Olli-Juhani Kaukoranta

Verkkolevypalvelimen asennus ja käyttöönotto

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Automaatiotekniikka

Insinöörityö

11.8.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Olli-Juhani Kaukoranta Verkkolevypalvelimen asennus ja käyttöönotto 39 sivua 11.8.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Automaatiotekniikka
Suuntautumisvaihtoehto	Kappaletavara-automaatio
Ohjaaja(t)	Lehtori, Jaana Wuorila-Stenberg Toimitusjohtaja, Pertti Kaukoranta

Nykypäivänä viimeisimmän tiedon saaminen nopeasti on elinehto yrityksen kannattavuudelle ja tehokkaalle toiminnalle, erityisesti yrityksissä, joissa useammat työntekijät muokkaavat yhteisiä tiedostoja. Tiedostojen version hallinta sekä keskitetty tiedostosijainti ovat tässä avainasemassa.

Tämän insinöörityön tarkoituksena oli luoda yhteinen verkkotallennusratkaisu Talosyke Oy:lle. Työn alkaessa yrityksellä ei ollut käytössä minkäänlaista yhteistä tallennusratkaisua, mikä johti siihen, että työntekijöillä oli yhteisistä tiedostoista eriävät versiot omilla koneillaan.

Insinöörityössä tutkittiin sekä vertailtiin erilaisia palvelinlaitteistoja ja ratkaisuja, jotka sopisivat yritykselle.

Tehdyn tutkimustyön perusteella kohdeyrityksen tarpeisiin hankittiin soveltuva palvelinlaitteisto, jonka perustana oli Synology-verkkolevypalvelin. Palvelimeen hankittiin erikseen kiintolevyt sekä yksi ulkoinen kiintolevy paikallista varmuuskopiointia varten. Lisäksi palvelimen yhteyteen hankittiin uusi nopeampi kytkin sekä WLAN-reititin.

Avainsanat	synology, palvelin, kytkin, VPN

Author(s) Title Number of Pages Date	Olli-Juhani Kaukoranta Installation and commissioning of the Network-attached storage 39 pages 11 August 2015
Degree	Bachelor of Engineering (AMK)
Degree Programme	Automation Engineering (AMK)
Specialisation option	Manufacturing Automation
Instructor(s)	Jaana Wuorila-Stenberg, Lecturer Pertti Kaukoranta, CEO

Nowadays obtaining the latest information rapidly is the lifeblood of those companies' profitability and effective operations where a lot of workers are editing the same shared files. File version management, and centralized file location are the key here.

The purpose of this thesis was to create a shared network storage solution for Talosyke Oy. At the beginning of this thesis work the company did not have any kind of common storage solution, which led workers to have different version of the common files on their own computers.

In this thesis we examined and compared a variety of server hardware and solutions that could fit for the company.

Based on the research for the target company a server was obtained, which was based on a Synology NAS-server. The hard drives for the server and one external hard drive for local backup was purchased separately from the server. In addition with the server new faster switch and wireless LAN-router was also obtained.

Keywords	synology, server, switch, VPN

Sisällys

LYHENTEET

ADSL2+	Asymmetric Digital Subscriber Line. Verkkokytkintekniikan viimeisin versio, joka mahdollistaa jopa 24 Mb/s nopeuden yhdessä puhelinparissa.
AES	Advanced Encryption Standard. Lohkosalausmenetelmä, jota käytetään tietotekniikassa.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jota voidaan käyttää IP-osoitteen, nimipalvelimen ja oletusyhteyskäytävän jakamiseen lähiverkkoon kytketyille verkkolaitteille.
DNS	Domain Name System. Nimipalvelujärjestelmä, jonka avulla Internet-verkkotunnukset muutetaan IP-osoitteiksi.
DSM	Disk Station Manager. Synology palvelimien käyttämä lyhenne käyttöjärjestelmästään.
ECC	Error Correcting Code. Keskusmuistin virheenkorjauskoodi, jolla virhetilanteet voidaan havaita ja korjata automaattisesti.
HDD	Hard Disk Drive. Tietokoneeseen kiinteästi asennettu massamuisti, jossa tieto säilytetään yhden tai useamman pyörivän metalli- tai lasikiekon pinnalla olevaan magneettiseen materiaaliin.
Hz	Hertsi. Taajuuden yksikkö.
IPv4	Internet Protocol. Neljäs versio Internet-protokollasta.
LVI	Lyhenne sanoista. Lämpö. Vesi. Ilma.
OSI	Open Systems Interconnection Reference Model. Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
RAID	Redundant Array of Independent Disks. Tekniikka, jolla tietokoneiden ja palvelimien vikasietoisuutta ja/tai nopeutta kasvatetaan käyttämällä useita erillisiä kiintolevyjä, jotka yhdistetään yhdeksi loogiseksi levyksi.
S.M.A.R.T	Self-Monitoring, Analysis and Reporting Technology. Tietokoneen kiintolevyjen kunnon sekä suorituskyvyn seurantajärjestelmä.
SSD	Solid State Drive. Tietokoneen massamuisti, missä ei ole liikkuvia osia ja jossa tieto säilyy laitteen ollessa virrattomana.
SSID	Service set Identifier. Langattoman lähiverkon verkkotunnus.
SSL	Secure Socket Layer. Salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.

TCP/IP	Transmission Control Protocol / Internet Protocol. Protokollaa käytetään Internet-liikennöinnissä, joka on tietoverkkoprotokollien yhdistelmä.
TKIP	Temporal Key Integrity Protocol. Langattoman lähiverkon tietoturvaprotokolla, mikä huolehtii yhteyksien salaamisesta ja turvaamisesta.
TLS	Transport Layer Security. Salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
USB	Universal Serial Bus. Sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi tietokoneeseen.
VPN	Virtual Private Network. Virtuaalinen erillisverkko, jolla kaksi tai useampi yrityksen verkko voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.
WEP	Wired Equivalent Privacy. IEEE:n 802.11-standardin ensimmäinen työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä.
WLAN	Wireless Local Area Network. Langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.
WPA	Wi-Fi Protected Access. WLAN-verkoissa käytettävä salausprotokolla. WPA kehitettiin siirtymävaiheen protokollaksi ennen WPA2:a.
WWW	World Wide Web. Internet-verkossa toimiva hajautettu hypertekstijärjestelmä.

1 Johdanto

Insinöörityön tavoitteena on suunnitella Talosyke Oy:lle verkkolevypalvelin ratkaisu, mikä mahdollistaa yrityksen tiedostojen tallentamisen keskitettyyn kohteeseen. Nykyisin yrityksen työntekijät tallentavat tiedostot henkilökohtaisille tietokoneilleen vailla version hallintaa sekä keskitettyä kohdetta.

Tavoitteen mukainen verkkolevypalvelin helpottaa, yksinkertaistaa ja tehostaa yrityksen tiedostojen keskitettyä säilyttämistä, käyttämistä ja hallintaa. Verkkolevypalvelimen kolmannen osapuolen ohjelmistot tarjoavat lisäksi laajennusmahdollisuuden muun muassa kameravalvonnan lisäämisen sekä oman sähköpostipalvelimen.

2 Insinöörityön kohdeyritys

Talosyke Oy on vuonna 2009 perustettu kiinteistöhuoltoyritys, joka toimii pääosin Uudenmaan alueella. Yritys tekee kaiken kattavaa kiinteistönhuoltoa, joka käsittää LVI- ja siivouspalvelut, maa- ja lumiurakoinnin sekä konevuokraukset. Yrityksen liikevaihto on noin 4,2 milj.€ vuodessa. Yritys työllistää tällä hetkellä 60 henkilöä. Yrityksellä on useita toimipisteitä Uudellamaalla. Päätoimipaikka sijaitsee Koivuhaassa Vantaalla. Yritys on muuttamassa uusiin tiloihin vuonna 2016.

Yrityksellä on noin 500 asiakkuutta, joista merkittävimpiä ovat Paulig ja Kamppikeskus Oy. Yritys tekee Pauligin tehtaalla Vuosaaressa muun muassa sisä- ja ulkotöitä sekä muuta kiinteistöhuoltoon liittyvää toimintaa. Kamppikeskus Oy:lle yritys tekee bussilaiturien kunnossapitoa, rahtilaiturin jätehuoltoa, lajittelua sekä puhtaanapitoa.

2.1 Insinöörityön lähtökohdat

Yrityksen toiminnan yhteydessä syntyy paljon erilaisia tiedostoja, joiden tallentaminen vaatii tilaa. Tiedostoja syntyy pääosin yrityksen normaalista liiketoiminnasta, kuten kirjanpidosta, palkkahallinnasta, pankkiohjelmista, huoltokohteiden tiedostoista, tarjouskyselyistä ja -pyynnöistä, henkilöstöhallinnasta ja huoltokalustosta. Tiedostot halutaan säilöä keskitetyssä paikassa, missä ne ovat helposti kaikkien autentikoitujen henkilöiden saatavilla.

Nykyinen toteutus

Tällä hetkellä työntekijöillä on tiedostot henkilökohtaisilla tietokoneillaan, eikä tiedostojen versiohallintaa ole lainkaan, minkä takia työntekijät saattavat työstää samaa tiedostoa muiden tietämättä. Tämä hidastaa työn edistymistä sekä kasvattaa työn määrää tarpeettomasti.

Työntekijöiden tietokoneita ei varmuuskopioida tällä hetkellä lainkaan, mikä omalta osaltaan voi aiheuttaa asiakirjojen tahattoman häviämisen ilman mahdollisuutta tiedoston palautukseen.

Tietokoneiden oletetun iän puitteissa myös riski koneen vaurioitumiselle kasvaa päivä päivältä suuremmaksi, mikä lisää paineita hankkia keskitetty tallennusratkaisu. Tällöin oman tietokoneen vaurioitumien ei välttämättä aiheuta kaikkien tiedostojen häviämistä.

