Tietoliikenneasiantuntijan päiväkirja

Tatu Anttila

Haaga-Helia ammattikorkeakoulu
Tradenomi, tietojenkäsittely
Amk-opinnäytetyö
2023

Tiivistelmä

Tekijä(t)
Tatu Anttila

Tutkinto
Tradenomi, Tietojenkäsittely

Raportin/Opinnäytetyön nimi
Tietoliikenneasiantuntijan päiväkirja

Sivu- ja liitesivumäärä
48

Opinnäytetyö on tehty päiväkirjamuotoisena. Opinnäytetyön tarkoituksena on kuvailla tietoliikenneasiantuntijan työtehtäviä. Opinnäytetyön luvut koostuvat neljästä luvusta, joista ensimmäisessä lukijalle kuvaillaan opinnäytetyön kannalta oleellisia tietoja, kuten toimenkuva ja käsitteet.

Toisessa luvussa kuvaillaan lähtötilannetta, eli omaa osaamista ja kehittymisen tarpeita ennen seurantajaksoa. Toisessa luvussa käydään läpi myös tarkemmin missä työtehtävissä työskenneltiin, minkälaisessa työympäristössä, sekä minkälainen osaamisen taso oli seurantajakson alussa.

Kolmannessa luvussa seurataan tietoliikenneasiantuntijan työtehtäviä kahdeksan viikon ajalta. Päiväkirjamerkinnöissä keskitytään työtehtävien sisältämiin ongelmiin ja niihin saatuihin ratkaisuihin. Päiväkirjamerkintöjen lisäksi jokaisella viikolla on erillinen viikkoanalyysi, jossa keskitytään viikon aikana, tai edeltävillä viikoilla kohdattuihin ongelmiin, tai tekniikkoihin. Viikkoanalyysin tarkoituksena on kuvailla ammatillista kehittymistä viikon ajalta.

Neljäs luku on pohdinta, jossa käydään läpi ammatillinen kehittyminen, sekä reflektoidaan omaa onnistumista opinnäytetyöprosessissa. Pohdinnassa verrataan lähtötilanteessa ollutta ammattitaitoa seurantajakson jälkeiseen ammattitaitoon. Pohdinnassa käydään läpi myös, miten opinnäytetyötä on pystytty hyödyntämään työtehtävissä, sekä miten omaa osaamista voidaan kehittää myös tulevaisuudessa.

Asiasanat
Tietoliikenne, tietoverkot, tietoturva

Sisällys

1 Johdanto

Tämä opinnäytetyö on tehty työpäiväkirja muotoisesti. Työpäiväkirja on tehty tietoliikenneasiantuntijan tehtävistä yrityksessä A. Päiväkirjamerkintöjen aikaväli on 21.08.2023 – 20.10.2023, eli päiväkirja tulee seuraamaan työtehtäviä kahdeksan viikon ajalta ottaen huomioon mahdolliset vapaapäivät ja sairastumiset.

Yritys A on riippumaton IT-integraattori, asiantuntijatalo ja ratkaisutoimittaja. Työtehtävät työpäiväkirjan ajalta koostuvat erilaisista asiakkaiden tukipyynöistä, sekä erilaisista asiakasprojekteihin liittyvistä tehtävistä. Työympäristönä toimivat yrityksen toimisto, sekä hybridimallia käyttäen myös oma koti. Joissakin asiakasprojekteissa työympäristönä toimii myös asiakkaan tilat.

Työtehtävissä tarvitaan perusosaamista ICT-alalta, sekä tietoliikenteestä. Koska kaikki työtehtävät liittyvät jollain tasolla tietoliikenteeseen, työtehtävistä selviytymiseen vaaditaan osaamista eri laitevalmistajien tuotteista, ja konfiguraatioista. Tietoturvallisuuden ymmärtäminen on tärkeää työtehtävien kannalta, sillä osa ympäristöistä, joissa työskennellään, saattavat olla kriittisiä ja salattuja ympäristöjä.

Koska työtehtävät koostuvat pääsääntöisesti asiakkaiden lähettämistä tukipyynnöistä, sekä asiakasprojekteista, on tärkeää omata hyvät asiakaspalvelu- sekä vuorovaikutustaidot. Tilanteissa, joissa asiakas ei ole kovin tekninen, on hyvä osata selittää teknisiä asioita myös yksinkertaistettuna yleiskielellä, että se on myös heidän ymmärrettävissä.

Ammatillisen kehittymisen tavoitteet kohdistuvat tietoverkkojen puolelle. Pyrin kehittämään osaamistani eri laitevalmistajien tuotteiden parissa, sekä ymmärtämään tietoverkoissa käytettäviä tekniikkoja. Tietoturva osaamisen puolesta kehittyminen tulee tapahtumaan tietoverkkojen sivussa, enkä todennäköisesti tule keskittymään siihen enempää kuin tietoverkkoihin.

1.1 Keskeiset käsitteet

CWDM = Coarse wavelength division multiplexing, valokuitutekniikassa käytettävä valon aallonpituuksien kanavointitekniikka.

DWDM = Dense wavelength division multiplexing, valokuitutekniikassa käytettävä valon aallonpituuksien kanavointitekniikka.

GUI = Graphical User Interface, graafinen käyttöliittymä johonkin tietokoneeseen tai laitteeseen.

Hyppykone = Erillinen kone, joka sijaitsee asiakasverkossa. Tämän koneen kautta siirrytään asiakkaiden verkkolaittelle, jotka sijaitsevat asiakkaan sisäverkossa.

Optiikka = Erillinen laite, joka laitetaan kytkimeen tai reitittimeen kiinni. Optiikan avulla voidaan kytkeä valokuitukaapelin tai Ethernet-kaapelin kiinni laitteisiin.

PoE = Power over Ethernet, verkkokaapelin läpi syötettävä sähkövirta kytkimestä siihen kytkettyihin laitteisiin.

RMA = Return Merchandise Authorization, numeroitu tunnus, jonka valmistaja myöntää laitteille niiden rikkoutumisen varalta. Rikkoutunut laite joko korjataan, tai tilalle lähetetään uusi korvaava laite.

TAC = Technical Assistance Center, laitevalmistajan tarjoama tukipalvelu.

Tiketti = Tukipyyntö, jonka asiakas lähettää yrityksen järjestelmään.

VLAN = Virtual Local Area Network, fyysisestä lähiverkosta jaettu looginen aliverkko.

VRRP = Virtual Router Redudancy Protocol, eli virtuaalisen reitittimen luomiseen käytetty protokolla.

2 Lähtötilanteen kuvaus

Työskentelen yrityksessä A tietoliikenneasiantuntijan roolissa. Yritys A on riippumaton IT-integraattori, asiantuntijatalo, ja ratkaisutoimittaja. Yritys A tekee tietoverkkoja, tietoturva- ja kyberturvallisuusratkaisuja, sekä tuottaa näihin liittyvää konsultointia ja muita palveluja.

2.1 Oman nykyisen työ analysointi

Ennen kuin aloitin päiväkirjan seurantajakson, minulle oli kertynyt tietoliikenteenalan kokemusta noin kahdeksan kuukautta. Työtehtäväni koostuvat pääsääntöisesti tuki- ja muutospyynnöistä, hallinnasta, kouluttautumisesta, sekä vaihtelevasti myös asiakasprojektitehtävistä. Kaikki tehtävät ovat jollain tavalla tietoliikenteen tehtäviä, eli tietoverkkoja sekä tietoturvaa. Työympäristöni koostuu enimmäkseen organisaation tiketöintijärjestelmästä, hallintajärjestelmistä, sekä laitevalmistajien tukiportaaleista. Samassa työtehtävässä on kaksi muutakin kollegaa, ja pyynnön mukaan, myös organisaation muut asiantuntijat hoitavat näitä tuki- ja muutospyyntöjä. Työtehtävän mukaan työtehtävät voidaan hoitaa hybridimallin mukaisesti joko toimistolta tai kotoa, sekä myös tarvittaessa asiakkaan tiloissa.

Työtehtävistä selviytymiseen tarvitaan perustason osaamista tietoliikenteestä sekä ICT-alalta. Koska organisaatiossa on käytössä useiden eri laitevalmistajien laitteita, tarvitaan vahva halu oppia uutta. Myös vuorovaikutustaidot ovat olennainen osa työtehtävistä suoriutumista, sillä tehtävissä ollaan tiiviisti yhteydessä asiakkaisiin, kollegoihin, ja muihin sidosryhmiin.

Tarvittavaa osaamista olen hankkinut alkujaan koulun kursseilla, jotka olivat Ciscon CCNA-kurssin osia. Työskennellessä olen opiskellut eri laitevalmistajien konfiguraatioita, sekä perustason osaamista. Suoritin aiemmin töideni ohella Juniperin JNCIA-Junos sertifikaatin, joka on associate-tason sertifikaatti. Olen myös opiskellut JNCIS-ENT sertifikaattia varten, joka on specialist-tason sertifikaatti yritysverkkojen osaamisesta.

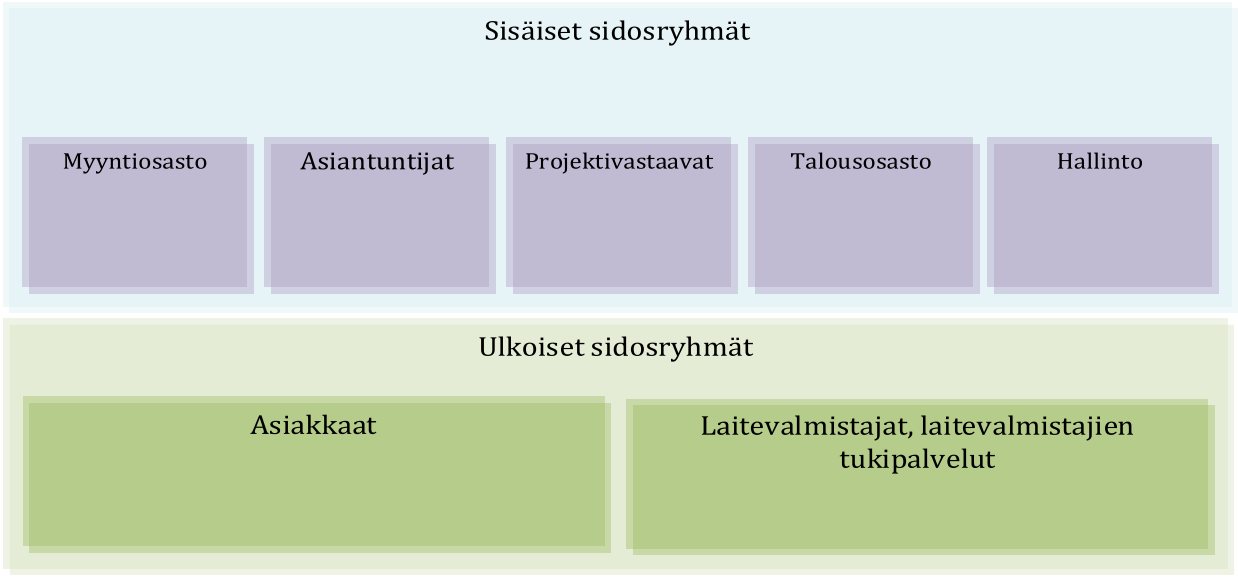
Ammatillinen kehittymiseni on toistaiseksi alkuvaiheessa. Olen työskennellyt alalla vain noin kahdeksan kuukautta, ja kehittämistä on vielä todella paljon. Jatkossa tulen panostamaan enimmäkseen tietoliikenteeseen, keskittyen reitittimiin ja kytkimiin. Pyrin myös kehittymään tietoturvan alueella. Tietoturva ja tietoliikenne ovat hyvin paljon kytköksissä toisiinsa, joten molempien osaamista tulee kehittää.

Jatkossa minun tulee panostaa oppimaan tehokkaasti tietoturvasta sekä tietoliikenteestä. Laitevalmistajien käyttöliittymät ja käyttöjärjestelmät tulisi ottaa hyvin haltuun, jolloin ammatillinen kehittymisenikin kasvaa. Mitä enemmän opin eri asioista, ja mitä syvemmin tutkin niitä, sitä paremmat mahdollisuudet ovat kehittyä urallani, sekä saada haastavampia työtehtäviä.

Oma osaaminen seurantajakson alussa suhteessa työtehtävien suoritusvaatimuksiin on hyvä. Seurantajakson alkuun mennessä olen ehtinyt oppimaan suurimman osan työtehtävistäni, mutta välillä tulee kuitenkin tehtäviä, joissa tulee vastaan haasteita. Toistaiseksi tehtävät ovat olleet sopivan haastavia, jolloin olen päässyt kehittymään, eikä vastaan ole tullut vielä ylitsepääsemättömiä ongelmia. Suurimman osan työtehtävistäni pystyn suorittamaan itsenäisesti, mutta tehtävästä ja ongelmasta riippuen saatan tarvita yrityksen muiden kokeneempien asiantuntijoiden tukea.

Koen tässä vaiheessa työsuhdettani osaavani tietoliikenteestä riittävästi osaamisvaatimuksiin nähden. Olen oppinut tekemään suurimman osan työtehtävistäni itsenäisesti, ja hyvin harvoin kohtaan työtehtäviä, joihin tarvitsen kokeneemman asiantuntijan tukea.

2.2 Sidosryhmien esittely



Kuva 1. Havainnollistava kuva sidosryhmistä.

Kuvan 1 mukaisesti, sisäisiä sidosryhmiä työssäni ovat myyntiosasto, asiantuntijat, projektivastaavat, yrityksen talousosasto, ja hallinto. Näistä tärkeimpänä omalta osalta ovat asiantuntijat, joihin itsekin kuulun. Asiantuntijoiden intressinä työssäni ovat asiakkaiden tarpeiden täyttäminen, oli se sitten suunnittelua, tukipalveluiden tarjoamista, konfigurointia tai konsultointia. Projektivastaavien intresseinä ovat asiantuntijoiden allokointi erinäisiin projekteihin, sekä toimia asiakkaiden ja asiantuntijoiden välissä olevana tekijänä. Talousosaston intresseinä ovat yrityksen menestys ja voitontavoittelu. Hallinnon intresseinä ovat yrityksen johtaminen.

Ulkoisia sidosryhmiä ovat asiakkaat, laitevalmistajat, sekä laitevalmistajien tarjoaman tukipalvelun henkilöt. Asiakkaiden intresseinä ovat yritykseltä tilatut palvelut erilaisissa muodoissa. Laitevalmistajien intresseinä ovat laitteiden myyminen, sekä tukipalveluiden tarjoaminen.

2.3 Työpaikan vuorovaikutustilanteet

Vuorovaikutustilanteet työpaikalla toteutetaan enimmäkseen sähköisesti. Toimistolla ollessani saatamme kuitenkin muiden tukipalvelussa työskentelevien kanssa keskustella tukipyynnöistä ja muista projekteista myös kasvotusten. Yrityksen viestintäkanavina toimivat pääsääntöisesti Microsoft Teams, Outlook, sekä Signal-applikaatio. Yrityksessäni Outlookiin, Teamsiin ja Signaliin on kaikkiin luotu osastokohtaiset ryhmät, sekä yrityksen yhteinen kanava. Outlookin kautta tapahtuu suurin osa asiakkaiden kanssa käydyistä vuorovaikutustilanteista, ja Teamsin avulla on helppoa palaveerata sidosryhmien kanssa. Signalia käytetään yrityksen sisäiseen informaation välitykseen Outlookin ohella.

Ulkoisien sidosryhmien vuorovaikutustilanteet tapahtuvat pääsääntöisesti erilaisien alustojen kautta. Esimerkiksi asiakkaiden kanssa viestiminen toteutetaan yleensä organisaation tiketöintijärjestelmän kautta, johon on liitetty tukipalvelumme sähköposti. Asiakkaiden kanssa saatetaan harvemmin keskustella myös suoraan sähköpostitse omalla sähköpostiosoitteella, tai puhelimitse. Laitevalmistajien tukipalvelun henkilöstön kanssa vuorovaikutustilanteet tapahtuvat pääsääntöisesti laitevalmistajien omissa verkkopalveluissa.

3 Seurantajakson raportointi viikkoanalyyseineen

Tässä luvussa seurataan työtäni tietoliikenneasiantuntijana, sekä ammatillista kehitystä seurantaviikkojen aikana. Seurantaviikkojen aikaväli on 21.08.2023 – 20.10.2023, eli kahdeksan viikkoa.

3.1 Seurantaviikko 1

Maanantai 21.08.2023

Viikko alkoi asiakkaan tukipyynnöstä uusien palvelimien pääsemiseen verkkoon. Asiakkaalla on ympäristössään Palo Alto Networksin VM (Virtual Machine) -tyyppiset palomuurit käytössä. Ongelmana oli siis se, että asiakkaalla oli testissä uuden web-pohjaisen palvelimen käyttö, eikä nykyiset palomuurisäännöt sallineet liikennettä sen suuntaan. Palo Alto Networksin palomuureilla pystyy konfiguroimaan myös GUI:n (Graphical User Interface) avulla, joten avasin sinne ohjaavan verkkosivun. Aloitin luomaan uutta sääntöä, jossa haluttiin, että Global Protect VPN (Virtual Private Network) -verkosta pääsisi kaksi nimettyä henkilöä liikennöimään testipalvelimen suuntaan. Asetin ilmoitetun lähdeosoitteen, kohdeosoitteen, sekä käyttäjät, jotka pääsisivät liikennöimään palvelimelle. Lopuksi vielä suoritin ja tallensin muutokset, ja kysyin asiakkaalta varmistusta säännön onnistumisesta, eli pääsivätkö he liikennöimään palvelimelle. Liikennöinti palvelimelle onnistui, ja suljin tiketöintipalvelusta kyseisen tapauksen.

