KARELIA-AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Janne Mäkisalo

TIETOVERKON SUUNNITTELU HURRY OY:LLE

Opinnäytetyö
Toukokuu 2016

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Toukokuu 2016** **Tietotekniikan koulutusohjelma** Karjalankatu 3 80200 JOENSUU 013 260 600

Tekijä
Janne Mäkisalo

Nimeke
Tietoverkon suunnittelu Hurry Oy:lle

Toimeksiantaja
Hurry Oy

Tiivistelmä

Opinnäytetyön tavoitteena oli suunnitella tietoverkko uuteen vielä valmistumattomaan teollisuushalliin. Opinnäytetyön oli myös tarkoitus toimia toimeksiantajalle pohjana vastaavanlaisten projektien varalle. Työn tehtävänä oli suunnitella verkko määritettyjen vaatimusten perusteella ja selvittää tietoverkon suunnittelun eri vaiheita ja käytäntöjä.

Opinnäytetyön toimeksianto saatiin joensuulaiselta Hurry Oy:ltä. Opinnäytetyön oli tarkoitus toimia heille ohjeena heidän syksyllä 2016 valmistuvan hallin tietoverkon toteutuksessa. Hallissa toimii useita eri yrityksiä, joten verkon tietoturva nousi keskeiseksi aiheeksi. Yrityksillä oli langallisen yhteyden lisäksi oma langaton verkko. Suunnitelmaan tuli myös kattava vierasverkko, joka jatkuu katkeamattomana koko rakennuksessa.

Opinnäytetyön toteutuksen suurin ongelma oli epävarmuus toimeksiantajan puolelta. Rakennuksessa toimivien yritysten tarkka lukumäärä ei ollut vielä tiedossa. Rakennuksen pohjapiirroskaan ei ollut vielä täysin valmis. Opinnäytetyössä kehitettiin ratkaisu, joka toimisi eri muuttujista huolimatta.

Kieli suomi	Sivuja 35 Liitteet 1

Asiasanat
suunnittelu, tietotekniikka, verkko

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
May 2016
Degree Programme in Information Technology
Karjalankatu 9
80220 JOENSUU
FINLAND
013 260 600

Author
Janne Mäkisalo

Title
Network plan for Hurry Oy

Commissioned by
Hurry Oy

Abstract

The main goal of this thesis was to plan a network for an office building. Another goal of the thesis was to create a document the commissioner could refer to in other similar projects. The task of this thesis was to plan a network based on the requirements and inform the commissioner of good practices and steps of network planning.

The thesis was commissioned by a Finnish company Hurry Oy which is based in Joensuu. This thesis will be used as a guide for their network in their new office building that will be finished in fall 2016. There are also other companies working in the same office complex so network security became an important focus. The companies will be using a wired as well as wireless connection. The plan also had a seamless guest network.

The main issue in the thesis was uncertainty from the commissioner. The number of companies working in the office building was uncertain and the floor plan of the building was not yet completely finalized. A solution that will work regardless of these variables was developed in this thesis.

Language
Finnish

Pages 35

Appendices 1

Keywords
planning, information technology, network

Sisältö

Liitteet

1 Johdanto

Tietoverkon suunnittelu on jatkuva prosessi, joka kiertää kehää suunnittelusta ylläpitoon. Nopeat ja vakaat tietoverkot ovat elinehto moderneille yrityksille. Tietoverkkojen vaatimukset kasvavat koko ajan, sillä verkon on oltava saatavilla milloin vain mistä vain. Tietoverkko on onnistunut silloin, kun se ei vaikuta käyttäjän työhön mitenkään vaan toimii kuin itsestään ja katkeamatta.

Opinnäytetyöni tavoitteena oli suunnitella tietoverkko Hurry Oy:n uuteen syksyllä 2016 valmistuvaan teollisuushalliin. Hurry Oy on joensuulainen markkinoinnin ja mainonnan kehittämispalveluita tarjoava yhtiö. (Hurry Oy, 2016.) Rakennuksessa toimii muitakin yrityksiä, joiden tarkka lukumäärä ei ole vielä tiedossa. Koska samaa verkkoa käyttävät useat eri yritykset, oli verkon tietoturva erittäin tärkeässä asemassa. Yritysten verkot oli kyettävä pitämään erillään toisistaan. Haastetta eristämiseen lisää se että heidän oli osittain tarkoitus pystyä käyttämään samoja resursseja, kuten tiedostopalvelinta ja tulostinta.

Opinnäytetyön toinen tehtävä oli luoda dokumentti Hurry Oy:lle, jota he voivat käyttää oppaana tietoverkon suunnittelussa vastaavanlaisissa projekteissa. Tässä työssä esitellään tietoverkon ylläpidon vaiheita valmistelusta optimointiin ja tietoverkon vaatimuksia käyttäjän näkökulmasta, sekä miten ne toteutetaan.

Opinnäytetyössä on verkkolaitteiden konfigurointiohje Hurry Oy:n uutta verkkoa esimerkkinä käyttäen. Verkko toteutettiin käyttäen UniFi-laitteistoa. Aihe rajattiin koskemaan vain tiedostopalvelinta ja sisäverkkoa. Muut palvelut ja sovellukset toimitettiin SaaS-palveluna.

2 PPDIOO

Tietoverkon suunnittelun vaiheita kuvaamaan on tehty useita eri malleja, joista yksi on Cisco Systemsin kehittämä PPDIOO-malli. PPDIOO tulee englannin kielen sanoista prepare, plan, design, implement, operate ja optimize, joka on suomennettuna valmistelu, suunnittelu, luonnostelu, käyttöönotto, käyttö ja viimeistely. (Wilkins, 2011.) PPDIOO-mallin tarkoitus on pitää suunnitteluprosessi organisoituna ja parantaa verkon ominaisuuksia vähentämällä verkosta aiheutuvia kustannuksia, nostaa verkon toimintavarmuutta, tehostaa yrityksen ketteryyttä ja nopeuttaa pääsyä palveluihin ja sovelluksiin. Tässä opinnäytetyössä käytiin läpi vaiheet valmistelusta luonnokseen.

PPDIOO-mallin ensimmäinen vaihe on valmistelu. Tässä vaiheessa selvitetään organisaation tarpeet ja luodaan verkkostrategia. Valmisteluvaiheessa asetetaan taloudellinen perustelu verkon muutostarpeelle. (Wilkins, 2011.) Tässä tapauksessa valmisteluvaiheen muutostarpeen syy on tietenkin tilojen vaihtaminen ja sitä seuraava uuden verkon rakentaminen. Muita syitä voi olla esimerkiksi verkkostrategiassa määritetyn verkkolaitteiden elinkaarenkaaren päättyminen.

Suunnittelussa tunnistetaan tarve muutoksille tai parannuksille esimerkiksi tavoitteiden, laitteiden tai käyttäjien näkökulmasta. Samassa vaiheessa tarkastellaan jo mahdollisia olemassa olevia verkkoja ja tunnistetaan niiden sekä uusien osioiden välinen ero suorituskyvyssä ja tukeeko vanha verkko uutta osiota. Suunnitelmassa määritellään projektin tehtävät, tavoitteet, vastuut, sekä vaaditut resurssit suunnitelman toteuttamiseksi. (Wilkins, 2011.) Aloitin suunnitteluvaiheen tunnistamalla tietoverkon vaatimukset. Kun on tiedossa, mitä verkon käyttäjät tarvitsevat verkolta, voidaan se suunnitella ja mitoittaa vastaamaan niitä vaatimuksia.

Luonnoksessa käytetään hyväksi aikaisemmassa kohdassa laadittuja vaatimuksia ja toteutetaan tekninen raportti siitä, miten työ toteutetaan. Siinä määritellään, miten verkon tuki, luotettavuus, turvallisuus, skaalautuvuus ja suoritus-

kyky saadaan konkreettisesti vastaamaan suunniteltua tasoa. (Wilkins, 2011.) Luonnoksessa selvitettiin, miten verkko ja sen vaatimukset toteutetaan.

Käyttöönottovaiheessa pannaan verkko toimeen aikaisemmin laaditun raportin pohjalta. Verkko rakennetaan tai lisäkomponentit lisätään jo olemassa olevaan verkkoon häiritsemättä sen toimintaa. Käyttövaihe on viimeinen testi suunnitelman toimivuudelle. Verkkoa ylläpidetään operaatioilla, jotka varmistavat verkon toimivuuden ja vähentävät kustannuksia. Ylläpidossa huomatut viat, tehdyt korjaukset sekä yleinen suorituskyvyn tarkkailu antavat alkutiedot seuraavaan optimointivaiheeseen. (Wilkins, 2011.) Nämä vaiheet toteuttaa Hurry Oy:n syksyllä 2016.

Viimeistely on PPDIOO-mallin viimeinen vaihe. Tämän vaiheen tarkoituksena on tunnistaa ja korjata mahdolliset ongelmat verkossa ennen kuin ne vaikuttavat organisaation toimintaan. Ongelmanratkontaa tarvitaan, mikäli vikoja ei voida tunnistaa ja välttää ennen niiden tapahtumista. Tämä vaihe voi käynnistää valmistelun verkon päivittämiselle ja koko prosessi alkaa taas alusta, mikäli nykyisen verkon suorituskyky ei vastaa käyttäjän odotuksia tai uudet sovellukset eivät ole yhteensopivia verkon kanssa. (Wilkins, 2011.)

3 Verkon vaatimukset

Tietoverkon suunnittelu ei voi alkaa ennen kuin tiedetään, mitkä ovat verkon vaatimukset. Vaatimuksien määrittelyssä on tärkeää huomioida käyttäjän tarpeet ja käyttötarkoitukset. Tässä kappaleessa käsitellään yleisiä verkon vaatimuksia verkon loppukäyttäjän näkökulmasta ja miten nämä vaatimukset toteutetaan Hurry Oy:n projektia esimerkkinä käyttäen.

3.1 Verkon vaatimukset käyttäjälle

Tietoverkon käyttäjän kannalta tärkeitä vaatimuksia ja ominaisuuksia verkon kannalta ovat nopeus, luotettavuus, laatu, mukautuvuus, turvallisuus, hinta, tuettavuus ja kasvun mahdollistaminen. Verkon nopeus ilmenee kahdella tavalla, joista ensimmäinen on nopeus, jolla käyttäjä pääsee käsiksi, siirtämään tai muokkaamaan haluamaansa tietoa. Riittävä nopeus on hyvin subjektiivinen käsite ja se voi tarkoittaa esimerkiksi, että käyttäjä haluaa ladata tiedostoja palvelimelta vähintään kymmenen minuutin kuluessa tai, että hän saa videollensa kuvan joka kolmaskymmenes millisekunti. Tälle käytetään käsitettä ”timeliness”, joka voidaan suoraan kääntää ajallisuudeksi. Tätä voidaan mitata esimerkiksi ping-viiveellä. (McCabe, 2010, 62–63.)

