SAVONIA

Redundanttisuus tietoverkoissa

Miika Räisänen

Opinnäytetyö

___. ___. _____ _____

Ammattikorkeakoulututkinto

SAVONIA-AMMATTIKORKEAKOULU **OPINNÄYTETYÖ**
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Miika Räisänen	
Työn nimi Redundanttisuus tietoverkoissa	
Päiväys 18.6.2012	Sivumäärä/Liitteet 56/5
Ohjaaja(t) laboratorioinsinööri Pekka Vedenpää	
Toimeksiantaja/Yhteistyökumppani(t) Savonia-ammattikorkeakoulu	

Tiivistelmä

Tämän insinöörityön aiheena oli redundanttisuus tietoverkoissa. Työn tavoitteena oli tutkia erilaisia redundanttisuuteen liittyviä menetelmiä ja toteuttaa toimiva kytkinten varmuuskopiontijärjestelmä Savonia-ammattikorkeakoulun tietoverkkoa varten.

Kytkinten varmuuskopionti ja varakytkinten käyttöönotto vikatilanteissa on olennainen osa tietoverkon redundanttisuutta ja toimintavarmuutta. Tätä varten luotiin testiympäristö, jossa testattiin Savonia-ammattikorkeakoulun yleisimpien kytkinten toimintaa varmuuskopiointijärjestelmässä.

Testaustulosten perusteella järjestelmä otetaan käyttöön Savonia-ammattikorkeakoulun tietoverkossa kesän 2012 aikana.

Avainsanat
redundanttisuus, varmuuskopiointi, Cisco, kytkimet, TFTP, VSS, EtherChannel

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Miika Räisänen			
Title of Thesis Redundancy in data networks			
Date	18.6.2012	Pages/Appendices	56/5
Supervisor(s) Laboratory Engineer Pekka Vedenpää			
Client Organisation/Partners Savonia University of Applied Sciences			

Abstract

Subject of this thesis was redundancy in data networks. The object was to study various methods relating to redundancy and implement a functional backup system for the switches of Savonia University of Applied Sciences' network.

Backing up the switches' configuration files and deployment of reserve switches are essential parts of the network redundancy and reliability. A test environment was created to try out the backup system with the most common switches of Savonia's network.

Test results show that the system was good enough to be implemented to Savonia's network. The implementation will be carried out in summer 2012.

Keywords
redundancy, backup, Cisco, switches, TFTP, VSS, EtherChannel

Esipuhe

Tämä työ on tehty Savonia-ammattkorkeakoululle kevään 2012 aikana.

Haluaisin esittää kiitokset Savonia-ammattikorkeakoulun laboratorioinsinööri Pekka Vedenpäälle työn valvomisesta ja ohjauksesta.

Kiitokset myös vanhemmilleni, jotka jaksoivat kannustaa ja tukea minua opiskelujeni aikana.

Kuopiossa 18.6.2012

Miika Räisänen

Sisältö

SANASTO

Archive – Cisco IOS:n konfiguraatiotiedostojen arkistointiohjelma

ASCII – American Standard Code for Information Interchange, tietokoneiden käyttämä merkistö

Broadcast – Tietoverkkolaitteiden käyttämä metodi, jolla lähetetään viesti kaikille verkon laitteille yhtäaikaa

DHCP – Dynamic Host Configuration Protocol, tietoverkkoprotokolla automaattiseen laitteiden konfigurointiin IP-verkossa

Flash-muisti – Sähköinen muistipiiri

IP – Internet Protocol, huolehtii tietoliikennepakettien toimittamisesta oikeaan paikkaan

ISO – International Organization for Standarization, kansainvälinen standardoimisjärjestö

Kron – Cisco IOS:n komentojen ajastusohjelma

LAN – Local Area Network eli lähiverkko on pienellä alueella toimiva tietoliikenneverkko

MAC – Media Access Control, OSI-mallin siirtokerroksella toimiva protokolla, joka huolehtii mm. laitteistojen osoitteista

Multicast - Tietoverkkolaitteiden käyttämä metod, jolla lähetetään viesti valituille kohteille

NSF – Non-stop forwarding, protokolla jonka tarkoituksena on keskeytymätön tiedonsiirto verkkokerroksella

OSI-malli – ISO:n standardoima viitemalli, joka kuvaa tiedonsiirtoprotokollien toimintaa seitsemässä kerroksessa

PuTTY – Telnet- ja ssh-asiakasohjelma ja pääte-emulaattori

ROM – Read Only Memory, tietokonelaitteiden lukumuisti, johon ei normaalikäytössä tehdä muutoksia

SSO – Stateful switchover, muodostaa aktiivisen/passiivisen yhteyden kahden kytkimen välille

STP – Spanning Tree Protocol, Cisco kytkimien käyttämä protokolla, jonka tarkoituksena on estää luuppien syntyminen verkosssa

TFTP – Trivial File Transfer Protocol, yksinkertainen tiedonsiirtoprotokolla

Unicast - Tietoverkkolaitteiden käyttämä metodi, jolla lähetetään viesti yhdeltä laitteelta toiselle

UPS - Uninterruptible Power Supply, akuilla toimiva varavirtalähde sähkökatkoksien varalle

VLAN – Virtual Local Area Network, virtuaalinen lähiverkko jolla fyysinen tietoliikenne jaetaan loogisiin osiin

VSL – Virtual Switching Link, VSS:n varsinaiset linkit kytkimien välillä

VSS – Virtual Switching System, Ciscon kehittämä tekniikka, jolla yhdistetään kytkimet yhdeksi virtuaaliseksi kytkimeksi

WAN – Wide Area Network eli laajaverkko yhdistää pienemmät verkon toisiinsa

1 JOHDANTO

Tässä työssä käsitellään tietoverkon redundanttisuutta ja siihen liittyviä menetelmiä. Työn ymmärtämiseksi raportissa käydään läpi myös tarvittavia taustatietietoja, kuten OSI-mallin perusteita, redundanttisuutta käsitteenä ja verkkotopologioita. Työn painopisteenä on Cisco-kytkinten konfiguraatioiden varmuuskopiontijärjestelmä ja suunnitelma sen saattamiseksi toimintakuntoon.

Opinnäytetyö tehtiin kevään 2012 aikana Savonia-ammattikorkeakoulun toimeksiannosta. Työssä tutkittiin Savonian verkon jo olemassa olevia dokumentteja ja laitteistoja testauslaboratoriossa, joka sijaitsi koulun tiloissa. Laitteisto laboratorioon hankittiin myös koulun puolesta.

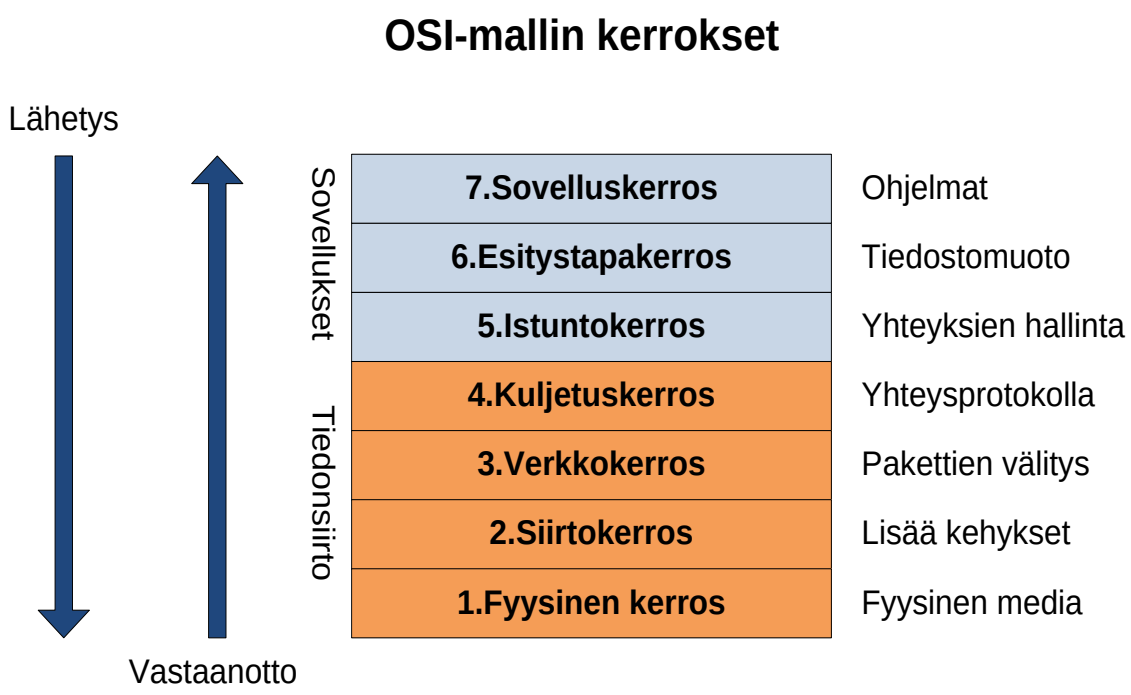
Savonia-ammattikorkeakoulun tietohallinnossa tarvittiin toimiva järjestelmä kytkinten konfiguraatioiden varmuuskopiointiin ja varakytkinten konfiguraatioiden pitämiseen ajan tasalla. Tavoitteena oli saada edullinen, yksinkertainen ja nopea järjestelmä koulun käyttöön. Tämän piti onnistua ilman aiheetonta kaapelointia ja ylimääräisiä hankintoja.

Savonia-ammattikorkeakoulu on perustettu 1992 ja sillä on yksiköitä Kuopion, Varkauden ja Iisalmen alueilla. Sitä ylläpitää Savonia-ammattikorkeakoulun kuntayhtymä, joka koostuu Iisalmen, Kiuruveden, Kuopion, Lapinlahden ja Varkauden jäsenkunnista. Se kuuluu Suomen suurimpiin ammattikorkeakouluihin. Opiskelijoita Savoniassa oli vuonna 2010 noin 5 800 ja henkilökuntaa noin 530. Rehtorina toimii Veli-Matti Tolppi, joka vastaa myös Savonia-ammattikorkeakoulun kuntayhtymän johdosta.

Savonia kouluttaa opiskelijoita muun muassa kulttuurin, ympäristötekniikan sekä tekniikan ja liikenteen aloille. Näistä suurin on tekniikan ja liikenteen ala, jota opiskelee noin neljännes opiskelijoista.

2 OSI-MALLI

OSI-malli (kuvio 1) eli Open Systems Interconnection Reference Model on kansainvälisen standardoimisjärjestön ISO:n (International Standards Organization) kehittämä ympäristö ja on nykyään pääarkitehtuurimalli havainnollistamaan tiedonsiirtoa verkon kautta. Se kuvaa, kuinka tieto siirtyy verkossa seitsemän kerroksen kautta ohjelmalta toiselle. Jokainen kerros esittää tiettyjä verkon toimintoja. Kerrokset ovat melko omavaraisia, eli jokaisella kerroksella tapahtuvat tehtävät voidaan suorittaa erillisinä. Tämä mahdollistaa sen, että yhdellä kerroksella tehtävät voidaan suorittaa ilman, että ne vaikuttavat muihin kerroksiin. (Cisco Systems 2010b.)



KUVIO 1. OSI-mallin kerrokset

2.1 OSI-mallin kerrokset

OSI-malli on jaettu seitsemään kerrokseen. Tietoa vastaanotettaessa neljä ensimmäistä kerrosta käsittää tiedonsiirron toiminnat. Nämä kerrokset ovat fyysinen, siirto-, verkko- ja kuljetuskerros. Sovellus-, esitystapa- ja istuntokerrokset toimivat tiedonsiirtokerroksien ylä- tai alapuolella sen mukaan vastaanotetaanko vai lähetetäänkö dataa. Ne kuuluvat ohjelmien käyttämiin kerroksiin.

2.1.1 Fyysinen kerros

Fyysinen kerroksella (physical layer) tapahtuu tiedon fyysinen siirtyminen. Kerros määrittelee, millaista mediaa pitkin tieto siirtyy. Näitä medioita voivat olla esimerkiksi kuparikaapeli, valokaapeli tai radioaallot. Se pitää sisällään myös määritteet siirtotien ominaisuuksista, kuten jännitemäärät ja niiden vaihtelun ajoitukset, suurimmat mahdolliset siirtoetäisyydet sekä fyysiset liittimet. (Cisco Systems 2010b.)

2.1.2 Siirtokerros

Siirtokerros (data link layer) toimii fyysisen kerroksen yläpuolella ja se tarjoaa kehyksien luonnin ylempien kerroksien lähettämälle datalle fyysistä siirtoa varten. Se myös havaitsee ja korjaa fyysisellä kerroksella tapahtuvia virheitä. Ylikuormituksen ehkäisemiseksi siirtokerros myös säätelee bittivirran nopeutta. Kytkimet toimivat tällä kerroksella ohjaten liikennettä MAC-osoitetaulujen mukaan. (Cisco Systems 2010b.)

2.1.3 Verkkokerros

Verkkokerroksella (network layer) datapaketit reititetään reitittimien välityksellä, jotka erottelevat kuljetuskerrokselta saamansa tiedon paketteihin ja antavat niille vastaanottajan IP-osoitteen. Itse reitittäminen hoidetaan reititystaulujen avulla. Verkkokerroksen tehtävänä on myös aliverkkojen yhdistäminen toisiinsa. (Colliander 1999.)

2.1.4 Kuljetuskerros

Kuljetuskerros (transport layer) hallinnoi pakettien kuljetusta. Se varmistaa, että paketit tulevat perille ja lähtevät oikeassa järjestyksessä. Kuljetuskerros seuraa paketin perille saapumisen onnistumista ja lähettää sen tarvittaessa uudestaan. (Cisco Systems 2010b.)

2.1.5 Istuntokerros

Istuntokerroksen (session layer) tehtävänä on verkon laitteiden välillä olevien yhteyksien luominen, hallinnointi ja sulkeminen. Nämä yhteydet ovat palvelupyyntöjä ja vastauksia ohjelmilta, jotka sijaitsevat verkossa olevilla laitteilla. Istuntokerros

koordinoi näitä yhteyksiä protokollien, kuten Zone Information Protocolin (ZIP), avulla. (Cisco Systems 2010b.)

2.1.6 Esitystapakerros

Esitystapakerros (presentation layer) sovittaa vastaanotetun tiedon sovellukselle. Tämä kerros tarjoaa useita toimintoja, joilla se muuntaa datan sovelluskerrokselle sopivaan formaattiin. Näitä formaatteja voivat olla esimerkiksi JPEG-kuvat (Joint Photographic Experts Group) tai MPEG-videot (Motion Picture Experts Group). (Cisco Systems 2010b.)

2.1.7 Sovelluskerros

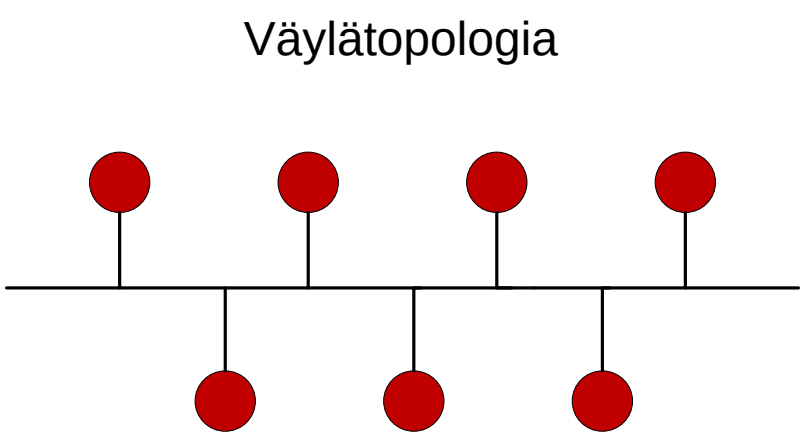
Sovelluskerros (application layer) on lähimpänä loppukäyttäjää OSI-kerroksista. Sen tehtävänä on määrittää ohjelmiston ja verkon rajapinta. Tämä kerros on vuorovaikutuksessa sovelluksien kanssa ja tarjoaa niille protokollat, joilla välittää tietoa verkkoon. Esimerkkejä tälläisistä sovelluksien käyttämistä protokollista ovat Telnet ja File Transfer Protocol (FTP). (Cisco Systems 2010b.)

