PELASTUSOPISTO

MONIKA HANKKEEN LOPPURAPORTTI

MONIKANAVAREITITYKSEN SUUNNITTELU VIRANOMAISTOIMINTAAN

Pelastusopiston julkaisu

B-Sarja: Tutkimusraportit

1/2013

ISBN 978-952-5905-38-0

ISSN 1795-9160

PELASTUSOPISTO

MoniKa-hankkeen loppuraportti

Monikanavareitityksen suunnittelu viranomaistoimintaan

Hassinen Marko, FT, Pelastusopisto, Tutkimus- ja kehittämisyksikkö

Tutkimusraportti 44 s., 2 liitetä (8 sivua)

Syyskuu 2013

TIIVISTELMÄ

Pelastusopiston tutkimus- ja kehittämisyksikön toteuttaman ja Palosuojelurahaston pääasiallisesti rahoittaman MoniKa hankkeen tavoitteena oli kehittää luotettava langaton laajakaista viranomaiskäyttöön. Vaikka työn konteksti oli luonnollisesti pelastustoimessa, työssä pyrittiin rakentamaan ratkaisua joka olisi kaikkien viranomaisten käytettävissä.

Hankkeen tärkeimpinä yhteistyökumppaneina olivat pelastuslaitokset sekä Erillisverkot Oy. Pelastuslaitoksilta kerättiin langattoman laajakaistapalvelun loppukäyttäjävaatimuksia sekä muita tietoja liittyen lähinnä loppukäyttäjäympäristöön, kuten pelastustoimessa käytettäviä sovelluksia. Tällä tavoin varmistettiin, että lopullinen tuote vastaisi mahdollisimman tarkkaan loppukäyttäjän tarpeita.

Koko hankkeen olennaisena lähtökohtana oli langattoman laajakaistan kautta saatavat palvelut, joten pelastustoiminnan kannalta tärkeiden palveluiden tunnistamiseen kiinnitettiin erityistä huomiota ja arkkitehtuuria rakennettiin siten, että nämä palvelut saadaan käyttöön. Perusajatuksena oli, että pelkän laajakaistaisen yhteyden hyöty jää vähäiseksi jos se ei mahdollista olennaisten palvelujen sujuvaa käyttöä. Koska tulevaisuuden olennaisimmat palvelut tulevat olemaan kaikille turvallisuusviranomaisille yhteisiä ja sijaitsemaan valtion turvallisuusverkko TUVEssa, oli yhteys TUVEssa tuotettuihin palveluihin koko kehitystyön keskiössä ja siihen liittyvät tietoturvamenettelyt nousivat verraten tärkeiksi.

Hankkeessa myös evaluoitiin ja pilotoitiin markkinoilla olevia päätelaitteita (monikanavareitittimiä). Kaikki evaluoidut tuotteet olivat kotimaisia. Laitteita myös kenttätestattiin, mutta hankkeen resurssien puitteissa ei lähdetty rakentamaan niin vakioitua testausympäristöä, että tulosten perusteella laitteiden paremmuutta voisi arvioida. Testituloksista saa kuitenkin yleiskäsityksen tarjolla olevasta laitekannasta ja monikanavareititykseen liittyvistä haasteista.

EMERGENCY SERVICES COLLEGE

Multichannel Routing Design for Safety and Security Officials

Hassinen Marko, Ph.D., Emergency Services College, R&D unit

Research report 44 pages, 2 attachments (8 pages)

September 2013

ABSTRACT

MoniKa was a project lead by the R&D unit of the Emergency Services College, Finland. This project was funded mostly by the Fire Protection Fund (Palosuojelurahasto). Most important partners in the project were the Finnish network operator Erillisverkot Oy and the network of Finnish fire departments.

The main goal of the project was to develop a secure, reliable mobile broadband access for safety organizations. Although main focus was in fire & rescue services, the scope of the work was the whole scale of safety organizations.

In order to get the most out of the broadband access, a lot of attention was paid to identify the services needed in the field work of emergency organizations, and to design the architecture so as to facilitate the availability of these services. As some of the most important services in the future will be located in the high security government network, data security played very important role in the architecture design. Certain challenges were met in data security as safety organizations, such as fire & rescue and emergency medical services, are provided by municipal organizations. Traditionally, very few data systems common for municipal and government safety & security organizations have existed in Finland. In Fire & Rescue the users are heterogeneous as are the service used, which makes the data security design challenging when the data systems contains sensitive data on various protection levels.

The MoniKa project also evaluated and tested a number of multichannel routers available on the market. The selection of devices labeled multichannel router is vast and heterogeneous. Clearly, there is certain correlation on price and what you get with the money. On device selection, the main decision should be made between cost and recognized needs. In order to make some intelligent and waterproof claims on the quality and performance of the devices, test environment have to be more standardized than the one used in this study. Hence, only very general observations on the test results are made in this document.

Sisällys

Johdanto ... 7
MoniKa hanke ... 8
Hankkeen lähtötilanteen kuvaus ... 8
Hankkeen tavoitteet ... 8
Toimintaympäristö ... 9
PEIP ... 9
VARANTO ... 9
ERICA ... 9
KEJO ... 10
TUVE ... 10
Pelastustoimen tarvitsemat palvelut ja niiden saatavuus ... 11
TUVE verkossa tuotettujen palvelujen saatavuus ... 11
Palvelujen saatavuus kuntien verkoista ja internetistä ... 12
Tietoturvaan liittyvät kysymykset ... 13
Monikanavareitityksen asemoituminen pelastustoimen IT infraan ... 13
Reititinvalmistajat ... 17
Goodmill Systems ... 17
Ajeco ... 19
Indagon ... 23
Tosibox ... 26
Räätälöinnit ... 27
OpenWRT ... 28
Kenttätestijärjestelyt ... 29
Tosibox ... 34
Indagon ... 34
Ajeco ... 35
Goodmill Systems ... 36
Kenttätestien tulokset ... 37
Luotettavuus ... 37
Helppokäyttöisyys ... 37
Kaistan leveys ... 37
Pilottikohteet ja pilottien tulokset ... 38

Keski-Suomen pelastuslaitos 38
Keski-Pohjanmaan ja Pietarsaaren alueen pelastuslaitos 40
Pelastustoimen langaton laajakaista palveluna 41
Palvelukuvaus 41
LIP –palveluun liittyminen 41
LIP palvelun sisältö 41
Palvelun rakentaminen 42
Yhteenveto 43
Suositukset 43
Laitteistojen ja hallintajärjestelmien source escrow 44
Laitteistojen ja tietoliikennejärjestelyjen tietoturva ja auditoinnit 44

Johdanto

Kiteytetysti MoniKa -projektin tarkoituksena oli määritellä ja tuotteistaa pelastusviranomaisille soveltuva varmennettu langaton laajakaistayhteys. Tämä määritelmä on jalostunut projektin edetessä ja poikennee sanamuodoltaan, jos ei jopa osittain sisällöltään alkuperäisestä. Projektin lähtökohdat, toimenpiteet ja saadu tulokset esitellään tässä raportissa. Raportista on koetettu saada yhtä aikaa sekä kattava että riittävän kompakti, jotta sen voi lukea yhdeltä istumalta.

Projektin tutkijan lähtökohtana projektin alkumetreillä oli ajatus, että yllä mainitun kaltainen yhteys on kutakuinkin yhtä käyttökelpoinen kuin ne palvelut, joita yhteyttä hyödyntäen voi käyttää. Pelkkä yhteys ei tyydytä loppukäyttäjää, oli kaistan leveys mitä tahansa, jos käytettävissä olevat palvelut eivät tue organisaation ydintehtävää, tässä tapauksessa pelastustoimintaa ja sen johtamista.

Näillä lähtökohdilla oli selvää, että pelkän verkkoteknologian ja markkinoilla olevien laitteiden tutkiminen ja niiden tulosten raportointi ei edistäisi loppukäyttäjän perimmäisiä tarpeita. Verraten suuri painoarvo projektin edetessä laitettiin työhön jossa luotiin lähtökohtia mahdollisimman laaja-alaisen palveluvalikoiman saatavuudelle. Konkreettisesti tällä tarkoitetaan sitä, että tavoitteeksi asetettiin tuotetun laajakaistayhteyden avulla saada käyttöön palveluita niin julkisesta internetistä kuin valtion korkean turvallisuuden TUVE -verkosta, unohtamatta kuntasektorin omia kunnallisia tietoverkkoja ja niissä sijaitsevia palveluita. Tavoite ei ollut, eikä ole, lainkaan vaatimaton, saati tuloksiltaan itsestään selvä. Myöskään lopullista vastausta siihen, tuleeko edellä kuvattu tavoitetila realisoitumaan, ei ole vielä saatavilla. Työ jatkuu toisten projektien muodossa ja voimin, mutta lienee turvallista väittää että tavoitetila on onnistuttu selkeästi määrittelemään ja useita esteitä tieltä on saatu raivattua.

Raportissa on poikettu parista tavanomaisesta tavasta, eli lyhenneluettelo on jätetty pois ja lyhenteet on pyritty esittämään pitkässä muodossaan silloin kun sellainen ensimmäistä kertaa esiintyy tai edellinen esiintymä on siinä määrin etäällä, että lukijan voi olettaa sen unohtaneen. Tällä on pyritty poistamaan lukemista haittaava tarve kaivella luetteloa esille lyhenteitä tulkittaessa. Toisena poikkeuksena lähdeluettelo on jätetty pois ja lähteisiin viitataan samalla tavoin esittäen lähde siinä kohdassa jossa siihen viitataan. Perusteluna tälle käytännölle on internet lähteiden varsin suuri määrä ja raportin luonne enemmän tuotekehitykseen kuin perustutkimukseen liittyvänä.

MoniKa hanke

MoniKa hanke alkoi 1.11.2011 ja päättyi 30.6.2013. Hankkeen rahoitus tuli pääosin Palosuojelurahastolta. Hankkeen toteuttamisesta vastasi Pelastusopiston tutkimusyksikkö. Hankkeen toteutukseen osallistuivat myös pelastuslaitosten verkosto ja Erillisverkot Oy. Hankkeessa toimi yksi tutkija miltei päätoimisesti, sekä pelastusopiston tutkimusyksikön muuta henkilökuntaa tarpeen mukaan.

Hankkeen lähtötilanteen kuvaus

MoniKa projektia ei käynnistetty nollatasolta, vaan sitä edeltäneet projektit, kuten PELTI (Pelastustoimen langaton tiedonsiirto tulevaisuudessa) olivat luoneet hankkeen pohjan ja hahmottaneet tarpeen. Projektin alkuvaiheen henkilöstömuutokset toivat oman akklimatisoitumisvaiheensa ja vaatimatonta alkukiihdytystä parannettiin hyvällä loppukirillä.

Hankkeessa tehtiin paljon yhteistyötä mm. Laurea AMK:n MOBI projektin kanssa, varsinkin reititinlaitteiden kenttätestien osalta. Projektien synergiaetu oli selkeä ja yhteistyö tuki selvästi molempia projekteja. MOBI projektin eteneminen ja sen aikainen yhteistyö toi uusia näkökantoja jotka varmasti näkyvät myös MoniKa projektin lopputuloksessa.

TOTI projektin työ ERICA järjestelmän toteutuksessa oli hyvässä vauhdissa projektin käynnistyessä ja MoniKa pyrki aktiivisesti pitämään yllä tietoisuutta ERICAn etenemisestä.

KEJO projektin suunnittelu oli myös jo verraten pitkällä MoniKan käynnistyessä ja hyvin aikaisessa vaiheessa KEJO nähtiin yhdeksi tärkeimmistä varmennetun laajakaistan avulla tarjottavista palveluista. Projekti tekikin tiivistä yhteistyötä pelastustoimea KEJO hankkeessa edustavien henkilöiden kanssa, etenkin tietoturva-asioiden osalta.

MoniKa hankkeen rahoitti suurelta osin Palosuojelurahasto. Hankkeessa oli yksi tutkija lähestulkoon täysipäiväisesti (n 20 % työajasta toiselle hankkeelle). Hanke päättyi kesäkuun 2013 lopussa.

Hankkeen tavoitteet

Hankkeen tavoitteet oli määritelty projektisuunnitelmassa seuraavasti:

• Määritellä monikanavaisuuden toteuttamisen vaatimukset pelastusajoneuvossa, ottaen huomioon eri palveluiden tarpeet esim. tietoturvan osalta. Tuotetut vaatimukset voidaan huomioida myös muissa hankkeissa.

• Analysoida ja evaluoida markkinoilla olevat MKR-ratkaisut (MKR = monikanavareititys)

• Määritellä ja tuotteistaa sellainen MKR-palvelu, jonka käyttöönotto on helppoa ja jota kaikki pelastuslaitokset/viranomaiset voivat käyttää.

• Valita muutama potentiaalinen MKR-ratkaisu, jotka parhaiten täyttävät viranomaisvaatimukset. Selvitetään MKR-toimittajien kyky tehdä räätälöintejä mahdollisia erityistarpeita (salaukset, verkkotuet) varten. Selvitetään toimittajien toimitus- ja ylläpitokyky. Lisäksi mahdollisesti tuotetaan kilpailutusdokumentaatio sekä kilpailutetaan MKR-ratkaisu.

• Rakentaa ja testata (niiltä osin kun sitä pystytään tekemään) pilottitoteutus valitun MKR-ratkaisun pohjalta pelastusajoneuvoon.

Näistä tavoitteista projektissa jouduttiin tinkimään lähinnä viranomaisten yhteiskäyttöisyydestä. Nykyisellä verkkoteknologialla on verraten haasteellista toteuttaa verkko johon ennalta määrittelemätön viranomainen voisi liittyä ja joka samalla tuottaa tietoturvan osalta riittävän tason viranomaisten yhteisten järjestelmien tarpeisiin. WiFi 2.0 yleistyessään tuo mukanaan työkaluja (varmennepohjainen autentikaatio) tällaisen ad-hoc autentikointia vaativan ratkaisun tuottamiseen, mutta riittävää markkinapenetraatiota laitteiden osalta jouduttaneen odottamaan vielä jonkin aikaa.

