Teemu Metso

Verkon modernisointi

Opinnäytetyö

Tietotekniikka

Joulukuu 2016

KYAMK
University of Applied Sciences

Tekijä/Tekijät	Tutkinto	Aika
Teemu Metso	Insinööri AMK	Joulukuu 2016
Opinnäytetyön nimi		
Verkon modernisointi		31 sivua 18 liitesivua
Toimeksiantaja		
Kymenlaakson ammattikorkeakoulu		
Ohjaaja		
Tuntiopettaja Vesa Kankare		

Tiivistelmä

Tämän opinnäytetyön aiheena oli Kymenlaakson ammattikorkeakoulun ICT-Laboratorion verkon modernisointi. Modernisoinnilla pyrittiin varmistamaan, että verkon tiedonsiirtonopeus on riittävä vielä tulevaisuudessakin. Tärkeimpinä muutoksina modernisoinnissa oli verkon ydinkerroksen uudistus, Ciscon VSS:n implementointi sekä runkolinkkien päivittäminen valokuituun. Opinnäytetyön tavoitteena oli parantaa kokonaisvaltaisesti verkon vikasietoisuutta sekä tiedonsiirtonopeuksia.

Opinnäytetyön teoriaosuus pyrkii vertailemaan uuden ja vanhan verkkotopologian eroja ja selventämään mitä hyötyjä uudella verkkoratkaisulla saatiin. Itse työ eteni tutustumalla aluksi Ciscon VSS-tekniikkaan ja sen hyötyihin. VSS:n luomiseen käytettiin kahta Ciscon 4500-sarjan kytkintä jotka tulivat muodostamaan verkon ydinkerroksen. Kun VSS oli saatu luotua, päivitettiin runkoverkko valokuituun ja liitettiin VSS osaksi verkkoa. Vasta kun fyysinen verkkotopologia vastasi suunnitelmaa, verkon reititys siirrettiin VSS:iin ja siitä tehtiin verkon ydinkytkin. Sen lisäksi yhteen luokkatiloista päivitettiin uusi liityntätason kytkin josta saatiin malli, miten muutkin luokkatilat tulevaisuudessa päivitetään.

Opinnäytetyö saatiin tehtyä onnistuneesti ja se jäi käyttöön ICT-Laboratorion verkkoon. Työssä käyttöön otettu VSS nosti verkon vikasietoisuuden täysin uudelle tasolle verrattuna vanhaan topologiaan. Tulevaisuudessa verkkoon oli vielä tarkoitus lisätä toinen palomuuri, sekä päivittää muidenkin luokkatilojen liityntätason kytkimet.

Asiasanat

vss, cisco, verkko, optinen, ict-lab

Author (authors)	Degree	Time
Teemu Metso	Bachelor of Science	December 2016

Thesis Title

Network modernization

31 pages
18 pages of appendices

Commissioned by

Kymenlaakso University of Applied Sciences

Supervisor

Vesa Kankare, Lecturer

Abstract

The subject of this thesis was to modernizise Kymenlaakso University of Applied Sciences' ICT-laboratory network. The modernization aims to assure that the bandwidth in the network will remain adequate in the future. The most important changes in the modernization were reforming the network core-layer, implementing Cisco VSS and updating the network backbone to optical fiber. The objective of this thesis was to improve overall network redundancy and bandwidth.

The theoretical part of the thesis aims to compare the old and the new network topologies and to clarify the benefits that were achieved with the new network solution. The work itself began with familiarizing oneself with the Cisco VSS technology and what benefits it had. VSS was created by using two Cisco 4500-series switches that came to form the core-layer for the network. After the VSS had been created, the network backbone was updated to optical fiber and VSS was connected to the network. When the physical network topology corresponded to the plan, the routing was moved to the VSS and it became the core switch. In addition to this, one access layer switch was updated in one of the classrooms. This switch acted as example for how other rooms would be updated in the future.

The thesis was done successfully and it was introduced to ICT-Laboratory network. The VSS implementation brought redundancy in the network to a whole new level compared to the old topology. In the future the plan is to add another firewall to the network and also update the access layer switches in other class rooms.

Keywords

vss, cisco, network, optic, ict-lab

SISÄLLYS

KÄYTETYT LYHENTEET JA TERMIT

Cisco	Yksi maailman johtavista verkkolaitevalmistajista.
VSS	Virtual Switching System: Tekniikka jonka avulla kaksi kytkintä saadaan toimimaan yhtenä loogisena kokonaisuutena.
VSL	Virtual Switching Link: VSS:n vaatima yhteys kahden kytkimen välillä.
VLAN	Virtual Local Area Network: Virtuaalilähiverkko, tekniikan avulla voidaan jakaa fyysinen lähiverkko useisiin loogisiin.
MEC	MultiChassis EtherChannel: Kahdesta tai useammasta ethernet-yhteydestä tehty nippu, jossa yhteydet ovat jaettu kahteen eri laitteeseen.
ICT-Lab	ICT-laboratorio, Kyamkin tietotekniikan laboratoriotilat.
Cyberlab	ICT-lab:ssa sijaitseva harjoitusdatakeskus.
SFP	Small form-factor pluggable: Verkkolaitteissa käytetty muunnin. Pääsääntöisesti käytetään muuttamaan optinen signaali sähkömagneettiseksi.
Port channel	Fyysisistä porteista muodostettu nippu joka toimii yhtenä loogisena kokonaisuutena.
LACP	Link Aggregation Control Protocol: Universaali protokolla port channelille.
PAgP	Port Aggregation Protocol: Ciscon oma verkkoprotokolla port channelille.
MDF	Main Distribution Frame: Pääjakokeskus, joka koostuu eri mediatyyppien ristikytkennöistä.
BFD	Bidirectional Forwarding Detection: protokolla verkkolaitteiden tilan tarkkailuun.

HSRP	Hot Standby Router Protocol: Ciscon oma yhdyskäytäväosoitteen kahdennukseen tarkoitettu reititysprotokolla.
VRRP	Virtual Router Redundancy Protocol: yhdyskäytäväosoitteen kahdennukseen tarkoitettu reititysprotokolla.
SSO	Stateful Switchover: tilallinen kytkimen vaihto, jolla reaaliaikainen tila voidaan siirtää toiselle laitteelle.
DAC	Direct Attach Copper: lyhemmille matkoille tarkoitettu erittäin nopea kaksoisakselinen kuparikaapeli.

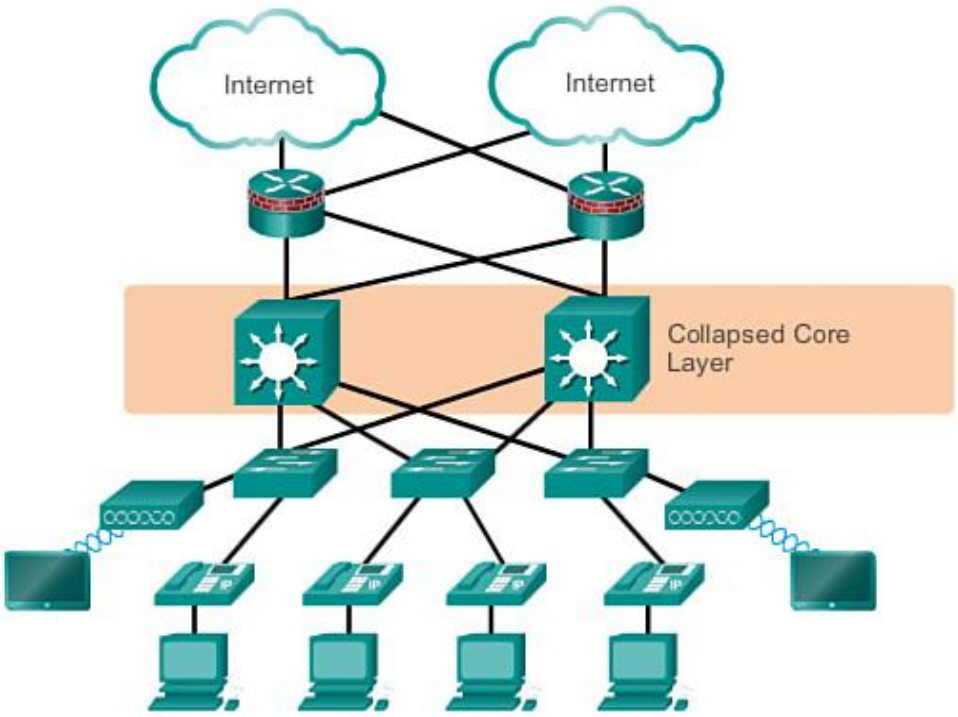
1 JOHDANTO

Opinnäytetyön tarkoituksena oli uudistaa Kymenlaakson ammattikorkeakoulun ICT-Lab:n tuotantoverkkoa. Tarve uudistukselle syntyi kasvavien luokkatilojen ja vähäisten verkon varayhteyksien myötä. Tärkeimpiä uudistuksia olivat Ciscon virtuaalikytkinjärjestelmän toteutus, joka paransi verkon luotettavuutta ja vikasietoisuutta, sekä valokuiturunkoyhteyksien käyttöönotto verkkolaitteiden välillä.

Työ suoritettiin harjoittelujakson aikana kesällä 2015, jolloin tiloissa oli vähiten häiriötekijöitä. Alustavan suunnitelman verkon uudistuksesta oli jo tehnyt tuntiopettaja Vesa Kankare, jonka suunnitelmaa työ seurasi. Pääpaino työssä olikin laitteiden konfigurointi ja itse asennus. Työssä perehdyttiin myös käyttöön otettuihin tekniikkoihin ja niiden hyötyihin.

2 ICT-LABORATORION VERKKO

ICT-Laboratorion verkko perustuu kaksikerroksiseen hierarkkiseen verkkomalliin, jossa ydin- ja jakelukerrokset ovat yhdistetty ja kerrosten toiminnot toteutetaan yhdellä laitteella (kuva 1). Tämä helpottaa pienemmän verkon hallittavuutta ja pienentää verkon ylläpidosta syntyviä kustannuksia, silti säilyttämällä suurimman osan normaalin, kolmekerroksisen verkkomallin hyödyistä. Laboratorioverkon tärkeimpiä käyttötarkoituksia ovat muun muassa riittävien yhteyksien luominen luokkatiloihin sekä tiedostojen ja ohjelmiston hallinta verkon yli, joilla pyritään takamaan parempi opiskelukokonaisuus tietotekniikan opiskelijoille. Verkon käytön kannalta suunnittelun kulmakivinä olivatkin siis käytettävyys, hallittavuus ja verkon varmuus. (Cisco Networking Academy 2014.)



