

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Opinnäytetyö

Petri Vesamäki

MOVA-MITTALAITTEVAUNUN ETÄKÄYTTÖYHTEYS

Työn ohjaaja
Työn teettäjä
Tampere 05/2010

Yliopettaja Jorma Punju
TAMK / TKI MOVA Pro -hanke

| | |
|-----------------|--|
| Tekijä | Petri Vesamäki |
| Työn nimi | MOVA-mittalaittevaunun etäkäyttöyhteys |
| Sivumäärä | 22 |
| Valmistumisaika | 05/2010 |
| Työn ohjaaja | Yliopettaja Jorma Punju |
| Työn teettäjä | TAMK / TKI MOVA Pro -hanke |

TIIVISTELMÄ

Tämän työn tavoitteena oli toteuttaa etäkäyttöyhteys MOVA-mittalaittevaunuun, jossa toimii ilman pienhiukkaspitoisuuksia mittaava laitteisto. Yhteyden tarkoituksena oli helpottaa siirrettäväksi tarkoitettua mittalaitteiston hallintaa, lukemien tarkistamista sekä mahdollisten vikatilanteiden hoitamista. Näin säästettäisiin aikaa ja voitaisiin vähentää matkustamisen tarvetta pitkäkestoisemmissä mittauksissa. Lisäksi mittauskohtaisen yhteyden luomisesta tehtiin kattava ja mahdollisimman ymmärrettävä ohjeistus.

Yhteyden toteuttamisessa käytettiin 3G-modeemia ja VPN-ohjelmistoa. Etäkäyttömenetelminä työssä olivat mittausohjelmiston etäkäyttöominaisuus sekä etätyöpöytä. Työssä käsiteltiin myös tietoturvaa ja palomuurin konfigurointia.

Työn tuloksena saatiin aikaan toimiva etäkäyttöyhteys. Kuten tietoteknisissä ratkaisuissa yleensä, parantamisen varaa ja kehittämiskohteita jäi kuitenkin runsaasti.

Osa työhön liittyvästä aineistosta on luottamuksellista ja se on esitetty liitteissä.

| | |
|----------------------|--|
| Writer | Petri Vesamäki |
| Thesis | Remote control connection for MOVA measurement trailer |
| Pages | 22 |
| Graduation time | 05/2010 |
| Thesis supervisor | Principal Lecturer Jorma Punju |
| Co-operating Company | TAMK / RDI MOVA Pro -project |

ABSTRACT

The aim of this thesis was to implement a remote control connection for MOVA measurement trailer. There is a fine particle measurement device operating in the trailer. The purpose of the connection was to ease the controlling, reading checking and fault management of the mobile trailer and its equipment. Therefore the need of travelling and the consumption of time would be reduced in long-term measurement periods. A comprehensive and intelligible instruction manual for establishing the connection was required as a part of the work.

Implementation was carried out using a 3G modem and VPN software. Methods for the remote use were remote desktop and a remote use feature in the measurement software. Security aspects and firewall are also covered in this thesis.

As a result an operational remote use connection was evoked. As usual in the field of information technology, there were plenty of things left to improve and enhance.

Part of the information related to this thesis is confidential and it is presented in the appendixes.

Keywords telecommunications technology, data networks, remote access,
TCP/IP, data security, VPN

Esipuhe

Aloitin tämän opinnäytetyön tekemisen syksyllä 2009. Työn tilanneet Pasi Arvela ja Jarmo Lilja TAMKin materiaali- ja mittaustekniikan osaamiskeskukselta ovat olleet hyvin joustavia ja antaneet minulle hyvin vapaat kädet työn tekemisen ja aikataulun osalta. Haluaisinkin kiittää heitä sekä työn valvojaa, yliopettaja Jorma Punjua, tästä ymmärtävästä asenteesta. Ajoittain on ollut hyvinkin haastavaa yhdistää tämän työn tekeminen muihin opiskeluihin sekä koulun ulkopuoliseen elämään.

Omasta mielestäni tällaisen konkreettista hyötyä tuovan työn tekeminen on aina innostavampaa ja mielekkäämpää kuin pelkkä asioiden teoreettinen käsittely. Kiitänkin koulutuspäällikkö Ari Rantalaa, joka osoitti minulle mahdollisuuden tehdä tämä työ.

Käytännön toteutuksessa olen saanut merkittävää apua monelta taholta. Näistä ensimmäisenä mainitsen TAMKin tietokonekeskuksen, sekä erityisesti Sami Setälän. Mittauslaitetta valmistavan Dekati Oyn puolesta olen saanut asiantuntemusta Jukka Kujanpäältä sekä Elina Niemiseltä. Lisäksi haluaisin osoittaa kiitokseni vielä TAMKin laboratoriomestari Juhani Pitkäselle ja Mikko Vaaralalle.

Toivon, että tekemäni työ tulee tarjoamaan todellista hyötyä materiaali- ja mittaustekniikan osaamiskeskukselle. Odotan myös innolla voivani tarjota apua, jos joku toinen tulee myöhemmin parantelemaan ja jatkokehittämään tätä aloittamaani työtä.

Tampereella 14. toukokuuta 2010

Petri Vesamäki

Sisällys

| | | |
|------|---|----|
| 1 | Johdanto..... | 1 |
| 2 | Tarpeiden kartoittaminen | 2 |
| 3 | Selvitystyö | 2 |
| 4 | Laitteisto | 4 |
| 4.1 | 3G-modeemi..... | 4 |
| 4.2 | Server-kone..... | 4 |
| 4.3 | Client-kone | 4 |
| 4.4 | Mittalaite | 5 |
| 5 | 3G-yhteys | 6 |
| 5.1 | Yleistä..... | 6 |
| 5.2 | Dial-up-yhteys | 7 |
| 5.3 | Mobile Partner -ohjelmisto | 8 |
| 6 | VPN-tunnelointi | 8 |
| 6.1 | Yleistä..... | 8 |
| 6.2 | Safemove-ohjelmisto..... | 9 |
| 7 | ELPIVI-ohjelmiston etäkäyttö | 10 |
| 8 | Etätyöpöytä | 11 |
| 8.1 | VNC-etätyöpöytä | 11 |
| 8.2 | Citrix-etätyöpöytä | 12 |
| 9 | Tiedostonsiirto | 12 |
| 10 | Palomuri | 13 |
| 10.1 | Yleistä..... | 13 |
| 10.2 | Server-koneen asetukset | 14 |
| 11 | Ongelmat..... | 14 |
| 11.1 | TCP-yhteys..... | 14 |
| 11.2 | ELPI-mittalaite | 16 |
| 11.3 | Dial-up-asetukset | 17 |
| 11.4 | Windows Remote Desktop ja Citrix..... | 17 |
| 11.5 | 3G-palveluntarjoajan vaihtuminen | 18 |
| 12 | Käyttöohje | 19 |
| 13 | Loppusanat..... | 19 |
| | Lähteet | 21 |
| | Liitteet..... | 22 |
| | Liite 1: MOVA-topologia | |
| | Liite 2: MOVA-käyttöohje | |
| | Liite 3: Server-koneen palomuurisäännöt | |
| | Liite 4: Pikaohje – Server-kone | |
| | Liite 5: Pikaohje – Client-kone | |
| | Liite 6: Pikaohje – Citrix-käyttö | |

Keskeisiä termejä ja lyhenteitä

| | |
|-------------------|--|
| Citrix | Etäkäyttöohjelmisto, jolla päästään turvallisesti käsiksi yksityisen järjestelmän resursseihin julkisen verkon ylitse. |
| Client-kone | Tällä termillä viitataan tässä työssä tiettyyn TAMKin tietoverkossa olevaan tietokoneeseen, joka on varattu etäkäyttötarkoitukseen. |
| Dial-up | Soittosarjamodeemi. Tässä työssä käytetään kuvaamaan Windowsin toimintoa, joka avaa yhteyden palveluntarjoajaan 3G-modeemin välityksellä. |
| EDGE | Enhanced Data rates for GSM Evolution. GSM-järjestelmän paranneltu datansiirtomenetelmä. GPRS:n seuraaja. |
| GPRS | General Packet Radio Service. GSM-järjestelmän perusmenetelmä pakettikytkentäisen dataliikenteen välittämiseksi. |
| HSDPA | High-Speed Downlink Packet Access. UMTS-järjestelmän paranneltu menetelmä verkosta käyttäjälle liikkuvan datan välittämiseksi. |
| IP-osoite | Internet Protocol -määrityksen mukainen looginen osoite verkon laitteiden tunnistamiseksi ja erittelemiseksi. Ei ole kiinteä, vaan käyttäjän tai järjestelmän määriteltävissä. |
| IPSec | IP Security. Protokolla IP-liikenteen turvaamiseksi tunnistamisen ja salauksen avulla. |
| Konsoli-istunto | Paikallisen käyttäjän istunto Windows XP:ssä. Käytetään myös nimitystä session 0. |
| Mobile Partner | 3G-modeemin mukana toimitettu yhteysohjelmisto. Muodostaa internetyhteyden palveluntarjoajaan. Käyttää Windowsin Dial-up-toimintoa. |
| Netstat | Windowsin komentokehoteen työkalu, joka listaa kuljetuskerroksen yhteydet. Näyttää TCP-yhteyksien lähde- ja kohdeisännät, käytetyt portit sekä yhteyksien tilat. |
| RealVNC | Etäkäyttöohjelmisto. Käytetty tässä työssä etättyöpöytäyhteyden toteuttamiseksi mittausvaunun tietokoneeseen TAMK-verkon sisältä. |
| Safemove | VPN-ohjelmisto. Käytetty tässä työssä yhdistämään mittalaittevaunussa sijaitseva kone TAMKin tietoverkkoon julkisen verkon ylitse. |
| Server-kone | Tällä termillä viitataan tässä työssä tiettyyn tietokoneeseen, joka on kytketty mittauslaitteistoon. |
| TCP | Transmission Control Protocol. Kuljetuskerroksen yhteydellinen protokolla. Varmistaa datan perillemenon ja oikeellisuuden. |
| Terminal Services | Windowsin komponentti, joka mahdollistaa etäkäytön verkon välityksellä. Käytetään myös nimeä Remote Desktop Services. |

| | |
|-----------|--|
| UDP | User Datagram Protocol. Kuljetuskerroksen yhteydetön protokolla. Ei tarkista saavuttaako data kohteensa. |
| UMTS | Universal Mobile Telecommunications System. Kolmannen sukupolven digitaalinen matkaviestijärjestelmä. Käytössä koko Euroopassa. |
| VPN | Virtual Private Network. Menetelmä yksityisten tietoverkkojen yhdistämiseksi vieraan verkon ylitse. |
| WCDMA | Wideband Code Division Multiple Access. UMTS-järjestelmän radiorajapintatekniikka. Erittelee käyttäjät toisistaan koodiavainten perusteella. |
| Wireshark | Protokolla-analysointityökalu. Työkaluohjelmisto, jolla voidaan tarkastella ja tallentaa verkkoliikenteen paketteja. |

1 Johdanto

Aluksi täytyi selvittää, minkälaisia vaatimuksia työn tilaaja oli sille asettanut ja minkälaisilla menetelmillä näihin päästäisiin. Työn tilaajana oli Tampereen ammattikorkeakoulun materiaali- ja mittaustekniikan osaamiskeskus, jonka käyttöön työn lopputulos tuli.

