

Juho Immonen

L2-kytkinten ominaisuudet ja konfigurointi

Katsaus Juniperin, Ciscon ja HP:n kytkinten perustoimintoihin

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

7.3.2017

Tekijä(t) Otsikko Sivumäärä Aika	Juho Immonen L2-kytkinten ominaisuudet ja konfigurointi Katsaus Juniperin, Ciscon ja HP:n kytkinten perustoimintoihin 30 sivua 7.3.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot ja tietoliikenne
Ohjaaja(t)	Janne Salonen, Osaamisaluepäällikkö
<p>Insinööriyössä vertaillaan Cisco IOS:n, Juniper JUNOS:n ja HP ProVisionin eli kolmen eri valmistajan kytkinkäyttöjärjestelmien ominaisuuksia ohjelmistotasolla sekä kytkinkonfiguraatioiden muotojen ja syntaksien eroavaisuuksia ja yhteensopivuutta. Lisäksi työssä tutkitaan tarkemmin joitain L2-verkkoihin olennaisesti kuuluvia elementtejä ja niiden konfigurointia eri käyttöjärjestelmissä.</p> <p>Työssä esitellään yksityiskohtaisesti kytkinten fyysiset ja loogiset portit, virtuaalilähiverkot ja 802.1q-protokolla, linkkien yhdistäminen loogiseksi linkkiryppäiksi ja multiple spanning tree -protokolla. Perusteiden lisäksi lukija viedään kädestä pitäen vertailussa olevien kytkinten konfiguraatioihin näiden ominaisuuksien osalta. Lisäksi jokaisen kytkimen kohdalla käydään läpi tavallisimmin tehtävät toimenpiteet kytkimen ensimmäisen käyttöönoton yhteydessä.</p> <p>Esitellyt toiminnot ovat kaikilla kytkimillä helposti määriteltävissä. Näin tulee ollakin, sillä ne ovat hallittavien kytkinten perustoiminnallisuuksia. Jokaisessa kytkimessä on omat etunsa ja omat haittapuolensa sekä syntaksin että konfigurointimukavuuden näkökulmasta. Objektivisesti käyttöjärjestelmiä ei voida pitää toistaan parempina, vaan valinnat tehdään usein muiden ominaisuuksien perusteella.</p>	
Avainsanat	Siirtokerros, tietoliikennekytkin, vlan, 802.1q, trunk, spanning tree

Author(s) Title	Juho Immonen Features and Configuring of L2 Switches
Number of Pages Date	30 pages 7 March 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunications and Data networks
Instructor(s)	Janne Salonen, Head of Department
<p>This paper is a study of the features and functions of three layer 2 network switch operating systems: Cisco IOS, Juniper JUNOS, and HP ProVision. Basic configuration elements are compared in terms of syntax and interoperability of the most fundamental functions in layer 2 networks.</p> <p>A more detailed exploration is performed for physical as well as logical switch interfaces, virtual LANs and 802.1q protocol, the bundling of multiple ports into one port channel, and the versatile multiple spanning tree protocol. In addition to these features some of the most often used pre-configuration and basic security hardening elements are presented for all the switches. All the above is presented first in a more general approach and then one by one in the three switch operating systems as configuration commands with proper commentary.</p> <p>The features presented are all relatively easy to configure to all the switches in the scope of the study. This is to be expected since they are in fact the basic features of any manageable switch. Each operating system has its strengths and weaknesses when it comes to configuration syntax as well as user experience. No operating system is objectively better than the other and switches are generally picked with different specifications in mind.</p>	
Keywords	Data link layer, network switch, vlan, 802.1q, trunk, spanning tree

Sisällys

Lyhenteet

1	Johdanto	1
2	Tuotevalmistajat	1
2.1	Hewlett Packard	2
2.2	Cisco	3
2.3	Juniper Networks	4
2.4	Verkkotuotteiden valikointi	5
3	Kytkimet ja käyttöjärjestelmät	5
3.1	HP Aruba (ent. ProCurve) ja ProVision-käyttöjärjestelmä	6
3.2	Cisco Catalyst ja IOS-käyttöjärjestelmä	6
3.3	Juniper EX ja Junos-käyttöjärjestelmä	8
4	Konfigurointi ja yhteensopivuus	9
4.1	Esikonfiguraatio	11
4.2	Sovittimet, portit, VLANit ja IEEE 802.1Q	15
4.3	Linkkien kanavointi	21
4.4	Spanning tree	25
5	Yhteenveto	29
	Lähteet	31

Lyhenteet

AAA	Authentication, Authorization, Accounting. Autentikointi, luvitus ja kirjanpito. Kirjainyhdistelmällä viitataan pääsynhallintaan ja käyttäjien seurantaan.
AE	Aggregated Ethernet. Juniperin käyttämä lyhenne linkkien kanavointia varten luotavalle virtuaali-interfacelle.
ASIC	Application-Specific Integrated Circuit. Sovelluskohtainen mikropiiri eli piiri, joka on suunniteltu varta vasten tiettyyn tarkoitukseen.
CAM	Content Addressable Memory. Ciscon käyttämä termi listalle, johon varastoidaan tunnettuja MAC-osoitteita verkkokytkeä varten.
CLI	Command Line Interface. Komentokehote.
DNS	Domain Name System. Hierarkkinen, hajautettu nimeämisjärjestelmä koneille, palveluille ja muille internetiin tai muuhun verkkoon kytketyille resursseille.
FreeBSD	Free Berkeley Software Distribution. Avoimen lähdekoodin Unixiin pohjaava käyttöjärjestelmä.
GUI	Graphical User Interface. Graafisen käyttöliittymän yleisnimitys.
GVRP	GARP VLAN Registration Protocol. VTP:n tavalla toimiva yleinen IEEE:n määrittelemä standardi, joka ei ole laajalti käytössä.
IEEE	Institute of Electrical and Electronics Engineers. Maailmanlaajuinen voittoa tavoittelematon järjestö.
IOS	Internetwork Operating System. Ciscon kehittämä käyttöjärjestelmä, joka on käytössä useissa Ciscon tietoverkkolaitteissa.

IP	Internet Protocol. IP-protokollasta on yksi TCP/IP-protokollapinon ja Internetin peruskivistä. Tällä hetkellä käytössä on IPv4, joka on vaihtumassa versioon IPv6.
ISO	International Organization for Standardization. Kansainvälinen standardeja julkaiseva ja hallinnoiva organisaatio.
L2	Layer 2. OSI-mallin toinen kerros eli siirtokerros kuljettaa pakettikehyksiä. Kytkentäiset verkot toimivat pääasiallisesti siirtokerroksella.
L3	Layer 3. OSI-mallin kolmas kerros eli verkkokerros, joka käsittelee IP-paketteja. IP-reititys tapahtuu pääasiallisesti verkkokerroksella.
L4	Layer 4. OSI-mallin neljäs kerros eli kuljetuskerros huolehtii vuonhallinnasta ja pakettien perillesaapumisesta ja oikeasta järjestyksestä.
LACP	Link Aggregation Control Protocol. Linkkien kanavointiin käytetty hallintaprotokolla esiteltiin ensimmäisen kerran IEEE 802.3ad -standardissa vuonna 2000.
LAG	Link Aggregation Group. Juniperin käyttämä termi kanavoitujen linkkien ryhmästä.
LAN	Local Area Network. Lähiverkko.
MAC	Media Access Control. Lyhennettä käyteään MAC-osoitteiden kohdalla, jotka ovat fyysisten verkkonoodien tai porttien uniikkeja osoitteita, minkä perusteella liikennettä ohjataan L2-verkoissa.
MSFC	Multilayer Switch Feature Card. Ciscon Catalyst 6500-sarjan kytkimiin suunniteltu monitasokytkentää tekevä moduuli.
MST	Multiple Spanning Tree. Spanning tree -protokolla, joka sallii useita verkkoalueita ja useita spanning tree -instansseja verkon sisällä.
MSTP	Katso MST.

NTP	Network Time Protocol. NTP on verkkoprotokolla verkkolaitteiden ja tietokoneiden kellojen synkronointiin.
OS	Operating system. Tietokoneen käyttöjärjestelmä.
OSI	Open Systems Interconnection. OSI-malli esitteli tietoverkon seitsenkerroksisen mallin ISO/IEC 7498-1 standardissa vuonna 1994.
OSPF	Open Shortest Path First. Sisäverkoissa yleisimmin käytetty ja parhaiten tuettu reititysprotokolla.
PAGP	Port Aggregation Protocol. Ciscon kehittämä, hiipuva verkkoprotokolla linkkien kanavoinnin hallintaprotokollaksi LACP-protokollan rinnalle.
PARC	Palo Alto Research Center. Xeroxin tutkimuskeskus Palo Altossa, Kaliforniassa.
PUP	PARC Universal Packet. Verkkoprotokolla joka aikanaan oli IP-protokollan haastaja. PUP kehitettiin vuonna 1974 PARC:ssä.
RAM	Random Access Memory. Tietokoneen käyttömuisti, joka pyyhkiytyy aina, kun tietokone sammutetaan.
RSA	Rivest-Shamir-Adleman. Yksi ensimmäisistä julkiseen avaimeen perustuvista kryptojärjestelmistä.
RSTP	Rapid Spanning Tree Protocol. Katso STP.
SFP	Small Form-factor Pluggable transceiver. SFP on olennaisesti kytkimeen kiinnitettävä erillinen kytkinportti.
SNTP	Simple Network Time Protocol. Katso NTP.
SSH	Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla. Verkkolaitteiden etäyhteyksiä muodostetaan useimmiten SSH-protokollalla.

STP	Spanning Tree Protocol. Siirtoverkkotason protokolla, joka estää looppien muodostumisen laskemalla verkon topologian ja muokkaamalla siitä puumaisen.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko, joka esiteltiin IEEE 802.1Q-standardin ensimmäisessä versiossa vuonna 2003.
VTP	VLAN Trunk Protocol. Ciscon kehittämä hiipuva protokolla, jonka avulla VLANit voidaan määrittää keskitetysti verkon kaikkiin kytkimiin.
VTY	Virtual Teletype. Telnetillä muodostettu CLI-yhteys verkkolaitteeseen. Nytemmin termiä käytetään myös SSH:lla muodostettuihin yhteyksiin.

1 Johdanto

Opinnäytetyössäni vertailen kolmen tietoliikennelaitteita valmistavan yhtiön tietoverkko-kytkinten ominaisuuksia ohjelmistotasolla sekä kytkinkonfiguraatioiden muotojen ja syntaksien eroavaisuuksia ja yhteensopivuutta. Valitsin vertailemani valmistajat sillä perusteella, että olen nähnyt näitä kolmea käytettävän selvästi eniten suurten ja keskisuurten yritysten lähiverkoissa, ja minulla on myös työtaustani puolesta kokemusta lähiverkkojen konfiguroinnista, ylläpidosta ja vianselvityksestä. Vertailemani yhtiöt ja niiden tuotteet ovat HP:n Aruba-kytkimet (ent. Procurve), Ciscon IOS-käyttöjärjestelmään pohjaavat Catalyst-kytkimet sekä Juniperin Junos OS -käyttöjärjestelmään pohjaavat EX-sarjan kytkimet.

Koska nykyaikaisten kytkinten ominaisuuksien kirjo on niin laaja, rajaan työni koskemaan ainoastaan tavallisimpia siirtokerroksen asetuksia ja protokollia. Näihin lukeutuvat virtuaalilähiverkot eli VLANit ja niiden myötä 802.1Q -standardin mukainen VLAN-täggäys, spanning tree -protokolla, linkkien kanavointi ja LACP sekä kytkinten portti- ja järjestelmäkonfiguraatio käyttöönottoa varten.

Seuraavassa luvussa tutustumme vertailemiani verkkokytkimiä valmistaviin yrityksiin. Luvussa kolme perehdymme itse kytkimiin ja niiden ohjelmistoihin ja konfiguraatioiden rakenteeseen. Luvun neljä aiheena on kytkinten määrittysten tarkempi tarkastelu, ja viimeisessä yhteenvetoluvussa pohdin jotain.

2 Tuotevalmistajat

Selvitän kolmen eri verkkolaittevalmistajan verkkokytkinten perustoiminnallisuuksia siirtokerroksella, joka on OSI-mallin toiseksi alin kerros (ISO/IEC 7498-1 1994: 28). Kytkinvalmistajat valitsin tunnettuuden sekä suurten ja keskisuurten yritysverkkojen yleisimpien kytkinten perusteella, jotka kokemukseni perusteella ovat Cisco Systems, Hewlett Packard ja Juniper Networks.

Eri kytkinvalmistajien tuotteita vertaillen on otettava huomioon ominaisuuksien vaihtelu ja erityisesti Ciscon kohdalla valmistajan omat protokollat, joita muut kytkinvalmistajat

eivät laitteissaan tue. Rautatason ominaisuuksiin kuten ASIC-piirien tehokkuuteen ja paremmuuteen, kytkimen käyttöikään ja luotettavuuteen en työssäni ota kantaa. En myöskään puutu kytkinten hintaeroihin, sillä esittämäni eivät päde mihinkään yksittäisiin kytkimiin. Tutkimani aiheet liittyvät enimmäkseen kytkinten käyttöjärjestelmien ominaisuuksiin, ja siten voi ottaa eroavaisuuksiin kantaa ainoastaan ohjelmistotasolla. Seuraavaksi esittelen valitsemani yhtiöiden historiaa ja hieman talouslukuja.