Kuva 1. Kaksikerroksinen verkkomalli (Cisco Networking Academy 2014.)

Vuosien mittaan verkko on kasvanut ja elänyt, joten jonkin verran turhaksi jääneitä laitteita sekä ylimääräisiä komentoja löytyi kytkimistä ja muista verkkolaitteista. Vastaan tulleet vanhat komennot ja laitteet pyrittiin siivoamaan pois tai järjestelemään uudestaan uutta verkkosuunnitelmaa varten. Uudessa verkkosuunnitelmassa eri luokkatilat jaettiinkin uudestaan omiin VLAN:ihin, palvelimet omaan VLAN:iin, sekä verkkolaitteet omaan hallinta VLAN:iin.

2.1 Vanha verkkosuunnitelma

Vanha verkkosuunnitelma perustui kaksikerroksiseen verkkotopologiaan, jossa yksi L3-kytkin vastasi reitityksestä verkon reunalla. Kytkimenä toimi Ciscon yksi 3570-kytkin, johon oli kytketty niin ikään loput kytkimet sekä palvelimet. Runkolinkit eli yhteydet keskitetyn kytkimen ja liityntätason kytkinten välillä, joihin tietokoneet ja palvelimet olivat kytketty, toteutettiin Cat6-standardin mukaisella kuparikaapeloinnilla. Runkolinjat kytkettiin laitteiden välille EtherChannel tekniikkaa käyttäen, eli kytkemällä tässä tapauksessa kaksi fyysistä porttia yhdeksi loogiseksi kokonaisuudeksi, jolloin laitteiden välisistä yhteyksistä saatiin nopeampia ja luotettavampia.

Vanhassa suunnitelmassa laitteet olivat nimetty eri kalojen mukaan, joka perustui aikoinaan käytössä olleisiin VLAN:ihin. Kalan nimi voitiin yhdistää tiettyyn luokka-tilaan, jossa oli käytössä tietty VLAN. Esimerkiksi, Hauki-kytkin saattoi sijaita tilassa BK0131 jolloin luokan koneet kuuluivat Hauki-VLAN:iin.

2.2 Uusi verkkosuunnitelma

Uudessa verkkosuunnitelmassa pysyttiin samassa kaksikerroksisessa verkkotopologiassa, mutta ydinkerros uudistettiin täysin. Aikaisemmin reitityksestä huolehtinut Ciscon 3570-kytkin korvattiin kahdella Ciscon 4500-X-kytkimellä joissa otettiin käyttöön VSS. Aikaisemmin yhdellä kytkimellä tapahtunut reititys saatiin jaettua näin kahdelle kytkimellä, joka teki verkosta vikasietoisemman. Ciscon 4500-X-kytkimissä ei itsessään ole enää perinteisiä ethernet-portteja vaan ne ovat oletuksena SFP+-portteja. Tämä ominaisuus pakotti myös vaihtamaan palomuurin samalla uudempaan Ciscon ASA5515-X-mallin palomuuriin. Tulevaisuudessa myös palomuuri on tarkoitus kahdentaa, jolloin runkoverkosta häviää viimeinenkin yksittäinen vikaantumispiste. Myös liityntätason kytkimiä päivitettiin uudempiin osassa luokkatiloista. Uutena liityntätason kytkimenä toimi Ciscon 2960-X, joita työssä asennettiin vain yksi. Muutkin kytkimet olivat tarkoitus päivittää, mutta aikataulullisista syistä ne asennettiin vasta syksyllä.

Tarve uudelle verkkosuunnitelma syntyi jatkuvasti kasvaneen tiedonsiirtotarpeen sekä tulevaisuuden suunnitelmien pakotteesta. Virtualisoinnin ja luokkakokojen kasvaessa vanha verkko olisi jäänyt auttamatta liian pieneksi, sekä lukuisten yksittäisten vikaantumispisteiden takia liian epäluotettavaksi. Aikaisempi, jokseenkin sekava nimeämiskäytäntö myös vaihdettiin toiseen, huomattavasti helpommin luettavaan. Uudessa suunnitelmassa verkkolaitteiden nimeäminen perustui fyysiseen sijaintiin ja laitteen tyyppiin, esimerkiksi BK0139-R1. Samassa tilassa olleet laitteet eroteltiin juoksevalla numeroinnilla. Tällä tavoin vähemmälläkin verkon tuntemuksella saadaan heti selville missä laite sijaitsee.

Uusia laitteita otettiin käyttöön tiloissa BK125, BK0026, BK0131 ja BK0139. BK0139 on ICT-laboratorion uusi konesali Cyberlab, johon sijoitettiin uusi palomuuri sekä verkon ydinkerros. Aikaisemmin konesalina toiminut BK125

muutettiin ristikytkentäkeskukseksi. Vaikka kaikkia laitteita ei vielä päivitetty, niiden nimet vaihdettiin kuitenkin uusiin. Laitteet nimettiin seuraavasti:

- BK0139-R1
- BK0131-S1
- BK0131-S2
- BK0125-S1
- BK0125-S2
- BK0125-S3
- BK0026-S1
- BK0139-FW1.

Uudesta nimestä näkee saman tien mistä laitteesta on kyse ja missä se sijaitsee. Samalla myös laitteiden hallinta IP-osoitteet vaihdettiin. Uusi hallintaverkon osoiteavaruus oli 10.69.2.xx/24.

3 KÄYTETYT LAITTEET JA TEKNIIKAT

3.1 Virtual Switching System

Ciscon kehittämä tekniikka Virtual Switching System, VSS mahdollistaa kahden kytkimen liittämisen toisiinsa niin, että ne toimivat yhtenä loogisena kokonaisuutena. Virtual Switching Systemiin voidaan liittää kaksi Catalyst 4500-X-kytkintä tai kaksi Catalyst 4500-sarjan kytkintä, joissa on Supervisor Engine 7-E tai Supervisor Engine 7-LE. Kytkinten pitää olla identtiset, jotta VSS saadaan toimimaan. Molemmat yhteen liitetyistä kytkimistä pysyvät aktiivisena ja ohjaavat liikennettä, mutta jakavat yhteisen hallintarajapinnan, joka on aktiivisena vain yhdessä laitteessa kerrallaan. Toinen kytkin on siis aktiivitilassa, jolla kytkimiä hallitaan ja toinen kytkin valmiustilassa (kuva 2). Tällöin mahdollisissa vika- ja päivitystilanteissa hallintarajapinta voidaan siirtää välittömästi valmiustilassa olevalle kytkimelle. (Cisco 2014.)

Jotta VSS saadaan toimimaan kahden kytkimen välillä, pitää kytkinten välille luoda Virtual Switching Link, jonka kautta laitteet kommunikoivat ja ohjaavat liikennettä. VSL on toteutettu EtherChannelin avulla ja se tukee maksimissaan kahdeksaa linkkiä. VSL jakaa myös oletuksena kuormaa VSS-kytkinten välillä.

```
BK0139-R1#sh switch virtual role

Executing the command on VSS member switch role = VSS Active, id = 1

RRP information for Instance 1

-------------------------------------------------------------------
Valid  Flags   Peer      Preferred  Reserved
               Count     Peer       Peer

-------------------------------------------------------------------
TRUE    V        1           1          1

Switch  Switch Status  Preempt       Priority  Role     Local   Remote
        Number         Oper(Conf)    Oper(Conf)         SID     SID
-------------------------------------------------------------------
LOCAL   1      UP      FALSE(N )     200(200)  ACTIVE   0       0
REMOTE  2      UP      FALSE(N )     100(100)  STANDBY  1969    9490

Peer 0 represents the local switch

Flags : V - Valid
In dual-active recovery mode: No
```

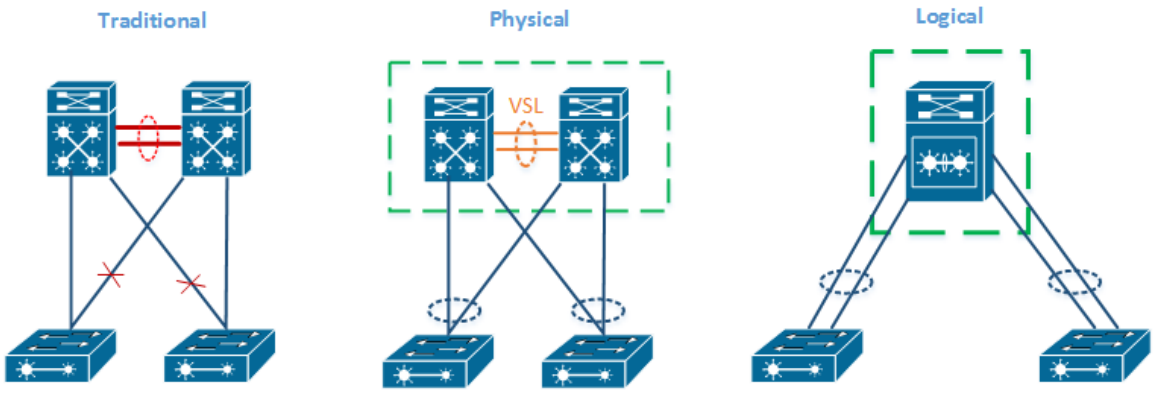
Kuva 2. Aktiivisen laitteen roolin tarkistus VSS:ssä

Perinteinen verkkoratkaisu, jossa liityntätason kytkin kytkettäisiin kahteen eri ydintason kytkimeen, saisi aikaan silmukan, joka pahimmassa tapauksessa voisi kaataa koko verkon. Silmukan muodostuminen voidaan estää spanning tree -protokollan avulla. STP sulkee toisen porteista, jolloin liityntätason kytkimeltä on vain yhteys yhteen ydintason kytkimeen. Jos yhteys liityntätason ja ydinkerroksen välillä jostakin syystä katkeaa, STP määrittää uudestaan mistä portista saadaan yhteys ydinkerrokseen. Näin verkosta saadaan vikasietoisempi, kun laitteilla on olemassa varareitti.