Tavoitteeksi muodostui toteuttaa sellainen yhteys, joka mahdollistaa paikasta toiseen siirrettävän mittauslaitteiston monitoroinnin ja etäkäytön. Tilaajalla oli jo alussa käytettävissä 3G-modeemi, joka mahdollisti fyysisen yhteyden käytännössä missä tahansa. Varsinaiseksi tehtäväksi tuli siis toteuttaa looginen yhteys järkevällä ja tietoturvaisella menetelmällä.

Tällaisen yhteyden toteuttamista oli aikaisemmin mietitty yhteistyössä TAMKin tietokonekeskuksen kanssa, joten alkuvaiheen selvitystyö oli luonnollista aloittaa heidän avullaan. Myös mittauslaitteistoa ja -ohjelmistoa valmistava yritys oli arvokas tiedon lähde.

Työssä on erikseen käsitelty yhteyden luomisessa käytetyt tekniikat sekä suppea perusteoria kustakin tekniikasta. Ilmenneet ongelmat ratkaisuihin on eritelty omaksi luvukseksi.

Toimivan yhteyden toteuttamisen jälkeen laadittiin käyttöohje, joka tarjoaisi loppukäyttäjille riittävän perusteelliset ohjeet yhteyden käyttämiseksi.

2 Tarpeiden kartoittaminen

Tärkein vaihe työtä aloittaessa oli selvittää, mitä työn tilannut taho lopputulokselta odotti. Näin minimoitiin turhan työn tekemisestä koitua vaiva ja ajanmenetys. Yhtä oleellista oli selvittää aikataulu, jonka puitteissa tilaaja halusi työn tehtävän.

Keskusteluissa selvisi, että yhteyttä tulnaisiin käyttämään liikuteltavaan vaunuun sijoitetun mittauslaitteiston etäkäyttöön ja valvomiseen. Mittausvaunussa oli jo hälytysjärjestelmä, joka ilmoittaa muun muassa sähkökatkoksista ja murtautumisista. Tilaaja kertoi esimerkin tilanteesta, jossa toteutettava etäkäyttöyhteys olisi ollut hyödyksi.

Mittausvaunu oli kuljetettu toiselle paikkakunnalle pitkäkestoista mittausta varten ja pian mittauksen alettua mittauspaikalla oli sattunut lyhyt sähkökatkos, joka oli kestänyt vain muutaman sekunnin. Vaunun hälytysjärjestelmä kuitenkin reagoi vain yli kymmenen sekunnin katkoksiin, joten tapahtuma ei tullut ilmi. Kun mittauslaitteistoa tultiin hakemaan pois, havaittiin mittalaitteeseen kytketyn tietokoneen sammuneen ja mittauksen näin epäonnistuneen.

Edellä mainitun kaltaisissa tilanteissa olisi ollut hyödyllistä ja vaivatonta tarkistaa silloin tällöin, että mittaus etenee kuten pitää. Tarve tämän työn tekemiselle oli siis selvä.

Ensisijaiseksi käyttökohteeksi yhteydelle tarkentui pienhiukkasmittalaite ELPI:n toiminnan seuranta. Toissijaisia käyttökohteita olivat muun muassa sääasema Davis Vantage Pro 2 sekä mahdolliset muut vaunussa käytettävät mittalaitteet. Työtä lähdettiin siis tekemään ELPI-mittalaitteen lähtökohdista.

Aikatauluvaatimukset työn tilaajalla olivat varsin väljät. Koska tämänkaltaiselle ratkaisulle oli ollut tarvetta jo pitkään, ei työn valmistumiselle ollut mitään kiirettä.

Tarpeita kartoitettaessa täytyi selvittää myös kustannukset, joita työn tekemisestä aiheutuisi. Tilaajalla oli jo entuudestaan käytettävissä 3G-modeemi kuukausimaksullisella liittymällä, jota toteutuksessa tulnaisiin käyttämään. Muut laitteet ja tarvittavat ohjelmistot olivat saatavissa koulun tietokonekeskukselta, joten minkäänlaisiin hankintoihin ei tarvinnut varautua.

3 Selvitystyö

Mahdollisia lähestymistapoja lähdettiin selvittämään tietokonekeskuksen kanssa, sillä heiltä oli saatavilla tieto ja osaaminen koulun tietojärjestelmistä. Lisäksi työn tilaaja oli aiemmin keskustellut heidän kanssaan tällaisen yhteyden toteuttamisen mahdollisuudesta.

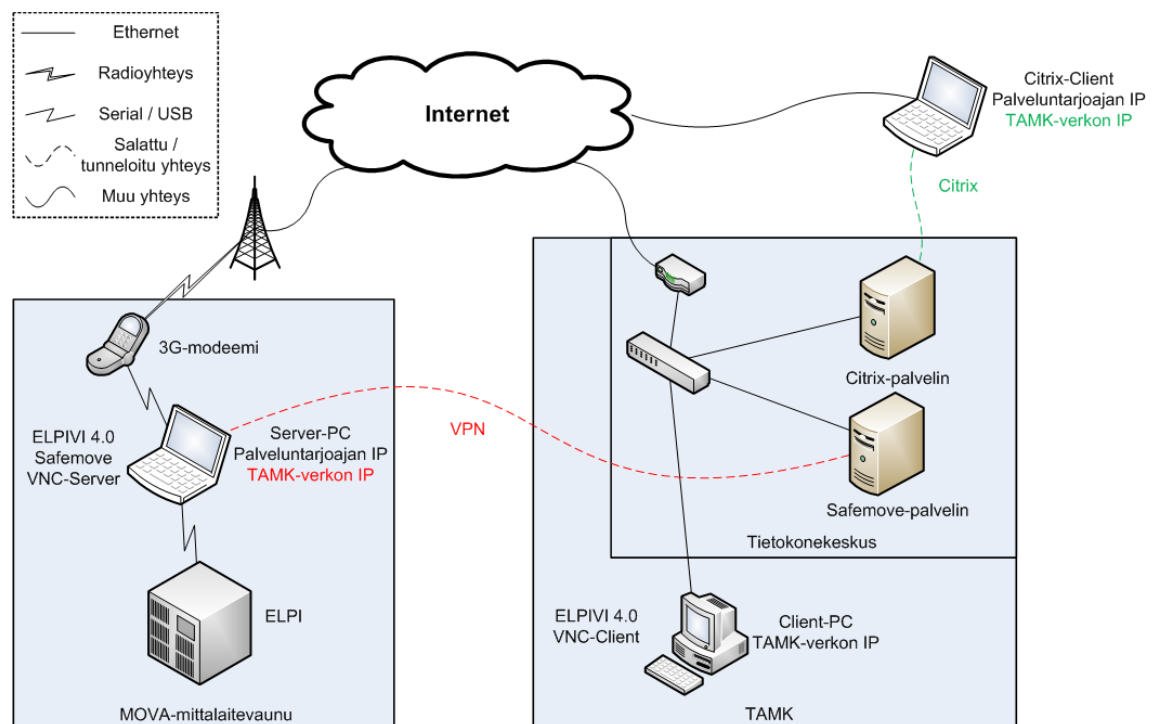
Ensimmäinen askel oli hankkia sopiva tietokone, johon mittalaitteisto tulnaisiin kytkemään. Tästä koneesta käytetään myöhemmin nimitystä Server-kone. Tähänärkevimmäksi ratkaisuksi valikoitui kannettava tietokone, joka olisi akkunsa turvin immuuni aiemmin mainitun kaltaisille lyhyille sähkökatkoille.

3G-palveluntarjoajan asettamat rajoitukset verkosta käyttäjälle päin avattavien yhteyksien suhteen, sekä joka yhteyskerralla vaihtuva IP-osoite, asettivat ensimmäiset kysymykset ratkaistaviksi. Molemmat näistä ongelmista pystyttäisiin kiertämään VPN-tunneloinnilla TAMK-verkkoon. /6/

Koska työn pääpaino oli ELPI-pienhiukkasmittalaitteen etäkäytössä, täytyi selvittää kuinka mittalaitteen ohjelmiston ELPIVIn oma etäkäyttötoiminto käyttäytyi. Lisäksi myöhemmässä vaiheessa työtä tutustuttiin myös etätyöpöytäyhteyksien toimintaan.

Server-koneen palomuurin vuoksi täytyi selvittää jokaisen käytettävän ohjelmiston osalta, mitä portteja palomuurista täytyisi avata. Myös fyysisten koneiden ja loogisten etäyhteyksien käyttämät IP-osoitteet oli selvitettävä, jotta pääsy voitaisiin rajoittaa mahdollisimman tarkasti.

Kuvassa 1 on esitetty etäkäyttöyhteyden topologia. Esitys on sama kuin liitteen 1 topologiakuvassa, ainoastaan IP-osoitetiedot on jätetty pois. Topologia ei muodostunut valmiiksi vielä selvitysvaiheessa, vaan se kehittyi työn edetessä. Periaate kuitenkin säilyi samanlaisena läpi koko työn. Kuvassa katkoviivalla merkityt yhteydet ovat loogisia eli ne osoittavat kuinka Citrix- ja VPN-yhteydet tuovat julkiseen verkkoon kytketyt koneet osaksi TAMKin tietoverkkoa.



Kuva 1 MOVA-etäkäyttöyhteyden topologia

4 Laitteisto

4.1 3G-modeemi

Tilaajan etäyhteyttä varten varaama 3G-modeemi oli Soneran liittymällä varustettu Huawei E220. Modeemi kytkettiin tietokoneen USB-porttiin. Se kykeni muodostamaan yhteyden käyttäen GSM- ja UMTS-järjestelmiä. Näistä tekniikoista on annettu lyhyt kuvaus 3G-yhteyskappaleessa.

