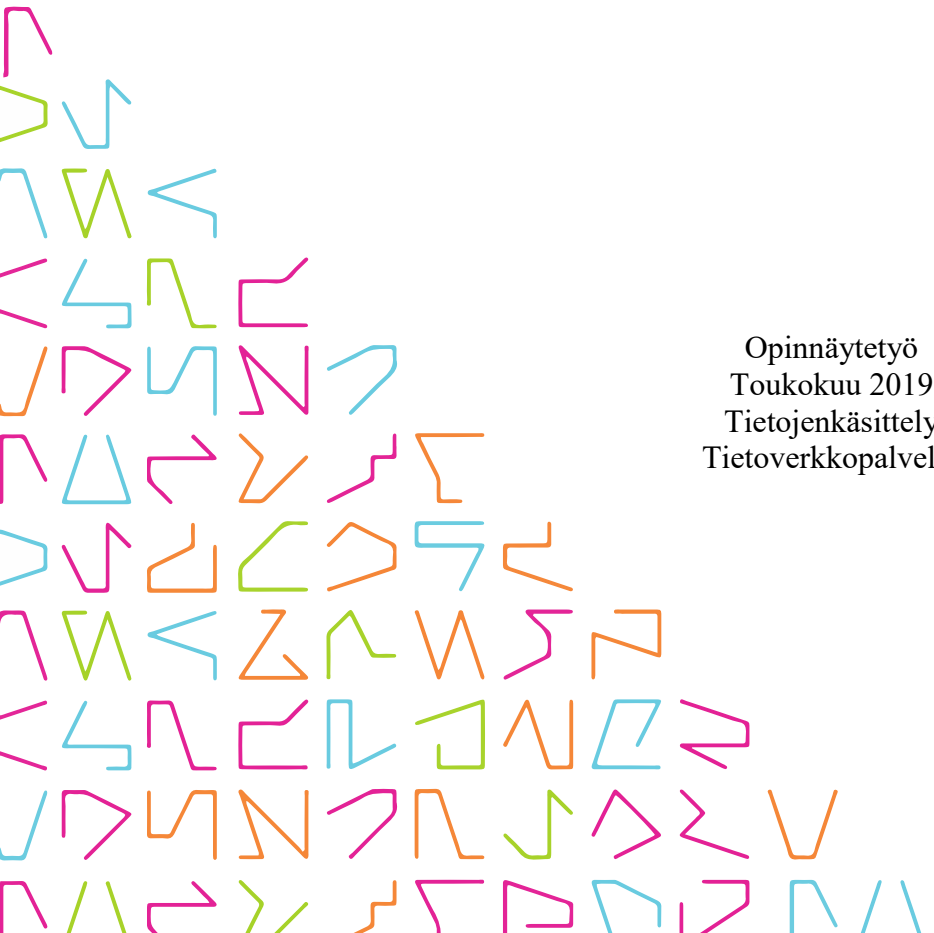
TAMPEREEN
AMMATTIKORKEAKOULU

Virtuaalinen verkkoluokkaympäristö

Julius Salonen



Opinnäytetyö
Toukokuu 2019
Tietojenkäsittely
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

SALONEN, JULIUS:
Virtuaalinen verkkoluokkaympäristö

Opinnäytetyö 25 sivua, joista liitteitä 3 sivua
Toukokuu 2019

Virtuaalinen verkkoluokkaympäristö on TAMKin Tietojenkäsittelyn koulutusohjelmalle tuotettu etäkäytettävä järjestelmä, joka vastaa koulutuslinjan tarpeisiin tarjoamalla mahdollisuuden testata ja kehittää luokkamateriaalia eristetyssä ja korkeasti saatavissa olevasta ympäristössä.

Opinnäytetyön tavoitteena on soveltaa kehittämistyön menetelmiä, jotta voimme parantaa nykyisen WPK-verkon käytettävyyttä sekä luoda opettajille ja opiskelijoille mahdollisuus hyödyntää WPK-verkon resursseja kellonajasta tai käyttäjän paikasta riippumatta. Työn tarkoituksena on tuottaa virtuaalinen verkkoluokkaympäristö WPK-verkkoon, joka olisi täysin etäkäytettävä myös WPK-verkon ulkopuolelta VPN:ää käyttäen, ilman käsin tehtäviä muutoksia fyysisiin laitteisiin.

Tarkoituksen täyttöä varten fyysiset reitityslaitteet asetetaan Ciscon viralliseen koe-konfiguraatioon, jolloin johdotusmuutokset ovat tarpeettomat, mutta virtuaalisten käyttäjäkoneiden määrä ja käyttötyyppi voi olla erilainen riippuen järjestelmän käyttötarkoituksesta. Tämän vuoksi tuotoksen tulee mahdollistaa verkkoluokkaopintojen koeympäristöä vastaavan järjestelmän etäkäyttö, ja selvittää onko tilatun kaltainen järjestelmä käytännöllinen Tietojenkäsittelyn koulutusohjelman tuottamiin tarpeisiin.

Asiasanat: cisco, reititys, virtuaalikone, verkkotekniikka

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

SALONEN, JULIUS:
Virtual Networking Class Environment

Bachelor's thesis 25 pages, appendices 3 pages
May 2019

This work – "Virtual networking class environment" is a remote controllable system produced for the TAMK (Tampereen ammattikorkeakoulu, Tampere University of Applied Sciences) Business Information Systems, which matches the needs of the degree programme by providing a test and development environment for producing class material in an enclosed and highly available system.

The goal for this thesis is to apply the methods of development to improve the usability of the currently available WPK-network, and to provide teachers and students an opportunity to utilize the resources of WPK-network regardless of the time of day or the physical user location. The intention of the work is to produce a virtual networking class environment inside the WPK-network, which would also be fully remote-accessible through a VPN, without needing physical access to the actual devices that form the system.

To fulfill the intention, the physical networking devices are set in an official Cisco examination configuration, which makes changes in cabling needless in most cases. However, virtual user machines and the type of said machines may be different from examination to examination. Therefore the work must provide remote access to a system similar to the networking class examination environment, and to find out if the system specified is practical for the needs of the Business Information Systems' Degree Programme.

Key words: cisco, routing, virtual machine, networking technology

SISÄLLYS

LYHENTEET JA TERMIT

ALS	Access Layer Switch (tavanomainen kytkin)
CDP	Cisco Discovery Protocol, Ciscon oma laitetunnistusprotokolla jolla reitittimet ja kytkimet voivat keskustella ja tunnistaa toisiaan ilman varsinaista konfigurointia.
Cisco	Cisco Systems. Monikansallinen tietoliikenneyritys. Tuottaa valtaosan maailman verkkoteknologiasta ja laitteistosta.
DLS	Distribution Layer Switch (reitittävä kytkin)
RRAS	Routing and Remote Access Services, Microsoftin reititysohjelmisto Windows-käyttöjärjestelmälle
TAMK	Tampereen ammattikorkeakoulu
vLab Console	vLabin konsolipalvelin, joka tarjoaa konsoliyhteyksiä laitteisiin SSH:n yli.
vLab Server	vLabin virtuaalikonepalvelin
vLab	Virtuaaliluokkaympäristön lyhennetty kutsumanimi
WPK-verkko	Tietojenkäsittelyn lähiverkko (kts. luku 2)

1 JOHDANTO

Nykyään siirrytään jatkuvasti poispäin täysin fyysisistä laiteympäristöistä. Tämä johtuu useista tekijöistä, joista nousee tärkeimpinä helppokäyttöisyys ja kustannustehokkuus – virtualisoiduilla ympäristöillä voidaan tuottaa yhden tehokkaan palvelimen päälle samat palvelut, joita ennen olisi tarjottu usealta fyysiseltä laitteelta. Samalla kerralla säästyy aikaa ja rahaa hallinnollisten tehtävien ja asennusten kanssa.