VSS:ssä STP:aa ei tarvita, jos verkkolaitteet kytketään EtherChannelin avulla molempiin VSS:n kytkimiin. Tästä käytetään nimitystä MEC eli Multichassis EtherChannel. MEC toteutetaan samalla tavalla kuin normaali EtherChannel, ainoana erona, että se on kytketty molempiin fyysisiin laitteisiin VSS:n päässä. Koska VSS toimii yhtenä loogisena kokonaisuutena, MEC näkyy ulospäin aivan tavallisena EtherChannelina (kuva 3).

Opinnäytetyössä käytettiin Virtual Switching Systemin luomiseen kahta Ciscon 4500-X-kytkintä. Tekniikan avulla verkosta saatiin luotettavampi, kytkemällä verkkolaitteet kahdennettuna 4500-X-kytkimiin. Tällöin, vaikka toinen VSS

kytkin olisikin poissa käytöstä, data kulkee silti toisen kytkimen kautta. (Cisco 2014.)



Kuva 3. Vertailu perinteisen ja Virtual Switching Systemin välillä (Cisco 2009.)

3.2 Dual-active recovery

Mahdolliset vikatilanteet, jossa jostain syystä VSL laitteiden välillä katkeaa aiheuttaa aktiivisen laitteen tilanvaihdon. Ilman tilanvaihtoa, VSL:n katketessa molemmat VSS-kytkimet toimisivat aktiivisina laitteina, mikä aiheuttaisi lukuisia kriittisiä ongelmia verkkoon, koska tällöin molemmilla laitteilla olisi samat IP-osoitteet, SSH avaimet sekä sama STP bridge ID. Tämä on estetty dual-active recovery ominaisuuden avulla, joka estää kahden aktiivisen laitteen samanaikaisen olemassa olon verkossa. Jotta VSS tunnistaa milloin kyseessä on dual-active-skenaario eli milloin molemmat kytkimet ovat aktiivisia, sen pitää pystyä tarkastaa molempien laitteiden tila. Tähän on olemassa kolme vaihtoehtoa; enhanced PAgP, IP BFD tai dual-active fast hello. Valitettavasti 4500-X-kytkimillä käytössä ovat vain enhanced PAgP ja dual-active fast hello (kuva 4).

3.2.1 Enhanced PAgP

Enhanced PAgP käyttää kommunikointiin jo olemassa olevaa MEC-linkkiä, joka kulkee naapurikytkimen kautta toiselle VSS-kytkimelle. Tässä on hyötynä se, että voidaan käyttää jo olemassa olevaa linkkiä, eikä näin ollen tarvitse käyttää yhtä porttia molemmista laitteista pelkkään tilan tarkkailuun. Tosin täl-

löin pitää luottaa, että naapurireititin on käynnissä eikä yhteys sen ja kummankaan VSS-kytkimen välillä katkea. Ainoa vaatimus menetelmässä on, että naapurikytkin tukee myös enhanced PAgP:a. (Cisco 2013.)

3.2.2 IP BFD

IP BFD eli Bidirectional Forwarding Detection on protokolla, joka on kehitetty nimenomaan häiriöiden havaitsemiseen. Se tarjoaa kevyen ja nopean menetelmän vikojen havaitsemiseen kahden rinnakkaisen reitittimen välillä. Cisco tukee asynkronista BFD:ia, joka toimiakseen vaatii lähettämään BFD hallintapaketteja kahden eri laitteen välillä aktivoidakseen ja ylläpitääkseen BFD naapuruutta. BFD pitää siis konfiguroida molempiin laitteisiin portti- ja reititystasolla, jolloin BFD sessio käynnistyy ja laitteet määrittelevät, kuinka usein paketteja lähetetään naapurille. BFD poistaa tarpeen käyttää naapurireititintä dual-active-skenaarion havaitsemiseen. (Cisco 2006.)

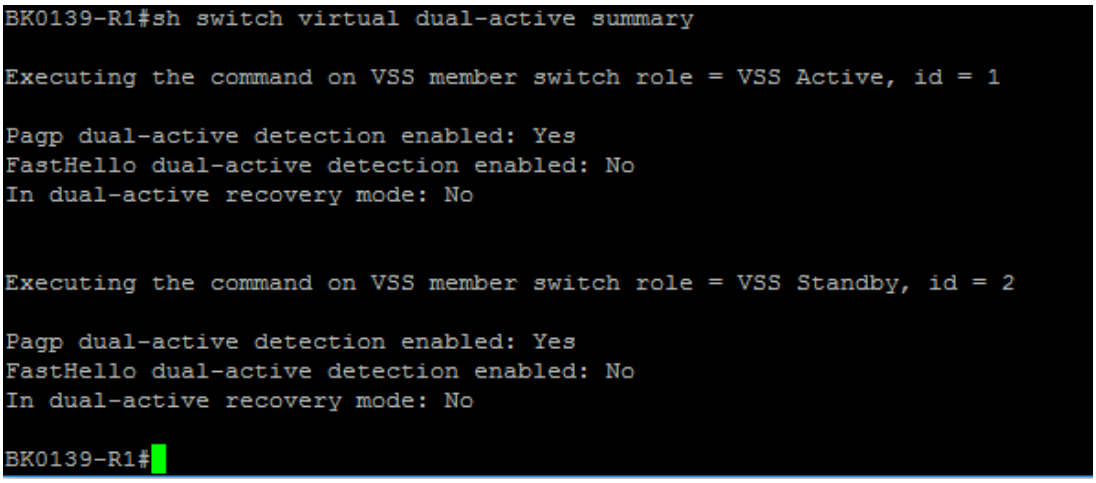
Jotta BFD toimii VSS-ympäristössä, pitää laitteiden välille varata minimissään yksi suoraan laitteiden välillä kytketty ethernet-linkki. Koska molemmilla fyysisillä laitteilla on saman IP, ne turvautuvat linkissä BFD protokollaan. Jos VSL-linkki katkeaa, molemmat kytkimet siirtyvät aktiivitilaan ja luovat omat BFD-naapurit ja yrittävät muodostaa naapuruuden toisen kytkimen kanssa. Kun yhteys muodostuu ja alkuperäinen aktiivisena toiminut kytkin saa tiedon, että naapuruus on muodostettu, se aloittaa dual-active recovery -tilan mukaiset palautumistoimenpiteet. (Cisco 2013.)

3.2.3 Dual-active fast hello

Dual-active fast hello vaatii laitteiden välille oman, vain fast hello -paketeille tarkoitetun ethernet-linkin. Menetelmässä voidaan käyttää maksimissaan neljää linkkiä fast hello -pakettien välitykseen. Jos laitteissa on enemmän kuin yksi SFP-porttimoduuli, voidaan kytkeä useita linkkejä eri moduulien välille, jolloin pelkkä moduulin vikaantuminen ei aiheuta dual-active-skenaariota.

3.2.4 Palautuminen

Kun aktiivinen laite huomaa dual-active-skenaarion se pudottaa itsensä pois verkosta, sulkemalla kaikki portit lukuun ottamatta VSL-portteja. Kytkin pysyy alhaalla kunnes VSL on palautunut laitteiden välillä ja se pystyy määrittämään roolin itselleen. VSL:n noustessa takaisin ylös, aktiivinen laite käynnistyy uudestaan valmiustilassa. On myös tärkeää huomioida, että dual-active recovery tilan aikana uusien loopback-osoitteiden luominen ei ole suotavaa, koska ne ovat automaattisesti käytössä, vaikka niiden on tarkoitus olla recovery-tilassa alhaalla.



Kuva 4. Dual-active-tiivistelmä

3.3 VSS ja eri tekniikoiden vertailu

Yksi yleinen tapa parantaa verkon vikasietoisuutta on käyttää jotakin First hop redundancy -protokollaa, joita ovat esimerkiksi HSRP eli Hot Standby Router Protocol tai Virtual Routing Redundancy Protocol eli VRRP. Molemmat protokollat kahdentavat verkon yhdyskäytäväosoitteen virtuaalisesti ja pystyvät vaihtamaan reitittävää laitetta ilman, että siitä seuraisi huomattavaa katkoa verkkoon. Koska HSRP ja VRRP toimivat samalla periaatteella, työssä verrataan vain HSRP:aa VSS:iin. Sen lisäksi verrataan myös Ciscon StackWise-tekniikkaa, joka sopi paremmin liityntätason kahdentamiseen.

3.3.1 HSRP

HSRP on Ciscon kehittämä virtuaalireititysprotokolla, joka toimii jokseenkin samalla periaatteella kuin VSS. HSRP luodaan kahden Ciscon kytkimen välille jolloin niistä muodostuu yksi looginen virtuaalireititin. Samoin kuin VSS, myös HSRP määrittää aktiivisen ja valmiustilan roolit, mutta ainoastaan reititykseen. Aktiivinen reititin määrittää muille verkkolaitteille, mitä kautta liikenne kulkee ja valmiustilassa oleva reititin nimensä mukaisesti on vain varalla, jos aktiivinen reititin lakkaa toimimasta. Laitteet toimivat muuten täysin itsenäisesti eikä niillä ole yhteistä hallintarajapintaa. HSRP ei myöskään jaa oletuksena kuormaa, vaan kuromanjako vaatii multigroup-konfiguraation. Ilman tätä kaikki liikenne kulkee aina aktiivisen reitittimen läpi, eli toisin kuin VSS, jossa liikenne kulkee molempien laitteiden kautta.

3.3.2 StackWise

StackWise on Ciscon kehittämä teknologia, jolla voidaan liittää useita kytkimiä toisiinsa niin, että ne toimivat yhtenä loogisena kokonaisuutena. Se tarjoaa paljon samoja ominaisuuksia kun VSS, kuten yhteisen hallintarajapinnan, konfiguraation ja reititystiedot. StackWise toimii Ciscon 3750-sarjan kytkimissä ja se tukee maksimissaan yhdeksää kytkintä. Toisiinsa kytkimet liitetään siihen tarkoitetuilla kaapeleilla, niin että kytkinten välille syntyy silmukka. Tämä tarjoaa kaksisuuntaisen 32 gigabitin yhteyden jokaisen laitteen välille. Jos linkki jostain syystä katkeaa, StackWise osaa puolittaa nopeuden, mutta yhteys laitteiden välillä silti säilyy. Laitteiden hallinta tapahtuu aina yhden kytkimen kautta, joka on äänestetty master-kytkimeksi. Kun kytkimiä lisätään tai poistetaan StackWisesta, master-kytkin päivittää konfiguraation automaattisesti, eikä näin vaikuta suorituskykyyn. (Cisco 2003.)

