# Etäkäyttöyhteys automaatiojärjestelmään

Arttu Simula

Opinnäytetyö
Kesäkuu 2012
Sähkötekniikka
Automaatiotekniikan
suuntautumisvaihtoehto
Tampereen ammattikorkeakoulu

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Sähkötekniikan koulutusohjelma
Automaatiotekniikan suuntautumisvaihtoehto

SIMULA, ARTTU: Etäkäyttöyhteys automaatiojärjestelmään

Opinnäytetyö 47 s.
Kesäkuu 2012

---

Opinnäytetyön aiheena oli suunnitella ja toteuttaa suojattu ja luotettava etäkäyttöyhteys ympäri vuoden asuttavaan vapaa-ajan asuntoon tulevaan automaatiojärjestelmään. Lisäksi automaatiojärjestelmän ohjaimen laitevalinta sekä etäkäyttöyhteyden vaatimat laitevalinnat oli tehtävä. Etäkäyttöyhteyden ohella myös siinä käytettävä HMI tuli toteuttaa. Laitevalintoja varten ohjaimelle asetettiin tiettyjä vaatimuksia, keskeisimpänä soveltuvuus käytettäväksi teollisuuden suuremmassa automaatiojärjestelmässä. Opinnäytetyön tarkoituksena oli laajentaa osaamista tietoverkkoasioissa sekä tutustua aikaisemmin tuntemattomaan ohjaimeen. Tarkoituksena oli myös lisätä valmiuksia työskennellä etäkäyttöasioiden parissa suuressa teollisuuden automaatiojärjestelmässä.

Laitevalintoja varten markkinoiden tarjontaa tarkasteltiin. Tarjouspyynnöt ohjaimesta lähetettiin kolmelle valmistajalle. Lopulta päädyttiin Beckhoffin tarjoamaan CX9001-ohjaimeen. Etäkäyttöyhteyttä varten selvitettiin sen eri toteutustapoja. Näin pystyttiin määrittämään, minkälaisia laitteita sen toteuttaminen vaatii. Etäkäyttöyhteys toteutettiin IPsec- ja PPTP-tekniikoilla. Suurten verkkolaitevalmistajien tarjontaan tutustuttiin. Lopulta päädyttiin TP-LINKin tarjoamiin ratkaisuihin. Hankitut verkkolaitteet konfiguroitiin etäyhteyksiä varten. Hankittuun ohjaimeen toteutettiin verkkosivu etäkäyttöä varten.

Lopputuloksena on järjestelmä, johon voidaan luoda turvallinen yhteys internetin kautta mistä tahansa sekä ohjata ja valvoa järjestelmää käyttäen verkkoselainta. Järjestelmä on käytössä ja sen suunnittelun ja toteuttamisen myötä osaaminen tietoverkkoasioissa laajeni merkittävästi. Kirjoittajan valmiudet työskennellä vastaavan etäkäyttöyhteyden parissa suuressa teollisuuden automaatiojärjestelmässä ovat kehittyneet huomattavasti opinnäytetyön tekemisen aikana.

---

Asiasanat: Etäkäyttöyhteys, VPN, IPsec, PPTP, Beckhoff

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Electrical Engineering
Option of Automation Technology

SIMULA, ARTTU: Remote Access for an Automation System

Bachelor's thesis 47 pages.
June 2012

---

The subject of this thesis was to design and implement a secure and reliable remote access connection for an automation system, which was to be implemented in a year-round recreational home. Device selection was made for the controller of the automation system and for the devices required by the remote access connection. HMI for the remote access connection was also created. Some criteria were defined for the device selection of the controller, the most essential being the suitability for use in a larger automation system in a real industrial environment. The purpose of this thesis was to expand competence in information network-related issues and to explore a previously unknown controller. Also the purpose was to increase the ability to work with remote access-related issues in a larger automation system in a real industrial environment.

The marketplace was explored for the device selection. Requests for quotations for the controller were sent to three different manufacturers. The selected controller was the model CX9001 offered by Beckhoff. Different ways of implementing the remote access connection were researched to find out what it required from the hardware. The remote access connection was implemented using IPsec and PPTP technologies. The supply of large IT manufacturers was explored. Devices manufactured by TP-LINK were selected. The acquired network devices were configured for the remote access connections. A web page was created for the acquired controller for remote control use.

The result is a system, which can be connected to via the internet securely from anywhere with an internet connection. The system can be monitored and controlled with a web browser displaying the created HMI. The system is in operation and with its design and implementation the know-how in information network-related issues has expanded considerably. The abilities to work with a similar remote access solution in a large automation system have improved significantly over the making of this thesis.

---

Key words: Remote control, VPN, IPsec, PPTP, Beckhoff

SISÄLTÖ

LYHENTEET

| | |
|---|---|
| 3G | Third Generation |
| ADS | Automation Device Specification |
| AH | Authenticating Headers |
| CSS | Cascading Style Sheets |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| ESP | Encapsulating Security Payload |
| FAT | Factory Acceptance Test |
| FBD | Function Block Diagram |
| GRE | Generic Routing Encapsulation |
| HMI | Human Machine Interface |
| HTML | Hypertext Markup Language |
| IKE | Internet Key Exchange |
| IOS | Internetwork operating System |
| IPSec | IP Security Architecture |
| L2TP | Layer Two Tunneling Protocol |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MPPE | Microsoft Point-to-Point Encryption |
| MySQL | My Structured Query Language |
| OPC | Ole for Process Control |
| OSI | Open Systems Interconnection |
| PLC | Programmable Logic Controller |
| PPTP | Point-to-Point Tunneling Protocol |
| SA | Security Association |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| UDP | User Datagram Protocol |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |

| | |
|---|---|
| VPN | Virtual Private Network |
| XML | Extensible Markup Language |

KÄSITTEET

| | |
|---|---|
| Protokolla | Tietoliikenteen yhteyskäytäntö. Protokolla on käytäntö, joka mahdollistaa ja määrittelee ohjelmien ja laitteiden väliset tiedonsiirtotavat ja yhteydet. |
| Tiivistefunktio | Funktio, joka muuntaa mielivaltaisen merkkijonon vakiomittaiseksi tiivisteeksi. |
| Tiiviste | Tiivistefunktion palauttama tietyn mittainen merkkijono, josta ei voida johtaa tai tulkita alkuperäistä tiivistefunktion syötettä. |
| Verkkotunnus | Kirjaimista tai/ja numeroista koostuva verkkopalvelun ihmiselle looginen nimi. |

# 1 JOHDANTO

## 1.1 Etäkäyttöyhteyksien yleisyys

Etäkäyttöyhteydet tuovat huomattavan paljon etuja teollisuuslaitosta huollettaessa ja käytettäessä. Etäkäyttöyhteyden avulla laitoksen valvonta ja jotkut ohjelmalliset huoltotoimenpiteet voidaan suorittaa mistä tahansa. Tästä syystä suurimmassa osassa laitoksista on jonkinlainen etäkäyttöyhteys. Teollisuudessa käyttö asettaa kuitenkin etäyhteydelle tiukat tietoturvalliset vaatimukset. Yhä enemmän vaaditaan tietoverkkoasioiden osaamista teollisuuslaitoksen automaatiojärjestelmään liittyvien asioiden hoidossa. Sama osaaminen pätee myös perinteisiä, tietokoneita toisiinsa yhdistäviä tietoverkkoja rakennettaessa esimerkiksi toimistolla. Etäyhteydet ovat myös toimistoilla erittäin yleisiä ja hyödyllisiä. Osaaminen etäyhteys- ja tietoverkkoasioissa on siis erittäin hyödyllistä ja arvokasta.

## 1.2 Opinnäytetyön aihe

Opinnäytetyön aihe saatiin Seilo Consultingilta. Opinnäytetyö tehtiin harjoituksen kaltaisena projektina toimeksiantajalle. Haluttiin tutustua aikaisemmin tuntemattomiin laitteistoihin ja laajentaa osaamista. Aiheena oli luoda etäkäyttöyhteys ympäri vuoden asuttavaan vapaa-ajan kiinteistöön tulevaan automaatiojärjestelmään käyttäen teollisuuteen soveltuvaa ohjainta. Myös ohjaimen laitevalinta kuului opinnäytetyön aiheeseen. Automaatiojärjestelmälle asetettiin tiettyjä vaatimuksia, kuten laajennettavuus, monipuolinen ohjelmoitavuus ja turvallisen etäkäyttöyhteyden toteutusmahdollisuus. Suuntaa antava noin tuhannen euron budjetti annettiin työhön liittyvän laitteiston ja mahdollisten ohjelmistojen kustannuksille. Minkään laitteiden merkkejä ja malleja ei määritelty.

Alun perin aiheeseen kuului koko automaatiojärjestelmän ja etäkäytön suunnittelu ja toteutus. Kävi kuitenkin ilmi, että työ on melko laaja ja siten se jaettiin kahdeksi erilliseksi opinnäytetyöksi. Lauri Jaakkola tekee työstä automaatiojärjestelmän osuuden: PLC:n (Programmable Logic Controller) ohjelmointi sekä säätöjen, mittausten ja ohjausten suunnittelu, toteutus ja niihin liittyvien laitevalintojen tekeminen. Tämä opinnäytetyö käsittää käytettävän ohjaimen laitevalinnan, turvallisen etäkäyttöyhteyden luomisen ja siihen liittyvät laitevalinnat sekä etäkäytön toteuttamisen.

## 1.3 Opinnäytetyön toimeksiantaja

Opinnäytetyön toimeksiantaja on Seilo Consulting. Yrityksen palveluihin kuuluu käyttöönotot, projektien esisuunnittelu ja -määrittely, asennusvalvonta, Factory Acceptance Test (FAT) -testien valvonta sekä vianetsintä. Useimmiten työt suoritetaan ympäri maailmaa olevilla laitoksilla. Yksi esimerkki toimitetuista projektista on voimalaitoksen ja sähkönjakelun ohjausjärjestelmien esisuunnittelu ja -määrittely öljyntuotantolautoille ja voimalaitokselle Total öljy-yhtiölle Gaboniin. Projekti sisälsi voimalaitoksen mantereella ja kaksi öljyntuotantolauttaa merellä. Yritys käsittää tämän opinnäytetyön tekemisen hetkellä toimitusjohtajan lisäksi 5 työntekijää.

## 1.4 Opinnäytetyön tavoite

Opinnäytetyön tavoitteena on suunnitella ja toteuttaa toimiva ja turvallinen etäkäyttöyhteys teollisuuteen soveltuvaan automaatiojärjestelmään. Etäkäyttöyhteydestä toteutetaan pilottiversio ympäri vuoden asuttavalle vapaa-ajan asunnolle, jossa on teollisuuteen soveltuva automaatiojärjestelmä. Tavoitteena on hyvien laitevalintojen tekeminen sekä toimivan ja turvallisen etäkäyttöyhteyden toteuttaminen kohteeseen. Laitevalinnat tullaan tekemään automaatiojärjestelmässä käytettävälle ohjaimelle sekä etäkäyttöyhteyden toteuttamiseen vaadittaville laitteille. Tarkoituksena on laajentaa osaamista etäkäyttö- ja tietoverkkoasioissa sekä selvittää turvallisen etäkäyttöyhteyden toteuttamisen vaatimukset.

# 2 TIEDONSIIRTO, TIETOVERKOT JA TURVATTU ETÄKÄYTTÖYHTEYS

## 2.1 Tiedonsiirto

Tiedonsiirto ja tietoverkot ovat erittäin laajoja asiakokonaisuuksia. Turvatun etäkäyttöyhteyden toiminnan ymmärtämiseksi on hyvä ottaa selvää tiedonsiirron perusasioista ja eri toteutustavoista. Etäkäyttöyhteyden toteuttamiseen tarvitaan myös tietämystä tietoverkkoasioista ja siksi niihin liittyvät tärkeimmät käsitteet on ymmärrettävä.

### 2.1.1 Tiedonsiirron perusteet

Kaikki tiedonsiirto nykyaikaisessa tietojärjestelmässä eri osien välillä on digitaalista. Digitaalisella signaalilla on kaksi tilaa: päällä (on) ja pois (off). Näitä tiloja kuvataan ykkösinä ja nollina. Tietotekniikassa yleisesti käytetään pääasiassa kahta tapaa siirtää tietoa: sarjasiirto ja rinnakkaissiirto. Tiedonsiirto tietokoneiden välillä tapahtuu pääsääntöisesti sarjamuodossa. Tietokoneiden välinen tiedonsiirto tapahtuu siis sarjoina ykkösiä ja nollia. Näitä kutsutaan myös biteiksi. Tietokoneiden välinen tiedonsiirto tapahtuu yleensä johdinparin tai valokuidun välityksellä. Sähköisesti johdinparissa bitti kuvataan jännitetasoilla: yleensä 1-bittiä vastaa +5 V jännite ja 0-bittiä 0 V jännite. (Hakala & Vainio, 2005)

### 2.1.2 Tietoverkot

Maailmassa on hyvin paljon erilaisia verkkotekniikoita. Moni yritys teki omia lähiverkkoratkaisujaan tietokoneiden verkottamisen alkuaikoina. Tietoverkot voidaan karkeasti jakaa kahteen tyyppiin. Toinen on datan ja toinen on puheen välittämiseen tarkoitettu verkko. Dataverkkotekniikat voidaan edelleen jakaa kahteen tyyppiin: Lähiverkko, Local Area Network (LAN) ja laajaverkko, Wide Area Network (WAN). (Anttila, 2000) Lähiverkolla useimmiten tarkoitetaan pientä verkkoa, jossa laitteet ovat toisiinsa yhteydessä yrityksen tai talouden sisäisesti. Laajaverkko peittää maantieteellisesti laajoja alueita. Laajaverkko yhdistää lähiverkot toisiinsa suureksi verkoksi. Internet on laajaverkon ääritapaus.

Verkkotekniikat käsittävät hyvin paljon erilaisia tapoja tiedon siirrolle. Näitä kutsutaan tietoliikennetekniikassa protokolliksi eli yhteyskäytännöiksi. Protokolla määrittelee ohjelmien tai tietokoneiden välisen tiedonsiirron tavan. Tietoverkkotekniikassa eri protokollia on satoja.

