Sami Suomalainen

Tietoliikenneyhteydet kiinteistöautomaation ylläpitotoiminnassa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

28.5.2021

Tiivistelmä

Tekijä:	Sami Suomalainen
Otsikko:	Tietoliikenneyhteydet kiinteistöautomaation ylläpitotoiminnassa
Sivumäärä:	33 sivua
Aika:	28.5.2021
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Tietoverkot
Ohjaajat:	Janne Salonen

Tämän opinnäytetyön aiheena on tietoliikenneyhteydet kiinteistöautomaation ylläpitotoiminnassa. Työ toteutettiin Noatek Oy:lle. Tarkoituksenani oli tutkia osana työtehtäviäni, miten nykyaikaiset tietoliikennejärjestelmät tukevat olemassa olevia valvontakamerajärjestelmiä ja miten niitä voitaisiin kehittää. Salassapitovelvoitteiden takia opinnäytetyöni on tutkiva, eikä se sisällä työtehtävieni materiaaleja.

Opinnäytetyöni rakentuu nykyaikaisten tietoliikennetekniikoiden, näiden tekniikoiden toimintaan sekä niiden tietoturvaan. Pääasiallisena tutkimuslähteenäni käytin kirjallista materiaalia, käyn opinnäytetyössäni läpi erityisesti vielä nykyäänkin jatkuvasti kehittyvää WLAN-teknologiaa, radioverkkojen laitteistovaatimuksia sekä tietoturvaa. Opinnäytetyöni käsittelee myös langattomien lähiverkkojen standardoituja sekä lupavapaita WLAN-verkkojen taajuuksia. Tutkin opinnäytetyöni aikana nykyaikaisten tietoliikennetekniikoiden tietoturvaa, sen merkitystä järjestelmissä sekä sen vaikutusta järjestelmiin.

Opinnäytetyöni lopputuloksena oli laaja-alainen tutkiva raportti nykyaikaisten tietoliikennetekniikoiden hyödyntämisestä tämän päivän kiinteistöautomaatiossa, erityispiirteenä kameravalvontajärjestelmät sekä radioverkkoteknologiat.

Opinnäytetyöni alkuperäinen tarkoitus oli oppia ymmärtämään, miten opintojeni aikana saamiani oppeja luonnontieteiden parissa voitaisiin jatkojalostaa työelämän tarpeisiin. Koen itse saaneeni paljon varsinkin WLAN-tekniikoihin tutustuessani. Radioverkkoteknologia kiinnosti aihealueena itseäni jo entuudestaan, mutta opinnäytetyöni aikana kehityin näiden parissa erityisen paljon.

Avainsanat: Tietoliikenne, tietoliikenneyhteydet, automaatiotekniikka, kiinteistöautomaatio, tietoturva

Abstract

Author:	Sami Suomalainen
Title:	Telecommunications in building automation maintenance
Number of Pages:	33 pages
Date:	28th May 2021
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Data networks
Instructors:	Janne Salonen, Head of School

This thesis describes the telecommunications networks in building automation maintenance. The thesis was conducted for a company called Noatek Ltd. The aim of the final year project was to carry out a study about the most common telecommunicating-, wireless network-, virtual private network and other cyber security techniques, and adapt the techniques to CCTV camera systems and at the same time enhance, develop, and add value for the company systems.

This thesis describes information about modern data network technique protocols, and cyber security. The thesis discusses network techniques as TCP/IP, wireless networks, wireless networks frequency ranges and devices in the WLAN-networks. The thesis also includes information about protected remote desktop techniques such as virtual private networks and SSH.

In conclusion, the thesis guidance to security technology employees. The thesis shows how to data network structures work and what employees should consider before they start planning new data networks or security technology systems.

Keywords: Data networks, security technology, building automation, cyber security

Sisällys

Lyhenteet

PoE: *Power over Ethernet*. Tekniikka, jolla ethernet-lähiverkkoon yhdistettävälle laiteelle saadaan käyttöjännite.

PTZ: Pan Tilt Zoom. Valvontakamera tyyppi, jolla on mahdollista kuvata laajoja kuva-aloja.

SSH Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.

VPN Virtual Private Network. Virtuaalinen erillisverkko.

IETF Internet Engineering Task Force. Internetprotokollien standardoinnista vastaava organisaatio.

OSI Open Systems Interconnection Reference Model. Kuvaaja TCP/IP-verkoissa tapahtuvalle tiedonsiirrolle.

IEEE Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.

ISO International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.

WLAN Wireless Local Area Network. IEEE 802.11 -standardin mukainen langaton lähiverkkojärjestelmä.

LLC Logic Link Control. IEEE 802-verkojen yhteinen osa siirtoyhteyskerrosta.

IBM International Business Machines Corporation. Teknologia-alan yritys.

1 Johdanto

Opinnäytetyön toimeksiantajana oli Noatek Oy. Noatek Oy on vuonna 2010 perustettu turvallisuus- ja tietoliikennetekniikan ratkaisujen ja palveluiden tuottaja. Yritys on erikoistunut turvallisuus-, tietoliikenne- ja teollisuusautomaatioalan asiantuntijatehtäviin sekä projektipalveluihin. Noatek Oy toteuttaa turvallisuusteknisiä ratkaisuja kuten kameravalvonta-, rikosilmoitin- ja kulunvalvontajärjestelmät sekä niihin liittyvät tiedonsiirto- ja tietoliikennetekniikkaratkaisut. Monipuolisen toimialaosaamisen johdosta Noatek Oy pystyy tuottamaan ratkaisuja niin energia-alan, kiinteistöjen, kuin eri teollisuuden toimialojen tarpeisiin.

Työn tavoitteena oli toteuttaa tekninen ohjeistus nykyaikaisten tietoliikennejärjestelmien toiminnasta ja sisällyttää siihen erityispiirteenä kameravalvontajärjestelmät sekä niiden käyttö kiinteistöautomatiikassa. Noatekin asiakassuhteiden joukossa oli opinnäytetyötäni toteutettaessa suuria kotimaisia energia-alan yrityksiä. Salassapitovelvollisuuksien takia jouduin jättämään yrityksen virallisia teknisiä dokumentointeja opinnäytetyöstäni pois. Ne on korvattu itse toteuttamillani esimerkkikuvilla lähdemateriaaliin nojaten.

Tässä insinöörityöraportissa esitellään ensin kiinteistöautomaatiotekniikan perusta, sekä mitkä ovat sen osa-alueet. Samalla johdetaan siirtyminen kameravalvontajärjestelmien tekniikkaan sekä järjestelmien rakenteeseen. Insinöörityönraportin loppuosa käsittelee suojattuja etäyhteysprotokollia.

Raportin lopuksi teen yhteenvedon itseäni askarruttaneista aiheista, miten onnistuin täyttämään omat tavoitteeni sekä millaisia asioita opin raportin toteuttamisen aikana.

2 Automaatiotekniikka

.

2.1 Kiinteistöautomaatio

Kiinteistöautomaation tehtävänä on ohjata kiinteistön automatisoituja teknisiä ratkaisuja kiinteistön omistajan haluamalla tavalla. Nykyaikaiset kiinteistöautomaatio sovellukset pyrkivät lähtökohtaisesti toimimaan energiatehokkaasti mahdollisuuksien mukaan ilman, että omistajan tarvitsee itse koskea säädettyihin arvoihin. Kiinteistöautomaationtekniikkaan kuuluvat kiinteistön lämmitys-, valaistus, ilmanvaihto-, vesi-, hissi- sekä hälytinjärjestelmät, jotka ovat yleisimmin erotettuna muusta kiinteistön automaatiojärjestelmästä omaksi järjestelmäkseen, mahdollisten vika- ja hälytystilojen takia. Kiinteistöautomaation tärkeimpiä ominaisuuksia ovat seuraavat.

- asetusten sekä arvojen säätäminen halutun kaltaisiksi olosuhteiden mukaan
- asetusten seuranta ja valvonta, pyydetyissä arvoissa pysyminen sekä vikailmoitusten tekeminen, mikäli on tarvetta
- hälytysjärjestelmän tietojen kerääminen sekä mahdollisen hälytyksen käynnistyessä toimia, kuten järjestelmälle on asetuksiin merkitty.

Kiinteistöautomaation järjestelmien piiriin eivät kuulu pelkästään asuintalojen automaatio. Samoja sovelluksia hyödynnetään myös virastojen, koulujen ja teollisuuslaitosten toimintojen ylläpidossa. Teknisen toteutuksen laatu ja sitä kautta järjestelmien kustannuserot ovat kumminkin merkittäviä, kun mietitään asuin- ja virastotalojen kiinteistöautomaatiojärjestelmien toiminnallisia eroja. Kiinteistön koko on yksi suurimmista vaikuttajista kiinteistöautomaation sovellusten kustannuksiin. Kiinteistön lämmitysjärjestelmät tarvitsevat paljon energiaa ja tästä johtuen niiden suunniteluun sekä optimointiin haluttuun ympäristöön käytetäänkin aikaa, kunnollisella selvitystyöllä ja suunnittelulla voidaan saavuttaa hyvä energiatehokkuus. Kiinteistöautomaation tuoma hyöty energiatehokkuuteen on mer-

kittävä ja yksi tärkeimmistä syistä sen sovellusten kehittämiseen tulevaisuudessakin. Tarpeenmukaisella käytöllä voidaan saavuttaa suuriakin hyötyjä pitkällä aikavälillä, kun järjestelmä on konfiguroitu oikein. Tarpeenmukaisella käytöllä tarkoitetaan teollisuuslaitosten ja virastotalojen ollessa kyseessä sitä, että kiinteistöjen ollessa suljettuna, ei ole tarvetta pitää ilmanvaihto- sekä valaisinjärjestelmiä turhaan päällä. [1.]

2.2 Kamerajärjestelmän käyttö

Valvontakamerajärjestelmien käyttö on yleistynyt paljon nykyaikana, kameroiden alhaiset hinnat, tekniikan kehittyminen sekä käyttökohteiden lisääntyminen ovat tehneet sen, että valvontakameroiden hyödyntäminen niin teollisuuden- ajoneuvojen- kuin raskaidenkoneidenkin tarpeisiin on normaalia. Kameroiden tarjoamien teknisten etujen vuoksi niiden käyttö on tehokas keino ehkäistä niin vandalismia, työtapaturmia kuin järjestyshäiriöitäkin. Kamerajärjestelmien hyödyntäminen kasvaa jatkuvasti teollisuudessa, kamera, kun ei väsy toisin kuin ihminen sen katseen ollessa lukittuna tiettyyn kohteeseen. Kameroita hyödynnetään osana konenäköä, konenäköä käytetään teollisuudessa laadunvalvonnassa sekä vikatilanteiden havainnoinnissa. Automatisoitujen linjastojen ohjauksen sekä vikatilojen korjauksen hoitavat jo nykyään konenäköjärjestelmät. Näin virheiden määrä laskee ja niiden havainnointi nopeutuu, lopputuotteiden laadun parantuessa myös konenäköjärjestelmien kiinnostus kasvaa ja järjestelmien kehittämiseen käytetään enemmän resursseja. [2.]