Tekniikasta on tullut myös kehittyneempiä versiota, kuten uusimpana StackWise 480, joka perustuu samaan tekniikkaan, mutta on huomattavasti nopeampi. Suurimpana erona StackWisen ja VSS:n välillä onkin lähinnä niiden käytettävyys. Siinä missä StackWise tarvitsee spesifin kaapelin, joka rajoittaa sen käytön käytännössä yhteen fyysiseen tilaan, mediasta riippumattomassa VSS:ssä ei ole rajoituksia kuinka kaukana laitteet toisistaan ovat. Sen lisäksi 3750- ja 3850-sarjan kytkimet, joissa StackWise voidaan ottaa käyttöön, ovat

pitkälti tarkoitettu liityntätasonkytkimiksi, kun taas VSS on tarkoitettu enemmän ydinkerrokseen.

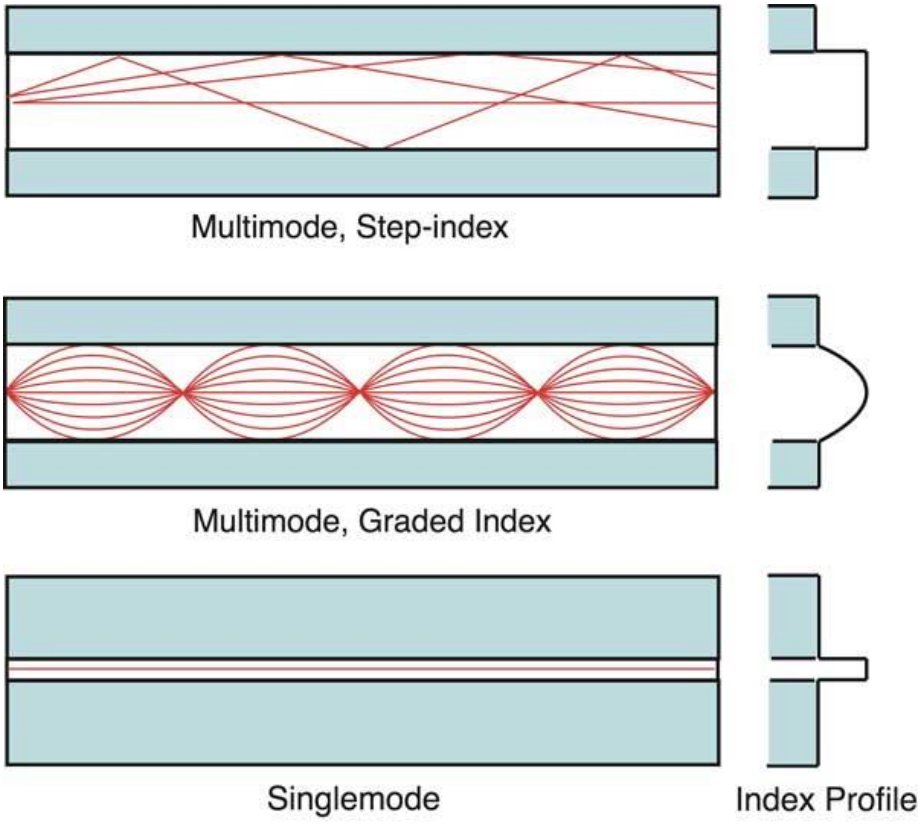
3.4 Optiset runkoyhteydet

Runkoyhteydet työssä toteutettiin valokuidun avulla. Optisessa kuidussa tiedonsiirto tapahtuu lähettämällä optisia signaaleja, joko LED-valolähteellä tai laserilla erittäin ohuesta lasista tai muovista valmistettua kuitua pitkin. Tätä kuitua kutsutaan ytimeksi. Ytimen ympärillä on vaippa, jonka tarkoitus on heijastaa valoa ytimessä, jotta vältytään valovuodolta ja vääristyneiltä signaaleilta. Uloimpana kerroksena on kuori, joka suojelee kuitua ulkoisilta häiriöiltä kuten murtumiselta ja kosteudelta.

Tiedonsiirrossa on käytössä kahdenlaista valokuitua, yksimuotokuitua ja monimuotokuitua (kuva 5). Yksimuotokuidussa kuidun halkaisija on erittäin pieni, noin 9 mikronia. Tällöin kuidussa kulkee vain yksi muoto suoraan kuidun päästä päähän.

Monimuotokuidussa kulkee useita muotoja, joita saadaan taitettua kuidun sisällä sen suuremman halkaisijan takia. Monimuotokuidun halkaisija on suurempi kuin yksimuotokuidussa, yleensä 50 tai 62,5 mikronia. (The Fiber Optic Association 2016.)

Optisessa kuidussa on huomattavasti pienempi vaimennus ja suurempi kaistanleveys kuin tavallisessa sähköisessä tiedonsiirrossa, joten sen hyödyt tulevat esille varsinkin tilanteissa, missä etäisyydet ovat pitkiä tai vaaditaan suuria tiedonsiirtonopeuksia. Kuitu ei myöskään kärsi sähköisen tiedonsiirron ongelmista, kuten sähkömagneettisista häiriöistä, ylijännitepiikeistä tai maadoitusongelmista.(TTK 1998.)



Kuva 5. Kuitutyypit (TTK 1998.)

3.5 Laitteet

Verkkoa suunnitellessa sopivien laitteiden valinta oli tärkeää. Vaikka verkko ei fyysisesti kovin iso ollutkaan, opetus- ja laboratoriokäytössä suuria tiedonsiirtonopeuksia kuitenkin tarvittiin. Tärkeää oli, että kaikki laitteet tukivat 10 gigabitin SFP+-moduuleja, jotta runkolinkeistä saatiin riittävän nopeita, eivätkä ne näin ollen muodostaneet pullonkaulaa verkkoon.

3.5.1 Cisco Catalyst 4500-X

Ciscon Catalyst sarjan 4500-X-kytkin oli ominaisuuksiltaan erinomainen valinta laboratorioverkkoon sen skaalautuvuuden ja virtualisointiominaisuuksien takia. Kytkimen tärkeimpiä ominaisuuksia ovatkin skaalautuvuus, korkea saatavuus, sovellusmonitorointi, turvallisuus ja yksinkertaistettu hallinta.

Koska kytkin on tarkoitettu runkoverkon laitteeksi, siinä ei nykypäivän mittapuun takia ollut perinteisiä RJ-45 ethernet -portteja ollenkaan, vaan kytkimessä oli 16 SFP+-porttia jotka tukevat 10 gigabitin tai yhden gigabitin SFP-

moduuleja. Kytkin osaa itse määrittää kumpi SFP on käytössä, jolloin erillistä konfiguraatiota ei tarvita. Porttimäärää saatiin tarpeen tullen vielä kasvatettua kahdeksalla erillisen moduulin avulla. Käytännössä tämä porttimäärä saatiin vielä tuplattua, kun yhdistettiin kaksi kytkintä VSS:n avulla toisiinsa.

VSS-tuki kytkimessä mahdollistaa yksinkertaisemman verkkoratkaisun vähentäen laitetarvetta ja kuluja. Suuren tiedonsiirtokapasiteetin ja virtualisointimahdollisuuksien lisäksi kytkin sopii verkon ydinlaitteeksi myös rautapuolensa ansiosta, sillä kaikki tuulettimet ja kahdennetut virtalähteet voidaan vaihtaa kytkimen ollessa päällä. (Cisco 2016.)

3.5.2 Cisco Catalyst 2960-X

Catalyst 2960-X on L3-tason kytkin, joka soveltuu toimintojensa puolesta erinomaisesti esimerkiksi toimistoihin tai luokkatiloihin, missä on käytössä paljon koneita ja tiedonsiirtotarve on suuri. 2960-X-kytkintä saa joko 24-porttisena tai 48-porttisena. Ethernet-porttien lisäksi kytkimessä on kaksi SFP+-moduuli paikkaa, jossa voidaan käyttää joko 10 gigabitin tai yhden gigabitin SFP-moduuleja. (Cisco 2016.)

Käyttöön valitut 48-porttiset kytkimet sopivat työhön hyvin, jolloin portit riittivät koneille sekä tarvittaviin ristikytkentöihin. Runkolinkit toteutettiin SFP+-porttien kautta, 10 gigabitin SFP-moduuleilla. Kytkimet kytkettiin kahdennettuna ydinkerroksen VSS-kytkimiin, jolla siitä saatiin redundanttinen.

3.5.3 Cisco ASA-5515-X

5515-X on yksi alan käytetyimmistä tilallisista palomuureista. Palomuuri tarjoaa useita turvallisuusominaisuuksia sekä redundanttisen virtalähteen, jolla pyritään takamaan palveluiden jatkuva saatavuus. Palomuurin suoritusteho ideaalitilanteessa on 1,2Gb/s. mutta todellinen luku on noin puolet tästä eli noin 600Mb/s. (Cisco 2016.)

Palomuuri soveltui hyvin laboratorioverkkoon, koska se on fyysisesti pieni eikä vie turhaa tilaa, jolloin vähäinen tila saatiin paremmin käyttöön. Sen lisäksi palomuuri tarjoaa riittävästi tiedonsiirtonopeutta suhteellisen vaatimattomaan käyttöön, eikä näin ollen ollut turhaan ylimitoitettu.