### 2.1.3 OSI-malli

OSI (Open Systems Interconnection) -malli on 80 -luvulla kansainvälisen standardisointiorganisaatio ISO:n (International Organization for Standardization) kehittämä malli. Tavoitteena oli, että siitä tulee kaikkien verkkotekniikoiden yhteensopivuusongelmat pois pyyhkäisevä tekniikka. Tässä se ei kuitenkaan onnistunut. OSI-mallista kuitenkin kehkeytyi ajan myötä niin sanottu referenssipinona toimiva seitsemän kerroksinen malli. Mallista puhutaankin monesti myös OSI-viitemallina. Vaikka täysin OSI-mallin mukaisia tietojärjestelmiä ei ole, on se kuitenkin erittäin hyödyllinen asia verkkojen toiminnan ymmärtämiselle. Tämä johtuu siitä, että OSI-mallin kerrosajatus on sama kaikille protokollille. OSI-mallin perusajatuksena on siihen kuuluvan kerroksen toiminta siten, että alemmalta kerrokselta saatu tieto käsitellään ja välitetään ylemmälle kerrokselle. (Anttila, 2000)

Kerrosmallin avulla jokainen kerros voidaan toteuttaa itsenäisenä kokonaisuutenaan. Tästä on etua monessa asiassa. Kerrosmallin avulla on eri protokollien toiminta helpompi ymmärtää kun tiedetään, missä kerroksessa toiminta tapahtuu. Myös suunnittelu ja kehitystyö helpottuvat ja nopeutuu, kun koko rakennetta ei tarvitse uudistaa kerralla. (Anttila, 2000)

OSI-mallissa tietojärjestelmälle on määritelty seitsemän perustehtävää. Nämä ovat mallissa kuvattu kerroksina. Alemmat kerrokset yhdestä kolmeen määrittelevät laitteistojen ja niihin läheisesti liittyvien protokollien toimintaa. Näitä kerroksia kutsutaan yleisesti alakerroksiksi. Ylemmät kerrokset määrittelevät asiakas-palvelin-sovelluksen ohjelmallisen toiminnan. OSI-mallin seitsemän tasoa alimmalta ylimmälle ovat fyysinen kerros, siirtoyhteyskerros, verkkokerros, kuljetuskerros, yhteysjakso- eli istuntokerros, esitystapakerros sekä sovelluskerros. (Hakala & Vainio, 2005)

Fyysinen kerros on OSI-mallin alin kerros. Tällä kerroksella määritellään yhden bitin siirtämiseen tarvitut fyysiset, mekaaniset ja sähköiset asiat kuten signaalien jännitetasot sekä liitin- ja kaapelityypit. (Anttila, 2000) (Hakala & Vainio, 2005)

Siirtoyhteyskerros määrittelee miten lähetettävästä datasta muodostetaan kaapelointijärjestelmässä siirrettäviä yksiköitä kuten kehyksiä tai soluja. Kehys on selvitetty tarkemmin kohdassa 2.1.4. Kaikki datapakettien liikkuminen tietoliikenneverkoissa tapahtuu jonkinlaisten osoitteiden perusteella. Siirtoyhteyskerros määrittelee lähettävän ja vastaanottavan laitteen fyysiset osoitteet (MAC, Media Access Control -osoite). Erilaisia osoitteita määritellään myös muilla OSI-mallin tasoilla. Siirtoyhteyskerros on useimmiten voimakkaasti riippuvainen fyysisestä kerroksesta. (Anttila, 2000) (Hakala & Vainio, 2005)

Verkkokerros määrittelee eri liikennöintimuotojen välisen priorisoinnin ja verkkojen välisessä tietoliikenteessä tarvittavan reitityksen. Reititys tapahtuu pääasiassa osoitteiden perusteella. Lähiverkoissa käytetään yleisimmin IP-protokollan määrittämiä osoitteita. (Hakala & Vainio, 2005)

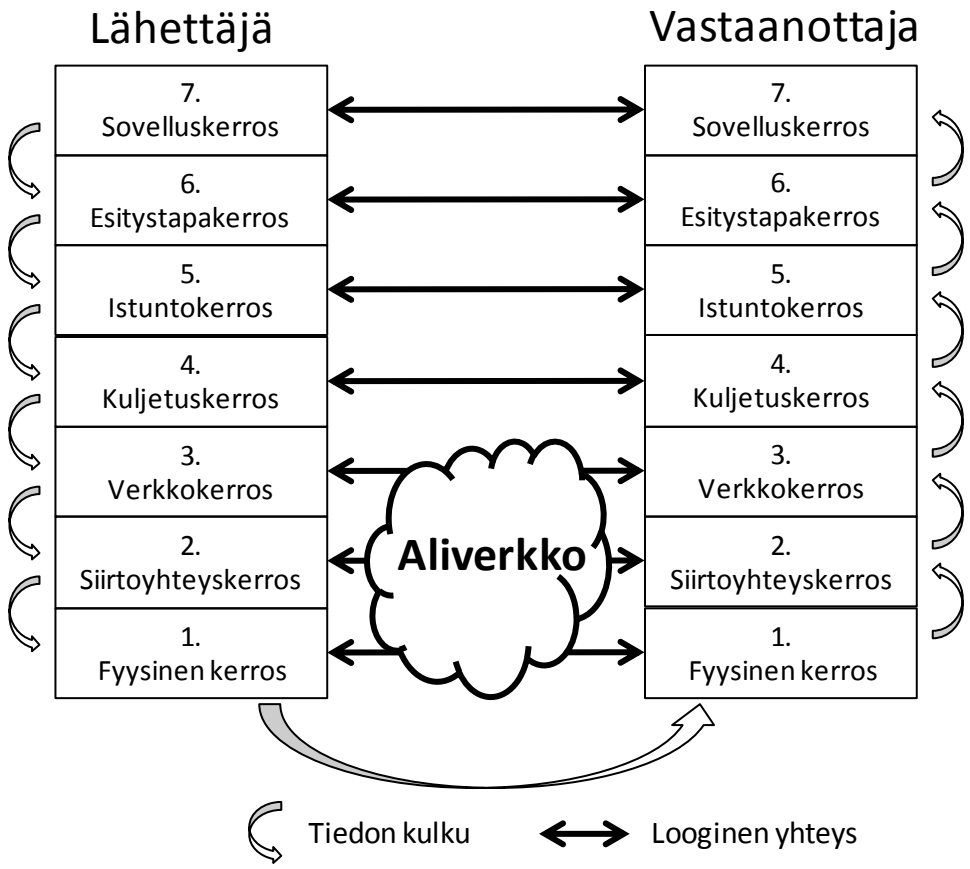
Kuljetuskerroksen tehtävänä on pilkkoa sovellusten lähettämä datavirta käsittelykokoisiin yksiköihin. Näistä käytetään yleisimmin nimityksiä segmentti tai paketti. Kerroksen tehtäviin kuuluu myös yhteyden muodostaminen ja purkaminen asiakas- ja palvelinohjelmistojen välillä. Lisäksi lähetetyn datan perille menon varmistus on myös kerroksen tehtävä. (Hakala & Vainio, 2005)

Istuntokerroksen tehtäviin kuuluvat sovellusten toimintojen koordinointi laitteiden välillä, käyttöoikeuksien tarkistukset sekä muut järjestelmän suojauksiin liittyvät asiat. Kerroksen ohjelmat tarjoavat tarvittavat salausmenetelmät ja kirjautumisrutiinit. Keskusmuistialueiden suojaus kuuluu myös istuntokerroksen tehtäviin. (Hakala & Vainio, 2005) (Anttila, 2000)

Esitystapakerros määrittelee, missä muodossa asiakkaan ja palvelimen välinen liikenne tapahtuu. Tiedon siirtäminen tapahtuu binäärimerkkijonona järjestelmien välillä. Koska tässä siirrossa käytetään vain yhtä tietotyyppiä, täytyy määritellä, miten alkuperäiset tietotyypit koodataan binäärimerkkijonoiksi ja miten ne puretaan takaisin alkuperäisiksi tietotyypeiksi vastaanottavassa sovelluksessa. Kerroksen tehtävät suorittaa käyttöjärjestelmä. (Hakala & Vainio, 2005)

Sovelluskerros tarjoaa verkkopalveluja sovelluksille. Sähköpostin siirtäminen, tiedostojen avaaminen, sulkeminen, kirjoittaminen ja lukeminen kuuluvat esimerkiksi kerroksen tehtäviin. Nykyisissä lähiverkkojen sovelluksissa ja käyttöjärjestelmissä neljää ylintä OSI-mallin kerrosta ei voida erottaa toisistaan, vaan ne muodostavat yhden ohjelmallisen kokonaisuuden. (Anttila, 2000) (Hakala & Vainio, 2005)

Laitteet kommunikoivat keskenään OSI-mallin seitsemän kerroksen kautta. Jokainen kerros kommunikoi vastapään vastaavan kerroksen kanssa (looginen yhteys). Laitteiden sisällä ylempi kerros käyttää alemman kerroksen palveluja hyväkseen. Kuvassa 1 on esitetty OSI-mallin kerrokset ja toiminta tietoa siirrettäessä.




KUVA 1. OSI-malli

### 2.1.4 Kehys

Kehys tiedonsiirtotekniikassa tarkoittaa lähetettävää datapakettia, jolla on tietty rakenne jonka avulla paketti löytää määränpäänsä ja jonka toiminta sisältää kehyksen tahdistuksen. Kuvassa 2 on esitettynä käytetyimmän lähiverkkotekniikan, ethernetin, kehyksen rakenne. Tietotekniikassa yksi tavu vastaa kahdeksaa bittiä. Kehyksen jokaisella osalla on oma toimintansa. Tahdistus kertoo vastaanottajalle, milloin varsinainen kehys alkaa. Tyyppi/pituus-kenttä kertoo kehyksen pituuden tai sisällön. Tarkistuskoodi-kentän avulla saadaan selville tuliko kehys vikaantumatta perille. (Anttila, 2000)

| 8 tavua | 6 tavua | 6 tavua | 2 tavua | 46 - 1500 tavua | 4 tavua |
|---|---|---|---|---|---|
| Tahdistus | Vastaanottajan osoite | Lähettäjän osoite | Tyyppi /pituus | Data | Tarkistus-summa |

KUVA 2. Peruskehyksen (Ethernet II) rakenne

### 2.1.5 TCP/IP

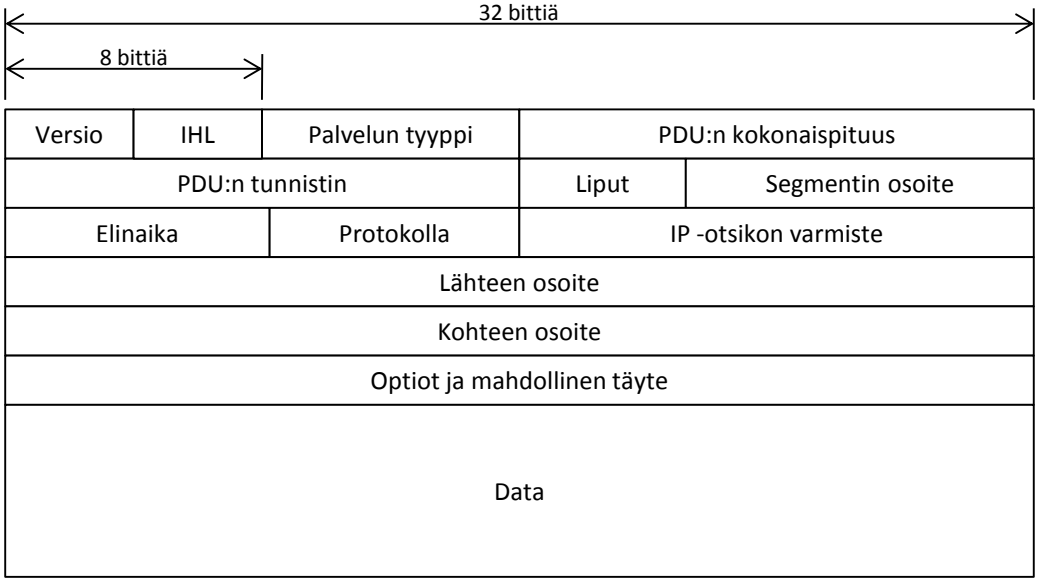
Transmission Control Protocol / Internet Protocol (TCP/IP) on ennen OSI-mallin kehittämistä toteutettu protokollaperhe. Internet on täysin erilaisista laitteista, käyttöjärjestelmistä ja verkoista koostuva verkkojen verkko. TCP/IP on alun perin suunniteltu internet-käyttöön, tehtävänä tarjota tälle useammista pienemmistä verkoista koostuvalle verkkojen verkolle tarpeelliset liikenne- ja viestinvaihtosäännöt. TCP/IP on luotu mahdollistamaan täysin erilaisten verkkojen ja laitteiden välinen liikennöinti. Suurin osa lähiverkoista ja internet perustuu TCP/IP protokollaperheeseen. (Puska, 2000) (Hakala & Vainio, 2005)

TCP on toinen TCP/IP protokollaperheen kuljetuskerroksen protokollista. Toinen on User Datagram Protocol (UDP), jota käsitellään tarkemmin kohdassa 2.1.7. TCP-protokolla on yhteydellinen. Tämä tarkoittaa, että ennen datasiirron aloittamista lähettäjä neuvottelee vastaanottajan kanssa yhteyden muodostamisesta. Yhteydetön protokolla tarkoittaa, että tätä neuvottelua ei tehdä ja siten pakettien välittymisestä ei voida olla varmoja. TCP-protokollan päätehtävänä on tarjota luotettava yhteydellinen tiedonsiirtotie kahden laitteen välille. Luotettavuus saavutetaan lähettämällä data tarvittaessa uudestaan siinä tapauksessa kun lähetettyyn dataan ei olla saatu kuittausta tietyssä ajassa.

IP-verkoissa liikutellaan IP-tietosähkeitä, joilla on tietty rakenne. Näitä kutsutaan myös datagrammeiksi. Kullakin protokollalla on omanlaisensa tietosähkeen rakenne. Tietosähkeen rakenne kuvataan usein pinona, jonka leveydeksi on kuvattu 32 bittiä. Kuvassa 3 on esitetty IP-tietosähkeen rakenne. Kuvattua tietosähkettä tulee lukea vasemmalta oikealle ja ylhäältä alas pitäen mielessä, että tiedonsiirto verkon yli tapahtuu pitkän bittijonon muodossa. Toiminnan kannalta tietosähkeen jokaista osiota ei ole tarpeellista selvittää tarkasti.

Elinaika (TTL, Time To Live) ilmaisee, kuinka kauan IP-tietosähkettä välitetään reititinverkossa. Jokainen reititin vähentää kentän arvoa yhdellä ja tuhoaa tietosähkeen jos kentän arvoksi tulee siirron aikana nolla. Lähettäjälle lähetetään tästä virheilmoitus. (Puska, 2000)

IP-otsikon varmiste sisältää otsikon varmistussumman. Reitittimet muuttavat IP-otsikon kenttiä ja siksi varmistussumma tulee laskea uudelleen joka reitittimessä. Näin varmistetaan otsikon eheys koko matkan lähettäjältä vastaanottajalle. (Puska, 2000)




KUVA 3. IP-tietosähkeen rakenne

Kaikki datapakettien liikkuminen tietoliikenneverkoissa tapahtuu jonkinlaisten osoitteiden perusteella. TCP/IP protokollaperhe käyttää IP-osoitteita datapakettien välittämiseen. IP-osoite koostuu 32 bitistä. Bittimuotoisia osoitteita on ihmisen vaikea muistaa ja käsitellä. Tämän vuoksi osoite esitetään normaalisti neljän arvoltaan 0 - 255 olevan, pisteillä toisistaan erotetun kentän avulla. Näitä kenttiä kutsutaan myös okteteiksi. Kentät määrittelevät hierarkkisesti verkon sekä tietokoneen tai muun laitteen osoitteen. IP-osoite voidaan jakaa kahteen osaan. Toinen osa määrittelee mihin verkkoon laite kuuluu ja toinen osa määrittelee laitteen osoitteen. Näistä puhutaan verkko- tai net-id:nä ja laite- tai device-id:nä. (Hakala & Vainio, 2005) (Anttila, 2000) Jonkin tietokoneen IP-osoite voisi olla sisäverkossa esimerkiksi 192.168.0.1. Perinteisten 32-bittisten IP-osoitteiden määrä käy vähiin niiden suhteellisen pienen määränsä vuoksi. Uusi IP Version 6 (IPv6) -protokolla on kehitetty nykyisen 32-bittisen IP Version 4 (IPv4) -protokollan seuraajaksi. Edelleen kuitenkin suurin osa kaikista verkon IP-osoitteista on IPv4-protokollan mukaisia.

TCP/IP ei ole täysin verrattavissa OSI-malliin vaan se on huomattavasti yksinkertaisempi. Kaikkia OSI-mallin mukaisia tehtäviä ei ole huomioitu ja yksittäinen TCP/IP-kerros huolehtii useamman OSI-mallin kerroksen tehtävän. (Anttila, 2000) (Hakala & Vainio, 2005) TCP/IP-protokollaperhettä kuvataan usein nelikerroksisena. Kuvassa 4 on kuvattu, miten TCP/IP-protokollaperhe voidaan suhteuttaa OSI-malliin.


KUVA 4. OSI-malli suhteessa TCP/IP-protokollaperheeseen

### 2.1.6 Aliverkotus

Aliverkon peitettä käytetään tietoverkkojen aliverkotukseen. Aliverkotuksella tarkoitetaan verkkojen jakamista pienempiin osiin.

