

Jasu Viiala

# L2-tason kytkimien vaihtaminen yrityksessä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Koulutusohjelman nimi

Insinöörityö

10.5.2015

Tekijä(t) Otsikko	Jasu Viiala L2-tason kytkimien vaihtaminen yrityksessä
Sivumäärä Aika	44 sivua + 1 liitettä 10.5.2015
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Janne Salonen tehtävänimike Etunimi Sukunimi
<p>Tämä insinöörityö suoritettiin suomalaisen suuryrityksen tarpeesta päivittää käytössä olevat Ciscon kytkimet. Työssä käydään läpi kytkimen vaihtoon tarvittavat toimenpiteet, kuten kytkimien asentaminen ja konfiguraatioiden kopioiminen vanhasta kytkimestä uuteen. Käydään läpi asioita, joita tulee ottaa huomioon vaihtaessa kytkimiä suuryrityksessä, jolla on oma tuotanto.</p> <p>Työ aloitettiin läpikäymällä toimipisteen kytkinkaapit ja ottamalla talteen kaappien sisältö ja kuituyhteyksien merkinnät. Näiden pohjalta tehtiin kuitukartta kuvaamaan toimipisteen sisäverkon yhteyksiä.</p> <p>Lopputuloksena yrityksen sisäverkossa käytettävät kytkimet vaihdettiin uudempiin GigabitEthernet-yhteyttä tukeviin Ciscon L2-tason kytkimiin. Uudet kytkimet tuovat verkolla lisää elinikää tarjoamalla tukea nopeammille verkkoyhteyksille mahdollistaen esimerkiksi vaakaamat videopalaveri-palvelut. Uudet kytkimet ovat myös vähemmän alttiita esimerkiksi hajoamiselle äkillisissä virtakatkoksissa. Työssä luotiin myös yrityksen IT-tuelle ohjeet kytkimien VLAN-asetuksien tarkistamisesta ja muokkaamisesta.</p>	
Avainsanat	Vaihto, kytkimet

Author(s) Title	Jasu Viiala Title of the Thesis
Number of Pages Date	44 pages + 1 appendices 10 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Janne Salonen, Senior Lecturer First name Last name, Title (for example: Principal Lecturer)
<p>The aim of this thesis was to change layer 2 Cisco network switches for a large Finnish company. This thesis goes through needed steps of changing switches and how to successfully copy configurations from old switch to new switch. This thesis examines things that need to be taken care of when you are changing switches large company with their own production.</p> <p>In beginning we go through all switch enclosures and we list everything inside switch enclosures. We use fiber optics marks to create new map which illustrates fiber optic lines between all switch enclosures.</p> <p>As a result of project company now have upgraded LAN network with new Cisco switches. Between switches LAN network is now supporting GigabitEthernet-network. If necessary it is possible to upgrade fiber optic lines between switches to support TenGigabitEthernet-network. Faster network provides better quality example to video meeting services. New switches are more stable and not as easily to be broken because of some sudden power shutdowns. In the end we made a guideline about changing VLAN port configurations. This guideline was meant to be used by IT Service Desk.</p>	
Keywords	Cisco, switch, L2

## Sisällys

### Lyhenteet

1	Johdanto	1
2	Kytkimien valmistelu	1
2.1	Stacking	7
2.2	Hi-Fog	8
3	Kytkinkaappien sisällön luetteloiminen	9
4	Kytkimien konfiguroiminen	12
4.1	Kytkimen alkuasetukset	14
4.2	Porttiasetukset	23
4.3	Loppuasetukset	27
4.4	Cisco 2960S kytkimen salasanan kierto	33
5	Kytkimien asentaminen paikoilleen	34
6	Ohjeiden teko VLAN-muutoksiin	39
7	Huomioitavia asioita	42
8	Yhteenveto	44
	Lähteet	1

### Liitteet

Liite 1. Vanhan L3-tason ja uuden L2-tason kytkimen konfiguraatioiden erot

## Lyhenteet

Cisco	Cisco Systems on yhdysvaltalainen yritys, joka valmistaa verkkolaitteita kuten kytkimiä ja reitittimiä. Suurin osa Internetin liikenteestä kulkee Ciscon valmistamien reitittimien kautta. Ciscon kytkimet ja reitittimet käyttävät Internetwork Operation System (IOS) -käyttäjärjestelmää.
GigabitEthernet	Ethernet-verkkotekniikka, joka pystyy 1 Gbit/s (1000 Mbit/s) siirtonopeuksiin. Yhteensopiva vanhempien 10 Mbit/s ja 100 Mbit/s Ethernet-verkkotekniikoiden kanssa.
Fastethernet	Ethernet-verkkotekniikka, joka pystyy 100Mbit/s siirtonopeuksiin.
PoE	Power over Ethernet, tekniikka, joka mahdollistaa virransyötön laitteille vähintään CAT5-tason kierrettyllä parikaapelilla. Näin kytkimen PoE-portista voidaan verkkokaapelia pitkin syöttää virtaa esimerkiksi IP-puhelimille ja WLAN-tukiasemille.
MPLS	Multiprotocol Label Switching on verkkomenetelmä, jolla voidaan esimerkiksi IP-paketteja ennalta määriteltäviä yhteyksiä pitkin. Operaattorin käytäessä MPLS-tekniikkaa ei pitkien matkojen päässä olevien toimipisteiden välisen verkon tarvitse välttämättä kulkea Internetin läpi.
STACK	Kytkimien kytkentätapa, jossa Cisco-kytkimet on pinottu keskenään stack kaapelilla. Pinoa hallinnoi master-kytkin, ja muut toimivat jäsenkytkiminä
Vlan	Virtual LAN -tekniikka mahdollistaa tietoliikenneverkon jakamisen loogisiin osiin. Esimerkiksi yrityksessä pystytään jakamaan osastot omiin verkkoihin ottamatta kantaa niiden fyysiseen sijaintiin.
Reititin	Laite, jonka tehtävänä välittää tietoa verkkojen välillä esimerkiksi kotiverkon ja Internetin. Topologia-sanaa käytetään kuvaamaan reitittimien muodostaman verkon rakennetta.

Konfigurointi	Tarkoitetaan kytkimen asetusten asettamista. Konfiguroimalla otetaan käyttöön kytkimen toiminnallisuudet.
Kytkin	Jakaa tietoliikenteen verkossa olevien laitteiden välillä. Lähettää tiedon ainoastaan laitteille, joille se on tarkoitettu.
Telnet	Yhteysprotokolla, jolla voidaan ottaa etäyhteys päätelaitteeseen internetin ylitse. Esimerkiksi tietokoneella voi hallita kytkimiä etänä. Telnet-yhteys on salaamaton.
Protokolla	Standardi tai toimintatapa, jolla on määritelty yhteyden kulku tietoliikenteessä.
Putty	Ohjelma SSH, Rlogin, Telnet ja serial yhteyksien muodostamiseen.
RADIUS	RADIUS-palvelin mahdollistaa AAA-palveluiden käytön lähiverkossa.
NAS	Network Attached Storage tarkoittaa verkkotallennusta. Tallennuspaikka, jonne pääsee käsiksi verkon yli. NAS-palvelin hoitaa käyttäjän autentikoinnin ja tarvittaessa tiedostojen lukitsemisen.
CLI	Command Line Interface tarkoittaa komentoriviä. Käytetään myös nimityksiä konsoli ja terminaali.
Server	Serverin eli palvelimen tarkoitus on tarjota palveluita muille ohjelmille. Palvelimen järjestelmänä voi toimia esimerkiksi Windows Server 2008 R2, johon on asennettu Active Directory.
IP	Internet Protocol on protokolla, jolla IP-paketit toimitetaan kohteille Internet-verkossa. Kaikilla Internet-verkossa olevilla laitteilla on ip-osoite, jolla laitteen tavoittaa.
AD	Active Directory on Microsoft Windowsin käyttäjätietokanta ja hakemistopalvelu.
Ethernet	Pakettipohjainen lähiverkkotekniikka (LAN).

Valokuitu	Valoa johtava kuitu, jolla voidaan lähettää LED- tai laservaloa suurella nopeudella. Tietoliikenteessä käytetään yksi- ja monimuotokuitukaapeleita.
AAA	Authentication Authorization Accounting eli AAA-protokollaa käytetään verkossa autentikoimaan eli tunnistamaan käyttäjä.
VTP	VLAN Trunking Protocol mahdollistaa VLAN:en hallinnoinnin ryhminä. VLAN:ien luonti ja poisto tapahtuvat automaattisesti kaikissa kytkimissä, eikä tarvetta tehdä jokaiselle erikseen.
Transparent	Transparent tilassa kytkin välittää VTP tietoa, mutta ei itse välitä siitä.
CDP	Cisco Discovery Protocol on Ciscon protokolla, joka lähettää verkkoon tietoa reitittimestä tai kytkimestä, kuten merkin, mallin ja versionumeron. Voidaan käyttää verkon topologian selvittämisessä.
Trunk	Kytken portti asetetaan trunk-tilaan, kun kiinnitettävän laitteen on tarkoitus ymmärtää VLAN-tietoa. Esimerkiksi kytkettäessä toinen kytkin kiinni niin näiden väliset portit asetetaan trunk tilaan.
L2-taso kytkin	Toimii OSI-mallin 2. kerroksella (siirtoyhteys). Kytkin välittää liikennettä verkkokorttien MAC-osoitteiden perusteella.
L3-taso kytkin	Toimii OSI-mallin 3. kerroksella (verkkokerros). Kytkin voi reitittää liikennettä IP-verkkojen välillä.
OSI-malli	Open Systems Interconnection Reference Model on ISO-standardi, joka kuvaa tiedonsiirtoprotokollien yhdistelmän jakamalla ne seitsemään osaan.
Räkki	Räkkikaappi on teline tai kaappi, johon voidaan kytkeä laitteita. Esimerkiksi 19 tuuman räkkikaappiin voidaan kytkeä 19 tuumaa (48,26cm) leveitä laitteita kuten kytkimiä tai servereitä.

## 1 Johdanto

Projektin tarkoituksena on vaihtaa yrityksen vanhoja kytkimiä uudempiin Cisco L2-tason kytkimiin. Samalla tehdään uusi kuitukartta, sillä osa vanhoista kaappien merkinnöistä on muuttunut. Ennen vaihtojen aloittamista tehdään myös listaus jokaisen kytkinkaapin sisällöstä. Tarkistetaan kytkimien IP-osoitteet, porttimäärät ja mallit. Osa vaihdettavista kytkimistä on L3-tason kytkimiä, jotka ovat olleet hankittaessa lähes samanhintaisia L2-tason kytkimien kanssa. Nämä L3-tason kytkimet korvataan L2-tason kytkimillä. Projektin tavoitteena on korvata vanhentuneet kytkimet uudempiin aiheuttamatta pitkiä häiriöitä verkkoon. Uusien kytkimien myötä vanhat FastEthernet-portit korvataan uusilla GigabitEthernet-porteilla. Samoin kytkinkaappien kytkimet kytketään keskenään kuitukaapeleilla. Työn lopuksi paikalliselle IT-tuelle luodaan ohjeet kytkimien porttikonfiguraatioiden muuttamiseen. Työssä ei erityisesti tarvittu ulkoisia lähteitä. Cisco verkkoakatemia toinen vuosi, v. 2002 -kirjasta tarkistettiin BPDU-protokollan tietoja ja Cisco sivuilta on tarkistettu muutaman komennon tiedot. Hi-Fog-sammutusjärjestelmän tiedot ovat yrityksen omilta sivuilta.

## 2 Kytkimien valmistelu

Koska vaihdettavia kytkimiä on useita kymmeniä, ne valmistellaan etukäteen. Täten tarpeen tullen kytkimiä voidaan vaihtaa nopeallakin aikataululla. Näin tarvitaan myös huomattavasti vähemmän säilytystilaa laitteille ja mahdolliset tilausvirheet tai puuttuvat laitteet huomataan nopeammin. Valmiita kytkimiä pinotessa on hyvä kytkimien väliin laittaa, esimerkiksi pahvinpalanen suojaamaan naarmuuntumiselta. Samoin tulee varoa kasaamasta liikaa painoa alimman kytkimen päälle (kuva 1).





Kuva 1 Esivalmisteltuja Cisco WS-C2960S-48LPD-L-kytkimiä pinossa

Tilattuja kytkinmalleja on projektissa neljä. Ciscon pieniä tuuletittomia WS-C290C-8TC-L-kytkimiä, joita kutsumme työssä "jotbar-kytkimiksi". Nämä kooltaan melko pienet kahdeksalla FastEthernet-verkkoportilla varustetut kytkimet on tarkoitettu korvaamaan vanhat jotbar-järjestelmän verkkoliikennettä kuljettavat kytkimet.

Yksi isokokoinen Cisco 4503-E-kytkin (kuva 2) korvaa, kolme pienempää 24-porttista kytkintä. Tähän kytkimeen lisätään 48 kappaletta Ciscon GLC-FE-100FX kuitumoduuleita. Kytkimen tarkoituksena on toimia tuotannon laitteiden kytkimenä. Kytkimeen on mahdollista lisätä lisävirta, joka tuo vikasietoisuutta ja mahdollistaa PoE-syötön. Projektissa oli tarkoituksena käyttää kytkimessä lisävirtaa, mutta ilmeisesti tilausta tehdessä oli lisävirtalähde jäänyt pois. Uuden virtalähteen odottaminen viivästyttäisi vaihtoa turhan paljon, joten kytkin otetaan käyttöön ilman lisävirtaa. Tästä johtuen esimerkiksi PoE-virtaa käyttävät Wlan-tukiasemat tulee kytkeä erillisen PoE-syötön avulla. Lisävirta asennetaan vasta, kun työ voidaan tehdä tuotantoa häiritsemättä.



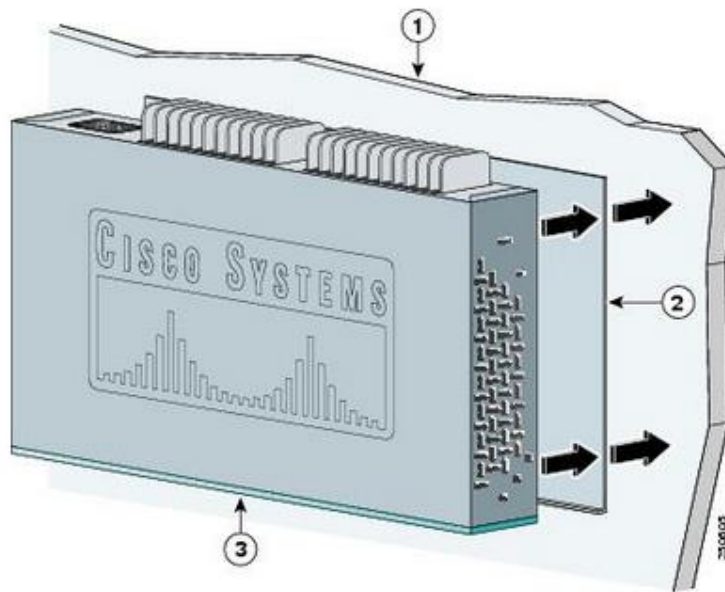
Kuva 2 Cisco 4503-E-mallin kytkin



Kuva 3 Cisco-yksimuotokuitumoduuli

Kaksi tavallisinta projektissa vaihdettavaa kytkinmallia ovat Ciscon WS-C2960S-48PD-L ja WS-C2960S-24PD-L (kuva 1). Kytkimet ovat muuten keskenään samanlaiset, mutta toisessa kytkimessä on 24 ja toisessa 48 GigabitEthernet-porttia. Molemmat kytkinmallit ovat PoE+-kytkimiä ja niihin saa kiinni kaksi kuitumoduulia.

Pienet jotbar-kytkimet kiinnitetään magneettikiinnityksellä esimerkiksi sähkökaappien sisälle. Kytkimeen kiinnitetään kahdella ruuvilla metallilevy, johon magneettimatto tulee kiinni. Magneettikiinnityksessä magneettimatto laitetaan kaapin seinään kiinni ja kytkin laitetaan kiinni magneettimattoon (kuva 4). Kiinnitys on helppoa ja nopeaa.



Kuva 4 Ciscon magneettikiinnitys [1]

Suurin esivalmistelu on C2960S-mallin kytkimissä johtuen laitteiden määrästä. C2960S-mallin kytkimet kiinnitetään kytkinkaappien räkkiin neljällä ruuvilla. Kytkimen kiinnikkeet on hyvä kiinnittää valmiiksi vaihtoja varten. Kiinnikkeet kiinnitetään tasapäisillä ruuveilla, jotta kytkimet mahtuvat räkkitelineeseen ilman suurta voimankäyttöä. Ei siis kuvan 5 kaltaisilla kuperilla ruuveilla.



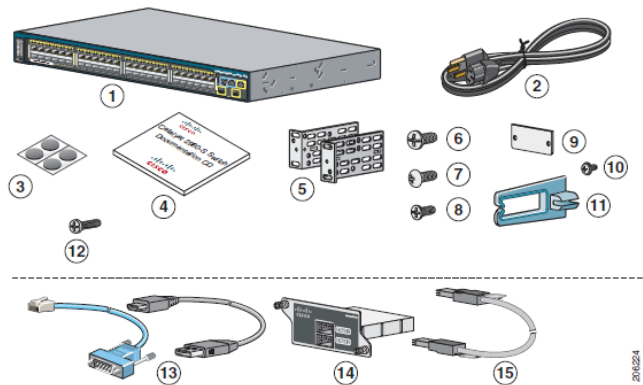
Kuva 5 Kiinnike on kiinnitetty väärnlaisia kuperilla ruuveilla

Myös kytkimen takana olevan lisävirtalähteen paikka peitetään mukana tulleeella peitelevyllä, koska sille ei projektissa ole käyttöä.



