SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

TIETOVERKON UUSIMINEN HYDROLINE OY:N VUORELAN TEHTAALLA

UPGRADING NETWORK IN HYDROLINE OY VUORELA FACTORY

TEKIJÄ: Joona Hiltunen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä Joona Hiltunen	
Työn nimi Tietoverkon uusiminen Hydroline Oy:n Vuorelan tehtaalla	
Päiväys 16.4.2017	Sivumäärä/Liitteet 45
Ohjaaja(t) Lehtori Pekka Vedenpää	
Toimeksiantaja/Yhteistyökumppani(t) Hydroline Oy, Tietohallintopäällikkö Matti Tiihonen	

Tiivistelmä

Tämän työn aiheena oli suunnitella ja valmistella uuden tietoverkon toteutus Hydroline Oy:n Vuorelan tehtaalla. Työssä kartoitettiin verkon nykyinen tilanne ja vaatimukset uudelle tietoverkolle. Tämän jälkeen tutkittiin, mitä verkkolaitteita ja tekniikoita työn toteutuksessa tullaan käyttämään. Lisäksi työhön kuului koko yrityksen verkon ylläpitoa helpottavien dokumenttien tekeminen ja pävittäminen.

Työssä tutustuttiin konfigurointeja varten tarvittaviin tekniikoihin ja protokolliin. Työssä tutkittiin HP:n ja Aruban verkkolaitteita, joita tullaan käyttämään toteutuksessa. Lisäksi työssä tutkittiin keinoja verkon monitorointiin, hallintaan ja tietoturvan kohentamiseen laitevalmistajan ohjelmistoilla ja niin sanotulla next generation -palomuurilla. Työn toteuttamista varten laadittiin VLAN ja IP-osoitesuunnitelmat. Lisäksi tutkittiin konfiguroinnit verkkolaitteille eri protokollia varten ja koostetiin esimerkki yhden laitteen koko konfiguroinnista. Verkkolaitteiden lisäksi työssä tutkittiin tarvittavat konfiguroinnit palomuurilla VLANien reititystä varten ja DHCP-palvelimella jokaisen VLAN-alueen IP-osoitteiden jakamiseen.

Työssä ei toteutettu uutta tietoverkkoa, mutta sen toteutus pystytään suorittamaan pohjautuen tähän työhön. Työ on onnistunut ja se vastaa työn tilaajan asettamia tavoitteita. Työn luonteen vuoksi koostetut dokumentit verkosta ja osa konfiguroinneista jätetään salaisiksi.

Avainsanat
Tietoverkko, Aruba, HPe, Verkon monitorointi, Hydroline

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author Joona Hiltunen			
Title of Thesis Upgrading network in Hydroline Oy Vuorela factory			
Date	16.4.2017	Pages/Appendices	45
Supervisor(s) Pekka Vedenpää			
Client Organisation /Partners Hydroline OY, Matti Tiihonen			

Abstract

The aim of this thesis was to plan and prepare the new internal network implementation in Hydroline Oy Vuorela factory. In this thesis, network's current state was described and the need for new network were examined. Next the network devices to be used and needed techiniques for configurations were examined and introduced. This thesis included also making documents for network administrator to ease work.

The theory section also included examining techniques for monitoring and managing network and improving information security with device manufacturer's software and so called "next generation" -firewall. For the new network the implementation plans for vlans and IP-adresses were made as well as configurations in network devices for every protocol to use. Also, an example of one swtich's whole configuration were made. Required settings in firewall and DHCP-server were examined and presented for network implementation.

Because the nature of this thesis parts of the work like network documentation or specific configurations remain secret. The implementation of new network was not made, but this thesis was still successful and the company is able to upgrade network environment based on this thesis.

Keywords
Network, Aruba, HPe, Monitoring network, Hydroline

SISÄLTÖ

1 JOHDANTO

Nykyään jokaisessa yrityksessä tietoverkkojen toiminta on jopa elintärkeää. Työntekijät tarvitsevat työasemia ja lukuisia eri järjestelmiä ja yhteisiä resursseja työn tekemiseen. Tietoa pitää liikutella yrityksen sisällä ja ulkoisten toimijoiden välillä jatkuvasti. Joissain yrityksissä tietoverkon kaatuminen voi pysäyttää työn tekemisen osalta työntekijöistä jopa kokonaan. Tämänkin työn tilaajan kaltaisessa tehdasympäristössä tietoverkon kaatuminen tarkoittaisi sitä, ettei esimerkiksi tuotannonohjausjärjestelmä toimisi, mikä puolestaan tarkoittaisi merkittäviä haittoja tuotantoon ja sitä myötä taloudellisia menetyksiä yritykselle.

Riskien minimoimiseksi tietoverkot tulee suunnitella ja toteuttaa siten, ettei kaikki ole niin sanotusti yhden pisteen varassa. Sisäisessä verkossa linjoja ja jopa verkkolaitteita on hyvä kahdentaa, ettei yhden laitteen hajoaminen ja verkkojohdon katkeaminen pysty kaatamaan koko verkkoa. Verkko on hyvä pitää myös ajantaisaisena, sillä mitä vanhempia laitteita ja kaapelointia verkossa käytetään, sitä epävarmemmaksi se koko ajan tulee. Nykyisin tietoverkkolaitteiden elinkaari on noin viisi vuotta.

Toinen uhka tietoverkoille tai tietojärjestelmille on erilaiset haittaohjelmat tai tietomurrot. Ei riitä, että suojautuu hyvin vain verkon vikaantumista varten, vaan on myös osattava suojautua ulkoisia uhkia kohtaan. Perinteisempien palomuurien ja antivirus-ohjelmistojen lisäksi nykyään on halua päästä seuraamaan verkossa tapahtuvaa liikennettä ja pystyä vastaamaan uhkiin reaaliajassa.

Tämän työn tilaaja on Hydroline Oy. Yrityksen tietoverkko on tulossa elinkaarensa päähän. Tietoverkosta halutaan entistä varmempi ja toimivampi ja lisäksi halutaan kohentaa myös tietoturvaa ja pystyä reagoimaan uhkiin reaaliajassa sekä havaitsemaan verkon ongelmakohtia. Tietoverkosta uudistetaan langattoman ja langallisen verkon verkkolaitteet. Työn tavoitteena on luoda tarvittavat suunnitelmat uuden tietoverkon käyttöönottoa ja asentamista varten. Työssä koostetaan myös dokumentointi verkosta ylläpitoa helpottamaan, mutta työn luonteen vuoksi se jää salaiseksi. Myös osa konfiguroinneista ja tarkoista suunnitelmamista jätetään salaisiksi työn tilaajan pyynnöstä.

2 HYDROLINE OY

Opinnäytetyö tehdään Hydroline Oy:lle Vuorelan päätoimipisteeseen. Yritys haluaa uudistaa tehtaan tietoverkon, koska tietoverkko on tulossa elinkaarensa päähän ja siinä on kohdattu jo ongelmia.

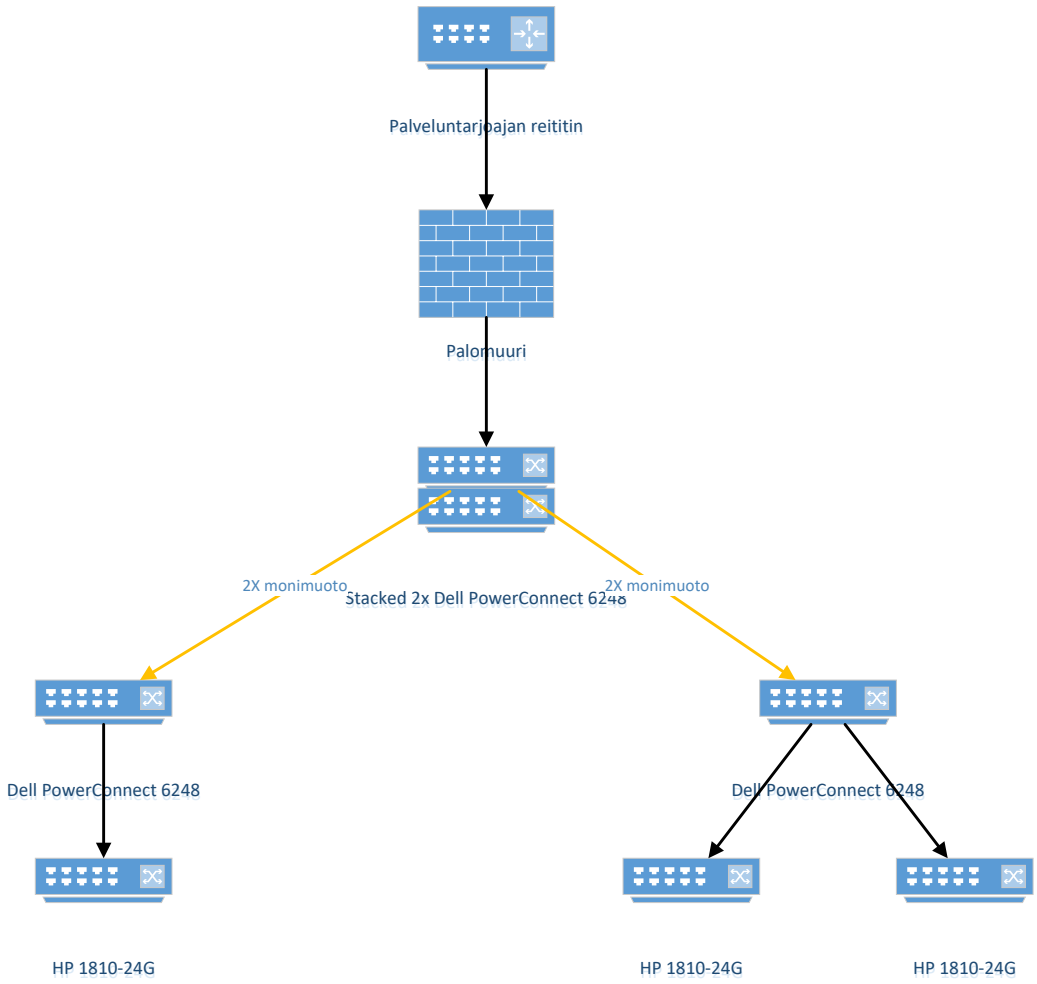
2.1 Yritysesittely

Hydroline Oy on Suomen johtava hydraulisylintereiden valmistaja. Yritys suunnittelee ja valmistaa korkealuokkaisia hydraulisylintereitä vaativaan teollisuuden käyttöön. Sen suurimmat asiakkaat toimivat kaivos- ja metsäteollisuuden aloilla. Yritys työllistää yhteensä noin 220 työntekijää Suomessa ja Puolassa. Sen liikevaihto oli noin 32 miljoonaa euroa vuonna 2015. (Hydroline Oy, ei pvm)

Yrityksen päätoimipiste sijaitsee Siilinjärven Vuorelassa. Siellä on pääasiallinen sylintereiden valmistus sekä toimistotilat. Vuorelassa sijaitsee myös Hydroline Services, jossa huolletaan ja kunnostetaan hydraulisylintereitä. Yrityksellä on lisäksi pienempi tehdas Puolassa Stargardin kaupungissa. (Hydroline Oy, ei pvm)

2.2 Tietoverkon nykytilanne

Tehtaan tietoverkko koostuu palvelinhuoneessa sijaitsevasta pääjakamosta, josta on valokuituyhteydet suunnittelun ja uuden hallin aluejakamoihin. Pääjakamossa on 2 kappaletta Dell PowerConnect 6248 -kytkimiä pinottuna, wlan-controller, palomuurilaite ja palveluntarjoajan reititin. Aluejakamoissa on molemmissa yksi Dell PowerConnect 6248 -kytkin, joihin valokuituyhteys tulee. Porttien lisäämiseksi Dellien perään on lisätty suunnittelussa yksi ja uudessa hallissa kaksi HP 1810-24G -kytkintä. Kuvassa 1 on yksinkertaistettu looginen kuvaus verkon rakenteesta.



KUVA 1. Yksinkertaistettu looginen kuva nykyisestä verkosta

Tehdasta on laajennettu useaan otteeseen vuosikymmenten kuluessa. Runkokaapelointi on tehtaan uusimmissa osissa hyvä lukuun ottamatta muutamia standardin (90 m) ylittäviä vetoja. Tehtaan vanhoissa osissa runkokaapelointikin alkaa olla hieman ikääntynyttä, mutta toimii kuitenkin vielä välttävästi. Runkokaapelointia ei uudisteta tässä työssä kustannuksen ja kaapeloinnin välttävä tilan vuoksi.

Verkkolaitteet lähestyvät viiden vuoden ikää. Laitteiden konfiguroinnissa on myös puutteita ja virheitä, mikä on aiheuttanut ongelmia tietoverkossa. Verkossa käytetään nyt sekaisin sekä Dellin että HP:n kytkimiä. Dellin kytkimet ovat täysin konfiguroitavia tason kolme kytkimiä ja toimivat ikään kuin runkona verkolle, kun taas HP:n kytkimet ovat tason kaksi laitteita, joiden konfiguroitavuus on vajaata. Uudessa toteutuksessa kaikki laitteet aiotaan korvata yhden valmistajan laitteilla. Tällä hetkellä kytkimissä on kokonaisuudessaan n. 250 porttia, jotka ovat lähes kokonaan käytössä. Vanhan hallin ja suunnittelun jakamoissa uusille verkkoon kytkettäville laitteille ei ole enää tilaa.

Tehtaalla on olemassa tällä hetkellä kolme langatonta verkkoa, jotka on toteutettu kahdella erillisellä järjestelmällä. Vanhempi Ciscon järjestelmä hoitaa tuontantolaitteiden tarvitseman wlan-verkon. Ciscon access pointit ovat stand alone -tyyppisiä. Vierailija- ja työntekijöiden wlan-verkko on toteutettu

Ruckuksen ratkaisulla, jossa sen omia access pointeja hallitaan wlan controllerin avulla. Ciscon järjestelmä on jo vanhentunut ja Ruckus lähestyy elinkaarensa loppua.

3 VERKKOLAITTEET

Uuden tietoverkon suunnittelussa otetaan huomioon erityisesti vikasietoisuus, skaalautuvuus, suorituskyky ja tietoturva. Vikasietoisuutta saavutetaan kahdennetuilla linjoilla ja kahdennetuilla core-kytkimillä. Skaalautuvuus toteutuu, kun kytkimien porttien määrä mitoitetaan yli tämän hetken tarpeen. Suorituskyky paranee edelliseen nähden jo uudemmilla laitteilla. Core-kytkimet toimivat verkon ytimenä, ja niihin yhdistetään kaikki muut alemman access-tason kytkimet. Myös core-kytkimiin yhdistetään päätelaitteita. Tietoturvaa parannetaan tekemällä vlan-jakoa verkkoon ja rajaamalla vlanien välistä liikennettä palomuurilla. Vlanien välisen liikenteen reititystä ei tehdä core-kytkimillä hankalasti ylläpidettävien access control listien vuoksi, joilla liikennettä rajattaisiin. Uusi tietoverkko toteutetaan HP- ja Aruban (nyk. HP) -laitteilla.