Kamerajärjestelmien sekä konenäön hyödyntäminen on myös yleistynyt raskaidenkoneiden kuten metsäkoneiden sekä ajoneuvojen turvallisuuden kehittämisessä. Metsäkoneen kuljettajan näkyvyys voi olla hyvinkin heikko ohjaamosta katsottuna, kamerajärjestelmien avulla näkyvyyttä saadaankin parannettua koneen runkoon kiinnitettyjen kameroiden avulla, jolloin kuljettajan on helpompi hahmottaa ympäristöä. Näkyvyyden parantuessa myös työtapaturmien määrä vähenee ja yleinen työhyvinvointi kasvaa. [3.] Ajoneuvoyhdistelmien turvallisuutta on kehitetty kamerajärjestelmien avulla, kamerajärjestelmien avulla on pystytty parantamaan kuljettajien havainnointia liikenteessä sekä parantamaan

näkyvyyttä. Kamerajärjestelmien kehittyminen sekä sen sovellusten kehittäminen ajoneuvoihin on parantanut liikenneturvallisuutta sekä ajomukavuutta, kamerasovellusten hyödyntäminen ei ole enää ainoastaan raskaankaluston käytössä vaan nykyään henkilöautoissakin hyödynnetään kameroita. Kaistavahtisovellusten kehittyminen parantaa liikenneturvallisuutta sekä ajomukavuutta, kamerasovelluksia hyödynnetään myös auton parkkeerausta helpottavien järjestelmien kanssa, jotka tuovat mukavuutta ajamiseen. [4.]

Kamerajärjestelmien suurin käyttökohde on kumminkin vielä tilan- ja omaisuuden turvaaminen, yleisötapahtuminen valvonta, vandalismin ja mahdollisten omaisuusrikosten selvittämisen helpottamiseksi. Kameroiden avulla voidaan tunnistaa vahingon- tai rikoksentekijä ilman läsnä olevia silminnäkijöitä. Tallentavien kamerajärjestelmien toiminta on kehittynyt ja niiden rinnalle on tullut kehittyneempiä tallennussovelluksia, joiden hyödyntäminen on helpottanut saadun tallenteen käsittelyä. Tietoliikenneyhteyksien nopeutuminen sekä kameroidenlaadun parantuminen on johtanut siihen, että nykyään kameroiden avulla voidaan tunnistaa yksittäisiä henkilöitä massasta. [5.]

3 Kameravalvonta

Kamera sekä hälytinjärjestelmät ovat suuressa osassa kiinteistöautomaation turvallisuutta. Niiden avulla valvotaan kiinteistön piha-alueita kuin sisätilojakin. Järjestelmien toteutukset sekä suunnittelu ovat tärkeässä osassa, kun halutaan valvoa kiinteistön sisä- ja ulkoalueilla alueille liikkuvien henkilöiden toimintaa. Murtohälytin- sekä kameravalvontajärjestelmien avulla mahdollistetaan rikollisen toiminnan kiinnijäämisen riskin suuri kasvu, joka taas puolestaan laskee kiinteistöön kohdistuvia uhkia. Kiinnijäämisen vaaran kasvaessa, ei rikoksiin ryhdytä niin herkästi kuin valvomattomiin kohteisiin. Järjestelmät mahdollistavat rikollisen toiminnan nopean havainnoinnin, jolla pystytään ehkäisemään omaisuuteen kohdistuvaa vahinkoa. [6, s.143.]

3.1 Kamerajärjestelmän rakenne

Kameravalvontajärjestelmä on kohteen tapahtumien kuvaamiseen sekä tallentamiseen tarkoitettu turvalaitejärjestelmä. Sen käytössä voidaan hyödyntää myös järjestelmään liitettäviä tarkkailulaitteita sekä ohjelmistoja, jotka mahdollistavat siirto- ja ohjaustarkoituksiin. [7, s. 2.10.]

Kamerajärjestelmien yleisimpiä käyttötarkoituksia sekä käyttökohteita ovat yleisvalvonta, jolla tarkoitetaan julkisten tilojen valvontaa kamerajärjestelmän avulla. Julkisilla tiloilla tarkoitetaan tässä tapauksessa kiinteistöjä, rakennuksia, kauppakeskuksia, puisto- sekä torialueita. [7, s. 2.10.]

- Turvallisuusvalvonta, turvallisuusvalvonnalla tarkoitetaan kamerajärjestelmän hyödyntämistä yleisötapahtumien, kauppakeskusten, teollisuus- sekä satama-alueiden ja lentokenttien turvallisuuden kehittämiseksi sekä ylläpitämiseksi.
- Omaisuusvalvonta, omaisuusvalvonnalla tarkoitetaan julkisesti esillä olevien arvoesineiden kuten museonäyttelyn tai historiallisten kohteiden kuvantamista ilkivallan ehkäisemiseksi.
- Prosessivalvonta, prosessivalvonnassa hyödynnetään kamerajärjestelmien käyttöä teollisuuden, tuotannon sekä logistiikan kehittämisen, tuottavuuden sekä turvallisuuden kehittämiseksi.
- Rajavalvonta, rajavalvonnassa käytetään kamerajärjestelmiä valtion maarajojen, merirajojen, satamien sekä lentokenttien turvallisuuden kehittämiseksi.
- Liikennevalvonta, liikennevalvonnassa kamerajärjestelmiä hyödynnetään tunneleissa, maanteillä sekä rautateillä.
- Kelivalvonta, kelivalvontaa tehdään kameroiden avulla maanteillä.
- Seuranta, seurantaa tehdään kamerajärjestelmien avulla sairaaloissa ja muissa julkishallinnonrakennuksissa sekä yksityisessä omistuksessa olevissa rakennuksissakin kuten maatiloilla sekä asuinkiinteistöjen piha-alueilla.

Kameravalvontaa ei hyödynnetä ainoastaan turvallisuuteen vaan sen tallenteiden tarjoamaa tietoa voidaan jatkojalostaa ja täten hyödyntää liiketoiminnan kehittämiseen. Kameroita on markkinoilla saatavilla erityyppisinä sekä eri käyttötarkoituksen edellyttämällä tavalla. Tavallisesti kamera koostuu kameranrungosta, objektiivista, virtalähteestä sekä kameranjalustasta. Kameroille on myös

saatavilla koteloita, joilla pystytään suojaamaan kameran objektiivi säältä, pölyltä sekä ilkivallalta. Kameroiden valinta tapahtuu käyttötarkoituksen sekä kohteen mukaan tilanteeseen sopivaksi. [7, s. 2.10.]

3.2 Kamerajärjestelmän tekninen toteutus

Runkokamerat

Runkokameralla viitataan kamerajärjestelmässä stabiloitua kameraa, joka kuvaa vakioituakohdetta. Kameran sijoittamista on aiheellista miettiä etukäteen ennen asennusvaihetta virheiden välttämiseksi. Runkokameran kuvanala on vakio, joten siihen ei voida vaikuttaa asennusvaiheen jälkeen, kameroiden objektiivit ovat vaihdettavissa asennuksen jälkeenkin, mutta tältä voidaan välttyä, mikäli asia huomioidaan jo asennus vaiheessa suoritettavalla suunnitelmallisuudella. Runkokameroiden käyttökohteet vaihtelevat laajasti, niitä voidaan hyödyntää sekä ulko-, että sisätiloissa. Ulkotiloissa oleville kameroille olisikin hyvä varata kotelo, joka kestää niin vettä, pölyä kuin kameraan kohdistuvaa vandalismiakin. [7, s. 2.10.]

Kiinteät kupukamerat

Kiinteät kupukamerat, jotka tunnetaan myös nimityksellä Dome-kamerat eroavat tekniseltä toteutukseltaan runkokameroista siten, että kameran objektiivi on sijoitettu akryylimuovista valmistetun kuvun sisäpuolelle. Dome-kameroiden käyttötarkoitukset, tekniset ominaisuudet sekä käyttökohteet eivät eroa runkokameroista. Kupukameran käyttö on harkittavaa tilanteissa, joissa kamera halutaan sijoittaa kohteeseen siten, että se ei herätä huomiota. Muotonsa tähden kupukamera ei ole yhtä silmiinpistävä kuin runkokamera. [7, s. 2.11.]

Kääntöpääkamerat

Kääntöpääkamerat, joita kutsutaan myös PTZ-kameroiksi ovat laajaa kuvausalaa vaativiin kohteisiin tarkoitettuja kameroita, joissa hyödynnetään moottorin tarjoamaa teknistä mahdollisuutta kääntää kameran objektiivia, jolloin valvottavan kohteen aluetta voidaan valvoa laajemmin sekä aktiivisemmin. Esimerkkinä käyttökohteista PTZ-kameroille ovat valvonnankohteet, jotka edellyttävät jatkuvaa valvontaa. Kameroille on mahdollista ohjelmoida ajastettuja siirtymiä, jolla mahdollistetaan ympärivuorokautinen valvonta tarpeen vaatiessa. PTZ-kameroiden ohjauksen voi toteuttaa osana hälytin- ja kulunvalvontajärjestelmää, asiattoman oleskelun tai mahdollisen vandalismin havainnointi valvotuilla-aluille on tällöin helpompaa. Kolmannen osapuolen ohjelmistojen avulla kameroilla voidaan myös mahdollistaa kameroiden kääntyminen sen havaitessa liikettä asetetun ajan ulkopuolella. PTZ-kameroiden käyttökohteiden luonteen vuoksi on asennusvaiheessa hyvä huomioida, onko kameraa tarvetta suojata mahdolliselta vandalismilta. PTZ-kameroiden käyttökohteet ovat usein laajoja piha- sekä tehdasalueita, mutta niitä on myös mahdollista soveltaa sisäkäyttöön. Esimerkkeinä sisätilojen käyttökohteista ovat kauppakeskusten parkkihallit, sairaaloidenaulatilat sekä lentokenttien- ja laivaterminaalien sisätilat. PTZ-kameroiden ohjaus voidaan toteuttaa joko automaattisesti, jolloin ajastettuohjelmisto antaa kameran moottoreille tiedon, milloin käynnistyä, jolloin kamerankuvaussuunta muuttuu. Kameroiden ohjaus on myös mahdollista toteuttaa käsin, kameran valmistajasta riippuen, kameroiden käsiohjaus voidaan toteuttaa joko erillisellä ohjaimella tai valmistajan verkkosivujen tarjoaman graafisenkäyttöliittymän kautta. Ympärivuorokautisessa valvonnassa olevissa kohteissa onkin yleistä, että päivällä valvomotyöntekijä ohjaa kameraa ja ajastettuohjelmisto käynnistyy automaattisesti valvomotyöntekijän lopetettua työvuoronsa. [7, s. 2.12.]