Modeemin toimintaa tuli testata, jotta selviäisi yhteyden toimivuus heikommillakin kuuluvuusalueilla. Testausmenetelmiä ja -tuloksia käsitellään tarkemmin kappaleessa 5.

Työn toteutuksen ollessa vielä kesken, 3G-yhteyden palveluntarjoaja vaihtui Sonerasta Elisaksi. Muutosta on käsitelty tarkemmin luvussa 11.5.

4.2 Server-kone

Tietokonekeskukselta saatiin kannettava tietokone käytettäväksi mittalaitavaunussa. Tietokoneen merkki ja malli oli Fujitsu Siemens Lifebook E8010. Kone oli henkilökunnan käytöstä jo poistettu, mutta riittävän tehokas tämän työn tarkoituksiin.

Käyttöjärjestelmänä koneessa oli Windows XP. Lisäksi asennettuna oli F-securen tietoturvaohjelmisto.

Tietokonekeskus loi koneelle paikallisen pääkäyttäjätunnuksen. Tämä mahdollisti ohjelmien asentamisen ja asetusten muuttamisen ilman rajoituksia. Esimerkiksi tietoturvaohjelmiston palomuurisääntöjen muuttaminen ja ELPIVI-mittausohjelmiston asentaminen eivät olisi onnistuneet ilman pääkäyttäjäoikeuksia.

Server-koneen virransäästöasetuksia muokattiin niin, että tietokone ei mene pois päältä automaattisesti. Tällä eliminoitiin mahdollisuus koneen sammumiseen kesken pitkäkestoisen mittauksen.

4.3 Client-kone

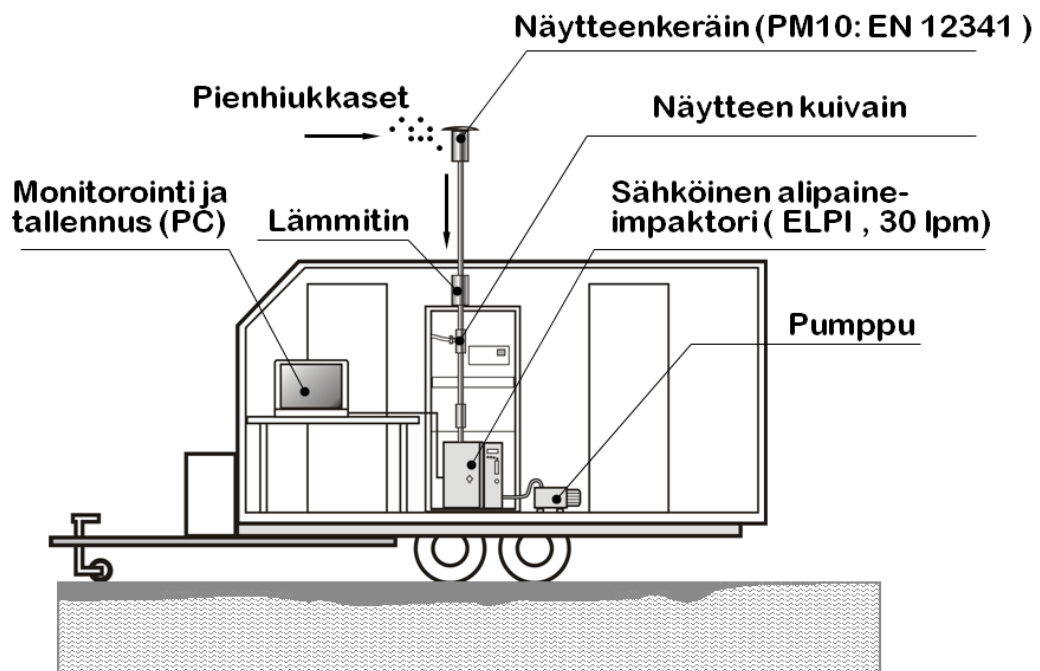
TAMKin sisältä tapahtuvaa etäkäyttöä varten varattiin E0-12-tilasta tietokone. Tilaan oli pääsy lähinnä sellaisilla henkilöillä, jotka toimivat materiaali- ja mittaustekniikan osaamiskeskuksen kanssa, joten sijainti oli hyvin tarkoituksenmukainen.

Myös Client-koneelle luotiin paikallinen tunnus pääkäyttäjäoikeuksin, jotta tarvittavia ohjelmistoja voitiin asentaa. Koska kone oli TAMKin sisäisessä verkossa, ei siihen ollut asennettu palomuuria, johon olisi tarvinnut tehdä muutoksia.

4.4 Mittalaite

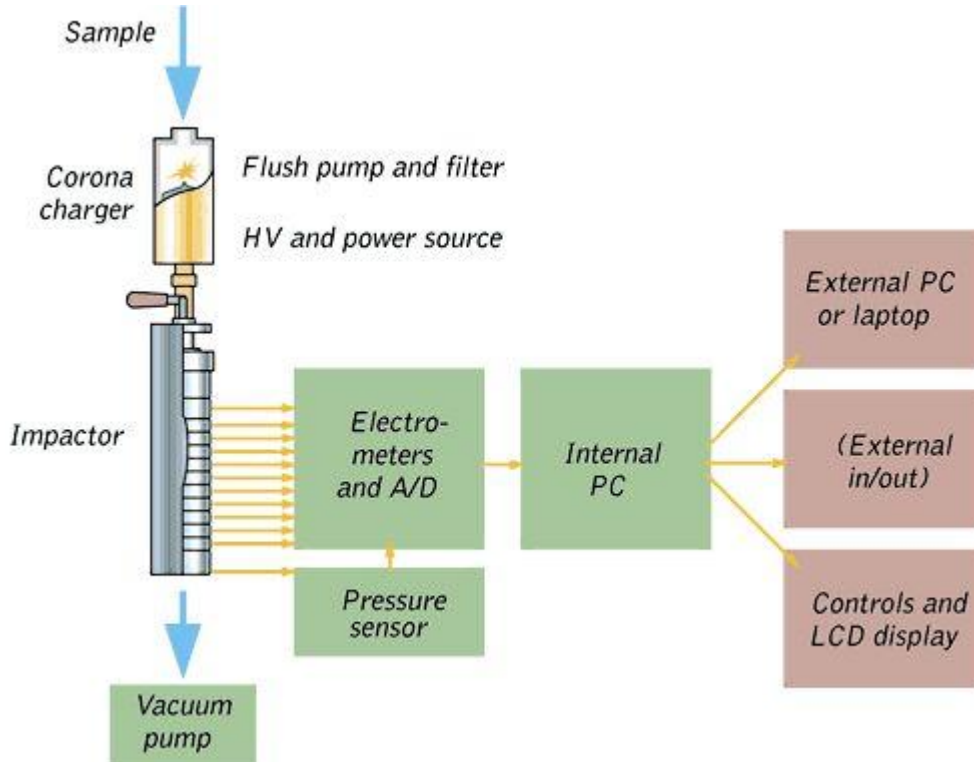
Toteutettavan yhteyden pääasiallinen käyttötarkoitus oli ELPI-pienhiukkasmittalaitteen käyttö. ELPI on Tamperelaisen Dekati Oy:n valmistama laite, jolla mitataan ilman pienhiukkaspitoisuuksia.

Yleisiä käyttökohteita ovat muun muassa kaupunki-ilman laadun mittaaminen sekä esimerkiksi louhostyömailla syntyvien pienhiukkaspitoisuuksien tarkkailu. Vaihtelevien käyttökohteiden vuoksi TAMKin mittalaite on sijoitettu siirreltävään vaunuun, joka tarjoaa kaikki tarvittavat oheistoiminnot ja suojatun ympäristön mittalaitteelle. Kaavio mittalaitevaunusta on esitetty kuvassa 2. /3/



Kuva 2 MOVA-mittalaitevaunu

ELPI-mittalaitteen toimintaperiaate on havainnollistettu kuvassa 3. Toiminta jakautuu kolmeen pääosaan: hiukkasten varaaminen unipolaarisessa koronavaraajassa, kokojaottelu moniasteimpaktorissa ja sähköinen havaitseminen herkillä elektrometreillä. Ensimmäiset näytehiukkaset varataan tunnettuun varaustasoon, minkä jälkeen ne saapuvat alipaineiseen impaktoriin, jossa on sähköisesti eristetyt keräinasteet. Hiukkaset kerätään impaktorin eri asteissa niiden aerodynaamisen halkaisijan mukaan. Hiukkasten kuljettama varaus eri impaktoriasteilla mitataan reaaliaikaisesti monikanavaisilla elektrometreillä. Mitatut virtasignaalit muunnetaan esittämään aerodynaamista kokojakaumaa. /1/



Kuva 3 Outdoor Air ELPI -mittalaitteen toimintaperiaate (Dekati Ltd 2007)

Mittalaitteen toimintaa ohjaa sisäinen tietokone. Kerätty mittaustiedot välitetään eteenpäin sarjaliikenneportin kautta. Mittalaitteeseen voidaan myös kytkeä näyttö ja näppäimistö asetusten muuttamista varten. Tähän jouduttiinkin turvautumaan eräässä ongelmatilanteessa, josta on kerrottu tarkemmin luvussa 11.2.

5 3G-yhteys

5.1 Yleistä

Työn toteuttamisessa käytettiin Huaweiin 3G-modeemia, jossa on Qualcommin valmistama piirisarja. Modeemi käyttää GPRS-, EDGE-, WCDMA- ja HSDPA-tekniikoita. Näistä GPRS ja EDGE ovat toisen sukupolven eli 2G-tekniikoita ja WCDMA sekä HSDPA varsinaisia 3G-tekniikoita.