3.1 LAN-verkon laitevaatimukset

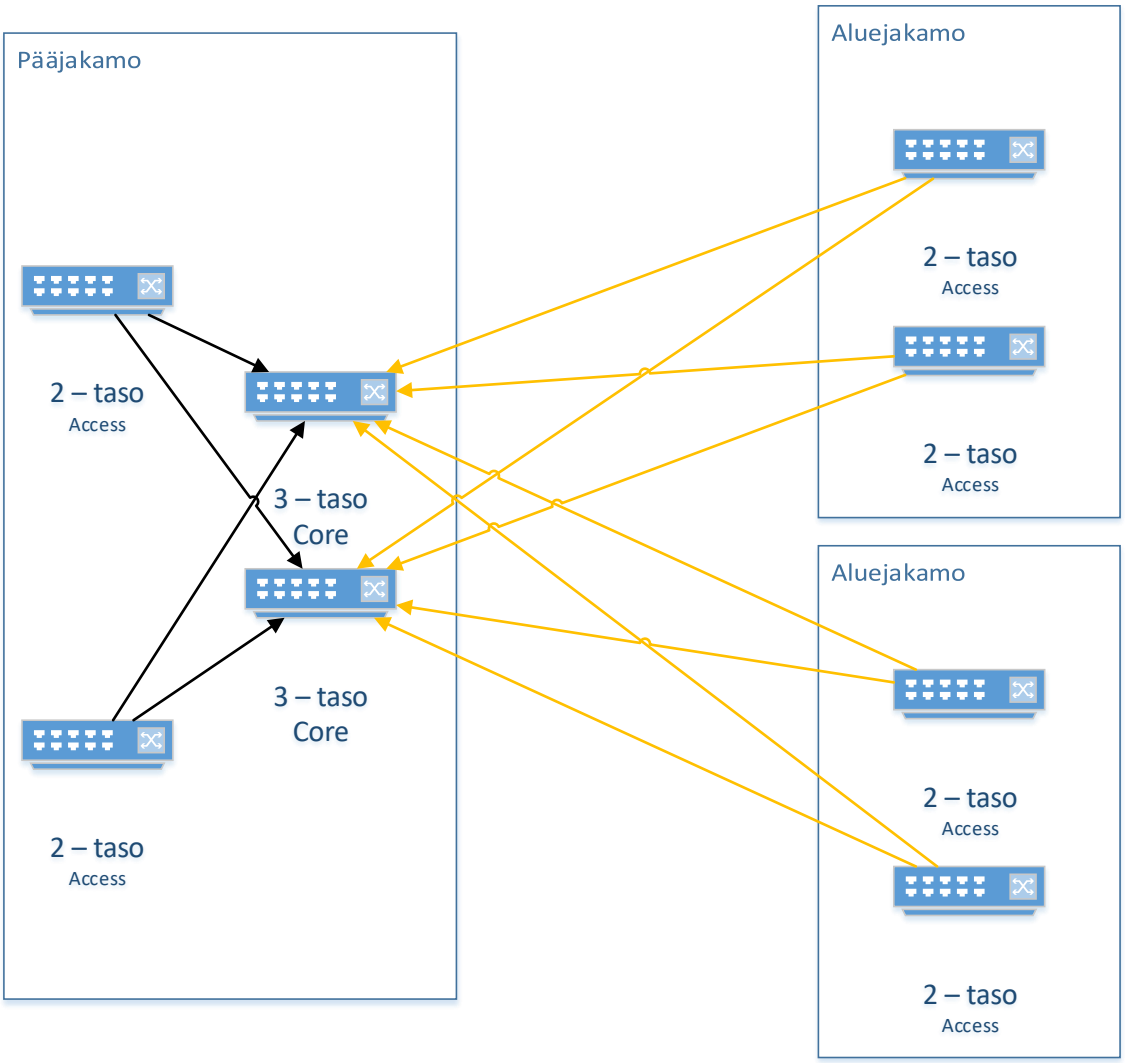
Tällä hetkellä kytkimissä käytettävissä olevia portteja on noin 250. Vuorelan tehtaalla verkkoon kytkettävien laitteiden määrä voi tulevaisuudessa kasvaa hieman, mutta ei merkittävästi, sillä tilat ovat jo tehokkaasti käytössä. Mahdollinen kasvu tulee todennäköisemmin kuormittamaan enemmän wlan- kuin kaapeliverkkoa, joten uusissa kytkimissä ei tarvitse olla merkittävästi enemmän portteja kuin nykyisissä. Sopiva määrä on noin 100 porttia yhtä jakamoa kohden. Pääjakamossa 100 porttia tulevat core-kytkimillä, joiden lisäksi pääjakamoon sijoitetaan kaksi access-kytkintä palvelimia varten. Yhteensä portteja päätelaitteita varten tulee olla n. 300 kappaletta. Verkolta vaaditaan 1 GB nopeutta.

Core-kytkimien on oltava peruskytkimistä hieman suorituskykyisempiä, sillä ne toimivat verkon solmukohtana ja iso osa verkon liikenteestä kulkee niiden kautta. Kytkimet tulevat olemaan käytännössä tason kolme kytkimiä, koska tason kaksi kytkimet eivät yleensä ole niin suorituskykyisiä. Vikasietoisuuden ja suorituskyvyn parantamiseksi core-kytkimiä tulee olla kaksi ja ne on pystyttävä pinoamaan yhdeksi loogiseksi kytkimeksi. Kummastakin kytkimestä tulee yhteys jokaiseen access-tason kytkimeen, joita on aluejakamoissa yhteensä neljä ja pääjakamossa kaksi. Näistä aluejakamoissa olevat yhdistetään valokuidulla, mutta samassa tilassa olevat kaksi Ethernet-kaapelilla core-kytkinten vaatimusten alentamiseksi. Valokuitumoduuleja tulee siis olla kummassakin kytkimessä neljä eli yhteensä kahdeksan. Yhteys core-kytkimistä palomuurille on Ethernet-kaapelilla. Ethernet-porttien tulee olla nopeudeltaan 1 GB. Core-kytkimiin liitetään päätelaitteita ja ne toimivat tavallaan pääjakamossa samalla aikaa myös access-kytkiminä. Kummassakin core-kytkimessä on hyvä olla 48 Ethernet-porttia päätelaitteita varten.

Aluejakamoita kohden tarvittavat sata porttia toteutetaan käytännössä kahdella 48-porttisella kytkimellä, joten tallaisia kytkimiä tarvitaan kokonaisuudessaan neljä. Access-kytkimien tulee olla hallittavia, mutta niiden ei tarvitse olla tason kolme laitteita. Aluejakamoissa olevat access-kytkimet yhdistetään core-kytkimiin jo olemassa olevilla valokuiduilla, joten kytkimissä on oltava kuituliitännät. Jo-

kaisesta kytkimestä tulee yhteys kumpaankin core-kytkimeen vikasietoisuuden parantamiseksi, jolloin access-kytkimiin riittää kaksi FSP-moduulia. Access-kytkimien Ethernet-porttien tulee olla nopeudeltaan yksi GB. Verkossa on muutamia PoE-laitteita, mutta niiden vähäisen määrän ja pitkien kaapelivetojen vuoksi niiden virransyöttö on järkevämpää tehdä PoE-adaptereilla kuin kytkimellä. PoE-ominaisuus nostaisi kytkimen hintaa merkittävästi. Kuvassa kaksi on nähtävissä langallisen verkon kytkennät.

Pääjakamossa otetaan lisäksi käyttöön kaksi 24-porttista access-tason kytkintä, joihin liitetään palvelimet. Kytkimissä ei tarvitse olla valokuitumoduulia, sillä ne sijaitsevat samassa tilassa core-kytkinten kanssa ja ne voidaan yhdistää kuparilla. Palvelinten kytkennät halutaan pitää erillään core-kytkimistä ylläpidon selkeyttämiseksi ja palvelinten toimintavarmuuden parantamiseksi. Kun palvelimilla on omat kytkimet, niin muun verkon kaatumien ei vaikuta palvelinten toimintaan.



KUVA 2. Looginen kuva Lan-verkon laitteista ja kytkennöistä

Nykyiset valokuitukaapelit ovat luokitukseltaan OM1 ja niiden pituus ylittää 33 m, joten niillä ei päästä 10 GB:n nopeuteen eikä näin ollen kytkimien fsp-moduulien tarvitse olla kuin 1 GB:n nopeuksisia (FlexOptix, 2011). 10 GB:n fsp+-moduulit lisäisivät merkittävästi laitteiden hintaa. Alla olevassa luettelossa on yhteenveto kiinteän verkon verkkolaitteiden tarvittavista ominaisuuksista.

Core-kytkin

- 2kpl
- väh. 48 x 10/100/1000 ethernet – porttia
- 4 x fsp moduulia
- 3-taso, hallittava
- Pinottava

Access-kytkin, aluejakamot

- 4 kpl
- 48 x 10/100/1000 ethernet – porttia
- 2 x fsp moduulia
- 2-taso, hallittava

Access-kytkin, palvelimet

- 2 kpl
- 24 x 10/100/1000 Ethernet-porttia
- 2-taso, hallittava

3.2 WLAN-verkon laitevaatimukset

Uuden wlan-järjestelmän on katettava koko tehdas ja nykyiset kaikki kolme wlania pitää pystyä toteuttamaan yhdellä järjestelmällä. Tehdas on suuri ja osittain kahdessa kerroksessa. Tukiasemia rakennukseen tulee sijoittaan ainakin 11, että langaton verkko kattaa koko rakennuksen, eikä signaali katkea liikuttaessa rakennuksen sisällä. Langattomasti yhdistettävien laitteiden määrä on arviolta noin sata. Suurin osa langattomista laitteista on vanhan hallin toimistotilojen ja suunnitteluosaston alueella, missä langattomilta tukiasemilta vaaditaan enemmän suorituskykyä. Tukiasemien tulee tukea sekä 2.4 GHz, että 5 GHz taajuutta. Nykyään suurin osa päätelaitteista on vielä 2.4 GHz toimivia, mutta koko ajan suurempi osa pystyy toimimaan jo nopeammalla 5GHz taajuudella.

Järjestelmästä toivottiin helppoa ylläpidettävää, selkeää ja helposti laajennettavaa. Esille nousi yrityksen kanssa pidetyissä palavereissa HP:n omistaman Aruban wlan-ratkaisu, jossa itsenäiset wlan tukiasemat voidaan yhdistää yhdeksi hallittavaksi järjestelmäksi ilman varsinaista zone controlleria. Yksi tukiasemista toimii masterina ja siihen tehdyt muutokset siirtyvät automaattisesti verkon muihin tukiasemiin. Tukiasemat tukevat useita virtuaalisia AP-profiileja, jolloin järjestelmän kautta saadaan toteutettua kaikki kolme wlania. Järjestelmään voidaan lisätä tai poistaa tukiasemia erittäin joustavasti. Mikäli jokin tukiasema hajoaa, niin se ei vaikuta järjestelmän toimivuuteen. Jopa masterina toimiva tukiasema voi hajota, jolloin vastuu siirtyy seuraavalle tukiasemalle lennosta. Liikkuminen eri tukiasemien kantoalueella on mahdollista ilman yhteyden katkeamista.

3.2.1 Tukiasemien sijainnit

Vanhan hallin toimisto	2 kpl	suurempi suorituskyky
Suunnittelu	1 kpl	
Pakkaamo	1 kpl	
Kokoonpanot	2 kpl	
PV – solut	2 kpl	
Uusi halli	3 kpl	
Laadun tilat	1 kpl	
Ruokala	1 kpl	
Yhteensä	**13 kpl**	

3.3 Laitevalinnat

Verkon toteutuksessa käytetään HP:n laitteita. Verkon asettamien vaatimusten mukaan sopiva access-kytkin on HPE Aruba 2530-48G aluejakamoihin, HPe Aruba 2530-24G pääjakamoon palvelimille ja core-kytkin on HPE 5130 48G-4SFP+ HI. Yrityksellä on jo valmiina yksi HPe Aruba 2530-24G kytkin. (Hewlett Packard enterprise, ei pvm) , (Hewlett & Packard enterprise, ei pvm)

Wlan tukiasemissa sopivat mallit löytyvät Aruban 210- ja 200-sarjoista. Vanhan hallin toimistotiloihin valitaan aruban suorituskykyisemmästä 210--sarjasta malli 215 Instant (Aruba networks, ei pvm). Kaikki muut tukiasemat voivat olla alemman sarjan 205 Instant malleja (Aruba networks, ei pvm). Tukiasemien tulee olla ”Instant”-tyyppisiä, että ne eivät tarvitse zone controlleria toimiakseen. Mallit ovat 802.11ac-protokollaa, tukevat sekä 2.4, että 5 GHz taajuutta. (Aruba networks, ei pvm)

3.3.1 HPE 5130 48G-4SFP+ HI

Hewlett Packard enterprisen 5130 -sarja on eräänlainen kompromissi täydestä tason kolme kytkimestä. Sarjan kytkimet eivät tarjoa kaikkia tason kolme ominaisuuksia, mutta ne ovat silti pienempään verkkoympäristöön täysin riittäviä ja suorituskykyisiä. Karsimalla niin sanotuista turhista ominaisuuksista, laitteen hinta on erittäin edullinen verrattuna täydelliseen tason kolme laitteeseen. Kytkin on täysin hallittava. Hallinta tapahtuu joko html-pohjaisella graafisella käyttöliittymällä tai komentokehotetasolla. Kytkin näkyy kuvassa 3. (Hewlett & Packard enterprise, ei pvm)

KUVA 3. HPe 5130-48G-4SFP+ HI (CDW, ei pvm)

Laitteeseen on mahdollista laittaa kaksi virtalähdettä, mikä parantaa huomattavasti vikasietoisuutta ja ylläpidettävyyttä. Toisen virtalähteen rikkoutuessa toinen pystyy pitämään laitteen vielä käytössä. Mahdollisissa huoltotilanteissa, joissa esimerkiksi virtajohtojen paikkoja joudutaan siirtämään, ei laitetta tarvitsisi sammuttaa välissä. Laitteeseen sopii HP 5500 150WAC Power Supply (JD362B) -virtalähde. (Hewlett & Packard enterprise, ei pvm)

Kytkimessä on 48 x 1GB Ethernet-porttia päätelaitteita varten. Lisäksi kytkimessä on 4 x SFP+ moduulipaikkoja, joihin voidaan asentaa moduulit valokuituyhteyksiä varten. SFP+ moduulipaikka tukee 10 GB nopeutta, mutta verkon valokuituyhteyksille riittää 1 GB nopeus. Kytkimen takana on laajennuspaikka vielä kahdelle SFP+ moduulille. Koska kaikki etupaneelin neljä valokuituporttia menevät yhteyksiin access-kytkimille, käytetään takaosan laajennuspaikkoja kytkinten pinoamiseen. Takapaneelin laajennuspaikkaan sopii HPen 5130/5510 10GBe SFP+ 2-port module (JH157A), joka tarjoaa kaksi SFP+-porttia lisää. Portteihin voidaan asentaa HPen X240 10G SFP+ SFP+ 0.65m valokuitumoduulit, joissa on valmiina 0.65 m pituinen kaapeli moduulien välissä, jolloin ne sopivat pinoamiseen erinomaisesti. Etupaneelin SFP+ -portteihin sopii HPen X130 10G SFP+ valokuitumoduulit. (Hewlett & Packard enterprise, ei pvm)

3.3.2 Aruba 2530-48G ja Aruba 2530-24G

2530 – sarja on täysin hallittava ja täysillä tason kaksi ominaisuuksilla varustettu kytkin. Kytkimet on tarkoitettu access-tasolle tarjoamaan yhteyttä verkkoon eri päätelaitteille. Kytkintä pystytään hallitsemaan joko html-pohjaisella graafisella käyttöliittymällä tai komentokehotetasolla. Kytkin on varustettu 48 x 1GB nopeuksisella RJ-45 ethernet portilla ja 4 x 1GB nopeuksisella SFP-portilla. SFP-port-

tiin sopivat HP:n X121 1GB valokuitumoduulit. Aruba 2530-24G on vastaava laite 2530-48G kytkimen kanssa, mutta siinä on 24 Ethernet-porttia 48:n portin sijaan. Kuvassa 4 on 2530-48G versio. (Hewlett Packard Enterprise, 2016)