IP-osoite jaetaan kahteen osaan aliverkon peitteen avulla. Aliverkon peite, jota myös aliverkon maskiksi kutsutaan, on IP-osoitteen tavoin 32-bittinen. Aliverkon peite on aina bittimuotoisena rivi 1-bittejä jota seuraa rivi 0-bittejä. Yksi aliverkon peitteen esitystapa on jakaa se IP-osoitteen kaltaisesti neljään desimaalilukumuotoiseen osioon pisteillä erotettuna. Toinen esitystapa aliverkon peitteelle on yksinkertainen IP-osoitteen perään merkattava ”/nn”, jossa nn kohdalle merkataan aliverkon peite desimaalilukuna 0 - 31. Desimaaliluku tässä esitystavassa siis kertoo suoraan aliverkon peitteen 1-bittien määrän. Esimerkiksi 192.168.0.1/24 voidaan ilmoittaa: IP-osoite: 192.168.0.1, aliverkon peite: 255.255.255.0. Lyhyempi merkkaustapa on yleistymässä. Aliverkon peitteen tehtävänä on erottaa net-id ja device-id IP-osoitteessa. Se ”peittää” tai ”maskaa” osan IP-osoitteesta, johon se on liitetty jättäen net-id:n pakettia välittävän laitteen tulkittavaksi. Net-id:n avulla laite voi nopeasti yksinkertaisin digitaalisin toimenpitein selvittää, onko

kyseessä oleva IP-osoite omassa aliverkossa, jolloin se voidaan välittää kohteeseensa lähiverkon menetelmin vai muualla, jolloin se täytyy välittää reitittimelle, joka välittää sen eteenpäin ulkoverkon kautta. Aliverkon peitteen ”peitto” määrittelee ykkösten ja nollien määrän ja siten myös kyseisen aliverkon laajuuden. Aliverkon peitteen avulla siis nähdään IP-osoitteesta nimenomaan sen verkko-osa. Tämä on erittäin tärkeä asia käytännön liikennöinnissä. (Anttila, 2000)

Aliverkotus tapahtuu kasvattamalla aliverkon peitettä. Kun aliverkon peitettä kasvatetaan yhdellä, jakautuu verkko kahteen aliverkkoon. Vastaavasti verkko laajenee kaksinkertaiseksi jos peitettä vähennetään yhdellä. Tätä kutsutaan yliverkottamiseksi. Reitittimien toisiinsa liittämisessä tulee ottaa huomioon aliverkotukseen, aliverkon peitteeseen ja reitittimien IP-osoitteisiin liittyvät asiat.

### 2.1.7 UDP

UDP (User Datagram Protocol) on TCP/IP-protokollaperheen toinen kuljetustason protokolla. UDP-protokollaa voidaan käyttää sovelluksissa, joissa ei vaadita luotettavuutta ja jotka lähettävät jatkuvasti, mutta epäsäännöllisin välein verkkoon lyhyitä viestejä. UDP on yhteydetön protokolla, eli tietosähkeiden perille pääsyä ei varmenneta. Esimerkiksi Domain Name System (DNS) -palvelu käyttää UDP:tä. (Hakala & Vainio, 2005)

UDP:n tietosähkeen pituus on huomattavasti TCP:n ja IP:n tietosähkeitä lyhyempi. Sen minimipituus on 8 tavua. Tietosähkeen lyhyys nopeuttaa datan siirtoa, mutta ilman tarkistussumman laskemista ja tietosähkeen perille pääsyn varmistamista datan siirron onnistumista ei voida varmentaa.

### 2.1.8 DNS ja DDNS

Domain Name System (DNS) on tärkeä osa internetin ja verkkojen käyttäjäystävällisyyttä. Palvelun avulla voidaan kääntää looginen nimi kuten www.google.fi tiedonsiirron edellyttämäksi IP-osoitteeksi. DNS on siis toiminto, jonka avulla loogiset, helposti muistettavat verkkotunnukset sidotaan tiettyihin IP-osoitteisiin. DNS toimii Domain Name Service -palvelimien kautta. Verkon selaamiseen käytetty ohjelma lähettää nimikyselyn siihen syötetystä verkkotunnuksesta tietyille nimipalvelimille, joiden kautta

lopulta saadaan tieto, mitä IP-osoitetta syötetty verkkotunnus vastaa ja datan siirtäminen voidaan aloittaa. (Anttila, 2000)

Dynamic DNS (DDNS) on palvelu, jonka avulla voidaan jatkuvasti päivittää määritetyn verkkotunnuksen sitoutumista IP-osoitteeseen. Tämä on erittäin hyödyllinen, jos palvelimen IP-osoite muuttuu jatkuvasti. DDNS palvelun avulla voidaan siis sitoa palvelin verkkotunnukseen vaikka palvelimen IP-osoite muuttuu. Verkossa on tarjolla monia ilmaisia DDNS palveluita, jotka tarjoavat muutaman käyttäjän itse määrittämän verkkotunnuksen.

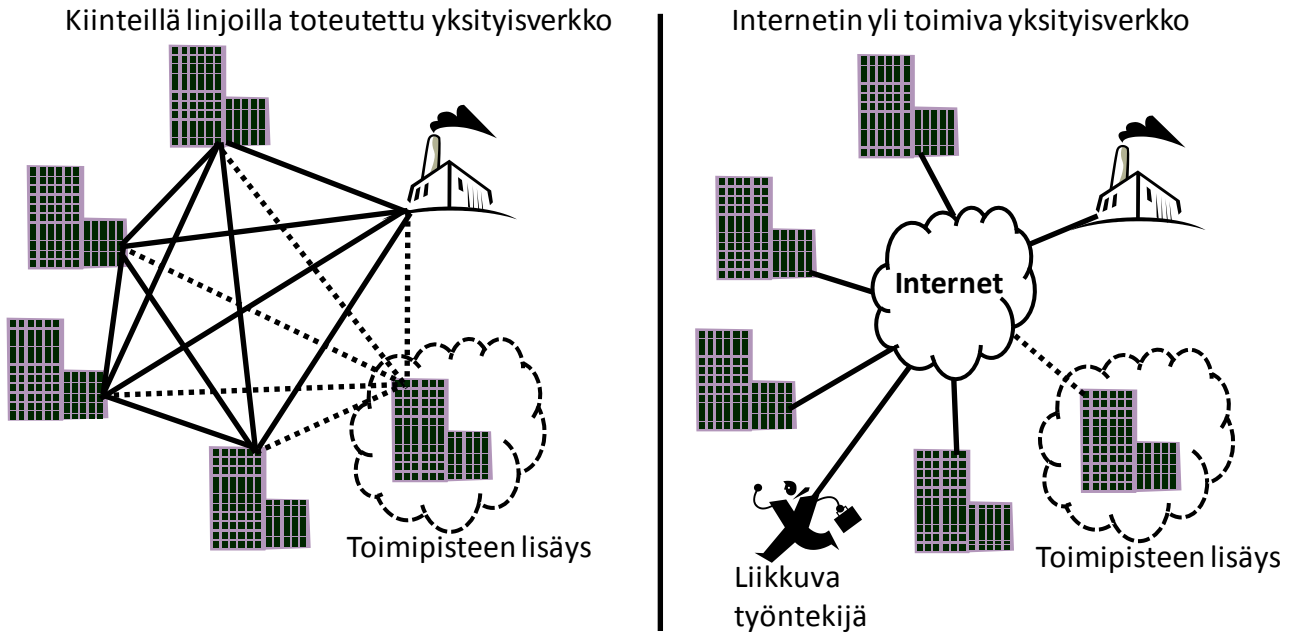
## 2.2 Etäkäyttöyhteydet ja VPN

Monella yrityksellä on tarve yhdistää toisistaan etäällä sijaitsevat toimipisteensä samaan tietoverkkoon. Tämän toteuttamiseksi voidaan palveluntarjoajalta tilata toimipisteiden välille kiinteä yhteys. Vaikkakin hieman vanhentunut, on tämä tapa edelleen käytössä monella yrityksellä. Kuitenkin kustannukset ovat melko suuria ja toimipisteiden määrän kasvaessa kustannukset kasvavat nopeasti. Jokaisen yhteyden ollessa pisteestä pisteeseen -tyyppinen ja toimipisteiden määrän kasvaessa kustannukset kasvavat nopeasti hyvin suuriksi. Etenkin maiden väliset kiinteät yhteydet ovat kalliita. (Bollapragada, Khalid, & Wainner, 2005)

Kustannustehokkaampi ja joustavampi tapa toteuttaa tämän kaltainen verkotus on käyttää internetin yli olevaa virtuaalista yhteyttä yhdistämään eri toimipisteet. Tämän kaltaisia ratkaisuita nimitetään Virtual Private Networkeiksi (VPN). VPN käsitteenä on hieman epäselvä ja vaihtelee. Tietoliikennealalla ei välttämättä olla samaa mieltä, mikä mielletään VPN:ksi ja mikä ei. Yleisesti VPN:n voisi määritellä tietoliikenneverkoksi, joka on rakennettu yrityksen tai yksilön yksityiseen käyttöön jaetun julkisen infrastruktuurin välityksellä. (Perlmutter & Zarkower, 2001) Jaetulla julkisella infrastruktuurilla tarkoitetaan yleensä internetiä.

Verrattaessa VPN kaltaista ratkaisua kiinteisiin pisteestä pisteeseen -menetelmällä toteutettuihin verkkoratkaisuihin ovat toimipisteet pelkästään internetiin yhteydessä eikä palveluntarjoajien kalliita vuokralinjoja tarvita. Ensimmäinen syy tällaisen ratkaisun toteuttamiselle on siis kustannusten pienentäminen. Etuna tämän kaltaiseen ratkaisuun on myös liikkuvien työntekijöiden yhdistämisen mahdollisuus. (Bollapragada, Khalid,

& Wainner, 2005) Kuvassa 5 on havainnollistettu virtuaalisen verkon etuja kiinteään yhteyteen verrattuna.



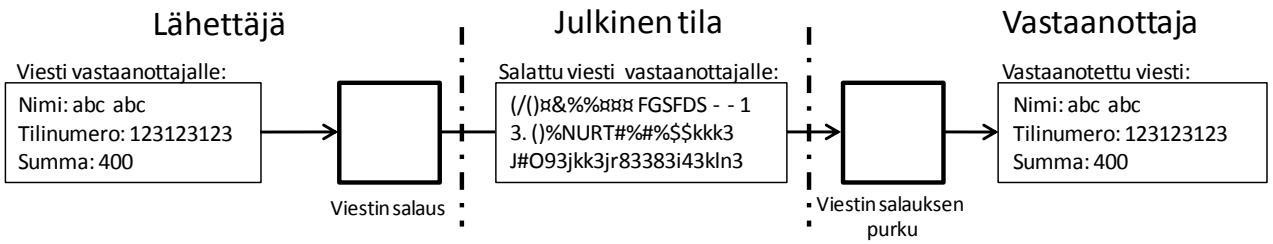

KUVA 5. Kiinteillä linjoilla toteutetun yksityisverkon vertailu internetin yli toimivaan virtuaaliseen yksityisverkkoon

Tuotantolaitoksilla on erityisiä perusteita etäkäyttöyhteyksien toteuttamiselle. Tietyt kunnossapidon toimenpiteet, joidenkin prosessien valvonta ja ohjaus sekä tuotannon ja prosessin pitkäaikainen analyysi ja valvonta voidaan suorittaa kokonaan etäyhteyden avulla jossain muussa toimipisteessä kuin itse tuotantolaitoksessa. Etäyhteys vähentää matkustamisen tarvetta.

## 2.3 Turvallisen tiedonsiirron perusteet

Riskejä löytyy aina käytettäessä julkista internetiä yksityisverkkojen muodostamiseen. Esimerkiksi tietoturva ja toimipisteiden välisen kaistanleveyden varauksen puuttuminen. (Bollapragada, Khalid, & Wainner, 2005)

Tietoturva on suuri kysymys etäyhteyksissä. Etenkin kohteen ollessa tuotantolaitos, jonka prosessiin mahdollisesti pystytään vaikuttamaan etäkäytön avulla. Kuinka tietoa voidaan siirtää julkisen median ylitse ilman, että sivusta mahdollisesti seuraavat eivät pysty sitä tulkitsemaan? Tieto voidaan salata tietyin algoritmein. Salausalgoritmit tarvitsevat jonkin syötteen tai toisin sanoen avaimen, jonka avulla tieto voidaan salata ja salattu tieto tulkita. Kuvassa 6 on esitetty salatun tiedon siirron periaate.




KUVA 6. Salatun tiedon siirtämisen periaate

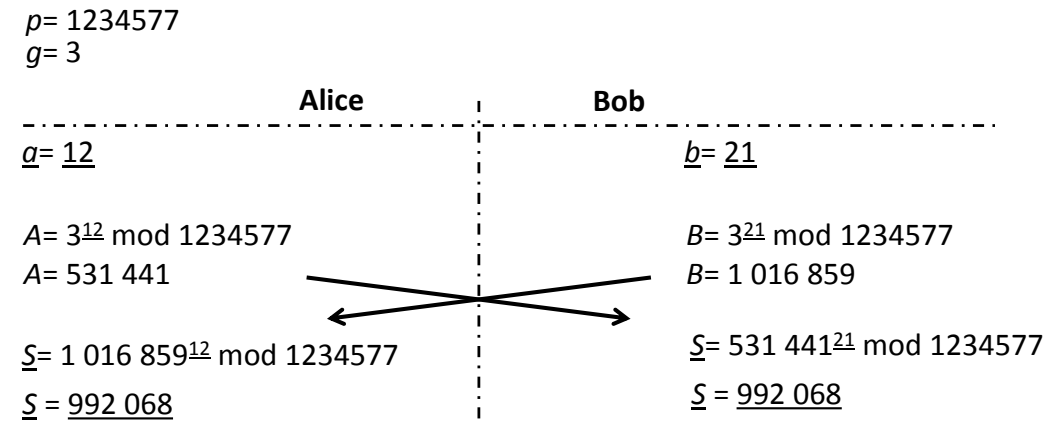
### 2.3.1 Tiedon salaus

On olemassa kaksi salausjärjestelmien luokkaa, joiden avulla osapuolet voivat viestiä toistensa kanssa turvallisesti: julkisten ja salaisten avaimien järjestelmät. Salaisten avaimien järjestelmässä kummatkin osapuolet sopivat ennakolta salaisesta avaimesta, jotka ainoastaan ne tietävät. Tätä avainta käytetään salaukseen ja salauksen purkuun käytetyissä algoritmeissa. Salaisten avaimien järjestelmät ovat nopeita ja helppoja tämän päivän verkottumisessa kohdatuille datavirroille. (Perlmutter & Zarkower, 2001)

Julkisen avaimen järjestelmässä kummallakin osapuolella on kaksi avainta. Julkinen avain, joka voi olla kaikkien tiedossa ja salattu yksityinen avain. Diffie-Hellmann (DH) -avaimenvaihdossa osapuolet keskustelevat keskenään julkisen ja yksityisen avaimen avulla ja lopulta päätyvät yhteiseen salattuun avaimeen, jota ulkopuolinen ei voi käytännössä selvittää tietojensa perusteella. Näin on keskusteltu yhteinen salattu avain julkisessa tilassa. Salatun avaimen avulla voidaan käynnistää turvattu tiedonsiirto osapuolten kesken käyttäen salaisen avaimen järjestelmää. Julkisen avaimen salausjärjestelmässä kuka tahansa voi lähettää toiselle osapuolelle tämän julkisen avaimen avulla salatun viestin jota kukaan muu ei voi tulkita. (Bollapragada, Khalid, & Wainner, 2005) (Perlmutter & Zarkower, 2001)

Diffie-Hellmann avaimenvaihtomenettely tapahtuu tarkemmin seuraavalla tavalla. Otetaan esimerkkinä tietotekniikassa usein keskenään keskustelevat Alice ja Bob. Alice ja Bob sopivat kaksi julkista parametria, $p$ ja $g$. Parametri $p$ on suuri alkuluku ja parametri $g$ on $p$:tä pienempi kokonaisluku, joka on sellainen, että funktio $g^n$ mod $p$, jossa $n$ on kokonaisluku, pystyy tuottamaan jokaisen kokonaisluvun välillä 1 ... $p$. Toisin sanoen $g$:n on oltava $p$:n primitiivinen alkio. Alice ja Bob sopivat käyttävänsä julkisia parametreja $p$ =1 234 577 ja $g$ = 3. Alice valitsee salaisen kokonaisluvun $a$ = 12 ja lähettää Bobille luvun $A = 3^{12}$ mod 1 234 577 = 531 441. Bob valitsee salaisen kokonaisluvun $b$ = 21 ja lähettää Alicelle luvun $B = 3^{21}$ mod 1 234 577 = 1 016 859. Alice laskee luvun $S$ =