3 VERKKOTOPOLOGIAT

Verkon fyysistä ja loogista perusrakennetta kuvataan yleensä kolmella eri topologiamallilla. Nämä mallit ovat väylä-, tähti- ja rengastopologia. Topologioilla havainnollistetaan, kuinka verkon laitteet ovat yhteydessä toistensa kanssa. Näiden topologioiden lisäksi on olemassa myös täydellinen mesh-topologia, jossa kaikkia laitteet ovat yhteydessä toisiinsa. Mesh-topologiasta löytyy lisäksi osittainen muunnelma, joka nimensä mukaan koostuu osittain kytketystä topologiasta. Näiden lisäksi tässä luvussa käydään läpi muutamaa vähemmän käytettyä verkkotopologiaa ja pohditaan niiden sovellettavuutta redundanttisessa tietoverkossa.

3.1 Väylätopologia

Väylätopologiassa (kuvio 2) verkon laitteet ovat kytkettyinä yhdellä kaapelilla toisiinsa. Kaapelin molemmista päissä on vastus eli terminaattori. Väylätyyppisiä verkkoja ei enää rakenneta, koska ne ovat hyvin herkkiä ruuhkaantumaan. Tämä johtuu siitä, että verkkoa pystyy käyttämään vain yksi laite kerrallaan. Monen laitteen liikennöidessä yhtä aikaa seurauksena on yleensä törmäyksiä, mikä ilmenee datahävikkinä. (Wikipedia 2012a.)

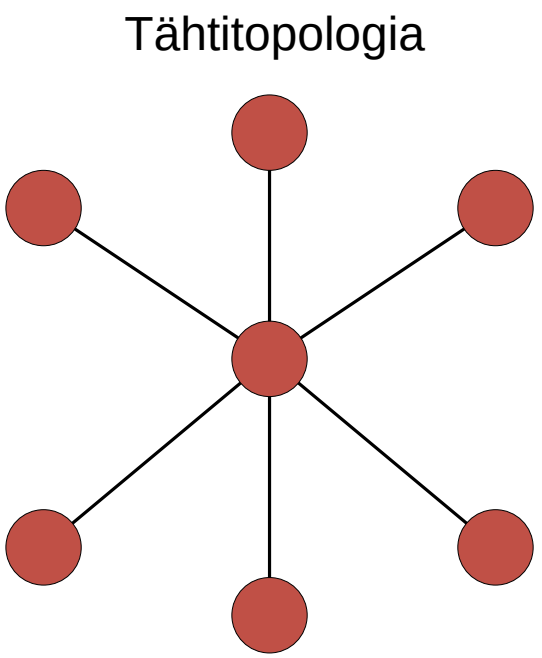


KUVIO 2. Väylätopologia

Vikasietoisuus tässä topologiassa on huono. Yhdenkin verkkokortin tai kaapelin vikaantuminen saattaa kaataa koko verkon. Palautuminen vaatii pikaista korjausta ja palveluihin tulee välttämättä huoltokatko. Sen vuoksi reduntanttisuuden kannalta tämä ratkaisu ei ole kannattava.

3.2 Tähtitopologia

Tähtitopologia (kuvio 3) perustuu keskuslaitteeseen, jonka läpi kaikki verkkoliikenne kulkee. Keskuslaitteena toimii yleensä kytkin tai keskitin, joka on liitetty toiseen keskuslaitteeseen. Keskittimien käyttö on vähentynyt, koska ne toistavat liikenteen kaikkiin siihen kytkettyihin laitteistoihin. Tämä ruuhkauttaa verkkoa sekä vaarantaa tietoturvan, koska liikennettä on tällöin helppo kaapata. (Wikipedia 2012a.)

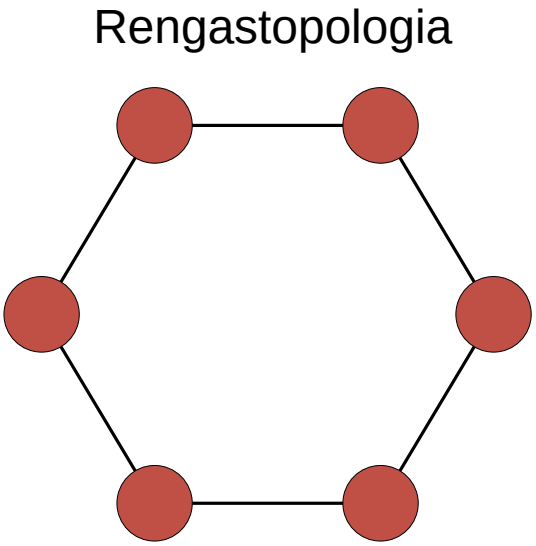


KUVIO 3. Tähtitopologia

Redundanttisuutta pohdittaessa tähtitopologia ei ole parhaimpia vaihtoehtoja. Keskuslaitteen vikaantuessa kaikki siihen liitetyt laitteet putoavat verkosta, minkä vuoksi keskuslaite täytyy korjata tai vaihtaa. Korjaus aiheuttaa yleensä pitkän katkoksen kyseisessä verkon osassa.

3.3 Rengastopologia

Rengastopologiassa (kuvio 4) verkon laitteet ovat kytkettyinä rengasmaisesti toisiinsa. Tietoliikenne liikkuu rengastopologiassa yhteen suuntaan laitteelta toiselle. Jokainen laite toimii toistimena, jotta signaali pysyy voimakkaana koko silmukan ympäri. Verkon toiminnalle on tärkeää, että se pystyy välittämään liikenteen koko renkaan läpi. Toisin kuin väylätopologiassa rengastopologiassa ei ole päätöspisteitä, jotka vaatisivat terminaattoreita. (Wikipedia 2012a.)

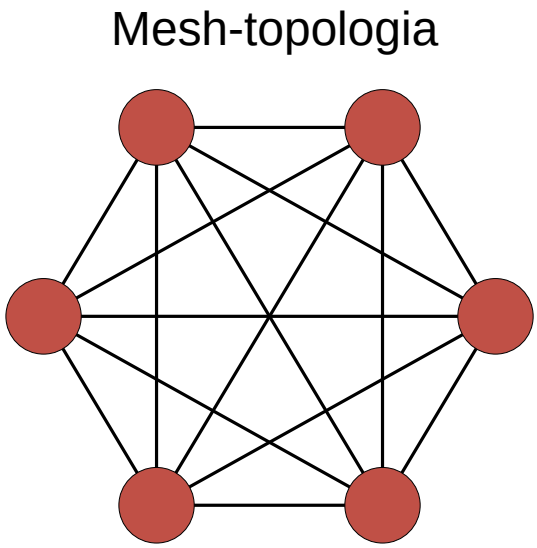


KUVIO 4. Rengastopologia

Topologian heikkous on signaalin kulkeminen jokaisen koneen kautta. Tämä aiheuttaa sen, että häiriö yhdessä laitteessa voi vaikuttaa koko silmukan toimintaan. Kuten muut edellä mainitut topologiamallit, tämäkään ei ole tarpeeksi vikasietoinen nykyajan vaatimuksiin.

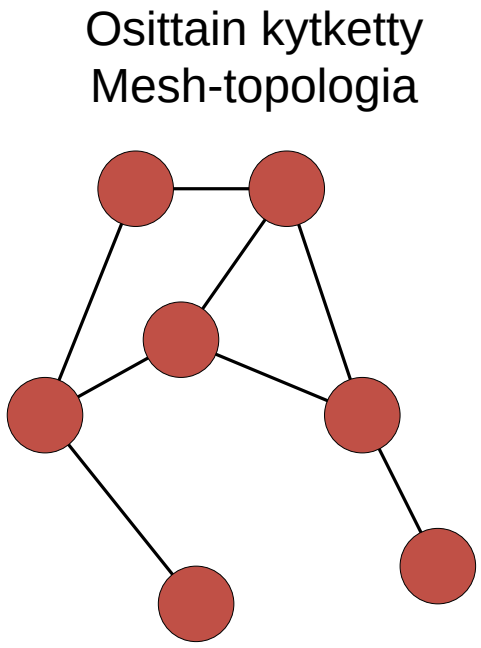
3.4 Mesh-topologia

Mesh-topologiassa (kuvio 5) kaikki verkon laitteet ovat kytkettyinä toisiinsa. Täysin fyysisesti kytketty Mesh-topologia on hyvin kallis ja monimutkainen ja sitä käytetään vain silloin, kun verkkolaitteita on vähän. Yleisin käytetty malli on osittain kytketty Mesh-topologia (kuvio 6), jonka avulla päästään tarvittavaan redundanttisuuteen ilman turhaa kaapelointia ja monimutkaisuutta. (Wikipedia 2012a.)



KUVIO 5. Mesh-topologia

Täydellinen mesh olisi ideaalinen vaihtoehto redundanttisessa tietoverkossa, sillä se on hyvin vikasietoinen. Yhden laitteen häiriöt eivät vaikuta olennaisesti koko verkon toimintaan. Yhteyden ollessa yhteen suuntaan poikki tieto liikkuu toista kautta perille. Täydellisen mesh-topologian huono kustannustehokkuus ja monimutkaisuus tekevät siitä epäedullisen vaihtoehdon.

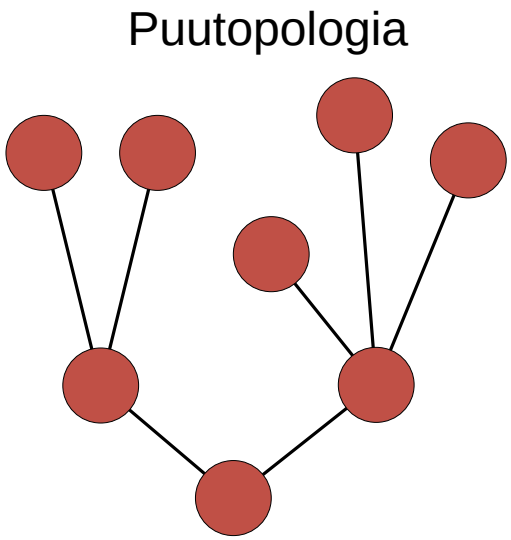


KUVIO 6. Osittain kytketty mesh-topologia

Osittain kytkettyllä mesh-topologialla saadaan aikaiseksi hyvinkin redundanttinen verkko. Häiriötilanteissa verkkoliikenne ohjataan toista kautta perille ja näin ollen verkon toiminta voi jatkua ilman merkittävää katkosta.

3.5 Puutopologia

Puutopologia (kuvio 7) perustuu siihen, että keskuslaitteelta lähtee kytkennät hierarkiassa alempana oleville laitteille kerroksittain. Yksi tai useampi kytkentä liittyy hierarkiassa alempana olevaan ja siitä eteenpäin. Näin verkolle muodostuu puumainen rakenne. (Wikipedia 2012a.)



KUVIO 7. Puutopologia

Hierarkiassa ylempänä olevan laitteen vikaantuminen aiheuttaa myös alempana oleviin katkoksen. Tämä johtaa siihen, että mitä ylempänä hierarkiassa häiriö esintyy, sitä laajempi ongelma siitä tulee verkolle. Puutopologia toimii hyvin pienissä verkoissa, joissa ei ole useita eri hierarkia tasoja.

4 LÄHIVERKON AKTIIVILAITTEET

Lähiverkko eli Local Area Network (LAN) on paikallinen verkko, joka yhdistää tietokoneet ja muut verkon päätelaitteet yhteen esimerkiksi kytkinten avulla. Lähiverkko on yleensä yhteydessä laajaverkkoon eli WAN:iin (Wide Area Network) reitittimen kautta, mutta se voi olla myös erillään muista verkoista.

Lähiverkon aktiivilaitteet toimivat tiedonsiirron välikappaleina. Laitteet voivat olla yhdistettyinä toisiinsa kaapeleiden avulla tai langattomasti (WLAN – Wireless Local Area Network). Tässä luvussa esitellään yleisellä tasolla tärkeimmät lähiverkon aktiivilaitteista.

4.1 Keskitin

Keskitin eli hub on jo vanhentunutta teknologiaa, jota vielä kuitenkin käytetään joissakin verkoissa. Keskitin lähettää vastaanotetun signaalin muuttamattomana eteenpäin muille verkonlaitteille. Se toimii OSI-mallin ensimmäisellä eli fyysisellä kerroksella. Keskittimen jokainen portti jakaa yhteisen kaistan. Se lähettää vastaanotetun datan jokaisesta laitteesta lähtevästä portista, joka taas aiheuttaa ruuhkaantumista liikenteen noustessa keskittimen kapasiteetin yli. Keskittimen lähettämää liikennettä voi salakuunnella suhteellisen vaivattomasti johtuen sen jo mainitusta ominaisuudesta lähettää tietoa eteenpäin. (Wikipedia 2012b.)

4.2 Kytkin

Keskittimet on nykyään korvattu kytkimillä (Switch). Kytkin toimii OSI-mallin siirtokehyskerroksella. On olemassa myös reitittäviä kytkimiä, jotka eroavat reitittimistä siten, ettei niissä ole WAN-liitäntää. Reitittäviä kytkimiä ovat esimerkiksi Cisco Catalyst 6500 ja 4500 -sarjan kytkimet.

Kytkin on lähiverkon laite, joka yhdistää lähiverkon osat toisiinsa. Ne perustuvat moniporttiseen siltaukseen. Siltauksen periaate on yhdistää kaksi eri verkkoa ja samalla suodattaa liikennettä. Se ohjaa liikennettä MAC-osoitetaulujen (Media Access Control) mukaan vain niihin portteihin, joihin data on menossa. Tästä poikkeuksena multicast, unicast ja broadcast, jotka lähetetään verkon yli kaikille laitteille. (Wikipedia 2012c.)

4.3 Reititin

Reititin (Router) toimii lähiverkon reunalla ohjaten tietoliikennettä laajaverkkoon. Sen tehtävänä on välittää tietoa eri verkon osien välillä. Reitittimiä voi olla langallisten eli Ethernet-kaapeleita käyttävien lisäksi myös langattomia. Kun datapaketti tulee reitittimelle, lukee se osoitetiedot paketin sisältä ja lähettää kyseisen paketin oikeaan suuntaan. Tämä tapahtuu reititystaulujen (routing table) tai reitityskäytännön (routing policy) mukaan. (Wikipedia 2012d)

Tyypillisimpiä reitittimiä ovat pienet koti- ja yritysreitittimet, jotka ovat palveluntarjoajan ja päätelaitteen välissä. Tälläinen on esimerkiksi DSL-modeemi (Digital Subscriber Line). Monimutkaisempia reitittimiä edustavat isojen yritysten ja palveluntarjoaijen reitittimet, sekä tehokkaat ”ydin” reitittimet (core router), jotka välittävät tietoa Internetin runkoverkossa kuitukaapeleita hyväksikäyttäen. (Wikipedia 2012d.)

4.4 Langaton tukiasema

Langattomat tukiasemat (wireless access point) antavat mahdollisuuden kytkeytyä lähiverkkoon WLAN-yhteensopivilla laitteilla. Tukiasemat ovat yleensä yhteydessä reitittimeen tai kytkimeen Ethernet-kaapelilla. Asemista on olemassa myös Power over Ethernet-tekniikkaa (PoE) tukevia. Niissä tarvittava virta syötetään Ethernet-kaapelia pitkin, jolloin tukiasema ei tarvitse erillistä virtalähdettä. Tavallisimmin tukiasemia käytetään kaapeloinnin ollessa mahdotonta tai sisäverkon lisäksi ettei liikuteltavia laitteita tarvitsisi kytkeä Ethernet-pistokkeisiin.

5 CISCO IOS:N KOMENTOTILAT

Cisco Catalyst kytkimet käyttävät Cisco-IOS (Interworking Operating System) käyttöjärjestelmää. Sen operointi hoidetaan CLI-käyttöliittymän (Command-Line Interface) avulla, jolla navigoidaan eri komentotilojen välillä ja syötetään halutut käskyt kytkimelle. Tässä luvussa käydään läpi peruskomentotilat, joita Cisco-IOS käyttää.