Toimintaympäristö

MoniKa hankkeen käytännön suunnitteluun ja toteutukseen vaikuttivat useat käynnissä olevat ja hankkeen aikana käynnistyneet pelastustoimea koskevat IT hankkeet, sekä jo olemassa oleva infrastruktuuri. Tässä kappaleessa käsitellään näitä hankkeita ja ympäristöä hyvin tiivistetyssä muodossa. Kaikista näistä hankkeista ja ympäristöistä löytyy kattavia esityksiä joita ei ole nähty järkeväksi toistaa tässä raportissa vaan lähinnä tuoda esiin niitä erityispiirteitä jotka vaikuttavat langattoman laajakaistan määrittelyyn.

PEIP

Pelastustoimen IP verkko (PEIP) on Erillisverkot Oy:n pelastuslaitoksille tuottama palvelu, joka on toteutettu olemassa olevalla verkkoinfrastruktuurilla MPLS (Multiprotocol Label Switching) verkkona. Verkko yhdistää pelastuslaitokset ja mahdollistaa pelastuslaitosten yhteisten palveluiden tuottamisen keskitetyssä, pelastustoimen hallinnoimassa verkkoympäristössä. PEIP verkkoa kehitetään edelleen pelastuslaitosten tietoliikenneverkkoprojektissa tavoitteena mm. yhteisten tietoverkkopalvelujen (mm- pääsynhallinta ja videoneuvottelu) tuotteistaminen.

VARANTO

MoniKa hankkeen kanssa samanaikaisesti käynnissä olleessa Prontox hankkeessa tutkittiin nykyisen Pronto tietojärjestelmän nykytilaa ja tulevaisuutta. Pronto järjestelmän nähtiin olevan elinkaarensa loppupuolella ja sille mietittiin korvaavia järjestelmiä. Pelastustoimen tietojärjestelmien nykyinen pirstaleisuus ei tue tiedon täysimittaista hyödyntämistä ja vaihtoehtona nähtiin rakentaa järjestelmä joka tuottaisi tiedon tallentamiseen tarvittavan alustan sekä tiedon käsittelyn perusrutiinit. Näin syntyi ajatus pelastustoimen tietovarannosta. Tavoitteena oli aikaansaada järjestelmä jossa erinäisissä pelastustoimen toiminnoissa syntyvä tieto tuodaan yhteen tietovarantoon ja tiedon saatavuus sekä tietoalkioiden yhdistämisestä syntyvä synergia saadaan uudelle tasolle. MoniKa hanke oli mukana VARANTO hankkeen suunnittelussa sen alkuhetkistä lähtien ja hankkeissa on lähtökohtaisesti pidetty huoli siitä että MoniKa konsepti mahdollistaa tulevien VARANTO palveluiden täysimittaisen hyödyntämisen.

VARANTO käynnistyi hankkeena 2013 kolmen täysipäiväisen tutkijan voimin. MoniKa hankkeen päättyessä yllä mainittu yhteistyö jatkuu edelleen tiiviinä.

ERICA

Uudeksi hätäkeskustietojärjestelmäksi hätäkeskuslaitoksen sivuilla kuvattu ERICA tullee muuttamaan myös pelastustoimen useita prosesseja. Lyhenne tulee sanoista E = Emergency, R = Response, I = Integrated, C = Common, A = Authorities, mikä viestii kyseessä olevan viranomaisten yhteinen tietojärjestelmä. (http://www.112.fi/hatakeskusuudistus/uusi_tietojarjestelma)

Näillä näkymin ERICA palveluja on harvoin tarve käyttää kentältä, langattoman laajakaistayhteyden läpi. ERICA käyttö keskittyy lähinnä pelastuslaitosten tilannekeskuksiin ja toimistokäyttöön. Näin ollen MoniKa hankkeessa laajakaistan käyttötapauksissa on lähinnä keskitytty KEJOon.

KEJO

KEJO hanke oli jo käynnissä MoniKan käynnistyessä. KEJO hankkeessa määritellään ja toteutetaan turvallisuusviranomaisten yhteinen kenttäjohtamisjärjestelmä. Pelastustoimessa käytössä oleva PEKE (Pelastustoimen kenttäjohtamisjärjestelmä) tullee korvautumaan KEJOlla aikanaan.

KEJO ja sen saaminen pelastustoimen käyttöön voidaan nähdä hyvin tärkeänä, jollei tärkeimpänä pelastustoimen IT hankkeena tällä hetkellä. Tällä on ollut selkeä vaikutus MoniKa hankkeen toimintaan, koska hankkeessa on pyritty kaikin tavoin varmistamaan, että tulevasta laajakaistaratkaisusta syntyy sellainen että se mahdollistaa KEJOn käytön pelastustoimessa. Tästä johtuen hankkeessa KEJOn käyttöön liittyvät verkkotekniset ja etenkin tietoturva-asiat ovat nousseet keskiöön. MoniKa hankkeen tutkija onkin toiminut tietoturvan asiantuntijana KEJOn tietoturvatyöpajoissa. KEJO palvelu tullaan ilmeisesti tuottamaan TUVE verkossa (kts. alla), joten projektissa on lähdetty tietotuvan osalta liikenteeseen siitä, että tuotettu palvelu pystyisi liittymään TUVEen ja hyödyntämään siellä olevia palveluja.

TUVE

TUVE (Valtion Turvallisuusverkkohanke) tuottaa korkean turvallisuustason tietoverkon jota tulee operoimaan Suomen Turvallisuusverkko OY (Erillisverkot Oy:n tytäryhtiö). Valtiovarainministeriön sivuilta löytyy yleiskuvaus hankkeesta:

Hallinnon turvallisuusverkkohankkeessa (TUVE) suunnitellaan ja toteutetaan valtion ylimmälle johdolle ja yli 30 000 turvallisuusviranomaiskäyttäjälle oma korkean varautumisen tietoverkko tarvittavine palveluineen. Verkon käyttäjiksi tulevat valtion ylimmän johdon ja ministeriöiden lisäksi valtion yleisen järjestyksen ja turvallisuuden, pelastustoiminnan, meripelastustoiminnan, rajaturvallisuuden, hätäkeskustoiminnan, maahanmuuton, ensihoitopalvelun sekä maanpuolustuksen kannalta keskeiset viranomaiset. (http://www.vm.fi/vm/fi/05_hankkeet/024_tuve/index.jsp)

TUVE verkkoa varten on valmisteltu omaa lakiaan, ja hallituksen esitys laista on löydettävissä mm. eduskunnan sivuilta *"Hallituksen esitys eduskunnalle laeiksi julkisen hallinnon turvallisuusverkkotoiminnasta ja viestintämarkkinalain 2 §:n muuttamisesta"*. (http://217.71.145.20/TRIPviewer/show.asp?tunniste=HE+54/2013&base=erhe&palvelin=www.eduskunta.fi&f=WORD)

Mitä ilmeiseimmin ERICAn ja KEJOn tuotantoympäristöt tulevat sijaitsemaan TUVEn sisällä ja liikennöinti näihin palveluihin on mahdollista vain TUVEn kautta. Tämä on pyritty huomioimaan MoniKa hankkeessa alusta lähtien.

Pelastustoimen tarvitsemat palvelut ja niiden saatavuus

Yhtenä hankkeen tavoitteena oli kartoittaa pelastustoimessa käytetyt tietotekniset palvelut ja arvioida palveluiden kriittisyyttä ja tietoliikennetarpeita. Lähtökohtana selvitystyölle oli tavoite pystyä priorisoimaan sovelluksia ja käyttäjiä tietoliikennekaistan ollessa rajallinen.

Kartoitetuista järjestelmistä selvitettiin seuraavat tiedot:

1. Kuvaus järjestelmästä
2. Tuotantopaikka, eli missä palvelu tuotetaan
3. Tuot. paikka 2 (mikäli edellistä voidaan tarkentaa)
4. Reititys tulevaisuudessa, eli miten palveluun päästään tulevaisuudessa
5. Käyttöliittymä (nyt)
6. Käyttöliittymä 2 (nyt) (mikäli edelliseen on vaihtoehto)
7. Käyttöliittymä tulevaisuudessa
8. Operatiivinen luokittelu (kiireellinen pelastustoiminta, kiireetön, hallinnollinen/toimistokäyttö)
9. Kuka omistaa palvelun
10. Lisätietoja

Lista tunnistetuista palveluista on liitteessä 1. Palveluiden kriittisyysluokitus on luonnollisesti subjektiivinen "makuasia" ainakin osan palveluista suhteen. Liitteeseen listattujen palveluiden osalta saatiin kohtuullisen hyvä konsensus aikaan sen suhteen mitä pidettiin kiireellisenä / kiireettömänä pelastustoiminnan palveluna. Palveluiden priorisoinnin perusteella voidaan verkon kaistaa priorisoida reititintasolla sekä myös työasematasolla. Priorisointeja tarkennetaan VOTI projektissa, jossa työaseman vakioinnin yhteydessä selvitetään työasematason priorisointimahdollisuudet. Hankkeen aikana tutkittiin myös roolipohjaiseen käyttäjänhallintaan perustuvaa mahdollisuutta priorisoida tiedonsiirtokapasiteettia käyttäjäkohtaisesti. Tällainen rooliperustainen priorisointiratkaisu, samoin kuin kriittisten palveluiden priorisointi, on helpointa toteuttaa reitittimen ja työaseman yhteisenä tehtävänä. Priorisoinnin toteutusta jatketaan työasemavakioinnin yhteydessä. Saarekekäytössä eri rooleilla tunnistautuneiden käyttäjien priorisointi reitittimeen vaatii myös työaseman "älykkyyttä" ja yhteensopivuus mm. TUVE ratkaisujen kanssa tulee tutkia tarkkaan.

TUVE verkossa tuotettujen palvelujen saatavuus

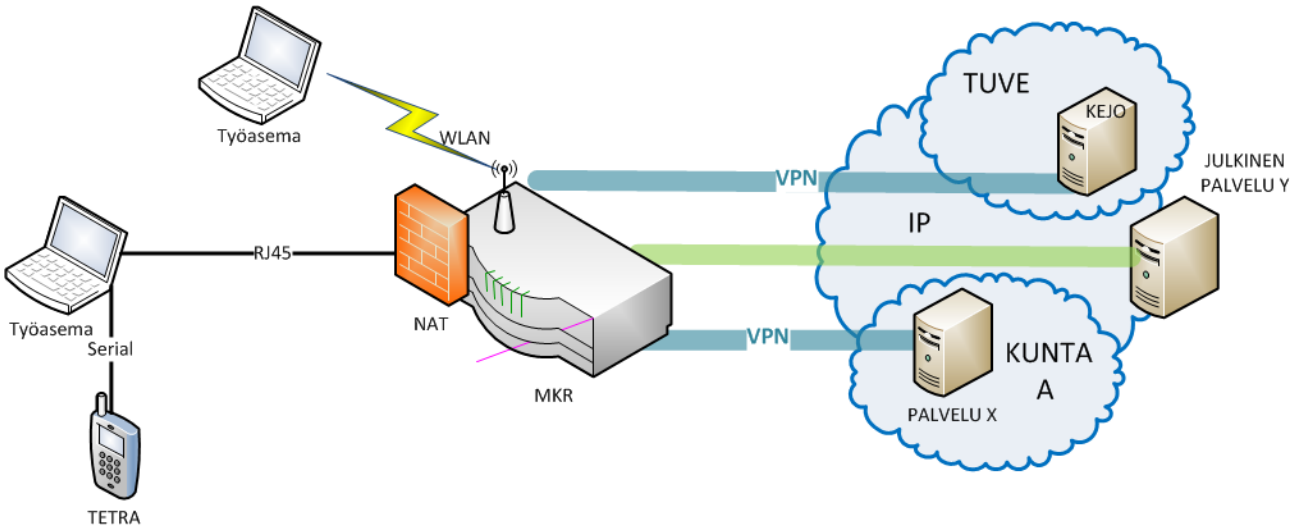
Yksi tulevaisuuden tärkeimmistä palveluiden tuotantopaikoista pelastustoimen osalta on valtion turvallisuusverkko, TUVE. Liikennöinti turvallisuusverkkoon on pääsääntöisesti sallittu vain luotetuista verkoista. Eräs tietoturvaan liittyvä vaatimus poimintana "Tietojärjestelmän tietoliikenne ei-luotettuihin verkkoihin tulee olla salattuna NCSA-FI hyväksymillä salausprotokollilla". Tämä viitannee siihen että on olemassa luotettuja ja ei-luotettuja verkkoja. Lienee turvallista veikata että kaupallisten mobiilioperaattoreiden avoimet verkot ovat lähtökohtaisesti ei-luotettuja.

Tällä hetkellä kaikilla pelastuslaitoksilla on jonkinlaisia mobiilidatayhteyksiä kentältä julkiseen internetiin ja monilla on VPN yhteyksiä mm. isäntäorganisaatioiden intranet verkkoihin. Lienee ylivoimaisen haasteellista tuottaa 22 "luotettua verkkoa" tai saattaa kaupallinen avoin operaattoriverkko "luotettu" tilaan, joten MoniKa hankkeen lähtökohtana oli tukeutua yhteen olemassa olevaan verkkoon, eli pelastustoimen IP verkkoon (PEIP).