Lämpökamerat

Lämpökamerat ovat kameratyyppi, joka tuottaa kuvaa perustuen kuvatun kohteen lämmönsäteilyyn. Kuva, joka tuotetaan lämpökameralla, on yleisimmin mustavalkoista. Kuvaa voidaan kumminkin tehostaa keinotekoisesti erilaisten värien avulla, jolla pyritään helpottamaan lämpötilojen vaihtelua kuvatussa kohteessa sekä näiden havainnointia. Kuvan tehostaminen sekä keinotekoisten värien lisääminen kuvaan tapahtuu kameratallennusjärjestelmän erillisellä tallennusohjelmistolla. Lämpökameralle optimaalisin käyttötarkoitus on tilassa, jossa lämpötilojen vaihtelu on suurta. Lämpökamera on tekniseltä ratkaisultaan parempi vaihtoehto kuin muut kameratyypit tilanteissa, joissa kuvatussa tilassa on heikko valaistus, mutta tilasta on tarpeen vaateissa havaittava henkilöitä tai objekteja. Valvottavan tilan valaistuksen muutos ja täten kohteen varjot eivät häiritse lämpökameran tuottamaa kuvaa. Parhaiten lämpökamerat toimivat teknisenä ratkaisuna tilanteissa, joissa halutaan tuottaa kuvaa laajoilta-alueilta sekä välimatkojen ollessa pitkiä. Lämpökameroiden käyttökohteet ovat muihin kameratyyppeihin vertailtuna hyvin erilaisia, lämpökameroiden tekniset ominaisuudet tarjoavat paljon hyötyä tilanteissa, joissa muiden kameratyyppien tekniset ominaisuudet eivät riitä tuottamaan selkeätä kuvaa. Käyttökohteeseen suunnitellessa kameroiden asennusta, olisi hyvä huomioida onko tilassa tarpeeksi valaistusta kameran toiminnalle. Korkeiden kustannusten vuoksi ei kumminkaan ole kannattavaa asentaa lämpökameroita tiloihin, joissa valaistus on riittävää muillekin kameratyypeille. Lämpökameran käyttökohteita voivat olla esimerkiksi ilmanvaihtokoneiden tilat, datakeskusten konesalit, sekä muut sellaiset tilat, joissa ei normaali tilanteessa ole tarvetta pitää valaistusta, tiloissa ei vieraile ihmisiä kuin tarpeen vaatiessa, mutta tiloissa halutaan silti pitää ympärivuorokautista valvontaa vandalismin sekä vikatilojen havainnointia varten. [7, s. 2.13.]

4 Kameroiden tekniikka

4.1 Kuvatahti sekä resoluutio

Digitaalisen IP-kameran teknisessä toteutuksessa kameran CMOS-kuvakennossa kuva koostetaan pikseleistä eli kuvapisteistä. Pikseleiden määrä kertoo kameran kuvakennon tarkkuuden. Kuvapisteiden kasvanut määrä IP-kameroiden kuvakennoissa mahdollistaa analogisia kameroita paremman kuvanlaadun, kuvanlaatuun vaikuttaa myös tiedonsiirtotekniikoiden kehittyminen. Analogiset kamerat hyödyntävät koaksiaaliteknologiaa, kun taas IP-pohjaiset kamerajärjestelmät ohjaavat tietoa TCP/IP-tekniikan avulla. Kiinteiden lähiverkkojen rakentaminen on siirtynyt viime vuosina Ethernet kaapeloinneista valokuituratkaisuihin, joilla pystytään takaamaan yhteyksien sisällä tapahtuvien katkosten määrä hyvin vähäisenä. Samaisesta syystä myös IP/TCP-kameroiden määrät ovat kasvaneet suhteessa vanhempiin analogisiin kameroihin. Koaksiaalikaapelia eli antenniverkkoa pitkin tietoaan siirtävät analogiset kamerat ovat verraten kalliita, hankalia sijoittaa sekä epäkäytännöllisiä verrattaessa nykyaikaisiin IP-kameravaihtoehtoihin. Kameroiden tiedonsiirtotapa vaikuttaa olennaisesti kuvan laatuun, pakettien kokoon ja sitä kautta suoraan tallentimelle päätyvän tallenteen laatuun. Kuvan laatuun vaikuttavat erittäin oleellisesti valvottavan kohteen valaistus, kameran objektiivin koko ja kunto, mikäli objektiivi on vaurioitunut, sen tuottama kuvanlaatu on heikompaa kuin teknisesti täysin toimivalla objektiivilla. Seuraavana on kuvannettu miten, kuvan resoluutio vaikuttaa IP-kameran kuvansiirtonopeuteen, pikseleiden määrän sekä tallenteesta saatavan kuvatahtiin. [7, s. 2.16.]

.

Resolution	Pixels	Frame Rate	Bitrate (Kb/s)
1.0 MP*	1280x720 (720p)	7fps**	900 to 1800
		15fps	1600 to 3100
		30fps	3100 to 6200
1.3 MP	1280x960	7fps	1200 to 2400
		15fps	2100 to 4100
		30fps	4100 to 8200
2.0 MP	1920x1080 (1080p)	7fps	1500 to 3000
		15fps	2600 to 5200
		30fps	5200 to 10,300
3.0 MP	2048x1536	7fps	2400 to 4400
		15fps	4100 to 7700
		30fps	8200 to 15,400
5.0 MP	2560x1920	7fps	3500 to 5700
		15fps	6100 to 10,100
		30fps	12,100 to 16,400

* MP- Megapixel

** fps- Frames per second

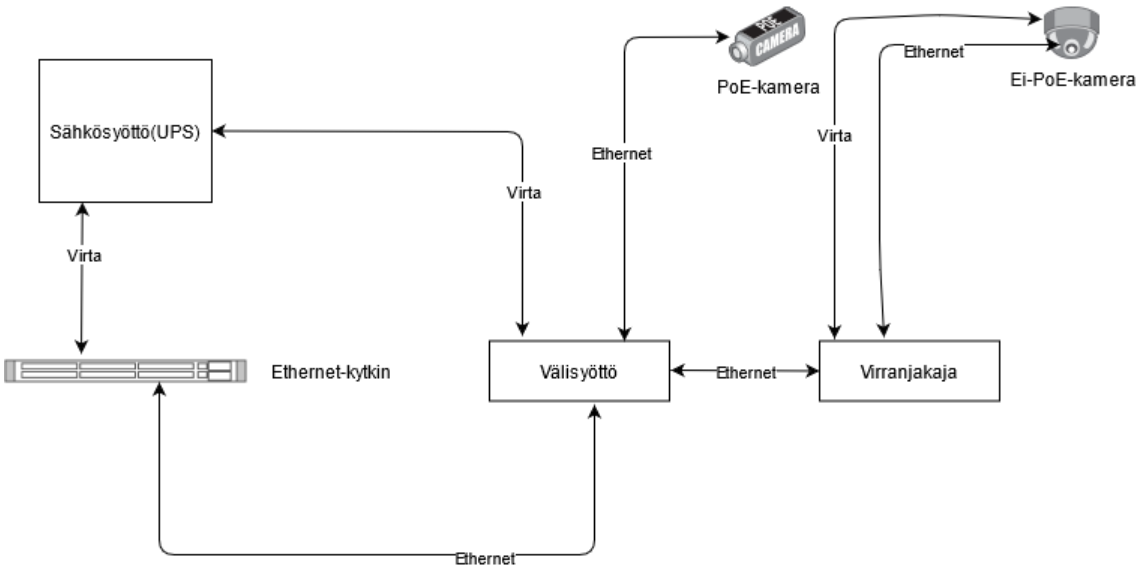
Kuva 1 Kameraresoluutiot

.

4.2 PoE

PoE eli Power Over Ethernet on IEEE 802.3af:n mukainen tekniikka-, jolla mahdollistetaan IP-pohjaisten valvontakameroiden kuin muidenkin IP-pohjaisten laitteiden käyttöjännitteen saanti. PoE-tekniikkaa käytettäessä laitteen virransyöttö tapahtuu samassa parikaapelissa kuin varsinainen tiedonsiirtokin. Käyttöjännitteen saanti sitä edellyttäville laitteille edellyttää, että käytössä on myös PoE-tekniikkaa tukeva kytkin, joka asennetaan verkkovirran sekä virtaa tarvitsevan päätelaitteen välille. Kytkin syöttää käyttöjännitteen päätelaitteelle siitä löytyvistä erillisistä PoE-porteista, jotka ovat valmistajan ilmoittamia. PoE-tekniikan käytölle on osoitettavissa moniakin hyötyjä sen käytöstä, sen avulla vähentää niin videovalvontajärjestelmien kuin muidenkin PoE-tekniikkaa tukevien järjestelmien vaatimaa kaapelointityötä. PoE-tekniikkaa tukevien laitteiden käyttö myös säästää aikaa huomattavasti asennus sekä kaapelointi vaiheessa, jolla saavutetaan taloudellista hyötyä. IP-pohjaisten laitteiden virransyöttö on tällöin mahdollista kuljettaa samoissa kaapeleissa kuin varsinainen tiedonsiirto. Mikäli järjestelmässä on jo olemassa olevat parikaapelit asennettuna, ei uusia kaapeleita ole tarvetta asentaa. PoE-tekniikan heikkona puolena teknisissä toteutuksissa on se, että sitä ei voida soveltaa ulkokäyttöön. Esimerkiksi ulkokäytössä olevien valvontakameroiden, joiden ohjaus tapahtuu verkon yli tai niissä on teknisenä

lisäominaisuutena lämmitys, ei ole mahdollista hyödyntää PoE-tekniikkaa sen maksimi tehon siirrosta johtuen. [7, s. 2.20.]