5.1 User EXEC Mode

User EXEC Mode eli käyttäjätilaa merkitään kytkimen nimeä seuraavalla >-symbolilla (Switch>). Tähän tilaan tullaan, kun kytkimelle kirjaudutaan. Tässä tilassa voi esimerkiksi muodostaa yhteyden muihin verkon laitteisiin, suorittaa yksinkertaisia testejä tai listata järjestelmän tietoja. (Cisco Systems 2012b, 1.)

5.2 Priviliged EXEC Mode

Priviliged EXEC Modeen pääsee syöttämällä komento ”enable” käyttäjätilassa. Tilan tunnistaan #-merkistä (Switch#) ja sitä kutsutaan pääkäyttäjätilaksi. Tämä tila on yleensä suojattu salasanalla ja sieltä pääsee suorittamaan koko järjestelmää koskevia komentoja. (Cisco Systems 2012b, 2.)

5.3 Global Configuration Mode

Global Configuration Mode eli suomeksi globaali konfiguraatiotila on tila, jossa annetaan kytkimeen yleisesti vaikuttavia komentoja. Globaalin konfiguraatio tilan tunnistaa kytkimen nimen edessä olevasta sulkeissa olevasta config-termistä (Switch(config)#). (Cisco Systems 2012b, 2.)

5.4 ROM Monitor Mode

ROM Monitor Mode-tila aktivoituu, jos kytkin ei löydä validia levykuvaa (image). Järjestelmä rekisteröityy niin kutsuttuun ROMMON-tilaan. Tässä tilassa laitteen voi käynnistää uudelleen tai suorittaa erinäisiä diagnostiikka testejä. Tilaan pääsee myös keskeyttämällä kytkimen käynnistyksen ctrl-c-näppäinyhdistelmällä. ROMMON-tila

näkyy käyttäjälle rommon, hakasulku ja numero (rommon1>) tunnisteena. (Cisco Systems 2012b, 2.)

5.5 Setup Mode

Setup-tila ei oikeastaan ole komentotila. Siinä asetetaan kysymysten perusteella peruskonfiguraatio ensimmäistä kertaa käynnistettävälle tai konfiguroimattomalle kytkimelle. Tähän tilaan pääsee konfiguroimattoman kytkimen käynnistyksen yhteydessä tai syöttämällä komennon ”setup” pääkäyttäjätilassa. (Cisco Systems 2012b, 2.)

5.6 Konfigurointi- ja alitilat

Konfiguraatioitiloihin (configuration mode) päästään globaalista konfiguraatiotilasta ja niistä alitiloihin (submode). Konfiguraatiotilan tunnistaa globaalin konfiguraatiotilan perässä olevasta tunnisteesta, joka esimerkiksi liitännässä on muotoa ”Switch(config-if)#”. Konfiguraatiotilojen alitilat merkitään yleensä varsinaisen tunnisteen perään. (Cisco Systems 2012b, 2.)

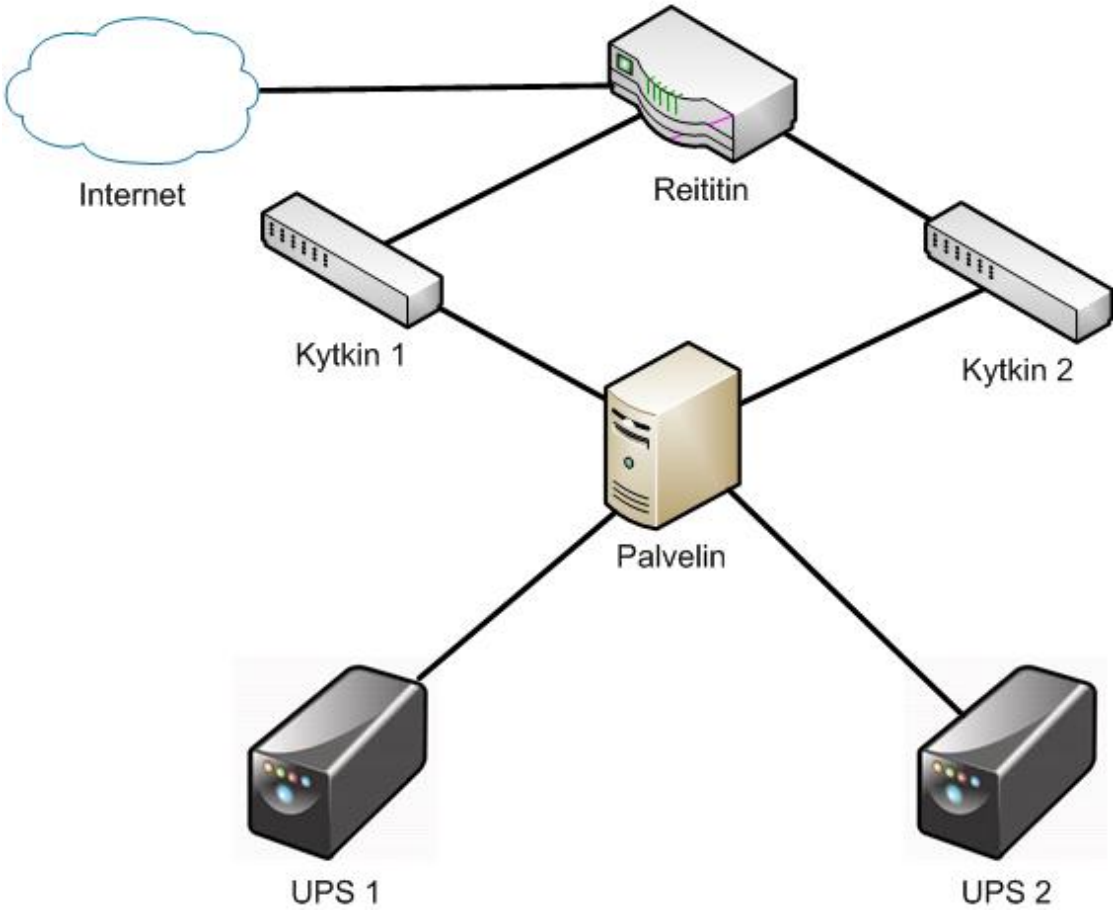
6 REDUNDANTTISUUS KÄSITTEENÄ

Tietoverkon redundanttisuudella tarkoitetaan vikasietoisuutta eli sitä, kuinka hyvin verkko pystyy toimimaan häiriötapauksissa. Hyvän redundanttisuuden saavuttamiseksi verkkolaitteiden, kuten kytkinten ja reitittimien, tulisi olla vähintään kahdennettu. Tämä ei aina ole esimerkiksi kustannussyistä mahdollista ja riittävän redundanttisuuden saavuttamiseksi täytyy käyttää muita keinoja.

Redundanttisuuteen kuuluu edellä mainitun kahdennuksen lisäksi myös erilaiset tekniikat ja järjestelmät, joilla voidaan saavuttaa vikasietoinen ja luotettava verkko. Näitä tekniikoita ovat esimerkiksi EtherChannel (7. EtherChannel) ja Virtual Switching System (8. Kytkinten virtualisointi). Laitteiden konfiguraatiotiedostojen varmuuskopiointi ja verkonvalvonta ovat myös osa onnistunutta redundanttisuutta.

6.1 Verkon kahdennus

Kahdennetulla verkolla (kuvio 8) tarkoitetaan verkon tärkeiden osien, kuten palvelimien, toiminta vikatilanteissa on varmistettu tuplaamalla yhteyksien ja varavirtalähteiden määrä. Yhden yhteyden tai virransyötön pettäminen ei näin ollen kaada koko verkkoa vaan toiminta voi jatkua ilman pitkää katkosta. Yleensä tämä katkos ei näy merkittävällä tavalla loppukäyttäjälle. Verkko voi olla myös kolmennettu, jolloin yhden laitteen poistuessa toiminnasta kaksi muuta pitävät järjestelmää yllä. Kytkimissä tämä tarkoittaa sitä, että vian tullessa johonkin kolmesta kytkimestä, kaksi jäljelle jäävää äänestävät, kumpi jatkaa tehtävää.



KUVIO 8. Kahdennettu verkko

6.2 Spanning Tree Protocol

Normaalissa lähiverkossa varayhteydet on hoidettu spanning tree -protokollan (Spanning Tree Protocol, STP) avulla. Se tarjoaa luupittoman topologian sillatussa lähiverkossa. STP:n tehtävänä on siis estää luuppien syntyminen verkossa. Se mahdollistaa myös automaattisten varayhteyksien ylläpidon. Käytännössä tämä tarkoittaa, että aktiivisen linkin mennessä alas STP korvaa sen varayhteydeksi määrätyllä linkillä. (Cisco Systems 2006.)

6.3 Varavirtalähteet

Varavirtalähteiden (kuva 1) eli UPS:ien (Uninterruptible Power Supply) tehtävänä on varmistaa virransyöttö verkon laitteille virtakatkoksien aikana. Ne toimivat varsinaisen virransyötön ja laitteen välillä. UPS ei ole tarkoitettu pitkien katkoksien varalle, mutta sillä pystytään eliminoimaan lyhyet eli muutamien minuuttien pituiset katkokset.

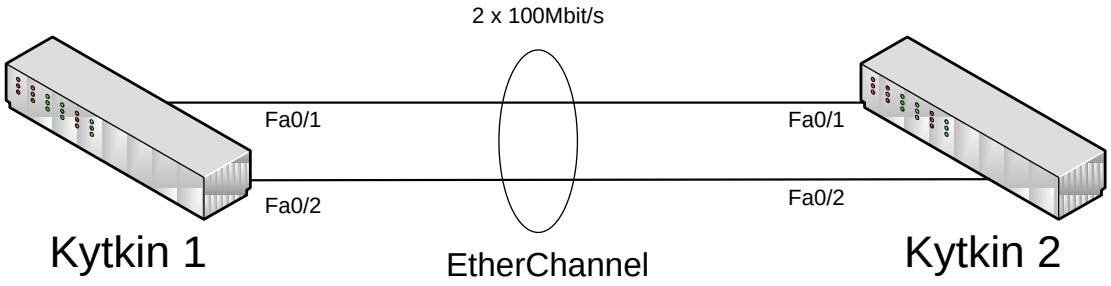
UPS:ssä on ns. tasasuuntaaja, joka muuntaa verkkovirran vaihtojännitteen tasajännitteeksi. Tämän rinnalle on liitetty sarja akkuja, joiden tehtävänä on syöttää virtaa katkoksien aikana. Vaihtosuuntaaja muuttaa tasajännitteen takaisin vaihtojännitteeksi, joka taas syötetään laitteille. Varavirtalähteet on varustettu yleensä ohjelmistolla, jonka tehtävänä on ajaa UPS:iin liitetetyt laitteistot turvallisesti alas ennen akkujen tyhjenemistä. (Wikipedia 2012e.)

KUVA 1. Kuva Savonia-ammattikorkeakoulun palvelinhuoneen UPS:sta. (Valokuva Miika Räisänen 2012)

7 ETHERCHANNEL

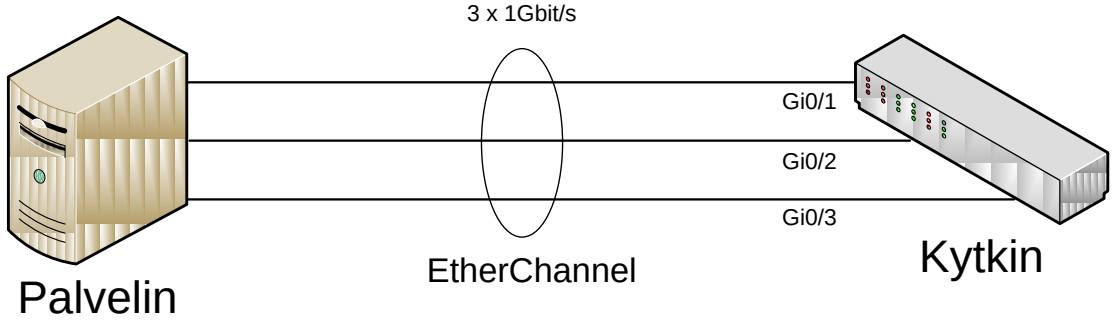
EtherChannel on ensisijaisesti käytössä Ciscon kytkimillä. Se on porttien yhdistämisteknologia, jolla fyysisistä porteista tehdään yksi looginen kanava. Se siis tarjoaa vikasietoisen ja tavallista nopeamman linkin kahden laitteen välillä. EtherChanneliin voidaan luoda kahdesta kahdeksaan aktiivista yhteyttä laitteiden välille. Porttien maksiminopeudet eri Ethernet-tekniikoissa ovat 100 Mbit/s (Fast Ethernet), 1 Gbit/s (Gigabit Ethernet) tai 10 Gbit/s (10 Gigabit Ethernet). Näin ollen suurimmaksi mahdolliseksi nopeudeksi saadaan 800 Mbit/s:sta 80 Gbit/s:ssa portissa käytettävän teknologian mukaan. (Cisco Systems 2003.)

Aktiivisten porttien lisäksi EtherChanneliin voi asettaa yhdestä kahdeksaan niin kutsuttua failsafe-porttia. Näiden porttien tehtävänä on olla varalla aktiivisille porteille, eli vian sattuessa failsafe-portti muuttuu aktiiviseksi portiksi. (Cisco Systems 2003.)



KUVIO 9. EtherChannel kahden kytkimen välilä

EtherChannelia käytetään pääasiassa kytkinten välillä (kuvio 9) runkoverkossa, mutta se voidaan myös asettaa toimimaan kytkimen ja päätelaitteen, kuten palvelimen, välillä (kuvio 10).



KUVIO 10. EtherChannel palvelimen ja kytkimen välillä

7.1 EtherChannelin hyödyt ja rajoitteet

Tärkein EtherChannelin hyöty on, että se toimii parhaimmillaan kahdeksan kertaa nopeammin verrattuna normaaliin yhtä porttia käyttävään yhteyteen. Tämä sillä rajoituksella, että nopeus pysyy entisellään yhdelle sovellukselle. Esimerkiksi kahdeksan 100 Mbit/s -linkin EtherChannelissa yksittäinen sovellus voi saada nopeudeksi vain 100 Mbit/s vaikka suurin mahdollinen kaistanleveys olisikin 800 Mbit/s. (Cisco Systems 2003.)

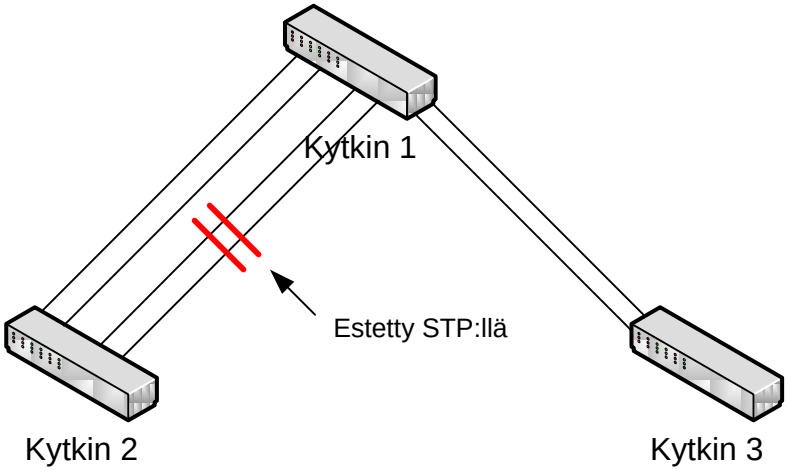
EtherChannel on myös hyvin joustava ja sitä voi käyttää missä tahansa verkon osassa, jossa on odotettavissa ruuhkautumista. Sillä voi myös helposti nostaa väylänopeutta lisäämällä linkkejä laitteiden välillä. Kuormantasaus (load balancing) on yksi tärkeistä EtherChannelin ominaisuuksista. Unicast-, broadcast- ja multicast-liikenne jaetaan tasaisesti linkkien yli, jotta yksi linkki ei kuormittuisi liikaa. Yhden linkin kaatuessa liikenne jaetaan tasaisesti EtherChannelin muille linkeille ilman käyttäjälle näkyviä katkoksia tai suurta pakettihävikkiä. (Cisco Systems 2003.)