Toinen puoli nopeudesta on vuorovaikutus, joka keskittyy järjestelmän ja verkon vastausaikaan. Aikaisempaa esimerkkiä hyödyntäen kymmenen minuutin latausaikaa palvelimelta voidaan pitää järjestelmän vastausaikana. Vuorovaikutusajan tulisi olla mahdollisimman lähellä käyttäjän reaktiota. Ajallisuus vastaa siis aikaa, jolla tiedosto tai kuva siirtyy verkon yli ja vuorovaikutus aikaa, joka kuluu esimerkiksi etäyhteyksien ja selaimien käytössä. (McCabe, 2010, 62–83.)

Luotettavuus näkyy käyttäjälle palvelun saatavuutena. Se tarkoittaa, että palvelut ja resurssit ovat jatkuvasti saatavilla. Laatu tarkoittaa tässä yhteydessä esityksen laatua, jonka käyttäjä havaitsee. Se voi tarkoittaa äänen tai videon laatua, jota käyttäjä tarvitsee ja haluaa. Nykypäivänä videokonferensseissa ja internet-puheluissa ei riitä välttävä laatu, vaan sen on oltava hyvä tai jopa parempi kuin muilla. (McCabe, 2010, 62–83.)

Mukautuvuus on verkon kyky mukautua käyttäjän muuttuviin tarpeisiin. Näitä voi olla esimerkiksi verkon toimivuus välimatkasta riippumatta. Käyttäjät eivät välitä siitä missä palvelimet ovat, kunhan palvelu vain toimii. Turvallisuus on käyttäjän näkökulmasta takuu käyttäjän tietojen ja fyysisten resurssien yksityisyydestä ja koskemattomuudesta. Se lisää verkon luotettavuutta, mutta voi vaikuttaa negatiivisesti verkon nopeuteen. (McCabe, 2010, 62–83.)

Hinta on verkon kyky pysyä budjetissa. Vaikka tämä vaatimus ei ole tekninen, se vaikuttaa hyvin suuresti verkon arkkitehtuuriin ja muotoon. Tuettavuus on ominaisuus, joka kertoo kuinka hyvin käyttäjä pystyy pitämään verkon toiminnassa suunnitellulla tasolla. Tuettavuuteen liittyy käyttäjän tarve tukeen verkon ylläpidolle. (McCabe, 2010, 62–83.)

3.2 Vaatimusten toteuttaminen

Turvallisuus on minkä tahansa verkon tärkeimpiä vaatimuksia. Sisä- ja ulkoverkon väliin asetettu fyysinen laitepalomuuri suojaa yrityksiä ulkoisilta uhkilta tehokkaasti ja suodattaa pois ei haluttua liikennettä. Se ei kuitenkaan korvaa ohjelmistopalomuuria työasemilla. Verkko, jossa toimii useita eri yritystä asettaa jo itsessään haasteensa tietoturvalle. Yritysten on tarkoitus päästä hyödyntämään yhteisiä resursseja, kuten tulostinta ja tiedostopalvelinta. Verkkojen eristäminen toteutetaan VLAN-tekniikalla. Yritykset voivat käyttää samaa fyysistä verkkoa pääsemättä vahingossakaan toistensa osioihin. Langattomien yhteyksien suojaus tapahtuu jakamalla yrityksille omat SSID:t ja salasanat. Vierailijat saavat oman WLAN-verkon, joka myöskin eristetään yritysten tietoliikenteestä. Tässä projektissa on otettava huomioon myös fyysinen turvallisuus. Rakennuksessa tulee valvontakameroita, jotka hyödyntävät samaa verkkoa.

Hyvä verkko on helposti laajennettava ja luotettava. Siihen pystyy tarpeen vaatiessa lisäämään uusia laitteita helposti ja se toimii varmasti. Toimivuuden varmistamiseksi yhteys varmistetaan lankayhteyden lisäksi langattomalla 4G-yhteydellä, joka käynnistyy jos valokuituyhteys katkeaa tai siinä on häiriöitä. Verkkoa voidaan laajentaa helposti sen vaatimatta suurempia toimenpiteitä. Verkkoa ylläpitää Hurry Oy.

4 Toteutuksessa käytettäviä tekniikoita

Virtualisointi on tekniikka, jolla laitteen fyysiset resurssit jaetaan ohjelmallisesti hypervisorin ohjauksella virtuaaliympäristöille tai -laitteille. Virtualisointi muuttaa fyysisen laitteen resurssit loogisiksi objekteiksi. (Portnoy. 2012.) Tässä työssä hyödynnettiin virtualisointia virtuaalilähiverkkojen ja tiedostopalvelimen muodossa. Virtuaalilähiverkko eli VLAN on tekniikka, jolla fyysinen verkko jaetaan loogisiin osioihin. VLAN jakaa verkon OSI-mallin toisella tasolla toimiviin ”broadcast domain” nimisiin segmentteihin. Ne määrittävät alueen, jolle lähetykset verkossa kulkevat. Jos samassa verkossa on määritetty useampi VLAN, lähetykset yhden virtuaalilähiverkon sisällä eivät koskaan ilmesty toisessa, ellei se erikseen tehdä mahdolliseksi reitittimen avulla ”router on a stick”-tekniikalla. (Cisco, 2014)

VPN eli virtual private network on tekniikka, jolla voidaan muodostaa turvallinen näennäinen lähiverkkoyhteys internetin yli. VPN-yhteydellä yrityksen työntekijä voi ottaa turvallisen yhteyden mistä tahansa yrityksen lähiverkkoon ja resursseihin. VPN voidaan muodostaa kahden reitittimen välillä, jolloin puhutaan site-to-site-yhteydestä. Tässä työssä käytetään kuitenkin remote-access-yhteyttä, joka mahdollistaa suojatun yhteyden muodostamista yrityksen verkkoon internetistä millä tahansa laitteella.

Langattomat lähiverkot perustuu IEEE 802.11-standardiin ja sen eri versioihin. Tällä hetkellä yleisimmät WLAN-standardit ovat esitettynä taulukossa 1. Toteutuksessa käytetään 802.11ac-standardia, koska sen tiedonsiirto nopeus on riittävän suuri yritystoimintaan. Lisäksi se käyttää 2,4 GHz:n ja 5 GHz:n taajuuksia, mikä vähentää häiriöitä ja katkoksia langattomassa verkossa. (Danielyan, Edgar, 2001)

Taulukko 1. yleisimmät IEEE 802.11-standardit

Standardi	Taajuus GHz	Teoreettinen kapasiteetti Mb/s
802.11g	2,4	54
802.11n	2,4 ja 5	600
802.11ac	2,4 ja 5	1300

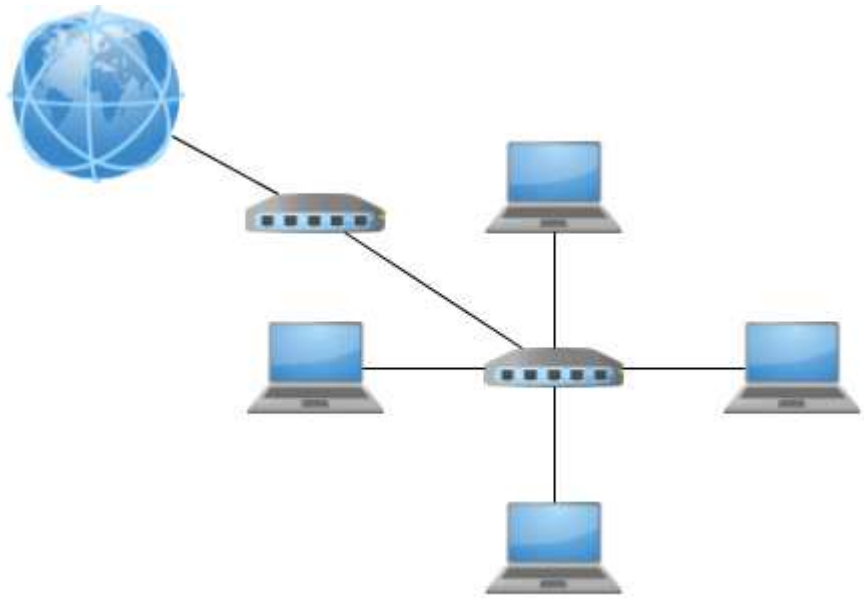
Langattoman verkon suojauksessa käytettiin WPA2-PSK-salausta. WPA2-PSK-salauksessa käytetään ennalta määritettyä avainta, joten tämä tapa ei vaadi erillistä autentikointipalvelinta. WPA2-PSK asetettiin käyttämään AES/CCMP-salausprotokollaa. AES/CCMP-salausprotokola kehitettiin vastaamaan IEEE 802.11i-standardin mukaisia langattoman tietoverkon tietoturvavaatimuksia. Se korvaa vanhemmat WEP- ja TKIP-salausprotokollat.

PoE eli power over Ethernet on tekniikka, jota jotkin kytkimet hyödyntävät. Se mahdollistaa käyttöjännitteen siirtämisen Ethernet-liitännän välityksellä. Yleisimmät tätä tekniikkaa käyttävät laitteet ovat WLAN-tukiasemat, mutta myös muut tietoverkkoon liitettävät laitteet kuten valvontakamerat ja IP-puhelimet voivat hyödyntää tekniikkaa. PoE pohjautuu IEEE 802.3af standardiin, jolloin suurin mahdollinen tehon tarve saa olla enintään 15.4W. Suurempaa tehon tarvetta varten on IEEE 802.3at standardiin pohjautuva PoE+, joka sallii 25.5W:n tehotarpeen. (Wikipedia, 2016.)