$1\,016\,859^{12}$ mod 1 234 577 = 992 068. Bob laskee luvun $S = 531\,441^{21}$ mod 1 234 577 = 992 068. Näin ollaan saatu laskettua yhteinen salattu avain 992 068. Kuva 7 havainnollistaa toimenpidettä. Selventämisen vuoksi kuvassa 7 alleviivatut arvot ovat salaisia. Menetelmä perustuu siihen, että Alicen ja Bobin keskustelua mahdollisesti sivusta seuraavan on hyvin vaikea ratkaista yhtälöt $S = 1\,016\,859^{a}$ mod 1 234 577 ja $S = 531\,441^{b}$ mod 1 234 577. (Bollapragada, Khalid, & Wainner, 2005) (Perlmutter & Zarkower, 2001)

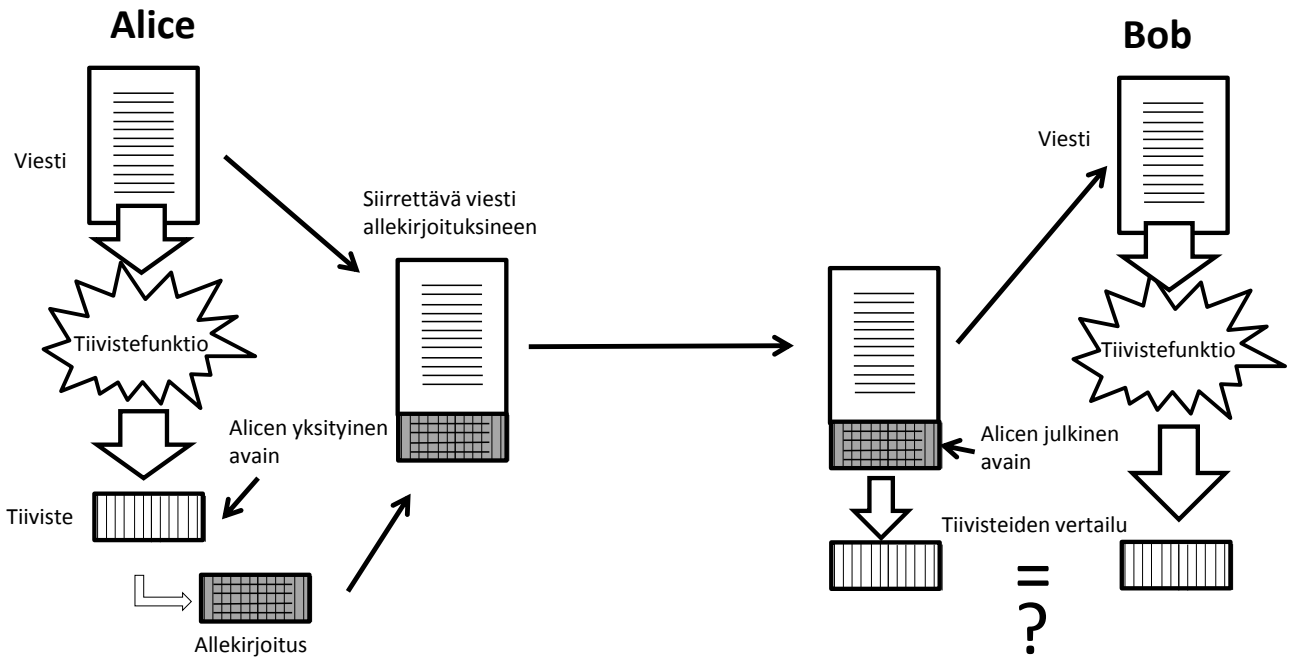



KUVA 7. Salatun avaimen neuvottelu

### 2.3.2 Tiivistefunktiot ja osapuolten todennus

Salatussa julkisen avaimen menetelmää käyttävässä tiedonsiirrossa osapuolten todennukseen käytetään apuna tiivistefunktioita. Tiivistefunktion tehtävänä on muuntaa mielivaltainen merkkijono tietyn mittaiseksi tiivisteeksi. Tiiviste esitetään usein heksadesimaalimuodossa ja ulkonäöltään se näyttää yksinkertaisesti jonolta sattumanvaraisia merkkejä. Tiivisteestä tulisi olla mahdotonta johtaa alkuperäinen mielivaltainen merkkijono. Alkuperäistä merkkijonoa ei pitäisi olla mahdollista tulkita millään tavalla: yhden merkin eroavaisuus muuttaa tuotetun tiivisteen täysin erilaiseksi. Lisäksi samaa tiivistettä tulisi olla mahdotonta johtaa kahdesta eri merkkijonosta. Esimerkkinä tiivistefunktion käyttämisestä osapuolten tunnistamisessa voidaan käyttää entuudestaan tuttuja Alicea ja Bobia. Alice haluaa varmistua, että vastaanottaja on oikeasti Bob, jolle hän lähettää tietoa. Alice tuottaa lähetettävästä datapaketista tiivisteen, jonka hän myös salaa käyttäen omaa yksityistä avaintaan. Alice lähettää datapaketin salatun tiivisteen kanssa Bobille. Bob purkaa salatun tiivisteen käyttäen Alicen julkista avainta ja tekee itse vastaanotetusta datapaketista, jonka hän on purkanut omalla salaisella avaimellaan, oman tiivis-

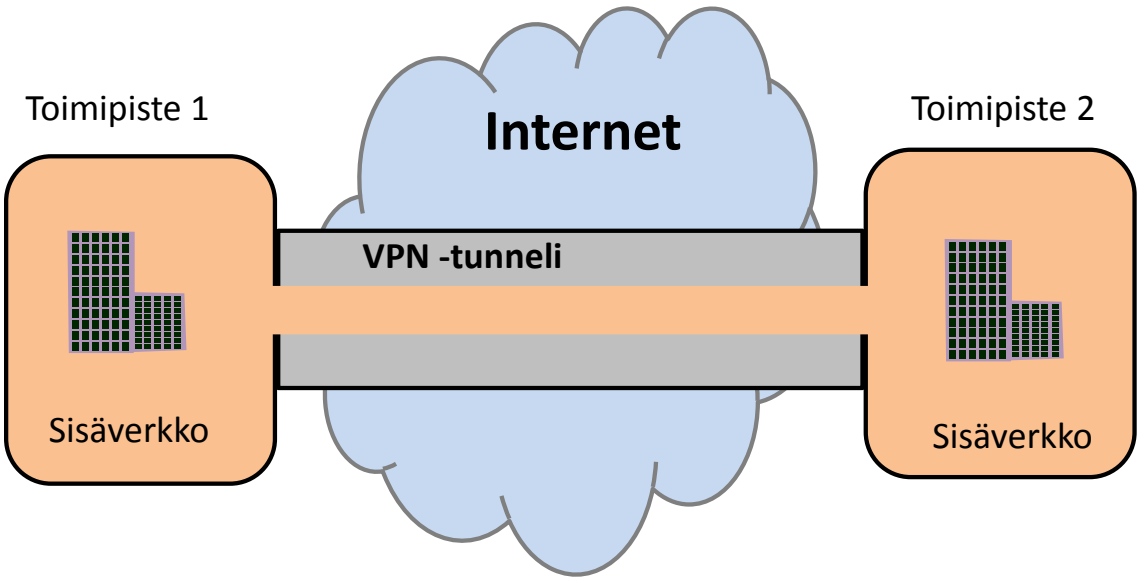
teen. Tämän jälkeen hän vertaa näitä kahta tiivistettä. Pieninkin muutos datassa aiheuttaa tiivisteiden eroavaisuuden ja näin osapuolet voivat olla varmoja keskustelevansa oikean henkilön kanssa. Kuvassa 8 on esitettynä lähettäjän todennuksen periaate. (Bollapragada, Khalid, & Wainner, 2005)




KUVA 8. Lähettäjän todennuksen periaate

## 2.4 VPN-yhteyden toteutustavat

VPN-yhteyksiä voidaan toteuttaa käyttämällä monia erilaisia protokollia. Yksinkertaisimmillaan kyse on kahden reitittimen välille toteutetusta tunnelista, jonka avulla sisäverkon liikenne kulkee internetin yli käyttäjien ja sovellusten sitä tarvitsematta tiedostaa. Tunneloinnilla tarkoitetaan yhtä protokollaa noudattavan datapaketin kapselointi toista protokollaa käyttävään datapakettiin. Tunneli-käsite on havainnollinen tapa kuvata datan kulkua verkon yli. Kuvassa 9 on esitetty VPN-yhteys internetin yli VPN-tunnelin läpi.




KUVA 9. VPN-tunnelin toimintaperiaate internetin läpi

Eri tapoja VPN-yhteyden toteuttamiselle on hyvin monia. Yleisimmin käytetty VPN etäyhteystekniikka on L2TP. (Bollapragada, Khalid, & Wainner, 2005) Muita yleisiä VPN-yhteyden toteuttamiseen tarkoitettuja protokollia ovat GRE- ja PPTP-protokollat sekä IPsec-protokollaperhe. Seuraavissa osioissa esitellään lyhyesti kaksi suosituista protokollista ja pureudutaan hieman syvällisemmin kahteen muuhun, joiden kanssa oltiin tämän opinnäytetyön merkeissä eniten tekemisissä.

### 2.4.1 L2TP

Layer 2 Tunneling Protocol on nimensä mukaisesti tarkoitettu kaikenlaisten OSI-mallin siirtoyhteyskerroksella toimivien yhteyksien hyödyntämiseen. L2TP muodostaa pisteestä pisteeseen -mallisia VPN-yhteyksiä. L2TP käyttää usein IPsec-protokollaperheen käyttämää salausta tiedon salaamiseen tunnelin sisällä. L2TP paketti on sisällytetty kokonaisuudessaan UDP-tietosähkeeseen. Etuna protokollalla on sen yleisyys ja laaja tuki laitteistoissa. (Perlmutter & Zarkower, 2001) (Hakala & Vainio, 2005)

### 2.4.2 GRE

General Routing Encapsulation -protokolla on yksinkertainen kapselointiprotokolla, joka pystyy tunneloimaan monia eri verkkokerroksen protokollia IP-verkon yli pisteestä pisteeseen. Lähetettävä tietosähke koostuu IP-verkon yli lähetettäessä IP-tietosähkeen

hyötykuormana olevasta GRE-paketista, jonka sisällä on toinen IP-tietosähke. GRE-kapselointia voidaan käyttää PPTP- sekä IPsec-tunneleiden muodostamiseen. (Tiso, 2012) (Perlmutter & Zarkower, 2001)

### 2.4.3 PPTP

Point to Point Tunneling Protocol (PPTP) on käytössä nykypäivänä useimmiten kotitoimistojen ja pienten toimipaikkojen liittämisessä yrityksen sisäverkkoon. PPTP hyödyntää siirtoyhteyskerroksen Point to Point Protocol (PPP) -protokollaa. PPP-protokolla mahdollistaa erilaisten lähi- ja laajaverkkoprotokollien siirtämisen samaa yhteyttä pitkin. PPTP:ssä PPP-kehys varustetaan GRE-otsakkeella, tämän jälkeen kehys asetetaan IP-tietosähkeeseen hyötykuormaksi. PPP-kehyksen sisältämä data myös salataan käyttämällä yksinkertaisia salausavaimia, jotka luodaan käyttäjätunnistuksen yhteydessä. Protokolla useimmiten käyttää käyttäjätunnus-salasana-yhdistelmää. (Hakala & Vainio, 2005) (Perlmutter & Zarkower, 2001)

PPTP-tunnelin aloittamiseksi PPTP-asiakas muodostaa TCP-istunnon PPTP-palvelimen kanssa. Tämän jälkeen tunnelin muodostaminen neuvotellaan käyttäjän valtuuttamisella palvelimelle. Tunnelin muodostuttua GRE-kapseloidut datapaketit voivat virrata kumpaankin suuntaan asiakkaan ja palvelimen välillä. Kun käyttäjä on lopettanut tehtävänsä PPTP-asiakas lähettää palvelimelle tiedon, että istunto voidaan lopettaa ja tunneli purkaa. PPTP-tunneli useimmiten toteutetaan asiakas-palvelin-mallisesti. (Perlmutter & Zarkower, 2001)

### 2.4.4 IPsec

IP Security Architecture (IPsec) ei ole yksittäinen protokolla vaan VPN-yhteyden muodostamiseen luotu protokollaperhe. IPsec koostuu kolmesta perustekijästä: todennus, salaus ja avaimenhallinta. Näitä asioita käsitellään kohdissa 2.3.1 ja 2.3.2. IPsec käyttää Internet Key Exchange -protokollaa määrittämään salausavaimet turvallisesti ennen tunnelin muodostamista. (Jackson, 2010) IKE käyttää kohdassa 2.3.1 kuvattua menetelmää salausavainten neuvotteluun. Todennus suoritetaan IPsec-otsakkeen avulla. IPsec-otsake voi koostua Authentication Header (AH) -otsakkeesta tai Encapsulating Security Protocol (ESP) -otsakkeesta. IPsec voi myös käyttää ESP- sekä AH-otsakkeita. Datakuorman salaus IPsecissä tapahtuu ESP-protokollan avulla. AH-protokolla ei siis

suorita datakuorman salausta, vain osapuolten todentamisen. ESP-protokollalla voidaan suorittaa kummatkin toiminnot. (Perlmutter & Zarkower, 2001)

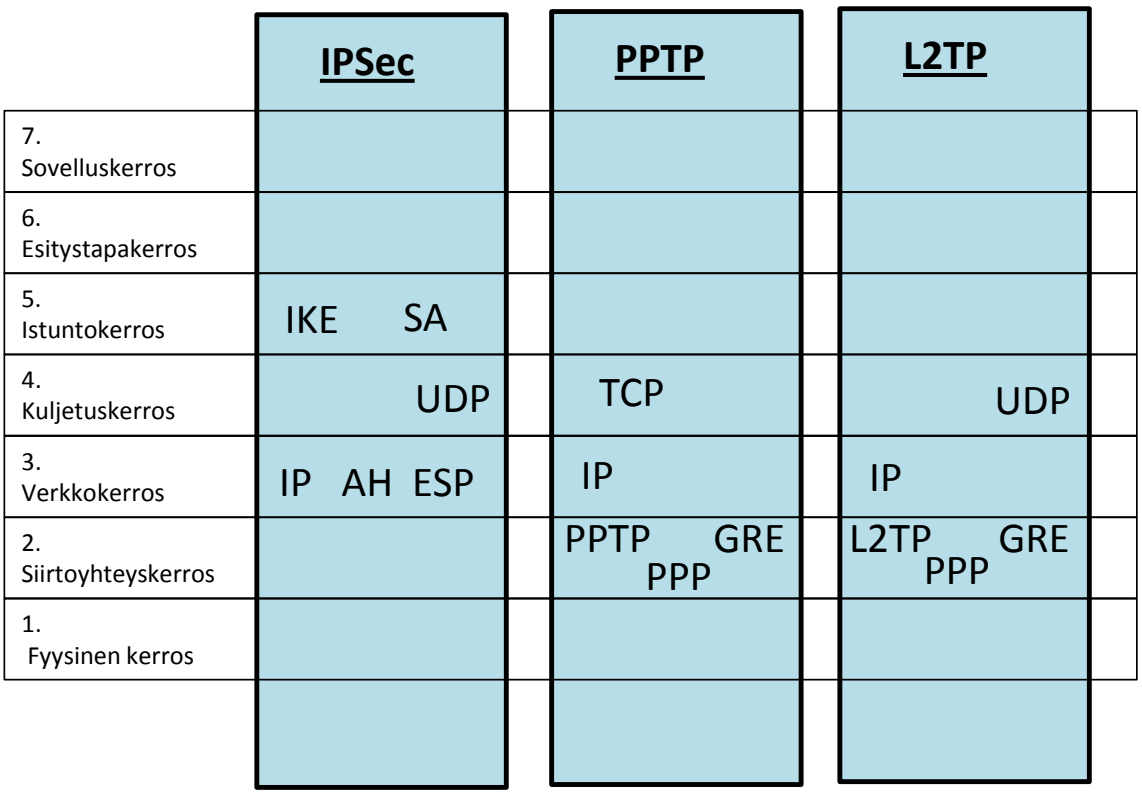
ESP:llä on kaksi eri toimintatilaa: tunneli- ja kuljetustila. Näiden tilojen erona on IP-paketin kapselointi tunnelitilassa: IP-paketti kapseloidaan toisen IP-paketin sisälle muodostaen sisäkkäisen pakettirakenteen, jossa IP-paketin kuormana on toinen ESP:llä salattu IP-paketti. Kuljetustila ainoastaan lisää ESP-otsakkeen alkuperäiseen pakettiotsakkeeseen ennen edelleen lähetystä. (Perlmutter & Zarkower, 2001)

IKE-protokollan avulla IPsec muodostaa turvallisuusliiton, SA:n (Security Association), tunnelin eri päiden välille. IKE:llä on myös ominaisuus, jonka avulla se voi sopia avaimista uudelleen tietyn ajanjakson tai tavumäärän jälkeen. Tämä lisää yhteyden tietoturvaa. (Bollapragada, Khalid, & Wainner, 2005) (Perlmutter & Zarkower, 2001)

IKE:llä on kaksi eri moodia: aggressiivinen moodi ja päämoodi. Päämoodia käytetään, kun tunnelin kummankin pään IP-osoitteet ovat tiedossa. Esimerkiksi kun kahta kiinteällä IP-osoitteella varustettua yrityksen toimipaikkaa yhdistetään IPsec-tunnelilla. Aggressiivista moodia käytetään siinä tapauksessa, kun tunnelin toisen pään IP-osoite muuttuu joka kerta, kun tunneli halutaan muodostaa. Tällöin IKE:lle luodaan näitä koskevat käyttäjätunnusasettelut.