WPK-verkossa löytyy jo kaksi tietoverkkolaboratoriota, joissa voidaan työskennellä reititys- ja kytkentälaitteiden kanssa, mutta tämä vaatii fyysistä johdotusta ja jatkuvaa töiden rakentamista sekä purkua. Koska tätä ei voida käyttää etäältä, mm. kokeiden ja muiden testien valmistelu on vaikeaa ja vaatii fyysistä paikallaoloa usein varatussa laboratoriotilassa. Ratkaisuna eräs opettaja ehdotti yhden kaapin virtualisointia serverihuoneeseen, jota voitaisiin käyttää etänä vaikka omasta kodista.

Tämä opinnäytetyöraportti selostaa hieman kuinka osittain virtualisoitua ympäristöä voidaan käyttää hyödyksi helppokäyttöisyyden saavuttamiseksi. Työn tuloksena luotiin ympäristö, jossa luokkatilan tietokoneet ovat virtualisoitu palvelimelle, joka palvelee valmiiksi kytkettyä verkkolaitekaappia. Koko järjestelmään voidaankin ottaa etähallintayhteys, jolloin kyetään hallinnoimaan yhtä kaappia, samoin kuin luokkatilankin kaappia, mahdollistaen testauksen ja töiden valmistelun kotoa tai muusta työtilasta kuin varsinaisesta verkkolaboratoriosta.

Tätä raporttia lukevan henkilön taitotaso tulisi olla mielellään Tietojenkäsittelyn ensimmäisen vuoden opiskelijan tasolla, eli IP-lähiverkon koostumuksen, virtuaalikoneiden ja muut IT-käsittelytaidon perusteet ovat opittuna tai opittavana. Näin ollen osaa vähemmän erikoisemmista termeistä ei välttämättä ole erikseen selitetty auki raportin turhan pitkittymisen välttämiseksi.

2 TAUSTA

2.1 WPK-Verkon esittely

WPK-verkko on kutsumanimi TAMK Tietojenkäsittelyn omalle lähiverkolle, jota ylläpitää Tietojenkäsittelyn koulutusohjelman oppilaista koostuva harjoittelijapari. Verkko on oma hallinnoitu ympäristönsä, jonka ”palveluntarjoajana” toimii TAMKin oma verkko, josta on allokoitu IP-avaruus ja tuotu tiettyjä palveluita WPK-verkon käytettäväksi. WPK-verkko tarjoaa domainin suomat palvelut suureen osaan Tietojenkäsittelyn siiven (C-rakennus) luokista, sekä erinäisiä www- ja muita lisäpalveluita mm. Pelituotannon ja Tietoverkkopalveluiden tarpeisiin.

Verkkoa hallinnoiva harjoittelijapari vaihtuu kuuden kuukauden välein, ja henkilöt yleensä valitaan tietoverkkopolun opiskelijoista. Tämä luo erityisvaatimuksia verkon dokumentoinnin osalta, sillä verkkoa pitää pystyä hallinnoimaan henkilöt, jotka eivät voi kysyä aiemmilta työntekijöiltä juurikaan apua. Tämä toistuu varsinkin epätavallisten tapausten osalta, joita ei kouluteta ohjelmassa, kuten opinnäytetöiden kaltaisten projektien parissa.

WPK-verkko on arkkitehtuurillisesti suunniteltu noin keskikokoisen yrityksen vastaavaksi, jolta löytyy yli 100 työasemaa sekä virtuaalisia että fyysisiä palvelimia, reilusti talletustilaa ja muuta. Verkon suunnittelupohjana on niin kutsuttu collapsed core-tyyli, jossa verkonrajalla toimiva reititin toimii palomuurina eikä varsinaisesti reititä yhteyksiä vaan syöttää ulkoyhteyttä reitittävälle DLS-kytkinparille. DLS-kytkimet kykenevät sekä reitittämään että kytkemään yhteyksiä huomattavasti korkeammalla tehokkuudella ja nopeudella kuin suurin osa tarjotuista reitittimistä.

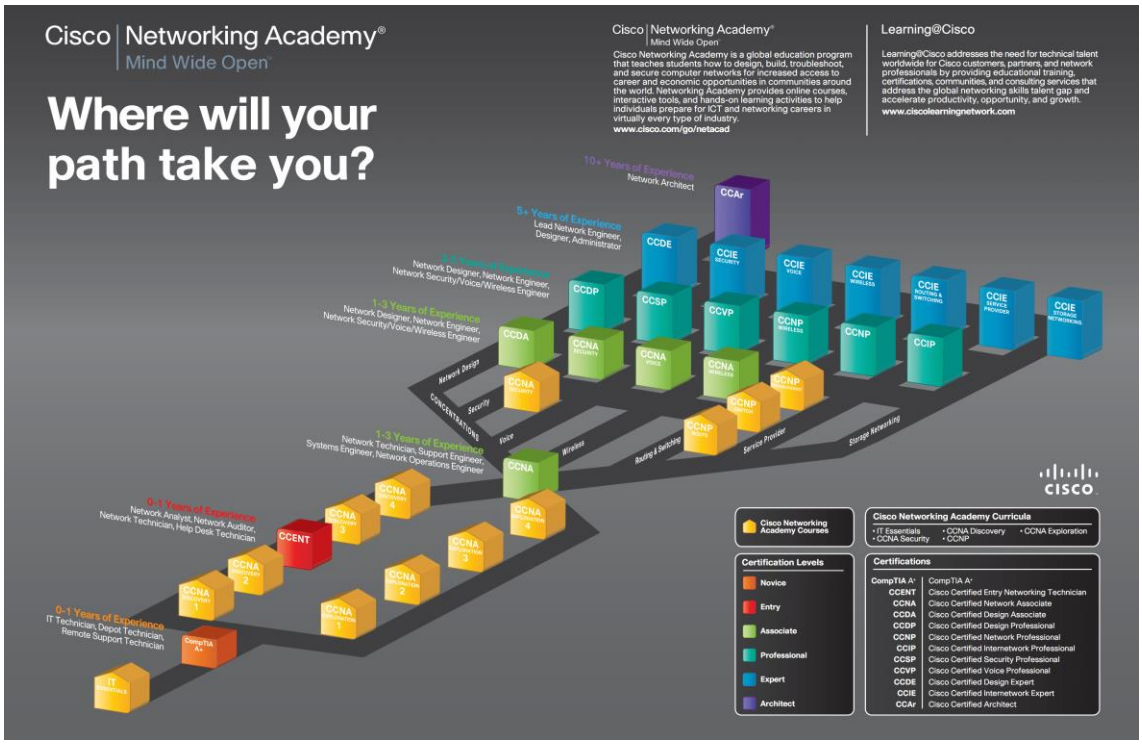
Verkkoon voidaan ottaa ulkoa yhteyttä turvallisen VPN:n kautta, jota tarjoaa RRAS-roolissa toimiva Windows-pohjainen palvelin. VPN:n yli verkkoa voidaan käyttää ja hallita kuin miltä tahansa domainin alla olevalta koneelta. Tämän opinnäytetyön verkkoluokkaympäristön käyttö perustuukin WPK-verkon VPN:n suomaan helppokäyttöisyyteen, sillä työ ei vaatinut minkäänlaista erikoista palomuuritusta tai portitusta verkon laidalle.

2.2 Cisco Networking Academy ja verkkokoulutus TAMKissa

TAMKin Tietojenkäsittelyn koulutusohjelma tarjoaa useita CCNA- ja CCNP-kursseja (Cisco Certified Networking Associate / Professional) Ciscon tarjoamasta netacad.com-palvelusta. Cisco Systems on suuri monikansallinen elektroniikkayritys, joka tuottaa suuren osan maailman tietoliikenne-laitteistosta. Ciscon opetussuunnitelman mukaisesti tehdyt kurssit varmistavat koulutettavien oppivan työelämän kannalta tärkeitä taitoja.