2.2 Vaatimukset ja tavoitteet

Palvelimelle tullaan tallentamaan kaikki yrityksen yhteiset sähköisessä muodossa olevat asiakirjat. Tämä asettaa palvelimelle tietyt ehdot. Palvelimen tulee olla vikasietoinen, toimintavarma sekä tietoturvallinen.

Laitteistoksi valitaan sellainen kokonaisuus, jonka tehokkuus ja ominaisuudet riittävät pitkälle tulevaisuuteen, lisätoimintoja ja muokattavuutta unohtamatta. Kaikkia laitteen ominaisuuksia ei tulla tämän opinnäytetyön aikana hyödyntämään rajoitetun ajan vuoksi, mutta tässä vaiheessa voidaan jo todeta, mitä ominaisuuksia tullaan ajan saatossa tarvitsemaan.

Palvelimen suunnittelussa tulee miettiä vikaherkimpien osien, kuten kiintolevyjen, mahdollista rikkoutumista. Mahdollisiin vahinkoihin tulee varautua siten, että yhden kiintolevyn rikkoutuminen ei aiheuta tietojen häviämistä, eikä palvelimen toimintakyvyn menettämistä.

Palvelimelle tulee varata riittävästi tallennuskapasiteettia tulevia tiedostoja varten, sekä vanhojen tiedostojen säilyttämistä varten. Tiedostot tullaan varmuuskopioimaan palvelimelta paikalliseen USB-kovalevyyn sekä verkon yli toiseen palvelimeen. Varmuuskopiointi tulee tapahtumaan automaattisesti säännöllisin väliajoin.

Palvelinlaitteiston käyttöjärjestelmän tulee olla selkeä ja sellaisten henkilöiden omaksuttavissa, joilla ei ole aikaisempaa kokemusta palvelimista tai niiden käyttöjärjestelmistä. Laitteistolla tulee kyetä määrittämään käyttäjätilien oikeuksia, jolloin käyttäjien pääsyä palvelimen tiedostoihin voidaan rajoittaa.

Asiakirjojen tietoturvallisuudesta huolehditaan palomuurin, päivitysten ja virustorjunnan avulla. Käyttöjärjestelmän ja virustorjunnan päivitys tulee tapahtumaan automaattisesti taustalla ilman erillistä ylläpitoa.

Laitteiston tulee mahdollistaa etäkäyttö, joka asettaa tietyt vaatimukset laitteen tietoturvalle. Etäkäyttöyhteys tullaan määrittämään salatuksi VPN-tunnelin avulla, jolloin saavutetaan haluttu tietoturvataso.

Tulevaisuutta ajatellen laitteen lisäominaisuudet esittävät isoa roolia laitteen hankinnassa, muun muassa seuraavia lisäominaisuuksia halutaan hyödyntää:

- kameravalvonta
- tulostinpalvelin
- sähköpostipalvelin.

Palvelinlaitteiston ohessa myös kytkin halutaan päivittää. Nykyisen kytkimen kapasiteetti ei tule tarjoamaan riittävää nopeutta palvelimen ja tietokoneiden välistä tiedonsiirtoa ajatellen. Toimistotilaan halutaan myös luoda langaton verkko kannettavia mobiililaitteita varten.

3 Laitteisto

Palvelinjärjestelmän laitteisto on suunniteltu siten, että sen kaikki komponentit ovat aina käytössä vuorokauden ajasta riippumatta. Laitteiston ylläpitäminen on tehty mahdollisimman helpoksi ja yksinkertaiseksi. Ylläpitoa on helpotettu siten, että verkkolevypalvelin lähettää sähköpostia järjestelmävalvojalle, mikäli järjestelmään tulee vika. Rikkoutunut kiintolevy, tallennustilan loppuminen sekä varmuuskopioinnin epäonnistuminen ovat muun muassa vikoja, joista tieto tulee sähköpostitse. Näin järjestelmään tulleisiin virkoihin voidaan reagoida mahdollisimman nopeasti.

3.1 Kytkin

Jotta saadaan muodostettua yhtenäinen OSI-viitemallin toisella kerroksella (siirtokerros) toimiva verkko, tarvitaan kytkin yhdistämään Ethernet tai muita pakettikytkennäisiä verkon osia toisiinsa. OSI-viitemalli on kuvassa 1.

Paketin saapuessa kytkimelle se tallentaa lähettäjän MAC-osoitteen sekä portin kytkimen numeron osoitetauluun. Tämän jälkeen kytkin vertaa paketissa olevaa vastaanottajan MAC-osoitetta osoitetauluun ja lähettää paketin eteenpäin oikeaan porttiin. Jos vastaanottajan osoitetta ei löydy taulusta tai kyseessä on yleis- tai ryhmälähetys kytkin lähettää paketin kaikkiin portteihin. Jos vastaanottajan portti on sama kuin lähettäjän portti, paketti hävitetään.

Kytkimien ansiosta on mahdollista käyttää full-duplex-liikennöintiä. Jokaisella portilla on oma kaistansa, jolloin 8-porttinen 10/100 Mbit/s-kytkin pystyy teoriassa välittämään jopa 1,6 Gbit/s. Yleensä rajoittavaksi tekijäksi muodostuu kuitenkin kytkimen taustaväylän nopeus. [1.]

Kuva 1. OSI-viitemalli [2.]

Kytkimen tuli olla varmatoiminen ja 19 tuuman räkkiin sopiva. Kytkimelle ei asetettu erityisiä vaatimuksia verkon yksinkertaisuuden takia. Pieni ja helppokäyttöinen peruskytkin ilman hallintaominaisuuksia oli riittävä valinta tähän tarkoitukseen. Työssä käytetty kytkin on kuvassa 2.

Kuva 2. HP 1410-16G-kytkin.

Työtä aloitettaessa vanhan kytkimen nopeus oli 10/100Mbps, jonka arveltiin olevan riittämätön nopeus kasvavalle yritykselle. Tästä syystä kytkimen nopeutta haluttiin painottaa uutta kytkintä hankittaessa. Uuden kytkimen nopeus on 1Gbps, joka takaa verkolle riittävän tiedonsiirtonopeuden. Kytkimessä on 16 porttia, joista kaikki tarjoavat 1Gbps nopeuden. Kytkimen kytkentäkapasiteetti on 32Gb/s.

> Kehittyneemmillä lähiverkon kytkimillä verkko voidaan ohjelmallisesti jakaa osiin, jotka on erotettu muista verkon osista kokonaan virtuaalisiksi työryhmiksi. Tällöin työasemat näkevät verkossa vain samaan virtuaalityöryhmään kuuluvat laitteet (työasemat, palvelimet). Virtuaalinen verkon osiin jakaminen, josta käytetään nimitystä VLAN, se tuo lisää ominaisuuksia verkon suunnitteluun, hallintaan ja tietoturvallisuuteen. [3, s.237].

3.2 Modeemi

Tässä työssä käytimme jo olemassa olevaa ZyXEL P-661-HNU-Fx-modeemia. Modeemi on kuvassa 3. Modeemi on 4-porttinen ADSL2+-modeemi, mikä sisältää palomuurin sekä WLAN-ominaisuuden. Koska modeemi on ADSL2+ tyyppinen modeemi, sen teoreettinen tiedonsiirtonopeus on 24MB/s, mikä on yritykselle todella alhainen nopeus. Kaikki uudet laitteet hankittiin uutta toimipaikkaa silmälläpitäen, joten niiden tiedonsiirtokapasiteettia ei vielä näillä nopeuksilla päästä hyödyntämään.

Kuva 3. ZyXEL P-661-HNU-Fx-modeemi.

Koska yritys on muuttamassa vuoden 2016 aikana uusiin toimitiloihin, ei uuteen modeemiin haluta investoida vielä tässä vaiheessa. Talon runkoverkon ollessa vanha ei nopeampaa internet yhteyttä ole saatavilla. Kuituyhteyden tuominen tiloihin olisi turhaa tulevan muuton takia sekä erittäin kallista, joten siihen ei haluta ryhtyä.

3.3 Palvelintyypit

Räkkipalvelin

Räkkipalvelimet asennetaan joko laitekaappeihin tai -telineisiin, joiden mitat ovat standardoituja. Räkkipalvelimien komponentit on sijoitettu litteän malliseen koteloon, jonka mitat ovat myös standardit. Laitekaappi koostuu useista asennus kerroksista, joihin räkkipalvelin kiinnitetään ruuvein. Räkkipalvelin on kuvassa 4.

Yhteen laitekaappiin voidaan sijoittaa useampi räkkipalvelin päällekkäin. Näin saadaan tehostettua verkon resursseja sekä minimoitua tilantarve. Myös palvelimien kaapelointi voidaan hoitaa järkevämmin. Useat päällekkäin asetetut räkkipalvelimet lämpiävät käytössä, siksi niiden jäähdytyksestä tulee huolehtia mahdollisimman tehokkaasti. Räkkeihin voidaan sijoittaa myös muuta palvelinlaitteistoa, mikä voi tehdä räkkipalvelimesta varteenotettavan vaihtoehdon. [4.]

Kuva 4. Hp ProLiant DL380p-räkkipalvelin. [5.]

Tornipalvelin

Toisin kuin räkkipalvelimet ovat tornipalvelimet pöytäkoneen kokoisia työasemia, joten niiden komponentit ovat helposti vaihdettavissa. Laajennettavuus on myös tornipalvelimien hyvä puoli. Tornipalvelin voidaan sijoittaa käytännössä minne vain, tosin yleensä niitä säilytetään lattialla. Tornipalvelin on kuvassa 5. Tornipalvelimia käytetään usein pienemmissä yrityksissä, koska ne on helppo asentaa ja ne eivät tarvitse erillistä palvelinhuonetta.[6.]

Kuva 5. HP ProLiant ML350 G5-tornipalvelin. [7.]