PEIP tarvitsee kuitenkin vielä työtä voidakseen täyttää TUVEssa vaaditun luotetun verkon kriteerit. Samalla PEIP verkkoon liitettävät päätelaitteet ja niiden tietoturvaympäristöt täytyy saattaa sellaiselle tasolle että luotetun verkon kriteerit voivat täyttyä. Luonnollista on että tässä vaiheessa ei enää voi olla pelastuslaitoskohtaisia tietojenkäsittely-ympäristöjä, vaan pelastustoimelle täytyy luoda koko maan kattava tietoturvaympäristö ja päätelaitteet täytyy vakioida yhteiseen kaavaan koko maan osalta. Pelastusopistolla on käynnissä kaksi hanketta jotka tähtäävät näihin tavoitteisiin. Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka (TUPO) hanke tuottaa nimensä mukaisesti tietoturvapolitiikan jota kaikki maan pelastuslaitokset voivat käyttää operatiivisten tietojärjestelmiensä osalta. Vakioitu operatiivinen työasemainfrastruktuuri (VOTI) puolestaan luo mainitun vakioinnin ja vie TUPOssa määritellyt tietoturvakäytänteet käytännön toteutukseksi. Hankkeessa on vahva usko siihen että näiden tulosten myötä PEIP voidaan auditoida luotetuksi verkoksi.

Palvelujen saatavuus kuntien verkoista ja internetistä

Yhtenä hankkeen lähtökohtana on ollut tutkia reititinlaitteiden toiminnallisuutta ja mukautumiskykyä. Ilmeisesti nykyiset TUVE verkkoon kytkeytyvät MKR ratkaisut reitittävät kaiken liikenteen TUVEn kautta. Tällaisessa menettelyssä julkisen internetin pavelujen "kierrätys" VPN:n kautta vaikuttaa pelastustoimessa tarpeettomalta. Samaten pelastustoimen isäntäorganisaatioiden intranet palvelut, joihin nykyisellään yleensä kytkeydytään myös VPN yhteydellä, voidaan varmaan reitittää palvelimelta suoraan isäntäorganisaation verkkoon. Kunnallisen organisaation omaan intraan kytkeytyvien palvelujen kytkeminen reitittimen VPN yhteyden kautta tarkoittaisi sitä, että reitittimen tulee kyetä rakentamaan useita suojattuja yhteyksiä eri kohteisiin ja reitittämään liikenne niihin oikein. Vaihtoehtona on VPN jonka sisään rakennetaan toinen VPN ja tämä kuulostaa hitaalta, vikaherkältä ja hallinnolisestikin monimutkaiselta.



Kuva 1 Palveluiden saatavuus monikanavareitityksessä

Tietoturvaan liittyvät kysymykset

MoniKa hankkeen yhdeksi tärkeimmistä työtehtävistä nousi aikaisessa vaiheessa pelastustoimen tietojärjestelmiin ja -verkkoihin liittyvien tietoturvakokonaisuuksien tutkiminen ja tietoturva-arkkitehtuurin hahmottelu reititysjärjestelmän osalta. Hankkeessa tutkittiin varsin kattavasti pelastustoimen järjestelmiin liittyvää tietoturvalainsäädäntöä, ohjeistuksia (mm. VAHTI ohjeet ja KATAKRI) sekä käytössä olevia menetelmiä. Kattava lainsäädännöllinen katsaus liitettiin Prontox hankkeen kanssa yhteistyössä tehtyyn VARANTO tietoturvaselvitykseen, joten sen toistaminen tässä raportissa ei ole tarpeen. Tietoturvaselvitys (VARANTO & TIETOTURVA - VARANTO-hankkeen tietoturvaselvitys) löytyy pelastusopiston www-sivulta, kirjaston julkaisusarjasta. (http://www.pelastusopisto.fi/fi/tutkimus-_ja_tietopalvelut/kirjasto-_ja_tietopalvelut/julkaisut/julkaisusarjat/d_muut_julkaisut)

Tietoturvaan liittyvät ohjeet ja määräykset kuitenkin määrittivät varsin selkeästi monikanavareitityksen verkkoarkkitehtuurin lähtökohdat. Kuten edellisessä kappaleessa selvisi, on olemassa luotettuja ja ei-luotettuja verkkoja. Monikanavareitityksen olisi näin ollen hyvä liittyä verkkoon, joka lasketaan luotettujen verkkojen joukkoon. Pelastustoimen oma PEIP verkko on hyvä kandidaatti tällaiseksi luotetuksi verkoksi, mikä on myös kuvattuna seuraavan kappaleen kuvassa.

Tietoturvamenettelyjen suunnittelun lähtökohtana voidaan pitää lakia viranomaisten toiminnan julkisuudesta (JulkL 21.5.1999/621). Lainsäädännön lähtökohtana on, että tieto jonka salassa pitämiseen ei ole laissa säädettyä perustetta, on julkisesti saatavissa. Näillä lähtökohdilla suunniteltiin pelastustoiminnan tietojärjestelmän tietoturva-arkkitehtuuri, joka julkaistiin kv. referoidussa konferenssissa nimellä Data Security Design as a Cooperation Facilitator: Data Security Architecture for Information Systems of Safety and Security Organisations (http://sdiwc.net/digital-library/data-security-design-as-a-cooperation-facilitator.html)

Monikanavareitityksen asemoituminen pelastustoimen IT infraan

Hyvin aikaisessa vaiheessa MoniKa hanketta syntyi hahmotelma (kuva 2), jossa pyrittiin jäsentämään pelastustoimessa käytettävien sovellusten, verkkojen ja toimijoiden suhteita. Keskiössä oli jäsentää ratkaisu jolla kaikki olennaiset palvelut olisivat käytettävissä kentällä, pelastustoiminnassa. Kuvaan oli kirjoitettu myös sanallinen selitys, joka tässä on sellaisenaan (ERICA nimi on lisätty myöhemmin, tietojärjestelmän nimi ei silloin vielä ollut tiedossa).

Kaavio ei noudata mitään standardia tai yleisesti käytössä olevaa notaatiota jonka vuoksi sanallinen selitys kaaviossa olevien asioiden suhteen on paikallaan. Kaavio itsessään jättää liiaksi tulkinnan varaa ilman sanallista selitystä.

Oletuksia: Kaavion piirtämisessä on tehty joukko oletuksia jotka ovat:

• ERICA (= Tuleva hätäkeskustietojärjestelmä) tulee sijaitsemaan valtion Turvallisuusverkossa (TUVE).

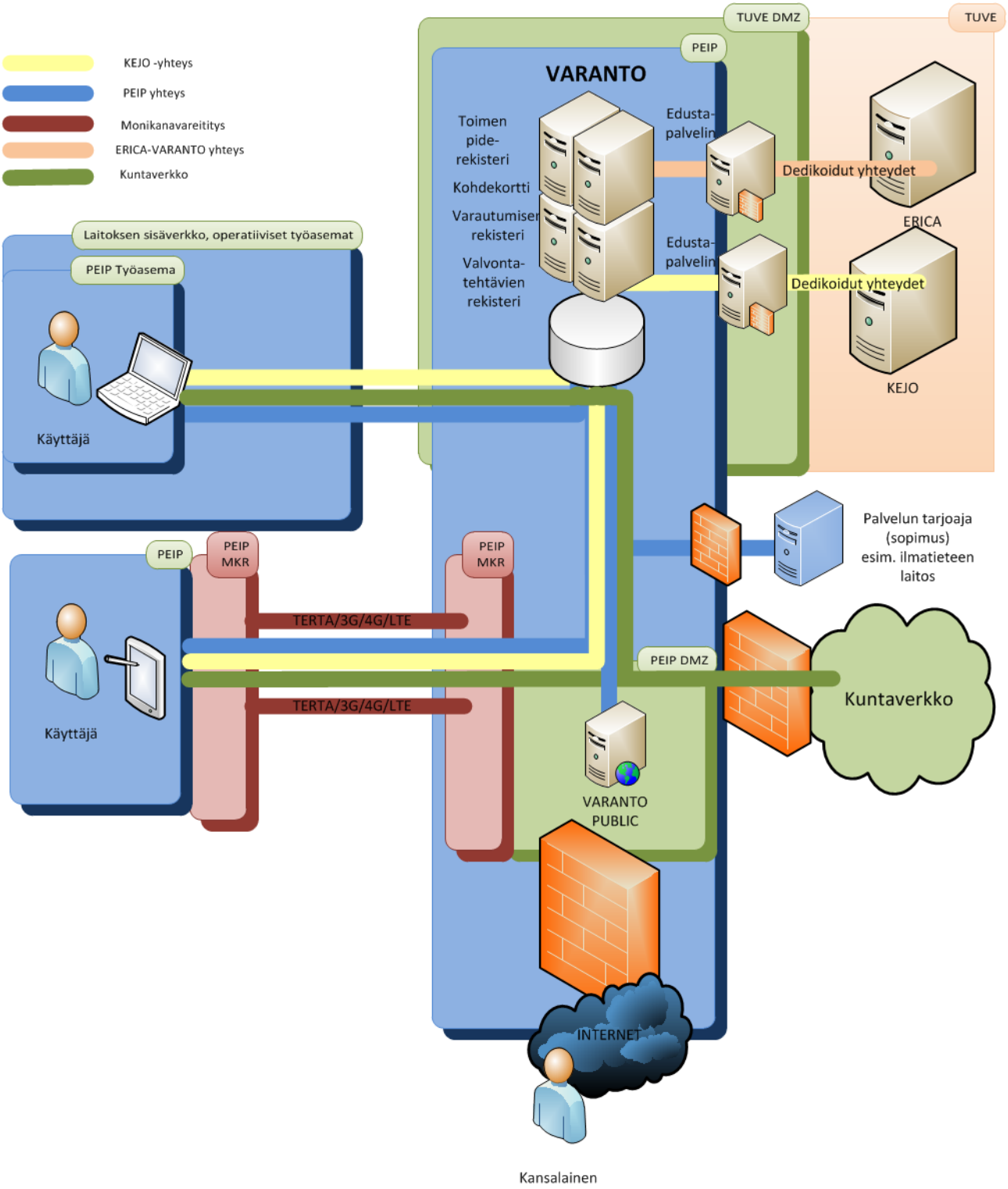
• KEJO (=Tuleva kenttäjohtamisjärjestelmä) tulee sijaitsemaan valtion Turvallisuusverkossa (TUVE).

• TUVEssa on demilitarisoitu vyöhyke, DMZ, jossa voi sijaita palveluita ja järjestelmiä joita ei katsota tarpeelliseksi / haluta sijoittaa TUVEn sisälle.

Lähtökohtia:

• PEIP on pelastustoimen jo käytössä oleva IP-verkko johon voidaan sijoittaa järjestelmiä ja palveluita, jotka ovat perustietoturvatasolla. PEIPiin voidaan rakentaa vaativampia tietoturvamekanismeja esimerkiksi sovellustasolle. Kuvassa sininen kuvaa PEIP verkkoa

• VARANTO on tulevaisuuden tietojärjestelmäkokonaisuus johon on kootusti rakennettu pelastustoimessa tarvittavia tietojärjestelmiä palveleva tietovaranto. Tietovaranto on kaikkien aluelaitosten ja alan toimijoiden käytössä myöhemmin tarkemmin määritetyin kriteerein. VARANTO tulee pitämään sisällään nykyiset, kuvassa luetellut rekisterit sekä soveltuvin osin niiden käsittelemiseen tarvittavat palvelut.



Kuva 2 Monikanavareitityksen asemoituminen pelastustoimen IT infrastruktuuriin

• PEIP MKR on pelastustoimen monikanavareititin joka tuottaa laadukkaan tietoliikenneyhteyden liikkuvaan operatiiviseen toimintaan. MKR liittyy olennaisesti PEIP verkkoon jonka kautta mm. VARANTO -palvelut ovat käytettävissä. PEIP verkkoa ja siihen liitettyä MKR ratkaisua tuottaa Erillisverkot. Vastaavalla monikanavareitityksellä tuotetaan sama palvelu muille viranomaisille muun kuin PEIP verkon kautta.

• Loppukäyttäjän tarvitsemien palveluiden tuotantopaikkaa (esim. TUVE, VY, PEIP, kuntaverkko, julkinen internet) ei haluta rajoittaa.

Piirroksessa:

• VARANTO on hyvä sijoittaa TUVEn demilitarisoituun vyöhykkeeseen. VARANNOSSA olevien rekisterien ja palveluiden on tarve pystyä vaihtamaa tietoa ERICAn kanssa. Samoin KEJO tarvinnee VARANNOSSA olevia tietoja ja palveluita.

• Samalla varantoon on saumaton turvallinen yhteys PEIPistä jolloin palvelut ovat helposti PEIP-käyttäjien (=pelastustoimi) saatavilla.

• VARANTO-ERICA yhteys voidaan rakentaa keskitetysti turvalliseksi kontrolloidun, tarkasti rajatun rajapintayhteyden (kuvassa "dedikoidut yhteydet") kautta. Tarvittaessa käytetään erillistä edustapalvelinta liikenteen kontrollointiin.

• Vastaavasti KEJO voidaan tuoda turvallisen tunnelin kautta (Kuvassa keltainen yhteys) pelastustoimen loppukäyttäjälle PEIPin sisällä PEIP työasemaan ja mobiilikäyttäjän PEIP päätelaitteeseen monikanavareitittimen kautta (Kuvassa PEIP MKR).

• PEIP verkossa on oma demilitarisoitu vyöhyke (DMZ) jonka kautta mobiilikäyttäjä pääsee julkiseen internetiin.

• PEIP DMZ vyöhykkeessä voi sijaita esim. VARANTOon liittyviä, julkisia, kansalaisille tarkoitettuja palveluita kuten pelastustoimen informaatiopalvelut tai kansalaisen omistamaan kiinteistöön liittyvän palotarkastustiedon (omavalvonta) kirjaaminen.