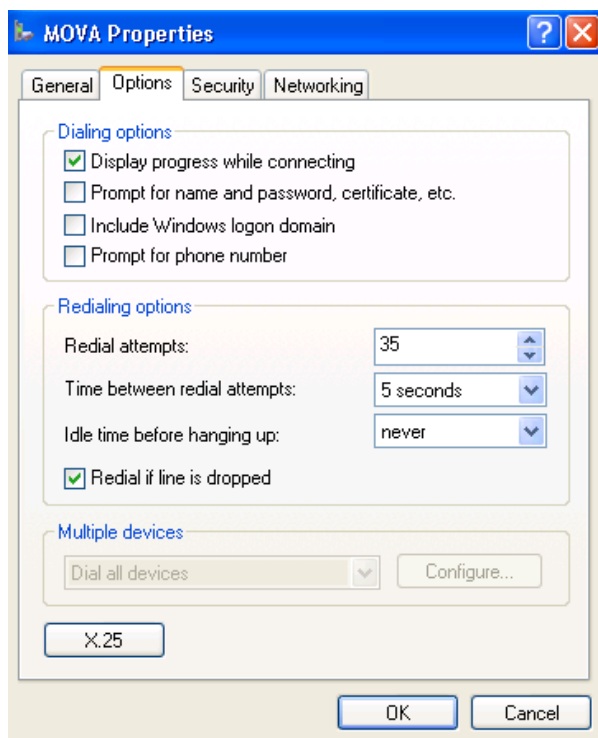
GSM-järjestelmään (Global System for Mobile communications) kuuluvat GPRS- ja EDGE-tekniikat (General Packet Radio Service ja Enhanced Data rates for GSM Evolution) ovat taajuus- ja aikajakaisia tekniikoita. Käyttäjälle on varattu tietty taajuus käytettäväksi ja tältä taajuudelta yksi tai useampi aikaväli verkon kuormituksesta riippuen. Teoreettiset maksimisiirtonopeudet downlink-suunnassa eli verkolta käyttäjälle päin ovat GPRS:llä 80 kb/s ja EDGE:llä 236,8 kb/s [2].

UMTS-järjestelmään (Universal Mobile Telecommunications System) kuuluvat WCDMA- ja HSDPA-tekniikat (Wideband Code Division Multiple Access ja High Speed Downlink Packet Access) ovat koodijakoisia tekniikoita. Useampi käyttäjä voi käyttää samaa taajuutta samaan aikaan ja signaalit erotellaan toisistaan koodausalgoritmein. Teoreettiset maksimisiirtonopeudet downlink-suunnassa ovat WCDMAlla 384 kb/s ja HSDPAlla 7,2 Mb/s /7/.

Mobiiliyhteyttä käytettäessä palveluntarjoajalta saadaan yhteyskohtainen IP-osoite, joka vaihtelee jokaisella yhteysistunnolla. Tämän vuoksi tarvittiin menetelmä, jolla Server-koneelle saataisiin kiinteä IP-osoite etäkäytön mahdollistamiseksi. Lisäksi palveluntarjoajat rajoittavat verkosta käyttäjälle suuntautuvaa liikennettä, mikä käytännössä estäisi etäistuntojen muodostamisen. Näihin ongelmiin saatiin ratkaisu luvussa 6 käsiteltävän VPN-tunneloinnin avulla.

5.2 Dial-up-yhteys

Yhteyttä testattaessa käytettiin pääasiallisesti Windowsin omaa Dial-up-toimintoa. Syynä tähän oli laajempi asetusten hallittavuus verrattuna 3G-modeemin mukana tulleeseen ohjelmistoon. Tärkeimmät asetukset, joita muutettiin, olivat katkenneen yhteyden automaattinen uudelleenyhdistäminen sekä käyttämättömänä olevan yhteyden aikakatkaisun estäminen. Dial-up-asetusikkuna on esitetty kuvassa 4.



Kuva 4 Dial-up-asetusikkuna

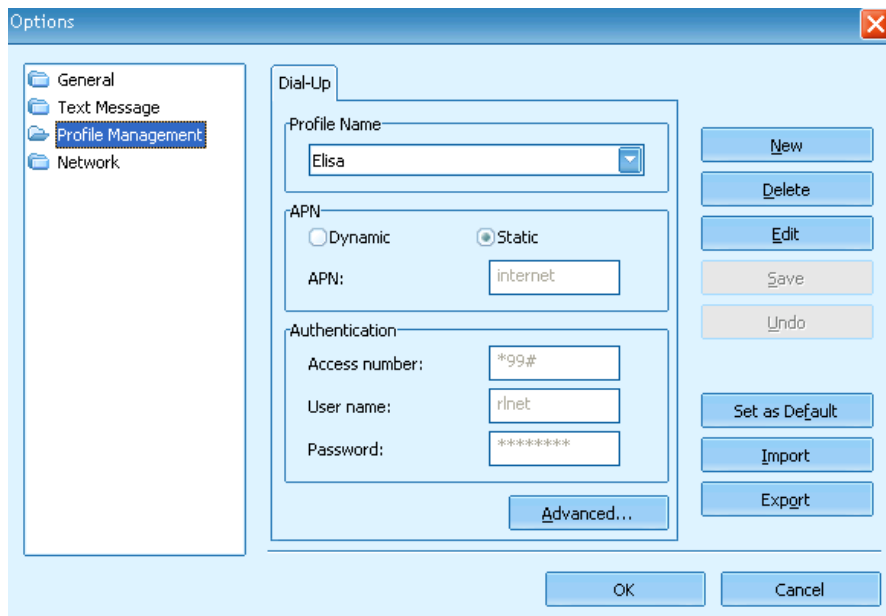
Asetusten muuttamisen jälkeen testattiin, kuinka Dial-up-yhteys toimisi huonolla kuuluvuusalueella. Tätä simuloitiin viemällä laitteisto sähkömagneettiselta säteilyltä suojattuun

tilaan. Ennen tilan sulkemista yhteys avattiin ja todennettiin toimivaksi käynnistämällä jatkuva ping-pakettien sarja. Tila suljettiin ja yhteys todettiin katkenneeksi modeemin merkkivalon vaihtumisen ja ping-vastausten katkeamisen perusteella. Kolmen minuutin kuluttua tila avattiin ja havainnoitiin aukeaisiko yhteys uudelleen. Kaikilla testauskerroilla yhdistäminen tapahtui automaattisesti ja ping-liikenne jatkui normaalisti.

5.3 Mobile Partner -ohjelmisto

Modeemin mukana asentuva yhteysohjelma oli mutkaton, mutta suppeammin hallittava tapa yhteyden luomiseen. Mobile Partner käyttää todellisuudessa myös käyttöjärjestelmän Dial-up-toimintoa, mutta piilottaen sen käyttäjältä. Tämä tuli ilmi eräässä ongelmatilanteessa, jota on käsitelty luvussa 11.3.

Ohjelmaan voidaan luoda yhteysprofiileja, jotka vastaavat Dial-up-profiileja. Näihin määriteltävät asetukset eivät kuitenkaan kattaneet kaikkia tarvittavia ominaisuuksia eli linjan automaattista uudelleenaukaisua ja aikakatkaisun estämistä. Mobile Partner -ohjelmiston asetussivuna on esitetty kuvassa 5. Ikkunassa ovat näkyvillä kaikki yhteysprofiiliin tehdyt asetukset.



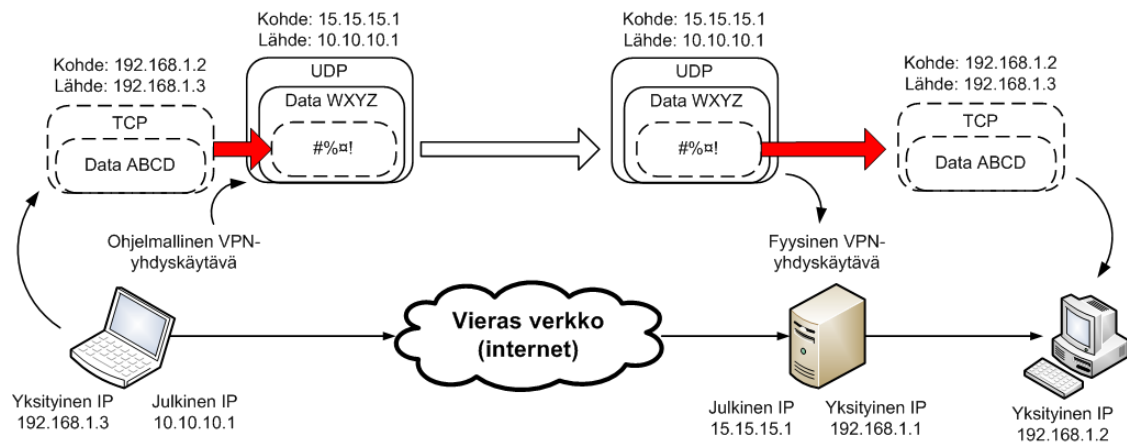
Kuva 5 Mobile Partner -ohjelman asetussivuna

6 VPN-tunnelointi

6.1 Yleistä

VPN eli Virtual Private Network on menetelmä, jolla päästään loogisesti osaksi yksityistä verkkoa julkisen tai vieraan verkon välityksellä. Yhteys toteutetaan yleensä suojaamalla viestit jollakin salausmenetelmällä, vaikka salaamatonkin yhteys voidaan joissain tapauksissa luokitella VPN-yhteydeksi. Kahden yksityisen verkon välinen yhteys vieraan verkon ylitse suojataan tunneloimalla. /5 s.95-96/

Tunnelointimenetelmä on tunneloitavan yhteysprotokollan piilottamista toisen protokollan sisään. Salauksilla varmistetaan tunneloitujen pakettien koskemattomuus ja suojaus. Kahden verkon välisessä tunneloinnissa tulee molemmissa verkoissa olla VPN-yhdyskäytävät, jotka muodostavat välilleen salatun yhteyden ja välittävät sitten yksityisen verkon viestejä kauttansa. Yhdyskäytävä voi olla erillinen laite, osa palomuuria tai ohjelmallinen. Tunneloinnin periaate on havainnollistettu kuvassa 6. /5 s.96/



Kuva 6 VPN-tunneloinnin periaate

6.2 Safemove-ohjelmisto

Safemove on Birdstep Technology Oyn valmistama VPN-ohjelmisto, jota käytettiin tässä työssä tunneloinnin luomiseen. Sen toiminta mahdollistaa salatun yhteyden pitämisen aktiivisena olosuhteiden muuttuessa ilman käyttäjän toimia. Esimerkiksi kytkeydyttäessä Ethernet-verkkoon 3G-yhteyden ollessa aktiivisena ohjelma vaihtaa itse käyttämään nopeampaa Ethernet-yhteyttä. Ainoa käyttäjältä vaadittava toimi on salauskoodin syöttäminen, kun yhdyskäytävä aukeaa ensimmäisen kerran tietokoneen käynnistymisen jälkeen.