Blade-palvelin

Blade-palvelin on standardikokoiseen laiteräkkiin asennettava palvelinjärjestelmä. Sillä on erillinen runko, mihin palvelinkortit asennetaan. Blade-palvelimen hyvät puolet ovat sen pieni tilan tarve sekä vähäinen energian kulutus. Tämä on toteutettu siten, että palvelinkorttien hallinta, virransyöttö, verkkotoiminta ja jäähdytys ovat keskitettynä erilliseen runkoon. Näin ollen jokainen palvelinkortti ei vaadi omaa virtalähdettä.[8,9.]. Blade-palvelin on kuvassa 6.

Kuva 6. HP BladeSystem c7000. [10.]

Palvelimeksi haluttiin valita laitteisto, joka ei veisi tilaa ja jonka hankintakustannukset olisivat matalat. Helppokäyttöisyys ja ylläpito olivat myös avainasemassa palvelinta hankittaessa. Palvelimen hankintahetkellä yrityksellä ei ollut henkilöä, jonka toimenkuvaan olisi kuulunut verkon sekä it-laitteiston ylläpito. Tästä johtuen parhaimmaksi nähtiin hankkia verkkolevypalvelin, jonka ylläpitäminen sekä käyttäminen tulee olemaan helpompaa kuin varsinaisen palvelimen. Verkkolevypalvelin on kuvassa 7.

Kuva 7. Synology DS-412+-verkkolevypalvelin.

Verkkolevypalvelimen ominaisuudet ovat laajennettavuudeltaan heikompia verrattuna varsinaisiin palvelimiin, sillä pääsääntöisesti sen komponentteja ei pysty vaihtamaan. Hankittuun verkkolevypalvelimeen voidaan vaihtaa ainoastaan keskusmuisti.

3.3.1 Palvelimen komponentit

Palvelimien komponentit vastaavat hyvin paljon tavallisen tietokoneen komponentteja. Eroavaisuuksia kuitenkin on. Palvelimien komponentit ovat yleensä laadultaan parempia ja kalliimpia kuin tavallisen tietokoneen komponentit. Palvelimen komponentit ovat luotettavuudeltaan hyviä, koska ne ovat valmistettu jatkuvaan käyttöön. Valmistajan tuki komponenteille on yleensä myös kattavampi ja pidempi tavallisen tietokoneen komponentteihin nähden.

Emolevy

Koska palvelimien emolevyiltä vaaditaan paljon luotettavuutta sekä suorituskykyä on emolevyissä useimmiten paikka kahdelle, jossain jopa useammalle prosessorille, jotka toimivat rinnakkain. Emolevyn suoritinkannat ovat useimmiten sellaisia, että niihin sopivat erityisesti palvelintarkoitukseen soveltuvat prosessorit. Palvelimilla suoritetaan usein paljon rinnakkaisia ohjelmia, täten emolevyltä löytyy useimmiten myös enemmän keskusmuistipaikkoja kuin tavallisesta emolevystä.

Prosessori

Palvelimisissa olevat suorittimet ovat moniytimisiä kuten tavallisissa nykytietokoneissa. Tällä saavutetaan tehokas samanaikainen ohjelmien suorittaminen. Palvelinkäytössä tämä on erittäin tärkeää. Usein palvelimien prosessoreissa onkin enemmän ytimiä, kuin tavallisessa tietokoneissa. Uusimmissa on jopa 18 ydintä. Palvelinsuorittimet tukevat usein virheenkorjaavaa muistia.

Muisti

Palvelimessa käytettävä keskusmuisti on pääasiallisesti samankaltainen kuin tavallisessa tietokoneessa, mutta sille tarkoitetut muistipiirit sisältävät ECC-virheenkorjauspiirin. Tämä tekee muistipiireistä hieman hitaampia verrattuna tavallisen tietokoneen muistiin, mutta tällä toiminnolla on mahdollista korjata virheitä, jotka kulkevat muistin läpi. Palvelimissa muistipaikkojen määrä on yleensä moninkertainen tavalliseen tietokoneeseen verrattuna.[11.]

3.3.2 Levyjärjestelmä ja liitännät

Kiintolevy on tietokoneeseen kiinteästi asennettu levymuisti, mitä käytetään tietokoneen massamuistina. Se tallentaa tiedon yhdelle tai useammalle pyörivälle metalli- tai lasikiekon pinnalla olevalle magneettiselle materiaalille. Tiedot säilyvät kiintolevyllä myös ilman virransyöttöä. Yleisimmät kiintolevy koot markkinoilla ovat 2,5” ja 3,5”. Tämän kokoisia kiintolevyjä käytetään yleisesti tietokoneissa sekä palvelimissa. Levyjen kierrosnopeudet vaihtelevat 5 400 aina 15 000 kierrokseen minuutissa. Näitä nopeimpia >10 000 kierrosta minuutissa pyöriviä levyjä käytetään pääsääntöisesti järeämmissä levyjärjestelmissä.[12.]

Perinteisiä kiintolevyjä on tullut korvaamaan uusi kiintolevytyyppi SSD (Solid State Drive). SSD-kiintolevyissä ei ole lainkaan liikkuvia mekaanisia osia vaan tiedot tallennetaan flash-muistipiirille. Levyt ovat tavallisia kiintolevyjä nopeampia sekä niiden virrankulutus on pienempi. Ne eivät myöskään pidä minkäänlaista ääntä, eivätkä ne lämpene käytössä. SSD-levyjen heikkous on niiden rajallinen kirjoituskerta jokaista piiriä kohden. Tämän takia niiden käyttöikä ja luotettavuus eivät ole vielä tavallisen kiintolevyn tasolla. SSD-levyjen hankintahinta on myös korkeahko tallennuskapasiteettiin nähden.

Koska yhä useampi yritys tallentaa datan jo SSD-levyille, on palvelinkäyttöön kehitetty eSSD-levyt, joissa tietoturvaa, suorituskykyä, luotettavuutta ja nopeutta on paranneltu muiden ominaisuuksien ohella. Yritystason SSD-levyt on suunniteltu siten, että ne suojaa ja säilyttää kaikki NAND-siruilla olevat tiedot, joita kirjoitetaan sähkökatkoksen aikana. ESSD-levyille on lisätty erityisiä kondensaattoreita, jotka syöttävät sähkövirtaa levylle, jotta tiedostojen kirjoittaminen levylle saataisiin valmiiksi.[13.]

3.3.3 RAID

> Redundant Array of Independent Disks (RAID) on tekniikka, millä tietokoneiden vikasietoisuutta sekä nopeutta lisätään käyttämällä useita erillisiä kiintolevyjä, jotka kootaan yhdeksi loogiseksi levyksi. RAID-tekniikkaa hyödynnetään usein siellä, missä levyn vasteajat ja vikasietoisuus ovat tärkeässä roolissa.[14; 15.]

RAIDin avulla saadaan kiintolevyjen tiedostot turvattua, koska jotkut RAID-tasot kahdentavat tai turvaavat datan pariteettijärjestelmällä. Pariteettijärjestelmä perustuu matemaattiseen algoritmiin, millä pyritään parantamaan vikasietoisuutta.

RAIDia voidaan käyttää kahdella eri tavalla. Toinen tapa on antaa käyttöjärjestelmän ohjata RAID:in toimintaa ja toinen on ohjata RAIDia erillisellä RAID-levyohjaimella. Levyohjain voi olla integroituna emolevyyn tai se voi olla erillinen ohjainkortti, joka asetetaan emoleyn lisäkorttipaikkaan.

RAID:in hyödyt ovat parhaimmillaan, mikäli sitä ohjataan levyohjaimella. Levyohjaimen avulla kiintolevyjen manipulaatio saadaan siirrettyä kokonaan RAID-ohjaimelle, joka vapauttaa prosessorilta laskentatehoa muille sovelluksille.

RAID 0

RAID 0 jakaa tiedostot tasaisesti useammalle levylle lomittamalla dataa ilman pariteettista ominaisuutta. Tämä nopeuttaa tiedon lukemista ja kirjoittamista, koska levyiltä tieto luetaan rinnakkain. Tämä taso on RAID tasoista nopein. RAID 0 on arka levyvaurioille, koska yhdenkin levyn vikaantuminen/rikkoutuminen tarkoittaa pahimmassa tapauksessa kaiken tiedon häviämistä levypakasta. Järjestelmän varmuuskopiointi on tästä johtuen suotavaa.

Kiintolevyjen vähimmäismäärä on kaksi kappaletta. Kaikki pakan kiintolevyt näkyvät tietokoneessa yhtenä fyysisenä kiintolevynä. Jos kiintolevyt ovat erikokoisia, kokonaistila määräytyy pienimmän kiintolevyn mukaan.

RAID 1

RAID 1 peilaa tiedostot kaikille kiintolevyille ja levyjä tulee olla aina parillinen määrä. Tämä hidastaa kirjoitusnopeutta oleellisesti, koska sama tieto tallennetaan useammalle levylle samanaikaisesti. Lukeminen toisaalta nopeutuu, sillä tiedot voidaan aina lukea levyltä, joka ei ole kyseisellä hetkellä käytössä. Tämän tason vikasietoisuus on hyvä, yhden levyn hajotessa järjestelmä toimii vielä normaalisti.

RAID 1 vaatii kaksinkertaisen määrän levykapasiteettia peilattavaan levytilaan verrattuna, aina kuitenkin vähintään kaksi levyä. Jos kiintolevyt ovat erikokoisia, kokonaistila määräytyy pienimmän kiintolevyn mukaan.

RAID 3

RAID 3 lomittaa tiedot tavuttain eri levyille. RAID 3 tarvitsee kuitenkin yhden ylimääräisen kiintolevyn pelkästään pariteettitiedon tallentamista varten. Tämä täytyy ottaa huomioon ko. järjestelmää valittaessa. Lukunopeudessa päästään RAID 5:n tasolle, mutta koska pariteettitieto tallennetaan erikseen pariteettilevylle, on järjestelmän toiminta hitaampaa kuin RAID 5:lla. Järjestelmä on jo käytännössä jäänyt taka-alalle RAID 5:n etulyöntiaseman takia.