5 Verkkosuunnitelma

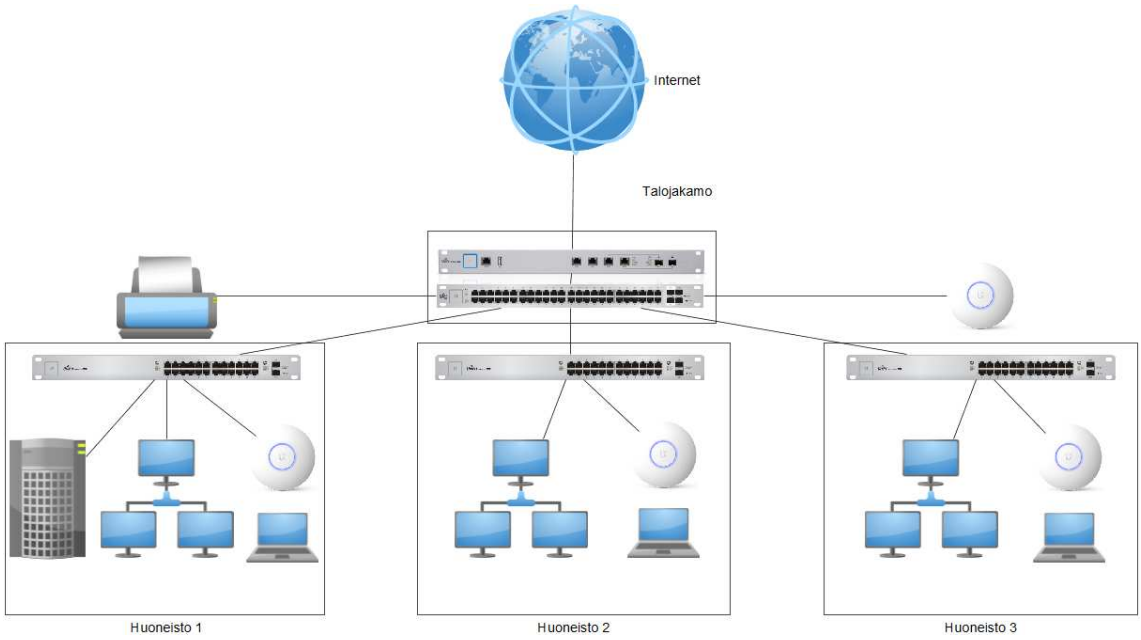
Aloitin verkkosuunnitelman luonnostelun tutustamalla rakennukseen ja sen sisäiseen atk-kaapelointiin. Verkkotopologian määrittäminen oli tämän vaiheen keskisimpiä tavoitteita. Verkkotopologia kuvaa tapaa, jolla tietokoneverkon laitteet kytkeytyvät toisiinsa. Yleisin verkkotopologia malli on tähti tai sen eri variaatiot. Tähtitopologiassa päätelaitteet ovat kytkettynä yhteen keskuslaitteeseen, joka ohjaa tietoliikennettä laitteiden välillä. (Ciccarelli & Faulkner, 2006.) Toiset

tunnetut topologiamallit kuten väylä ja rengas ovat jääneet suurelta osin pois käytöstä. Kuvassa 1 on esimerkki tähtitopologiasta. Siinä päätelaitteet ovat kytkettynä kytkimeen, josta on yhteys myös reitittimeen ja sitä kautta internettiin.



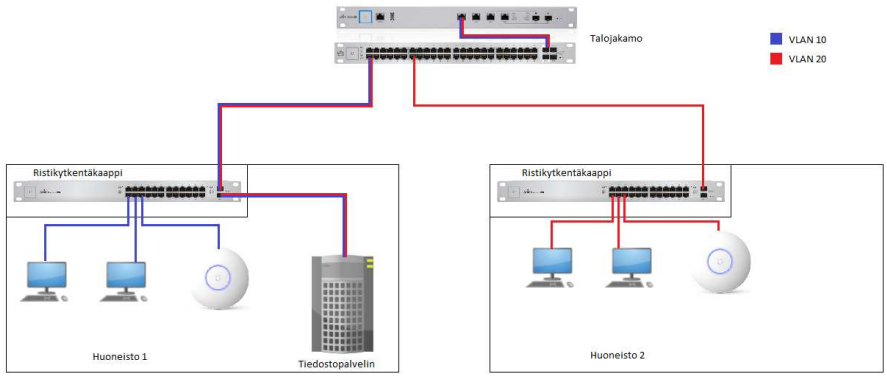
Kuva 1. Tähtitopologia

Kuvassa 2 on esitettynä tämän verkon topologia. Kuvassa talojakamoon on sijoitettuna reititin ja kytkin. Reitittimen kautta saatiin yhteys internettiin. Reitittimen internet yhteys oli kuituyhteyden lisäksi varmistettu 4G-yhteydellä, joka käynnistyi jos kuituyhteys ei toimi. Reititin oli kytketty runkokytkimeen, jonka kautta tieto siirtyi huoneistoihin ja sitä kautta päätelaitteille. Talojakamon kytkin ei varsinaisesti ollut runkokytkin, mutta käytin sitä nimitystä erottaakseni talojakamon ja huoneistojen kytkimet toisistaan. Osa yhteisistä tukiasemista ja tulostimista olivat suoraan yhteydessä runkokytkimeen. Huoneistossa olevat kytkimet jakoivat liikenteen huoneiston sisällä. Jokaisessa huoneistossa oli oma ristikytkentäkaappi, jonne tehtiin kytkennät kytkimen ja talon sisäisen atk-kaapeloinnin välillä. Huoneistoihin tuli myös omat tukiasemat. Huoneistokytkennät toteutettiin kuvan 1 tapaisella tähtitopologialla.



Kuva 2. Verkkokuva

Virtuaalilähiverkon tehtävä oli jakaa yritysten verkot omiin osioihinsa. Niiden ei ollut tarkoitus pystyä kommunikoimaan keskenään, mutta osalta niistä oli tarkoitus päästä käyttämään tulostinta ja tiedostopalvelinta. VLAN-tunnuksella merkitty liikenne jakautuu kuvan 3 esimerkin mukaisesti.



Kuva 3. VLAN-liikenne

6 Laitteisto

Laitteiston valmistajaksi valitsin toimeksiantajan toiveesta Ubiquiti-merkkiset laitteet. Toimeksiantajalla oli jo kokemusta niiden hallinnasta, mikä helpotti siirtymistä uuteen verkkoon. Laitteet olivat kilpailukykyisä verrattuna suurempiin ja tunnetumpiin valmistajiin hintansa ja helpon hallittavuuden kannalta.

Käyttämällä vain yhden valmistajan laitteita verkon ylläpito pysyi yksinkertaisempana ja hallittavampana, kuin useiden eri valmistajien laitteista koostuva verkko. Ubiquitilla oli UniFi controller-niminen verkonhallintatyökalu, jonka kautta kaikki heidän UniFi-malliset laitteet pystyttiin konfiguroimaan selkeää graafista käyttöliittymää hyödyntäen. (UniFi Controller, 2016.)

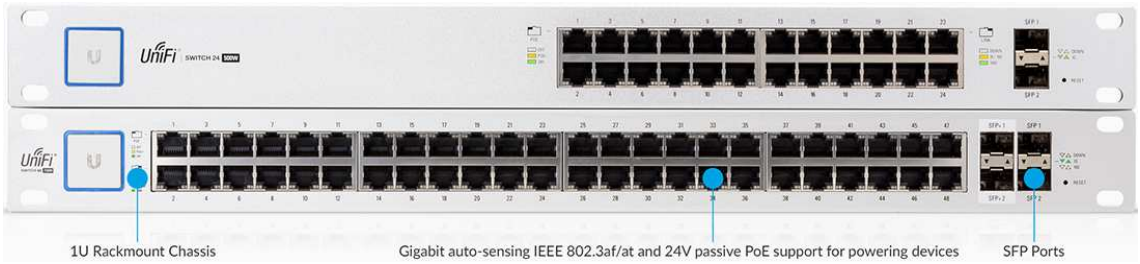
6.1 Reititin

Tietoliikenne kulkee rakennukseen ensimmäisenä reitittimen ja palomuurin läpi. Tilan ja rahan säästämiseksi valitsin laitteen, joka suoriutuu molemmista tehtävistä. UniFi Security Gateway Pro on laite, jossa on palomuurin ja reitittimen ominaisuudet. Laite lupaa kehittyneet palomuurisäännöt, sekä kattavat VLAN- ja DHCP-palvelut sisäverkolle. Laitteessa on kaksi RJ45 LAN-porttia, sekä kaksi RJ45-SFP-yhdistelmäporttia WAN-yhteyttä varten (kuva 4). (UniFi SG, 2014.)

Kuva 4. Security Gateway Pro (UniFi SG, 2014.)

6.2 Kytkimet

Runkokytkimeksi valitsin UniFi US-48-500W-mallisen kytkimen. Kytkin sijoitettiin suunnitellun verkkotopologian mukaisesti talojakamoon reitittimen lisäksi. Tähän kytkimeen tehdään ristikytkennät, jotka yhdistävät huoneistot talojakamoon ja sitä kautta ulkoverkkoon. Kytkimessä on 48 RJ45-porttia sekä kaksi SFP- ja SFP+-porttia (kuva 5). (UniFi Switch, 2014.)



Kuva 5. US-24-250W ja US-48-500W. (UniFi Switch, 2014.)

Huoneistoihin sijoitettavat kytkimet eivät vaadi yhtä suurta suorituskykyä kuin runkokytkin, mutta tulevaisuuden kasvun kannalta valitsin kytkimet, jotka eivät hidasta liikennettä vielä pitkään aikaan. US-24-250W on kuin aikaisemmin esitelty kytkin, mutta siinä on 24 RJ45-porttia ja kaksi SFP-porttia. (UniFi Switch, 2014.) Näitä kytkimiä tulee yksi jokaisen huoneiston ristikytkentäkaappiin. Taulukossa 1 on tarkemmin vertailtu kytkimien eroja.

Taulukko 2. Kytkimien ominaisuudet. (UniFi Switch, 2014.)

Malli	US-24-250W	ES-48-500W
Rajoittamaton tiedonsiirtonopeus	26 Gb/s	70 Gb/s
RJ45-portit	24	48
SFP+-portit	0	2
SFP-portit	2	2
Virrankulutus maksimissaan	250 W	500 W
PoE+	Kyllä	Kyllä

6.3 WLAN-tukiasemat

UniFi UAP-AC-Pro käyttää IEEE 802.11ac-standardia, mikä tekee siitä sopivan laitteen rakennuksen langattoman verkon toteuttamiseen. Laitteessa on antennit 2,4GHz ja 5GHz taajuuksille. 2,4GHz taajuuden suurin mahdollinen tiedonsiirtonopeus on 450 Mb/s ja 5GHz taajuuden 1300Mb/s. IEEE 802.11ac-standardi mahdollistaa nopean ja vakaan tavan siirtää dataa langattomasti. Signaalin kantavuus optimaalisissa olosuhteissa on 122 m, joten sijoittamalla muutaman laitteen tasaisin välimatkoin rakennukseen pystytään tekemään kattava ja katkeamaton langaton lähiverkko. (UniFi AP, 2015.)

Laite on helppo kiinnittää kattoon tai seinään. Laitteessa on kaksi RJ45-porttia. Laite tukee PoE+ tekniikkaa eli se ei vaadi erillistä virtalähdettä, jos se on suoraan kytketty kytkimeen, jonka portti on asetettu tukemaan samaa standardia. (UniFi AP, 2015.)

Kuva 6. UniFi UAP-AC-Pro. (UniFi AP, 2015.)

6.4 Muut laitteet

UniFi Cloud Key on pieni tietokone, jolle on esiasennettu UniFi Controller (kuva 7). Se kytketään johonkin runkokytkimen porteista. UniFi Cloud Key mahdollistaa verkon hallinnan ja tarkkailun etänä, eikä sitä varten tarvitse omistaa erillistä tietokonetta. Cloud Key tukee PoE+-tekniikkaa, joten se ei tarvitse erillistä virtalähdettä. (UniFi Cloud Key, 2015.)

Kuva 7. UniFi Cloud Key (UniFi Cloud Key, 2015.)