Kuva 6 Purettu Cisco 2960S-kytkimen laatikko sisältöineen

Catalyst 2960-S Switch Getting Started Guide



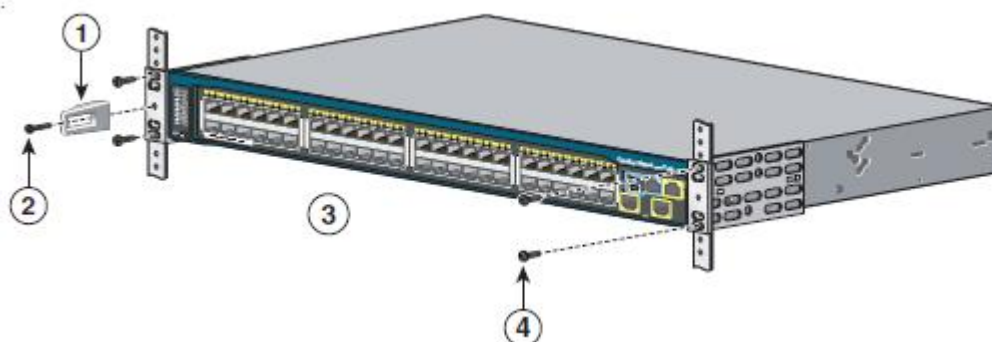
1	Catalyst 2960-S switch <sup>1</sup>	9	Connector cover for redundant power system
2	AC power cord	10	Two number-4 pan head screws
3	Four rubber mounting feet	11	Cable guide
4	Documentation	12	One black Phillips machine screw
5	Two 19-inch mounting brackets	13	(Optional <sup>2</sup> ) Console cable or universal serial bus (USB) cable
6	Four number-12 pan head screws (48-0523-01)	14	(Optional <sup>2</sup> ) Cisco FlexStack module
7	Four number-8 Phillips truss-head screws (48-05656-01)	15	(Optional <sup>2</sup> ) Cisco FlexStack cable
8	Six number-8 Phillips flat-head screws (48-0655-01)		

1. Catalyst 2960S-48FPD-L switch shown for example. Your switch model might look different.

2. Item is orderable.

Kuva 7 Kytin ja sen mukana tulleet osat [2, s. 3]

Kuvassa 7:n on lajiteltu Cisco-2960S-kytkimen mukana tulleet osat. Ensimmäisenä on kytkin. Toisena on tavallinen virtakaapeli. Kolmantena on neljä pientä kumin palaa. Kumeissa on liimapinta, jolla ne saadaan kiinnitettyä kytkimen pohjaan. Kumit estävät kytkimen metallipohjaa naarmuttamasta. Projektissa näitä kumeja ei käytetty, sillä niiden kanssa kytkimiä ei mahdu kytkinkaapissa pinoamaan päällekkäin. Neljäntenä on CD, jolta löytyy takuu- ja turvallisuusohjeet pdf-tiedostoina. CD:ltä löytyy myös aloitusohjeet usealla kielellä, mutta ei suomeksi. Kuva 7:n on otettu CD:n englanninkielisistä ohjeista. Ohjeista löytyy muun muassa ohjeet kytkimen kasaamiseen ja kuinka kytkintä pääsee hallinnoimaan. Viidentenä ovat kiinnikkeet (kuva 5). Kiinnikkeet kannattelevat kytkintä kytkinkaapin räkissä. Kohdat 6, 7 ja 8 ovat erilaisia ruuveja. Kohdan kahdeksan ruuveilla kiinnitettiin kiinnikkeet. Kohta yhdeksän on peitelevy, jolla lisävirrän paikka peitetään. Lisävirta mahdollistaisi vikasietoisuutta, koska silloin yhden virtalähteen irrottaminen tai hajoaminen ei vielä katkaise laitteesta virtoja. Kohdan kymmenen ruuvit on tarkoitettu lisävirrän peitelevyn kiinnitykseen. Tuote 11 on muovinen kaapeleiden pidike. Pidike tulee kytkimen kiinnikkeessä olevasta keskimmäisestä reiästä kiinni kytkinkaapin räkkiin. Pidike on tarkoitettu pitämään kaapelit siistissä linjassa, jotta eivät pääse liikkumaan valtoimenaan. Kytkinkaapissa. Siististi kiinnitettyjen kaapeleiden kytkentöjä on tarvittaessa huomattavasti helpompi selvittää. Näitä pidikkeitä ei projektissa käytetty sillä suurimmassa osassa kytkinkaappeja oli erikseen kaapeleiden kulkuun tarkoitettut rimat.



Kuva 8 Kytkimen kiinnikkeet ja kaapelipidike [3, s. 22]

Kohdan kaksitoista kuvaama ruuvi on tarkoitettu kaapelipidikkeen kiinnitykseen. Kohdassa kolmetoista on konsolikaapeli ja kytkimen USB-kaapelit. Molemmat kaapelit on tarkoitettu kytkimen hallinnointia varten. Kumpikaan kaapeli ei kuulu vakiona pakkaukseen. Konsolikaapelissa toinen pää on tavallinen RJ-45-liitin, joka kiinnitetään kytkimen Console-porttiin. Kaapelin toisessa päässä on DB9- eli sarjaporttiliitin. Tunnetaan yleisesti myös COM-liittimenä. Projektin aikana käytetyssä kannettavassa tietokoneessa ei

ollut COM-porttia, joten tähän piti hankkia erillinen USB-COM-liitin, jolla kannettavan USB-portista saatiin COM-portti. USB-kaapelissa kaapelin tavallinen USB-liitin kiinnitetään tietokoneeseen ja Micro-USB pääkytkimeen. Kytkimessä RJ-45- ja Micro-USB-hallinnointiportit on ympyröity vaaleansinisellä viivalla. Kytkintä ei voi hallita samanaikaisesti console- ja USB-porttien kautta.



Kuva 9 USB to COM -muunnin



Kuva 10 Console-kaapeli

Kohta neljätoista on flexstack-lisämoduuli ja kohta viisitoista tähän tarkoitettu flexstack-kaapeli. Nämä ovat molemmat erikseen hankittavia, eikä kuulu alkuperäiseen pakkaukseen.

## 2.1 Stacking

Stacking tarkoittaa useamman kytkimen kytkemistä yhden pääkytkimen taakse. Kytkinpinoa voidaan hallinnoida yhden IP-osoitteen takaa. Stacking-pino toimii yhtenä loogisena kytkimenä. Kytkinpinoon voi kerrallaan kuulua neljä jäsentä. Mahdollista lisätä toinen pääkytkin, mutta silloin tämä toimii niin sanotusti standalone-kytkimenä, joka ei kuulu varsinaiseen pinoon vaan toimii omana yksittäisenä pinona. [4]

Yksi pinon kytkimistä konfiguroidaan master-kytkimeksi eli pääkytkimeksi. Kun uusi kytkin lisätään pinoon ajaa pääkytkin automaattisesti uuteen kytkimeen konfiguraatiot. Ciscon FlexStack-teknologia säästää IP-osoitteita, koska kytkimet toimivat yhden IP-osoitteen takaa. Samalla hallittavuus paranee, koska useita kytkimiä konfiguroidaan yhden kytkimen kautta. FlexStack-pinoamiseen käytetään Ciscon omia tätä varten ke-

hitettyjä FlexStack-kaapeleita. Vaikka FlexStack-kaapeleilla pääseekin 10 Gbps nopeuksiin pinon jäsenten välillä, ei kyseistä pinoamisteknologiaa otettu projektissa käyttöön. Kytkimet päätettiin kytkeä keskenään kuitukaapeleilla.

Stacking-ominaisuudesta ja GigabitEthernet-porteista johtuen kytkimen porttien nimeäminen on muuttunut. Vanhemmat kytkimet on varustettu FastEthernet-porteilla ja ilman stacking-ominaisuutta. Vanha porttinimeäminen oli esimerkiksi ensimmäiselle portille FastEthernet0/1, kun uusissa kytkimissä ensimmäinen portti on GigabitEthernet1/0/1. Tämä hyvä tiedostaa, mikäli tarkoituksena kopioida konfiguraatiot suoraan vanhasta kytkimestä.

## 2.2 Hi-Fog

Konesalit on suojattu Hi-Fog-veisisammutusjärjestelmällä. Samoin on varastohuone, minne uudet kytkimet on varastoitu. Varoittimet ovat herkät ja saattavat reagoida pahveista irtoavaan ”pahvipölyyn”. Tästä johtuen kytkimet puretaan laatikoista pienissä erissä. Puretaan esimerkiksi viisi laatikkoa kerralla ja ruuvataan kiinnitettävät osat kytkimiin. Tämän jälkeen laitetaan kytkimet lavalle odottamaan vaihtoja. Näin ei synny kerralla liikaa pahveista irtoavaa pölyä. Pahvit ja styrox säilötään niitä varten raivatulle seinustalle, josta ne on myöhemmin helppo siirtää roskalaatikkoon. Näin jää pakattavia laatikoita, mikäli kytkimiä tarvitsee lähettää eteenpäin toiseen osoitteeseen.

Hi-Fog-järjestelmässä varoittimen tunnistessa savua tai riittävästi pölyä aktivoituu ensimmäinen hälytystila. Näin on aiemmin tapahtunut, kun konesalissa on lakaistu pölyä. Toisessa vaiheessa otetaan huomioon lämpö. Mikäli lämpötila on liian korkea, laukeaa Hi-Fog-järjestelmä. Tällöin tilaan suihkutetaan kovalla paineella vähän vettä, jonka seurauksesta tilaan syntyy palon sammuttava sumu.

Hi-Fog-järjestelmä on Marioff Corporation Oy:n vesisumusammutusjärjestelmä. Yritys toimii maailmanlaajuisesti toimittaen sprinklerijärjestelmiä. Hi-Fog-sammutusjärjestelmän tarkoituksena on sammuttaa palo suihkuttamalla tilaan huomattavasti tavallista sprinklerijärjestelmää vähemmän vettä. Näin vältetään suuremmat vesivahingot. Sumu ei myöskään riko kytkimiä eikä palvelimia. Järjestelmän on keksi-



nyt suomalainen keksijä Göran Sundholm. Sundholm perusti Marioffin vuonna 1985. Hi-Fog-vesisumutussprinklereitä yritys on kehittänyt vuodesta 1991.

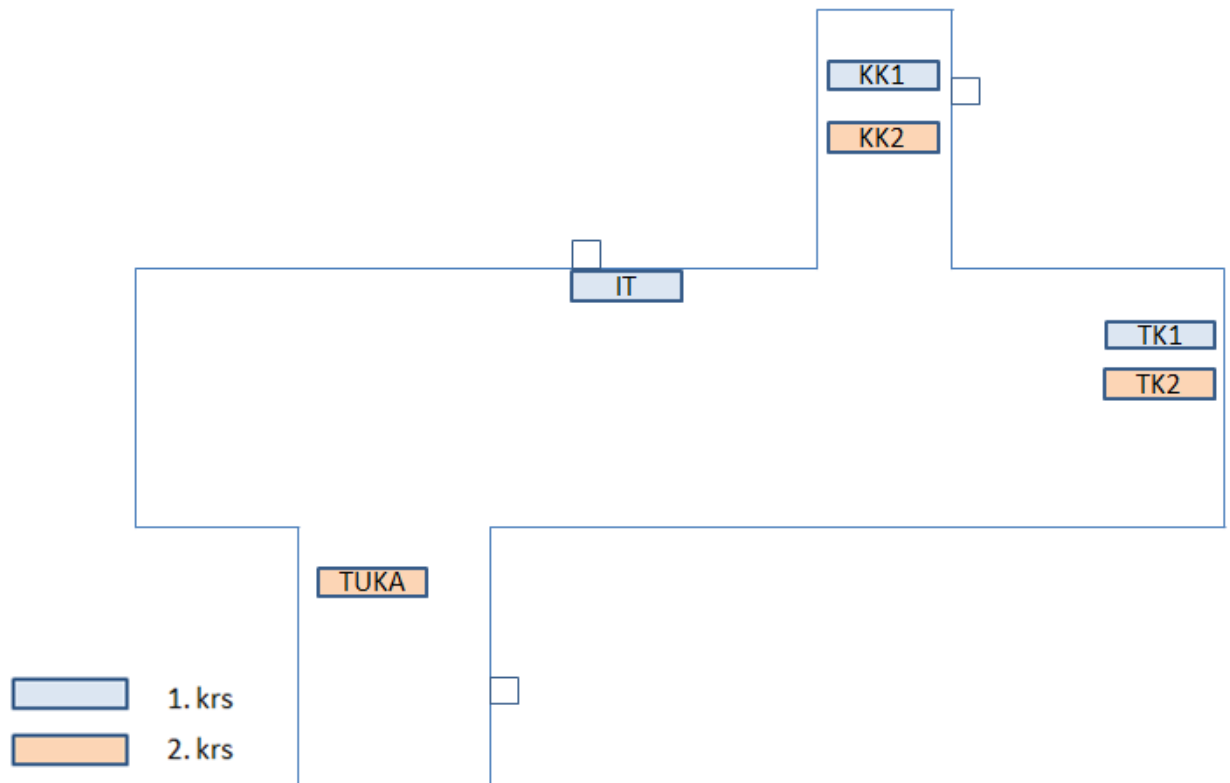
Järjestelmässä vesi ajetaan tilaan erittäin korkealla paineella, joka hajottaa veden vesisumuksi. Esimerkiksi 15 litralla vettä ja 200 barin paineella saadaan suojattua kone-sali. Järjestelmä ei aiheuta vanhan vesisammutusjärjestelmän kaltaisia vesivahinkoja eikä riko sähkölaitteita. Järjestelmää on näistä syistä ruvettu käyttämään konesaleissa, sairaaloissa ja erilaisissa teollisuuslaitoksissa. Alun perin järjestelmä otettiin käyttöön risteilyaluksissa. Järjestelmän ympäristöystävällisellä vesisumulla voidaan korvata kaasujärjestelmiä, joilla saattaa olla haitallisia terveys- ja ympäristövaikutuksia. [5; 6; 7]

### **3 Kytkinkaappien sisällön luetteloiminen**

Ennen kytkimien asentamista ja konfigurointia suoritetaan kytkinkaappien sisällön luetteloiminen. Kytkinkaappien sijainnista on olemassa kartta, jota ei ole päivitetty. Karttaan päivitetään poistettut, lisätyt ja kaapit, joiden sijainti on muuttunut. Kuva 11 esittää yksinkertaistettua mallia oikeasta kartasta. Kaappien sijainti näkyy summittaisesti talon pohjaan nähden. Laatikon väri ilmoittaa, kuinka monennessä kerroksessa kytkinkaappi sijaitsee.

Toimistotiloissa ja tuotantotiloissa sijaitsevat verkkopaikat on merkitty tarroin. Tarroista ilmenee kytkinkaapin nimi, minne linja on kytketty, riman nimi ja rimassa oleva verkkopaikka. Esimerkiksi KK1 A10 -tarra tarkoittaisi, että kyseinen verkkopaikan kaapelin toinen pää löytyy kytkinkaapista KK1 rimalta A ja paikalta 10. Tämän jälkeen on helppo kytkinkaapin luona tarkistaa, mihin kytkimen porttiin kyseinen käyttäjän verkkopaikka on kytketty. Tai tarvittaessa voidaan kyseinen verkkopaikka kytkeä kytkinkaapista löytyvään vapaaseen verkkopaikkaan.



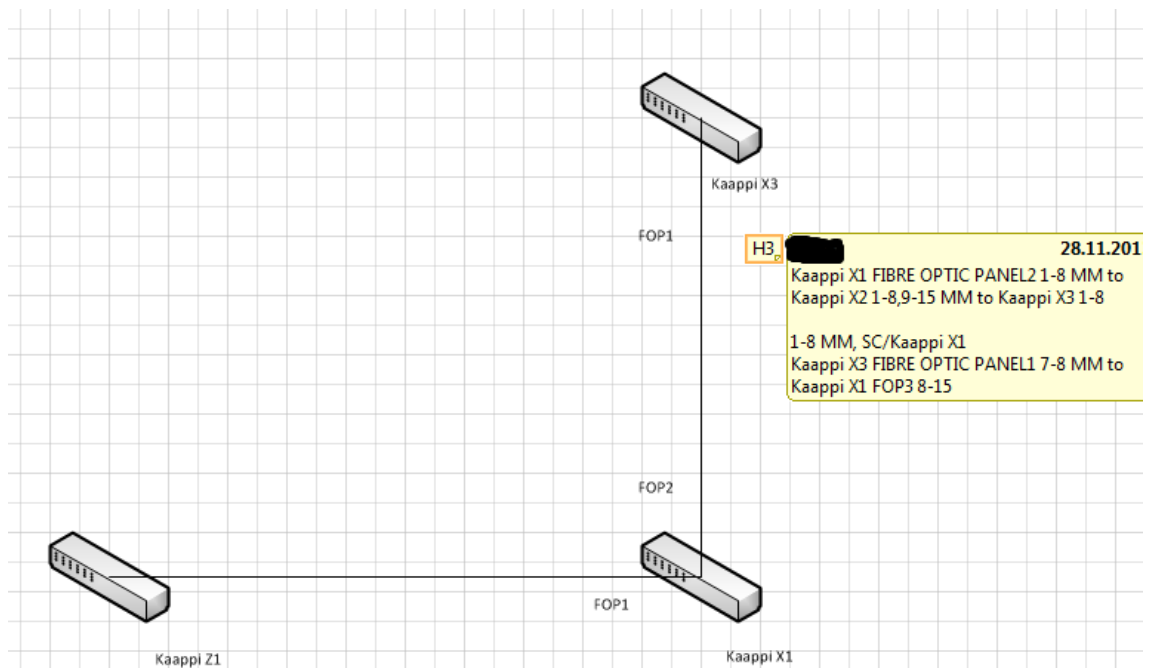


Kuva 11 Mallikartta kytkinkaapin sijainnista

Lisäksi listataan Excel-taulukko jokaisen kytkinkaapin sisältö. Otetaan ylös kytkinmallit, porttimäärät, kytkimien nimet ja IP-osoitteet. Kirjataan myös kaikki kuiturimojen merkinnät. Tarkistetaan, kuinka monta kuituporttia kytkimistä on kytketty ja minne ne on kytketty. Näin osataan varautua, mikäli vaihdossa tarvitsee muokata kytkimien kuitukytkentöjä. Samalla tarkistetaan, mikäli kaksi 24:n portin kytkintä voidaan korvata yhdellä 48:n portin kytkimellä. Vai tarvitaanko ylimääräinen kytkin, jotta tarvittavat kytkennät voidaan suorittaa? Nämä on otettava huomioon, koska osassa vanhoista kytkimistä on neljä kytkinporttia, joista saattaa kolme tai kaikki neljä olla kytkettynä. Uusissa 2960S-sarjan kytkimissä on paikka vain kahdelle kuitumoduulille.