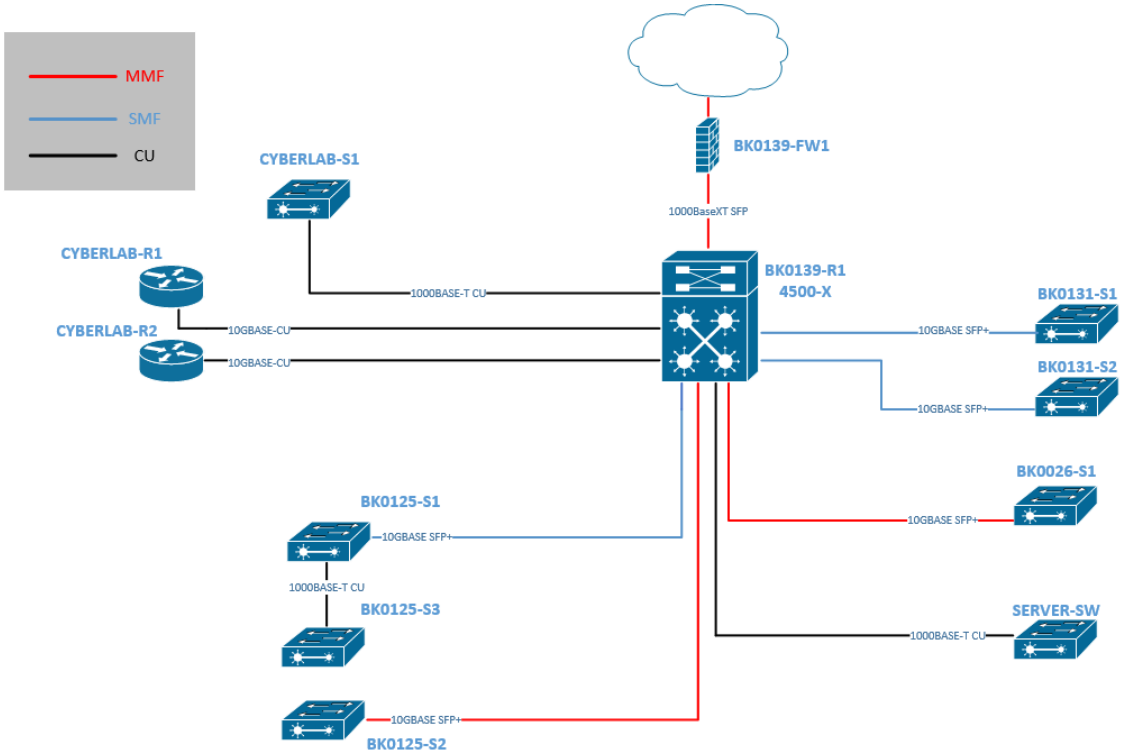
4 TYÖN TOTEUTUS

Opinnäytetyö toteutettiin Kymenlaakson ammattikorkeakoulun ICT-laboratorion tiloissa, harjoittelujakson aikana kesällä 2015. Kokonaisuudessaan työhön kuului uusien verkkolaitteiden implementointi ja konfigurointi, sekä runkoverkon kaapelointi. Tarkoituksena työssä oli uusia koko verkko, mutta ajankohdan ja resurssien takia vai yhteen luokkatilaan asennettiin 2960-X-sarjan kytkin. Tästäkin sai jo hyvän kuvan implementoinnin toteutuksesta, kun muutkin 2960-X-sarjan kytkimet asennettaan samalla tavalla.

Työ eteni ensin tutustumalla VSS:iin sekä sen rakentamiseen ja sen jälkeen runkoverkon kaapeloinnilla, missä vanhat kuparikaapeloinnit korvattiin optisella kuidulla. Optiset kuidut tuotiin jokaisen luokkatilan liityntäkytkimelle ja kytkettiin joko yksi- tai monimuotokuidulla kuitupaneelista kytkimeen. Kuidulle tehtiin oma ristikytkentäkeskus tilaan BK0125, josta kuidut oli mahdollista kytkeä haluttuun tilaan. Kun runkoverkko oli saatu tehtyä ja VSS todettu toimivaksi, se kytkettiin osaksi verkkoa. Aluksi liityntätason kytkimet kytkettiin VSS:iin kiinni, mutta vanha ydinkytkin hoiti silti reitityksen. Vasta kun kaikki kytkimet oli fyysisesti kytketty VSS:iin, reititys siirrettiin vanhalta verkon ydinkytkimeltä VSS kytkimille. Lopuksi kytkettiin vielä palvelinverkko sekä uusi palomuuri uusiin ydinkytkimiin (kuva 6).

Suurin syy verkon uudistamiselle johtui jo aikaa nähneiden laitteiden uudistamistarpeesta ja alati kasvavasta tiedonsiirtokapasiteetin tarpeesta, joihin vanhan verkon tiedonsiirtonopeudet eivät olisi riittäneet. Vanha verkkoratkaisu ei myöskään ollut juurikaan vikasietoinen, joten tähänkin tartuttiin ja pyrittiin pääsemään mahdollisimman monesta yksittäisestä vikaantumispisteestä eroon. Ydinkerroksen kytkin kahdennettiin VSS:n avulla ja siihen kytketyt liityntätasonkytkimet kytkettiin kiinni MEC:in avulla, jolloin vaikka toinen ydinkerroksen kytkimistä vikaantuisi, yhteys toimisi vielä toisen kytkimen kautta.

Työn loppuvaiheessa kaikkiin kytkimiin lisättiin myös RADIUS-todennus, jonka avulla voitiin määrittää käyttöoikeudet vain halutuille käyttäjille. Näin saatiin parannettua tietoturvaa ja verkonhallintaa, kun paikallista pääkäyttäjän salasanaa ei tarvitse jakaa kaikille, vaan oikeutetut käyttäjät voivat kirjautua verkkolaitteisiin omilla ICT-Labin tunnuksilla. Tällöin myös lokitietoihin tallentuu selkeästi, kuka laitteilla on tehnyt mitäkin muutoksia.



Kuva 6. Päivitetty verkkoratkaisu.

4.1 VSS-käyttöönotto

VSS vaatii toimiakseen kaksi identtistä Ciscon 4500-X- tai 6500-sarjan kytkintä. ICT-laboratorion verkkoon valittiin 4500-X-sarjan kytkimet niiden soveltuen vastaamaan paremmin pienemmän verkon tarpeita. VSS on käytännössä yksi looginen kokonaisuus, jossa on vain yksi yhteinen hallintarajapinta, jota voidaan konfiguroida aktiivisena olevan laitteen kautta. Häiriötilanteissa hallintarajapinta siirtyy passiivisena olevalle kytkimelle ilman verkkokatkoja. Jotta tämä olisi mahdollista, luodaan kahden kytkimen välille VSL, jonka kautta laitteet välittävät tietoa keskenään.

Kun VSS:iä aloitetaan konfiguroimaan, pitää aluksi tarkastaa, että laitteissa on sama ohjelmistoversio käytössä. Jos näin ei ole, laitteet pitää ensin päivittää

samaan versioon, jotta VSS saadaan toimimaan. Kun molemmissa kytkimissä on sama versio, niihin pitää määrittää sama virtual domain -numero väliltä 1 ja 255. Tämän jälkeen määritellään kytkimille numero, jolla ne erotetaan toisistaan domainin sisällä eli toinen kytkimistä saa numeron yksi ja toinen numeron kaksi. Kytkimille voidaan määrittää myös prioriteetti, jolloin VSS pyrkii käyttämään suuremman prioriteetin kytkintä aina aktiivisena. Kytkimen prioriteetti määritetään seuraavasti.

sw virtual domain 1
switch 1
switch 1 priority 200
switch 2 priority 100
exit
!

Samat komennot suoritettaan myös toisessa kytkimessä.

sw virtual domain 1
switch 2
switch 2 priority 100
switch 1 priority 200
exit
!

Tämän jälkeen kytkimiin konfiguroidaan VSL. Molempiin kytkimiin luodaan port channel, jonka numerointi pitää olla eri kuin toisessa kytkimessä, koska yhdistymisvaiheessa VSS konfiguroi molemmat port channelit VSL:n käyttöön. Molemmissa kytkimissä luotuihin port channeleihin liitetään VSL, joka numeroidaan kytkimen numeron mukaan. Tämä saadaan toteutettua alla olevilla komennoilla.

int port-channel 1
switchport
sw virtual link 1
no shut
exit

Samat komennot suoritetaan taas toisessa kytkimessä, erona ainoastaan numerointi.

int port-channel 2
switchport

switch virtual link 2
no shut
exit

Seuraavaksi liitetään halutut portit VSL:n port channeliin alla olevilla komennoilla. Kun portit ovat liitetty port channeliin ja kytketty fyysisesti toisiinsa, ne pysyvät alhaalla eivätkä nouse ylös ennen kuin molemmat kytkimet ovat käynnistyneet uudelleen virtuaalitilassa.

int range ten1/1-2
sw mode trunk
channel-group 1 mode on
exit
!
switch convert mode virtual

Jälleen samat komennot myös toisessa kytkimessä.

int range ten1/1-2
sw mode trunk
channel-group 2 mode on
exit
!
switch convert mode virtual

Kun komento *switch convert mode virtual* on suoritettu, kytkin varmistaa vielä, että halutaanko varmasti suorittaa komento. Tähän pitää vastata kyllä. Tämän jälkeen kytkimet käynnistyvät uudelleen virtuaalitilassa ja luovat VSS:n. Koska kytkimiä hallitaan tämän jälkeen vain yhden laitteen kautta, eri laitteiden fyysiset portit erotellaan toisistaan portin ensimmäisen numeron mukaan. Esimerkiksi interface ten1/1/1 olisi kytkimen 1 ensimmäinen portti ja interface ten2/1/1 olisi taas kytkimen 2 ensimmäinen portti.

Vikatilanteiden varalle kytkimissä on käytössä tilallinen kytkimenvaihto, joka minimoi katkoksen ajan siirtämällä tilatiedot, reititystaulun ja käytössä olevan konfiguraation valmiustilassa olevalle kytkimelle. Kun VSS on muodostettu, voidaan redundanttisuus todeta toimivaksi komennolla *show switch virtual redundancy* (kuva 7). Jos käytössä ei ole stateful switchover, se voidaan vaihtaa komennoilla:

conf t
redundancy

mode sso

exit

```
BK0139-R1#sh switch virtual redundancy

Executing the command on VSS member switch role = VSS Active, id = 1


                My Switch Id = 1
              Peer Switch Id = 2
       Last switchover reason = none
    Configured Redundancy Mode = Stateful Switchover
     Operating Redundancy Mode = Stateful Switchover

Switch 1 Slot 1 Processor Information :
-----------------------------------------------
        Current Software state = ACTIVE
                Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch  So
ftware (cat4500e-UNIVERSALK9-M), Version 15.2(3)E1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Tue 28-Apr-15 12:27 by prod_rel_team
                        BOOT =
        Configuration register = 0x2101
                Fabric State = ACTIVE
          Control Plane State = ACTIVE

Switch 2 Slot 1 Processor Information :
-----------------------------------------------
        Current Software state = STANDBY HOT (switchover target)
                Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch  So
ftware (cat4500e-UNIVERSALK9-M), Version 15.2(3)E1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Tue 28-Apr-15 12:27 by pr
                        BOOT =
        Configuration register = 0x2101
                Fabric State = ACTIVE
          Control Plane State = STANDBY


Executing the command on VSS member switch role = VSS Standby, id = 2
```

Kuva 7. Redundanttisuuden tarkastus *show switch virtual redundancy* komennolla

4.2 Dual-active detection

Jotta VSL:n vikaantuminen ei aiheuttaisi dual-active-skenaariota, pitää käyttöönottaa dual-active detection. Tähän valittiin käytettäväksi enhanced PAgP, joka toimi VSS:n ja BK0026-S1:n välillä. BK0026-S1-kytkintä voitiin helposti hyödyntää tähän, koska se oli tässä kohtaa työtä ainut uusi Catalyst 2960-X-sarjan kytkin, joka kytkettiin MEC:nä VSS:n 10 gigabitin yhteydellä.