Tiistai 22.08.2023

Tiistaina tuli aamupäivän aikaan tukipyyntö asiakkaalta Ciscon kytkinten keskusteluun liittyen. Kontekstina tähän, että asiakkaalla on rakentumassa uusi suuri ympäristö, jossa kytkimiä on todella paljon. Yksi kyseisen ympäristön access-tason kytkimistä ei pystynyt keskustelemaan aggregointikytkimen kanssa. Aloitin purkamaan ongelmaa tarkistamalla kytketyn portin tilan aggregointi kytkimellä ajamalla komennon *”show running-config interface TwentyFiveGigE x/x/x”* , ja huomasin kyseisen portin olevan suspended tilassa. Uplink-porteissa käytetään tässä ympäristössä LACP (Link Aggregation Control Protocol) -protokollaa, joka aggregoi useamman portin samaan kaistaan. Asetin portin shutdown tilaan, ja nostin uudelleen ylös, jonka jälkeen etsin logeista syytä siihen, minkä takia portti menee suspended tilaan. Komennolla *’’show log last 50”* huomasin virherivin, joka kertoi minulle, että *”Twex/x/x/x suspended: LACP currently not enabled on the remote port.”.* Tämä kertoi minulle, että access-kytkimeltä puuttui LACP konfiguraatiot porteilta. Purin port-channel konfiguraatiot aggregointikytkimeltä komennolla *’’no channel-group X”*, jolloin pääsin käsiksi access-kytkimeen. Access-kytkimellä loin port-channel konfiguraatiot porteille, jotka olivat yhteydessä aggregointikytkimeen komennolla *’’channel-group x mode active”*, ja menetin yhteyden kytkimeen sen jälkeen. Aggregointi-kytkimen päässä loin uudelleen port-channel konfiguraatiot vastaavalla

tavalla, jolloin portti nousi normaaliin tapaan ylös, ja liikennöinti kytkinten välillä onnistui. Normaaliin tapaan kirjoitin lopuksi wr, eli write memory, joka kopioi käynnissä olevan konfiguraation myös käynnistäessä ladattavaan konfiguraatioon.

Keskiviikko 23.08.2023

Keskiviikko jatkui samalla tyylillä tiistain kanssa, sillä samalta asiakkaalta tuli porttimuunnoksia koskeva tukipyyntö. Asiakkaalla on ympäristössään useita eri VLAN (Virtual Local Area Network) -verkkoja käytössä, ja hän halusi yhdelle access-kytkimistä asettaa näitä. Siirryin etäyhteyden avulla kyseiselle kytkimelle, ja aloin konfiguroimaan haluttuihin portteihin haluttuja VLAN-verkkoja. VLAN-verkot tulevat kytkimelle VTP (Vlan Trunking Protocol) -protokollan avulla aggregointikytkimeltä. VLAN-verkkoja ei kuitenkaan tässä tapauksessa ollut valmiina kytkimellä, sillä VTP-konfiguraatio puuttui, tämän totesin komennolla *”show vtp status”*. Asetin konfiguraatioon oikean VTP domainin komennolla *”vtp domain x””*, version komennolla *”vtp version x”*, sekä salasanan komennolla *”vtp password x”*, jolloin vlanit ilmestyivät myös tälle kytkimelle. VLAN-verkkojen ilmestyttyä siirryin halutuille porteille. Koska portit eivät vielä olleet switchport access tilassa, asetin sen komennolla *”switchport mode access”*, jonka jälkeen asetin halutun vlanin kullekin portille komennolla *”switchport access vlan x”*. Tuttuun tapaan lopetin työn kirjoittamalla wr, kun olin tarkistanut konfiguraatiot pyydetyiksi.

Torstai 24.08.2023

Torstai oli tällä viikolla hiljaisempi päivä, ja tukipyyntöjä saapui minulle vain yksi. Asiakkaalta oli rikkoutunut yksi CWDM10G-1940-MIN optiikka. Optiikka on moduuli, joka kiinnitetään reitittimeen tai kytkimeen. Optiikkojen avulla voidaan muuntaa Ethernet-signaalit valopulsseihin, joita kulkee valokuitujen sisällä, ja päinvastoin. Se toimii lähettäessä, sekä vastaanottaessa. Pyysin asiakasta lähettämään viallisen optiikan meidän suuntaamme, jonka jälkeen ohjaamme sen korjaukseen, tai korvattavaksi valmistajalle. RMA (Return Merchandise Authorization) -prosessit ovat yleisesti hyvin yksinkertaisia ja nopeita itse tekemisen suhteen, mutta korvaavia osia saattaa joutua odottamaan riippuen kiireellisyydestä. Sähköpostia hyödyntäen ilmoitin valmistajalle rikkoutuneesta osasta, ja jäin odottamaan osaa meille.

Perjantai 25.08.2023

Perjantai oli melko samanlainen päivä torstain kanssa, sillä vain yksi tukipyyntö saapui minulle. Kyseessä oli jälleen RMA-tapaus, mutta tällä kertaa laite oli kriittisessä konesaliympäristössä hajonnut Juniperin MX204-reititin. Yrityksemme tarjoaa osalle asiakkaista varaosapalvelua, eli säilytämme vastaavaa laitetta meillä, jotta vikatilanteen sattuessa laite saataisiin mahdollisimman nope-

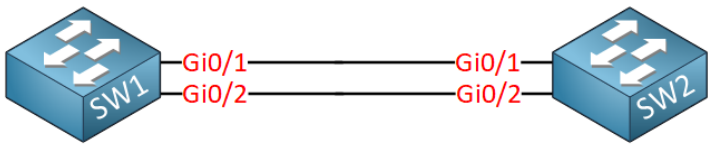
asti korvattua, ja asiakkaan tuotanto ei kärsisi pitkästä seisonnasta. Lähdin toimittamaan korvaavaa varalaitetta asiakkaalle, jonka he itse vaihtoivat päikseen rikkoutuneen laitteen kanssa. Takaisin saavuttuani tarkistin, mistä syystä laite oli rikkoutunut komennolla *”show chassis alarms no-forwarding”*, josta ilmeni syy *”Major FPC 0 Hard errors”*. Tämä viittasi siihen, että reititinalustan komponentti oli hajonnut. Olin jo avaamassa TAC:n (Technical Assistance Center) kautta RMA-pyyntöä Juniperille, kunnes kollegani ilmoitti, että laitteella olevassa järjestelmä versiossa on ohjelmointivirhe, joka aiheuttaa kyseistä virheilmoitusta, vaikka laite olisi itsessään ehjä. RMA-pyyntöä ei siis tarvinnutkaan tehdä, vaan tyhjensin laitteen konfiguraatioista komennolla *”request system zeroize”*, joka poistaa kaiken laitteelta, root-salasana mukaanlukien. Lopuksi piti vielä pyytää Juniperia vaihtamaan näiden kahden laitteen tuet keskenään, sillä ne olivat eri tasoiset.

Viikkoanalyysi 1

Tämän viikon työhtehtävät olivat monipuolisia. Viikko sisälsi eri asiakkaiden IT-ympäristöjen laitteistoja, sekä eri laitevalmistajien teknologioita. RMA-tapaukset olivat entuudestaan tuttuja minulle, eikä niiden osalta kertynyt juurikaan uutta osaamista. Perjantaina sattunut Juniper MX204-reitittimen ongelma kuitenkin kertoi minulle, että kehitettävää vielä löytyy. Minun pitäisi tarkemmin tutkia laitevalmistajien ilmoittamia ”known issues” artikkeleita, jotka käsittävät heidän tiedossaan ja työnallaan olevia virheitä järjestelmissä, ennen kuin teen johtopäätöksiä, että olisi rikkinäinen laite kyseessä. Yleisesti nämä artikkelit käsittelevät käyttöjärjestelmän ohjelmointivirheitä. Todennäköisesti Juniperin TAC olisi myös kertonut kyseisestä tunnetusta ongelmasta, eivätkä olisi suoraan myöntäneet RMA:ta laitteelle.

Eniten haastetta tuotti tiistaipäivä, jolloin suspended-tilassa oleva portti ei ollut minulle entuudestaan tuttu. Tähän tukipyyntöön meni aikaa tutkimiseen, sillä aiemmat kokemukset LACP-protokollasta olivat vähäiset. Olen aiemmin kouluni kursseilla hyödyntänyt EtherChannel-protokollaa, mutta vianselvitystä ei silloin tarvinnut tehdä. Ennen kuin tajusin käyttää logeja hyödykseni, pähkäilin hakukoneiden kanssa mistä ongelma voisi johtua. Tässä asiassa on itsellä kehittämistä, sillä en ollut aivan varma mistä lähtisin aloittamaan vianselvitystä.

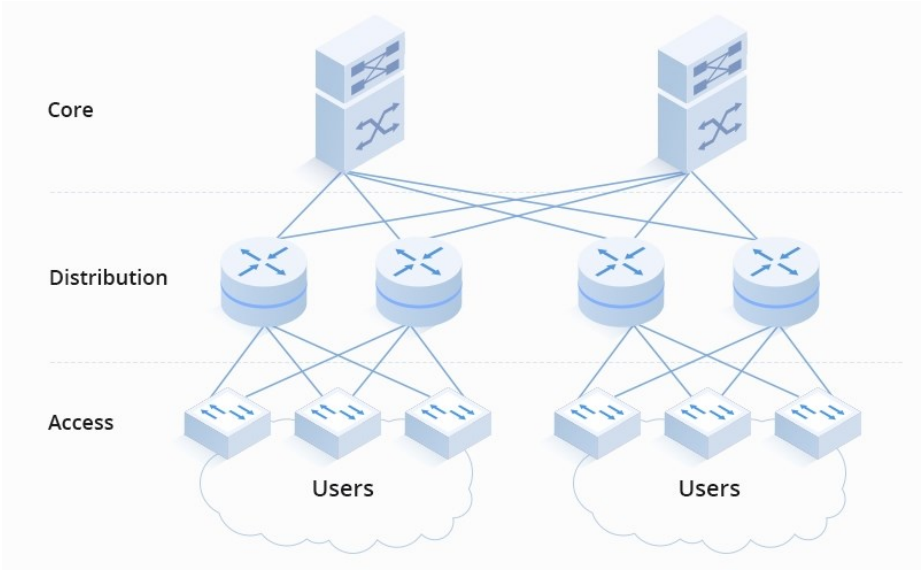
EtherChannel on Ciscon omistusoikeuden alaisuudessa oleva Ciscon kehittämä protokolla. EtherChannel on yksi tapa hyödyntää porttien linkkien aggregointi teknologiaa. LAG (Link Aggregation Group) on yleinen termi, jota käytetään kuvastamaan ryhmää, johon on konfiguroitu kaksi tai useampi fyysinen yhteys. Ciscon kytkimissä ja reitittimissä EtherChannelia voidaan konfiguroida käyttäen joko PAgP (Port Aggregation Protocol) -protokollaa, joka on sekin Ciscon kehittämä ja omistama protokolla. (Cisco 2) Vaihtoehtoinen ja kokemuksieni mukaan yleisempi tapa konfiguroida LAG:ia, on edellä mainittu LACP. Esimerkiksi Juniperin laitteita käyttävissä ympäristöissä mitä olen aikaisemmin tarkastellut, on ollut LACP käytössä.



Kuva 2. Kuva linkin aggregoinnista havainnollistamaan EtherChannelia, kaksi yhteyttä yhden sijaan. (Molenaar R. 1.)

Ciscon tapauksessa puhutaan EtherChanneleista, mikä tarkoittaa kahden tai useamman fyysisen yhteyden ryhmittämistä yhdeksi loogiseksi yhteydeksi. Tämän tarkoitus on nostaa verkkoyhteyden nopeutta, sekä tarjota vikasietoisuutta tilanteisiin, missä yhden yhteyden varassa oleva liikenne katkeaa. (Kuva 2)

Samassa tapauksessa pääsin myös tutustumaan ja oppimaan Multi-Tier mallista arkkitehtuuria. Multi-Tier mallin arkkitehtuurissa on kolme eri tasoa, jotka ovat access, aggregation, sekä core. Core-taso on ylin taso, aggregaatio-taso on keskellä, ja access-taso on alimmaisin. Multi-Tier mallista, eli useamman tason arkkitehtuuria voidaan käyttää niin yrityksen kampuksella, kuin vaikka konesaliympäristössä. Toimintatavaltaan kampus ja konesali toteutukset poikkeavat hieman toisistaan, ja perehdynkin tässä enemmän kampusmalliseen toteutukseen, sillä en ollut toistaiseksi konesaliympäristöissä työskennellyt, joten koin parhaakseni opiskella ensin yritysverkkojen toimintatapoja sekä -malleja.



Kuva 3. Havainnollistava kuva Multi-Tier arkkitehtuurista. (Howard. FS. 2023)

Kuvan 3 mukaisesti, access-tason kytkimet ovat niitä laitteita, jotka toimivat verkon reunoilla. Access-tason kytkimiin ovat tyypillisesti yhdistetty kaikki päätelaitteet, printterit, palvelimet, sekä muut

laitteet, jotka tarvitsevat verkkoa. Access-tason kytkinten päärooli verkkoympäristössä on siis tarjota verkkoyhteys muille laitteille, sekä ohjata liikenne aggregointitason kytkimille. Aggregointi-tasolle liikenteen ohjaaminen tapahtuu yleisesti käyttäen edellä mainittua LACP-protokollaa. (Cisco 1)

Aggregointi-taso toimii arkkitehtuurin keskellä. Sen pääsääntöinen tehtävä on kerätä kaikki liikenne access-tason kytkimiltä, ja ohjata liikenne edelleen core-tasolle. Aggregointi-kytkimet ovat yleisesti tehokkaampia ja nopeampia kuin access-tason kytkimet, jonka vuoksi ne myös käsittelevät liikennettä enemmän. Aggregointi-tasolla kytkimet tarkistavat liikkuvan datan tietoturvallisuuden, kuorman tasauksen, sekä QoS:n (Quality of Service) kannalta. Käsittelyn jälkeen, mikäli datassa ei esiintynyt mitään normaalista poikkeavaa, aggregointikytkin lähettää liikenteen core-tason kytkimelle. Aggregointi-kytkin myös jakaa access-kytkimille uplink-yhteyden, jonka saa core-tasolta. Tässä mielessä se on melkein sama asia kuin distribution-kytkimet, mutta ympäristössä, johon tämä liittyy, käytettiin aggregointikytkin tyyliä ja nimitystä. Uplink-yhteydellä tarkoitetaan verkkoyhteyttä, joka johtaa Internet-palveluntarjoajan verkkoon päätelaitteesta, ja ylipäätään yhteyteen ulkomaailmaan. Vastakohtana uplink-yhteydelle on olemassa downlink-yhteys, jolla tarkoitetaan esimerkiksi päätelaitteeseen tulevaa verkkoyhteyttä reitittimeltä ja Internet-palveluntarjoajalta. Uplink:n ja downlink:n erot voi helposti ymmärtää siten, että kun lataat internetistä tiedoston päätelaitteellesi, puhutaan downlink:stä. Vastaavasti kun lähetät, puhutaan uplink:stä. (Cisco 1)

Core-taso toimii arkkitehtuurin ylimpänä kerroksena. Sen pääsääntöinen tehtävä on tarjota uplink-yhteyttä alemmille tasoille, sekä lähettää edelleen sieltä saatuja datapaketteja ulkomaailmaan reitittimien välityksellä. Core-kytkimet ovat suoraan yhteydessä Internet-palveluntarjoajan verkkoon. Se on siis käytännössä kriittisin osa yrityksen verkkoa. Core-tason kytkimiä ei tyypillisesti konfiguroida jaottelemaan liikennettä eri tavalla, vaan se hoidetaan jo aggregointitasolla. Koska kyseisessä ympäristössä, jossa tein muutostöitä on suuri määrä access-tason kytkimiä, on oleellista olla erikseen core-kytkimet. Pienemmissä ympäristöissä on mahdollista käyttää ’’collapsed core’’ menetelmää, jolloin aggregointitason kytkimet toimivat samalla core-kytkiminä. (Cisco 1)

3.2 Seurantaviikko 2

Maanantai 4.9.2023

Viikko alkoi jälleen Palo Alton palomuurien parissa. Asiakkaalta tuli tukipyyntö, jossa ongelmana oli heidän asiakkaansa ympäristöön pääseminen. Aikaisemmalla viikolla toinen organisaationi asiantuntija oli koventanut URL (Uniform Resource Locator) Filtering profiileja, eli sellaisia konfiguraatioita, joilla pystytään sallimaan tai estämään liikenne verkkosivuille kategorioiden perusteella. Profii-

leja voi myös säätää käyttäjän tai käyttäjäryhmän perusteella. Tässä tapauksessa Palo Alton palomuuri tunnisti väärin asiakkaamme asiakkaan ympäristön, ja luokitteli sen ‘‘Gambling’’-kategoriaan, joka profiilien asetusten mukaisesti olisi estettyä liikennettä. Siirryin asiakkaan palomuurin GUI:lle, ja siirryin URL Filtering Profile asetuksiin. Siellä muokkasin olemassa oleviin sääntöihin ‘’Gambling’’-kategorian kohdalle ‘’Block’’ toiminnon sijaan ‘’Alert’’ toiminnon, joka sallii liikenteen, sekä tekee siitä logikirjauksen, kun sitä käytetään. Suoritin ja tallensin muutokset, jonka jälkeen monitoroin palomuurin liikennettä supistamalla tulokset henkilöihin, jotka yrittivät kyseiseen ympäristöön päästä. Huomasin liikennöinnin onnistuvan, ja kysyin vielä asiakkaalta varmistusta asiasta. Asiakas ilmoitti liikenteen toimivan, jonka jälkeen suljin tiketin.

Tiistai 5.9.2023

Tiistai oli todella hiljainen päivä. Minulle ei saapunut yhtäkään tukipyyntöä, mikä on tietenkin asiakkaan näkökulmasta hienoa. Päivä kului suurimmalta osin JNCIS-ENT sertifikaattia varten opiskellessa. Aihealueita mitä päivä aikana ehdin opiskelemaan, olivat esimerkiksi IS-IS reititysprotokolla, sekä VRRP (Virtual Router Redundancy Protocol), eli reitittimien viansietoisuuteen käytettävä protokolla.

Keskiviikko 6.9.2023

Keskiviikkona minulle saapui tukipyyntö liittyen rikkinäiseen MX204-reitittimeen. Asiakas ilmoitti ongelmasta optiikkojen kytkemisen kanssa. Kyseisen laitteen FPC0 (Flexible Pic Concentrator) PIC0 (Physical Interface Card) porteissa 2 ja 3 esiintyi erilaiset ongelmat, jotka molemmat vaikuttivat fyysisiltä laitevioilta. PIC on reitittimen osa, johon kiinnitetään fyysiset yhteydet, eli valokuidut optiikkoineen, tai Ethernet-kaapelit. FPC vastaavasti on yhteydessä PIC:iin, ja sen rooli on ohjata kaapeleista saapuvat datapaketit eteenpäin.