Tämän lisäksi tehdään kuitukartta. Kuitukartan tekoon käytetään avuksi Microsoft Visio -ohjelmaa. Karttaan merkitään kytkimet ja se, minne niissä olevat kuidut on kytketty. Samalla tehdään toinen kuitukartta, johon merkitään, minne mistäkin kytkinkaapista on kuituyhteys vedetty. Listataan myös käytetyt kuitumallit ja liitinten mallit. Esimerkiksi yksi- tai monimuotokuitu SC- tai LC-liittimellä ja GBIC- tai SFP-kuitumoduulilla. Uusissa kytkimissä käytetään SFP-kuitumoduuleja. SFP-kuitumoduuliin tulee LC-liittimellä varustettu kuitukaapeli. Mikäli kuituyhteys tulee suoraan kytkimeltä toiselle, tarvitaan kah-

della LC-liitinpäällä varustettu kuitukaapeli. Mikäli kuituyhteys tulee kytkimeltä kaapin ulkopuolelle, tarvitaan kuitukaapeli, jossa toinen kuidunpää on LC-liittimellä varustettu ja toinen SC-liittimellä. Mikäli vanhassa kytkimessä on käytössä SFP-kuitumoduuli, ei tarvitse uuteen kytkimeen enää uutta kuitumoduulia kytkeä, vaan vanha voidaan siirtää suoraan uuteen kytkimeen. Samalla otetaan ylös mahdolliset UPS-laitteet ja niiden mallit.

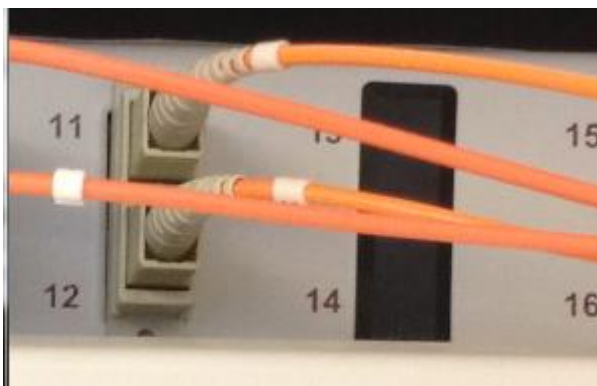


Kuva 12 Malliesimerkki kuitukartasta

Kuva 12 on malli kuitukartasta. Jokainen kytkin kuvastaa tässä tapauksessa kytkinkaappia. Viiva näyttää, minne kaikkialle kytkinkaapista on kuitukaapeilla reitti vedetty. Jokaisesta kaapista on pyritty saamaan ainakin yksi kuituveto kytkinkaappiin, jossa reunareititin eli reititin, jolla yhteys talon ulkopuoliseen verkkoon sijaitsee. Näin ei pääse syntymään liian pitkiä reittimatkoja, jotka voisivat vaikuttaa yhteysnopeuksiin. Projektissa kytkinkaappien ylin tai alin kytkin pyritään aina kytkemään kytkinkaappiin, jossa sijaitsee reunareititin.

Kytkinkaapin viereen on nimetty kyseinen kaappi esimerkiksi Kaappi X3. Samalla kuituviivaan on merkitty, millä kuiturimalla kytkentä sijaitsee. Esimerkiksi FOP1 tarkoittaa fibre optic panel 1 eli kuitupaneeli 1. Keltaiselle muistilapulle on merkitty kaapissa X3 sijaitsevan kuitupaneelin merkinnät.

Kuitumerkinnät (kuva 12) luetaan niin, että kaapin X1 kuiturimalta kaksi kuitupaikoilta 1-8 menee monimuoto-kuitukaapelit kaappiin X2 paikoille 1-8. Kaapin X1 paneelin 2 paikat 9-15 menevät kaappiin X3 paikoille 1-8. Kaappi X2 on purettu, eikä tältä osin merkinnät pidä enää paikkansa. Yhteydet on siirretty kaappien X1 ja X3 välille. Alempana mainitaan, että kaapin X1 paikat 1-8 ovat SC-liittimillä varustetuilla monimuoto-kuitukaapeleilla kytketty (kuva 13). Kaapissa X3 sijaitsevan kuitupaneelin paikat 7-8 ovat monimuoto-kuitukaapelilla kiinni kaapissa X1 sijaitsevan kuitupaneelin 3 paikoilla 8-15. Tämä kytkentä merkitty näin, koska kuitumerkintöjä tehdessä on ollut vain portin 7 ja 8 kytkettynä. Tällaisessa tilanteessa tarroitetaan kaapin kuitutarrat vastaamaan tämänhetkistä tilannetta.



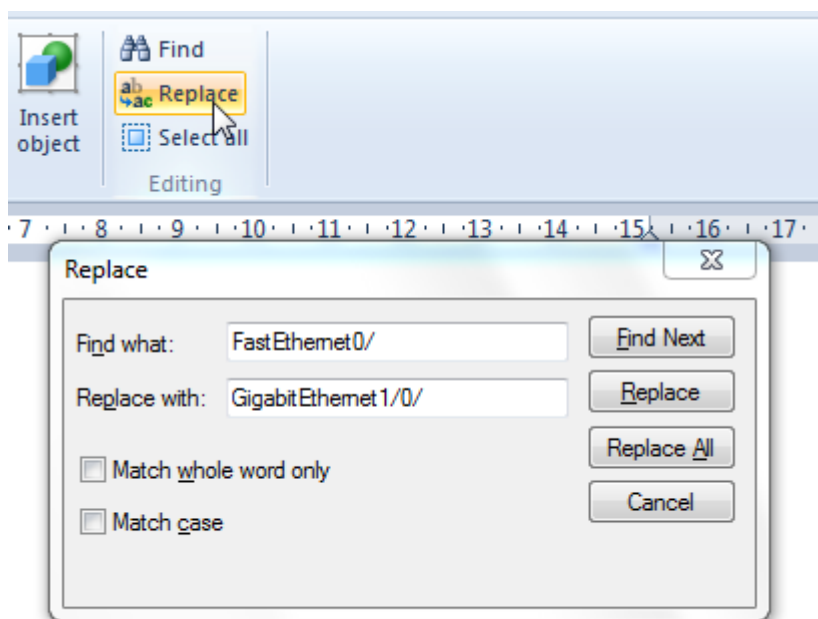
Kuva 13 Kuitupaneelin kuitupaikat 11,12 SC-liitännällä

#### 4 Kytkimien konfiguroiminen

Porttinimet eivät täsmää vanhoissa ja uusissa kytkimissä. Tästä johtuen pelkkä konfiguraatioiden kopioiminen ja siirtäminen eivät riitä.

Porttinimien muuttaminen on helppoa. Projektissa tähän käytetään Windowsin Wordpad-ohjelmaa. Kopioidaan vanhan kytkimen porttikonfiguraatiot Wordpad-ohjelmaan ja Replace-toiminnolla korvataan halutut sanat uusilla.

Vaihdetaan kaikki FastEthernet0/-porttinimet GigabitEthernet1/0/-porteiksi (kuva 14). Replace-toiminto hakee kaikki FastEthernet0/-sanat ja korvaa sanalla GigabitEthernet1/0/. Näin jää vielä oikea porttinumero loppuun. Esimerkiksi kytkimen portti FastEthernet0/4 on tämän jälkeen GigabitEthernet1/0/4.



Kuva 14 Sanojen korvaaminen Wordpadissa

Tässä työssä muokataan kytkimien konfiguraatiot käsin. Näin päästään karsimaan mahdollisesti turhat tai vanhentuneet konfiguraatioasetukset. Samalla nähdään, mikäli jotakin menee pieleen konfiguraatioita kopioidessa. Vaihtoehtona olisi kehittää ratkaisu konfiguraatioiden syöttämiseen kytkimiin verkon yli käyttäen DHCP:tä ja TFTP-palveluita. Näin ei tehdä, koska vanhoja konfiguraatioita ei tällöin käytäisi saman lailla läpi, eikä mahdollisia virheitä välttämättä huomattaisi. Käsin konfiguraatioita kopioidessa uuteen kytkimeen huomataan kopioinnissa mahdollisesti tapahtuvat virheet saman tien. Mikäli komentoa ei tunnisteta uudessa kytkimessä, tulee uudessa kytkimessä virheilmoitus. Samalla huomataan, mikäli vanhasta kytkimestä puuttuu asetuksia kuten salasanan kryptaus.

Yrityksessä kytkimien etähallintaan käytetään Active Directory -tunnuksia. AD (Active Directory) -tunnukset on lisätty sopivaan pääsryhmään (Access group), joka määriteltä TACAS+-palvelimelle. IT-lähituella on oma pääsryhmä, jolla on oikeudet nähdä ja muokata porttikonfiguraatioita, mutta ei esimerkiksi SNMP-asetuksia. Tunnus on tarkoitettu yrityksen verkkopaikkojen kytkemistä varten. Projektin lopussa IT Service Deskille luodaan ohjeet, kuinka kytkimien portteihin tehdään VLAN-muutoksia.

Projektin alussa minulla ei vielä ole pääsyoikeuksia kytkimiin, joten konfiguraatiot pitää muokata vaihdettavien kytkimien backup-konfiguraatioista.

Käydään vaihdettavan kytkimen konfiguraatitiedosto tarkasti läpi ja muutetaan vanhat FastEthernet-porttinimet oikeaan muotoon (kuvat 14 & 15). Tämän jälkeen poistetaan tarpeettomat komennot ja lisätään samalla tarvittavat puuttuvat komennot. Tämän jälkeen uusi tiedosto on valmis ja kopioidaan kytkimelle.

!	!
interface FastEthernet0/1	interface GigabitEthernet1/0/1
!	!
interface FastEthernet0/2	interface GigabitEthernet1/0/2
!	!
interface FastEthernet0/3	interface GigabitEthernet1/0/3
!	!
interface FastEthernet0/4	interface GigabitEthernet1/0/4
!	!
interface FastEthernet0/5	interface GigabitEthernet1/0/5

Kuva 15 Portit nimetty Replace-toiminnolla

#### 4.1 Kytkimen alkuasetukset

Liitteessä yksi on vaihdetun ja vaihdettavan kytkimen konfiguraatio. Konfiguraatioon on värein merkitty uuden ja vanhan kytkimen konfiguraatioiden erot. Liitteen IP-osoitteet, VLAN-nimeämiset, yhteystiedot ja domain-nimet on kaikki muutettu tunnistamattomiksi. Samoin salasanojen salausavaimet ovat muokattu.

Konfiguraation alkuun näkyy NVRAM-kohdassa, milloin tiedostoa on viimeksi muokattu. Tämän jälkeen tulee kytkimen versionumero.

No service pad -komento poistaa käytöstä PAD (Packet Assembler/Disassembler) -komennot. PAD-komentoja käytetään X.25-pakettiverkkotekniikassa, jota käytetään DTE- ja DCE-laitteiden välillä Määritelty ITU-T-standardissa yhteyden korvasi aikanaan suurelta osin Frame Relay -protokolla. [8]

Kun kytkimessä ajetaan debug-komento, lisää service timestamps debug datetime localtime -komento siihen päivämäärän ja kellonajan. Vastaavasti service timestamps log -komento lisää halutut tiedot tavalliseen lokitiedostoon.

Service password-encryption piilottaa paljaat salasanat heikolla salauksella. Tämä auttaa tilanteissa, joissa toinen henkilö on selän takana, kun konfigurointitietoja selataan. Salaus on helposti murrettavissa. Tämän takia kaikki työssä esiintyvät salausavaimien sarjat on muokattu. Tietoturvan puolesta kytkimet ovat lukittujen ovien takana ja etähallintaa varten tarvitsee olla sekä Active Directory -tunnukset oikeilla pääsyoikeuksilla sekä pääsy yrityksen sisäverkkoon.

Hostname-komennolla määritellään kytkimen nimi. Esimerkin konfiguraatiossa laite on nimellä fin-rov-tk2-sw2. Näin laitteen nimestä voisi päätellä laitteen sijainnin. Fin tarkoittaa maata eli Suomea. Rov tarkoittaa paikkakuntaa eli tässä tapauksessa Rovaniemeä. Tk2 tarkoittaa, että laite on toimistokonttoreiden toisessa kerroksessa. Sw2 tarkoittaisi, että kyseinen laite on kytkin numero kaksi kyseisessä tilassa.

Boot-start-marker ja boot-end-marker eivät ole oikeastaan komentoja. Kaikki boot eli käynnistyskomennot tulevat näkyviin näiden kahden väliin.

Logging buffered -komento määrittelee kytkimen sisään tallentuvien log-tiedostojen enimmäiskoon. Oletuskoko on 4096 tavua. Tällä estetään, etteivät log-tiedostot pääse viemään liikaa kytkimen muistia. Mikäli koon asettaa liian suureksi, voi kytkimeltä loppua muisti kesken. Show memory -komennolla voi tarvittaessa tarkistaa kytkimen prosessorin muistin määrän. Tämä on maksimimuistinmäärä, jota kytkimellä on, joten ei ole viisasta valita kaikkea muistikapasiteettia log-tiedostojen käyttöön. [9]

Kytkimessä enable password -komento luo salaamattoman salasan, joka näkyy running-configuration-tiedostossa salaamattomana. Selatessa konfigurointitiedostoja voi kuka tahansa lukea olan yli ja nähdä salasan. Enable secret näyttää salasan MD5 hash -tiedon salasan sijaan. Tämä on tänä päivänä melko helposti murrettavissa, mutta

huomattavasti hankalampi muistaa nopealla vilkaisulla. Kuvassa 16 näkyy miten enable password- ja enable secret -komentojen salasanat näkyvät running-config -tiedostossa.

switch>enable	switch>enable
switch#configure terminal	switch#configure terminal
switch(config)#enable password salasana	switch(config)#enable secret salattusalasana
switch>enable	switch>enable
Password:	Password:
switch#show running-config   include enable password	switch#show running-config   include enable
enable password salasana	enable secret 5 \$1\$BX5\$5FTz.ZAbADFRSv4fds514

**Kuva 16 Enable password- ja enable secret -komentojen erot kytkimessä**

Seuraavaksi username administrator password 7 88KD3B4428HJH -komennossa kytkimelle on luotu yksi local-tunnus varmuuden vuoksi. Mikäli yhteydet palvelimelle kaatoavat, on yksi tunnus jolla vielä pääsee kytkimeen kiinni. Ilman service password-encryption -komentoa perässä näkyisi paljas salasana.

AAA new-model -komento global configuration -tilassa ottaa AAA-protokollan käyttöön. AAA authentication fail-message \_fail-message^C Failed login. Three consecutive fails will revoke.^C antaa tunnuksen väärin syötettyä viestin "Failed login. Three consecutive fails will revoke."

AAA authentication login -komennolla määritellään autentikointitavat, joilla käyttäjän oikeudet kytkimelle tunnistetaan (tty, vty, console ja aux).

Komento "aaa authentication login default group radius local" määrittelee, että on kaksi tapaa autentikoida. Kaikki käyttäjät autentikoidaan RADIUS-palvelimen avulla, mutta mikäli yhteyttä RADIUS-palvelimelle ei saada, niin käytetään kytkimen sisälle tietokantaan määriteltäviä local-tunnuksia. Tässä tapauksessa local-tunnus olisi administrator, joka määriteltiin aikaisemmin username-kohdassa. Default-listan käyttö aaa authentication login -komennossa asettaa autentikointiasetukset voimaan automaattisesti kaikkiin kirjautumisyhteyksiin (esimerkiksi tty, vty, console ja aux).

Komento `aaa authorization exec default group radius if-authenticated` määrittelee kyt-kimen kysymään kirjautuessa RADIUS-palvelimelta, onko käyttäjällä oikeutta käyttää `exec`-komentotulkkia.

`AAA authentication enable default group radius enable` määrittelee `enable`-tilaan pääsyn autentikoinnin käyttämään RADIUS-palvelinta. Käyttäjätunnus on `$enab15$`, mutta tunnus pitää määritellä erikseen AAA-palvelimelle. Vain salasana pyydetään. Mikäli RADIUS-palvelin ei vastaa, niin täytyy laitteelle syöttää lokaalisti määriteltä `enable` salasana. [10]

`AAA authorization exec default group radius none` antaa `exec`-tilaan oikeudet, mikäli autentikointi RADIUS-palvelimen kanssa onnistuu. Mikäli yhteyttä RADIUS-palvelimelle ei ole, niin `none`-valinnan seurauksesta käyttäjä saa automaattisesti oikeudet. Tämä toiminto on pääsääntöisesti järjestelmänvalvoja varten, joilla on mahdollisuus päästä fyysisesti laitteelle.