KUVA 4. HPe Aruba 2530-48G (Verkkokauppa.com, ei pvm)

3.3.3 Aruba 215 Instant ja 205 Instant

Mallit käyttävät langattoman verkon 802.11ac-protokollaa. Aruba 205 yltää 2.4 GHz:lla jopa 300 MBps ja 5 GHz:lla jopa 867 MBps nopeuksiin, kun taas Aruba 215:lla vastaavat luvut ovat 450 MBps ja 1.3 GBps. 215 mallit ovat varustettu kolmella ja 205 mallit neljällä ympärisäteilevällä antennilla. Mallit ovat tarkoitettuja sisäkäyttöön. Kuvassa 5 on Aruba 2015 Instant malli. (Aruba Networks, ei pvm), (Aruba Networks, ei pvm)

KUVA 5. Aruba 215 Instant (Verkkokauppa.com, ei pvm)

Molemmissa malleissa on Aruban ”wifi client -optimization” -ominaisuus, joka seuraa jatkuvasti siihen yhdistettyjen laitteiden matkaa tukiasemaan. Mikäli client-laite siirtyy kauas tukiasemasta tai yhteydessä on häiriötä, niin järjestelmä etsii automaattisesti paremman tukiaseman. Molemmilla malleilla pystytään tekemään myös hyvinkin yksilöllistä datan priorisointia jopa sovellustasolla. (Aruba Networks, ei pvm), (Aruba Networks, ei pvm)

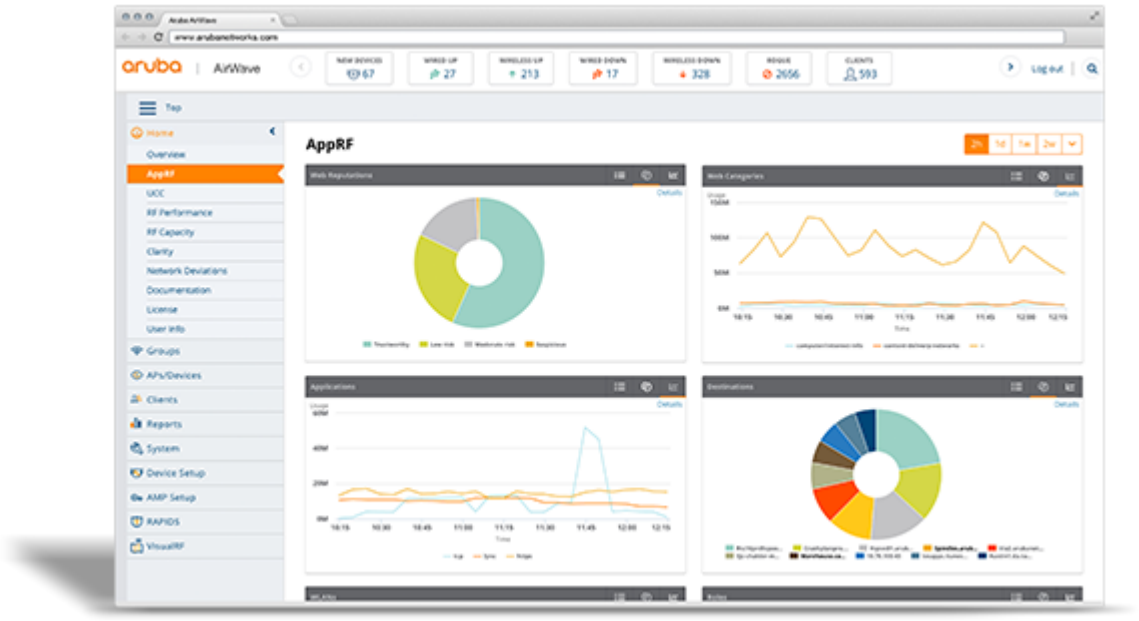
Instant tarkoittaa mallin nimessä sitä, että se ei tarvitse controlleria toimiakseen. Tällöin yksi tukiasemista määritetään master-laitteeksi, joka osaa automaattisesti jakaa tehdyt asetukset verkon kaikkiin yksittäisiin tukiasemiin, jotka lisätään verkkoon. Aruba lupaa prosessin vievän noin viisi minuuttia. (Aruba Networks, ei pvm), (Aruba Networks, ei pvm)

3.4 Verkkolaitteiden keskitetty monitorointi ja hallinta

Tällä hetkellä yrityksen on mahdollista seurata ulospäin menevää liikennettä palomuurilla sovellus- ja käyttäjätasolla. Yrityksellä on kuitenkin kiinnostusta pystyä seuraamaan sisäverkossa tapahtuvaa liikennettä tarkemmin niin langallisessa kuin langattomassa verkossakin. Nykytrendin mukaisesti sisäverkossa tapahtuviin virheisiin, väärinkäytöksiin tai ongelmakohtiin halutaan pystyä puuttumaan mielellään jo ennakkoon tai ainakin tunnistamaan ongelmat tarkasti. Perinteisen IP-osoitteisiin perustuvan liikenteen seuraamisen lisäksi halutaan pystyä tunnistamaan liikennettä sovellustasolla. Monitorointi tulee olla mahdollista sekä langattomassa että langallisessa verkossa. Langattoman verkon monitorointi on vielä tärkeämpää, koska siihen liitetään suurempi määrä erilaisia laitteita kuin langalliseen verkkoon ja nykyisin tietoturvauhkat kohdistuvat enimmäkseen langattomaan verkkoon. Yrityksellä on myös halua seurata, miten langattomat tukiasemat toimivat tehdasympäristössä ja miten laitteet liikkuvat tukiasemien välillä.

Laitevalmistajat ovat vastanneet yritysten kasvavaan kiinnostukseen päästä seuraamaan niiden sisällä tapahtuvaa liikennettä ja siten kohottamaan omaa tietoturvaansa. Koska tässä työssä käytetään Aruban ja sen omistavan HP enterprisen laitteita, keskitytään tässä Aruba Networksin tarjoamaan Aruba AirWave -ratkaisuun. Aruba AirWave on suoraan yhteensopiva Aruban langattomien tukiasemien sekä kytkimien kanssa. Ohjelmisto tukee lisäksi laajaa kirjoa muita laitevalmistajia.

Aruba AirWave on verkon monitorointiin ja laitteiden keskitettyyn hallintaan tarkoitettu reaaliaikainen ohjelmisto, jota toimii web-selaimessa olevan graafisen käyttöliittymän kautta (kuva 6). Palvelu voidaan ottaa pilvestä, mutta Aruba tarjoaa myös paikallisiin palvelimiin pohjautuvaa ratkaisua. Sovellus on suunniteltu nimenomaan mobiililaitteita ja sovellustason seurantaa ajatellen ja on näin ollen juuri sitä, mitä yrityksessä halutaan. Ohjelmistolla pystytään seuraamaan esimerkiksi verkkoon liitettyjä laitteita IP-osoite ja DNS-nimi tasolla, liikenteen määrää sovellustasolla, langattomien tukiasemien signaalien vahvuuksia tai verkkolaitteiden ja päätelaitteiden fyysistä sijaintia ympäristössä. Ohjelmiston kautta voidaan myös hallita ja konfiguroida ainakin Aruban langattomia tukiasemia ja kytkimiä. Sovelluksen kautta nähdään myös koko sisäverkon toiminta ja laitteiden kunto. AirWaven avulla pystytään tunnistamaan myös laajasti langattomaan verkkoon kohdistuvia hyökkäyksiä ja suojatumaan niitä vastaan. Yritys mainostaa ohjelmiston tunnistavan yli 25 erityyppistä langattomaan verkkoon kohdistuvaa uhkaa. (Aruba Networks AirWave, 2017)



KUVA 6. Aruba AirWave selainpohjainen hallintapaneeli (Aruba Network AirWave, 2017)

3.5 Liikenteen seuranta palomuurilla

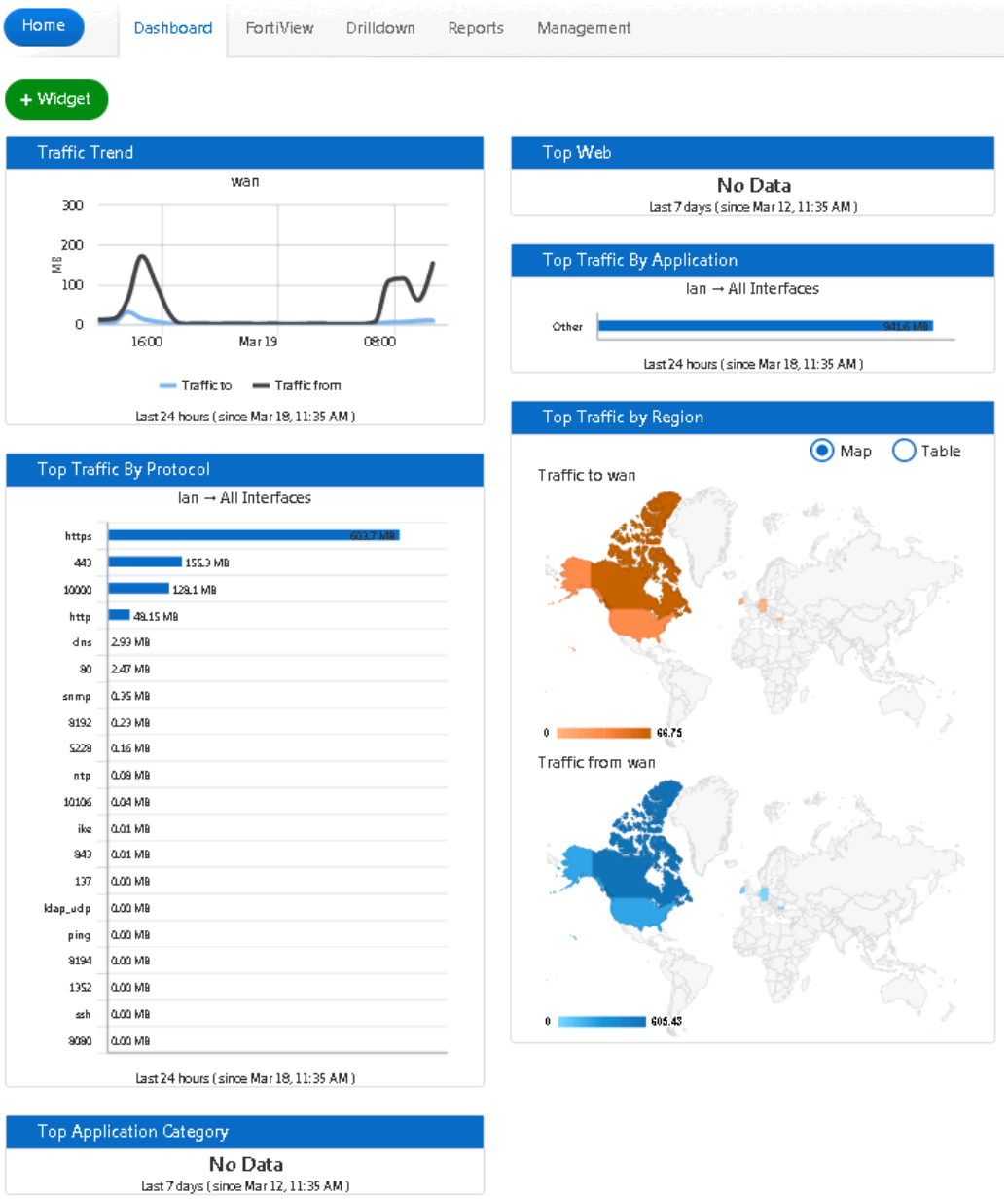
Yrityksellä on käytössään Fortinetin niin sanottu next generation -palomuuri. Next generation -ominaisuuksilla tarkoitetaan palomuurin kykyä tutkia liikennettä sovellustasolla, havaita tunkeilijoita verkosta, tunnistaa verkon käyttäjiä, tutkia salattua ssl-liikennettä ja havaita vielä tuntemattomia uhkia, joihin ei ole olemassa tunnisteita virustietokannoissa. Toiselta nimeltään tällaista laitetta voidaan sanoa UTM-palomuuriksi. UTM-ominaisuudet vaativat paljon tehoa palomuurilaitteelta, koska se joutuu tekemään hyvin syvää analyysiä läpi menevistä paketeista. Fortinet-palomuureilla ominaisuuksia voidaan kytkeä päälle yksitellen ja ne kohdistetaan johonkin palomuurin sääntöön. Esimerkiksi jos halutaan tutkia vain sovellustason ulospäin menevää liikennettä, kytketään kyseinen ominaisuus ja kohdistetaan se sääntöön, missä tulevaksi liikenteeksi (source) on määritetty kaikki yrityksen sisäiset interfacet ja ulospäin meneväksi liikenteeksi (destination) internetiin kytketty interface. Tällä tavalla palomuurin toimintaa ja tehon riittämistä saadaan optimoitua tarvittaviin kohteisiin. (Fortinet, 2017)

3.5.1 Raportointi ja seuranta

Next generation (tai UTM-) -ominaisuuksiin liittyy oleellisesti kattavat raportointijärjestelmät kerätyistä havainnoista ja logeista. Esimerkiksi Fortinetin palomuurit saadaan liitettyä FortiCloud- pilvipalveluun. Palomuurit lähettävät kerätyn datan ja uhkatiedot pilveen, josta tietoja voidaan tutkia mistä päin tahansa tunnistautumisen jälkeen. FortiCloud osaa koostaa datan perusteella valmiita raportteja ottaen huomioon esimerkiksi viimeiset 24 tuntia, mistä verkon ylläpitäjä saa nopean katsauksen verkosta olleista uhista tai käytetystä liikenteestä. Kuvassa 7 näkyy FortiCloudin dashboard -näkymä, josta saa nopean kuvan verkon tapahtumista. (Fortinet, 2017)

FortiCloudissa on myös FortiView-ominaisuus, jolla dataa voidaan tutkia hyvinkin tarkasti. FortiView'llä voidaan tutkia verkkoliikennettä, uhkia tai järjestelmätietoja. Verkkoliikennettä voidaan tut-

kia sovelluksen, lähteen tai kohteen perusteella. Pääkäyttäjä voi havaita esimerkiksi epäilyttävän sovelluksen alaista liikennettä verkosta ja päästä sitä kautta käsiksi tietoihin, mistä IP-osoitteesta data on lähtöisin ja minne se menee. Mikäli käyttäjätunnistus on käytössä ja palomuuri synkronoi käyttäjätietoja esimerkiksi yrityksen active directory -palvelimelta, voidaan nähdä myös suoraan käyttäjänimi sisäisen IP-osoitteen takaa. (Fortinet, 2017)



KUVA 7. FortiCloud Dashbord (Weebly.com, 2015)

3.5.2 Tuntemattomien uhkien havaitseminen

Toinen edistyksellinen UTM-ominaisuus on tuntemattomien uhkien havaitseminen. Palomuuri osaa tutkia erittäin kattavasti kaikkea vähänkin epäilyttävää toimintaa pakettien sisällä. Mikäli palomuuri havaitsee mahdollisen uhkan, jota se ei löydä virustietokannoistaan, lähettää palomuuri epäilyttävän tiedoston FortiNetin Sandbox palveluun. FortiSandboxia voidaan käyttää joko pilvipalveluna tai sitä varten voidaan ostaa oma laite. Oma laite tulee kyseeseen yrityksissä, joissa tietosuojalait estävät tiedon lähettämisen ulos yrityksen verkosta pilvipalveluun. (Fortinet, 2017)