Kursseilla saavutetaan sertifikaattikokeisiin valmistava taitotaso, joka vastaa muutamien vuosien kokemusta työalalla. Cisco itse suosittelee 3-5 vuoden kokemusta työalalta ennen CCNP-kurssien suorittamista. Vaikka koulutus keskittyykin käytännön puolelta Ciscon laitteistoon, teoriaa voidaan soveltaa myös muiden tarjoajien laitteistojen parissa.

Tietoverkkopalveluiden koulutusohjelmassa CCNA- ja CCNP-kursseja käydään reitityksen, kytkennän, tietoturvan ja vianhallinnan puolesta. Netacad tarjoaa myös muun muassa suunnittelua, langattomien palveluiden toteutusta sekä pilvipalveluiden käyttöön ohjaavaa koulutusta. Kuva 1 havainnollistaa Netacad-kurssien opintokokonaisuuksia.



Kuva 1, Cisco NetAcad opintopolkukuvaus

Reititys ja kytkentä tarjoavat erilaisten reititysprotokollien ymmärtämiseen ja hallinnoimiseen vaadittavaa koulutusta. Tietoturva käy tietoturvaa läpi sekä käyttäjäkohtaiselta puolelta että verkkohallinnan puolelta, jossa hyväksikäytetään Ciscon ASA-palomuureja (Adaptive Security Appliance). Vianhallinta on hieman työelämään valmistavampi kokonaisuus, jossa käydään läpi reitityksen ja kytkennän koulutuskokonaisuutta valmiiden mutta viallisten ympäristöjen korjauksen ja parantavien asennusten näkökulmasta.

Englanniksi kyseiset kurssit tunnetaan paremmin nimillä Routing, Switching, Security ja Troubleshooting, jotka ovat kurssien ja sertifikaattien viralliset nimet. R&S ja TSHOOT-kurssit ovat yleensä koottu yhdeksi verkkopalvelukoulutuslinjaksi, sillä ne muodostavat yhdessä yhtenäisen kokonaisuuden.

Verkko-opintojen koulutus on hyvin käytännönläheistä TAMKissa. Suurin osa koulutuksesta vietetään laboratorioiden parissa, jossa rakennetaan kokonaisia verkkoja virtuaalikoneiden ja fyysisten verkkolaitteiden kanssa. Työt tehdään pääasiallisesti pareittain tai ryhmissä – joka parille varataan kokonaista koekokoonpanoa vastaava määrä laitteita, ja joissain ympäristöissä muun muassa TSHOOT-kurssilla saatetaan tarvita kahden parin laitteet.

Virtuaalinen verkkolaboratorio sisältää koekokoonpanoa vastaavan laiterakenteen, jollainen olisi yhdellä opiskelijaparilla normaalisti käytettävänä.

3 TEKNOLOGIAT JA TARPEET

3.1 Telnet

Telnet on selkokielinen kaksisuuntainen verkkoprotokolla pääasiallisesti terminaalin käyttöön verkon kautta. Se on jo vanha tietoliikenneprotokolla jonka nimi tulee sanoista ”teletype network”. (Wikipedia 2018a) Telnetiä ei juurikaan käytetty tässä työssä, mutta sen korvaajaa, SSH:ta kylläkin. Virtuaalilaboratorion laitteistolla kuitenkin on tuki telnetinkin käyttöön, jota usein demonstroidaan esimerkiksi tietoturvallisuuskoulutuksessa.

3.2 SSH

SSH eli Secure Shell on protokolla, joka hyödyntää kryptografisia metodeja tietoliikenteen salaamiseen. SSH:n ensimmäinen versio luotiin Suomessa tekniikan lisensiaatti Tatu Ylösen toimesta vuonna 1995 (Wikipedia 2018b) korvaamaan muut epäturvalliset remote shell-protokollat kuten telnet, rsh, rlogin ym. Shell-sanalla tarkoitetaan käyttöjärjestelmän käyttöliittymää – usein Linux-yhteydessä komentolinjapohjaista terminaalinäkymää (kuten sh, bash tai zsh, joissa -sh-pääte tarkoittaa shelliä), joka on pääasiallinen käyttöliittymä useissa palvelinkäyttöön tarkotettuihin Linux-järjestelmien jakeluissa.

Tämän työn laitteistosta suurin osa on saavutettavissa ja konfiguroitavissa SSH-standardin mukaisen yhteyden kautta, SSH 2-versiolla. Reitittimet ja verkkolaitteet tukevat myös telnetiä ja konsoliporttiyhteyttä.

3.3 Konsoliyhteys

Ciscon ja monen muun valmistajan tuottamat verkkolaitteet sisältävät ohjauspaneelin (management console), jonka tekstipohjaista käyttöliittymää kutsutaan konsoliksi. Konsoliyhteys on vanha ja pääasiallinen vakioyhteystapa laitteisiin, sillä sitä on vaikea toteuttaa pitkien matkojen ylitse ja näin ollen on myöskin tietoturvallinen, sillä sen käyttäjällä tulee usein olla suora fyysinen yhteys käsiteltävään laitteeseen.

Verkkolaitteiden konsoliyhteys on nykyäänkin pääasiallisesti toteutettu sarjaporttiyhteydellä DB9-liittimen kautta, jonka löytää useimmista vanhemmista tietokoneista. Sarjaportti on nykyään usein vaihdettu verkkolaitteen päässä RJ45-liittimeen (tyypillinen verkkojohto), joten erilaiset konversiokaapelit ovat yleisiä. Nykyään voi myös löytää laitteita, jotka tarjoavat konsoliyhteyttä USB:stä USB:hen-kaapelilla.

3.4 VLAN

Virtual Local Area Network eli virtuaalinen lähiverkko. VLANit ovat hyvä tapa jakaa verkon elementtejä eri alueille käyttämättä ylimääräisiä laitteita. Yksittäinen kytkin voi esimerkiksi turvallisuussyistä jakaa jokaisen eri porttinsa eri VLANiin estäen näin yhdistettyjä laitteita ’näkemästä’ toisiaan vaikka ne ovatkin kytketty samaan kytkimeen. VLANeja voi myös kuljettaa kytkimestä toiseen, mahdollistaen laaja-alaiset eritellyt verkot, jossa useat laitteet eri verkoista voidaan jakaa ja yhdistää toisiinsa järkevästi. (Cisco 2018)