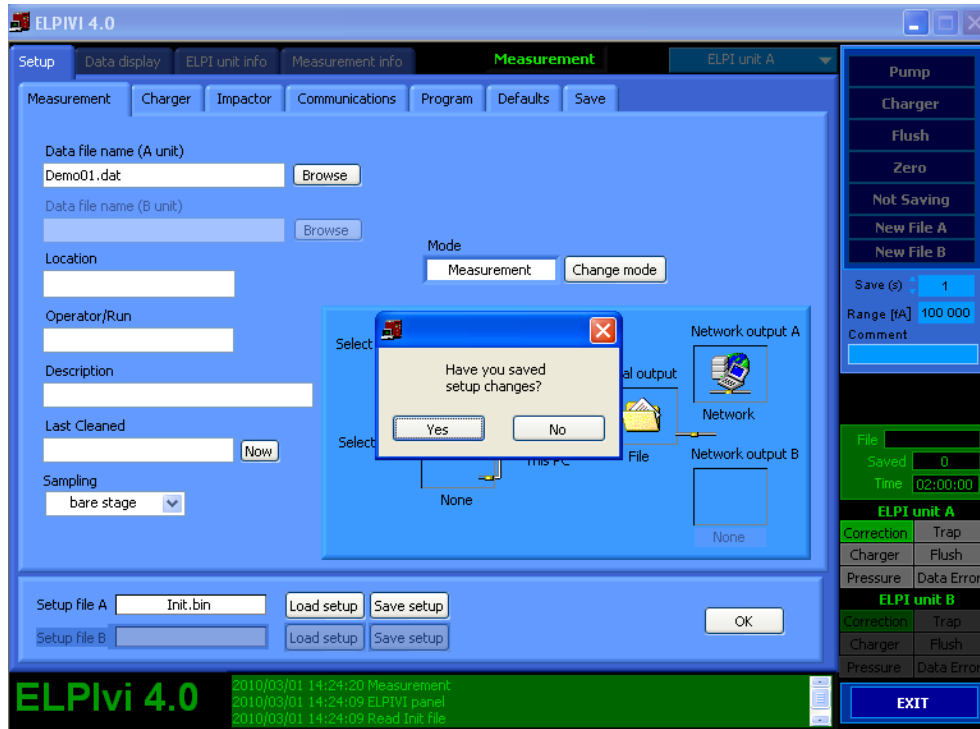
Ohjelma käyttää IPSec-salausprotokollan tunnelimoodia, jolla voidaan tunneloinnin lisäksi varmistaa viestien eheys ja lähettäjä sekä salata viestien sisältö. Ainoa avoin tieto menetelmässä on tunneliyhteyden viestin IP-otsikkotiedot. /5 s.291/

Tämän työn vaatimukseen Safemove vastasi todella hyvin. Loppukäyttäjälle mahdollisimman yksinkertaiseksi tehty ja kaikki tietoturva-vaatimukset täyttävä ratkaisu sopi aiottuun ympäristöön, jossa useimmilla käyttäjillä ei välttämättä ole tarvittavaa kokemusta monimutkaisempien ratkaisujen käyttöön.

Mahdollisen ongelman tämän ohjelmiston käyttämisessä tässä työssä aiheutti piakkoin umpeutuva käyttöoikeus. Tietokonekeskuksen mukaan lisenssi oli vanhentumassa kesällä 2010, eikä päätöstä sen uusimisesta ollut vielä tehty. Vaihtoehdoisen ratkaisun selvittäminen saattaa siis olla edessä tulevaisuudessa. Yksi tällainen ratkaisu voisi Mikko Vaaralan ehdotuksen mukaan olla julkisen domain-nimen käyttäminen.

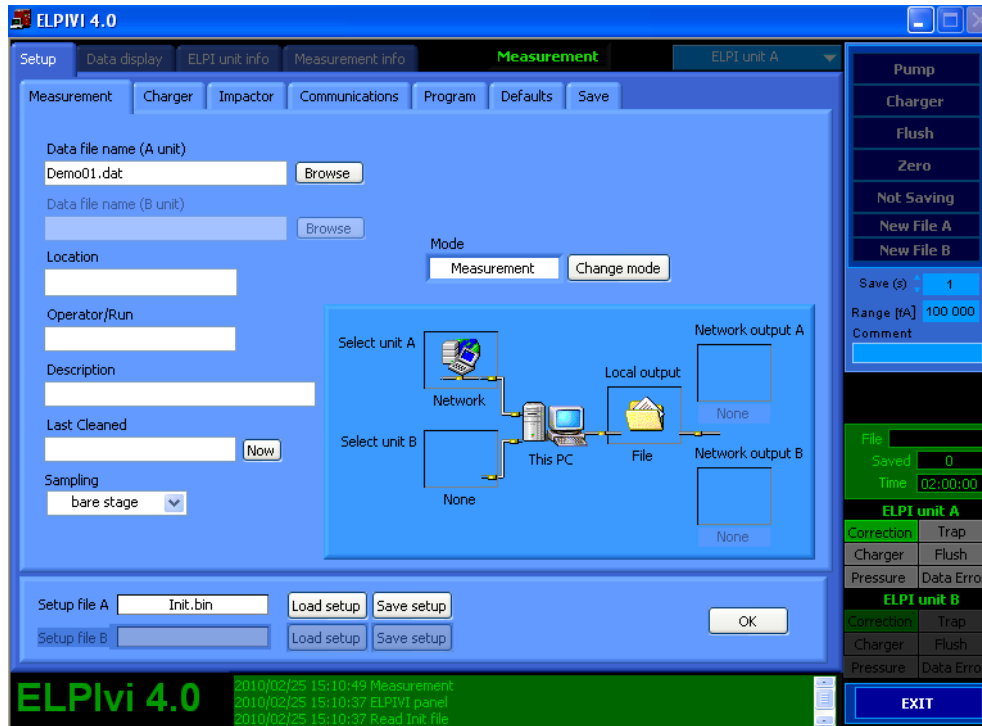
7 ELPIVI-ohjelmiston etäkäyttö

Mittausohjelmisto ELPIVI:ssä on itsessään etäkäyttöominaisuus, jolla mittausta voidaan valvoa lähiverkon välityksellä. Aina mittausta aloitettaessa täytyi Server-koneen ohjelmisto asettaa kuuntelemaan määrätystä TCP-portista yhteydenottoa Client-koneelta valitsemalla Network output A -kohtaan valinta Network. Asetusikkuna on esitetty kuvassa 7.



Kuva 7 Server-koneen ELPIVI-asetusikkuna

Avattaessa etäyhteyttä Client-koneelta, toimittiin samoin kuin mittausta käynnistettäessä. Input A -kohtaan valittiin verkkoyhteys mittausyksikön liitännäksi. Tämä on esitetty kuvassa 8. Lisäksi Communications-välilehdellä asetettiin kohdeosoitteeksi Server-koneen IP-osoite.



Kuva 8 Client-koneen ELPIVI-asetusikkuna

Kun yhteys koneiden välille oli muodostunut, kuvan 8 alareunassa näkyvään vihreään tapahtumakenttään tuli Client-koneella ilmoitus ”Unit A connected”. Tämän jälkeen Client-koneen ELPIVI toimi kuin se olisi kytketty suoraan mittalaitteeseen.

Client-kone avasi aina yhteyden satunnaisesta TCP-portista Server-koneen määrättyyn TCP-porttiin. Jos yhteys koneiden välillä katkesi, siitä ilmestyi tapahtumakenttään ilmoitus ”Unit A disconnected”. Tämän jälkeen Client-kone yritti avata uuden yhteyden järjestyksessä seuraavasta TCP-portista.

8 Etätyöpöytä

8.1 VNC-etätyöpöytä

RealVNC on kevyen ja varsin monipuolisen etäkäyttömahdollisuuden tarjoava ohjelmisto. Se koostuu kahdesta erilaisesta palvelinkomponentista ja yhdestä etäkäyttösovelluksesta. Palvelinkomponenteista toinen on taustaprosessina käynnistyvä Service mode ja toinen käyttäjän käynnistystä vaativa User mode. Etäkäyttösovellus on nimeltään VNC Viewer.

Palvelinkomponenttien asetuksissa voidaan määrittää etäyhteyden tietoturvaan vaikuttavia asetuksia. Yhteydelle voidaan määrittää käyttäjätunnus ja salasana, joita kysytään etäyhteyttä avattaessa. Lisäksi Server-koneen paikallinen käyttö voidaan estää etäyhteyden ollessa aktiivisena ja kone voidaan asettaa lukitustilaan, kun etäkäyttö päättyy. Nämä ovat hyödyllisiä asetuksia, joilla asiaton käyttö voidaan estää vaikka Server-konetta ei voida valvoa fyysisesti.

Merkittävä ero RealVNC-ohjelman etätyöpöydässä verrattuna Windows Remote Desktop -työpöytään on paikallisen konsoli-istunnon käyttäminen Terminal Service -istunnon sijaan. Konsoli-istunto vastaa fyysisesti koneella olevan käyttäjän tekemiä toimia ja Terminal Service on Windowsin etäkäyttökomponentti. Käytännössä tämä ero näkyy etäkäytön ja paikallisen näyttöpäätteen yhtenäisyytenä jopa hiiren osoittimen liikkeissä.

Tämän työn toteutuksessa käytettiin Server-koneella RealVNC Service mode - palvelinkomponenttia, sillä lukitulle koneelle ei voitu kirjautua User mode -komponentin ollessa käytössä. Tietoturva-asetuksista käyttöön asetettiin salasana-asetus, paikallisen käytön esto ja koneen lukitus etäyhteyden katkettua.

Client-koneella VNC Viewer -ohjelman asetuksissa määriteltiin visuaalisten elementtien rajoituksia turhan liikenteen minimoimiseksi. Esimerkiksi etätyöpöydän väriavaruus asetettiin kahdeksanbittiseksi eli 256 väriin, kun paikallisessa käytössä väriavaruus on 32-bittinen.

8.2 Citrix-etätyöpöytä

TAMKin tietoverkon ulkopuolinen etäkäyttö ei ollut mahdollista aikaisemmin mainituilla menetelmillä, johtuen käytetyistä yksityisen alueen IP-osoitteista. Citrix-ohjelmiston avulla TAMKin verkon ulkopuolinen kone pääsee kuitenkin käyttämään joitain sisäisiä resursseja. Koneelle asennettu ohjelma avaa yhteyden haluttuun Citrix-palvelimeen, tässä tapauksessa *et.tamk.fi*. Tämän jälkeen Citrix-käyttäjällä on käytössään palvelimella toimiva, virtuaalinen, sisäverkon tietokone, jolta voidaan avata etätyöpöytäyhteys Server-koneeseen. Citrix-yhteys on kuvattu liitteen 1 ja kappaleen 3 topologiakuvissa.