FortiSandbox on käytännössä virtuaalinen ympäristö, joka yrittää aktivoida epäilyttävän tiedoston sisällä mahdollisesti olevan viruksen kokeilemalla lukuisia eri keinoja. Mikäli tiedoston sisällä aktivoituu jokin haittaohjelma, kerää Sandbox tiedot siitä talteen Fortinetin virustietokantoihin, josta ne levittäytyvät kaikille palomuureille seuraavan kerran, kun palomuuri käy päivittämässä virustietonsa. Mikäli tiedoston sisältä ei löydy mitään epäilyttävää, palauttaa Sandbox tiedon palomuurille. Prosessi vie kokonaisuudessaan noin viisi minuuttia. Käytäntö on kuitenkin osoittanut, että varsinkin Suomessa tuntemattomien viruksien kohtaaminen pienissä ja keskisuurissa yrityksissä on kohtuullisen harvinaista. (Fortinet, 2017)

3.5.3 Salatun liikenteen tutkiminen

Nykyiset palomuurit pystyvät purkamaan SSL-salatun liikenteen ja tutkimaan sen sisällön. Nykyään jopa puolet verkkoliikenteestä on salattua, joten sen tutkiminen uhkien varalta on perusteltua. Perinteiset palomuurit eivät pysty havaitsemaan uhkia salatun liikenteen sisältä. Palomuurilla saa käyttöönsä CA sertifikaatin, jonka avulla se pystyy purkamaan tulevan liikenteen. Purkamisen jälkeen palomuuri tutkii sisällön ja sen jälkeen suojaa sen uudelleen ja luo uuden SSL-yhteyden itsensä ja vastaanottajan välille. Voidaan siis sanoa, että palomuuri toimii liikenteen välissä ikään kuin välityspalvelimena. (Martin, 2015)

SSL-liikenteen tutkimien käyttää paljon palomuurilaitteen resursseja, sillä pakettien purkaminen ja uudelleen suojaaminen on suhteellisen raskas toimenpide. Fortinetin laitteilla voidaan tehdä täyttä SSL-liikenteen tutkimista tai vaihtoehtoisesti kevyempää SSL certificate inpectionia. Jälkimmäinen tarkistaa ainoastaan pakettien header-osiot, jolloin prosessiin kuluu huomattavasti vähemmän resursseja. Toisaalta taas uhkat pystytään tunnistamaan paljon luotettavammin Full SSL inspectionilla. (Martin, 2015)

4 TAUSTAA KONFIGUROINNEISTA

Kaikkiin kytkimiin konfiguroidaan seuraavat asetukset:

- VLAN (Virtual Local Area Network)
- STP (Spanning Tree Protocol)
- Hallintaa varten IP – osoite, admin tunnukset, telnet, hostname
- Port Security (mahdollisesti)
- SNTP (Simple Network Time Protocol)
- LACP
- Port Security

Lisäksi tason kolme kytkimissä:

- SVI (Switch Virtual Interface)
- IPv4 routing
- Static route
- IP Helper Address
- IRF stacking

4.1 VLAN

VLAN tulee sanoista Virtual Local Area Network. Vlanin tarkoituksena on jakaa yksi iso paikallinen verkko pienempiin osioihin tietoturvan parantamiseksi, tason kaksi broadcast-alueiden pienentämiseksi ja verkon hallinnan selkeyttämiseksi. Vlan ei ole sidottu fyysisesti mihinkään paikkaan, vaan useisiin verkon kytkimiin voidaan määrittää useita vlaneja porttikohtaisesti. Tämä tarkoittaa sitä, että esimerkiksi samaan vlaniin voi kuulua kaksi laitetta toisesta ja neljä laitetta toisesta päästä tehdasta, vaikka ne ovat useiden verkkolaitteiden päässä toisistaan. Vlan toimii samalla tavalla kuin fyysinenkin Lan-verkko. Niiden välistä liikennettä voidaan reitittää ja rajata ja niihin kuuluvat laitteet ovat aina omalla IP-alueellaan. (Cisco, ei pvm)

Virtuaalisiin lähiverkkoihin jakoa voidaan tehdä esimerkiksi sijainnin, osaston tai toiminnon perusteella. Yksi tavallinen ratkaisu on, että verkkoon luodaan vlanit osastoittain jossa esimerkiksi tuotanto, suunnittelu ja hallinto ovat omissa verkoissaan. Tietoturvan kannalta on hyvä myös tehdä verkon ylläpitämiseksi oma vlan, johon kuuluvat kaikki verkkolaitteet, eikä yhtään päätelaitetta. Tähän verkkoon ei ole pääsyä muilla kuin ylläpitäjillä.

Konfiguroidessa vlaneja sille annetaan numero ja nimi. kytkinten väliset linjat konfiguroidaan trunklinjoiksi, joissa voidaan hyväksyä kaikkien tai vain tiettyjen vlanien liikenne. Portit, joihin kytketään päätelaite, ovat access-portteja. Access-portti kohdistetaan yhteen vlaniin, jonka jälkeen siihen kytketty päätelaite kuuluu nimenomaiseen lähiverkkoon.

4.2 Spanning Tree Protocol

Kahdennetuissa tietoverkoissa verkkoon voi muodostua silmukoita, joissa data jää kulkemaan laitteiden välillä loputtomasti lopulta halvaannuttaen koko verkon toiminnan. Esimerkiksi kun kolme kytkintä liitetään kaikki toisiinsa, muodostuu kolmiosilmukka. Spanning treen tehtävänä on ehkäistä silmukoiden muodostumista sulkemalla osan yhteyksistä laitteiden välillä. Protokolla osaa laskea kaikista edullisimmat ja nopeimmat reitit käytettäviksi yhteyksiksi. Mikäli jokin yhteyksistä katkeaa, protokolla ottaa käyttöön jonkin suljetuista varayhteyksistä. (Äikäs, 2015)

4.3 SVI

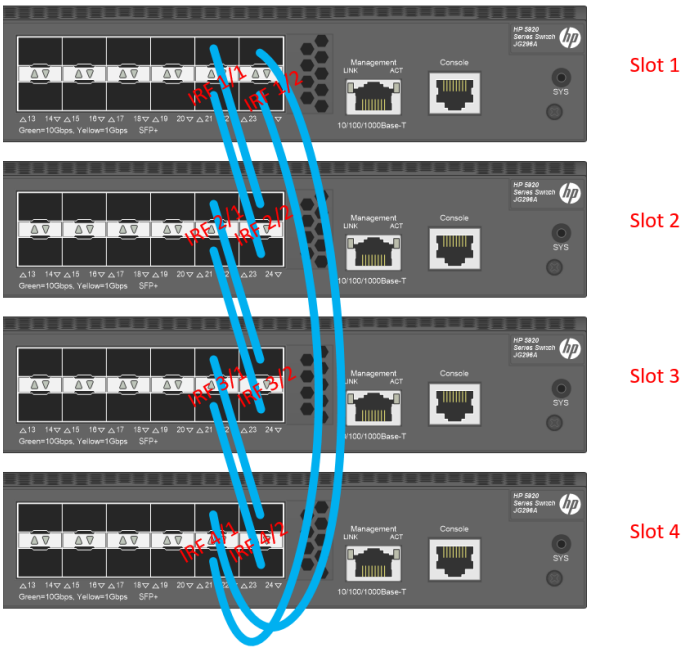
SVI eli Switch Virtual Interface on kytkimeen konfiguroitava vlaniin kuuluva portti. Portti ei ole fyysinen vaan toimii ohjelmallisesti kytkimen sisällä. SVI:lle pystytään antamaan IP-osoite ja se pystyy tekemään tason kolme pakettien prosessointia. Tavallisimmin SVI:tä käytetään konfiguroidessa vlanien default gatewayta ja reititystä vlanien välillä, sekä mahdollistamaan kytkimen tason kolme yhdistettävyyttä ylläpidon kannalta. (Bilgi, 2015)

4.4 IP Helper Address

Tässä työssä IP-osoitteet jaetaan laitteille DHCP-palvelimelta, joka on eri IP-alueella. Tällöin laitteen default gatewaylla (tässä tilanteessa core-kytkimellä) on määritettävä IP helper address, että gateway osaa välittää laitteiden DHCP-kyselyt palvelimelle ja palvelin osaa jakaa IP-osoitteet laitteille. IP helper address on käytännössä DHCP-palvelimen IP-osoite.

4.5 IRF stacking

IRF tulee sanoista Intelligent Resilient Framework. Sillä pystytään yhdistämään useita kytkimiä yhdeksi hallittavaksi laitteeksi. Tällöin puhutaan laitteiden stackauksesta eli pinoamisesta. Yksi laitteista määritetään ryhmän ensisijaiseksi laitteeksi, jonka jälkeen ryhmän muut kytkimet seuraavat ensi sijaista kytkintä. Laitteiden pinoaminen helpottaa niiden ylläpidettävyyttä, parantaa suorituskykyä ja vikasietoisuutta ja yksinkertaistaa verkon rakennetta. Mikäli ensisijainen kytkin hajoaa, vastuu siirtyy automaattisesti ryhmässä seuraavalle. IRF-tekniikka ei käytä kytkimien yhdistämiseen erillisiä stacking-portteja tai kaapeleita vaan yhdistämien tehdään kytkimien 1 tai 10 GB nopeuksisien Ethernet-porttien kautta, kuten kuvassa 8 näkyy. (Hewlett Packard, 2010)



KUVA 8. IRF-pinon kaapelikytkennät (Michel, 2015)

4.6 SNTP

SNTP tulee sanoista Simple Network Time Protocol. Sitä käytetään eri verkkoon liitettyjen laitteiden kellojen synkronointiin, ettei jokaiselle laitteelle tarvitsisi syöttää kellonaikaa manuaalisesti joka kerta kun laite käynnistyy uudestaan. Internetissä on lukuisia NTP – aikapalvelimia, joilta laitteen voi konfiguroida hakemaan aika. Aikapalvelimet käyvät hakemassa ajan itselleen joko toiselta aikapalvelimelta tai suoraan ulkoiselta aikalähteeltä kuten atomikellolta. Aikapalvelimen etäisyyttä aikalähteestä kuvataan stratum – luvulla, jossa numeron 1 aikapalvelin hakee ajan suoraan aikalähteeltä. Luku siis kertoo, kuinka mones laite se on hierarkisesti aikalähteestä. Suurin stratum voi olla 16, mutta tavallisesti aika haetaan stratum 2 aikapalvelimelta. (NTP.org, 2017)

4.7 Port Security

Port Security ominaisuudella tarkoitetaan kytkimen porttien konfiguroimista niin, että ne sallivat vain tiettyjen laitteiden liittämisen porttiin. Portti tunnistaa laitteen MAC-osoitteella, joka on jokaisella laitteella yksilöllinen. Mikäli laitteen MAC-osoite ei ole sallittujen listalla, kytkin sulkee portin, eikä mahdollisesti haitallinen laite pääse verkkoon sisälle. Port Security voidaan konfiguroida joko staattisilla manuaalisesti syötettävillä MAC-osoitteilla tai niin, että kytkimen portti oppii MAC-osoitteen siihen ensimmäiseksi liitetyltä laitteelta, eikä salli sen jälkeen enää uusia laitteita. Mikäli porttiin on kytketty ylimääräinen laite ja kytkin on sulkenut portin, voi sen avata ainoastaan henkilö, jolla on pääse kytkimen hallintaan. (Cisco, 2017)

5 VLAN-SUUNNITELMA

Nykytilanteessa kaikki laitteet ovat samassa lähiverkossa. Vlan-jakoa ei kannata tehdä liian pieniin palasiin ongelmien välttämiseksi, eikä verkosta tulisi liian monimutkainen ylläpitää. Yrityksestä löytyy viisi toisistaan poikkeavaa laiteryhmää, jotka erottamalla saadaan lisättyä tietoturvaa ja jaettua erityyppistä liikennettä omiin alueisiinsa. Nämä ryhmät ovat toimiston käyttämät päätelaitteet, tuotannon käyttämät päätelaitteet, tuotannon työkoneet, palvelimet sekä tulostimet ja vierailijaverkko. Näiden lisäksi itse verkkolaitteet laitetaan omaan lähiverkkoonsa, jonne on pääsy ainoastaan ylläpitäjillä. Verkkolaitteissa oletuksena olevaa default Vlan 1:tä ei sallita kytkinten välisissä linjoissa. Tulevaisuutta ajatellen optiona voidaan pitää myös oman vlanin luomista langattomia mobiililaitteita varten.

5.1 Vlanit

Toimiston käyttämillä päätelaitteilla käytetään yleisesti hyvin laajasti eri palveluita. Näillä laitteilla käsitellään myös luottamuksellista ja salaista tietoa. Laitteilta on tärkeää päästä verkkoon koko ajan ilman katkoksia käyttäjien työn luonteen vuoksi. Tähän ryhmään kuuluu pääasiassa tietokoneita, kännyköitä ja tabletteja.

5.1.1 Konfiguroitavat vlanit

Tuotannon käyttämät päätelaitteet ovat enimmäkseen tietokoneita, joilla käytetään pääasiassa tuotannonohjausjärjestelmää ja sisäistä intra-sivustoa. Tietokoneet ovat yhteiskäytössä eri työntekijöiden kesken. Näihin laitteisiin kohdistuu suurin tietoturvariski, koska periaatteessa kuka tahansa voi päästä käyttämään laitteita ja niiden kautta verkkoon. Lisäksi osalla laitteista on yhteys internetiin ja niihin kytketään omia USB-tikkuja, jotka voivat levittää haittaohjelmia. Niillä tietokoneilla, joilla ei ole pääsyä internetiin, ei ole virustorjuntaohjelmistoa, joten haittaohjelman leviäminen sisäverkossa olisi haitallista.

Tuotannon työkoneet ovat tuotannossa käytettäviä robotteja, sorveja tai työstökeskuksia. Ne on kytketty verkkoon ja ne muodostavat liikenteen kannalta oman ryhmänsä. Osa laitteista on hyvinkin vanhoja. Yrityksessä on huomattu, että osa työkoneista luo verkkoon ajoittain paljonkin liikennettä.

Palvelimet ja tulostimet jaetaan omaan lähiverkkoonsa sen vuoksi, että niiden palveluita tarvitaan muista vlaneista. Palvelimilta ja tulostimilta voidaan sallia eri verkkoihin niiden tarvitsemia palveluita ja estää turha liikenne. Lisäksi kun palvelimet ja tulostimet otetaan omaksi alueekseen eivätkä ne kuulu esimerkiksi toimiston laitteisiin, voidaan estää liikenne kokonaan tuotannon ja toimiston välillä.

Vierailijaverkko on nykyiselläänkin jaettu jo omaan vlaniinsa. Käytännössä vierailijaverkko tarkoittaa julkista wlan-verkkoa, johon vierailijat voivat yhdistää laitteensa. Vierailijaverkosta estetään liikenne kokonaan yrityksen muihin lähiverkkoihin tietoturvan vuoksi. Vaikka vierailija-WLAN suojataankin

salasanalla, on tietoturvan kannalta hyvä ajatella, että kuka tahansa pääsee tähän verkkoon käsiksi. Vierailijaverkon osalta toteutus pidetään samana kuin vanhassakin verkkoratkaisussa, jossa vieras-vlan ei osallistu mitenkään muiden vlanien tavoin reititykseen, vaan sillä on oma kaapeli palomuurille, josta liikenne ohjataan suoraan ulospäin.

