomennot, jotka toimivat oikeissakin laitteissa. GNS3 pystyy maksimissaan käsittelemään noin tuhat pakettia sekunnissa. Tähän vaikuttaa paljon alustan suoritusteho, jolla GNS3:sta ajetaan. Oikeat verkkolaitteet voivat olla tätä tuhansia kertoja nopeampia, joten GNS3:a ei voida käyttää oikean laitteen korvikkeena. Verkkotopologioihin on kuitenkin mahdollista kytkeä mukaan oikeita fyysisiä laitteita isäntäkoneen verkkokortin kautta. (35.) Tämä voi tulla tarpeeseen erityisesti, jos topologioihin haluaa mukaan monipuolisempia kyt-

kiä. GNS3 ei tue useita kytkimen ominaisuuksia, koska kytkinten sovelluskohtaisten mikroprosessoripiirien (ASIC) emulointi ei ole mahdollista. (36.)

## 6.2 Lisenssiongelmat

GNS3 on avoimen lähdekoodin ohjelma, joka on GNU-hankkeen yleisen lisenssin versio 2 (GPL v2) alaisena (37). Käytännössä tämä tarkoittaa sitä, että ohjelman tai sen lähdekoodin käyttöä, kopioimista, muokkaamista ja jakelua ei ole rajoitettu (38). Ohjelman mukana asennettavat Dynamips, QEMU/PEMU, VirtualBox ja Wireshark kuuluvat saman GPL-lisenssin alaisuuteen (37; 39; 40; 41). Virtual PC Simulator sekä WinPcap kuuluvat BSD-lisenssin (Berkeley Software Distribution) alaisuuteen, joka sisältää pitkälti samat ehdot kuin GPL (42; 43). Puttyn lisenssi vastaa BSD:tä (44). Lisenssit eivät kata kuitenkaan GNS3:n ilmaisuutta (38), mutta tekijät eivät ainakaan toistaiseksi peri ohjelman käytöstä maksua. Itse GNS3-ohjelman tai sen mukana tulevien ohjelmien käytössä opetustarkoitukseen ei siis näyttäisi lisenssien osalta olevan mitään ongelmia.

GNS3 tarvitsee emulointiin kuitenkin Ciscon ja Juniperin käyttöjärjestelmien IOS:n ja Junosin aitoja levykuvia (image). Käyttöjärjestelmät ovat omisteisia ohjelmistoja. Käytännössä tämä tarkoittaa sitä, että ohjelmistojen omistajat ovat rajoittaneet niiden käyttöä. Juniperin loppukäyttäjän lisenssisopimuksen (EULA), erityisesti kohtien

Use Prohibitions. Notwithstanding the foregoing, this license does not permit the Customer to, and Customer agrees that it shall not, alone or through another party:

(g) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (h) use Embedded Software on non-Juniper equipment... (45.)

mukaan Junosin käyttö GNS3:ssa laillisesti on mahdotonta. Vastaavasti Ciscon ohjelmistojen loppukäyttäjän lisenssisopimuksen kohdan

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order"). Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Cisco equipment) for com-

munication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. (46.)

mukaan asiakkaalla ei ole oikeutta käyttää myöskään IOS:ia GNS3:ssa. GNS3:sta ei siis voi käyttää käyttöjärjestelmien aidoilla levykuvilla opetustarkoitukseen ilman että rikkoisi yhtiöiden lisenssisopimuksia.

## 7 Vyatta-käyttöjärjestelmä

### 7.1 Vyatta Network OS

Vyatta-käyttöjärjestelmä tarjoaa hyvin samanlaisen käyttöliittymän kuin Junos (47). Vyatta Network OS, tai lyhyemmin Vyatta, on Vyatta-yhtiön kehittämä käyttöjärjestelmä, jota voidaan käyttää verkkotyöskentelyyn fyysisillä, virtuaalisilla, sekä pilvilaskentaluustoilla. Vyattassa toimivat pitkälti samat ominaisuudet kuin fyysisissä verkkolaitteissa, kuten esimerkiksi IPv6, yleisimmät dynaamiset reititysprotokollat, tilallinen palomuu-ri, VPN-tunnelit ja palvelunlaatupolitiikat. Vyatta-käyttöjärjestelmä ei tarvitse omaa tiettyä laitteistoa kuten Ciscon IOS tai Juniperin Junos, vaan toimii standardeissa x86- ja X64-arkkitehtuureissa. Koska nämä arkkitehtuurit ovat käytössä hyvin monissa kotitietokoneissa ja palvelinkoneissa, Vyatta voidaan käyttää lähes kaikilla tietokonealustoilla. (48.)

Vyattasta löytyy kaksi eri laitosta: avoimen lähdekoodin editio ja tilaajaeditio. Avoimen lähdekoodin editiota tai yhteisöeditiota kutsutaan Vyattan ydinohjelmistoksi (VC). Pääasiassa molemmat editiot ovat samanlaisia. Ydinohjelmistosta tulee uusi versio noin puolen vuoden välein, kun taas tilaajaeditio pyritään pitämään mahdollisimman vakaina jatkuvien päivityksin (49). Tilaajaeditio sisältää ydinohjelmiston ominaisuuksien lisäksi enemmän asiakastukea, kuten täyden teknisen tuen, sekä ilmoitukset uusista ohjelmistopäivityksistä ja bugikorjauksista. Tilaajille on heidän liiketoiminnan varmistamiseksi tarjolla erilaisia tukipaketteja, joihin voidaan määritellä esimerkiksi ympärivuorokautinen puhelintuki tai palvelutasosopimus (SLA). (48.)

Vyatta on testattu toimivaksi VMWare-, RedHat KVM-, Microsoft Hyper-V- ja Citrix Xen/Xenserver -virtuaaliympäristöissä. Vyatta mahdollistaa aiemmin tunnetusti laitteistodonnaisten verkkoelementtien virtualisoinnin. Virtualisoinnilla voidaan merkittävästi

vähentää fyysisten laitteiden määrää, koska jokaista virtuaalikonetta ei tarvitse ajaa omassa laitteessaan. Vyatta pystyy tehokkaasti hyödyntämään moniydinprosessoreita. Virtualisointia voidaan hyödyntää myös datacentereissä ja pilvilaskennassa. Vyatta on mahdollista asentaa Amazonin pilvipalveluun (AWS). AWS:n ytimessä toimii Amazon Machine Image (AMI) virtuaalikonealusta. Vyatta AMI ja levykuva Redhat KVM -virtuaalikoneeseen ovat saatavilla vain tilaajaeditionissa. (50; 51, s. 4–6.)

## 7.2 Vyatta graafisessa verkkosimulaattorissa

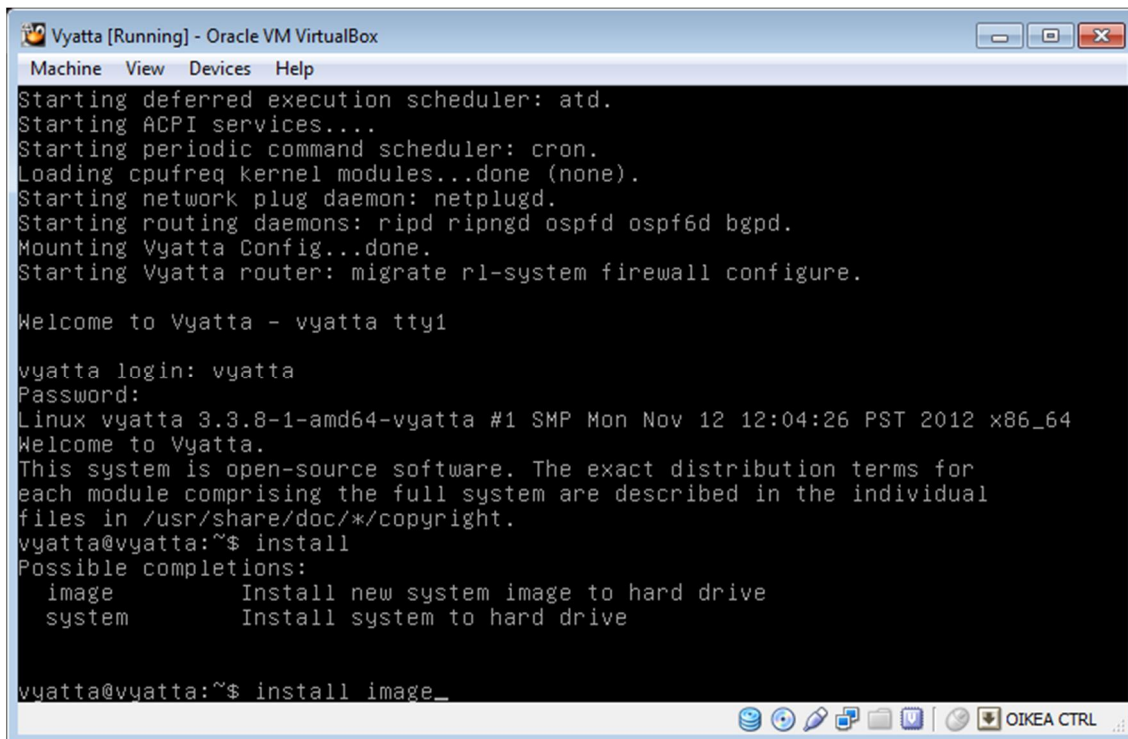
Kaikki Vyattan ydinohjelmiston komponentit kuuluvat avoimen lähdekoodin lisenssin alaisuuteen. Ne ovat joko GNU GPL- tai BSD -lisenssien alaisuudessa. (52.) Tämä tarkoittaa sitä, että Vyatta voidaan käyttää GNS3:ssa laillisesti. Asensin ja testasin Vyattan toiminnan GNS3:ssa Oraclen VirtualBox -virtuaalikoneella, joka on natiivisti tuettu GNS3:ssa.