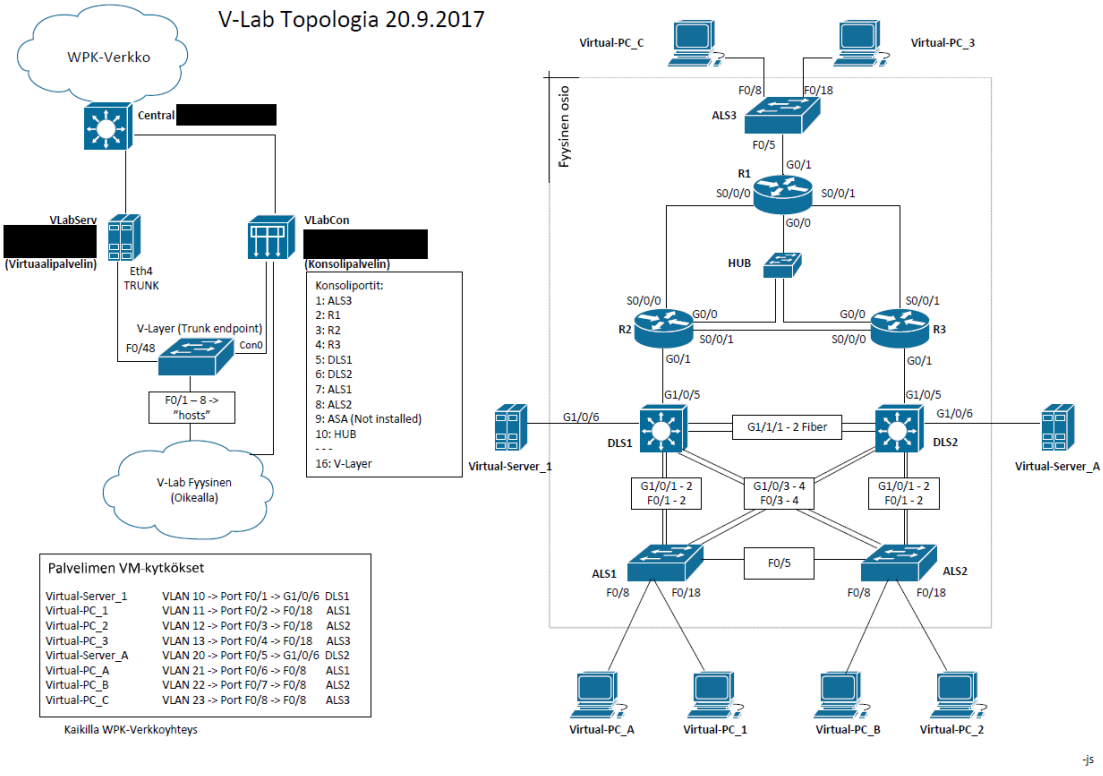
3.5 RRAS

Routing and Remote Access Service on Windows-palvelin-palvelu joka tarjoaa reititys- ja etäkäyttömahdollisuudet Windows-pohjaiseen ympäristöön.

4 FYYSINEN YMPÄRISTÖ

4.1 Ympäristön esittely

Verkkoluokkaympäristö koostuu sekä fyysisestä että virtuaalisesta (loogisesta) puolesta. Fyysinen puoli on hyvin sitoutunut virtuaaliseen puoleen, ja käytännössä virtuaalinen puoli toimii eräänlaisena välikappaleena fyysisen palvelinpuolen ja fyysisen reitityspuolen välillä. Alla oleva topologiakuva (Kuva 2) on eriytetty kahteen osaan, jossa vasemmalla kuvataan vLabia tukevia kappaleita: VLabServ, VLabCon, VLayer, jotka ovat liitetty ”Central” DLS-kytkimiin, WPK-verkon ytimeen, ja oikealla kuvataan varsinaista verkkoluokkaa, jossa reitittävä ja kytkevä laitteisto on fyysisesti paikallaan, mutta tietokoneet ja palvelimet ovat VLabServerillä pyöriviä osioita.



Kuva 2, Virtuaalisen verkkoluokkaympäristön topologiakuva (osa tiedoista sensuroitu)

4.2 Laitteiston esittely

Nimi	KPL	Kuvaus
VLabServ Windows-palvelin	1	Windows-virtuaalikoneita pyörittävä palvelin
VLabCon Konsolipalvelin	1	Konsolikytkentöjen palvelin, yhdistetty virtuaaliverkon laitteisiin hallintaa varten
VLayer Cisco-kytkin	1	Kytkin VLabin yhteyksien purkamiseen virtuaalisen ympäristön laitteille
Virtuaalisen verkkoympäristön laitteisto:		
Reititin	3	Koekäyttöön tarkoitetut Ciscon reitittimet.
DLS	2	Distribution Layer Switch eli maallisemmin reitittävä kytkin – DLS kykenee sekä reitittämään että kytkemään liikennettä
ALS	3	Access Layer Switch, tavallinen kytkin
HUB	1	Kytkin reitittimien 1-3 kytkemiseen tavallisella ethernet-verkkokaapelilla

4.2.1 VLabServ

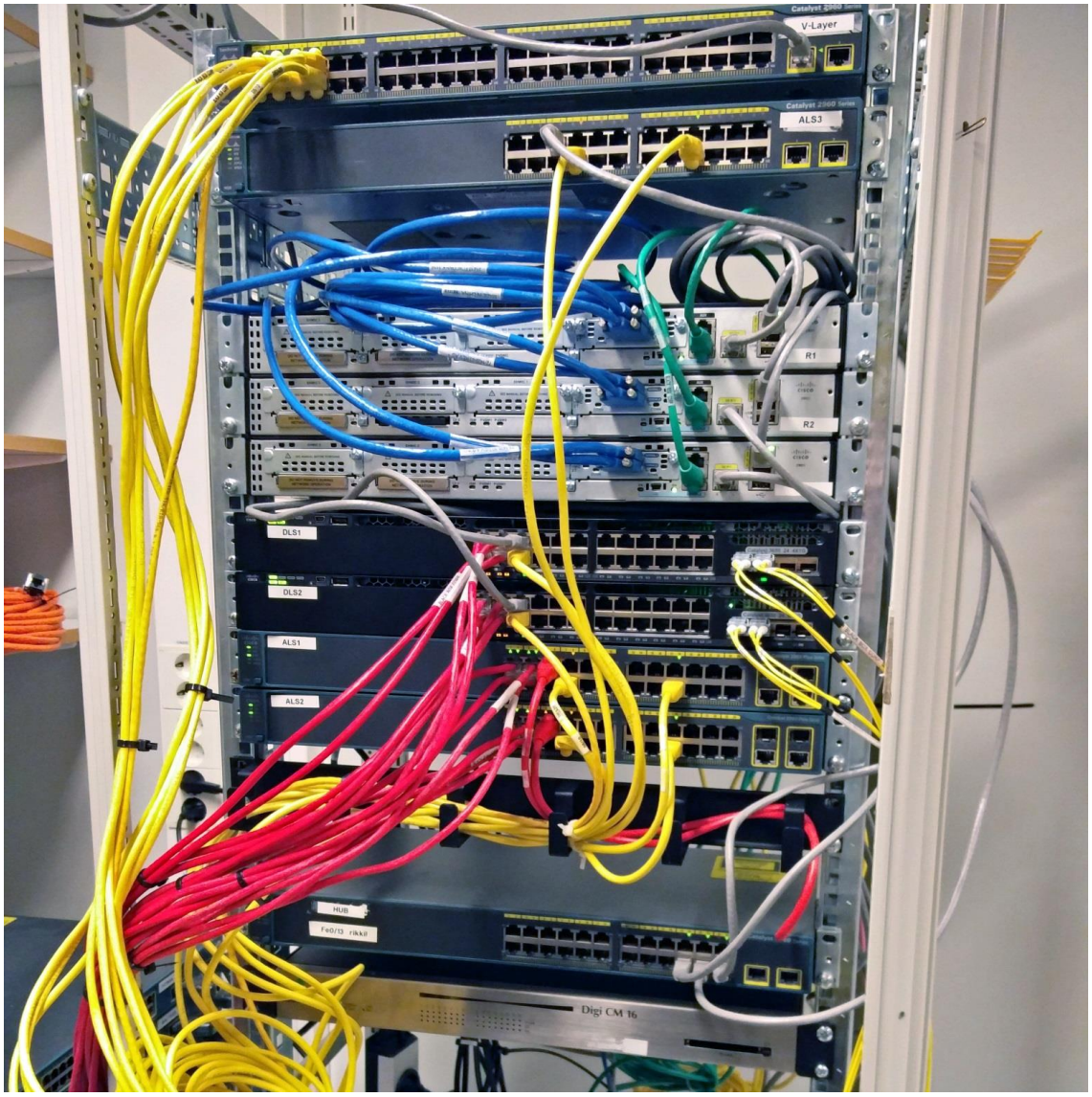
Virtuaalikoneita pyörittävä palvelin, HP ProLiant Gen 5. Suorittaa Windows Server-palvelinympäristön Hyper-V-virtualisointipalvelua, joka mahdollistaa usean päätelaitteen liittämisen yhdestä fyysisestä palvelimesta. Palvelin on yhdistetty fyysisesti WPK-verkkoon ja sen kautta internetiin, sekä VLayeriin. Loogisten liitäntöjen kautta kytketty kaikkiin virtuaaliympäristön kytkimistä (Virtual-PC jne. kuvassa 2)

4.2.2 VLabCon

Konsolipalvelin joka on yhdistetty kaikkiin ympäristön verkkolaitteisiin hallintayhteyden muodostamiseksi, joka toimii konsoliporttien yli. Konsolipalvelin on suorassa yhteydessä WPK-verkkoon, joten autentikoidut käyttäjät voivat yhdistää sen kautta suoraan mihin vaan vLab-ympäristön laitteeseen.