2.1 Hewlett Packard

Hewlett Packard perustettiin vuonna 1939 Kalifornian Palo Altossa. Stanfordissa ystävyystyneet William Hewlett ja Dave Packard aloittivat yhtiönsä autotallissa, jossa he rakensivat prototyyppejä mm. lääketieteen ja paikallisen observatorion tarpeisiin. Yhtiötä ajatellen todellinen läpimurto oli kuitenkin resistanssiviritettävä oskillaattori, josta tuli Hewlett Packardin ensimmäinen kaupallinen tuote. Tuotteen seuraavaa versiota, mallia 200B käytettiin jo Disneyn ikonisen animaatioelokuvan Fantasian esittämisessä elokuvateattereissa vuonna 1940. Autotalli, josta käsin Hewlett ja Packard aloittivat uransa, on nykyään Kalifornian osavaltion tunnustama historiallinen maamerkki: Silicon Valleyn virallinen synnyinpaikka. (hp.com 6.12.2016.)

HP alkoi valmistaa tietokoneita vuonna 1972. Uusi HP 3000 oli yritysten tiedonkäsittelyyn suunniteltu, alun perin usean arkistokaapin kokoinen tietokone, joka jo pari vuotta myöhemmin korvautui työpöytään upotettavalla stabiilimmalla mallilla. Ensimmäinen pöydälle sopiva tietokone, ja sitä myöten ensimmäinen PC HP:lta tuli ulos vuonna 1980. 80-luvulla HP julkaisi myös ensimmäiset LaserJet- ja DeskJet-tulostimensa. LaserJet on tähän päivään asti HP:n kaikkien aikojen menestynein tuoteperhe, ja se on rikkonut rajoja niin teknologiansa kuin designinsa puolesta. (Baker 2010; hp.com 7.12.2016; Wikipedia, HP 3000, HP LaserJet, Hewlett Packard 7.12.2016.)

HP:n verkko-osasto aloitti vuonna 1979 osana Data Systems Divisionia Kalifornian Rosevillessä, mutta erkani myöhemmin omaksi osastokseen. Vuonna 1998 rekisteröitiin tuotenimi ProCurve, ja sen alla HP on kehittänyt verkkokytkimiään viime aikoihin asti. Sittemmin Aruba Networksin yritysoston myötä ProCurve-kytkimet siirrettiin Aruba-tuoteperheeseen. (Gold 2016; Wikipedia, Procurve luettu 15.12.2016.)

HP:n vuoden 2015 liikevaihto oli yhteensä 103,4 miljardia dollaria (USD), josta HPE Groupin eli Hewlett Packard Enterprise Groupin osuus on 27,9 miljardia dollaria. Viime vuodesta kokonaisliikevaihto on pudonnut 8 miljardia tai 7,2 %, kun taas HPE Groupin liikevaihto on noussut yhdellä prosentilla ja verkkotuotteiden liikevaihto on noussut peräti 8 %. HPE Groupin osuus kokonaisliikevaihdosta on n. 27 %. Yhtiön toiminnasta 46 % sijoittuu Amerikan mantereelle Euroopan kirieessä 35 %:n osuuteen. Aasian ja Tyynenmeren alueen osuus jää 19 %:ään liikevaihdosta. (hp.com 15.12.2016.)

2.2 Cisco

Cisco Systemsin perusti vuonna 1984 Leonard Bosack ja Sandy Lerner, molemmat Stanfordin yliopiston eri tiedekuntien ATK-vastaavia ja lisäksi aviopuolisoja. Ajatus yhtiön perustamiseen lähti tarpeesta saada yliopiston eri tiedekuntien verkot keskustelemaan keskenään, mikä tuona aikana onnistui lähinnä Arpanetin kautta. Ongelmaa ratkomassa oli useita Stanfordin tutkijoita, mukaan lukien Kirk Lougheed, josta tuli Ciscon ensimmäinen varsinainen työntekijä. (Bort 2014; Corcoran 2011; Wikipedia, Cisco Systems 3.11.2016.)

Reititinteknologian oli alun perin tarkoitus perustua PARC Universal Packet (PUP) -protokollaan, mutta Lougheed kollegoineen ymmärsi vuonna 1981 RFC 791:ssä määritellyn IPv4-protokollan yleistyvän sellaista vauhtia, että he päättivät perustaa teknologiansa siihen PUP:n sijaan. Syntyi ensimmäinen versio ohjelmistosta, joka tunnetaan tänä päivänä nimellä Cisco Internetworking Operating System eli IOS. (Bort 2014; Corcoran 2011; Wikipedia, Cisco Systems; Wikipedia, Internet Protocol.)

Cisco Systems aloitti tuotemyynnin vuonna 1986 perustajien jäätyä eturistiriitojen vuoksi pakostakin pois päivätöistä, ja ensimmäisen vuoden jälkeen myyntiä oli 1,5 miljoonaa dollaria. Kasvu jäi ensimmäisinä vuosina kuitenkin vähäiseksi, ja vuonna 1988 Bosack ja Lerner lähestyivät sijoittajia. Donald Valentine suostui rahoittamaan Ciscoa osakkeiden enemmistöosuuden hinnalla, mihin perustajat suostuivat. Tästä seurasi muutoksia yhtiön hallinnossa, minkä seurauksena perustajat lopulta myivät osuutensa yhtiöstä 170 miljoonalla dollarilla. Ammattijohtajien vetämänä yhtiö lähti lopulta kasvuun, ja vuonna 1995 nimitetty toimitusjohtaja John Chambers nosti Ciscon suvereenin markkinajohtajan asemaan 20-vuotisella urallaan. (Garza 2001.)

Cisco Systemsin vuoden 2015 liikevaihto oli yhteensä 49,2 miljardia dollaria, ja ennuste vuoden 2016 liikevaihdolle ei siitä poikkea. Yhtiön toiminnasta suurin osa (60 %) on Amerikoissa. Loput 40 % jakaantuvat Aasian ja Tyynenmeren (15 %) sekä Euroopan (25 %) alueille. 30 % Ciscon myymistä tuotteista ja palveluista muodostaa kytkimet. Seuraavaksi suurin kategoria on kaikki Ciscon tarjoamat palvelut (25 %). Kytkimet ovat Ciscon selvästi suurin tuote. (Cisco.com 1.11.2016.)

2.3 Juniper Networks

Vuonna 1995 Xerox PARC -tutkimuskeskuksen tutkija Pradeep Sindhu jäi lomalle pohtimaan tulevaisuuttaan. Hän kiinnostui reititinlaitteiden potentiaalista ja päätti kokeilla onneaan korkean suorituskyvyn reitittimien parissa. Vuoden 1996 helmikuussa Kaliforniassa rekisteröitiin yhtiö Juniper Networks. Yhtiön premissi oli normaalista start-up:sta poikkeava: sen oli määrä puuttua erityisesti vaikeimpiin haasteisiin ja ratkoa ne. Yhtiön ensimmäinen tuote julkaistiin vuoden 1998 syyskuussa. Se oli reititin M40, joka lunasti yhtiön lupaukset ja varmisti paikan ”suurena pelaajana” verkkolaittebisneksessä. M40 käytti Juniper Networksin kehittämää Junos OS -käyttöjärjestelmää, jota edelleen kehitetään ja käytetään yhtiön verkkolaitteissa, nykyään reitittimien lisäksi kytkimissä ja osin ScreenOS -käyttöjärjestelmästä poimitujen lisäysten ansiosta myös palomureissa. (juniper.net 4.1.2017; wikipedia.org, Junos OS.)

Yhtiö listautui pörssiin vuonna 1999 ja lähes kolminkertaisti osakkeidensa arvon heti ensimmäisenä päivänä. Vuoden 2000 loppupuolella tietoliikennekuplan puhjetessa Juniper Networksin osakekurssi kääntyi rajuun laskuun, ja vuoden 2002 lokakuuhun mennessä se oli pudonnut yli 200 dollarista alle kuuteen dollariin. Siitä eteenpäin yhtiö on lähinnä yritysostojen kautta laajentanut tuotevalikoimaansa ja niiden ominaisuuskirjoa. Vuonna 2008 yhtiö toi markkinoille oman EX-verkkokytkinmallistonsa. (Greene 2009.)

Juniper Networksin vuoden 2015 liikevaihto oli yhteensä 4,86 miljardia dollaria, mikä on 5 % enemmän kuin vuoden 2014 liikevaihto. Vuonna 2014 yhtiö myi Junos Pulse -liiketoimintansa Siris Capitalille, ja liikevaihto suhteutettuna tähän kasvoi 7 %. Yhtiön tuotemyynnistä suurin osa on reitittimiä: 2,36 miljardia dollaria eli 66,2 % liikevaihdosta. Kytkimet muodostavat 21,6 % osuuden 768,3 miljoonalla dollarilla ja tietoturva 12,2 % osuuden 435,6 miljoonalla dollarilla. Yhtiön tarjoamat palvelut muodostavat kokonaisliikevaihdosta 26,6 % osuuden eli 1,3 miljardia dollaria. (juniper.net 4.1.2017.)

2.4 Verkkotuotteiden valikointi

Pohtiessani mahdollisia kytkimiä ja niiden ominaisuuksia, joita tarkastelin opinnäytetyössäni, törmäsin nopeasti runsaudenpulaan. Pelkästään verkkolaitteiden valmistajia on niin suuri määrä, että tarkka rajaaminen on välttämättömyys, puhumattakaan kytkinmalleista ja niiden ominaisuuskirjosta. Päätin valita kolme tunnettua kytkinvalmistajaa ja tutkia ainoastaan tiedonsiirtokerrokseen sijoittuvia ominaisuuksia välttämättömien perustoiminnallisuuksien kuten etäyhteyksien lisäksi.

En halua valita tarkkoja kytkinmalleja tutkimusta varten, sillä tarkastelen komentoja ja konfiguraatioita tiukan teoreettisesti. Lukija voi kuitenkin vertailla konfiguraatioita Cisco Catalyst 2960-X-, HP Aruba 2530- ja Juniper EX-2200-kytkimiin niin halutessaan. Suurin osa ellei kaikki komennot ja konfiguraatiot ovat yhteensopivia näiden kanssa. Seuraavassa luvussa esittelen kytkinten käyttöjärjestelmät ja selvitän hieman konfiguraation ja konfiguroinnin syntaksieroja.

3 Kytkimet ja käyttöjärjestelmät

Kaikissa hallittavissa verkkolaitteissa on käyttöjärjestelmät, kuten missä tahansa tietokoneissa. Kytkimen käyttöjärjestelmä ei periaatteiltaan poikkea esimerkiksi tietokoneiden käyttöjärjestelmistä, ja kaikki verkkolaitteet ovatkin pohjimmiltaan erityiseen käyttötarkoitukseen suunniteltuja tietokoneita. Tästä seuraa loogisesti, että periaatteessa mikä tahansa yleiskäyttöinen tietokone pystyy tekemään pakettien kytkentää.

Nykyaikaiset kytkimet on suunniteltu käyttämään erityisesti pakettikytkentää varten suunniteltuja ASIC-piirejä, jotka suoriutuvat tästä tehtävästä energiatehokkaammin, vievät yleensä piirilevyllä vähemmän tilaa kuin yleiskäyttöiset mikropiirit ja ovat edullisia valmistaa. Esimerkiksi HP:n Aruba 2530-24 -kytkinmallin maksimitehönkäyttö on vain 14,7 wattia, joskin sen sovittimet ovat tyyppiä Fast Ethernet eli ne toimivat nopeudella 100 Mbps. ASIC-piirien suunnittelu on kuitenkin huomattavasti vaikeampaa ja siten kalliimpaa niiden erikoistuneen luonteen vuoksi, minkä vuoksi yleiskäyttöiset mikropiirit kuten PC-prosessorit ja RAM-muistit ovat yhä paras vaihtoehto useimpiin laskentatehtäviin. Seuraavaksi kerron tarkemmin kunkin tarkasteltavan kytkinmalliston ja niiden käyttöjärjestelmien perusominaisuuksista. (hp.com; Poole 11.1.2017; Techopedia 11.1.2017; Wikipedia.org, Application-specific integrated circuit, Fast Ethernet.)

3.1 HP Aruba (ent. ProCurve) ja ProVision-käyttöjärjestelmä

Entiset ProCurve-kytkimet ovat tulleet tunnetuiksi ennen kaikkea edullisesta hinnastaan verrattuna muihin yhtä luotettaviin ja vakaisiin yritystason kytkimiin. Vuoden 2016 loppupuolella kytkinten nimi on vaihtunut ProCurvesta Arubaksi, mutta muita muutoksia mallistoon tai kytkinten ominaisuuksiin ei toistaiseksi ole tullut. Kytkinmallistosta löytyy kaikenlaisia ratkaisuja pienistä 8-porttisista kytkimistä aina 48-porttisiin pinottaviin kytkimiin ja reitittäviin L3-kytkimiin.