Kuva 2 POE-tekniikkaa, kytkentäkaavio

5 Tietoliikenneyhteydet

5.1 TCP/IP-protokolla

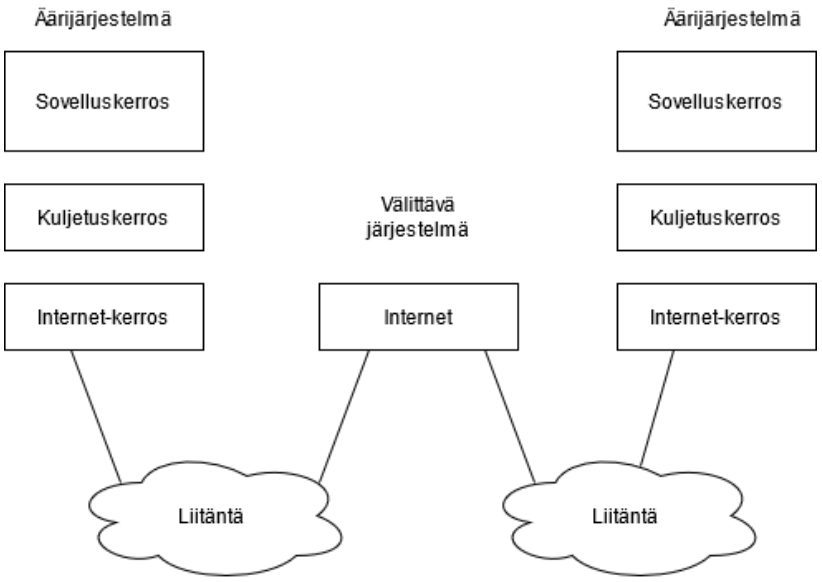
TCP/IP- protokollat sekä arkkitehtuuritoteutukset saivat syntynsä 1970-luvulla, kun USA:n puolustusvoimat yhdessä paikallisten yliopistojen sekä tutkimuslaitosten kehittivät ne olemassa olleen ARPA-verkon laajennukseksi. Myöhemmin Arpa-verkosta jalostettiin nykyinen Internet. [8, s. 18.]

Ohessa on kuvannettu TCP/IP-tietoliikenne arkkitehtuuri. TCP/IP-protokollan tietoliikennearkkitehtuuri eroaa OSI-viitekehyksen vastaavasta arkkitehtuurimallista siten, että se ei sisällä kuin kolme tietoliikenteen kerrosta. Kuvan mukaisesti TCP/IP-tietoliikennearkkitehtuuri koostuu sovellus-, kuljetus sekä Internet-kerroksista. Kerrosten välillä on tiedon välittävä Internet, johon kerrokset saavat yhteyden liitännän kautta. TCP/IP-arkkitehtuurissa, kuten myös OSI-viitekehyksessä jokaisella kerroksella on oma tehtävänsä. [8, s. 18.]

Sovelluskerroksen tehtävänä on mahdollistaa äärijärjestelmille toiminta. Tietoliikenteen peruspalveluiden tarjonta, kuten tiedostonsiirron. [8, s. 18.]

Kuljetuskerroksen tehtävänä on nimensäkin mukaisesti kuljettaa tiedot haluttuun kohteeseen. Kuljetuskerroksen tehtävänä on myös selvitä tilantanteista, joissa tiedot ovatkin menneet väärään kohteeseen. [8, s.18.]

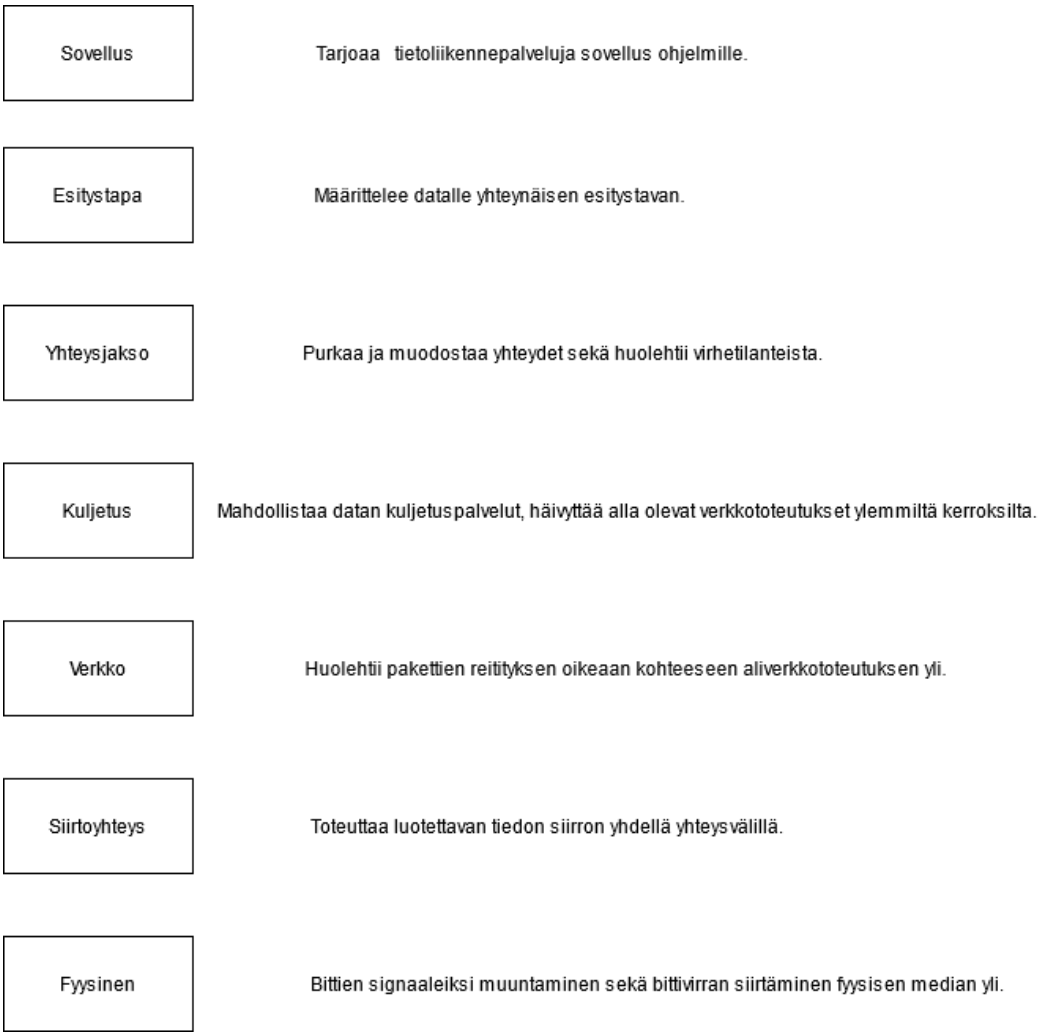
Internet-kerroksen tehtävänä on lähettää ja vastaanottaa sekä huolehtia niiden jatkosta seuraaviin kerroksiin. [8, s.18.]



Kuva 3 TCP/IP-tietoliikennearkkitehtuuri

5.1.1 OSI-viitekehys

OSI-viitekehys on kehitetty jatkona TCP/IP-arkkitehtuurimallinukselle. OSI-viitekehys on syntynyt vuonna 1980. sen tarkoituksena on auttaa havainnollistamaan tietoliikennearkkitehtuuria, siinä missä TCP/IP-tietoliikennearkkitehtuuri mallinnuksessa on vain kolme kerrosta, OSI-viitekehyksessä kerroksia on seitsemän. Ohessa on kuva OSI-Mallin kerroksista sekä selitteet niiden tarkoitukselle. [8, s. 19.]

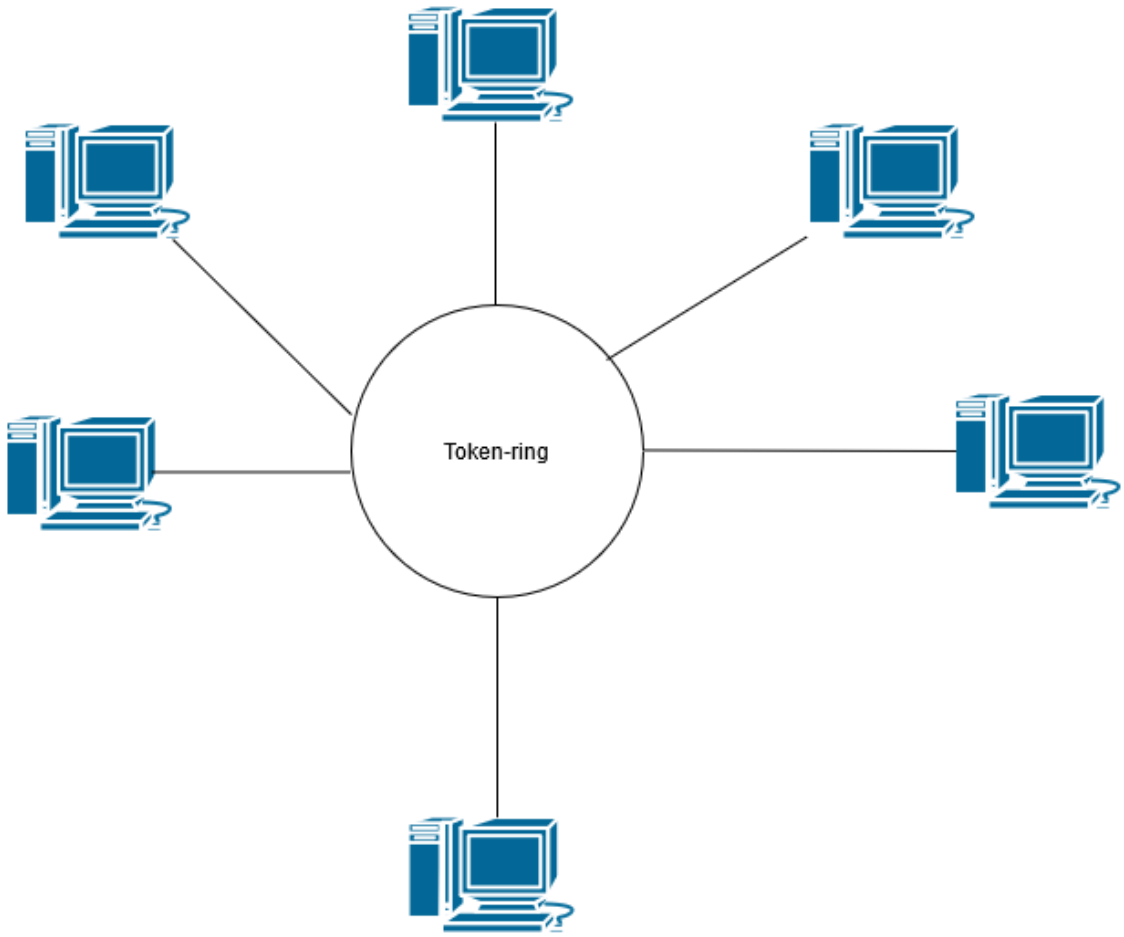


Kuva 4 OSI-viitekehys

5.1.2 IEEE 802.-lähiverkkostandardit

IEEE 802.-lähiverkkostandardit ovat Institute of Electrical and Electronics Engineerings:n määrittelemät lähiverkkostandardit, joilla on pyritty kehittämään lähiverkkojen toiminnallisuutta. IEEE 802.-lähiverkkostandarteista tunnetuimpia

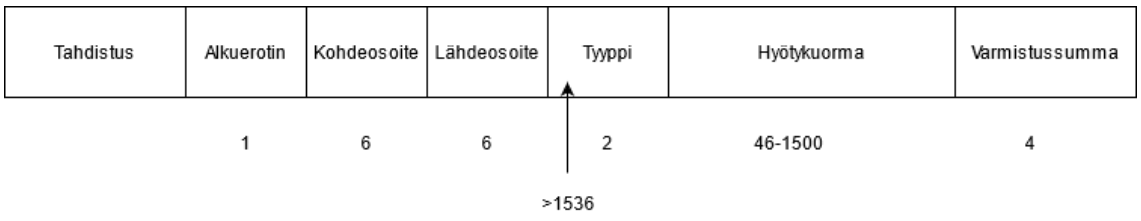
tänä päivänä ovat standardit 802.3 ja 802.11, jotka tunnetaan myös nimillä Ethernet sekä WLAN. [8, s. 144–152.] Ennen Ethernetin yleistymistä, kiinteiden lähiverkkotekniikoiden ratkaisuissa hyödynnettiin myös IBM:n vuonna 1985. julkistamaa Token Ring lähiverkkoratkaisua, IEEE on standardoinut sen 802.5:ssa. Ethernet lähiverkkoratkaisujen matalammat kustannukset erityisesti verrattuna IBM:n kehittämiin verkkosovittimiin ovat kumminkin aiheuttaneet sen, että Ethernet lähiverkkoratkaisut ovat korvanneet Token Ringin lähes kokonaan. [8, s. 86.]