Konfiguroitaessa vlania sille annetaan numero ja nimi. Alla olevassa taulukossa on esitettynä yhteenveto VLANeista. Taulukossa mobiililaitteiden vlan on esitetty optiona.

TAULUKKO 1. Yhteenveto VLANeista

VLAN	**Nimi**
xx	Toimisto
xx	Tuotanto
xx	Tyokoneet
xx	Server
xx	Vieras
xx	Hallinta
(xx) Mahd.	(Mobiili)

5.1.2 Mobiililaitteiden vlan

Tietoturvan kannalta langattomia mobiililaitteita varten voisi tehdä oman vlanin. Mobiili-vlan olisi yrityksen työntekijöiden kännyköitä ja tabletteja varten. Mobiililaitteissa on yleisesti huomattavasti heikompi päätelaitesuojaus kuin työasemissa ja tätä kautta ne ovat helpommin haavoittuvia hyökkäyksiä vastaan. Mobiililaitteiden haavoittuvuuksia hyödynnetään yhä kasvavissa määrin. Lisäksi iso osa laitteista voi olla jo tietoturvaominaisuuksiltaan vanhentuneita.

Toinen syy rajoittaa mobiililaitteen omaan vlaniinsa on se, että niillä käytetään yrityksen ympäristössä hyvin rajallista määrää palveluita. Laitteille voisi riittää hyvin pääsy ainoastaan raporttijärjestelmään, sekä yrityksen sisäiseen intraverkkoon. Palomuurilla voidaan monitoroida vlanien liikennettä ulospäin yrityksen verkosta ja tietoturvan kannalta ylläpitäjää kiinnostaa tietää minkä tyyppistä liikennettä mobiililaitteiden kautta kulkee.

5.2 Vlanien välinen liikenne

Vlanien välistä liikennettä reititetään palomuurilla. Tätä tapaa kutsutaan router-on-a-stick -nimellä. Nimi tulee siitä, että reititin tai tässä tapauksessa palomuuri on yhden linjan päässä kytkimistä, eikä jokaisella vlanilla ole omaa kaapelia ja interfacea palomuurilla. Kaapeli konfiguroidaan trunk-linjaksi. Reititys voitaisiin tehdä myös tason kolme core-kytkimillä, mutta niissä liikenteen rajaaminen ja salliminen ACL-listoilla on käytännössä hankalaa. Palomuurilla on huomattavasti helpompi tehdä ja ylläpitää sääntöjä vlanien välistä liikennettä varten. Palomuurilla saadaan tehtyä myös paljon tarkempia

sääntöjä kuin kytkimellä esimerkiksi liikenteen sallimiseksi tai estämiseksi sovellustasolla, ei ainoastaan IP-osoitteiden tai porttien perusteella. Myös raporttien ajaminen palomuurilta tapahtuneesta liikenteestä on huomattavasti helpompaa kuin kytkimellä.

Alussa säännöt tehdään palomuurilla vlan-kohtaisiksi ilman tarkempia rajauksia. Vieras-vlan eristetään kokonaan eli sieltä ei sallita liikennettä mihinkään muuhun vlaniin. Lisäksi Hallinta-vlan eristetään niin, ettei sinne pääse käsiksi mistään muusta vlanista. Server vlanin palveluita tarvitaan Toimisto, Tuotanto ja Tyokoneet -vlanissa eli niiden välinen liikenne sallitaan. Myöhemmin on mahdollista tehdä tarkempia rajauksia laitetasolla liikenteeseen. Toimiston, Tuotannon ja Tyokoneiden välillä ei tarvitse sallia liikennettä. Alla olevassa taulukossa 2 on yhteenveto siitä, mistä vlanista on yhteys mihinkin vlaniin.

TAULUKKO 2. Liikenteen salliminen vlanien välillä

VLAN	**Nimi**	**Sallitut yhteydet**
xx	Toimisto	Server
xx	Tuotanto	Server
xx	Tyokoneet	Server
xx	Server	Toimisto, Tuotanto, Tyokoneet
xx	Vieras	-
xx	Hallinta	-
(xx) Mahd.	(Mobiili)	Sovellustasolla sallittu ainoastaan Intranet

6 IP-OSOITESUUNNITELMA

Vanhan tietoverkon IP-osoitealue otetaan uudessa verkossa käyttöön palvelinten vlanille, jotta vältyttäisiin monilta ongelmilta. Palvelin-vlanin laitteilla on pääasiassa staattisesti määritetty IP-osoite ja niiden vaihtaminen olisi iso työ ja vaatisi erittäin tarkan suunnittelun. Muista laitteista voi olla myös suoria viittauksia IP-osoitteella palvelin-vlanin laitteisiin, joten kun IP-osoitealue pidetään samana, vältytään myös mahdollisilta ongelmilta muiden vlanien laitteissa. IP-osoitteiden yhteenvedossa on suunnitelma myös mahdollista mobiili-vlania varten.

Toinen erikoisuus on vierailijaverkko, joka nykyäänkin on omassa vlanissaan. Vieras-vlan saa IP-osoitteensa FortiNetin palomuurilaitteelta, kun taas muu sisäverkko saa ne Windows-pohjaiselta DHCP-palvelimelta. Palomuurilla on omat porttinsa vierailijaverkolle ja muulle sisäverkolle. Molempiin portteihin tulee omat kaapelit core-kytkimeltä. Tällä ratkaisulla on haettu parempaa tietoturvaa, sillä nyt vierailijaverkolla ole mitään rajapintaa yrityksen sisäverkon kanssa. Vierailijaverkon liikenne ohjataan palomuurilla suoraan ulos internetiin. Uudessa suunnitelmassa pitäydytään vanhassa ratkaisussa ja vieras-vlan saa edelleen IP-osoitteensa palomuurilta.

Toimisto-, tuotanto- ja työkoneet-vlaneilla annetaan IP-osoitteet kullekin omalta verkkomaskin /24 kokoiselta alueelta. Jokaisella vlanilla on käytössään siis 254 IP-osoitetta. Toimisto- ja tuotanto-vlanien laitteet saavat IP-osoitteensa pääasiassa DHCP-palvelimelta. DHCP–palvelimella edellä mainituille vlaneille on annettava isompi alue, mistä IP-osoitteita jaetaan automaattisesti. Toimisto-vlanissa jaettavia osoitteita on 200 kpl, jolloin staattisesti määritettäviä IP-osoitteita varten jää käyttöön osoitteita alueen alku- ja loppupäästä. Tuotanto-vlanissa voi olla suurempi tarve määrittää IP-osoitteita staattisesti. Vlanin laitemäärä on kuitenkin vähäinen ja vlanille riittää hyvin, jos DHCP-palvelimella varataan automaattisesti jaettaville osoitteilla 100 IP-osoitetta ja jätetään välit alkupäästä ja loppupäästä staattisesti määritettäviä IP-osoitteita varten. Työkoneet-vlanissa laitteille määritetään pääasiassa IP-osoite staattisesti. Laitemäärä on kuitenkin vähäinen verrattuna saatavilla olevien IP-osoitteiden määrään, joten vlanille voidaan tehdä samanlainen jako DHCP-osoitteiden ja staattisesti määritettävien osoitteiden välillä kuten tuotanto-vlanissakin.

Hallinta-vlan on varattu vain verkkolaitteiden tai niihin rinnastettavien ainoastaan ylläpidolle kuuluvien laitteiden IP-osoitteita varten. Tähän vlaniin ei jaeta IP-osoitteita DHCP-palvelimelta, vaan osoitteet määritetään aina staattisesti. Tietoturva paranee hieman, kun esimerkiksi vlaniin vahingossa kytketty laite ei saa automaattisesti IP-osoitetta eikä näin ollen voi keskustella vlanissa olevien laitteiden kanssa. Oletuksena tietysti hallinta-vlaniin ei pitäisi pystyä kytkemään yhtään ylimääräistä laitetta.

Jokaisessa vlanissa verkon ensimmäinen IP-osoite xxx.xxx.xxx.1 on varattu default gatewaylle ja viimeinen xxx.xxx.xxx.255 on yleislähetysosoite (Broadcast). Yleislähetysosoitetta ei voida antaa millekään laitteelle. Alla olevassa taulukossa kolme on vielä yhteenveto vlanien IP-osoitteista.

TAULUKKO 3. Yhteenveto vlanien IP-osoitteita

VLAN	**Nimi**	**IP-osoitealue**	**DHCP**	**Staattinen**
xx	Toimisto	/24	200	54
xx	Tuotanto	/24	100	154
xx	Tyokoneet	/24	100	154
xx	Server	/23	Vanhan ratkaisun mukaisesti	Vanhan ratkaisun mukaisesti
xx	Vieras	/24	vanhan ratkaisun mukaisesti	vanhan ratkaisun mukaisesti
xx	Hallinta	/24	-	kaikki
(xx) Mahd.	(Mobiili)	/24	200	54

7 KONFIGUROINNIT

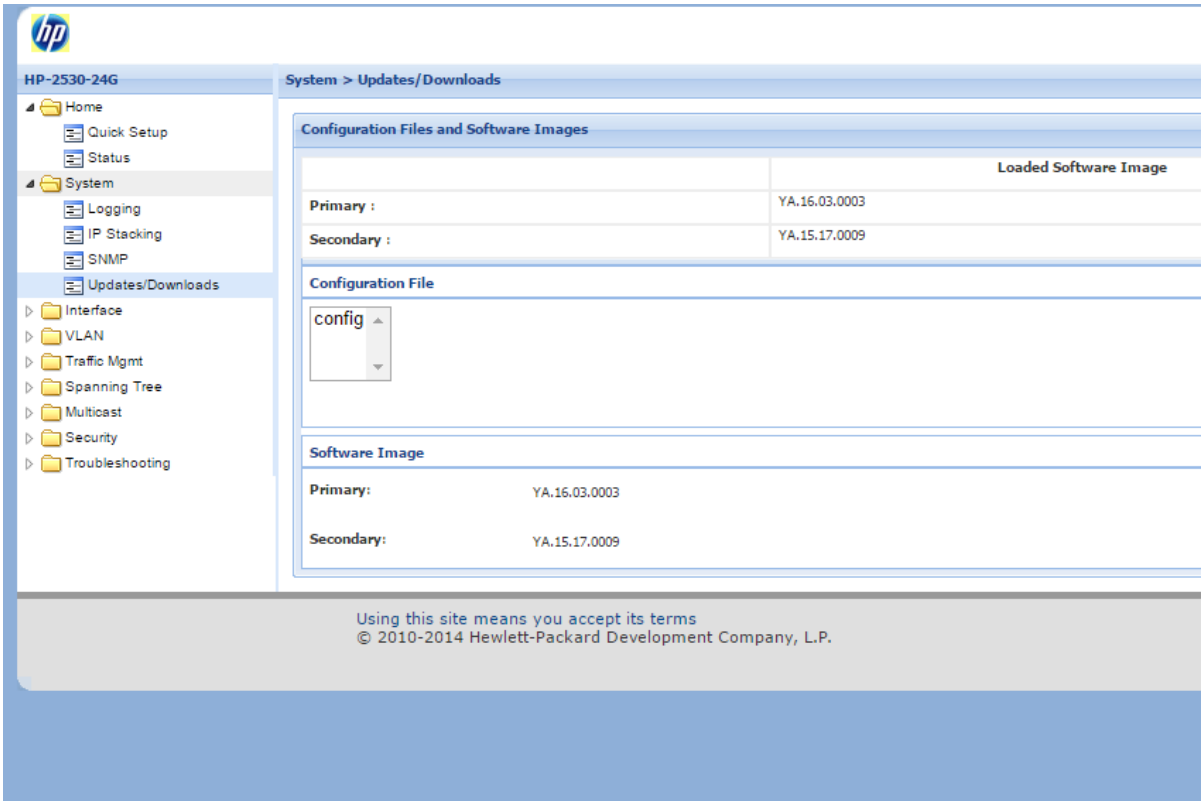
Kytkimiin konfiguroidaan alustavasti niiden perusasetukset, vlanit, kytkinten väliset LACP-linjat ja spanning tree. Myöhemmin voidaan konfiguroida myös Port Security-ominaisuus, mikäli tietoturvaa halutaan parantaa. Kytkinten konfiguroinnin lisäksi konfiguroidaan wlan-tukiasemat, palomuurille interfacet vlaneja varten ja säännöt vlanien väliseen reititykseen, sekä DHCP-palvelimelle alueet, joilta vlanit saavat IP-osoitteita.

7.1 Kytkimien konfiguroinnit

Ennen varsinaista konfigurointia kytkimet päivitetään uusimpaan saatavilla olevaan ohjelmistoversioon. Uusimmat ohjelmistopäivitykset löytyvät HPe:n support sivulta. Tällä hetkellä uusin ohjelmistoversio Aruba 2530-kytkimille on 16.03.0003 ja 5130-kytkimille CMW710-R1121P03-US. Ohjelmistoversioiden image tiedostot ladataan sivustolta, jonka jälkeen ne voidaan päivittää kytkimiin helpoiten graafisen käyttöliittymän kautta. Tätä varten kytkimiin on konfiguroitava IP-osoite komennoilla

- configure
- vlan xx
- name Hallinta
- ip address xxx.xxx.xxx.xxx 255.255.255.0

Kun IP-osoite on konfiguroitu, päästään web-selaimella kytkimen graafiseen käyttöpaneeliin. Valikossa Systemin alla on Updates/Downloads sivu, mistä löytyy kohta software images. Valitaan primary software imageen oikea tiedosto ja ladataan se kytkimelle. Lataamisen jälkeen kytkin käynnistetään uudelleen, jolloin se käynnistyy uuteen ohjelmistoonsa. Kuvassa 9 on Aruba 2530-kytkimeen päivitetty uusin ohjelmisto. Uudelleen käynnistyksen jälkeen kytkimen ohjelmistoversio voidaan todentaa käskyllä ”show version”. (HPe Support, 2017), (HPe Support, 2017)



KUVA 9. Aruba 2530-kytkimen ohjelmistoversio vanhassa hallintapaneelissa

Uusi ohjelmistoversio tuo täysin uudistetun graafisen hallintapaneelin Aruban 2530-kytkimille. Ohjelmistoversion myötä tulee myös uusia ominaisuuksia, kuten esimerkiksi tuki Aruba AirWave järjestelmää varten, jolla kytkimiä ja wlan-tukiasemia voidaan seurata ja hallita keskitetysti. Uudessa ohjelmistoversiossa voidaan myös olettaa olevan tuki pidemmäksi aikaa ja siinä on todennäköisesti korjattu mahdollisia haavoittuvuuksia tai virheitä.

7.1.1 Perusasetukset

Perusasetuksissa kytkimille määritetään hostname, aika ja päivämäärä, määritetään manager ja operator salasanat, määritetään laitteen IP-osoite ja sallitaan SSH – yhteys konfigurointeja varten. Hostnamet ja IP-osoitteet käyvät ilmi taulukosta 4. Aika laitteelle haetaan palomuurilta, joka toimii NTP – palvelimena sisäverkkoon päin. WLAN-tukiasemille määritetään ainoastaan staattiset IP-osoitteet. Ne saavat automaattisesti Hostnamen ja asetuksena Master tukiasemalta.