Tiedostopalvelin toteutetaan Hyper-V-virtualisointityökalulla Hurry Oy:n omalle palvelinlaitteistolle. Palvelin sijaitsee fyysisesti Hurry Oy:n tiloissa, mutta muillakin toimijoilla on pääsy omaan virtuaaliosioon palvelimella. Rakennuksessa on myös yhteinen tulostin. Turvalaitteet, kuten valvontakamerat käyttävät samaa verkkoa.

7 Yrityskohtainen ratkaisu

Koska rakennuksessa toimivien yritysten määrä ei ollut vielä tarkassa tiedossa, oli välttämätöntä kehittää paketti, joka toimii samalla tavalla yrityksestä huolimatta. Verkon laajentamisen ja ylläpidon helpottamiseksi kaikille rakennuksessa toimiville yrityksille tarjotaan samanlainen verkkoratkaisu. Tätä tapaa hyödyntäen verkkoa voidaan laajentaa tarpeen mukaan koskemaan niin montaa yritystä kuin on tarve.

Jokaiselle yritykselle tarjotaan oma yksityinen verkko. Reititin ja hallintatyökalu hoitavat verkon osoitteiden jaon sisäänrakennetulla DHCP-ominaisuudella. Jokainen verkko saa oman VLAN-tunnuksen, joka mahdollistaa yksityisen toiminnan heidän omissa verkko-osiossaan. Jokainen yritys saa myös oman WLAN-tukiaseman, jolle on konfiguroitu verkko heidän nimellään ja valitsemallaan salasanalla. Mikäli yritys haluaa, vierasverkko voidaan lisätä heidän tukiasemalleen. Taulukossa 3 on esitelty miten verkko-osoitteet jaettiin. VLAN 1 on järjestelmässä vakiona. VLAN-tunnukset 10–30 ovat yritysten käytössä, mutta VLAN 100 on omistettu vierasverkolle. Aliverkkoja voi luoda samalla kaavalla tarpeen vaatiessa lisää.

Taulukko 3. Verkko-osoitteet

VLAN ID	Aliverkko	Käytettävät osoitteet
1	192.168.1.1/24	192.168.1.6 - 192.168.1.254
10	192.168.10.1/24	192.168.10.6 - 192.168.10.254
20	192.168.20.1/24	192.168.20.6 - 192.168.20.254
30	192.168.30.1/24	192.168.30.6 - 192.168.30.254
100	192.168.100.1/24	192.168.100.6 - 192.168.100.254

Jokaisen yrityksen kytkennät noudattavat samaa kaavaa. Yrityksen kytkimen ja talojakamossa sijaitsevan kytkimen välinen yhteys toimii runkoporttina. Runkoportti ohjaa liikenteen kytkimien välillä ja siirtää VLAN-tunnuksella merkityt paketit kohti reititintä. Yrityksen kytkimien tila asetetaan alla olevan taulukon 4 mukaisesti. Portit, jotka eivät ole käytössä kytketään pois päältä.

Taulukko 4. Kytkimen portit

Portin numero	Portin tila	Porttiin kytketty laite
0/1	Trunk	Runkokytkin
0/2-0/23	Access	Päätelaite
0/24	Access	WLAN-tukiasema

8 Laitteiden asetukset

Tässä kappaleessa esitellään mitä laitteille täytyy tehdä, jotta ne saadaan toimimaan halutulla tavalla. Esimerkkinä konfiguroinnista on käytetty Hurry Oy:n osiota verkosta. Seuraamalla näitä ohjeita voidaan toteuttaa myös muut vastaavat verkot. Verkko-osoitteet ja nimet täytyy kuitenkin muuttaa tapauksen mukaan.

Ennen konfiguroinnin aloittamista on syytä päivittää kaikkien laitteiden ohjelmistot viimeisimpään versioon. Tämä tapahtuu menemällä virallisen valmistajan sivuille ja lataamalla uusimmat firmware-versiot. Kun laitteiden uusimmat versiot on ladattu, ne voidaan siirtää laitteille käyttämällä hallintatyökalun päivitys ominaisuutta.

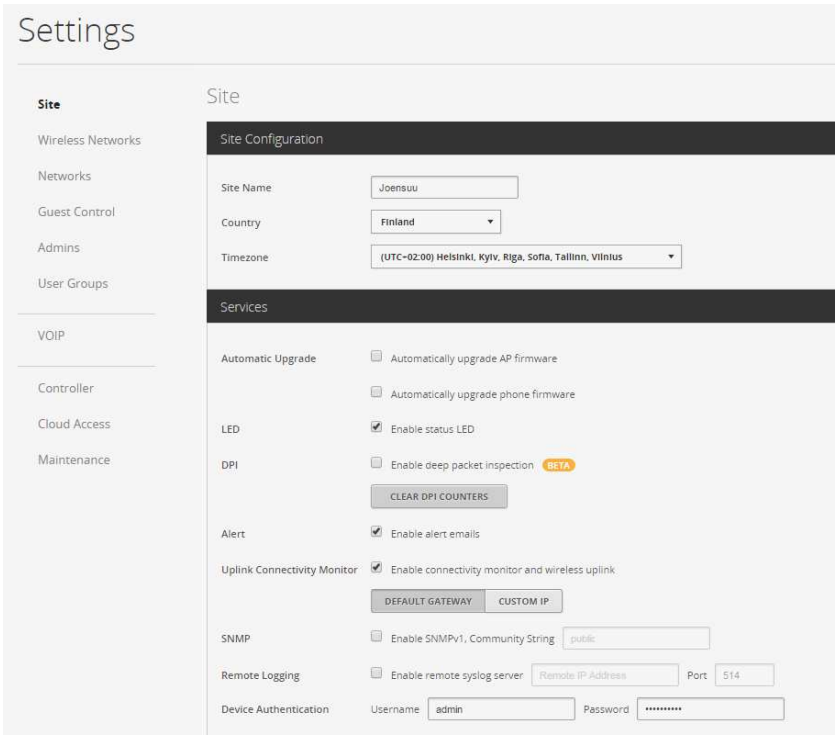
8.1 Cloud Key

Cloud Key kytketään johonkin runkokytkimen porteista. Jotta Cloud Key saadaan toimimaan, on samaan kytkimeen kiinnitettävä tietokone, jolla tehdään Cloud Key:n alkuasetukset. Oletuksena selaimella saadaan yhteys Cloud Key hallintatietokoneeseen osoitteella https://192.168.1.30. Seuraamalla ruudun ohjeita asennus onnistuu ongelmitta.

Asennuksen jälkeen muutetaan avaimen asetuksia. Navigoitua avaimen osoitteeseen, selaimella valitaan Configure Cloud Key. Sen jälkeen kirjaudutaan sisään. Oletuksena nimi ja salasana ovat ”ubnt”. Ensimmäisenä on vaihdettava salasana valitsemasta ikkunan oikeasta yläkulmasta Change Password. Sen jälkeen vaihdetaan Cloud Key:lle kiinteä IP-osoite. Osoitteen on hyvä olla kiinteä, jotta siihen saadaan aina yhteys samalla osoitteella. Annetaan laitteelle osoite oletusverkosta esimerkiksi 192.168.1.100. Se tehdään configure-välilehdellä valitsemalle network-osion configuration mode-kohdasta ”static”. Tämän jälkeen yhteys hallintatietokoneeseen otetaan määritellyllä IP-osoitteella.

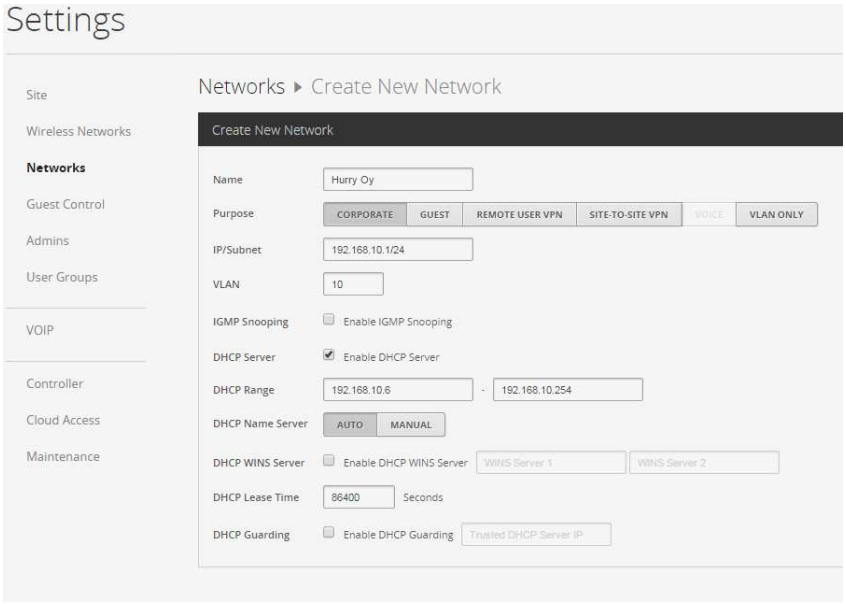
8.2 UniFi Security Gateway

UniFi Controller voi hallita useita verkkoja site eli sijaintiominaisuudella. Jokaisella sijainnilla on omat kartat, statistiikat, vierailija-asetukset, laitteet ja verkon hallitsijatunnukset. Kuvassa 8 on esimerkki ratkaisu.



Kuva 8. UniFi Controller sijainti esimerkki

Seuraavaksi controlleriin luodaan halutut verkot. Hurry Oy:n verkon asetukset tehtiin määritellyn suunnitelman mukaisesti (kuva 9). Sama toimenpide toteutetaan kaikille halutuille verkoille verkkosuunnitelman mukaan.

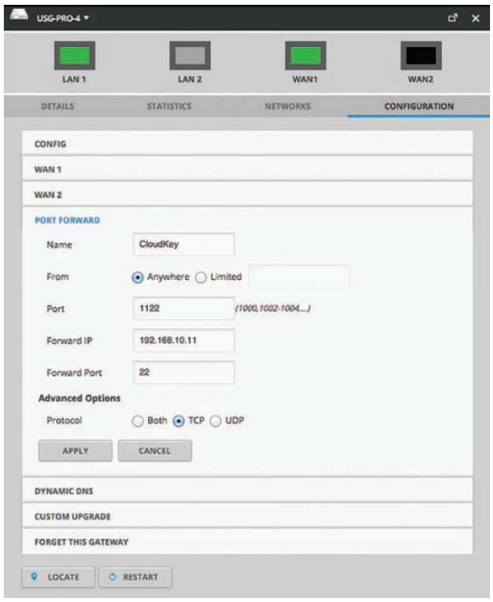


Kuva 9. Hurry Oy:n verkko

Seuraavaksi voidaan aloittaa reitittimen konfigurointi. Laitteiden konfigurointi aloitetaan hallintatyökalun devices-osiossa, josta valitaan konfiguroitava laite klikkaamalla. Reitittimen WAN 1-portti asetetaan hakemaan osoite automaattisesti palveluntarjoajalta valitsemalla configuration-välilehden WAN 1 kohdasta Using DHCP (kuva 10). Kohtaan DNS laitetaan palveluntarjoajan DNS-palvelimen osoite. WAN 2-portti konfiguroidaan samalla tavalla, mutta se asetetaan käynnistymään vain jos WAN 1 ei toimi.