RAID 3 tarvitsee toimiakseen vähintään kolme kiintolevyä. Yhden levyn rikkoutuessa säilytetään vielä tiedot, mutta useamman levyn rikkoutuessa tiedot menetetään.

RAID 4

RAID 4:n toimintaperiaate on käytännössä sama kuin RAID 3:n, mutta tiedot tallennetaan lohkoittain. Lohkotason tallennus tapahtuu lomittamalla tiedot isoihin lohkoihin, jotka osaltaan parantavat kiintolevyjen suorituskykyä. Kuten RAID 3 myös tämä taso hidastaa järjestelmän toimintaa. RAID 5 korvaa käytössä RAID 4:n.

RAID 5

RAID 5 järjestelmä tallentaa lomittamalla lohkoina kaikki tiedot ja pariteettitiedot kaikille kiintolevyille varmistaen, että ne eivät ole koskaan samalla levyllä. Koska pariteettitiedot ovat hajautettuina ei erillistä pariteettilevyä tarvita.

RAID 5 järjestelmä on kohtuullisen vikasietoinen. Yhden levyn hajotessa voidaan hävinnyt tieto vielä saada takaisin jäljelle jääneiden pariteettitietojen avulla. RAID 5 vaatii vähintään kolme levyä toimiakseen.

RAID 6

RAID 6 on käytännössä samankaltainen RAID 5:n kanssa, mutta pariteettidata kahdennetaan, jonka ansiosta järjestelmä kestää kahden kiintolevyn rikkoutumisen. Järjestelmää voidaankin pitää erittäin vikasietoisena, joskin nopeuden kustannuksella.

RAID 6 vaatii toimiakseen vähintään neljä kiintolevyä. Tätä kokoonpanoa käytetään harvemmin sen kustannuksista johtuen. Tämä järjestelmä voidaan korvata hybridi-raideilla, jotka ovat tehokkaampia ja toisinaan edullisempiakin.

Hybridi-raidilla tarkoitetaan kahta päällekkäistä RAID ratkaisua. Hybridi-raidia käytetään yleisimmin isoissa yrityksissä, joissa levyjen tallennus- ja lukunopeudet on oltava huippuluokkaa. [14; 15; 16; 17.]

3.4 WLAN-reititin

Langaton lähiverkko eli WLAN mahdollistaa tietokoneiden ja lisälaitteiden liittämisen langattomasti tietoverkkoon. WLAN tarvitsee toimiakseen laitteen, joka kykenee lähettämään IEEE 802.11 standardin mukaista radiotaajuutta. Tällaisia laitteita ovat muun muassa modeemi tai WLAN-reititin.[18.]

WLAN-reitittimen tarkoitus on reitittää verkkoliikennettä, eli se ohjailee eri protokollien paketit oikeaan osoitteeseen useille eri tietokoneille ja muille laitteille.

Tätä työtä aloittaessani toimistossa ei ollut lainkaan WLAN-reititintä, vaikka sen hankinta olikin ollut suunnitteilla. Suurimmalla osalla toimistossa työskentelevillä henkilöillä on käytössään kannettava tietokone, joten sen hankkiminen tähän yhteyteen oli järkevää. WLAN-reititin on kuvassa 8.

Kuva 8. Zyxel E-900-WLAN-reititin.

4 Asennus

Laitteiston asennus oli varsin suoraviivaista ja yksinkertaista. Varsinaisia ongelmia laitteiston asennuksessa tuotti välikattoon vedettävät kaapeloinnit.

4.1 Kytkin

Laitteiden asennus aloitettiin kytkimen asentamisesta ristikytkentätilan kytkinräkkiin ja kytkemällä kaikki toimistosta tulevat verkkokaapelit kytkimen portteihin. Kytkimen asennus kävi nopeasti ja helposti, koska kyseessä on hallitsematon kytkin, kytkimellä ei siis ole etämäärityksiä, etähallinta tai -ohjaus mahdollisuutta. Näitä ominaisuuksia ei tulla tarvitsemaan.

4.2 Modeemi

Tässä työssä käytettiin jo olemassa olevaa modeemia. Modeemista kytkettiin yksi verkkokaapeli kytkimelle ja toinen WLAN-reitittimeen. Modeemin asetuksia hallitaan selainpohjaisella ohjelmistolla. Ohjelmistoon kirjaudutaan sisään kirjoittamalla internet selaimen osoiteriville laitteen IP-osoite, joka oletuksena on 192.168.1.1. Syöttämällä käyttäjätunnus ja salasana päästään hallintapaneeliin. Modeemin hallintapaneeli on kuvassa 9.

Kuva 9. Modeemin hallintapaneeli

Modeemin hallintapaneelin etusivulla näkyvät kaikki lähiverkossa päällä olevat työasemat. Hallintapaneelin alalaidassa on kaikki järjestelmän ylläpitoon tarvittavat valikot.

Modeemista asetettiin ensimmäiseksi DHCP-palvelin päälle, jolloin se jakaa kaikille lähiverkon laitteille oman IP-osoitteen. Koska DHCP:n antama osoite laitteille on voimassa vain ennalta määrätyn ajan, tarvitsi verkkolevypalvelimelle, tulostimelle ja WLAN-reitittimelle asettaa kiinteät IP-osoitteet. Näin kyseisten laitteiden osoitteet eivät vaihdu esimerkiksi uudelleen käynnistyksen yhteydessä. Modeemi jakoi oletusarvoisesti IP-osoitteet laitteille väliltä 192.168.1.30 -192.168.1.99.

Palomuurin asetukset laitettiin mahdollisimman tiukaksi, kuitenkin siten, että internetin käyttö olisi mahdollisimman sujuvaa. Palomuuri estää asiattoman tietoliikenteen julkisesta verkosta yksityiseen verkkoon. Palomuurilla voidaan myös estää osoitteen väärennöksiä sekä tietokoneviruksia.[19.]

Koska verkkolevypalvelimeen haluttiin saada etäyhteys, piti modeemiin tehdä porttiohjaus. Porttiohjauksen tehtävänä on määrätä ulkoa tuleva liikenne tietylle laitteelle, tässä tapauksessa verkkolevypalvelimelle. Porttiohjaus tarjoaa näin suoran pääsyn yrityksen ulkopuolelta verkkopalvelimen tiedostoihin.

4.3 Verkkolevypalvelin

Verkkolevypalvelin toimitettiin ilman kiintolevyjä, joten ne jouduttiin hankkimaan erikseen. Kiintolevyksi haluttiin ostaa NAS-käyttöön soveltuvat kiintolevyt, sillä niiden luotettavuus on parempi ja lisäksi ne kestävät paremmin tärinää kuin tavalliset kiintolevyt. Kiintolevyt on suunniteltu vaativaan 24/7 käyttöön, joten ne ovat oivallisia kiintolevyjä palvelintarkoitukseen. Kiintolevyjä hankittiin kaksi kappaletta, jotta RAID 1 – taso saavutettaisiin. Koska tilantarvetta oli hankala määrittää etukäteen, työssä päädyttiin hankkimaan yhteensä 4 TB:n verran kiintolevytilaa, jolloin käytettäväksi tilaksi jää 2TB. Verkkolevypalvelimeen on tulevaisuudessa mahdollista lisätä vielä kaksi kiintolevyä. Verkkolevypalvelin tukee kokonaisuudessaan 16TB:n kiintolevy kokoonpanoa.

Kiintolevyjen asennus onnistui helposti palvelimen mukana tulleiden kiintolevykehikoiden avulla. Kiintolevyt ruuvattiin kehikkoihin kiinni neljällä ruuvilla, jonka jälkeen kehikot työnnettiin laitteen sisälle oikeille paikoilleen. Palvelimessa voidaan halutessaan käyttää

joko 2,5” tai 3,5” kiintolevyjä. Tässä työssä käytettiin 3,5” kiintolevyjä. Myös SSD-kiintolevyjä voidaan käyttää. Verkkolevypalvelin tukee Hot Swap-toimenpidettä, jolloin rikki mennyt kiintolevy voidaan vaihtaa uuteen ilman palvelimen sammuttamista, näin voidaan ehkäistä mahdollisen kiintolevyrikon aiheuttamaa käyttökatkoa.

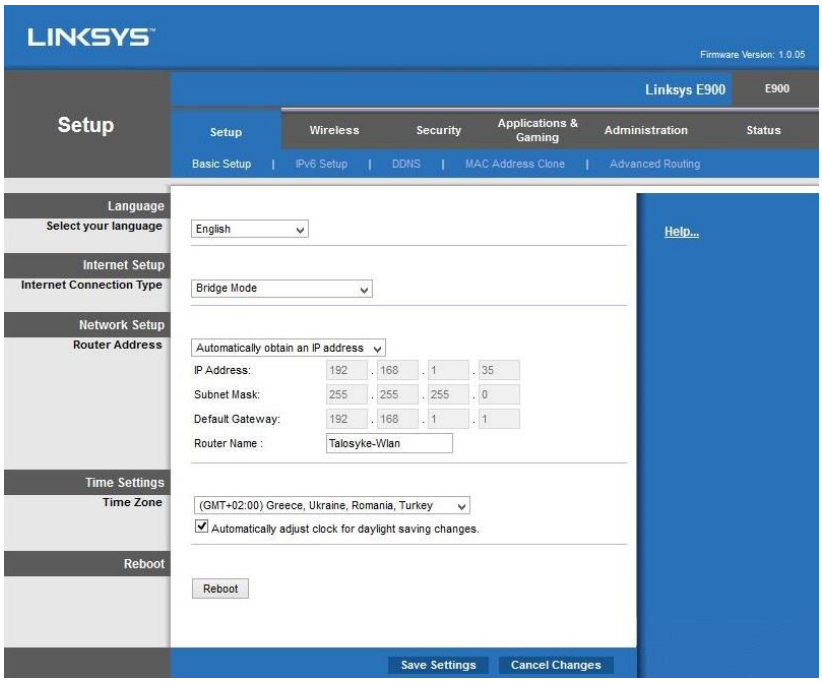
Verkkolevypalvelin sijoitettiin ristikytkentätilaan, jotta sen tuulettimista sekä kiintolevyistä kantautuva ääni ei häiritse työntekijöitä. Verkkolevypalvelin sekä siihen liitetty ulkoinen kiintolevy menevät horrostilaan, kun ne ovat olleet käyttämättömänä tietyn ajan.