Kuva 5 Token Ring lähiverkkotekniikka

5.2 Ethernet

Lähiverkkojen yleisin toteutustapa on ainakin vielä toistaiseksi Ethernet. Ethernet-lähiverkot ovat saaneet alkunsa 1970-luvun alussa, kun se kehitettiin Alohan saarilla Havaijilla toteutettujen pakettiradiotestien lopputuloksena. Ethernet on ensimmäinen standardinmukainen lähiverkkoratkaisu. Havajilla toteutettujen radiopakettitutkimusten johdosta Ethernet-teknologian tutkimus- sekä kehitystyötä jatkettiin Palo Altossa Xeroxin tutkimuslaitoksessa. Tuohon aikaan Xeroxin tutkimuslaitoksella työskenteli Ethernetin keksijänäkin pidetty Robert Metcalf. Ethernetin ensimmäisen version kehitys työhön osallistuivat DIX-ryhmän jäsenet, jotka saavat nimensä yrityksistä Digital, Intel ja Xerox, He esittelivät vuonna 1980 Ethernet 1:n. Ethernet 2 standardoitiin vuonna 1985 IEEE:n toimesta. Digital julkaisi vuonna 1983 ensimmäisen version Ethernet 2 lähiverkkotekniikasta, josta myöhemmin johdettiin standardi 802.3. ISO nimesi standardin numeroin 8802–3. Vuodesta 1985 ovat Ethernetin käyttökohteet ja tekniikat kehittyneet paljonkin. Ethernetin toimivuus perusratkaisuissa on niin hyvä, että sitä hyödynnetään vielä tänäkin päivänä. [8, s. 47.]



Kuva 6 Ethernet II -kehys

5.3 WLAN

Langattomat lähiverkot eli Wireless Local Area Network on tietoliikennetekniikka, jolla pystytään jakamaan verkkoyhteys niille laitteille, joista löytyy WLAN-

tekniikkaa tukeva vastaanotin. Langattomat lähiverkot mahdollistavat kustannuksiltaan edullisen mahdollisuuden mobiililaitteiden sekä kannettavien tietokoneiden liittämisen yrityksen tai organisaation sisäverkkoon. WLAN-tekniikka toimii radioverkkotekniikkaa hyödyntäen, osa langattomista lähiverkkoratkaisuista käyttää luvanvaraisia radiokanavia. Luvanvaraiset radiokanavat ovat kumminkin Suomessa harvinaisia ja niiden hankintaan langattomia verkkopalveluita tarjoavilta yrityksiltä. Luvanvaraisten radiokanavien avulla voidaan toteuttaa langattomia laajaverkkoja suurten yritysten tai organisaatioiden sisäiseen käyttöön tai julkiseen verkkoon liittymiseen. Yleisin suomalaisten yritysten ja organisaatioiden käyttämä lähiverkko onkin IEEE 802.11 -standardeihin perustuva, lupamenettelystä vapautettu Wi-FI-ratkaisu, Wireless Fidelity. Edellä mainitusta IEEE-standardista onkin useita eri versioita, jotka edustavat useampaa eri teknologia-aikakautta. Langattomien tiedonsiirtojärjestelmien tekninen kehitys on ollut viimeisten vuosien aikana huomattavan nopeata. Tiedonsiirtokapasiteetti on kasvanut huomattavasti, sekä yhteydet ovat stabiilimpia kuin aikaisempien teknistenratkaisujen aikana. Ohessa on taulukoitu IEEE802.11 -standardien teknisiä tietoja. [9, s. 152.]

Taulukko 1 WLAN-verkon IEEE802.11 -standardit

Numero	Taajuusalue	Modulointi	Kapasiteetti
802.11	2,4GHz	FHSS tai DSSS	2 Mb/s
802.11a	5GHz	OFDM	54 Mb/s
802.11b	2,4GHz	DSSS + CCK	11 Mb/s
802.11g	2,4GHz	DSSS + CCK tai OFDM	54 Mb/s
802.11h	5GHz	OFDM	54 Mb/s

5.3.1 Lupavapaiden WLAN-verkkojen taajuusalueet

Langattomien verkkojen toiminta perustuu radioaaltotekniikkaa. Samoja mikroaaltoaluita hyödyntävät toiminnassaan myös langattomat puhelimet sekä Bluetooth-laitteet. [9, s. 153.]

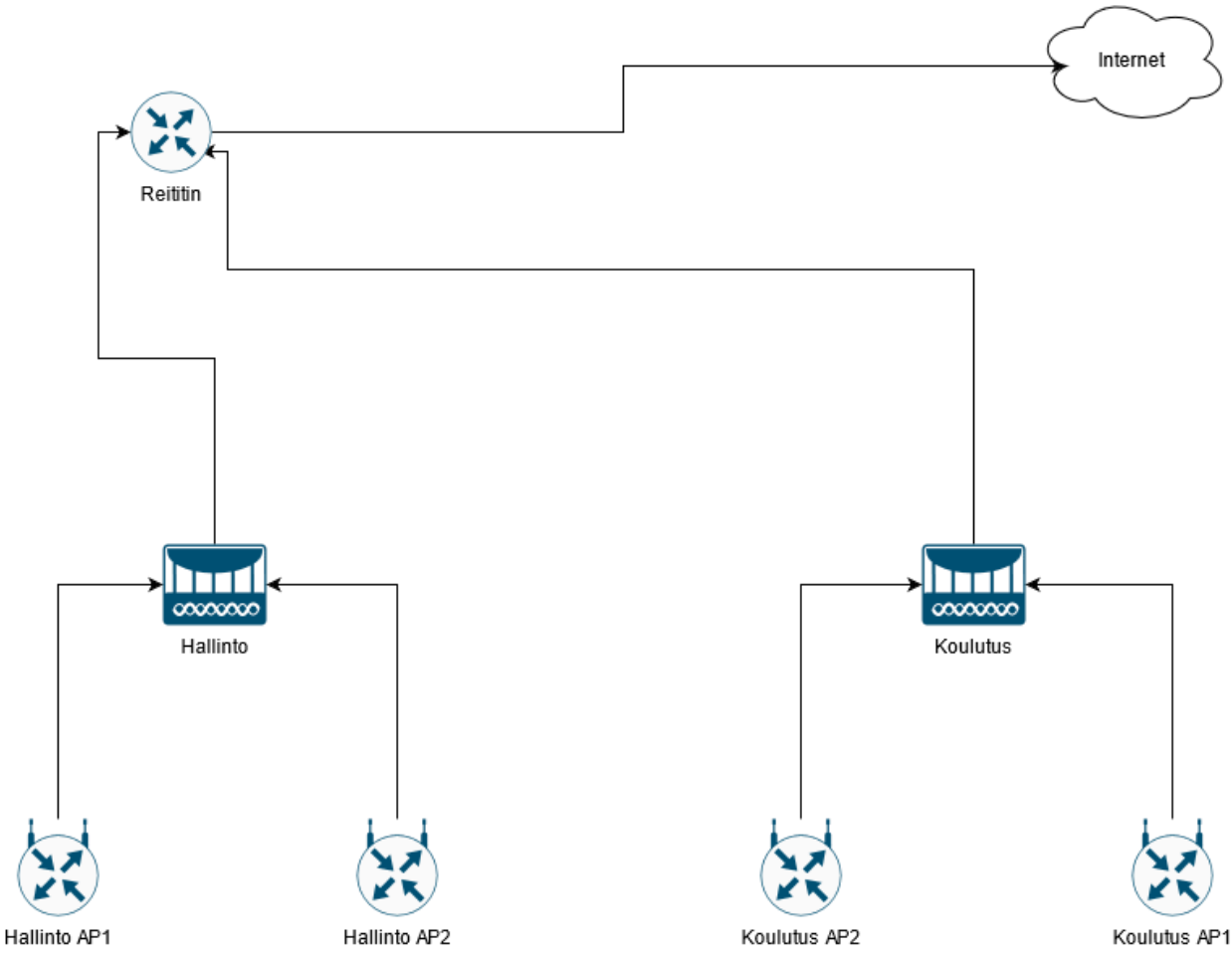
Taajuuksiltaan heikkojen radioaaltojen, kuten edellä mainitut mikroaallot on hyvin haastavaa päästä läpi kiinteistä esteistä. Ne ovat hyvät hyvin herkkiä kärsimään ulkopuolisten elektromagneettisten laitteiden aiheuttamista häiriötilanteista. [9, s. 153.]