Porttiin 2 kytketty optiikka ja sen myötä laseri eivät rekisteröityneet jostain syystä laitteelle. Pyysin asiakkaalta kuvat porteista, ja ne vaikuttivat olevan vauritoituneita, sillä ne näyttivät kuvissa vinoilta. Portissa 3 taas esiintyi ongelma jo kytkemisvaiheessa, sillä optiikka ei edes mennyt sisälle asti paikalleen.

Pyysin asiakkaalta RSI (request support information) -, ja log-tulostukset, sillä Juniper usein pyytää niitä. Tulostuksista näkee laitteen virheilmoitukset, sarjanumerot, sekä muuta tärkeää tietoa. Tämän jälkeen avasin Juniperille TAC-pyynnön, että haluaisimme tehdä RMA:n kyseiselle laitteelle. Sisällytin pyyntöön myös asiakkaalta saamani kuvat, jolloin pyyntö eteni RMA-vaiheeseen.

Torstai 7.9.2023

Tämän viikon torstai kului hyvin paljon opiskellessa. Kertasin JNCIS-ENT-sertifikaattia varten aihealueen materiaalit läpi. Keskityin enimmäkseen STP (Spanning Tree Protocol)-, RSTP (Rapid Spanning Tree Protocol), OSPF (Open Shortest Path First)-, sekä BGP (Border Gateway Protocol) -protokolliin. STP ja RSTP ovat protokollia, jotka estävät silmukan muodostumisen verkkoympäristössä. OSPF ja BGP puolestaan ovat reititysprotokollia. Olin varannut myös ajan sertifikaattikokeeseen, ja sain siitä toistaiseksi ’’provisional pass’’ tuloksen, mikä tarkoittaa sitä, että valvovat tahot tai seritifikaatin myöntävä taho analysoi vielä kokeen suorituksen ja sen jälkeen antavat lopullisen arvion.

Perjantai 8.9.2023

Perjantai aamusta tuli asiakkaalta langattomasta verkosta tukipyyntö. Heillä oli eräällä työmaalla vaihdettu viallinen palomuuri, sekä uudelleenkäynnistetty kaikki langattoman verkon tukiasemat. Työmaalla oli käytössä vanhempia laitteita, jotka oli ilmeisesti tuotu toiselta työmaalta sinne. Tukiasemilla oli oikein asetetut IP-osoitteet, mutta langattomat verkot eivät mainostuneet päätelaitteille. Tukiasemat olivat Cisco-merkkisiä AIR-CAP16012 laitteita.

Aloitin ratkaisemaan ongelmaa kysymällä asiakkaalta lisätietoja ongelmasta ja avasin dokumentaatiostamme kyseisen sijainnin verkkotopologiakuvan. Viestittelyt asiakkaan yhteyshenkilön kanssa ja vianselvitys Ciscon materiaaleja hyväksikäyttäen paljastivat, että toinen tukiasemista olisi rikkinäinen. Se korvattiin Ciscon 2802 -mallin tukiasemalla.

Ongelmat eivät kuitenkaan loppuneet tähän. Myöskään korvaava laite ei mainostanut langatonta verkkoa työmaalla. Huomasin laitteen asetuksista, että se sai virtaa kytkimeltä vain 15.4 wattia. Tarkastin Ciscon tekniset spesifikaatiot kyseiselle mallille, jossa mainittiin sen tarvitsevan 26.5 wattia, jotta kaikki ominaisuudet toimivat. Asiakas kertoi, että heillä olisi kytkimen ja tukiaseman välissä PoE (Power over Ethernet) -injektori, joka on myös todella vanha. Pyysin asiakasta vaihtamaan tehokkaamman PoE-injektorin, ja vaihdon jälkeen tukiasema sai tarpeeksi virtaa, ja alkoi mainostamaan verkkoa.

Viikkoanalyysi 2

Perjantain tukiasemaongelma oli haastava. Aikaisempaa kokemusta langattomasta verkosta ei juurikaan ollut ja tuli opittua valtavasti uutta. Ongelmana oli siis, että tukiasemat ei pystynyt ottamaan yhteyttä asiakkaan WLC:hen (Wireless LAN Controller), eikä jakanut verkkoa päätelaitteille. WLC on laite, joka nimensä mukaisesti hallinnoi langattoman verkon tukiasemia.

Pyysin asiakkaalta lisätietoja, kuten mainostuuko SSID:t (Service Set IDentifier) eli verkon nimet, vai eikö yhteys toimi ulkoverkkoon, ja saako tukiasemat yhteyden WLC:hen. Vastauksena tuli, että SSID:t eivät mainostu, eikä yhteys WLC:hen onnistu.

Tarkastin WLC:ltä logitietoja, joista huomasin, että toinen tukiasema jäi jumiin ’’AP Join’’-prosessiin, joka ajan kuluessa epäonnistui, ja johti WLC:n katkaisemaan DTLS (Datagram Transport Layer Security) -yhteyden. Logitiedoissa oli myös viittauksia sertifikaatteihin, joiden päättymispäivät oli konfiguroitu laitteilla sivuutettaviksi, sillä tukiasemat olivat sen verran vanhoja, että ne olivat myös EOS (End of Support). WLC kuitenkin evaluoi tukiaseman sertifikaatin, vaikka ei ottanutkaan kantaa niiden päättymispäivään. *” Certificate verification - failed! <<<<<<----------”. ” DTLS Connection 0x1a47b390 closed by controller”*.

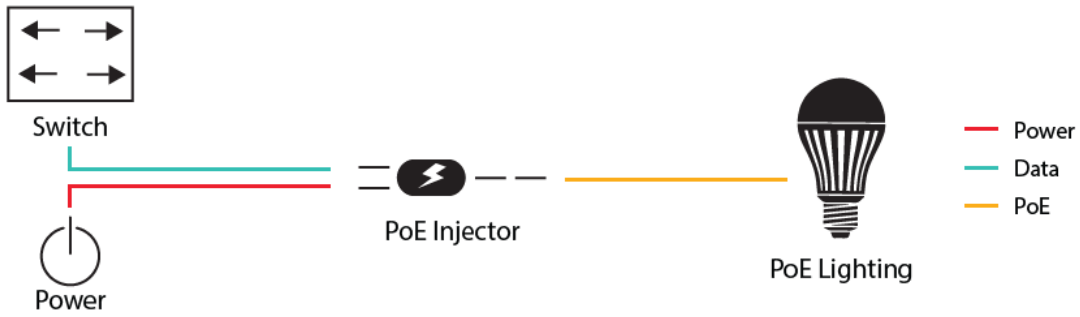
Tämä kyseinen tukiasema vaihdettiin Cisco 2802 -malliseen tukiasemaan, mutta siinäkin tukiasemassa ilmeni sama ongelma, eli tukiasema ei jakanut verkkoa, vaikka sertifikaattivirheitä ei esiintynyt. WLC:llä kirjoitin komennon *’’ show ap config general tukiasemannimi”*, jonka avulla huomasin PoE-tilan olevan ”*PoE/Medium Power”*, joka Ciscolla viittaa siihen, että tukiasema saa virtaa 15.4 wattia. Ciscon tekniset spesifikaatiot tukiasemille kertoivat, että tukiasema vaatisi 26.5 wattia, jotta kaikki ominaisuudet olisivat käytössä. (Cisco 3) Asiakkaalla oli käytössä vanhanaikaisia PoE-injektoreita, jotka ei päästänyt tarpeeksi virtaa läpi tukiasemalle. Molemmat PoE-injektorit vaihdettiin uudemman mallisiin, jolloin vaadittu virransyöttö saatiin vietyä tukiasemille.

PoE eli Power over Ethernet, tarkoittaa tekniikkaa, jolla voidaan syöttää virtaa laitteelle Ethernet-kaapelin välityksellä. Ensimmäinen PoE-standardi, IEEE 802.3af, hyväksyttiin vuonna 2003. Standardissa julkaistiin PoE-tyyppi 1, jossa luvattiin vähintään 13W teho. Maksimiksi standardissa oli asetettu 15.4W, mutta sitä ei voitu taata, sillä osa tehosta häviää kulkiessaan Ethernet-kaapelissa. Laitteet, joiden kanssa tyypin 1 PoE:ta käytetään, ovat esimerkiksi VoIP (Voice over Internet Protocol) -puhelimet, ja erilaiset sensorit. (FS 2) 802.3af standardin mukaista PoE:ta kutsutaan yleisesti myös termillä ”low-power”. (Maniktala S. 2013. Luku 2.1)

Vuonna 2009 päivitetyssä standardissa IEEE 802.3at, teholukemat nostettiin minimissään 25.5W asti, jolloin tämän version termiksi tuli PoE+ tai tyypin 2 PoE. Maksimiteho mitä standardissa määriteltiin oli 30W, mutta myös tämä standardi kärsii Ethernet-kaapelin hävittämästä tehosta. IEEE 802.3at mukainen PoE tukee esimerkiksi biometrisiä sensoreita, älylaitteita, kameroita, sekä langattoman verkon tukiasemia. (FS 2) IEEE 802.3at standardia kutsutaan yleisesti myös termillä ”medium-power”. (Maniktala S. 2013. luku 2.1)

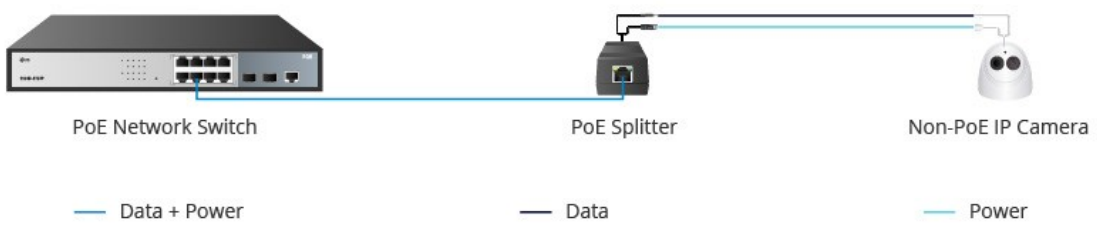
Viimeisin hyväksytty PoE-standardi on IEEE 802.3bt, jossa määriteltiin tyypin 3 ja 4 PoE:t, tyypin 3 tukiessa minimissään 51W ja maksimissaan 60W, ja tyypin 4 tukiessa minimissään 71W ja maksimissaan 100W. IEEE 802.3bt mukainen PoE kykenee syöttämään virtaa laitteille, jotka vaativat enemmän tehoa, kuten esimerkiksi televisiot, kannettavat tietokoneet tai videokonferenssilaitteet. (FS 2) Kaikki kehittyneemmät PoE-versiot ovat taaksepäin yhteensopivia.

PoE toimii laitteissa olevien PSE (Power sourcing equipment) -sirun avulla. Ilman sitä, sähkövirtaa ei pystytä ohjaamaan yhdistetylle laitteelle. PoE toimii aina 100 metriin asti, jolloin esteeksi tulee Ethernet-kaapelien rajoitukset datasiirron osalta vastaan. Kaikissa kytkimissä PSE:tä ei kuitenkaan ole, jolloin tarvitaan PoE-injektori. PoE-injektorit pystyvät kuljettamaan tehoa riippuen standardista minkä mukaan se on valmistettu. (Arubanetworks 1)



Kuva 4. Havainnollistava kuva siitä, miten PoE-injektori toimii. (planettechusa)

Poe-injektori on erillinen ulkoinen laite, jonka avulla voidaan lähettää sekä dataa, että sähkövirtaa yhdistetylle laitteelle. (Kuva 4) PoE-injektorissa on tyypillisesti kolme porttia. Yksi portti on virtakaapelille, toinen sisääntulevalle datalle mikä tulee esimerkiksi kytkimeltä, ja kolmas uloslähtevälle datalle esimerkiksi tukiasemaa kohti. Kolmas portti toimii samalla myös sähkövirran siirtäjänä. Koska kaikki kytkimet tai laitteet eivät ole PoE-yhteensopivia, injektori säästää sekä suunnittelussa, ja toteutuksessa aikaa ja tilaa. Sen sijaan, että jokaiseen tukiasemaan pitäisi yhdistää virtakaapeli ja Ethernet-kaapeli, data ja sähkövirta voidaan tuoda laitteeseen yhden Ethernet-kaapelin avulla. (FS 3)



Kuva 5. Havainnollistava kuva siitä, miten PoE-muunnin toimii. (FS 4)

Osa yhdistetyistä laitteistakaan eivät välttämättä ole PoE-yhteensopivia. Varsinkin vanhemmissa laitteissa kyseinen ominaisuus puuttuu. Sitä varten on kehitetty PoE-muunnin, eli injektorin kaltainen laite, joka toimii päinvastoin. (Kuva 5) PoE-muuntimen avulla pystytään lähettämään data sekä sähkövirta yhteensopimattomalle laitteelle, sillä siinä on kaksi eri ulosmenoporttia yhden sijaan. Yksi sähkövirralle ja yksi datalle. Sisääntuloja on yksi, josta sähkövirta ja data kulkeutuvat kytkimeltä muuntimelle. (FS 4)

3.3 Seurantaviikko 3

Maanantai 11.9.2023

Maanantaina tuli projektipäälliköltä sähköpostia erään asiakkaan kytkinten päivityksistä. Kytkimissä oli käytössä vanha järjestelmäversio, jotka tuli päivittää samaan versioon kuin ympäristössä olevat muut samanlaiset laitteet. Kytkimiä, joita minulle tuli päivitettäväksi oli kahdeksan kappaletta. Päivitettäviä malleja oli kaksi, Cisco IE-3300-8P2S-E joka on rugged-kytkin, eli huonoihin olosuhteisiin suunniteltu kytkintyyppi, sekä Cisco WS-C9200-24P. Kytkimissä oli käytössä Cisco IOS Xe käyttöjärjestelmät.

Päivitys toteutettiin hyppykoneen kautta, jolta otettiin SSH (Secure Socket Shell) -yhteys kytkimiin. Hyppykone tarkoittaa erillistä palvelinta, jolta otetaan etäyhteys ympäristön sisällä oleviin laitteisiin. Hyppykone oli konfiguroitu toimivaksi myös SFTP (Secure File Transfer Protocol) -palvelimena, jolta siirrettiin uudet käyttöjärjestelmäversiotiedostot kytkimille. Päivityksissä kesti melko kauan aikaa, sillä siirto SFTP:n avulla hyppykoneelta palvelimelle kesti yli tunnin. Varsinainen järjestelmäversion päivitys tapahtui melko nopeasti ja vei aikaa vain 15 minuuttia.

Tiistai 12.9.2023

Maanantai iltapäivästä oli tullut tukipyyntö asiakkaan VPN (Virtual Private Network) -sääntöjen purkuun liittyen. Asiakas oli luopunut yhden operaattorin tarjoamista konesalipalveluista, ja halusi näin ollen purkaa heidän palomuureillansa olleet konesaliin liittyvät säännöt. Tiistaina aamupäivästä pidimme asiakkaan kanssa lyhyen palaverin aiheesta, ja katselmoimme yhdessä kaikki säännöt mitä tulisi poistaa.

Palaverin jälkeen aloitin sääntöjen purkamisen. Sääntöjä mitä purettiin, olivat esimerkiksi IPSec (IP Security) -tunnelin poisto, konesalin suuntaan kohdistuvat verkot, NAT (Network Address Translation) -sääntöjä, sekä monia muita yhteyteen liittyviä palomuurisääntöjä. Poistojen jälkeen vertasin vielä muurin käytössä olevaa konfiguraatiota ja kandidaatti konfiguraatiota, josta näkee mitä muutoksia suorittamisesta tulee. Varmistuttuani oikeiden asetusten poistamisesta, suoritin muutokset.

Keskiviikko 13.9.2023

Keskiviikkona tuli tukipyyntö asiakkaalta Palo Alto Networksin Prisma Access-ongelmasta. Prisma Access on Palo Alto Networksin pilvipohjainen tuote, joka tarjoaa turvalliset yhteydet verkkoon ja applikaatioihin. Asiakas ei päässyt käsiksi hallintaansa, vaan Prisma Access herjasi *"Prisma Access application failed to launch, please try launch from the tenant switcher or hub. If issue persists please contact Palo Alto Networks support. Failed to initialize due to ajax error 400".* Kyseessä tuntui olevan muutenkin Palo Alton päässä oleva konfiguraatio-ongelma, joten avasin TAC-pyynnön Palo Altolle.

Palo Altolta pyydettiin HAR (HTTP ARchive format) -tiedosto, jonka saa selaimesta ladattua. Ongelma ratkesi Palo Alton puolelta nopeasti, sillä olin asettanut tukipyynnön prioriteetiksi tason 2, joka on kiireellisille asioille tarkoitettu. Loppujen lopuksi ongelma johtui asiakkaan lisensseistä, ja se saatiin Palo Alton puolella korjattua.

Torstai 14.9.2023

Torstaina merkittävimmäksi työtehtäväksi esiintyi Juniperin CSAM (Customer Support Access Management) -työkalun käyttö asiakastilien luontia varten. Tukipyyntö ei tullut tällä kertaa suoraan asiakkaalta, vaan sen lähetti tikettijärjestelmään yksi yritykseni myyjistä. Myyjämme oli myynyt asiakkaalle tukisopimuksen yhteydessä palvelun, jonka avulla asiakas pystyy itse lataamaan käyttöjärjestelmäversioita.

Siirryin Juniperin CSAM-työkaluun, johon aluksi loin uuden loppukäyttäjäyrityksen. Luonnin yhteydessä on pakko lisätä ainakin yksi henkilö yrityksen työntekijäksi. Tukipyynnössä pyydettiin luomaan kuudelle henkilölle käyttäjätunnukset ja oikeudet latauksiin. Näistä kuudesta, neljä onnistuin luomaan ilman mitään ongelmia, mutta kahdella henkilöllä oli entuudestaan omat tunnukset Juniperin järjestelmässä. Avasin Juniperille TAC-pyynnön aiheesta, ja päivän päätteeksi heiltä tuli ilmoitus, että vanhat käyttäjätunnukset on poistettu, jolloin sain luotua viimeisetkin käyttäjätunnukset.

