Henri Huhtanen

VIDEOVALVONTAJÄRJESTELMÄ VANHUKSEN KOTIHOIDON TUKENA

Tietotekniikan koulutusohjelma
2018

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VIDEOVALVONTAJÄRJESTELMÄ VANHUKSEN KOTIHOIDON TUKENA

Huhtanen, Henri
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Toukokuu 2018
Ohjaaja: Aromaa, Juha DI
Sivumäärä: 54
Liitteitä: -

Asiasanat: videovalvontajärjestelmä, etähallinta, salattu yhteys, tiedostopalvelin

---

Opinnäytetyössä keskityttiin videovalvontajärjestelmän rakentamiseen ja määrittelyyn liittyviin asioihin, mukaan lukien laitteiden luotettavuus.

Keskeinen painopiste oli videovalvontajärjestelmän käyttö iäkkään vanhuksen kotihoidon tukena. Työssä vertailtiin videovalvontajärjestelmiä ja niiden soveltuvuutta eri tarkoituksiin. Lopuksi pohdittiin, miten videovalvontajärjestelmää voitaisiin kehittää paremmaksi.

VIDEO SURVEILLANCE SYSTEM TO SUPPORT ELDERLY HOME CARE

Huhtanen, Henri
Satakunta University of Applied Sciences
Degree Programme in Information Technology
May 2018
Supervisor: Aromaa, Juha M.Sc.
Number of pages: 54
Appendices: -

Keywords: video surveillance system, remote control, encrypted connection, file server

---

The thesis focused on building and configuring a video surveillance system, including reliability of devices.

The central focus was the use of the video surveillance system to support elderly senior home care. The video surveillance systems and their suitability for different purposes were compared in the thesis. Finally it was considered how to develop the video surveillance system even better.

LYHENNELUETTELO

4G	Fourth-Generation Wireless
ADSL	Asymmetric Digital Subscriber Line
APN	Access Point Name
BIOS	Basic Input-Output System
Cat 5	Category 5 cable
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVR	Digital Video Recorder
HDMI	High Definition Multimedia Interface
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec VPN	IP Security Architecture Virtual Private LAN
LAN	Local Area Network
NAS	Network-Attached Storage
NVR	Network Video Recorder
PTZ	Pan Tilt Zoom
RAID	Redundant Array of Independent Disks
RDP	Remote Desktop Protocol
SMB	Server Message Block
TCP	Transmission Control Protocol
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VGA	Video Graphics Array
WAN	Wide Area Network
WLAN	Wireless Local Area Network

SISÄLLYS

1 JOHDANTO

Videovalvontajärjestelmä on rakennettu iäkkäälle yksin asuvalle muistisairaalle vanhukselle. Tarve valvonnalle tuli, koska vanhuksen terveydentila huononi ja kaatuilut lisääntyivät. Valvonnan avulla avunsaanti ja hoitoon pääseminen nopeutuu.

Valvontajärjestelmä koostuu Valueline-tuoteperheestä, joka sisältää neljä kameraa infrapunaominaisuudella (kamera näkee myös pimeässä kuvata), digitaalisesta videotallentimesta eli DVR:sta (Digital Video Recorder) ja lisäksi hallintakoneesta, DNS (Domain Name Server) ja DHCP (Dynamic Host Configuration Protocol)-palvelimesta, NAS:sta (Network-Attached Storage), UPS:sta (Uninterruptible Power Supply) ja reitittimestä.

Tässä opinnäytetyössä käsitellään, mitä kameroiden kaapelointitekniikoita ollaan käytetty, kameroiden paikan valitsemisesta ja niiden suuntaamisesta haluttuun paikkaan, sekä kameroiden ja monitorin kytkemisestä tallentimeen.

Työssä käydään läpi myös miten tallentimen saa kytkettyä verkkoon ja mitä asetuksia täytyy reitittimeen tehdä, porttiohjauksen määrittely reitittimeen, julkisen IP (Internet Protocol)-osoitteen käyttämisen reitittimessä ja IP-osoitteen määrittelyn tallentimelle, sekä IPsec VPN (IP Security Architecture Virtual Private LAN)-yhteyden määrittely reitittimien välille.

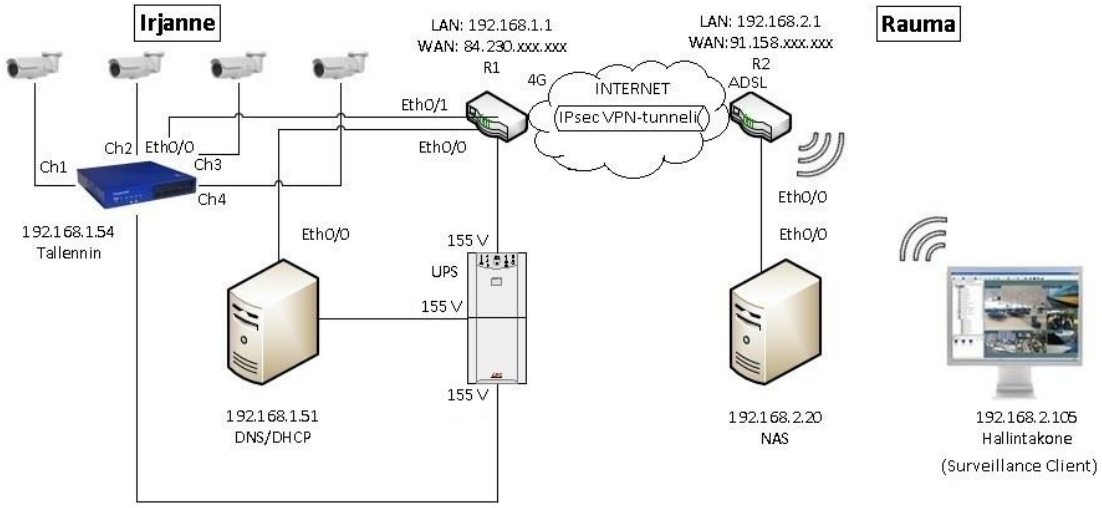
Käytännön osiossa selvitetään, miten valvontajärjestelmää hallitaan ja asetuksia määritellään: käyttäjätilin luominen valvontajärjestelmälle etähallintaa varten, liiketunnisteen- ja kuvausajan määrittelyä kameroille, tallennuksien ja lokien hallintaa, etähallinnan käyttöliittymän toimintojen määrittely ja tallentimen nauhoituksien tallentaminen tiedostopalvelimelle.

Opinnäytetyössä valvontajärjestelmälle tehtiin erilaisia huoltotöitä, yhteyksien monitoroinnista verkkoanalysaattorilla ja vianhakua. Erilaisiin videovalvontajärjestelmien

käyttösovellutuksiin tutustutaan yleisesti. Lopuksi esitetään, mitä muita valvontajärjestelmiä on olemassa ja miten opinnäytetyössä käytettävää valvontajärjestelmää voidaan kehittää paremmaksi.

2 VIDEOVALVONTAJÄRJESTELMÄN RAKENTAMINEN

2.1 Videovalvontajärjestelmän rakenne



Kuva 4. Kokonaiskuva videovalvontajärjestelmästä

Kuvassa 4 nähdään laitteet, joista videovalvontajärjestelmä rakentuu. UPS:sta syötetään 155 V jännite tallentimelle, kameroille, DNS/DHCP-palvelimelle ja reitittimelle R1. Kamerat on kytketty tallentimen kanaville yhdestä neljään. Reitittimen R1 portista 0/0 liittyy Ethernet-verkkokaapeli DNS/DHCP-palvelimen porttiin 0/0 ja reitittimen R1 portista 0/1 Ethernet-verkkokaapeli on kytketty tallentimen porttiin 0/0. DNS/DHCP-palvelimesta tallennin saa IP-osoitteen. Reitittimen R1 ja R2 välille on rakennettu IPsec VPN-tunneli internetin yli. Reitittimen R2 portista 0/0 liittyy verkkokaapeli NAS:in porttiin 0/0. R2 ja hallintakoneen välillä langaton yhteys eli WLAN (Wireless Local Area Network). IPsec VPN-yhteydellä hallintakoneella Surveillance Client-ohjelmalla ollaan yhteydessä tallentimeen, josta nauhoitteet tallennetaan tiedostopalvelimelle. R1-reititin käyttää 4G (Fourth-Generation Wireless)-yhteyttä internettiin yhdistyessä ja R2-reititin käyttää internettiin muodostaessa ADSL (Asymmetric Digital Subscriber Line)-yhteyttä.

4G on neljännen sukupolven mobiiliverkko, jonka ITU on specifoinut ja joka kykenee jopa 100 mb/s tiedonsiirtoon. ADSL-tiedonsiirto tapahtuu puhelinkaapelia pitkin, jolla modeemi erottaa datan puheesta ja ADSL-yhteyden maksimi nopeus on 6 mb/s (Rouse 2010; techopedia www-sivut 2018).

2.2 Kameroiden sijoittaminen

Neljä SVL-CAM 110 merkistä kameraa on asennettu rakennuksen eri kohtiin ruuvikiinnityksellä seinään kiinni. Ensimmäinen kameroista on asennettu käytävälle, toinen kamera on asennettu rakennuksen ulkoseinään kiinni, kolmas kamera on asennettu tupaan ja neljäs kamera on asennettu vieraskamariin.

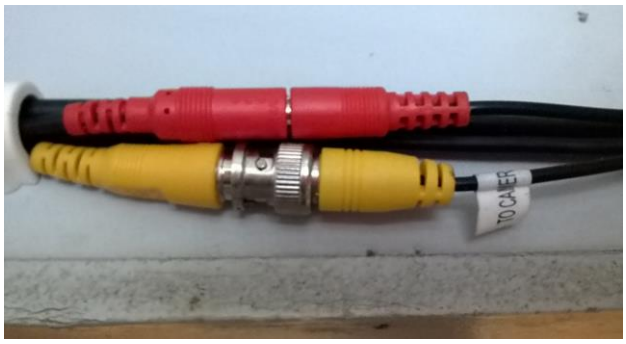
Ensimmäinen kamera näkyy tallentimen kanavapaikalla yksi ja kuvaa käytävää ulkoovelle asti. Toinen kamera näkyy tallentimen kanavapaikalla yksi ja kuvaa talon etupihaa ja sitä ympäröivää ulkorakennusta. Kolmas kamera näkyy tallentimen kanavapaikalla kolme ja kuvaa tuvasta kamariin saakka. Neljäs kamera näkyy tallentimen kanavapaikalla neljä ja kuvaa vieraskamaria, jossa näkyy asennettu videovalvontajärjestelmä.

Kuva 1. Käytävän kamera, pihan kamera, tuvan kamera ja vieraskamarin kamera

Kuvasta 1 nähdään, millaisiin paikkoihin kamerat on sijoitetut ja sekä niiden kiinnitystapa.

2.3 Kaapelointi

Kameroiden videosignaalin siirrossa käytettiin koaksiaalikaapelia 75 ohmin vaimennuksella ja yhden voltin jännitteellä, koska se on edullinen menetelmä alle 400 metrin siirtoetäisyyksillä. Koaksiaalikaapeli liitetään BNC–liittimeen ja lisälaitteita ei tarvita (Aalto ym. 2009, 45). Kamerat toimivat tasavirralla virtakaapelin syöttäessä tulona 12 voltin jännitteellä ja yhden ampeerin virralla. Virta- ja koaksiaalikaapelit on niputetut yhteen ja kiinnitetty seinään nastoilla.



Kuva 2. Virta- ja koaksiaalikaapelin niputus

Käytettävän digitaalisen videotallentimen malli on SVL-DVR104, johon on kytketty kameroista sisään tulevalla koaksiaalikaapelit BNC–liittimet kanavoille yhdestä neljään. Monitorille kuvaa siirretään reaalialiaikaisella ulostulolla VGA (Video Graphics Array)-kaapelilla 1024x764-kuvantarkkuudella. Modeemireititin on kytketty Cat 5 (Category 5 cable)-kaapelilla tallentimeen. Sen tiedonsiirto nopeus on 100mbit/s. Tallentimeen sisään tuleva on tasavirtaa 12 voltin jännitteellä ja 5 ampeerin virralla.

Kuva 3. Digitaalisen videotallentimen liitännät

Kuvassa 3 nähdään kameroista ja virtakaapelin sisään tulevat liitännät, hiiren USB (Universal Serial Bus)-liitäntä, tallentimesta ulostulolla lähtevä VGA-kaapeli monitorille ja LAN (Local Area Network)-verkkoportista lähtee Cat 5-kaapeli modeemireitittimelle.

Cat 5 on Ethernet-kaapeli, joita käytetään erilaisten laitteiden tietoliikenneyhteyksissä.Cat 5-kaapeli on suojaamaton, maksimi lähetysnopeus on 10/100 Mb/s ja maksimi kaista on 100Mhz. (Hastings 2017.)

2.4 DNS ja DHCP-palveluiden määrittely

2.4.1 VMware vSphere Hypervisor (ESXi) 6.5 asentaminen

Tietokoneeseen on asennettu ilmainen patentoitu VMware vSphere Hypervisor (ESXi) 6.5 käyttöjärjestelmä, joka on aktivoitu evaluointilisenssillä.

Sen sijaan että tietokoneelle asennettaisiin palvelimen käyttämä käyttöjärjestelmä, sille asennetaan virtualisointialusta eli hypervisor, jolla voidaan käynnistää useita käyttöjärjestelmiä yhtäaikaisesti. Virtualisoinnin etuna on, että jos palvelin lakkaa toimimasta se voidaan palauttaa toimimaan levykuvasta tai snapshotista eli aiemmin tallennetusta kohdasta. (Vähimaa 2017.)

Ennen virtualisointialustan asentamista tietokoneeseen täytyy BIOS:sta (Basic Input-Output System) kytkeä virtualisointi teknologia päälle.

Teknologia mahdollistaa sen, että prosessori luulee toimivansa useissa eri itsenäisissä tietokoneissa. Samassa tietokoneessa voidaan käynnistellä samanaikaisesti useita eri käyttöjärjestelmiä. (Torres 2012.)

VMware Sphere Hypervisor ESXi (6.5) käyttöjärjestelmä asennetaan ISO-levykuvana, joka on tallennettu buutattavalle USB-tikulle. Buutattava muistitikku on tehty ilmaisella Rufus-työkalulla. BIOS:sta valitaan käynnistettäväksi asemaksi USB, jonka jälkeen latautuu ESXi-installer-ohjelma.

Valitaan levyksi tietokoneen paikallinen 225 GB kokoinen sata-levy, jonka jälkeen valitaan näppäimistön layoutiksi US. Seuraavaksi valitaan root-pääkäyttäjälle tarpeeksi vahva salasana. Vahvistetaan asennus, joka osioi uudelleen sen levyn joka valittiin ESXi:n käyttöön. Lopuksi uudelleen käynnistetään virtualisointialusta ja poistetaan muistitikku tietokoneen asemasta.

Käynnistyksen jälkeen kirjaudutaan root-käyttäjänä sisällä, jotta voidaan määritellä käyttöjärjestelmän asetuksia.