Tästä johtuen langattoman verkon komponenttien ja erityisesti langattomien verkkojen tukiasemien sijoitteluun tulisi kiinnittää huomiota jo verkon suunnitteluvaiheessa. Erityisesti rakennuksien piirustuksiin tutustumalla voidaan ehkäistä tukiasemien heikkoa sijoittamista. Raskaat betoni-, tiili- ja teräsrakenteet estävät mikroaaltojen etenemisen. Samaiset materiaalit kumminkin samanaikaisesti heijastavat mikroaaltoja, jolloin niitä voidaan hyödyntää. Tukiasemalle etsittäessä optimaalisinta asennuspaikkaa olisikin hyvä, jos asennusvaiheessa voisi yhteyttä tarkkailla esimerkiksi kannettavalla tietokoneella. Tukiaseman asennuspaikan merkitys vaikuttaa järjestelmän rakentamiseen huomattavasti. Optimaalisimman asennuspaikan löydyttyä voidaan aloittaa kiinteän lähiverkon yhdistävän kaapelointityöt. Parhaan kuuluvuuden löytämiseksi ei aina riitä pelkästään rakennuksen runkomateriaalin tarkkailu. Tukiaseman asennuspaikan voikin olla optimaalisimmillaan mahdollisimman korkealla. Korkein mahdollinen asennuskorkeus ei kumminkaan aina takaa parasta kuuluvuutta. Erityistä huomiota tulisikin käyttää erityisesti toimistorakennuksien yleisesti käytettävien metalliverkolla vahvistettujen lasiovien läheisyydessä. Metalliverkko on asennettu laseihin, jotta lasin mahdollisen särkymisen johdosta sirpaleita ei leviäisi laajalle alueelle, mutta samalla metalliverkko estää mikroaaltojen läpipääsyn erittäin tehokkaasti. Useista tukiasemista koostuvaa suurempaa lähiverkkoa suunnitellessa

tulisi myös huomioida tukiasemien käyttämät taajuusalueiden kanavat. Tukiasemat, jotka eivät ole toisiinsa suorassa yhteydessä, tulisi aina asettaa eri taajuusalueiden kanaville. Järjestelmän suunnitteluvaiheessa tulisi myös huomioida, muita mikroaaltoja käyttäviä laitteita järjestelmän vaikutuksen alueella sijaitsee, kuten älypuhelimet. Mahdollisissa häiriötilanteissa tulisikin testata järjestelmän ulkopuolisten laitteiden poisto järjestelmän vaikutuksen piiristä, jolloin saadaan varmuus siitä, onko varsinainen häiriö itse järjestelmässä. [9, s. 153.]

5.3.2 Langattoman lähiverkon laitteet ja niiden suojaaminen

Langaton lähiverkkojärjestelmä toteutetaan peruskomponenttien kautta. Seuraavana on kuvannettuna tilanne yksinkertaisesta langattomasta lähiverkosta. Langattoman lähiverkon peruskomponentit ovatkin langattomat tukiasemat sekä langattomat verkkokortit. Langattomiin lähiverkkoihin voidaan kumminkin lisätä paljon erilaisia komponentteja kuten etäsiltoja, antenneja sekä toistimia, joiden avulla voidaan jakaa verkkoyhteyttä verkkojen välillä. Käynkin seuraavaksi WLAN-verkon peruskomponentteja läpi kuvan 9 avustuksella. [9, s. 157.]



Kuva 7 Kaaviokuva langattomasta lähiverkosta.

Ohessa on kuvannettu oppilaitoksen langaton lähiverkko. Oppilaitoksella on käytössään kolme erillistä langatonta verkkoa. Yksi langaton tukiasema on varattu oppilaitoksen opiskelijoille sekä vierailijoille käytettäväksi vierailun ajaksi yleisissä tiloissa. Kuvatussa tilanteessa langattoman lähiverkon laitteet esitellään seuraavana. [9, s. 157.]

Tukiasema

WLAN-teknologiassa sekä langattomien verkkojen toiminnassa tukiasemat eli Access pointit ovat kaiken keskipisteenä. Tukiasema jakaa muihin langattoman verkon laitteisiin verkkoyhteyden, joka on tuotu sille kiinteätä lähiverkkoa pitkin. Tukiasemaa valittaessa omaan langattomaan järjestelmään kannattaa huomioida ennen kaikkea mitä, standardeja muut langattoman verkon komponentit tukevat. Tukiasemien kustannustehokas hinta mahdollistaa sen, että virheen sattuessa tukiaseman vaihtaminen ei ole taloudellinen riski. Nykyaikaiset mobiililaitteet tukevat yleisimmin IEEE 802.11b- tai 11g-standardeja, joten tukiaseman olisi hyvä tukea tässä esimerkki tapauksessa IEEE 802.11g -standardia. Tukiasemien käyttö on lisääntynyt sen verran paljon viime vuosina, että niiden tekniikkaa on jalostettu myös. Ne voivatkin nykyään toimia etäsiltoina ja reitittiminä. [9, s. 158.]

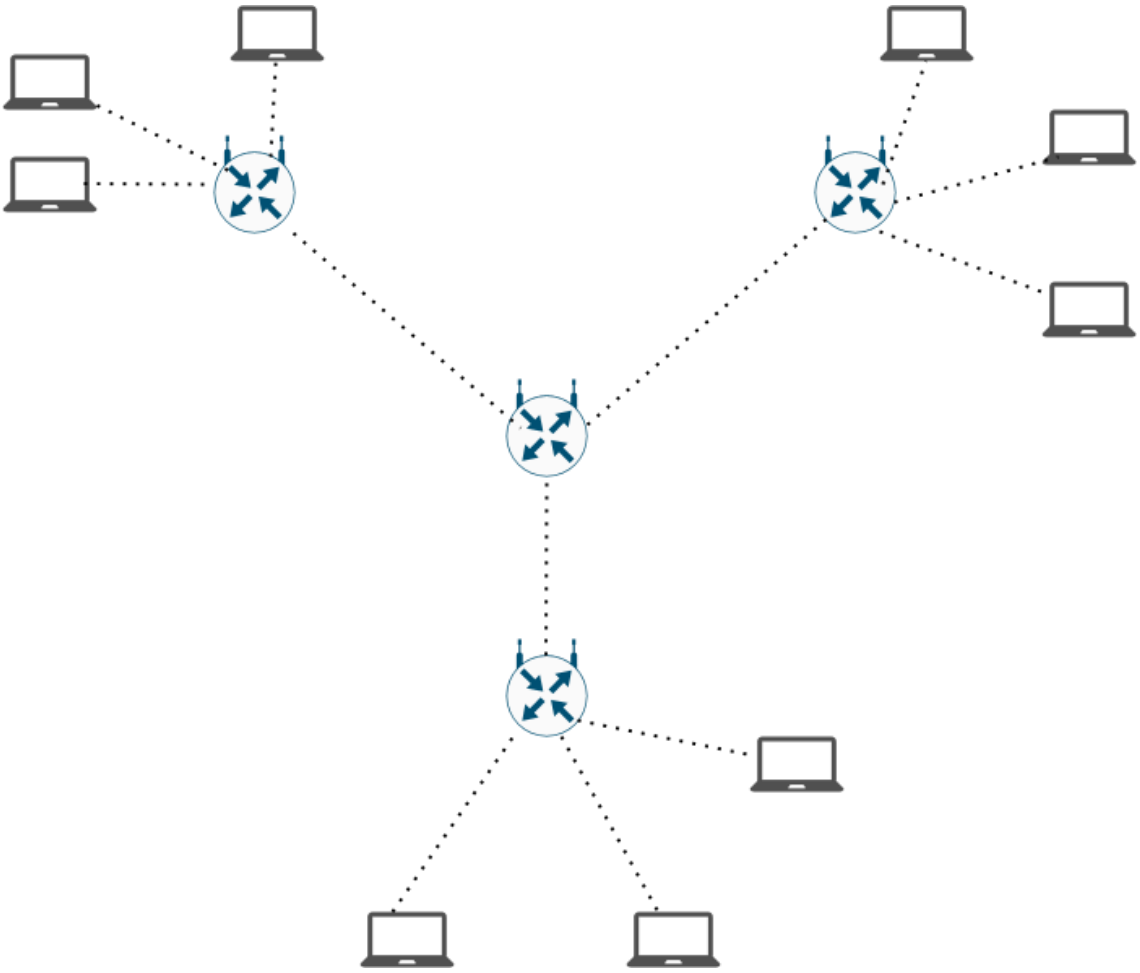
Etäsilta

Etäsiltojen käyttö langattomissa lähiverkoissa on yleisesti ottaen järkevintä silloin, kun langatonta yhteyttä halutaan jakaa pidemmälle välimatkalle. Etäsiltojen suurin käyttökohde WLAN-verkoissa on kahden erillisen rakennuksen välillä. Tällöin etäsillan tehtävänä on yhdistää kahden toisistaan erillään olevat langattomat verkot tai vaihtoehtoisesti etäsiltoja voidaan hyödyntää, mikäli kiinteän lähiverkon

suunnitteluvaiheessa on havaittu, että langattoman lähiverkkoteknologian käyttö on järkevämpää tietyissä osissa verkkoa. [9, s. 162.]

Monipistesilta

Monipistesilta on langattoman lähiverkon peruskomponentti, jolla teoriassa on hyvinkin yksinkertainen tehtävä WLAN-verkon sisällä. Sen tarkoituksena on jakaa langaton verkkoyhteys useampaan kohteeseen samanaikaisesti. Käytettäessä monipistesiltoja olisikin hyvä konfigurointivaiheessa huomioida, että tietoturvauhan vuoksi ei ole järkevää sijoittaa monipistesiltojen langattomien linkkien vastapäässä sijaitsevien siltojen MAC-osoitteita. Pääsääntöisesti WLAN-verkoissa olisi myös hyvä salata liikennettä niin paljon kuin vain mahdollista toimivuutta heikentämättä. [9, s. 163.]



Kuva 8 Langattomien verkkojen yhdistäminen etäsillan avulla

Toistin

Toistimien tehtävä langattomissa lähiverkkoratkaisuissa on kasvattaa verkon peittoaluetta. Peittoalue tarkoittaa verkon aluetta minkä sisällä verkon laitteet saavat yhteyden langattomaan lähiverkkoon. Toistimien varsinainen tehtävä ei ole kumminkaan laajentaa peittoaluetta aina vain isommaksi ja isommaksi vaan parantaa olemassa olevan peittoalueen signaalia. Toistimien käyttöön liittyy langattomissa lähiverkkoratkaisuissa negatiivinenkin puoli: toistimen käyttämä lähetyskanava on sama kuin verkon tukiasemat, joten toistimien käyttökohdetta kannattaa suunnitella hyvinkin tarkasti. Toistimen sijaan järjestelmässä voidaankin

hyödyntää esimerkiksi monipistesiltaa, mikäli toistimen käyttö aiheuttaa teknisiä häiriöitä järjestelmään. [9, s. 164.]

Langattomat verkkokortit

Langattomien lähiverkkojen toiminta perustuu langattomien tukiasemien lisäksi langattomiin verkkokortteihin. Järjestelmän suunnitteluvaiheessa kannattaakin huomioida langattoman verkkokortin noudattama WLAN-standardi. Tämän lisäksi kannattaakin huomioida langattoman verkkokortin herkkyyteen. Herkkyys määrittelee langattoman verkkokortin kyvyn käsitellä sen havaitsemaa signaalia. [9, s. 165.]