Etätyöpöytäyhteys toimii käyttäen Windowsin Remote Desktop -toimintoa. Kuten edellisessä luvussa on mainittu, toiminto käyttää Terminal Services -komponenttia, joka eroaa paikallisesta käyttäjäistunnosta. Avattaessa yhteys paikallinen konsoli-istunto menee lukitustilaan, sillä Windowsin käyttäjäversio sallii vain yhden aktiivisen istunnon kerrallaan /4/. Tämä tuo tiettyjä rajoituksia ja ongelmia, joita on käsitelty luvussa 11.4.

Ongelmien vuoksi Citrix-etäkäyttö ei osoittautunut hyväksi menetelmäksi perusluontoiseen etäkäyttöön. Mittauksen tuloksiin mahdollisesti vaikuttava häiriö rajoitti käytön vain selvien vikatilanteiden hoitoon. Jos mittausvaunulta saataisiin hälytys esimerkiksi sähkökatkoksesta, eikä mittauspaikalla käynti tai etäkäyttö TAMK-verkon sisältä tulisi kysymykseen, voitaisiin asiaa tutkia Citrix-yhteyden avulla. Muutoin tulisi kuitenkin käyttää VNC-etätyöpöytää normaaliin valvontaan ja etäkäyttöön.

9 Tiedostonsiirto

Työn tilaaja esitti ensimmäisten testausten jälkeen toiveen tiedostonsiirron mahdollisuudesta Client- ja Server-koneiden välillä. Pääasiallinen käyttötarkoitus oli mittaustuloksia sisältävien tiedostojen siirto. Käytettäessä ELPIVI-mittausohjelman etäkäyttötoimintoa oli mahdollista

tallentaa mittausdataa Client-koneelle, mutta ainoastaan etäkäytön ajalta. Pidemmän aikavälin mittaustuloksia ei siis voitu siirtää.

Molemmissa etätyöpöytäsovelluksissa piti olla mahdollisuus tiedostonsiirtoon leikepöydän kautta. Tämä tarkoitti tiedoston siirtoa Windowsin "Kopioi-Liitä"-toimintoa käyttäen. Server-koneen etätyöpöydällä voitaisiin siis kopioida tiedosto ja liittää se sitten Client-koneen paikalliselle työpöydälle. Tätä ominaisuutta ei kuitenkaan saatu toimimaan Remote Desktop-, tai RealVNC-etätyöpöytien avulla.

Koska ongelman ratkaisuun ei ollut riittävästi aikaa, päädyttiin etsimään vaihtoehtoinen menetelmä. Server-koneen ollessa loogisesti osa TAMKin sisäverkkoa, oli siltä pääsy myös TAMKin verkkolevyille. Vaikka automaattista verkkolevyihin yhdistämistä ei ollutkaan valmiiksi asetettu, oli levyihin yhdistäminen kuitenkin varsin yksinkertaista. Tarkempi kuvaus on annettu liitteen 2 käyttöohjeessa.

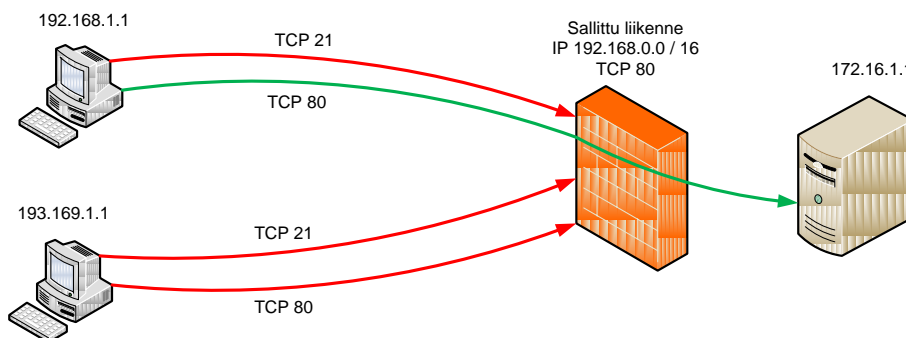
Tiedostojen siirto Server-koneelta TAMKin verkkolevyille osoittautui riittävän suoraviivaiseksi menetelmäksi. Näin ollen ei ollut tarpeellista tämän työn puitteissa etsiä muita ratkaisuja tiedostonsiirtoa varten.

10 Palomuri

10.1 Yleistä

Palomuurin tarkoituksena on ei-toivotun liikenteen suodattaminen halutun liikenteen seasta. Tällä voidaan estää esimerkiksi omalle koneelle päässeiden haittaohjelmien leviäminen, sekä asiaton pääsy jaettuna oleviin resursseihin. Palomureja on sekä erillisinä laitteina että ohjelmallisina.

Yleensä toimintaperiaate on, että kaikki paitsi erikseen hyväksyty liikenne torjutaan. Poikkeussääntöjä voidaan luoda käytettävän portin, taikka IP-osoitteiden perusteella. Kuvassa 9 on esitetty palomuurin toiminta yksinkertaistettuna. Käytännössä palomuurisäännöt voivat olla, ja niiden tuleeekin olla, huomattavasti monimutkaisempia kuin esimerkissä.



Kuva 9 Palomuurin toimintaperiaate yksinkertaistettuna

10.2 Server-koneen asetukset

Server-koneelle asennettuun palomuriin täytyi tehdä sääntöjä, jotta etäkäyttöliikenne oli mahdollista. Kullekin etäyhteyskäytännölle luotiin omat palomuurisääntönsä, jotta mahdollisten muutosten hallinta olisi suoraviivaista. Tarkat kuvaukset tehdyistä säännöistä on esitetty liitteessä 3.

Palomuurisääntöjen luominen oli kaksivaiheista. Ensiksi luotiin palvelusääntö, jossa määriteltiin käytettävä kuljetuskerroksen protokolla sekä lähettävät ja vastaanottavat portit. Protokolla oli kaikissa tapauksissa TCP, kun taas käytettävät portit riippuivat ohjelmasta, jolle sääntöä luotiin. Esimerkiksi ELPIVI-ohjelman säännössä vastaanottavia portteja oli vain yksi, joka oli ohjelman oletusasetusportti. Palvelusäännöt nimettiin aina kyseessä olevan ohjelman mukaan sekaannuksien välttämiseksi.

Toinen vaihe oli luoda yhteysääntö. Määriteltäviä asioita olivat säännön tyyppi, osoitteet, käytettävä palvelusääntö ja suunta, johon sääntöä sovellettiin. Säännön tyyppejä ovat estävä tai salliva sääntö. Tyyppi määrää mitä ehdot täyttävälle liikenteelle tehdään. Osoitteet voitiin määrittää IP-verkon, yksittäisen IP-osoitteen tai isäntänimen mukaan. Käytettävällä palvelusäännöllä voitiin rajata protokolla- ja porttikohtaisia ehtoja. Soveltamissuunta määrää koskeeko sääntö tulevaa, lähtevää vai kummankinsuuntaista liikennettä. Lisäksi yhteysääntö voitiin määrittää hälyttämään, jos ehdot täyttävää liikennettä havaittiin.

Luodut yhteysäännöt noudattivat pitkälti samaa rakennetta. Jokaisen säännön tyyppiä asetettiin sallia ehdot täyttävä liikenne. Osoitteina käytettiin Client-koneen isäntänimeä ELPIVI- ja VNC-sääntöjen osalta, sekä Citrix-säännössä Citrix-palvelimelle osoitettuja TAMKin sisäverkon osoitteita. Palvelusäännöt oli luotu jokaiselle etäkäyttömenetelmälle erikseen, kunkin käyttämien porttien mukaan. Kaikki yhteysäännöt asetettiin sallimaan liikenne molempiin suuntiin.

11 Ongelmat

11.1 TCP-yhteys

Testattaessa ELPIVI-ohjelmiston etäkäyttöä, havaittiin ongelmia Server- ja Client-koneiden välisessä yhteydessä. Ensiksi ongelma havaittiin ELPIVI:n tapahtumalistassa, joka antoi jatkuvasti Client-koneella ilmoituksia "Unit A disconnected". Lisäksi ohjausdata Client-koneelta Server-koneelle ei mennyt perille kuin harvoin. Ongelman tarkastelu aloitettiin käyttäen käyttöjärjestelmän komentokehoteen netstat-toimintoa. Netstat näyttää kaikkien kuljetuskerroksen yhteyksien tilan, lähde- ja kohdelaitteiden nimet tai IP-osoitteet sekä käytetyt porttinumerot.

Tarkastelussa selvisi, että TCP-yhteys aukesi Client- ja Server-koneiden välillä kuten pitikin. Client-kone aloitti yhteyden aloituskättelyn lähettämällä satunnaisesta portista TCP_SYN-viestin

Server-koneen määrättyyn porttiin. Jos Server-kone vastasi kättelyyn normaalisti, siirtyi yhteys tilaan ESTABLISHED. Tällöin myös ELPIVI ilmoitti "Unit A Connected". Yhteys kuitenkin katkesi yleensä noin kymmenen sekunnin kuluttua, jolloin netstat näytti ensin TIME_WAIT-tilaa ja hetken päästä yhteys katosi listalta. Tämän jälkeen Client-kone lähetti uuden TCP_SYN-viestin järjestyksessä seuraavasta portista Server-koneen määrättyyn porttiin.

Ensin koitettiin olisiko Client-koneen ELPIVIN "Remote ELPI timeout" -asetuksella vaikutusta ongelmaan. Oletusarvona asetuksella oli 10 000 millisekuntia, mikä vastasi aikaa, jonka yhteys yleensä pysyi aktiivisena. Asetus muutettiin 1 000 000 millisekuntiin, mutta se ei vaikuttanut ongelmaan millään tavalla.