`Accounting` seuraa käyttäjän tai ryhmän laitteiden käyttöä. `AAA accounting` -toiminnon päällä ollessa reitin kirjaa käyttäjän toiminnan RADIUS-palvelimelle. `Accounting`-komento sisältää kolme parametria. Mitä palveluita halutaan seurata, mitkä toiminnot aktivoivat sen ja minne tiedot lähetetään. Komennossa `aaa accounting exec default start-stop group radius` kohta `exec` tarkoittaa valvonnan alkamista, kun käyttäjä pyrkii `exec`-tilaan. `Default`-listan käyttö tarkoittaa, että tämä on voimassa yhteysmuodoissa `tty`, `vty`, `console` ja `aux`. `Start-stop`-toiminto tarkoittaa, että seuranta alkaa heti yhteyden alussa ja loppuu, kun yhteys on päättynyt. `Group radius` tarkoittaa, että käytetään RADIUS-palvelimien listaa käyttäjien autentikointiin. Mikäli käytössä useita seurantoja, kuten `exec` (`aaa accounting exec`) ja `resource` (`aaa accounting resource`) seurannat on hyvä varmistaa suorituskyvyn riittävyys. [10]

`AAA session-id` -komento määrittelee käytetäänkö istunnossa samaa istunto ID:tä autentikointiin (`authentication`), valtuutukseen (`authorization`) ja seurantaan (`accounting`). Oletuksena on `common`, joka käyttää samaa ID:tä kaikissa `AAA accounting` -palveluissa (`exec`, `connection`, `network`, `command`, `system` ja `resource`). Mahdollista myös määritellä uniikki-ID eri `aaa accounting` -palveluille. `AAA session-id unique` -komennolla. Mikäli halutaan palata takaisin oletusasetukseen, niin laitetaan `no aaa session-id unique` -komento. [10]



Switch 1 provision ws-c2960s-48lpd-l on kytkimen numerointi stack-pinossa. Tämä tavallisesti löytyy, kun kytkin tukee stack-pinoamista, mutta ei kuulu pinoon. Tämän saa halutessa pois komennolla no switch 1 provision ws-c2960s-48lpd-l.

Clock timezone -komennolla määritellään kytkimellä näytettävä aika. Toiminto ajetaan global configuration -tilassa. Komennon syntaksi on clock timezone zone hours-offset[minutes-offset]. Zone määrittää mitä aikavyöhykettä käytetään. Hours-offset määrittää, kuinka monta tuntia eroaa UTC (Coordinated Universal Time eli koordinoitu yleisaika) ajasta. Minutes-offset vastaavasti, kuinka monta minuuttia eroaa UTC ajasta. Eli komento clock timezone EET 2 tarkoittaa aikavyöhykettä Eastern Europe Time. UTC +2 ja 2 tarkoittaa kahden tunnin eroa. Kytkin sisäisesti pitää ajan UTC-ajassa, mutta komento muuttaa kellonajan näkymään asetuksissa halutun aikavyöhykkeen ajassa. [11]

Clock summer-time CDT recurring määrittää kesäajan muutokset kytkimelle Clock summer-time asettaa kytkimen vaihtamaan automaattisesti kesäaikaan. CDT (Central Daylight Saving Time, as UTC -5 hours) määrittää taas aikavyöhykkeen ja recurring-toiminto määrittää, että kesäaika alkaa ja päättyy tiettyinä päivinä joka vuosi. Voidaan halutessa myös itse määrittää alkamaan ja päättymään tiettyinä päivinä. Mikäli ei haluta, että kytkin vaihtaa automaattisesti kesäaikaan laitetaan komennon eteen no (no clock summer-time). Mikäli kesäaika määritellään antamatta mitään erillisiä parametreja, niin käytetään Yhdysvaltojen asetuksia. Aika-asetukset haetaan erikseen palvelimelta, joten nämä voidaan jättää uudesta konfiguraatiosta pois. [11]

System mtu routing 1500 on L3-kytkimissä oleva komento. Maximum Transmission Unit (MTU) määrittää, minkä kokoisia kehyksiä kytkin vastaanottaa ja lähettää. Oletusarvo on 1500 tavua. Vaihdeettavat kytkimet eivät ole reitittäviä, joten kyseisen komennon voi uudesta konfiguraatiosta poistaa. [12]

IP subnet-zero on nykyään Ciscon kytkimissä oletuksena päällä. Komento antaa käyttää aliverkkojen nollaverkkoja (subnet zero). Subnet zero on aliverkkojen ensimmäinen osoite. Tämän käyttöä aliverkoissa on suositeltu vältettäväksi, koska saattaa sekoittaa verkko-osoitteen (network address) kanssa. Esimerkiksi IP-osoite 172.16.1.10. olisi laskettaessa tätä vastaava aliverkon osoite 172.16.0.0 (subnet zero). Tämä kuitenkin on sama osoite, kun itse verkon osoite mitä alun perin oltiin jakamassa eli 172.16.0.0.

Eli suorittaessa aliverkotusta saadaan verkon ja aliverkon osoitteita, joita ei toisistaan erota. Tämä aikanaan aiheuttanut hämmennystä, jonka takia subnet zero -osoitteiden käyttö ei ole suositeltavaa. Niitä on kuitenkin mahdollista käyttää esimerkiksi tilanteessa, jossa jaettavat IP-osoitteet alkavat olemaan lopussa. Mikäli kuitenkin kyseinen mahdollisuus halutaan varmuuden vuoksi pois käytöstä, voi no IP subnet-zero -komennolla kieltää subnet zero -osoitteiden käytön. Projektin konfiguraatioissa otetaan IP subnet-zero pois käytöstä. [13]

IP source-route antaa verkkopaketin lähettäjän määrittää, mitä reittiä pitkin paketti tulisi kuljettaa. Mikäli toimintoa ei ole otettu pois päältä, voi rikollinen yrittää lähettää paketin perille palomuurin kiertämällä. Samoin ulkopuolinen voi kerätä tietoa verkkoliikenteestä reitittämällä paketin järjestelmän läpi. Toiminnon voi poistaa käytöstä kyseisellä no source-route -komennolla. [14]

Global configuration -tilassa määriteltä no IP domain-lookup ottaa pois käytöstä Cisco IOS -järjestelmässä käsiteltävät DNS-kyselyt. IP-paketteja, jotka sisältävät DNS-pyyntöjä ja vastauksia ei ole estetty. Kun IP domain-lookup otetaan pois käytöstä, niin väärin kirjoitetun komennon vuoksi ei tarvitse odottaa useita sekunteja. Odotus johtuu, kun laite suorittaa DNS-kyselyn verkkoon. Esimerkiksi kirjoittaessa inface eikä interface. Tietoturvan kannalta IP domain-lookup mahdollistaa DNS-kyselyiden tarkastelun, mikäli rikollinen pääsee käsiksi verkon liikenteeseen. [14; 15]

IP domain-name kohtaan tulee käytettävän domain name -palvelimen domain-nimi. Tässä tapauksessa käytettävä DNS-palvelin on mt.testi.com

IP name-server kohtaan tulee samaisen DNS-palvelimen IP-osoite. Global configuration -tilassa voidaan ottaa komennolla mls qos käyttöön QoS (Quality of Service) -laadunmäärittely. QoS mahdollistaa verkon priorisoinnin. Priorisoinnin avulla voidaan osaa liikenteestä hidastaa tai kokonaan katkaista liikenne, mikäli verkon välityskyky ei syystä tai toisesta riitä. Verkon seuraamiseen on useita tapoja kuten error-viestien määrä, viive ja siirtonopeus. [16]

Errdisable recoveryn ansiosta kytkimen portissa ilmetessä liikaa error-viestejä tai huomautusta, että kuituportti on vain toisesta päästä kytketty, menee portti shutdown-tilaan. Portin mentyä kiinni, tulee viesti minkä takia. UDLD (UniDirectional Link Detection) -protokolla antaa monitoroida Ethernet- tai kuitukaapeleiden yhteyksiä, Mikäli protokolla

huomaa, että on olemassa kaapelilinkki, joka ei vie mihinkään, niin kyseisen linkin portti suljetaan. Errdisable recovery UDLD nostaa portin automaattisesti takaisin ylös, kun kaapelin molemmat päät on kytketty. Porttivalo kytkimellä muuttuu oranssiksi, kun portti on mennyt kiinni ja muuttuu takaisin vihreäksi, kun portti on taas ylhäällä ja toiminnassa. Errdisable-asetukset jätetään uusista konfiguraatitiedoista pois. [17]

BPDU (Bridge Protocol Data Unit) tarkoittaa STP (Spanning Tree Protocol) -kehyksiä. Kytkimet lähettävät BPDU-kehyksiä tasaisen väliajoin ja niitä käytetään spanning tree -topologian määrittelyyn [18, s. 57]. BPDUGuard päällä ollessaan tarkkailee access-portteja eli portteja, joissa on end user device kiinni. BPDUGuard sulkee access-portin, mikäli siinä on BPDU-liikennettä. Tämä tehdään sen takia, että ainoastaan kytkimet voivat luotettavasti luoda ja lähettää BPDU-kehyksiä. Errdisable recovery cause bpduguard -komento nostaa portin takaisin ylös automaattisesti, kun BPDU-liikenneportista on poistettu esimerkiksi kytkemällä porttiin, jokin trunk-liikennettä käyttävä laite.

Crypto pki trustpoint -komento määrittelee CA:n (certification authority), jota reitittimen tulisi käyttää. Tässä tapauksessa TP-Self-Signed-nimi viittaa siihen, että turvasertifiikaatit on luotu lokaalisti. PKI (Public key infrastructure) on julkisten varmenneavainten hallinnointijärjestelmä. PKI-protokollassa CA eli varmentaja allekirjoittaa digitaalisen julkisen avaimen, jossa on omat tunnistetiedot. Tämän jälkeen allekirjoitettua avainta (certificate) voidaan jakaa, ja teoriassa vastaanottaja voi varmistua, että allekirjoitus on oikea. Allekirjoittavan tahon ja allekirjoituksen oikeellisuuden perusteella voidaan luottaa, että vastaanotetun avaimen tunnistetiedot ovat oikeat. Varmennetta (eng. certificate) voidaan monistaa ja jakaa vapaasti. Varmennetta voidaan jopa käyttää salaukseen ilman tunnistetta. Varmenne voidaan saada esimerkiksi osana yhteyden avausta. Salaja tarvitsee itselleen vastaanottajan julkisen avaimen ja vastaavasti tunnistava taho tarvitsee tunnistettavan tahon julkisen avaimen. CA eli varmentaja myöntää varmenteet. CA:n tehtävänä on varmistaa, että varmenteen hakija on oikeasti hän, joka väittää olevansa. Sähköisessä allekirjoituksessa eli PKI-allekirjoituksessa viestin sisältö allekirjoitetaan. Allekirjoitus yhdistetään varmenteeseen ja varmistutaan, ettei viestiä ole muutettu. [19]

Allekirjoitusta kytkimessä käytetään esimerkiksi SSH-yhteyksiin. Mikäli kytkimiä hallitaan vain telnet-yhteydellä, ei kyseisellä asetuksella ole vaikutusta.

Enrollment määrittelee miten varmenne hankitaan eli tässä tapauksessa selfsigned. Voisi esimerkiksi olla jokin http-osoite mistä varmenne haettaisiin.

Subject-name määrittelee nimen, jota käytetään varmennetta pyytäessä. Eli varmenne on TP-Self-Signed-4245666245.

Revocation-check none -komento ottaa pois käytöstä sertifikaattien eli varmenteiden voimassaolopäivän tarkistuksen.

Rsakeypair määrittelee nimen RSA-varmenteen avainparille eli tässä tapauksessa TP-Self-Signed-4245666245.

Certificate chain on lista salauksia. Mikäli luotettua yhteyttä ei saada ensimmäisellä avaimella siirrytään aina seuraavaan, kunnes avaimet loppuvat. Yhteys muodostuu, mikäli sopiva avain löytyy.

Spanning tree -protokollan käyttämä algoritmi estää silmukat verkossa. Protokolla laskee verkolle spanning tree -topologian. Spanning tree -protokollan päätarkoitus on sallia kahdennetut polut esimerkiksi kytkimien välillä. Kehykset toimitetaan eteenpäin MAC-osoitteiden perusteella. Mikäli MAC-osoite on tuntematon, niin lähetetään kehys jokaiseen porttiin, jotta kehys saataisiin perille haluttuun osoitteeseen. Samoin tehdään kaikille yleislähetys-kehyksille. Eli vikasietoista verkkoa halutessa pyritään silmukattomaan polkuun. Mikäli spanning-tree havaitsee silmukan niin poistaa se sen asettamalla osan yhteyksistä odotustilaan. Spanning-tree määritetään VLAN-kohtaisesti. [20]

Komento spanning-tree mode pvst asettaa spanning-tree -protokollan pvst (per-vlan spanning-tree) -tilaan. Eli jokaiselle Vlanille määritetään oma spanning-tree.

Spanning-tree portfast bpduguard default asetetaan global configuration -tilassa ja se asettaa portfast bpduguardin päälle oletuksena kaikille porteille. Spanning-tree pyörii porteissa, kunnes portti vastaanottaa bpdue-kehysten, jonka jälkeen bpduguard asettaa portin err-disable-tilaan.

Myös spanning-tree portfast bpdufilter default -komento suoritetaan global configuration -tilassa. Tämä asettaa portfast bpdufilter -toiminnon oletuksena päälle kaikkiin portteihin. Portfast bpdufilter estää portfast-portteja lähettämästä ja vastaanottamasta

bpdu-kehyksiä. Portit lähettävät muutaman bpdu-kehyksen ennen filterointia, jotta oikea linkitys saadaan spanning-tree -protokollaan. Mikäli portfast -portti vastaanottaa bpdu-kehyksen, niin lopettaa portti portfast-toiminnallisuutensa ja bpdufilter menee disabled-tilaan. [21]

Spanning-tree extend system-id -komentoa ei voida ottaa pois käytöstä kytkimissä joissa on sisäinen tuki vain 64 MAC-osoitteelle. Kytkimissä joissa sisäinen MAC-tuki tukee 1024 MAC-osoitteen listaa. Kaikilla VLAN:lla on oma STP-topologia, mutta yhteinen MAC-osoitteiden lista. System ID -numero on sama, kuin VLAN id -numero. Kaikilla Spanning-tree -topologioilla pitää olla oma Bridge id (BID). Käytössä on pvst eli jokaisella VLAN:lla oma STP ja täten oltava oma BID. Eli ollessa x määrä VLAN:ja on käytössä x määrä STP:tä ja tarvitaan siis x määrä BID:jä. Jotta varmistetaan uniikit BIDit eri VLAN:ille, on kytkimillä nykyään otettu käyttöön extended system ID. Käytetään BID:in määrittämiä kytkimien prioriteetteja ja lisätään siihen Vlan ID -numero. Näin saadaan helposti uusi uniikki-BID ja samoilla prioriteeteilla. Prioriteettien mukaan valitaan oletusreitit. Oletusreitin katketessa etsii STP uuden reitin. Eli saadaan pidettyä useita reittejä ilman loopbackia, koska vain yksi reitti on käytössä kerrallaan. [22]

Kun päälinkki (root port) katkeaa, niin rupeaa kytkin etsimään uutta reittiä määränpäähän. Uusi reitti etsitään, kun STP on määrittänyt uuden root-portin. Kun global configuration -tilassa määritellään spanning-tree uplinkfast -toiminto, niin voidaan määritellä uusien root-porttien valintaa siltä varalta, että oletusreitti katkeaa. Näin uusi root-port-liikenne saadaan forwardin-tilaan samantien ilman, että alkuun käytäisiin tavallinen STP:n listening- ja learning-tilojen prosessi. Uplinkfast on tuettu vain, kun kytkimeen on määritelty pvst.

Vlan internal allocation policy ascending kertoo, että kytkin varaa omaan käyttöönsä VLAN:it 1006:sta ylöspäin. Mikäli ascending sanan tilalla olisi descending, alkaisi kytkin varaamaan VLAN:ja 4094:stä alaspäin.

IP ssh time-out 60 asettaa ajan, kuinka kauan ssh-vastausta odotetaan. Eli ssh-vastausta odotetaan 60 sekuntia, mikäli vastausta ei tule niin yhteys katkaistaan. IP ssh version 2 asettaa käyttöön ssh 2 -version, joka on versio 1:stä turvallisempi ja tukee usean shell-istunnon ajamista yhden ssh-yhteyden sisällä.

IP scp server enable –komento mahdollistaa tiedostojen kopioimisen laitteelta käyttäen

ssh-yhteyttä. Secure copy protocol (scp) antaa kopioida laitteelta ja laitteelle. IOS-järjestelmässä tämä on oletuksena kiellettyä.

Näiden asetusten jälkeen alkaa porttikonfiguraatiot. Käydään läpi vain oleelliset komennot ja erot porteissa ilman, että läpikäydään yksitellen jokaista porttia.

## 4.2 Porttiasetukset

Fastethernet0 eli ethernet-hallinnointiportti on L3-kytkimen host-portti, johon voi kytkeä PC:n. Fastethernet0-portille määritellään IP-osoite, jonka jälkeen kytkintä voidaan hallinnoida verkon yli console-portin sijaan. Portti on yleisesti tunnettu, joten sitä ei ole otettu konfiguraatioissa käyttöön.

Vanhassa kytkimessä on vielä portit FastEthernet-portteja. Uusissa kytkimessä on Gigabit-portteja ja stack-ominaisuuden vuoksi porttinumerointi on muuttunut. FastEthernet0/1 on kytkimessä ns. ensimmäinen portti eli ykkös-portti. Uusissa kytkimissä vastaava portti on GigabitEthernet1/0/1-portti. Vastaavasti FastEthernet0/2 on vastaava portin GigabitEthernet1/0/2-portti.