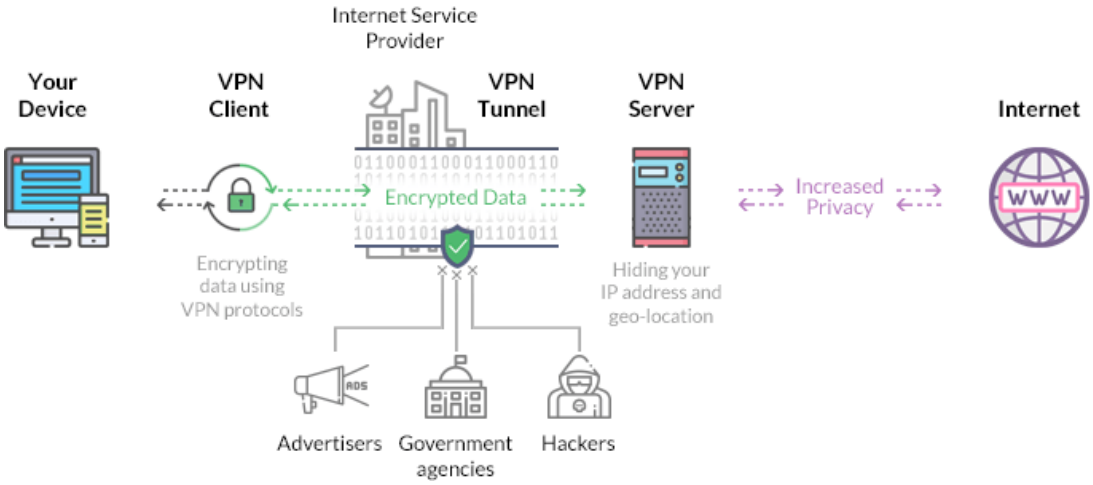
Perjantai 15.9.2023

Perjantaille oli merkitty varmuuskopioiden toimivuuden varmistus. Tarkistin organisaationi verkkolaitteiden konfiguraatiot, sekä niiden palautettavuuden. Varmuuskopioympäristössä, jossa yritykseni verkkolaitteet ovat, on myös muutamia asiakkaiden laitteita, joten tarkistin ne samalla.

Ongelmaksi tässä tuli eteen varmuuskopiopalveluntarjoajan ohjelmointivirhe tai ominaisuus. Omilla käyttäjätunnuksilla kirjautuessani palveluun, en nähnyt yhtään laitetta laitelistan alla. Kysyin kolleegaltani onko hänellä sama ongelma, ja hänkään ei nähnyt niitä. Kirjauduin admin-käyttäjätunnuksilla palveluun, jolloin kaikki laitteet näkyivät, mitkä pitikin. Tarkistin käyttäjäluettelosta tunnusteni oikeudet, ja ne olivat samat kuin admin-käyttäjätunnuksella. Ilmoitin asiasta tietohallintopäälliköllemme, jonka vastuualueena kyseinen palvelu on, joka delegoi sen edelleen eteenpäin palveluntarjoajalle tukipyyntönä.

Viikkoanalyysi

Viikko kolme oli todella monipuolinen työtehtävien osalta. Ciscon laitteiden päivitys oli minulle entuudestaan tuttua, joten haasteita ei tullut sen osalta. Palo Alton laitteiden ja ympäristön kanssa en ole työskennellyt yhtä paljon, mutta oli sekin melko tuttua. Mielenkiintoisimpana haasteena koin tiistain VPN-tukipyynnön. Tiesin entuudestaan mitä VPN tarkoittaa, mutta syvempää ymmärrystä minulla ei siitä ollut.



Kuva 6. Kuvaus VPN-tekniikan toiminnallisuudesta (CactusVPN)

VPN eli virtuaalinen yksityinen verkko on tekniikka, jonka avulla pystytään toteuttamaan turvallisia internet yhteyksiä julkisia verkkoja käytettäessä. VPN salaa kaiken verkkoliikenteen kahden pisteen välillä, tyypillisesti käyttäjän ja yrityksen verkon välillä, piilottaen käyttäjän tunnistamiseen käytettävät muuttujat. (Kuva 6) Tämän vuoksi kolmansien osapuolien on vaikeaa seurata käyttäjän liikennettä verkossa ja varastaa dataa. Salaus tapahtuu reaaliajassa. (Kaspersky)

VPN toimii muodostamalla tunnelin internetiin. Kaikki liikenne kulkee tämän tunnelin läpi, ja se kulkee salattuna. Kun laite on yhdistettynä VPN-verkkoon, se käyttäytyy kuin olisi samassa lähiverkossa VPN:n kanssa. Käyttäjän piilotettuihin tietoihin kuuluvat esimerkiksi käyttäjän IP-osoite. Salaukseen käytetyistä tekniikoista suosituimpia ovat yleisesti SSL tai siitä uudempi versio TLS, sekä

IPsec. VPN tyyppejä on monia erilaisia olemassa, mutta yleisimmät ovat SSL VPN, Site-to-site VPN, sekä Client-to-server VPN. Riippuen käyttäjän tarpeesta, osa sopii ympäristöihin toisia paremmin. (Palo Alto Networks)

IPsec-protokolla on pidempään ollut käytössä kuin SSL / TLS-protokolla. IPsec-protokolla tarjoaa salauksen käyttäen sekä fyysistä laitteistoa, että ohjelmistoa. SSL / TLS vastaavasti tarjoaa salauksen vain ohjelmistojen avulla. Koska IPsec-protokolla käyttää myös fyysistä laitteistoa salauksen tekemiseen, se on silloin myös raskaampi käyttää, mutta myös turvallisempi. IPsec toimii OSI (Open Systems Interconnection) -mallin verkkokerroksessa. Tämä tarkoittaa sitä, että verkosta vastaavien henkilöiden tulee fyysisesti ja manuaalisesti hallita salausta ohjelmistojen käytön sijaan. Kääntöpuolena on tehokkaampi tietoturva ja salaus, sillä kolmansien osapuolien on vaikeampi hyökätä salausta kohti, koska laitteistotkin ovat osa sitä. Tästä syystä IPsec myös vaatii usein erikoislaitteistoa ja -ohjelmistoa käyttäjän verkkoon pääsemiseen. (Fortinet)

Sen sijaan SSL ja TLS-protokollat toimivat verkkoselainten avulla. Ne eivät vaadi käyttäjältä ylimääräisiä laitteisto- tai ohjelmistovaatimuksia. Jokaisessa nykyaikaisessa älylaitteessa tai tietokoneessa on vakiona jokin selain, joka tukee SSL ja TLS-protokollia salaukseen. Se on siis kevyempi tapa salata liikennettä. (Fortinet)

SSL VPN mahdollistaa yksittäisten käyttäjien pääsemisen yrityksen tai organisaation verkkoon, asiakkaidensa työympäristöihin ja ohjelmistoihin ilman minkäänlaista erillistä ohjelmistoa. SSL VPN:n avulla voidaan liikennöidä salatusti ja suojatusti siitä välittämättä, onko käyttäjä yhteydessä julkiseen verkkoon tai johonkin muuhun suojattuun verkkoon. Liikennöinti tapahtuu siis käyttäjän verkkoselaimen ja erillisen SSL VPN -laitteen välillä, eikä käyttäjän tarvitse vaikuttaa käytetyn salaustekniikan valintaan. Käytetty tekniikka valikoituu automaattisesti uusimman ja viimeisimmän mukaan. (Fortinet)

SSL VPN voidaan edelleen jakaa kahteen eri kategoriaan, SSL Portal VPN -tyyppiin, sekä SSL Tunnel VPN -tyyppiin. SSL Portal VPN:ssä käyttäjä vierailee verkkosivulla, johon syöttää omat tunnistetietonsa. Koska tämä tekniikka sallii vain yhden yhteyden, sitä käytetäänkin usein kirjautumaan yrityksen tai organisaation verkkoon, jonka kautta voidaan käyttää muita palveluja. SSL Tunnel VPN:n avulla voidaan yhdistää salatusti useampaan verkkopalveluun, eikä ne ole rajattu pelkästään verkkopalveluihin. Käyttäjä voi yhdistää esimerkiksi yrityksen ohjelmistoihin tai yksityisiin verkkoihin, jotka eivät ole suorassa yhteydessä internetiin. (Fortinet)

Site-to-site VPN on hyödyllinen suurten organisaatioiden käytössä. Site-to-site VPN on käytännössä yksityinen verkko, johon on yhdistettynä organisaation eri toimipisteitä. Jos organisaatiolla on useita eri toimipisteitä, joilla on kaikilla oma lähiverkkonsa, voidaan kaikki lähiverkot yhdistää

tähän samaan verkkoon, jolloin eri toimipisteistä voidaan päästä käsiksi muiden toimipisteiden resursseihin. Tämän tyyppiset VPN-toteutukset ovat usein monimutkaisia ottaa käyttöön, eivätkä tarjoa käyttäjilleen joustoa, kuten SSL VPN-toteutukset. (Kaspersky)

Client-to-server VPN on todella yleinen tapa toteuttaa yritykselle VPN. Tässä toteutustavassa käyttäjän tietokoneelle asennetaan erillinen ohjelmisto, jonka kautta käyttäjä ottaa yhteyden yrityksen sisäiseen verkkoon. Tämä toteutus eroaa muista siten, että tässä käyttäjä ei käytä omaa Internet-palveluntarjoajaansa ohjaamaan liikennettään haluttuun osoitteeseen, vaan muodostaa ensin suoran yhteyden VPN-palveluntarjoajaansa, jonka kautta liikenne ohjautuu eteenpäin. Tämä edesauttaa salausta ja pitämään käyttäjän anonyyminä, sillä sen sijaan, että VPN-tunneli luotaisiin olemassa olevan internet-yhteyden päälle, client-to-server mallin toteutus salaa tiedot ennen kuin ne ovat käyttäjän saatavilla. Client-to-server mallin toteutus on todella hyödyllinen esimerkiksi käytettäessä julkisia langattomia verkkoja, sillä se estää kolmansien osapuolten pääsemistä verkkoyhteyteen kiinni. Client-to-server myös poistaa mahdolliset internet-yhteyksiä koskevat rajoitukset mitä käyttäjä saattaisi kohdata, esimerkiksi maakohtaiset rajoitukset, koska yhteyden reititys tapahtuu loppujen lopuksi yrityksen VPN-palveluntarjoajan kautta, eikä käyttäjän oman internet-palveluntarjoajan kautta. (Kaspersky)

3.4 Seurantaviikko 4

Maanantai 18.9.2023

Maanantaina aamusta saapui vikailmoitus asiakkaalta. Heillä olevassa Juniper MX240-reitittimessä oli esiintynyt linjakorttivikoja. Yksi MPC4E-mallin linjakortti oli alkanut katkomaan yhteyksiä, ja loppujen lopuksi jäi kokonaan offline-tilaan.

Pyysin asiakasta kokeilemaan tyypillisiä korjausehdotuksia, kuten linjakortin tuulettamista, jolloin otetaan linjakortti irti runkolaitteesta ja laitetaan hetken päästä takaisin kiinni. Asiakkaan mukaan tämä toimenpide auttoi vain hetkellisesti ja vika tuli esiin uudelleen. Pyysin asiakkaalta Juniperin TAC:n tarvitsemia tietoja ja huomasin logeissa esiintyvän useita eri ’’Link failure’’-kirjauksia.

Avasin RMA-tukipyynnön Juniperille ja pyysin asiakasta lähettämään viallisen linjakortin meille. Linjakortissa oli Juniperin RTF (Return to Factory) -tuki, mikä tarkoittaa sitä, että viallinen laite tulee lähettää Juniperille ennen kuin asiakas saa korvaavan laitteen tilalle.

Tiistai 19.9.2023

Tiistaina oli pitkä päivä töiden osalta. Asiakkaalta oli vanhenemassa palomuurilla heidän palvelinten varmenne, joka tuli päivittää. Varmenteen päivitys olisi vaikuttanut palomuurin läpi kulkevaan

liikenteeseen, joten se tuli tehdä toimistoaikojen ulkopuolella heidän huoltoikkunansa aikana. Varmenteen vaihto oli omalta osalta hyvin yksinkertaista, eikä se vaatinut kovinkaan paljon aktiivista työntekoa.

Siirryin asiakkaan Palo Alto Networksin palomuurin GUI-näkymään, josta annoin asiakkaalle hetkellisesti admin-oikeudet palomuurille. Asiakas tarvitsi nämä, sillä he halusivat itse ladata uuden varmenteen palomuurille, sillä ladattaessa varmennetta, ladataan myös salausavain. Yrityksessäni emme tarvitse näkyvyyttä asiakkaan salausavaimeen, joten tämä menetelmä oli helpompi. Asiakkaan ladattua uuden varmenteen, poistin asiakkaalta admin-oikeudet ja vaihdoin varmennetta käyttäviin sääntöihin uuden varmenteen. Eniten aikaa prosessissa meni siihen, kun asiakas päivitti varmenteen myös heidän palvelimilleen

Keskiviikko 20.9.2023

Keskiviikko kului Ciscon kytkinten parissa. Asiakkaalta tuli tukipyyntö puhelimen välityksellä, että tarvitsisivat pikaisesti asetettua muutamien kytkimien porteille VLAN-verkkoja. Asiakas oli testaamassa uusia laitteita kytkimien päässä, ennen kuin ne siirretään kokonaan tuotantoon. Aloitin tukipyynnön purkamisen siirtymällä asiakkaan hyppykoneelle, josta edelleen siirryin SSH-yhteyden avulla kytkimille. Asetin oikeille porteille oikeat VLAN-verkot ja suoritin muutokset. Varmistin asiakkaalta vielä puhelimitse, että yhteys nousi laitteiden välillä, minkä asiakas tarkisti yhdistetyltä laitteelta.

Torstai 21.9.2023

Torstai jatkui Ciscon laitteiden parissa. Asiakkaalta tuli tukipyyntö synkronoida heidän kytkinten aika ja päivämäärä. Verkkolaitteille aika ja päivämäärä yleisesti määritellään NTP (Network Time Protocol) -tekniikan avulla. NTP:n avulla aika ja päivämäärä haetaan nimetyltä palvelimelta, minkä pystyy itse määrittelemään palvelimille tai kytkimille.

Siirryin asiakkaan kytkimille SSH:n avulla, ja määritin jokaiseen kytkimeen samat NTP-palvelinten IP-osoitteet, jolloin ne kaikki hakevat aika- ja päivämäärätiedot samalta palvelimelta. Tämä varmistaa sen, että aikatietojen välille tulisi minimaalinen ero.

Perjantai 22.9.2023

Perjantai alkoi ongelmanratkaisun parissa. Tiistain varmenteenvaihdossa oli esiintynyt ongelmia, sillä salaus ei toiminut varmenteen vaihdon kohteena olevilla palvelimilla. Tutkittuamme ongelmaa,

yritimme uudelleen ladata varmenteen palvelimelle, jos siinä olisi tapahtunut tiedoston korruptoituminen tai vastaava virhe. Kun salaus ei lähtenyt vieläkään toimimaan, jouduin pyytämään tukea kollegaltani, joka tuntee paremmin Palo Alton palomuurit.

Ongelmaksi selvisi tiedoston varmennepolku. Vaikka palomuuri osasi sijoittaa varmenteen oikeaan kohtaan varmennepuuta, eli ylempien CA (Certificate Authority) -varmenteiden alle, se ei osannut ilman koko polkua käyttää sitä. Eli varmennetiedostossa piti olla kaikki ylemmätkin varmenteet, eikä riittänyt pelkästään se palvelinvarmenne.

Viikkoanalyysi

Viikko oli jälleen hyvin monipuolinen. Maanantain ja keskiviikon työhtehtävät hoituivat jo helposti ja rutiinimaisesti, mutta tiistain, torstain ja perjantain työtehtävät olivat jokseenkin uusia minulle. Varmenteen vaihto ei itsessään ollut kovinkaan monimutkaista, mutta esiintyneen ongelman ratkominen oli mielenkiintoista. Opin samalla varmenteista ja varmenneketjuista.

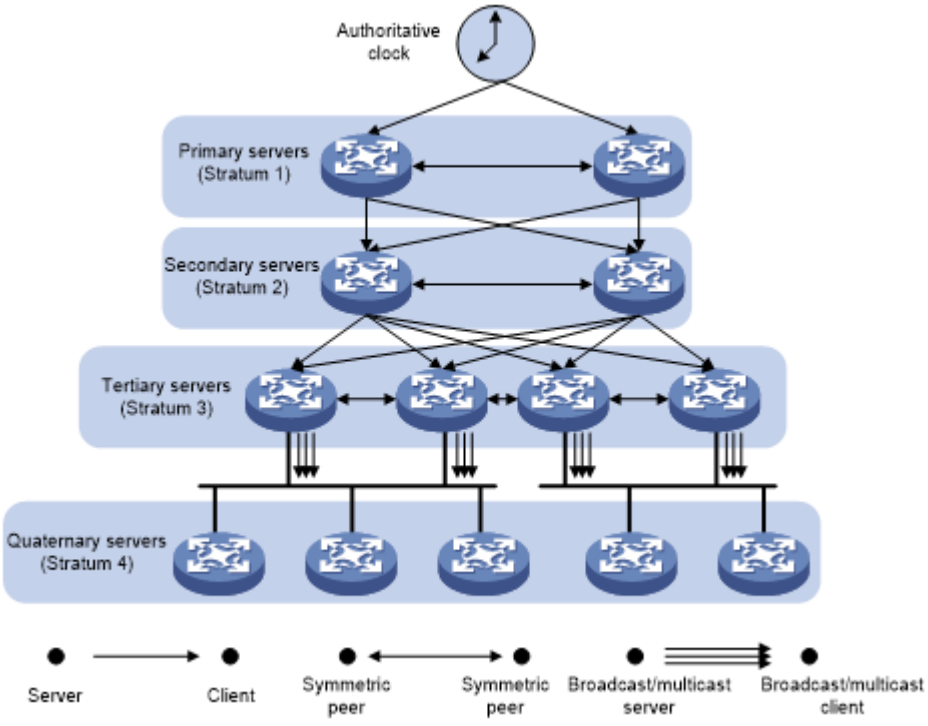
Myös torstain NTP-synkronointitehtävä oli mielenkiintoinen. Työtehtävää suorittaessa minulle heräsi monia kysymyksiä siitä miten NTP toimii, ja päätinkin tutkia asiaa enemmän.