### 2.4.5 L2TP, PPTP ja IPsec OSI-mallissa

Kuvassa 10 on esitetty kolme suosittua VPN-yhteyden protokollaa ja niiden käyttöön liittyviä muita keskeisimpiä protokollia suhteutettuna OSI-malliin.




KUVA 10. VPN-yhteys OSI-mallissa

# 3 LAITTEISTOVALINNAT

## 3.1 Automaatiojärjestelmän valinta

Järjestelmälle asetettiin muutamia suuntaa antavia kriteerejä ja vaatimuksia. Lähtökohtaisesti ei määritelty mitään tiettyä merkkiä tai mallia millekään järjestelmän osalle. Tuli siis ottaa selvää, minkälaisia ratkaisuja markkinoilla on tarjolla.

### 3.1.1 Automaatiojärjestelmän kriteerit

Toimeksiantaja määritteli muutamia järjestelmältä vaadittavia asioita. Tuloja ja lähtöjä järjestelmälle arvioitiin lähtökohtaisesti 10 digitaalista tuloa, 10 digitaalista lähtöä, 5 analogista tuloa, jotka olivat lämpötilamittauksia sekä 2 analogista lähtöä. Tärkeimmät perusteet automaatiojärjestelmän valinnalle tuli olla helppo ja selkeä ohjelmoitavuus, järjestelmän laajennusmahdollisuudet, soveltuvuus suuremmassa teollisuuden automaatiojärjestelmässä käyttöön sekä mahdollisuus luoda turvallinen etäkäyttöyhteys järjestelmään. Automaatiojärjestelmän laajennettavuuden tuli ulottua suureen automaatiojärjestelmään asti, jossa voisi olla satoja tuloja ja lähtöjä. Vaatimuksena ei kuitenkaan ollut, että täysin samalla ohjaimella tulisi tämän olla mahdollista. Lähtökohtana oli, että tämä järjestelmä toteutetaan tietyllä ohjaimella ja siten saadaan käsitys, miten suurempi järjestelmä toteutettaisiin saman valmistajan tarjoamalla järeämmällä ohjaimella. Järjestelmään tuli olla myös mahdollista liittää paikallisnäyttö. Järjestelmää tuli olla mahdollista ohjata paikallisesti.

Toimeksiantaja määritteli myös muutamia vaihtoehtoisia ominaisuuksia järjestelmälle: kommunikointi LonWorks-kenttäväylän kanssa, GSM-hälytykset sekä valvontakameran liittäminen. Laitteistovalintaa tehtäessä ja markkinoiden soveltuvia laitteistoja kartoittaessa nämä ominaisuudet eivät olleet vaadittuja, mutta kuitenkin suuria etuja.

### 3.1.2 Markkinoiden tarjonta

Markkinoilla on tarjolla paljon ratkaisuja haluttuun sovellukseen. Eri ratkaisuja etsittiin muutamilta tunnetuilta valmistajilta, sekä internet-hakukoneiden avulla löydetyiltä aikaisemmin tuntemattomilta valmistajilta.

Yksi hyvin tunnettu, pieni ja edullinen PLC on Siemensin LOGO!. Eräs tärkeimpiä laitteiston valinnan kriteerejä on ohjaimen ohjelmoitavuus. Kävi ilmi, että LOGO!:lla ohjelmointi on melko rajoitettua. Koko PLC ohjelma on tehtävä FBD (Function Block Diagram) -ohjelmointikielellä yhteen suureen näkymään. Lisäksi aliohjelmien ja muiden hyödyllisten ominaisuuksien käyttö on rajoitettua. Lisäksi LOGO!:n käytettävyys suuremmassa automaatiojärjestelmässä on kyseenalainen. Siemensin PLC:stä on myös ennestään kokemusta ja siksi myöskään muut Siemensin ohjaimet eivät sovellu tähän tarkoitukseen.

Mitsubishi on suuri japanilainen monialainen yritysryhmä joka tarjoaa myös automaatioalan tuotteita. Mitsubishin valikoimassa on kaksi eri PLC sarjaa. Toinen on pieniin sovelluksiin tarkoitettu Alpha ja toinen on suurempiin sovelluksiin tarkoitettu Q. Kävi ilmi, että Alpha-sarjan ohjaimissa oli hieman epätavallinen ja rajoitettu ohjelmointitapa. Lisäksi järjestelmän skaalattavuus oli huono. Toinen Mitsubishin tarjoama PLC-tyyppi Q oli haluttuun sovellukseen hieman liian järeä. Q-tyypin PLC:den suositellut I/O-määrät lähtivät 256:sta. Mitsubishin ohjain haluttuun sovellukseen olisi ollut varteenotettava vaihtoehto, jos Alpha-mallissa olisi sama ohjelmointiympäristö kuin Q-mallissa.

Yksi tunnettu PLC valmistaja on Omron, jolta löytyy myös haluttuun sovellukseen soveltuvia ratkaisuja. Omron on kuitenkin entuudestaan tuttu järjestelmä joka vaatii myös kalliin lisenssin PLC:n ohjelmoinnin toteuttamiseen.

Unitronics on Israelilainen yritys joka tuottaa mm. laitteita, joissa on yhdistetty PLC ja HMI (Human Machine Interface). Tällainen ratkaisu olisi täysin sopiva kiinteistöautomaatiojärjestelmän toteuttamiseen. Kuitenkin suuremmassa automaatiojärjestelmässä tämän kaltaisia ratkaisuja käytetään prosessin ohjaukseen hyvin harvoin.

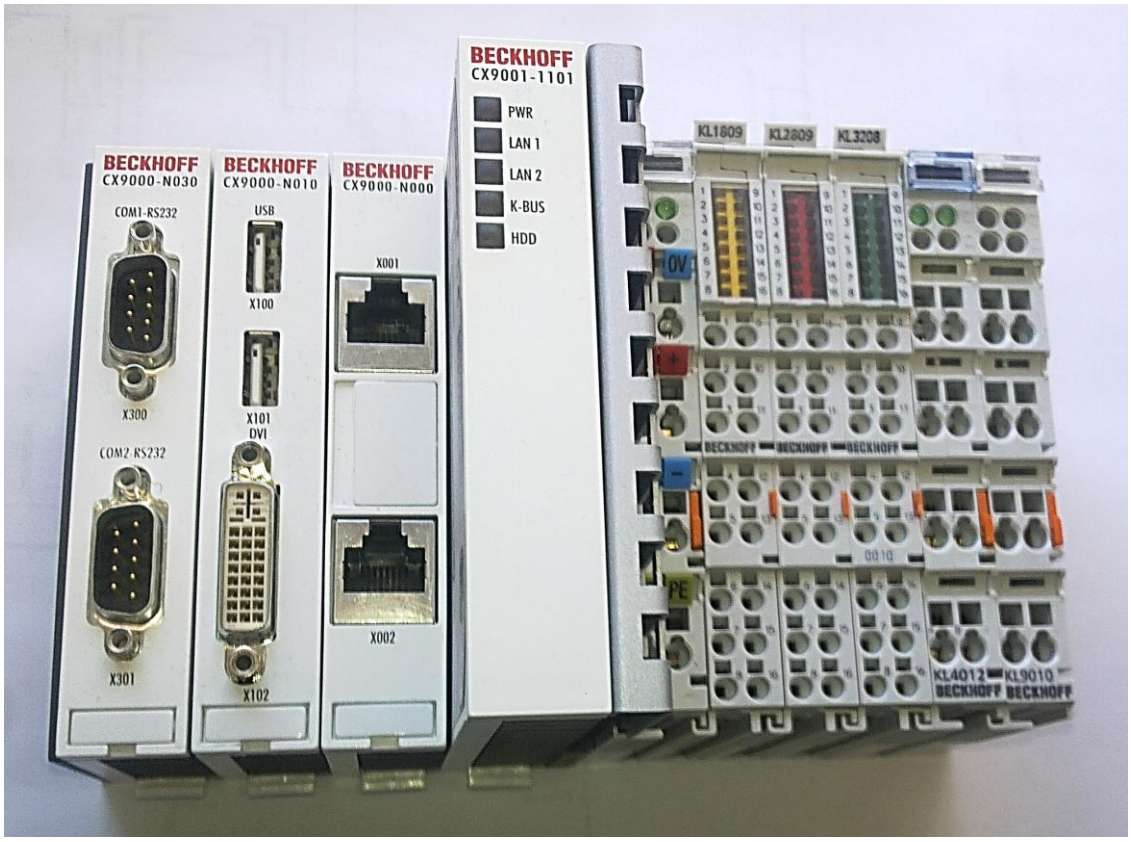
Mitsubishin Alpha-mallin kaltaisia ratkaisuja on hyvin monella valmistajalla. Esimerkkinä Mitsubishin lisäksi Allen Bradley, IMO, Crouzet ja Schneider. Monet ovat ulkonäöltäänkin hyvin samankaltaisia. Jotkut valmistajat käyttävät myös "smart relay" -nimitystä tämän kaltaisille ratkaisuille. Vaikka nämä ratkaisut voivat soveltua pienten kiinteistöautomaatiosovellusten toteuttamiseen, ovat ne liian kevyitä suurempaan järjestelmään. Tämän lisäksi ohjelmointi on usein rajoitettua ja monesti erilaista kuin saman valmistajan suurempaan automaatiojärjestelmään tarkoitetulla ohjaimella.

### 3.1.3 Tarjouspyynnöt

Phoenixille, Schneiderille ja Beckhoffille lähetettiin tarjouspyynnöt, joissa kuvattiin järjestelmän tarpeet ja vaatimukset. Phoenix ja Schneider ovat hyvin suuria ja tuotevalikoimaltaan laajoja sähkö- ja automaatioalan tuotteiden valmistajia. Lisäksi kummankin valmistajan katalogeista löydettiin mahdolliset vaihtoehdot käytettävään järjestelmään. Beckhoff on automaatioalan PC-pohjaisista ohjaimista tunnettu saksalainen valmistaja, jolla on laaja valikoima eri suorituskykyisiä ohjaimia. Lähetettyjä tarjouspyyntöjä seurasi nopeasti tarjoukset ja laitteistovalinta tehtiin niiden perusteella.

### 3.1.4 Valittu laitteisto

Ohjaimeksi valittiin Beckhoffin tarjoama CX9001. Ohjain kortteineen on esitettynä kuvassa 11. Kortteja ohjaimessa on viisi: yksi 16-kanavainen digitaalilähtökortti, yksi 16-kanavainen digitaalitulokortti, yksi 8-kanavainen PT-1000-kortti, johon voidaan kytkeä kahdeksan PT-1000-anturia suoraan, yksi 2-kanavainen analogialähtö-kortti sekä ohjaimen väylän terminointikortti.




KUVA 11. Beckhoff CX9001-1101

Verrattuna kahteen muuhun saatuun tarjoukseen vaikutti Beckhoffin tarjoama ratkaisu parhaalta. Suuria etuja Schneiderin ja Phoenixin tarjoamiin järjestelmiin oli järjestelmän helppo laajennettavuus, ohjelmointiin käytetyn ohjelman lisenssiasiat sekä hinta. LonWorks-väylän kanssa kommunikointia varten voidaan CX9001-ohjaimeen liittää yksinkertaisesti yksi kortti lisää, johon väylä voidaan liittää. Phoenixilla LonWorks-väylän kanssa kommunikointia varten tarvitaan erillinen ohjain. Phoenixin ja Schneiderin PLC-ohjelmointia varten olisi täytynyt hankkia lisenssi erikseen. Beckhoffin ohjaimessa on tarvittavan ohjelmointiohjelmiston lisenssi mukana. PLC:n ohjelmointia voidaan siis tehdä kun ollaan yhteydessä ohjaimeen. Beckhoffin valikoima korteista, mitä voidaan järjestelmään liittää on myös hyvin laaja ja korttien liittäminen järjestelmään on yksinkertaista.

## 3.2 Etäkäyttöyhteyden muodostamiseen tarvittavien laitteiden valinta

Etäkäyttöyhteys toteutetaan VPN-tekniikalla. Haluttu etäkäyttösovellus vaatii kohteeseen VPN-tunnelin sekä 3G-yhteyden. VPN ja 3G yhteyksien muodostamista varten tarvitaan niihin soveltuvat reitittimet. Tuli selvittää, mitä VPN-yhteys vaatii käytettäviltä laitteilta. Etsittiin myös reititinvaihtoehtoa, jossa 3G ja VPN ominaisuudet olisivat olleet samassa reitittimessä.

### 3.2.1 Vaadittavat laitteiden ominaisuudet VPN-yhteyden muodostamiseen

Laitteita valittaessa on varmistuttava muutamasta asiasta, jotta VPN-yhteyden muodostaminen on mahdollista. Jos VPN yhteys halutaan muodostaa reitittimellä, on sillä oltava täysi VPN tuki. Jos VPN yhteyden halutaan menevän reitittimen kautta, on reitittimellä oltava VPN läpäisy -ominaisuus. Yleensä valmistajat listaavat tarkemmin VPN tuen yhteydessä, mitä protokollia tarkalleen reititin tukee. VPN ominaisuuden yhteydessä myös monesti mainitaan, kuinka monta samanaikaista VPN yhteyttä reititin pystyy muodostamaan.

### 3.2.2 Markkinoiden tarjonta

Muutaman tietoverkkotuotteiden valmistajan tarjontaa kartoitettiin. Yksinkertainen tapa ottaa selvää valmistajien tarjonnasta on yksinkertaisesti selata suurimpia verkkokauppo-

ja. Hakuun voidaan laittaa ehtoja ja valita tuloksista kiinnostavat oman hintaluokan laitteet. Valmistajien sivujen selauksessa on se ongelma, että kaikkia malleja ei välttämättä tuoda Suomeen. Verkkokauppojen tarjonta on hyvin kattavaa ja laitteen saatavuudesta saadaan varma tieto. Verkkokauppojen selaamisen jälkeen käytiin myös muutamassa paikallisessa tietotekniikkaa myyvässä liikkeessä tiedustelemassa toivottuja laitteita, niiden hintoja ja käyttökokemuksia. Käyttökokemuksia selvitettiin myös internetistä hakukoneen avulla keskustelupalstoilta.

Cisco Systems on maailman suurin verkkolaitteiden valmistaja. Ciscon panostus verkkotekniikoiden kehittämiselle on myös ollut hyvin suuri. Valmistajalta löytyy monta erilaista ratkaisua haluttuun sovellukseen.

Myös muiden suurten valmistajien, kuten Dlinkin, ZyXELin, TP-Linkin ja Buffalon tarjoamia laitteita tarkasteltiin. Jokaiselta valmistajalta löytyy haluttuun tarkoitukseen soveltuvat ratkaisut. Lopulliseen laitevalintaan vaikutti laitteen ominaisuuksien lisäksi sen hinta ja muiden kertomat käyttökokemukset.