4.4 WLAN-reititin

Modeemin ollessa ristikytkentätilassa sen WLAN kantama ei ollut tarpeeksi hyvä, jotta työasemilla internetin käyttäminen langattomasti olisi ollut sujuvaa ja siksi toimiston puolelle asennettiin WLAN-reititin langatonta internetyhteyttä varten. WLAN-reitittimen asetuksia päästiin muokkaaman selainkäyttöliittymän avulla.

WLAN-reitittimen asennus koostui SSID:n, salasanan, salauksen sekä kanavan asettamisesta. Reitittimen mukana tuleva ohjelmisto tuli asentaa ensin yhdelle koneelle, jotta reititin voitiin ottaa käyttöön.

Ohjelma etsi aluksi reitittimen yrityksen lähiverkosta, minkä jälkeen siihen piti luoda järjestelmävalvojan käyttäjätunnus sekä salasana. Kun tunnukset oli luotu, ohjelma avasi selainpohjaisen verkkosivun, missä kaikki reititintä koskevat asetukset voitiin tehdä. Reitittimen hallintasivu on kuvassa 10.



Kuva 10. Linksys E-900 hallintasivu.

Ensimmäinen asia, mikä reitittimeen tuli luoda oli SSID. Sen avulla voidaan erottaa samalla alueella olevat langattomat verkot toisistaan ja kytkeytyä haluttuun verkkoon. SSID voi olla enintään 32-merkkinen, aakkosista ja numeroista koostuva merkkijono. Tässä työssä reitittimen SSID:ksi asetettiin Talosyke-WLAN, jotta se on helppo tunnistaa muiden vieressä toimivien yrityksien verkoista.

Jotta reitittimen WLAN-verkkoon voitiin kytkeytyä, täytyi sille asettaa salasana. Tämä estää vieraiden ihmisten pääsyn yrityksen verkkoon. Salasanalla on samanlaiset attribuutit kuin SSID:llä.

WLAN-reitittimissä käytetään pääasiallisesti kolmea erilaista salausprotokollaa. Ne ovat WEP, WPA ja WPA2.

> WEP on WLAN-tekniikan alkuperäinen, vanhentunut ja verkkohyökkäyksille alttiiksi osoittautunut salausprotokolla. WEP käyttää 40-, 104- tai 232-bittistä salausta, mutta sen RC4-salausprotokollassa olevan puutteen vuoksi joidenkin pakettien kehyksissä lähetetään salaamattomia bittejä, *alustusvektoreita* (initialization vector, IV) ja niiden perusteella voidaan helposti laskea käytetty salausavain. Monet uudemmista WLAN-korteista sisältävätkin tekniikkaa, jolla pystytään vähentämään näiden tietojen lähettämistä.

WPA:n uusi salausmetodi poistaa kokonaan WEP-salauksen tunnetut ongelmakohdat, jotka johtuvat WEP:in käyttämästä staattisesta salausavaimesta. TKIP korvaa WEP:in käyttämän tukiasemaan ja asiakkaalle manuaalisesti syötetyn 40-bittisen staattisen avainparin 128-bittisellä pakettikohtaisella salausavaimella. WEP:in purkamisessa oleellisena osana oleva salausavaimen ennustettavuus poistuu TKIP-avainta käytettäessä, koska avainparit luodaan dynaamisesti pakettikohtaisesti.

IEEE 802.11i eli WPA2 on langattomien 802.11-verkkojen viimeisin tietoturvastandardi, jolla pyritään ratkaisemaan niissä olevat tietoturvaongelmat.
Standardissa määritellään IEEE 802.1X:n mukainen todennus- ja avaintenhallintakäytäntö sekä parannetut menetelmät tiedon salaukseen. 802.11i tarjoaa samat ratkaisut kuin aiempi WPA-standardi mutta lisäksi valittavana on kokonaan uudenlainen salausmekanismi AES (Advanced Encryption Standard). AES on salausalgoritmina hyvin erilainen kuin WPA:n käyttämä RC4 ja vaatii jonkin verran enemmän prosessointitehoa. Se pystyy käyttämään eripituisia avaimia, vaihtoehtoina 128-, 192- ja 256-bittiset pituudet. 802.11i-standardin yhteydessä käytettäneen aluksi 128-bittistä salausta.[20,21.]

Langattoman verkon tietoturvan kannalta käyttäjän autentikointi on erittäin tärkeää. Tässä työssä päädyttiin käyttämään tehokkainta salausprotokollaa, WPA2:sta. Kun asiakas haluaa saada yhteyden WLAN-verkkoon WPA – ja WPA2 standardeissa, sekä asiakas, että tukiasema autentikoidaan. Mikäli käyttäjää ei saada tunnistettua tukiasema evää käyttäjän pääsyn verkkoon.[20,21.]

Käyttäjän tunnistustiedot lähetetään autentikointipalvelimelle. Tunnistautuminen verkkoon tapahtuu IEEE 802.1X/EAP-rajapintaa käyttäen. Käyttäjä sekä autentikointipalvelin tunnistautuvat toisilleen tukiaseman kautta. Molemminpuolisella tunnistautumisella pyritään lisäämään verkon turvallisuutta, siksi myös palvelimen pitää tunnistautua käyttäjälle.[20,21.]

Mikäli kirjautumispalvelin hyväksyy käyttäjän, tämä liitetään WLAN-verkkoon. Mikäli tunnistautumista ei hyväksytä, käyttäjän pääsy WLAN-verkkoon evätään. Kun käyttäjä on onnistuneesti tunnistettu ja palvelin on hyväksynyt käyttäjän verkkoon, kirjautuminen viedään loppuun tukiaseman ja käyttäjän välillä. Palvelin muodostaa salausavaimen, jonka se asentaa käyttäjälle. Salausavaimen protokolla on WPA-standardissa TKIP ja WPA2-standardissa AES.

Reitittimen lähetystaajuus oli 2.4GHz, eikä sitä voitu muuttaa tässä mallissa. 2.4GHz taajuusalue on laajemmin tuettu, mutta kuitenkin kapeampi ja ongelmallisempi kuin uudemmissa laitteissa valittavana oleva 5GHz taajuusalue. 5GHz:n lähetystaajuuksilla tiedonsiirtonopeus on parempi kuin 2.4GHz:n taajuuksilla.[22.]

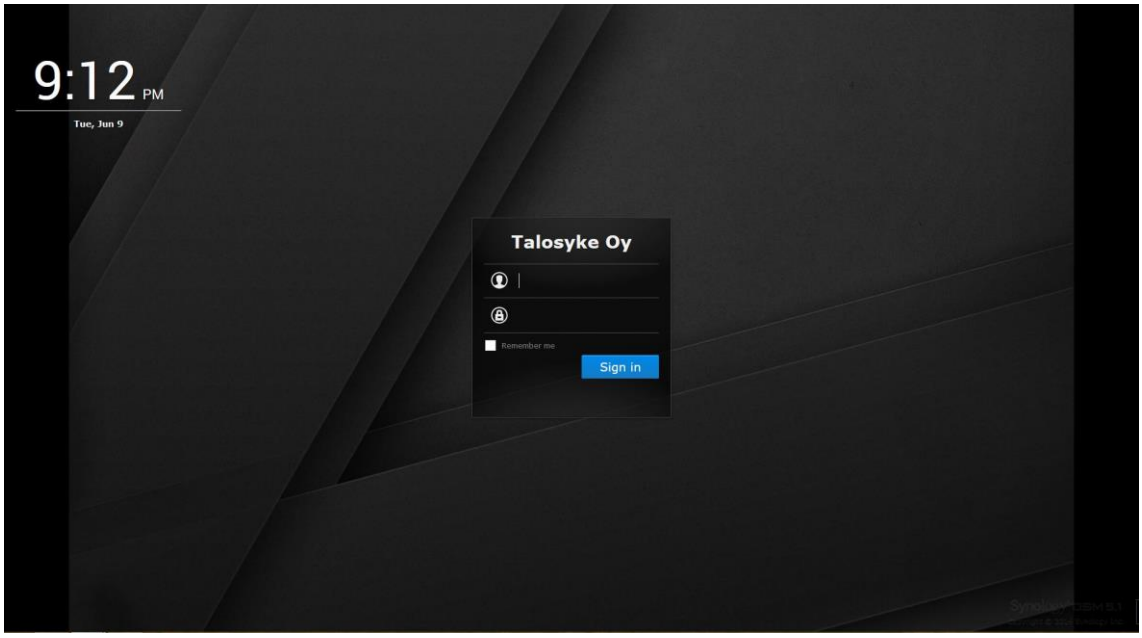
2.4GHz:lla maksimaalinen teoreettinen tiedonsiirtonopeus on 600Mbit/s kun taas 5GHZ:lla se on 7Gbit/s. Näihin tiedonsiirtonopeuksiin ei käytännössä päästä koskaan verkon häiriöiden ja muiden tekijöiden takia.[22.]

Koska yleisimmin WLAN-verkot toimivat 2.4GHz:n taajuudella, voi häiriötä esiintyä muista lähellä toimivista WLAN-verkoista. 2.4GHz:n WLAN-verkko koostuu 13 kanavasta, mitkä ovat viiden megahertsin välein. Koska yhden kanavan kaistanleveys on 20 MHz, menevät vierekkäiset kanavat päällekkäin. Kanavat 1, 6, ja 11 ovat ainoat kanavat, mitkä eivät häiritse toisiaan.