Verkkovelluksille EtherChannel on läpinäkyvä, eli se ei vaadi erillistä määrittelemistä verkon yli toimiville ohjelmille. Se on myös täysin yhteensopiva Cisco IOS VLAN- ja reititysteknologioiden kanssa. Useamman VLAN:n toiminta EtherChannelin yli onnistuu Inter-Switch Linkin (ISL) VLAN Trunking-protokollan (Virtual Local Area Network Trunking Protocol, VTP) avulla. (Cisco Systems 2003.)

Yhtenä EtherChannelin rajoituksena on, että fyysisten porttien pitää sijaita samalla kytkimellä. Tästä poikkeuksena on stack eli useasta kytkimestä koostettu kytkinpino, joka toimii yhtenä kytkimenä. (Cisco Systems 2003.)

7.1.1 Spanning Tree Protocol EtherChannelissa

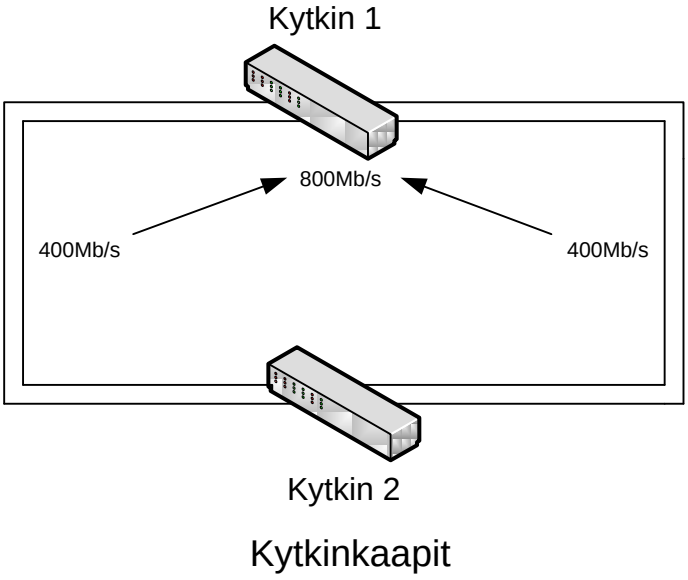
Kuviossa (kuvio 11) kytkimen 1 ja 2 välillä on kaksi erillistä EtherChannelia. Spanning tree protocol estää tämän vuoksi toisen toiminnan luuppien ehkäisemiseksi. Tämä topologia on käytännöllinen vikasietoisuuden kannalta, koska EtherChannel yhteydet ovat erillisillä verkkokorteilla.



KUVIO 11. Spanning tree protocol EtherChannelissa

7.1.2 Kaistanleveyden vikasietoinen skaalaus

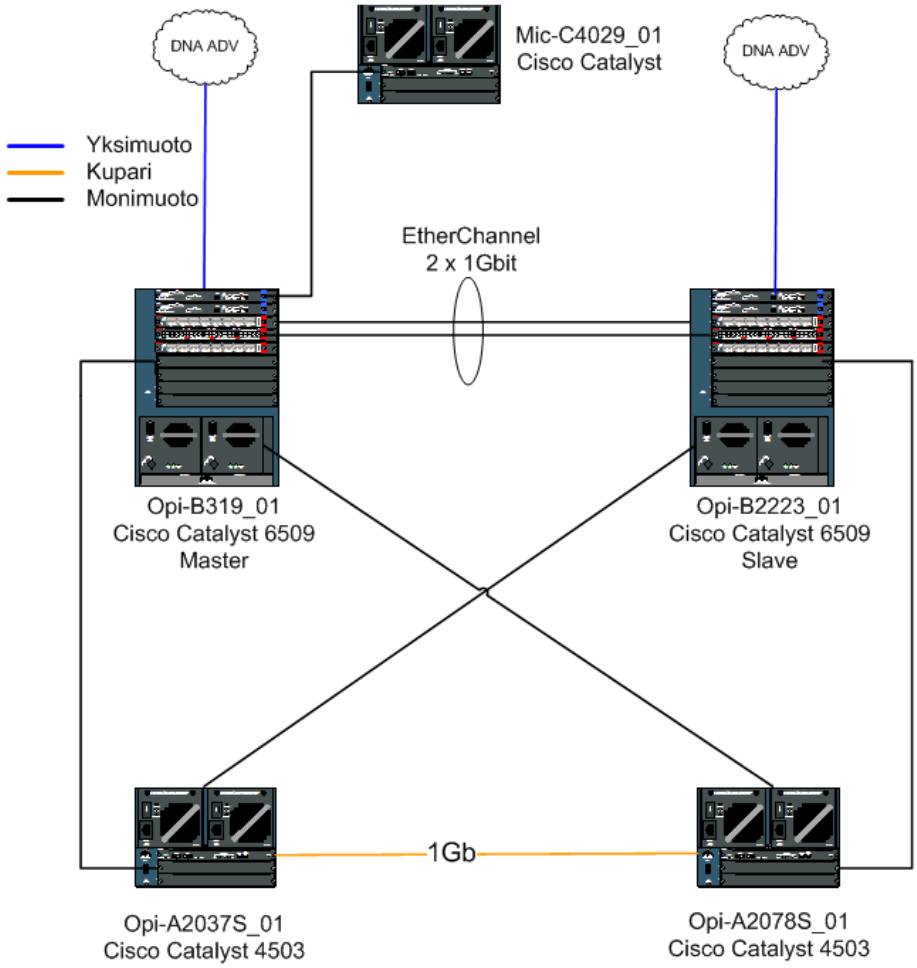
Kytkimet yksi ja kaksi ovat kytkettyinä neljällä Fast Ethernet -yhteydellä toisiinsa. Nämä yhteydet ovat EtherChannelissa. Kuvion (kuvio 12) ajatuksena on se, että kaapelointi tehdään eri teitä pitkin. Jos jostakin syystä toista reittiä menevät kaapelit vioittuvat, EtherChannel huolehtii yhteyksien uudelleenkanavoinnin ilman käyttäjille näkyvää katkosta. (Cisco Systems 2003)



KUVIO 12. Kaistanleveyden vikasietoinen skaalaus

7.2 EtherChannel Savonian verkossa

Savonian verkossa EtherChannel on toiminnassa kahden Cisco Catalyst 6509 -mallin runkokytkimen eli masterin (Opi-B319_01) ja slaven (Opi-B2223_01) välillä (kuvio 13). Se koostuu tällä hetkellä kahdesta Gigabitin linkistä. Näin ollen kaistanleveydeksi muodostuu 2 Gbit/s. Muutamia 2 Gbit/s EtherChannel -linkkejä on muodostettu myös palvelimille menevien kytkinten ja pääkytkinten välille.

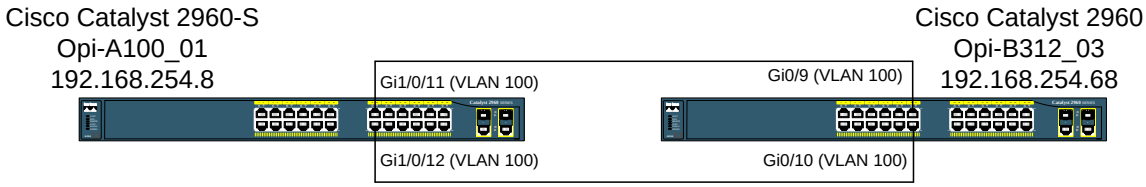


KUVIO 13. EtherChannel Savonian verkossa

7.3 EtherChannelin konfigurointi

EtherChannelin konfigurointi on suhteellisen yksinkertaista. Tässä esimerkissä käydään lyhyesti läpi kahden linkin EtherChannelin asettaminen kahden Cisco Catalyst 2960 -sarjan kytkimen välille. Testauksessa käytettiin kytkimiä ”Opi-A100_012” ja ”Opi-A110_01” (9.3 Testausympäristö). Kytkimet yhdistettiin kahdella Ethernet-kaapelilla seuraavan kuvion mukaan (kuvio 14). EtherChannelin

konfigurointi on suoritettu Ciscon kotisivuilta löytyvän verkkodokumentin (Cisco Systems 2010a, 862-865.) mukaan.



KUVIO 14. EtherChannelin testausympäristö

Ensimmäiseksi tehdään kytkimelle ”Opi-A100_01” seuraavat asetukset, joissa määritellään VLAN ja channel-group 5:n tila aktiiviseksi porteissa 11 ja 12:

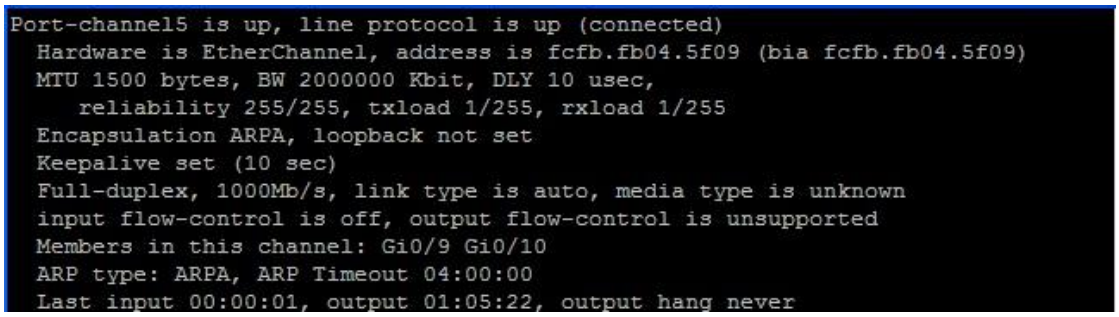
Opi-A100_01# configure terminal
Opi-A100_01(config)# interface range gigabitethernet1/0/11-12
Opi-A100_01(config-if-range)# switchport mode access
Opi-A100_01(config-if-range)# switchport access vlan 100
Opi-A100_01(config-if-range)# channel-group 5 mode active
Opi-A100_01(config-if-range)# end

Sama tehdään kytkimelle “Opi-B312_03” portteihin 9 ja 10:

Opi-B312_03# configure terminal
Opi-B312_03(config)# interface range gigabitethernet0/9-10
Opi-B312_03(config-if-range)# switchport mode access
Opi-B312_03(config-if-range)# switchport access vlan 100
Opi-B312_03(config-if-range)# channel-group 5 mode active
Opi-B312_03(config-if-range)# end

Tämän jälkeen voidaan katsoa, mikä on port-channelin tila komennolla:

Opi-B312_03#show interface port-channel 5

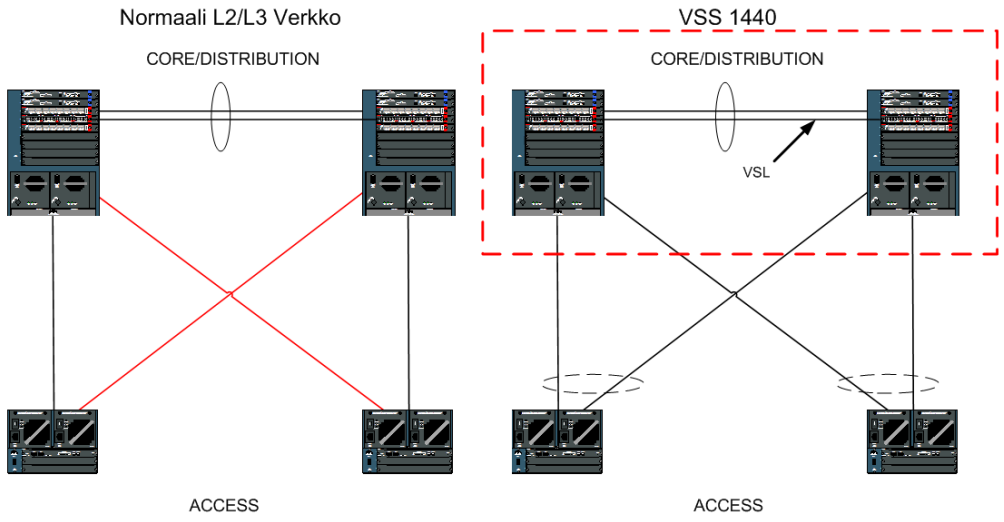


KUVA 2. Kuvankaappaus port-channelin tiedoista

Kuvankaappauksesta (kuva 2) selviää, että port-channel 5:n kaistanleveytenä on 2 Gbit/s (2 000 000 Kbit) ja sen jäseniä ovat portit ”Gi0/9” ja ”Gi0/10”. EtherChannel kytkimien välillä on näin ollen konfiguroitu.

8 KYTKINTEN VIRTUALISOINTI

Tässä luvussa käydään läpi Virtual Switching Systemin (VSS) toimintaperiaate, sen hyödyt ja kuinka virtualisointi teoriassa tapahtuu. Alla näkyvä kuvio (kuvio 15) esittää normaalin verkkoratkaisun ja VSS-verkon eroja. Siinä näemme, että normaalissa verkossa reunakytkimille menevät yhteydet ovat poissa käytöstä STP:n toimesta luuppien ehkäisemiseksi. Kahden Cisco Catalyst 6500 -sarjan kytkimen välillä on toiminnassa EtherChannel. VSS:ssä kytkimet ovat yhdistettu Virtual Switching Linkkien (VSL) avulla ja ne näkyvät ulospäin yhtenä. Näin ollen varalla olleet yhteydet otetaan hyötykäyttöön tuplaten nopeuden reunakytkimille (access).



KUVIO 15. Normaali L2/L3 verkko ja VSS-verkko

8.1 Virtual Switching Systemin toiminta

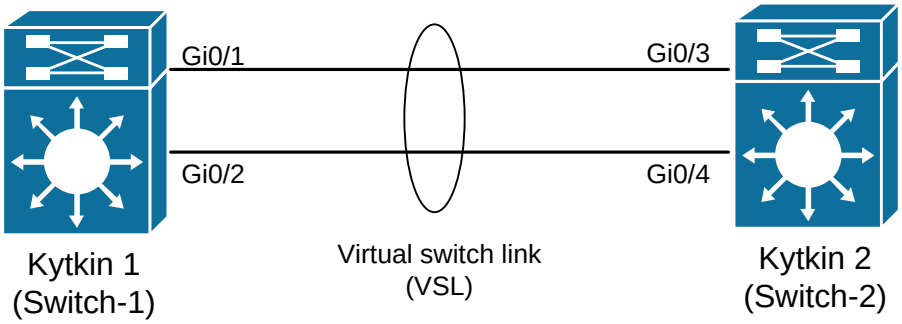
Virtual Switching System toimii kahden Cisco Catalyst 6500 -sarjan kytkimen välillä. Sen tarkoituksena on yhdistää nämä kytkimet niin että ne näkyvät ulkopuolelle yhtenä kytkimenä. VSS käyttää hyväkseen VSL-linkkejä, jotka varsinaisesti muodostavat linkin virtualisoinnin kohteena olevien kytkinten välille. (Cisco Systems 2012a, 3.)

8.2 Virtual Switching Systemin hyödyt

VSS:llä päästään jopa 1440 Gbit/s kaistanleveyteen. Maksimi nopeus on siis kahdeksantoistakertainen verrattuna EtherChannel-teknologiaan. VSS:llä voi kumpaakin kytkintä ohjataan yhden konfiguraation avulla ja se tarvitsee vain yhden yhdyskäytävän IP-osoitteen VLAN:ia kohden. Spanning tree-protokollaa ei enää tarvitse, vaan se korvaantuu Multichassis EtherChannel-teknologialla (MEC). (Cisco Systems 2012a, 1-2.)

8.3 Virtual Switching Systemin konfigurointi

Testauslaitteiston puutteesta johtuen tämä osio käydään vain teoriassa. Se noudattaa Cisco Systemsin sivuilta löytyvää ohjetta (Cisco Systems 2012c.). Toiston eliminoimiseksi X:llä merkityt kytkinten numerot viittaavat konfiguroitavaan kytkimeen. Alla näkyvä kuvio (kuvio 16) esittää virtualisoitavien kytkinten tiedot ja topologian.