Asiaa alettiin tutkia käyttäen Wireshark-protokolla-analysaattoria, jolla voidaan tarkastella ja tallentaa verkkoliikenteen paketteja. Havainnot vastasivat netstat-toiminnolla saatuja, minkä lisäksi paketeista nähtiin, että Client- ja Server-koneiden välillä liikkui dataa, eikä pelkkiä TCP-viestejä. Hyötydatan havaittiin kuitenkin koostuvan pääosin muutamista toistuvanlaisista paketeista. Verrattaessa Client- ja Server-koneiden Wireshark-logeja kävi ilmi, että pakettien kulku-aika vaihteli alle puolesta sekunnista jopa lähes kymmeneen sekuntiin. Tämä on huomattavan pitkä aika jopa 3G-yhteyttä käytettäessä.

Mobiilipalveluntarjoajan asettamia rajoituksia alettiin pohtia mahdolliseksi syyksi ilmiöön. Yleisen käytännön mukaan verkosta käyttäjälle päin suuntautuva liikenne oli rajoitettua. Tätä oletusta tuki myös havainto, että ongelma oli useammin läsnä käytettäessä 3G-yhteyttä, kuin testattaessa TAMKin vierailija-WLANiin kytkettyä Server-konetta. Toisaalta VPN-tunneloinnin olisi pitänyt eliminoida tämä mahdollisuus, sillä Safemove avasi aina yhteyden Server-koneelta TAMKin verkkoon. Varsinainen etäkäyttöliikenne oli näin ollen näkymätöntä palveluntarjoajalle. Myös tietokonekeskuksen Sami Setälän mukaan 3G-yhteyden rajoitusten ei pitäisi vaikuttaa käytettäessä VPN-tunnelointia. /6/

Ongelmasta oltiin yhteydessä mittausohjelmiston valmistaneeseen Dekatiin ja Safemoven valmistaja Birdstepiin, mutta kummallakaan taholla ei ollut kokemusta vastaavista tapauksista. Dekatin kanssa tutkittiin myös mahdollisuutta siitä, olisiko itse mittalaite voinut olla ongelman syynä. Tämä tehtiin, kun ELPI käytettiin huollossa luvussa 11.2 kuvatun ongelman vuoksi. Testauksessa todettiin kuitenkin mittalaitteen etäkäytön toimivan Dekatin tietoverkossa ilman ongelmia.

Mikko Vaaralan kanssa pidetyn tapaamisen jälkeen päädyttiin koittamaan, toisiko RealVNC-etätyöpöytä luotettavamman tavan etäkäytön toteuttamiseen. Oletuksena oli edelleen, että ELPIVI-ohjelman etäkäyttö oli ongelman syynä. Testattaessa asiaa TAMKin vierailija-WLAN-verkossa RealVNCn TCP-istunto pysyi aktiivisena ongelmitta. 3G-modeemilla ei kuitenkaan saatu avattua edes verkkoyhteyttä. Tämä tosin johtui Dial-up-asetusten muuttumisesta, jota on käsitelty luvussa 11.3.

Ongelman syy ja ratkaisu löytyivät lopulta tietokonekeskuksen ja Sami Setälän avulla. Tietokonekeskuksella oli selvinnyt, että Safemove-ohjelmiston kanssa oli ilmennyt ongelmia myös muissa sovelluksissa. VPN-tunnelin yhdyskäytävänä TAMK-verkosta ulospäin toimivassa virtuaalipalvelimessa oli häiriöitä järjestelmän kellon tahdistuksen kanssa. Safemovea ylläpitävä virtuaalikone kävi väärää aikaa jättäen noin kymmenen sekuntia joka minuutti. Palvelin joutui toistuvasti korjaamaan kelloa, mikä johti Safemoven salausavainten vaihtokäyttelyiden epäonnistumisiin ja viivästymisiin. Server-koneen kaiken verkkoliikenteen kulkiessa tämän yhdyskäytävän kautta, olivat myös etäkäyttösovellukset toistuvissa häiriötilanteissa. /6/

Tietokonekeskuksen päivitettyä palvelinalustan ongelma poistui. Tahdistusongelmat ja viiveet selittänevät myös Wireshark-logeissa havaitut aikaerot sekä TCP-yhteyksien sulkemiset. Kun TCP-segmentit eivät saapuneet perille ennen timeout-laskurin umpeutumista, yhteydet todettiin katkenneiksi. Näin ollen Client-kone joutui toistuvasti avaamaan uuden yhteyden Server-koneeseen. Tästä ongelmasta muodostui kynnyksikysymys yhteyden toteutuksessa ja sen korjaaminen oli suuri askel eteenpäin.

11.2 ELPI-mittalaite

Koska mittalaitteen toiminta rakentuu sisäisen tietokoneen ympärille, ovat myös jotkut vikatilanteet samankaltaisia kuin muissa tietokoneissa. Eräs tällainen ongelma ilmeni, kun ELPI ei käynnistynyt normaalisti. Ensiksi ongelma havaittiin koetettaessa yhdistää Server-konetta ELPIVI-ohjelman avulla mittalaitteeseen. Ohjelman tapahtumalistassa ei kuitenkaan näkynyt ilmoitusta mittausyksikön kytkemisestä. Aluksi oletettiin ongelman johtuvan viallisesta sarjakaapelista, mutta kaapelin vaihto ei korjannut asiaa.

Tarkasteltaessa mittalaitetta havaittiin, että näyttöpaneeliin ei ilmestynyt mitään. Laite toimitettiin valmistajan huoltoon, jossa selvisi, että sisäisen tietokoneen BIOS-asetukset olivat väärät. BIOS (Basic Input/Output System) on koneen emolevyllä olevalle piirille kiinteästi tallennettu järjestelmä, jonka avulla määritellään tietokoneen käynnistysasetukset. Laite yritti käynnistettäessä ladata käyttöjärjestelmänsä levykeasemalta kovalevyn sijaan. Asia korjattiin huollossa, mutta jo seuraavana päivänä ongelma uusiutui.

BIOS-asetukset osattiin nyt korjata ilman valmistajan huoltoa kytkemällä näyttö ja näppäimistö mittalaitteeseen. Koska ongelma kuitenkin toistui nyt aina kun laite oli sammutettu, alettiin epäillä sisäisen varmistuspariston olevan tyhjentynyt. Tämän pariston avulla BIOSiin tehdyt muutokset pysyvät tallessa koneen ollessa ilman sähköä. Laite toimitettiin jälleen huoltoon, jossa vaihdettiin mittalaitteen koko emolevy, sillä varmistusparisto oli kyseisessä mallissa kiinteä osa emolevyä. Emolevyn vaihtamisen jälkeen ongelma poistui.

Toinen vähäisempi ongelma ilmeni, kun Server-kone jouduttiin uudelleenkäynnistämään sen ollessa kytkettynä päällä olevaan mittalaitteeseen. Kun Server-kone oli ladannut käyttöjärjestelmänsä, havaittiin hiiren osoittimen pyrkivän kohti näyttöalueen oikeaa alakulmaa. Aluksi oletettiin ilmiön johtuvan juuri asennetusta ohjelmasta, jonka käynnistämä taustapalvelu

olisi saattanut aiheuttaa vian. Taustapalvelu poistettiin käytöstä, mutta ongelma ei hävinnyt. Tämän jälkeen Server-kone käynnistettiin ELPIn ollessa irtikytkettynä, jolloin ilmiö poistui. Tästä pääteltiin, että ELPIn sarjaporttiin tuottama liikenne jostain syystä sotki kannettavan tietokoneen kosketushiiren toiminnan. Ongelman havaittiin poistuvan myös irrottamalla sarjakaapeli Server-koneen ollessa käynnissä ja kytkemällä se sitten uudelleen. Tietokoneen uudelleenkäynnistys ei siis ollut välttämätöntä.

11.3 Dial-up-asetukset

Alun perin Server-koneelle luotiin Dial-up-profiili, joka nimettiin palveluntarjoajan mukaan: Sonera. Suoritettaessa testausta käyttäen vaihtelevasti Dial-up-toimintoa ja Mobile Partner -ohjelmaa, havaittiin Dial-up-asetusten muuttuvan. Aluksi oletus oli, että asetusten muuttumisen aiheutti juuri asennettu VNC-ohjelmisto, jonka taustaprosessi käynnistyi aina käyttöjärjestelmän käynnistyessä. Tämän vuoksi VNC-Service-osa poistettiin, mutta ongelma ei kuitenkaan poistunut.

Mobile Partner -ohjelman havaittiin myös nimeävän yhteysprofiilinsa Soneraksi. Server-koneelle luotiin uusi Dial-up-profiili "MOVA" ja alkuperäinen profiili "Sonera" poistettiin. Profiilin nimen muuttuminen poisti ongelman, mistä pääteltiin Mobile Partner -ohjelman toimivan Dial-up-toimintoa käyttäen.

11.4 Windows Remote Desktop ja Citrix

Ennen VNC-ohjelmiston käyttämistä koetettiin etäyöpöytäyhteys toteuttaa Windowsin Remote Desktop -toimintoa käyttäen. Yhteyden luominen onnistui ilman ongelmia, mutta sisäänkirjautumisen jälkeen yhteys katkesi.

Aluksi oletettiin, että kirjaututtaessa tietokoneelle etäyhteydellä, käynnissä olevat prosessit siirtyivät eräänlaiseen lepotilaan. Näin ollen myös VPN-yhteyttä ylläpitävä Safemove olisi mennyt lepotilaan, jolloin etäyhteys katkesi. Osoittautui kuitenkin, että ongelman syy oli Safemove-palvelimessa, joka aiheutti yhteyden hidastelua ja katkeilua. Tätä ongelmaa on käsitelty tarkemmin luvussa 11.1.

Kun Safemove-palvelimen vika oli korjattu tietokonekeskuksella, oli etäyhteyden toteuttamisessa siirrytty kokeilemaan VNC-etäyöpöytää. Seuraavan kerran Windows Remote Desktop -ongelmat ilmenivät testattaessa TAMK-verkon ulkopuolelta tehtävää etäkäyttöä Citrix-ohjelmiston avulla.

Testattaessa etäyöpöytäyhteyttä Citrix-ympäristön kautta, vastaan tuli ensiksi ongelmia huomattavan pitkän vasteajan osalta. Viive komennon antamisen ja vasteen saamisen välillä oli joissakin testeissä jopa useita minutteja. Lisäksi etäyöpöytäyhteys katkeili usein. Ongelman oletettiin johtuvan Citrix-ympäristöstä aikaisempien kokemusten perusteella. Asiasta ilmoitettiin tietokonekeskukselle.