Vyattan ydinohjelmiston LiveCD-levykuvat löytyvät osoitteesta [packages.vyatta.com/vyatta/iso/](http://packages.vyatta.com/vyatta/iso/). LiveCD-levykuva käynnistetään virtuaalikoneen CD-asemasta, jonka jälkeen käyttöjärjestelmä asennetaan virtuaalikoneen kovalevyille. Latasin LiveCd:n 64-bittisen version koska testiympäristönä toimiva Windows 7 on myös 64-bittinen. Kävin asettamassa testilaitteen BIOS:sta prosessorin asetuksista laitteistopohjaisen virtualisoinnin päälle, koska tämä tehostaa huomattavasti virtuaalikoneen toimintaa.

Konfiguroin ensiksi VirtualBoxin hallinnasta uuden virtuaalikoneen. Käyttöjärjestelmäksi valitsin Linuxin ja Oraclen 64-bittisen version. Tällä ei sinällään ole merkitystä, koska Vyatta-käyttöjärjestelmä käynnistetään virtuaaliselta CD-levyltä. Muistin määräksi valitsin Vyattan minimisuosituksen eli 512 MB. Seuraavaksi loin uuden VDI-tyyppisen (VirtualBox Disk Image) 2 GB:n virtuaalikoalevyn, joka allokoii fyysistä kovalevytilaa tarpeen mukaan eli dynaamisesti. Koska laite ei tule olemaan todellisessa raskaassa verkkokäytössä, muistia ja levytilaa ei tarvitse enempää. Tämän jälkeen käynnistin virtuaalikoneen ja valitsin käynnistyslevyksi lataamani Vyattan CD-levy kuvan. (53.)

Vyattan käynnistys kesti hetken, jonka jälkeen käyttöjärjestelmä kysyi käyttäjätunnusta ja salasanaa. Molemmat ovat oletuksena vyatta. Tämän jälkeen päädytään Vyattan komentoliittymän (CLI) toiminnalliseen tilaan. Tästä tilasta voidaan käynnistää kuvan 9

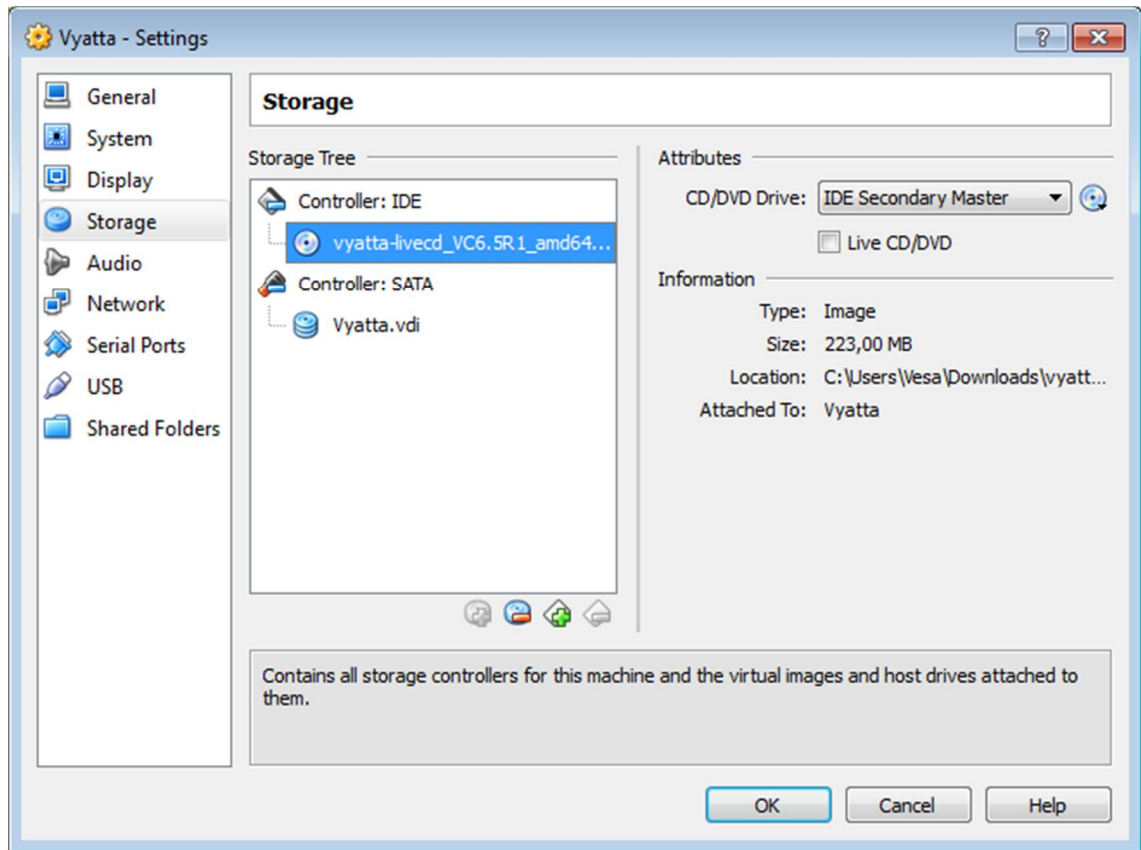
mukaisesti install image -komennolla Vyattan levykuvan asennus virtuaalikoneen kovalevyille. Ohjelma kysyy asennuksen aikana tietoja, joihin normaalikäytössä käy kaikkiin ohjelman antama oletusasetus.

The image shows a terminal window titled "Vyatta [Running] - Oracle VM VirtualBox". The terminal output displays the following text:

```
Starting deferred execution scheduler: atd.  
Starting ACPI services...  
Starting periodic command scheduler: cron.  
Loading cpufreq kernel modules...done (none).  
Starting network plug daemon: netplugd.  
Starting routing daemons: ripd ripngd ospfd ospf6d bgpd.  
Mounting Vyatta Config...done.  
Starting Vyatta router: migrate rl-system firewall configure.  
  
Welcome to Vyatta - vyatta tty1  
  
vyatta login: vyatta  
Password:  
Linux vyatta 3.3.8-1-amd64-vyatta #1 SMP Mon Nov 12 12:04:26 PST 2012 x86_64  
Welcome to Vyatta.  
This system is open-source software. The exact distribution terms for  
each module comprising the full system are described in the individual  
files in /usr/share/doc/*/copyright.  
vyatta@vyatta:~$ install  
Possible completions:  
  image          Install new system image to hard drive  
  system         Install system to hard drive  
  
vyatta@vyatta:~$ install image_
```

Kuva 9. Levykuvan asennus kovalevyille.

Asennuksen jälkeen virtuaalikone voidaan sammuttaa ja CD-levy voidaan käydä poistamassa virtuaalikoneen levyasetuksista kuvassa 10 esitetystä kohdasta. Vyattaa ei tarvitse enää käynnistää CD-levyltä. Tässä vaiheessa virtuaalikonetta voi halutessaan optimoida poistamalla turhia laitteita, kuten levykeaseman ja äänikortin, ja asettamalla näyttömuistin minimiin.



Kuva 10. Vyatta LiveCD:n poistaminen VirtualBoxin asetuksista.

Vyattan käynnistyksessä tulevan virheilmoituksen

```
pi i x4_smbus 0000.00.07.0: SMBus base address uninitialized
- upgrade bios or use force_addr=0xaddr
```

saa poistettua lisäämällä tiedoston blacklist.conf loppuun rivin

```
blacklist i2c_piix4
```

Rivi estää tämän viiallisen moduulin käynnistymisen. Muutos voidaan tehdä Vyattassa esimerkiksi vi-tekstieditorilla seuraavalla komennolla:

```
sudo vi /etc/modprobe.d/blacklist.conf
```