Kytkimet käyttävät HP:n kehittämää ProVision-käyttöjärjestelmää, joka on luonteeltaan hyvin samankaltainen kuin Ciscon IOS-käyttöjärjestelmä sillä erotuksella, että ProVisionissa VLAN-konfiguraatio tehdään VLANien kautta, kun IOS:ssa VLAN-konfiguraatio on porttikohtaista. ProVisionin peruskonfiguraatio on suurelta osin implisiittinen, eli konfiguraatiolistaus ei ole kovin pitkä ennen kuin siihen tekee suurempia muutoksia. Komennon ”show configuration” tuloste voi hyvinkin mahtua yhdelle sivulle.

Komentokehotteeseen yhdistäessä aukeaa manager- tai operator-moodi riippuen yhdistämistavasta ja käyttäjätunnuksista. Operator-moodissa toiminnot on rajattu kapeaan listaan työkaluja статистиikan ja kytkimen tilojen tarkasteluun. Manager-moodi avaa loput komennot käyttäjän käyttöön. Komennolla ’configure’ siirrytään konfiguraatiomoodiin, jossa laitteen asetuksia säädetään. Tässä moodissa on useita alatasoja, kuten porttikonfiguraatiot ja VLAN-konfiguraatiot. ProVisionin erikoisuutena on komentokehotteeseen aukeava menu. Menun kautta voi säätää monia perusasetuksia, ja kuriositeettina kytkimen hallinta-IP-osoitteen vaihtaminen onnistuu menun kautta, vaikka etäyhteys olisi muodostettu IP:llä kommunikoivan yhteyden eli SSH:n tai telnetin yli.

3.2 Cisco Catalyst ja IOS-käyttöjärjestelmä

Ciscon Catalyst-sarja on todennäköisesti maailman tunnetuin tietoverkkolaitteperhe. Catalyst-sarjan kytkinvalikoima ulottuu massiivisista 20 rack unitin (~89cm korkeista) modulaarisista kytkinkehikoista tavallisiin 24-porttisiin kampus-kytkimiin, ja väliin mahtuu kaikenkokoisia ratkaisuja L2- ja L3-toiminnallisuuksilla. Catalyst-sarja on tilkkutäkki eri yritysostoista kertynyttä teknologiaa niin rauta- kuin softatasolla, joskin tuotekehityksen myötä sarjasta on muodostunut suhteellisen yhtenäinen kokoelma erikokoisia kytkimiä. (The Server Rack FAQ 11.1.2017; cisco.com 11.1.2017; wikipedia.org, Cisco Catalyst.)

Catalyst-sarjan käyttöjärjestelmä oli alun perin osassa kytkimiä Crescendo Communicationsin mukana ostettu CatOS, alkuperäiseltä nimeltään XDI (Clark & Hamilton 2002, Chapter 4. Configuring the Catalyst; Wikipedia.org, Cisco Catalyst). Siinä missä IOS keskittyi L3-protokollien ja palveluiden tukemiseen, oli CatOS:n vahvuus L2-, L3- ja L4-toiminnallisuuksissa. Catalyst 6500 -runkokytkimille on ollut saatavana kahta eri MSFC-moduulia (Multilayer Switch Feature Card): hybrid-moduulia, jossa kytkinprosessoria ajetaan CatOS:lla ja reititysprosessoria IOS:lla, sekä native-moduulia, jossa molempia prosessoreita ajetaan IOS:lla. CatOS:n IOS:sta puuttuvat ominaisuudet on sittemmin hiljalleen sulautettu IOS-käyttöjärjestelmään. Versio 12.2SX oli viimeinen hybrid-versio ja sen myynti lopetettiin 29.1.2008. Nykyään IOS on numerossa 15, josta versio 4 on uusin tällä hetkellä. (Comparison of the Cisco Catalyst and Cisco IOS Operating Systems for the Cisco Catalyst 6500 Series Switch 2004; Cisco.com, software browser.)

Kuten luvussa 3.1 mainitsin, IOS on samankaltainen konfigurointiympäristö kuin HP:n ProVision sillä erotuksella, että porttien VLAN-määrytykset tehdään IOS:ssa porttikonfiguraatioon VLAN-konfiguraation sijaan. Kytkentäisissä verkoissa VLANit ovat niin keskeisessä osassa, että tämä yksi eroavaisuus muuttaa konfiguraation mekaniikkaa ja ole-musta merkittävästi. IOS:n konfiguraatio on joitain poikkeuksia lukuun ottamatta eksplisiittinen, ja komennon "show startup-config" tuloste esittää konfiguraation, joka laitteelle on tallennettu. Konfiguraatiotulosteessa tyhjät rivit merkitään huutomerkkein tulosteen luettavuuden parantamiseksi, eikä huutomerkeillä ole muuta virkaa konfiguraatiossa. Laitteelle konfiguroidut VLANit näkyvät tai eivät näy konfiguraatiossa riippuen VTP (VLAN Trunk Protocol) -asetuksista. VTP on Ciscon oma protokolla, jonka suosio on jäänyt hyvin vähäiseksi, eikä se toimi kaikkien nykyaikaisten protokollien kuten MSTP:n kanssa. Hyvän konfigurointikäytännön mukaan VTP määritetään aina moodiin transparent, joka käytännössä tarkoittaa, ettei VTP:tä käytetä, jolloin VLAN-konfiguraatio näkyy startup-configissa ja running-configissa, eikä verkkoon kytkettävä VTP server -moodiin määritetty kytkin pääse vahingossakaan tekemään VLAN-asetuksiin muutoksia.

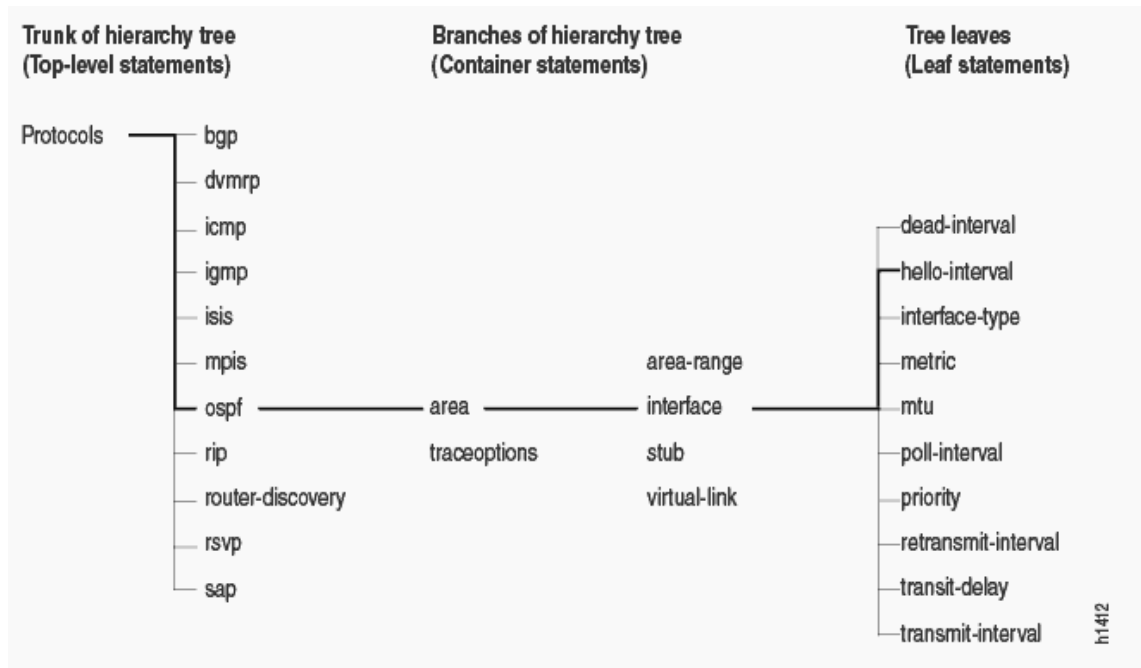
Kytkimen komentokehoteeseen kirjaudutaan useimmiten User EXEC -moodissa, joka vastaa HP:n operator-moodia. Seuraava taso, Privileged EXEC -moodi, vastaa HP:n manager-moodia, josta komennolla 'configure terminal' siirrytään konfiguraatiomoodiin. Konfigurointi on alatasoisen hyvin samankaltaista kuin HP:n ProVisionissa, mutta Ciscon käyttöjärjestelmä ei sisällä CLI:n kautta toimivaa valikkoa.

3.3 Juniper EX ja Junos-käyttöjärjestelmä

Nuorimpana tulokkaana kolmesta valitsemastani yhtiöstä Juniper on päässyt lyhyessä ajassa pitkälle tietoverkkolaitteiden kehityksessä. EX-kytkimet tulivat markkinoille vasta vuonna 2008, joskin ne perustuvat samaan Junos-käyttöjärjestelmään, joka on ollut Juniperin itse kehittämien verkkolaitteiden peruspilari yhtiön perustamisesta lähtien. EX-sarja sisältää yhdeksän eri tarkoituksiin sopivaa kytkintä, 12-porttisesta EX2200-C-kytkimestä modulaariseen EX9200-kytkimeen, jonka maksimiläpisyötöksi ilmoitetaan huikeat 13,2 Tbps. Perusmallissa EX2200-C:ssäkin sovittimet pystyvät 1Gbps nopeuteen toisin kuin Ciscon ja HP:n edullisimmissa malleissa, ja Juniper onkin keskittänyt voimavaroja korkeamman tasoluokan kytkinten valmistamiseen. (Juniper.net; wikipedia.org, Juniper EX-Series.)

Junos-käyttöjärjestelmä poikkeaa olennaisesti IOS:sta ja ProVisionista. Se on rakennettu FreeBSD:n päälle, ja root-käyttäjällä on pääsy FreeBSD:n komentokehoteeseen, jossa voi ajaa unix-komentoja. FreeBSD-tilasta pääsee normaaliin kytkimen komentokehoteeseen komennolla 'cli'. Toisin kuin muissa käyttöjärjestelmissä, Junosissa on mainitun FreeBSD-tilan lisäksi vain kaksi muuta komentotilaa: operational-moodi ja configuration-moodi. Ensin mainitussa tilassa voi tarkastella laitteen tilaa ja tehdä vianmäärittäystä, kun jälkimmäisessä voi ajaa konfiguraatiokomentoja, tarkastella konfiguraatiota lähemmin ja ajaa commit- ja rollback-komentoja aktiivisen konfiguraation muuttamiseksi. (Juniper TechLibrary, Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies; Wikipedia.org, Junos OS.)

Konfiguraationsa osalta Junos poikkeaa myös muista valmistajista. Kytkimen konfiguraatiossa on puumainen rakenne, joka Juniperin dokumentaatiossa jaetaan kolmeen osaan: runkoon, oksiin ja lehtiin kuten kuvan 1 esimerkistä käy ilmi. Konfiguraation ylin taso on juuritaso, sen alla on kourallinen runkoja, ja niiden alla enemmän oksia, ja lopulta lehdet. Kuva esittää protocols-rungon alta löytyvät oksat, ja ospf-oksan alta löytyvien alaoksien kautta lopulta hello-interval-lehden.



Kuva 1. Konfiguraation lausehierarkia (Juniper TechLibrary, Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies)

Junosin configuration-moodissa muokataan aina kandidaattikonfiguraatiota, eikä pelkää sen muokkaaminen muuta kytkimen sen hetkistä toimintaa. Konfiguraatio tulee muutosten käyttöön ottamiseksi ajaa aktiivisen konfiguraation päälle komennolla 'commit'. Käyttöjärjestelmän poikkeuksellisuus ulottuu myös konfiguraation versiohistorian ylläpitoon, ja konfiguraatioita tallennetaan automaattisesti peräti 50 kappaletta ennen kuin vanhimmat ylikirjoitetaan (Juniper TechLibrary, rollback).

Seuraavassa luvussa pureudun syvemmälle käyttöjärjestelmien syntaksiin ja filosofiaan, sekä erinäisiin kytkentäisen verkon tärkeimpiin ominaisuuksiin ja niiden konfigurointiin.

4 Konfigurointi ja yhteensopivuus

Huolimatta laitteiden konfiguroinnissa esiintyvistä suuristakin peruseroista sekä nimeämisessä että konfiguraation esitys- ja syöttötavassa perustuvat laitteiden tietokerroksen operaatiot pitkälti samoihin protokoliin ja standardeihin. Yhteisistä standardeista poikkeaa lähinnä Cisco useilla patentoiduilla verkkotekniikoillaan, mutta käytännön verkkosuunnittelussa nämä ovat aina vaihdettavissa muidenkin valmistajien laitteiden tukemiin yleisiin standardeihin. Kerroin edellisessä luvussa käyttöjärjestelmä kerrallaan kytkinten

eroavaisuuksista. Käytän tämän luvun alussa lyhyen hetken joidenkin eroavaisuuksien kertaamiseen, sillä on tärkeää ymmärtää tietyt perustavanlaatuiset erot, jotta voi helpommin pysyä mukana tulevissa alaluvuissa.