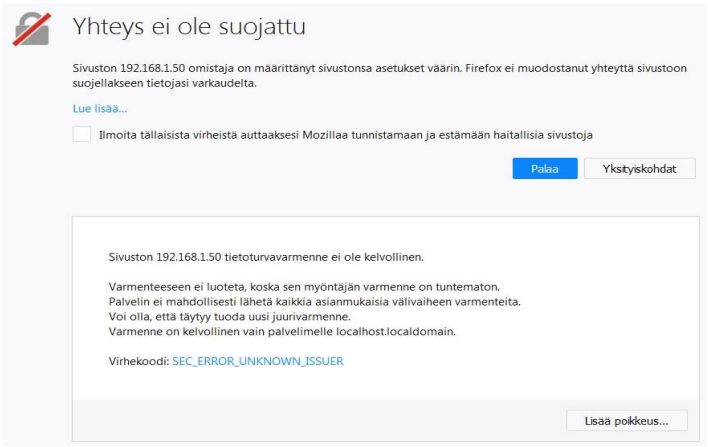
Virtualisointialustan verkkoasetuksista asetetaan staattiseksi IPv4-osoite, joka on 192.168.1.50 ja aliverkon maskiksi 255.255.255.0. Oletusportin osoitteeksi määritellään reitittimen osoite, joka on 192.168.1.1. ESXi:lle määritetään ensisijaiseksi DNS osoitteeksi 8.8.8.8 ja toissijaiseksi osoitteeksi 8.8.4.4. Hostname määritellään oletukseksi localhost.

Osoitteet 8.8.8.8 ja 8.8.4.4 ovat Googlen julkisia nimipalvelun osoitteita, jonka etuja ovat parempi suoja ja selaimen hakujen nopeutuminen. (Google public DNS www-sivut 2018.)

Google tarjoaa suojaa erilaisilta uhilta, jotka kohdistuvat DNS-palvelimeen esimerkiksi spoofing- ja DDoS-hyökkäykset. (Google public DNS www-sivut 2018.)

DDoS-hyökkäys tarkoittaa hajautettua palvelunestohyökkäystä. Hyökkääjällä on apunaan useita kaapattuja tietokoneita, joista rakentuu bottiverkosto. Hyökkäys tulee monesta eri IP-osoitteista samanaikaisesti, mikä tekee siitä hankalemman torjua. (Kataja 2015.)

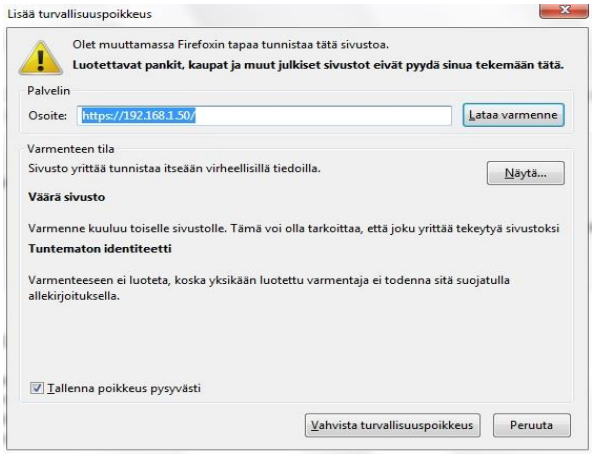
Palvelimen hallintatyökalut saadaan ladattua selaimen kautta osoitteesta 192.168.1.50.



Kuva 5. Ensimmäinen kirjautuminen palvelimelle

Ensimmäisellä kirjautumiskerralla Mozilla Firefox-selaimella palvelimelle tulee ilmoitus, että yhteys ei ole suojattu.

Virhekoodi SEC_ERROR_UNKNOWN_ISSUER tulee näkyviin, jos URL alkaa https:// protokollalla, kun käytetään suojattua yhteyttä. Selaimen täytyy todentaa sivuston sertifikaatit päteviksi, jos selain ei pysty todentamaan niin yhteys sivulle katkaistaan. (Mozilla support www-sivut 2018.)



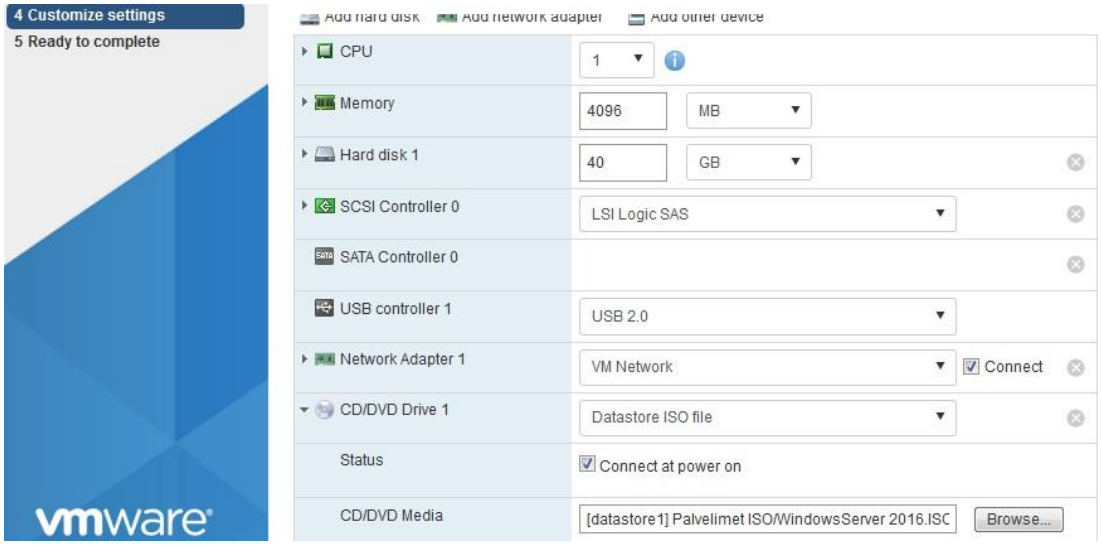
Kuva 6. Palvelimen osoitteen lisääminen turvallisuuspoikkeuksiin

Palvelimen osoite täytyy tallentaa turvallisuuspoikkeuksiin ja vahvistaa, jotta selain päästää kirjautumaan palvelimelle.

2.4.2 Windows Server 2016 asentaminen

Kuva 7. Uuden virtuaalikoneen luominen

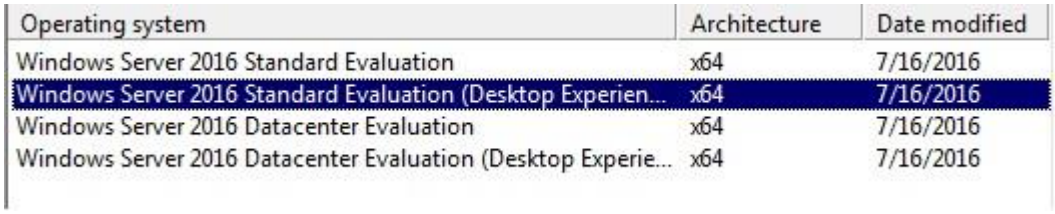
Selaimen kautta VMware ESXi:ssä luodaan uusi virtuaalikone, jonka nimeksi annetaan WindowsServer2016. Määritellään ESXi 6.5 Virtual Machine yhteensopivaksi, käyttöjärjestelmä perheestä valitaan Windows ja käyttöjärjestelmän versioksi otetaan Microsoft Windows Server 2016 (64-bit). Massamuistiksi valitaan datastore1, jonka suuruus on 225 GB.



Kuva 8. Windows Server 2016 laitemääritykset

Määritellään virtuaalikoneen laiteasetukset oletuksiksi ja ainoastaan CD/DVD Drive 1 valitaan datastore1 Palvelimet kansiosta Windows Server 2016 ISO-levykuva. Statukseksi valitaan Connect at power on. Lopuksi päätetään virtuaalikoneen luominen.

Käynnistetään luotu virtuaalikone ja aloitetaan Windows Server 2016-palvelimen asennus. Valitaan asennettavaksi kieleksi englanti (US). Aika, valuuttamuoto ja näppäimistö asetuksesta valitaan suomi.



Kuva 9. Käyttöjärjestelmän tyypin valinta

Valitaan asennettavaksi käyttöjärjestelmäksi Windows Server 2016 Standard Evaluation (Desktop Experience).

Desktop Experience on graaffinen käyttöliittymä palvelimessa.
(Jaimeo & Poggemeyer.)

Seuraavaksi hyväksytään lisenssiehdot. Käyttöjärjestelmän asennustavaksi valitaan Custom: Install Windows only (advanced) ja valitaan osioimaton levy 0, jonne käyttöjärjesetelmä Windows Server 2016-palvelin asennetaan. Asennuksen jälkeen Administrator salasanaksi annetaan vahva salasana.

Kuva 10. Kirjautuminen palvelimelle

Windows Server 2016:lle kirjautuminen täytyy tehdä virtualisointialustalta, josta annetaan komento Ctrl-Alt-Delete komento, joka valitaan Guest valikosta Send keys. Komennolla saadaan kirjautumisikkuna auki, johon saadaan syötettyä käyttäjäntunnus ja salasana.

Kuva 11. Remote Desktop-yhteyden salliminen

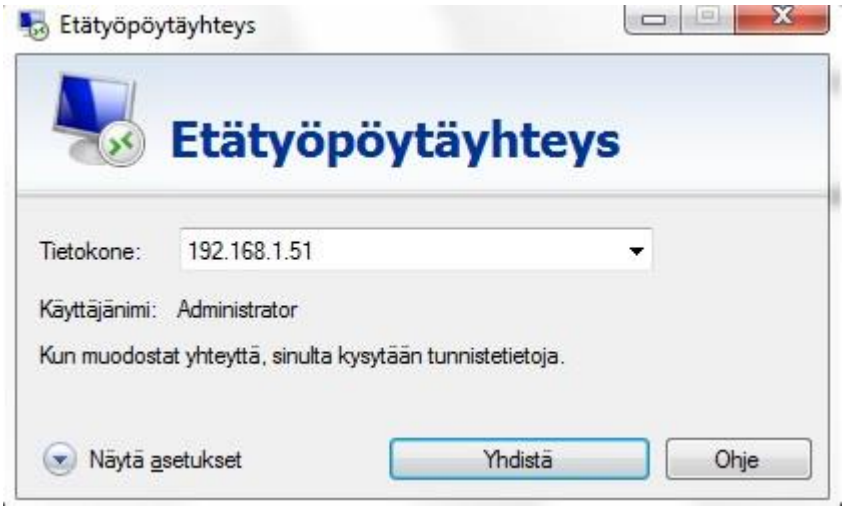
Palvelimessa Server Manager-ikkunasta valitaan Local Server, josta Remote Desktop kohdasta valitaan System Properties. System Properties valikosta Remote Desktop kohdasta laitetaan ”täpät” tarvittaviin kohtiin kuvan 11 mukaisesti.

Etäpöytäyhteys on Microsoftin oma etäkäyttöprotokolla, jotta järjestelmävalvoja voi etähallita työpöytäkoneelta RDP (Remote Desktop Protocol)-yhteydellä Windows Server-palvelimia. (Warner 2016.)

Kuva 12. Remote Desktop säännön käyttöönotto

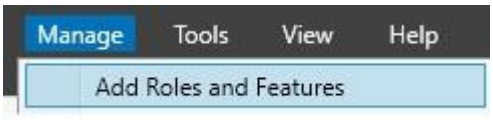
Windows Server:in edistyneistä palomuurin turva-asetuksista Inbound Rules valikosta etsitään Remote Desktop – User Mode (TCP-in) (Transport Control Protocol), josta otetaan sääntö käyttöön. Nyt etäpöytäyhteys on mahdollista työpöytäkoneelta palvelimelle.

2.4.3 DNS-palvelun asentaminen ja määrittely



Kuva 13. Etäpöytäyhteydellä yhdistäminen palvelimeen

Kirjaudutaan Windows Server 2016-palvelimelle käyttäen etäpöytäyhteyttä työpöytäkoneelta ja antamalla Administrator käyttäjän salasana.



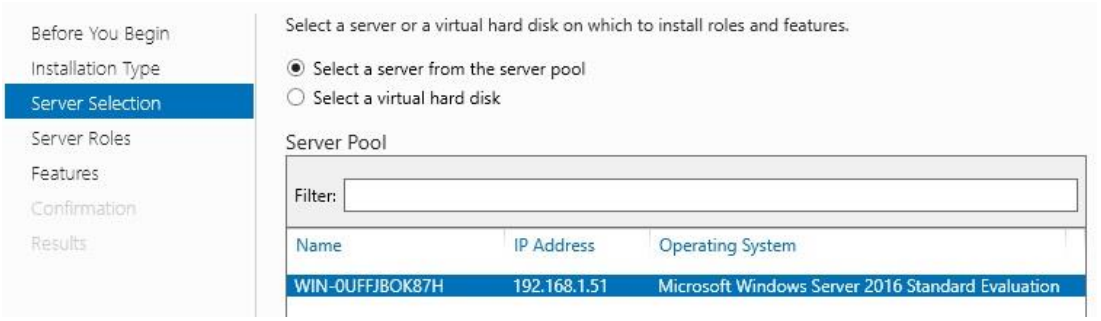
Kuva 14. Roolin lisääminen

Sen jälkeen käynnistetään Server Manager-ohjelma, josta Manage-ikkunasta avataan Add Roles and Features välilehti auki.

Kuva 15. Asennustyypin valinta

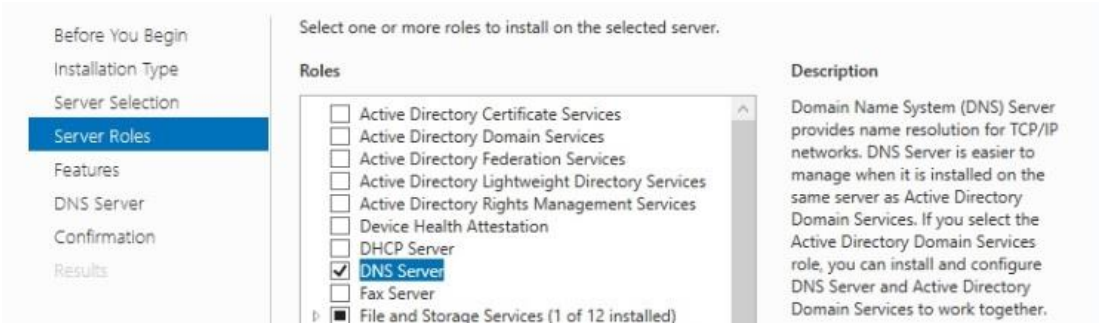
Välilehdeltä valitaan asennustyypiksi Role-based or feature-based installion kuvan 15 mukaan.

Role-based or feature-based installion asennustyypit ovat kaikki Microsoft Windows 2008 lisäosia ja eivät ole kolmannen osapuolen sovelluksia. (Davis 2007.)