Ennen kuin dual-active detection voidaan ottaa käyttöön, luodaan VSS:n ja liityntätason kytkimen välille PAgP:aa käyttävä port channel. PAgP port channel saadaan luotua komennoilla

conf t
int port-channel 10
switchport
switchport mode trunk

Seuraavaksi liitetään fyysiset portit port channeliin. Koska tarkoitus on tehdä MEC, konfiguroidaan yksi portti molemmista fyysisistä VSS:n kytkimistä port channeliin.

conf t
int te1/1/5
switchport mode trunk
channel-group 10 mode desirable
exit
!
int te2/1/5
switchport mode trunk
channel-group 10 mode desirable
exit

Port channel saadaan luotua liityntätason kytkimeen samoilla komennoilla lukuun ottamatta portteja. 2960-sarjan kytkimissä on runkolinkkiä varten kaksi SFP-moduuli paikkaa, jotka ovat numerojärjestyksessä aina kytkimen viimeiset portit. Liityntätasonkytkimessä ei myöskään tarvitse huomioida sitä, että se kytketään kahteen fyysiseen laitteeseen, vaan port channel näkyy ja toimii aivan normaalisti.

Kun port channel kytkinten välille on luotu, voidaan määrittää VSS:iin dual-active detection. Tämä tapahtuu määrittämällä käytössä olevaan virtual domainiin, mitä tekniikkaa käytetään. Huomioitavaa on myös, että PAgP:ia tukeva port channel täytyy ensin sulkea ja vasta sitten määrittää se VSS:iin. PAgP dual-active detection saadaan konfiguroitua komennoilla:

interface port-channel 10
shutdown
exit
!
switch virtual domain 1

dual-active detection pagp trust channel-group 10
exit
!
int port-channel 10
no shutdown
!

Dual-active detection voidaan todeta toimivaksi kahdella komennolla, joko komennolla *show switch virtual dual-active pagp* tai komennolla *show pagp dual-active*. (NetCraftsmen 2010.)

4.3 Runkolinkit

Uudet runkolinkit toteutettiin optisella kuidulla. Kuitu tilattiin määrämittaisena ja valmiiksi päätettynä, jolloin kuituhäntiä ei tarvinnut itse hitsata. Kuidut olivat yhdistelmäkuitua eli jokaisessa kaapelissa oli 24 paria, joista puolet olivat yksimuotokuitua ja puolet monimuotokuitua. Koska ICT-Labin luokkatilat kuuluvat samaan palotilaan, kuitujen vetäminen MDF:n ja luokkatilojen välillä hoitui helposti, sillä läpivientejä ei ollut massattu umpeen. Jokaiseen luokkatilaan vietiin aina yksi kuitukaapeli, joka kytkettiin tilan laitekaapissa sijanneeseen kuitupaneeliin. Kuitupaneelista otettiin vain kaksi paria per kytkin käyttöön, joten paneeliin jäi myös reilusti kasvuvaraa. Kuitujen toiset päät kytkettiin BK0125-tilassa sijaitsevaan ristikytkentäkaappiin, josta tehtiin pääjakamo.

Vanhan kuparikaapeloinnin päivitys kuituun toi lisää varmuutta verkon toimivuuteen, koska valokuitu ei kärsi sähköisen tiedonsiirron ongelmista kuten ylijännitepiikeistä. Suurin ero vanhaan kumminkin on valtaisa tiedonsiirtonopeuden kasvu. Aikaisemmin käytössä olleet runkolinkit toimivat yhden giganbitin nopeudella, mutta nyt ne saatiin päivitettyä kymmeneen gigabittiin. Vaikka nopeus saatiinkin jo kymmenkertaistettua, päästään kuidulla vielä suurempiin nopeuksiin tulevaisuudessa. Näin ollen pullonkaula tiedonsiirtonopeuksissa muodostuukin enemmänkin laitteille eikä niinkään fyysiselle kaapeloinnille.

4.4 Tilat

Laboratorion tilat koostuivat pääosin luokkatiloista BK0026, BK0131 ja GameLab. BK0131-tilassa käytössä oli kaksi 24-porttista kytkintä, jotta kaikki luokan koneet saatiin kytkettyä verkkoon. Tulevaisuudessa vanhat kytkimet tullaan korvaamaan uusilla 2960-X-sarjan kytkimillä. GameLab-luokkatilassa ei sijainnut laitekaappia, vaan ristikytkennät sijaitsivat suoraan tilassa BK0125. Pääsääntöisesti GameLabin laitteet olivat kytketty BK0125-S1- ja BK0125-S3-kytkimiin. Näistä tiloista BK0026 oli uusin ja se kaapeloitiin ja kalustettiin kesän 2015 aikana. Tämän takia tila oli ensimmäinen johon päätettiin sijoittaa uusi 2960-X-sarjan kytkin. ICT-laboratoriossa sijaitsee myös uusi opetuskäyttöä varten rakennettu minidatakeskus, Cyberlab. Vaikka tila onkin pääosin varattu Cyberlab-projektin laitteita varten, konesalista varattiin yksi laitekaappi laboratorioverkon laitteita varten.

4.4.1 BK0131

BK0131 luokassa käytettiin siellä jo aiemmin sijanneita liityntätasonkytkimiä, koska uudemmat 2960-X-sarjan kytkimet eivät vielä kesän aikana ehtineet saapua. Aiemmin kytkimet olivat ketjutettu toisiinsa niin, että runkolinkki oli kytketty ainoastaan toiseen kytkimeen, jolloin kaikki liikenne kulki yhden kytkimen kautta.

Uudistuksen yhteydessä molemmat kytkimet kytkettiin suoraan kiinni ydinkytkimeen, jolloin vanhasta yksittäisestä vikaantumispisteestä päästiin eroon. Kiitos uuden valokuitukaapeloinnin kytkimet voitiin kytkeä ydinkytkimeen 10 gigabitin SFP-moduuleilla entisen yhden gigabitin sijaan. Itse kuitukaapeli tuotiin BK0125-tilasta BK0131-tilan laitekaappiin, missä molemmat kytkimistä sijaitsivat. Molempiin kytkimiin luotiin port channel, joka kytkettiin VSS:n molempiin fyysisiin laitteisiin. Tämän lisäksi BK0131-tilan kytkimissä säästettiin aiemmin käytössä ollut linkki niiden välillä. Tällöin, vaikka jommankumman kytkimen runkolinkki katkeaisikin, liikenne voidaan ohjata toisen kytkimen kautta. Kytkimeen luotiin myös uusi VLAN, joka nimettiin luokan mukaan. Tähän VLAN:in lisättiin kaikki luokan koneet ja laitteet, jotta ne saatiin selkeästi eroteltua muista luokkatiloista.

4.4.2 BK0026

BK0026 toimi aikaisemmin luentoluokkana, mutta kesällä 2015 siitä tehtiin laboratorioluokka, jolloin verkkokaapeloinnin takia sinne tarvittiin uusi kytkin. Luokassa käytettiin myös paljon virtuaalikoneita, joten oli tärkeää, että yhteys palvelinverkkoon oli riittävän nopea.

Työn osalta BK0026 vastasi pitkälti samaa mitä BK0131 tilassa tehtiin. Tilaan tuotiin yhdistelmäkuitukaapeli BK125-tilasta ja se kytkettiin kuitupaneeliin, joka asennettiin luokkatilaan vietyyn laitekaappiin. Kuitukaapelista valittiin yksi pari yksimuotokuitua ja kytkettiin se 10 gigabitin SFP-moduuleilla BK0026-S1-kytkimeen. Kytkimen ja VSS:n välille luotiin MEC, jolla pyrittiin lisäämään vikasietoisuutta. Samoin kuin BK0131-tilassa, myös BK0026-tilaa varten kytkimeen luotiin uusi VLAN johon koneet liitettiin.

4.4.3 MDF

Aikaisemmin konesalina toimineesta tilasta BK0125 siirrettiin laboratorio-verkon laitteet Cyberlabiin tilan puutteen ja huonon ilmanvaihdon takia. Samalla tilasta tehtiin ristikytkentäkeskus eli MDF. MDF:ssa tapahtui eri tilojen välinen ristikytkentä pääosin liityntätason kytkinten ja verkon ydinkerroksen välillä. Ristikytkennät toteutettiin lisäämällä tilaan uusi laitekaappi, johon asennettiin kaikkien tilojen kuitupaneelit, sekä tilassa sijainneet kytkimet BK0125-S1, BK0125-S2 ja BK0125-S3. Kaapin viereen jätettiin vielä toinen ristikytkentäkaappi, johon jätettiin vanhat kuparikaapeloinnit ja vielä käytössä olleet GameLabin kaapeloinnit.

4.4.4 Cyberlab

Cyberlab on ICT-Labin uusi, opetuskäyttöä varten rakennettu minidatakeskus. Datakeskus koostui käytännössä kahdesta laitekaapista, akustosta ja jäähdytysyksiköstä. Cyberlabin laitteille varattiin yksi laitekaappi ja laboratorioverkon laitteille toinen, johon sijoitettiin laboratorioverkon palvelimet, VSS-kytkimet ja palomuuri. Kuten muissakin tiloissa, myös Cyberlabiin tuotiin kuitukaapeli, jonka toinen pää sijaitsi MDF:ssa. Kuituja pitkin liityntätason kytkimet liitettiin

ydinkytkimiin. Ylimääräisiä kuituja voitiin käyttää myös Cyberlab projekteissa, luokkatilojen ja datakeskuksen välillä.