TAULUKKO 4. Kytkimien ja tukiasemien sijainnit, hostname ja IP – osoitteet

Tyyppi	**Laite**	**Sijainti**	**Hostname**	**IP-osoite**
Kytkin	HPe 5130 48G-4SFP+ HI stacked 2x	Palvelinhuone	xx	xx
Kytkin	HP 2530-24G	Palvelinhuone	xx	xx
Kytkin	Aruba 2530-24G	Palvelinhuone	xx	xx
Kytkin	Aruba 2530-48G	Suunnittelu jakamo	xx	xx
Kytkin	Aruba 2530-48G	Suunnittelu jakamo	xx	xx

Kytkin	Aruba 2530-48G	Uusi halli jakamo	xx	xx
Kytkin	Aruba 2530-48G	Uusi halli jakamo	xx	xx
Tukiasema (Master)	Aruba 215	Vanha halli toimisto	auto	xx
Tukiasema	Aruba 215	Vanha halli toimisto	auto	xx
Tukiasema	Aruba 205	Suunnittelu	auto	xx
Tukiasema	Aruba 205	Pakkaamo	auto	xx
Tukiasema	Aruba 205	Kokoonpano	auto	xx
Tukiasema	Aruba 205	Kokoonpano	auto	xx
Tukiasema	Aruba 205	PV-solut	auto	xx
Tukiasema	Aruba 205	PV-solut	auto	xx
Tukiasema	Aruba 205	Uusi halli	auto	xx
Tukiasema	Aruba 205	Uusi halli	auto	xx
Tukiasema	Aruba 205	Uusi halli	auto	xx
Tukiasema	Aruba 205	Laatu	auto	xx
Tukiasema	Aruba 205	Ruokala	auto	xx

7.1.2 IRF-stacking core-kytkimiin

Core-kytkimet pinotaan yhdeksi loogiseksi kytkimeksi IRF-tekniikalla. IRF-konfigurointi tehdään ensimmäiseksi ennen kaikkia muita konfigurointeja. Kytkimet yhdistetään toisiinsa SFP+ porttien kautta kahdella 10GB valokuituliitännällä. Konfiguroinnissa annetaan ”ylemmälle” kytkimelle member numerot, jotka määräävät kumpi kytkimistä toimii masterina. Member numeron konfiguroinnin jälkeen kytkin käynnistetään uudelleen. Tämän jälkeen annetaan IRF-pinon jäsenille vielä prioriteetit, joilla varmistetaan pinon toimiminen. Korkein prioriteetti on 32, joka annetaan master-kytkimelle. Ennen porttien kohdistamista IRF-porteiksi täytyy fyysiset portit sulkea. Sulkemisen jälkeen kohdistetaan fyysiset portit IRF-portteihin ja otetaan IRF-konfiguroinnit aktiiviseksi. Viimeiseksi laitteet käynnistetään uudelleen, jonka jälkeen pinon toiminta voidaan todentaa show komennolla. Konfigurointi tapahtuu käskyillä:

- *irf member 1 priority 32*
- *save*
- *reboot*
- *interface range [Portit]*
- *shutdown*
- *irf-port 1/1*
- *port group interface [Portti1]*
- *port group interface [Portti2]*
- *interface range [portit] undo shutdown*
- *irf-port-configuration active*
- *save*

- *reboot*

Vastaavat konfiguroinnit tehdään toiselle kytkimelle, missä member on 2, priority 31 ja irf-port 1/2. (Michel N. , 2015)

7.1.3 SNTP

Kytkimiin konfiguroidaan SNTP-protokolla, jolloin ne saavat ajan automaattisesti ja ovat kaikki varmasti samassa ajassa. Verkon NTP-palvelimeksi on valmisteltu palomuuri. SNTP-konfiguroinnissa kytkimelle määrätään sijainti, aikavyöhyke, ajan synkronointitapa ja NTP-palvelimen IP-osoite. Konfigurointi tapahtuu käskyillä

- *time daylight-time-rule western-europe*
- *time timezone 120*
- *timesync sntp*
- *sntp unicast*
- *sntp server priority 1 [IP-osoite] 4*

7.1.4 Vlan

Jokaiseen kytkimeen konfiguroidaan vlan-suunnitelman mukaiset vlanit ja nimetään ne. Alustavasti kaikki päätelaitteille menevät portit kohdistetaan vlaniin 40, jonka IP-osoitealue on sama kuin vanhassa verkossa. Kytkinten väliset linjat konfiguroidaan trunk linjoiksi, ja niissä hyväksytään kaikki vlanit. Kytkinten väliset trunk-linjat käyttävät lacp-protokollaa, joka yhdistää kaksi erillistä linjaa yhdeksi fyysiseksi linjaksi. Vlanien reititystä varten palomuurille konfiguroidaan yksi trunk-linja muille kuin vieras-vlanille. Vieras-vlania varten konfiguroidaan yksi access-linja palomuurille, kuten vanhassakin verkkoratkaisussa. Vlan konfiguroidaan kytkimiin käskyillä

- *vlan [ID]*
- *name [NIMI]*
- *tagged [Trunk-portit]*
- *untagged [Access-portit]*
- *(ip address x.x.x.x y.y.y.y)*

IP-osoite annetaan hallinta-vlanille.

7.1.5 Spanning tree

Jokaiseen kytkimeen konfiguroidaan spanning tree protocol toimimaan jokaisessa vlanissa. Jokaisen vlanin root bridgeksi määritetään core-kytkin. Porttien ja kytkimien prioriteetteja ei konfiguroida tarkemmin. Spanning tree saadaan käyttöön yksinkertaisesti antamalla käsky :

- *spanning-tree*

config-komentotasolla. Core-kytkimellä annetaan lisäksi käsky

- *spanning-tree priority 0*

, joka tekee kytkimestä root bridgen.

7.1.6 Port Security

HP:n ja Aruba kytkimissä port securitya ei konfiguroida porttitasolla. Konfigurointi tapahtuu yleisellä config-tasolla heti configure käskyn syöttämisen jälkeen. Käskyssä määritetään portit joihin käsky vaikuttaa, tyyppi sekä sallittujen MAC-osoitteiden määrä ja toiminto, jos porttiin kytketään kielletty laite. Tyypitkin valitaan ”learn-mode static”, jolloin portti oppii siihen kytketyn laitteen MAC-osoitteen ja tallentaa sen muistiin. Osoitteiden enimmäismääräksi laitetaan 1, jolloin ainoastaan ensimmäisenä porttiin kytketty laite on sallittu. Toiminnoksi väärän laitteen kytkennän jälkeen valitaan ”send-disable”, jolloin kytkin tallentaa tapahtuman logiinsa ja sulkee portin. Esimerkki käskystä:

- *port-security ethernet 1-10 learn-mode static address-limit 1 action send-disable*

Alustavasti port-security-ominaisuutta ei konfiguroida kytkimiin. (Aruba Networks, 2017)

7.1.7 Esimerkki Aruba 2530-24G konfiguroinneista

- hostname SW-2L-A2
- no tftp server
- password manager user-name [tunnus]
- [salasana]
- password operator
- [salasana]
- crypto key generate ssh
- ip ssh

- time daylight-time-rule western-europe
- time timezone 120
- timesync sntp
- sntp unicast
- sntp server priority 1 [IP-osoite] 4

- spanning-tree
- (Core – kytkimellä lisäksi spanning-tree priority 0)

- trunk ethernet 1-2 trk1 lacp

- vlan xx
- name Toimisto
- tagged trk1
- untagged eth [portit]
- no ip address

- vlan xx
- name Tuotanto
- tagged trk1
- untagged eth [portit]
- no ip address

- vlan xx
- name Tyokoneet
- tagged trk1
- untagged eth [portit]
- no ip address

- vlan xx
- name Server
- tagged trk1
- untagged eth [portit]
- no ip address

- vlan xx
- name Vieras
- tagged trk1
- untagged eth [portit]
- no ip address

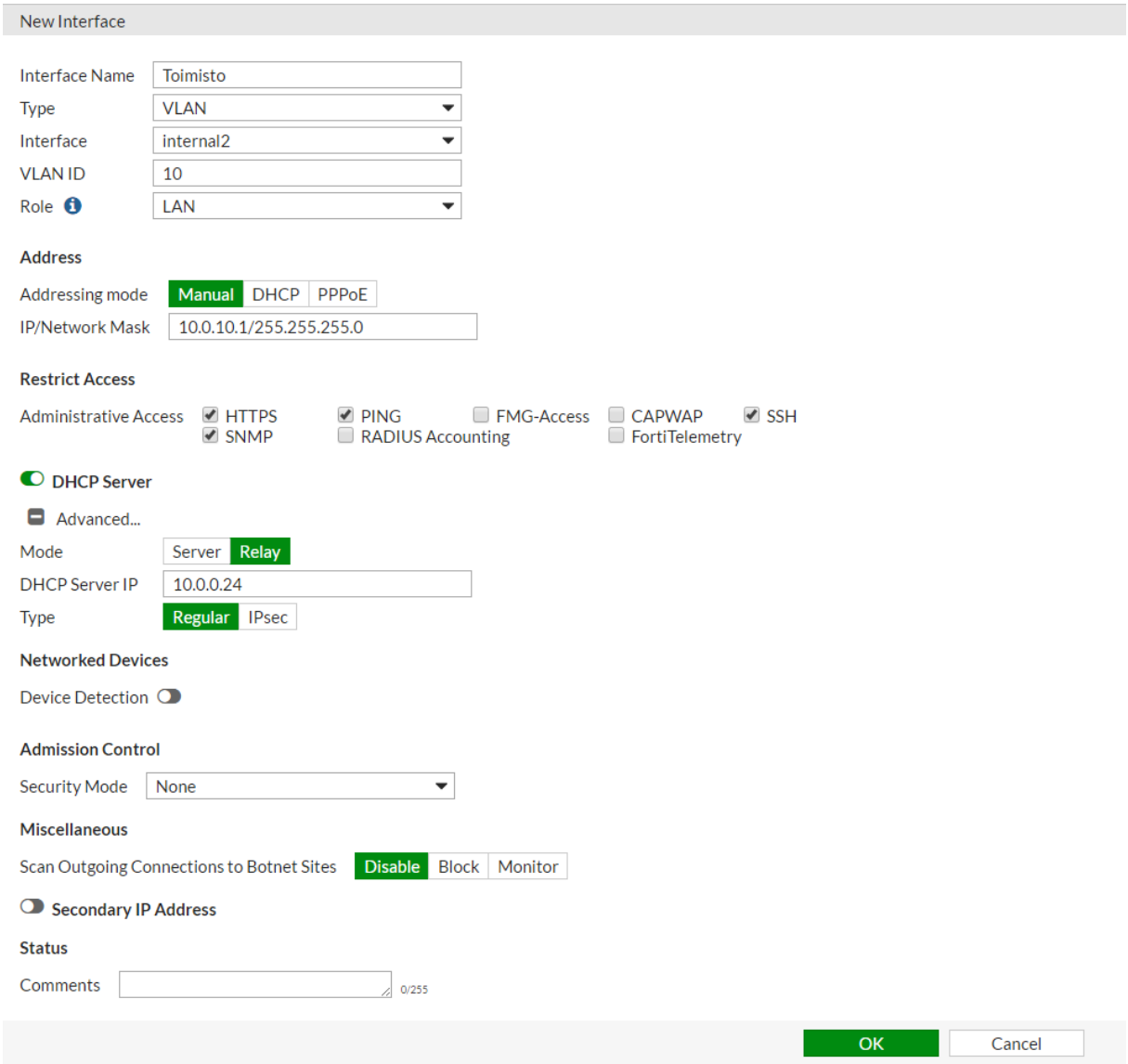
- vlan xx
- name Hallinta
- tagged trk1
- ip address x.x.x.x 255.255.255.0

- write memory

7.2 Konfiguroinnit palomuurilla

Palomuurille luodaan subinterfacet vlaneja varten esimerkiksi internal2 portin alle. Palomuurin konfiguroinnissa käytetään sen graafista web-käyttöliittymää. Subinterface tehdään menemällä Networks

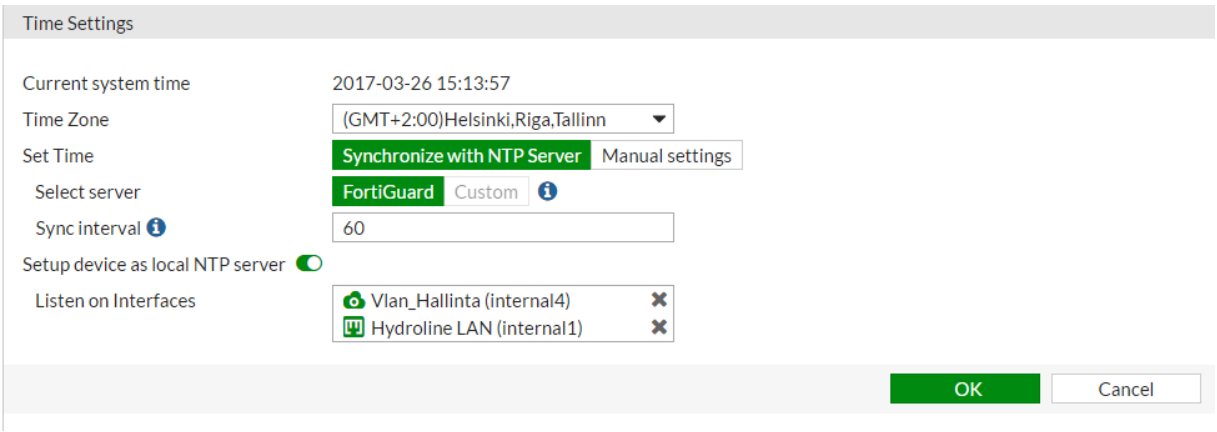
→ Interfaces valikkoon. Täältä valitaan Create New →Interfaces, minkä jälkeen avautuu uusi ikkuna. Näkymässä interfacelle syötetään nimi (esimerkiksi vlanin nimi), valitaan tyypiksi VLAN, kohdistetaan se oikean fyysisen interfacen alle (Internal2), syötetään oikea vlan ID (esimerkiksi toimisto-vlanissa 10) ja valitaan rooliksi LAN. Subinterfacelle annetaan IP-osoite, sillä se toimii vlanin default gatewayna. IP-osoitteen tyypiksi valitaan manual ja sen jälkeen syötetään kenttään osoite muodossa [IP-osoite/maski]. Jotta vlaniin kytkeytyvät päätelaitteet saisivat IP-osoitteensa DHCP-palvelimelta, joka tässä tilanteessa sijaitsee eri vlanissa, pitää subinterfacella laittaa päälle valinta DHCP Server. Avautuvien valintojen alla on kohta Advanced, jonka alta voidaan valita Relay. Tämän jälkeen syötetään kenttään DHCP-palvelimen IP-osoite, niin palomuuri osaa välittää vlaneista tulevat DHCP-kyselyt oikealle palvelimelle. Subinterfacen konfiguroinnit näkyvät kuvassa 10.