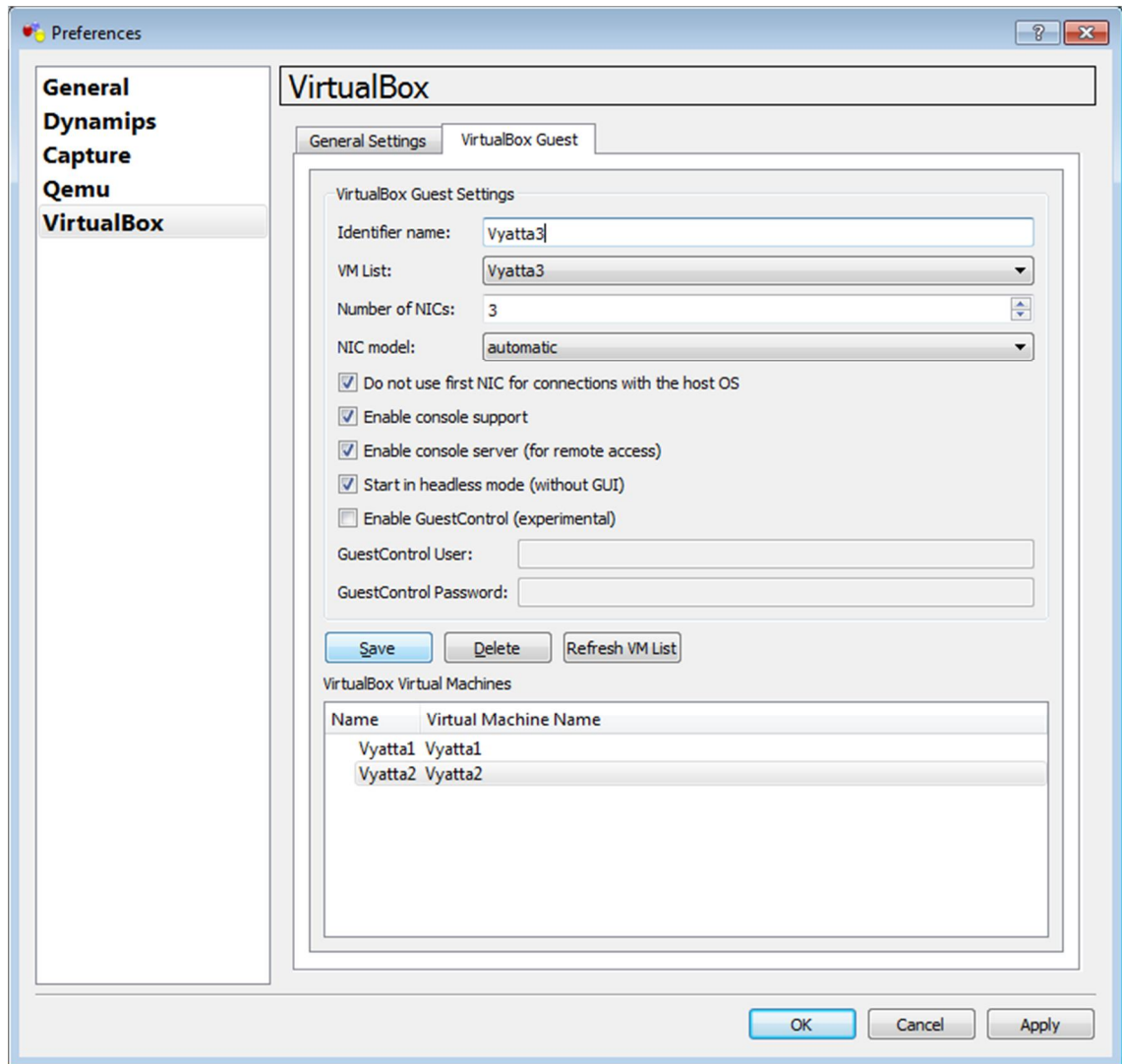
Kun muutos on tehty, se saadaan voimaan päivittämällä kernelin initramfs-arkistot.

```
sudo update-initramfs -u -k all
```

Virheilmoituksen ei pitäisi olla mitenkään haitallinen, mutta se hidastaa käynnistystä ja tulee joka kerta, kun Vyattan käynnistää. (54.)

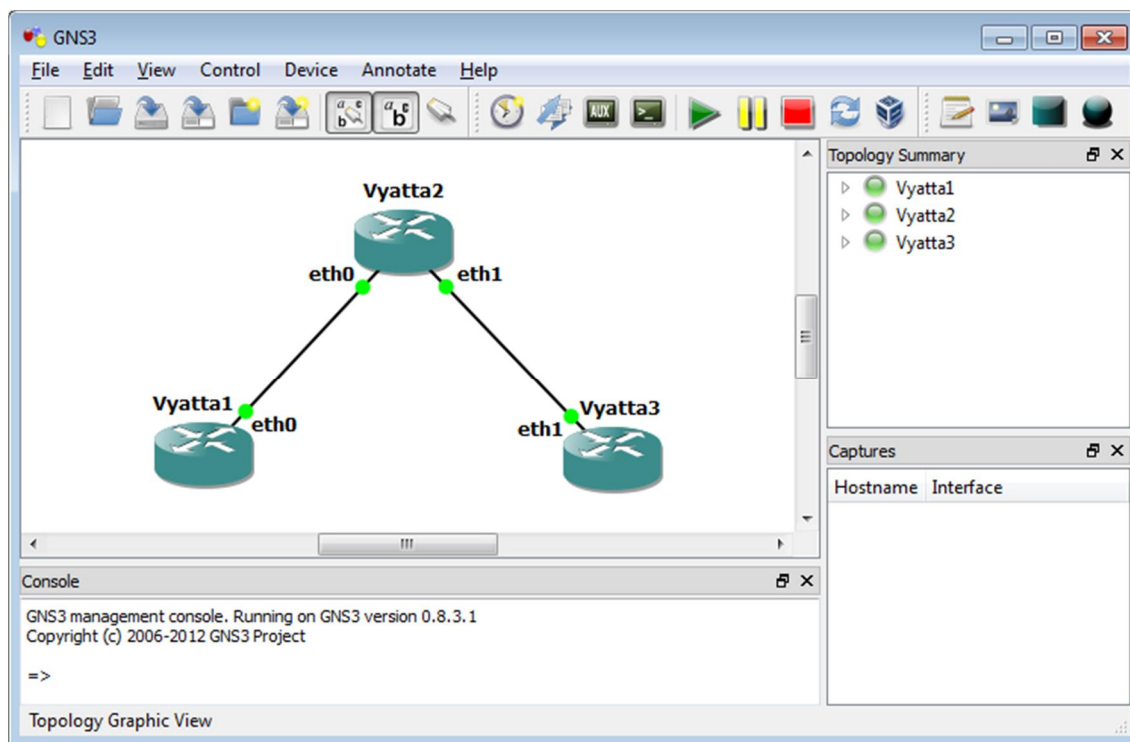
Jotta GNS3:ssa voidaan käyttää useampaa Vyatta-virtuaalikonetta, virtuaalikoneesta on oltava useampi kopio. Tein alkuperäisestä virtuaalikoneesta VirtualBoxin hallinnasta kolme täydellistä kloonia, joita käytetään GNS3:ssa. Täydellinen kloonin tarkoittaa, että kloonin toimii itsenäisesti alkuperäisestä virtuaalikoneesta ja sillä on täysin oma levykuvansa. Kloonattaessa tulee muistaa alustaa jokaisen kloonin verkkosovittimen (NIC) MAC-osoite. MAC-osoite yksilöi laitteen verkossa, joten sama MAC aiheuttaisi pahoja ongelmia verkon toiminnassa. (55.)

Seuraavaksi konfiguroin VirtualBoxin-asetukset GNS3:ssa kuvan 11 mukaisesti. Jokaisesta Vyatta-kloonista kohden tulee luoda GNS3:n asetuksissa VirtualBox Guest. Nimeksi ne samannimisiksi kuin itse virtuaalikoneet ja laitoin jokaiseen kolme NIC:ää. Asetuksista on mahdollista varata ensimmäinen NIC isäntäkoneen käyttöön. Topologia muodostuu tässä tapauksessa kuitenkin vain virtuaalikoneista, joten tätä ei tarvitse tehdä. Asetuksista pitää muistaa kytkeä konsolituki ja -palvelin toimintaan, jotta GNS3 pystyy ottamaan laitteeseen konsoliyhteyden Putty-ohjelmalla. Vyattan GUI:a ei käytetä, joten sen voi myös kytkeä pois (Start in headless mode). (55.)



Kuva 11. VirtualBox asetukset GNS3:ssa.

Lisäsin Vyattan VirtualBox Guesteille oman reititinsymbolinsa ennen topologian luomista. Normaalisti Guest-kuvake on oletuksena pöytäkoneen mallinen. Tämä on täysin kosmeettinen muutos, mutta esimerkiksi harjoitustehtävissä voi olla tarpeen topologian selkeyden vuoksi, jos topologiaan lisätään muitakin laitteita, kuten isäntäkoneita (host). Tein kuvan 12 mukaisen yksinkertaisen kolmen laitteen topologian, käynnistin laitteet ja avasin jokaiseen konsoliyhteydet.



Kuva 12. Testitopologia GNS3:ssa.

Kun tarkistin liitännät Vyattan CLI:ssä komennolla `show interfaces`, huomasin että liitännöiden numerointi alkaa 0:sta toisin kuin topologiassa, jossa ne alkavat 1:stä. Liitännöiden nimet saa kuitenkin helposti korjattua vastaamaan oikeita. Kuvassa 12 korjaus on jo tehty. Tämä on myös otettava huomioon, jos GNS3:een aletaan suunnitella harjoitustehtäviä.

VirtualBox-virtuaalikoneet käyttävät keskinäisiin yhteyksiin UDP-tunnelointia. UDP-tunnelissa on kolme parametria: kohteen IP-osoite, lähde UDP-portti ja kohde UDP-portti. Nämä GNS3 osaa yleensä automaattisesti määrittellä virtuaalikoneiden liitännöiden verkkosovittimiin kun laitteet käynnistetään. Määritykset näkyvät VirtualBoxin hallinnassa verkkoasetuksista. Jos kytkennöissä tehdään muutoksia, parametrien pitäisi muuttua muutosten mukaisesti. Koska testitopologian kaikki laitteet ovat samassa isäntäkoneessa, käytetään UDP-tunneloinnissa localhost IP-osoitetta 127.0.0.1. Jos yhteydet eivät jostain syystä toimi on syytä tarkistaa VirtualBoxin hallinnasta UDP-tunneloinnin parametrien vastaavuus. Laitteen liitännän lähde UDP-portin tulee vastata toisessa päässä olevan laitteen liitännän kohde UDP-porttia ja päinvastoin. (56.)