KUVIO 16. Virtualisoitavien kytkinten topologia

8.3.1 Runkojen konfiguraatiotiedostojen varmuuskopiointi

Ennen virtualisoinnin aloittamista on hyvä tehdä kummankin kytkimen konfiguroinneista varmuuskopiot vaikka kytkimen flash-muistille, jotta palautus virtualisoinnista olisi vaivatonta. Ensimmäiseksi kopioidaan ajossa olevat asetukset aloituskonfiguraatioksi:

Switch-X# copy running-config startup-config

Tämän jälkeen aloituskonfiguraatio tallennetaan flash-muistille:

Switch-X# copy startup-config flash:old-startup-config

Kopioinnin jälkeen voidaan jatkaa itse virtualisoinnin pariin.

8.3.2 NSF ja SSO

VSS:ssa kytkimen vikasietoisuus toimii nonstop forwarding (NSF) ja stateful switchover (SSO) avulla. SSO:n aktivoimiseksi tehdään seuraava konfiguraatiomuutos molemmille kytkimille:

Switch-X(config)# redundancy
Switch-X(config-red)# mode sso
Switch-X(config-red)# exit
Switch-X(config)# router "routing_protocol" "processID"
Switch-X(config-router)# nsf
Switch-X(config-router)# end

Router komennossa parametreiksi (routing_protocol, processID) tulisi esimerkiksi Savonian kytkimillä käytetyt ”bgp” (Border Gateway Protocol) ja ”65022”. Tämän jälkeen varmistetaan, että SSO ja NSF ovat päällä ja kytkin operoi redundanssitilassa:

Switch-X# show running-config
Switch-X# show redundancy states

Virtuaalikytkinten domain ja numerointi

Kummankin kytkimen täytyy olla samassa virtual switch domainissa. Numerointi voi olla mikä tahansa välillä 1-255 ja sen täytyy olla jokaiselle verkon VSS:lle yksilöllinen. Domainin asettaminen ja numerointi tapahtuu seuraavalla tavalla:

Switch-X(config)# switch virtual domain 100
Switch-X(config-vs-domain)# switch X
Switch-X(config-vs-domain)# exit

8.3.3 Virtual Switch Link -porttien ja -channelien konfigurointi

Kun VSL konfiguroidaan, täytyy porttikanavien (port channel) numeroiden olla kummallekkin kytkimelle yksilölliset. Ensin täytyy kuitenkin tarkistaa, että kyseiset kanavanumeroinnit eivät ole käytössä:

Switch-X(config)# show running-config interface port-channel

Asetetaan kytkimelle 1 porttikanava numerolla 10 ja tehdään kyseessä olevasta kytkimestä sen omistaja:

Switch-1(config)# interface port-channel 10
Switch-1(config-if)# switch virtual link 1
Switch-1(config-if)# no shutdown
Switch-1(config-if)# exit

Tehdään samat konfiguraatiot kytkimelle 2, mutta numeroidaan porttikanava numerolla 20:

Switch-2(config)# interface port-channel 20
Switch-2(config-if)# switch virtual link 2
Switch-2(config-if)# no shutdown
Switch-2(config-if)# exit

Tämän jälkeen lisätään kytkimen 1 gigabitethernet 0/1-2 portit kanavaryhmään (channel group) 10:

Switch-1(config)# interface range gigabitethernet 0/1-2
Switch-1(config-if)# channel-group 10 mode on
Switch-1(config-if)# no shutdown

Tehdään samat muutokset kytkimelle 2 portteihin gigbitethernet 0/3-4 ja lisätään ne kanavaryhmään 20:

Switch-2(config)# interface range tengigabitethernet 0/3-4
Switch-2(config-if)# channel-group 20 mode on
Switch-2(config-if)# no shutdown

8.3.4 Kytkinten muuntaminen virtuaalikytkintilaan

Muuntaminen vaatii lopuksi kummankin kytkimen uudelleenkäynnistyksen. Ennen käynnistystä varmistetaan, että PFC-operointimoodi (policy feature card) on toiminnassa:

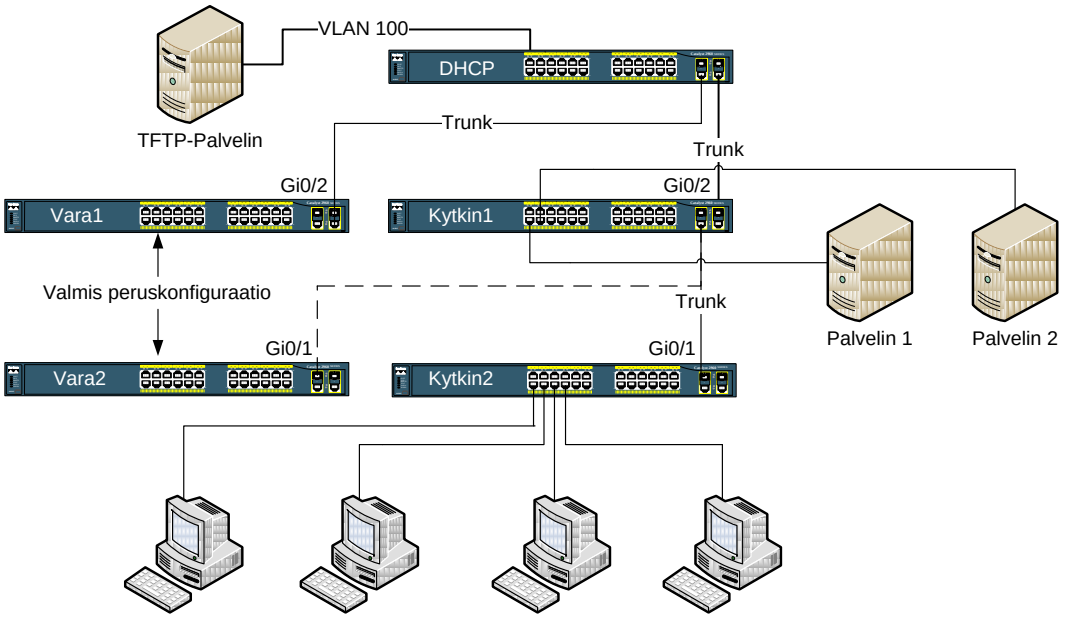
Switch-X# show platform hardware pfc mode
Switch-X(config)# platform hardware vsl pfc mode pfc3c

9 KYTKINTEN KONFIGURAATIOIDEN VARMUUSKOPIOINTIJÄRJESTELMÄ

Tässä luvussa käydään läpi suunnitelma kytkinten konfiguraatiotiedostojen varmuuskopionnista ja niiden palautuksesta. Suunnitelma pitää sisällään tärkeiden varakytkinten nopean käyttöönoton ja rikkoutuneiden sijalle tuotujen kytkinten saattamisen käyttökuntoon. Ajatuksena oli saada helppo ja toimiva järjestelmä ajan tasalla olevien konfiguraatioiden nopeaan siirtämiseen varakytkimelle.

9.1 Varmuuskopiointijärjestelmän suunnitelma

Alla näkyvässä kuviossa (kuvio 17) kytkin1 edustaa tärkeää kytkintä, johon on liitetty palvelimia. Tämä kytkin lähettää automaattisesti tietyin väliajoin konfiguraatiotiedostonsa hallinta-VLAN:ssa (VLAN 100) olevalle TFTP-palvelimelle (Trivial File Transfer Protocol). Tälle kytkimelle on olemassa varakytkin (Vara1) odottamassa välittömässä läheisyydessä. Vara1 on oletuksena kytketty pois päältä, mutta se on kaapeloitu hierarkiassa ylempänä olevaan samasta portista kuin kytkin1. Vara1:lle on säädetty peruskonfiguraatio, jolla se käynnistyksen yhteydessä ottaa yhteyden TFTP-palvelimeen (9.4 TFTP-Palvelin). Vara1 lataa palvelimelta kytkin1:n varmuuskopioidun konfiguraation. Tähän varakytkimeen ei saa kytkeä virtaa, jos kytkin1 on toiminnassa.



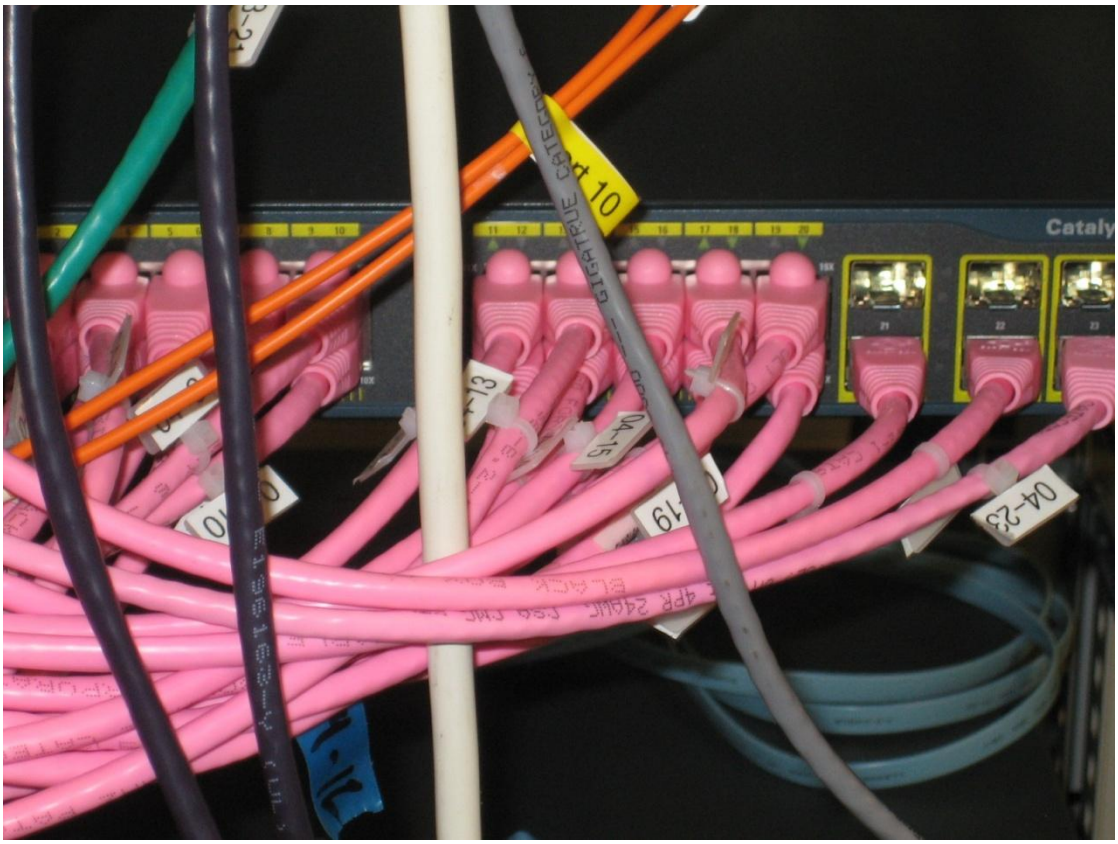
KUVIO 17. Varmuuskopointijärjestelmän suunnitelma

Järjestelmä tarvitsee DHCP-palvelimen (Dynamic Host Configuration Protocol) automaattista konfiguraation latausta varten (9.8 DHCP-palvelin). Toimivuuden kannalta DHCP-palvelin pitää asentaa verkon hierarkiassa mahdollisimman lähellä TFTP-palvelinta olevalla kytkimelle.

Kytkimet, joille ei ole odottamassa valmista varakytkintä, tulee olla samaa varalla samaa mallia oleva kytkin. Tässä varalla olevassa kytkimessä on valmis peruskonfiguraatio. Tällä konfigraatiolla on valmius telnet-yhteyteen, ja sen hallinta-VLAN:lle on annettu väliaikainen IP-osoite. Tätä osoitetta ei saa löytyä mistään muusta hallinta-VLAN:ssa olevasta laitteesta. Kytkimen ensimmäiseen porttiin on säädetty trunk-asetukset. Valmis peruskonfiguraatio näille kytkimille löytyy liitteestä 1.

9.2 Kaapeleiden merkinnät ja vaihto

Kytkimissä olevat kaapelit täytyy olla hyvin ja selkeästi merkattuja (kuva 3), jotta uuden kytkimen käyttöönotto olisi mahdollisimman vaivatonta. Samalta kytkimeltä lähtevien kaapelien yhtenäinen väritys auttaa myös selkeyttämään vaihtoa.

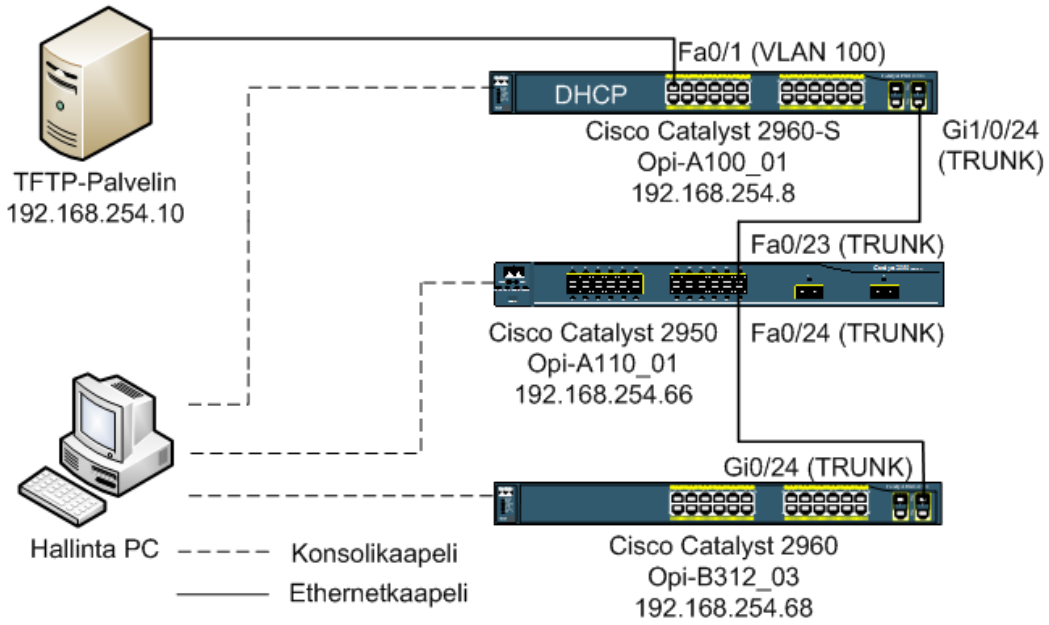


KUVA 3. Kaapeloinnin merkinnät. (Valokuva Miika Räisänen 2012)

Varakytkimen käynnistyksen yhteydessä, tai sen jälkeen, kaapelit siirretään manuaalisesti alkuperäisestä kytkimestä uuteen. Koska kaapelit on numeroitu porttien mukaan, saadaan ne nopeasti samoihin paikkoihin kuin alkuperäisessä kytkimessä.

9.3 Testausympäristö

Työ toteutettiin testausympäristössä (kuvio 18), johon kuului TFTP-palvelimena toiminut Windows XP-PC (Opi-TFTP), kolme kappaletta Cisco Catalyst 2900 -sarjan kytkintä ja PC-laitteisto kytkinten hallintaa varten. Kytkinten hallinta tapahtui konsolikaapeleiden ja TFTP-palvelin koneelle asennetun PuTTY telnet/ssh-asiakasohjelman avulla. Kytkimet olivat liitettyinä toisiinsa trunk-porttien kautta. TFTP-palvelin hallinta-VLAN:ssa oli kytkettynä DHCP-palvelina toimivaan kytkimeen (Opi-A100_01).