WLAN-verkot skannattiin puhelimeen ladattavalla Wi-Fi Analyzer-sovelluksella. Sovelluksen avulla kyettiin määrittämään lähistöllä toimivat WLAN-verkot ja niiden käyttämät kanavat. Näin pystyttiin valitsemaan omalle WLAN-verkolle kanava, jossa muita WLAN-verkkoja olisi mahdollisimman vähän. Kanavaksi valittiin kanava 11. Tämä nopeutti selvästi langattoman verkon käyttöä. Sovelluksella pystyttiin määrittämään myös reitittimen paras paikka toimistossa.

5 Käyttöjärjestelmä

Synology-verkkolevypalvelin sisältää oman DSM 5.2 käyttöjärjestelmän, jonka pohjana toimii Linux. DSM on Web-pohjainen, mikä mahdollistaa sen käyttämisen kaikilla yleisimmillä käyttöjärjestelmillä sekä internetselaimilla. Käyttöjärjestelmän kirjautumissivu on kuvassa 11.

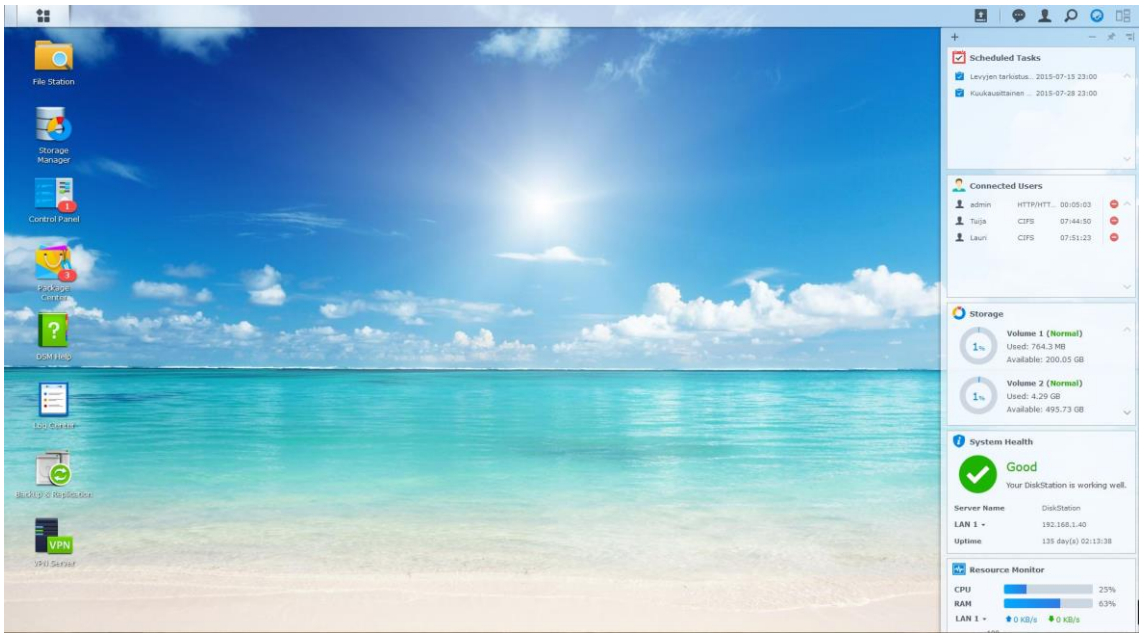


Kuva 11. DSM 5.2:n kirjautumissivu.

Järjestelmään kirjaudutaan oman internetselaimen kautta laitteen omalla IP-osoitteella 192.168.1.40. Järjestelmään kirjautuessa ohjelma kysyy käyttäjänimeä sekä salasanaa.

Käyttöjärjestelmä on hyvin helposti omaksuttavissa, etenkin Windows käyttäjille. Järjestelmän yleisimmät peruskomponentit ovat sijoitettuna pikakuvakkeina työpöydälle, josta niitä on helppo käyttää.

Työpöydälle voidaan halutessa sijoittaa inforuutuja, jotka kertovat käyttäjille reaaliaikaista informaatiota laitteen tapahtumista. Ruudulla voidaan ilmoittaa muun muassa sisään kirjautuneet käyttäjät, kiintolevyjen käyttöasteet, tulevat virus- ja levytarkastukset (S.M.A.R.T) sekä järjestelmän tilaa koskevaa dataa. Järjestelmävalvojan työpöytä on kuvassa 12.



Kuva 12. Järjestelmävalvojan työpöytä.

5.1 Konfigurointi

Verkkolevypalvelimen konfigurointi on aikaa vievää työtä. Se kannattaa tehdä heti alusta asti huolella, jotta vältytään vasta myöhemmin mahdollisesti esiin tulevilta ongelmilta tai töiltä joita voi olla mahdotonta tehdä enää jälkikäteen. Verkkolevypalvelimen tunnistaessa kaksi kiintolevyä ensimmäisellä käynnistyskerralla se ehdottaa RAID:n luomista. Tässä työssä valitsimme RAID 1:n, koska se oli paras vaihtoehto tarpeisiimme. Palvelin mahdollistaa RAID tason muuttamisen jälkikäteen kiintolevymäärän kasvaessa.

Kiintolevyt osioitiin kolmeksi erilliseksi levyksi, minkä vuoksi Windowsissa levyt näkyy kolmena erillisenä kiintolevynä. Osioista tehtiin erikokoiset niiden käyttötarkoituksen mukaisesti. Jotta kiintolevyt tulivat näkyviin jokaiselle työntekijälle, tuli heidän hakea kiintolevyt omalle työasemalleen.

Windowsissa levyt haettiin yhdistäminen verkkoasemaan- toiminnolla. Mikäli käyttäjän oikeudet olivat riittävät, tuli heille tarkoitetut kiintolevyt näkyviin käyttäjätunnuksen ja salasanan syöttämisen jälkeen. Koska verkkopalvelinta käytetään päivittäin, asetettiin yhteyden muodostus kiintolevyihin aina koneelle uudelleen kirjauduttaessa.

Verkkolevypalvelimessa olevia kiintolevyjä halutaan seurata mahdollisten tulevien levyrikkojen varalta. Näin kiintolevyn hajoaminen voidaan ennakoida hyvissä ajoin ostamalla tilalle uusi kiintolevy jo ennen vanhan rikkoutumista. Kiintolevyjen seurannan mahdollistaa S.M.A.R.T-toiminto, joka on määritetty tarkastamaan levyt kuukauden välein.

S.M.A.R.T seuraa muun muassa kiintolevyjen lämpötilaa, käynnistys- ja sammutuskertoja ja käyttöikää. Erilaisia seurattavia attribuutteja on kymmeniä. Pelkkään S.M.A.R.T-tarkastukseen ei kuitenkaan voida luottaa, koska se tarkoituksena on keskittyä enimmäkseen kiintolevyn mekaanisiin toimintoihin. Sähköisiä vikoja ei tämän takia välttämättä huomata.[23.]

Verkkolevypalvelin sisältää oman virustorjuntaohjelman, joka ohjelmoitiin tarkistamaan kaikki verkkolevypalvelimella olevat tiedostot kerran viikossa. Virustorjuntaohjelmalla on oikeus siirtää tarkistuksen yhteydessä kaikki epäilyttävät tiedostot karanteeniin. Ohjelma ilmoittaa yhteenvedon tarkastuksesta sen päätyttyä järjestelmävalvojan työpöydällä. Järjestelmävalvoja voi näin itse varmistua, että karanteeniin menevät tiedostot ovat oikeasti sinne kuuluvia.

Verkkolevypalvelin tarjoaa mahdollisuuden lisäominaisuuksiin, mikä mahdollistaa laitteen monipuolisen käytön. Uusia ominaisuuksia on saatavilla laitteeseen jatkuvasti. Joitain uusia sovelluksia tullaan hyödyntämään vasta tulevaisuudessa. Mahdollisesti käyttöön otettavia sovelluksia ovat muun muassa kameravalvonta ja sähköpostipalvelin.

Myös päivityksiä verkkolevypalvelimeen tulee jatkuvasti. Osa päivityksistä on ollut erittäin tervetulleita. Päivitysten myötä verkkolevypalvelimen käyttö on muuttunut sujuvammaksi.

5.1.1 Käyttäjätilit

Palvelimeen voidaan luoda 2048 käyttäjätiliä ja 256 jaettua kansiota sekä jokaiselle työntekijälle voidaan luoda myös oma henkilökohtainen kansio, joka ei näy muille työntekijöille.

Palvelimeen voidaan myös luoda useita erilaisia käyttäjätasoja, joilla on erilaisia oikeuksia käyttää palvelimen tarjoamia palveluita. Tässä työssä palvelimelle asetettiin kolme

eri käyttäjätasoa, Management, Supervisor ja Users. Users käyttötaso on työntekijöille, Supervisor on työnjohtajille sekä Management taso yrityksen ylimmälle johdolle. Näiden käyttäjätasojen lisäksi on vielä Administrator- taso, jolla on oikeus tehdä kaikki palvelimeen liittyvät muutokset.