Vyattan konfigurointitilaan päästään komennolla `configure`. Laitoin isännänimet (hostname) topologian mukaisesti jokaiselle laitteelle seuraavalla komennolla:

```
vyatta@vyatta# set system host-name <hostname>
```

```
vyatta@vyatta:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L  Description
-----
eth0           -               u/u
eth1           -               u/D
eth2           -               u/D
lo             127.0.0.1/8    u/u
              ::1/128
```

Kuva 13. Show interfaces -komennon tulostus.

Isännänimet näkyvät ainoastaan konfigurointitilassa. Toiminnallisessa tilassa `show interfaces` komennolla voi tarkistaa, että liitännät ovat ylhäällä. Kuvassa 13 on Vyatta1:n esimerkkitulostus, josta nähdään, että eth0-liitäntä on toiminnassa niin kuin pitääkin. Vyatta1:n ja Vyatta2:n väliset IP-osoitteet valitsin osoiteavaruudesta 192.168.0.0/24. Vyatta2:n ja Vyatta3:n väliset IP-osoitteet valitsin verkosta 192.168.1.0/24. Seuraavassa ovat vastaavat komennot jokaisella laitteella:

```
vyatta@Vyatta1# set interfaces ethernet eth0 address
192.168.1.1/24
vyatta@Vyatta2# set interfaces ethernet eth0 address
192.168.1.2/24
vyatta@Vyatta2# set interfaces ethernet eth1 address
192.168.3.1/24
vyatta@Vyatta3# set interfaces ethernet eth1 address
192.168.3.2/24
```

Tein seuraavaksi staattiset reitit Vyatta1:een ja Vyatta3:een seuraavasti:

```
vyatta@Vyatta1# set protocols static route 192.168.3.0/24
next-hop 192.168.1.2
vyatta@Vyatta3# set protocols static route 192.168.1.0/24
next-hop 192.168.3.1
```

Lopuksi komennot tulee hyväksyä, kuten Junosissa, `commit`-komennolla. Ping-viestit menivät kaikkiin liitäntöihin läpi jokaisesta laitteesta. Konfiguraatiot tallennetaan konfigurointitilassa virtuaalikoneen kovalevylle komennolla `save`. Jos konfigurointeja ei tal-

lenna, Vyatta palautuu oletuskonfiguraatioon, kun se sammutetaan samaan tapaan kuin fyysisilläkin laitteilla. Oletuskonfiguraation saa palautettua seuraavilla komennoilla:

```
load /opt/vyatta/etc/config.boot.default
save
```

Seuraavassa luvussa tarkastellaan hieman tarkemmin Vyattan komentoja ja sitä miten Juniversen laitteille suunnitellun harjoituksen tekeminen onnistuu.

### 7.3 Vertailua Junosiin ja arviointi

Vyatta ei ole Junos, mutta käyttöjärjestelmissä on paljon yhteisiä piirteitä. Molemmat käyttöjärjestelmät ovat Unix-pohjaisia. Junos pohjautuu FreeBSD:hen ja Vyatta Debian GNU/Linux:iin. Kummassakin käyttöjärjestelmässä toimivat useimmat Unix-komennot. (57.)

Toisin kuin Junosissa, Vyattaan kirjaututaan ensimmäisellä kerralla vyatta-käyttäjänä. Salasana käyttäjälle määritetään käyttöjärjestelmän asennuksen yhteydessä. Vyattan root-käyttäjän saa tosin käyttöön su-komennolla, kun asettaa sille ensin salasanan konfigurointitilassa.

```
[edit]
vyatta@vyatta# set system login user root authentication
plain-text-password
```

Tämä on täysin sama komento, jolla vaihdetaan Junosissa käyttäjän salasana. Tosin Junosissa on lisäksi erillinen root-käyttäjän salasananvaihtokomento. Junosissa konfigurointeja ei pysty aktivoimaan ennen kuin root-käyttäjän salasana on määritelty konfigurointitilassa.

```
[edit]
root# set system root-authentication plain-text-password
```

Junosin root-käyttäjä on ensimmäisellä kerralla Unix shell -tilassa. Toiminnalliseen tilaan pääsee komennolla cli. Toiminnallisen tilan tunnistaa käyttäjänimen edessä olevasta >-merkistä. Vyatta on kirjautumisen jälkeen suoraan toiminnallisessa tilassa, jonka ilmaisee :~\$ -merkit. Peruskomennot, kuten show, set, ping, telnet ja traceroute,

löytyvät molemmista toiminnalliselta tasolta. Vyattassa on hieman enemmän toiminnallisen tason komentoja, kuten kuvasta 14 näkyy. Help-komento avaa Junosissa Junosin käyttöjärjestelmä manuaalin. Manuaalia voi käyttää tarkempien ohjeiden hakemiseen esimerkiksi halutulle komennolle. Vyattassa help-komennolla saa sitä vastoin tietoa käytössä olevista Unix-komennoista. Molemmissa käyttöjärjestelmissä toimii kysymysmerkki ja tabulaattori samaan tapaan.

<pre> root&gt; ? Possible completions: clear configure file help monitor mtrace op ping quit request restart set show ssh start telnet test traceroute root&gt; █ </pre>	<pre> vyatta@vyatta:~\$ Possible completions: add          Add an clear       Clear clone      Clone configure  Enter connect    Establ copy       Copy a delete     Delete disconnect Take d force      Force format     Format generate   Genera install    Instal monitor    Monito ping       Send I poweroff   Powero reboot     Reboot release    Releas rename     Rename renew      Renew reset      Reset restart    Restar set        Set op show       Show s telnet     Telnet traceroute Track update     Update  vyatta@vyatta:~\$ █ </pre>
--	---

Kuva 14. Junosin (vas.) ja Vyattan (oik.) toiminnallisen tason komennot.

Monet show-komennot ovat myös samoja, mutta jotkin löytyvät eri alitasolta. Esimerkiksi reititystaulu saadaan Vyattassa näkyviin komennolla `show ip route`, kun Junosissa vastaava komento on `show route`. `Show configuration` -komento näyttää konfiguraatiot samaan tapaan hierarkkisesti { ja } -merkkien sekä sisennyksien avulla. Jotkin komennot antavat hieman erilaisen tulostuksen. Esimerkiksi Vyattassa komento `show interfaces` listaa lyhyesti kaikki liitännät, kun Junosissa sama komento listaa kaikki liitännät yksityiskohtaisesti.

Molemmissa käyttöjärjestelmissä konfigurointitilaan päästään toiminnallisesta tilasta komennolla `configure`. Kaikki tärkeimmät komennot ovat samoja, kuten `set`, `commit`, `edit` ja `save`, kuten kuvasta 15 näkyy. Tosin pieniä eroja on joissain peruskomennoissa. Esimerkiksi Vyattan yksittäinen komento `commit-confirm` on Junosissa jaettu kahteen osaan. Commit-komennon perään laitetaan Junosissa lisänä `confirmed` eli `commit confirmed`. Toiminnallisen tilan komentoja ajetaan molemmissa käyttöjärjestelmissä samaan tapaan run-komennolla.

<pre> root# ? Possible completions: &lt;[Enter]&gt; activate annotate commit copy deactivate delete edit exit extension help insert load prompt protect quit rename replace rollback run save set show status top unprotect up wildcard [edit] root# █ </pre>	<pre> vyatta@vyatta# Possible completions: confirm      Confir comment      Add co commit       Commit commit-confirm               Commit compare      Compar copy         Copy a delete       Delete discard      Discar edit         Edit a exit         Exit f load         Load c loadkey      Load u merge Load  Load configura rename       Rename rollback     Rollba run          Run ar save         Save c set          Set th show         Show t  [edit] vyatta@vyatta# █ </pre>
---	---

Kuva 15. Junosin (vas.) ja Vyattan (oik.) konfiguraatiotason komennot.

Molempien käyttöjärjestelmien CLI:t näyttävät konfigurointitilassa täysin samalta sen jälkeen kun isäntänimi on vaihdettu. Tämä tapahtuu kummassakin host-name-komennolla.

```
set system host-name <hostname>
```

Komennon aktivoimisen jälkeen commit-komennolla kummankin CLI on konfigurointitilassa username@hostname#. Vyattassa hostname-vaihto päivittyy tosin vasta, kun käyty ensin toiminnallisessa tilassa ja palattu sitten takaisin konfigurointitilaan. Vyattassa ei ole konfiguraation tarkistuskomentoa commit check, kuten Junosissa. Molemmissa rollback toimii kuitenkin samaan tapaan.