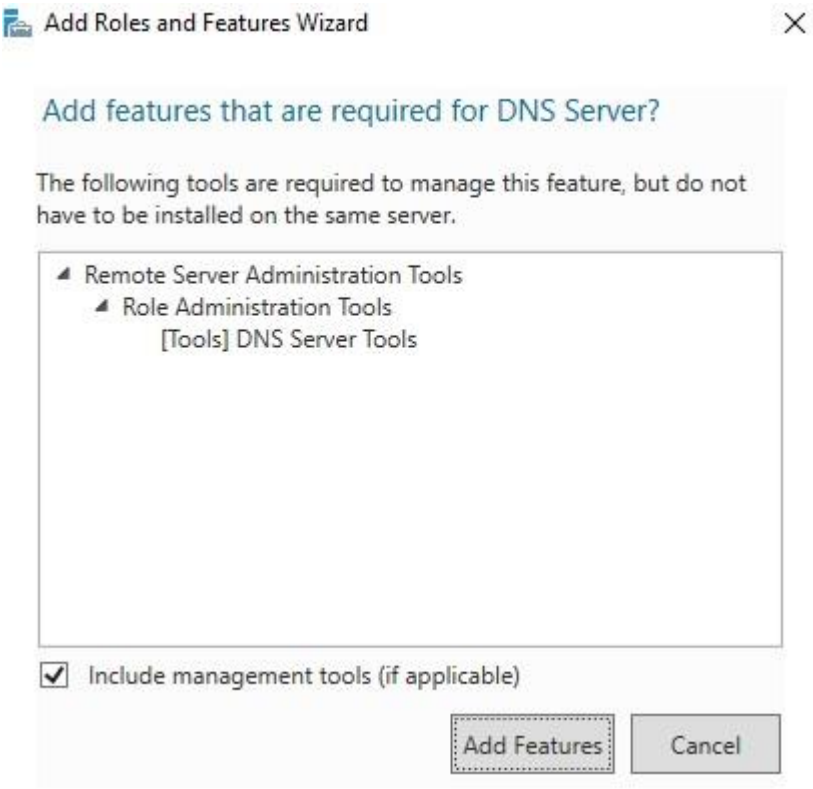


Kuva 16. Palvelimen valinta

Laitetaan ”täppä” Select a server from the server pool, josta valitaan palvelimeksi virtualisointialustalle luodusta virtuaalikoneesta.



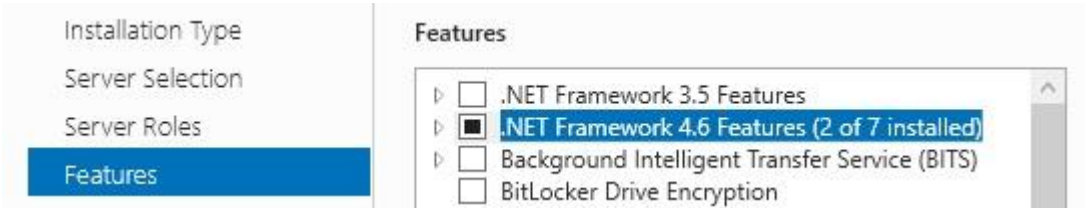
Kuva 17. Palvelimen rooli



Kuva 18. DNS-palvelun hallintatyökalut

Valitaan palvelimen rooliksi DNS Server kuvan 17 mukaan, jonka jälkeen aukeaa uusi ikkuna, jossa oletuksena on lisäominaisuuksina valittu DNS-palvelun hallintatyökalut kuvan 18 mukaisesti.

DNS on internetin nimipalvelujärjestelmä, joka tarjoaa eri internettiin kytketyille laitteille IP-osoitteet, joilla internetsivusto löytyy. (Dadkhah Rasmussen 2018.)

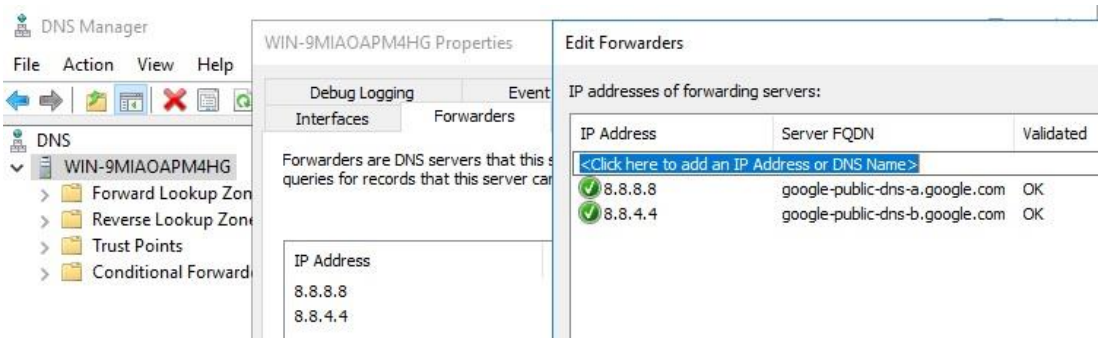


Kuva 19. Net Framework 4.6 asennus

Features kohdasta annetaan oletuksena ”täpän” olla. NET Framework 4.6 Features asennus ruudussa. Lopuksi asennetaan DNS-palvelun rooli, jonka jälkeen käynnistetään palvelin uudelleen. Sen jälkeen tehdään tarvittavat määritykset DNS-palvelulle.

Kuva 20. DNS-palvelun hallintatyökalun käynnistys

Käynnistetään DNS-palvelun hallintatyökalu kuvan 20 mukaisesti. Windows Administrative Tools kansiosta käynnistetään DNS-ohjelma.



Kuva 21. DNS-palvelun Googlen julkisten nimiosoitteiden määrittely

DNS-hallintatyökalussa avataan Properties välilehti auki klikkaamalla palvelimen nimen päältä. Välilehdeltä avataan Forwarders välilehti auki, johon määritellään Googlen julkisten nimipalveluiden osoitteet. Ensisijaiseksi osoitteeksi annetaan 8.8.8.8 ja toissijaiseksi osoitteeksi annetaan 8.8.4.4, jonka jälkeen voidaan kuvasta 21 nähdä, että nimipalveluiden osoitteiden vahvistus on ok.

DNS uudelleenohjaus eli Forwarder lähettää nimikyselyitä ulkoisille Domaineille etäyhteydellä olevista DNS-palveluista paikalliseen verkkoon, ja sisäisistä nimikyselyistä vastaa sisäinen DNS-palvelin. (E. Alvarez 2016.)

2.4.4 DHCP-palvelun asentaminen ja määrittely

DHCP-palvelun roolin lisääminen tehdään samanlaisesti kuin DNS-palvelun kohdalla, eli Server Managerista, Manage kohdasta valitaan Add Roles and Features välilehti auki kuvan 14 mukaisesti.

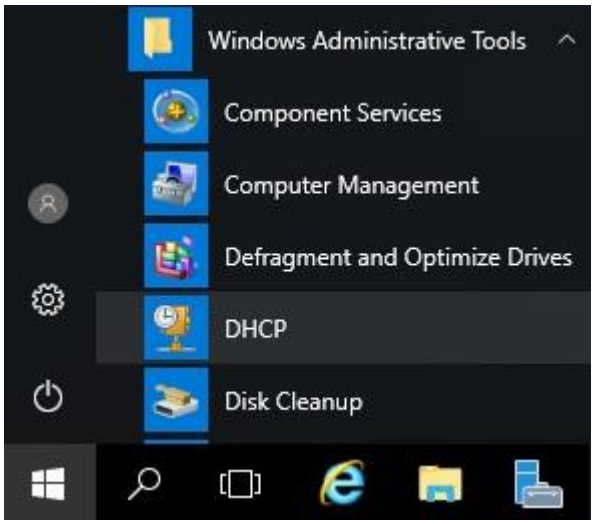
Valitaan asennustyypiksi Role-based or feature-based installation. Valitaan palvelimeksi virtualisointialustalle luodusta Windows Server 2016-virtuaalikoneesta.

Kuva 22. DHCP-roolin valinta

Palvelimen rooliksi otetaan DHCP Server ja uudesta esille tulevasta Add Roles and Features Wizard ikkunasta lisätään oletuksena DHCP-hallintatyökalut. Features kohdasta asennetaan oletuksena .Net Framework 4.6 Features. Lopuksi vahvistetaan asentaminen, ja asentamisen jälkeen uudelleen käynnistetään palvelin.

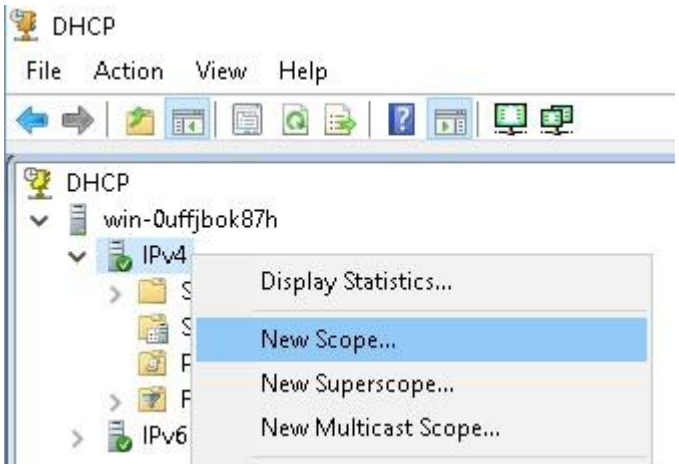
DHCP eli Dynamic Host Configuration Protocol, joka on verkkoprotokolla.

DHCP:n tehtävänä on jakaa IP-osoitteita paikallisverkkoon yhdistyneille laitteille annetusta osoiteavaruudesta. DHCP-palvelimen muihin tehtäviin kuuluu esimerkiksi oletuskäytävän ja nimipalvelun IP-osoitteiden jakaminen. (Web-opas www-sivut 2018.)



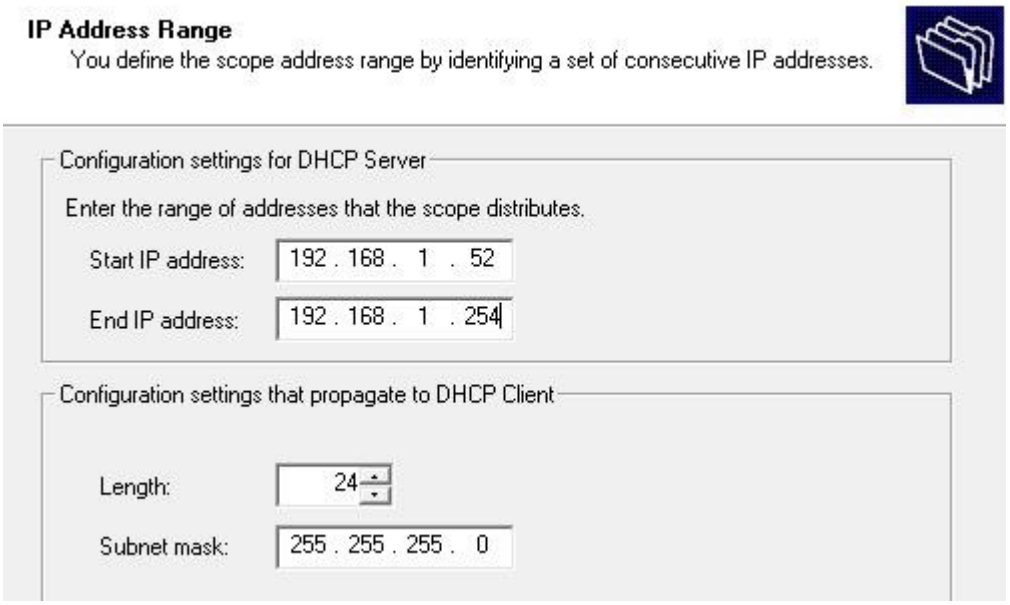
Kuva 23. DHCP-työkalusovelluksen käynnistäminen

Palvelimen uudelleen käynnistymisen jälkeen avataan Windows Administrative Tools kansio auki ja käynnistetään DHCP-työkalusovellus.



Kuva 24. Uuden Scopen lisääminen

DHCP-työkalusta määritellään palvelimelle uusi Scope käyttämällä IPv4-verkkoprotokolla osoitteita. Scope:n nimeksi kirjoitetaan palvelin.

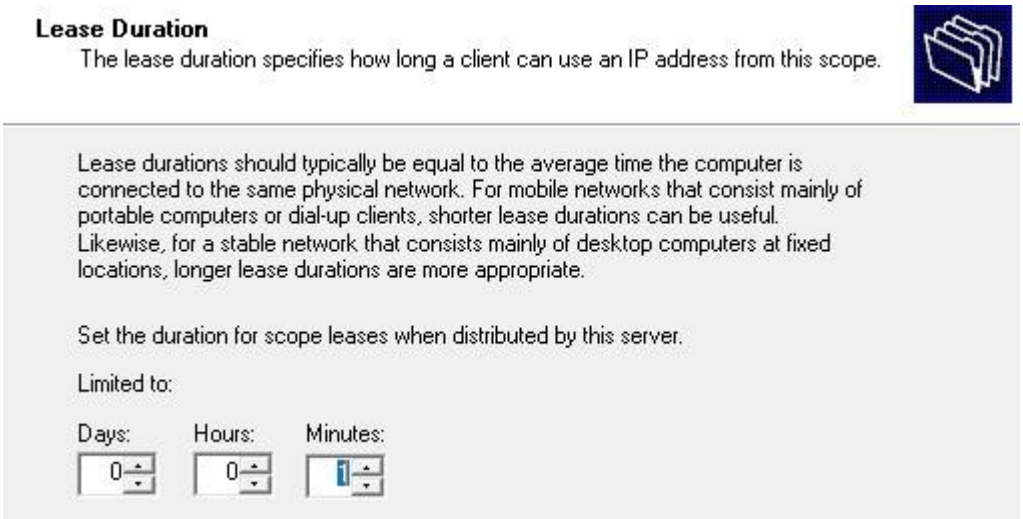


Kuva 25. Osoiteavaruuden määrittely

Seuraavaksi määritellään IP-osoite avaruus. IP-osoite alkaa 192.168.1.52 ja päättyy 192.168.1.254. Aliverkon peitteen osoite on 255.255.255.0 (Aelius www-sivut 2018). Aliverkko peitteen suuruus on 254 hostia C-luokan IP-osoitteissa.

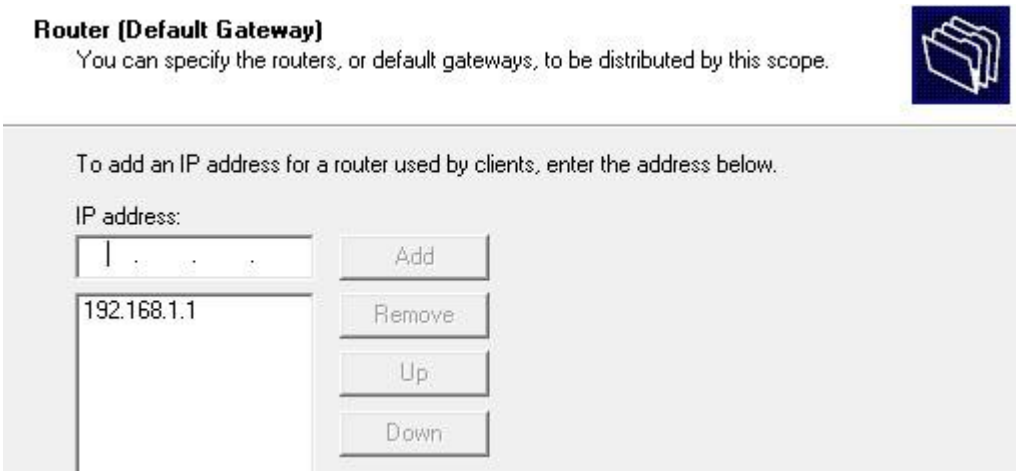
C-luokan verkkoalue alkaa osoitteesta 192.0.0.0 ja päättyy osoitteeseen 223.255.255.0. (Microsoft docs www-sivut 2018.)