4.2.3 VLayer

Virtuaalikoneiden yhdistyskytkin, joka purkaa yhteyden VLabServiltä virtuaalisen verkkoympäristön laitteisiin. VLayer sisältää vain vähän konfiguraatioasetuksia, ja on suoraan yhdistetty vain VLabServiin, VLabin laitteisiin sekä VLabConiin hallintaa varten. Ylimpänä kuvassa (Kuva 3), ulostuleva johdotus keltaisella, johto VLabServistä harmaalla.



Kuva 3, Fyysinen ympäristö asennettuna WPK-verkon serveritilaan

4.3 Verkkoratkaisut

Itse vLab on WPK-verkosta osioitu erilleen turvallisuus- ja selkeyssyistä. VLayer-kytkin ja ympäristön konsolipalvelin ovat ainoat suoranaiset linkit WPK-verkkoon, ja kumpikaan ei pysty kuljettamaan WPK-verkkoon reititettyä tai kytkettyä tietoa vLabista eikä WPK-verkosta vLabiin. Näin vältetään mahdolliset ongelmatilanteet erilaisista virhekonfiguraatioista, joita Ciscon laboratorioissa tehdään testausmielessä. Näin myöskään WPK-verkko ei voi häiritä testikonfiguraatioita.

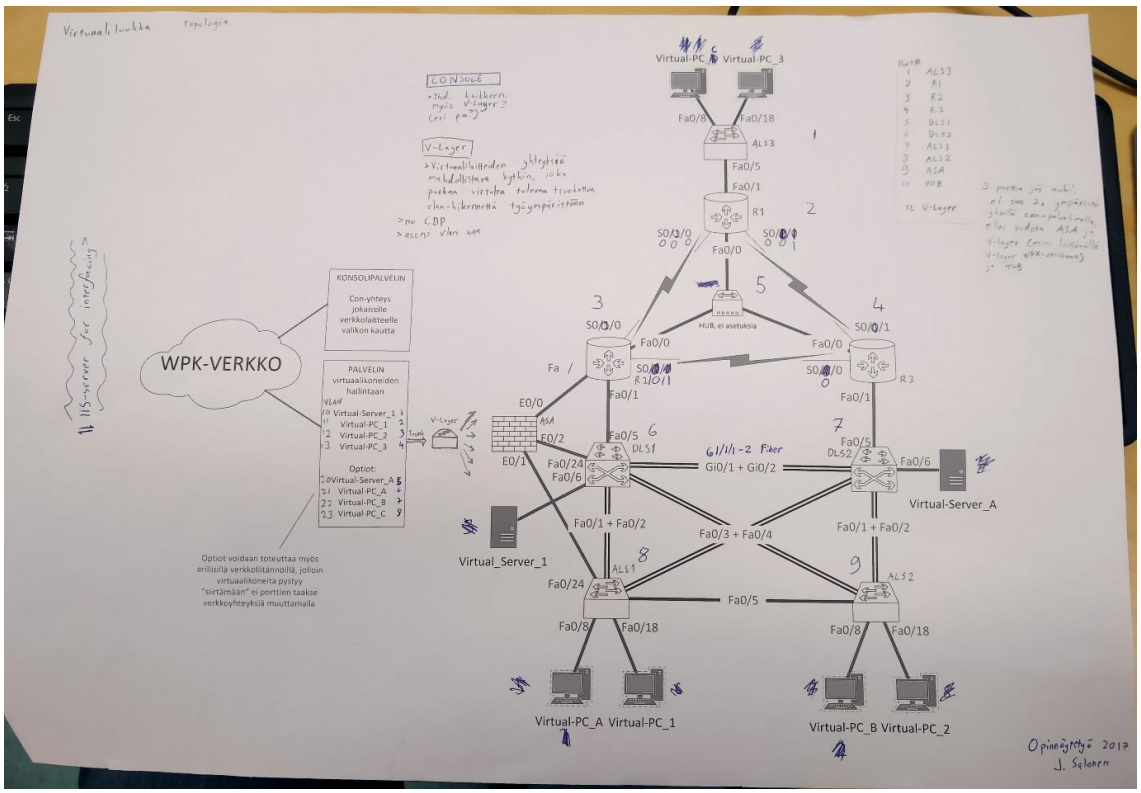
Koska konsolipalvelin on kiinni vain konsoliporteissa, joiden yli verkkoyhteydet eivät voi kulkea, ainoaksi mahdolliseksi virhelinkiksi muodostuu VLayer-kytkin. Tästä syystä VLayeriä ei ole kytketty WPK-verkkoon, vaikkakin se olisi mahdollista tehdä turvallisesti, ja helpottaisi sen hallintaa. Ympäristöturvallisuuden vuoksi VLayerin hallinta suoritetaan laboratorion konsolipalvelimen kautta kuten muidenkin ympäristön laitteiden konfigurointi. VLayeristä on myös kytketty pois päältä kaikki Ciscon omat protokollat ja muut hallintaa auttavat teknologiat, sillä esimerkiksi CDP (Cisco Discovery Protocol) voisi tuottaa ongelmatilanteita, jos laboratorion kytkimet yrittäisivät keskustella VLayerin kanssa.

Käytännössä VLayeriin vain tuodaan yhdellä gigabitin linkillä suoraan VLabServ-virtuaalipalvelimelta kaikkien virtuaalikoneiden yhteydet trunk-yhteyden yli, jotka kaikki ovat eriteltyinä omiin VLAN:eihinsa. Trunk-yhteydellä tässä yhteydessä tarkoitetaan runkoyhteyttä, jossa kulkevaa dataa ei uudelleenkäsitellä eikä muokata kuljetuksen aikana. VLayer purkaa VLAN:it yksitellen portteihin, joten se toimii lähinnä porttilaajennuksena virtuaalikoneiden palvelimelle. Tarvittaessa VLayerille voitaisiin kytkeä rinnan toinen tai kolmas kytkin, jos ympäristöä haluttaisiin laajentaa suuremmaksi, tosin kytkimellä on jo 48 käytettävää porttia, joista kahdeksan on kytketty yhteen kaapilliseen. Pikaisella laskutoimituksella VLayer pystyisi näin yksin tukemaan kuutta kaapillista samoissa konfiguraatioissa, sillä linkit eivät juuri koskaan tule täyttymään maksimeihinsa. Jos virtuaalipalvelimilta lähdettäisiin laskemaan suurta määrää dataa portista toiseen, voitaisiin haluta esim. ylimääräinen gigabitin linkki VLabServ-palvelimen ja kytkimen välille.