Seuraavaksi selvitetään eroja, joita tulee vastaan, kun Vyattalla tekee liitteenä 2 olevan harjoitustehtävän. Kohdassa 10 asetettiin IP-osoitteet kaikkiin liitäntöihin. Vyattassa liitäntöjen asettaminen on hyvin erilaista, mutta myös yksinkertaisempaa kuin Junosissa. Sanojen Set interfaces jälkeen asettaminen muuttuu. Loopback-osoite laitetaan myös eri tavalla. Vyattassa loopbackissa on lisäksi valmiina localhost osoite 127.0.0.1.

```
set interfaces ethernet <interface> address <ip-addr/mask>
set interfaces loopback lo address <ip-address/mask>
```

Harjoituksen kohdan 11 OSPF-konfigurointi on myös hieman erilaista Vyattassa. Junosissa verkot liitetään OSPF-alueeseen liitäntäkohtaisesti, mutta Vyattassa se tehdään kuten Ciscon IOS:ssa verkkokohtaisesti. Komento on Junosissa ja Vyattassa sama 'set protocols ospf area <area>' kohtaan asti. Passiivinen liitäntä on Vyattassa lyhyempi kirjoittaa:

```
set protocols ospf area <area> network <ip-address/mask>
set protocols ospf passive-interface <interface>
```

Kohdan 12 staattisten reittien konfigurointi on lähes samanlaista. Ainoa ero on, että Junosissa komento sijaitsee routing-optionsin alla, kun Vyattassa se on protocolsin alla. Paketin pudotuskomento on Vyattassa blackhole Junosin discardin sijaan.

```
set protocols static route <ip-address/mask> next-hop
<ip-address>
set protocols static route 0.0.0.0/0 blackhole
```



Liitteessä 2 olevan harjoituksen tekeminen sujui Vyattalla ilman ongelmia. Kuvassa 16 on SRX2:n reititystaulu konfiguroinnin jälkeen. Vyattan CLI:llä on monia yhtäläisyyksiä Junosin kanssa. Eroa on kuitenkin sen verran, että itse Junosin harjoitteluun sitä ei voi varsinaisesti suositella. Jotkin asiat, kuten BGP:n konfigurointi, eroavat merkittävästi Junosin vastaavasta. Vyatta on kuitenkin itsessään intuitiivinen ja vaikuttaa erittäin hyvin toteutetulta käyttöjärjestelmältä. Koin Vyattan käyttämisen miellyttävänä, ja mielestäni se yhdistää useita Junosin ja IOSin hyviä puolia.

```
vyatta@SRX2# run sho ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/0] via 172.16.2.1 (recursive via 80.195.200.226), 00:38:25
O  10.1.1.0/30 [110/10] is directly connected, eth0, 03:51:58
C>* 10.1.1.0/30 is directly connected, eth0
O>* 10.1.20.1/32 [110/20] via 10.1.1.1, eth0, 03:51:40
C>* 80.195.200.224/30 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
O  172.16.1.1/32 [110/10] is directly connected, lo, 03:51:58
C>* 172.16.1.1/32 is directly connected, lo
S>* 172.16.2.1/32 [1/0] via 80.195.200.226, eth1
[edit]
vyatta@SRX2#
```

Kuva 16. Show ip route -komennon tulostus SRX2 reitittimessä liitteen 2 harjoituksen jälkeen.

GNS3 mahdollistaa hyvin laajojen virtuaaliverkkojen tekemisen täysin ilmaiseksi. Ainoastaan tietokoneen prosessorin tehokkuus ja muistin määrä ovat rajana. Vyatta ei ole mitenkään erityisen raskas ajaa. Esimerkkiharjoituksen kolme Vyatta VirtualBox-virtuaalikonetta käynnistyi yhtä aikaa nopeasti ja toimi hyvin vaikka testikoneena käytin yli kaksi vuotta vanhaa netbookia. Netbookissani on Intel Core i3, 1,33 GHz:n tuplaydin prosessori, joka tukee virtualisointia, sekä 2 gigatavua keskusmuistia. Käyttöjärjestelmänä on 64-bittinen Windows 7. Tavallisella nykyaikaisella pöytätietokoneella GNS3:n topologioihin olisi todennäköisesti mahdollista liittää kymmeniä Vyatta-koneita ja suorittaa niissä hyvin monimutkaisia konfiguraatioita.

## 8 Yhteenveto

Insinööriyössä selvitettiin Junosphere-pilvipalvelun, Cisco terminaalipalvelimen ja GNS3 verkkosimulaattorin käyttöönottoa ja soveltuvuutta Junos-käyttöjärjestelmän käytön opetteluun. Lisäksi tutkittiin Vyatta-käyttöjärjestelmän käyttöä GNS3:ssa ja eroja Junosiin. Metropolia Ammattikorkeakoulu voi hyödyntää tutkimuksen tuloksia Junos-opintojaksojen, Junos-harjoitusten ja muiden Juniperin laitteita hyödyntävien opintojaksojen suunnittelussa ja toteutuksessa. Lisäksi esimerkiksi opiskelijat voivat hyödyntää GNS3 verkkosimulaattorista ja Vyatta-käyttöjärjestelmästä saatuja tietoja itsenäiseen opiskeluun.

Juniper Networksin tarjoama Junosphere-pilvipalvelu sopisi ominaisuuksiensa puolesta erinomaisesti Junos-harjoitteluun. Käytössä olevien virtuaalikoneiden toiminta vastaa Juniperin aitojen J-sarjan, SRX-sarjan ja PTX-sarjan laitteiden toimintaa ja ne tukevat samoja Junosin ominaisuuksia. Junospheren käyttöliittymä näyttää intuitiiviselta ja harjoitusverkon suunnittelu sen topologiavelholla vaikuttaisi helpolta. Junospheren käyttöoikeusasetuksilla pystytään estämään palvelun luvaton käyttö ja maksettujen virtuaalikonepäivien tuhlaaminen. Harjoitusten ohjaajan ja oppilaiden oikeudet saadaan selkeästi erotettua. Harjoitusverkon laajuus riippuu siitä, kuinka paljon rahaa virtuaalikoneisiin ollaan valmiita satsaamaan. Palvelun hinta on todennäköisesti suurin este sen käyttöönotossa. Yksi virtuaalikone maksaa viisi dollaria vuorokautta kohden ja hintaan lisätään verot.

Arviot Junospheren soveltuvuudesta Junos-harjoitteluun perustuvat palvelun käyttöoppaista, verkkolähteistä ja käyttövideoista tehtyihin johtopäätöksiin. Kokeellinen tutkimus jäi tämän opinnäytetyön ulkopuolelle. Soveltuvuutta voisi tutkia lisää esimerkiksi ostamalla halvimman eli kymmenen virtuaalikoneen-paketin kokeiluun muutamaksi päiväksi. Näin saataisiin selville esimerkiksi palvelun vakaus ja se, millaiset vasteajat sen web-pohjaisessa käyttöliittymässä on.

Terminaalipalvelin tai Juniverse-varausjärjestelmä mahdollistivat insinööriyön tekemishetkellä vain yksinkertaiset kolmen laitteen harjoitustehtävät (ks. liite 2). Juniverse mahdollistaisi harjoitusten tekemisen etänä, mutta ohjelma ei ole vielä valmis. Ohjelman kehitys on harjoittelijaopiskelijoiden vastuulla, eikä aikataulusta ollut insinööriyötä tehdessä vielä tietoa. Tästä syystä konfiguroitiin terminaalipalvelimen, jolla Juniversen laitteet on mahdollista ottaa harjoituskäyttöön koulun laboratorioluokkien tietokoneilta

telnet-yhteyttä käyttäen. Järjestely soveltuu hyvin Junosin harjoitteluun, mutta laitteita on toistaiseksi vain yhdeksän, joten ne eivät riitä isoille oppilasryhmille.

Avoimen lähdekoodin GNS3-verkkosimulaattoriin voidaan rakentaa laajoja ja kompleksia verkkoja virtualisoiduilla verkkolaitteilla. Verkon laajuudessa tulee vastaan ainoastaan tietokoneen prosessorin ominaisuudet ja muistin määrä. Ohjelman käyttö on ilmaista. GNS3:n virtuaalikoneissa ei kuitenkaan lisenssioikeudellisista syistä voi käyttää Junosin levykuvia. Vyatta-nimisen avoimen lähdekoodin käyttöjärjestelmän käyttöliittymä muistuttaa Junosia ja sen käyttö GNS3:ssa on laillista. Vyatta toimii hyvin GNS3:ssa, mutta kokeellisessa tutkimuksessa selvisi, että käyttöliittymässä on muutamia merkittäviä eroja Junosiin, joten varsinaiseen Junos-harjoitteluun sitä ei voi varaketta suositella. GNS3:n ja Vyattan toimintaa voisi tutkia lisää käyttämällä nykyaikaisempaa tietokonealustaa ja tekemällä monimutkaisempia topologioita ja konfiguraatioita. Näin saataisiin selville muun muassa tarkempaa tietoa Vyattan tehovaatimuksista ja yhteensopivuudesta VirtualBoxin kanssa. Samalla selviäisi tarkemmin erot Junosiin.

Tutkimustyön tekeminen oli mielenkiintoista ja mielekästä sen monipuolisuuden vuoksi. Tutkimuksessa pääsi tiedonhaun lisäksi käytännössä asentamaan ja konfiguroimaan niin fyysisiä kuin virtuaalisiakin verkkolaitteita.