Add Exclusions and Delay kohta jätetään oletukseksi tyhjiksi, koska määritellyssä IP-avaruudessa on vapaita osoitteita.



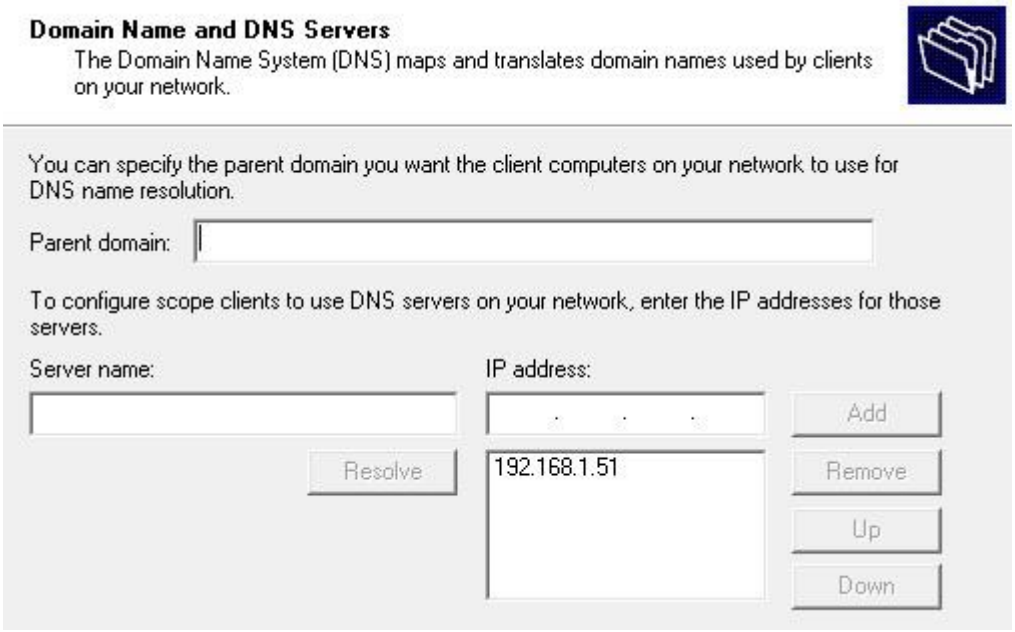
Kuva 26. Osoitteen varausaika

Lease Duration kohdassa määritellään, kuinka kauan laite saa pitää IP-osoitteen, kun on lähtenyt verkosta. Annetaan laitteiden pitää minuutin verran IP-osoitteen, jonka jälkeen laite saa uuden osoitteen, kun tulee uudelleen verkkoon. Seuraavaksi Configure DHCP Options kohdassa määritellään reitittimen oletusportti ja DNS-palvelin Scope:lle.



Kuva 27. Reitittimen oletusportin määrittely DHCP:lle

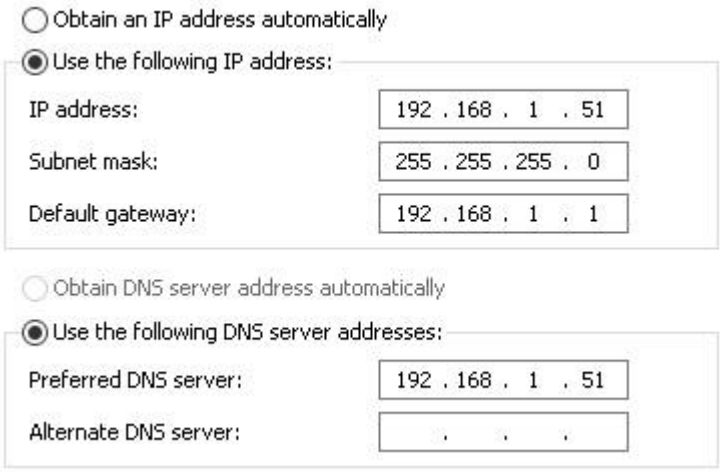
Lisätään DHCP:lle reitittimen oletusportin osoite 192.168.1.1, jonka kautta DHCP saa jaettua IP- ja DNS-osoitteet hosteille.



Kuva 28. DNS-palvelimen osoitteen antaminen DHCP:lle

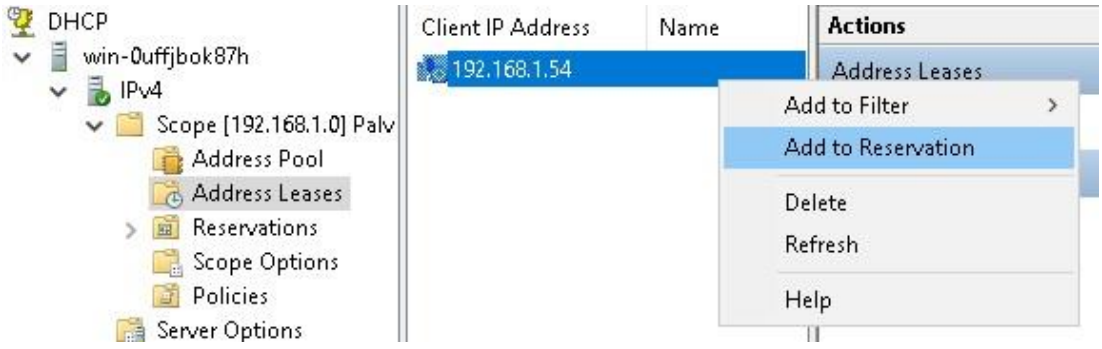
Kuvassa 28 Domain Name and DNS Servers muut kohdat jätetään oletuksena tyhjiksi paitsi DNS-palvelimen osoite, joka on 192.168.1.51 DHCP:lle.

WINS Servers kohta jätetään oletuksena tyhjäksi. DHCP määrittelyn lopuksi hyväksytään Scopen aktivointi.



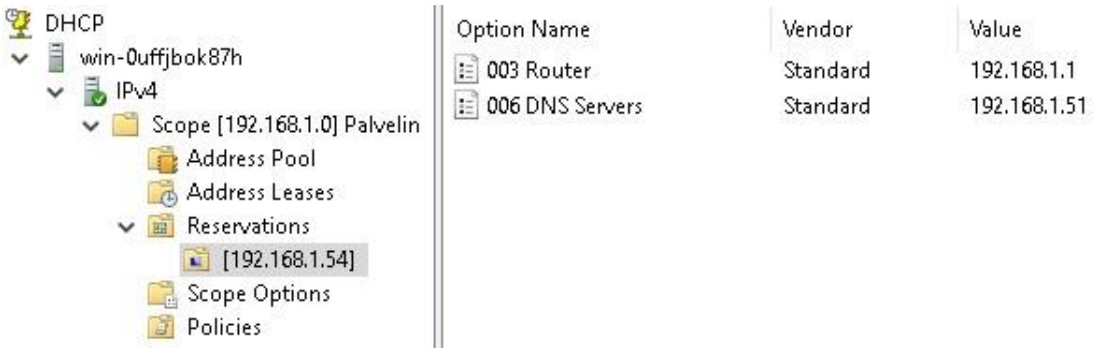
Kuva 29. Windows-palvelimelle osoitteiden antaminen

Kuvassa 29 palvelimelle annetaan staattisesti osoitteet. Annetaan IP-osoitteeksi 192.168.1.51, aliverkon peitteeksi 255.255.255.0 ja oletusportiksi 192.168.1.1. DNS-osoitteeksi annetaan luodun Windows-palvelimen osoite, joka on 192.168.1.51.



Kuva 30. Tallentimen osoitteen varaus

DHCP-työkalusta Address Leases kansiosta valitaan tallentimen osoite, joka on 192.168.1.54. Lisätään osoite varaukseen.



Kuva 31. Tallentimen oletusportin ja DNS-palvelun osoitteiden tuominen

Reservations kansiosta nähdään tallentimen osoite, josta nähdään myöskin oletusportin osoite ja DNS-palvelimen osoite. Tallentimen osoite pysyy nyt samana, vaikka tallennin lähtisi verkosta pois ja tulisi takaisin verkkoon.

2.5 UPS:in ohjelmointi ja kytkentä

UPS lyhenne tulee sanoista Uninterruptible Power Supply ja tarkoittaa katkeamatonta virtalähdettä. Akkua ladataan automaattisesti verkkovirralla. Sähkön loppuessa UPS aloittaa syöttämään verkkovirtaa tarvitseville laitteille heti ilman, että laitteissa loppuu virta. UPS antaa virtaa laitteille, jos jännite on asetettu UPS:in määrityksissä sopivaan arvoon. Virran syöttö katkeaa, jos jännite UPS:ssa nousee liian korkeaksi tai liian alhaiseksi, jolloin virtaa aletaan syöttämään laitteille akkujen kautta. (Ylä-Jääski 2012).

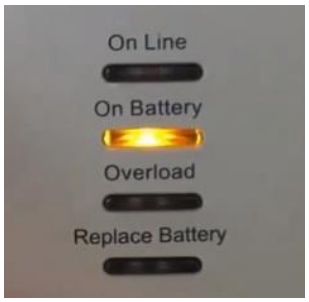
Kuva 32. Videovalvontajärjestelmän sähkönsyötöstä vastaava UPS (Tokopedia www-sivut 2018.)

Videovalvontajärjestelmässä käytetty UPS mallina toimii Back-UPS RS 1000 APC-varavirtalähde, jonka tuleva sähkö on kytketty 230 V sähköverkkoon. UPS:in lähtevään 155 V syöttöön on kytketty tallennin, palvelin ja reititin.

Varavirtalähteen maksimikuorma 600 W ja akkujen latausaika on kahdeksan tuntia. Syötön taajuusalue vaihtelee 47-63 Hz taajuudella ja akun aallon muotona on askellettu siniaalto. (APC user’s manual www-sivut 2018.)

Kuva 33. UPS:in ohjelmointila (Schneider-Electric 2017)

UPS:in syötön herkkyyden ohjelmoinnissa varavirtalähde täytyy kytkeä toimivaan 230 V sähköverkkoon, jonka jälkeen UPS sammutetaan ja käynnistetään uudelleen pitämällä virtapainiketta kymmenennen sekunnin ajan pohjassa, jolloin UPS menee ohjelmointitilaan.



Kuva 34. UPS ohjelmoitu 155 V tilaan (Schneider-Electric 2017.)

Ohjelmointitilassa painetaan virtapainiketta niin kauan, että ainoastaan On Battery valo palaa keltaisena ja muut valot palavat pimeinä. Lopuksi päästetään virtapainikkeesta irti, joka sammuttaa virtalähteen.

Nyt käynnistyksen UPS on ohjelmoitu toimimaan alhaisemmalla syötön herkkyydellä 155 V. UPS ei pysy On Line tilassa 165 V tai 175 V tilassa vaan siirtyy On Battery tilaan ja syöttää tällöin ainoastaan akusta virtaa siihen kytketyille laitteille.

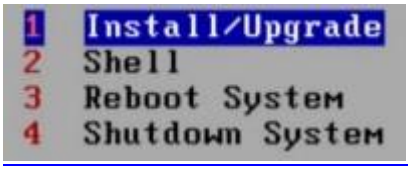
2.6 NAS:in rakentaminen ja kytkentä verkkoon

NAS tarkoittaa suomennettuna verkkoon liitettyä tallennustilaa. NAS:iin pääsee tallentamaan ja lukemaan tietoja paikallisverkon kautta. NAS mahdollistaa usean käyttäjän samanaikaisesti lukea ja kirjoittaa tallennustilaan. NAS tukee myös RAID (Redundant Array of Independent Disks)-tekniikkaa, jolla voidaan useita kovalevyjä yhdistää yhdeksi loogiseksi levyksi. (Rouse 2015.)

Videovalvontajärjestelmään kuuluu myös NAS, jolla saadaan tallentimen videokuvatallenteet kopioitua tiedostopalvelimelle. Videokuvatallenteiden kopioinnista vastaa videovalvontajärjestelmän hallintakone, jonka käyttöjärjestelmä on Windows 10 Education ja johon on asennettu Surveillance Client-asiakasohjelma.

Surveillance Client-ohjelmalle tallennukset ohjataan tiedostopalvelimelle ja tallennuksia voidaan katsoa millä tahansa tietokoneelta, joka on samassa paikallisverkossa NAS:in kanssa.

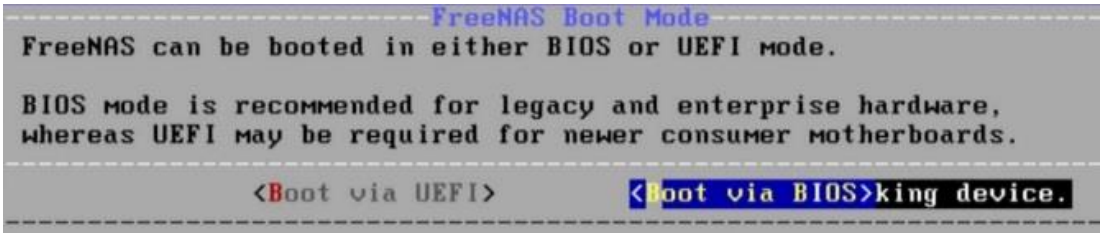
Tallennuksien videokuva tyyppinä on .264-tiedosto ja tallennuksia voidaan katsoa Video Player-ohjelmalla.



Kuva 35. NAS:in asentaminen tietokoneelle

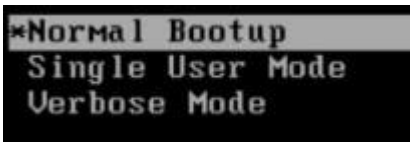
NAS asennetaan tietokoneelle bootattavalta USB-tikulta, johon on kopioitu FreeNAS versio 11.1 ISO-levykuva. Tietokoneesta valitaan bootattavaksi asemaksi muistitikku, josta asennetaan NAS-käyttöjärjestelmä.

Valitaan da0-levy, jonka koko on 250 GB. Alustetaan levy, johon FreeNAS asennetaan. Annetaan root:lle vahva salasana, jolla asennuksen lopuksi päästään kirjautumaan NAS:lle selaimen kautta.



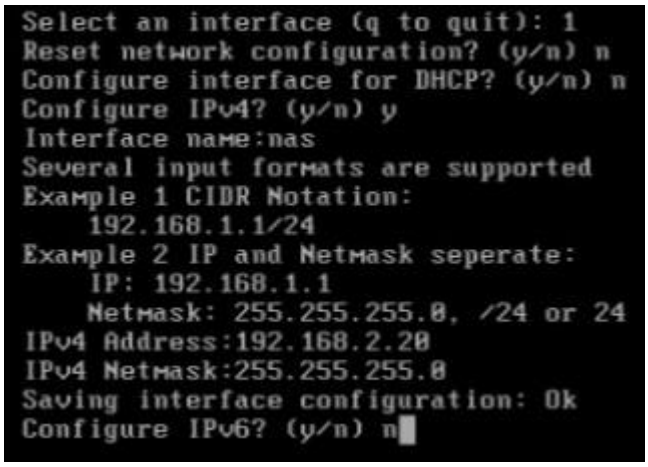
Kuva 36. NAS:in käynnistystilan valinta.