Toisin kuin Junosissa, Ciscon IOS:ssa ja HP:n ProVisionissa kaikki konfiguraatiomuutokset tulevat voimaan heti. Ciscolla ja HP:lla on käytössään kaksi eri konfiguraatiota, running-config ja startup-config. Startup-config on tallennettuna pysyvään muistiin, mutta running-config tallennetaan vain käyttömuistiin, joten se pyyhkiytyy kytkimen uudelleenkäynnistyksellä. Näin ollen konfiguraatio on tärkeä muistaa tallettaa startup-configiin muutosten jälkeen, mikäli muutosten halutaan olevan pysyviä. IOS:ssa tallennus tapahtuu joko komennolla 'write memory' tai 'copy running-config startup-config', joskin ensin mainittua komentoa Cisco on pyrkinyt ajamaan alas jo jonkun aikaa. ProVisionissa toimii pelkkä 'write memory'. Myös Junosissa on kaksi konfiguraatiota. Kun käyttäjä siirtyy configuration-moodiin, muokattavaksi luodaan aktiivisesta konfiguraatiosta työkopio: kandidaattikonfiguraatio. Komento 'commit' ajaa kandidaattikonfiguraation laitteen aktiiviseksi konfiguraatioksi pysyvään muistiin. Junos varastoi myös vanhoja konfiguraatioita yhteensä 50 kappaletta. (Juniper TechLibrary, Understanding How the Junos OS Configuration Is Stored.)

Suurin Cisco IOS:n ja HP ProVisionin välinen ero lienee niiden suhtautuminen VLAN- ja porttikonfiguraatioon. IOS:ssa kaikki VLAN-konfiguraatio tehdään porttikonfiguraatiossa, kun ProVisionissa VLANien alle määritellään, mitkä portit kuljettavat niiden liikennettä tagattuna ja mitkä ilman tagia. Ciscoon tottuneelle HP:n tapa käsitellä näitä määreitä voi olla hyvinkin vieras, ja sen suhteen Junos on paljon helppotajuisempi, sillä Junosissa porttikonfiguraation alle voidaan määritellä VLANit kuten Ciscossa.

Junosin syntaksissa on usein monta tapaa tehdä kytkimen peruskonfiguraatioita, varsinkin porttien konfiguraatiot ovat erittäin monipuolisia. Samoin Junos:n konfigurointitapah-tuman voi tehdä monella tavalla. Komento 'edit' antaa käyttäjän hypätä konfiguraatorun-golle tai sen oksille, aina alimmalle oksalle asti (ks. Kuva 1). Komennolla 'up' hypätään yksi oksa ylöspäin ja komennolla 'top' siirrytään suoraan konfiguraation juuritasolle. Konfiguraatiomuutoksia tehdäkseen käyttäjän ei kuitenkaan ole pakko hyppiä konfiguraation alatasoille, vaan kaikki komennot ovat suoritettavissa juuresta asti, sillä komentosyntaksi on samalla tavalla hierarkkinen. Ciscon ja HP:n kytkimissä on huomattavasti vähemmän puumaisuutta, mutta joitain tiettyjä alatasoja niidenkin konfiguroinnissa on hyvä tietää. Tämän insinööriyden teemaan liittyen tärkein IOS:n alaluokka on interface-konfiguraatiot.

Jotta portin konfiguraatiota voidaan muuttaa, täytyy ensin siirtyä interface-alatasolle sen portin tai porttijoukon alle, minkä asetuksia halutaan muuttaa. Vasta alatasolla voidaan tehdä muutoksia konfiguraatioon. HP:lla tärkeimpiin vastaaviin kuuluu VLAN-konfiguraatio. Joskin configure-moodissa voidaan tehdä suoraan muutoksia VLANien porttikonfiguraatioon, on vaihtoehtoinen tapa siirtyä VLAN-alatasolle ja tehdä muutokset suoraan sieltä.

Seuraavissa alaluvuissa käyn läpi kohta kohdalta kaikkiin kytkimiin päteviä peruskonfiguraatioelementtejä, ja niiden konfiguraatiosyntaksia kussakin tarkastelemassani kytkimessä. Esikonfiguraatio-otsikon alle liitän useita tavallisimpia asetuksia liittyen nimeämiseen ja etäyhteyksiin ja kytkimen tietoturvan koventamiseen.

4.1 Esikonfiguraatio

Kytkimen käyttöönotto ensimmäistä kertaa tapahtuu lähes poikkeuksetta konsolikaapelilla konsoliportin kautta. Jotta kytkimeen voi jatkossa kirjautua etäyhteydellä, tulee kytkimelle määritellä vähintään IP-osoite ja aliverkon peite, oletusyhdyskäytävä sekä riippuen kytkimestä ainakin yksi salasana. SSH-yhteyden sallimiseksi tarvitaan myös lokaa- listi luotava RSA-avain. Pakollisten konfiguraatioiden lisäksi annetaan kytkimelle isäntä- nimi, toimialue (domain), DNS- ja NTP-palvelimien osoitteet ja määritellään web-GUI- etäyhteydet pois käytöstä tietoturvan parantamiseksi. Kaikkien tässä esiteltävien konfi- guraatiomuutosten jälkeen on hyvä tallentaa konfiguraatio, etteivät tehdyt muutokset ka- toa uudelleenkäynnistyksen myötä.

Aivan aluksi on hyvä määritellä kytkimelle isäntänimi ja toimialue, DNS- ja NTP-palveli- mien osoitteet ja aikavyöhyke sekä poistaa web-GUI käytöstä. Nämä määrittelyt ovat hyvin yksinkertaisia ja komennot melkein itsestään selviä. Komentojen jälkeen tallen- taan konfiguraatio levyille. Tallennuksen komennot ja logiikan esittelen vain kerran, mutta tallennus on hyvä muistaa aina muutoksia tehdessään. HP:n Aruba L2-kytkimissä ei ole mahdollisuutta asettaa toimialuetta ja DNS-palvelinta, joten ne jäävät ProVisionin koh- dalla väliin. HP käyttää täyden NTP:n sijaan yksinkertaisempaa pakettien lukutapaa SNTP:tä, joka jättää NTP-paketeista lukematta drift-arvot ja on siten vähemmän luotet- tava. Ensin esittelen ProVisionin konfiguraation, sitten IOS:n ja lopuksi Junosin.

```

Switch# configure
Switch(config)# hostname HP_switch
HP_switch(config)# snmp
HP_switch(config)# snmp server < NTP-palvelimen IP-osoite >
HP_switch(config)# snmp unicast
HP_switch(config)# timesync snmp
HP_switch(config)# time timezone < aikavyöhyke minuutteina >
HP_switch(config)# no web-management
HP_switch(config)# exit
HP_switch# write memory

Switch> enable
Switch# configure terminal
Switch(config)# hostname CiscoSwitch
CiscoSwitch(config)# ip domain-name < toimialueen nimi >
CiscoSwitch(config)# ip name-server < DNS-palvelimen IP-osoite >
CiscoSwitch(config)# ntp server < NTP-palvelimen nimi tai IP-osoite >
CiscoSwitch(config)# clock timezone < aikavyöhyke >
CiscoSwitch(config)# no ip http server
CiscoSwitch(config)# no ip http secure-server
CiscoSwitch(config)# exit
CiscoSwitch# copy running-config startup-config

root@% cli
root@> configure
root@# set system host-name Jswitch
root@# set system domain-name < toimialueen nimi >
root@# set system name-server < DNS-palvelimen IP-osoite >
root@# set system ntp boot-server < NTP-palvelimen nimi tai IP-osoite >
root@# set system ntp server < NTP-palvelimen nimi tai IP-osoite >
root@# set system ntp time-zone < aikavyöhyke >
root@# delete system services web-management
root@# commit
root@Jswitch# exit
root@Jswitch>

```

Ennen hallinta-IP:n määrittelyä tulee kytkimiin asettaa salasanat. HP:ssa salasanan voi määrittää sellaisenaan tai käyttäjänimen kanssa operator- ja manager-käyttäjätasolle. Ciscossa salasanan voi määrittellä sellaisenaan etäyhteydelle tai luoda käyttäjiä, joille voidaan määrittellä eri pääsytaasoja. Lisäksi Ciscolla on käytössään enable-salasaana, jolla User EXEC -moodista pääsee Privileged EXEC -moodiin. Aaa-asetuksilla voidaan määrittellä User EXEC -moodin ohitus siten, että etäyhteyuskäyttäjä kirjautuu suoraan Privileged EXEC -moodissa. Junosissa on aina olemassa root-käyttäjä, jolla on rajaton pääsy kytkimen hallintaan. Lisäksi voidaan määrittää käyttäjiä neljällä eri pääsytaasolla: operator, read-only, super-user ja unauthorized. Luodaan kaikkiin kytkimiin käyttäjät korkeimmalla mahdollisella pääsyyllä ja asetetaan SSH-etäyhteys toimimaan.

ProVisionissa käyttäjä luodaan yhdellä komennolla. Käyttäjän luonti on yksinkertaista, sillä lokaalikäyttäjille määrittellään luodessa pääsytaaso, joka pätee kaikenlaiseen kirjautumiseen. Sen lisäksi on luotava RSA-avain SSH-yhteyttä varten ja enableitava SSH.

```

HP_switch(config)# password manager user-name < käyttäjänimi > plaintext
< salasana >
HP_switch(config)# crypto key generate ssh
HP_switch(config)# ip ssh

```

IOS:ssa määritellään aivan ensimmäiseksi enable-salasana, jotta etäkirjautuminen onnistuu. Enableoidaan ja määritellään seuraavaksi aaa-ryhmä 'default' päästämään käyttäjä suoraan Privileged EXEC -tilaan, minkä jälkeen luodaan korkeimman tason 15 käyttäjä. Tämän jälkeen luodaan 1024-bittinen RSA-avain SSH-yhteyttä varten. Kun kytkin on konfiguroitu SSH:ta varten, sallitaan SSH-yhteydet luodulla aaa-profiililla hallintayhteyttä varten: line vty:llä siirrytään terminaaliyhteyksien 0-15 alikonfiguraatioon. Määritellään yhteyksien tyypiksi pelkästään SSH tietoturvallisen tiedonsiirron vuoksi ja määritellään sisäänkirjautumisen autentikointi aaa-ryhmälle 'default'. (Catalyst 2960-X Switch Security Configuration Guide, Cisco IOS Release 15.0(2)EX.)

```

CiscoSwitch(config)# enable secret < enable-salasana >
CiscoSwitch(config)# aaa new-model
CiscoSwitch(config)# aaa authentication login default local
CiscoSwitch(config)# aaa authorization exec local
CiscoSwitch(config)# username < käyttäjänimi > privilege 15 password 0
< salasana >
CiscoSwitch(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
CiscoSwitch(config)# ip ssh version 2
CiscoSwitch(config)# line vty 0 15
CiscoSwitch(config)# transport input ssh
CiscoSwitch(config)# login authentication default

```

Junosissa määritellään ensin root-käyttäjälle salasana, minkä jälkeen estetään root-käyttäjän kirjautuminen muutoin kuin konsolin kautta. Luodaan lokaalikäyttäjä suurimmilla pääsyoikeuksilla. SSH-yhteys toimii oletuksena, mutta säädetään se toimimaan vain SSHv2-versiolla. Estetään vielä lopuksi telnet-yhteyksien muodostaminen tietoturvan parantamiseksi. (Garrett 2006; Juniper TechLibrary, Configuring SSH Service for Remote Access to the Router or Switch.)

```

root@Jswitch# set system root-authentication plain-text-password
New password:
Retype password:
root@Jswitch# set system services ssh root-login deny
root@Jswitch# set system login user < käyttäjänimi > class super-user
authentication plain-text-password
New password:
Retype new password:
root@Jswitch# set system services ssh protocol-version v2
root@Jswitch# delete system services telnet

```

Hallinta-IP-osoitteen määrittämiset voidaan tehdä joko suoraan portin asetuksiin, jolloin hallintayhteys toimii vain sen kytkinportin kautta, tai VLANin virtuaali-interfaceen, jolloin kaikkialta, mistä kyseinen VLAN on saavutettavissa, voi ottaa etäyhteyden kytkimeen. Esittelen ainoastaan jälkimmäisen vaihtoehdon, sillä ensimmäinen tapa varaa yhden sovitin pelkästään hallintayhteyden käyttöön. Hallintaosoitteen voi määrittää minkä tahansa VLANin virtuaali-interfaceen. Yksinkertaisuuden vuoksi käytämme oletus VLANia (VLAN1), sillä se on automaattisesti natiivi VLAN ja toimii oletuksena kaikissa kytkimen porteissa ilman dot1q-tagia.