• Tiettyihin, kotimaassa tuotettuihin pelastustoimen käyttämiin palveluihin (kuten LUOVA tms) voidaan rakentaa suora PEIP yhteys joka takaa palvelun saatavuuden eikä ole julkisen internetin saatavuudesta riippuvainen (Kuvassa vaalean sininen palvelin)

• Kunnallisiin sisäverkkoihin (intranet) sijoittuvat palvelut voivat olla käytössä joko DMZ:n (julkinen internet) kautta tai PEIP liittymän kautta. Nämä palvelut harvoin ovat operatiivisen toiminnan palveluita.

• Julkisen internetin ja PEIP DMZ:n välillä on palomuurijärjestelmä ja IPS (Intrusion Prevention System) hyökkäyksen esto.

Jälkikommenttina reilua vuotta viisaampana voidaan todeta seuraavaa:

Kuvan yksityiskohdat ovat jossain määrin kehittyneet ja toimintoihin liittyvät yksityiskohdat selkeytyneet, mutta alkuperäisen kuvan perusajatus on edelleenkin voimissaan.

Reititinvalmistajat

Yhtenä hankkeen tavoitteista oli arvioida markkinoilla olevat monikanavareititysratkaisut. Periaatteessa monikanavareitittimen voi rakentaa kohtuullisin tietoteknisin ja ohjelmointivalmiuksin hyvin monenlaisista markkinoilla olevista reitittimistä. Useissa edullisissa ns. bulkkireitittimissä on sisällään Linux -pohjainen käyttöjärjestelmä, jonka muokkaaminen tukemaan monikanavaisuutta ei ole kovin monimutkaista. Eri asia on sitten se, mitä monikanavaisuudella halutaan ymmärtää. Käytännössä kaikissa evaluoiduissa ratkaisuissa useammasta käytettävissä olevasta tiedonsiirtoväylästä käytetään kerrallaan vain yhtä. Tämä kappale luo katsauksen arvioituihin toimittajayrityksiin. Samalla tarkastellaan tuotteiden teknisiä ominaisuuksia verraten korkealla tasolla ja niihin liittyviä hallintajärjestelmiä. Lähteinä on käytetty yrityksen omia www sivuja sekä niiltä löytyviä teknisiä dokumentteja, Fonectan Finder sivustoa (yritysten perustiedot ja taloustiedot) sekä yrityksissä vierailujen aikana tehtyjä muistiinpanoja. Tässä esitetyt tiedot laitteistoista ja niiden käyttöjärjestelmistä ovat peräisin laitevalmistajilta.

Goodmill Systems

Goodmill Systems Oy on 2005 perustettu yritys, joka ilmoittaa päätoimialakseen IT-sovelluksia ja IT-ohjelmistoja. Yrityksen kotipaikka on Espoo. Yrityksestä löytyy seuraavat perustiedot: (www.finder.fi)

Toimipaikan henkilöstöluokka: 10-19 henkilöä

Yrityksen liikevaihtoluokka: 1-2 milj. euroa

Toimialaluokitus (TOL2008): Z62010 Ohjelmistojen suunnittelu ja valmistus

Goodmill Systems Oy	2008/12	2009/12	2010/12	2011/12	2012/12
Yrityksen liikevaihto (1000 EUR)	7	36	398	1789	1183
Liikevaihdon muutos%		400.00	1005.60	349.50	-33.90
Tilikauden tulos (1000 EUR)	-738	-796	-748	-37	-351
Liikevoitto%	-9535.90	-2125.00	-181.20	0.60	-19.40
Yrityksen henkilöstömäärä	N/A	9	N/A	10	10

Lähde: Suomen Asiakastieto

Goodmill Systems on erikoistunut ajoneuvojen laajakaistayhteyksiin pääasiallisina kohderyhminä poliisi, ensihoito ja pelastustoimi. Yhtiön tuotteita on myös mm. junissa ja apteekeissa (e-reseptijärjestelmän varayhteydet).

Laitteiston kuvaus

Goodmillin tuotevalikoimaan kuuluva w24e-R tukee WiFi, 3G HSPA, LTE, CDMA2000/450, WiMAX, Flash OFDM ja satelliittiyhteyksiä. Käyttökohteita on mm. junissa ja ajoneuvoissa. Laite toimii ajoneuvovirralla, joka on akkuvarmennettu. Näin laite pystyy toimimaan keskeytyksettä lyhyen virtakatkon ajan. Laitteet kootaan Suomessa komponenttien tullessa ulkomailta.

Laite on modulaarinen siten, että laitteessa käytettävät radiomodeemit ovat erillisiä, vaihdettavia piirikortteja. Näin teknologian muutokset eivät välttämättä aiheuta laitteen laajamittaista päivitystarvetta.

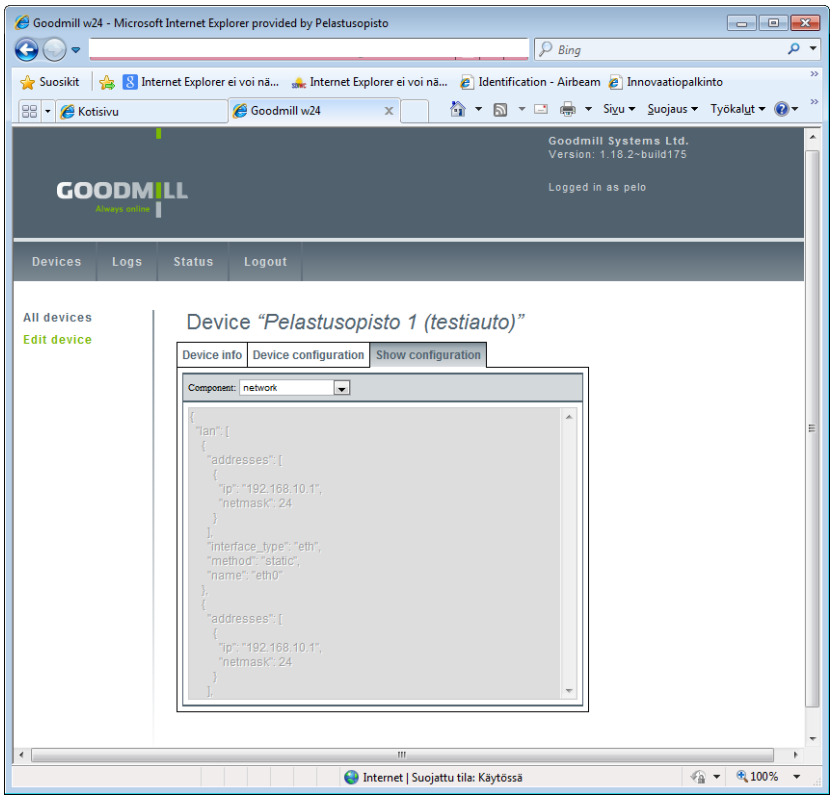
Antennien ja muiden johtojen liittimet laitteeseen ovat roiskeveden kestäviä, kuten itse laitekin. Laitteeseen kytkettyjen radiorajapintojen tilaa osoittaa led valot laitteen etupaneelissa (kuva 3).

Kuva 3 Goodmill Systems Oy:n reititin, malli w24e-R

Laitteessa voi olla esimerkiksi eri operaattoreiden 3G/4G yhteyksiä, joten laitteen liikkuessa se vaihtaa verkkoa jos parempi yhteys on tarjolla toisessa verkossa. Tällöin laitteen IP osoite luonnollisesti vaihtuu, mikä normaalisti aiheuttaisi ongelmia VPN yhteyksien kohdalla (yhteys katkeaa). Goodmill käyttää MIP (Mobile IP) tekniikkaa yhteyksien pysyvyyden hallinnassa. Näin ollen kaikki VPN yhteydet laitteesta kulkevat MIP palvelimen kautta.

Hallinnointi

Goodmillin laitteita voidaan hallinnoida www -käyttöliittymällä. Käyttöliittymässä laitteen asetusten tekeminen kuitenkin vaatii tarkkaavaisuutta ja perehtyneisyyttä. Muutokset tehdään tekstitiedostoihin joiden sisältöön täytyy perehtyä ennen kuin laitetta voi alkaa muokkaamaan. Asetusten tekemiseen on kuitenkin olemassa informatiivisia video-ohjeita (lisätietoja valmistajalta).



Kuva 4 Goodmill Systems Oy:n laitteiden hallinnointiympäristö

Ajeco

Ajeco Oy on 1984 perustettu yritys, joka ilmoittaa päätoimialakseen elektroniikkasuunnittelun. Yrityksen kotipaikka on Helsinki. Yrityksestä löytyy seuraavat perustiedot: (www.finder.fi)

Toimipaikan henkilöstöluokka: 5-9 henkilöä

Yrityksen liikevaihtoluokka: 0.4-1 milj. euroa

Toimialaluokitus (TOL2008): Z62010 Ohjelmistojen suunnittelu ja valmistus

Ajeco Oy	**2007/12**	**2008/12**	**2010/06**	**2011/06**	**2012/06**
Yrityksen liikevaihto (1000 EUR)	573	455	399	225	402
Liikevaihdon muutos%	36.40	-20.60	-41.60	-15.30	78.70
Tilikauden tulos (1000 EUR)	-95	-279	-14	-38	14
Liikevoitto%	-15.20	-58.50	2.40	-4.20	3.80
Yrityksen henkilöstömäärä	7	7	6	7	N/A

Lähde: Suomen Asiakastieto

Poimintoina yrityksen kotisivuilta:

" Ajecon henkilökunta koostuu elektroniikan ja ohjelmistosuunnittelun ammattilaisista. Erinomainen laatu ja hyvä palvelu ovat synnyttäneet myyntiä yli kahteenkymmeneen maahan. Työskentelemme tiiviisti yhdessä asiakkaittemme kanssa ja asiantuntemuksemme on arvostettua. Monet haastavat hankkeet ovat tuoneet laaja-alaista osaamista ja kokemusta yrityksellemme.

Ajecon tuotteita käytetään erilaisissa ohjaus- ja tiedonkeruujärjestelmissä muun muuassa sähkönjakeluverkkojen ohjauksessa, SCADA-järjestelmissä sekä

merialuevalvonnassa."

Kuva 5 Ajecon 4Com reititin testiautossa johtohässäkän seassa

(http://ajeco.fi/fi/yritys.html)

Ajecon reititintuote valmistetaan laitteistonkin osalta yrityksen omissa tiloissa Suomessa. Komponentit luonnollisesti ostetaan kolmannelta osapuolelta. Yrityksen referenssejä löytyy mm. sähköverkon valvonnasta ja hallinnasta sekä merialuevalvonnasta. Liikkuvien kohteiden referenssejä on Rajavartiolaitokselta ja Tampereen aluepelastuslaitokselta.

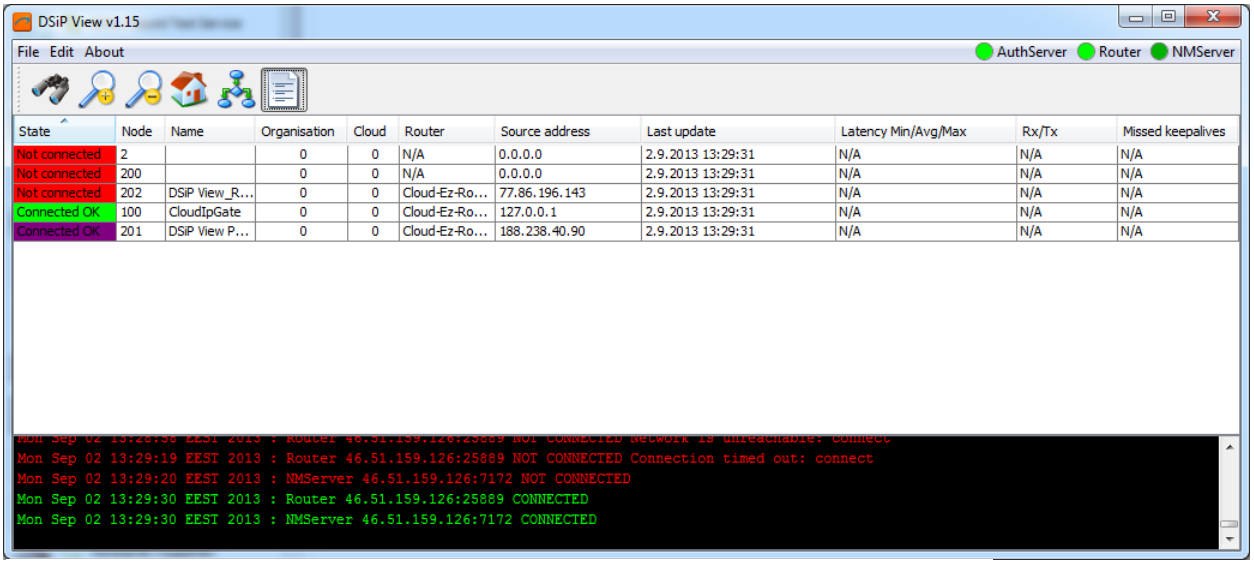
Laitteiston kuvaus

Ajecon erottaa muista monikanavareitittimiä tarjoavista yrityksistä DSiP tuoteperhe , joka on yrityksen itsensä rakentama tietoliikenneohjelmisto monikanavaiseen tiedonsiirtoon ja reititykseen. DSiP:n etuna voidaan nähdä hyvin monipuolinen muunneltavuus ja mukautuvuus eri käyttöjärjestelmiin ja alustoihin. *"DSiP on turvallinen tunneloiva monikanavainen protokolla, joka sallii yhteyden muodostamisen kahteen suuntaan, sallii L2 virtuaaliverkkojen ja muun liikenteen (esim. VPN) tunneloimisen itsensä kautta."* 4Com laitteeseen voidaan DSiP:n sijaan asentaa myös OpenWRT tai MIP. Käyttöjärjestelmänä 4Com laitteessa on Linux.