Kuva 10. WAN 1-portin konfiguraatio

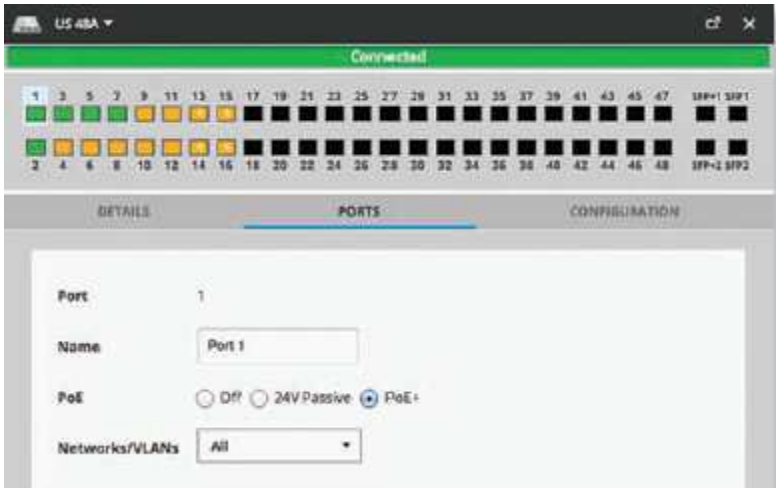
Port forwarding-välilehdellä voidaan tehdä yksinkertaisia ohjauksia tietoliikenteeseen. Jotta ulkoverkosta saadaan yhteys Cloud Key hallintatietokoneeseen, täytyy tehdä kuvan 11 mukainen sääntö. Tarkempien palomuurisääntöjen lisääminen ei vielä opinnäytetyön tekemisen hetkellä onnistu graafista käyttöliittymää käyttäen. Palomuurisäännöt täytyy tehdä komentorivillä. Jotta komentorivillä tehdyt muutokset jäisivät voimaan, täytyy luoda erillinen tiedosto, joka ladataan reitittimelle. Liitteessä 1 on ohjeet, kuinka konfigurointitiedostoa muokataan UniFi-reitittimessä.



Kuva 11. Cloud key-portin avaaminen

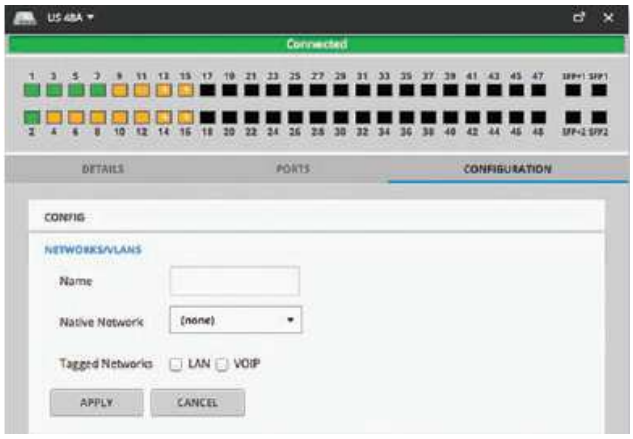
8.3 UniFi Switch

Kytkimien konfigurointi on yksinkertainen ja nopea prosessi. Huoneistokytkimellä portit 2-23 asetetaan käyttämään yrityksen verkkoa. Esimerkiksi Hurry Oy:n huoneistoon sijoitetun kytkimen portit 2-23 asetetaan käyttämään Hurry Oy:n verkkoa 192.168.10.1/24. Kytkimen porttien asetuksia vaihdetaan laitteen ports-välilehdellä valitsemalla haluttu portti. Portti 1 toimii runkoporttina, joten sen networks/VLANs-tilaksi jätetään all (kuva 12). Portit, joihin täytyy päästä myös muilla aliverkoilla ja VLAN-tunnuksilla jätetään ”All” tilaan. Portti, johon kiinnitetään tukiasema, asetetaan käyttämään ”PoE+” toimintoa.



Kuva 12. Porttien konfigurointi

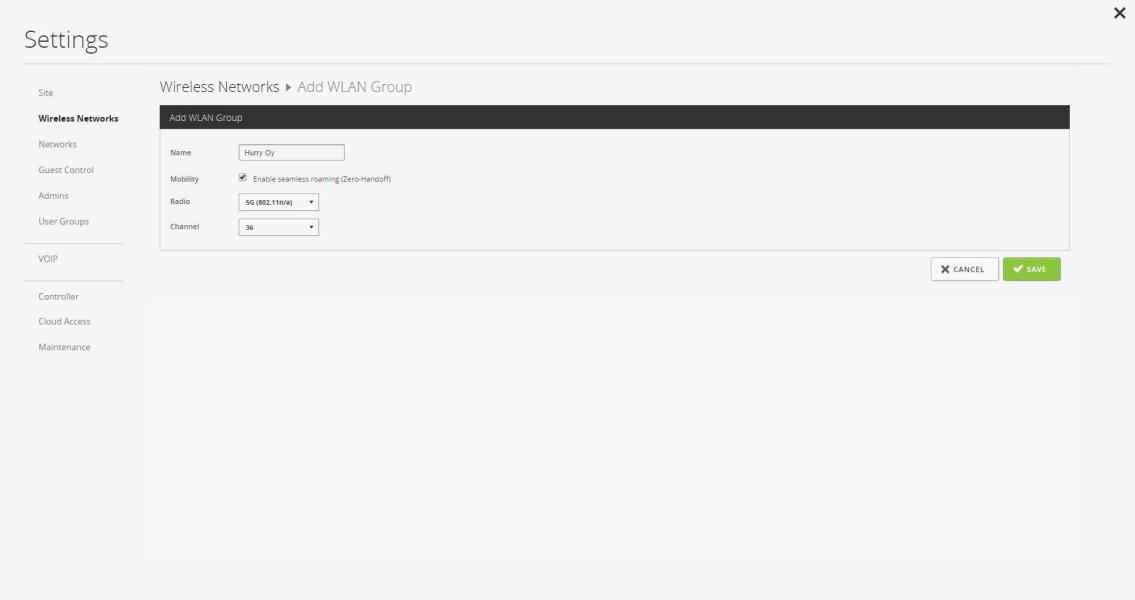
Kytkimiin asetetaan configuration-välilehdeltä networks/VLANs-osiossa native network-kohtaan oletusverkko eli VLAN 1 (kuva 13). Tagged networks kohtaan valitaan kaikki VLAN-tunnukset, jotka käyttävät kytkintä. Esimerkiksi vierasverkko ja muiden yritysten verkot, jotka haluavat käyttää tiedostopalvelinta tulee olla valittuna ”Tagged networks” kohdassa. Tämä mahdollistaa sen, että liikenne, joka on merkitty muilla VLAN-tunnuksilla voi liikkua saman kytkimen kautta häiritsemättä Hurry Oy:n verkon liikennettä. Runkokytkimellä tehdään sama toimenpide. Kytkimet tunnistavat automaattisesti mitkä portit toimivat runkokytkiminä. Portit, jotka eivät ole käytössä kytketään pois päältä.



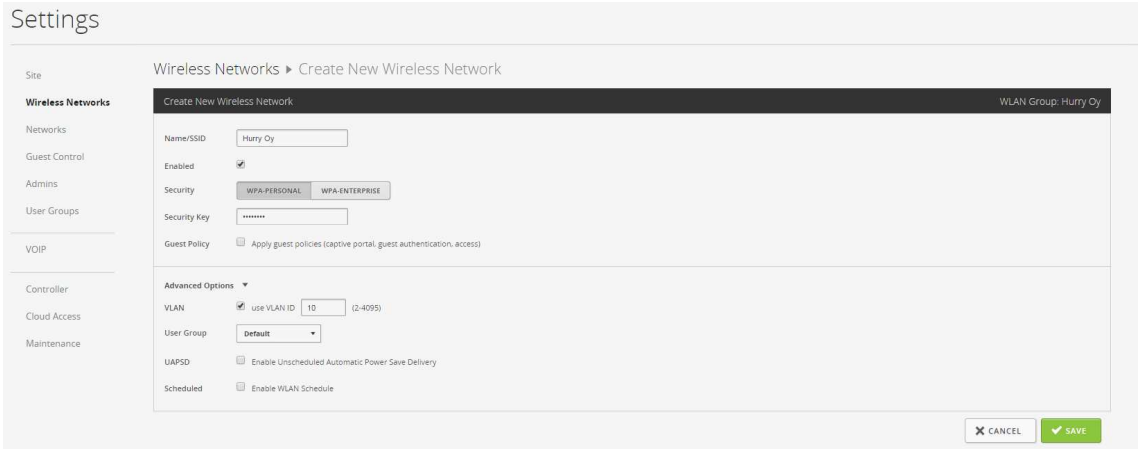
Kuva 13. Kytkimen konfigurointi

8.4 UniFi Access Point

UniFi controller-hallintatyökalun WLAN-ryhmillä voidaan tehdä malli, jota valitut tukiasemat hyödyntävät. Se tarkoittaa, että jokaista laitetta ei tarvitse konfiguroida erikseen. WLAN-ryhmät asetetaan hallintatyökalun asetuksissa wireless networks-välilehdellä painamalla plus-painiketta ikkunan yläreunassa. Kuvassa 14 on esimerkki WLAN-ryhmän luonnista. Jos halutaan luoda saumaton WLAN-verkko, niin valitaan mobility-kohdasta enable seamless roaming. Se tarkoittaa, että WLAN-verkko on katkeamaton siirryttäessä WLAN-tukiaseman läheisyydestä toiseen. Jotta katkeamaton verkko toimisi, täytyy sille asettaa sama taajuus ja kanava. Yhdelle laitteelle voidaan asettaa kaksi WLAN-ryhmää toinen 2,4GHz taajuudelle ja toinen 5GHz taajuudelle. Kun WLAN-ryhmä on luotu, siihen voidaan lisätä maksimissaan neljä verkkoa. Kuvassa 15 on tehty Hurry Oy:n langaton verkko, joka käyttää samaa VLAN-tunnusta kuin heidän muu sisäverkkonsa.