Porttiin voidaan määritellä teksti, joka kuvaa porttia description-komennolla. Komento suoritetaan portin asetuksiin.

```
switch>enable
switch#configure terminal
switch(config)#interface fastethernet0/1
switch(config-if)#description Toimisto-VLAN45
```

Kuva 17 Description-komento

Switchport access vlan -komento määrittelee minkä VLAN:in liikennettä portti liikennöi. Portti on access-tilassa, joten portti voi liikennöidä vain yhden sille määritellyn VLAN:in liikennettä. Mikäli erillistä VLAN:ia ei määritellä on oletuksena VLAN 1.

Switchport access asettaa portin access-tilaan eli ei ole trunk-portti, eikä dataan lisätä

tagging-merkintää. Oletuksena kytkin kuljettaa VLAN 1:en liikennettä, mikäli switchport access vlan -komennolla ei muuta VLAN:ia määritetä.

Switchport voice vlan määrittää ääniliikenteen (voice traffic) kulkemaan komennossa määritellyn VLAN:in läpi. Portfast -toiminto otetaan automaattisesti päälle, mikäli Voice VLAN otetaan käyttöön. Portfast ei kuitenkaan automaattisesti kytkeydy pois päältä vaikka voice VLAN otettaisiin käytöstä pois. Voice VLAN:in kautta kuljetetaan ääniliikennettä kuten Ciscon IP-puhelimien liikennettä.

Mls qos trust määrittää, että COS (class of service) -arvo kehyksissä otetaan huomioon. Mikäli COS ei ole luotettu on portin oletusarvo sille 0. Eli QOS (Quality of Service) ottaa huomioon COS-arvot verkon palvelunlaatua määrittäessä.

No snmp trap-link status -komento global configuration -tilassa annettuna estää portteja lähettämästä tietoa, kun portti menee alas (portti kiinni) tai nousee ylös (portti päälle). Tämä asetus jätetään uusista konfiguraatio-tiedostoista pois.

Spanning-tree portfast -komento asettaa portin portfast-tilaan. Portfast jättää pois kokonaan kuuntelu (listening)- ja oppimis (learning) -tilat, kun porttiin kytketään vaikka PC. Portti nousee suoraan välittävään (forwarding) -tilaan. Näin jää n. 30 sekunnin viive, mikä muuten syntyisi laitetta kytkettäessä. Aina vikatilan tullessa portin nouseminen takaisin välittäväksi kestäisi normaalisti puoli minuuttia, joka voi tietyissä tilanteissa olla liian paljon, kuten videolähetyksissä, joissa yhteys saattaisi katketa kokonaan.

Uusissa kytkimissä ei enää ole mls qos trust cos -asetukselle ollut tarvetta ja no snmp trap link-status -komentoa ei enää ole (kuva 18), joten nämä voitiin uusista konfiguroinneista jättää pois.

```

su2#show snmp tr
su2#show snmp ?
chassis      show snmp chasis
community    show snmp communities
contact       show snmp contacts
context       show snmp contexts
engineID      show local and remote SNMP engine IDs
group         show SNMPv3 groups
host          show snmp hosts
location      show snmp location
mib           show mib objects
pending       snmp manager pending requests
sessions      snmp manager sessions
sysobjectid   Show sysObjectID
user          show SNMPv3 users
view          show snmp views
|            Output modifiers
<cr>

```

Kuva 18 2960S-kytkimet eivät tunnista komentoa snmp trap

Portteihin FastEthernet0/41 ja FastEthernet0/42 asennettu tulostimet, joten description-kenttään on merkitty tämä tieto.

Vanhan kytkimen GigabitEthernet0/1-portissa on ollut kiinni kytkin, jonka takia portti on laitettu trunk-tilaan. Description-kenttään on hyvä laittaa kytketyn kytkimen nimi, jotta ei tarvitse aina erikseen selvittää esimerkiksi CDP neighbors detail -komennolla, mikä laite on kytkimeen kytkettynä. Uudemmat kytkimet eivät enää tue, kuin 802.1Q-kapselointia. Koska dot1q-kapselointi ei ole tuettu, niin ei kytkimessä tarvitse olla dot1q encapsulation -komentoakaan. Sen sijaan riittää komento switchport access trunk (kuva 19).

Logging event trunk-status ilmoittaa aina, kun switchport lakkaa toimimasta trunk-porttina, vaikka linkki olisikin vielä muuten pystyssä. Tämä voidaan jättää uuden kytkimen konfiguraatiosta pois.

UDLD (UniDirectional Link Detection) -protokolla monitoroi fyysisiä kuitu- tai ethernet-kaapeleita. Protokolla havaitsee mikäli, jossakin on vain yksisuuntainen linkki. Tämä voi johtua esimerkiksi viallisesta kaapelista tai toista kaapelin päädyistä ei ole kytketty oikein. Mikäli yksisuuntainen linkki löytyy, niin protokolla sulkee portin ja ilmoittaa viasta. Normal-tilassa UDLD havaitsee vian kuituyhteyksissä porttien yhteyskatkoksista. Aggressive-tilassa yksisuuntainen yhteys huomataan vaikka liikenne olisi yksisuuntaista kuitu- tai kierrettyssä parikaapelissa. Myös aggressive-tila huomaa kuituyhteyksissä



vian, mikäli tulee yhteyskatkoksia. Tämä asetus jätetään uudesta konfiguraatitiedostosta pois. [23]

```
sw2(config-if)#switchport trunk ?
allowed  Set allowed VLAN characteristics when interface is in trunking mode
native   Set trunking native characteristics when interface is in trunking
         mode
pruning  Set pruning VLAN characteristics when interface is in trunking mode
```

Kuva 19 Trunk encapsulation dot1q ei enää tuettu uusissa kytkimissä

Projektissa uudet kytkimet kytkettiin keskenään vaihdettavilla SFP-kuitumoduulipaikoilla. Näitä varten käytössä on porttipaikat GigabitEthernet1/0/49 ja GigabitEthernet1/0/50. Vaihtoehtoisesti nämä kaksi voisi ottaa käyttöön TengigabitEthernet-portteina, mutta siihen ei projektissa ollut tarvetta. Vanhassa kytkimessä vastaavasti on ollut neljä GigabitEthernet-porttia, joista kaksi on kytketty. Koska käytössä ollut vain kaksi GigabitEthernet-porttia niin näiden kahden kuitumoduulin porttipaikkojen konfiguraatiot siirrettiin uuden kytkimen portteihin 49 ja 50 jättäen pois dot1q-kapseloinnin ja logging event trunk status -komennon. Mikäli olisi ollut kolme tai neljä GigabitEthernet paikkaa kytkettynä, niin olisi pitänyt katsoa olisiko osan kuitukytkennöistä voinut jättää kytkemättä. Tarvittaessa olisi voinut kytkeä myös tavalliseen GigabitEthernet porttiin ethernet-kaapelilla. Uuden kytkimen myötä ei olisi suurta nopeuseroa kuituihin verrattuna tullut, koska kaikki portit toimivat GigabitEthernet-portteina.

VLAN1 on jätetty pois tietoturvasyistä. VLAN1 on yleisesti tunnettu default-vlan, eikä sitä voi poistaa. VLAN 1 on oletuksena kaikissa porteissa, eikä sitä voi poistaa sillä se lähettää ja vastaanottaa hallinnallisten protokollien viestejä kuten CDP-kehyksiä. Vaikka VLAN 1:stä ei voi poistaa, niin voi sen ottaa pois käytöstä. Tällöin se ei kuljeta käyttäjäliikennettä vaan ainoastaan hallinnollista liikennettä kuten CDP-kehyksiä. VLAN 1 on hyvä olla pois käytöstä, koska se on tunnettu VLAN, joka käytössä ollessa on kaikissa porteissa nostaa haitallisen broadcast-tulvan riskiä ja laajuutta. Samoin Spanning-tree -looppien riski kasvaa, kun käytetään VLAN 1:stä. Tämän sijaan käytetään VLAN 79:ä hallinnointiin. Tälle VLAN:lle annetaan IP-osoite, josta kytkimen tavoittaa. IP-osoite määritetään VLAN:in sisällä ajamalla komento IP address ja perään IP-osoite ja verkon peite (mask) (Kuva 20). [24]

```
switch>enable
switch#configure terminal
switch(config)#interface vlan79
switch(config-if)#ip address 10.20.88.20 255.255.255.0
```

Kuva 20 IP-osoitteen asettaminen VLAN:lle

### 4.3 Loppuasetukset

ip default-gateway 10.20.88.1 määrittää kytkimen oletusyhdykäytäväksi (default gateway) osoitteen 10.20.88.1. Oletusyhdykäytävä on verkko-osoite jonka kautta kuljetaan toiseen verkkoon. Mikäli kytkin ei löydä omasta verkostaan kohdeosoitetta lähettää se kyselyn oletusyhdykäytävän toisessa päässä olevaan laitteeseen, joka usein on reititin. Mikäli toisessa päässä tunnetaan reitti kohdeosoitteeseen, niin paketti lähetetään eteenpäin oletusyhdykäytävää pitkin.

Ip classless on oletusasetus. Tämä mahdollistaa aliverkkojen tiedon jakamisen. Ip http server -komennon avulla voisi kytkimiä käyttää web-hallinnan (Cisco web browser) kautta. Tälle ei projektissa ollut tarvetta, eikä tätä ominaisuutta haluta käyttöön. Hallitaan suoraan komennoilla CLI:n kautta, joten no ip http server -komennolla estetään web-hallinta. Http secure-server -komento mahdollistaisi vastaavasti web-hallinnan käyttäen Secure http:tä (HTTPS). Tätä toimintoa ei myöskään haluta tukea, joten no ip http secure-server -komennolla saadaan tämä estettyä.

Command Scheduler (KRON) mahdollistaa ajastettujen komentojen ajamisen. Komennot ajetaan global configuration -tilassa. Kron occurrence weekly\_backup at 0:00 Sun recurring -komento luo ajastetun toiminnon nimeltä weekly\_backup. Tämä ajetaan aina kello 0:00 sunnuntaisin. Policy-list configuration\_backup määrittää, että tässä weekly\_backup tapahtumassa ajetaan configuration\_backup niminen sääntöpolitiikka.

Alapuolella seuraavaksi on määritelty sääntöpolitiikka nimeltä configuration\_backup. Tässä säännössä ensin ajetaan CLI:ssä write memory -komento. Tämän jälkeen ajetaan sh run -komento, jonka tulos ohjataan tftp-protokollaa käyttäen osoitteeseen pio.mt.testi.com/FIN/fin.rov-tk2-sw2.conf -tiedostoksi.

Eli kron occurrence- ja kron policy-list -toiminnoilla tässä tapauksessa ajetaan kerran viikossa backup-tiedosto, kytkimen running-config -tiedostosta suoraan erilliselle palvelimelle tfpt-palvelun kautta. Tiedosto on nimetty kytkimen mukaan, jotta tunnistetaan helposti minkä kytkimen backup konfiguraatio kyseessä.

No logging trap global configuration -tilassa määritetään, ettei lokitiedostoja tallenneta syslog-palvelimelle.

Seuraavana tulee SNMP-asetuksia. Näistä oleellisia uudelle kytkimelle ovat vain community-, trap-source-, location- ja contact-määrittelyt.

Snmp-server community -komennolla annetaan oikeudet lukea tietoa agentilta (NMS). Käytössä selkokielineen salasana, jota on moitittu tietoturvatomuudesta. Community-salasanat (Community-string) ovat selkokielineisä ja täten helposti luettavissa esimerkiksi olkapään yli. Vanhassa kytkimessä on useita community-salauksia, sillä kaksi ensimmäistä ovat vanhoja. Kukaan ei ole vain poistanut vanhoja tietoja kytkimeltä. Uuteen kytkimeen jätettiin vain käytössä oleva community-salasanaa Kiva-Nimi-Kolmas. RO perässä ilmaisee että tämä on Read-Only-salaus eli kytkin vain lukee tietoa SNMP-palvelimelta. Kytkin voi ottaa vastaan konfigurointikomentoja, mutta ei voi itse muokata SNMP-palvelimen asetuksia. Voidaan suorittaa ainoastaan Get-kyselyjä. Vanhassa kytkimessä on ollut Kiva-Nimi-Eri! RW99 on antanut read-write oikeudet, joilla voi asettaa set-operaatioita, joilla taas voidaan kirjoittaa tietoa NMS-agentille. [25]

SNMP trap-source määrittelee oletusrajapinnan (interface), josta SNMP-liikenteen tulisi kulkea. Eli snmp-server trap-source VLAN79 asettaa VLAN79:n rajapinnaksi, josta SNMP-viestejä kuunnellaan. VLAN79:lle on määritetty IP-osoite ja se on kytkimen hallinta-VLAN. [25]

Tämän jälkeen on asetettu tietoja, joilla tämän laitteen tunnistaa. Snmp-server location Suomi-Rovaniemi kertoo, että laite sijaitsee Rovaniemiellä. Toimistokonttori-sw2 auttaa tunnistamaan tarvittaessa, missä kyseinen kytkin sijaitsee. Snmp-server contact -kohtaan voitaisiin määritellä vaikka henkilö, joka kytkimestä jotakin tietäisi ja kyseisen henkilön puhelinnumeron. Vastaavasti voisi

laittaa vaikka paikallisen IT-tuen puhelinnumeron, johon henkilö voisi tarvittaessa soittaa. Vanhemmissa Cisco-kytkimissä ei välttämättä laitteen asetuksista löytynyt sarjanumeroa. Mikään sarjanumeroista ei välttämättä vastannut kytkimen päällä ollutta tarraa. Snmp-server chassis-id -komento lisää snmp-palvelimelle lähetettäviin viesteihin tekstikentän, jossa on teksti, jolla laitteen tunnistaa. Tähän on siis laitettu kytkimen sarjanumero, jotta laitteen sarjanumeron on voinut tarkistaa CLI:n kautta menemättä fyysisesti laitteen luokse. Uusissa kytkimissä tämä on oletuksena kytkimen sarjanumero, joten kyseistä komentoa ei tarvitse erikseen asettaa. Jokaisen verkkovastaavan tulisi tietää omien Ciscon kytkimiensä sarjanumerot sillä niitä tarvitaan esimerkiksi Ciscon Technical Assistant Centeriin (TAC) tehtäviin tukipyyntöihin.

Snmp traps -sanomat raportoivat laitteessa tapahtuvista muutoksista. Esimerkiksi snmp-server enable traps config ilmoittaa, kun laitteen konfiguraatioita on muokattu. Trap-viestit voidaan ohjata Device Fault Managerille (DFM), jonka avulla voidaan tarkastella vikaraportteja. DFM vastaanottaa muun muassa trap-viestejä verkon laitteilta. DFM myös ylläpitää kytkimien virhetilastoja joiden avulla voidaan havaita ongelmakohdat verkossa. DFM voi myös välittää trap-viestit toiselle hallintalaitteelle. Snmp-server host 156.44.15.55 Kiva-Nimi määrittää Network Management Station (NMS) palvelimen osoitteeksi kyseisen IP-osoitteen ja community salasanana toimii Kiva-Nimi. NMS-palvelimelle voidaan esimerkiksi määritellä, että aina trap-viestin vastaanottaessa lähetetään kytkin viestin valmiiksi määritellyyn puhelinnumeroon. Näin esimerkiksi snmp-server enable traps config -komennolla voidaan lähettää tekstiviesti puhelimeen aina, kun kytkimen konfigurointitiedostoa on muokattu. Traps-komennon perässä on haluttu toiminto, jota valvotaan. Traps eigrp lähettää viestin, mikäli eigrp naapurilaitteen linkki katkeaa ja traps vtp ilmoittaa vtp-muutoksista. Ciscon verkkosivuilta löytyy 2960-mallin kytkimien mahdolliset traps-komennot. Cisco-2960S-mallin kytkin on L2-tason kytkin, joten ei voida käyttää traps eigrp:tä, koska eigrp on reititysprotokolla. [25]

Snmp-asetuksista konfiguraatiotiedostoon jätettiin vain "snmp-server community..."-, "snmp-server trap-source..."-, "snmp-server location..." - ja "snmp-server contact..." - komennot.

Radius-server host 10.55.3.13 auth-port 1648 acct-port 1649 key 7 767H4473025 - komennossa määritetään RADIUS-palvelimen osoitteeksi 10.55.3.13. Autentikointiliikenteeseen (authentication) käytetään porttia 1648. Kirjanpidon (accounting) liikenteeseen käytetään porttia 1649. Key on laitteen ja palvelimen välinen salasana, jossa

numero 7 ennen varsinaista salasanaa tarkoittaa piilotettua (hidden) salasanaa, joka ei näy paljaana tekstinä konfigurointitiedostossa.

RADIUS-palvelimelle tulee konfiguroida salasana RADIUS-palvelimen ja verkkolaitteen välille. Mikäli laitetta ei ole lisätty RADIUS-palvelimelle, niin esimerkiksi AAA-autentikointi ei toimi. Esimerkiksi projektissa muutaman kerran uuden kytkimen konfiguroinnin jälkeen kytkimelle ei päässyt kirjautumaan Active Directory -tunnuksilla. Tämä johtui siitä, että kyseistä laitetta ei ollut määritetty RADIUS-palvelimelle. Osalla kytkimistä oli vanha RADIUS-palvelimen IP-osoite. Konfiguraatitiedostoihin korjattiin tällöin uusi toimiva IP-osoite.