## Lähteet

- 1 Juniper Networks. 2013. Verkkodokumentti. Answers Corporation. <[www.answers.com/topic/juniper-networks-inc](http://www.answers.com/topic/juniper-networks-inc)>. Luettu 20.2.2013.
- 2 Uusitalo, Marko. 2013. Lehtori. Metropolia Ammattikorkeakoulu. Helsinki. Tutustuminen Bulevardin toimipisteen Junos-opetukseen. 11.3.2013.
- 3 Opintojakso TT00AC17 Junos-perusteet. 2012. Verkkodokumentti. Metropolia Opinto-opas. <<http://opiskelijanopas-ops.metropolia.fi/index.php?koala=2&lang=fi&type=N&ko=2061&ops=TT13S1H&sm=39914&studyElement=29957>>. Luettu 12.3.2013.
- 4 Company Profile. 2011. PDF-tiedosto. Juniper Networks. <[www.juniper.net/us/en/local/pdf/fact-sheets-backgrounder/3000054-en.pdf](http://www.juniper.net/us/en/local/pdf/fact-sheets-backgrounder/3000054-en.pdf)>. Luettu 20.2.2013
- 5 Goralski, Walter; Gadecki, Cathy; Bushong, Michael. 2011. Junos OS for dummies, 2nd Edition. John Wiley & Sons, Inc., Hoboken, New Jersey
- 6 Gadecki, Cathy; Scruggs, Michael. 2011. PDF-tiedosto. Day One: Exploring the Junos CLI. Juniper Networks Books.
- 7 Garrett, Aviva. 2006. JUNOS Cookbook. O'Reilly Media.
- 8 Getting Started with Juniper Networks. 2010. Kuva. Juniper Learning Portal. Juniper Networks. <<https://learningportal.juniper.net/>>. Luettu 16.3.2013
- 9 Juniper Networks learning paths. 2012. PDF-tiedosto. Juniper Networks. <<http://www.juniper.net/us/en/training/certification/certification-paths-by-credential.pdf>>. Luettu 16.3.2013.
- 10 Juniper Networks Academic Alliance -esite. 2012. PDF-tiedosto. Juniper Networks. <<http://www.juniper.net/us/en/local/pdf/fact-sheets-backgrounder/3000052-en.pdf>>. Luettu 17.3.2013.
- 11 Junosphere datasheet. 2013. PDF-tiedosto. Juniper Networks. <<http://www.juniper.net/us/en/local/pdf/datasheets/1000376-en.pdf>>. Luettu 20.3.2013
- 12 Cloud computing. 2013. Verkkodokumentti. Wikipedia. <[http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing)>. Luettu 20.3.2013.

- 13 Guide for Bank Administrators. PDF-tiedosto. 2013. Juniper Networks. <[http://www.juniper.net/techpubs/software/junosphere/junosphere2.0/junosphere\\_bank\\_admin.pdf](http://www.juniper.net/techpubs/software/junosphere/junosphere2.0/junosphere_bank_admin.pdf)>. Luettu 22.3.2013.
- 14 Junosphere Guide for Users. 2013. PDF-tiedosto. Juniper Networks. <[http://www.juniper.net/techpubs/software/junosphere/junosphere2.0/junosphere\\_user.pdf](http://www.juniper.net/techpubs/software/junosphere/junosphere2.0/junosphere_user.pdf)>. Luettu 26.3.2013.
- 15 Virtual Networking Reality -blogi. 2012. Kuva. <<http://forums.juniper.net/t5/Virtual-Networking-Reality/Has-it-Been-A-While-Check-out-the-New-Junosphere-Features/ba-p/156568>>.
- 16 Junosphere Network Topology Guide. 2013. PDF-tiedosto. Juniper Networks. <[http://www.juniper.net/techpubs/software/junosphere/junosphere2.0/junosphere\\_topology\\_guide.pdf](http://www.juniper.net/techpubs/software/junosphere/junosphere2.0/junosphere_topology_guide.pdf)>. Luettu 26.3.2013.
- 17 Jncp quarterly update. Marraskuu 2012. PDF-tiedosto. Juniper Networks, Inc. <[http://forums.juniper.net/jnet/attachments/jnet/Training\\_and\\_Certification/3706/1/JNCP%20Nov%2013%202012%20Webcast.pdf](http://forums.juniper.net/jnet/attachments/jnet/Training_and_Certification/3706/1/JNCP%20Nov%2013%202012%20Webcast.pdf)>. Luettu 3.4.2013.
- 18 Junosphere Release Notes. 2013. PDF-tiedosto. Juniper Networks. <<http://www.juniper.net/techpubs/software/junosphere/junosphere2.0/junosphere-release-notes-2-7.pdf>>. Helmikuu 2013. Luettu 3.4.2013.
- 19 What are the components of Junosphere?. 2013. Verkkodokumentti. Juniper Networks. <[http://www.juniper.net/techpubs/en\\_US/junosphere2.0/topics/concept/junosphere-faq-components.html](http://www.juniper.net/techpubs/en_US/junosphere2.0/topics/concept/junosphere-faq-components.html)>. 9.2.2013. Luettu 3.4.2013.
- 20 Junosphere Ordering. 2013. Verkkodokumentti. Juniper Networks. <<http://www.juniper.net/us/en/products-services/software/junosphere-platform/junosphere/#ordering>>. Luettu 3.4.2013.
- 21 Juniper Networks unveils Junosphere Classroom. 2011. Verkkodokumentti. CCIETalk. <<http://www.ccietalk.com/2011/05/18/juniper-networks-unveils-junosphere-classroom>>. 18.3.2011. Luettu 5.4.2013.
- 22 Juniverse Developer Information -esite. 2012. Luovuttaja Rahkonen Heikki, Projekti-insinööri. Metropolia. 22.11.2012.
- 23 Juniverse topologiakuva. 2013. Luovuttaja Bruk Yirdaw, Laboratorioinsinööri. Metropolia. 19.4.2013.
- 24 Secure Shell. 2013. Verkkodokumentti. Wikipedia. <[http://en.wikipedia.org/wiki/Secure\\_Shell](http://en.wikipedia.org/wiki/Secure_Shell)>. 17.4.2013. Luettu 7.4.2013.

- 25 Telnet. 2013. Verkkodokumentti. Wikipedia. <<http://en.wikipedia.org/wiki/Telnet>>. 26.3.2013. Luettu 9.4.2013.
- 26 Reverse Telnet. 2013. Verkkodokumentti. Wikipedia. <[http://en.wikipedia.org/wiki/Reverse\\_telnet](http://en.wikipedia.org/wiki/Reverse_telnet)>. 1.2.2013. Luettu 9.4.2013.
- 27 Pätynen, Erik. Lehtori. 2013. Tietotekniikka, Metropolia Ammattikorkeakoulu, Espoo. Keskustelu lopputyöaiheesta. 20.3.2013.
- 28 Serial Connectivity Network Modules. 2003. PDF-tiedosto. Cisco Systems. <[http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/seral\\_ds.pdf](http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/seral_ds.pdf)>. Luettu 12.4.2013.
- 29 Interface Circuits for TIA/EIA-232-F. 2002. PDF-tiedosto. Texas Instruments. <<http://www.ti.com/lit/an/slla037a/slla037a.pdf>>. Luettu 12.4.2013.
- 30 Null Modem. 2013. Verkkodokumentti. Wikipedia. <[http://en.wikipedia.org/wiki/Null\\_modem](http://en.wikipedia.org/wiki/Null_modem)>. 22.4.2013. Luettu 12.4.2013.
- 31 CAB-OCTAL-ASYNC Cable Pinouts. 2005. PDF-tiedosto. Cisco Systems. <<http://www.cisco.com/image/gif/paws/14958/24.pdf>>. 9.9.2005. Luettu 12.4.2013.
- 32 Understanding reverse telnet and IOS terminal lines. 2004. Verkkodokumentti. Michael J. Martin, Router Expert. <<http://searchnetworking.techtarget.com/tip/Router-Expert-Understanding-reverse-telnet-and-IOSterminal-lines>>. Heinäkuu 2004. Luettu 14.4.2013.
- 33 Configuring a Terminal/Comm Server. 2008. Verkkodokumentti. Cisco Systems. <[http://www.cisco.com/en/US/tech/tk801/tk36/technologies\\_configuration\\_example09186a008014f8e7.shtml](http://www.cisco.com/en/US/tech/tk801/tk36/technologies_configuration_example09186a008014f8e7.shtml)>. 29.1.2008. Luettu 14.4.2013.
- 34 High CPU Utilization in the EXEC and Virtual EXEC Processes. 2008. PDF-tiedosto. Cisco Systems. <[http://www.cisco.com/image/gif/paws/41100/highcpu\\_exec.pdf](http://www.cisco.com/image/gif/paws/41100/highcpu_exec.pdf)>. 12.12.2008. Luettu 14.4.2013.
- 35 GNS3 introduction. 2013. Verkkodokumentti. <<http://www.gns3.net/gns3-introduction/>>. Luettu 15.4.2013.
- 36 Switching simulation in GNS3. 2013. Verkkodokumentti. <<http://www.gns3.net/gns3-switching-simulation/>>. Luettu 15.4.2013.
- 37 GNS3 ja Dynamips lisenssi. 2012. Verkkodokumentti. <<http://redmine.gns3.net/projects/1/wiki/License>>. Luettu 18.4.2013