Valitaan käynnistys BIOS:in kautta. Lopuksi päätetään asennus ja uudelleenkäynnistetään NAS.



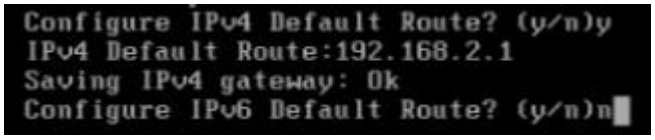
Kuva 37. NAS:in normaalikäynnistyksen valinta

Valitaan NAS:ille normaalikäynnistys, jonka jälkeen tehdään seuraavat määritykset verkon rajapinnalle, oletusreitille ja DNS:lle.



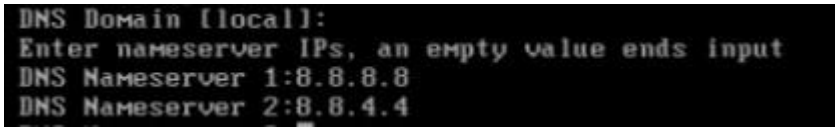
Kuva 38. Verkkorajapinnan määrittely

Määritetään rajapinnalle DHCP pois päältä ja määritetään IPv4-osoite. Rajapinnan nimeksi annetaan nas. IP-osoitteeksi annetaan 192.168.2.20 ja maskin osoitteeksi 255.255.255.0. Ei määritellä IPv6-osoitetta NAS:ille.



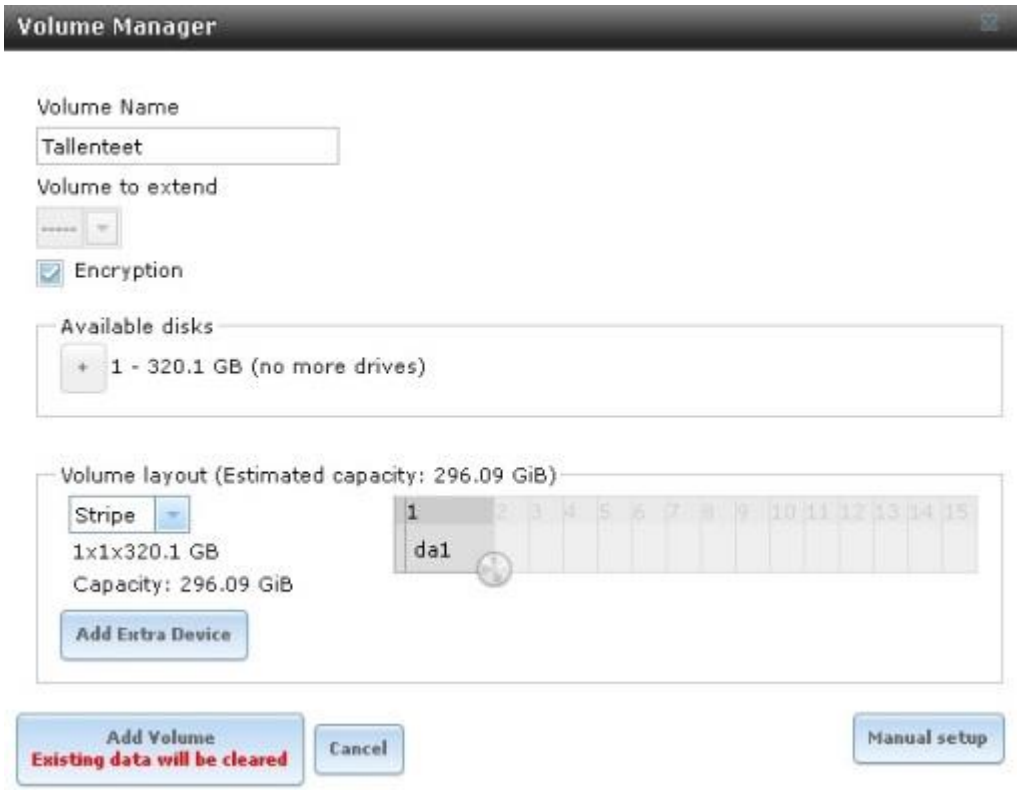
Kuva 39. Oletusreitin määrittely

Määritellään oletusreitiksi reitittimen osoite, joka on 192.168.2.1.



Kuva 40. DNS-osoitteen määrittely

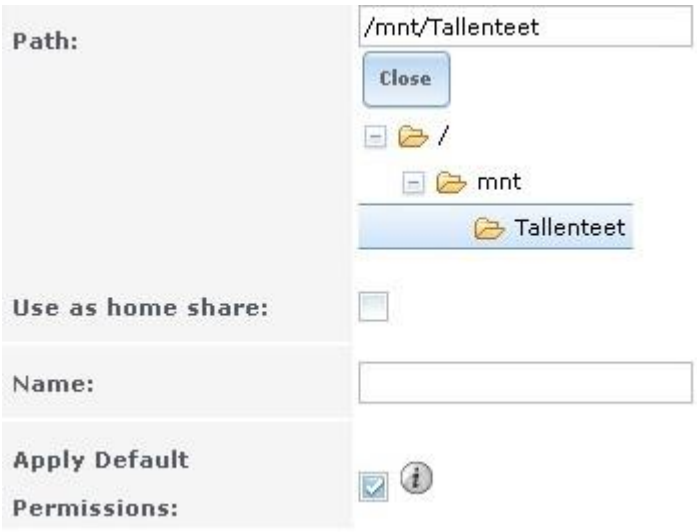
Määritellään tiedostopalvelimelle ensisijaiseksi nimipalvelimen osoitteeksi 8.8.8.8 ja toissijaiseksi osoitteeksi 8.8.4.4.



Kuva 41. Kiintolevyn lisääminen

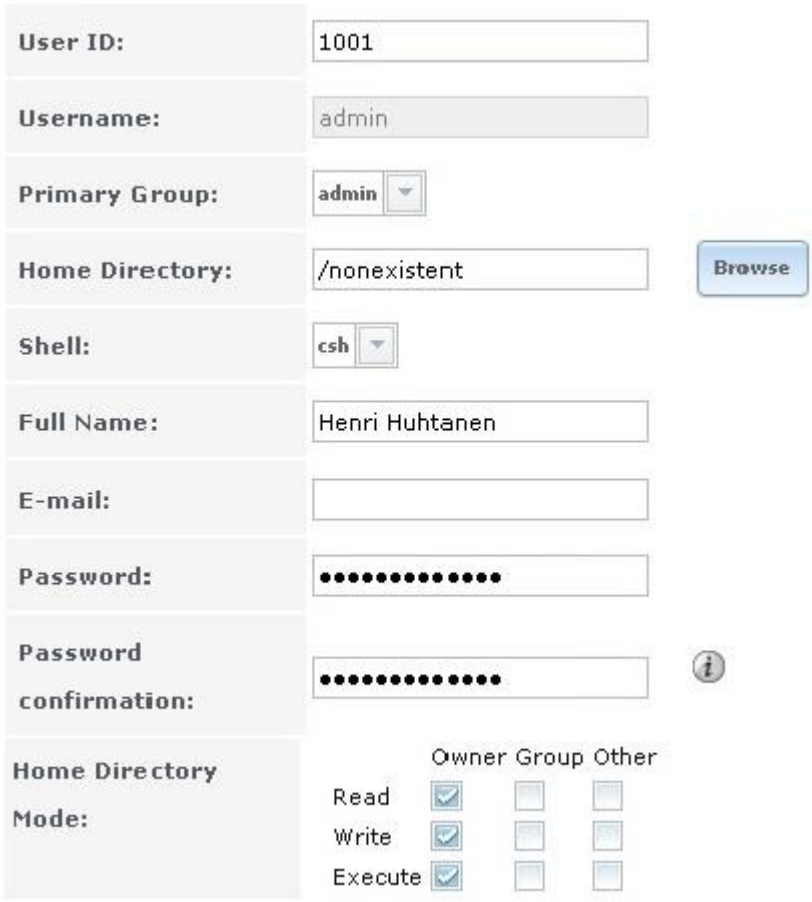
Kirjaudutaan Mozilla Firefox-selaimella NAS:iin osoitteella 192.168.2.20 ja annetaan root-käyttäjän salasana. Avataan Storage ikkuna auki, josta lisätään 320 GB ulkoinen kovalevy NAS:iin ja annetaan nimeksi tallenteet. Valitaan levyn kryptaus, joka salaa levyn datan. Pohjaksi valitaan Stripe ja otetaan koko ulkoinen kovalevy käyttöön.

Stripe (suom. raita) tarjoaa levylle korkeamman suorituskyvyn. (Rouse 2015.)



Kuva 42. Windows SMB (Server Message Block)-kansion jako

Sharing kohdasta valitaan Windows (SMB) -välilehti auki ja lisätään Windows SMB-jakokansio. Poluksi valitaan /mnt/Tallenteet ja määritellään oletusoikeudet.

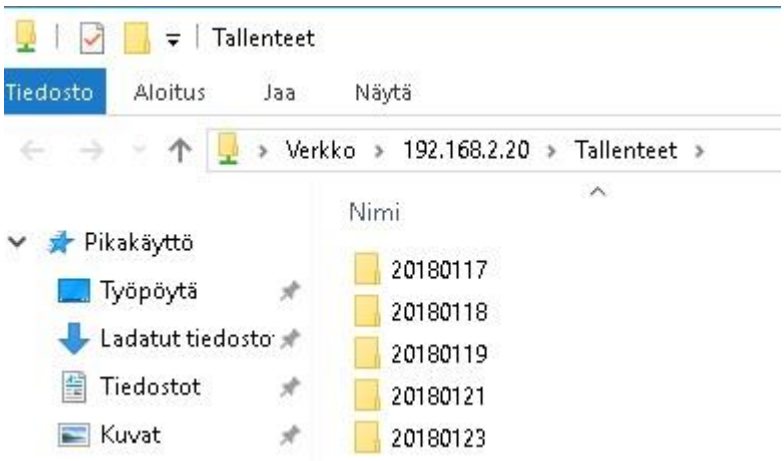


Kuva 43. Käyttäjän luominen

Luodaan ryhmä admin, johon tehty admin-käyttäjä liitetään. Tehdään kuvan 43 mukaiset asetukset käyttäjälle ja annettaan käyttäjän omistajanoikeudet lukea, kirjoittaa ja suorittaa.

Kuva 44. Tallentimen videokuvan kopioiminen NAS:iin

Videovalvontajärjestelmä hallintakoneella Surveillance Client-ohjelmalle määritetään kansio, johon tallentimen ottamaa videokuvaa tallennetaan //192.168.2.20/Tallenteet kansioon, joka sijaitsee tiedostopalvelimessa. Määritetään levylle 600 MB rajoitus, jolloin siitä tulee hälytys lokitiedostoon.



Kuva 45. Videokuvan tallentuminen tiedostopalvelimelle

Kuvasta 45 nähdään tallenteiden kopioituminen tiedostopalvelimelle ja tällöin voidaan varmistua siitä, että NAS toimii oikein.

Kuva 46. Video Player-ohjelmalla tiedostopalvelimesta videokuvan toistamista

Hallintakoneelta Video Player-ohjelmalla voidaan toistaa tiedostopalvelimille tallennettua videokuvaa kameroiden kanavilta yhdestä neljään.

3 VIDEOVALVONTAJÄRJESTELMÄN HALLINTA

3.1 Lähiverkon määrittely tallentimelle

Tallentimessa määritellään, että tallennin saa DHCP-palvelimelta IP-osoitteen, joka on 192.168.1.54 ja aliverkon peite on 255.255.255.0. Portin osoitteeksi 192.168.1.1, joka on reitittimen osoite. Ensisijaiseksi DNS-osoitteeksi 192.168.1.51 ja toissijaiseksi osoitteeksi 195.74.0.47.

DHCP-palvelua käytettäessä annetaan automaattisesti IP-osoite tallentimelle.

Aliverkon peitteellä voidaan rajata käytettävät IP-osoitteet osoiteavaruudesta. DNS-osoitteet tallennin on saanut ensisijaisen osoitteen paikalliselta DNS-palvelimelta ja toissijaisen osoitteen Elisan DNS-palvelimelta. DNS on internetin nimipalvelujärjestelmä. Järjestelmä muuntaa luettavat nimet tallentimen osoitteiksi (Viljanen 2013-2017.)

3.2 Portin uudelleenohjauksen määrittely

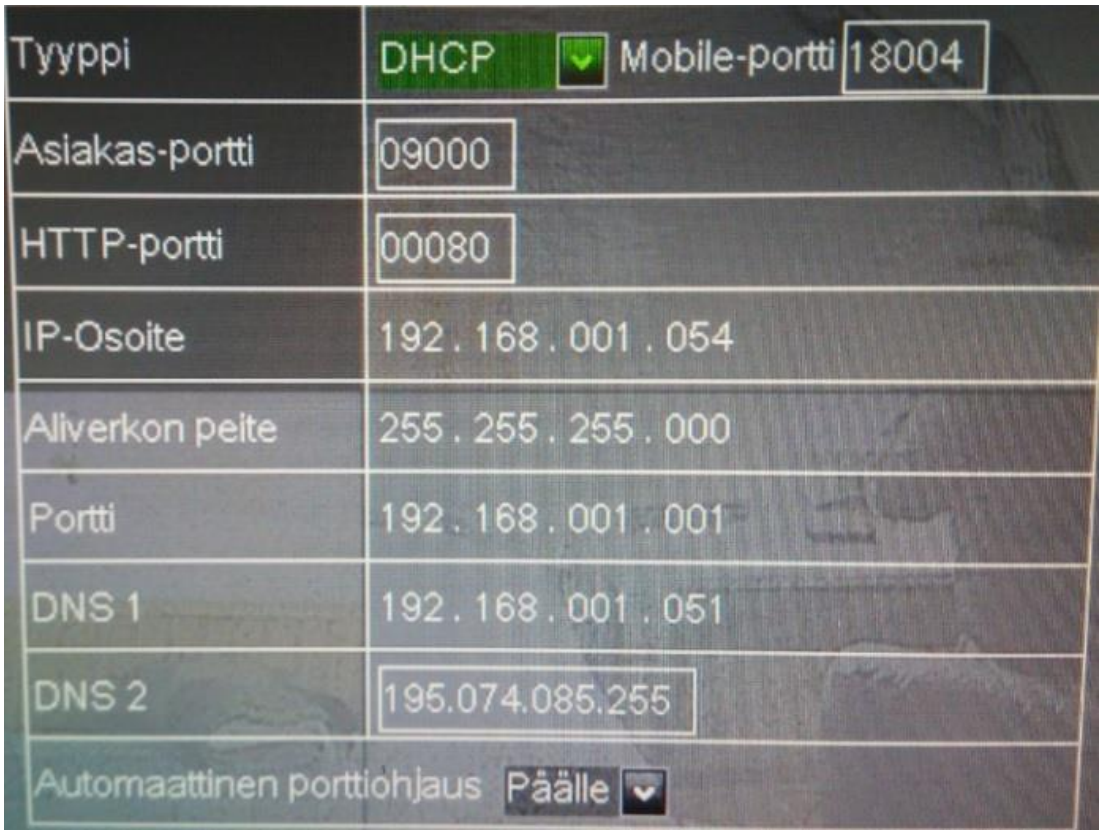
Portin uudelleenohjauksella tarkoitetaan, että reititin voidaan määritellä vastaanottamaan tiettyyn porttiin osoitettu data reitittimen julkisesta osoitteesta ja siirtämään se ennalta määrättyyn lähiverkon IP-osoitteeseen. (Mattila 2010.)