NTP eli Network Time Protocol on TCP/IP (Transmission Control Protocol/Internet Protocol) -pinon applikaatiotasolla toimiva protokolla. Sitä käytetään palvelimen ja asiakaslaitteen väliseen kellonaikojen synkronointiin. NTP tarjoaa hyvin tarkan kellonajan synkronoinnin, jonka NTP-palvelin vastaanottaa luotetulta lähteeltä, kuten atomikellolta tai GPS (Global Positioning System) -laitteelta. Asiakaslaite saa vastaavasti NTP-palvelimelta tarkan kellonajan. NTP-protokolla toimii käyttäen UDP (User Datagram Protocol) -protokollan porttia 123. (Huawei)

NTP määriteltiin alun perin RFC 958-standardissa nimellä NTPv0. Koska alkuperäinen NTP:n määritelmä oli julkaistu jo vuonna 1981, on NTP-protokollaa kehitetty ajansaatossa uudempiin versioihin. NTPv1 määriteltiin RFC 1059-standardissa ja sen kehittymisen myötä määriteltiin uudet NTP-säännöt, algoritmit, sekä kuvailtiin asiakaslaite-palvelinlaite suhde ja vertaisverkon toimintamallit. Vertaisverkolla tarkoitetaan tässä kontekstissa tilannetta, jossa kaksi samassa verkossa olevaa reititintä on konfiguroitu vastaanottamaan ja lähettämään toisilleen NTP-protokollan välityksellä kellonajat. Ne siis synkronoivat kellonajat toisistaan. NTPv2 määriteltiin standardissa RFC 1119, jossa myös määriteltiin NTP-protokollalle autentikointi ja hallintaviestit. NTPv3 määriteltiin standardissa RFC 1305, jonka myötä NTP kykeni toimimaan broadcast-lähetyksillä. Viimeisin NTP standardi mikä on julkaistu, on RFC 5905, jossa määriteltiin NTPv4. NTPv4 toi uutena asiana IPv6-protokollan tuen, sillä aiemmat versiot kykenivät toimimaan vain IPv4-protokollalla. NTPv4 myös tarjoaa paremman salauksen ja autentikoinnin. (Huawei)

NTP-protokollan toimintaperiaate on yksinkertainen. Sen toiminta voidaan kuvata kokonaisuudessaan kolmella vaiheella. Ensimmäisessä vaiheessa asiakaslaite lähettää kellonaikapyynnön NTP-palvelua tarjoavalle palvelimelle. Seuraavaksi asiakaslaite laskee yhteyden viiveen ja säätää kellonaikansa samaan aikaan kuin palvelimen kellonaika. Kolmannessa vaiheessa laitteet lähettävät toisilleen kuusi pakettia noin viiden ja kymmenen minuutin välillä, mitkä vaaditaan, että saadaan asetettua ensimmäisen kerran kellonaika. Kun asiakaslaitteen ja palvelimen kellonajat ovat synkronoituneet, asiakaslaite päivittää kellonaikaa kerran kymmenessä minuutissa. (Techtarget 1)

Suurin osa verkkolaitteista ympäri maailman käyttävät NTP-protokollaa synkronoimaan kellonaikansa. Suomessa laitteet saavat kellonajan MIKES:ltä (Mittatekninen Keskus). MIKES on suomalainen metrologian tutkimuslaitos, jonka atomikellot ja GPS-laitteet laskevat suomen kellonajan, ja pystyvät lähettämään sen NTP-protokollan välityksellä muille laittelle, pahimmillaan yhden millisekunnin virheellisyydellä. MIKES omistaa neljä stratum-tasojen korkeimmalta tasolta olevaa palvelinta, joista kaksi on synkronoitu suoraan atomikelloista ja kaksi GPS-vastaanottimista. (VTT)



Kuva 7. Kuvaus stratum-tasoista ja niiden rakenteesta. (HPE)

Maailmassa on monia suuria verkkoympäristöjä, joissa käytetään NTP-protokollaa. NTP-lähteitä on vastaavasti valtava määrä, joten asiakaslaitteet tarvitsevat jonkinlaisen tiedon siitä, mikä lähteistä on luotettava ja mahdollisimman tarkka. Tätä varten on kehitetty stratum-tasot. Stratum-tasot voidaan hahmottaa ylhäältä alaspäin laskeutuvalla tiedolla. (Kuva 7) Stratum-tason 0 laitteet ovat kai-

kista tarkimmat, ja ne ovatkin yleisesti atomikelloja tai GPS-vastaanottimia. Näitä laitteita ei kuitenkaan pystytä yhdistämään verkkoon, vaan ne toimivat stratum-tason 1 laitteiden kellonajanlähteinä. Stratum-tason 1 laitteet ovat tarkimmat verkosta saatavat kellonajanlähteet ja ne saavat kellonaikansa suoraan tasolta 0. Stratum-tason 1 laitteet jakavat edelleen kellonajan alemmille stratum-tason 2 laitteille. Koska verkossa esiintyy viiveitä, stratum-tason 2 laitteet eivät ole yhtä tarkkoja kuin tason 1. Vastaavasti jos laite saa kellonajan stratum-tason 2 laitteelta, kutsutaan niitä laitteita stratum-tason 3 laitteiksi. Mitä alemmas tasoilla mennään, sitä epätarkemmaksi kellonaika muuttuu. (Worldtimesolutions)

3.5 Seurantaviikko 5

Maanantai 25.9.2023

Viikko alkoi päivitystöillä. Asiakkaan Palo Alto Networksin palomuureilla oli esiintynyt ongelma, mikä esti muutosten suorittamisen muureille. Logitiedostojen mukaan palomuurien CPU:n (Central Processing Unit) käyttöaste oli jatkuvasti lähes 100 %, joka tiedostojen mukaan esti muutosten suorituksen. Kyseessä oli VM-mallin palomuuripari eli virtuaalinen toteutus, joka pyörii toisen laitteen päällä.

Lähetin valmistajalle tukipyynnön sähköpostitse, sillä epäilin laitteen olevan rikkoutunut. Tukihenkilö kysyi käyttöjärjestelmäversiota ja hän ehdotti sen jälkeen sen päivittämistä. Päivitys tuli taas tehdä toimistoaikojen ulkopuolella. Vaikka kyseessä on HA (High Availability) -pari, saattaisi se silti häiritä palomuurin läpi kulkevaa liikennettä. Latasin palomuurin GUI-näkymästä uuden käyttöjärjestelmäversion ja aloitin päivittämisen parin passiiviselta palomuurilta.

Palomuurien päivitys kesti noin tunnin yhtä palomuuria kohden, jonka jälkeen tein testisäännön ja yritin suorittaa muutokset. Muutokset menivätkin päivityksen jälkeen läpi, eli kyseessä oli tällä kertaa käyttöjärjestelmän ohjelmointivirhe. Ilmoitin vielä vastaavalle tukihenkilölle ongelman ratkenneen.

Tiistai 26.9.2023

Tiistaina tuli tukipyyntö asiakkaalta liittyen heillä esiintyneeseen ongelmaan Ciscon laitteiden kanssa. Kyseiselle asiakkaalle oli myyty yritykseni kautta tuki Ciscolle, mutta asiakkaan kaikilla yhteyshenkilöillä ja laitteista vastaavilla ei ollut oikeuksia näkemään tehtyä sopimusta. Asiakas pyysi myöntämään oikeudet yritysten väliseen sopimukseen, jolloin he pystyvät antamaan Ciscon TAC:lle tarvittavia lisätietoja.

Koska minulla ei ole oikeuksia seurata myynnin tekemiä sopimuksia, jouduin delegoimaan tukipyynnön myyntiosastolle. Ilmoitin myynnille asiakkaasta sekä tukipyynnöstä, ja kerroin myös sopimusnumeron, jolla he saisivat lisättyä oikeudet. Noin tunnin päästä sain vastauksen myynnin henkilöltä, jonka jälkeen vastasin asiakkaalle, että heillä pitäisi olla nyt oikeudet.

Keskiviikko 27.9.2023

Keskiviikkona tuli mielenkiintoinen tukipyyntö asiakkaalta. Asiakkaan verkossa on esiintynyt flooding-ongelmaa, eli kytkin lähettää datapaketteja kaikkiin yhdistettyihin laitteisiin, eikä pelkästään osoitettuun kuten halutaan. Asiakkaan verkkoympäristössä on kaksi reitintä, kaksi kytkintä ja kaksi palomuuria. Flooding tapahtui tässä tapauksessa sen vuoksi, että liikenne oli epäsymmetristä. Epäsymmetrinen liikenne tarkoittaa sitä, että tulevalla liikenteellä ja poistuvalla liikenteellä on eri reitti, vaikka kyseessä on samat lähde- ja kohdeosoitteet.

Asiakas pyysi tukea ongelmaan ja kysyi hinta-arvioista VRRP:n (Virtual Router Redundancy Protocol) konsultaatiotyöstä, sekä mahdollisesti verkkoympäristön auditointiin ja tarkastukseen. Ilmoitin asiakkaalle hinta-arviot konsultoinnista, sekä korjausehdotuksen rauhoittamaan floodingin tapahtumista. Ehdotus oli, että jos MAC (Media Access Control) -taulut eivät ole läheskään täynnä, voisi asiakas yrittää nostaa MAC-osoitteiden ikääntymisaikaa, mikä on muuttuja, joka vaikuttaa MAC-osoitteiden poistamiseen verkkolaitteilla.

Torstai 28.9.2023

Torstai aamu alkoi asiakaspalaverilla asiakkaan tiloissa. Palaverin aiheena oli uusi projekti, jossa yritykseni toimii ns. alihankkijana asiakkaan yritykselle erilaisissa ongelmanratkaisu- ja tukipyyntöasioissa. Iltapäivästä tuli vielä tukipyyntö toiselta asiakkaalta palomuuri puolella. Asiakkaan pyynnöstä lisäsin lisää oikeuksia yhdelle asiakkaan työntekijöistä. Kyseisellä työntekijällä oli pelkästään monitorointioikeudet, eikä hän siten pystynyt tekemään muutoksia muurille. Kyseessä oli Palo Alto Networksin VM-tyyppinen palomuuritoteutus. Siirryin palomuurin GUI-näkymään, josta etenin *device*-välilehden alla olevaan *administrators*-osioon. Valitsin käyttäjän jolle oikeudet tuli lisätä ja valikoin oikean käyttäjäprofiilin, johon tarvittavat oikeudet oli valmiiksi määritetty.

Perjantai 29.9.2023

Perjantaina minulla oli muuttopäivän vuoksi muuttovapaa.

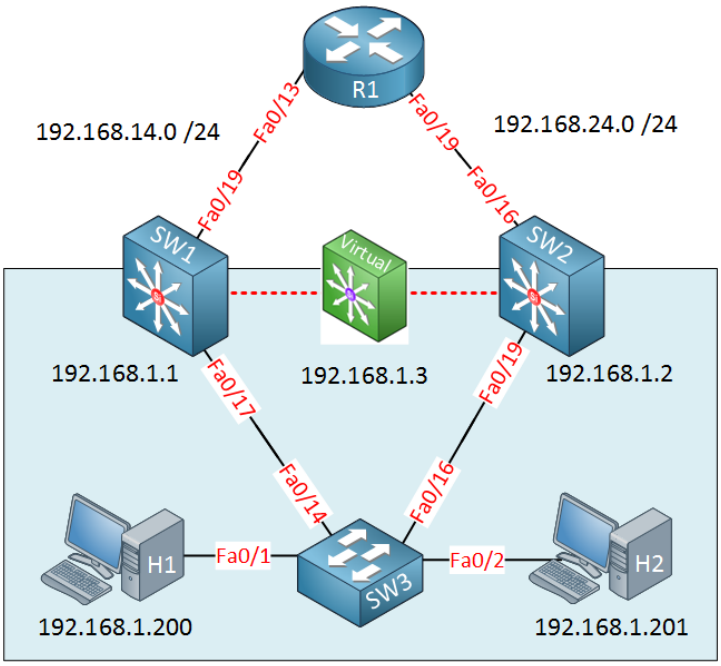
Viikkoanalyysi

Seurantaviikolla viisi, mieleenpainuvin aihe oli VRRP. VRRP:tä olen käsitellyt aikaisemmin JNCIS-ENT-sertifikaattikurssilla, mutta en ole koskaan miettinyt sen toteuttamista oikeassa ympäristössä.

Kurssin harjoitustehtävät antoivat kuitenkin kohtalaisen hyvän perehdytyksen sen konfigurointiin ja siihen, milloin sitä kannattaa käyttää.

VRRP eli Virtual Router Redundancy Protocol on viansietoisuuteen kehitetty protokolla. VRRP on määritelty IETF:n (Internet Engineering Task Force) toimesta standardissa RFC 3768. VRRP:llä on toinen hyvin samanlainen vaihtoehto, joka on HSRP (Hot Standby Routing Protocol). HSRP on Ciscon kehittämä ja omistama protokolla, jota ei voi käyttää muissa kuin Ciscon laitteissa. VRRP toimii hyvin yksinkertaisesti. Jos master-roolia ylläpitävä reititin menee jostain syystä vikatilaan, ottaa yksi VRRP-ryhmän varareititin master-roolin itselleen, jolloin liikenne jatkuu. Master-roolin reitittin lähettää oletusarvoisesti sekunnin välein viestejä varareitittimille, ja mikäli varareititin tai reitittimet eivät asetetun ajan aikana saa viestiä master-reitittimeltä, seuraavaksi korkeimman prioriteetin omaava reititin ottaa master-roolin itselleen. (Juniper Networks 1)

VRRP:tä on kahta eri laatua, VRRPv2, sekä VRRPv3. Siinä missä VRRPv2 tukee pelkästään IPv4-protokollaa, VRRPv3 tukee sekä IPv4-, että IPv6-protokollia. VRRP-protokolla toimii lähiverkossa, jolloin lähiverkon käyttäjät eivät tarvitse kuin yhden reitin reitittimelle, joka on yleisesti jo laitteilla oleva oletusreitti. Tämä reitti on edelleen kohdistettu virtuaalisen reitittimen IP-osoitteeseen eli VIP (Virtual IP address) -osoitteeseen. VRRP mahdollistaa myös useamman erinäisen instanssin luomisen, jolloin jokaisella instanssilla on oma VIP-osoite, jota voidaan käyttää aliverkkojen seuraavana hyppynä. Näiden instanssien avulla lähiverkon laitteet pystyvät liikennöimään ulkoverkon suuntaan halutun master-roolin omaavan reitittimen kautta. (study-ccnp)



Kuva 8. Havainnollistava kuva VRRP-protokollasta (Molenaar R. 2.)

Kuvasta 8 voidaan huomata keskellä oleva virtuaalireititin. Virtuaalireitittimelle on asetettu VIP-osoite 192.168.1.3. Kyseisessä kuvassa on käytössä kahden reitittimen välinen virtuaalireititin, joka on yleisin tapa toteuttaa VRRP.

Koska VRRP-protokolla on viansietoisuuteen kehitetty protokolla, on siinä aina vähintään kaksi reititintä käytössä. Reitittimille asetetaan identtiset VRRP-konfiguraatiot, jonka jälkeen ne keskustelevat keskenään ja dynaamisesti päättävät tiettyjen arvojen perusteella, mistä reitittimisestä tulee master-reititin ja mistä varareititin. Vaikka kaikilla reitittimillä olisikin oma staattinen IP-osoite, VRRP:tä konfiguroidessa määritetään myös VIP-osoite, joka toimii virtuaalisen reitittimen osoitteena. Liikennettä ei siis ohjata enää reitittimien omiin IP-osoitteisiin, vaan haluttu liikenne ohjataan tähän yhteen virtuaaliseen IP-osoitteeseen.

VRRP-protokolla konfiguroidaan reitittimillä porttitasolla. VRRP otetaan käyttöön luomalla reitittimillä numeraalinen uniikkitunniste virtuaaliselle reitittimelle. Muut VRRP:hen osallistuvat reitittimet konfiguroidaan myös saman numeraalisen tunnisteen alle. Virtuaalireitittimen käyttöönotto vaatii suoran yhteyden kaikkien virtuaaliseen reitittimeen osallistuvilla reitittimillä, jolloin liikenne pystyy kulkemaan mahdollisimman sujuvasti. VRRP-protokolla päättää reitittimillä olevan prioriteetin kautta, mistä reitittimestä tulee master ja mistä varareititin. Oletus prioriteetti reitittimillä on 100, mutta sitä pystyy konfiguroimaan manuaalisesti aina 0–255 välillä halutusti. Suurimman prioriteetin omaava reititin omaksuu master-roolin. Mikäli kahdella tai useammalla reitittimellä on samanaikaisesti yhtä suuri prioriteetti, se reititin, jonka VRRP-portilla on korkein IP-osoite, omaksuu master-roolin.

Virtuaalireititin on kriittinen osa ympäristöä, johon se on konfiguroitu. Sen vuoksi VRRP-ryhmälle voidaan asettaa autentikointi, joka tapahtuu konfiguroimalla osallistuvia laitteita. Yleinen tapa konfiguroida autentikointi VRRP-ryhmälle on MD5-salausta hyödyntävät avainparit. Kun yksi virtuaalireitittimeen osallistuvista reitittimistä lähettää dataa toisille, lähettävä reititin sisällyttää oman avaimensa lähetettyyn pakettiin. Vastaanottavat reitittimet vertaavat saapuneen paketin avainta omaansa, ja sen perusteella joko hylkää paketin tai vastaanottaa sen. Avainten tulee olla identtisiä, muuten reitittimet luokittelevat paketit kielletyiksi. Tämä estää kolmansia osapuolia pääsemästä liikenteeseen käsiksi tai rikkomasta verkkotopologiaa ottamalla master-roolin itselleen. (Arubanetworks 2)

3.6 Seurantaviikko 6

Maanantai 2.10.2023

Viikko alkoi yritykseni tukipyyntöjärjestelmän läpikäymisen kanssa. Keräsin tiistaina olevaa kuukausittaista katsausta varten dataa järjestelmästä, jonka voin esittää osastostani vastaavalle henkilölle. Datat jotka keräsin, olivat avatut tukipyynnöt syyskuun ajalta, tällä hetkellä avoinna olevat tukipyynnöt, sekä tukipyyntöjen ratkaisuajat asiakaskohtaisesti. Loin kerättyjen tietojen perusteella Powerpoint-esityksen helpottaakseni esitystä, sekä loin siihen erilaisia kuvaajia hahmottamaan tilannetta.