- 38 GNU General Public License, version 2. 2013. Verkkodokumentti. Gnu.org.  
<<http://www.gnu.org/licenses/gpl-2.0.html>>. 16.3.2013. Luettu 18.4.2013.
- 39 Qemu license. 2013. Verkkodokumentti. Fabrice Bellard.  
<<http://wiki.qemu.org/License>>. Luettu 18.4.2013.
- 40 VirtualBox Licensing: Frequently Asked Questions. 2013. Verkkodokumentti.  
Oracle. <[https://www.virtualbox.org/wiki/Licensing\\_FAQ](https://www.virtualbox.org/wiki/Licensing_FAQ)>. Luettu 18.4.2013.
- 41 Wireshark User's Guide, license. 2013. Verkkodokumentti.  
<[http://www.wireshark.org/docs/wsug\\_html\\_chunked/ChapterIntroduction.html#idp962208](http://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#idp962208)>. Luettu 18.4.2013.
- 42 Virtual PC Simulator sourceforge-sivu. 2013. Verkkodokumentti. Sourceforge.net.  
<<http://sourceforge.net/projects/vpcs/>>. 16.2.2013. Luettu 18.4.2013.
- 43 Winpcap features. 2013. Verkkodokumentti. Riverbed Technology.  
<<http://www.winpcap.org/misc/features.htm>>. Luettu 18.4.2013.
- 44 Putty License. 2012. Verkkodokumentti.  
<<http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html>>. 27.1.2012.  
Luettu 18.4.2013.
- 45 Juniper EULA. 2011. Verkkodokumentti. Juniper Networks.  
<<http://www.juniper.net/support/eula.html>>. Luettu 18.4.2013.
- 46 Cisco EULA. 2011. PDF-tiedosto. Cisco Systems.  
<[http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\\_.pdf](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.pdf)>. Luettu 18.4.2013.
- 47 Puska, Matti. Yliopettaja. 2013. Tietotekniikka, Metropolia Ammattikorkeakoulu,  
Espoo. Keskustelu lopputyöaiheesta. 20.3.2013.
- 48 Vyatta Network OS datasheet. 2013. PDF-tiedosto. Vyatta Inc.  
<[http://www.vyatta.com/sites/vyatta.com/files/pdfs/vyatta\\_software\\_datasheet.pdf](http://www.vyatta.com/sites/vyatta.com/files/pdfs/vyatta_software_datasheet.pdf)>. Luettu 1.4.2013
- 49 Subscription release vs Community edition -foorumiviesti. 2008.  
Verkkodokumentti. <<http://www.vyatta.org/node/667>>. 30.7.2008. Luettu 1.4.2013
- 50 Vyatta Network OS for Virtualization. 2013. Verkkodokumentti. Vyatta Inc.  
<<http://www.vyatta.com/learn/vyatta-virtual-datasheet>>. Luettu 25.3.2013
- 51 Vyatta Deployment Options. 2012. PDF-tiedosto. Vyatta Inc.  
<[http://www.vyatta.com/downloads/documentation/VC6.5/Vyatta-DeploymentOptions\\_6.5R1\\_v01.pdf](http://www.vyatta.com/downloads/documentation/VC6.5/Vyatta-DeploymentOptions_6.5R1_v01.pdf)>. Lokakuu 2012. Luettu 2.4.2013.

- 52 Understanding Vyatta Core License. 2012. Verkkodokumentti. <<http://www.vyatta.org/node/6757>>. Luettu 1.4.2013.
- 53 Vyatta installation. 2012. Youtube-video. Techxpert Infotech. <<http://www.youtube.com/watch?v=mrIU7rnaAs>>. 30.08.2012.
- 54 Foley, Karl. Boot error in VirtualBox. 2011. Verkkodokumentti. <<http://blog.thefoleyhouse.co.uk/2011/02/ubuntu-boot-error-in-virtualbox.html>>. 19.2.2011. Luettu 20.4.2013.
- 55 Configure Vyatta in GNS3. 2013. Youtube-video. Techxpert Infotech. <<http://www.youtube.com/watch?v=mrIU7rnaAs>>. 11.3.2013.
- 56 UDP Tunnel networking. 2013. Verkkodokumentti. Oracle Corporation. <[http://www.virtualbox.org/manual/ch06.html#network\\_udp\\_tunnel](http://www.virtualbox.org/manual/ch06.html#network_udp_tunnel)>. Luettu 25.3.2013.
- 57 Vyatta. 2013. Verkkodokumentti. Wikipedia. <<http://en.wikipedia.org/wiki/Vyatta>>. 28.2.2013. Luettu 20.4.2013.

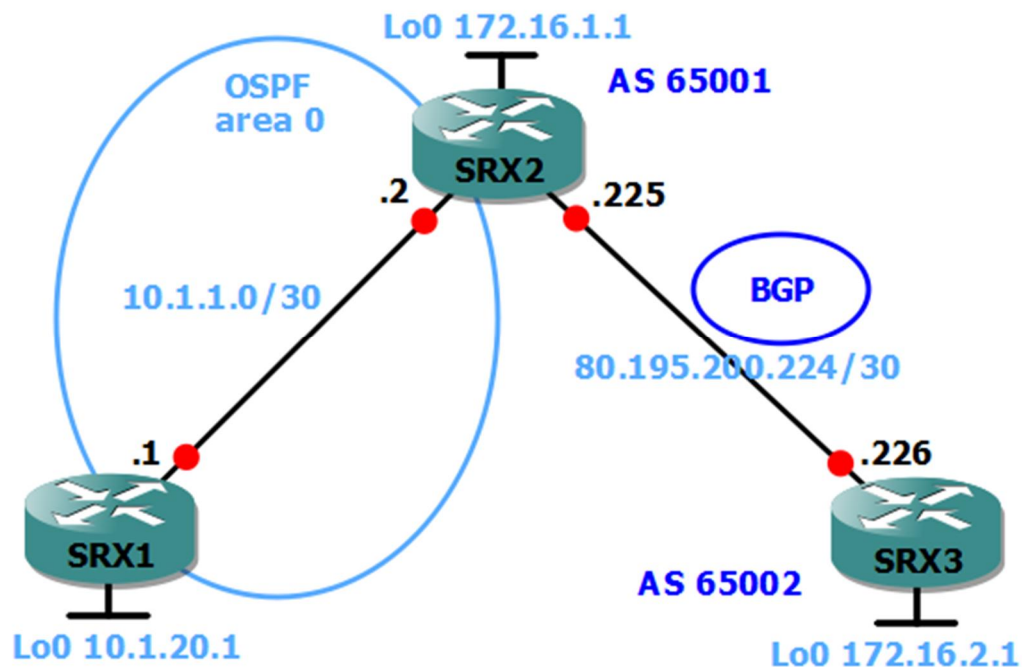
## Terminaalipalvelimen konfiguraatio

```
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
no service dhcp
!
hostname Termserver
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging message-counter syslog
enable secret 5 $1$a9ya$wqm974HE/eCuD71sDPk90/
!
aaa new-model
!
aaa authentication login LOCAL_AUTHEN local
aaa authentication login RTELNET none
aaa authorization exec LOCAL_AUTHOR local
!
aaa session-id common
!
dot11 syslog
no ip source-route
!
ip cef
!
no ip bootp server
no ip domain lookup
ip domain name metropolia.fi
ip host SRX1 2066 X.X.X.X
ip host SRX2 2067 X.X.X.X
ip host SRX3 2068 X.X.X.X
ip host SRX4 2069 X.X.X.X
ip host SRX5 2070 X.X.X.X
ip host SRX6 2071 X.X.X.X
ip host SRX7 2072 X.X.X.X
ip host SRX8 2073 X.X.X.X
ip host SRX9 2074 X.X.X.X
no ipv6 cef
!
multilink bundle-name authenticated
!
```

```
voice-card 0
!
crypto key generate rsa modulus 1024
!
username ops-clear privilege 2 password 7 0030165F5509530B1D
username admin-metropolia privilege 15 password 7 055E522534421F5B0A0A
archive
  log config
  hidekeys
!
ip tcp synwait-time 10
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
!
interface Loopback0
  ip address Y.Y.Y.Y 255.255.255.0
  no ip redirects
  no ip unreachable
  no ip proxy-arp
  ip flow ingress
!
interface FastEthernet0/0
  ip address Z.Z.Z.Z 255.255.255.0
  no ip redirects
  no ip unreachable
  no ip proxy-arp
  ip flow egress
  duplex auto
  speed auto
  no mop enabled
!
ip default-gateway XY.XY.XY.XY
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
banner login ^CAuthorized access only!
  Disconnect IMMEDIATELY if you are not an authorized user!^C
privilege exec level 15 connect
privilege exec level 15 telnet
privilege exec level 15 rlogin
privilege exec level 15 show ip access-lists
privilege exec level 1 show ip
privilege exec level 15 show access-lists
privilege exec level 15 show logging
privilege exec level 1 show
```

```
privilege exec level 2 clear line
privilege exec level 2 clear
!
line con 0
 logging synchronous
 login authentication LOCAL_AUTHEN
line aux 0
 login authentication LOCAL_AUTHEN
line 1/0 1/31
 session-timeout 60
 absolute-timeout 300
 login authentication RTELNET
 no exec
 transport input telnet
line vty 0 4
 exec-timeout 60 0
 authorization exec LOCAL_AUTHOR
 login authentication LOCAL_AUTHEN
 transport input ssh
!
scheduler allocate 20000 1000
end
```

## Esimerkkiharjoitus



Kuva 1. Harjoitustopologia

Laboratorioharjoituksen tavoitteena on konfiguroida laitteet yllä olevan topologian mukaisesti. Yrityksen sisäisissä reitittimissä on toiminnassa OSPF-reititys. SRX2-reunareitittimen ja palveluntarjoajan SRX3-reitittimen välillä on BGP-naapuruus. Yhteyttä internetiin simuloi SRX3:n loopback0 osoitteessa 172.16.2.1.

Aluksi kerrataan Junosin perusteita. Jos perusteet on hallussa harjoituksen voi aloittaa suoraan kohdasta 10.