Jotta porttien kautta päästään hallitsemaan videovalvontajärjestelmää, on käytettävä reitittimen julkista osoitetta, joka on 80.186.xxx.xxx. Julkinen osoite on lisäpalveluna otettu Elisan operaattorilta, joka soveltuu laitteiden etähallintaan. Julkinen osoite mahdollistaa sen, että reititin näkyy internetissä ja siihen voidaan yhdistää ulkoverkosta. Reititin saa julkisen osoitteen Elisan DCHP-palvelimelta, jonka osoite muuttuu aina kun reititin menee verkosta pois ja tulee verkkoon.

APN (Access Point Name) tarkoittaa, että 4G-reititin muodostaa yhteyden operaattorin mobiiliverkon ja julkisen internetin välille. Operaattori määrittele nämä asetukset ja päättää laitteelle oikean IP-osoitteen. (Hildenbrand 2017.)

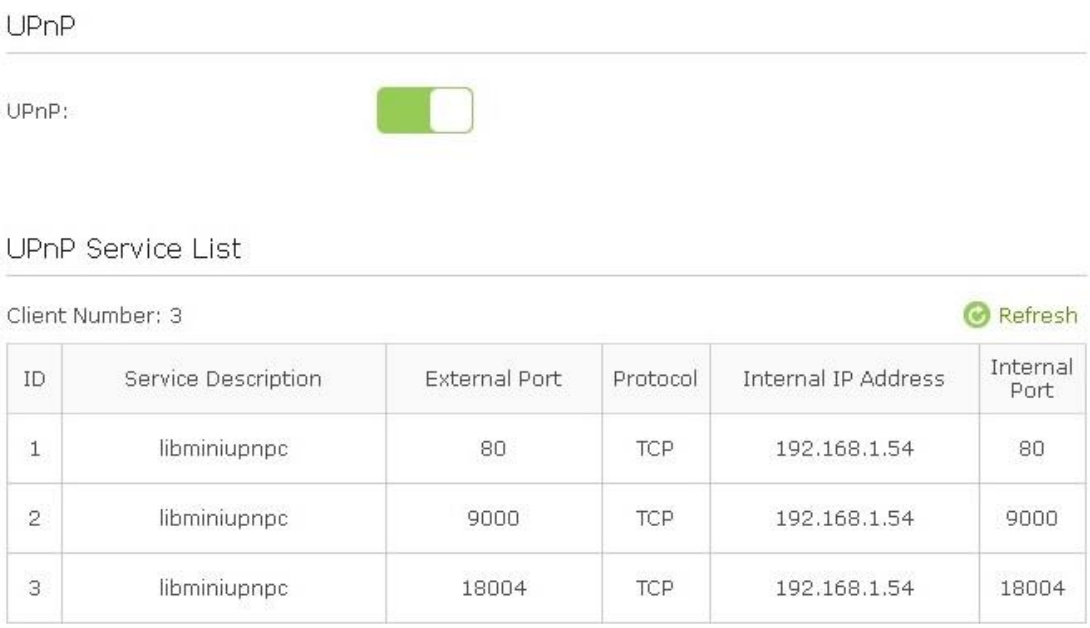
Julkinen osoite otetaan käyttöön reitittimessä määrittelemällä WAN:n (Wide Area Network) rajapinnassa APN:n tyypiksi staattinen ja APN:n nimeksi kirjoitetaan internet4. Tallentimessa määritellään portin automaattinen uudelleenohjaus eli UPnP (Universal Plug and Play), josta reititin näkee tallentimen avoimet portit ja reitittimessä täytyy myös olla UPnP päällä.

Reitittimen julkiseen osoitteeseen tuleva yhteys uudelleenohjataan portteihin, jossa tallentimen lähiverkon osoite on ja välitettävä liikenne siirretään TCP-protokollaa käyttäen.



Kuva 47. Tallentimen verkkomäärittelyt

Kuvassa 47 määritellään lähiverkon osoitteet käyttämällä DHCP:tä ja portit on määritelty automaattista portinohjausta käyttäen.



ID	Service Description	External Port	Protocol	Internal IP Address	Internal Port
1	libminiupnpc	80	TCP	192.168.1.54	80
2	libminiupnpc	9000	TCP	192.168.1.54	9000
3	libminiupnpc	18004	TCP	192.168.1.54	18004

Kuva 48. Reitittimestä määritelty UPnP päälle

Kuvassa 48 reitittimestä määritellään automaattinen porttiohjaus päälle, jolloin reititin saa tietoonsa tallentimen avoimet portit.

Tallentimen portit ovat 9000, 80, 18004. Portti 9000 on asiakasportti, jota voidaan etähallita tietokoneelta valvontajärjestelmän Surveillance Client-ohjelmalla.

3.2.1 Tallentimen hallinta Surveillance Client-ohjelmalla

Videovalvontajärjestelmän etähallintaa varten käytetään ohjelmaa Surveillance Client, joka asennettiin tallentimen mukana tulleelta CD-levyltä. Ohjelmaan määritellään reitittimen julkinen osoite tallentimen osoitteeksi ja portiksi 9000.

3.2.2 Tallentimen hallinta selaimella

Portti 80 on HTTP-portti, jota voidaan tietokoneella hallita selaimen kautta. Selaimeen kirjoitetaan reitittimen julkinen osoite ja sen perään kaksoispisteen jälkeen portin numero, joka on tässä tapauksessa 80.

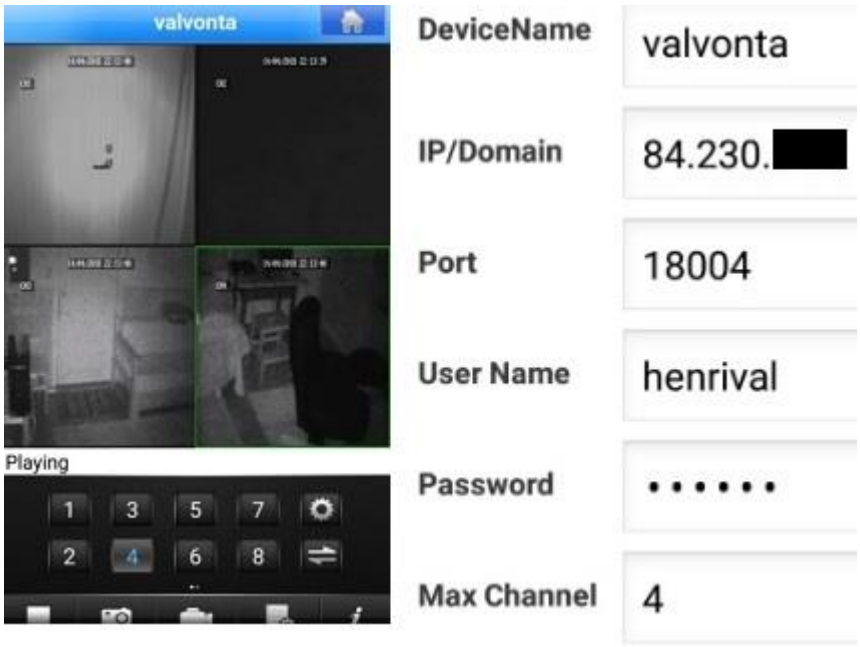
Jotta tallenninta voidaan hallita Google Chrome-selaimen kautta, on ladattava selaimeen IE Tab-laajennus. Kirjoitetaan IE Tab-osoiteriville http://84.230.xxx.xxx:80, jonka jälkeen tulee kirjautua tallentimeen ja tämän jälkeen voidaan katsoa kameran tallenteita tai muokata tallentimen asetuksia kuvan 49 mukaisesti.

Kuva 49. Tallentimen hallinta selaimella

3.2.3 Tallentimen hallinta Android-puhelimella

Portti 18004 on mobile-portti, jota käytetään esimerkiksi älypuhelimissa tai tableteissa valvontajärjestelmän etähallintaa varten.

Android-puhelimella tallentimen livekuvaa voidaan katsoa lataamalla Play-kaupasta ilmainen MEyePro-sovellus.



Kuva 50. Tallentimen määrittely Android-puhelimella

Käynnistetään MEyePro ja tehdään kuvan 50 mukaiset asetukset tallentimen lisäämiseksi. Nyt voidaan valita tallennin, joka määriteltiin ja katsoa tallentimen live-kuvaa kanavilta yhdestä neljään.

3.3 IPsec VPN-yhteyden määrittäminen

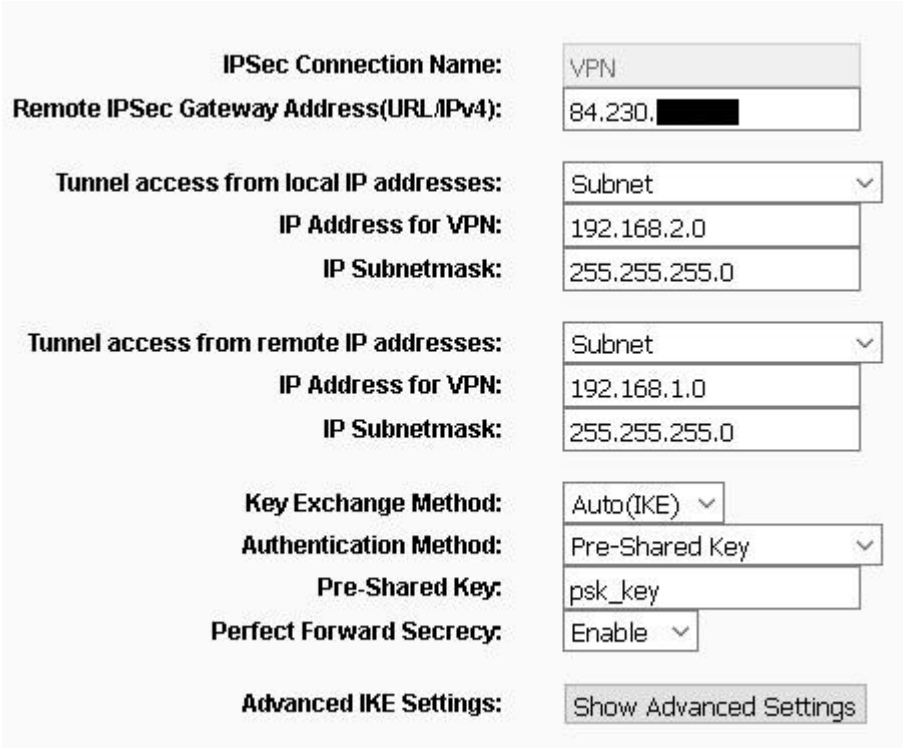
Tallentimen turvallinen etähallintayhteys on rakennettu IPsec VPN-tunneli Irjanteen ja Rauman reitittimien välille.

IPsec VPN-tekniikalla voidaan yhdistää kaksi paikallisverkkoa VPN-tunnelilla julkisen verkon (internet) ylitse. VPN suomennettuna tarkoittaa virtuaalista yksityistä verkkoa. IPsec tarkoittaa kryptograaffista suojattua yhteyttä IP-pakettikerroksessa. (Juniper www-sivut 2018.)

IPsec tukee automaattisesti avainten generointia ja kommunikointia avainten välillä. IPsec käyttää avainten vaihdossa IKE (Internet Key Exhange)-protokollaa. Autokey IKE ominaisuus jakaa ennalta avaimia ainoastaan autentikoiduilta osallisilta istunnon aikana. Molempien osapuolien täytyy käyttää samaa IKE-avainta yhteyden aikana. (Juniper www-sivut 2018.)

Kuva 51. IPsec VPN-yhteyden määrittely Irjanteen reitittimelle

Tehdään kuvan 51 mukaiset asetukset Irjanteen reitittimille. Kirjaudutaan Mozilla Firefox-selaimen kautta reitittimelle osoitteella 192.168.1.1, josta avataan Advanced ikkuna auki. Network valikosta valitaan IPsec VPN välilehti, josta tehdään tarvittavat määritykset. IPsec-yhteyden nimeksi annetaan VPN ja annetaan Raumalla olevan reitittimen julkinen osoite, joka on 91.158.xxx.xxx. VPN-yhteyteen pääsee Irjanteen aliverkon osoitteella 192.168.1.0 ja Rauman osoitteella 192.168.2.0. Avainten vaihtometodina käytetään Auto (IKE)-protokollaa ja todennusmetodina Pre-Shared Key. Liikenne ohjataan salattuna.

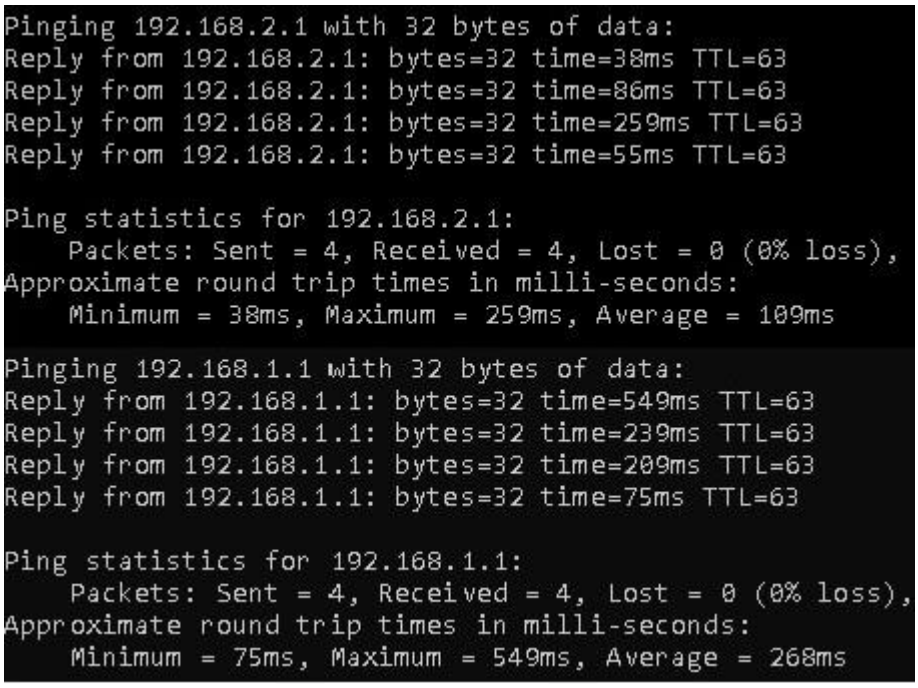


Kuva 52. IPsec VPN-yhteyden määrittely Rauman reitittimelle

Määritellään Rauman reitittimille yhteyden nimeksi VPN ja reitittimen julkiseksi osoitteeksi 83.230.xxx.xxx. VPN-yhteyteen pääsee Rauman aliverkon osoitteella 192.168.2.0 ja Irjanteen osoitteella 192.168.1.0. Rauman ja Irjanteen reitittimissä käytetään samaa avainta ja todennusmetodia.

Määrittelyiden jälkeen VPN-yhteys Rauman ja Irjanteen reitittimien välillä toimii. Tallentimen videokuvaa voidaan kopioida Raumalla sijaitsevaan tiedostopalvelimeen kryptatulla liikenteellä.