Tiistai 3.10.2023

Tiistai alkoi osastoni kuukausittaisella katsauksella. Palaveriin osallistui molemmat kollegat osastostani, projektikoordinaattori, yksi yritykseni ohjelmoija, sekä osastostani vastaava esihenkilö. Palaverissa kävimme läpi syyskuun aikana tulleet tukipyynnöt, sekä avoinna olevat tukipyynnöt. Palaverissa keskusteltiin myös tulevista mahdollisista asiakkuuksista ja teknologioista, joihin tulemme tarjoamaan tukipalvelua.

Palaverissa käytiin myös läpi käytäntöjen parannuksia ja mahdollisten päivystystilanteiden saavutettavuudesta, sillä minulle ja kollegoilleni tulee uusia projekteja työn alle. Pohdimme esimerkiksi sitä, olisiko puhelinvaihde hyvä ratkaisu siihen, että kaikki pyynnöt kohdistuvat yhdelle henkilölle niissä tilanteissa, kun muut ovat muissa työtehtävissä kiinni.

Keskiviikko 4.10.2023

Keskiviikkona oli hyvin varastopainotteinen päivä. Yrityksellemme oli saapunut kuormalavallinen kytkimiä, joihin tuli kiinnittää kytkinkaappia varten olevat kiinnikeraudat, sekä konfiguroida esikonfiguraatiot. Suoritin työtehtävää yhdessä kollegani kanssa. Kytkimiä, joita tuli valmistella, oli 43. Tämä tehtiin valmiiksi siksi, koska yrityksessäni on alkamassa projekti, jossa asiakkaiden kohteisiin tullaan asentamaan näitä kytkimiä. Näiden toimenpiteiden suorittaminen nopeuttaa asentamista, sillä niitä ei tarvitse tehdä asennuspäivinä, vaan ne voidaan suoraan hakea valmiina varastolta. Kiinnikerautojen asennus oli yksinkertaista ruuvausta. Esikonfiguraatiossa, jonka konfiguroimme, oli etähallintaa varten yhteydet, sekä tilapäinen käyttäjätunnus ja salasana sitä varten. Työtehtävässä meni lähes koko päivä, eikä muita työtehtäviä ehtinyt tekemään enää sinä päivänä.

Torstai 5.10.2023

Torstaina tuli tukipyyntöä asiakkaan palomuurin liikenteen sallimisesta. Asiakkaalla on käytössä HTTP (Hypertext Transfer Protocol) -proxy, eli tekniikka, joka toimii käyttäjän ja kohdeosoitteen välillä. HTTP-proxy suodattaa liikennettä, sekä tarkistaa sen haitallisten tekijöiden varalta. HTTP-proxyä käytettäessä myös kohdepalvelin näkee yhteyttä ottavan käyttäjän IP-osoitteena proxyn osoitteen.

Tukipyynnössä pyydettiin sallimaan liikenne HTTP-proxyltä heidän asiakkaansa gitlab-ympäristöön. Gitlab on palvelu, joka tarjoaa versionhallintaa, sekä muita tehtävienhallintatoimintoja. Kirjauduin asiakkaan palomuurin GUI-näkymään, josta siirryin Policies-välilehden alla olevaan security-osioon. Konfiguroin uuden palomuurisäännön asiakkaan toiveiden mukaisesti sallimaan liikenteen heidän asiakkaansa ympäristöön. Pyysin asiakasta vielä kokeilemaan toimiiko liikennöinti, ja kun sain varmistuksen, suljin tukipyynnön.

Perjantai 6.10.2023

Viikon päätepäivälle tuli kollegalta viestiä Ciscon SNS (Secure Network Server) -laitteiden asennuksesta ja esikonfiguroinnista. Laitteet olivat saapuneet edellisenä päivänä toimistollemme, eikä kollega päässyt itse toimistolle perjantaina. SNS-laitteille tuli asentaa ISE (Identity Service Engine), joka on tietoturvajärjestelmä, jonka avulla laitteet ja käyttäjät pystyvät autentikoitumaan ja pääsemään verkkoon.

Laitteisiin tuli asentaa ISE-järjestelmän versio 3.2, joka piti ladata erikseen Ciscon sivuilta. Tiedosto, joka ladattiin, oli ISO (identical storage image of optical media) -muotoinen, eli se on virtuaalinen versio CD, DVD, tai Blu-ray levystä. ISO-tiedostosta piti luoda liveUSB (Universal Serial Bus), eli USB-kiintolevyllä oleva valmis käyttöjärjestelmä, joka voidaan käynnistäessä ladata laitteelle. Kun live USB:n luonti oli valmis, asetin USB-kiintolevyn kiinni laitteeseen, josta valittiin käynnistysvaihtoehdoista USB. Käynnistin laitteen uudelleen, jonka jälkeen käyttöjärjestelmä alkoi asentumaan laitteelle. Samat toimenpiteet tuli tehdä vielä uudestaan, sillä käyttöjärjestelmään piti asentaa vielä päivityspaketti. Kun käyttöjärjestelmänpäivitykset olivat asentuneet, asetin esikonfiguraation laitteille, sekä kytkin ne yritykseni testiverkkoon.

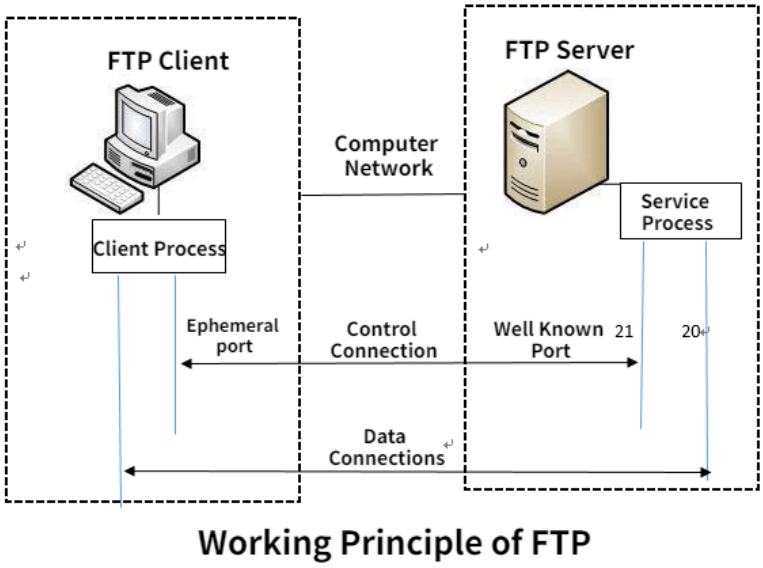
Viikkoanalyysi

Viikon aikana ei kovin paljon tullut uutta asiaa. Käytännössä kaikkia työtehtäviä olin tehnyt jo aiemmin, paitsi perjantain esiasennuksia. Perjantaina esiintyi ongelmaa käyttöjärjestelmätiedoston saamisessa laitteelle. Laitteella oli BIOS (Basic Input/Output System) -asetuksissa USB-portit jostain

syystä oletuksena pois käytöstä. En tätä huomannut kuin vasta iltapäivästä, ja ehdinkin jo suunnitella vaihtoehtoisia tapoja siirtää tiedosto. Ajattelin aluksi siirtäväni SFTP-protokollan avulla tiedoston laitteille, mutta tutkimisen jälkeen löysin laitteiden BIOS-asetuksista kyseiset USB-portti asetukset. Päätin kuitenkin tutkia enemmän, miten SFTP-protokolla ja FTP-protokolla johon SFTP perustuu, toimivat.

FTP eli File Transfer Protocol on protokolla ja applikaatio, jota käytetään tiedostojen ja hakemistojen siirtoon laitteiden välillä. FTP määriteltiin IETF RFC 959-standardissa. FTP toimii OSI-mallin applikaatiokerroksessa ja se toimii TCP/IP-protokollan päällä. FTP toimii asiakaspalvelin periaatteella. Asiakas-laite yleisesti tekee pyynnön aloittaa yhteys laitteiden välillä, johon palvelinlaite vastaa. Kun yhteys on muodostettu ja autentikointi on mennyt läpi, laitteet voivat siirtää tiedostoja molempiin suuntiin. Koska protokolla suunniteltiin tietokoneiden varhaisessa vaiheessa, sen turvallisuuteen ja yksityisyyteen ei kiinnitetty huomiota. FTP ei salaa yhteyttä, tiedostoja tai salasanoja, eikä sen avulla siirrettyjen tiedostojen eheydestä voida olla varmoja. Tämän vuoksi IETF onkin suositellut FTP-protokollaa käytettävän vain luotetuissa verkoissa, eikä julkisissa verkoissa. (SSH)

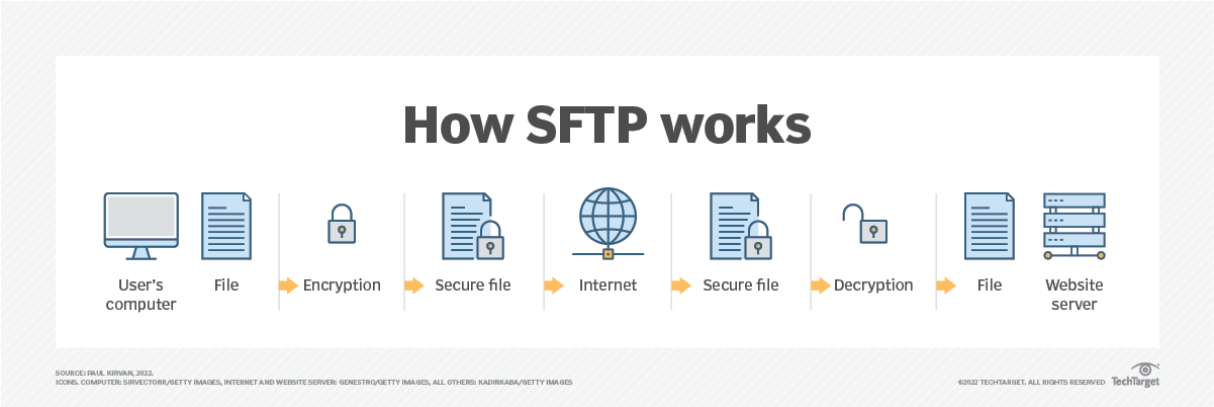
FTP-protokolla käyttää kahta erilaista yhteyttä. Ensimmäimäistä yhteyttä kutsutaan ohjausyhteydeksi. Ohjausyhteyden tarkoitus on esimerkiksi käyttäjän tunnusten ja salasanan lähettäminen, sekä tiedoston siirtokomentojen lähettäminen. Ohjausyhteys tapahtuu portin 21 kautta. Toinen yhteys on datayhteys. Datayhteyden tarkoitus on varsinainen tiedostojen lähetys ja siirto, ja se käyttää porttia 20. (Geeksforgeeks)



Kuva 9. FTP-protokollan toiminnan kuvaus (Raysync)

Kuvan 9 mukaisesti, FTP-istunnon aloitusvaiheessa asiakaslaite lähettää ohjausyhteys-pyynnön TCP-protokollan yli palvelinlaitteelle, jonka kautta tapahtuu esimerkiksi käyttäjätunnusten ja salasanan ilmoitus palvelinlaitteelle. Palvelin-laite saa pyynnön ja tekee datayhteyden aloituspyynnön asiakaslaitteelle. Yhden datayhteyden yli voi lähettää vain yhden tiedoston, jolloin uusi datayhteys tarvitaan useampien tiedostojen siirtoon. (Geeksforgeeks)

FTP-protokollan tietoturvallisuussyistä kehitettiin SFTP eli Secure File Transfer Protocol. SFTP-protokolla toimii SSH-protokollan päällä, käyttäen hyödykseen SSH-protokollan tarjoamia tietoturva- ja autentikointiominaisuuksia. Tämän vuoksi SFTP-protokolla onkin melkein kokonaan korvannut vanhemman turvattomamman FTP-protokollan, sillä se tarjoaa kaikki samat ominaisuudet kuin FTP-protokolla, mutta turvallisemmin ja helpommin konfiguroitavana. (SSH)



Kuva 10. SFTP-protokollan toiminta (Techtarget 2)

SFTP-protokolla toimii pohjimmiltaan samalla tavalla kuin FTP-protokolla. SFTP-protokollassakin on käytössä asiakaspalvelin tyyppinen toteutus. Komennot, joita laitteiden viestimiseen käytetään ovat samat. Erona kahden protokollan välillä on tietoturvallisuus. Kuten kuvasta 10 huomataan, SFTP-protokolla salaa tiedostot ennen kuin ne siirretään. SFTP-protokolla käyttää porttia 22, kuten SSH-protokolla. (Techtarget 2)

Koska SFTP-protokolla toimii SSH-protokollan päällä, SFTP-protolla käyttää SSH-protokollan avaimia tai muita kryptografisia avaimia salauksen tekoon. Näiden avainten avulla voidaan automatisoida ohjelmakoodien avulla käyttäjien pääsyä palvelinlaitteelle. SSH-avaimia käytettäessä toinen puolikas säilytetään asiakaslaitteella ja toinen puolikas palvelinlaitteella, joka on myös liitettynä julkiseen avaimeen. Kun SSH-avainparit ovat todettu täsmääviksi, käyttäjät voidaan autentikoida. Näiden avainparien vuoksi laitteet ovat myös suojattuja esimerkiksi man-in-the-middle-hyökkäyksiä

vastaan. Man-in-the-middle on hyökkäystapa, jossa hyökkääjä sijoittaa itsensä laitteiden väliin saadakseen liikenteessä kulkevan datan näkyviin itselleen. (Techtarget 2)

SFTP-protokollaa käytetään loppukäyttäjän puolella yleisesti jonkin SSH-protokollaa käyttävällä ohjelmalla. Näistä esimerkkejä ovat etähallintaa varten suunniteltu ohjelma PuTTy, sekä puhtaasti tiedostonsiirtoja varten kehitetyt WinSCP ja FileZilla. (SSH)

3.7 Seurantaviikko 7

Maanantai 9.10.2023

Viikko alkoi reissulla Länsi-Uudellemaalle. Lähdin kollegani mukaan Inkoon seudulle asiakkaan tiloihin päivittämään tukiasemia. Tukiasemat olivat vanhoja, joten ne tuli vaihtaa uudempiin laitteisiin. Rakennuksessa oli yhteensä 5 tukiasemaa. Asiakkaalta oli tullut tukipyyntö, että yhdessä huoneista ei toimi langaton verkko kunnolla. Tätä varten otimme mukaan langattoman verkon mittauslaitteen, jonka avulla pystymme mahdollisimman hyvin suunnittelemaan uuden tukiaseman sijaintia. Tukiasemien vaihto ja asennus olivat yksinkertaisia prosesseja. Otimme vanhat tukiasemat irti ja laitoimme uudet tilalle. Kiskot tai telineet eivät olleet laitteiden välillä yhteensopia, joten nekin vaihdettiin.

Tiistai 10.10.2023

Iltapäivästä saapui tukipyyntö asiakkaalta liittyen Juniperin käyttöjärjestelmäversioiden latausoikeuksiin. Asiakkaalla ei ollut oikeuksia ladata käyttöjärjestelmiä ja hänellä oli kiire saada päivitettyä laitteensa. Yritin luoda asiakkaalle CSAM-työkalun avulla käyttäjätunnukset, mutta työkalu herjasi asiakkaalla olevan jo käyttäjätunnus.

Koska asiakkaalla oli kiire saada uusi käyttöjärjestelmäversio, on Juniperin tapauksessa mahdollista jakaa eteenpäin latausosoite, jonka kautta voi 15 minuutin aikana ladata valitun käyttöjärjestelmän. Lataus tehtiin siis käytännössä minun tunnuksillani, mutta asiakkaalla ei ollut mahdollisuutta tehdä mitään muuta osoitteen kautta, kuin ladata käyttöjärjestelmä. Kun asiakas oli saanut ladattua käyttöjärjestelmän, avasin TAC-pyynnön Juniperille, missä pyysin TAC-henkilöä poistamaan asiakkaan olemassa olevan käyttäjätunnuksen. Ongelma jäi vielä keskiviikolta auki, sillä asiakkaan tunnuksissa oli toisen yrityksen puolesta myönnetty oikeuksia, eikä niitä vielä saatu poistettua.

Keskiviikko 11.10.2023

Keskiviikkona saapui mielenkiintoinen tukipyyntö. Asiakas oli kohdannut heidän reitittimellään jälleen linjakorttivikoja. Ongelmia löytyi myös heidän reitityspuoleltansa. Asiakkaan kahdennettu reititys ei toiminut oikein, sillä kun toinen reitititimistä meni vikatilaan, laitteiden tulisi automaattisesti

ohjata liikenne toimivalle reitittimelle. Tätä ei kuitenkaan jostain syystä tapahtunut, vaan laitteet yrittivät virheellisesti ohjata liikenenttä vialliselle reitittimelle.

Koska kyseessä oli suuri ympäristö ja käytössä oli monia eri protokollia kuten EVPN (Ethernet Virtual Private Network) ja MPLS (Multiprotocol Label Switching), pyysin tukea yritykseni yhdeltä kokeneemmalta asiantuntijalta ongelman hoitamiseen. Otin itse vastuun viallisen linjakortin hoitamisesta korvattavaksi, mutta en kokenut, että tuntemukseni käytetyistä teknologioista olisi ollut tarpeeksi hyvä, joten kollegani otti hoidettavakseen reititys- ja kahdennusongelmat.