HP ProVisionissa hallinta-IP-osoitteen määrittäminen on yksinkertaista. Ensimmäin siirrytään halutun VLANin alavalikkoon ja valikossa määritetään IP-osoite ja aliverkon peite yhdellä komennolla. Tämän jälkeen poistutaan VLAN-alavalikosta ja määritellään konfiguraation juureen oletusyhdyskäytävä.

```
HP_Switch# configure
HP_Switch(config)# vlan 1
HP_Switch(vlan-1)# ip address < IP osoite > < aliverkon peite >
HP_Switch(vlan-1)# exit
HP_Switch(config)# ip default-gateway < oletusyhdyskäytävän IP-osoite >
```

Ciscon IOS:ssa määrittäminen on lähes identtinen prosessi, paitsi että IP-osoite määritetään VLAN-interfacen alle eikä suoraan VLANin alle. Jos halutaan määrittää hallinta-IP-osoite VLANiin, jota ei vielä ole olemassa, tulee VLAN luoda ennen VLAN-interfacen määrittämisen tekemistä.

```
CiscoSwitch# configure terminal
CiscoSwitch(config)# interface vlan1
CiscoSwitch(config-if)# ip address < IP-osoite > < aliverkon peite >
CiscoSwitch(config-if)# exit
CiscoSwitch(config)# ip default-gateway < oletusyhdyskäytävän IP-osoite >
```

Junos ja kaikki EX-sarjan kytkimet ovat luonnostaan kykeneviä L3-operaatioihin, ja myös hallinta-IP-osoitteen määrittäminen on hiukan erilaista. VLAN1 on Junos:ssa nimeltään 'default', ja tätä nimeä käytetään myös VLAN-konfiguraatiossa. Konfiguraatiossa luodaan ensin VLAN-interfacelle yksikkö 1. Yksikkö voi olla mikä tahansa numero, mutta hyvän käytännön mukaisesti määritetään yksikön numero vastaamaan kyseisessä interfacessa käytettävää VLANia. Saman komennon perään voi lisätä suoraan protokollaperheen. Tällä kertaa käytetään perhettä 'inet', joka määrittelee yksikön käyttämään verkokerroksen protokollia ja perään määritellään IP-osoite ja desimaaliluku, joka kuvastaa aliverkon peitettä. Tämän jälkeen määritetään default VLANille (huom. Kuten

aiemmin mainittiin, default on Junosissa oletusarvoinen nimi oletus-VLANille eli VLAN1:lle) L3-interfaceksi juuri luotu VLAN-interfacen yksikkö 1. Tämän jälkeen määritellään vielä oletusyhdyskäytävä, eli Junosissa staattinen reitti ohjaamaan kaikki verkot oletusyhdyskäytävän IP-osoitteeseen.

```
user@Jswitch> configuration
user@Jswitch# set interfaces vlan unit 1 family inet address < IP-osoite/peite >
user@Jswitch# set vlans default l3-interface vlan.1
user@Jswitch# set routing-options static route 0.0.0.0/0 next-hop < oletusyhdyskäytävän IP-osoite >
```

Kytkimet ovat näiden määritteiden jälkeen enemmän tai vähemmän valmiita etähallittaviksi. Jotkin tekemäni määrytykset parantavat tietoturvaa, mutta näin vähällä koventamisella, jos millään määrällä, ei kytkimestä vielä täysin tietoturvallista saa. Etähallintaa varten säädettävät pääsilystat, ulkoverkoista tulevia yhteyksiä estävä palomuri ja erillinen, rajallisesti reitittyvä hallintaverkko ovat tärkeitä tietoturvallisen etähallinnan aikaansaamiseksi.

4.2 Sovittimet, portit, VLANit ja IEEE 802.1Q

Kytkimen keskeisin komponentti on Ethernet-portti eli sovitin, ja englanniksi interface. Käytän tässä tekstissä kaikkia kolmea siten, että pelkästään fyysistä laitetta kutsun sovittimeksi, konfiguraation kontekstissa käytän usein porttia ja joskus interfacea, jälkimmäinen useimmiten liitettyinä toiseen termiin kuten esimerkiksi VLAN-interface.

Ethernet-portin perusominaisuudet ovat nopeus ja dupleksisuus. Tavallisesti nopeus on joko 10 Mbps, 100 Mbps tai 1000 Mbps eli 1 Gbps. Nykyään on myös 10 Gbps- ja 40 Gbps-nopeuksisia portteja, mutta ne toimivat yleensä SFP:llä (small form-factor pluggable transceiver), eivätkä niin suuret nopeudet ole olennaisia tämän tutkielman kannalta. 10 Mbps portit ovat katoava luonnonvara, eikä niin hitaalle tiedonsiirrolle tänä päivänä juuri ole tarvetta. 100 Mbps on työssäni keskeisten kytkinperheiden edullisimpien mallien porttien nopeus lukuunottamatta Juniperin EX2200-C:tä, jossa on 1 Gbps:n portit. Portin dupleksisuus – paremman suomennoksen puutteessa – tarkoittaa kytkimen, portin sekä käytetyn protokollapinin kykyä käsitellä saapuvaa ja lähtevää liikennettä. Half-duplex-liikenne toimii vain toiseen suuntaan kerrallaan, eli kytkinportti osaa vain lähettää tai vastaanottaa tietoa. Tällöin on mahdollista syntyä pakettien törmäyksiä, kun

paketit kulkevat samaa linjaa pitkin. Full-duplex-liikenne toimii molempiin suuntiin samanaikaisesti jolloin törmäyksiä ei synny ja tosiasiallinen läpisyöttö on molempiin suuntiin portin nopeuden mukainen. 10 Mbps nopeudet toimivat alun perin ainoastaan half-duplex-tekniikalla, mutta nykyään full-duplexia voi käyttää kaikilla nopeuksilla. Itse asiassa half-duplex-tekniikkaa ei edes tueta 1 Gbps ja nopeammilla nopeuksilla. Mitään etuja half-duplex-tekniikan käytöllä ei ole. Se on yksinkertaisesti vanhentunut tekniikka, joka on hiljalleen katoamassa. Kytkinporteissa on ominaisuus automaattiseen nopeuden ja dupleksisuuden neuvotteluun, mutta se ei aina ole luotettava. Käytännössä virheitä tulee hyvin vähän, ja siksi automaattista neuvottelua usein käytetään virheiden mahdollisuudesta huolimatta.

Kytkemällä kytkimiä toisiinsa ethernet-kaapelilla saadaan aikaan LAN-verkko (local area network), jonka sisällä verkkoon liitetyt laitteet voivat keskustella keskenään. LAN-verkolle on tyypillistä, että kaikki siihen liitetyt koneet käyttävät samaa IP-aliverkkoa, jolloin verkkoliikennettä ei tarvitse reitittää. Tietoverkoissa, niin L3-verkkokerroksella kuin L2-siirtokerroksellakin käytetään erityistä broadcast-osoitetta, jonka avulla laitteet voivat kommunikoida jokaiselle verkossa olevalle laitteelle yhdellä kertaa. IP-tasolla broadcast-osoite on aliverkon viimeinen osoite, ja siirtokerroksen tasolla broadcast-liikenteen kohdeosoite on aina MAC-osoiteavaruuden viimeinen osoite (FF:FF:FF:FF:FF:FF). Laitteet, joihin yksi broadcast paketti kerralla lähetetään, muodostavat yhdessä broadcast-alueen. Siirtokerroksen broadcast-alue muodostaa siis käytännössä yhden LAN-verkon. Suurissa yritysverkoissa siirtokerroksen broadcast-alue voi muodostua niin suureksi, että sen koon rajoittaminen alkaa tulla tarpeelliseksi sekä liikenteen määrään, käytännön tehtävärajauksen, että myös tietoturvakäytänteiden vuoksi. (ISO/IEC7498-1 1994; Wikipedia, Virtual LAN, Broadcast address, OSI-malli.)

VLAN eli Virtual Local Area Network mahdollistaa LAN-verkon pilkkomisen segmentteihin, joiden välillä ei kytkentäisesti kulje liikennettä. Tietoverkkopioneeri Walter David Stancoskie kehitti jo 1980-luvulla mallin Ethernet-kehyksiin lisättävistä tageista, joskin niiden käyttötarkoitus oli siihen aikaan paljolti eri kuin nykyään. IEEE 802.1Q -standardi esitteli virallisesti Ethernet-VLANit ensimmäisessä painoksessaan vasta vuonna 2003. VLAN-tagin tai dot1q-tagin on käytännössä numero, jolla erotetaan L2-verkko toisesta saman fyysisen verkon päällä olevasta L2-verkosta. Kun kytkimen porttiin kytketään isäntälaitte, portti on tyypillisesti access-tilassa, jolloin portille voi määrittää yhden VLANin, missä portti liikennöi. ProVision ei tunne käsitettä access-tila, vaan siinä määritellään VLANeille liikennöintiportit joko tagged- tai untagged-tilaan. Untagged-VLAN portissa

tarkoittaa jokseenkin samaa kuin access-portti IOS:ssa ja Junosissa. Access-portti – tai untagged-portti – tarkoittaa, että portissa kulkevalle liikenteelle ei aseteta dot1q-tagia, vaan kytkin käsittelee konfiguraationsa perusteella portin liikennettä määritellyn VLANin liikenteenä. Access-portin vastaparina toimii trunk-portti, jonka ydinominaisuus on usean eri VLANin liikenteen kuljettaminen dot1q-tagattyna. Termiä trunk käytetään ProVisionissa täysin eri asiaan kuin muiden valmistajien järjestelmissä, eikä näitä tule sekoittaa. HP:n järjestelmässä puhutaan vain tageista, eikä porttien tyyppejä määritellä erikseen. Jos portille määritellään tagged-VLANeja sekä yksi untagged-VLAN, vastaa jälkimmäinen Ciscon ja Juniperin native VLAN -käsitettä. (wikipedia.org, Virtual LAN.)

Määritetään aivan ensimmäiseksi portit 11–20 sekä 24 100Mbps full-duplex-tilaan. Luodaan seuraavaksi kytkimille VLAN2 nimellä 'tuotanto', VLAN10 nimellä 'vieras' ja VLAN99 nimellä 'natiivi', asetetaan portit 11–15 tuotanto-VLANiin sekä portit 16–20 vieras-VLANiin access-porteiksi (HP:n untagged) ja tehdään portista 24 trunk-portti (HP:n tagged), joka kuljettaa sekä VLAN2- että VLAN10-liikennettä dot1q-tageilla ja jonka natiivi VLAN on VLAN99. Nimetään portit VLANin mukaan konfiguraation selkeyttämiseksi.

HP ProVision

Porttikonfiguraation alle tehdään HP:lla ainoastaan dupleksisuuden ja nopeuden valinta ja portin nimeäminen. Kun portteihin tulevat VLANit tiedetään ennakkoon, voidaan portit nimetä jo nyt. ProVisionissa interface-määrittämiä voi tehdä komento kerrallaan konfiguraation juuresta tai siirtyä interface-konfiguraatiotilaan ja suorittaa lyhyemmät komennot sieltä. Huomaa jälkimmäisen speed-duplex säädön porttilista. Siinä käytetään sekä joukon määrettä että erotinta, ja portit, joihin kyseinen lista pätee, ovat 16, 17, 18, 19, 20 ja 24.

```
HP_switch(config)# interface 11-15
HP_switch(eth-11-15)# speed-duplex 100-full
HP_switch(eth-11-15)# name tuotanto
HP_switch(eth-11-15)# exit
HP_switch(config)# interface 16-20,24 speed-duplex 100-full
HP_switch(config)# interface 16-20 name vieras
HP_switch(config)# interface 24 name trunk
```

Seuraavaksi luodaan uudet VLANit ja määritellään niitä käyttävät portit VLAN-konfiguraatioon. VLAN-määrittäykset toimivat kuten interface-määrittäyksetkin, eli joko suoraan konfiguraation juuresta tai VLAN-konfiguraatiotilasta. Huomaa portin 24 eli dot1q-tagejä käyttävän portin konfiguraatio.

```

HP_switch(config)# vlan 2 name tuotanto
HP_switch(config)# vlan 2 untagged 11-15
HP_switch(config)# vlan 2 tagged 24
HP_switch(config)# vlan 10
HP_switch(vlan-10)# name vieras
HP_switch(vlan-10)# untagged 16-20
HP_switch(vlan-10)# tagged 24
HP_switch(vlan-10)# exit
HP_switch(config)# vlan 99 name natiivi
HP_switch(config)# vlan 99 untagged 24

```

Cisco IOS

Mikäli HP:n VLAN-konfiguraatio tuntui loogiselta, tuntuu Ciscon ja Juniperin konfiguraatio todennäköisesti vieraalta. Sama pätee myös toisin päin. IOS:ssa kaikki tässä aluvussa konfiguroitavat toiminnallisuudet tehdään porttikonfiguraation alle, lukuun ottamatta itse VLANien luontia ja nimeämistä. Ciscon kytkimissä on erityinen VTP-protokolla (VLAN Trunking Protocol), jonka avulla VLAN-konfiguraation voisi osittain automatisoida siten, että yksi verkkolaite lähettäisi muille verkkolaitteille tiedot siitä, mitä VLANeja verkossa kuuluu milloinkin olla. Käytännössä sen käyttö on hyvin harvinaista, ja hyvän konfiguraatitavan mukaisesti laitetaan VTP transparent-moodiin, jolloin se ei häiritse VLANien konfigurointia. Luodaan sen jälkeen VLANit ja käydään sitten porttikonfiguraatioiden kimppuun. Portteja valitessa on tiedettävä, minkä tyyppinen kytkin on kyseessä ja sitä myöten, kuinka kytkinportit on nimetty kyseisessä kytkimessä. Interfacen tyyppi voi olla joko FastEthernet tai GigabitEthernet, ja numero sen perässä voi olla esimerkiksi portin 11 tapauksessa muotoa 1/0/11 tai 0/11, tai jotain muuta. Helpoin tapa tarkistaa tämä on katsoa interface-listaus Privileged EXEC -moodissa komennolla 'show interfaces description'.

```

CiscoSwitch(config)# vtp mode transparent
CiscoSwitch(config)# vlan 2
CiscoSwitch(config-vlan)# name tuotanto
CiscoSwitch(config-vlan)# exit
CiscoSwitch(config)# vlan 10
CiscoSwitch(config-vlan)# name vieras
CiscoSwitch(config-vlan)# exit
CiscoSwitch(config)# vlan 99
CiscoSwitch(config-vlan)# name natiivi
CiscoSwitch(config-vlan)# exit
CiscoSwitch(config)# interface range < interfacen tyyppi > (#/#)/11 – 15
CiscoSwitch(config-if)# speed 100
CiscoSwitch(config-if)# duplex full
CiscoSwitch(config-if)# switchport mode access
CiscoSwitch(config-if)# switchport access vlan 2
CiscoSwitch(config-if)# description tuotanto
CiscoSwitch(config-if)# exit
CiscoSwitch(config)# interface range < interfacen tyyppi > (#/#)/16 – 20

```

```

CiscoSwitch(config-if)# speed 100
CiscoSwitch(config-if)# duplex full
CiscoSwitch(config-if)# switchport mode access
CiscoSwitch(config-if)# switchport access vlan 10
CiscoSwitch(config-if)# description vieras
CiscoSwitch(config-if)# exit
CiscoSwitch(config)# interface < interfacen tyyppi > (#/#)/24
CiscoSwitch(config-if)# switchport mode trunk
CiscoSwitch(config-if)# switchport trunk allowed vlans 2 10
CiscoSwitch(config-if)# switchport trunk native vlan 99
CiscoSwitch(config-if)# description trunk

```

Huomattavaa on, kuinka paljon enemmän komentoja Ciscon vastaava konfiguraatio vaatii, vaikka käytin 'interface range' -komentoa access-porttien konfigurointiin. Exit-komennot eivät ole pakollisia, vaan interface-konfiguraatiosta voi siirtyä suoraan toiseen interface-konfiguraatioon halutessaan. Jätin ne paikalleen, jotta konfiguraation osiot erottuivat paremmin.