Laitteen 3G yhteyksien SIM kortit ovat laitteessa näkyvillä, joten kortin vaihtaminen onnistuu laitetta avaamatta. Ilmarajapintojen tilaa ilmaisevat ledit ovat myös laitteen etupaneelissa. Antenniliitynnät ovat SMA liittimin toteutettu. Testilaitteessa ei ollut akkuvarmennusta, vaan virtakatkoihin voidaan varautua superkondensaattoreilla ja on ajoneuvokäyttöön varsin suositeltavaa lyhyiden virtakatkojen aiheuttamia ongelmia vähentämään.

Hallinnointi

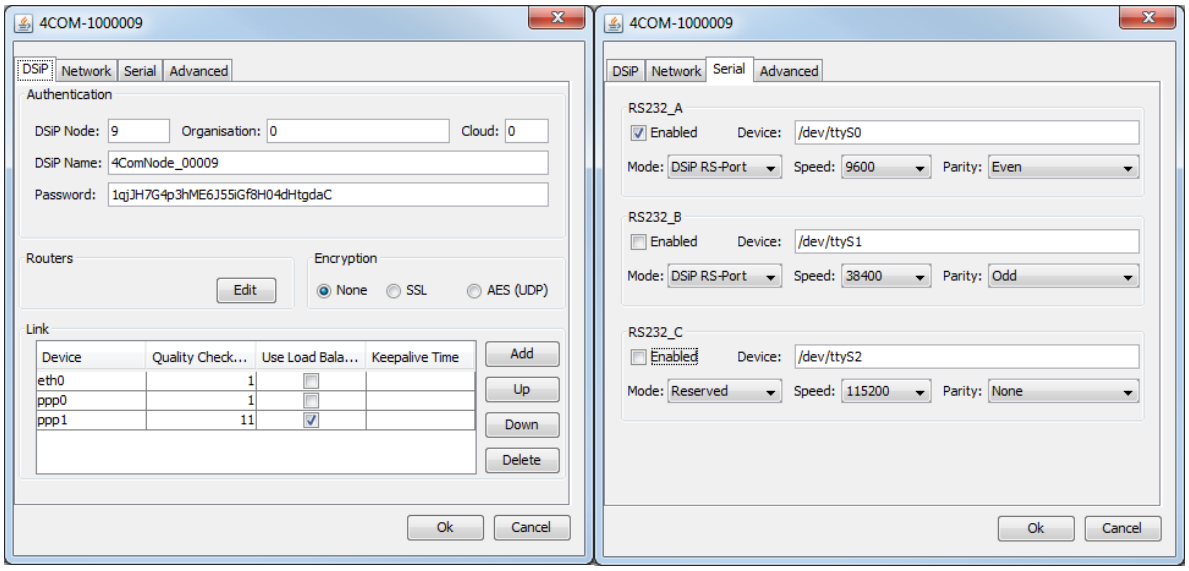
Laitteiden tilaa voi valvoa ja tarkastella DSIPView sovelluksella. Sovellus on javaohjelma (.jar paketti), jonka voi ajaa komentoriviltä esim: "C:\Users\p47826>"c:\Program Files (x86)\Java\jre6\bin\java.exe" -jar DSiPView_15.zip". Ohjelman mukaan tulee konfigurointitiedosto, jossa kerrotaan mm. mihin serveriin ja porttiin DSiPView ottaa yhteyttä. Itse käyttöliittymässä (kuva 6) näyttää DSiP verkon solmujen (node) tilaa.



Kuva 6 DSiPView sovelluksen näkymä (reitittimet offline)

Laitteen varsinainen hallinnointi tapahtuu SSH yhteyden avulla unix komentokehotteessa. SSH yhteyttä varten tarvitaan luonnollisesti käyttäjätunnus ja salasana. Konfigurointi tapahtuu unix -komennoilla ja tekstitiedostoja editoimalla. Raportin kirjoittajalle tämä edustaa ehkä kaikkein tutuinta tietojenkäsittely-ympäristöä, joten reitittimen käsittely tuntui kotoiselta. Asiaan kuitenkin vaikuttanee 90-luvun puolessa välissä alkanut yliopistoura kyseisen ympäristön piirissä. Unix komentoihin ja terminaaliyhteyksiin tottumattomalle oppimiskäyrä saattaa alussa olla jyrkähkö. Sovelluspohjainen käyttöliittymä (kuva 7) konfigurointiin on kuitenkin olemassa. Edellisen sukupolven 2Com laitteessa on web-käyttöliittymä laitteen konfigurointiin ja samanlainen on tekeillä myös 4Com laitteeseen. Pääsääntöisesti konfiguroinnit kuitenkin tehdään etänä konfiguraatiopalvelimen avulla.

DSiP:n kommunikaatiossa käytetään salaus- ja yhteydenmuodostamisessa vahvoja menetelmiä: AES256-GCM-SHA384, TLSv1.2, ja Diffie-Hellman. DSiP järjestelmä ja 4Com-laitteet ovat tietoturva-auditoituja (Louhi Security Oy).



Kuva 7 Ajecon laitteen hallinnointisovelluksen pari näyttöä

Indagon

Indagon Oy on 2002 perustettu yritys, joka ilmoittaa päätoimialakseen IT-sovelluksia ja IT-ohjelmistoja. Yrityksen kotipaikka on Helsinki. Yrityksestä löytyy seuraavat perustiedot: (www.finder.fi)

Toimipaikan henkilöstöluokka: 10-19 henkilöä

Yrityksen liikevaihtoluokka: 1-2 milj. euroa

Toimialaluokitus (TOL2008): Z62010 Ohjelmistojen suunnittelu ja valmistus

Indagon Oy	**2008/12**	**2009/12**	**2010/12**	**2011/12**	**2012/12**
Yrityksen liikevaihto (1000 EUR)	1463	1365	1398	939	1276
Liikevaihdon muutos%	69.60	-6.70	2.40	-32.80	35.80
Tilikauden tulos (1000 EUR)	427	154	-205	-119	63
Liikevoitto%	33.10	14.70	-12.70	-14.00	6.80
Yrityksen henkilöstömäärä	15	16	16	16	11

Lähde: Suomen Asiakastieto

Idagon tekee pääsääntöisesti paikannusjärjestelmiä päämarkkina-alueenaan lähi-itä. Kotimaassa Indagonilla on kokemusta paikannusjärjestelmien rakentamisesta TETRA verkkoon. Indagonin reititintuotteet syntyvät kustomoimalla kolmannelta osapuolelta ostettuja laitteistoja asiakkaan tarpeisiin. Poimintoina yrityksen kotisivuilta:

"Indagon Oy on kokenut ja innovatiivinen henkilöstön sekä Nokia OyJ:n omistama paikannusteknologian ja paikannuspalvelujen osaaja, joka kehittää, valmistaa sekä markkinoi tarkkoja ja luotettavia GPS-satelliittipaikannukseen pohjautuvia paikannusterminaaleja, -järjestelmiä ja -sovelluksia."

"Olemme mobiilin tiedonsiirron kokenut osaaja paikannuksessa, m2m-raportoinnissa ja kameravalvonnassa. Tunnemme radioteknologiat ja niihin liittyvät haasteet. Osaamme sovittaa tiedonsiirtoprotokollat taustajärjestelmiin. Rakennamme avoimin standardein käyttäjälle soveltuvia tiedonsiirron ja valvonnan käyttöliittymiä.

Olemassa olevat mobiilit tiedonsiirtoratkaisut käyttävät elinkaarensa lopussa olevaa GPRS tiedonsiirtoa, jonka tuki operaattoreilla on hiipumassa lähivuosina. Indagon on luonut 3G/LTE tiedonsiirtoratkaisun ja siihen liittyvät tukipalvelut vaativiin teollisuusolosuhteisiin.

Kokonaisratkaisumme erottuu kilpailevista toimijoista markkinoiden edistyneimmällä etähallintaratkaisulla ja sitä tukevilla elinkaaripalveluilla."

(http://www.indagon.fi/)

Kuva 8 Indagon Oy:n reititin

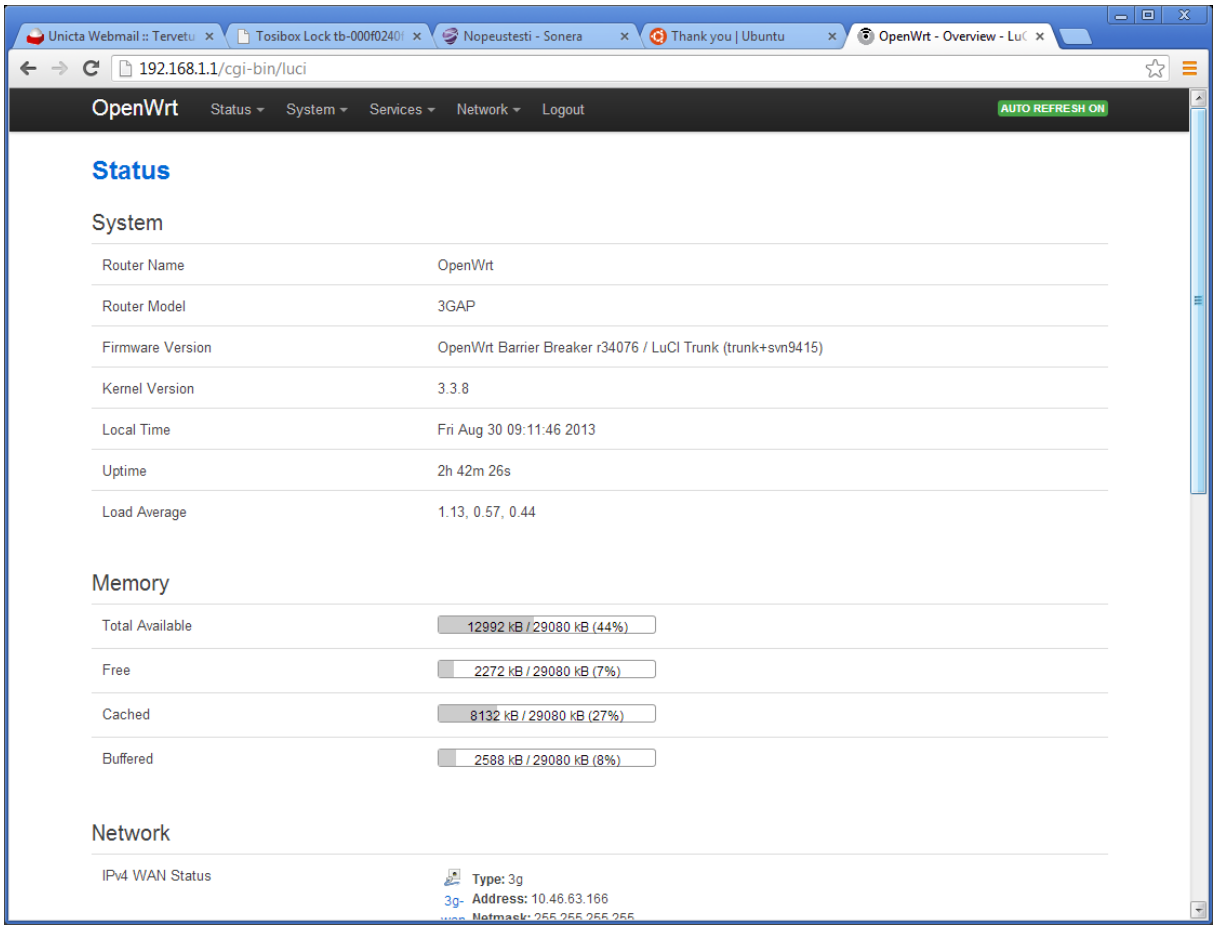
Laitteiston kuvaus

Indagon toimitti testejä varten laitteen joka räätälöitiin hankkeen testeihin soveltuvaksi. Laitteeseen oli paketoitu reititin 3G sekä @450 yhteys. Virran syöttö laitteelle oli 220 v vaihtovirta, joten kenttätesteissä käytettiin invertteriä laitteiston virran syötössä. Laitteistossa ei näin muodoin myöskään ole akkuvarmennusta. Antenniliitynnät 3G:n ja WiFin osalta ovat SMA liittimiä, @450 käyttää samanlaisia antenneja kuin Datame Oy:n @450 liittymien mukana toimittava AccessTel reititin (kuva 8).

Indagonin laitteisto perustuu vapaasti markkinoilta ostettavaan kolmannen osapuolen valmistamaan reitittimeen, jonka käyttöjärjestelmä on Linux pohjainen (Open WRT). Laitteiston ohjelmistoa voidaan räätälöidä asiakkaan tarpeisiin. Open WRT tarjoaa perehtyneelle käyttäjälle koko joukon mahdollisuuksia tehdä laitteestaan itselle sopiva. Sinällään tämä lähestymistapa on edullinen (ns. bulkkirauta) ja antaa vapauden valita laitetoimittaja. Open WRT tarjoaa myös VPN toiminnallisuuden.