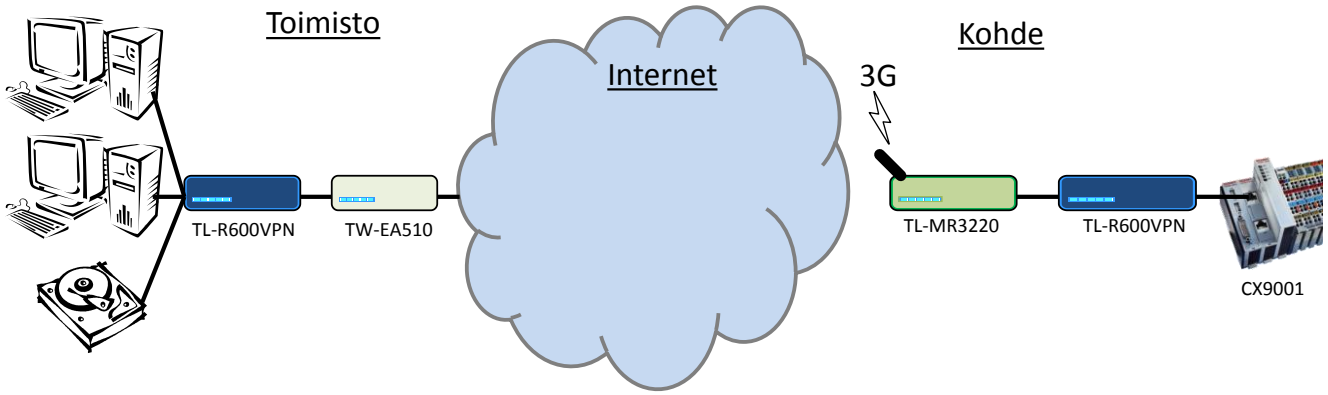
### 3.2.3 Valittu laitteisto

Käytetyksi laitteistoksi valittiin TP-Linkin kaksi eri mallia: TL-R600VPN ja TL-MR3220. Reitittimiä tilattiin 3 kappaletta: kaksi VPN-reititintä ja yksi 3G-reititin. Kohteeseen tulee yksi VPN- ja yksi 3G-reititin. Toimistolle tulee yksi VPN-reititin. Toimiston ja kohteen VPN-reitittimien välille on tarkoitus luoda pysyvä turvattu VPN-tunneli.

# 4 ETÄKÄYTTÖYHTEYDEN TOTEUTTAMINEN

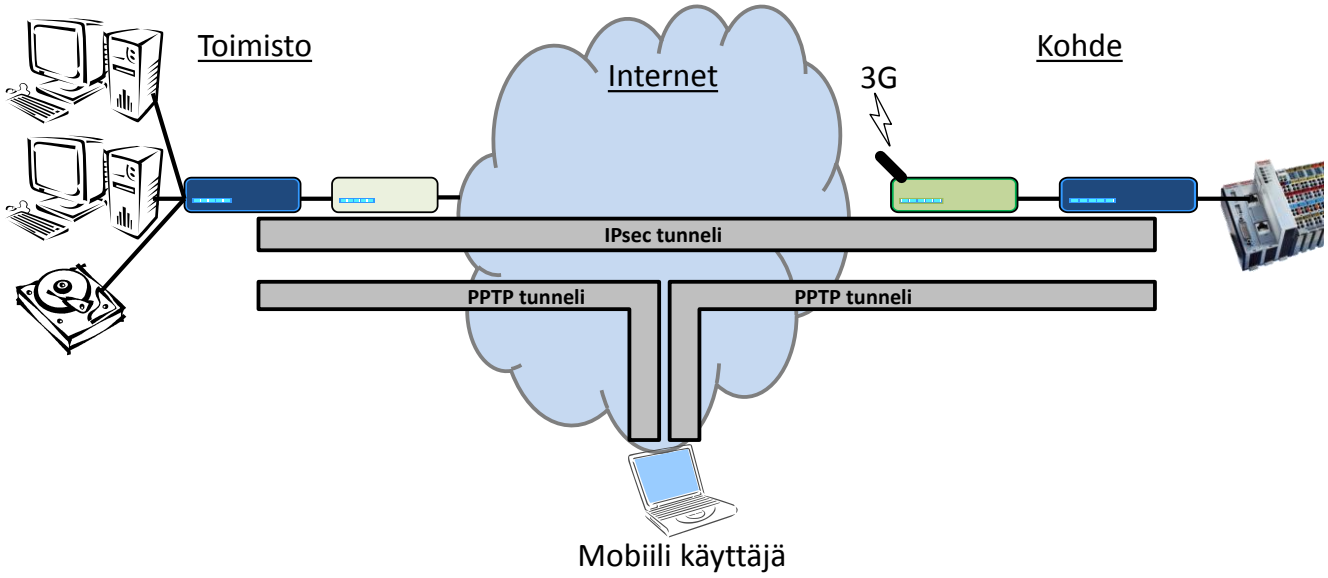
## 4.1 Toteutettu verkkoratkaisu

Hankituilla laitteilla toteutettiin kuvan 12 mukainen verkkoratkaisu toimistolle ja kohteeseen. Toimistolla oli jo valmiina TeleWellin TW-EA510 -ADSL reititin/modeemi. Toimistolla oleva verkkolevy haluttiin myös VPN-tunnelin taakse.




KUVA 12. Toteutettu verkkoratkaisu

VPN-tunneleiden toimintaa havainnollistetaan kuvassa 13. Toimiston ja kohteen välille muodostetaan pysyvä IPsec-tunneli. PPTP-tunneli voidaan muodostaa liikkuvan käyttäjän ja kohteen tai toimiston välille.




KUVA 13. VPN-tunneleiden toiminta toteutetussa verkkoratkaisussa

## 4.2 TW-EA510- ja TL-MR3220-reitittimien konfigurointi

Reitittimien asetuksia pääsee muokkaamaan yksinkertaisesti yhdistämällä internet selaimella reitittimen sisäverkon IP-osoitteeseen. Jos reitittimen IP-osoite ei ole tiedossa, voidaan se selvittää tietokoneen verkkoasetuksista. Windowsissa tämä voidaan tehdä CMD.exe:llä komennolla ipconfig. Reitittimen IP nähdään ”Default Gateway” -kohdasta. Ipconfig-komennon palaute on esitetty kuvassa 14.

```
C:\Users\Arttu>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9183:d568:75be:bdd4%10
   IPv4 Address. . . . . . . . . . . : 192.168.2.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1
```

KUVA 14. Reitittimen IP-osoitteen selvittäminen ipconfig-komennolla

Muutamia asetuksia täytyi muokata internetiin yhdistävistä reitittimistä, jotta VPN-yhteydet olisivat mahdollisia. TW-EA510-reitittimestä asetettiin VPN-reitittimen portti siltaavaksi. Portin ollessa siltaava, on siihen kytketty laite suoraan internetiin yhteydessä ja siten hakee IP:nsä ulkoverkosta.

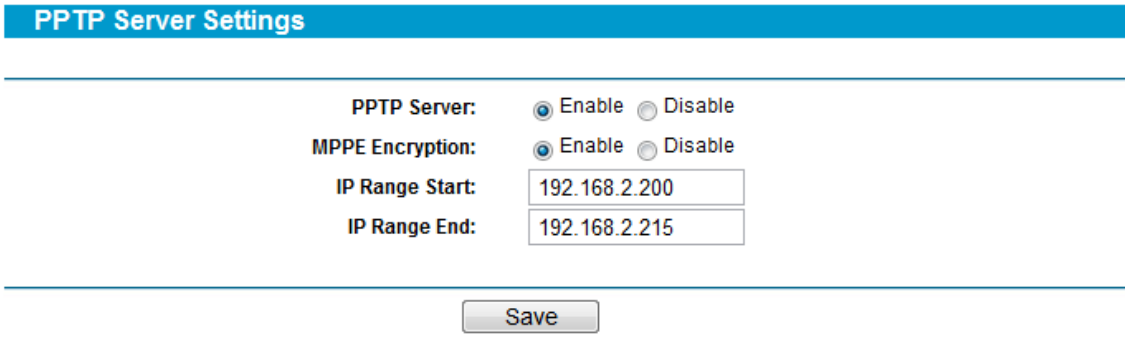
TL-MR3220-reitittimeen kytkettiin 3G-modeemi. Reitittimen WLAN (Wireless Local Area Network) -ominaisuus kytkettiin pois päältä sen ollessa turha. Reitittimen DDNS-asetuksia muokattiin kohdan 4.3.3 mukaisesti. Lisäksi reitittimelle asetettiin DMZ (Demilitarized Zone) -asetus päälle siihen kytketylle VPN-reitittimelle. DMZ-asetuksella kaikki ulkoverkon liikenne ohjataan myös määritettyyn sisäverkon IP-osoitteeseen.

## 4.3 TL-R600VPN reitittimien konfigurointi

Käytössä oli kaksi samanlaista VPN reititintä. Näiden välille luotiin pysyvä IPsec-tunneli. Lisäksi reitittimille luotiin käyttäjätunnuksia PPTP-yhteyksien muodostamista varten.

### 4.3.1 PPTP

Reitittimen PPTP-asetukset ovat yksinkertaiset. Kuvassa 15 on esitetty reitittimen PPTP-palvelinta koskevat asetukset.



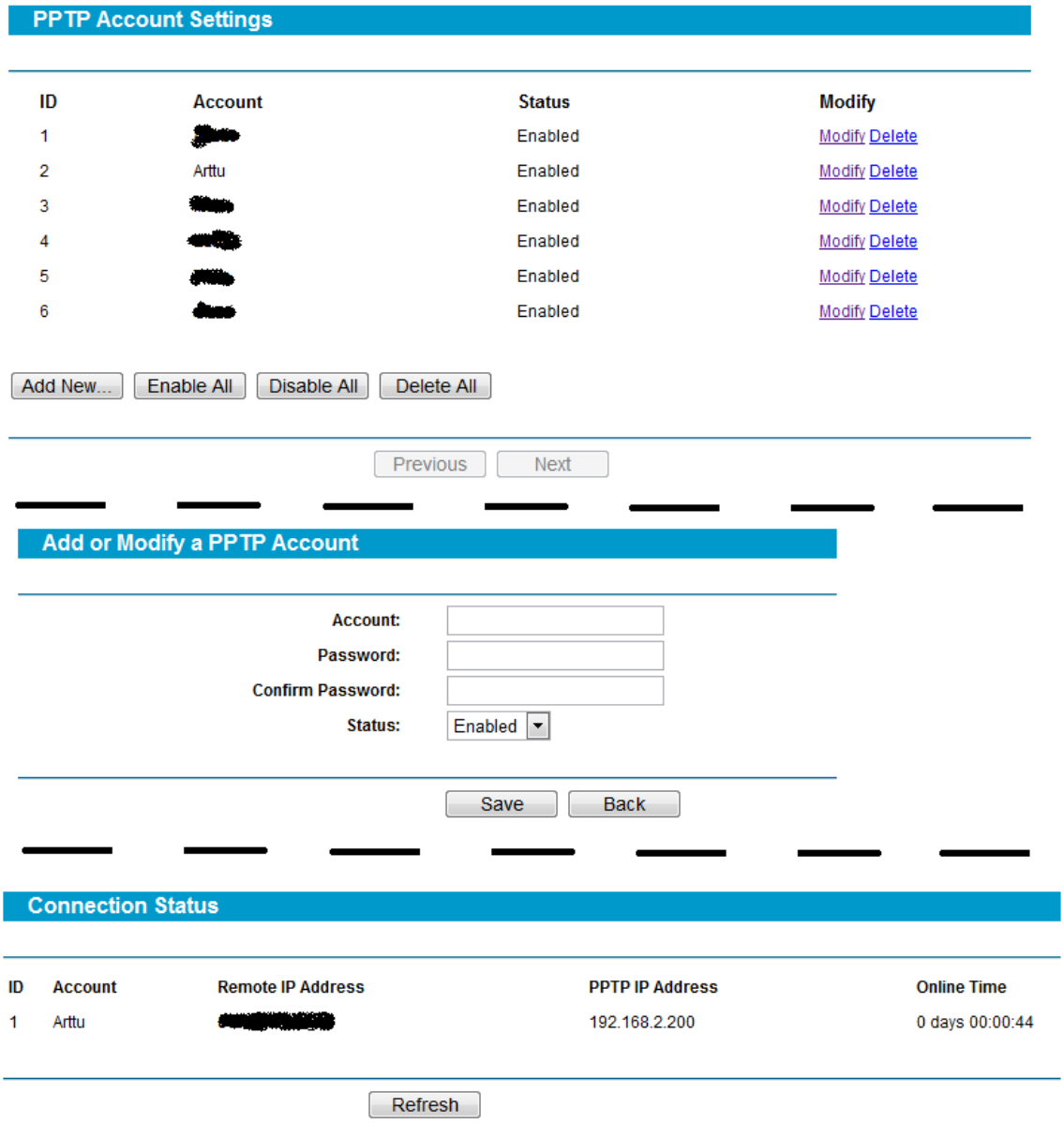

KUVA 15. VPN-reitittimen PPTP-palvelimen asetukset

PPTP palvelin voidaan kytkeä päälle ja pois. "MPPE Encryption" -kohta koskee yhteydessä käytettävää salausta. MPPE (Microsoft Point-to-Point Encryption) -protokollaa voidaan haluttaessa käyttää tiedon salaamisessa PPTP- ja PPP-yhteyksissä.

Asetuksissa voidaan määritellä PPTP-palvelimen jakamat IP-osoitteet asiakkaille. Hankittu VPN-reititin tukee 16 yhtäaikaista PPTP-yhteyttä.

PPTP-yhteyden luomiseksi täytyy reitittimelle lisätä PPTP-käyttäjätilejä. Tilejä voidaan hallita, muokata ja seurata reitittimen asetuksista eri näkymistä. PPTP tilien hallintaa koskevat näkymät ovat esitettynä kuvassa 16.

Reitittimen asetuksissa ei päästä muokkaamaan kaikkia mahdollisia PPTP-yhteyteen liittyviä määrittelyitä. Monissa kaupallisissa reitittimissä on erilaisia rajoituksia eri ominaisuuksille.

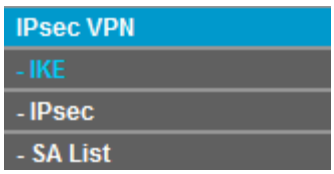



KUVA 16. Reitittimen PPTP-käyttäjätilien hallinnointiasetuksia

PPTP-tunnelin toimintaan saattaminen oli helppoa. Windowsin omalla VPN-asiakasohjelmalla pystytään yhdistämään reitittimen IP-osoitteeseen ja PPTP-tunneli saatiin toteutettua. Kuvassa 16 voidaan nähdä "Connection Status" -kohdassa yksi yhdistynyt käyttäjätili.

### 4.3.2 IPsec

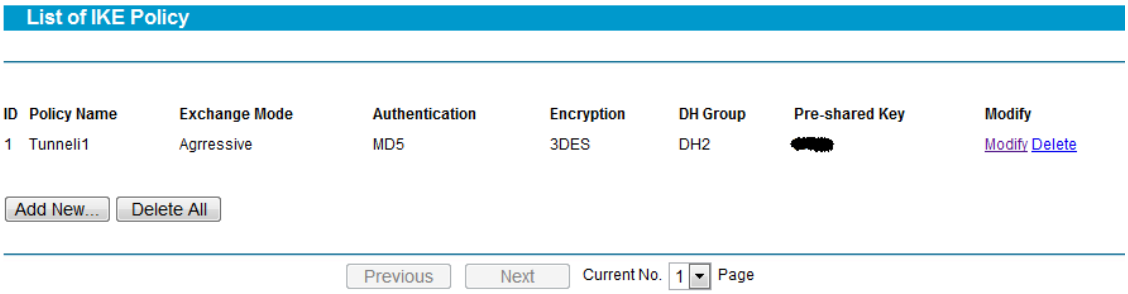
Verrattuna PPTP-tunnelin toteuttamiseen oli IPsec-tunneli huomattavasti haastavampi saada toimimaan. Reitittimen IPsec-asetukset oli jaoteltu kolmen eri linkin taakse. Kuvassa 17 on esitetty nämä kohdat reitittimen asetuksissa.