4.4 Rakennustyö

Rakennustyö oli suoraviivaista ja onnistui ilman vaikeuksia, ottaen huomioon jo opiskeluajalla hankitun tietotaidon reitityksen ja palvelinten parissa. Tilatun luokkakokoonpanon pohjalta luotiin suunnitelma, joka näytti suurinpiirtein nykyiseltä topologiakuvalta, tosin hieman rujommalta ja käsintehdyltä. Suunnitelma (Kuva 4) perustui pääasiallisesti Ciscon viralliseen koekokoonpanoon, joka sisältää mahdollisimman suuren osan mahdollisista kytkennöistä ja teknologioista yhdessä järjestelmäpinossa.

Tähän suunnitelmaan tuli muutamia muutoksia; mm. ASA-palomuuria ei koettu pakolliseksi ympäristössä, sillä sitä käytetään vain harvoissa tapauksissa, ja sellaista ei löytynyt ylimääräistä käytettäväksi. Myös osa liitännöistä kuvattiin kokonaan uusiksi, sillä uusilla DLS-kytkimillä porttikartoitus tapahtuu muodossa module/slot/port vanhan module/port-muodon sijaan, ja useat portit löytyvät Gigabit Ethernet-tasolla (1gbps duplex) vanhan Fast Ethernetin (100mbps duplex) sijaan. Gigabit-tason portit mahdollistavat yhden gigabitin lähettämisen ja vastaanottamisen yhtäaikaisesti, kun taas vanha Fast Ethernet-standardi on rajoittunut sataan megabittiin sekunnissa.



Kuva 4, Verkon alkuperäinen suunnittelukuva

Ympäristö toteutettiin WPK:n omaan palvelinhuoneeseen, johon on sijoitettu myös useita muita kouluprojekteja, palvelimia ja muita laitteita. Työtä varten käytettiin lähinnä aiemmin valittuja verkkolaitteita – osa laitteista on luokista uusilla korvattuja laitteita, mutta muutamat ympäristön laitteista ovat uusia, esimerkiksi sen DLS-pari. Asennus suoritettiin yhteen palvelinhuoneen vapaista laitehyllyistä. Asennuksen johdotus on pääosin hyllykohtaista. Sekä vLabServ-palvelin että vLabCon-palvelin ovat kytkettyjä kahdennettuun core-kytkimeen (Central2), joten laitekaapista ei tehty monia kytköksiä muihin huoneen johdotuksiin.

Johdotuksen jälkeen suoritettiin laitteiden konfigurointi – konfiguraatio-ohjeet konsolipalvelimelle löytyvät valmistajan omilta sivuilta, ja se onnistuu normaalilla selaimella https-yhteyden yli yhdistämällä konsolipalvelimen IP-osoitteeseen. Konfiguraatiokäyttöliittymässä asetetaan lähinnä autentikaatiopalvelu. Windows-ADFS:n kanssa Kerberos, jota varten saattaa joutua lataamaan erillisen Linux-moduulin toimivuutta varten, jos laitten järjestelmäversio on liian vanha tukeakseen Kerberosta valmiiksi. Tämän jälkeen annetaan vain nimet eri porteille, jonka jälkeen palvelin käynnistetään uudelleen. Uudelleenkäynnistyksen jälkeen laite on valmis käyttöä varten.

Windowspalvelin, jolla virtuaalikoneet pyörivät, on hyvin yksinkertaisesti konfiguroitu. Hyper-V-tuki Windows Server-pohjaisiin palvelimiin löytyy perusominaisuuksista, jonka kytkemisen jälkeen palvelimelle tarvitsi vain asentaa ja kloonata tarvittava määrä virtuaalipalvelimia, jotka kaikki perustuvat LabraVM-koneeseen. Asetuksista määritetään kaikki koneet käyttämään porttia, joka on yhdistetty VLayeriin, ja sen jälkeen tarvitsee vain asettaa jokainen virtuaalikone omaan VLANiinsa.

Näiden toimenpiteiden jälkeen fyysisen ympäristön esittely ja asennus on valmis.

5 VIRTUAALINEN YMPÄRISTÖ

5.1 Esittely

Virtuaalinen ympäristö vLab sisältää kaikki itse verkkoluokkaympäristöä vastaavat tietokoneet ja palvelimet, jotka voivat löytyä eri koekonfiguraatioista. Virtuaalikoneet on toteutettu Windows 7-käyttöjärjestelmällä, ja ne pyörivät VLabServ-palvelimella. Palvelimen käyttöjärjestelmä on Windows Server 2012R2, sillä on luontevaa ajaa Windows-pohjaisia virtuaalikoneita Windows-pohjaiselta palvelimelta.

Windows-pohjaiseen järjestelmään on päädytty Ciscon tarjoamien ohjelmien ja ehdotusten perusteella, vaikka täysin Linux-pohjainen ympäristö olisi huokeampi ja kevyempi laitteistolle. Lisäksi WPK-verkon jo olemassa olevat laitteet ovat lähinnä Windows-pohjaisia, joten saman käyttö vLabissa on luonnollisempaa verkonhallinnan puolella. Näin harjoittelijoilta ei myöskään tarvitse vaatia Linux-osaamista.

Lisäksi Windows-pohjaisen palvelimen kytkeminen WPK-verkkoon mahdollistaa helpon yhdistämisen domain-palveluihin, eikä etäkäytölle tarvita väliin minkäänlaista erillistä ohjelmistoa, sillä Windowsin oma Remote Desktop Connection-ohjelma mahdollistaa helpon etäkäytön lähiverkossa tai VPN:än ylitse.

VLabissa pyörii kahdeksan virtuaalikonetta, joista on suositeltavaa enintään neljän yhdenaikainen käyttö. Tämä johtuu sekä Windowsin raskaudesta virtuaalisenakin koneena että virtuaalipalvelimen tehollisista rajoitteista. Lisäämällä käyttömuistia voitaisiin mahdollistaa kaikkien koneiden yhtäaikainen käyttö perustuen jo saatavilla olevaan tietoon: WPK-verkossa tarjottava yksityinen ”Palopilvi”-virtuaalipalvelinklusteri kykenee ajamaan kahdella vastaavalla palvelimella joissa on reilusti enemmän käyttömuistia ja levytilaa jopa neljääkymmentä Windows-palvelinta samanaikaisesti ilman huomattavaa hidastumista.

5.2 Ylläpito ja sen tarpeet

Ylläpidollisesti vLab ei vaadi uusia toimintatapoja – WPK:n WSUS-palvelin (Windows Server Update Services-päivitysjärjestelmä) hoitaa vLabServin päivittämisen normaalin toiminnan aikana, ja ylläpidon tarvitsee lähinnä asentaa uusi versio LabraVM-virtuaalikoneesta, joka on kaikkien tietojenkäsittelyn verkkolaboratorioiden käytössä oleva virtuaalikonepohja. LabraVM sisältää kaiken Cisco- ja Windows-laboratorioiden käyttöön tarvittavan softan valmiiksi asennettuna, ja sitä käytetään kaikissa muissakin verkkolaboratorioissa TAMKin tietojenkäsittelyssä.

Liite 1 sisältää käyttöohjeet, jotka ovat luotu WPK-harjoittelijoille tämän ympäristön ylläpitotarpeita varten.

5.3 Käyttö ja testaus

Käyttö perustuu lähinnä yhteyteen konsolipalvelimeen ja virtuaalikonepalvelimeen. Konsolipalvelimen kautta kaikkien virtuaaliverkon laitteiden konfigurointi sujuu helposti. Virtuaalikonepalvelimella voidaan suorittaa testausta ja muuta verkkotoimintaa ympäristön pystytyksen jälkeen. Käyttö onnistuu hyvin WPK-verkon sisäpuolella.

Jotta virtuaaliverkkoa voidaan käyttää WPK-verkon ulkopuolella, täytyy käyttäjän ensin kirjautua WPK-verkon VPN-palomuurin läpi verkon sisäpuolelle. Yhdistäminen sujuu Windowsin sisäisellä VPN-sovelluksella antamalla sille WPK-verkon asetukset. Käyttäjät tulee olla sallittuja VPN:än käytölle, joka on yleensä rajoitettu hallintakäyttöön opettajille ja verkon ylläpitäjille. Ajankohtaiset ohjeet Tikas-VPN-koneen käyttöön saa WPK:n ylläpidolta.