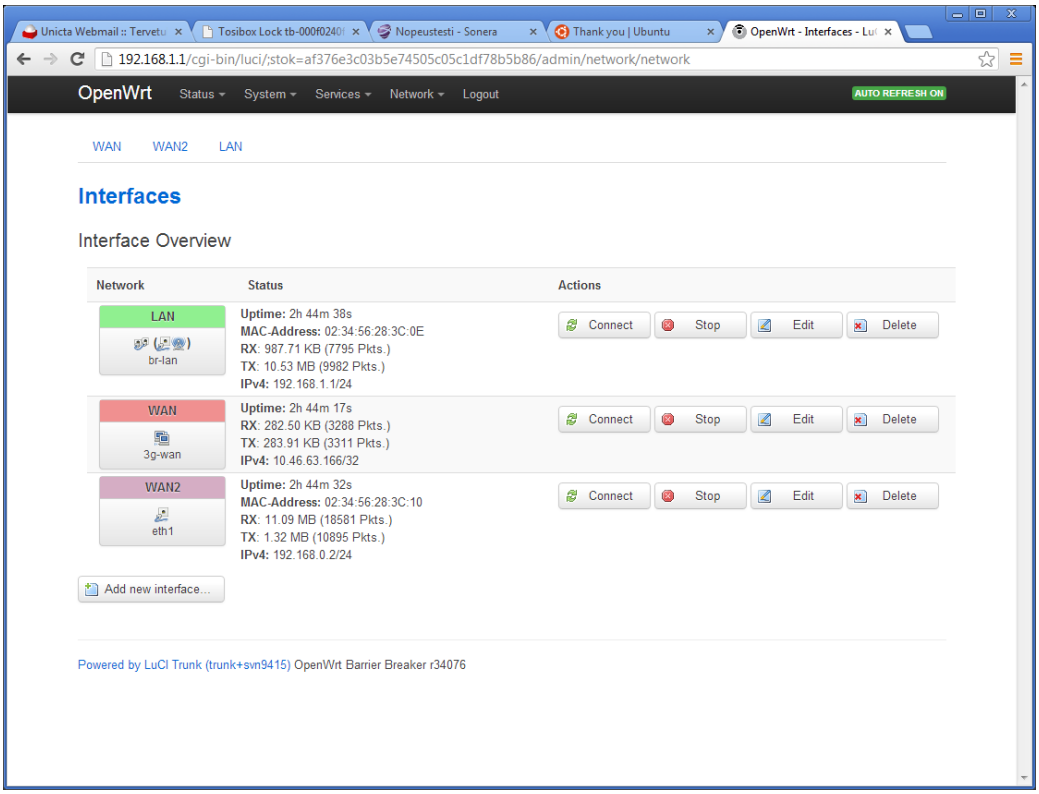
Hallinnointi

Indagonin toimittamaa laitetta hallinnoidaan www sovelluksella (loppukäyttäjänä) . Sinällään käyttöliittymä on Open WRT (kuva 9) jota on muokattu hyvin vähän, jos lainkaan. Open WRT tuottaa verraten kattavan konfigurointimahdollisuuden, eikä tämän raportin osalta ole tarpeellista uppoutua yksityiskohtiin.

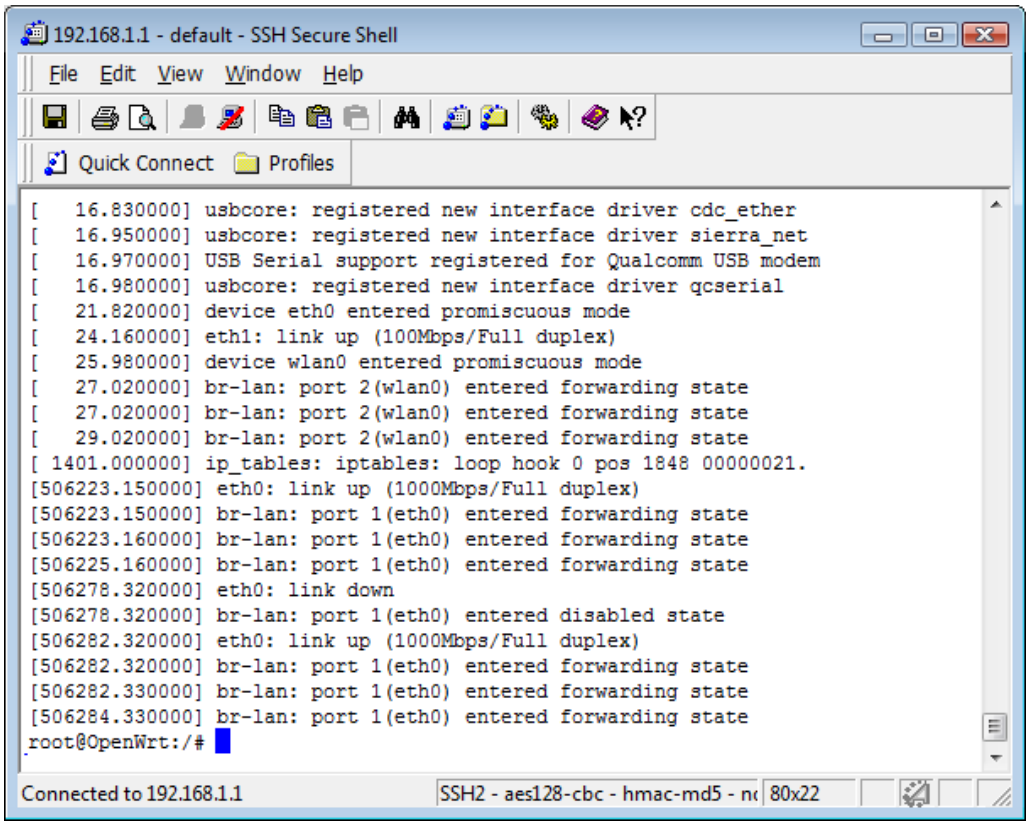


Kuva 9 Indagonin reitittimen konfigurointikäyttöliittymä

SSH yhteys (kuva 11) ei liene tarkoitettu loppukäyttäjälle, koska se vaatii verraten paljon unix osaamista. Www käyttöliittymästä saa myös loppukäyttäjä hyödyllistä tietoa, kuten ilmarajapintojen tiedot (Kuva 10).



Kuva 10 Indagon Oy:n reitittimen ilmarajapintojen tiedot



Kuva 11 SSH yhteys OpenWRT laitteeseen

Tosibox

Tosibox Oy on v. 2011 perustettu yritys, joka ilmoittaa päätoimialakseen suunnittelutoimisto. Yrityksen kotipaikka on Oulu. Yrityksestä löytyy seuraavat perustiedot: (www.finder.fi)

Toimipaikan henkilöstöluokka: 1-4 henkilöä

Yrityksen liikevaihtoluokka: 0.4-1 milj. euroa

Toimialaluokitus (TOL2008): Z62010 Ohjelmistojen suunnittelu ja valmistus

Tosibox Oy	**2011/12**	**2012/12**
Yrityksen liikevaihto (1000 EUR)	N/A	497
Liikevaihdon muutos%		
Tilikauden tulos (1000 EUR)	-12	-4
Liikevoitto%	N/A	1.80
Yrityksen henkilöstömäärä	N/A	N/A

Lähde: Suomen Asiakastieto

Tosiboxin kotisivut eivät juuri kuvaa itse yritystä, vaan lähinnä heidän tuotettaan:

"TOSIBOX laitteiden myynti on alkanut Suomessa vuoden 2012 tuokokuussa. 2013 vuonna TOSIBOX-tuotteiden myynti on käynnistynyt Ruotsissa, Norjassa ja Iso-Britanniassa. Innovaatioon on saatu ja haettu useita patentteja. TOSIBOX OY:n tuotteet valmistetaan Suomessa." (www.tosibox.fi)

Laitteiston kuvaus

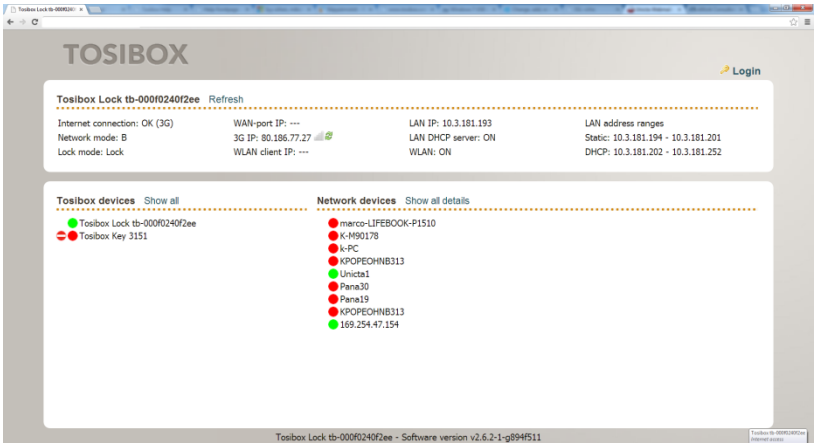
Tosibox on aluperin rakennettu TCP/IP liitännäisten laitteiden etäyhteystuotteeksi. Tuotteella luodaan VPN yhteys Tosibox reitittimeen (jota valmistaja kutsuu lukoksi) USB "tikun" (dongle, token) avulla. Reititin tukee kahta yhdenaikaista tapaa liittyä internetiin, eli 3G verkkoon USB "mokkulaa" käyttäen ja @450 (tai mihin tahansa ulkoiseen verkkoon) verkkojohdolla (RJ45). Testeissä käytetty kokoonpano näkyy kuvassa 12. 3G verkossa käytettiin ukoista antennia mokkulan kuuluvuuden parantamiseksi. Alkuperäisessä käyttötarkoituksessaan reititin on helppo asentaa ja tuottaa VPN toiminnallisuuden kuten lupaakin. USB tikku asentui vaivatta Windows XP koneeseen samoin kuin MacBook Pro:hon.

Kuva 12 Tosibox laitteiston testikokoonpano

Lukkoja pystyy ilmeisesti liittämään useampia yhteen ja siten rakentamaan laajemman VPN kokonaisuuden.

Tällaiselle toiminnolle ei kuitenkaan nähty hankkeessa tarvetta joten sitä ei testattu.

Monikanavareititystä varten tosiboxiin on rakennettu menettely, jolla lukko valvoo olemassa olevien ulkoisten yhteyksien (USB/RJ45) toimintaa ja valitsee näistä paremman yhteyden.



Kuva 13 Tosibox konfiguroinnin www liittymä

Laitteen virran syöttö valmistajan ilmoituksen mukaan voi olla 12-24 volttia. Pakkauksen mukana ei ollut ajoneuvoasennukseen sopivaa virtakaapelia, joten sellainen tehtiin itse. Laitteessa ei ole akkuvarmennusta, joten lyhyetkin katkot virran saannissa resetoivat laitteen. Käytetyssä testiajoneuvossa oli moderni stop-and-go järjestelmä joka sammuttaa auton esim. liikennevaloissa samalla katkaisten virran 12 v syötöistä. Alkuun tämä aiheutti hieman ongelmia.

Hallinnointi

Lukkoa voi hallinnoida selainsovelluksella (kuva 13), johon täytyy kirjautua. Hallinnointisovellus on hyvin kattava, selkeä ja testin laitteista viimeistellyin. Sinällään se noudattaa tuttua Open WRT mallia. Hallinnoinnissa saa esille lukon tilan (kirjautumatta) ja siihen voi kirjautua peruskäyttäjänä (user), jolla on rajoitetumpi näkymä ja mahdollisuus tehdä muutoksia reitittimen toiminnallisuuteen. Testien yhteydessä hallinnointia käytettiin lähinnä ilmarajapintojen prioriteettien määrittelyyn (kuva 14) sekä rajapinnan vaihtojen perusteena olevien ping viiveiden määrittelyyn.

Kuva 14 Tosibox reitittimen ilmarajapintojen prioriteetit

Räätälöinnit

Yhtenä hankkeen selvitettävänä asiana reititinvalmistajien osalta oli heidän kyky tehdä räätälöintejä asiakkaan tarpeen mukaan. Jokainen tutkituista valmistajista kertoi tämän olevan mahdollista, jokainen tutkittu tuote perustuu ohjelmiston osalta valmistajan omaan tuotantoon.

Räätälöintitarpeita pelastustoimen näkökulmasta on lähinnä nähtävissä useamman suojatun yhteyden (vpn) osalta, jolloin suojattuja yhteyksiä voi yhtä aikaa olla mm. TUVEen ja kunnallisen organisaation omaan verkkoon. Toisaalta räätälöinti saattaa tulla tarpeen myös liikenteen priorisoinnissa silloin kun sitä halutaan tehdä rajoitettua tiedonsiirtokapasiteettia jaettaessa. Priorisoinnin tekeminen IP-tasolla, porttitasolla tai protokollatasolla voitaneen useimmiten hoitaa laitteen konfiguroinnilla. Mikäli halutaan priorisoida eri käyttäjiä, vaatii tämä varmasti räätälöintiä laitteistoon, eikä ole suoraan nähtävissä järkeväksi toteuttaa reitittimessä.

OpenWRT

Ainakin kaksi testatuista laitteista näyttäisi perustuvan OpenWRT (https://openwrt.org/) linux jakeluun. OpenWRT on sulautettujen järjestelmien, kuten esimerkiksi reitittimien käyttöjärjestelmäksi muokattu linux käyttöjärjestelmä. OpenWRT mahdollistaa COTS (Commercial Off The Shelf) laitteiston ja omaan tarkoitukseen muokatun ohjelmiston käyttämisen. Reititinmaailmassa tällainen ns. bulkkirautapohjainen lähestymistapa on luonnollisesti varsin edullinen verrattuna oman laitteiston tuottamiseen. OpenWRT:n kanssa yhteensopivia laitteistoja löytyy edellä mainitulta sivustolta varsin mittava listaus. Näin ollen ei liene yllätys, että erilaisia monikanavareititysratkaisuja on myös maailmalla varsin paljon tämän yhtälön ympärillä. Luonnollisesti näiden kaikkien tutkimista voisi harjoittaa eliniän, ilman että ne loppuisivat kesken.

Positiivista tässä lähestymistavassa on kohtuullinen riippumattomuus laitteistotoimittajasta. Jos käytetty laitteistotoimittaja kokee toimitusvaikeuksia, voi ottaa toisen valmistajan laitteen. Toisaalta oma laitteistotuotanto on joka tapauksessa paremmin yrityksen omassa kontrollissa, joten lienee mahdotonta löytää absoluuttista paremmuutta näiden ratkaisujen välillä.