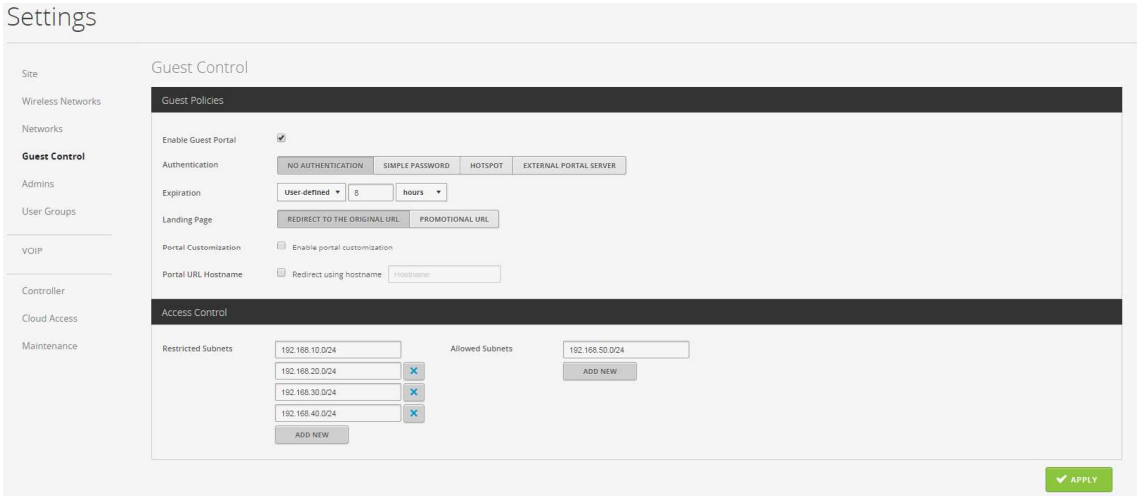


Kuva 14. WLAN-ryhmä



Kuva 15. langattoman verkon luonti

Rakennukseen tulee langaton verkko vierailijoille. Ennen kuin vierasverkko luodaan, tulee tehdä muutamia muutoksia hallintatyökalun guest control-asetuksissa. Kuvassa 16 on asetettu vierasverkko, joka ei käytä autentikointia. Se sallii yhteyden kahdeksaksi tunniksi. Access control-osiossa voidaan estää ja sallia pääsy eri aliverkkoihin. Tässä esimerkissä on kielletty liikenne kaikkiin yritysten aliverkkoihin ja sallittu vierasverkkoon. Vierasverkon luonti onnistuu samalla tavalla, kuin aikaisemmassa Hurry Oy esimerkissä, mutta VLAN-numeroksi tulee muuttaa 100 ja valita Guest policy aktiiviseksi.



Kuva 16. vierasverkon asetukset

Kun WLAN-ryhmään on luotu kaikki halutut verkot, se voidaan lisätä laitteisiin. Hallintatyökalun devices-välilehdellä valitaan haluttu WLAN-tukiasema. Avautuvan ikkunan configure-välilehdellä valitaan WLANS-osio, jonne lisätään vasta

luotu WLAN-ryhmä. Kuvassa 17 on ympyröity kohta, johon WLAN-ryhmä lisätään.

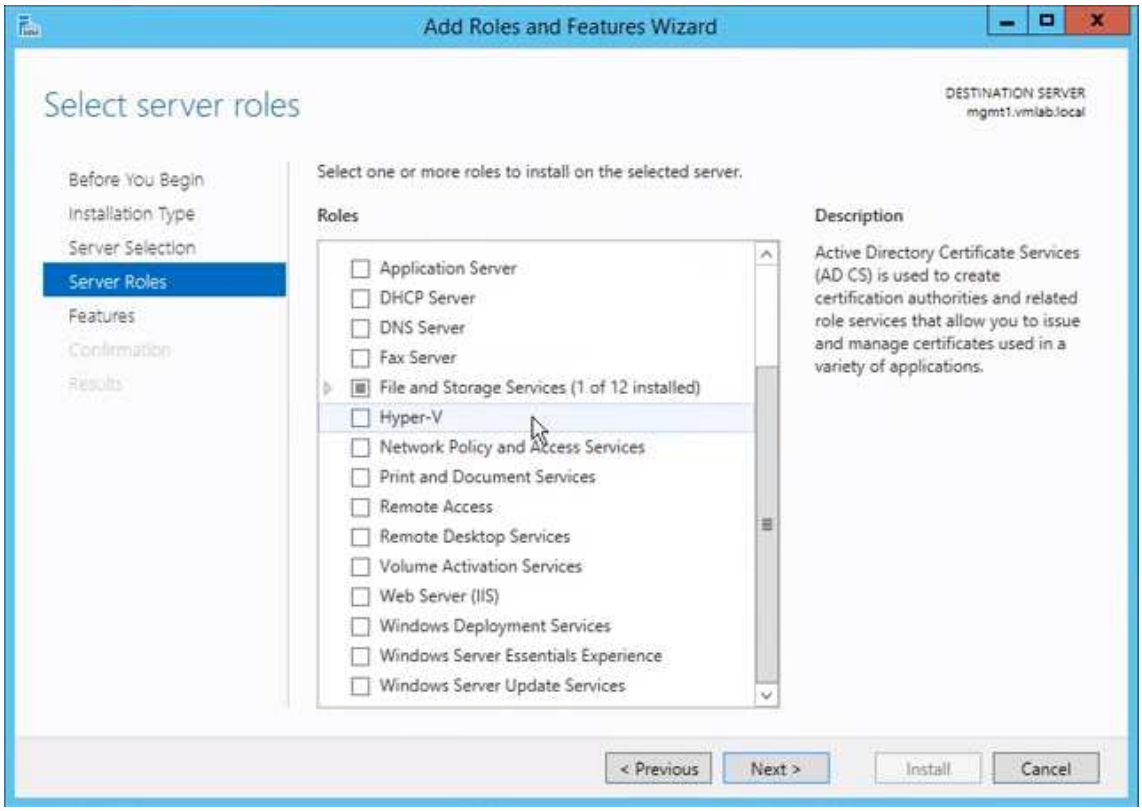
Kuva 17. WLAN-ryhmän asettaminen tukiasemalle

8.5 Tiedostopalvelin

Tiedostopalvelimen virtualisointi toteutetaan Hyper-V-virtualisointityökalulla. Hyper-V on palvelinrooli Windows-palvelimissa, joka mahdollistaa virtuaalilaitteiden luonnin ja hallinnan. Hyper-V:n asennus aloitetaan Windows Server 2012-käyttöjärjestelmällä lisäämällä se aktiiviseksi rooliksi server manager-työkalusta add roles and features-valikosta kuvan 18 mukaisesti. (Technet, 2016.) Asennuksen yhteydessä voidaan lisätä virtuaalikytkimiä ja määrittää oletusvarastot, mutta ne voidaan asettaa myös myöhemmin. Asennuksen jälkeen on hyvä käynnistää palvelin uudestaan. Hyper-V voidaan asentaa PowerShell-komennolla.

```
Install-WindowsFeature –Name Hyper-V -ComputerName “<tietokoneen nimi>” -IncludeManagementTools –Restart
```

Komento lisää ominaisuuden, jonka nimi on Hyper-V. Tietokoneen nimi kohtaan lisätään nimi, joka palvelimelle on annettu. Viimeisenä lisätään hallintatyökalut ja käynnistetään palvelin uudestaan.



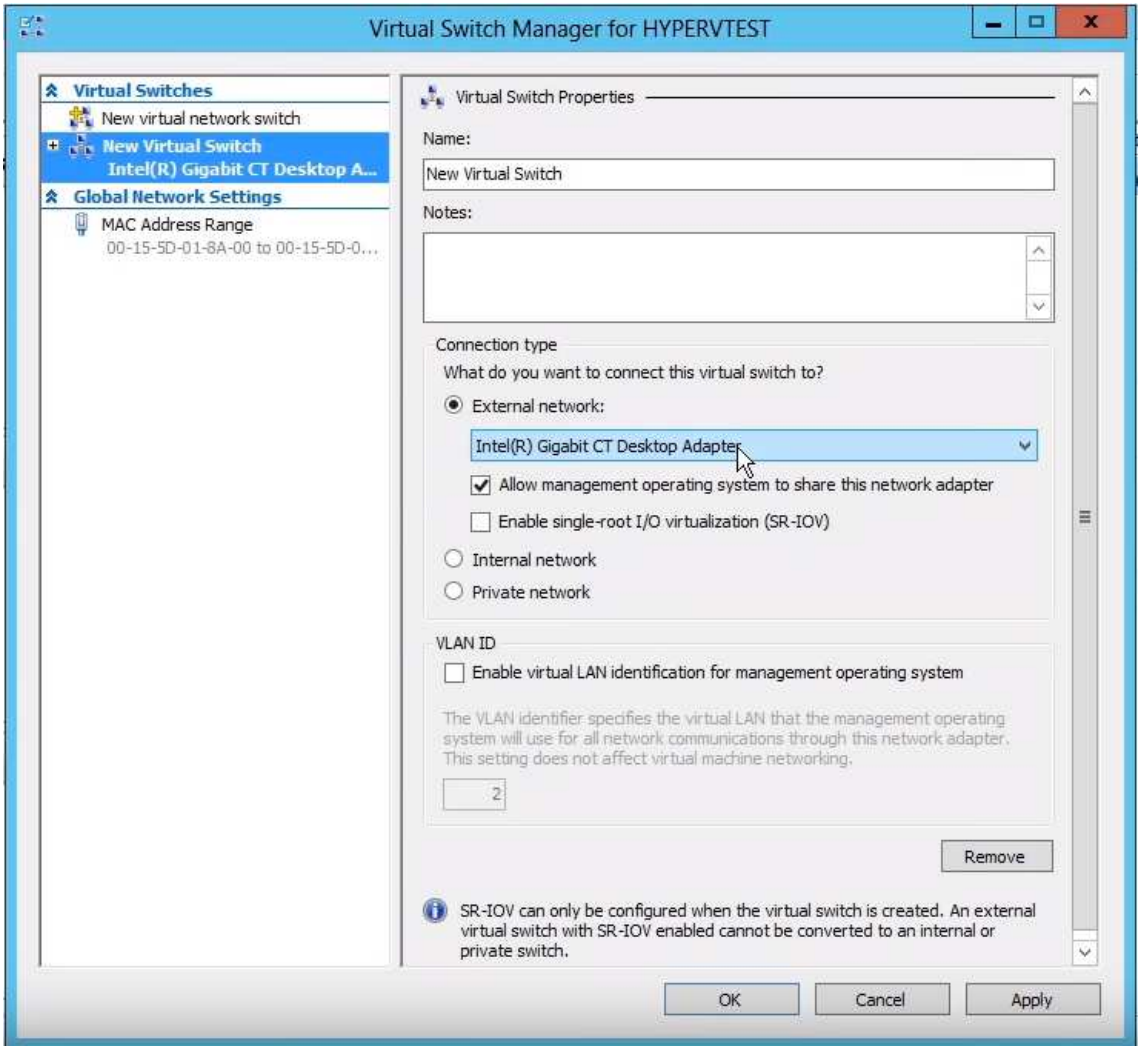
Kuva 18. Hyper-V roolin lisääminen

Virtuaalipalvelimien lisääminen tapahtuu Hyper-V-managerissa. Ennen palvelimen lisäämistä on kuitenkin luotava virtuaalikytkin. Virtuaalikytkintä luodessa on mahdollista valita kytkimen tyyppi kolmesta vaihtoehdosta. Private-vaihtoehto sallii liikenteen vain eri virtuaalipalvelimien välillä. Internal-vaihtoehto sallii liikenteen virtuaalipalvelimen ja hypervisorin välillä. Tässä tapauksessa käytetään kuitenkin external-vaihtoehtoa, mikä tarkoittaa että virtaalipalvelin on yhteydessä koko rakennuksen sisäverkkoon. Virtuaalikytkin luodaan virtual switch manager-ikkunnassa. Ensin valitaan kytkimen tyyppi, eli tässä tapauksessa external, jonka jälkeen painetaan create virtual switch. Sen jälkeen avautuu kuvan 19 mukainen ikkuna. Ikkunassa annetaan kytkimelle nimi ja valitaan verkkoadapteri, joka on yhteydessä rakennuksen sisäverkkoon. Lisäksi asetetaan VLAN-numeroksi sama virtuaalilähiverkon numero, joka on yritykselle aikaisemmin

määritetty. Hurry Oy:n tapauksessa VLAN ID kohtaan tulee 10. Virtuaalikytkin voidaan lisätä myös PowerShell-komennolla

New-VMSwitch –Name ”<kytkimen nimi tähän>” –Notes ”<kytkimen lisätiedot>” –NetAdapterName ”<verkkoadapterin nimi>” –AllowManagementOS $false

Komento lisää uuden kytkimen, jolle annetaan haluttu nimi, lisätiedot ja verkkoadapterin nimi, johon kytkin liitetään fyysisellä palvelimella.