Citrix-käytössä ilmeni ongelmia varsinkin mittausohjelmisto ELPIVIN yhteydessä. Mainitut viiveet olivat pisimmillään juuri kyseisen ohjelman kanssa. Lisäksi mittausdata vaikutti vääristyvän, ja ELPIVI antoi toistuvia ilmoituksia mittalaitteen sarjaliikennedatan epätahdistumisesta. Ensin tämän oletettiin johtuvan ELPIN emolevyn vaihdosta, josta on kerrottu tarkemmin kappaleessa 11.2. Varsin pian huomattiin kuitenkin ongelman esiintyvän vain Citrix-käytön yhteydessä. Tietokonekeskukselle välitettiin tieto myös tästä havainnosta.

Kerrottujen kuvausten perusteella tietokonekeskuksen Sami Setälä esitti, että Citrix tuskin oli syy ongelmiin. Luultavampi selitys oli ongelman liittyminen Server-koneena käytettyyn kannettavaan tietokoneeseen. Oletuksia olivat laskentatehon loppuminen sekä käyttöjärjestelmän rakenteelliset ominaisuudet. Asia voitiin selvittää testaamalla Windows Remote Desktop -yhteyttä, jota myös Citrix-etätyöpöytä käyttää. /6/

Testaus suoritettiin käyttäen TAMKin verkossa olevaa Client-konetta, jonka oli aikaisemmin todettu toimivan RealVNC-etätyöpöytää käytettäessä. Näin minimoitiin kaikki mahdolliset tuntemattomat muuttujat testauksessa. Server-koneessa käytettiin 3G-modeemia ja Dial-up-yhteyttä, kuten muutoinkin. Erityistä huomiota testauksessa kiinnitettiin siihen, vaikuttiko Remote Desktop -käyttö mittausdatan vääristymiseen ja sarjaliikenneportin virheilmoituksiin ELPIVI-mittausohjelmassa.

Saadut tulokset tukivat oletusta siitä, että ongelma liittyi Terminal Services -komponenttiin Server-koneen käyttöjärjestelmässä. Remote Desktop -käyttö TAMK-verkon sisältä oli muuten ongelmatonta, mutta ELPIVI-mittausohjelman kanssa esiintyi pitkiä viiveitä, mittausdatan vääristymistä ja sarjaliikenneportin virheilmoituksia. Tämä johtui todennäköisesti kommunikointiongelmista Terminal Services -istunnon kanssa /6/.

Ongelman korjaaminen tämän työn puitteissa ei ollut mahdollista, joten Citrix-etäkäyttö jäi ainoastaan akuutteihin vikatilanteisiin sopivaksi menetelmäksi. Tämäkin vain sillä edellytyksellä, että käynti mittauspaikalla tai etäkäyttö TAMK-verkon sisältä aiheuttaisi kohtuutonta haittaa.

11.5 3G-palveluntarjoajan vaihtuminen

Työn käytännön toteutuksen ollessa jo loppuvaiheessa TAMKin kaikki matkapuhelinliittymät vaihdettiin Elisan tarjoamiin liittymiin. Tämä koski myös etäkäyttöyhteyden 3G-modeemia. Asiasta oli annettu etukäteen julkinen tiedote TAMKin sisällä. Muiden huomiota vaativien seikkojen vuoksi asian selvittäminen oli kuitenkin jäänyt tekemättä.

Etäkäyttöympäristöä oltiin valmistelemassa koekäyttöön, kun havaittiin että 3G-modeemi ei saanut yhteyttä verkkoon. Mobile Partner -ohjelman avulla selvitettiin, että Soneran verkossa oli edelleen peittoa testauspaikalla. Oletuksia ongelman syistä oli kolme: modeemin lähetysteho ei ollut paikkaan nähden riittävä eli signaali ei saavuttanut tukiasemaa, modeemi oli vikaantunut tai liittymä ei ollut enää voimassa.

Yhteyttä yritettiin avata useaan kertaan paikkaa vaihtaen, mutta siitä ei ollut apua. Näin ollen ongelman syynä ei katsottu olevan lähetystehon riittämättömyys. Keskusteltaessa asiasta työn tilanneiden henkilöiden kanssa tultiin pian siihen tulokseen, että liittymä ei ollut enää voimassa TAMKin operaattorivaihdon takia. Asia oli inhimillisesti jäänyt huomiotta sekä työn toteuttajalta että tilaajilta. Uuden operaattorin liittymä saatiin käyttöön onneksi pian.

Liittymän vaihdon vuoksi Server-koneella jouduttiin tekemään muutoksia Dial-up- ja Mobile Partner -profiileihin. Palveluntarjoajan yhteysnumero vaihdettiin kumpaankin yhteydenmuodostusprofiiliin. Lisäksi Mobile Partner -ohjelmassa vanha profiili ”Sonera” poistettiin kokonaan ja korvattiin uuden palveluntarjoajan mukaan nimetyllä profiililla. Uuteen profiiliin tehtiin Elisan internetsivuilta haetun ohjeen mukaiset asetukset, jotka on esitetty luvun 5.3 yhteydessä. Muutosten jälkeen 3G-yhteys toimi jälleen ongelmitta.

12 Käyttöohje

Yhteyden toteutuksesta luotiin käyttöohje, jonka lopullinen versio on esitetty liitteessä 2. Ensimmäisessä versiossa ohjeistus jaoteltiin aihealueisiin samaan tapaan kuin tässä selostuksessa. Aihealueet olivat tietokoneiden käyttäjätunnukset, 3G-yhteys, VPN-yhteys, etäkäyttö ELPIVI-ohjelmistolla, etäkäyttö VNC-ohjelmistolla sekä Citrix-yhteys TAMKin ulkopuolisesta verkosta. Aihealueet oli pääosin jaoteltu vielä alilukuihin sen mukaan, koskiko ohje Server- vai Client-konetta.

Tilaajan kanssa tehdyn koekäytön yhteydessä kävi kuitenkin ilmi, että selkeämpi ja suoraviivaisemmin etenevä ohjeistus oli tarpeen. Käyttöohjeen ensimmäinen versio ei aina ollut riittävän yksiselitteinen loppukäyttäjän näkökulmasta. Ratkaisuna päädyttiin tekemään erilliset pikaohjeet Client- ja Server-koneilla käytettäväksi sekä erikseen Citrix-etäkäyttöön. Nämä pikaohjeet on esitetty liitteissä 4-6.

Pikaohjeista käyttäjä voi seurata askel askeleelta etenevää yksinkertaista ohjeistusta. Tarkempaan käyttöohjeeseen voidaan turvautua, jos ei tiedetä kuinka jokin asia tarkalleen tehdään. Esimerkiksi ensimmäistä kertaa etäyhteyttä käyttävä voisi käyttää varsinaista käyttöohjetta pikaohjeen tukena.

Lopulliseen käyttöohjeversioon lisättiin vielä kappale tiedostonsiirrosta. Citrix-käytön mahdollisista vaikutuksista mittaustuloksiin täytyi lisätä riittävän selkeä huomautus sekä käyttöohjeeseen että Citrix-pikaohjeeseen.

13 Loppusanat

Työn lopputuloksena saatiin aikaan toimiva etäyhteys MOVA-mittalaitteistoon laitteiston käyttämiseksi. Monta seikkaa jäi kuitenkin odottamaan tulevia parannuksia, kuten jatkuvasti

kehittyvän tietotekniikan alalla yleensäkin. Toivottavasti tämä työ tarjoaa hyvän pohjan mahdollisille kehitysideoille.

Huomioitavia seikkoja kehityksessä ovat ainakin vaihtoehto Safemove-ohjelmalle, tietoturvan parantaminen sekä TAMK-verkon ulkopuolelta tapahtuvan etäkäytön mahdollistaminen paremmalla menetelmällä. Jos Safemove-lisenssiä ei uusita tietokonekeskuksella, täytyy etsiä vaihtoehtoinen ratkaisu tietoturvallisten yhteyden toteuttamiseksi. Tietoturvan parantamista tulee pohtia tietokonekeskuksen kanssa, sillä heiltä löytyy tieto vaatimuksista ja mahdollisesti valmiita ratkaisumalleja. Citrix- ja Remote Desktop -käytön ja Terminal Services -komponentin aiheuttamat häiriöt mittauksissa tuovat tarpeen paremman ratkaisun löytämiselle. Ei ole suotavaa, että apukeinoksi tarkoitettu menetelmä häiritsee varsinaista mittaustoimintaa.

Keskeisiä tekijöitä työn eteenpäinviemisessä olivat vastaantulevat ongelmat. Tällaisessa käytännönläheisessä työssä oli hyvin haastavaa esittää selkeästi eri ongelmat ja niiden ratkaisut suhteessa toisiinsa. Jatkuva työn seuranta sekä havaintojen ja päätelmien kirjaaminen helpottaa lopullisen raportoinnin tekoa. Valitettavasti kyseinen menetelmä tuntuu usein hidasteelta käytännön ratkaisua tehtäessä ja jää liian helposti huomiotta. Ei voida siis liiaksi painottaa oman työn seurannan merkitystä yhteyden jatkokehityksessä.

Lähteet

- 1 *Dekati Ltd 2007. Outdoor Air ELPI operating principle. [www-sivu]. [viitattu 8.3.2010].*
dekati.com/cms/outdoor_air_elpi/operating_principle.
- 2 *General Packet Radio Service. [www-sivu]. [viitattu 8.3.2010].*
en.wikipedia.org/wiki/General_Packet_Radio_Service.
- 3 *Lilja, Jarmo & Arvela, Pasi. Perehdytys MOVA-mittalaittevaunuun 29.9.2009.*
Tampereen ammattikorkeakoulu.
- 4 *Remote Desktop Services. [www-sivu]. [viitattu 8.4.2010].*
en.wikipedia.org/wiki/Remote_Desktop_Services.
- 5 *Ruohonen, Mika 2002. Tietoturva. Peruskirjat-sarja. Jyväskylä: Docendo.*
- 6 *Setälä, Sami, erikoissuunnittelija. Keskustelut ja sähköpostit lokakuu 2009 –*
maaliskuu 2010. Tampereen ammattikorkeakoulu.
- 7 *Universal Mobile Telecommunications System. [www-sivu]. [viitattu 8.3.2010].*
en.wikipedia.org/wiki/Umts.

Liitteet

Liite 1: MOVA-topologia

Liite 2: MOVA-käyttöohje

Liite 3: Server-koneen palomuurisäännöt

Liite 4: Pikaohje – Server-kone

Liite 5: Pikaohje – Client-kone

Liite 6: Pikaohje – Citrix-käyttö