Kaikille työntekijöille annettiin palvelimen käyttöönoton yhteydessä oletussalasana, joka tuli vaihtaa mahdollisimman nopeasti. Koska käyttäjien salasanojen turvallisuudesta haluttiin varmistua, otettiin käyttöön järjestelmän ehdottamat vaatimukset salasanoille:

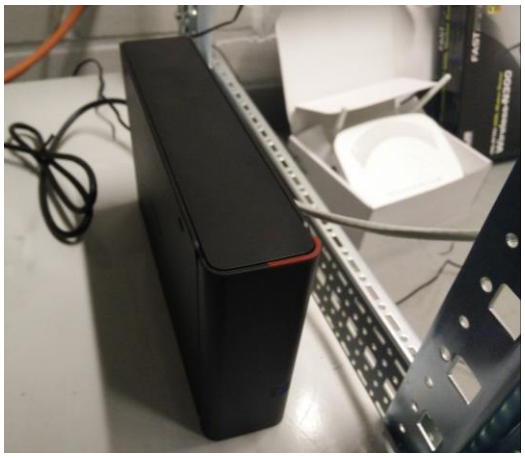
- Käyttäjänimen käyttö salasanassa: Käyttäjänimeä ei saa käyttää salasanassa.
- Isot ja pienet kirjaimet: Salasanassa sallitaan sekä isot että pienet kirjaimet.
- Numerot: Salasanan tulee sisältää vähintään yksi numero.
- Erikoismerkit: Salasanan tulee sisältää vähintään yksi seuraavista erikoismerkeistä (~, `,!, @, #, $, %, ^, &, *, (,), -, _, =, +, [, {,], }, \, |, ;, :, ', '', <, >, /, ?).
- Salasanan pituus: Salasanassa tulee olla vähintään 6 ja enintään 127 merkkiä.

Salasanojen monimutkaistuessa myös salasanojen muistamien kävi yhä hankalammaksi, etenkin jos/kun salasana jouduttiin vaihtamaan usein. Järjestelmä ei tarjoa mahdollisuutta vaatia salasanan vaihtamista käyttäjiltä tietyn väliajoin. Tämä osoittautui pieneksi puutteeksi ja tullaan mahdollisesti korjaamaan tulevien järjestelmäpäivityksien myötä. Työntekijöitä kehotettiin kuitenkin vaihtamaan salasanaa tasaisin väliajoin.

5.1.2 Varmuuskopiointi

Koska työntekijät säilyttivät kaikki työhön liittyvät tiedostot verkkolevypalvelimella, koettiin turhaksi varmuuskopioida kaikki yrityksen tietokoneet päivittäin. Kone, joka sisältää kaikki yrityksen kirjanpitoon liittyvät tiedostot tullaan varmuuskopioimaan ajastetusti joka päivä virka-ajan ulkopuolella.

Verkkolevypalvelin varmuuskopioidaan jokaisen kuukauden viimeisenä päivänä ulkoiselle kiintolevylle, joka sijaitsee verkkolevypalvelimen läheisyydessä. Tällä tavalla tiedostojen nopea palautus on tarvittaessa mahdollista. Ulkoinen kiintolevy on kuvassa 13.



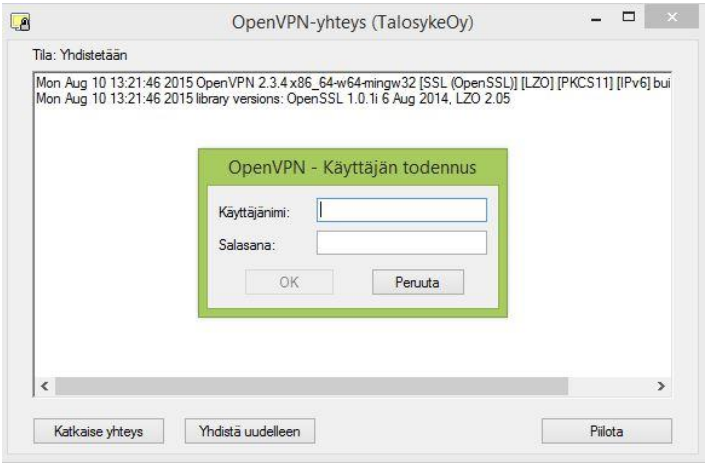
Kuva 13. Buffalo DriveStation.

Verkkolevypalvelin tullaan myös varmuuskopioimaan toiselle verkkolevypalvelimelle verkon yli, milloin kohdetallennin tullaan sijoittamaan toiseen toimipaikkaan. Tällä tavalla voidaan ehkäistä mahdollisesta ilkivallasta sekä tulipalosta johtuva haitta. Tämän opinnäytetyön aikana ei ehditty hankkimaan toista verkkolevypalvelinta, mihin varmuuskopio olisi tehty.

5.1.3 Etäyhteys

Etäyhteys verkkolevypalvelimeen toteutettiin OpenVPN-ohjelmalla. Tätä varten jokaisen työntekijän tuli asentaa OpenVPN-ohjelma omalle työasemalleen. Verkkolevypalvelimesta tuli laittaa VPN-yhteys päälle sekä määrittää käyttäjille oikeudet. Verkkolevypalvelin loi sertifikaatti-avaimen, jonka avulla OpenVPN-ohjelma tunnistaa yhteyden järjestelmään ottavien koneiden oikeellisuuden. Tämä sertifikaatti tuli kopioida OpenVPN-ohjelman konfigurointi tiedostoon käyttäjien tietokoneella. Tähän samaiseen tiedostoon tuli laittaa yrityksen julkinen verkko-osoite sekä portti, jonka takana verkkolevypalvelin sijaitsi. Tiedostoon määritettiin myös salasanakysely yhdistettäessä verkkolevypalvelimeen, sekä käyttöoikeudet vastaamaan lähiverkon kirjautumisoikeuksia.

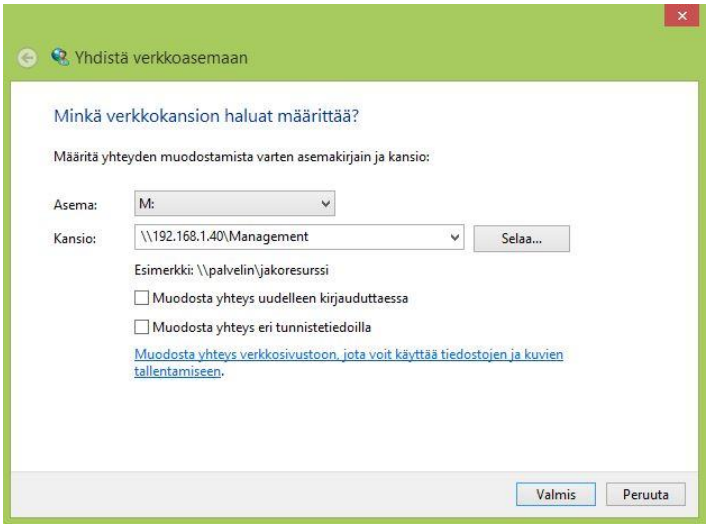
OpenVPN-ohjelma on pieni, kevyt ja helppokäyttöinen ohjelma, mikä avautuu pieneksi kuvakkeeksi Windowsin tehtäväpalkkiin. Ohjelmaa käynnistettäessä esiin tulee käyttäjän todennusikkuna, mihin tulee laittaa käyttäjätunnus sekä salasana. OpenVPN-ohjelman yhteyden luonti-ikkuna on kuvassa 14.



Kuva 14. OpenVPN-ohjelman yhteyden luonti-ikkuna.

Kun tunnukset on syötetty oikein, ohjelma ottaa yhteyden verkkolevypalvelimeen. Ohjelman kuvake tehtäväpalkissa muuttuu vihreäksi yhteyden onnistumisen merkiksi. Nyt verkkopalvelimeen voidaan kirjautua internet selaimen avulla, syöttämällä osoiteriville laitteen IP-osoite ja kirjautumalla sisään.

Mikäli pääsy vaikkapa yhdelle verkkolevyn kiintolevyistä riittää tai käyttäjä ei halua muuttaa henkilökohtaisia asetuksiaan, voidaan levyt hakea yhdistä verkkoasemaan- toiminnolla. Jotta yhdistäminen verkkoasemaan onnistuu, täytyy käyttäjän tietää verkkolevypalvelimen IP-osoite ja verkkolevyn nimi. Aseman tunnuksella ei ole merkitystä. Yhdistä verkko-asemaan-toiminto on kuvassa 15.



Kuva 15. Yhdistäminen verkkoasemaan.

Näin voidaan yhdistää vain siihen verkkolevyyn, jonka tiedostoja halutaan tutkia. Verkkolevypalvelimen kiintolevyt olivat nyt nähtävissä Windowsissa, kunhan kaikki levyt ensin haettiin yhdistä verkkoasemaan- toiminnolla.

Yrityksellä on käytössään kiinteä julkinen verkko-osoite, joten yhteyden ottaminen verkkolevypalvelimeen pitäisi aina olla mahdollista. Tämän työn aikana internet-palveluntarjoajan verkko kaatui kertaalleen, minkä aikana verkkolevypalvelimeen ei saatu etäyhteyttä lainkaan. Katkoksen aikana yrityksen julkinen verkko-osoite oli jostain syystä muuttunut. Palveluntarjoajaan oltiin yhteydessä tästä, ja tilanne saatiin korjattua muuttamalla OpenVPN-ohjelmiin uusi julkinen verkko-osoite.

OpenVPN on ilmainen avoimeen lähdekoodiin perustuva VPN-ohjelma. Ohjelmalla voidaan luoda yksityinen vahvasti salattu yhteys kodin ja työpaikan välille. Ohjelma käyttää TLS/SSL-protokollaa yhteysosapuolten avainten vaihtamiseen. Tietoliikenteen salaukseen ohjelma käyttää OpenSSL-kirjastoa.[24.]

Tiedon siirtoon OpenVPN-ohjelma käyttää UDP sekä TCP-protokollia.

> UDP on ns. yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedostojen siirron.
> UDP eroaa TCP:stä monin tavoin. Muun muassa paketin perillemenoa ei varmisteta päästä päähän (alempi taso kyllä varmistaa seuraavaan solmuun asti). UDP:ta käytetään esimerkiksi DNS-pyyntöjen lähettämiseen, verkkopeleissä ja reaaliaikaisen videon ja äänen välittämiseen. UDP:n yleisrasite on pienempi kuin TCP:n, siinä ei suoriteta alkukättelyä, pakettien kuittausta eikä kolmivaiheista yhteyden lopettamista. Se ei silti välttämättä ole nopeampi kuin TCP, koska TCP:n liikkuva ikkuna (sliding window) kompensoi tehokkaasti kuittausten viemää aikaa.