Juniper Junos

Juniper on tehnyt porttikonfiguraatiosta vielä Cisconkin konfiguraatiota monitasoisempaa, kuten Junosin tapauksessa muutenkin. Interfaces-rungon alta valitaan portti, minkä alle tehdään fyysisten ominaisuuksien määrytykset ja luodaan loogiset portit eli yksiköt (unit). Jos yksiköitä ei tarvita montaa, tavataan portin määrytykset tehdä yksikön 0 alle. Yksikön alle määritellään protokollaperhe, kytkentäisen portin tapauksessa family ethernet-switching. Seuraavan oksan konfiguraatio vaihtelee protokollaperheen valinnan mukaan. Ethernet-switching protokollaperheen alle määritellään, onko portti access- vai dot1q-portti, sekä mahdollinen natiivi VLAN ja portin käyttämät VLANit. Porttien konfigurointiin ei Junosissa ole helpottavaa usean portin valintatyökalua kuten IOS:ssa ja Provisionissa, mutta Juniper on kiertänyt asian toista kautta. Junosissa voi luoda interface-range-konfiguraatioelementtejä, joiden alle voi määritellä siihen kuuluvien porttien asetukset kerralla. (Juniper TechLibrary.)

Luodaan ensin VLANit ja sen jälkeen määritellään porttiasetukset. Sovellan interface-range-objektin käyttöä, sillä yksittäisten komentojen määrä nousisi turhan suureksi yksi portti kerrallaan konfiguroidessa. Esittelen ensin VLAN2:n kohdalla 'suoran tavan', jossa konfiguraation juuresta annetaan kaikki komennot, ja sen jälkeen VLAN10:n kohdalla käytän hyväkseni konfiguraation puumaisuutta ja mahdollisuutta "hyppiä oksalta oksalle" konfiguraatiossa.

```

root@Jswitch# set vlans tuotanto vlan-id 2
root@Jswitch# set vlans vieras vlan-id 10
root@Jswitch# set vlans natiivi vlan-id 99
root@Jswitch# set interfaces interface-range tuotanto member-range ge-1/0/11
to ge1/0/15
root@Jswitch# set interfaces interface-range tuotanto ether-options speed 100m
root@Jswitch# set interfaces interface-range tuotanto ether-options link-mode
full-duplex
root@Jswitch# set interfaces interface-range tuotanto unit 0 family
ethernet-switching vlan members tuotanto
root@Jswitch# set interfaces interface-range tuotanto description tuotanto
root@Jswitch# edit interfaces interface-range vieras
[interfaces interface-range vieras]root@Jswitch# set member-range ge-1/0/16 to ge-1/0/20
[interfaces interface-range vieras]root@Jswitch# set ether-options speed 100m
[interfaces interface-range vieras]root@Jswitch# set ether-options link-mode full-duplex
[interfaces interface-range vieras]root@Jswitch# set unit 0 family ethernet-switching vlan
members vieras
[interfaces interface-range vieras]root@Jswitch# set description vieras
[interfaces interface-range vieras]root@Jswitch# top
root@Jswitch# set interfaces ge-1/0/24 ether-options speed 100m
root@Jswitch# set interfaces ge-1/0/24 ether-options link-mode full-duplex
root@Jswitch# set interfaces ge-1/0/24 unit 0 family ethernet-switching
port-mode trunk
root@Jswitch# set interfaces ge-1/0/24 unit 0 family ethernet-switching vlan
members [ tuotanto vieras ]
root@Jswitch# set interfaces ge-1/0/24 unit 0 family ethernet-switching
native-vlan-id 99
root@Jswitch# set interfaces ge-1/0/24 description trunk

```

Näiden määrittelyjen toiminnallisuus on sellainen, että laitteet tuotanto-VLANissa eli portteissa 11-15 pystyvät keskustelemaan keskenään, mutta eivät vieras-VLANissa eli portteissa 16-20 olevien laitteiden kanssa. Sama pätee toisin päin, eli portit 16-20 keskustelvat keskenään, mutta eivät porttien 11-15 kanssa. Portissa 24 kulkevat molemmat VLANit ja natiivi VLAN 99 ilman dot1q-tagia. Jos kytkin ja molemmat VLANit ovat yhteydessä reitittävään laitteeseen, ja kyseisten VLANien verkot on määritelty reititettäväksi avoimesti, voivat eri VLANeissa olevat koneet keskustella keskenään, mutta liikenne kulkee aina reitittävän laitteen kautta. Samassa VLANissa olevat laitteet keskustelvat suoraan kytkentäisesti. Portit määriteltiin staattisesti 100 Mbps ja full-duplex-asetuksin, joten vastapään täytyy pystyä samanlaiseen konfiguraatioon – ja mielellään staattisesti, koska automaattisen neuvottelun kanssa suositellaan, että molemmat päät neuvottelevat automaattisesti.

4.3 Linkkien kanavointi

Kytkinverkon tärkeimpiä linkkejä on monesti tapana vahvistaa linkkejä yhdistämällä eli kanavoimalla. Tämä tapahtuu vetämällä useamman kuin yhden kaapelin kytkimeltä toiselle ja yhdistämällä portit loogisesti kytkimen konfiguraatiossa, jotta verkkoon ei synny silmukkaa. Linkkien kanavointi voi mahdollistaa suuremman kaistanleveyden kytkinten välillä, ja luo redundanttisuutta kytkinten väliseen yhteyteen. Linkkien kanavointiin voidaan käyttää neuvotteluprotokollaa tai se voidaan tehdä ilman sitä. Neuvotteluprotokollia on kaksi, joista toinen on Ciscon oma, käytännössä legacy-protokollaksi jäänyt PAgP. Toinen, yleisimmin käytetty protokolla on LACP, joka perustuu IEEE 802.3ad -standardiin. (EtherChannel considerations 2010.)

Neuvotteluprotokollien etu on vian- ja virheensietokyky, ja toisaalta haittana on pieni viive portin ylösnostossa ja toisaalta pieni ylimääräisen kaistan tarve protokollaa ajettaessa. Ilman protokollaa kanavoidut linkit nousevat toimintaan käytännössä yhtä nopeasti kuin kanavoimattomat linkit, eikä ohjausprotokolla luo kaistantarvetta, mutta tällaisen asetelman konfigurointi on tarkempaa ja virhelyönti saattaa rikkoa yhteyden kokonaan. (Frazier ym. 2007; EtherChannel considerations 2010.)

Kaikki kolme kytkinvalmistajaa käyttävät eri nimitystä linkkien kanavoinnista. HP:n sanastosta löytyy ”port trunking” eli ”trunkkaus”, Cisco käyttää käsitteitä channel-group, port channel -interface eli porttikanava ja EtherChannel, kun taas Juniper puhuu dokumentaatioissaan Aggregated Ethernet -interfaceista ja link aggregation groupeista (LAG). Kaikki nämä termit tarkoittavat enemmän tai vähemmän samaa, ja eri valmistajien versioihin pätevät samat lainalaisuudet ilman kontrolliprotokollaa ja LACP:n kanssa yhdistäessä. Portteja kanavoidessa on tärkeää luoda laitteille konfiguraatiot tai määritellä portteihin shutdown- tai disable-komento ennen kaapelien kytkemistä, jotta vältetään broadcast-myrsky. Mikäli spanning-tree konfiguraatio on kunnossa, ei myrskyjä pitäisi syntyä, mutta siitä aiheesta kerron enemmän luvussa 4.4. (HP Series 2530 Switches Management and Configuration Guide 2012; Juniper Techlibrary, Aggregated Ethernet Interfaces Overview, luettu 27.1.2017; Cisco Layer 2 Configuration Guide, Configuring EtherChannels, luettu 27.1.2017.)

HP ProVision

Porttikanavan eli "trunkin" voi konfiguroida HP ProVisionissa joko staattisesti tai dynaamisesti. Staattinen porttien kanavointi tehdään konfiguraation perustasolla yhdellä komennolla. Komento luo toisessa argumentissa määritellyn trk-interfacen, johon liitetään ensimmäisen argumentin portit. Porttilistauksessa käytetään pilkkua erottimena ja viivaa joukon määritteenä. Kolmas ja viimeinen argumentti määrittelee, käytetäänkö LACP-protokollaa vai luodaanko protokollaton trunk-kanava. LACP:lle tyypillistä aktiivi-passiivi-valintaa ei staattisessa porttikanavassa tehdä, sillä staattisuuden vuoksi LACP neuvotellaan aina ja poikkeuksetta. Staattisen porttikanavan etuihin voi lukea sen kyvyn käsitellä dot1q-tageja, jolloin usean VLANin kuljettaminen staattisessa porttikanavassa konfiguroidaan samaan tapaan kuin mikä tahansa portin VLAN-konfiguraatio. (HP Series 2530 Switches Management and Configuration Guide 2012.)

```
HP Switch(config)# trunk < porttilistaus > < trk1 ... trk24 > < trunk | lacp >
```

Dynaamisen porttikanavan voi ProVisionissa luoda niin ikään yhdellä komennolla. Tämä komento luo automaattisesti numeroidun dynaamisen trunkin: dyn-portin. Ensimmäinen argumentti toimii samoin kuin staattisen trunkin porttilistausargumentti ja aktiivi-passiivi-valinta liittyy LACP-standardin mukaisiin neuvottelupositioihin: aktiivimoodi pyrkii neuvottelemaan LACP-moodin, kun taas passiivimoodi ottaa sen vastaan muttei neuvottele sitä aktiivisesti. LACP jää neuvottelematta, jos molemmat kytkimet ovat passiivimoodissa tai toisessa päässä ei ole ollenkaan LACP-konfiguraatiota. Tällöin portti jää itsenäiseen moodiin, eikä osallistu porttikanavaan, mutta voi silti kuljettaa liikennettä normaalisti. Dynaaminen porttikanava voi sellaisenaan kuljettaa vain oletus-VLANia ilman dot1x-tagia. Jos dynaamisen porttikanavan läpi on tarkoitus siirtää monen VLANin liikennettä, tarvitaan GVRP-protokollaa. GVRP ei kuitenkaan sisälly tämän insinööriyön laajuuteen. (HP Procurve Switch Series - LACP: Static vs Dynamic (Explained/Configuration), luettu 28.1.2017; HP Series 2530 Switches Management and Configuration Guide 2012.)

```
HP_Switch(config)# interface < porttilistaus > lacp < active | passive >
```

HP ProVision -käyttöjärjestelmä sisältää myös valikkopohjaisen konfiguraatiomenetelmän CLI:n sisällä. Sen kautta on myös mahdollista konfiguroida ainakin staattisia trunk-

keja sekä LACP-protokollalla että ilman. Valikon kautta konfigurointi ei kuulu tämän insinööriyden laajuuteen. (HP Series 2530 Switches Management and Configuration Guide 2012.)