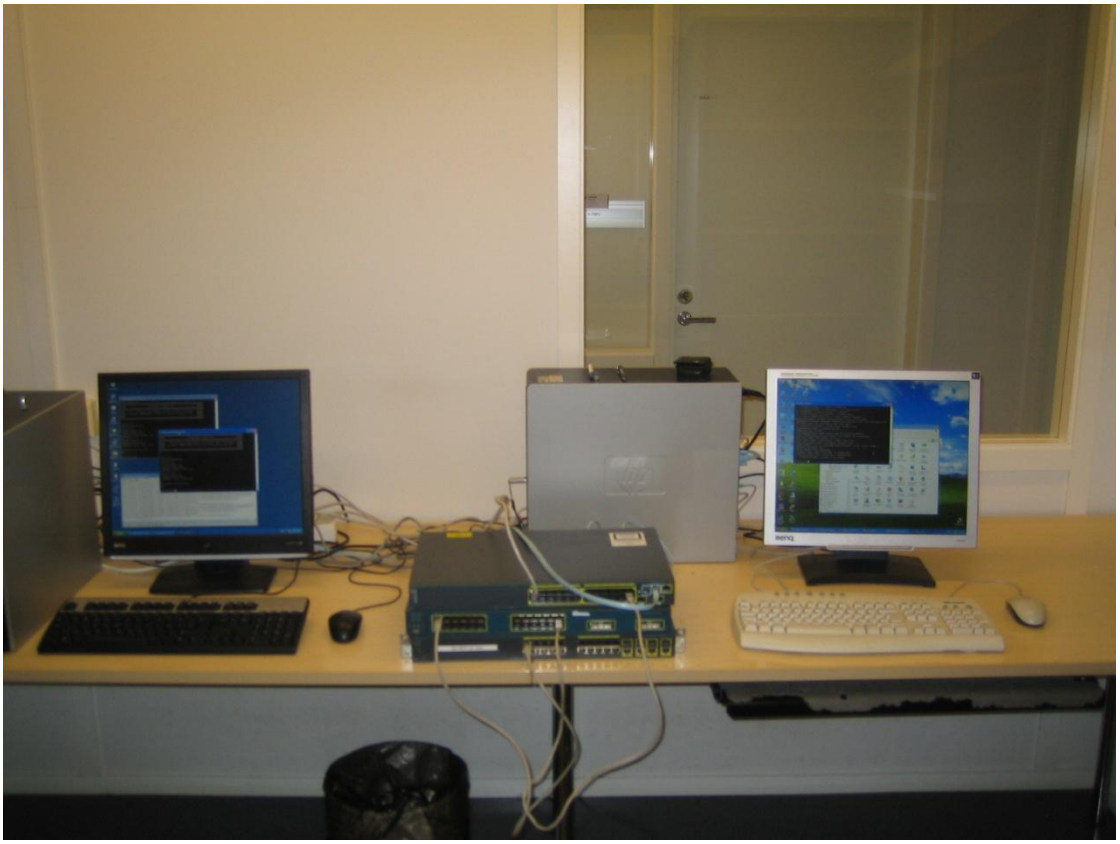
KUVIO 18. Testausympäristön kaaviokuva

Seuraava taulukko (taulukko 1) esittää tarkemmin laitteiden mallit, roolin testauksessa, nimet, IP-osoitteen, aliverkon maskin, sekä sen, mistä liitteestä kyseisen kytkimen konfiguraatiotiedosto löytyy. Kytkinten konfiguraatiot ovat muokattuja versioita Savonian käyttämistä konfiguraatioista.

TAULUKKO 1. Testauskokoonpanon tiedot

Laite	Rooli	Nimi	IP/Aliverkon maski	Liite
Cisco Catalyst 2960-S	DHCP-palvelin	Opi-A100_01	192.168.254.8/24	2
Cisco Catalyst 2950	Testialusta	Opi-A110_01	192.168.254.66/24	3
Cisco Catalyst 2960G	Testialusta (Backup)	Opi-B312_03	192.168.254.68/24	4
HP Compaq dc5750	TFTP-palvelin	Opi-TFTP	192.168.254.10/24	-

Kuva 4 esittää testauslaboratoriota, jossa testaus suoritettiin. Vasemmalla on TFTP-palvelimena toiminut Windows XP-PC. Keskellä ovat kytkimet ja oikealla Windows XP:lla varustettu kytkinten hallintaan käytetty PC.



KUVA 4. Testauslaboratorio. (Valokuva Miika Räisänen 2012)

Kuva 5 on lähikuva testauksessa käytetyistä kytkimistä. Päällimmäisenä DHCP-palvelimena käytetty Cisco Catalyst 2960-S (Opi-A100_01), keskellä vanha Cisco Catalyst 2950 (Opi-A110_1) ja alimmaisena Cisco Catalyst 2960G (Opi-B312_03).

KUVA 5. Testauksessa käytetyt kytkimet. (Valokuva Miika Räisänen 2012)

9.4 TFPT-palvelin

TFTP (Trivial File Transfer Protocol) on yksinkertainen tiedostonsiirtoprotokolla. Sitä käytetään usein konfiguraatiotiedostojen ja boottitiedostojen siirtoon lähiverkossa. TFTP on hyvin rajattu protokolla. Siitä puuttuu esimerkiksi FTP:stä (File Transfer Protocol) tuttu autentikointi ja lisäksi kaikki tiedostot lähetetään salaamattomana.

Konfiguraatiotiedostojen varmuuskopiot tallennetaan tekstimuodossa TFTP-palvelimelle. Koska tiedostojen siirto tapahtuu salaamattomana, palvelin toimii erillisessä hallinta-VLAN-verkossa. Tämä verkko on palomuurein suojatussa Savonian sisäverkossa, joten ulkopuolelta tuleva tietoturvauhka on suhteellisen pieni.

9.4.1 TFTP-palvelimen asennus

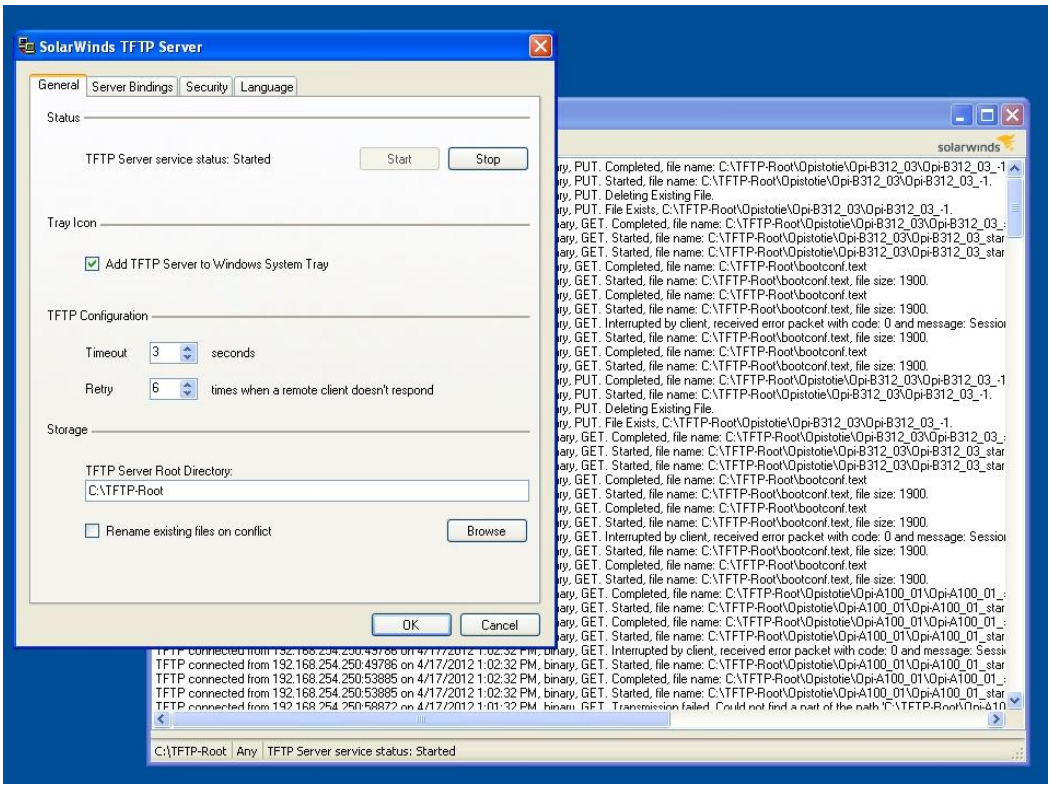
Testausympäristössä käytettiin Solarwinds:n ilmaista TFTP-palvelinta, jollainen on myös asennettuna Savonian verkkoon. Palvelin tarvitsee toimiakseen Windows-

käyttöjärjestelmällä toimivan PC-koneen tai Palvelimen. Testauksessa palvelin asennettiin Windows XP käyttöjärjestelmään.

Asennus tapahtuu normaalisti käynnistämällä asennustiedosto ja seuraamalla asennusohjetta. Tavanomaisesti asennuskansion saa valita, mutta tämä ohjelma asentuu automaattisesti oletuskansioon. Asennuksen lopuksi TFTP-palvelin käynnistyy.

9.4.2 TFTP-palvelimen käyttöönotto

Solarwinds TFTP-palvelin on periaatteessa suoraan käytettävissä asennuksen jälkeen. Testausympäristössä ei perusasetuksiin ollut tarvetta puuttua. Tärkeintä on jättää kohta ”Rename existing file on conflict” (kuva 6) valitsematta, jotta tiedostojen nimet pysyvät johdonmukaisina. Asia on tarkemmin esitettynä seuraavassa alaluvussa (9.4.3 TFTP-palvelimen tiedostorakenne).



KUVA 6. Kuvankaappaus Solarwinds TFTP-palvelimen asetuksista ja logi-ikkunasta

9.4.3 TFTP-palvelimen tiedostorakenne

Järjestelmä on hyvin tarkka tiedostojen ja kansioiden nimistä. Nimien täytyy olla täsmälleen oikein, koska tallennus ja haku tapahtuu tiedostopolkujen mukaan.

Hakemistopolku lähtee TFTP-Root-kansiosta (C:\TFTP-Root). Tätä palvelimella olevaa kansioita ei oteta huomioon.

TFTP-Root-kansioon luodaan manuaalisesti pääkansiot, jotka nimetään kytkinten sijainnin mukaan. Tällä tarkoitetaan tässä tapauksessa kampuksen sijaintia. Näitä ovat esimerkiksi Opistotie ja Microkatu. Pääkansioiden alle luodaan alikansiot kytkinten nimien mukaan. Hakemistopoluksi tulee näin ollen esimerkiksi ”Opistotie\Opi-B312_03\”.

9.5 Archive

Archive on Cisco-kytkinten komento, jolla kytkimelle tallennetut konfiguraatiomuutokset voidaan automaattisesti tallentaa haluttuun paikkaan. Tähän kuuluu tallentaminen muistiin ja varmuuskopiointi palvelimelle tietyin väliajoin, sekä käyttäjän manuaalisesti tallentaman konfiguraation arkistointi.

9.5.1 Automaattinen tallennus TFTP-palvelimelle

Archive-komennon toimeen saattamiseksi täytyy kytkimelle asettaa seuraavat komennot globaalissa konfigirointitilassa.

```
Opi-B312_03(config)#archive
 Opi-B312_03(config-archive)#path tftp://192.168.254.10/Opistotie/$h/$h_
 Opi-B312_03(config-archive)#write-memory
 Opi-B312_03(config-archive)#time-period 1440
```

Komennolla archive päästään archiven konfigurointitilaan (config-archive), jossa asetetaan halutut parametrit. Path määrittää käytettävän polun ja tiedoston nimen eli tässä tapauksessa se ohjaa konfiguraatiotiedoston TFTP-palvelimelle valmiiiksi tehtyyn kansioon. Polussa $h-merkintä viittaa kytkimen nimeen, joka toimii tässä tapauksessa Opistotie-kansion alikansiona. Sama pätee myös tiedoston nimeen sillä poikkeuksella, että kytkimen nimen jälkeen tulee alaviiva. Kytkimen nimen ollessa esimerkiksi ”Opi-B312_03” tiedostopoluksi tulee näin ollen ”Opistotie/Opi-B312_02/Opi-B312_03_”.

Archive lisää jokaiselle uudelle tallennukselle tunnisteen tiedoston nimen perään. Tämä tunniste on vanhoissa kytkimissä nouseva järjestysluku, joka alkaa ykkösestä

(Opi-B312_03_**-1**). Joissakin uusimmissa kytkimissä (esim. Cisco Catalyst 2960-S) lisätty oletuksena vielä päivämäärä ja kellonaika (Opi-B312_03_**-Mar—1-10-47-11.167**-2) tähän nimeen.

Jotta archive tietäisi koska tallennus tehdään, lisätään rivi ”write memory”. Tällöin käyttäjän tallentaessa kyseisellä komennolla kytkin lähettää konfiguraation TFTP-palvelimelle.

Time period määrää kuinka monen minuutin välein kytkimen konfiguraatio tallennetaan automaattisesti. Esimerkkitapauksessa tallennus tapahtuu 1440 minuutin välein eli kerran vuorokaudessa.

9.5.2 Arkistoitujen konfiguraatioiden palautus

Archiven tallentamat tiedostot luetteloidaan järjestyksessä kytkimelle. Tämän saa näkyviin syöttämällä pääkäyttäjätilassa komennon ”show archive”. Viimeisin tallennus on merkattu nuolella (kuva 7) ja seuraavan tallennuksen nimi on kerrottu ensimmäisellä rivillä. Tämä luettelointi nollautuu ja tiedostojen numerointi aloitetaan alusta, jos kytkimestä sammutetaan virta. Näin ollen vanhat TFTP-palvelimella samoilla nimillä olevat tiedostot joutuvat ylikirjoitetuiksi.

```
Opi-B312_03#sh archive
The next archive file will be named tftp://192.168.254.10/Opistotie/Opi-B312_03/
Opi-B312_03_-5
 Archive #  Name
   0
   1        tftp://192.168.254.10/Opistotie/Opi-B312_03/Opi-B312_03_-1
   2        tftp://192.168.254.10/Opistotie/Opi-B312_03/Opi-B312_03_-2
   3        tftp://192.168.254.10/Opistotie/Opi-B312_03/Opi-B312_03_-3
   4        tftp://192.168.254.10/Opistotie/Opi-B312_03/Opi-B312_03_-4 <- Most Re
cent
   5
   6
   7
   8
   9
   10
   11
   12
   13
   14
Opi-B312_03#
```

KUVA 7. Kuvankaappaus Archiven arkistointiluettelosta

Luettelosta otetaan ylös viimeisin tai haluttu tiedostopolku ja konfiguraation voi palauttaa pääkäyttäjätilassa seuraavalla komennolla:

Opi-B312_03#configure replace tftp://192.168.254.10/Opistotie/Opi-B312_03/Opi-B312_03_-4

Esimerkissä käytetään testauksessa käytettyä TFTP-palvelimen IP-osoitetta ja tiedoston nimeä, jonka lopussa näkyy archiven tekemä arkistointinumero eli ”-4”. Tämän jälkeen on syytä ajaa *”write memory”* komento, jotta tallennetut muutokset siirtyvät aloitusasetuksiksi.

9.6 Kron

Kron on Cisco IOS 12.3(1) -version mukana tullut pääkäyttäjätilassa tapahtuvien komentojen ajastusominaisuus. Toiminnolla voidaan ajastaa pääkäyttäjätilan komentoja. Rajoituksena on ettei komennoissa saa olla käyttäjän väliintuloa vaativia kyselyitä. Tälläinen kysely voi olla esimerkiksi, että halutaanko tallennettava tiedosto ylikirjoittaa jo olemassa olevan tiedoston päälle. Tästä johtuen samalla tiedoston nimellä tallentaminen esimerkiksi kytkimen flash-muistille ei onnistu.

Kronin käyttö archiven sijasta johtuu siitä, että archive tallentaa tiedostot aina eri nimellä. Tiedostolle tarvittiin staattinen nimi, jotta automaattinen installointi toimisi. Kronilla tapahtuva konfigurointitiedostojen varmuuskopointi antaa tähän mahdollisuuden.

9.6.1 Kron policy-list

Ensimmäiseksi täytyy laatia Kron policy-list. Tässä listataan mitä kron tekee, kun policy-listiä käytetään. Testauksessa käytettiin listan nimenä ”talleta”. Tähän listaan lisätään käynnistyskonfiguraation näyttö, joka ohjataan TFTP-palvelimelle samaan polkuun kuin archivella (9.5.1 Automaattinen tallennus TFTP-palvelimelle). Erona on vain se, että tiedoston nimi on muotoa ”Kytkimen_nimi_start”.