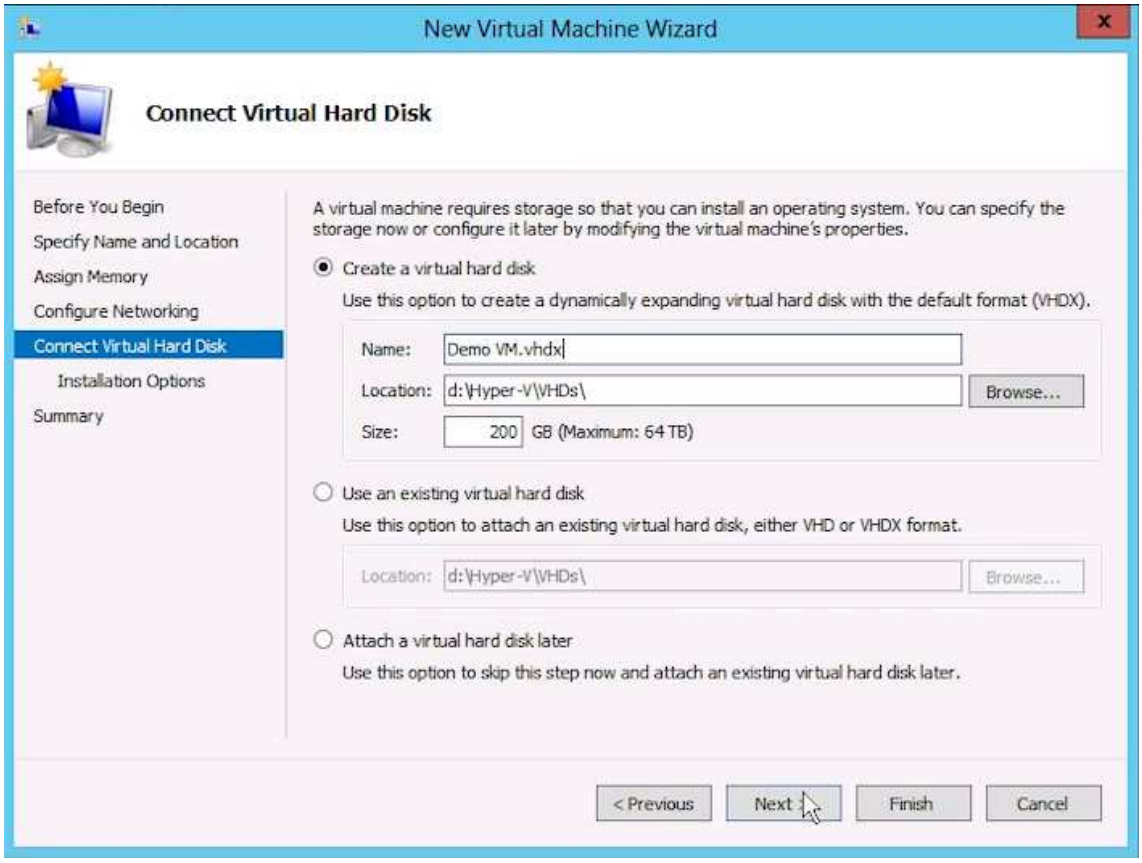
Kuva 19. Virtuaalikytkin

Kun kytkin on asennettu, voidaan luoda itse palvelin. Uusi palvelin lisätään actions-valikosta valitsemalla new virtual machine. Se avaa ohjatun asennuksen, jossa määritellään kohta kohdalta virtuaalilaitteen asetukset. Ensin määritellään palvelimelle nimi ja asennussijainti. Seuraavassa kohdassa määritetään muistin

määrä, joka laitteelle annetaan käyttöön. Tässä kohdassa kannattaa ottaa huomioon tulevan ohjelmiston järjestelmävaatimukset. Tässä tapauksessa palvelimelle tulee vain tiedostopalvelin Windows Server 2012-käyttöjärjestelmälle. Tiedostopalvelinroolille ei ole määritetty muistin vaatimuksia, mutta Windows Server 2012-käyttöjärjestelmä vaatii toimiakseen vähintään 512 MB muistia. Seuraavassa kohdassa asetetaan verkko, johon virtuaalilaite liittyy. Tässä kohdassa valitaan aikaisemmin luotu virtuaalikytkin. Seuraavaksi luodaan laitteelle virtuaalikovalevy ja sille määritetään sijainti ja koko. On myös mahdollista käyttää aikaisemmin luotua virtuaalikovalevyä. Kuvassa 20 on esimerkki uuden virtuaalikovalevyn luonnista. Käyttöjärjestelmää ei kannata asentaa tässä vaiheessa, vaan vasta myöhemmin. Asennus lopetetaan painamalla finish. Tämäkin vaihe voidaan tehdä PowerShell-komennolla.

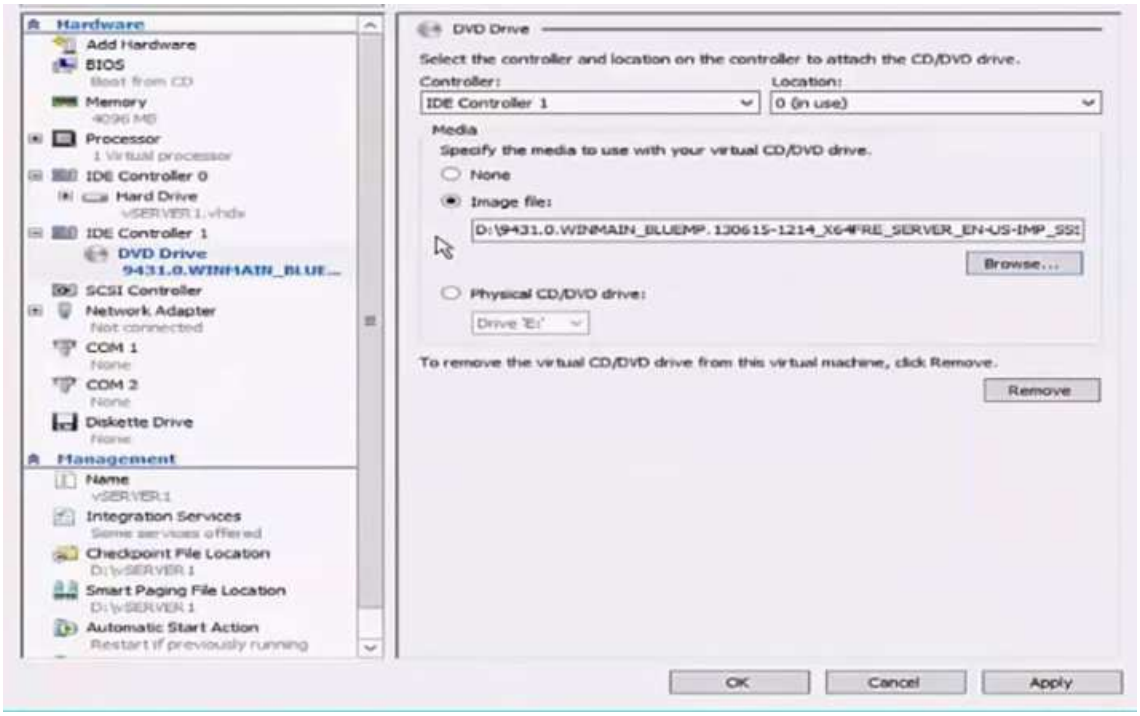
New-VM –Name “<kytkimen nimi tähän>” –MemoryStartupBytes <muistin määrä> –VHDPath d:\vhd\BaseImage.vhdx

Komento lisää uuden virtuaalilaitteen valitulla nimellä ja antaa sille halutun määrän muistia käyttöön. Komennon viimeinen osio määrittää jo valmiina olevan virtuaalikovalevyn sijainnin.



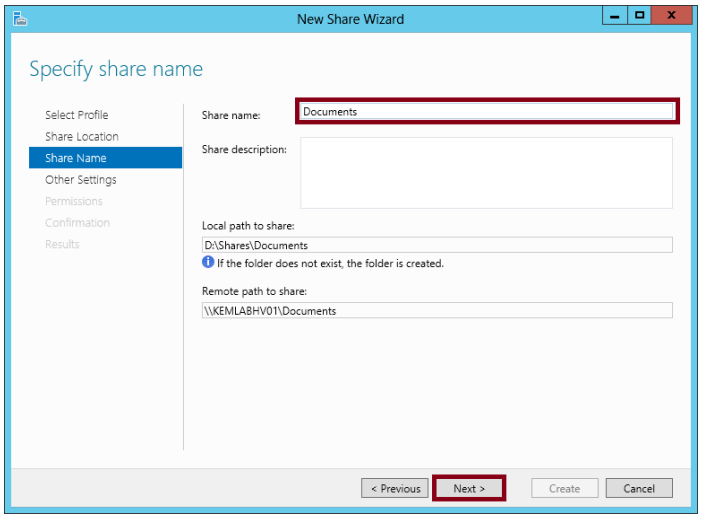
Kuva 20. Uuden virtuaalikovalevyn luonti

Seuraavaksi asennetaan virtuaalilaitteelle käyttöjärjestelmä. Se tapahtuu painamalla vasta luotua palvelinta oikealla hiiren painikkeella ja valitsemalla settings. Avautuvassa ikkunassa valitaan kuvan 21 mukaisesti palvelimen virtuaalinen dvd-asema. Siellä on mahdollista liittää käyttöjärjestelmän asennusmedia palvelimeen kahdella tavalla. Mikäli palvelimessa on levyasema, käyttöjärjestelmä voidaan asentaa cd- tai dvd-levyltä. Se tapahtuu valitsemalla kuvassa 21 alempi vaihtoehto eli Physical CD/DVD drive ja valitsemalla pudotusvalikosta oikea levyasema. Toinen vaihtoehto on käyttää levykuva asennusmediaa, joka sijaitsee palvelimella. Tässä tapauksessa valitaan Image File ja etsitään levykuvan sijainti browse-painikkeesta. Kun asennusmedia on valittu, voidaan virtuaalipalvelin avata kaksoisklikkaamalla sitä Hyper-V-managerissa. Avautuvassa ikkunassa painetaan Start ja käyttöjärjestelmän asennus alkaa.