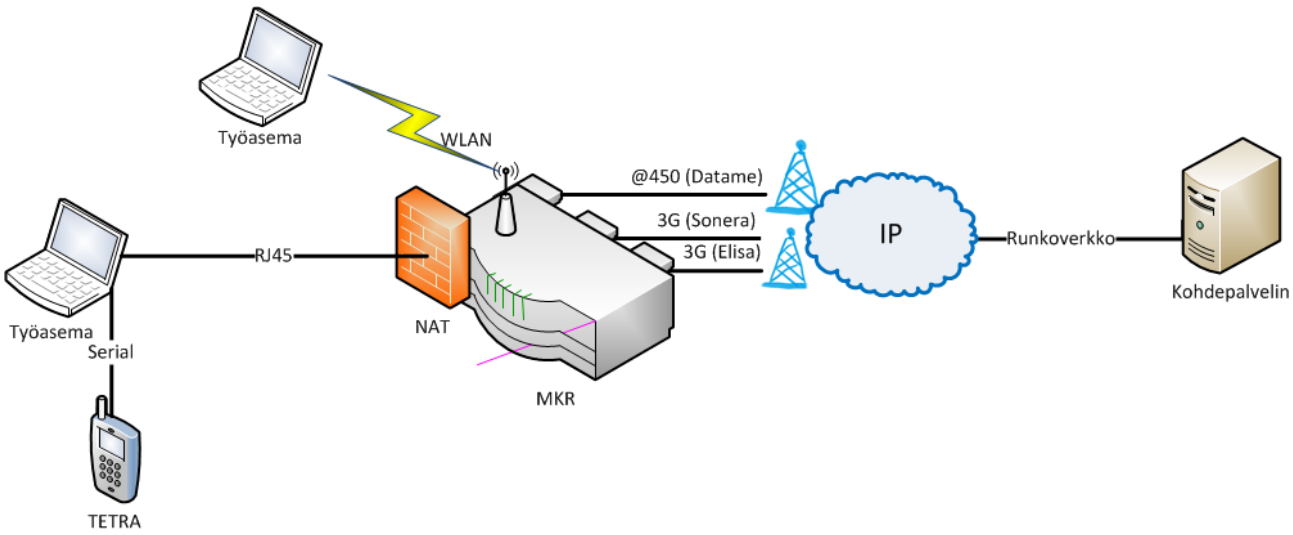
OpenWRT näyttää tällä hetkellä olevan voimissaan, viimeisin release on huhtikuulta 2013. Kehittäjäjoukko ei kuitenkaan liene kovin suuri, tarkkaa tietoa on vaikea löytää nopealla etsiskelyllä. Riskinä tällaisessa vapaaehtoisten henkilöiden kehittämässä järjestelmässä saattaa olla yhteisön "uupuminen" ja kehitystyön hidastuminen ja lopulta pysähtyminen. Laajamittaisten kaupallisten tuotteiden perustamisessa avoimen lähdekoodin tuotteisiin, on syytä varmistua siitä, että mikäli kehittäjäyhteisön kiinnostus tuotteen ylläpitoon lopahtaa, löytyy vaadittava osaaminen ja resurssi omasta takaa.

Kenttätestijärjestelyt

Kenttätestejä ja pilotteja varten päädyttiin ottamaan mukaan seuraavanlainen joukko mobiileja tietoverkkoja.

1. @450 yhteys Datame Oy:ltä
2. 3G yhteys Sonera Oyj:ltä
3. 3G yhteys Elisa Oyj:ltä
4. Tetra (VIRVE) yhteys Erillisverkot Oy:ltä (suoraan työasemaan)

Kuvana ympäristö on kuvattu kuvassa 15.



Kuva 15 Monikanavareitittimien testiympäristön yleiskuvaus

Satelliittiyhteyden käyttökelpoisuutta tutkittiin pitkään ja monen palvelun tarjoajan osalta. Sitä ei kuitenkaan nähty käyttökelpoiseksi pelastustoimen käyttöön, koska satelliittiyhteyden vaatiman näköyhteyden kulma (12 astetta) tekee yhteyden miltei käyttökelvottomaksi rakennusten läheisyydessä (taajamissa) ja kustannusvaikutus on käytettävyyteen nähden kohtuuton. @450 paikkaa satelliittidatan puutetta tilanteissa joissa kommunikaatiovaikeuksia aiheuttaa 3G verkon tukkeutuminen (esim. suuret yleisötapahtumat), koska verkossa ei kulje varsinaista puheliikennettä, eikä verkko ole laajamittaisesti suuren yleisön käytössä.

TETRA-yhteyden voisi ottaa mukaan reitittimeen, mutta silloin reitittimestä tulee koko tietoliikenteen kriittinen osa. Reitittimen vikaantuessa kaikki sen kautta kulkevat yhteydet saatetaan menettää ja tällöin on syytä olla jokin varajärjestelmä. Nykyinen PEKE voi toimia pelkän TETRA yhteyden kautta ja tämä yhteys jää käyttöön yllä olevassa konfiguraatiossa vaikka reitin vikaantuisikin.

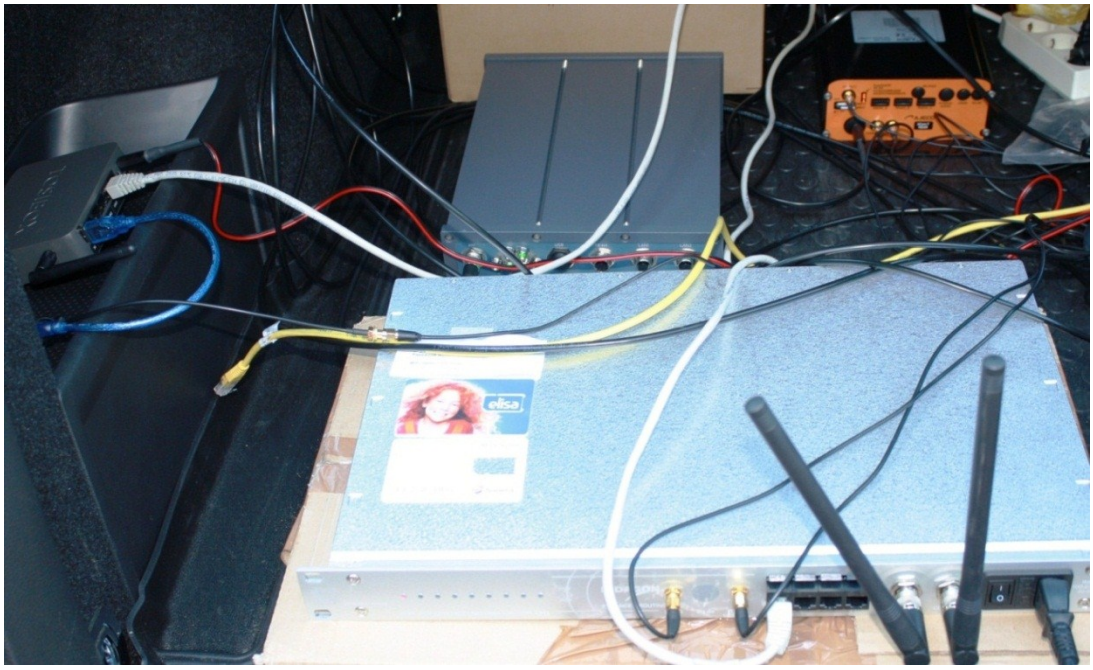
Yhteyksien valinnassa myös tutkittiin 4G yhteyksiä, mutta todettiin että 3G:n päivittäminen 4G yhteyteen ei ole kovinkaan vaativa operaatio siinä vaiheessa kun 4G peitto alkaa olla riittävä. Alueilla joilla tilanne jo on tällainen, kannattanee valita yhteyksiksi yksi 3G ja yksi 4G. Testejä varten todettiin 3G yhteyksien olevan riittävän edustavia ja tulosten hieman yhteismitallisempia.

Testejä aloitettaessa priorisoitiin testattavia asioita seuraavasti:

1. Luotettavuus

2. Helppokäyttöisyys
3. Kaistan leveys

Kenttätestejä tehtiin pelastusopiston autolla (ZR013), johon reitittimet asennettiin peräkonttiin (kuva 16). Kullekin reitittimelle tuli oma virran syöttö, Indagonin laitteeseen virta tuli invertteriltä (laite ei toimi 12 voltin tasavirralla). Virran syötössä ei havaittu ongelmia testin aikana.



Kuva 16 Reitittimet kenttätestissä

Kullekin reitittimelle varattiin ajoneuvoon oma kannettava (kuva 17), jolla reitittimen tarjoaman verkkoyhteyden luotettavuutta ja suorituskykyä monitoroitiin. Kannettavia ladattiin autolatureilla.

Kuva 17 Testissä käytetyt kannettavat

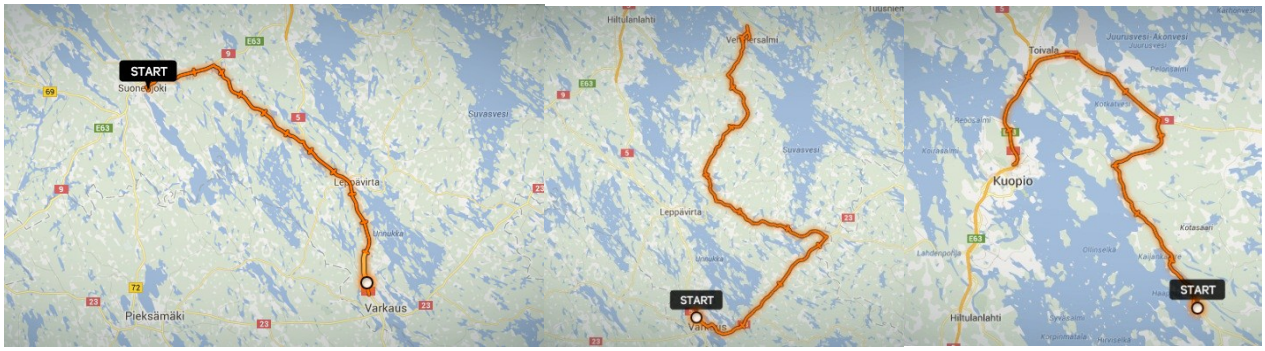
Reitittimien magneettiantennit sijoiteltiin katolle siten, ettei niistä tulisi aivan kohtuuttomasti häiriötä toisilleen (kuva 18). Todellisuudessa katolla saattaa olla enemmänkin antenneja, joten testijärjestelyn voisi

Kuva 18 Testiajoneuvon antennihässäkkä

kuvitella vastaavan kohtuudella reaalitilannetta. Kuvassa 19 on koritehtaalla valmistuvan ensihoidon johtoauton antennikalustusta.

Kuva 19 Modernissa johtoautossa voisi olla vähemmänkin antenneja ?

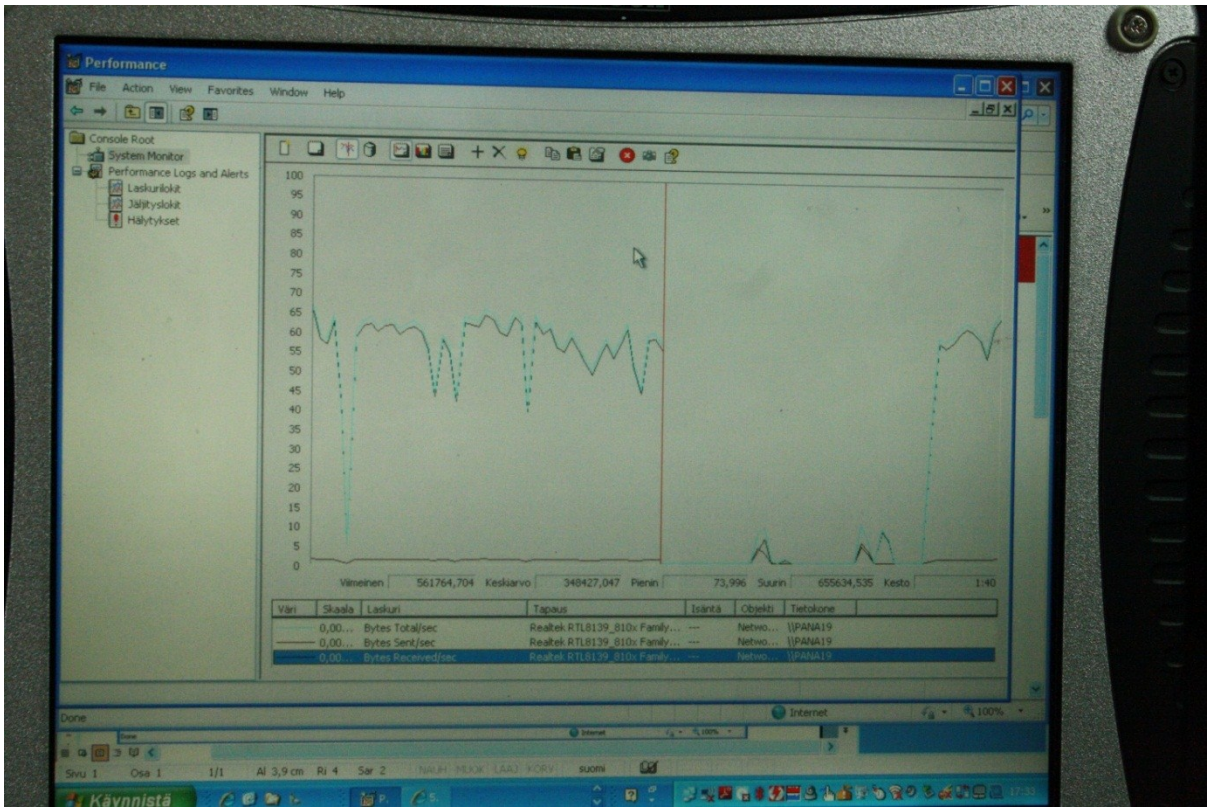
Reitittimien testaamista varten ajettiin useita reittejä, mm Suonenjoki-Jyväskylä-Suonenjoki, Suonenjoki-Espoo-Suonenjoki ja viimeisimpänä Suonenjoki-Varkaus-Vehmersalmi-Kuopio (kuva 20). Viimeisimmällä reitillä reitittimien ympäristöt olivat lähimpänä yhdenmukaisuutta, joten kyseisen reitin data otettiin tarkempaan tarkasteluun.