Opi-B312_03(config)#kron policy-list talleta
Opi-B312_03(config-kron-policy)#cli show start | redirect tftp://192.168.254.10/Opistotie/Opi-B312_03/Opi-B312_03_start

9.6.2 Kron occurrence

Kron occurence määrää sen kuinka usein tai milloinka policy-list otetaan käyttöön. Ajastukselle määrätään nimi ja aika (at) tai aikaväli (in). Työssä käytettiin aikaväliä kerran vuorokaudessa. Tämä ilmoitetaan muodossa ”vuorokaudet:tunnit:minuutit” (dd:hh:mm). Näin ollen kaikki kytkimet eivät lähetä tiedostoja yhtä aikaa vaan riippuen siitä milloin viimeinen lähetys on tapahtunut. Tapahtuman voi ajastaa käynnistymään joko toistuvasti (recurring) tai kerran (one-shot).

Opi-B312_03(config)#kron occurrence ajastus in 1:0:0 recurring
Opi-B312_03(config-kron-occurrence)#policy-list talleta

Ajastus on siis asetettuna tapahtumaan kerran vuorokaudessa ja käyttää policy-list:iä “talleta”.

9.7 Konfiguraatiotiedoston siirto manuaalisesti varakytkimelle

9.7.1 Varakytkimen peruskonfiguraatio

Manuaalisesti konfiguroitaville varakytkimille pitää asettaa VLAN ja sille väliaikainen IP-osoite. Tämä tapahtuu globaalissa konfiguraatiotilassa käskyillä:

Opi-B312_03(config)#interface vlan100
Opi-B312_03(config-if)#ip address 192.168.254.250 255.255.255.0

IP-osoitteen pitää olla hallinta-VLAN:in osoitealueella eli 192.168.254.0/24, mutta se ei saa olla sama kuin jonkin muun laitteen kyseisessä VLAN:ssa. Trunk-portiksi asetetaan kytkimen ensimmäinen portti:

Opi-B312_03(config)# interface GigabitEthernet0/1
Opi-B312_03(config-if)# switchport mode trunk
Opi-B312_03(config-if)# switchport nonegotiate

Toinen tapa on laittaa yksi kytkimen porteista VLAN100 access -tilaan ja kytkeä se vastaavasti toiseen VLAN100:ssa olevaan porttiin:

Opi-B312_03(config)# interface GigabitEthernet0/1

Opi-B312_03(config-if)# switchport mode access
Opi-B312_03(config-if)# switchport access vlan 100

Mahdollista telnet-yhteyttä varten konfiguroidaan seuraavat rivit:

Opi-B312_03(config-if)#line vty 0 15
Opi-B312_03(config-line)#password paastasisaan
Opi-B312_03(config-line)#login

Yhteys telnetillä tarvitsee salasanan eli tässä tapauksessa se on ”paastasisaan”. Salasana voi olla mikä vaan, koska se korvautuu konfiguraation vaihtuessa oikeaan. Varakytkimen täydellinen konfiguraatiotiedosto on esitettynä liitteessä 1.

9.7.2 Konfiguraatiotiedoston kopiointi manuaalisesti kytkimelle

Kronilla tallennetut tiedostot voi palauttaa käyttämällä samaa käskyä kuin archivella tallennetut. Tiedoston polkuna käytetään kronille määrättyä polkua:

Opi-B312_03#configure replace tftp://192.168.254.10/Opistotie/Opi-B312_03/Opi-B312_03_start

Kytkimen otettua muutokset käyttöön, tallennetaan uusi konfiguraatio kytkimen muistille:

Opi-B312_03#write memory

9.8 DHCP-palvelin

AutoInstall (9.9 AutoInstall) tarvitsee toimiakseen IP:n DHCP-palvelimelta. Testausympäristössä palvelin asennettiin Cisco Catalyst 2960-S -kytkimelle (Opi-A100_01). Varsinaisessa toteutuksessa tämän palvelimen tulee olla mahdollisimman ylhäällä lähiverkon hierarkiassa.

9.8.1 DHCP-palvelimen asennus kytkimelle

DHCP-palvelimen saatamiseksi käyttöön täytyy kytkimellä ajaa globaalissa konfiguraatiotilassa käsky:

Opi-A100_01(config)#service dhcp

Tällä käskyllä kytkin asettuu DHCP-palvelintilaan. Näin kytkin kuuntelee DHCP-pyyntöjä ja jakaa niiden mukaan IP-osoitteet DHCP-poolien mukaan (9.8.2 DHCP pool).

9.8.2 DHCP pool

Testauksessa käytettiin neljää DHCP-poolia, koska haluttiin varmistaa, että asetukset tulevat oikeasta paikasta. Pooli määritellään globaalissa konfiguraatiotilassa antamalla käsky:

Opi-A100_01(config)#ip dhcp pool Opi-B312_03

Käskyllä päästään DHCP:n konfigurointitilaan (dhcp-config), jossa säädetään AutoInstallia varten IP-osoite, hallinta-VLAN tunnistetiedot, käynnistystiedoston sijainti sekä TFPT-palvelimen verkko-osoite.

Opi-A100_01(dhcp-config)#host 192.168.254.250 255.255.255.0

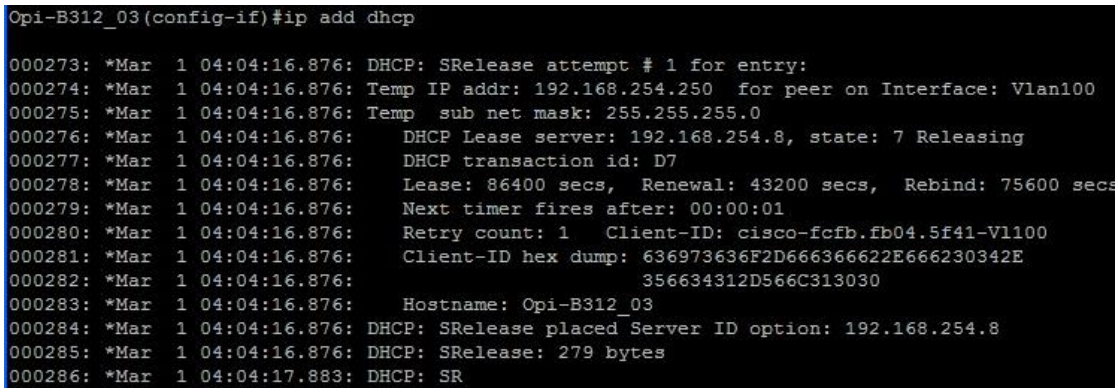
Host-komennolla määritetään IP-osoite ja verkon maski, jonka varakytkin saa väliaikaisesti AutoInstallia varten.

Opi-A100_01(dhcp-config)#client-identifier
0063.6973.636f.2d66.6366.622e.6662.3034.2e35.6634.312d.566c.3130.30

AutoInstallin lähettäessä DHCP pyynnön tulee sen mukana ascii-muotoinen client-id kenttä, jolla palvelin tunnistaa kytkimen. Koska kyseessä on L2-tason kytkin, portteihin ei voi määrätä IP-osoitteita. Tästä syystä tunnistamiseen ja IP-osoitteen hankkimiseen käytetään VLAN:ia. Client-identifierinä toimii siis hallinta-VLAN:n tunniste.

Normaalisti tunnistamiseen käytetään hardware address -komentoa ja hallinta-VLAN:in MAC-osoitetta, mutta se ei tuntemattomasta syystä toiminut. Client-identifier ei myöskään toiminut suoraan, ja sen joutui muuntamaan heksadesimaalimuotoon. Varmimmin heksadesimaalimuodon saa selville laittamalla VLAN etsimään IP-

osoitetta komennolla ”ip dhcp”. Jotta IP-osoitteen hakuyritys onnistuisi, kytkin täytyy olla yhdistettynä trunk-portista toiseen kytkimeen. Tämän jälkeen pääkäyttäjätilassa syötetään komento ”debug dhcp detail”. Kytkin menee debuggaustilaan (KUVA 8), josta client-id:n heksadesimaalimuodon voi poimia ”HEX dump” -kohdasta. Tähän pitää lisätä vielä kaksi nollaa eteen. Debuggaus tilasta pääsee pois kirjoittamalla ”undebug all” tai ”undebug dhcp detail”.



KUVA 8. Kuvankaappaus debuggerin tulosteesta

Toinen tapa muuntaa client-id heksadesimaalimuotoon on käyttää kääntäjää, jolla saa ascii-muodon heksadesimaaliksi. Kääntäjiä on saatavana ilmaiseksi googlen avulla ohjelmistoina sekä selainpohjaisina.

Client-id on ascii-muodossa ”cisco-[VLAN 100 MAC-osoite]-Vl100”. VLAN 100:n MAC-osoitteen saa selville pääkäyttäjätilassa komennolla:

Opi-B312_03#show interface vlan 100

Esimerkkitapauksessa se on ”fcfb.fb04.5f41”, joten client-id on muotoa ”cisco-fcfb.fb04.5f41-Vl100”. Kun tämä ajetaan kääntäjän läpi, saadaan sama heksadesimaaliluku kuin kuvassa 8. Myös tähän lukuun täytyy lisätä kaksi nollaa eteen.

Seuraavaksi määritellään bootfile-komennon avulla varsinaisen kytkimen varmuuskopioidun tiedoston polku TFTP-palvelimella:

Opi-A100_01(dhcp-config)#bootfile Opistotie/Opi-B312_03/Opi-B312_03_start

Option -komennolla asetetaan erinäisiä valintoja, joita palvelin noudattaa. Näitä voi olla esimerkiksi WWW- tai DNS-palvelimen sijainnin määritys. Tässä tapauksessa option komennolle annetaan arvo 150 eli TFTP-palvelimen sijainti.

Opi-A100_01(dhcp-config)#option 150 ip 192.168.254.10

9.9 AutoInstall

AutoInstall on Cisco Catalyst -kytkinten ohjelma, jolla kytkimelle voidaan automaattisesti käynnistyksen yhteydessä ladata aloituskonfiguraatio. Sen ensisijainen tarkoitus on ladata peruskonfiguraatio, jossa on vain tärkeimmät asetukset laitteen telnet-yhteyden saattamiseksi toimintakuntoon. Tämän jälkeen laite konfiguroitaidaan manuaalisesti telnet-yhteyden avulla. Toinen vaihtoehto on että laitteen koko konfiguraatio ladataan laitteelle. Koska varmuuskopiontijärjestelmän toimivuus perustuu siihen, että varakytkimelle saadaan tuorein versio konfiguraatiotiedostosta, valitaan jälkimmäinen vaihtoehto. AutoInstallia varten tehty konfiguraatio löytyy liitteestä 5.

9.9.1 Ip helper-address

Ip helper-address -komento sijoitetaan hallinta-VLAN liitäntään (VLAN 100). Tämä täytyy tehdä jokaiselle verkon kytkimelle järjestelmän toiminnan varmistamiseksi. Komennolla viitataan DHCP-palvelimeen, jotta AutoInstall osaa hakea IP-osoitteen oikealta palvelimelta. Testauksessa DHCP-palvelimen IP-osoite oli 192.168.254.8. Ip helper-adressin asettaminen tapahtuu siis globaalissa konfiguraatiotilassa komennoilla:

Opi-B312_03(config)#interface Vlan100
Opi-B312_03(config-if)#ip helper-address 192.168.254.8

9.9.2 Varakytkimen konfigurointi AutoInstallia varten

Varakytkimelle tehdään yksinkertainen konfiguraatio, jolla se saadaan toimimaan hallinta-VLAN:ssa ja käyttämään AutoInstallia käynnistyksen yhteydessä. Ensimmäiseksi konfiguroidaan VLAN 100 ja sille ip helper-address (9.9.1 Ip helper-address). Sen jälkeen tehdään trunk-portti samasta portista kuin varsinaisella

kytkimellä sisään tulevasta (uplink) portista. Esimerkissä käytetään porttia gigabitethernet 0/24. Käskyt annetaan globaalissa konfiguraatiotilassa:

Opi-B312_03(config)#interface GigabitEthernet0/24
Opi-B312_03(config-if)#switchport mode trunk
Opi-B312_03(config-if)#switchport nonegotiate

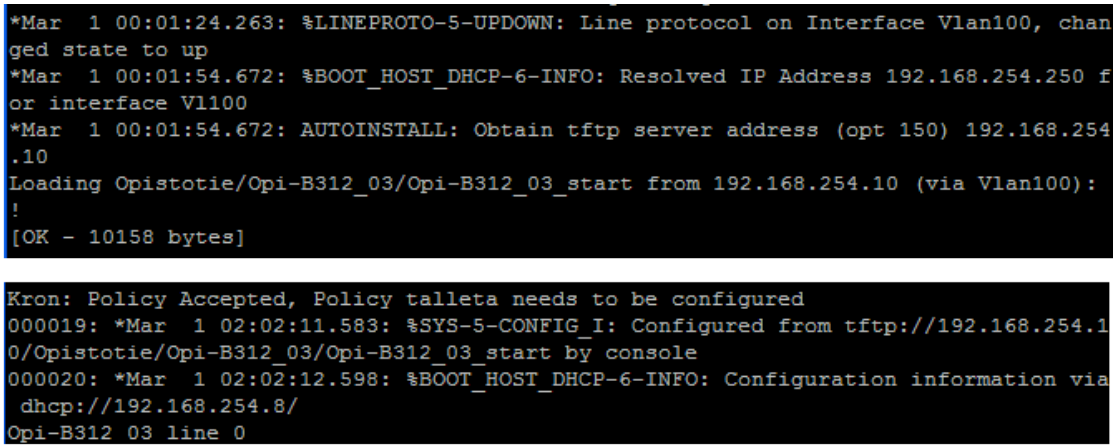
Tämän jälkeen asetetaan globaalissa konfiguraatiotilassa boot-valinnat:

Opi-B312_03(config)#boot host dhcp
Opi-B312_03(config)#boot host retry timeout 300

Tässä “boot host dhcp” määrää kuinka käynnistys tapahtuu. Toinen kohta eli ”boot host retry timeout 300” kertoo kuinka monta sekuntia AutoInstallia yritetään. Asetuksen pois jättäminen johtaa siihen, että kokeiluja on loputtomasti.

9.9.3 AutoInstallin toiminta ja eteneminen

Oheisessa kuvassa (kuva 9) on kuvankaappaus AutoInstallin onnistumisesta. Kuvaa on muokattu jättämällä tarpeettomat rivit pois. Ylimmäisellä rivillä näkyy, että VLAN 100:n tilan muuttuessa aktiiviseksi, kytkin saa haettua sille IP-osoitteen DHCP-palvelimelta. Tämän jälkeen AutoInstall saa TFTP-palvelimen osoitteen ja lataa konfigurointitiedoston kytkimelle. Seuraavaksi kytkin ilmoittaa, että se on konfiguroitu TFTP-palvelimella olevan tiedoston mukaan eli konfiguraation asettaminen on onnistunut.



KUVA 9. Kuvankaappaus AutoInstallin onnistumisesta

10 YHTEENVETO

Opinnäytetyön tavoitteina oli tietoverkon redundanttisuuden tutkiminen ja varmuuskopiointijärjestelmän luominen Savonia-ammattikorkeakoulun verkkoon. Kummassakin tavoitteessa onnistuttiin hyvin. Työn aikana opin paljon redundanttisuuteen liittyvistä asioista ja kuinka vikasietoisen tietoverkon rakentamisesta. Testauksen aikana Ciscon kytkimien toiminta ja niiden konfigurointi tuli erittäin tutuksi. Osaan hallita huomattavan paljon paremmin näiden toimintaa, kuin ennen työn aloittamista.

Testauksen ja työn tilaajan mielipiteen perusteella varmuuskopiointijärjestelmästä tuli toimiva ja se otetaan Savonian verkossa tuotantokäyttöön kesällä 2012.