Cisco IOS

Toisin kuin HP ProVisionissa, Ciscon käyttöjärjestelmässä trunk tarkoittaa aivan muuta kuin porttikanavaa, eikä näitä tule sekoittaa keskenään. IOS käyttää porttiryhmästä nimitystä channel-group, virtuaali-interfacesta nimitystä port channel ja näiden muodostamasta kokonaisuudesta yleisnimitystä EtherChannel. Porttikanava konfiguroidaan Ciscoissa aina siten, että jokaisen siihen osallistuvan portin konfiguraatioon määritellään channel-group-komennolla porttikanavan numero ja moodi. Moodivalinnalla määritetään porttikanavan tyyppi ja mahdollisen protokollan tila. Valinta 'on' määrittää kanavan toimimaan ilman protokollaa, ja active tai passive määrittää LACP:n sekä sille tilan. Näiden valintojen lisäksi on mahdollista konfiguroida valinnat desirable tai auto, jotka kuvastavat PAgP-protokollan tiloja. PAgP on kuitenkin Ciscon oma protokolla, jota muut kytkinvalmistajat eivät tue, joten se jää lyhyeksi maininnaksi tämän insinööriyden osalta. Porttikanava-asetuksen lisäksi valitaan kytkinportin moodiksi joko access tai trunk. Jos valitaan access-portti, tulee konfiguroida myös VLAN-numero. Trunk-portiksi konfiguroidessa voidaan valita natiivi VLAN. VLAN-konfiguraation tulee olla kaikissa porttikanavaan osallistuvissa porteissa identtinen, jotta porttikanava toimii oikein. Konfiguroitaessa useita vierekkäisiä portteja yhdeksi porttikanavaksi voidaan käyttää interface range -komentoa, joka valitsee useita portteja konfiguroitavaksi kerralla. Porttiryhmä konfiguroidaan syntaksilla porttityyppi aloitusportti – lopetusportti (esim. FastEthernet1/0/1 – 4). (Cisco Layer 2 Configuration Guide, Cisco IOS Release 15.2(2)E (Catalyst 2960-X Switch), Configuring EtherChannels.)

```
CiscoSwitch(config)# interface (range) < portti | porttiryhmä >
CiscoSwitch(config-if)# switchport mode < access | trunk >
(CiscoSwitch(config-if)# switchport access vlan < vlan-numero >)
(CiscoSwitch(config-if)# switchport trunk native vlan < vlan-numero >)
CiscoSwitch(config-if)# channel-group < numero > mode < on | active | passive >
```

Channel-groupin määrittäminen yhteen tai useampaan porttiin luo dynaamisesti virtuaalisen portchannel-interfacen, joka toimii kytkinverkossa kuin fyysinen sovitin. Kun porttikanava konfiguroidaan trunkiksi, voidaan sallittujen VLANien lista tehdä kahdella tavalla: joko jokaiseen porttikanavaan osallistuvaan porttiin erikseen identtinen VLAN-lista tai vain kerran portchanneliin. Nähdäkseni paras käytäntö on konfiguroida sallittujen

VLANien lista portchanneliin, sillä mahdollisten muutosten teko listaan on siten huomattavasti yksinkertaisempaa. Portchannelissa listaa muokattaessa lista päivittyy myös siihen liitettyjen porttien konfiguraatioon sillä varauksella, että niiden tulee olla tyhjiä tai sisältää tasan sama informaatio kuin portchannelin määritteissä. (Cisco Layer 2 Configuration Guide, Cisco IOS Release 15.2(2)E (Catalyst 2960-X Switch), Configuring EtherChannels.)

Juniper Junos

Kolmannella kytkinvalmistajalla on luonnollisesti kolmas tapa nimetä porttien kanavointiin liittyvä termistö. Porttikanavasta käytetään Juniperin dokumentaatioissa nimitystä LAG eli link aggregation group. Porttikanavaa edustava virtuaali-interface on aggregated ethernet (ae). Junos-käyttöjärjestelmässä LAG:n konfigurointi aloitetaan asettamalla ae-interfacejen määrä. Näiden virtuaaliporttien numerointi alkaa aina nolasta, joten esimerkiksi käytetään ae0-sovitinta. Tämän jälkeen liitetään yksi tai useampi portti ae-interfaceen. Muiden valmistajien porttikanavista poiketen Juniper antaa mahdollisuuden määrittellä porttikanavan nopeuden ae:n tasolla sekä minimimäärän fyysisiä linkkejä joiden täytyy olla toimintatilassa, jotta porttikanava merkitään toimivaksi. Ae:lle määritellään protokollaperhe, L2-kytkimen tarkoituksiin aina ethernet-switching. (Juniper TechLibrary.)

```
user@Jswitch# set chassis aggregated-devices ethernet device-count < numero
>
user@Jswitch# set interfaces < fyysinen sovitin > ether-options 802.3ad ae0
(user@Jswitch# set interfaces ae0 aggregated-ether-options lacp <active | pas-
sive>)
(user@Jswitch# set interfaces ae0 aggregated-ether-options minimum-links <nu-
mero>)
(user@Jswitch# set interfaces ae0 aggregated-ether-options link-speed <nop-
eus>)
```

Junos antaa useita mahdollisuuksia VLAN- ja dot1q-konfigurointiin. Yhden ae:n sisään voi konfiguroida yksiköitä sekä access- että trunk-moodiin. Käytän yksinkertaisuuden vuoksi yhden yksikön konfiguraatiota kuvaamaan sekä trunkin että access-portin esimerkkikonfiguraatiot. Molemmissa vaihtoehdoissa käytetään ethernet-switching protokollaperhettä. Access-portti on oletuskonfiguraatio, joten ainoastaan VLAN täytyy määrittää.

```
user@Jswitch# set interfaces ae0 unit 0 family ethernet-switching vlan members
<vlan-nimi>
```


Trunk-portin konfiguraatiossa täytyy määrittää ensin portti trunk-moodiin ja sen jälkeen määrittellä sallitut VLANit.

```
user@Jswitch# set interfaces ae0 unit 0 family ethernet-switching port-mode
trunk (native vlan-id < vlan-id >) vlan members [ välilyönnillä eroteltuna sallittujen
VLANien nimet tai ID:t ]
```

Dot1q-tagien lukemisen voi määrittää Junosissa myös portin pääoksalla. Tällöin voidaan käyttää useita yksiköitä, jos halutaan kytkimen käsittelevän eri VLAN-tagillä tulevaa liikennettä eri tavoin. Tällaiset konfiguraatiot ovat harvoin tarpeisiin soveltuvia, eikä tässä opinnäytetyössä niitä kata. (Juniper TechLibrary; Configuring VLANS and Trunkin on the EX-series Switch.)

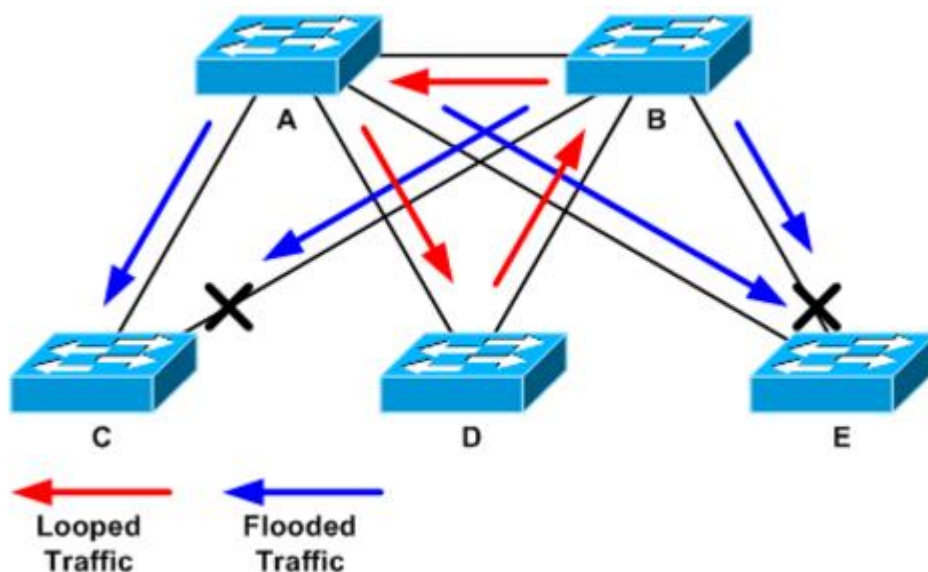
4.4 Spanning tree

Algorhyme

```
I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree which must be sure to span.
So packets can reach every LAN.
First the Root must be selected
By ID it is elected.
Least cost paths from Root are traced
In the tree these paths are placed.
A mesh is made by folks like me
Then bridges find a spanning tree.
```

- Tohtori Radia Perlman

Kun kytkinverkkoa laajennetaan ja redundanttisia linkkejä kytkimien välillä lisätään, alkaa syntyä kytkinverkolle tyypillisiä loopppeja ja niistä aiheutuvia broadcast-myrskyjä. Loopppeja syntyy, koska kytkentäisessä verkossa broadcast-paketti lähetetään aina kaikkiin portteihin paitsi siihen, josta liikenne tuli, eikä siirtokerroksen pakettikehys sisällä time-to-live arvoa samoin kuin IP-paketit. Näin jo kolme kytkintä voi muodostaa loopin.



Kuva 2. Looppi lähiverkossa (Troubleshooting STP on Catalyst Switches Running Cisco IOS System Software)

Kuten kuvasta 2 käy ilmi, ei ongelma rajoitu pelkästään loopin muodostaviin kytkimiin, vaan sama kiertävä paketti lähetetään myös kaikille muille kytkimissä kiinni oleville laitteille joka kerralla, kun paketti tulee niiden viereisille laitteille. Nämä laitteet puolestaan lähettävät sitä yhä edelleen eteenpäin, ja koko verkko täyttyy broadcast-liikenteestä. Paketteja tapaa kertyä looppiin jatkuvasti myös lisää, joten ongelma eskaloituu itsestään ja pian verkko voi olla käyttökelvottomassa tilassa, kun kaikki kapasiteetti käytetään näiden looppaavien pakettien ja niitä seuraavan myrskyn hyväksi.

Sun Microsystemsillä verkkoinsinöörinä tänäkin päivänä työskentelevä tietojenkäsittelytieteiden tohtori Radia Perlman kehitti tällaisten kytkinkonfiguraatioiden varalle vuonna 1992 patentoidun spanning tree -protokollan (Brachmann 2016). Spanning tree -protokolla eli STP toimii pitkälti niin kuin kehittäjänsä luvun alussa olevassa runossa kertoo. Ensin valitaan juurisilta, josta puurakenne versoo. Sitten lasketaan lyhyimmät tai 'halvimmat' (eng. least cost) reitit juurisillasta jokaiseen spanning treehen osallistuvaan laitteeseen, ja redundanttiset yhteydet, jotka eivät tule valituksi lyhyimpien reittien joukkoon, blokataan. Juurisilta valitaan 'bridge-ID:n' perusteella, joka on kaksiosainen luku. Ensimmäinen, merkitsevämpi osa määritetään konfiguraatiossa, ja se on 4096:n kertaluku kertoimella 0 – 16. Toisen osan muodostaa kytkimen kanta-MAC-osoite. Ensimmäisen osan oletusarvo on 32768 eli kerroinluku 8. Juurisillaksi valitaan se kytkin, jolla on pienin bridge-ID. Kytkinverkkoon liitetyt kytkinportit saavat 'Port Path Cost' -arvon, joka määrittyy oletuksena linkin nopeuden ja viimekädessä portin numeron mukaan. Jokainen

spanning treehen osallistuva kytkin saa 'Root Path Cost' -arvon, joka määrittää sen loogisen lyhyimmän etäisyyden juurisillasta. 'Root Path Cost' -arvo on juurisillan ja kytkimen portin välisten 'Port Path Cost' -arvojen summa, eli käytännössä 'Port Path Cost' + vierisen kytkimen 'Root Path Cost'. Mikäli useita kytkimen portteja osallistuu spanning treehen, valitaan kytkimen 'Root Path Cost' -arvoksi pienin arvo, ja valitaan sen arvon omistava kytkinportti juuriportiksi. Loput portit ovat joko redundanttisia portteja tai jonkun muun kytkimen juuriportin vastaportteja. (IEEE802.1D 2004, 139, 153, 159.)

Spanning treen kontekstissa portilla voi olla viisi erilaista tilaa. Spanning treen laskennan ja neuvottelun aikana kytkimet ovat ensin kuuntelu- eli 'Listening-tilassa'. Tämän tilan aikana kytkimet lähettävät toisilleen tietoa bridge-ID:stään ja toimivat tämän tilan ajan kuin olisivat juurisilloja. Liikennettä ei vielä välitetä verkossa. Oletusaika kuuntelutilalle on 15 sekuntia, minkä jälkeen kytkimet siirtyvät oppimis- eli 'Learning-tilaan'. Tämäkin tila on aktiivisena 15 sekuntia, eikä liikennettä vielääkään välity verkossa, mutta kytkin ottaa vastaan paketteja ja lisää niiden MAC-osoitteita CAM-tauluunsa, eli opettelee niitä. Vasta näiden jälkeen alkaa normaali liikenne kulkea verkossa, ja portit siirtyvät joko forwarding- tai blocking-tilaan riippuen niiden asemasta spanning treessä. Viides tila on disabled, jolloin portti on manuaalisesti poistettu käytöstä verkossa. (Juniper TechLibrary.)

Perinteisen STP:n ensimmäinen korvaaja oli rapid spanning tree -protokolla, RSTP. Sen etuna oli nopeampi konvergenssi, sillä listening-, learning- ja blocking-tilat yhdistettiin yhdeksi discarding-tilaksi, ja kolme kahden sekunnin välein lähetettävää hello-pakettia riittivät verkon uudelleenjärjestämiseksi. RSTP:n haastajaksi nousi multiple spanning tree -protokolla, joka määriteltiin IEEE 802.1Q standardissa vuonna 2005. Nimensä mukaisesti se tukee useamman spannin treen luomista yhteen verkkoon, ja liikenteen jaottelua näiden instanssien välille VLANien perusteella. Yhteen spanning tree -instanssiin voi liittää useampia VLANeja, ja verkon voi jakaa myös moneen alueeseen, minkä perusteella spanning treet rakentuvat. (wikipedia.org, Multiple Spanning Tree Protocol.)