Torstai 12.10.2023

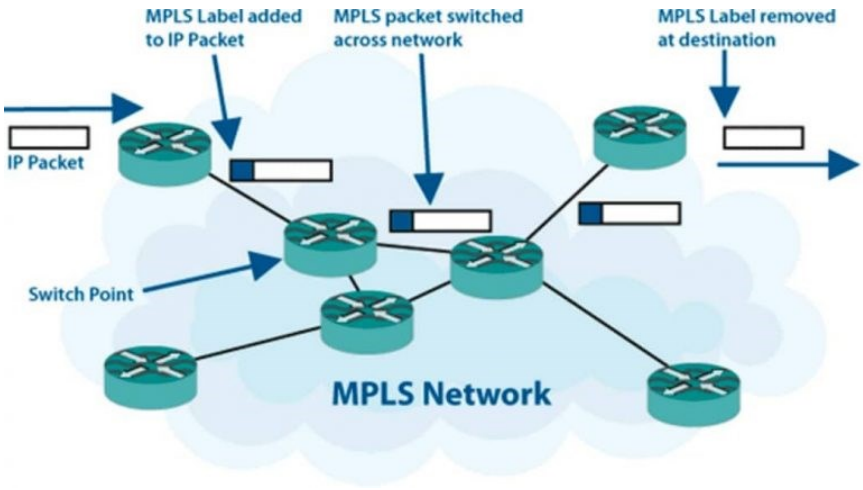
Torstai jatkui keskiviikon tukipyynnön parissa. Pyysin asiakasta käyttämään viallista linjakorttia laitteesta ulkona ja laittamaan takaisin sisään. On melko yleistä, että komponentit saattavat mennä vikatilaan, vaikka ne olisivatkin ehjiä. Tällä tavalla on mahdollista poistaa se vaihtoehto, että olisikin vain jokin kosketushäiriö tai pienempi virhe laitteessa. Seurasin myös aktiivisesti viestinvaihtoa toisen asiantuntijan ja asiakkaan välillä, sillä tämänkaltaisista vianselvitysprosesseista voi oppia todella paljon.

Perjantai 13.10.2023

Perjantaina oli kokousta tulevasta projektista, joka on suunniteltu alkavaksi seuraavalla viikolla. Lähden kollegani kanssa työmatkalle Kuopioon, jossa on tarkoitus kartoittaa ja mahdollisesti asentaa uudempaa laitteistoa erinäisiin toimipisteisiin. Siirsin samalla toiselle servicedeskissä työskentelevälle kollegalleni auki olevat tukipyyntöni, sillä en välttämättä kykene vastaamaan asiakkaille ensi viikon aikana. Suunnittelimme myös kollegani kanssa tulevaa viikkoa ja valmistelimme tarvitsemamme työkalut ja laitteet, mitä otamme mukaan työmatkalle.

Viikkoanalyysi

Viikosta jäi päällimmäisenä mieleen keskiviikon ja torstain ongelma. Huomasin tukipyyntöä ratkoessa, että oma osaaminen käytettyjen protokollien parissa oli hyvin minimaalista, ja päätinkin tutkia enemmän MPLS-protokollaa.



Kuva 11. Havainnollistava kuva MPLS-protokollan toiminnasta (Mushroomnetworks)

MPLS eli Multiprotocol Label Switching on protokolla, jossa paketit leimataan reititystä varten sen sijaan, että käytettäisiin IP-osoitteita reititykseen. (Kuva 11) Ilman MPLS-protokollaa reititys tapahtuu siten, että jokainen laite joka paketin vastaanottaa, tarkistaa kohde IP-osoitteen, tekee reititys-haun, käy läpi reititystaulut ja päättää niiden perusteella mihin seuraavaan hyppyyn paketit ohjataan. MPLS-protokollaa käytettäessä vain ensimmäinen laite selvittää mitä reittiä paketti kulkee. Sen sijaan, että se etsisi seuraavan hypyn, laite etsii lopullisen määränpään ja reitin kyseiseen määränpäähän. MPLS-leima lisätään pakettiin, joka sisältää neljä eri kenttää. Ensimmäinen kenttä on kooltaan 20-bittinen ja se osoittaa mihin paketti ohjataan. Toinen kenttä on kooltaan kolme bittinen ja sitä käytetään nykyisin enimmäkseen QoS (Quality of Service) -prioriteetin määrittämiseen. Kolmas kenttä on vain yhden bitin kokoinen, joka lisättäessä ilmoittaa, kun paketti on saavuttanut MPLS-verkon viimeisen laitteen. Viimeinen kenttä on TTL (Time to Live) -kenttä, joka on kahdeksan bitin kokoinen. TTL on arvo, joka vähenee aina kun paketti siirtyy laitteelta toiselle. TTL on oleellinen tekniikka estämään verkon hidastumista niissä tilanteissa, joissa paketti jää pyörimään verkkoon, eikä saavuta lopullista määränpäätä. (Checkpoint)

Reittiä, mitä MPLS-protokollalla lähetetyt paketit käyttävät, kutsutaan LSP (Label-Switched Path) -reitiksi. Verkon muut laitteet, jotka ovat konfiguroitu käyttämään MPLS-protokollaa ja minkä kautta paketti kulkee, poistavat edellisen laitteen laittaman leiman paketista ja lisäävät uuden. Viimeisin laite, joka vastaanottaa paketin, poistaa leiman paketista ja toimittaa sen kohdeosoitteeseen. (Juniper Networks 2)

MPLS-protokolla määriteltiin IETF RFC 3031 -standardissa. Se toimii OSI-mallin siirtoyhteyskerroksen ja verkkokerroksen välissä. Siirtoyhteyskerros kuljettaa IP-paketteja lähiverkkojen tai point-to-

point WAN (Wide Area Network) -verkkojen välillä. Verkkokerros vastaavasti käyttää Internetin laajuisia osoitteita ja reititystä IP-protokollien avulla. MPLS sijaitsee siis näiden kahden kerroksen välillä, koska se hyödyntää molempien kerroksien teknologioita. (Paloaltonetworks 2)

MPLS-protokolla tarjoaa erityisesti hyötyjä Internet-palveluntarjoajapuolella, sekä yritysten sivukonttorien yhdistämisessä yrityksen konesaliin tai pääkonttoriin. Koska MPLS-protokolla käyttää reitityksessään leimoja, se vähentää edelleenlähetystaulun käyttöä. Edelleenlähetystaulut ovat yleisesti kokonsa puolesta rajoitettuja riippuen käytetyistä laitekomponenteista, jolloin MPLS-protokollan käyttö myös mahdollistaa edullisempien verkkolaitemallien käytön, joissa on pienempi edelleenlähetystaulun koko. Tämän lisäksi MPLS-protokolla tarjoaa myös mahdollisuuden hallita sitä, miten ja mihin liikenne ohjataan verkossa. MPLS-protokollan toimenpiteet tehostavat verkon toimivuutta, sekä tekee siitä luotettavamman. (Juniper Networks 2)

Muita MPLS-protokollan hyötyjä ovat esimerkiksi protokolla riippumattomat yhteydet, sekä tietoturvallisuus. MPLS-protokollan avulla voidaan kuljettaa datapaketteja millä protokollalla haluaa, oli se sitten Ethernet-, Transport over IP-, ATM (Asynchronous Transfer Mode) -, tai Frame Relay-protokolla. (Arubanetworks 3)

Vaikka MPLS-protokollan käytön ensisijainen tarkoitus on tehostaa verkkoa ja tehdä siitä luotettavampi, on sillä myös tietoturvallisia ominaisuuksia. Vaikka MPLS-verkon yhteydet eivät ole salattuja, ovat ne erillisessä osiossa verrattuna muuhun Internet-verkkoon, jolloin MPLS-verkon yhteydet tarjoavat tietoturvallisuutta samaan tapaan kuin VPN-verkko. (Checkpoint)

MPLS-protokollalla on myös haittapuolia hyvien ominaisuuksien rinnalla. MPLS-verkon keskitys, kustannukset, maantieteelliset rajoitukset, sekä saatavuusviiveet ovat esimerkkejä näistä. Keskityksellä tarkoitetaan MPLS-verkon reitittämistä esimerkiksi yrityksen konesalin kautta. Nykyään ihmiset yhä enemmän työskentelevät etänä ja pilvipohjaiset ratkaisut yleistyvät, on reititys konesalin kautta mahdollisesti hitaampaa kuin muilla tekniikoilla. Etenkin ulkomailla kustannukset ovat myös huomattavasti korkeammat kuin silloin, jos käytettäisi tavallista laajakaistaa. Koska MPLS-tekniikan vaatimat yhteydet ovat Internet-palveluntarjoajien omistuksessa ja ositettu julkisesta verkosta, on mahdollista kohdata maantieteellisiä rajoituksia sen suhteen, missä MPLS-protokolla voidaan ottaa käyttöön. Saatavuusviiveellä tarkoitetaan edellä mainittuja MPLS-yhteyksiä, sillä yhteyksien toimitus voi olla Internet-palveluntarjoajilta hidasta. (Checkpoint)

3.8 Seurantaviikko 8

Maanantai 16.10.2023

Maanantaina oli aamusta yritykseni viikkopalaveri. Viikkopalaverin aikana tuli puhelu asiakkaalta liittyen kytkimen porttimuunnoksiin. Laitteelle haluttiin liittää PoE-virran yli videokamera, eikä kytkin suostunut antamaan portin kautta tarpeeksi virtaa kameralle oletusasetuksilla. Siirryin asiakkaan hyppykoneen kautta kytkimelle ja konfiguroin portin antamaan aina staattisesti 30W sähkövirtaa kytketylle laitteelle, jonka jälkeen asiakas ilmoitti kameran lähteneen toimimaan. Iltapäivästä kello yhden ja kahden välissä lähdimme kollegani kanssa ajamaan Kuopiota kohti työmatkalle, minkä parissa menikin koko loppupäivä.

Tiistai 17.10.2023

Tiistaina Kuopiossa olevan asiakkaan toimipisteessä tuli asentaa uusia kytkimiä vanhojen EoL (End of Life) -laitteiden tilalle. EoL-laitteet tarkoittavat laitteita, joiden elinkaari on loppunut. Tässä tilassa olevat laitteet eivät saa laitevalmistajalta enää päivityksiä, eikä niitä myydä enää. Lähdimme kollegani kanssa hakemaan asiakkaan toimistolta sinne saapuneet uudet Juniper EX-sarjan kytkimet, sekä ACX-sarjan reitittimet. Toimipisteestä meillä ei ollut kovinkaan paljon ennakkotietoja, joten jouduimme myös kartoittamaan teletilojen sijainnit, sekä toimipisteen ristikytkennät. Teletiloja ja sitä myöten jakamoita oli kaksi, ja ne sijaitsivat eri puolilla rakennusta. Asensimme kytkimet ja reitittimet ja kytkimme Ethernet-kaapelit sekä valokuidut uusiin kytkimiin vanhoista.

Keskiviikko 18.10.2023

Keskiviikko jatkui hyvin samankaltaisella toimenkuvalla kuin tiistai. Valmistelimme kollegani kanssa erään toimipisteen tietoliikenneyhteyksiä tulevaa yliheittoa varten. Asensimme jälleen kahteen eri teletilaan kahdet kytkimet kumpaankin. Erityisesti haasteita osoittautui tällä kertaa edellisten asentajien tekemien ristikytkentöjen vuoksi. Kaapin avattuamme, oli Ethernet-kaapelit yhdistetty laitteiden välillä hyödyntämättä lainkaan kaapelikouruja, joten jouduimme selvittelemään solmuja molemmissa teletiloissa. Myös tuotannossa olevat kytkimet oli asennettu kaappiin siten, että jouduimme siirtämään niitä. Itse laitekaappi oli erikoisesti suunniteltu, sillä kaapelikouruja piti paikallaan ruuvit, jotka tuntuivat olevan liian pitkiä kyseiseen kaappiin. Ruuvit estivät laitteiden asennuksen yhdestä kohtaa, sillä kytkimet eivät leveydeltään mahtuneet kyseisiin kohtiin.

Torstai 19.10.2023

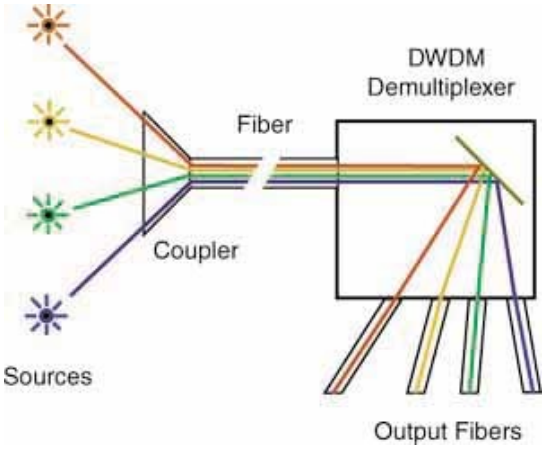
Torstaina työskenneltiin samalla teemalla kuin aiemmin samalla viikolla. Asennettavana oli tällä kertaa kolme kytkintä ja kaksi reititintä. Kytkimet olivat jälleen Juniperin EX-sarjan kytkimiä, ja reitittimet ACX-sarjan reitittimiä. Kytkimet piti kytkeä valokuitukaapeleiden ja optiikoiden avulla reitittimiin. Ongelmia ei juuri esiintynyt, mutta hidasteita ilmeni. Optiikat, joita asensimme eivät olleet bidirectional-optiikoita, eli sellaisia optiikoita, joiden avulla voidaan sekä lähettää että vastaanottaa saman kaapelin avulla. Tämän vuoksi yhteys ei jokaisen fyysisen yhteyden kautta heti toiminut, joten mietimme aluksi kaapelien päiden olevan likaisia. Puhdistimme kaapelit, mutta sekään ei nostanut yhteyttä toimivaksi. Syynä ongelmaan esiintyi kaapelien päiden sekottuminen. Koska toinen kaapeleista, joita optiikkaan kytketään, toimii vain vastaanottaen ja toinen lähettäen, olivat ne menneet ristiin kytkimen ja reitittimen välillä. Tarkastettuamme kaapelien oikein asennukset, lähti yhteydet toimimaan.

Perjantai 20.10.2023

Perjantaina tehtäväksi tuli kartoittaa kolme kohdetta tulevia asennuksia varten. Ensimmäinen kohde meni helposti ja saimme huoltomiehen avaamaan meille teletilojen ovet. Dokumentoimme ja kuvasimme ristikytkentäpaneelit, sekä selvitimme mistä jakamosta tulee mihinkin huoneeseen yhteydet seinärasioihin. Toisessa kohteessa esiintyi ongelmia, sillä emme päässeet katsomaan rakennuksen pääjakamoa, sillä edes huoltomiehellä ei ollut avaimia sinne. Tässä kohteessa olisi pitänyt soittaa puhelinoperaattorille, minkä kautta heidän henkilönsä olisi tullut avaamaan jakamon oven. Asiaa ei kuitenkaan keretty samanpäivän aikana hoitamaan, joten kartoitimme vain kerroksissa sijainneet jakamot. Kolmanteenkaan kohteeseen emme päässeet, koska ovenavaukset jakamoihin olisi pitänyt tehdä tilaustyyppisesti rakennuksen huoltoyhtiölle. Saman päivän aikana tapahtuvat avaukset olisivat maksaneet todella paljon, joten päätimme projektipäällikön kanssa tehdä sen seuraavalla reissulla Kuopioon. Loppupäivä kuluikin ajaessa kotiinpäin.

Viikkoanalyysi

Viikko kului Kuopiossa erilaisissa asennus- ja kartoitustehtävissä. Uutta asiaa ei tullut kovinkaan paljon, vaan olin aikaisemmin työurani aikana tehnyt hyvin samankaltaisia tehtäviä. Yksi uusi asia kuitenkin löytyi torstailta, nimittäin kuitujen kytkemisen parissa tapahtunut ongelma. Olen aikaisemmin kytkenyt valokuituja yleisesti bidirectional-optiikoilla, eli kaksisuuntaisilla optiikoilla, joissa lähetys ja vastaanotto tapahtuu saman kuidun kautta. En siis ollut kohdannut kyseistä ongelmaa aikaisemmin, mutta oli hyvä oppia siitä tulevaisuuden kannalta. Päätinkin siis tutkia enemmän CWDM (Coarse wavelength division multiplexing) -, sekä DWDM (Dense wavelength division multiplexing) -tekniikkaa.

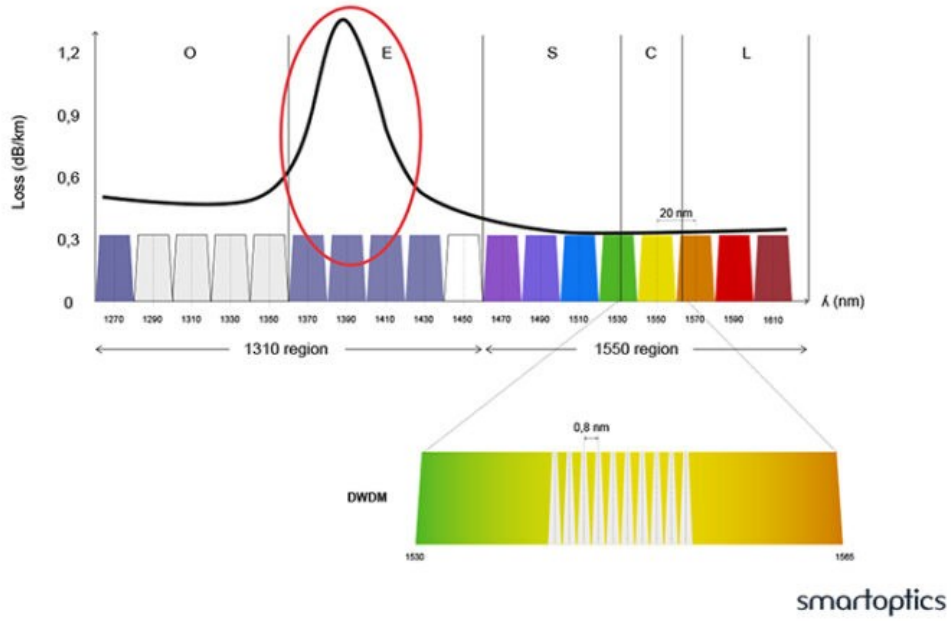


Kuva 12. Havainnollistava kuva valon aallonpituuksien hajauttamisesta käyttäen lähtövalitsinta. (FOA)

WDM eli wavelength division multiplexing on tekniikka, jonka avulla voidaan kuljettaa erinäisiä dataliikenteitä saman valokuitukaapelin kautta. Valo lähetetään kuitukaapeliin käyttäen eri aallonpituuksia, joka estää liikenteiden sekoittumisen kuljetuksen aikana. (FOA)

Kaksi käytetyintä tekniikkaa, joita käytetään aallonpituuksien ohjaamiseen eri suuntiin, ovat CWDM-tekniikka, ja DWDM-tekniikka. Kumpikin näistä tekniikoista ovat protokolla riippumattomia, mikä tarkoittaa sitä, että mitä tahansa esimerkiksi videon, äänen tai datan yhdistelmää voidaan käyttää eri aallonpituuskanavilla. CWDM-tekniikan ja DWDM-tekniikan erona onkin se, kuinka eri kanavat on sijoiteltu sähkömagneettisella spektrillä. Kuten kuvasta 12 havaitaan, eri valon aallonpituuksilla tulevat lähteet jaetaan kuvan mukaisesti neljään eri kanavaan käyttäen lähtövalitsinta. (smartoptics)

Lähtövalitsin ja tulovalitsin ovat erillisessä laitteessa olevia virtapiirejä, joiden tehtävänä on säädellä lähetettyä ja vastaanotettua valoa. Lähtövalitsimen tehtävä on jakaa yksi sisään tuleva signaali useampaan eri lähtevän signaalin kanavaan ja se toimii lähettävässä päässä liikennettä. Tulovalitsin toimii päinvastoin kuin lähtövalitsin. Tulovalitsin jakaa yhden uloslähtevän signaalin useampaan eri signaaliin ja se toimii vastaanottavassa päässä. (Teja R.)