Antennit

Erillisten antennien käyttö langattomassa lähiverkossa on yleisesti harvinaista ainakin peruskomponentteja mietittäessä WLAN-verkossa. Antennit ovatkin usein integroituna langattomissa verkkokorteissa sekä tukiasemissa. Erillisten antennien käyttö tuleekin kysymykseen silloin, kun järjestelmää suunnitellessa tiedostetaan, että yhteys on mahdollisesti heikko. Mikäli heikko langattoman verkon yhteys on sisätiloissa, kannattaa käyttää ympärisäteilevää lisäantennia peittoalueen parantamiseksi. [9, s. 165.]

Langattoman verkon suojaaminen

Langattomien verkkojen suojaamisen osalta pätee samat perussäännöt kuin kiinteidenkin verkkojen tietoturvassa. Kotikäytössä olevien langattomien verkkojen suojaamisessa kumminkin kannattaa lähteä liikkeelle pienin askelin, jotta syntyy ymmärrys siitä, että verkkoihin voi kohdistua tietoturvauhkia on vaikuttajana siihen, että käyttäjällä tulisi olla motivaatiota suojata langattomat yhteytensä mahdollisimman hyvin. Nämä ovat hyviä perussääntöjä langattomien verkkojen sekä kiinteän verkon päätelaitteiden salasanahallinnalle.

- Vaihda oletussalasanat sekä verkon oletus nimi. [10, s. 1.4.]
- Aseta järjestelmään tarpeeksi vahva sekä uniikki salasana. [9, s. 2.3.]
- Hyödynnä langattomissa verkoissa niille kehitettyjä suojaustekniikoita. [10, s. 1.3.]
- Älä pidä langatonta verkkoa turhaan päällä. [10, s. 4.2.]
- Älä salli etäkäyttöä laitteistolle. [10, s. 5.1.]
- Pidä verkon laitteiden ohjelmistopäivitykset ajan tasalla. [10, s. 5.1.]

6 Suojatut yhteydet

6.1 VPN-teknologia

VPN eli Virtual Private Network on salattu verkkoyhteys, jossa päätepisteiden välille muodostetaan salattu yhteys julkisenverkon kautta. VPN-verkossa käyttäjien yhteydet perustuvat Internet-palveluntarjoajan tai muun palveluntarjoajan yhdysliikennepisteeseen otettavin paikallisiin yhteyksiin. [11, s. 236.]

VPN-verkon avulla verkon käyttäjät voivat käyttää yrityksen yksityistä verkkoa turvallisesti sekä luotettavasti julkisen verkon kautta. VPN-verkon konfigurointi sekä käyttäjätietojen lisääminen yrityksen tai organisaation toimipisteiden välillä on helpompaa kuin kiinteiden yhteyksien. VPN-verkkojen yksi eduista onkin sen skaalautuvuus. Kiinteiden yhteyksien kustannukset määräytyvät suoraan välimatkojen mukaan, kun taas VPN-verkossa yrityksen tai organisaation toimipisteiden välimatka ei vaikuta kustannuksiin. [11, s. 236.]

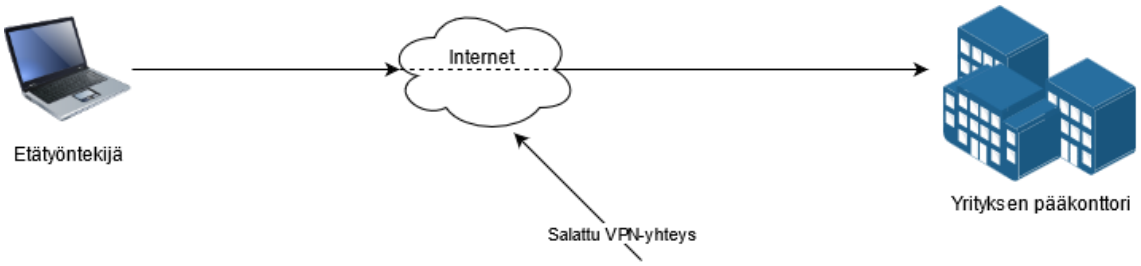
VPN-verkossa yrityksen tai organisaation sisäisessä verkossa, intranetissä voidaan hyödyntää IPSec-skaalausta, jonka avulla mahdollistetaan turvallinen Internetin tai muun verkkopalvelun käyttö. Tällä tavoin mahdollistetaan turvallinen

sähköinen kaupankäynti sekä extranet-yhteydet etätyöntekijöiden, liikekumppanien, toimittajien sekä asiakkaiden kanssa. VPN-teknologiaa hyödyntäviä verkkoja on kolmen tyyppisiä. [11, s. 237.]

6.1.1 VPN-etäyhteysverkot

VPN-etäyhteysverkot

VPN-etäyhteysverkkojen tarkoituksena on mahdollistaa yksittäisen käyttäjän turvallinen yhteydenottaminen yrityksen tai organisaation verkkoon. VPN-etäyhteysverkon toiminta perustuu siihen, että yksittäinen käyttäjä hyödyntää VPN-palveluntarjoajan erillistä VPN-asiakasohjelmaa, jonka avulla hän sää yhteyden yrityksen intranettiin. Yleisimmät sovellukset joihin VPN-etäyhteyttä sovelletaan ovat yrityksen sisäinen tiedonsiirto sekä sähköpostipalveluiden salaaminen. [11, s. 237.]

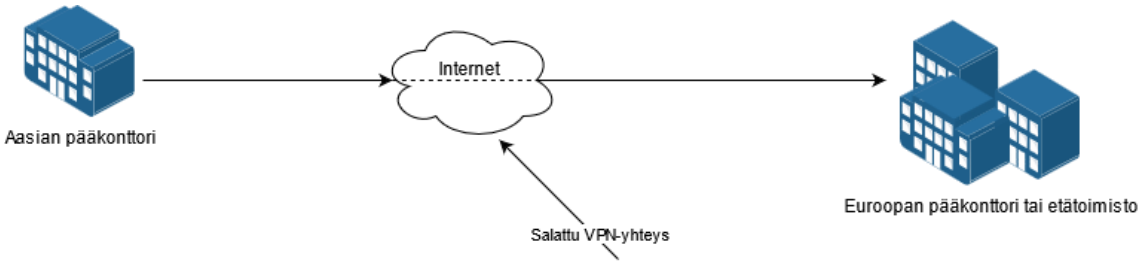


Kuva 9 VPN-etäyhteysverkko

6.1.2 Toimipisteiden etäyhteysverkot

Toimipisteiden väliset VPN-verkot eroavat VPN-etäyhteysverkoista siten, että tällöin VPN-verkon yhteys on kiinteän lähiverkon takana. Olemassa olevaa lähiverkkoa hyödynnetään laajentamalla sitä muihin rakennuksiin tai toimipisteisiin. Tällä mahdollistetaan se, että eri toimipisteissä työskentelevät henkilöt voivat

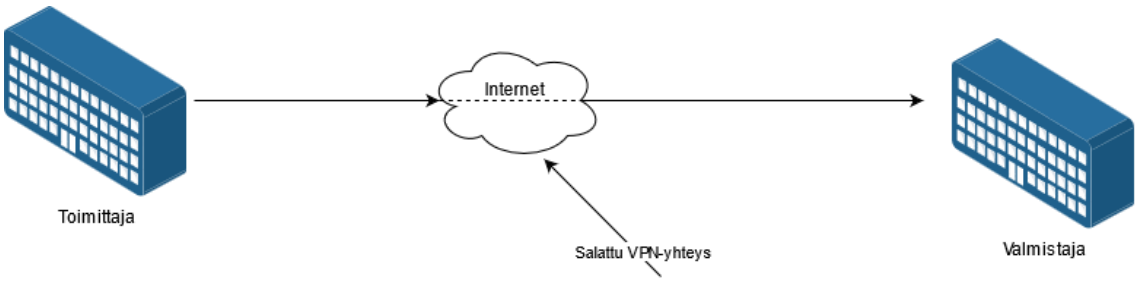
käyttää samoja verkkopalveluita. Toisin kuin VPN-etäyhteysverkot, toimipisteiden etäyhteysverkot ovat jatkuvasti päällä. Niitä kutsutaankin myös nimityksillä intranet tai lähiverkkojen välisinä VPN-verkkoina. [11, s. 237.]



Kuva 10 Toimipisteiden etäyhteysverkko

6.1.3 VPN-extranet

VPN-extranetin toiminta on hyvin samanlainen kuin yrityksen sisäisten toimipisteiden väliset VPN-yhteydet. VPN-extranetin käyttö tapahtuu yrityksen sisäisen lähiverkon sijaan yrityksen toimittajien, yrityksen tuotteen tai palveluiden valmistajan sekä asiakkaiden välillä. VPN-extranetin suurin yksittäinen hyöty on turvallinen sähköinen kaupankäynti. VPN-extranetin kautta yritysten välinen tiedonsiirto myös nopeutuu sekä on turvallisempaa. [11, s. 238.]



Kuva 11 VPN-extranet

6.1.4 VPN-verkkojen tavoitteet

VPN-verkon tavoitteena on tarjota yritykselle tai organisaatiolle hyötyä sekä turvallisuutta tietojen välittämisessä toimipisteiden, asiakkaiden sekä toimittajien välillä. Tämä edellyttää kumminkin VPN-verkon suunnitelmallista toteuttamista, jotta VPN-verkkojen käyttöönotosta saadaan etua. [11, s. 239.]

VPN-teknologioiden hyödyntäminen tarjoaa yrityksen tai organisaation etätyöskentelevien tai yrityksen ulkopuolella tapahtuvan työnteon turvallisuuden sekä tuottavuuden. Erityisesti pienyrittäjille VPN-teknologioiden hyödyntäminen on taloudellisesti käyttökelpoinen ratkaisu työnteon tehostamiseksi sekä tietoturvan parantamiseksi. [11, s. 239.]

Isompien yritysten sekä organisaatioiden kustannuksia sekä verkon kuormitusta voidaan laskea hyödyntämällä VPN-verkkoteknologiaa, yrityksen toimipisteiden sekä etätoimipisteiden väliset yhteydet voidaan täten yhdistää toisiinsa sijainnista riippumatta VPN-verkon avulla. [11, s. 239.]

Toimistokustannusten alentuminen, henkilöstön mahdollisuus joustavampaan etätyöskentelyyn kotoa käsin, työskentelyolojen sekä täten työhyvinvoinnin parantaminen, stressin vähentyminen sekä tuottavuuden lisääminen ja turvallisten yhteyksien luominen yrityksen sekä etätyöntekijän toimipisteen välillä ovat erinomaisia syitä hyödyntää VPN-verkkoteknologioita. [11, s. 239–240.]