Vendor-specific attributes (VSA) antaa laitevalmistajien käyttää heidän omia lisättyjä attribuutteja, joita ei voi kaikkien valmistajien laitteissa käyttää. send authentication rajoittaa attribuutit koskemaan vain autentikointia.

Control-plane ei ole tuettu Ciscon 2960S-mallin kytkimissä. Control-plane -pakettien avulla voisi esimerkiksi kaikki ARP-paketit lähettää ennalta määritettyyn IP-osoitteeseen.

Message of the day (motd) näyttää, jokaiselle terminal-yhteyden ottavalle tähän kirjoitetun viestin (Kuva 22). Viesti kirjoitetaan global configuration -tilassa. Banner motd C määrittää viestin. Viestin alkuun ja loppuun tulee C-kirjain. Kuvassa 21 asetetaan banner motd -viesti kytkimelle.

```
Switch1(config)#banner motd cOngelmatilanteissa ota yhteys IT asiantuntijaan.c
```

Kuva 21 Banner motd -viestin asettaminen global configuration -tilassa

```
Press RETURN to get started.
```

```
Ongelmatilanteissa ota yhteys IT asiantuntijaan.
```

```
Switch1>
```

Kuva 22 Banner motd -viesti terminal-yhteyden alussa

Privileged näyttää minkä tason oikeudet käyttäjällä on. Privileged interface level 7 description –komento asettaa description-komennon tasolle 7. Tämä tarkoittaa, että käyttäjällä täytyy olla vähintään tason 7 -oikeudet, jotta voi ajaa komennon description interface-tilassa.

Käyttäjällä tulee myös olla vähintään tason 7 -oikeudet, jotta voi ajaa switchport access vlan -komennon, jolla määritetään mihin VLAN:in portti kuuluu. Privileged exec level 7 write network asettaa komennon ajamiseen vaadittavan minimi oikeustason tasolle 7:n. Eli tason jälkeen tulee komento, jota asetus koskee. Ensin tulee tila, kuten exec ja interface. Tämän jälkeen oikeustaso, joka vaaditaan komennon suorittamiseen. Tämän jälkeen tulee vielä itse komento, jota asetus koskee.

Line con 0 tarkoittaa console-porttia. Komento exec-timeout 30 0 asetettaessa line console 0 -rajapinnassa asettaa odotusajaksi 30 minuuttia. Mikäli 30 minuutin aikana ei tule mitään viestejä yhteys katkaistaan. Nolla lopussa tarkoittaa sekunteja. History size 100 asettaa muistettavien komentojen määräksi 100. Show history -komento oletuksena näyttää 10 viimeistä komentoa.

Line vty 0 4 tarkoittaa virtuaalisia pääteyhteyksiä linjoilta 0-4. Eli viisi henkilöä voi samanaikaisesti ottaa telnet- tai ssh-yhteyden kytkimelle. Password rajapinnan sisällä asettaa kyseiselle yhteydelle vaadittavan salasanan. Exec-timeout asettaa ajan, mihin mennessä yhteys katkaistaan ja history size asettaa muistettavien komentojen määrän. Transport input telnet ssh määrittää sallittaviksi yhteysmuodoiksi telnet- ja ssh-yhteydet. Kytkimet voivat tukea useampaakin samanaikaista yhteyttä. Näet kytkimen

tukeman yhteyksien määrän katsomalla configuration tilassa line vty ?. Cisco 2960S-kytkimet voivat tukea 16 yhteyttä samanaikaisesti. Line vty 5 15 asettaa lopuille yhteyksille eri salasanan, kuin ensimmäiselle viidelle.

Ntp clock-period -komentoa ei tulisi itse koskaan asettaa ilman hyvää syytä. IOS automaattisesti asettaa ajan Network Time Protocol:an (ntp) mukaan. Tämän vuoksi kyseistä komentoa ei myöskään kopioida uuteen kytkimeen. Ntp server -komennolla annetaan osoite ntp-aikapalvelimelle, josta ajan synkronointi haetaan. Preferred vanhan konfiguraation IP-osoitteen perässä asettaa kyseisen osoitteen ensisijaiseksi.

End-komento tulee viimeisenä, jolla palataan takaisin privileged exec -tilaan. Ennen tätä tulee konfiguraatioon, joka kopioidaan uuteen kytkimeen asettaa vtp (VLAN Trunk Protocol) -asetukset. VTP mode client -komennolla asetetaan laite client-tilaan. Tällöin kytkin toimii, kuten VTP-palvelin, mutta ei voi luoda, muuttaa tai poistaa VLAN:ja. Tämän lisäksi VTP domain name -komennolla ilmoitetaan mitä domainia käytetään. Name kohtaan tässä tapauksessa tulee domainin nimi. Tämä määrittää minkä VTP-domainin asetukset kytkin hakee. Lopuksi vielä vtp password salasana, jossa salasana kohtaan tulee VTP-palvelimella määritelty domain-salasana. Domain-nimen tai salasanan ollessa väärin kytkin ei saa VTP-palvelimelta kyseiselle domainille määritettyjä VLAN:ja. Mikäli kytkin ei tunne VLAN:ja ja niiden asetuksia, niin ei voida myöskään kytkimen portteja niihin liittää.

Komentoja joita ei tarvinnut uudelle kytkimelle asettaa oli mm. clock time\_zone ja clock summertime, koska nämä haetaan muualta.

Kun komennot on kopioitu tekstitiedostoon josta turhat komennot poistettu, porttinimet muutettu, VTP-asetukset lisätty, IP-osoitteet ja kytkimen nimet muutettu oikein niin konfigurointitiedosto on valmis. Tämän jälkeen asetukset kopioidaan uuteen kytkimeen copy-paste-toiminnolla. Tiedoston voisi esimerkiksi tftp-palvelimen kautta siirtää kytkimelle. Tälle ei kuitenkaan nähty tarvetta.

Projektissa havaittiin, ettei konfiguraatioita kannata kaikkia liittää kerralla, sillä komennot saattavat jostakin syystä keskeytyä. Tästä syystä kopioitiin ensin komennot portti-asetuksiin asti. Tämän jälkeen kopioitiin kerralla kaksitoista porttiasetusta. Portti-asetusten jälkeen on vielä erikseen omana osana loput komennot. Samoin erään usb-to-com-adapterin kanssa oli ajurien kanssa ongelmia. Tästä johtuen koneella console-

yhteys saattoi yhtäkkiä katketa komentoja syöttäessä ilman syytä. Tämän jälkeen tietokone käynnistettiin uudelleen ja avattiin consolekaapelin kanssa uusi fyysinen console-yhteys kytkimelle. Mikäli esimerkiksi autentikointiasetukset ehtivät mennä läpi, mutta RADIUS-palvelimen osoite ei, niin kytkimelle pääsi kiinni, mutta ei voinut kirjautua sisään. Tällöin piti kytkimen salasana kiertää ja lisätä puuttuvat asetukset.

#### 4.4 Cisco 2960S kytkimen salasanan kierto

Salasanan kierto Ciscon laitteissa on yksinkertaista. Erillistä virtakatkaisijaa ei ole, joten kytkimen sai uudelleenkäynnistettyä irrottamalla virtapiuhan. Painetaan kytkimessä oleva mode-näppäin pohjaan ja kiinnitetään virtapiuha. SYST-LED-valon muuttuessa vihreäksi vapautetaan MODE-painike. Näin päästään kehote-tilaan, joka paremmin tunnetaan prompt-tilana. Syötetään `flash_init` -komento. Tämän jälkeen annetaan `load_helper` -komento. Tarkistetaan `dir flash` -komennolla flash-muistiin tallennetut tiedostot ja niiden nimet. Tämän jälkeen uudelleen nimetään `config`-tiedosto komennolla `rename flash:config.text flash:config.old`. Tässä tapauksessa tiedosto nimettiin `config.old` -tiedostoksi, mutta tämän voi nimetä kukin itse haluamallaan tavalla. `Config.text`-tiedosto sisältää käytössä olevan konfiguroinnin. Tämän jälkeen järjestelmä uudelleen käynnistetään `boot`-komennolla. Järjestelmän kysyessä "Continue with configuration dialog?" vastataan `n` eli ei. Tämän jälkeen `enable`-komennolla siirrytään `enable`-tilaan. `Enable`-tilassa konfigurointitiedosto voidaan palauttaa, jonka jälkeen salasana muutetaan.

Alla työvaiheet, kuinka toimitaan kytkimellä salasanan kiertämisen jälkeen. Suluissa on tapahtumien selitykset.

```
switch# En (Enable-tila/privileged exec-tila)
```

```
switch# rename flash:config.old flash:config.text (Muutetaan config-tiedosto takaisin oikeaan muotoon)
```

Painetaan enter (hyväksytään muutokset)

```
switch#copy flash:config.text system:running-config (Kopioidaan tiedosto laitemuistiin)
```



Painetaan enter (hyväksytään muutokset)

Nyt konfigurointitiedosto on laitteen muistissa. Tämän jälkeen voidaan muuttaa salasanaa.

```
switch# Conf t (mennään konfigurointi-tilaan)
```

```
switch(config)#enable secret SALASANA (Salasanaksi SALASANA)
```

```
switch(config)#end (Palataan takaisin enable-tilaan)
```

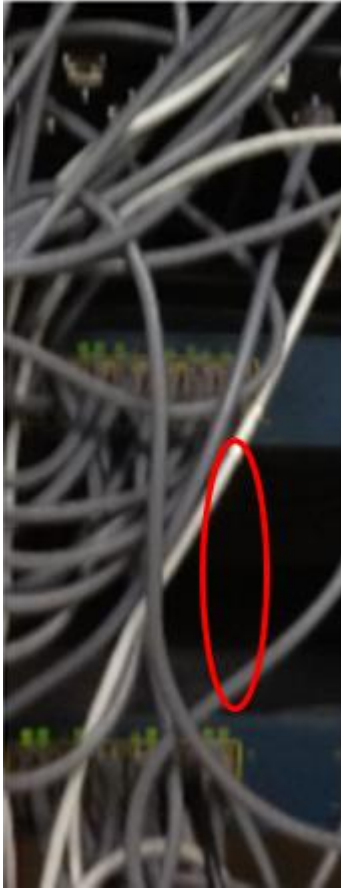
```
switch#wr mem (write memory -tallentaa laitteen asetukset muistiin, jotta uudelleenkäynnistyksessä asetukset eivät häviä.)
```

Vaihtoehtoisesti voidaan jättää vanha tiedosto palauttamatta ja syöttää kokonaan uudet konfigurointiasetukset ja tallentaa nämä laitteen muistiin. Tällöin ilman erillistä poistoa jää flash-muistiin talteen vanhat kytkinasetukset nimellä config.old, joka voidaan tarvittaessa palauttaa.

## 5 Kytkimien asentaminen paikoilleen

Ennen kytkimen vaihtoa on hyvä varmistaa, että kytkin mahtuu kytkinkaappiin. PoE-virralla varustetut kytkimet ovat PoE-virrattomia kytkimiä isompia. Tämä on hyvä tarkistaa inventaarion aikana. Tuotantoympäristössä, jossa verkkokatkokset tulee tehdä hallitusta, voi tällainen yhtäkkinen ongelma viivästyttää kytkimen vaihtoa jopa päivillä.

Mikäli kytkinkaapissa on kytkimien välille jätetty tyhjää tilaa (kuva 23), voi tätä tilaa käyttää vaihdoissa hyväksi lyhentämään verkkokatkoksen aikaa. Kiinnitetään uusi kytkin vaihdettavan kytkimen ylä- tai alapuolelle riippuen kummalla puolella on paremmin tilaa.



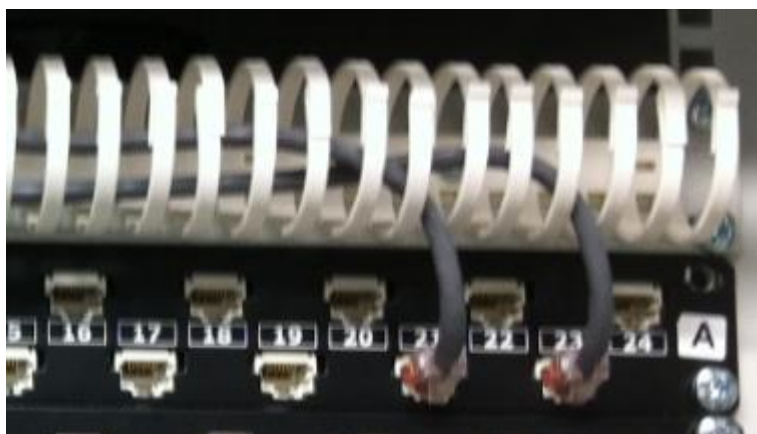
Kuva 23 Kytkimien väliin jätetty tyhjä tila

Kiinnitetään uusi kytkin kaappiin ruuveilla (kuva 24), jotta laite ei pääse putoamaan.



Kuva 24 Kytкин kiinnitetään ruuveilla

Vaihdetaan vanhasta kytkimestä uuteen ethernet-verkkokaapelit laittamalla ensimmäisen portin kaapeli uuden kytkimen ensimmäiseen, toisen portin kaapeli uuden kytkimen toiseen porttiin ja niin edelleen jatkaen viimeiseen verkkokaapeliin saakka. Tällöin lopussa kiinni oleville laitteille ei tule verkkokatkosta heti. Samalla on hyvä tarkistaa, että kaapelit eivät estä vanhan kytkimen poistoa kaapista. Vaihtoon on hyvä varata varmuuden vuoksi mukaan muutama pidempi verkkokaapeli. Paras tapa olisi vaihtaa kaikki kaapelit oikeanmittaisiin ja kuljettaa ne nätisti esimerkiksi kaapeleille tarkoitettua riimaa pitkin (Kuva 25) kytkimelle. Tämä kuitenkin veisi huomattavasti enemmän aikaa aiheuttaen pidempiä verkkokatkoksia, jonka takia projektissa tähän ei ryhdytty.

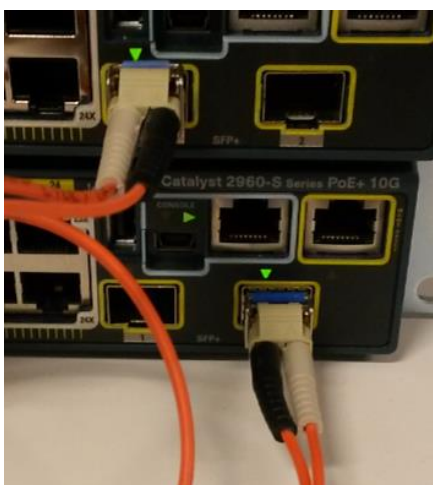


Kuva 25 Kaapelit kulkevat niille tarkoitettua pidikettä pitkin

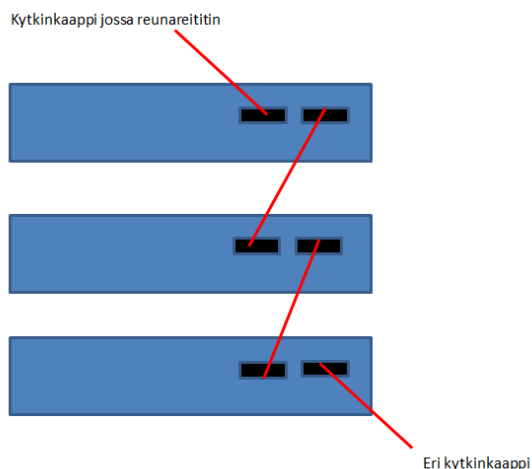
Kuitukaapelit kiinnitetään viimeiseksi. Kuidun päät kiinnitetään porteissa oleviin kuitumoduuleihin varmistaen, että ovat oikein päin. Kuitupäiden parit on merkitty A- ja B-renkailla, helpottamaan tunnistusta (Kuva 26). Kuitupäät voi myös olla erotettu toisistaan erivärisillä päillä (Kuva 27). Kuitukaapeleita käsitellessä on tärkeää, ettei kaapeli pääse taipumaan liikaa. Ohut kuitukaapeli taipuu helposti. Taipuminen aiheuttaa helposti särön suojan sisällä olevaan kuituun. Vioittuneen kuidun vaimennus saattaa kasvaa ajan myötä aiheuttaen hitautta verkossa tai verkkokatkoksia. Projektissa kuitumoduulit kytketään niin, että ensimmäisestä portista data tulee sisään ja toisesta portista lähtee ulos. Ensimmäisen kytkimen kuituportti kytketään kuitupaikalle, josta on suora reitti kytkinkaapille, missä sijaitsee reunareitin. Vastaavasti viimeisestä kytkimestä menee kytkentä johonkin toiseen kytkinkaappiin (Kuva 28). Tällöin mikäli yksi kytkin hajoaa kytkinkaapista, ei muilta kytkimiltä katkea verkko kokonaan vaan ne ”löytävät” vaihtoehdoisen reitin.



Kuva 26 Kuitukaapeleiden päät on merkitty, jotta helpompi kytkeä oikein



Kuva 27 Kuitukaapeli kytkettynä ristiin kuitumoduuleihin



**Kuva 28 Kuitujen kytkeminen kytkimien välillä**

Vanhasta kytkimestä irrotetaan virtakaapeli ja kiinnitetään uuteen kytkimeen. Vanha ja uusi kytkin ei voi olla samanaikaisesti päällä ja verkossa, koska kytkimillä on sama IP-osoite.

Kytkimen käynnistymisessä voi kestää useita minuutteja. Tämä on normaalia. Mikäli kuituporttiin ei syty valoa on hyvä tarkistaa, että kuidut ovat oikein päin. Kuidun päät tulee kytkeä ristiin (Kuva 27). Toisessa kuidussa pitäisi kokoajan kulkea dataa, joten kuidun sisällä näkyy punaista valoa. Katsomalla kuidun päihin voi tarkistaa onko päät oikein päin. Tämä on hyvä tiedostaa, mikäli kaapelissa ei esimerkiksi ole mitään muita merkintöjä. Portissa pitäisi kulkea dataliikennettä ja täten porttivalon tulisi oikein kytkettynä syttyä vihreäksi.