KUVA 10. Subinterfacen luonti

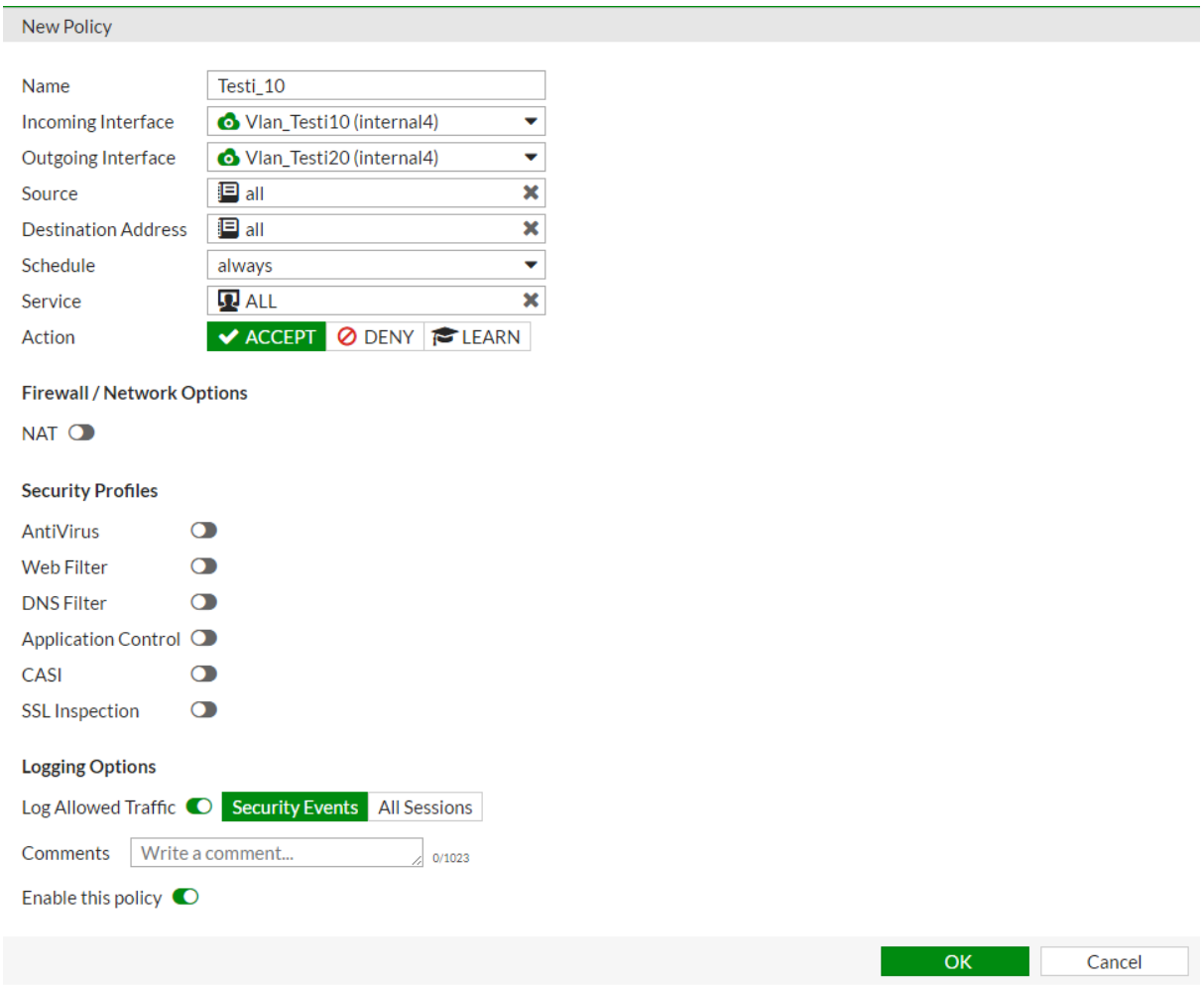
Palomuuri konfiguroidaan lisäksi toimimaan NTP-palvelimena verkon laitteille. Palomuuri käy itselleen ajan ulkoiselta NTP-palvelimelta. Konfigurointi tehdään menemällä valikossa Dashboard-etusivulle ja etsimällä sieltä kohta System Information. System Informationin alla on kohta System Time, jonka perässä linkki ”Change”. Klikataan Change, minkä jälkeen avautuvassa ikkunassa valitaan

kohta ”Setup device as local NTP server” ja tämän jälkeen määritetään Interfacet, joita palomuuri kuuntelee aikapyynnöissä. NTP-asetukset näkyvät kuvassa 11.



KUVA 11. Fortigate-palomuurin NTP-asetukset

Kun palomuurille on luotu tarvittavat subinterfacet, luodaan palomuuriin säännöt, joiden perusteella liikennettä sallitaan vlanien välillä. Oletuksena kaikki liikenne on estetty. Palomuurisääntöjä pystytään luomaan menemällä valikossa Policy & Object → IPv4 Policy ja valitsemalla Create New. Sääntöön määritetään From- ja To-portit, Source ja Destination IP-osoitteet sekä palvelut. Tämän jälkeen säännöstä tehdään joko Accept tai Deny, eli salliiko vai estetäänkö se liikenteen tehtyjen asetusten perusteella. Vlanien välisissä säännöissä ei käytetä NAT-protokollaa. Kuvassa 12 näkyy säännön luonti kahden testi-vlanin välillä, jossa sallitaan kaikki liikenne. NAT otetaan käyttöön, kun tehdään sääntö vlanista ulkoverkkoon, että sisäinen IP-osoite kääntyy julkiseksi palomuurilla.



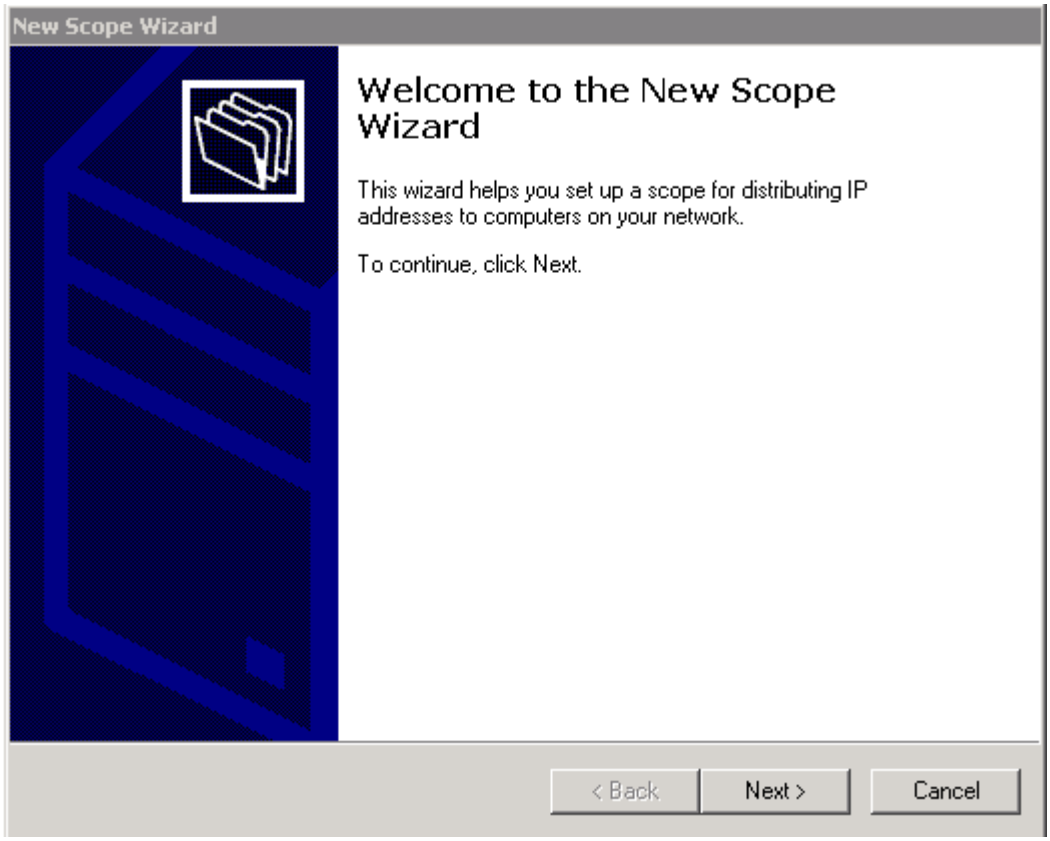
KUVA 12. Palomuurisäännön luonti

7.3 DHCP scopen luonti palvelimella

DHCP-palvelin on yrityksen Windows 2008R2 active directory -palvelin. Palvelimella luodaan DHCP scope kaikkia muita, paitsi Hallinta-vlania kohden. Scopen luonti tehdään menemällä Server Manageriin ja avaamalla vasemmalla olevasta puurakenteesta Roles → DHCP Server → [palvelimen nimi] → IPv4. Klikataan hiiren oikealla IPv4 ja valitaan New scope. Tämän jälkeen avautuu New Scope Wizard (kuvassa 13), joka ohjaa scopen luomisen läpi. Wiazrdin vaiheet on esitetty alla olevalla luettelossa.

- Scope Name kohdassa annetaan scopella nimi, joka on hyvä olla vlanin nimi. → Next
- Seuraavalla sivulla määritetään mistä IP-osoitteesta mihin DHCP-palvelin jakaa osoitteita. Lisäksi määritetään IP-osoitteen maskin pituus ja subnet mask. → Next
- Seuraavalla välilehdelle voidaan tehdä poikkeuksia määritettyyn IP-osoitealueeseen, mitä palvelin ei saa jakaa päätelaitteille. → Next
- Seuraavaksi määritetään lease time eli se, miten pitkään menee, ennen kuin palvelin vapauttaa jonkin päätelaitteen IP-osoitteen seuraavalle, jos päätelaitteeseen ei saada yhteyttä. → Next
- Seuraavalla välilehdelle valitaan, että halutaan määrittää DHCP-valinnat nyt → Next
- Syötetään kenttään vlanin default gatewayn IP-osoite ja klikataan Add → Next

- DNS-palvelimet pitäisi tulla kenttään automaattisesti. Jos ne eivät tule, syötetään kenttään DNS-palvelimen IP-osoite ja klikkaa Add. → Next
- → Next
- Valitaan, että scope aktivoidaan saman tien. → Next
- Finish



KUVA 13. New Scope Wizard DHCP-palvelimella

7.4 Aruba 215- ja 205- Access Point -konfiguroinnit

Aruba 2015- ja 205- access pointeihin konfiguroidaan pääkäyttäjän tunnukset, ip-osoitteet laitekohtaisesti taulukon 4 mukaisesti, ip-osoite virtuaaliselle kontrollerille ja access point -profiilit kaikille tarvittaville wlaneille. Alustavasti käyttöönotettavat wlanit ovat HydrolineWlan, TuotantoWlan ja VierailijaWlan.

7.4.1 Perusasetukset IP-osoite, hallintatunnus, NTP

Access pointeille konfiguroidaan staattiset IP-osoitteet. Konfigurointi tapahtuu laitteiden console-portin kautta komentokehoterivillä. Staattinen IP-osoite annetaan ja tarkistetaan käskyillä

- *setenv ipaddr x.x.x.x*
- *setenv netmask y.y.y.y*
- *setenv gatewayip x.x.x.x*
- *save*
- *printenv*

Käyttäjätunnus ja salasana hallintakäyttäjälle luodaan komennoilla

- *mgmt-user [User] [password]*
- *end*
- *commit apply*

Perusasetuksissa konfiguroidaan laitteelle vielä NTP-palvelin, mistä kaikki laitteet saavat päivitettyä aikatietonsa. Konfigurointi tapahtuu komennoilla

- *ntp-server [ip-osoite]*
- *end*
- *commit apply*

Muutoksien jälkeen laite käynnistetään uudelleen. (Aruba Networks Community, 2017)

7.4.2 Virtual Controller

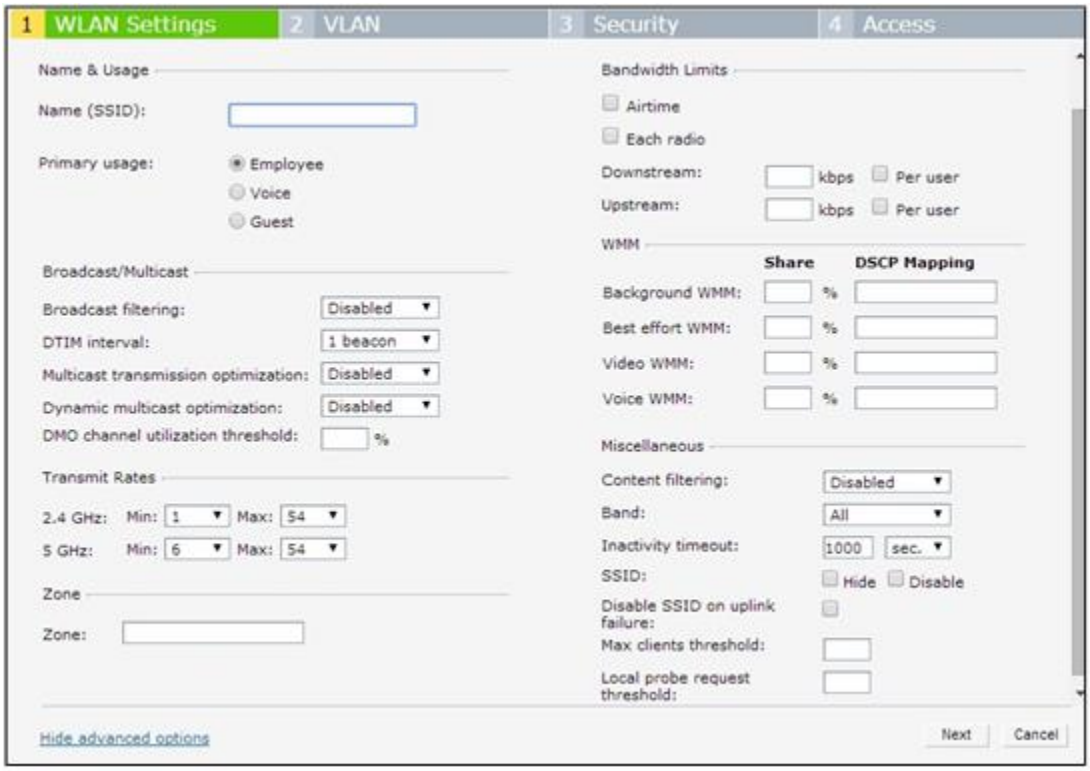
Verkkoon lisättävät instant access pointit löytävät toisensa automaattisesti, jos ne ovat samassa vlanissa. Tämän jälkeen kaikkien access pointien hallinta onnistuu virtuaalisella kontrollerilla, jolle voidaan antaa IP-osoite käskyillä

- *virtual-controller-ip x.x.x.x*
- *end*
- *commit apply*

Virtuaaliseen kontrolleriin päästään syöttämällä IP-osoite web-selaimeen. (Aruba Networks Community, 2017)

7.4.3 Wlan-profiilien lisääminen

Virtuaalisen kontrollerin kautta voidaan langattomaan verkkoon lisätä AP-profiileja, joista jokainen näkyy loppukäyttäjällä omana langattomana verkkonaan. Järjestelmään luodaan AP-profiilit HydrolineWlan, TuotantoWlan ja VierailijaWlan. AP-profiilin luonti tapahtuu menemällä Networks-välilehdelle, missä klikataan New. Näkymässä (kuva 14) annetaan SSID eli wlan verkon nimi ja verkon ensisijainen käyttötarkoitus. Tarvittaessa asetuksia voidaan muuttaa enemmän avaamalla Show advanced options-näkymä. Seuraavaksi liikutaan VLAN välilehdelle, jossa valitaan mihin vlaniin langaton verkko kohdistuu. Lisäksi valitaan, että verkon laitteet saavat IP-osoitteensa muualta verkosta, eikä virtuaaliselta kontrollerilta. Security välilehdellä valitaan salaustasoksi Personal, salaustavaksi WPA-2 Enterprise ja syötetään salasana verkkoon liittymistä varten. Viimeiseksi asetukset tallennetaan. (Aruba Networks Community, 2017)



KUVA 14. Uuden WLAN-verkkoprofiilin luonti Aruba Instant virtual controllerilla (Aruba Networks Community, 2017)

8 VERKON KÄYTTÖÖNOTTO

Uuden tietoverkon käyttöönotto ei saa aiheuttaa katkoksia eikä haittaa tuotannolle. Työ on siis tehtävä viikonloppuisin, kun tehtaalla ei ole tuotantoa ja suoritetut vaiheet on testattava tarkasti, jotta tiedetään ettei ongelmia esiinny tuotannon jatkuessa. Käyttöönotto on syytä suorittaa vaiheittain työmäärän jakamisen vuoksi kahdelle tai useammalle viikonlopulle. Työ jaetaan kolmeen vaiheeseen, jotka ovat: langallisen verkon käyttöönotto ilman vlaneja, vlanien käyttöönotto ja langattoman verkon käyttöönotto.