LÄHTEET

1. Colliander, A. 1999. *ISOn OSI-mallin rakenne ja käyttö* [verkkojulkaisu]. Sähkö- ja tietoliikennetekniikan osasto. Teknillinen korkeakoulu [viitattu 14.3.2012]. Saatavissa: http://www.tml.tkk.fi/Studies/Tik110.300/1999/Essays/essee_OSI.html

2. Cisco Systems 2003. *Cisco EtherChannel Technology* [verkkodokumentti]. Cisco Systems [viitattu 28.4.2012]. Saatavissa: http://www.cisco.com/warp/public/cc/techno/lnty/etty/fsetch/tech/fetec_wp.pdf

3. Cisco Systems 2006. *Understanding and Configuring Spanning Tree Protocol on Catalyst Switches* [verkkodokumentti]. Cisco Systems [viitattu 5.5.2012]. Saatavissa: http://www.cisco.com/image/gif/paws/5234/5.pdf

4. Cisco Systems 2010a. *Catalyst 2960 and 2960-S Switch Software Configuration Guide* [verkkojulkaisu]. Cisco Systems [viitattu 25.4.2012]. Saatavissa: http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_53_se/configuration/guide/2960scg.pdf

5. Cisco Systems 2010b. *Cisco DocWiki: Interworking basics* [verkkojulkaisu]. Cisco Systems [viitattu 14.3.2012]. Saatavissa: http://docwiki.cisco.com/wiki/Internetworking_Basics

6. Cisco Systems 2012a. *Cisco Catalyst 6500 Series Virtual Switching System (VSS) 1440* [verkkodokumentti]. Cisco Systems [viitattu 7.4.2012]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/white_paper_c11_429338.pdf

7. Cisco Systems 2012b. *Cisco IOS Command Modes* [verkkodokumentti]. Cisco Systems [viitattu 23.4.2012]. Saatavissa: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf019.pdf

8. Cisco Systems 2012c. *Configuring Virtual Switching Systems* [verkkodokumentti]. Cisco Systems [viitattu 2.4.2012]. Saatavissa:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.pdf

9. Wikipedia 2012a. *Network Topology* [verkkojulkaisu]. Wikipedia Foundation [viitattu 17.3.2012]. Saatavissa: http://en.wikipedia.org/wiki/Network_topology

10. Wikipedia 2012b. *Keskitin* [verkkojulkaisu]. Wikipedia Foundation [viitattu 20.3.2012]. Saatavissa: http://fi.wikipedia.org/wiki/Keskitin

11. Wikipedia 2012c. *Kytkin (tietoliikenne)* [verkkojulkaisu]. Wikipedia Foundation [viitattu 20.3.2012]. Saatavissa: http://fi.wikipedia.org/wiki/Kytkin_(tietoliikenne)

12. Wikipedia 2012d. *Reititin* [verkkojulkaisu]. Wikipedia Foundation [viitattu 20.3.2012]. Saatavissa: http://fi.wikipedia.org/wiki/Reititin

13. Wikipedia 2012e. *UPS* [verkkojulkaisu]. Wikipedia Foundation [viitattu 1.5.2012]. Saatavissa: http://fi.wikipedia.org/wiki/UPS

Peruskonfiguraatiotiedosto varakytkimelle

```
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 100
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/3
!
interface GigabitEthernet0/4
!
interface GigabitEthernet0/5
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
```

```
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan100
 ip address 192.168.254.250 255.255.255.0
 no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
line vty 5 15
 password paastasisaan
 login
!
end
```

Cisco Catalyst 2960-S (Opi-A100_01) -konfiguraatiotiedosto

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service linenumber
service sequence-numbers
!
hostname Opi-A100_01
!
boot-start-marker
boot-end-marker
!
logging buffered 16000
enable secret 5 XXXXXX
!
username XXXXXX secret 5 XXXXXX
!
!
aaa new-model
!
!
aaa authentication login default local
!
!
!
aaa session-id common
clock timezone EET 2
clock summer-time EDT recurring last Sun Mar 3:00 last Sun Oct 4:00
switch 1 provision ws-c2960s-24td-l
!
ip dhcp pool Opi-B312_03
   host 192.168.254.250 255.255.255.0
   client-identifier
0063.6973.636f.2d66.6366.622e.6662.3034.2e35.6634.312d.566c.3130.30
   bootfile Opistotie/Opi-B312_03/Opi-B312_03_start
```

```
   option 150 ip 192.168.254.10
!
ip dhcp pool Opi-A110_01_fake
   host 192.168.254.249 255.255.255.0
   client-identifier
3f63.6973.636f.2d66.6330.342e.3535.3034.2e35.6666.312d.566c.3130.30
   bootfile Opistotie/Opi-A110_01/Opi-A110_01_start
   option 150 ip 192.168.254.10
!
ip dhcp pool Opi-A220_02_fake
   host 192.168.254.248 255.255.255.0
   client-identifier
3f63.6973.636f.2d30.3466.622e.3535.3034.2e35.6631.312d.566c.3130.30
   bootfile Opistotie/Opi-A220_02/Opi-A220_02_start
   option 150 ip 192.168.254.10
!
!
no ip domain-lookup
ip domain-name savonia-amk.fi
vtp mode transparent
!
!
crypto pki trustpoint TP-self-signed-629746304
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-629746304
 revocation-check none
 rsakeypair TP-self-signed-629746304
!
!
crypto pki certificate chain TP-self-signed-629746304
 certificate self-signed 01 nvram:IOS-Self-Sig#3436.cer
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
 quit

archive
 path tftp://192.168.254.10/Opistotie/$h/$h_
 write-memory
 time-period 1440
!
```

```
spanning-tree mode mst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
spanning-tree mst configuration
 instance 1 vlan 1-4094
!
!
!
!
!
vlan internal allocation policy ascending
!
vlan 100
 name verkon_hallinta
!
ip tcp path-mtu-discovery
ip tftp source-interface Vlan100
ip ssh version 2
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/2
 switchport access vlan 100
```

```
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/3
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/4
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/5
 switchport access vlan 100
```

```
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/6
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/7
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/8
 switchport access vlan 100
```

```
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/9
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/10
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/11
 switchport access vlan 100
```

```
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/12
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/13
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/14
 switchport access vlan 100
```

```
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/15
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/16
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/17
 switchport access vlan 100
```

```
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/18
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/19
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/20
 switchport access vlan 100
```

```
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/21
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/22
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/23
 switchport mode trunk
```

```
 switchport nonegotiate
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
!
interface GigabitEthernet1/0/24
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
!
interface Vlan100
 description Verkonhallinta
 ip address 192.168.254.8 255.255.255.0
!
ip default-gateway 192.168.254.1
ip http server
ip http access-class 1
ip http secure-server
ip sla enable reaction-alerts
kron occurrence ajastus in 1:0:0 recurring
 policy-list talleta
!
kron policy-list talleta
 cli   show   start   |   redirect   tftp://192.168.254.10/Opistotie/Opi-
A100_01/Opi-A100_01_start
!
logging trap errors
logging source-interface Vlan100
access-list 1 permit 192.168.254.0 0.0.0.255 log
```

```
access-list 1 permit 212.146.13.192 0.0.0.15 log
access-list 1 deny   any log
access-list 2 permit 212.146.13.192 0.0.0.15
access-list 2 deny   any log
access-list 3 permit 212.146.13.197
access-list 3 deny   any log
access-list 4 permit 10.212.29.2
access-list 5 permit 192.168.254.0 0.0.0.255
snmp-server view iso iso included
snmp-server community amkread RO 2
snmp-server community konfigtalteen RW 3
snmp-server community wlseread view iso RO 4
snmp-server community wlsewrite view iso RW 4
snmp-server trap-source Vlan100
snmp-server location B312A
snmp-server contact Datatiimi datacenter@kpy.fi
snmp-server enable traps snmp authentication
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps stpx root-inconsistency loop-inconsistency
snmp-server enable traps port-security
snmp-server host 212.146.13.193 public
banner login _
#########################################################################
#####                     AUTHORIZED ACCESS ONLY                    #####
#########################################################################
#####   This system is the property of Pohjois-Savo Polytechnic  #####
##### Disconnect IMMEDIATELY if you are not an authorized user ! #####
#####                                                               #####
#########################################################################_
!
line con 0
 logging synchronous
line vty 0 4
 access-class 1 in
 logging synchronous
 transport input telnet ssh
line vty 5 15
 access-class 1 in
```

```
 logging synchronous
 transport input telnet ssh
!
ntp server 192.168.254.1
end
```

Cisco Catalyst 2950 (Opi-A110_01) -konfiguraatiotiedosto

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Opi-A110_01
!
aaa new-model
aaa authentication login default local
enable secret 5 XXXXX
!
username XXXXXX secret 5 XXXXX
clock timezone EET 2
clock summer-time EDT recurring last Sun Mar 3:00 last Sun Oct 4:00
ip subnet-zero
!
ip tcp path-mtu-discovery
ip tftp source-interface Vlan100
no ip domain-lookup
ip domain-name savonia-amk.fi
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
spanning-tree mst configuration
 instance 1 vlan 1-4094
!
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode access
```

```
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 switchport access vlan 100
```

```
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/7
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/8
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/9
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/10
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/11
```

```
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/12
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/13
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/14
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/15
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
```

```
interface FastEthernet0/16
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/17
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/18
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/20
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
```

```
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/23
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/24
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan100
 ip address 192.168.254.66 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.254.1
```

```
ip http server
ip http access-class 1
logging trap errors
logging source-interface Vlan100
access-list 1 permit 192.168.254.0 0.0.0.255 log
access-list 1 permit 212.146.13.192 0.0.0.15 log
access-list 1 deny   any log
access-list 2 permit 212.146.13.193
access-list 2 deny   any log
access-list 3 permit 212.146.13.197
access-list 3 deny   any log
access-list 5 permit 192.168.254.0 0.0.0.255
snmp-server community amkread RO 2
snmp-server community konfigtalteen RW 3
snmp-server trap-source Vlan100
snmp-server location Teku A2078
snmp-server contact Datatiimi datacenter@kpy.fi
snmp-server enable traps snmp authentication
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps port-security
snmp-server host 212.146.13.193 public
banner login _CCCCCC
##########################################################################
#####                    AUTHORIZED ACCESS ONLY                      #####
##########################################################################
#####   This system is the property of Pohjois-Savo Polytechnic  #####
##### Disconnect IMMEDIATELY if you are not an authorized user ! #####
#####                                                                #####
##########################################################################
_
!
line con 0
 logging synchronous
line vty 0 4
 access-class 1 in
 logging synchronous
 transport input telnet ssh
line vty 5 15
```

```
 access-class 1 in
 logging synchronous
 transport input telnet ssh
!
!
end
```

Cisco Catalyst 2960 (Opi-B312_03) konfiguraatiotiedosto

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service linenumber
service sequence-numbers
!
hostname Opi-B312_03
!
boot-start-marker
boot-end-marker
!
logging buffered 16000
enable secret 5 XXXXXXX
!
username XXXXXX secret 5 XXXXXX
aaa new-model
!
!
aaa group server radius ACS
 server 10.212.29.4 auth-port 1812 acct-port 1813
!
aaa authentication login default local group ACS
aaa authorization network default group ACS
aaa accounting network default start-stop group ACS
!
!
!
aaa session-id common
clock timezone EET 2
clock summer-time EDT recurring last Sun Mar 3:00 last Sun Oct 4:00
system mtu routing 1500
vtp mode transparent
ip subnet-zero
!
```

```
no ip domain-lookup
ip domain-name savonia-amk.fi
!
!
crypto pki trustpoint TP-self-signed-4211367680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4211367680
 revocation-check none
 rsakeypair TP-self-signed-4211367680
!
!
crypto pki certificate chain TP-self-signed-4211367680
 certificate self-signed 01
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  quit
!
!
!
archive
 path tftp://192.168.254.10/Opistotie/$h/$h_
 write-memory
 time-period 1440
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
spanning-tree mst configuration
 instance 1 vlan 1-4094
!
!
vlan internal allocation policy ascending
!
vlan 2
 name Teku_opetus
!
vlan 3
 name teku_hlok
!
vlan 13
```

```
 name thk_serverit
!
vlan 18
 name Tietohallinto_AD_palvelimet
!
vlan 19
 name Hallinto_Palvelimet
!
vlan 20
 name Tietihallinto_hlokunta_Wlan
!
vlan 21
 name TekuOT_hlokunta_vierailija
!
vlan 23
 name tietohallinto_hlokunta
!
vlan 46
 name vierailija_lan
!
vlan 50
 name Server_Side
!
vlan 60
 name TeKu_ODMZ
!
vlan 98
 name CheckPoint_management
!
vlan 100
 name verkon_hallinta
!
vlan 101
!
vlan 200
 name TekuOT_Tyoasemat
!
vlan 201
 name TekuOT_hlokunta_Wlan
```

```
!
vlan 202
 name TekuOT_opetus_Wlan
!
vlan 210
 name eduroam_802.1x
!
vlan 220
 name TekuOT_Wlan_Hallinta
!
vlan 300
 name Virtuaali_Serverit
!
ip tcp path-mtu-discovery
ip tftp source-interface Vlan100
ip ssh version 2
!
!
interface GigabitEthernet0/1
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/2
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
!
interface GigabitEthernet0/3
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/4
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/5
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/6
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
```

```
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/7
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/8
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/9
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

```
interface GigabitEthernet0/10
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/11
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/12
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/13
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
```

```
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/14
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/15
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/16
 switchport access vlan 100
 switchport trunk allowed vlan 13,18
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
!
interface GigabitEthernet0/17
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 5
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/18
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/19
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/20
 switchport access vlan 100
 switchport mode access
 switchport port-security maximum 5
```

```
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/21
 switchport access vlan 100
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/22
 switchport access vlan 100
 switchport trunk native vlan 220
 switchport trunk allowed vlan 20,21,46,200-202,210,220
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/23
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/24
 switchport mode trunk
```

```
 switchport nonegotiate
 media-type rj45
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan100
 ip address 192.168.254.68 255.255.255.0
 ip helper-address 192.168.254.8
 no ip redirects
 no ip proxy-arp
 no ip route-cache
!
ip default-gateway 192.168.254.1
ip http server
ip http access-class 1
ip http secure-server
kron occurrence ajastus in 1:0:0 recurring
 policy-list talleta
!
kron policy-list talleta
 cli   show   start   |   redirect   tftp://192.168.254.10/Opistotie/Opi-
B312_03/Opi-B312_03_start
!
logging trap errors
logging source-interface Vlan100
access-list 1 permit 192.168.254.0 0.0.0.255 log
access-list 1 permit 212.146.13.192 0.0.0.15 log
access-list 1 deny   any log
access-list 2 permit 212.146.13.192 0.0.0.15
access-list 2 deny   any log
access-list 3 permit 212.146.13.197
access-list 3 deny   any log
access-list 4 permit 10.212.29.2
access-list 5 permit 192.168.254.0 0.0.0.255
tftp-server flash:config.text 5
tftp-server flash flash:config1.text 5
```

```
snmp-server view iso iso included
snmp-server community amkread RO 2
snmp-server community konfigtalteen RW 3
snmp-server community wlseread view iso RO 4
snmp-server community wlsewrite view iso RW 4
snmp-server trap-source Vlan100
snmp-server location B312A
snmp-server contact Datatiimi datacenter@kpy.fi
snmp-server enable traps snmp authentication
snmp-server enable traps entity
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps stpx root-inconsistency loop-inconsistency
snmp-server host 212.146.13.193 public
control-plane
!
banner login _CCCCC
##########################################################################
#####                    AUTHORIZED ACCESS ONLY                      #####
##########################################################################
#####   This system is the property of Pohjois-Savo Polytechnic  #####
##### Disconnect IMMEDIATELY if you are not an authorized user ! #####
#####                                                            #####
##########################################################################
_
!
line con 0
 logging synchronous
line vty 0 4
 access-class 1 in
 logging synchronous
 transport input telnet ssh
line vty 5 15
 access-class 1 in
 logging synchronous
 transport input telnet ssh
!
ntp server 192.168.254.1
end
```

Peruskonfiguraatiotiedosto AutoInstallia varten

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot host dhcp
boot host retry timeout 3000
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
crypto pki trustpoint TP-self-signed-4211367680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4211367680
 revocation-check none
 rsakeypair TP-self-signed-4211367680
!
!
crypto pki certificate chain TP-self-signed-4211367680
 certificate self-signed 01 nvram:IOS-Self-Sig#3001.cer
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/3
!
interface GigabitEthernet0/4
!
interface GigabitEthernet0/5
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
```

```
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
 switchport mode trunk
 switchport nonegotiate

!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan100
 no ip address
 ip helper-address 192.168.254.8
 no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
end
```


SAVONIA