Järjestelmän testaukseen sovellettiin kokeisiin sopivia perusasetuksia, joilla varmistettiin ympäristön toimivuus reitityksen, kytkennän sekä reititysprotokollien osalta (OSPF, EIGRP). Käytännössä jokaisella verkkolaitteella liityttiin yhteiseen verkkoon, jota ohjasi automaattinen reititysprotokolla. Tämän jälkeen kaikilta laitteilta tehtiin yhteyskokeilu jokaiseen toiseen laitteeseen ping-työkalun avulla. Batch-pohjaisesti suoritettuna ping on serialisoitu testi, jossa laite käy yksi kerrallaan jokaisen yhteyden läpi, lähettäen muutaman testipaketin joihin toinen laite onnistuneessa tapauksessa vastaa.

6 JATKOKEHITYS

Jatkokehityksellisestä näkökulmasta työ tukee hyvin sen parantamista – järjestelmä on suunniteltu alustapitäen toimimaan yksittäisenä esimerkkikappaleena, jota olisi mahdollista joko kasvattaa tai jatkaa ilman suurempia ongelmia. Tämän mahdollistaa skaalautuva ympäristövalinta ja yhteyssuunnittelu, sillä useampia palvelimia voidaan kytkeä VLayeriin kiinni, ja sen kaltaisia kytkimiä voidaan linkittää useita yhteen sarjaan ilman konfiguraatiomuutoksia.

Ympäristöä voitaisiin aluksi helposti jatkaa suuremmaksi ja tehokkaammaksi kasvattamalla palvelimen fyysistä ja talletusmuistia, mahdollistaen näin ehkä kaapilla tai parilla kasvattamista ilman uudempien palvelimien hankkimista. Ympäristö voitaisiin myös sisällyttää jo WPK-verkossa olevan yksityisen pilvipalvelun Palopilven alle, joka on Microsoft Azure-pilven kaltainen ratkaisu toteutettuna paikallisilla koneilla. Siirto yksityiseen pilveen mahdollistaisi suuren käyttökapasiteetin, mutta toisi myös uusia ongelmia mm. virtuaalikoneiden VLAN-verkottamisen ja liittämisen fyysisiin laitteisiin.

Ympäristö on myös tällä hetkellä vaikea ajoittaa tietyn henkilön tai henkilöiden käyttöön – laitteet eivät varoita, jos useampi käyttäjä on kirjautuneena, joka mahdollistaa vahingollisen päällekävelyn jossa toinen käyttäjä sotkisi ensimmäisen käyttäjän konfigurointityön omallaan. Helpoin ratkaisu olisi sisällyttää virtuaaliverkkoluokka nykyiseen luokkatilajärjestelmään, jotta ympäristö voitaisiin varata tietyn luokan tai henkilön käyttöön samalla tavalla kuin normaalitkin luokkatilat.

Mielekkäämpi ratkaisu olisi toteuttaa eräänlainen portaalisivusto joka voisi pyöriä esim. päävirtuaalipalvelimen päällä, ja sisältäisi ajanvaraus- ja hallintamahdollisuudet sekä pikalinkit virtuaalikoneisiin. Tämä helpottaisi ympäristön käyttöä, jos portaalin avaamalla voisi helposti nähdä onko joku käyttämässä laitteita. Portaalissa voisi myös olla reboot-mahdollisuus, joka komentaisi virransyöttöä käynnistämään laitteet uudestaan, alustaen näin ympäristön uutta työskentelyä varten.

7 POHDINTA

Työ on hieman epätavallinen, sillä nykyään siirretään paljon tuotteita kokonaan pilveen, ja työn tuotteen kaltaista hybridiympäristöä tuskin löytyy muualta. Tämä johtuu siitä, että verkkolaitteet ovat kallein osa tämänlaista luokkaympäristöä, ja tässä ympäristössä ne löytyvät fyysisinä eikä virtualisoituina laitteina. Tämä mahdollistaa tarkemman oikean elämän kokemuksen kartuttamisen, sillä fyysisillä laitteilla saattaa tulla erilaisia erikoistapauksia vastaan, joihin virtualisoiduilla klooneilla ei koskaan törmäisi.

Yleisesti ottaen opinnäytetyöni kuitenkin vastasi jotenkuten pääasiallista osaamisaluettani – verkkoteknistä työskentelyä. Kuitenkin verrattuna myöhempiin opintoihin työn tuotteen rakentaminen oli matala haastetasoltaan, tosin varsin vapaasti suunniteltava ja oma-aloitteellinen, joka oli luonteeltaan toisenlaista kuin opintokurssien ohjauksellisesti tuotetut työt.

Kaikenkaikkiaan työ oli mielestäni ihan yleishyödyllinen, tosin hankala kirjoituksen kohde – suurin osa työn materiaalista on lähteistetty suoraan oppimateriaalista tai ohjekirjoista, sillä järjestelmä ei varsinaisesti vaadi mitään erityisosaamista sen tuottamiseen. Satuin miettimään useaan kohtaan työn järkevyyttä, mutta puolen vuoden jälkeen en itse halunnut enää vaihtaa aihetta, ja työmotivaatio raportin kanssa työskentelyyn väheni huomattavasti työllistyttyäni.

Raportin tuottamiseen, vaikkakin lyhyt onkin, kului yli 500 työtuntia. Työn rakentamiseen, dokumentoinnin tuottamiseen ja ohjeistamiseen kului noin 60 tuntia. On vaikeaa työskennellä ’luovan’ työn kanssa joka tuntuu täysin turhalta. Jälkikäteen mietittynä työni olisi pitänyt olla huomattavasti haastavampi projekti, jonka raportin luova tuottaminen olisi tuntunut haastavammalta, arvokkaalta tai edes hieman kiinnostavalta.

LÄHTEET

Cisco 2018. Understanding and Configuring VLANs. Luettu 1.5.2018. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html

Koulutus.fi. CCNA-tutkintoon tähtäävä valmennus, Santa Monica Networks. Luettu 8.10.2017. https://www.koulutus.fi/koulutukset/santa-monica-networks/cisco-ccent-ccna-tutkintoon-tahtaava-valmennus-407658

Wikipedia 2018a. Secure Shell. Luettu 1.5.2018. https://en.wikipedia.org/wiki/Secure_Shell

Wikipedia 2018b. Telnet. Luettu 1.5.2018. https://en.wikipedia.org/wiki/Telnet

LIITTEET

Liite 1. Käyttöohjeet 1 (3)

Lyhyesti:

Mikä V-Lab?

V-Lab on Virtuaalinen verkkoluokkaympäristö joka koostuu VM-palvelimesta (VLabServ), konsolipalvelimesta (VLabCon), virtualisointikytkimestä (V-Layer) sekä fyysisestä Cisco:n koe-ympäristöstä. Kaikki kyseinen komeus sijaitsee WPK-verkon serverihuoneessa C3.

Mihin tätä käytetään?

V-Labin tarkoituksena on mahdollistaa Ciscon verkkolabrojen etäsuorittaminen ilman ympäristön täyttä virtualisointia, näin mahdollistaen kevyen ja todenmukaisen työskentelyn. Todennäköisesti tätä tulee käyttämään lähinnä opettava henkilökunta kokeiden ym. valmisteluun kotoa tai toimistosta.

Miten tätä käytetään?