MST:n määrittäminen on kaikista spanning tree -versioista monimutkaisinta, mutta yksinkertaisen spanning tree -konfiguraation rakentaminen ei ole vaikeaa. Kytkimien määrittäessä on kiinnitettävä huomiota siihen, että MST:n alue-, instanssi-, nimi- ja revision-määrytykset tulee olla identtisiä, jotta kytkimet osallistuvat saman puun rakentamiseen. Määrytykset on hyvä tehdä siten, että ennen spanning treen käyttöönottoa kaikki muu konfiguraatio on oikein, eli oikea kytkin valitaan juurisillaksi ja vain halutut portit

osallistuvat neuvotteluun. Jos portin ei odoteta osallistuvan spanning treehen, se laiteetaan usein edge-moodiin, jolloin siihen ei lähetetä STP-paketteja. Ciscon kytkimissä tätä kutsutaan nimellä PortFast. MST-määritykset vaativat vähintään alueen nimen, instanssin numeron, revision-numeron sekä instanssiin osallistuvat VLANit. Annetaan alueelle nimeksi 'verkkoalue', instanssin sekä revisionin numeroiksi 1, ja instanssiin osallistuvat VLANit 1, 2, 10 ja 99. Lisäksi määritellään portit 11-20 edge-porteiksi. Vasta kaikkien näiden määritysten jälkeen käynnistetään spanning tree -operaatio.

HP ProVision

ProVisionin määritykset tehdään suoraan konfiguraation juuresta. Yksittäiset määritykset ovat helppolukuisia, ja edge-portteja myöten kaikki määritellään spanning-tree -komennon alla.

```
HP_switch(config)# spanning-tree config-name verkkoalue
HP_switch(config)# spanning-tree config-revision 1
HP_switch(config)# spanning-tree instance 1 vlan 1 2 10 99
HP_switch(config)# spanning-tree priority 0
HP_switch(config)# spanning-tree 11-20 admin-edge-port
HP_switch(config)# spanning-tree
```

Cisco IOS

Cisco on määritellyt MST:lle oman konfiguraatiotilansa, jonka alla spanning tree -konfiguraatio tehdään. Asetukset tulevat voimaan vasta, kun MST-konfiguraatiotilasta poistutaan exit-komennolla. Juurisillan valitsemisen voi IOS:ssa tehdä valitsemalla instanssi-kohtaisesti ensisijainen juurisilta. Toiseksi paras juurisiltakandidaatti voidaan määrittää samalla komennolla valitsemalla 'root secondary'. Edge-portit eli Ciscon PortFast-portit määritetään interface-konfiguraation alle portti tai porttijoukko kerrallaan.

```
CiscoSwitch(config)# spanning-tree mst configuration
CiscoSwitch(config-mst)# name verkkoalue
CiscoSwitch(config-mst)# revision 1
CiscoSwitch(config-mst)# instance 1 vlan 1,2,10,99
CiscoSwitch(config-mst)# exit
CiscoSwitch(config)# spanning-tree mst 1 root primary
CiscoSwitch(config)# interface range FastEthernet 1/0/11 – 20
CiscoSwitch(config-if)# spanning-tree portfast
CiscoSwitch(config-if)# exit
CiscoSwitch(config)# spanning-tree mode mst
```

Juniper Junos

Junosissa spanning treen määrittely on sekoitus Ciscon ja HP:n konfiguraatiotyylejä. Tuttuun tapaan konfiguraatioille on oma oksansa protocols-rungon alla, ja sinne konfiguroidaan kaikki MST:n ajamiseen tarvittavat tiedot. Myös edge-portit määritellään mstp-konfiguraatioon.

```
root@Jswitch# set protocols mstp configuration-name verkkoalue
root@Jswitch# set protocols mstp revision-level 1
root@Jswitch# set protocols mstp msti 1 vlan [1 2 10 99]
root@Jswitch# set protocols mstp msti 1 bridge-priority 0
root@Jswitch# set protocols mstp interface ge-1/0/11 edge
root@Jswitch# set protocols mstp interface ge-1/0/12 edge
root@Jswitch# set protocols mstp interface ge-1/0/13 edge
root@Jswitch# set protocols mstp interface ge-1/0/14 edge
root@Jswitch# set protocols mstp interface ge-1/0/15 edge
root@Jswitch# set protocols mstp interface ge-1/0/16 edge
root@Jswitch# set protocols mstp interface ge-1/0/17 edge
root@Jswitch# set protocols mstp interface ge-1/0/18 edge
root@Jswitch# set protocols mstp interface ge-1/0/19 edge
root@Jswitch# set protocols mstp interface ge-1/0/20 edge
root@Jswitch# commit
```

Näillä määryksillä saadaan verkko toimimaan paremmin ja ilman looppien pelkoa. Spanning tree on nykyaikaisissa kytkinverkoissa hyvän konfiguraatiokäytännön mukaisesti aina käytössä jossain muodossa, sillä verkot harvoin ovat niin yksinkertaisia, ettei pieni muutos tai vahinkokytkentä voisi aiheuttaa suuria ongelmia verkossa. MST:n käyttöönotto ja muutokset konfiguraatiossa tai verkon topologiassa aiheuttavat aina verkoon joidenkin sekuntien mittaisen katkon. Tämä on hyvä pitää mielessä määryksiä ja kytkentöjä tehdessä, sillä katkoja syntyy helposti, mikäli spanning tree -prosessi on jo käynnissä.

5 Yhteenveto

Tässä työssä olen perehtynyt, ja toivon mukaan perehdyttänyt lukijaakin niin kolmen kytkinvalmistajan käyttöjärjestelmien toimintaan kuin myös verkkokytkinten L2-ominaisuuksiin ja niiden toimintaperiaatteisiin. Olen tuonut esiin Ciscon, HP:n ja Juniperin erilaisia lähestymistapoja eri määrysten tekemiseen, sekä esitellyt näiden määrysten yleistä toiminnallisuutta kytkinverkossa.

Junos OS:n puumainen rakenne on mielestäni selkein lukea ja ymmärtää, ja on tunteistani kytkinkäyttöjärjestelmistä myös miellyttävin käyttää. Sen taipuvaisuus sekä suoraan juuresta tehtäviin komentoihin, että oksien kautta tehtävään täsmällisempään konfigurointiin on uniikki lähestymistapa verkkolaitteiden keskuudessa. Tietääkseni vain Juniperista erkaantunut palomuurivalmistaja Palo Alto käyttää samankaltaista puurakennetta hyväkseen. Ciscon ja HP:n kytkimet ovat suosittumia, kenties osin Ciscon sertifikaattijärjestelmän suosittuuden vuoksi, sillä HP:n ProVision -käyttöjärjestelmää on helppo opetella käyttämään, jos tuntee jo Ciscon IOS:n.

Esittelemäni toiminnot ovat kaikilla kytkimillä helposti määriteltävissä, ja näin tulee olla, sillä ne ovat kytkinten perustoiminnallisuuksia. Vanhempien spanning tree -protokollien suoran tuen puute tuli minulle yllätyksenä, mutta yhteensopivuusominaisuuksien kautta niitäkin vielä tuetaan.

Luonnollisia jatkopolkuja tutkielmaani on monia. Aihetta voisi tarkastella syvemmin joko useamman kytkinvalmistajan laitteiden kautta tai perehtymällä tarkemmin protokolliin ja toiminnallisuuksiin. Myös vertailun laajentaminen kytkinten L3-ominaisuuksiin tai jopa reititinlaitteisiin voisi tuoda laajempia näkökulmia asiaan.

Lähteet

Baker, Liana. 2010. TIMELINE – How HP became the world's largest tech company. Verkkodokumentti. Reuters. <<http://in.reuters.com/article/idINIndia-50870320100816>>. Luettu 7.12.2016.

Bort, Julie. 2014. Cisco Just Turned 30: This Is The Dramatic Story Of How The Founders Were Ousted. Verkkodokumentti. Business Insider. <<http://www.businessinsider.com/how-ciscos-founders-were-ousted-2014-12>>. Luettu 3.11.2016.

Brachmann, Steve. 2016. The Evolution of the Internet: The spanning tree protocol, a major achievement in Internet routing. Verkkootikkeli. <<http://www.ipwatchdog.com/2016/02/04/spanning-tree-protocol-internet-routing/id=65051/>>. Luettu 4.2.2017.

Catalyst 2960-X Switch Security Configuration Guide, Cisco IOS Release 15.0(2)EX. Verkkodokumenttikokoelma. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg.html>. Luettu 2.2.2017.

Catalyst 2960 Switch Software Configuration Guide. 2007.

Cisco.com. Verkkosivusto. <<http://www.cisco.com>>. Luettu 1.11.2016.

Cisco Layer 2 Configuration Guide, Cisco IOS Release 15.2(2)E (Catalyst 2960-X Switch). Verkkodokumenttikokoelma. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-2_2_e/layer2/configuration_guide/b_layer2_1522e_2960x_cg.html>. Luettu 27.1.2017.

Clark, Kennedy, Hamilton, Kevin. 1999. Cisco LAN Switching (CCIE Professional Development series). Cisco Press.

Comparison of the Cisco Catalyst and Cisco IOS Operating Systems for the Cisco Catalyst 6500 Series Switch. 2004. Verkkodokumentti. <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper09186a00800c8441.html>.

Configuring VLANs and Trunking on the EX-series Switch. Verkkodokumentti. <<https://kb.juniper.net/InfoCenter/index?page=content&id=KB11013&actp=search>>. Luettu 30.1.2017.

Corcoran, Elizabeth. 2011. Network Trailblazers: A Conversation with Kirk Lougheed. Verkkodokumentti. <<https://newsroom.cisco.com/feature-content?type=webcontent&articleId=362188>>. Luettu 21.11.2016.

EtherChannel considerations. 2010. Verkkodokumentti. <<http://packetlife.net/blog/2010/jan/18/etherchannel-considerations/>>. Luettu 26.1.2017.

Frazier, Howard, Van Doorn, Schelto, Hays, Robert, Muller, Shimon, Tolley, Bruce, Kolesar, Paul, Thompson, Heoff, Turner, Brad. 2007. IEEE 802.3ad Link Aggregation (LAG), what it is, and what it is not. Verkkodokumentti. <http://www.ieee802.org/3/hssg/public/apr07/frazier_01_0407.pdf>. Luettu 26.1.2017.

Garrett, Aviva. 2006. JUNOS Cookbook. O'Reilly Media, Inc. <<https://www.safaribooksonline.com/library/view/junos-cookbook/0596100140/>>.

Garza, George. 2011. The History of Cisco. Verkkodokumentti. <<http://www.bright-hub.com/computing/enterprise-security/articles/65663.aspx>>. Luettu 21.11.2016.

Gold, Jon. 2016. Aruba CEO: 'We acquired HP Networking when HP acquired us'. Verkkodokumentti. Network World. <<http://www.networkworld.com/article/3042414/mobile-wireless/aruba-ceo-we-acquired-hp-networking-when-hp-acquired-us.html>>. Luettu 15.12.2016.

Greene, Tim. 2009. Juniper Networks: A brief history. Verkkodokumentti. Network World. <<http://www.networkworld.com/article/2869940/lan-wan/juniper-networks--a-brief-history.html>>. Luettu 4.1.2017.

hp.com. Verkkosivusto. <<http://www.hp.com>>. Luettu 6.12.2016.

HP Procurve Switch Series - LACP: Static vs Dynamic (Explained/Configuration). Verkkodokumentti. <http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=mmr_kc-0105343>. Luettu 28.1.2017.

HP Series 2530 Switches Management and Configuration Guide. 2012. Verkkodokumentti. <http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c03594944-1.pdf>.

IEEE 802.1D. 2004. IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Bridges. Kansainvälinen standardi. <<http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>>.

ISO/IEC 7498-1. 1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. Kansainvälinen standardi. <<http://www.ecma-international.org/activities/Communications/TG11/s020269e.pdf>>.

juniper.net. Verkkosivusto. <<http://www.juniper.net>>. Luettu 4.1.2017.

Juniper TechLibrary. Verkkodokumenttikokoelma. <<https://www.juniper.net/documentation/index.html>>. Luettu 27.1.2017.

Poole, Ian. ASIC basics tutorial. Verkkodokumentti. <<http://www.radio-electronics.com/info/data/semicond/asic/asic.php>>. Luettu 11.1.2017.

Techopedia, Application-Specific Integrated Circuit (ASIC). Verkkodokumentti. <<https://www.techopedia.com/definition/2357/application-specific-integrated-circuit-asic>>. Luettu 11.1.2017.

The Server Rack FAQ. Verkkosivusto. <www.server-racks.com>. Luettu 11.1.2017.

Troubleshooting STP on Catalyst Switches Running Cisco IOS System Software. Verkkodokumentti. <<http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/28943-170.html>>. Luettu 3.2.2017.

Understanding RSTP for EX Series Switches. Verkkodokumentti. <https://www.juniper.net/documentation/en_US/junos12.3/topics/concept/spanning-trees-ex-series-rstp-understanding.html>. Luettu 4.2.2017.

Wikipedia. Verkkosivusto / hakuteos. <<https://www.wikipedia.org>>