3.3.1 VPN-yhteyden testaus ping-komennolla

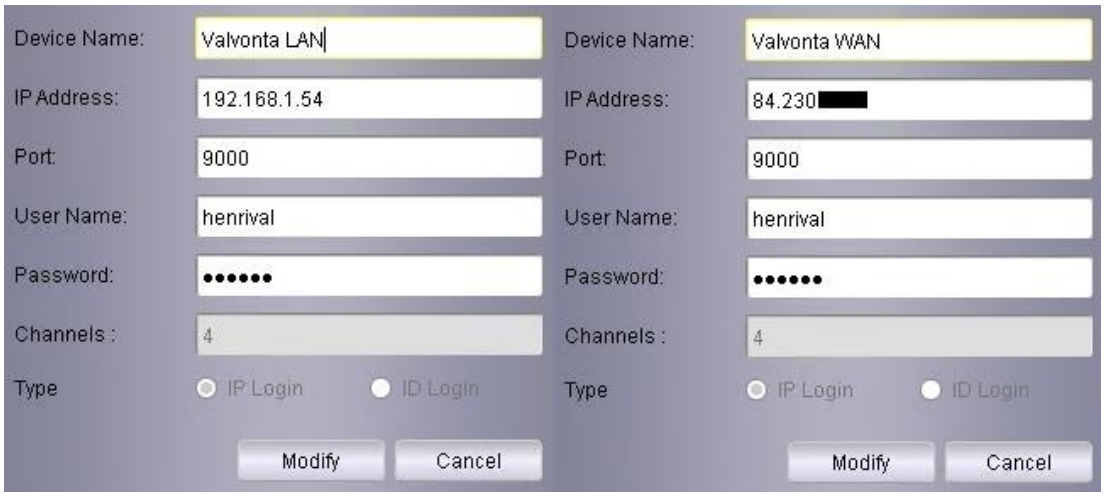


Kuva 53. VPN-yhteyden testaus Rauman ja Irjanteen verkon välillä

Kuvasta 53 todetaan, että VPN-yhteys toimii Irjanteen palvelimelta Rauman reitittimelle ja Rauman hallintakoneelta Irjanteen reitittimelle on lähetetty 4 pakettia ja ne kaikki ovat saapuneet perille.

3.4 Etähallinta

Tallenninta voidaan hallita hallintakoneelta IPsec VPN-yhteydellä Surveillance Client-ohjelmalla tai portinohjauksella mistä tahansa verkosta, jolloin esimerkiksi yhteys voi olla ulkomaan verkosta.



Kuva 54. Surveillance Client-ohjelmaan osoitteiden määrittely

Surveillance Client-ohjelmalla avataan Group Device ikkuna auki, josta lisätään kaksi tallenninta. Ensimmäiseen tallentimeen määritellään nimeksi valvonta WAN, joka käyttää reitittimen julkista osoitetta. Toiselle tallentimelle määritellään nimeksi valvonta LAN, joka käyttää tallentimen paikallisosoitetta. Tehdään kuvan 54 mukaiset asetukset.

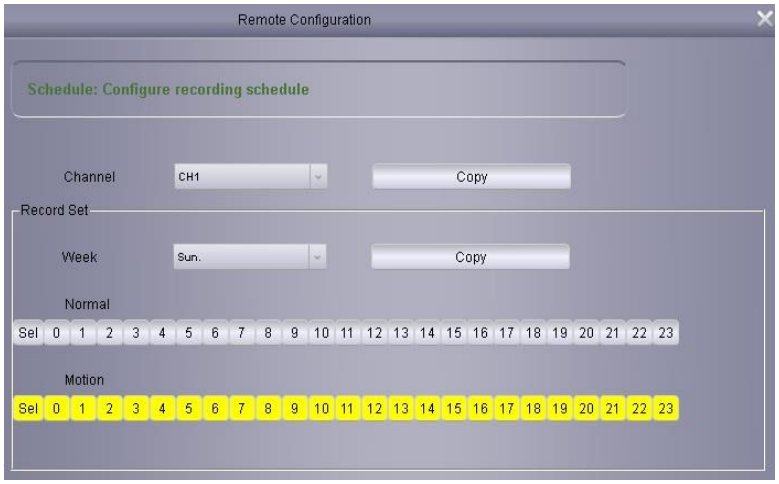
Kuva 55. Tallentimen lisäämien ryhmiin

Lisätään molemmat tallentimet omiin ryhmiinsä. Valvonta LAN lisätään Valvonta LAN-ryhmään, josta päästään hallitsemaan tallenninta paikallisosoitteella. Valvonta WAN lisätään Valvonta WAN-ryhmään, josta päästään hallitsemaan reitittimen julkisella osoitteella.

3.5 Tietoturvan määrittely

Tallentimeen on määritelty vahva käyttäjätunnus ja salasana etähallintaa varten. Reitittimestä on piilotettu ja otettu pois päältä langattomat yhteydet, jotka tekevät laitteeseen murtautumisen vaikeaksi. Reitittimen etähallinta on otettu pois käytöstä ja ainoa hallintayhteys reitittimeen on Ethernet-kaapelilla paikallisesti. Reitittimen oletussalasana on vaihdettu vahvempaan salasanaan, mikä tuo turvallisuutta. Irjanteen ja Rauman reitittimien välille on rakennettu IPsec VPN-yhteys, joka takaa videokuvan siirtymisen salattuna.

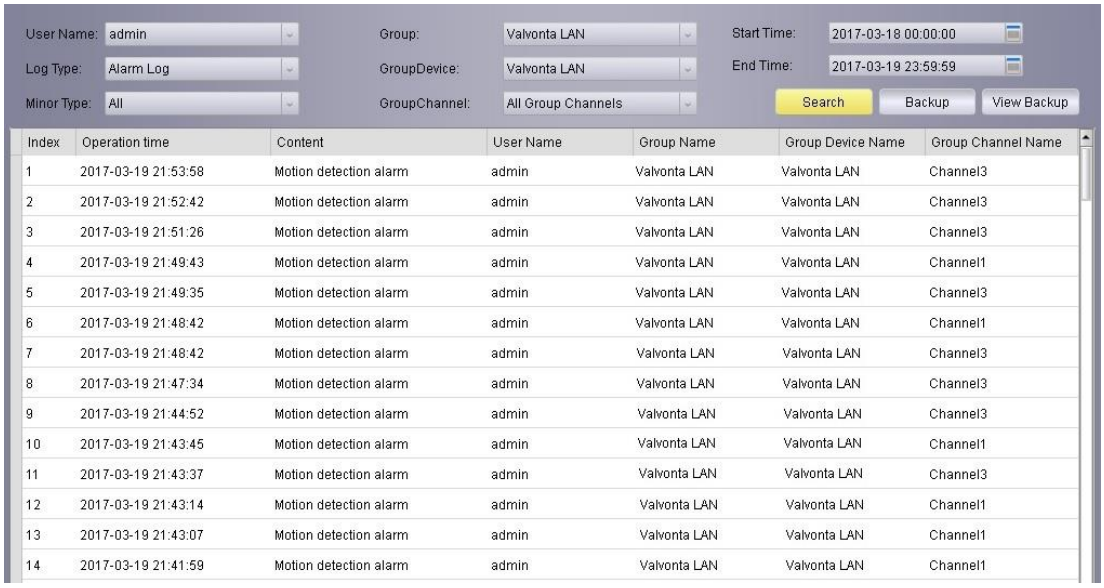
3.6 Kameroiden etähallinta



Kuva 58. Kameroiden määrittely

Kuvassa 58 ollaan etähallintayhteydessä valvontajärjestelmään, jossa määritellään kameroiden kanavien videon tallentamisen ajankohta ja liiketunnisteiden käyttö. Kanavapaikoilla yksi, kolme ja neljä olevat kamerat on määritelty tallentamaan kuvaa kaikkina ajanhetkinä liiketunnisteiden aktivoiduttua. Kanavapaikalla kaksi oleva kamera on määritelty tallentamaan kaikkina ajanhetkinä ilman, että liiketunnistus on päällä. Kanavapaikalla kaksi olevasta kamerasta on otettu liiketunnistus pois päältä, koska kameroiden liiketunnisteen kantama on noin 10 metriä, ja piha-aluetta kuvaavan kameran pitää pystyä tallentamaan koko aluetta.

3.7 Lokien hallintaa etäyhteydellä



Index	Operation time	Content	User Name	Group Name	Group Device Name	Group Channel Name
1	2017-03-19 21:53:58	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel3
2	2017-03-19 21:52:42	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel3
3	2017-03-19 21:51:26	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel3
4	2017-03-19 21:49:43	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel1
5	2017-03-19 21:49:35	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel3
6	2017-03-19 21:48:42	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel1
7	2017-03-19 21:48:42	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel3
8	2017-03-19 21:47:34	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel3
9	2017-03-19 21:44:52	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel3
10	2017-03-19 21:43:45	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel1
11	2017-03-19 21:43:37	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel3
12	2017-03-19 21:43:14	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel1
13	2017-03-19 21:43:07	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel1
14	2017-03-19 21:41:59	Motion detection alarm	admin	Valvonta LAN	Valvonta LAN	Channel1

Kuva 59. lokien tarkastelua etähallintayhteydellä

Kuvassa 59 on lokin tarkastelua, jossa pääkäyttäjä valitsee ryhmäksi Valvonta LAN ja ryhmän laitteeksi Valvonta LAN. Lokien tyypiksi valitaan hälytykset ja hälytyksien alatyypiksi valitaan All (kaikki), josta nähdään lokissa kameroiden kanavien 1 ja 3 liiketunnistimien havaitsemat hälytykset. Aikaväliksi valittiin kaksi päivää. Kyseiseltä aikaväliltä haetaan kaikki liiketunnistimen havaitsemat hälytykset.

Määrittelyjen jälkeen saadaan kyseisistä hälytyksistä lista, josta nähdään tarkka aika siitä, milloin liiketunnistin on havainnut liikettä ja minkä kameran kanavalta se on tullut.

3.8 Videovalvontajärjestelmän tallenteiden hallinta etäyhteydellä

Kuva 60. tallenteiden hallinta

Kuvassa 60 valitaan ryhmäksi Valvonta LAN ja tallentimeksi Valvonta LAN, jonka kanavilta valitaan kameroiden tallenteet. Tiedostotyypiksi valitaan kaikki, jotka pitävät sisällään kanavilta tulevat jatkuva- ja liiketunnisteiden välittävää videokuvaa. Videovalvontajärjestelmän tallenteet haetaan 13.3.2017, ja sen päivän ajalta kaikki videokuvatallenteet kaikilta kanavilta.

Tallentimen videokuva jakaantuu neljään eri ikkunaan omille kanavilleen yhdestä neljään. Tallenteiden videokuvan ajankohta näkyy punaisina palkkeina, milloin liiketunnistus menee päälle ja pois päältä. Kamera, jossa on liiketunnistus määritelty pois päältä, näkyy tallenteessa vihreänä palkkina eli videokuvaa on nauhoitettu jatkuvana.

Kanavien videolla nähdään mihin kellonaikaan kamera on ottanut videota. Kanavat kaksi ja neljä kuvaavat normaalia kuvaa. Kanavien yksi ja kolme kameroilla on mennyt LED-infrapunavalo-ominaisuus päälle, koska kuvattavalla alueella on liian hämärää ja videokuva näkyy mustavalkoisena.

Tallentimen prosessorin kuormitus näkyy vihreänä palkkina ja kuormituksen lisääntyessä palkit muuttuvat vihreästä punaisiksi.

3.9 Videovalvontajärjestelmän kiintolevyn hallinta ja uudelleenkäynnistys

Tallentimen kiintolevyltä voidaan monitoroida monia eri asioita. Kiintolevyn kunnon tilaa voidaan tarkastella, onko se kunnossa, vai täytyykö vaihtaa levyä. Kiintolevyn vapaan muistin määrää ja aikaa tunneissa voidaan tarkkailla. Voidaan määritellä, alustetaanko kiintolevy manuaalisesti tyhjäksi kerralla tai käytetäänkö automaattista ylikirjoitusta. Muistin täyttyessä määritellään automaattisesti tallenteiden ylikirjoitus, joka ylikirjoittaa vanhempien tallenteiden päälle. Kiintolevyn hallintaa voidaan toteuttaa ainoastaan paikallisesti, ei etähallinnalla.

Valvontajärjestelmässä määritellään uudelleenkäynnistyksen oikeudet ainoastaan pääkäyttäjälle. Uudelleenkäynnistys on määritelty automaattiseksi jokaisen viikon sunnuntaina kello 00.00. Järjestelmä käynnistyy uudelleen hallitusti. Menetelmällä voidaan esimerkiksi korjata kanavien videokuvien tallentumisen virheet.

3.10 Etäyhteyden testaaminen

Kuva 61. porttien tarkastus

Kuvassa 61 tarkastetaan, että asiakas-, mobiili- ja HTTP-portit ovat auki. Voidaan todeta, että internet näkee valvontajärjestelmän avoimien porttien kautta ja dataliikenne on mahdollista verkon yli.

Käytetään porttien tarkastamiseen selaimessa toimivaa canyouseeme.org-sivun porttien tarkastustyökalua, joka on ilmainen ohjelma. Ohjelmalla varmistetaan, että portin uudelleenohjaus toimii ja voidaan tarkastaa, onko palvelu käynnissä vai onko palomuuri tai palveluntarjoaja estänyt liikenteen ohjautumisen tiettyihin portteihin. (Canyouseeme www-sivut 2017.)