Koska Cyberlabissa etäisyydet olivat lyhyitä, kuidun sijaan tilassa olleiden laitteiden välillä voitiin myös käyttää DAC-kaapeleita, jotka ovat lyhemmille matkoille tarkoitettuja kuparikaapeleita, joissa on SFP+-liitin molemmissa päissä. Rajoituksena tässä kaapelissa on, että sitä voidaan tyypillisesti käyttää passiivisena maksimissaan viiteen metriin asti. Alle viiden metrin matkoilla DAC-kaapelista saadaan hyvä korvaaja kuidulle sen halvemman hinnan puolesta, mutta silti saavuttamalla 10 gigabitin tiedonsiirtonopeuden.

5 LOPPUTULOSTEN TARKASTELU

Työ saatiin tehtyä onnistuneesti loppuun. Koko verkkoa ei työn aikana saatu päivitettyä, kun riittävästi laitteita ei ollut saatavilla. Sen takia työ painottuikin paljolti VSS:n ympärille, joka tarjosi hyvän pohjan verkon kasvulle. Sen lisäksi runkoverkon uudistuksesta ja BK0026-S1:n liittämisestä verkkoon saatiin jo hyvä kuva kuinka tämän päivän verkkoratkaisu saadaan toteutettua tehokkaasti ja vikasietoisesti.

5.1 Ongelmat

Opinnäytetyössä esiintyi loppujenlopuksi yllättävän vähän ongelmia. Suurimmat ongelmat tulivat vastaan VSS:n konfiguroinnissa, koska joistakin kriittisistä komentoja ei ollut dokumentoitu kovinkaan selkeästi. Suurin kompastuskivi luultavasti olikin dual-active detection käyttöönotossa se, kuinka enhanced PAgP saadaan toimimaan oikein, koska sitä ei suoraan mainittu Ciscon dokumenteissa. Toinen ongelmakohta oli dual-active recovery mode, jossa ei aluksi ollut SSO käytössä. Molemmat ongelmat saatiin ratkaistua, kun dokumentteihin paneuduttiin hieman perusteellisemmin ja varmistettiin lopulta toimivuus testaamalla järjestelmää.

5.2 Jatkomahdollisuudet

Jatkomahdollisuuksia työ tarjosi runsaasti. Seuraavana verkon päivityksessä oli BK0131-luokan kytkinten päivitys uusiin 2960-X-kytkimiin ja topologian muutos niin, että se vastasi BK0026-S1:n ja VSS:n väliä. BK0131-luokan kytkimet saatiin päivitettyä loppusyksyn aikana yhteen 2960-X-kytkimeen, joka korvasi tilassa aikaisemmin olleet kaksi 2960-kytkintä. Uuden kytkimen suuremman porttimäärän takia tilaan ei ollut tarvetta laittaa toista kytkintä. Sen lisäksi tarpeellista oli palvelinverkon liittäminen VSS:n kuidulla ja 10 gigabitin SFP+-moduuleilla. Tulevaisuudessa myös palomuuri oli tarkoitusta kahdentaa, mutta tämä vaatisi palveluntarjoajalta varayhteyden ulkoverkkoon, että siitä saataisiin irti konkreettista hyötyä.

Kun työ oli saatu tehtyä ja verkko oli tuotannossa, siihen lisättiin toistaiseksi kiinni Cyberlab-verkko. VSS:iin liitettiin Cyberlabin hallintaverkonkytkin, sekä kaksi reititintä, jolloin VSS simuloi ulkoverkkoa. Tällä tavoin opinnäytetyö tarjosi pohjan toisellekin opinnäytetyölle.

LÄHTEET

Cisco Networking Academy. (2014). Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. Hierarchical Network Design Overview Saatavilla: http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4 [viitattu 14.2.2016].

Cisco. (2014). *Catalyst 4500 Series Switch Software Configuration Guide, Release IOS XE 3.4.xSG and IOS 15.1(2)SGx*. Saatavilla: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/15-1-2/XE_340/configuration/guide/config.html [viitattu 8.3.2016].

Cisco. (2009). *Virtual Switching System (VSS) Q&A*. Saatavilla: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-virtual-switching-system-1440/prod_qas0900aecd806ed74b.html [viitattu 15.1.2016].

Cisco, (2013). *Catalyst 6500 Release 12.2SX Software Configuration Guide - Virtual Switching Systems (VSS)*. Saatavilla: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vss.html#wp1063718 [viitattu 6.9.2016].

Cisco, (2006). *Bidirectional Forwarding Detection*. Saatavilla: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.html [viitattu 6.9.2016].

Cisco. (2003). *Cisco StackWise and StackWise Plus Technology*. Saatavilla: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/prod_white_paper09186a00801b096a.html [viitattu 27.10.2016].

The Fiber Optic Association. (2015). *The FOA Reference For Fiber Optics - Optical Fiber*. Saatavilla: http://www.thefoa.org/tech/ref/basic/fiber.html [viitattu 12.5.2016].

TKK. (1998). *Optinen kuitu*. Saatavilla: https://www.netlab.tkk.fi/opetus/s38118/s98/htyo/6/index.shtml [viitattu 12.5.2016].

Services, P., Switches, C., Literature, D. and Sheets, D. (2016). *Cisco Catalyst 4500-X Series Fixed 10 Gigabit Ethernet Aggregation Switch Data Sheet*. Saatavilla: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-x-series-switches/data_sheet_c78-696791.html [viitattu 24.3.2016].

Cisco. (2016). *Cisco Catalyst 2960-X Series Switches Data Sheet*. Saatavilla: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html [viitattu 2.8.2016].

Cisco. (2016). *Cisco ASA 5505 Adaptive Security Appliance and ASA 5500-X Series Next-Generation Firewalls Data Sheet*. Saatavilla: http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-701253.html [viitattu 17.8.2016].

NetCraftsmen. (2010). *Cisco VSS Dual-Active Detection - NetCraftsmen*. Saatavilla: http://www.netcraftsmen.com/cisco-vss-dual-active-detection/ [viitattu 19.10. 2016].