1. Kirjaudu laitteisiin ohjaajan antamilla tunnuksilla. Kirjautumisen jälkeen käyttäjä saapuu Unixin shell-komentotilaan (%). Komennolla cli päästään CLI:n toiminnalliseen tilaan (>).

```
user% cli
user>
```

2. Kysymysmerkillä näet kaikki vaihtoehdot mitä voit sen hetkessä tilassa tehdä. Lisäksi tabulaattorilla voi täydentää komentoja automaattisesti.

```
user> ?
Possible completions:
  clear                Clear information in the system
  configure            Manipulate software configuration information
  file                Perform file operations
  ...

user> show c
      ^
'c' is ambiguous.
Possible completions:
  chassis              Show chassis information
  class-of-service    Show class-of-service (CoS) information
  cli                  Show command-line interface settings
  configuration        Show current configuration
  connections          Show circuit cross-connect connections
```

3. Komento show configuration näyttää toiminnallisessa tilassa laitteen nykyisen konfiguraation.

```
user> show configuration
```

4. Komennolla configure päästään CLI:n konfigurointitilaan (#).

```
user> configure
  Entering configuration mode
[edit]
user#
```

5. Konfigurointitilasta voidaan kutsua toiminnallisen tilan komentoja kirjoittamalla ensin run.

```
[edit]
user# run show configuration
```

6. Set-komennolla voidaan syöttää haluttu konfiguraatio. Tehdyt konfiguraatiomuutokset aktivoidaan commit-komennolla. Esimerkiksi isäntänimen vaihto tehdään seuraavasti:

```
[edit]
user# set system host-name UUSINIEMI
[edit]
user# commit
```

7. Jos konfiguraatioon tehdään vahingossa virhe, voidaan edelliseen palata rollback-komennolla. Taaksepäin voi palata yhden tai useamman tehdyn commit kerran. Vanha konfiguraatio aktivoidaan uudelleen commit-komennolla. Seuraavat komennot poistavat isäntänimen muutoksen.

```
[edit]
user@UUSINIEMI# rollback 1
load complete
[edit]
user@UUSINIEMI# commit
commit complete
[edit]
user#
```

8. Edit-komennolla päästään CLI:n konfiguraatiohierarkiassa halutulle tasolle. Up-komennolla päästään hierarkiassa taaksepäin ja top-komento palauttaa ylimpään hierarkiaan eli takaisin konfigurointitason juureen. Mikä tahansa konfiguraatio voidaan tehdä suoraan set-komennolla, joten edit-komennon käyttö ei ole pakollista, mutta voi selkiyttää joskus konfigurointia. Seuraavassa esimerkkiä, kun on siirrytty ensin tasolle interfaces ge-0/0/0 unit 0 family inet.

```
[edit]
user# edit interfaces ge-0/0/0 unit 0 family inet
[edit interfaces ge-0/0/0 unit 0 family inet]
user# up 2
[edit interfaces ge-0/0/0]
user# top
[edit]
user#
```

9. Ennen commit-komentoa kannattaa tarkistaa konfiguraatiomuutokset mahdollisilta virheiltä commit check -komennolla.

```
[edi t]
user# set system host-name SRX1
[edi t]
user# commi t check
configurati on check succeeds
[edi t]
user# commi t
commi t compl ete
[edi t]
user@SRX1#
```

10. Konfiguroi isäntänimet kaikkiin laitteisiin. Konfiguroi jokaisen laitteen liitântien sekä loopback 0:ien IP-osoitteet joko suoraan set-komennolla tai siirtymällä ensin oikealle tasolle edit-komennolla. Alla esimerkkinä SRX1:n konfiguraatio suoraan set-komennolla.

```
user@SRX1# set interfaces ge-0/0/0 uni t 0 fami ly i net address
  10. 1. 1. 1/30
user@SRX1# set interfaces lo0 uni t 0 fami ly i net address 10. 1. 20. 1
```

Muista aina aktivoida konfiguraatiomuutokset komennolla commit.

```
user@SRX1# commi t
commi t compl ete
```

Konfiguroidut liitännät voidaan tarkistaa.

```
user@SRX1# show i nterfaces
```

Voit kokeilla lopuksi pingata viereisen laitteen liitântää.

```
user@SRX1# run pi ng 10. 1. 1. 2
```

11. Konfiguroi OSPF reititys SRX1:een ja SRX2:een.

```
user@SRX1# set protocol s ospf area 0.0.0.0 interface ge-0/0/0
user@SRX1# set protocol s ospf area 0.0.0.0 interface lo0
```

```
user@SRX2# set protocol s ospf area 0.0.0.0 interface ge-0/0/0
user@SRX2# set protocol s ospf area 0.0.0.0 interface lo0
```

SRX2:sta SRX3:een menevä liitäntä voidaan laittaa passiiviseksi.

```
user@SRX2# set protocol s ospf area 0.0.0.0 interface ge-0/1/1 passive
```

Voit tarkistaa ospf-konfiguraatiot.

```
user@SRX1# show protocol s ospf
```

12. Konfiguroi staattiset reitit SRX2:een ja SRX3:een.

```
user@SRX2# set routing-options static route 172.16.2.1 next-hop
80.195.200.226
```

```
user@SRX3# set routing-options static route 172.16.1.1 next-hop
80.195.200.225
user@SRX3# set routing-options static route 10.1.0.0/16 next-hop
80.195.200.225
```

Konfiguroi SRX3:een oletusreitti, joka estää reitityssilmukat pudottamalla paketit:

```
user@SRX3# set routing-options static route 0.0.0.0/0 discard
```

Konfiguraatiot voi lopuksi tarkistaa.

```
user@SRX3# show routing-opti ons
```

13. Konfiguroi eBGP-sessio SRX2:n ja SRX3:n välille.

Aseta autonominen järjestelmä -numero topologian mukaisesti.

```
user@SRX2# set routing-options autonomous-system 65001
user@SRX3# set routing-options autonomous-system 65002
```

Määritä eBGP SRX2:ssa, aseta loopback0:n IP session osoitteeksi ja naapuriksi toisen AS:n loopback0 osoite. Koska SRX2:n ja SRX3:n loopback:ien välissä on 2 reititintä multihop tulee olla 2.

```
user@SRX2# edit protocols bgp group EBGp
```

```
[edit protocols bgp group EBGp]
user@SRX2# set type external
user@SRX2# set local-address 172.16.1.1
user@SRX2# set peer-as 65002
user@SRX2# set neighbor 172.16.2.1
user@SRX2# set multihop ttl 2
```

BGP-konfiguraation voi tarkistaa.

```
user@SRX2# show protocols bgp
```

Määritä politiikka oletusreitille SRX3:ssa, jotta reittiä voidaan mainostaa BGP:ssä

```
user@SRX3# edit policy-options policy-statement DEFAULT term 1
```

```
[edit policy-options policy-statement DEFAULT term 1]
user@SRX3# set from route-filter 0.0.0.0/0 exact
user@SRX3# set then accept
```

Tarkista politiikka.

```
user@SRX3# show policy-options
```

Konfiguroi eBGP SRX3:ssa samaan tapaan kuin SRX2:ssa ja mainosta oletusreitettä.

```
user@SRX3# edit protocols bgp group EBGP
```

```
[edit protocols bgp group EBGP]  
user@SRX3# set type external  
user@SRX3# set local-address 172.16.2.1  
user@SRX3# set export DEFAULT  
user@SRX3# set peer-as 65001  
user@SRX3# set neighbor 172.16.1.1  
user@SRX3# set multipath ttl 2
```

Aseta loopback0 osoitteet reitittimien id:ksi (router-id).

```
user@SRX1# set routing-options router-id 10.1.20.1  
user@SRX2# set routing-options router-id 172.16.1.1  
user@SRX3# set routing-options router-id 172.16.2.1
```

Tarkista molemmissa reitittimissä, että BGP-sessio on aktiivinen.

```
user@SRX2# run show bgp summary
```

#### 14. Mainosta oletusreitettä OSPF:ssä.

Tee ensin politiikka BGP:stä saatavalle oletusreitille.

```
user@SRX2# edit policy-options policy-statement BGP-T0-OSPF term 1  
  
[edit policy-options policy-statement BGP-T0-OSPF term 1]  
user@SRX2# set from protocol bgp  
user@SRX2# set from as-path upstream  
user@SRX2# set from route-filter 0.0.0.0/0 exact  
user@SRX2# set then accept
```

Määritä upstream-ilmaus, niin että AS-polku viittaa SRX3:een.

```
user@SRX2# set policy-options as-path upstream "^65002 "
```

Aseta SRX2:een viimeisen vaihtoehdon reitti (route of last resort).

```
user@SRX2# set routing-options generate route 0.0.0.0/0 policy BGP-T0-OSPF
```

Lisää oletusreitti OSPF:ään.

```
user@SRX2# set protocol s ospf export BGP-T0-OSPF
```

15. Kun olet aktivoinut kaikki konfiguraatiomuutokset commit-komennolla, tarkista että kaikki toimii.

Hyödyllisiä komentoja:

```
show route  
show ospf route  
show bgp nei gbor  
show ospf nei ghor  
ping <kohde> source <loopback osoi te>
```

Lähteet

Example: Configuring EBGP Multihop Sessions. 11.11.2011. Verkkodokumentti. Juniper Networks. <[http://www.juniper.net/techpubs/en\\_US/junos11.3/topics/example/bgp-multihop.html](http://www.juniper.net/techpubs/en_US/junos11.3/topics/example/bgp-multihop.html)>.

Example: Conditionally Generating Static Routes. 10.8.2012. Verkkodokumentti. Juniper Networks. <[http://www.juniper.net/techpubs/en\\_US/junos12.1/topics/topic-map/policy-generated-route.html](http://www.juniper.net/techpubs/en_US/junos12.1/topics/topic-map/policy-generated-route.html)>.