Kuva 13. Valon aallonpituudet ja kanavat (smartoptics)

Kuten kuvasta 13 havaitaan, CWDM-tekniikka tukee yhteensä 18 eri aallonpituus kanavaa, jonka kautta voidaan lähettää samanaikaisesti liikennettä käyttämättömän valokuidun kautta. Jokainen näistä kanavista on toisistaan erillään 20 nanometrin välein. CWDM-tekniikkaa hyödyntäessä käytetään yleisesti kahta eri aallonpituusaluetta, 1310 nanometristä ja 1550 nanometristä. 1550 nanometrinen aallonpituusalue on suosituin, sillä sitä hyödynnettäessä valonlähetyksessä havaitaan vähemmän häviötä kuidussa. CWDM-tekniikka tukee 10 gigabittisiä tiedonsiirtonopeuksia, ja haaroitetulla kuidulla 40 gigabittisiä nopeuksia. CWDM-tekniikalla tehdyt yhteydet ovat yleisesti halvempia toteuttaa kuin DWDM-tekniikalla toteutetut, mutta samalla tiedonsiirtonopeudet ovat heikommat. (smartoptics)

CWDM-tekniikkaa voidaan käyttää aina 70 kilometriin asti. Yli 40 kilometrin matkoilla CWDM-tekniikka kohtaa kuitenkin rajoituksia. Aallonpituuskanavat rajoittuvat yhdeksään toimivaan kanavaan johtuen kuiduissa käytetyistä materiaaleista, joka johtaa valonhäviöön kuidussa. Kuvassa 13 ympyröidyt 1370 nanometristä 1430 nanometriin olevat aallonpituusalueet kärsivät häviöstä nelinkertaisesti verrattuna 1550 nanometriseen aallonpituusalueeseen. (smartoptics)

DWDM-tekniikka vastaavasti tukee yhteensä 80 eri aallonpituus kanavaa samanaikaisesti, joissa jokainen kanava on 0,8 nanometrin etäisyydellä erillään toisistaan. Kuten kuvasta 13 voidaan huomata, DVDM-tekniikan käyttämät kanavat sijaitsevat enimmäkseen 1530 nanometrin ja 1550 nanometrin välillä silloin, kun tarkastellaan CWDM-tekniikan käyttämiä aallonpituusalueita. Oletuksena

DWDM-yhteyksiä voidaan toteuttaa aina 80 kilometriin asti, mutta vahvistamalla yhteyksiä erinäisillä laitteilla niistä voidaan tehdä jopa yli 1000 kilometrin pituisia. CWDM-tekniikan nopeuksiin eroten DWDM-tekniikalla toteutetut yhteydet saavuttavat 100 gigabitin tiedonsiirtonopeuden jokaista aallonpituuskanavaa kohden. (smartoptics)

4 Pohdinta

Päiväkirjamuotoinen opinnäytetyö oli elämäntilanteeni kannalta todella hyvä. Olen vakituisessa ja täysipäivisessä työsuhteessa, jonka vuoksi aikaa ylimääräiseen tutkimiseen ei jää kovin paljoa. Päiväkirjamuotoisessa opinnäytetyössä pystyin kertomaan päivittäisistä työtehtävistäni, sekä viikkoanalyysien muodossa kehittää omaa osaamistani, sekä seurata sen kasvua.

Päiväkirjamerkinnät toteutin jokapäiväisesti, mutta analyysien kirjoittaminen kohdistui yleensä viikonlopuille työ- ja arkikiireiden vuoksi. En kokenut päivittäistä kehittymisen seurantaa erityisen realistiseksi tavoitteeksi ja huomasin sen seurannan olevan hankalaa myös viikkotasolla. Päivittäistä kehittymistä ei kuitenkaan välttämättä joka päivällä tapahdu, vaan työtehtäviksi saattavat asettua entuudestaan tutut rutiininomaiset työtehtävät. Viikkotasolla kehittymisen seuranta oli samasta syystä hankalaa, jonka vuoksi kehittymisen seuranta tapahtuikin enimmäkseen itsenäisellä opiskelulla kohdatuista tekniikoista.

Seurantajakso opinnäytetyön aikana jätti mielestäni toivomisen varaa. Yrityksessä, jossa työskentelin seurantajakson aikana, oli tavallista hiljaisempaa seurantajakson viikkojen aikana. Tämän vuoksi työtehtävät olivat hyvin rutiininomaisia työtehtäviä, joita kohdataan kyseisessä työssä jatkuvasti. Uusia tekniikoita tai protokollia ei kovin montaa tullut eteen, vaikka niitäkin mahtui lähes jokaiselle viikolle vähintään yksi. Sain kuitenkin viikkoanalyysien avulla syvennyttyä enemmän tekniikkoihin ja protokolliin, joita opin ja käytin työtehtävissäni.

Kehitystä omassa taidossani huomasin kuitenkin melko paljon seurantajakson ajalta. Vaikka erilaisia työtehtäviä ei tullutkaan minulle hirveän montaa, opin enemmän ja enemmän suoriutumaan niistä itsenäisesti. Esimerkiksi porttimuunnoksia tehdessäni Ciscon kytkimillä, toistoista tuntui olevan suuri apu kehittymiseen, sillä hiljakseen ne alkoivat tapahtumaan rutiininomaisesti. Osasin entistä nopeammin ja tehokkaammin tehdä asiakkaiden pyytämiä muunnoksia, sekä tehdä niitä ulkomuistista sen sijaan, että tarvitsisin dokumentaatiota avuksi. Näihin voi esimerkkinä käyttää porteille määritettyjä VLAN-verkkoja. Sen sijaan, että yksi kerrallaan osoittaisin portteihin tietyn VLAN-verkon, opin tekemään sen käyttämällä komentoja, joiden avulla kaikkiin tarvittuihin portteihin saatiin asetettua sama tietty VLAN-verkko.

Koen saaneeni eniten kehitystä tietoliikenneasiantuntijana suorittamastani Juniper Networksin tuottamasta JNCIS-ENT-sertifikaattikurssista. Kyseisen kurssin sisältönä olivat Juniper Networksin asteikolla specialist-tason osaamiset kytkimistä, sekä reitittimistä. Sertifikaattikurssi opetti minulle paljon erilaisista kytkimiin sovellettavista tietoturvatekniikoista, kytkimien sekä reittitimien konfiguraatioista, sekä reititysmenetelmistä kuten BGP, OSPF, ja ISIS. Iso apu kehittymiseen Juniperin laittei-

den parissa olivat harjoitustehtävät, joita kurssin aikana suoritin. Lähes jokaisesta kurssin osa-alueesta oli harjoitustehtäviä ja niiden myötä sai myös vähän käytännön kokemusta aiheista pelkän teorian sijaan.

Kehitystä tapahtui myös selkeästi asiakaspalvelupuolella. Ammattikielenkäyttö ja ymmärrys asiakkaan ongelmia kohtaan kokivat kohdallani valtavia kasvuja. Empatiakyky asiakkaan kiiretilannetta ja ongelmaa kohtaan ovat kuitenkin avainasemassa tukipalvelussa työskennellessä, jolloin opin myös ajanhallinnan kannalta priorisoimaan tiettyjä tehtäviä, jos työnalla oli useampia tukipyyntöjä samanaikaisesti. Myös keskustellessa tilanteissa, joissa asiakas ei välttämättä aina ollut kovin tekninen henkilö, tuli minun osata selittää asiat hänelle sillä tavalla, jolloin myös tietoliikenteestä ymmärtämätön henkilö sai selkoa.

Ongelmanratkaisutaitoni ovat kehittyneet myös melko paljon. Mieleen tulee seurantajakson ajalta ainakin tukiaseman toimimattomuuden selvittäminen. Opin askel kerrallaan purkamaan ongelmaa siitä päästä lähtien, mikä vaikutti todennäköisimmältä ongelman juurisyyn sijainnilta. Langattomat verkot eivät olleet entuudestaan minulle kovin tuttuja, joten niiden ongelmienratkaisu oli haastavaa. Kyseisen tukipyynnön parissa jouduinkin osaamattomuuteni vuoksi opiskelemaan Ciscon materiaaleja, sekä vianselvitysvaiheita kyseisestä tuotteesta. Vaikka ongelma sijaitsikin kyseisen laitteen ulkopuolella olevassa PoE-injektorissa, oli silti mielenkiintoista tutkia, mitä tukiaseman lähettämät lokitiedostot kertoivat ongelmasta. Ongelmanratkaisussakin on siis yhä paljon kehitettävää, jotta löytäisin nopeammin ja helpommin ongelman juurisyyn.

Epäonnistumisiakin tuli kuitenkin vastaan opinnäytetyön aikana, joista viimeisimpänä on mieleen jäänyt valokuitujen kytkemisessä tapahtunut ristiinmeno. Reitittimien välinen yhteys ei lähtenyt toimimaan, mutta siitäkin selvisin tutkimalla tarkemmin kytkentöjä ja valokuitutekniikkaa. Onnekseni työnantajan puolesta on mahdollisuus opiskella monilta eri laitevalmistajilta materiaaleja, jotka selkeyttävät tekniikkojen yksityiskohtia, sekä niiden ongelmanratkaisuja. Tähänkin ongelmaan löysin erään laitevalmistajan keskustelupalstan kautta vinkin, että kytkennät saattavat olla ristissä.

Tulevaisuudessa tulen opiskelemaan entistä enemmän erilaisia tekniikoita. Ala, jolla työskentelen, on kuitenkin jatkuvasti kasvava ja kehittyvä, joten oppiminen ei tule loppumaan ikinä. Sertifikaateista saa todella hyvin ymmärrystä erilaisista käytetyistä tekniikoista, sekä laitevalmistajien tuotteista. Niiden opiskeluun tulenkin tulevaisuudessa käyttämään todennäköisesti todella paljon aikaa, ja sitä kautta pystyn myös kehittämään osaamistani eri asioissa. Tällä hetkellä on suunnitelmissa aloittaa seuraavan vuoden aikana opiskelu professional-tason sertifikaatteja varten, sekä myös langattoman verkon puoleen.

Sertifikaatit ei mielestäni itsessään kuitenkaan anna kovin hyviä valmiuksia työtehtävien suorittamiseen. Vaikka eri tekniikoista saa todella hyvän teoreettisen osaamisen, kurssien harjoitustehtävät eivät kuitenkaan aina heijastu suoraan työtehtävien käytännölliseen osuuteen. Sen vuoksi pyrin osallistumaan mahdollisimman usein erilaisiin projekteihin myös tulevaisuudessa, joista voi hyvin saada oppia kokeneemmilta asiantuntijoilta, sekä paremmin käytännönkokemusta, kuin kurssien harjoitustehtävistä.

Lähteet

Arubanetworks 1. S.a. Power-over-Ethernet (PoE). Luettavissa: https://www.arubanetworks.com/techdocs/AOS-CX/10.11/HTML/monitoring_6300-6400/Content/Chp_PoE/pow-ove-eth-oveview.htm. Luettu: 12.9.2023

Arubanetworks 2. S.a. Virtual Router Redundancy Protocol (VRRP). Luettavissa: https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7858/Content/Chp_VRRP/vir-rou-red-pro-vrr.htm. Luettu: 1.10.2023

Arubanetworks 3. S.a. What is MPLS? Luettavissa: https://arubanetworks.com/faq/what-is-mpls/. Luettu: 21.10.2023

CactusVPN. S.a. VPN Encryption (All You Need to Know) Luettavissa: https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-encryption/. Luettu: 16.9.2023

Checkpoint. S.a. What is Multiprotocol Label Switching (MPLS)? Luettavissa: https://www.checkpoint.com/cyber-hub/network-security/what-is-mpls/. Luettu: 21.10.2023

Cisco 1. 15.4.2008 Enterprise Campus 3.0 Architecture: Overview and Framework. Luettavissa: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html. Luettu: 5.9.2023

Cisco 2. S.a. Configuring EtherChannels. Luettavissa: https://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/trash/swethchl.html. Luettu: 5.9.2023

Cisco 3. 2.12.2021. Cisco Aironet 2800 Series Access Points Data Sheet. Luettavissa: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2800-series-access-points/datasheet-c78-736497.html. Luettu: 5.9.2023

FOA. S.a. Wavelength Division Multiplexing (WDM). Luettavissa: https://www.thefoa.org/tech/dwdm.htm. Luettu: 4.11.2023

Fortinet. S.a. What is SSL VPN? Luettavissa: https://www.fortinet.com/resources/cyberglossary/ssl-vpn. Luettu: 16.9.2023

FS 1. 20.1.2023. What is an aggregate switch? Luettavissa: https://community.fs.com/blog/what-is-an-aggregate-switch.html. Luettu: 5.9.2023

FS 2. Charlene. 24.3.2022. Understanding PoE Standards and PoE Wattage. Luettavissa: community.fs.com/blog/understanding-poe-standards-and-poe-wattage.html. Luettu: 12.9.2023

FS 3. Charlene. 13.7.2021. What Is a PoE Injector and How to Use it? Luettavissa: https://community.fs.com/blog/what-is-poe-injector-how-to-use-it.html. Luettu: 12.9.2023

FS 4. Charlene. 24.6.2020. What is PoE Splitter and How Does It Work? Luettavissa: https://community.fs.com/blog/what-is-poe-splitter-and-how-does-it-work.html. Luettu: 12.9.2023

Geeksforgeeks 2. 24.3.2023 File Transfer Protocol (FTP) in Application Layer. Luettavissa: https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/. Luettu: 15.10.2023

HPE. S.a. NTP Architecture. Luettavissa: https://techhub.hpe.com/eginfolib/networking/docs/switches/12500/5998-4870_nmm_cg/content/378584213.htm. Luettu: 23.9.2023

Huawei. 30.9.2023. What is NTP? Luettavissa: https://info.support.huawei.com/info-finder/encyclopedia/en/NTP.html. Luettu 23.9.2023

Juniper Networks 1. 9.5.2023. Understanding VRRP. Luettavissa: https://www.juniper.net/documentation/us/en/software/junos/high-availability/topics/concept/vrrp-overview-ha.html. Luettu: 1.10.2023

Juniper Networks 2. 16.6.2023. MPLS Overview. Luettavissa: https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/mpls-overview.html. Luettu: 21.10.2023

Kaspersky. S.a. What is VPN? How It Works, Types of VPN. Luettavissa: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn. Luettu: 16.9.2023

Maniktala, S. 2013. Power Over Ethernet Interoperability Guide. McGraw-Hill. E-kirja. Luettu 12.9.2023

Molenaar R 1. S.a. NetworkLessons. Etherchannel on Cisco IOS Catalyst Switch. Luettavissa: https://networklessons.com/switching/etherchannel-cisco-ios-catalyst-switch. Luettu: 5.9.2023

Molenaar R. 2. S.a. NetworkLessons. VRRP (Virtual Router Redundancy Protocol). Luettavissa: https://networklessons.com/cisco/ccie-routing-switching/vrrp-virtual-router-redundancy-protocol. Luettu: 1.10.2023

Mushroomnetworks. S.a. Technology – MPLS Alternative. Luettavissa: https://www.mushroomnetworks.com/what-is-mpls/. Luettu: 21.10.2023

Palo Alto Networks 1. S.a. What is a VPN? Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn. Luettu: 16.9.2023

Palo Alto Networks 2. S.a. MPLS | What Is Multiprotocol Label Siwtching. Luettavissa: https://www.paloaltonetworks.com/cyberpedia/mpls-what-is-multiprotocol-label-switching. Luettu: 21.10.2023

Planettechusa. S.a. What is a PoE Injector and how can you use it? Luettavissa: https://planetechusa.com/do-you-need-a-poe-injector/ Luettu: 12.9.2023

Raysync. 20.11.2022. What is FTP server and how does it work? Luettavissa: https://www.raysync.io/news/what-is-ftp-server-and-how-does-it-work/. Luettu: 15.10.2023

Smartoptics. S.a. CWDM and DWDM explained. Luettavissa: https://smartoptics.com/knowledge-bank-post/cwdm-dwdm-explained/. Luettu: 4.11.2023

Study-ccnp. S.a. Understanding VRRP: Virtual Router Redundancy Protocol. Luettavissa: https://study-ccnp.com/understanding-vrrp-virtual-router-redundancy-protocol/. Luettu: 1.10.2023

Techtarget 1. 2.2022. Network Time Protocol. Luettavissa: https://www.techtarget.com/searchnetworking/definition/Network-Time-Protocol. Luettu: 23.9.2023

Techtarget 2. S.a. Secure File Transfer Protocol (SSH File Transfer Protocol). Luettavissa: https://www.techtarget.com/searchcontentmanagement/definition/Secure-File-Transfer-Protocol-SSH-File-Transfer-Protocol. Luettu: 15.10.2023

Teja R. ElectronicsHub. 14.4.2021. Multiplexer and Demultiplexer. Luettavissa: https://www.electronicshub.org/multiplexer-and-demultiplexer/. Luettu: 4.11.2023

VTT. S.a. Suomen aika: NTP-palvelu. Luettavissa: https://www.vttresearch.com/fi/palvelut/suomen-aika-ntp-palvelu. Luettu: 23.9.2023

Worldtimesolutions. S.a. What is NTP Server Stratum? Luettavissa: https://www.worldtimesolutions.com/support/ntp/What_is_NTP_server_stratum.html. Luettu: 23.9.2023