3.11 Videovalvontajärjestelmän liikenteen monitorointia Wiresharkilla

Source	Destination	Protocol	Length	Info
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54046 [ACK] Seq=2908389 Ack=1 Win=7300 Len=1406
192.168.2.105	192.168.1.54	TCP	54	54046 → 9000 [ACK] Seq=1 Ack=2909795 Win=32768 Len=0
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54044 [ACK] Seq=2903883 Ack=1 Win=7300 Len=1406
192.168.2.105	192.168.1.54	TCP	54	54044 → 9000 [ACK] Seq=1 Ack=2905289 Win=32768 Len=0
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54044 [ACK] Seq=2905289 Ack=1 Win=7300 Len=1406
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54045 [ACK] Seq=1059911 Ack=1 Win=7300 Len=1406
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54046 [ACK] Seq=2909795 Ack=1 Win=7300 Len=1406
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54047 [ACK] Seq=2917521 Ack=1 Win=7300 Len=1406
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54047 [ACK] Seq=2918927 Ack=1 Win=7300 Len=1406
192.168.2.105	192.168.1.54	TCP	54	54047 → 9000 [ACK] Seq=1 Ack=2920333 Win=32768 Len=0
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54044 [ACK] Seq=2906695 Ack=1 Win=7300 Len=1406
192.168.2.105	192.168.1.54	TCP	54	54044 → 9000 [ACK] Seq=1 Ack=2908101 Win=32768 Len=0
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54045 [ACK] Seq=1061317 Ack=1 Win=7300 Len=1406
192.168.2.105	192.168.1.54	TCP	54	54045 → 9000 [ACK] Seq=1 Ack=1062723 Win=32768 Len=0
192.168.1.54	192.168.2.105	TCP	216	9000 → 54045 [PSH, ACK] Seq=1062723 Ack=1 Win=7300 Len=162
192.168.1.54	192.168.2.105	TCP	450	9000 → 54047 [PSH, ACK] Seq=2920333 Ack=1 Win=7300 Len=396
192.168.1.54	192.168.2.105	TCP	1146	9000 → 54046 [PSH, ACK] Seq=2911201 Ack=1 Win=7300 Len=1092
192.168.2.105	192.168.1.54	TCP	54	54046 → 9000 [ACK] Seq=1 Ack=2912293 Win=32768 Len=0
192.168.1.54	192.168.2.105	TCP	762	9000 → 54044 [PSH, ACK] Seq=2908101 Ack=1 Win=7300 Len=708
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54046 [ACK] Seq=2912293 Ack=1 Win=7300 Len=1406
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54047 [ACK] Seq=2920729 Ack=1 Win=7300 Len=1406
192.168.2.105	192.168.1.54	TCP	54	54047 → 9000 [ACK] Seq=1 Ack=2922135 Win=32768 Len=0
192.168.1.54	192.168.2.105	TCP	1460	9000 → 54044 [ACK] Seq=2908809 Ack=1 Win=7300 Len=1406
192.168.2.105	192.168.1.54	TCP	54	54044 → 9000 [ACK] Seq=1 Ack=2910215 Win=32768 Len=0
192.168.2.105	192.168.1.54	TCP	54	54045 → 9000 [ACK] Seq=1 Ack=1062885 Win=32747 Len=0

Kuva 62. videovalvontajärjestelmän liikenteen monitorointia

Kuvassa 62 monitoroidaan hallintakoneen ja valvontajärjestelmän välillä olevaa suoratoistona tulevaa videokuvaa. Kuljettava protokolla on TCP. Kohdepäässä oleva hallintatietokone osoitteella 192.168.2.105 vastaa videovalvontajärjestelmän pyyntöihin osoitteeseen 192.168.1.54 ACK- ja PSH-sanomilla.

ACK-sanoma ilmoittaa, että kuittausnumero on oikea. PSH-sanomalla selvitetään, että tällä bitillä TCP:n käyttäjä voi vaatia kaiken puskurissa olevan datan lähetyksen, jos esimerkiksi datavirrassa on looginen tauko; vastaanottopäässä menettely on vastaava. (Kaario 2002, 169.)

3.12 Videovalvontajärjestelmän vianhakua ja huoltotyöt

Valvontajärjestelmään yhteys voi mennä poikki monestakin syystä. Yhteyttä lähdetään testaamaan pingillä valvontajärjestelmän reitittimeen päin. Jos yhteys reitittimeen toimii, niin vika voi olla esimerkiksi se, että tallennin on sammunut, jolloin kytketään tallentimeen virta takaisin päälle. Portinohjaus ei toimi tallentimessa tai reitittimessä, jolloin tarkistetaan portinohjaus reitittimestä tai tallentimesta, ja määritellään uudelleen portinohjaus. Jos verkkokaapeli on vioittunut tallentimen ja reitittimen välissä tai tallennin on ”tiltannut”, jolloin korjauskeino on ollut verkkokaapelin vaihtaminen uuteen.

Tiedostopalvelin lakkaa toimimasta tai sammuu, jolloin korjauskeinona on tiedostopalvelimen uudelleenkäynnistys ja IP-osoitteen tarkistus.

Laitteiden yhtäaikainen sammuminen voi johtua siitä, että UPS on jostain syystä mennyt akku tilaan ja akkujen loputtua UPS on lopettanut virransyötön laitteille. Tarkistetaan, onko talon sähkökaapista mennyt sulake ja jos on, niin vaihdetaan ehjä sulake. Sammutetaan UPS, käynnistetään se uudelleen ja katsotaan, syttyykö On Line-valo päälle.

DNS ja DHCP-palvelimen kaatumisen seurauksena tallennin menettää IP-osoitteen, jolloin tallentimeen ei ole enää internetyhteyttä. Korjauskeinona on ESXi:n virtuaalikoneen sammuttaminen ja ESXi:n uudelleenkäynnistys. Käynnistetään ESXi ja virtuaalikone uudelleen ja tarkastetaan, että tallennin on saanut IP-osoitteen DHCP-palvelimelta ja on internetyhteydessä.

Jos yhteys ei pingillä toimi reitittimeen, niin syynä voi olla esimerkiksi reitittimen osoitteen vaihtuminen sähkökatkoksen seurauksena, jolloin korjauskeinona on reitittimen IP-osoitteen määrittäminen uudelleen Surveillance Client-ohjelmalla tallentimelle.

4 VIDEOVALVONTAJÄRJESTELMÄN SOVELLUTUKSET

4.1 Videovalvontajärjestelmän käyttösovellutukset

Videovalvontajärjestelmän tarkoitus on tuoda iäkkäälle vanhuksella turvallisuuden tunnetta, estää ulkopuolisten tunkeutuminen tontille ja vanhuksen terveydentilan tarkkailu, esimerkiksi erilaiset sairauskohtaukset ja karkaamiset.

Kyltillä ilmoitetaan muille, että talossa ja talon ulkopuolella on tallentava videovalvonta.

Valvontajärjestelmän yleisiä käyttösovellutuksia ovat esimerkiksi huoltoaseman kameravalvonta, jossa tavoitteena on tunnistaa bensaa varastavat henkilöt ja heidän käyttämänsä ajoneuvo; taksin kameravalvonta, jossa on tarkoituksena suojata yksin työskentelevää ajajaa omaisuus- ja väkivaltarikoksilta; kaupunkien kameravalvonta, jossa on tarkoitus lisätä kansalaisten turvallisuutta levottomiksi koetuissa paikoissa, ennalta ehkäistä ilkivalta ja muita rikoksia yleisillä paikoilla. (Ellonen ym. 2011, 62.)

4.2 Erilaiset videovalvontajärjestelmäratkaisut

Valvontajärjestelmä voidaan toteuttaa monilla erilaisilla valvontakameraratkaisuilla esimerkiksi kiinteillä sisäkameroilla, jotka kuvaavat aina samaa vakioitua kuvausaluetta ja on tarkoitettu käytettäväksi rakennusten sisätiloissa. Voidaan myös käyttää kiinteitä ulkokameroita, jotka on varustettu lämmitetyllä sääsuojakotelolla ja jotka on tarkoitettu ulkokäyttöön. PTZ (Pan Tilt Zoom)-kameroissa on sama varustetaso kuin ulkokameroilla ja niissä on moottoroitu kääntöpää, joka pyörii akselinsa ympäri 360 astetta ja kääntyy ylös ja alas. Kiinteissä kupukameroissa kameran objektiivi on sijoitettu kirkkaseen tai tummaan akryylikupuun ja objektiivina käytetään zoomattavaa objektiivia. (Ellonen ym. 2011, 22.)

Valvontajärjestelmissä voidaan käyttää monenlaisia eri tallenninmalleja, esimerkiksi DVR:ta, joka tarkoittaa digitaalista videotallenninta ja on tarkoitettu analogisten ka-

meroiden kuvan tallentamiseen. NVR (Network Video Recorder) tarkoittaa verkkovideotallenninta ja on tarkoitettu IP-kameroiden kuvan tallentamiseen. Hybrid DVR:lla, voidaan tallentaa samanaikaisesti sekä analogisten että IP-kameroiden kuvaa. (Ellonen ym. 2011, 22.)

Opinnäytetyössä käytettävässä videovalvontajärjestelmässä on kiinteitä ulkokameroita, jotka toimivat sisällä ja ulkona ja ovat myös hintansa puolesta halvempia kuin PTZ-kamerat. Tallenninvaihtoehdoksi on valittu DVR, koska sillä voidaan tallentaa videokuvaa ilman verkkoyhteyttä toisin kuin NVR-tallentimella, joka vaatii toimiakseen jatkuvan verkkoyhteyden.

5 YHTEENVETO

Videovalvontajärjestelmä kokonaisuudessaan toimii moitteettomasti, mutta katson järjestelmässä silti olevan parantamisen varaa.

Kehittäisin järjestelmän verkkoa parantamalla Irjanteen reitittimen 4G-signaalin laatua ja nopeutta asentamalla ulkoiset 4G-antennit talon katolle tolppaan ja kytkisin antennin johdot reitittimelle, jolloin signaalin laatua saisi kasvatettua ja nostettua verkon nopeutta.

Korvaisin Rauman ADSL-verkon 4G-verkolla, joka tuo vakaamman ja nopeamman yhteyden reitittimien välille, jolloin nauhoitukset NAS:lle tulisivat kokonaisina tallenteina eikä osina, joka tarkoittaa sitä, että tallenteiden välistä puuttuu tunteja.

Hallintakoneen ja reitittimen välisen langattoman siirtoyhteyden korvaisin Ethernet-kaapelilla, joka nopeuttaisi yhteyden ottamista NAS:iin ja tallentimeen.

Tallentimeen ja tiedostopalvelimeen lisäisin enemmän kiintolevyn muistia, joka mahdollistaisi useamman kuukauden videokuvan tallentumisen.

Vanhuksen turvallisuutta lisäisin vaihtamalla neljä kanavaisen tallentimen kahdeksan kanavaiseen tallentimeen, mihin saisin kytkettyä kahdeksan kameraa. Lisäkameroilla saisin kuvattua enemmän kohtia asunnosta, jolloin katvealueiden määrä pienesi nykyisestä ja näköyhteys vanhukseen säilyisi jatkuvana.

Tallentimen monitorin korvaisin teräväpiirtomonitorilla HDMI (High Definition Multimedia Interface)-liitännöillä, mikä mahdollistaa videokuvien katsomisen tarkemmalla 1920x1080-resoluutiolla.

Suosittelen rakentamaani järjestelmää osaksi vanhusten kotihoitoa.

LÄHTEET

Aalto, S. Hovinen, R. Kuisma, L. Kylä, H. Lehtonen, R. Leskinen, M. Marttila, H. Lehtonen, R. Leskinen, M. Marttila, H. Marttila, J. Seppänen, J. & Vuonoranta, E. 2009. Kameravalvontajärjestelmät. 4. uud. P. Espoo: Sähköinfo Oy.

Aelius www-sivut. Viitattu 17.4.2018. https://www.aelius.com/njh/subnet_sheet.html

APC user's manual www-sivut. Viitattu 17.4.2018. http://www.apc.com/sales-tools/ASTE-6Z7V3E/ASTE-6Z7V3E_R0_EN.pdf

Canyouseeme www-sivut. Viitattu 22.3.2017. https://canyouseeme.org

Dadkhah Rasmussen, H. 2018. Mikä on DNS-palvelin. Viitattu 17.4.2018. http://koti-mikro.fi/internet/mika-on-dns-palvelin

Davis, D. 2007. What is the difference between a role and a feature when customizing your Windows 2008 server. Viitattu 17.4.2018. http://techgenix.com/whatisthedifferencebetweenaroleandafeaturewhencustomizingyourwindows2008server/

E. Alvarez, A. 2016. DNS forwarding and conditional forwarding. Viitattu 17.4.2018. https://medium.com/tech-jobs-academy/dns-forwarding-and-conditional-forwarding-f3118bc93984

Ellonen, V. Kauppi, V. Kinnunen, H. Käyhkö, P. Laitinen, J. Lehtikangas, M. Lehtinen, T. Lehtonen, R. Pänkäläinen, A. Pöysä, H. Sallinen, P. Starck, K. & Woitsch, P. 2011. Kameravalvontaopas. Espoo: Sähköinfo Oy.

Google public DNS www-sivut. Viitattu 16.4.2018. https://developers.google.com/speed/public-dns/?csw=1

Google public DNS www-sivut. Viitattu 16.4.2018. https://developers.google.com/speed/public-dns/docs/security

Hastings,.N. 2017. differences between ethernet cables. Viitattu 16.4.2018. https://www.digitaltrends.com/computing/differences-between-ethernet-cables/

Hildenbrand, J. 2017. What is an APN, and how do I change it. Viitattu 17.4.2018. https://www.androidcentral.com/what-apn-and-how-do-i-change-it

Jaimeo & Poggemeyer, L. 2017. Install server with desktop experience. Viitattu 17.4.2018. https://docs.microsoft.com/en-us/windows-server/get-started/getting-started-with-server-with-desktop-experience

Juniper www-sivut. Viitattu 17.4.2018. https://www.juniper.net/documentation/en_US/junos/topics/concept/vpn-security-overview.html

Kaario, K. 2002. TCP/IP -verkot. Jyväskylä: Docendo Finland Oy.

Kataja, J. 2015. Mikä on palvelunestohyökkäys. Viitattu 16.4.2018. https://www.zoner.fi/mika-on-palvelunestohyokkays/

Mattila, M. Valvontakameran nettikäyttö-osa 1. Viitattu 10.3.2017. http://mattimattila.fi/valvontakameran_nettikaytto_osa_1.html

Microsoft docs www-sivut. Viitattu 17.4.2018. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc940018(v=technet.10)

Mozilla support www-sivut. Viitattu 17.4.2018. https://support.mozilla.org/fi/kb/troubleshoot-SEC_ERROR_UNKNOWN_ISSUER

Rouse M. 2015. Network attachment storage (NAS). Viitattu 17.4.2018. https://searchstorage.techtarget.com/definition/network-attached-storage

Rouse, M. 2010. 4G (fourth-generation wireless). Viitattu 23.4.2018. https://searchmobilecomputing.techtarget.com/definition/4G
Rouse, M. 2015. Disk striping. Viitattu 17.4.2018. https://searchstorage.techtarget.com/definition/disk-striping

Schneider-Electric. 2017. Adjusting Input Sensitivity on Back-UPS RS/XS Towers | Schneider Electric Support. Viitattu 17.4.2018. https://www.youtube.com/watch?v=as9_d01b6_k

Techopedia www-sivut. Viitattu 23.4.2018. https://www.techopedia.com/definition/5267/asymmetric-digital-subscriber-line-adsl

Tokopedia www-sivut. Viitattu 17.4.2018. https://www.tokopedia.com/upsku/ups-apc-rs1000i-br1000i-tanpa-baterai

Torres, G. 2012. Everything you need to know about the intel virtualization techology. Viitattu 16.4.2018. http://www.hardwaresecrets.com/everything-you-need-to-know-about-the-intel-virtualization-technology/

Warner, T. 2016. How to enable remote desktop in windows server 2016. Viitattu 17.4.2018. http://www.tomsitpro.com/articles/enable-remote-desktop-in-windows-server-2016,2-1102.html

Web-opas www-sivut. Viitattu 17.4.2018. http://www.webopas.net/dhcp.html

Viljanen, V. 2013-2017 DNS. Viitattu 12.3.2017. https://www.yksityisyydensuoja.fi/dns

Vähimaa, A. 2017. Miten virtuaalikone toimii? Asenna XP, Linux tai testaa haittaojelmia turvallisesti omalla PC:llä. Viitattu 16.4.2018. https://www.mikrobitti.fi/2017/09/miten-virtuaalikone-toimii-asenna-xp-linux-tai-testaa-haittaohjelmia-turvallisesti-omalla-pclla/

Ylä-Jääski, V. 2012. Tm vertailu ups laitteet. Viitattu 17.4.2018. https://tekniikanmaailma.fi/tm-vertailu-ups-laitteet/