Porttien ollessa ylhäällä ja palaessaan vihreänä pitäisi liikenteen toimia. Tämän jälkeen on hyvä tarkistaa, että kytkin vastaa verkkoon vaikkapa pingaamalla kytkimen IP-osoitetta. Tämän lisäksi on hyvä testata, että kytkimeen pääsee etänä kiinni.

Kun uusi kytkin on toiminnassa, voidaan vanha kytkin poistaa. Irrotetaan vanha kytkin pois varoen samalla, etteivät kytkimen kannakkeet mahdollisesti tartu kuitu- tai verkko-kaapeleihin repien tai pahimmassa tapauksessa rikkoen niitä. Kun vanha kytkin on irti, voidaan uusi kytkin halutessa siirtää vanhan kytkimen paikalle. Irrotetaan ruuvit pidellen samalla kytkintä paikallaan, jotta kytkin ei pääse putoamaan. Nostetaan tai laske-

taan riippuen oliko vanha kytkin ylempänä vai alempana ja kohdistetaan kytkimen kannakkeet vanhojen kiinnikkeiden kohdalle. Kiinnitetään ruuvit paikalleen riittävän kireälle. Tämän jälkeen kyseisen kytkimen vaihto on valmis.

Mikäli kytkinkaapissa ei ole ylimääräistä tilaa johon kytkimen voisi valmiiksi kiinnittää, voi vaihdon suorittaa kannattelemalla kytkintä vaikka sylissä. Mikä mahdollista on tähän hyvä pyytää, jotakuta auttamaan. Vanha kytkin irrotetaan ja otetaan ulos kaapista. Toinen siirtää kaapelit uuteen kytkimeen silla välin, kun toinen pitelee vanhaa kytkintä sylissä. Mikäli ruuvien ruuvaamiseen käytetään erillistä akkukäyttöistä ruuvinväännintä, tulee varoa, ettei vahingossa riko ruuvin pintaa. Ruuvit voivat olla hyvin tiukassa ja ruuvimeisselin lipsuminen ruuvin urasta voi rikkoa ruuvin pään. Varsinkin ison kytkimen kanssa käytetään ruuvinväännintä, jotta ruuvaus tapahtuu mahdollisimman nopeasti. Kytkin on hyvin painava. Jotta kytkin saadaan nostettua kytkinkaappiin, tarvitaan kaksi henkilöä nostamaan ja kannattelemaan kytkintä. Samalla yksi henkilö ruuvaa ruuvit paikoilleen. Iso kytkin on reitittävä joten minä en tee porttikonfiguraatioita.

Jotbar-kytkimet, eivät vaadi erillistä aikataulun sopimista. Kytkimien vaihdosta ei aiheudu käyttäjille näkyviä häiriöitä. Vaihto saattaa vaikuttaa hetkellisesti ovien aukaisuun, joten on hyvä katsoa, ettei ihmisiä ole kulkemassa ovista vaihdon aikana. Kytkimien konfiguroinnissa ei ole suurta eroa. Porttinimiä ei tarvitse muuttaa, koska jotbar-kytkimissä on kahdeksan FastEthernet-porttia. Kytkimiin tulee perusasetukset, kuten enable password, enable secret, line vty x x login, ja service password-encryption. Näiden lisäksi määritellään gateway, IP- osoite, domain-osoite, nimipalvelimen-osoite, kytkinporttien asetukset ja VTP-asetukset. Samoin tulee muistaa konfiguraatioiden syöttämisen jälkeen tallentaa muutokset laitteen muistiin write memory -komennolla.

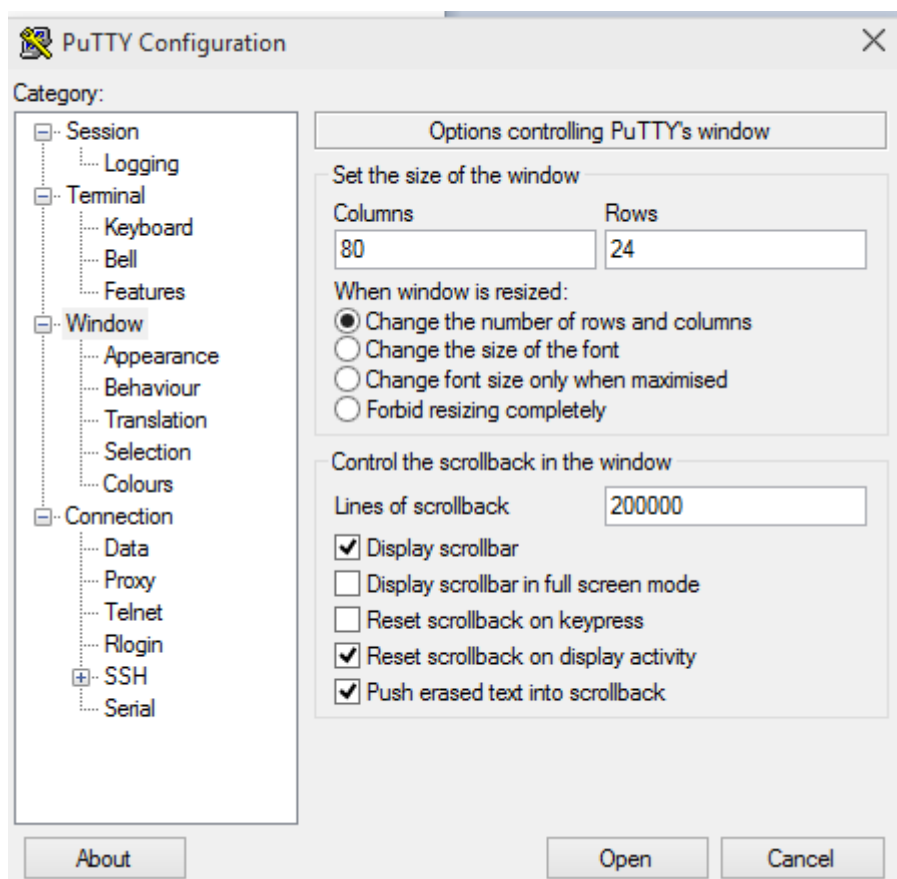
## 6 Ohjeiden teko VLAN-muutoksiin

Microsoft Word -ohjelmalla tehtiin kytkimien VLAN-muutosten teosta ohjeet yrityksen IT Service Deskille. Tarkoituksena on, että osa IT Service Deskin työntekijöistä tekee jatkossa VLAN-muutoksia. Näin saadaan asiakkaille nopeampaa palvelua. IT Service Desk käy esimerkiksi kytkemässä uuden verkkopaikan ja samalla asettaa portin oike-

aan VLAN-verkkoon laitteesta riippuen. VLAN-verkko määräytyy tarpeen mukaan. Mikäli kytkettävä laite on tulostin, niin asetetaan portti tulostimille tarkoitettuun VLAN:iin.

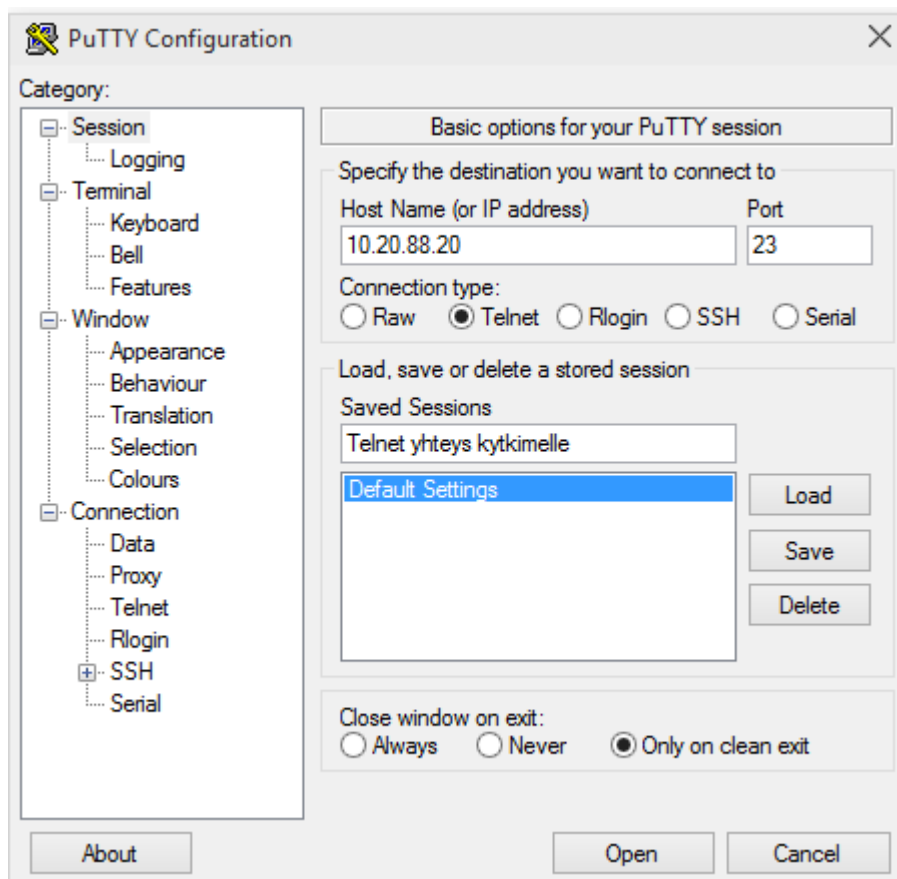
Ohjeiden alussa neuvotaan putty-ohjelman asetusten laitto. Tämän jälkeen opastetaan kytkimelle kirjautuminen ja tavallisimmat komennot. Listataan myös yleisimmät VLAN:it ja porttiasetukset, joita voi tarvittaessa käyttää mallina.

Avataan Putty-ohjelma ja mennään Window-välilehdelle. Lisätään Lines of scrollback -kohdalla muutama nolla perään. Lines of scrollback tarkoittaa, kuinka monta riviä tekstiä Putty muistaa. Oletusasetuksilla ei välttämättä näy sh run -komennolla kaikki porttiasetukset samaan aikaan. Mikäli halutaan kopioida konfiguraatiot kytkimeltä talteen, tarvitsee Lines of scrollback -kohdasta valita enemmän muistettavia rivejä esimerkiksi 20000 riviä (Kuva 29).



Kuva 29 Lines of scrollback

Mennään takaisin alkuun eli Session-välilehdelle. Yhteysmuodoksi valitaan Telnet. Saved session -kohtaan kirjoitetaan nimi, jolla asetukset halutaan tallentaa ohjelmaan. Kun asetukset on tallennettu, niin laitetaan Host Name kohtaan kytkimen IP-osoite ja painetaan Open (Kuva 30).



Kuva 30 Asetusten tallentaminen

Kytkimelle kirjaututaan henkilön omilla Active Directory -käyttäjätunnuksilla. Kirjautumiseen tapahtuu tyylillä domain\käyttäjätunnus. Salasana on käyttäjätunnuksen salasana. Ohjeessa kerrotaan myös yleisimmät komennot kuten (komento ja selitykset):

show running-config (sh run)	/ Näyttää kytkimeen tallennetut konfiguraatiot
show interface status (sh int status)	/Näyttää porttien tilat ja niihin määritetyt VLAN:it
show vlan (sh vlan)	/ Näyttää kaikki käytettävissä olevat VLAN:it
configure terminal (conf t)	/Päästään configure-tilaan. Näyttää kytkimellä switch(config)#



interface gigabitethernet1/0/x	/ Päästään portin x asetuksiin. Näyttää kytkimellä switch(config-if)#
switchport mode access	/ Portti access-tilaan
switchport mode trunk	/Kytkin trunk-tilaan
switchport description "kuvaus"	/ Miten saadaan kommentti kytkinporttiin
switchport access vlan X	/ Portille määritetään käytettäväksi vlan X
shutdown & no shutdown	/Portti kiinni ja portti päälle
end	/ Päästään takaisin enable tilaan switch#
write memory (wr mem)	/Tallentaa asetukset kytkimen muistiin
write network (wr net)	/Tallentaa asetukset verkkolevylle
Address or name of remote host? X.X.X.X /tallennettavan palvelimen IP-osoite	
Destination file "kytkimen nimi-config"?[confirm]: Paina Enter	
Write file tftp://x.x.x.x/"kytkimen nimi-config"?[confirm]: Paina Enter	
!![OK] / Kuittaus	
logout	/Kirjautuu ulos kytkimeltä

Lopuksi vielä listataan yleisimmät VLAN- ja porttiasetukset malleiksi.

## 7 Huomioitavia asioita

Kytкимиä ei isossa tuotantoyrityksessä voida vaihtaa milloin vain. Ennen vaihtoa tulee huomioida mihin kaikkeen vaihto saattaa vaikuttaa. Mahdollisista häiriöistä tulee aina ilmoittaa etukäteen osastoille, joihin muutostyöt saattavat vaikuttaa. Erityisesti tulee huomioida vaikutukset tuotantoon. Tuotantoon tulee aina hyvissä ajoin ilmoittaa mahdollisista verkkokatkoksista. Väärällä hetkellä katkaistu verkko, saattaa pysäyttää tuo-

tannon aiheuttaen yritykselle tarpeettomia ja mahdollisesti suuriakin lisäkustannuksia. Samoin tulee ottaa huomioon, että tuotannossa aikataulut voivat muuttua. Suunniteltu tuotantokatkos ei välttämättä olekaan kaikilla tuotantolinjoilla oletetusti. Tarvittaessa tuotanto pyörii ja menee muun edelle. Tämän takia erityisen tärkeätä ilmoittaa hyvissä ajoin, jopa viikkoja etukäteen, mikäli tuotannon verkkoon on tulossa katkoksia. Tämä on tarpeen, jotta tuotannossa ehditään ajoissa varautua häiriöihin. Toimistotiloissa, missä ei kriittisiä järjestelmiä kiinni vaihdetaan kytkimet toimistotyöajan ulkopuolella, jotta käyttäjille aiheutuisi mahdollisimman vähän häiriötä.

Samalla on hyvä tiedostaa verkon jatkuva muuttuminen. Kytkennät muuttuvat koko ajan. Kokonaan uusia kytkimiä otetaan käyttöön, kun portit loppuvat ja tarvittaessa rakennetaan kokonaan uusia kytkinkaappeja. Toimistotilojen kunnostustöiden myötä yksi kytkinkaappi oli purettu pois. Tästä ei ollut kulkeutunut ajoissa tietoa IT-tiimille. Lukitun kytkinkaapin sisällä olleet muutaman kuukauden vanhat kytkimet imaisivat sisälleen kittipölyä. Kyseiset kytkimet tuli purkaa ja putsata paineilmalla. Ruuvattiin kaikki ruuvit irti ja irrotettiin kansi, jotta saatiin puhallettua pölyt pois. Putsatut kytkimet otetaan käyttöön projektin kytkinvaihtoihin. Nämä kytkimet korvaavat vähemmän tärkeät kytkimet siltä varalta, jos kytkimissä ilmenee ajan myötä vikoja.

Kuitukaapeleiden määrä kartoitettiin etukäteen, jotta kuidut eivät loppuisi kesken. Show interfaces status -komennolla nähdään onko käytössä yksi- vai monimuotokuitua. Esimerkiksi 1000BaseSX SFP tarkoittaa, että portissa kiinni monimuotokuitu. Mikäli 1000BaseLX SFP (Kuva 31), niin käytössä yksimuotokuitua.



```

G11/0/25 TRUNK connected trunk a-full a-1000 1000BaseLX SFP

```

Kuva 31 Portti on kytketty yksimuotokuidulla



```

G11/0/26 connected trunk a-full a-1000 1000BaseSX SFP

```

Kuva 32 Portti on kytketty monimuotokuidulla

Uusien kytkimien kuitumoduulit ovat kaikki LC-liittimillä, joten tarvittavat liitinpäät voidaan selvittää etänä. Mikäli kuitukaapeli tulee kytkinkaapin sisällä kytkimeltä kytkimelle, on kaapeli LC-LC-liittimillä. Mikäli kytkentä on kytkinkaapin kuiturimalle, niin tarvitaan SC-LC-kuitukaapeli.

Write memory -komento tärkeä muistaa laittaa aina konfiguraatioiden muuttamisen jälkeen. Muuten muutokset häviävät, kun kytkin käynnistyy uudelleen. Kovalla ukkosella oli maadoituskaapelia pitkin tullut virtapiikki kytkimille. Tämän johdosta muutama vanhempi, kytkin oli siirtynyt uudelleenkäynnistyksessä VTP transparent -tilaan. Kytkimille tuli tästä johtuen väärät VLAN:it, eikä verkko kytkimien kautta enää toiminut. Samoin muutama vanhempi kytkin hajosi virtapiikin saatuaan. Rikkinäiset kytkimet kuuluvat vaihdettaviin kytkimiin, joten otettiin lavalta uudet kytkimet joihin syötettiin tarvittavat konfiguraatiot. Porttiasetukset saatiin kytkimien backup-tiedostoista.

## 8 Yhteenveto

Projekti onnistui hyvin. Ciscon vanhat kytkimet vaihdettiin uudempiin aiheuttamatta ongelmia tuotannolle tai loppukäyttäjille. Projektin aikana ilmeni, että osa kytkinkaapeissa sijaitsevista UPS-laitteista oli vanhoja ja viallisia. Mikäli tuli sähkökatko niin kaikki UPS-laitteet eivät välttämättä enää lähteneet uudelleen päälle, jolloin kaikki kaapin kytkimet olivat ilman virtaa. Tehdyn inventaarion avulla oli helppo selvittää, missä kaikissa kytkinkaapeista oli vielä käytössä vanhoja UPS-laitteita, jotka piti vaihtaa.