Kuva 21. asennusmedian valinta

Kun palvelimelle on asennettu käyttöjärjestelmä ja sen alkuasetukset kuten IP-osoite, nimi ja aika, se voidaan asettaa toimimaan tiedostopalvelimena. File and Storage Services-valikossa painetaan shares, josta valitaan tasks ja new share. Avautuvassa ikkunassa valitaan ”SMB share – Quick”. Seuraavassa kohdassa valitaan vasta luotu virtuaalipalvelin ja kovalevy, jolle jako tehdään. Seuraavaksi määritetään jaon nimi, paikallinen- ja verkkosijainti kuvan 22 mukaisesti.



Kuva 22. Jaetun sijainnin nimi

Seuraavassa ikkunassa valitaan Access-Based Enumeration, Offline folder caching ja Encryption of end-to-end SMB network traffic aktiivisiksi ja painetaan next. Seuraavaksi määritetään jaetun kansion oikeudet. Customize permissions-painikkeesta voidaan määrittää yksityiskohtaiset oikeudet ryhmille ja käyttäjille. Kun oikeudet on määritetty, jako voidaan hyväksyä painamalla create. Jaetussa sijainnissa uusien kansioiden jako voidaan automatisoida PowerShell-komennoilla.

```
MD D:\Shares\Documents
```

```
New-SMBShare -Name Documents -Path D:\Shares\Documents -FolderEnumerationMode AccessBased -CachingMode Documents -EncryptData $True -FullAccess Everyone
```

Komento luo uuden jaon valitussa sijainnissa ja antaa siihen pääsyn kaikille, joille pääsy jaettuun sijaintiin määriteltiin aikaisemmin.

9 Pohdinta

Opinnäytetyön tavoitteena oli saada aikaan dokumentti, jota seuraamalla Hurry Oy pystyy toteuttamaan oman tietoverkkonsa teollisuushallin valmistuttua. Tavoitteeseen päästiin melko hyvin. Verkon suunnittelu onnistui hyvin aikaisemman tiedon ja uusien lähteiden avulla. Työ eteni pitkälti suunnitelman mukaisesti. Ensimmäisenä määrittelin tietoverkon vaatimukset, jonka jälkeen mietin kuinka ne toteutetaan. Seuraavaksi perehdyin toimeksiantajan toivomiin laitteisiin ja kehitin verkkotopologian saatujen tietojen pohjalta.

Verkon suunnittelun keskeisimpiä haasteita oli rakennukseen ja siinä toimivien yritysten epävarmuus. Rakennuksen pohjapiirros ei ollut vielä täysin valmis, eikä siinä toimivien yritysten määrä ollut tarkassa tiedossa. Sen takia oli ehdottoman tärkeää kehittää ratkaisu, joka toimisi eri muuttujista huolimatta. Yrityskohtainen ratkaisu mahdollisti verkon laajentamisen koskemaan niin montaa

yritystä kuin oli tarve. Se helpotti uusien yritysten liittymistä verkkoon, koska kaikille rakennuksessa toimiville yrityksille tarjotaan samanlainen paketti. Hallintatyökalu toteutti verkkojen hallinnan, sekä osoitteiden jaon, mikä helpottaa verkon ylläpitoa huomattavasti.

Jos tekisin opinnäytetyön uudestaan, valitsisin toiset verkkolaitteet. UniFi-reitittimet ja -kytkimet olivat tuotteena vielä uusia, joten kaikkia luvattuja ominaisuuksia ei ollut vielä hallintatyökalussa saatavilla. Lisäksi laitteiden dokumentointi oli mielestäni puutteellista, mikä hankaloitti konfigurointiohjeen kirjoittamista. Saman laitevalmistajan EdgeMax-tuotteet olisivat olleet parempi vaihtoehto, mikäli verkko olisi tarvinnut enemmän tarkempia asetuksia. Toisaalta niiden hallitseminen olisi myös hankalampaa, koska niissä ei ole automatisoitu niin paljon asetuksia.

Koska laitteita ei ollut vielä hankittu, konfiguraatioiden toteuttaminen opinnäytetyössä täytyi tehdä virallisia laitevalmistajien oppaita seuraten. Hankaluuksia esiintyi etenkin reitittimen kanssa, joka lupasi kehittyneet palomuuriominaisuudet. Graafisesta käyttöliittymästä löytyi opinnäytetyön tekohetkellä ainoastaan yksinkertainen porttiohjaustyökalu. Kehittyneemmät palomuurisäännöt täytyi tehdä kankealla komentorivillä. Tukiasemat olivat helpompi ohjeistaa. Niihin löytyi paremmin dokumentaatiota, sekä käyttäjäkokemuksia internetistä. UniFi onkin parhaiten tunnettu WLAN-tukiasemistaan. Reitittimet ovat uudempi lisäys valikoimaan.

Mielestäni opinnäytetyö oli hyvin mielenkiintoinen ja opetti paljon uutta. Työ oli helppo aloittaa aikaisemman tiedon pohjalta, mutta hankaloitui edetessään. Työtä voidaan jatkossa laajentaa koskemaan erilaisia verkkoratkaisuja ja täydentää laitteisto-osio vastaamaan vaatimuksia paremmin.

Lähteet

Ciccarelli, P. Faulkner, C. 2006. Networking Foundations: Technology Fundamentals for IT Success. Hoboken, New Jersey: Sybex.

Cisco. 2014. Routing between VLANs Overview http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfvl.html. 5.3.2016

Danielyan, Edgar. 2001. IEEE 802.11 - The Internet Protocol Journal - Volume 5, Number 1. http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-21/ieee.html. 5.3.2016

Hurry Oy. 2016. http://hurry.fi/. 1.4.2016

McCabe, J. 2010. Network Analysis, Architecture and Design. Burlington, Massachusetts: Morgan Kaufmann.

Portnoy, M. 2012. Essentials: Virtualization Essentials. Hoboken, New Jersey: Sybex.

Technet. 2016. Hyper-V. Microsoft. https://technet.microsoft.com/en-us/library/mt169373.aspx. 3.4.2016

Ubiquiti. 2016. UniFi - How to further customize USG configuration with config.gateway.json. https://help.ubnt.com/hc/en-us/articles/215458888-UniFi-How-to-further-customize-USG-configuration-with-config-gateway-json. 30.4.2016

UniFi AP. 2015. UniFi AC Aps Datasheet. Ubiquiti https://dl.ubnt.com/datasheets/unifi/UniFi_AC_APs_DS.pdf. 15.3.2016

UniFi Cloud Key. 2015. UniFi Cloud Key Datasheet. Ubiquiti https://dl.ubnt.com/datasheets/unifi/UniFi_Cloud_Key_DS.pdf. 10.4.2016

UniFi Controller. 2016. UniFi Controller v4 User Guide. Ubiquiti https://dl.ubnt.com/guides/UniFi/UniFi_Controller_V4_UG.pdf. 2.5.2016

Unifi SG. 2014. UniFi Security Gateway Datasheet. https://dl.ubnt.com/datasheets/unifi/UniFi_Security_Gateway_DS.pdf. 13.3.2016.

UniFi Switch. 2014. UniFi Switch Datasheet. Ubiquiti https://dl.ubnt.com/datasheets/unifi/UniFi_Switch_DS.pdf. 13.3.2016. 13.3.2016

Wikipedia. 2016. Wikipedia PoE. https://fi.wikipedia.org/wiki/Power_over_Ethernet. 13.4.2016

Wilkins, S. 2011. Cisco's PPDIOO Network Cycle. Cisco Press. http://www.ciscopress.com/articles/article.asp?p=1697888. 12.2.2016

Reitittimen lisäasetukset

Config.gateway.json-tiedostoa käytetään haastavimmissa reitittimen konfiguraatioissa. Tiedosto mahdollistaa konfiguraatioiden säilymisen reitittimellä. Config.gateway.json-tiedostoon kannattaa tehdä vain muutoksia, joita ei ole mahdollista tehdä graafista käyttöliittymää käyttäen. Tiedoston formaatissa on oltava tarkkana, sillä väärä formaatti voi aloittaa silmukan, joka käynnistää laitteet aina uudelleen. Tiedosto ei ole laitteella oletuksena, vaan se täytyy luoda sinne. Tiedosto luodaan sijaintiin [UniFi base]/data/sites/the_site. (Ubiquiti, 2016.)

Jokaisella UniFi controllerin luomalla sijainnilla on oma tunnus. Tässä esimerkissä se on ceb1m27d. Tunnuksen voin löytää laitteen verkko-osoitteesta https://127.0.0.1:8443/manage/s/ceb1m27d/dashboard. Kansio nimeltä ceb1m27d luodaan [UniFi base]/data/sites/the_site hakemistoon ja config.gateway.json-tiedosto. (Ubiquiti, 2016.)

Ennen muutoksia, kannattaa tarkistaa, että nykyisessä config.boot tiedostossa ei ole sääntöjä samalla numerolla. Sen voi tarkistaa esimerkiksi ottamalla SSH-yhteys reitittimeen ja antamalla alla olevan komennon. (Ubiquiti, 2016.)

cat /config/config.boot.

Tässä esimerkissä luodaan DNAT-sääntö DNS:lle. Konfiguratiot tehdään EdgeOS formaattia käyttäen.

```
configure
set service nat rule 1 type destination
set service nat rule 1 inbound-interface eth0
set service nat rule 1 protocol tcp_udp
set service nat rule 1 source port 53
set service nat rule 1 inside-address address 10.0.0.1
set service nat rule 1 inside-address port 53
commit;save;exit
```

Seuraavaksi voidaan lisätä konfiguraatio config.gateway.json-tiedostoon. Tässä konfiguraatiossa ei ole mitään muut, kuin DNAT-sääntö, joten alla oleva konfiguraatio tulisi kokonaisuudessaan config.gateway.json-tiedostoon. (Ubiquiti, 2016.)

```
{
    "service": {
        "nat": {
            "rule": {
                "1": {
                    "destination": {
                        "port": "53"
                    },
                    "inbound-interface": "eth0",
                    "inside-address": {
                        "address": "10.0.0.1",
                        "port": "53"
                    },
```

Reitittimen lisäasetukset

```
                    "protocol": "tcp_udp",
                    "type": "destination"
                }
            }
        }
    }
}
```