LIITE 1

```
BK0139-R1#sh run
Building configuration...

Current configuration : 12554 bytes
!
! Last configuration change at 06:53:39 UTC Thu Oct 1 2015 by teemu.metso
! NVRAM config last updated at 06:53:43 UTC Thu Oct 1 2015 by teemu.metso
!
version 15.2
no service pad
service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year
no service password-encryption
service compress-config
service unsupported-transceiver
!
hostname BK0139-R1
!
boot-start-marker
boot-end-marker
!
!
vrf definition mgmtVrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
```

```
 exit-address-family
!
enable secret 5 $1$AEFP$ZgwsWmb35XKETT8/Ysamw/
!
username temp secret 5 $1$x5ZG$PthFrD5BjJC7G6qUxYvei1
username admin secret 5 $1$Gs12$7Umm/GTMs6uZWXDW8wiES/
aaa new-model
!
!
aaa authentication login default group radius local
aaa authentication login CONSOLE local
aaa authorization exec default group radius local
!
aaa session-id common
!
switch virtual domain 1
 switch mode virtual
 switch 1 priority 200
 mac-address use-virtual
!
 dual-active detection pagp trust channel-group 10
no dual-active detection fast-hello
!
ip vrf Liin-vrf
!
ip domain-name ictlab.kyamk.fi
!
vtp mode transparent
!
!
power redundancy-mode redundant
```

```
!
mac access-list extended VSL-BPDU
 permit any 0180.c200.0000 0000.0000.0003
mac access-list extended VSL-CDP
 permit any host 0100.0ccc.cccc
mac access-list extended VSL-DOT1x
 permit any any 0x888E
mac access-list extended VSL-GARP
 permit any host 0180.c200.0020
mac access-list extended VSL-LLDP
 permit any host 0180.c200.000e
mac access-list extended VSL-MGMT
 permit any 0022.bdcd.d200 0000.0000.00ff
 permit 0022.bdcd.d200 0000.0000.00ff any
mac access-list extended VSL-SSTP
 permit any host 0100.0ccc.cccd
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
 mode sso
!
vlan internal allocation policy ascending
!
vlan 2
 name NETMGMT
!
vlan 3
 name CYBERLAB-MGMT
!
vlan 16
```

```
 name STAFF
!
vlan 17
 name STAFFW
!
vlan 32
 name CLASS131
!
vlan 33
 name CLASS026
!
vlan 34
 name CLASS128
!
vlan 40
 name Outside
!
vlan 41
 name game
!
vlan 48
 name RD-CYBERLAB-ESX
!
vlan 79
 name Insinooristudio
!
vlan 123
 name Lohi
!
vlan 125
 name Hauki
```

```
!
vlan 126
 name Ahven
!
vlan 128
 name Taimen
!
vlan 131
 name Kuha
!
vlan 136
 name Lahna
!
vlan 138
 name DMZ
!
vlan 140
 name IPv6
!
vlan 145
 name GuestWLAN
!
vlan 150
 name WLAN
!
vlan 201
 name VPN-inside
!
vlan 300
 name BK0131-R1-FW INSIDE
!
```

```
vlan 301
 name LINKS
!
!
class-map match-any VSL-MGMT-PACKETS
 match access-group name VSL-MGMT
class-map match-any VSL-DATA-PACKETS
 match any
class-map match-any VSL-L2-CONTROL-PACKETS
 match access-group name VSL-DOT1x
 match access-group name VSL-BPDU
 match access-group name VSL-CDP
 match access-group name VSL-LLDP
 match access-group name VSL-SSTP
 match access-group name VSL-GARP
class-map match-any VSL-L3-CONTROL-PACKETS
 match access-group name VSL-IPV4-ROUTING
 match access-group name VSL-BFD
 match access-group name VSL-DHCP-CLIENT-TO-SERVER
 match access-group name VSL-DHCP-SERVER-TO-CLIENT
 match access-group name VSL-DHCP-SERVER-TO-SERVER
 match access-group name VSL-IPV6-ROUTING
class-map match-any VSL-MULTIMEDIA-TRAFFIC
 match dscp af41
 match dscp af42
 match dscp af43
 match dscp af31
 match dscp af32
 match dscp af33
 match dscp af21
 match dscp af22
```

```
 match dscp af23
class-map match-any VSL-VOICE-VIDEO-TRAFFIC
 match dscp ef
 match dscp cs4
 match dscp cs5
class-map match-any VSL-SIGNALING-NETWORK-MGMT
 match dscp cs2
 match dscp cs3
 match dscp cs6
 match dscp cs7
!
policy-map VSL-Queuing-Policy
 class VSL-MGMT-PACKETS
  bandwidth percent 5
 class VSL-L2-CONTROL-PACKETS
  bandwidth percent 5
 class VSL-L3-CONTROL-PACKETS
  bandwidth percent 5
 class VSL-VOICE-VIDEO-TRAFFIC
  bandwidth percent 30
 class VSL-SIGNALING-NETWORK-MGMT
  bandwidth percent 10
 class VSL-MULTIMEDIA-TRAFFIC
  bandwidth percent 20
 class VSL-DATA-PACKETS
  bandwidth percent 20
 class class-default
  bandwidth percent 5
!
interface Port-channel1
 description VSL
```

```
 switchport
 switchport mode trunk
 switch virtual link 1
!
interface Port-channel2
 description VSL
 switchport
 switch virtual link 2
!
interface Port-channel10
 description TRUNK BK0026
 switchport
 switchport mode trunk
 switchport nonegotiate
!
interface Port-channel11
 description TRUNK BK0125_LOHI
 switchport
 switchport mode trunk
!
interface Port-channel12
 description TRUNK BK0131_IKKUNA
 switchport
 switchport mode trunk
!
interface Port-channel13
 description TRUNK BK0131_OVI
 switchport
 switchport mode trunk
!
interface Port-channel20
```

```
 description -> BK0139-FW1 Po1
 switchport
 switchport trunk allowed vlan 138,145,300
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet1
 vrf forwarding mgmtVrf
 no ip address
 speed auto
 duplex auto
!
interface TenGigabitEthernet1/1/1
 description Port-channel 1 1/2 sw1->sw2
 switchport mode trunk
 no lldp transmit
 no lldp receive
 channel-group 1 mode on
 service-policy output VSL-Queuing-Policy
!
interface TenGigabitEthernet1/1/2
 description Port-channel 1 2/2 sw1->sw2
 switchport mode trunk
 no lldp transmit
 no lldp receive
 channel-group 1 mode on
 service-policy output VSL-Queuing-Policy
!
interface TenGigabitEthernet1/1/3
 description Port-channel 20 -> BK0139-FW1 Gi1/2
 switchport trunk allowed vlan 138,145,300
```

```
 switchport mode trunk
 switchport nonegotiate
 channel-group 20 mode active
!
interface TenGigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/5
 description Port-channel 10 1/2 ->BK0026
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode desirable
!
interface TenGigabitEthernet1/1/6
 description Port-channel 11 1/2 ->BK0125_LOHI
 switchport mode trunk
 channel-group 11 mode active
!
interface TenGigabitEthernet1/1/7
 description Port-channel 12 1/2 ->BK0131_IKKUNA
 switchport mode trunk
 channel-group 12 mode active
!
interface TenGigabitEthernet1/1/8
 description Port-channel 13 1/2 ->BK0131_OVI
 switchport mode trunk
 channel-group 13 mode active
!
interface TenGigabitEthernet1/1/15
 switchport mode trunk
 no lldp transmit
 no lldp receive
```

```
 no cdp enable
 channel-group 1 mode on
 service-policy output VSL-Queuing-Policy
!
interface TenGigabitEthernet1/1/16
 switchport mode trunk
 no lldp transmit
 no lldp receive
 no cdp enable
 channel-group 1 mode on
 service-policy output VSL-Queuing-Policy
!
interface TenGigabitEthernet2/1/1
 description Port-channel 2 1/2 sw2->sw1
 no lldp transmit
 no lldp receive
 channel-group 2 mode on
 service-policy output VSL-Queuing-Policy
!
interface TenGigabitEthernet2/1/2
 description Port-channel 2 2/2 sw2->sw1
 no lldp transmit
 no lldp receive
 channel-group 2 mode on
 service-policy output VSL-Queuing-Policy
!
interface TenGigabitEthernet2/1/3
 description Port-channel 20 -> BK0139-FW1 Gi1/4
 switchport trunk allowed vlan 138,145,300
 switchport mode trunk
 switchport nonegotiate
```

```
 channel-group 20 mode active
!
interface TenGigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/5
 description Port-channel 10 2/2 ->BK0026
 switchport mode trunk
 switchport nonegotiate
 channel-group 10 mode desirable
!
interface TenGigabitEthernet2/1/6
 description Port-channel 11 2/2 ->BK0125_LOHI
 switchport mode trunk
 channel-group 11 mode active
!
interface TenGigabitEthernet2/1/7
 description Port-channel 12 2/2 ->BK0131_IKKUNA
 switchport mode trunk
 channel-group 12 mode active
!
interface TenGigabitEthernet2/1/8
 description Port-channel 13 2/2 ->BK0131_OVI
 switchport mode trunk
 channel-group 13 mode active
!
interface TenGigabitEthernet2/1/15
 no lldp transmit
 no lldp receive
 no cdp enable
 channel-group 2 mode on
 service-policy output VSL-Queuing-Policy
```

```
!
interface TenGigabitEthernet2/1/16
 switchport mode trunk
 no lldp transmit
 no lldp receive
 no cdp enable
 channel-group 2 mode on
 service-policy output VSL-Queuing-Policy
!
interface Vlan1
 no ip address
!
interface Vlan2
 description Network and Facility Management
 ip address 172.16.0.1 255.255.255.0 secondary
 ip address 172.16.0.44 255.255.255.0 secondary
 ip address 10.69.2.1 255.255.255.0
 no ip redirects
 counter ipv4
!
interface Vlan3
 description Cyberlab Platform Management
 ip address 10.69.3.1 255.255.255.0
 counter ipv4
!
interface Vlan16
 description Staff Workstations DHCP
 ip address 10.69.16.1 255.255.255.0
 ip helper-address 193.167.58.26
 ip helper-address 193.167.58.28
 counter ipv4
```

```
!
interface Vlan17
 description Staff Wireless DHCP
 ip address 10.69.17.1 255.255.255.0
 ip helper-address 193.167.58.26
 ip helper-address 193.167.58.28
 counter ipv4
!
interface Vlan32
 description BK0131 Cisco Lab
 ip address 10.69.32.1 255.255.255.0
 ip helper-address 193.167.58.26
 ip helper-address 193.167.58.28
 counter ipv4
!
interface Vlan33
 description BK0026 Computer Class
 ip address 10.69.33.1 255.255.255.0
 ip helper-address 193.167.58.26
 ip helper-address 193.167.58.28
 counter ipv4
!
interface Vlan34
 description BK0128 GameLab
 ip address 10.69.34.1 255.255.255.0
 ip helper-address 193.167.58.26
 ip helper-address 193.167.58.28
 counter ipv4
!
interface Vlan48
 ip address 10.69.48.1 255.255.255.0
```

```
!
interface Vlan79
 description IPv6 linkki insinooristudiolle
 no ip address
!
interface Vlan123
 description Lohi
 ip address 193.167.58.65 255.255.255.192
 ip helper-address 193.167.58.2
 ip helper-address 193.167.58.3
 ip pim sparse-mode
 ipv6 enable
!
interface Vlan125
 description Hauki
 ip address 193.167.58.1 255.255.255.224
 ip helper-address 193.167.58.2
 ip pim sparse-mode
 ipv6 enable
!
interface Vlan126
 description Ahven
 ip address 193.167.58.225 255.255.255.240
 ip helper-address 193.167.58.2
 ip helper-address 193.167.58.3
 ip pim sparse-mode
!
interface Vlan128
 description Taimen
 ip address 193.167.58.33 255.255.255.224
 ip helper-address 193.167.58.2
```

```
 ip helper-address 193.167.58.3
 ip pim sparse-mode
 ipv6 address ictlab ::2:0:0:0:33/64
 ipv6 enable
!
interface Vlan131
 description Kuha
 ip address 193.167.58.129 255.255.255.192
 ip helper-address 193.167.58.2
 ip helper-address 193.167.58.3
 ip pim sparse-mode
 ipv6 enable
!
interface Vlan136
 description Lahna
 ip address 193.167.58.193 255.255.255.224
 ip helper-address 193.167.58.2
 ip helper-address 193.167.58.3
 ip pim sparse-mode
 ipv6 enable
!
interface Vlan140
 description Link to Simunet IPv6
 no ip address
 ipv6 enable
!
interface Vlan150
 description WLAN
 ip address 10.150.0.2 255.255.0.0
!
interface Vlan300
```

```
 description -> BK0139-FW inside
 ip address 10.69.0.2 255.255.255.248
!
ip default-gateway 10.69.2.1
no ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.69.0.1
ip route 10.69.0.0 255.255.128.0 Null0
ip route 10.69.18.0 255.255.255.0 10.69.0.1
!
ip access-list standard SNMP-IN
 permit 10.69.2.0 0.0.0.255
 permit 10.69.16.0 0.0.0.255
!
ip access-list extended VSL-BFD
 permit udp any any eq 3784
ip access-list extended VSL-DHCP-CLIENT-TO-SERVER
 permit udp any eq bootpc any eq bootps
ip access-list extended VSL-DHCP-SERVER-TO-CLIENT
 permit udp any eq bootps any eq bootpc
ip access-list extended VSL-DHCP-SERVER-TO-SERVER
 permit udp any eq bootps any eq bootps
ip access-list extended VSL-IPV4-ROUTING
 permit ip any 224.0.0.0 0.0.0.255
!
ip radius source-interface Vlan2
!
snmp-server community CL15read RO SNMP-IN
snmp ifmib ifindex persist
```

```
radius-server host 193.167.58.25 key 7
11061B3738042858297B0713783121173E06022E147D5C5C505B5C2E4A37570C11644
80C060D592D575F42411210247D39563A16686D263907334A2300080E2260
!
ipv6 access-list VSL-IPV6-ROUTING
 permit ipv6 any FF02::/124
!
!
line con 0
 logging synchronous
 login authentication CONSOLE
 stopbits 1
line vty 0 4
 logging synchronous
 transport input ssh
line vty 5 15
 logging synchronous
 transport input ssh
!
!
module provision switch 1
 chassis-type 71 base-mac 80E0.1D4C.F800
 slot 1 slot-type 401 base-mac 80E0.1D4C.F800
 !
module provision switch 2
 chassis-type 71 base-mac 80E0.1D4C.F880
 slot 1 slot-type 401 base-mac 80E0.1D4C.F880
!
 ntp server 193.167.63.21 prefer
 !
end
```