8.1 1. vaihe

Verkkolaitteet konfiguroidaan aluksi lopullisen konfiguroinnin mukaisesti muuten, mutta kaikki portit kohdistetaan vlaniin 40, jonka IP-osoitealue on sama kuin vanhassa verkossa. Tämä siksi, että ensimmäisenä viikonloppuna voidaan ottaa käyttöön uudet verkkolaitteet ja testata niiden ja verkon perustoiminta ilman, että päätelaitteiden IP-osoitteita tarvitaan vielä muuttaa. Päätelaitteita ei siis jaeta suunnitelman mukaisiin vlaneihin vaan jako pidetään ennallaan vanhan verkon mukaisesti. Näin varmistetaan, että yhden viikonlopun aikana aika riittää varmasti saada uudet verkkolaitteet ja verkko toimimaan niin, että tuotannossa ei ilmene ongelmia.

Uuden verkon käyttöönotto valmistellaan mahdollisimman pitkälle jo tuotannon aikana, että työt viikonloppuisin jäisivät mahdollisimman vähäisiksi ja aikaa jäisi enemmän mahdollisten vikatilanteiden selvittämiseen Uudet verkkolaitteet konfiguroidaan ja verkon toimivuus testataan demoympäristössä. Toisin sanoen verkkolaitteet konfiguroidaan 1. vaiheen mukaisesti ja kytketään toisiinsa tulevan kaapeloinnin mukaisesti työpöydällä, jolloin runkoverkon toimivuus voidaan testata ja mahdollisia ongelmia korjata. Kun verkon toimivuus on saatu todennettua, voidaan verkkolaitteet asentaa jakamoihin räkkitelineisiin vanhojen laitteiden rinnalle. Asennukset voidaan tehdä tuotannon aikana, sillä kaapeleita ei vielä kytketä paikalleen.

Viikonlopun aikana kaikki vanhat verkkokaapelit ristikytkentärimoilla vaihdetaan uusiin kytkimiin. Tässä vaiheessa IP-osoitteita ei tarvitse vaihtaa päätelaitteilla, koska IP-osoitealue on sama kuin vanhassa verkossa. Verkon toimivuus testataan päätelaitteilla käyttämällä eri ohjelmistoja, jotka käyttävät yhteyttä palvelimiin. Verkkolaitteista on syytä testata varsinkin spanning treen toiminta, ettei verkkoon vain ole muodostunut silmukoita, jotka puurouttaisivat verkkoliikenteen ennen pitkää.

8.2 2. ja 3. vaihe

Toisena viikonloppuna aletaan ottaa käyttöön vlaneja portaittain. Eriytetään ensimmäisenä tuotannon laitteet omaan vlaniinsa, jonka jälkeen niihin vaihdetaan IP-osoitteet alueen mukaisiksi ja testataan yhteydet sekä laitteiden toiminta. Seuraavaksi tehdään samat vaiheet toimisto vlanin päätelaitteille. Viimeiseksi siirretään työstökoneet omaan vlaniinsa laite kerrallaan ja testataan koko ajan koneiden yhteydet ja toiminta.

Wlan-tukiasemat voidaan asentaa paikoilleen jo tuotannon aikana ja kytkeä päälle vanhojen tukiasemien rinnalle. Käyttöön otetaan langattomat verkot vierailija, hydrowlan ja tuotanto. Wlanilla yhdistettävät laitteet yhdistetään uudelleen uusiin langattomiin verkkoihin, jonka jälkeen testataan niiden toiminta. Uusien wlanien toiminto voidaan testata muutamalla päätelaitteella, jonka jälkeen päätelaitteiden siirtäminen uuteen wlaniin pitäisi sujua ongelmitta ja voidaan suorittaa tuotannon aikanakin. Kun kaikki päätelaitteet on saatu siirrettyä uusiin wlaneihin, voidaan vanhat järjestelmät sammuttaa ja purkaa.

9 DOKUMENTOINTI

Hyvä dokumentointi auttaa verkon ylläpidossa. Ylläpitäjän tueksi tuotetaan ainakin taulukko kaapeleista kytkimien ja ristikytkentärimojen välillä, kattavat loogiset kuvaukset verkosta, verkkolaitteiden sijainnit tehtaassa (tärkeää ainakin WLAN-tukiasemien osalta) ja taulukko staattisesti määritetyistä IP-osoitteista. Tuotettava dokumentointi on salaista, eikä sitä anneta kuin yrityksen sisäiseen käyttöön verkon ylläpitäjälle.

Ristikytkentätaulukkoon listataan jokaisen kytkimen jokainen portti. Portin kohdalle merkitään mihin tietoliikennerasiaan portista on kytketty kaapeli (ristikytkentärimalle), mikä vlan porttiin on määritetty ja onko portissa mitään erikoista tai huomautettavaa. Ristikytkentätaulukko on keino hallita, minne mikäkin laite on verkossa kytketty ja mihin vlaniin se kuuluu ja mitä portteja on vielä vapaana.

Loogisesta kuvauksesta käy ilmi verkkolaitteiden hierarkinen sijainti verkossa. Fyysistä sijaintia tehtaassa kuvasta ei käy ilmi. Loogiseen kuvaan piirretään kaikki verkkoon liittyvät verkkolaitteet kuten kytkimet, WLAN-tukiasemat, palomuuri tai reititin ja ainoastaan ylläpidolle kuuluvat laitteet kuten palvelimet tai IP-kamerat. käyttäjien päätelaitteita kuvaukseen ei tule. Kuvaukseen piirretään laitteiden väliset yhteydet. Loogisen kuvauksen rinnalle tehdään kuva tehtaan pohjapiirroksesta, jonka päälle sijoitetaan verkkolaitteet. Tästä kuvasta käy ilmi laitteiden sijainnit tehtaassa.

IP-osoite taulukko auttaa seuraamaan mitä staattisia IP-osoitteita on varattu ja millekin laitteelle. Taulukosta käy myös ilmi mitkä alueet on varattu DHCP-palvelimelle automaattisesti jaettavaksi. Ylläpidolle IP-osoitetaulukko on ainoa keino seurata, mikä IP-osoite milläkin laitteella on annettu. Ympäristössä, jossa on satoja laitteita, laitteiden IP-osoitteiden selvittäminen ilman taulukkoa on aikaa vievää ja hankalaa.

10 YHTEENVETO

Tämän työn aikana tietoverkon uudistamista ei vielä toteutettu yrityksessä muiden projektien kiireellisyyden vuoksi. Tämä työ antaa koosteen tietoverkon suunnittelun vaiheista ja toteuttamisesta. Työn vaiheet, teoriatiedot ja konfiguroinnit ovat sovellettavissa moneen yritykseen ja tarjoavat hyvää perustietoa verkossa tarvittavissa yleisimmistä tekniikoista sekä nykyisistä keinoista kohentaa tietoturvaa ja verkon monitorointia. Työssä on painotettu verkon vikasietoisuutta sekä ulkoisiin uhkiin varautumista, mikä on monessa yrityksessä tavoitteena.

Verkkolaitteista työssä on käsitelty ainoastaan Hewlett & Packard Enterprisen ja Aruban laitteita. Tässä työssä ei siis vertailla laitteiden apremmuutta tai soveltuvuutta, mikä olisi varmasti kiinnostavaa tutkia ennen verkon toteutusta. Myös konfiguroinnit on suunniteltu kyseisille verkkolaitteille eivätkä ne suoraan sovi muiden valmistajien tai jopa saman valmistajan eri sarjan laitteisiin. Periaatteet ovat kuitenkin usein samat, joten konfiguroinnit ovat helposti sovellettavissa.

Kokonaisuutena työtä voidaan pitää onnistuneena. Työ täyttää tilaajan vaatimukset ja yrityksessä pystytään tekemään tietoverkon päivitys tämän työn pohjalta. Työhän voi tulla vielä verkkolaitteita koskevia muutoksia toteuksessa.

11 LÄHTEET

Aruba Network AirWave. (28. maaliskuu 2017). *Aruba AirWave*. Noudettu osoitteesta http://www.arubanetworks.com/products/networking/management/airwave/

Aruba Networks. (4. huhtikuu 2017). *Aruba Networks*. Noudettu osoitteesta http://whp-aus1.cold.extweb.hp.com/pub/networking/software/Security-Oct2005-59906024-Chap09-Port_Security.pdf

Aruba Networks AirWave. (28. maaliskuu 2017). *Aruba Networks AirWave*. Noudettu osoitteesta http://www.arubanetworks.com/assets/ds/DS_AW.pdf

Aruba networks. (ei pvm). *Aruba networks*. Haettu 13. Tammikuu 2017 osoitteesta http://www.arubanetworks.com/products/networking/access-points/210-series/

Aruba networks. (ei pvm). *Aruba networks*. Haettu 13. Tammikuu 2017 osoitteesta http://www.arubanetworks.com/products/networking/access-points/200-series/

Aruba networks. (ei pvm). *Aruba networks*. Haettu 20. Tammikuu 2017 osoitteesta http://www.arubanetworks.com/products/networking/access-points/

Aruba Networks. (ei pvm). *Aruba Networks*. Haettu 15. Tammikuu 2017 osoitteesta http://www.arubanetworks.com/assets/ds/DS_AP200Series.pdf

Aruba Networks. (ei pvm). *Aruba Networks*. Haettu 15. Tammikuu 2017 osoitteesta http://www.arubanetworks.com/assets/ds/DS_AP210Series.pdf

Aruba Networks Community. (4. huhtikuu 2017). *Aruba Networks Community*. Noudettu osoitteesta https://community.arubanetworks.com/aruba/attachments/aruba/IAP/6915/1/Aruba%20Instant%206.4.0.2-4.1%20User%20Guide.pdf

Bilgi, G. (10. kesäkuu 2015). *The Cisco Learning Network*. Haettu 15. Tammikuu 2017 osoitteesta https://learningnetwork.cisco.com/thread/62241

CDW. (ei pvm). *cdw.com*. Haettu 7. Maaliskuu 2017 osoitteesta https://webobjects2.cdw.com/is/image/CDW/3907793?$product-main$

Cisco. (12. helmikuu 2014). *Cisco*. Haettu 15. Tammikuu 2017 osoitteesta http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html

Cisco. (4. huhtikuu 2017). *Cisco.com*. Noudettu osoitteesta http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html

Cisco. (ei pvm). *Cisco*. Haettu 20. Tammikuu 2017 osoitteesta http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html

FlexOptix. (7. syyskuu 2011). *felxoptix.net*. Haettu 13. Tammikuu 2017 osoitteesta https://www.flexoptix.net/en/blog/2011/09/getting-a-10g-stable-ethernet-link-even-when-using-old-multimode-fiber-om2-om1/

Fortinet. (7. huhtikuu 2017). *Fortinet*. Noudettu osoitteesta https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-firewall/next-generation-firewall-ngfw.html

Fortinet. (7. Huhtikuu 2017). *Fortinet.com*. Noudettu osoitteesta https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

Fortinet. (7. huhtikuu 2017). *Fortinet.com*. Noudettu osoitteesta https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiCloud.pdf

Hewlett & Packard enterprise. (ei pvm). *HPe.com*. Haettu 7. Maaliskuu 2017 osoitteesta https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-2927ENN.pdf

Hewlett Packard. (syyskuu 2010). *Hewlett Packard Enterprise*. Haettu 15. Tammikuu 2017 osoitteesta https://h17007.www1.hpe.com/docs/reports/irf.pdf

Hewlett Packard Enterprise. (elokuu 2015). *Hewlett Packard Enterprise*. Haettu 14. Tammikuu 2017 osoitteesta https://h50146.www5.hpe.com/products/networking/datasheet/HP_5130EI_Switch_Series_J.pdf

Hewlett Packard Enterprise. (elokuu 2016). *Hewlett Packard Enterprise*. Haettu 15. Tammikuu 2017 osoitteesta https://www.hpe.com/h20195/v2/GetDocument.aspx?docname=c04111414

Hewlett Packard enterprise. (ei pvm). *Hewlett Packard enterprise*. Haettu 13. Tammikuu 2016 osoitteesta https://www.hpe.com/us/en/product-catalog/networking/networking-switches/pip.overview.networking-switches.5333809.html

Hewlett Packard enterprise. (ei pvm). *Hewlett Packard enterprise*. Haettu 13. Tammikuu 2017 osoitteesta https://www.hpe.com/us/en/product-catalog/networking/networking-switches/pip.overview.networking-switches.6845578.html

HPe Support. (27. Maaliskuu 2017). *HPe Support*. Noudettu osoitteesta https://h10145.www1.hpe.com/Downloads/DownloadSoftware.aspx?SoftwareReleaseUId=19003&ProductNumber=J9776A&lang=en&cc=us&prodSeriesId=5333803&SaidNumber=

HPe Support. (27. maaliskuu 2017). *HPe Support*. Noudettu osoitteesta https://h10145.www1.hpe.com/Downloads/DownloadSoftware.aspx?SoftwareReleaseUId=19179&ProductNumber=JH324A&lang=en&cc=us&prodSeriesId=1008605458&SaidNumber=

Hydroline Oy. (ei pvm). *Hydroline Oy*. Haettu 6. Maaliskuu 2017 osoitteesta http://www.hydroline.fi/en/people/history/

Martin, V. (31. joulukuu 2015). *The Fortinet Cookbook*. Noudettu osoitteesta http://cookbook.fortinet.com/why-you-should-use-ssl-inspection/

Michel. (15. joulukuu 2015). *Network Guy*. Haettu 7. Maaliskuu 2017 osoitteesta https://networkguy.de/wp-content/uploads/2015/12/IRF-5920.png

Michel, N. (16. joulukuu 2015). *Network Guy*. Noudettu osoitteesta https://networkguy.de/?p=1124

NTP.org. (26. maaliskuu 2017). *NTP.org*. Noudettu osoitteesta http://www.ntp.org/ntpfaq/NTP-s-def.htm

Weebly.com. (20. maaliskuu 2015). *Weebly.com*. Noudettu osoitteesta http://1.bp.blogspot.com/-1SsLqqA06aY/VQrua520fgI/AAAAAAAAD1o/a2GM95QLIPQ/s1600/2015-03-19_11-36-48.png

Verkkokauppa.com. (ei pvm). *verkkokauppa.com*. Haettu 7. Maaliskuu 2017 osoitteesta https://cdn-c.verkkokauppa.com/images/63/2_159223-2000x567.jpeg

Verkkokauppa.com. (ei pvm). *verkkokauppa.com*. Haettu 7. Maaliskuu 2017 osoitteesta https://cdn-b.verkkokauppa.com/576/images/36/2_283085-816x926.jpeg

Äikäs, J. (15. toukokuu 2015). *Theseus*. Haettu 15. Tammikuu 2017 osoitteesta https://www.theseus.fi/bitstream/handle/10024/96063/Aikas_Jussi.pdf?sequence=1