KUVA 17. Reitittimen IPsec VPN-asetukset ovat jaoteltu kolmeen näkymään

IPsec-tunneli toteutettiin kahden samanlaisen reitittimen välille. Tässä kohdassa kuvatut asetukset tuli siis tehdä kummallekin reitittimille. Joidenkin asetusten on oltava reitittimien välillä samoja ja jotkut asetukset on määriteltävä vastakkaisiksi.

Reitittimen IKE-asetuksissa määritellään käytettävät IKE-käytännöt. Reitittimessä voi olla useita IKE-käytäntöjä. Kuvassa 18 on esitetty reitittimen listaus luoduista käytännöistä. Listauksessa on esitetty tärkeimmät protokollamäärittelyn asetukset eri sarakkeissa. IKE-käytäntö täytyy luoda ennen IPsec-asetusten määrittämistä, sillä IPsec asetuksissa käytetään luotua IKE-käytäntöä.




KUVA 18. IKE-käytäntöjen listaus.

IKE-käytäntöä luodessa tai muokatessa tulee kuvan 19 mukainen asetusnäkymä esiin. Käytäntö nimetään ja muut asetukset voidaan tehdä.

IKE moodiksi valittiin Aggressive, sillä tunnelin toisella päällä ei ole kiinteää IP-osoitetta. Aggressive-moodi valittaessa käytännölle tulee määrittää paikallinen tunniste ja etätunniste. Main-moodin asetukset eroavat aggressivesta siten, että siinä ei ole kohtia koskien tunnisteita. Aggressive-moodiin määritetyt asetukset tehtiin vastakkaisiksi tunnelin toisen pään reitittimelle.

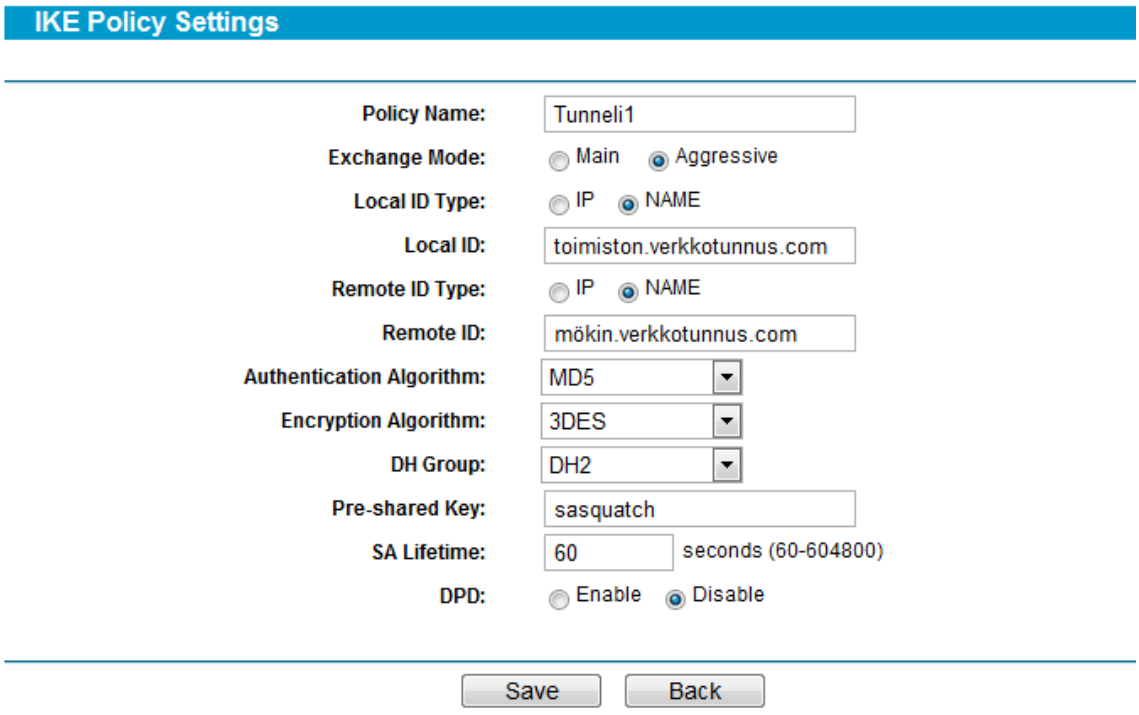
”Authentication algorithm” -kohta tarkoittaa IKE-käytännössä käytettyä käyttäjien todennustapaa. Kohdassa määritellään mitä tiivistefunktiota käytetään. MD5 (Message Digest Algorithm) -valinnan lisäksi käytetyissä reitittimissä voidaan käyttää myös SHA (Secure Hash Algorithm) -tiivistefunktiota. Valinnalla ei varsinaisesti ole merkitystä muuten kuin, että se tulee olla sama tunnelin muodostavilla laitteilla. Todennuksen toimimisen ja tietoturvan kannalta MD5- ja SHA-tiivistefunktioilla ei ole merkittävää eroa.

”Encryption algorithm” -sekä ”DH group” -kohdat määrittelevät käytetyn salaustavan. Näiden asetusten tulee olla myös samoja tunnelin muodostavilla laitteilla.

”Pre-shared key” -kohtaan määritellään tunnelin muodostavien laitteiden käyttämä julkinen avain. Tämä on myös oltava yhtenäinen laitteiden kesken.

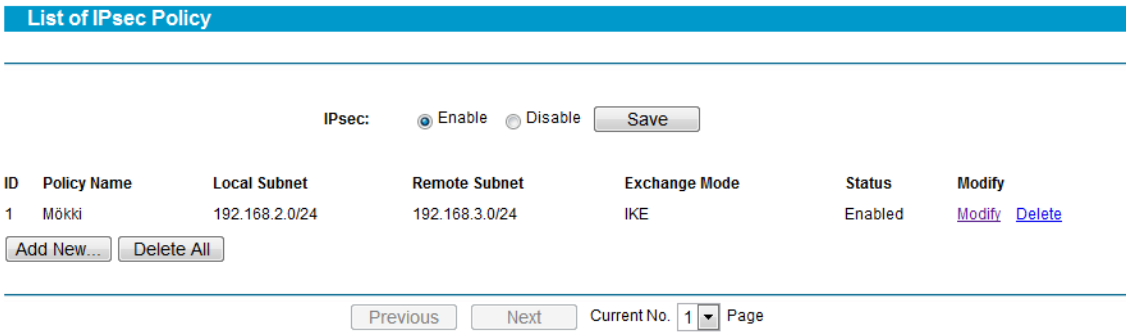
SA lifetime tarkoittaa aikaa, jonka neuvoteltu turvallisuuskäytäntö on voimassa. Määritellyn ajan kuluttua IKE kättelee tunnelin päiden välille uuden turvallisuuskäytännön. Kohtaan asetettiin 60 sekuntia. Oletuksena kohdassa on 28800 joka vaikutti liian pitkältä. Kohteen IP-osoite voi muuttua milloin tahansa ja haluttiin varmistua tunnelin muodostumisesta IP-osoitteen muuttuessa.

DPD (Dead Peer Detection) on IKE-protokollan ominaisuus, jonka avulla voidaan varmistua tunnelin päiden aktiivisuudesta.




KUVA 19. IKE-protokollan asetukset.

Reitittimen IPsec-asetuksiin määritellään tunnelin muodostamista koskevat asiat. Reitittimen IPsec-asetusten näkymä on esitettynä kuvassa 20. Asetuksissa näkyy IPsec-käytäntöjen listaus samankaltaisesti kuin IKE-asetuksissa. Käytäntöjä voi olla monia ja tärkeimmät tiedot ovat esitettynä sarakkeittain.




KUVA 20. IPsec protokollamäärittelyjen listaus.

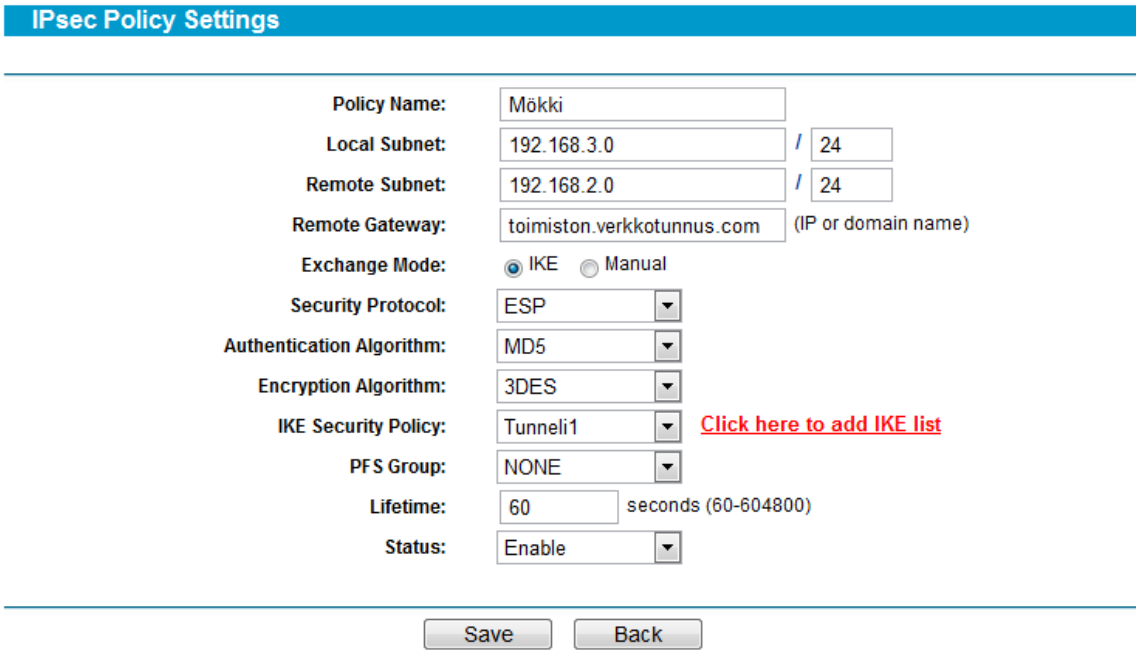
IPsec-käytäntöä muokattaessa tai lisättäessä uutta päästään kuvassa 21 esitettyyn näkymään määrittämään asetuksia. Käytäntö voidaan nimetä ja muut asetukset määrittää.

Aliverkot asetuksiin täytyy määrittää tunnelin päiden välille vastakkaisiksi. Paikallinen aliverkko täytyy olla samassa aliverkossa reitittimen kanssa.

”Remote Gateway” -kohta on oleellinen. Tähän määritellään tunnelin toisen pään IP-osoite tai verkkotunnus. Tunnelin toisen pään IP-osoite muuttuu jatkuvasti ja siksi jouduttiin käyttämään kohdassa 4.3.3 kuvattua DDNS-palvelua. DDNS-palvelun lisäksi toimeksiantaja halusi sitoa siellä määritetyn verkkotunnuksen itse määrittämäänsä verkkotunnukseen erillisen DNS-palvelun avulla, jotta osoitteen muistaminen olisi helpompaa.

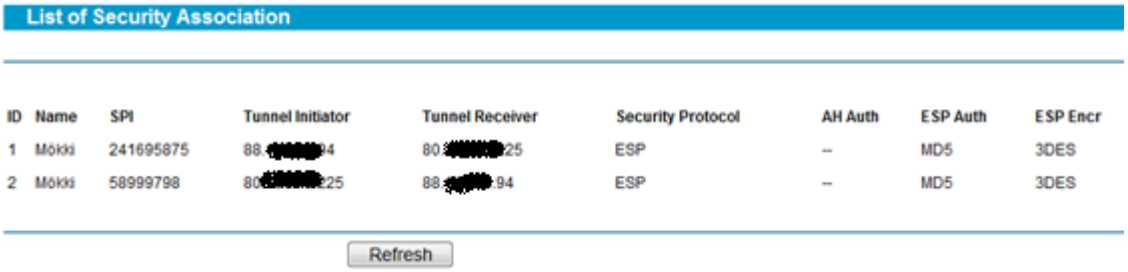
Reititin antaa mahdollisuuden valita käytetty turvallisuusprotokolla. ESP lisäksi voidaan valita AH. Muut todennukseen ja datan salaamiseen käytetyt asetukset voidaan määrittää. Aikaisemmin määritelty IKE-käytäntö asetetaan käytettäväksi kohdassa "IKE Security Policy".

Asetukset liittyen todennukseen, datan salaamiseen ja turvallisuuteen on oltava samat tunnelin muodostavien laitteiden välillä.



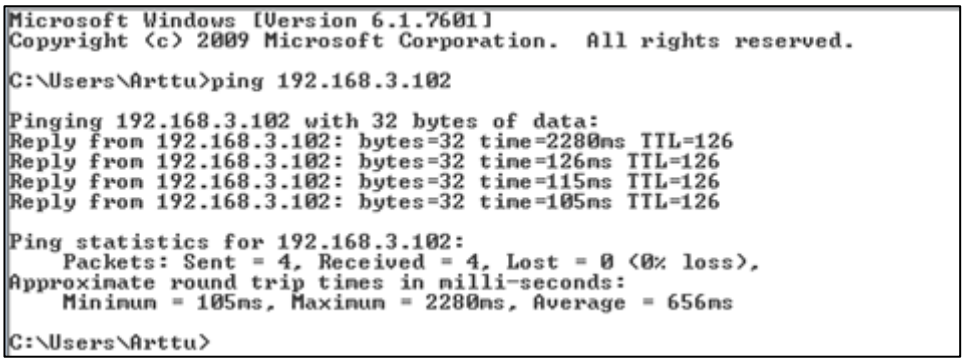

KUVA 21. IPsec-määrittelyt.

SA-listauksesta nähdään muodostetut turvallisuusliitot. Kuvassa 22 on esitettynä muodostettu IPsec-turvallisuusliitto. Listauksessa nähdään jälleen liiton keskeisimmät tiedot sarakkeittain.




KUVA 22. Muodostettujen IPsec käytäntöjen listaus.

IPsec-tunnelin muodostuminen voidaan todentaa ping-komennolla komentorivillä. Kuvassa 23 on esitetty tunnelin toisessa päässä annettu ping-komento. Komentoon annettiin tunnelin toisen pään reitittimeen kytketyn CX9001-ohjaimen sisäverkon IP-osoite. Ping-pyyntöön tuli vastaus ja näin voidaan päätellä tunnelin toimivuus.



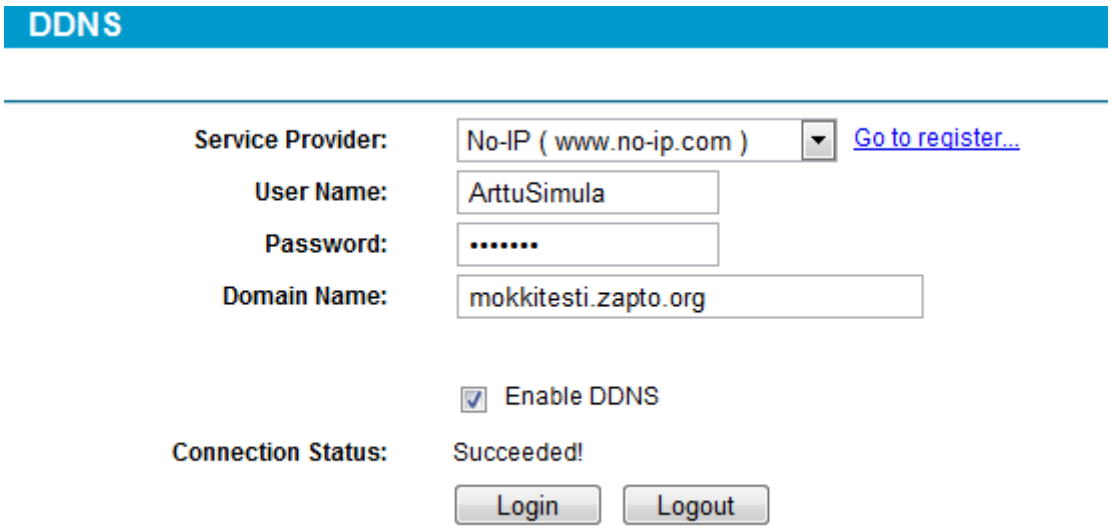

KUVA 23. IPsec tunnelin muodostamisen todennus

### 4.3.3 No-IP DDNS-palvelu

Kohteeseen tulevaa 3G-reititintä käytetään mobiililaajakaistaan kytkettynä. 3G Reititin ja siihen kytketyt VPN-reititin ja CX9001-ohjain ovat internetiin yhteydessä siis 3G mobiililaajakaistan kautta. Mobiililaajakaistan IP muuttuu melko usein. Tästä syystä on käytettävä DDNS-palvelua, jos halutaan ulkoverkosta päästä käsiksi mobiililaajakaistan kautta internetissä olevaan palvelimeen. Myös IPsec-tunnelin muodostamista varten käytettiin DDNS-palvelua.