6.2 SSH

6.2.1 SSH yleisesti

Secure Shell eli SSH on protokolla, jolla mahdollistetaan kirjautuminen etäyhteyden varassa olevaan järjestelmään, SSH-yhteyden avulla pystytään parantamaan etäohjattavan järjestelmän turvallisuutta käyttäjän tunnistautumisvaiheessa. SSH on ohjelma, joka tarjoaa salatun tiedonsiirto polun järjestelmä sisällä, julkisenverkon yli, josta voidaan käyttää myös termiä turvaton verkko. Tämän seurauksena järjestelmässä ei kulje käyttäjien kirjautumistiedot kuten käyttäjänimet sekä salasanat selkokielisinä, jolla pystytään ehkäisemään järjestelmään kuulumattomien henkilöiden pääsy sinne. [11, s. 145.]

6.2.2 SSH-protokollan historia

SSH-protokolla on saanut alkunsa vuonna 1995, sen ensimmäinen versio SSH1 otettiin käyttöön. SSH1 suunniteltiin alun perin korvaamaan UNIX-järjestelmien tietoturvaltaan heikot etäyhteysprotokollat, kuten rologin, rsh: sekä rcp:n. Edellä mainitut etäyhteysprotokollat tarjosivat UNIX-järjestelmien käyttäjille runsaasti työkaluja käyttöön, mutta niiden heikon tietoturvan takia niihin liittyi enemmän ongelmia kuin hyötyjä. Vuonna 1997 IETF julkaisikin SSH2-protokollan, jonka tarkoituksena oli parantaa SSH1-protokollassa olleita turvallisuus- sekä toiminnallisuusongelmia. [11, s. 145.]

6.2.3 SSH-protokollan käyttö

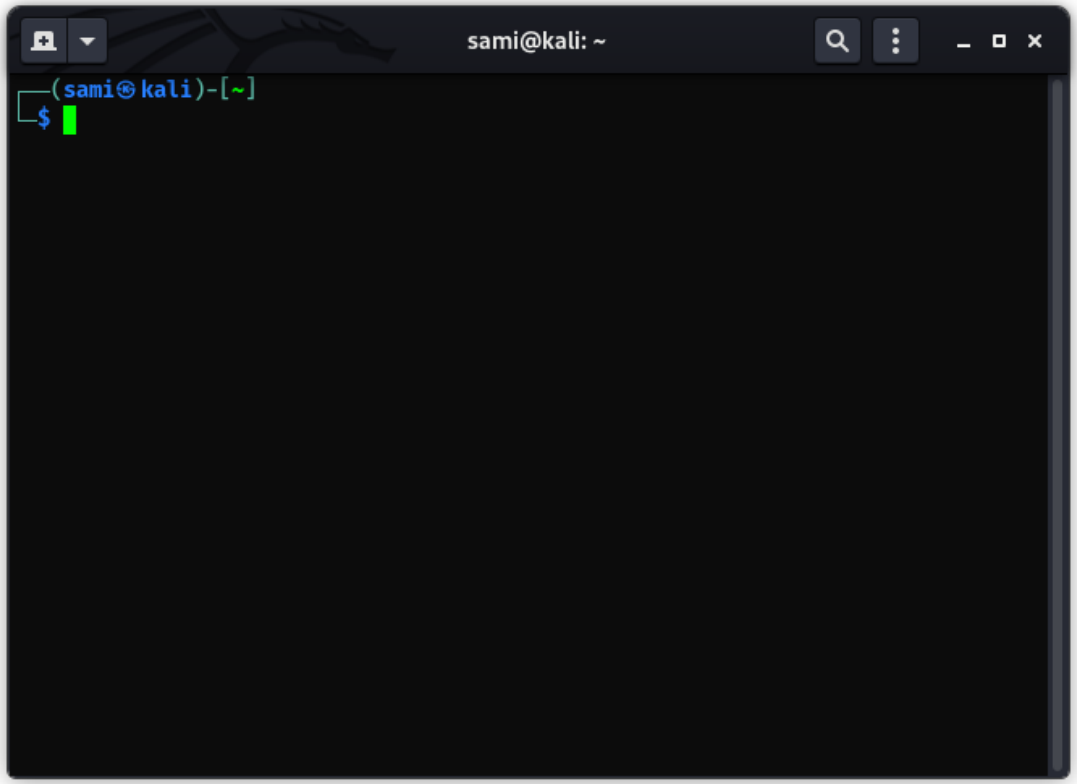
SSH-protokollan tavallisin käyttötarkoitus on sama kuin Telnet-protokollakin. Sen avulla mahdollistetaan turvallisen komentotulkin käynnistäminen. SSH-protokollan eroavaisuus Telnet-protokollaan on kumminkin suuri, kun huomioidaan

toiminnallisuuteen sekä haavoittuvuuteen liittyvät ongelmat. SSH-protokolla onkin tästä syystä etäyhteyksien teollisuusstandardi. [11, s. 145–146.]

SSH-protokolla on ominaisuuksiltaan sekä toiminnaltaan Telnet-protokollaa paljon laajempi. SSH-protokollaa tukevat komentotulkit ovat saatavilla yleisimmille käyttöjärjestelmille. Tyypillinen SSH-protokollan käyttötarkoitus on julkisenverkon tai mahdollisesti jonkin muun ei-luotettavan verkon kautta tapahtuva etäyhteyden ottaminen järjestelmään kirjautumista varten. Tällöin voidaan suorittaa jokin SSH-protokollan kolmesta toiminnosta. [11, s. 145–146.]

- turvallinen komentotulkki
- turvallinen tiedonsiirto
- turvallinen portin uudelleenohjaus.

Vaikkakin SSH-protokollaa käytetään pääasiassa etäyhteyden saavuttamiseksi järjestelmään, voidaan protokollan avulla luoda myös yleiskäyttöisiä salaustunneleita, joita hyödyntämällä voidaan kopioida tiedostoja, salaamaan sähköpostiyhteyksiä sekä käynnistämään sovelluksia etäyhteyden yli. [11, s. 145–146.]



Kuva 12 Linux-järjestelmän komentotulkki

7 Insinöörityön yhteenveto

Insinöörityöni raportin oli tarkoitus kuvata nykyaikaisten tietoliikenneyhteyksien ja standardien toimintaa sekä hyödyntämistä osana kiinteistöautomaatiota. Raporttini alussa kuvaan, kiinteistöautomatiikan tehtäviä sekä sovelluksia. Kiinteistöautomatiikan kehitys on suunnannut viimevuosina hyvin vahvasti energiatehokkuuteen, niin asuinkiinteistöjen automatiikkajärjestelmissä kuin suurempienkin rakennuksien automatiikantoteutuksissa. Onnistuin raportissani kuvaamaan automatiikan nykytilaa ja sen kehityssuuntaa, uskonkin, että tulevaisuudessa kiinteistöautomaatio- ja tietoliikennetekniikan alat suuntautuvat enemmän samaan suuntaan, automaatiojärjestelmien tiedonkeruun siirtyvän vahvemmin ohjelmistopohjaisiin ratkaisuihin, kun taas tietoliikennetekniikan ratkaisut hakeutuvat suunnitelmallisuudessaan enemmän automaatiotekniikan suuntaan. Raportissani käsittelen raportissani myös valvontakamerajärjestelmien toimintaa, sen tehtäviä sekä peruskomponentteja. Kirjoittaessani Insinöörityönraporttiani mietin, onko eettisesti oikein, että nykyaikaisilla konenäkö- sekä kamerajärjestelmillä voidaan tunnistaa yksittäisiä ihmisiä suuresta massasta. Tämän on tehnyt mahdolliseksi teknisesti laadukkaat kamerat, tallennusohjelmistojen korkea taso sekä tietoliikenneyhteyksien huippunopeudet. Ajoneuvo- ja metsäkoneteollisuus on saanut kamerasovelluksista paljon hyödyllisiä sovelluksia käyttöönsä, joiden hyöty on todellinen, tieliikenteessä on turvallisempaa, kuljetukset pääsevät ehjänä perille sekä kuljettajien työolot ovat paremmat. Konenäkösovellusten sekä koneälyteknologian kehitys on mielenkiitoista tulevaisuudessa, tuloksia on saavutettu jo nykyisillä sovelluksilla, mutta kameroiden ja tietokoneidenlaskentatehon kasvaessa järjestelmien virhemarginaali pienenee ja niiden tehokkuus kasvaa entisestään. Tietoliikennetekniikan tulevaisuus on kiinnostava moneltakin kannalta, käyn raportissani läpi nykyaikaisia lähiverkontekniikoita sekä sovelluksia sen ympärillä. Olenkin kiinnostunut erityisesti näkemään mikä on tulevaisuudessa langattomien lähiverkkojen kehitys. Raporttini loppupuolella käyn vielä tietoliikennetekniikan tulevaisuuden kannalta tärkeää asiaa läpi, tietoturvan merkitys kasvaa koko ajan vain enemmän ja enemmän, raportissani käynkin läpi nykyhetken toimivimpia suojattujen yhteyksien sovelluksia sekä niiden vaikutuksia ihmisten työskentely mahdollisuuksiin.

Lähteet

1 Pirhonen, Tero. 2011. Kiinteistöautomaation peruselementit ja -toiminnot sekä kiinteistöautomaatioprojektin toteutus. Insinöörityö. Metropolia Ammattikorkeakoulu. Theseus-tietokanta.

2 Peltoniemi, Tommi. 2011. Konenäön hyödyntäminen huonekalutehtaalla. Opinnäytetyö. Keski-Pohjanmaan Ammattikorkeakoulu. Theseus-tietokanta.

3 Valtioneuvoston asetus STM/2019/140.

4 Nikula, Jussi. 2018. Kamera- ja tutkajärjestelmien yleistymisen vaikutukset monimerkkikorjaamon varustelutarpeeseen. Insinöörityö. Metropolia Ammatti Korkeakoulu. Theseus-tietokanta.

5 Muurinen, Niko. 2019. Työkalu rikostutkinnan avuksi. Poliisiammattikorkeakoulun opinnäytetyö / AMK. Poliisiammattikorkeakoulu. Theseus-tietokanta.

6 Värjä, Pertti, Mikkola, Jukka-Matti. 2012. Uusi kiinteistöautomaatio. Koria: Cadnet Oy.

7 Kameravalvontaopas. Verkkoaineisto. Finanssiala. < https://www.finanssiala.fi/wp-content/uploads/2020/10/Kameravalvontaopas.pdf>. Luettu 1.4.2021.

8 Puska, Matti. 2000. Lähiverkkojen tekniikka Pro Training. Jyväskylä: Gummerus Kirjapaino Oy.

9 Hakala, Mika, Vainio, Mika. 2005. Tietoverkkojen rakentaminen Porvoo: Docento Finland Oy.

10 . Ohje 2/2011 langattomien verkkojen tietoturvasta. Verkkoaineisto. Kyberturvallisuuskeskus. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf >. Luettu 14.5.2021.

11 Thomas, Tom. 2005. Verkkojen tietoturva. Helsinki: Edita Prima Oy.

.