Kuituverkon kartta on tehty ja siinä näkyy mistä kaapista on mihinkin yhteys. Samoin toisesta kuitukartasta näkee miltä kytkimeltä on minnekin kuituyhteys. Näitä voidaan käyttää hyödyksi jatkossa, kun tehdään uusia kytkinkaappeja tai lisätään uusia kytkimiä. Samoin kytkinkaappien sijainnin näyttävä kartta on päivitetty. Karttaan lisättiin uudet kytkinkaapit ja vanhat poistuneet kaapit poistettiin. Karttaan on korjattu myös siinä olleet kaappien sijaintivirheet.

Uudet kytkimet ovat nyt kytketty niin, ettei yhden hajoaminen katkaise verkkoa useammalta kytkimeltä. Mikäli kaapissa yksi kytkin hajoaisi, niin kaikilla muilla kytkimillä pysyy verkkoyhteys. Tämä tuo turvaa, joka tärkeää varsinkin tuotantoympäristössä.

## Lähteet

- 1 Catalyst 3560 Switch Getting Started Guide. Verkkodokumentti.  
<[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/hardware/guide/guide/3560gsg\\_08.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/hardware/guide/guide/3560gsg_08.html)> Kuva otettu 2.6.2015.
- 2 Catalyst 2960-S Switch Getting Started Guide s. 3, joka löytyy kytkimen mukana tulleen CD:n 2960S\_gsg\_en.pdf-tiedostosta.
- 3 Catalyst 2960-S Switch Getting Started Guide s. 22, joka löytyy kytkimen mukana tulleen CD:n 2960S\_gsg\_en.pdf-tiedostosta.
- 4 Creation and Management of Catalyst 3750 Switch Stacks. 2007. Verkkodokumentti. <<http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html>>. Luettu 14.4.2015.
- 5 Fire Protection for Industry & Energy. Verkkodokumentti.  
<http://www.marioff.com/fire-protection/fire-protection-for-industry-and-energy>.  
Luettu 10.3.2015.
- 6 Fire Protection for Marine & Offshore. Verkkodokumentti.  
<http://www.marioff.com/fire-protection/fire-protection-for-marine-offshore>. Luettu 10.3.2015.
- 7 Marioff. 2014. Verkkodokumentti. <https://fi.wikipedia.org/wiki/Marioff>. Luettu 10.3.2015.
- 8 Cisco Guide to Harden Cisco IOS Device. 2014. Verkkodokumentti.  
<http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>. Luettu 25.4.2015.
- 9 Configuring System Message Logging. Verkkodokumentti.  
<[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1\\_9\\_ea1/configuration/guide/scg/swlog.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_9_ea1/configuration/guide/scg/swlog.html)>. Luettu 25.4.2015.

- 10 Configuring Authentication. Verkkodokumentti.  
<[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c/scfathen.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html)>. Luettu 25.4.2015.
- 11 Basic System Management Commands. Verkkodokumentti.  
[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/configfun/command/reference/ffun\\_r/frf012.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf012.html). Luettu 26.4.2015.
- 12 Configuring System MTU. Verkkodokumentti.  
[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/software/15-0\\_2\\_EX1/int\\_hw\\_components/configuration\\_guide/b\\_int\\_152ex1\\_2960-xr\\_cg/b\\_int\\_152ex1\\_2960-xr\\_cg\\_chapter\\_0110.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/software/15-0_2_EX1/int_hw_components/configuration_guide/b_int_152ex1_2960-xr_cg/b_int_152ex1_2960-xr_cg_chapter_0110.html). Luettu 26.4.2015.
- 13 Subnet Zero and the All-Ones Subnet. 2005. Verkkodokumentti.  
<http://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/13711-40.html#subnetzero>. Luettu 26.4.2015.
- 14 How Vulnerable Are Your Cisco IOS Routers?. 2010. Verkkodokumentti.  
<http://www.infosecisland.com/blogview/4377-How-Vulnerable-Are-Your-Cisco-IOS-Routers.html>. Luettu 29.4.2015.
- 15 Enabling and Disabling DNS Lookup. Verkkodokumentti.  
<[https://www.informit.com/library/content.aspx?b=CCNA\\_Practical\\_Studies&seqNum=34](https://www.informit.com/library/content.aspx?b=CCNA_Practical_Studies&seqNum=34)>. Luettu 29.4.2015.
- 16 mls qos (global configuration mode) through mpls experimental. Verkkodokumentti.  
<[http://www.cisco.com/c/en/us/td/docs/ios/qos/command/reference/qos\\_book/qos\\_m2.html](http://www.cisco.com/c/en/us/td/docs/ios/qos/command/reference/qos_book/qos_m2.html)> Luettu 1.5.2015.
- 17 Errdisable Port State Recovery on the Cisco IOS Platforms. 2009. Verkkodokumentti. < <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html>> Luettu 1.5.2015.
- 18 Cisco verkkoakatemia toinen vuosi, v. 2002 s. 57.

- 19 Deploying RSA Keys Within a PKI. Verkkodokumentti.  
<[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_pki/configuration/xs-3s/sec-pki-xe-3s-book/sec-deploy-rsa-pki.html#GUID-DCB20ADF-1F8E-434B-AE97-54802879F34F](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xs-3s/sec-pki-xe-3s-book/sec-deploy-rsa-pki.html#GUID-DCB20ADF-1F8E-434B-AE97-54802879F34F)>. Luettu 4.5.2015.
- 20 Spanning Tree Protocol. 2015. Verkkodokumentti.  
<[http://en.wikipedia.org/wiki/Spanning\\_Tree\\_Protocol](http://en.wikipedia.org/wiki/Spanning_Tree_Protocol)>. Luettu 4.5.2015
- 21 Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard. Verkkodokumentti.  
<[http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp\\_enha.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html)>. Luettu 4.5.2015
- 22 show vlan through spanning-tree vlan. Verkkodokumentti.  
<[http://www.cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw\\_book/lsw\\_s2.html#wp1110581](http://www.cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book/lsw_s2.html#wp1110581)>. Luettu 4.5.2015.
- 23 Understanding and Configuring the Unidirectional Link Detection Protocol Feature. Verkkodokumentti. <<http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10591-77.html>>. Luettu 4.5.2015.
- 24 VLANs. Verkkodokumentti. <<http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10591-77.html>>. Luettu 4.5.2015
- 25 Configuring SNMP Support. Verkkodokumentti.  
<[http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/configfun/configuration/guide/ffun\\_c/fcf014.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.html)>. Luettu 4.5.2015

**Vanhan L3-tason ja uuden L2-tason kytkimen konfiguraatioiden erot**

```
vanha
 uusi

!
! NVRAM config last updated at 00:00:00 CDT Sun Jul 14 2014
!
version 12.2
no service pad
service timestamps debug datetime localtime
service timestamps log datetime msec localtime show-timezone
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname fin-rov-tk2-sw2
!
boot-start-marker
boot-end-marker
!
logging buffered 409600
enable secret 5 $5$c3kK$ZTFaNMtubOLVTwh6LKBar
!
username administrator password 7 88KD3B44428HJH
!
aaa new-model
!
aaa authentication fail-message ^CFailed login. Three consecu-
tive fails will revoke.^C
aaa authentication login default group radius local
aaa authorization exec default group radius if-authenticated
aaa authentication enable default group radius enable
aaa authorization exec default group radius none
aaa accounting exec default start-stop group radius
!
!
!
aaa session-id common
switch 1 provision ws-c2960s-48lpd-1
!
clock timezone EET 2
clock summer-time CDT recurring
system mtu routing 1500
ip subnet-zero
no ip source-route
no ip domain-lookup
ip domain-name mt.testi.com
ip name-server 10.25.156.45
ip name-server 10.16.76.124
!
!
```

```
mls qos
!
!
!
!
!
errdisable recovery cause udd
errdisable recovery cause bpduguard
!
!
crypto pki trustpoint TP-Seld-Signed-4245666245
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-4245666245
revocation-check none
rsakeypair TP-self-signed-4245666245
!
crypto pki certificate chain TP-seld-signed-4245666245
certificate self-signed 01
32522456 4084224D A4960400 6004865B 511D0072 4A564995 F46D3232 84966855
72410B40 02050455 04051402 5554410B 40020504 55040814 02444141 15401405
0455040A 140F4452 74545F20 54727474 555D4120 401T0504 55040B14 17747552
5F725420 745F205B 5158755F 75522042 50425455 41244022 05045504 04141B72
5T522D75 05866544 22049586 99204561 2495669T 634T5678 574968T 356D7966
31343233 46745632 95744A65 6D345724 35783467 41457754 345A7833 4456770F
45363235 2A543652 2235657F 2356777T 23557A85 3457F75D 47470405 44053B25
2D777345 3T665456 234F5T46 3F5D745F 235D7908 4A467834 F36D3456 34677865
4B224500 425675B4 03478941 4B4145T1 657A3456 3AF7T74T F73AF677 B5A44564
24T253F2 52356378 40FF55D2 45A56B2F 2225A76A 23500F32 ABA36720 64TF3DD6
3F467ANB 5F2F5256 05437800 A446F657 51F6700B 4045573D 6F749904 08567005
1F535455 1D330575 44576547 473B588D 3457532T 34683325 4F6T754F 5D841D25
36551D6T 32578474 456D2234 163C2A22 25D264FF 3DD66A2A 3F77F614 43464624
441DJ505 17063503 13BD252F T125T817 1D532D57 585255B6 D8524AeF 74005195
0346781D 1F345T60 7F406A50 3FA67AA3 46437321 0T507F05 3467070A 13467542
05333F51 52660323 04630670 145B366T 5633J541 40245756 72749345 52235744
77232D55 6T215667 73A213A4 12345541 0T422F04 0553240A 12563462 64374F41
95883295 06744385 151B422T 663D2567 25786544 23788557 53467884 63484D51
2T564366 94577D03 643A8638 26F73D06 03467833 75440015 BF76TFF4 234667DF
T337507F 7A6DA36G 4TD33G85 F6F34566 23567773 3F15436D 03467A73 6346635B
1A52640A 23460T63 3B6N445R 24F6D236 3DD7734F 245F77
quit
```



```
!  
!  
spanning-tree mode pvst  
spanning-tree portfast bpduguard default  
spanning-tree portfast bpdufilter default  
spanning-tree extend system-id  
spanning-tree uplinkfast  
!  
vlan internal allocation policy ascending  
!  
ip ssh time-out 60  
ip ssh version 2  
ip scp server enable  
!  
!  
interface FastEthernet0  
no ip address  
shutdown  
!  
interface FastEthernet0/1  
description KUVAUS PORTIN TARKOITUKSESTA  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
mls qos trust cos  
no snmp trap link-status  
spanning-tree portfast  
!  
!  
interface GigabitEthernet1/0/1  
description KUVAUS PORTIN TARKOITUKSESTA  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
mls qos trust cos  
spanning-tree portfast  
!  
interface FastEthernet0/2  
description KUVAUS PORTIN TARKOITUKSESTA  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
mls qos trust cos  
no snmp trap link-status  
spanning-tree portfast  
!  
interface FastEthernet0/3  
description KUVAUS PORTIN TARKOITUKSESTA  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
mls qos trust cos  
no snmp trap link-status
```

```
    spanning-tree portfast
!
interface FastEthernet0/4
    description KUVAUS PORTIN TARKOITUKSESTA
    switchport access vlan 10
    switchport mode access
    switchport voice vlan 20
    mls qos trust cos
    no snmp trap link-status
    spanning-tree portfast
!
interface FastEthernet0/5
    description KUVAUS PORTIN TARKOITUKSESTA
    switchport access vlan 10
    switchport mode access
    switchport voice vlan 20
    mls qos trust cos
    no snmp trap link-status
    spanning-tree portfast
!
interface FastEthernet0/6
    description KUVAUS PORTIN TARKOITUKSESTA
    switchport access vlan 10
    switchport mode access
    switchport voice vlan 20
    mls qos trust cos
    no snmp trap link-status
    spanning-tree portfast
!
interface FastEthernet0/7
    description PRINTTERI
    switchport access vlan 30
    switchport mode access
    switchport voice vlan 20
    mls qos trust cos
    no snmp trap link-status
    spanning-tree portfast
!
interface FastEthernet0/8
    description KUVAUS PORTIN TARKOITUKSESTA
    switchport access vlan 10
    switchport mode access
    switchport voice vlan 20
    mls qos trust cos
    no snmp trap link-status
    spanning-tree portfast
!
interface FastEthernet0/9
    description KUVAUS PORTIN TARKOITUKSESTA
    switchport access vlan 10
    switchport mode access
    switchport voice vlan 20
    mls qos trust cos
```

```
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/10
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/11
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/12
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/13
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/14
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/15
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
```

```
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/16
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/17
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/18
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/19
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/20
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/21
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
```

```
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/22
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/23
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/24
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/25
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/26
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/27
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
```

```
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/28
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/29
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/30
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/31
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/32
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/33
description KUVAUS PORTIN TARKOITUKSESTA
```

```
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/34
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/35
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/36
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/37
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/38
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/39
```

```
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/40
description KUVAUS PORTIN TARKOITUKSESTA
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/41
description PRINTTERI
switchport access vlan 30
switchport mode access
mls qos trust cos
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/42
description PRINTTERI
switchport access vlan 30
switchport mode access
no snmp trap link-status
spanning-tree portfast
!
!
interface GigabitEthernet1/0/42
description PRINTTERI
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/43
description PRINTTERI
switchport access vlan 30
switchport mode access
no snmp trap link-status
spanning-tree portfast
!
interface FastEthernet0/44
description PRINTTERI
switchport access vlan 30
switchport mode access
no snmp trap link-status
spanning-tree portfast
!
```



```
interface FastEthernet0/45
  description PRINTTERI
  switchport access vlan 30
  switchport mode access
  no snmp trap link-status
  spanning-tree portfast
!
interface FastEthernet0/46
  description PRINTTERI
  switchport access vlan 30
  switchport mode access
  no snmp trap link-status
  spanning-tree portfast
!
interface FastEthernet0/47
  description PRINTTERI
  switchport access vlan 30
  switchport mode access
  no snmp trap link-status
  spanning-tree portfast
!
interface FastEthernet0/48
  description PRINTTERI
  switchport access vlan 30
  switchport mode access
  no snmp trap link-status
  spanning-tree portfast
!
interface GigabitEthernet0/1
  description KYTKIMEN NIMI, JOKA KIINNI PORTISSA
  switchport trunk encapsulation dot1q
  switchport mode trunk
  logging event trunk-status
  uddld port aggressive
!
!
interface GigabitEthernet1/0/49
  description KYTKIMEN NIMI, JOKA KIINNI PORTISSA
  switchport mode trunk
!
interface GigabitEthernet1/0/50
  description KYTKIMEN NIMI, JOKA KIINNI PORTISSA
  switchport mode trunk
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/3
  description KYTKIMEN NIMI, JOKA KIINNI PORTISSA
  switchport trunk encapsulation dot1q
```

```
switchport mode trunk
logging event trunk-status
udld port aggressive
!
interface GigabitEthernet0/4
description KYTKIMEN NIMI, JOKA KIINNI PORTISSA
switchport trunk encapsulation dot1q
logging event trunk-status
udld port aggressive
!
interface Vlan1
no ip address
shutdown
!
interface Vlan79
description HALLINTA
ip address 10.20.88.20 255.255.255.0
!
ip default-gateway 10.20.88.1
ip classless
no ip http server
no ip http secure-server
!
kron occurrence weekly_backup at 0:00 Sun recurring
policy-list configuration_backup
!
kron policy-list configuration_backup
cli write mem
cli show run | redirect tftp://kopio.mt.testi.com/FIN/fin-rov-
tk2-sw2.conf
!
no logging trap
snmp-server community Kiva-Nimi RO 98
snmp-server community Kiva-Nimi-Eri! RW99
snmp-server community Kiva-Nimi-Kolmas RO
snmp-server trap-source Vlan79
snmp-server location Suomi-Rovaniemi-Toimistokonttori-SW2
snmp-server contact Tässä sopiva yhteyshenkilö
snmp-server chassis-id rov-tk-sw2
snmp-server enable traps snmp authentication linkdown linkup
coldstart warmstart
snmp-server enable traps transceiver all
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
```

```
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature
status
snmp-server enable traps cef resource-failure peer-state-change
peer-fib-state-change inconsistency
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency
loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 156.44.15.55 Kiva-Nimi
radius-server host 10.55.3.13 auth-port 1648 acct-port 1649 key
7 767H44730258
radius-server vsa send authentication
!
control-plane
!
banner motd^CC
*****
* Unauthorized access prohibited
*
* Authentication
* Use FDOM accounts
*
* Contact Tähän yhteyshenkilö
* Phone Puhelinnumero
* Email sähköpostiosoite
*
* Location
* Suomi - Rovaniemi
*
*****
^C
privilege interface level 7 description
privilege interface level 7 switchport access vlan
privilege configure level 7 interface
privilege exec level 7 write network
privilege exec level 7 ping
privilege exec level 7 exit
privilege exec level 7 configure terminal
privilege exec level 7 write memory
privilege exec level 7 show running-config
!
line con 0
  exec-timeout 30 0
  history size 100
line vty 0 4
```

```
password 7 95978L842N5E43
exec-timeout 30 0
history size 100
transport input telnet ssh
line vty 5 15
password 7 85460A312B4D52
exec-timeout 30 0
history size 100
transport input telnet ssh

!
ntp clock-period 36029280
ntp clock-period 22518982
ntp server 10.16.76.124 prefer
ntp server 189.127.45.174
end
```