Ilmaisia DDNS-palveluita on useita. Valittu palvelu löytyy www.no-ip.com-verkko-osoitteesta. Palveluun tehtiin käyttäjätunnus ja sinne määritettiin kaksi verkkotunnusta. Palvelu toimii siten, että asiakasohjelma ottaa yhteyden palveluun ja kertoo oman IP-osoitteensa ja verkkotunnuksen, johon se halutaan liittää. Monissa reitittimissä on DDNS-ominaisuus, joka toimii asiakasohjelman tavoin ja päivittää DDNS-palveluun oman julkisen verkon IP:nsä.

Reitittimen DDNS-ominaisuuden avulla voidaan suoraan reitittimen asetuksiin asettaa käytetty DDNS-palvelu ja sinne tehty käyttäjätunnus ja salasana. Lisäksi asetuksiin asetetaan haluttu verkkotunnus, johon reitittimen IP sidotaan. DDNS-ominaisuus otettiin käyttöön toimistolla olevaan TP-R600VPN-reitittimeen sekä kohteeseen tulevaan TP-MR3220-reitittimeen. TL-R600VPN-reitittimen DDNS asetusnäkymä on esitettynä kuvassa 24. TL-MR3220-reitittimen DDNS-asetusnäkymä oli samanlainen ja sinne tehdyt määrittelyt erosivat VPN-reitittimen asetuksista käytetyn verkkotunnuksen osalta.




KUVA 24. TL-R600VPN-reitittimen DDNS-asetukset.

## 4.4 CX9001 konfigurointi

CX9001-ohjaimessa on oletuksena web-palvelin aktiivisena. Ohjaimessa on Windows CE -käyttöjärjestelmä. Erityisiä asetuksia ohjaimeen verkkosivun näkyviin saamiseksi ei tarvinnut tehdä. Ohjaimen liittäminen verkkoon onnistuu yksinkertaisesti ethernet-kaapelin avulla. Verkkosivun toteuttamisen helpottamiseksi ohjaimen FTP (File Transfer Protocol) -palvelin asetettiin aktiiviseksi. FTP-yhteyden avulla ohjaimen ja työkoneen välillä pystytään siirtämään tiedostoja. Tämä helpotti huomattavasti verkkosivun toteutusta.

CX9001-ohjaimeen voidaan luoda etäyhteys ilmaisen Remote Display Control for Windows CE -ohjelman avulla. Näin ohjaimen käyttöjärjestelmää voidaan käyttää ja sen kautta tehtäviä asetuksia ja määrittelyjä päästään muokkaamaan etäyhteyden avulla.

# 5 WEB KÄYTTÖLIITTYMÄ

## 5.1 Toteutusmahdollisuudet valitulla järjestelmällä

Valittu CX9001-ohjain tarjoaa monia ohjelmallisia mahdollisuuksia tiedonsiirtoon PLC:n ja verkkosivun välillä. Beckhoff tarjoaa erillistä verkkosivun generointiohjelmistoa, jonka avulla voidaan helposti luoda verkkosivu etäkäyttöä varten. Tätä ei kuitenkaan hankittu käyttöliittymän tarpeiden ollessa hyvin yksinkertaisia, vaan verkkosivu etäkäyttöä varten luotiin itse. Lisenssi verkkosivun generointiohjelmistoon hankittaisiin, jos kyseessä olisi suurempi automaatiojärjestelmä joka toteutettaisiin Beckhoffin ohjaimella.

Ohjaimen verkkosivu voidaan toteuttaa monin eri tavoin, esimerkiksi HTML (Hypertext Markup Language), ASP (Active Server Page), CSS (Cascading Style Sheets), JScript, VBscript ja XML (Extensible Markup Language) ovat tuettuina. Ohjain tukee myös MySQL (My Structured Quert Language) -tietokantaa ja Flash-kehitysympäristöä. Ohjaimeen voidaan myös luoda omia ohjelmia käyttäen Visual Basic -, JAVA -, C++ -ja C# -ohjelmointikieliä. (Beckhoff, 2012)

## 5.2 Tiedonsiirto Beckhoffin ohjaimissa

Beckhoff käyttää ADS (Automation Device Specification) -protokollaa tiedonsiirtoon ohjaimien välillä. ADS toimii palvelin-asiakas-periaatteella TCP -tai UDP-protokollan kanssa. ADS tarjoaa useita tapoja lukea tietoja ohjaimilta. Jokaisella järjestelmän osalla, joka keskustelee ADS:n avulla on oma ohjelmallinen ADS-reititin. ADS toimii yhdessä AMS (Automation Message Specification) -protokollan kanssa. AMS-protokolla antaa jokaiselle ohjelmalliselle ADS-reitittimelle oman osoitteensa. AMS-osoite on IP-osoitteen kaltainen, mutta kuuden tavun pituinen neljän sijasta. Jokaisella ohjaimella järjestelmässä on oma IP-osoite ja jokaisella ADS-reitittimellä on oma AMS-osoitteensa. (Beckhoff, 2012)

## 5.3 Tiedonsiirto etäkäyttäjän ja järjestelmän välillä.

CX9001-ohjaimessa on oletuksena yksinkertainen verkkosivu näkyvissä. Ohjaimen Windows CE -käyttöjärjestelmässä on samankaltainen hakemistorakenne kuin muissa

Windows-käyttöjärjestelmissä. Verkkoon näkyvissä oleva verkkosivu on ohjaimen WWW-kansiossa. Haluttu verkkosivurakenne voidaan siirtää sinne.

Yhteyden muodostamiseksi laitteelle ulkoverkosta käsin, on ensin muodostettava VPN-yhteys reitittimelle käyttäen erillistä VPN-asiakasohjelmaa. Tämän jälkeen ohjaimelle luotu verkkosivu saadaan näkyviin selaimella yhdistämällä ohjaimen sisäverkon IP-osoitteeseen http://192.168.3.102/index.html. Reitittimelle, johon ohjain kytkettiin, määritettiin DHCP (Dynamic Host Configuration Protocol) -asetus, joka varaa määritetyn sisäverkon IP-osoitteen halutulle laitteelle MAC-osoitteen mukaan.

## 5.4 Verkkosivulle luotu HMI

Verkkosivun toteuttamiseen käytettiin HTML-, CSS-, ASP- ja JScript-ohjelmointimenetelmiä. Verkkosivun ulkonäkö ja toiminnallisuudet toteutetaan CSS:llä, ASP:lla ja HTML:llä. JScriptiä tarvitaan muuttujien lukemiseen ja kirjoittamiseen ohjaimelta. Tehty koodi oli rakenteeltaan hieman tyypillisestä HTML:stä poikkeava. Samassa tiedostossa oli HTML:ää edeltävä osio, jossa JScriptillä muodostettiin yhteys PLC:lle ja määriteltiin verkkosivun koodissa käytettyjen muuttujien yhteys PLC:llä oleville muuttujille. HTML-koodin seassa pystyttiin käyttämään JScriptin muuttujia eri tarkoituksissa. Kuvassa 25 on esitettynä esimerkki verkkosivun koodista. Koodissa Jscriptillä ensin yhdistetään PLC:lle. Tämän jälkeen luodaan esimerkkimuuttuja johon luetaan ”.esim” -niminen muuttuja PLC:ltä. JScriptin esimerkkimuuttujaa voidaan sitten kutsua HTML-koodin seassa kuvassa esitetyllä tavalla.

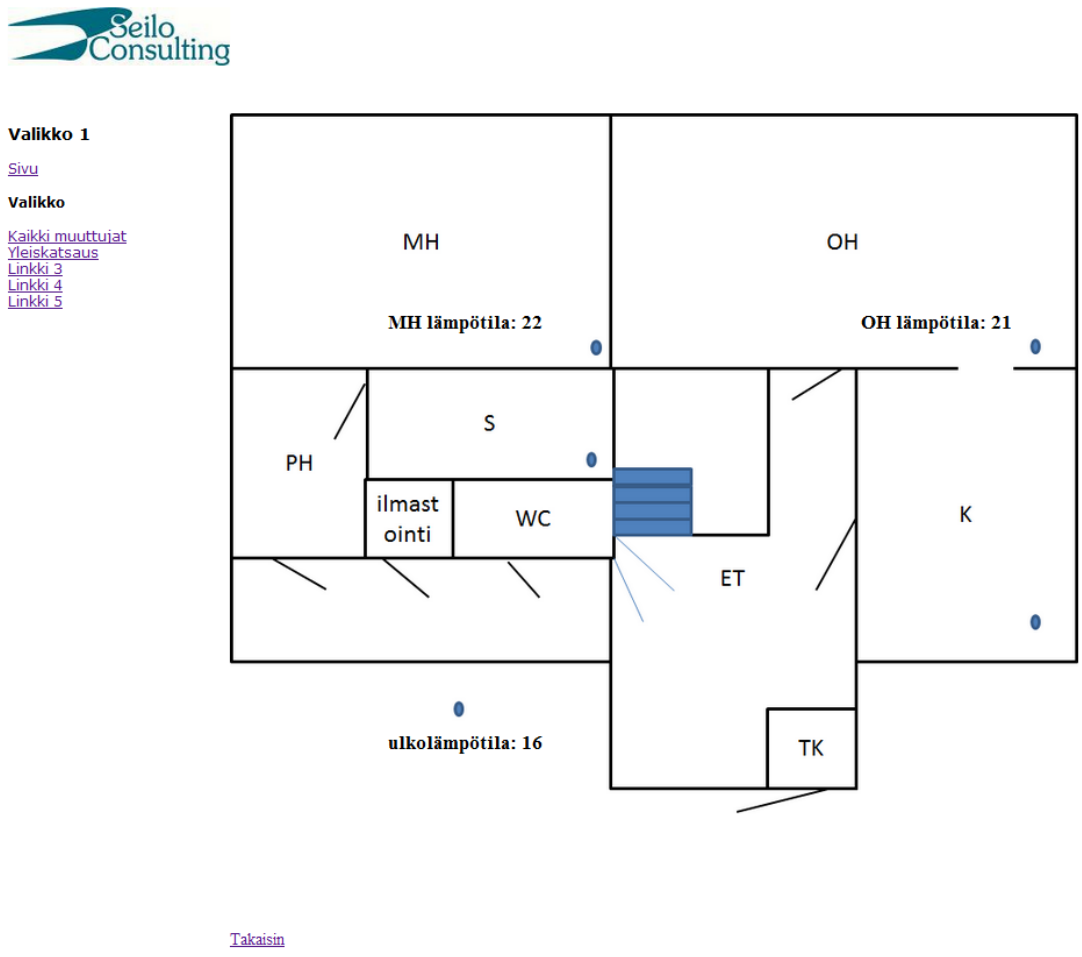
```
<%@ language=JScript %>
<%
   TcClient = new ActiveXObject("TcScript.TcScriptSync");
   TcClient.ConnectTo("", 801);
   var esimerkki = 0;
   esimerkki = TcClient.ReadVar(".esim");
%>

<html>
   <head>
      <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" >
      <title>Esimerkki</title>
   </head>
   <body>
   <h1>Esimerkki</h1>

   Esimerkkimuuttuja: <% Response.Write( esimerkki ); %>

   </body>
</html>
```

KUVA 25. Esimerkki muuttujan lukemisesta verkkosivulle PLC:ltä

Kuvassa 26 on esitettynä esimerkkikoodin palauttama verkkosivu. PLC:llä ”.esim” -muuttujan arvona oli 0.


KUVA 26. Esimerkkikoodin palauttama verkkosivu

Muuttujia voidaan kutsua useita. Muuttujiin kirjoittamiseen käytetään HTML:ssä tekstikenttää. Kuvassa 27 on esitettynä kuvakaappaus toteutetusta HMI:stä verkkosivulla. HMI:tä tullaan kehittämään käyttökokemusten myötä.




KUVA 27. Toteutettu HMI verkkosivulla

# 6 LOPPUTULOS JA JOHTOPÄÄTÖKSET

Tavoitteena oli toteuttaa järjestelmä, johon voidaan luoda turvallinen yhteys internetin yli mistä tahansa sekä ohjata ja valvoa järjestelmää käyttäen verkkoselainta. Laitteiston valinta automaatiojärjestelmän osalta arvioitiin onnistuneeksi. Beckhoff on ollut viime vuosina suuressa kasvussa ja on hyvin todennäköistä, että sen kanssa tullaan olemaan tekemisissä jossain vaiheessa myös työelämässä. Määritetty suuntaa antava tuhannen euron budjetti ylitettiin noin kolmella sadalla eurolla.

Opinnäytetyön ja oppimisen kannalta huomionarvoista on toteutusosuuden merkitys. Jos työ olisi käsittänyt pelkän suunnitteluosuuden, oltaisiin oltu huomattavasti pienemmän määrän asioita kanssa tekemisissä. Kun VPN-ratkaisu toteutettiin, jouduttiin miettimään aliverkotuksia, DHCP-asioita, DDNS-palveluita ja muita asioita, joita ei suunnitteluosuudessa välttämättä kohdata ollenkaan.

Verkkolaitteiden valinta verkkoratkaisun toteuttamisen kannalta oli oikea. Suunniteltu ratkaisu saatiin toteutettua. Käytössä on kuitenkin tullut vastaan laitteiden toiminnan luotettavuus. 3G-reitittimen toiminnassa on ollut hieman toivomisen varaa. Myös reitittimien asetusten konfigurointimahdollisuudet voisivat olla laajemmat. Jälkikäteen ajateltuna Ciscon verkkolaitteiden hankkimisen myötä oltaisiin voitu myös tutustua Ciscon kehittämään Cisco IOS (Internetwork Operating System) -käyttöjärjestelmään reitittimille. Laitteet olisivat mahdollisesti olleet myös luotettavampia ja konfigurointimahdollisuuksiltaan laajempia.

Valitut verkkolaitteet ovat kaupallisia yksityiseen tai pieneen yrityskäyttöön tarkoitettuja laitteita. Teollisuusympäristössä käytettävät reitittimet ovat joka suhteessa tässä opinnäytetyössä käytettyjä kehittyneempiä. Kuitenkin etäkäyttöyhteyksissä ollaan ainakin osittain samojen asioiden kanssa tekemisissä toteutustavasta ja käytetystä laitteistosta riippumatta. Toteutettu IPsec-tunneli on täysin soveltuva teollisuuskäyttöön tietoturvaan ja toiminnallisuuteen liittyvien asioiden kannalta.

Opinnäytetyön tekemisen myötä osaaminen tietoverkkoasioissa laajeni huomattavasti. Valmiudet työskennellä vastaavan etäkäyttöyhteyden parissa suuressa teollisuuden automaatiojärjestelmässä ovat selvästi paremmat.

LÄHTEET

Anttila, A. (2000). *TCP/IP -tekniikka.*

Beckhoff. (2012). Beckhoff Information System. Noudettu osoitteesta http://infosys.beckhoff.com/

Bollapragada, V., Khalid, M., & Wainner, S. (2005). *IPsec VPN Design.* Cisco Press.

Hakala, M.;& Vainio, M. (2005). *Tietoverkon rakentaminen.* Jyväskylä.

Jackson, C. (2010). *Network Security Auditing.* Indianapolis, USA: Cisco Press.

Perlmutter, B.;& Zarkower, J. (2001). *Virtuaaliset yksityisverkot.*

Puska, M. (2000). *Lähiverkon rakentaminen - Pro training.* Jyväskylä.

Tiso, J. (2012). *Designing Cisco Network Service Architectures (ARCH).* Indianapolis, USA: Cisco Press.