Easy. Yhdistä VLabCon:iin ja VLabServ:iin ja aja ympäristöä kuin normaalissakin verkkoluokassa. Suosittelen käyttämään lähinnä cisco/cisco tai cisco/class-tunnuksia, sillä fyysisen verkon uudelleenkäynnistys vaatii serverihuoneeseen pääsyä. Reitittimet ja reitittävät kytkimet (R1-3, DLS1-2) ovat rekisterimoodissa 0x2142 ja eivät näinollen lue startup-configia. Pois ja päälle kytkeminen riittää resetoimiseen.

Huom!

Uuden tyypin IOS sis. kertakäyttöiset tunnukset cisco/cisco joilla logataan sisään. Esim. tämänhetkiset R1-R3 ovat tälläisiä, ja nuo tunnukset on tosiaan kertakäyttöiset. Jos timeouttaat tms. tavalla putoat konsoliyhteydestä, laitteita ei saa auki ilman sähköresettiä. Vaihda tunnukset aina!

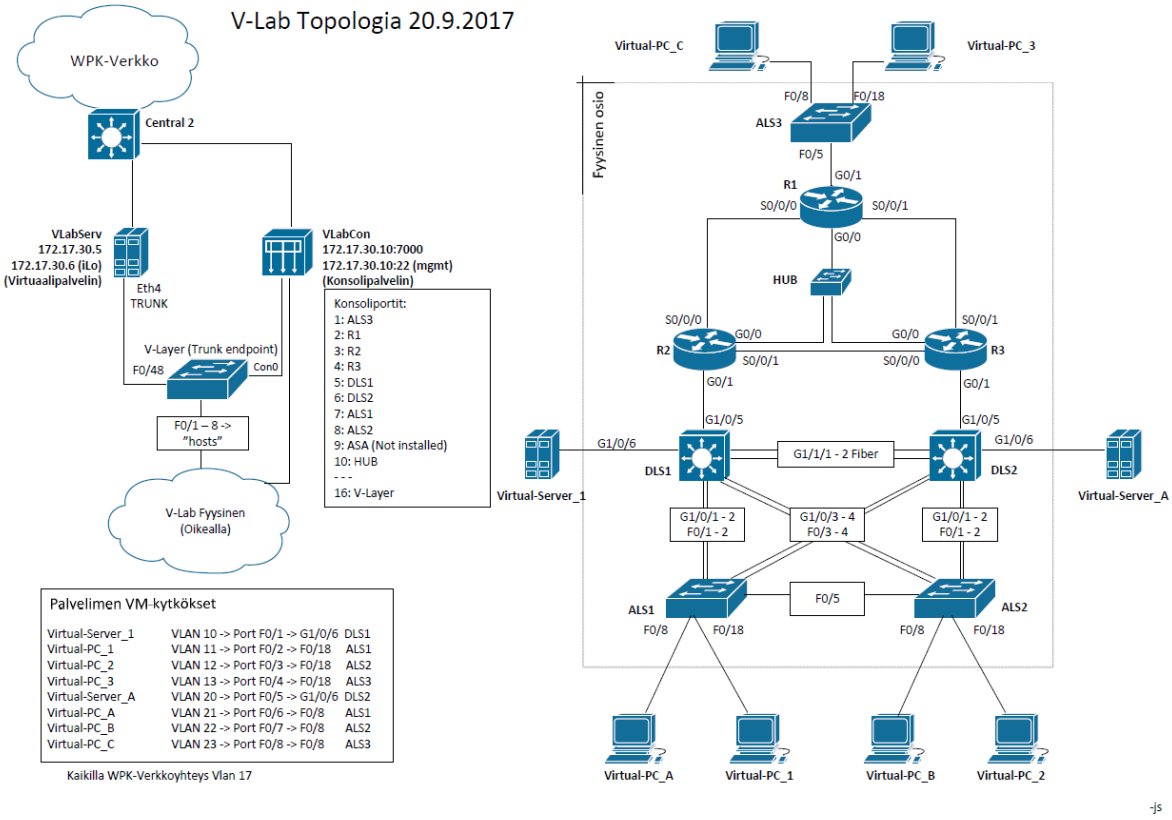
Topologiasta

V-Labin käyttäjälle tärkeimmät laitteet ovat VLabServ (virtuaalipalvelin), VLabCon (konsolipalvelin) ja V-Layer (trunk-kytkin).

VLabServ:in kautta hoituu kaikki virtuaalikoneiden hallinta, niiden käynnistely, kontrollointi ja sammuttelu ym.

VLabCon on taas kiinni kaikkien laitteiden konsolikytkeinnöissä, joten sillä voidaan kontrolloida kaikkia ympäristön reitittäviä ja kytkeviä laitteita, muk.luk. V-Layer:iä.

V-Layer toimii trunk endpointtina - VLabServ:istä kulkee trunk-kytkentä V-Layeriin, jonka sisällä kulkevat kaikki virtuaalikoneet eriteltyinä VLAN:eissa. V-Layerin hallinta voidaan suorittaa VLabConin kautta, jos ympäristöön tarvitsee tehdä muutoksia.



VLab Topologia Sharepoint link, full resolution PDF

Käyttö

Kts. Topologia ensin. VLabServ ja VLabCon ovat lisättynä Palo10:n DNSään, joten niihin voi yhdistää suoraan nimellä (esim. FQDN vlabserv.wpk.tpu.fi tai lyhyesti vlabserv) kaikilta domainin koneilta.

VLabServ

VLabServ on Windows 2012R2-serveri jolla pyörii Hyper-V:n päällä kaikki ympäristön 'tietokoneet'. Yhdistä Remote Desktopilla ja käytä kuin normaalia luokkakonetta, Hyper-V Managerista kannattaa laittaa pois päältä tai pauselle kaikki laitteet joita ei välittömästi tarvitse - serverillä ei ole loputtomasti RAMia.

Eth1 syöttää WPK-verkkoa Central 2:sesta, iLo-portti on kytketty omaan porttiinsa ja Eth4 trunkkaa Hyper-V:n virtuaalikoneiden ympäristöportit V-Layerille.

VLabCon

VLabCon on normaali konsolipalvelin kuten luokassa C4-03 olevatkin ovat. Siltä löytyy sama lokaali root-käyttäjät, ja se tarkistaa käyttäjätilit Kerberoksella Palo10/Palo11-palvelimilta. Hallinta HTTPSn yli niinkuin normaalistikin, käyttää samaa salasanaa kuin muutkin vastaavat laitteet.

V-Layer

V-Layer on 48-porttinen kytkin joka trunkaa VLabServiltä tulevaa liikennettä ympäristön laitteille. Siitä on kytketty pois kaikki mahdollinen (cdp ym.) jotta se olisi mahdollisimman 'läpinäkyvä' ympäristölle. Serveriltä tulee valmiiksi vlanitettua dataa jonka V-Layer vain jakaa yksittäisille porteille.

Jos välttämättä haluaa ettei reitittimellä/kytkimellä näy up/up yhteydessä jonka ei pitäisi olla päällä, V-Layeriltä voi käydä sammuttamassa portin erikseen. Tämä kuitenkin luo ylimääräisen virhemahdollisuuden ellei käyttäjä muista käydä avaamassa porttia järjestelmän käytön jälkeen, joten se ei ole suositeltavaa.

Muut laitteet ja käytännöt

Ei pitäisi joutua sanomaan erikseen, mutta normaalit verkkoluokka-käyttöohjeet pätevät myös VLabiin: Muista siivota jälkesi käytön jälkeen ja käytä vain cisco/cisco, cisco/class tai admin/salasana-yhdistelmiä.

Huolto ja ylläpito

> Pidä VLabServ päivitettynä (WSUS ja reboot aina välillä)

> Päivitä LabraVM myös VLabServillä jos LabraVM päivitetään luokissa

> Varmuuskopioi V-Layer jos teet pysyviä muutoksia konfiguraatioon (esim. lisäät laitteita