> TCP on tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille, joilla on pääsy Internetiin. TCP-yhteyksien avulla tietokoneet voivat lähettää toisilleen tavujonoja luotettavasti. TCP-protokolla pitää myös huolta, että paketit saapuvat perille oikeassa järjestyksessä. Tarvittaessa hävinnyt paketti voidaan lähettää uudestaan. Tätä tarkoitusta varten TCP-protokollaan on kehitetty erilaisia vuonvalvonta- ja ruuhkanhallintamekanismeja. Suurin osa Internetin liikenteestä perustuu TCP-protokollaan ja koko TCP/IP-protokollaperhe on saanut nimensä TCP-protokollan perusteella.[25,26]

Kuten aikaisemmin mainittiin, modeemista täytyi avata portti, jotta etäyhteys olisi mahdollinen. Tässä työssä avattiin tietty UDP-portti etäyhteyttä varten. Näin modeemi osasi ohjata liikenteen suoraan verkkolevypalvelimelle.

OpenVPN-yhteys salataan oletusarvoisesti 128-bittisellä salauksella. Tämä oli riittävän korkea salaus etäyhteydelle.

6 Laitteisto

Kaikki laitteiston komponentit valittiin tunnetuilta laitevalmistajilta, joiden luotettavuus on hyväksi todettu. Osa laitteistosta hankittiin Data-systems:ltä ja osa Verkkokauppa.comista. Komponentit on lueteltu taulukossa 1.

Taulukko 1. Hankittu palvelinlaitteisto.

Komponentti	Valmistaja ja laite	Lukumäärä	Hinta € / Alv 0%
Verkkolevypalvelin	Synology Disk Station DS-412+	1	603,90
Kiintolevyt	Western Digital Red 2 TB SATAIII 64MB - 3.5" kiintolevy	2	199,00
Ulkoinen kiintolevy	Buffalo DriveStation DDR USB 3.0 3 TB -ulkoinen kiintolevy USB 3.0 -liitännällä	1	199,99
Kytkin	HP 1410-16G Switch - 16-porttinen 10/100/1000 Ethernet-kytkin	1	154,90
WLAN-reititin	Linksys E900 -WLAN-reititin	1	24,90
		Yhteensä	1182,69

Verkkolevypalvelimeksi hankittiin Synology Disk Station DS-412+, joka sisältää 2-ytimisen prosessorin, 1GB keskusmuistia, neljä kiintolevypaikkaa, kaksi gigabitin verkkoliitäntää sekä useita usb 3.0 portteja.

Verkkolevypalvelimeen voidaan tarvittaessa lisätä muistia 8GB:n asti. Verkkolevypalvelin tukee RAID tasoja 0, 1, 5, 5+Spare, 6 ja 10.

Kiintolevyiksi hankittiin 2 kappaletta 2 TB:n kokoisia Western Digital Red-sarjan kiintolevyä. Kiintolevyt on suunniteltu nimenomaan ympärivuorokautiseen palvelinkäyttöön.

Varmuuskopiointia varten hankittiin ulkoinen, USB 3.0-liitännällä oleva kiintolevy. Se sisältää yhden 3TB:n kokoisen kiintolevyn. Ulkoisen kiintolevyn tiedonsiirtonopeutta on kasvatettu sisäänrakennetulla 1GB:n puskurimuistilla, johon tiedostot siirretään odottamaan ennen varsinaista levylle kirjoittamista.

Kytkimeksi valittiin mahdollisimman yksinkertainen 16-porttinen gigabitin kytkin, mikä on nopeampi kuin edellinen kytkin. Kytkimen nopeutta ei pystytä vielä hyödyntämään muuta kuin paikallisessa tiedonsiirrossa.

WLAN-reititin oli odotettu parannus yrityksen verkkoon. Nyt kannettavalla tietokoneella pystyy käyttämään internet-yhteyttä ilman Ethernet-kaapelia. Myös mobiililaitteet on nyt mahdollista liittää yrityksen lähiverkkoon.

7 Yhteenveto

Tässä insinöörityössä haluttiin selvittää mahdollisimman helppokäyttöinen palvelinlaitteisto yritykselle, jossa ei ollut minkäänlaista keskitettyä tallennusratkaisua. Jo kohtalaisen alussa tuli selväksi, että yritykselle tulee riittämään pelkkä verkkolevypalvelin. Verkkolevypalvelimelta toivotaan pitkää käyttöikää sekä tiettyjä ominaisuuksia, jotka halutaan ottaa myöhemmin käyttöön uudessa toimipaikassa.

Verkkolevypalvelin ja sen oheislaitteet saatiin onnistuneesti ajallaan toimintakuntoon. Käyttökokemukset ovat tähän asti olleet hyviä, muutamia alun hankaluuksia lukuun ottamatta. Verkkopalvelin sekä oheislaitteet ovat toimineet moitteetta alusta alkaen. Voidaan siis sanoa, että nämä hankinnat olivat onnistuneita.

Lähteet

1. Kytkin. 2004. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/Kytkin_%28tietoliikenne%29. Muokattu 3.2.2015 Luettu 5.7.2015.

2. OSI-malli. 2015. Verkkodokumentti. Wikipedia http://fi.wikipedia.org/wiki/OSI-malli. Muokattu 4.2.2015. Luettu 11.6.2015.

3. Paananen, Juha. 2005. Tietotekniikan peruskirja. Jyväskylä. Luettu 28.7.2015

4. Rack server. 2011. Verkkodokumentti. WhatIs. http://whatis.techtarget.com/definition/rack-server-rack-mounted-server. Muokattu 25.3.2011. Luettu 16.7.2015

5. HP ProLiant DL330p.Verkkodokumentti. Storagereview. http://www.storagereview.com/hp_proliant_dl380p_gen8_server_review. Luettu 16.7.2015

6. What is a tower server? Verkkodokumentti. Ehow. http://www.ehow.com/info_8692763_tower-server.html. Muokattu .... Luettu 16.7.2015

7. HP ProLiant ML350 G5. Verkkodokumentti. Lelong. http://www.lelong.com.my/hp-proliant-ml350-g5-server-quad-core-4gb-ram-bee-153335102-2014-08-Sale-P.htm. Luettu 16.7.2015

8. Blade Server. Verkkodokumentti. Wikipedia. https://en.wikipedia.org/wiki/Blade_server. Muokattu 1.6.2015 Luettu 20.7.2015

9. The pros and cons of tower, rack and blade servers. Verkkodokumentti. TechRepublic. http://www.techrepublic.com/blog/the-enterprise-cloud/the-pros-and-cons-of-tower-rack-and-blade-servers/. Muokattu 5.5.2011 Luettu 20.7.2015

10. HP BladeSystem c7000. Verkkodokumentti. Flickr.com https://www.flickr.com/photos/seeweb/5989706885. Luettu 17.7.2015

11. ECC.2013. Verkkodokumentti. Pugetsystems. https://www.pugetsystems.com/labs/articles/Advantages-of-ECC-Memory-520/. Muokattu 5.11.2013 Luettu 7.7.2015.

12. Kiintolevy.2005.Verkkodokumentti.Wikipedia. https://fi.wikipedia.org/wiki/Kiintolevy. Muokattu 30.6.2015 Luettu 13.7.2015.

13. Miksi valita SSD yrityskäyttöön? Verkkodokumentti. Elektroniikka lehti. http://etn.fi/index.php?option=com_content&view=article&id=1786%3Amiksi-valita-ssd-yrityskayttoon&catid=26&Itemid=140. Muokattu 16.9.2014. Luettu 14.7.2015.

14. RAID. 2002. Verkkodokumentti. Mbnet. http://koti.mbnet.fi/~stinger/index.php. Muokattu 3.6.2002. Luettu 15.6.2015.

15. RAID.2004. Verkkodokumentti. Wikipedia. http://fi.wikipedia.org/wiki/RAID_%28tietotekniikka%29. Muokattu 4.2.2015 Luettu 15.6.2015.

16. RAID. 2006. Verkkodokumentti. Wikipedia. https://en.wikipedia.org/wiki/Standard_RAID_levels .Muokattu 8.6.2015 Luettu 15.6.2015.

17. RAID. 2011. Nettilehti. MPC. http://mpc.fi/nettilehti/pdf/1310201140.pdf. Luettu 22.6.2015.

18. WLAN. 2015. Verkkodokumentti. Wikipedia. http://fi.wikipedia.org/wiki/WLAN. Muokattu 2.5.2015. Luettu 12.6.2015

19. Tekninen suojaus. Verkkodokumentti. Internetopas. http://www.internetopas.com/yleistietoa/tietoturva/tekninensuojaus/. Luettu 25.7.2015

20. Langattoman lähiverkon tietoturva. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/Langattoman_l%C3%A4hiverkon_tietoturva. Muokattu 10.2.2015. Luettu 5.8.2015

21. IEEE 802.11i. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/IEEE_802.11i. Muokattu 8.3.2013. Luettu 5.8.2015.

22. 802.11ac Wi-FI Gets Speed Boost to 7 Gbps. Verkkodokumentti. Enterprise networking planet. http://www.enterprisenetworkingplanet.com/netsp/802-11ac-wi-fi-gets-speed-boost-to-7-gbps.html. Muokattu 8.1.2014. Luettu 6.8.2015

23. S.M.A.R.T. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/S.M.A.R.T. Muokattu 5.4.2013. Luettu 4.8.2015

24. OpenVPN. Verkkosivu. https://openvpn.net/index.php/access-server/overview.html. Luettu 15.6.201526

25. UDP. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/UDP. Muokattu 25.2.2015. Luettu 10.8.2015

26. TCP. Verkkodokumentti .Wikipedia. https://fi.wikipedia.org/wiki/TCP. Muokattu 22.2.2015. Luettu 10.8.2015.

27. Lätti, Tomi. 2011. Pk-yrityksen ensimmäisen palvelimen suunnittelu. Opinnäytetyö. Metropolia Ammattikorkeakoulu. Luettu 15.6.2015