Kuva 20 Viimeisimmän testiajon reitit

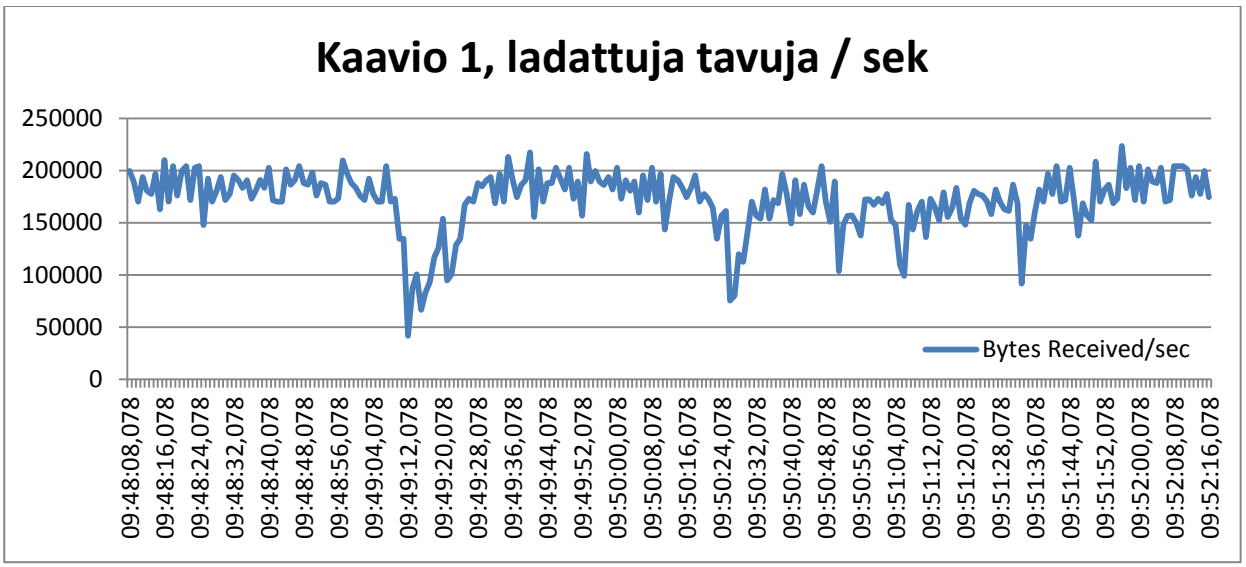
Testien tärkeimpänä testattavana ominaisuutena nähtiin verkkoyhteyden pysyvyys tilanteissa joissa ensisijainen käytössä oleva yhteys katoaa. Kontrolloidusti tätä tilannetta simuloitiin siten että reitittimen antenni suljettiin metallikuoreen (Faradayn häkki) tai antenni irrotettiin kokonaan ajoneuvon ollessa

paikallaan. Yhteyden katoamisen jälkeistä yhteydetöntä aikaa mitattiin sekuntimääräisesti. Kuvassa 21 tapahtumaa on tarkkailtu Windowsin Performance monitorilla, jossa yhteys on jo palautunut (punainen pystyviiva merkkaa kuvanottohetken tilanteen). Samalla työkalulla tallennettiin testiajojen suorituskykytiedot lokiin.



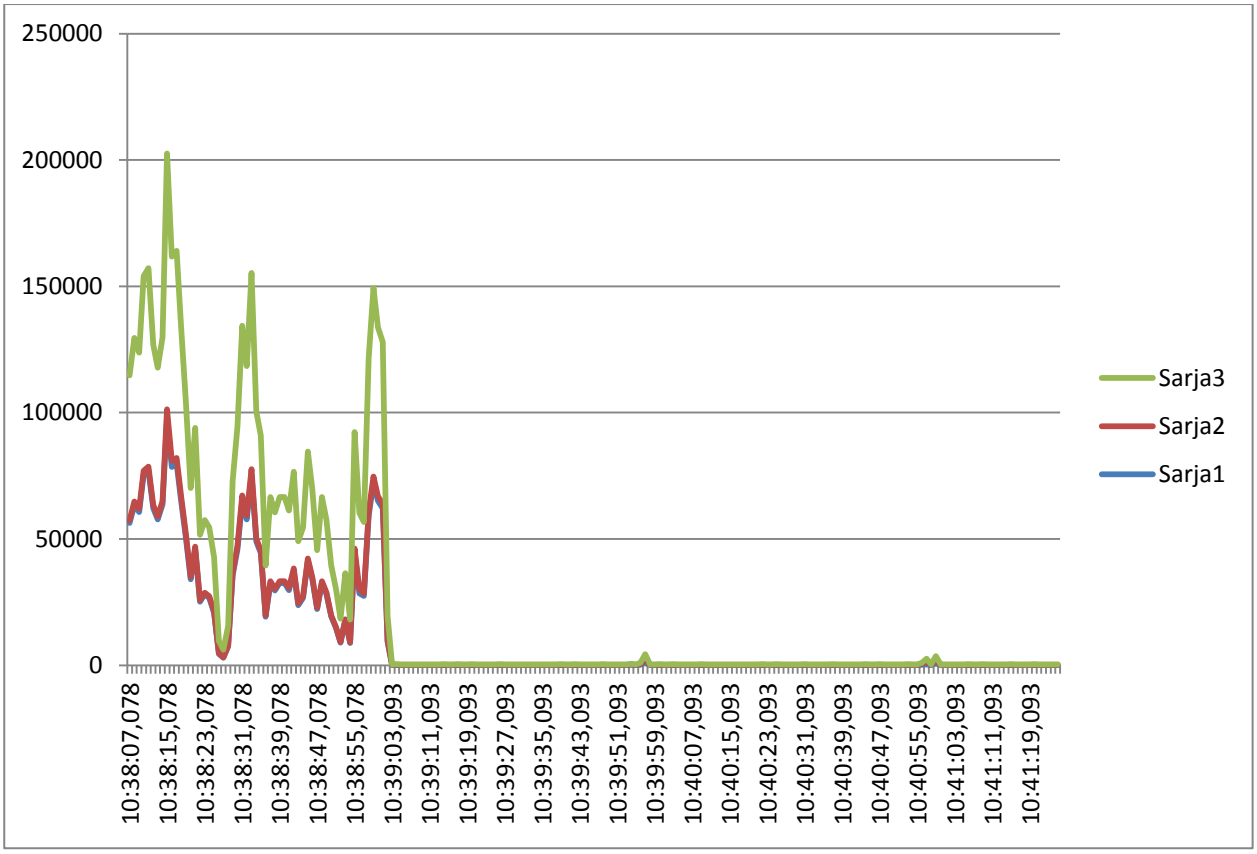
Kuva 21 Windows performance monitor

Lokeista muokattiin csv (comma separated values) tiedostoja joita voitiin käsitellä ecxelillä ja tuottaa erilaisia graafeja. Kaavio 1 kuvaa lyhyen otannan vastaanotettujen tavujen määrästä (Bytes Received / sec). Itse kaavioita mielenkiintoisempaa olisi varmaan tutkia keskiarvoja jonkin ajanjakson aikana.



Kaavio 1 Otos tiedoston latauksesta liikkuvassa ajoneuvossa

Pidemmistä testeistä ei liene järkevää piirrellä graefeja, muutoin kuin mielenkiintoisilta osin. Alla kaavio 2 on otos kohdasta, jossa reititin menettää tietoliikenneyhteyden jossain Vehmersalmen ja Kuopion välillä.

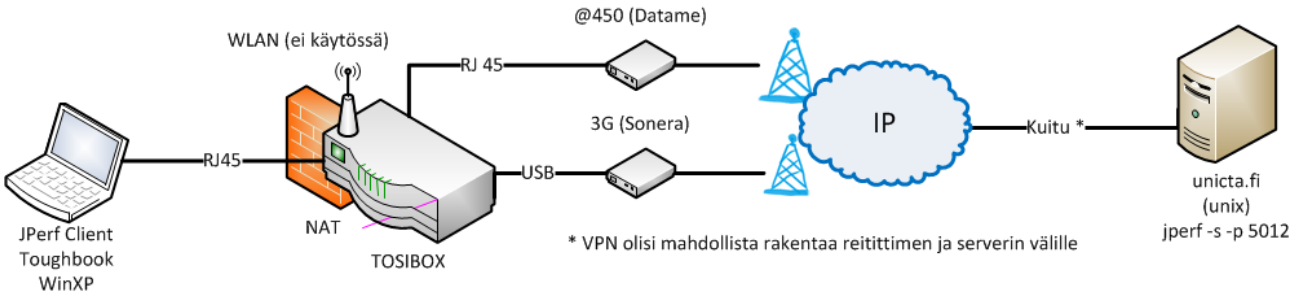


Kaavio 2 Tietoliikenneyhteyden katoaminen

Jotta suorituskykylukemat pidemmässä testiajossa olisivat vertailukelpoisia, tulisi reitittimiin priorisoida ilmarajapinnat yhdenmukaisesti ja vakioida antennisijoittelu ajoneuvossa. Lisäksi luonnollisesti reititin, jossa on vain yksi 3G yhteys, ei ole verrattavissa reitittimeen jossa niitä on kaksi. Näin ollen testidatan yksityiskohtainen vertailu on lähinnä oman mielenkiinnon suhteen relevanttia eikä tuloksia ole tässä järkevää ottaa tarkasteluun.

Tosibox

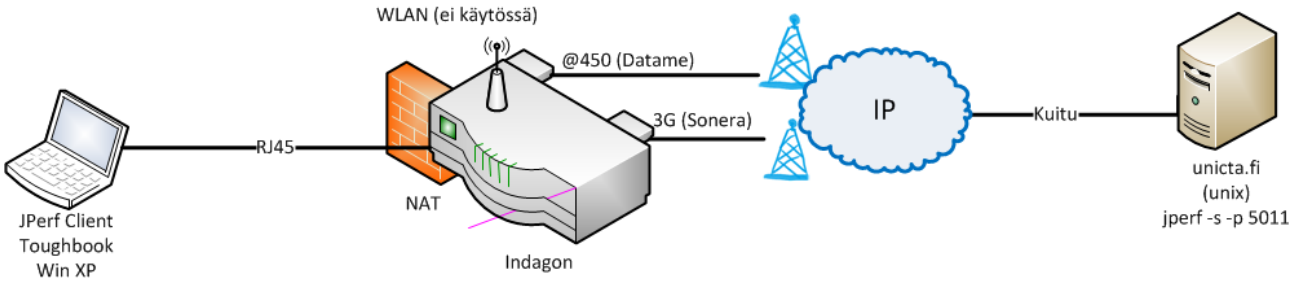
Tosibox reititin tukee kahta yhdenaikaista tapaa liittyä internetiin, eli 3G verkkoon USB "mokkulaa" käyttäen ja @450 (tai mihin tahansa ulkoiseen verkkoon) verkkojohdolla (RJ45). Edellä kuvatusta testiympäristöstä poiketen siis järjestelmässä oli vain yksi 3G yhteys (kuva 22). Myöskään VPN yhteyttä ei järjestelmään rakennettu, koska se olisi vaatinut USB tikun palvelinpäähän, ja kyseessä oli oikeassa tuotantokäytössä oleva palvelin. Lisäksi palvelimen linux server versio ei ollut tuettujen ympäristöjen joukossa.



Kuva 22 Tosiboxin testiasetelma

Indagon

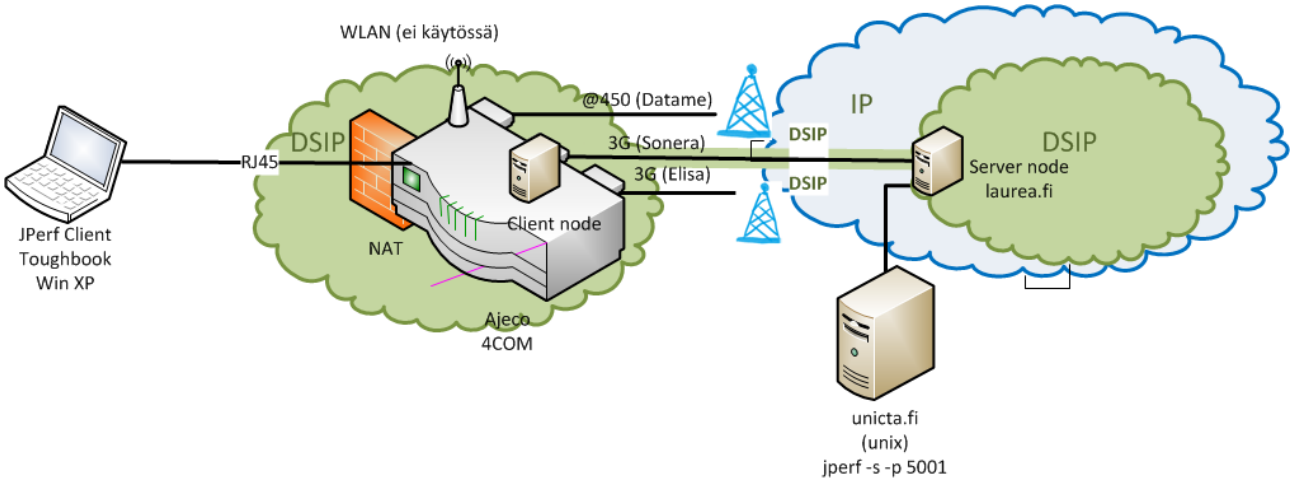
Indagon Oy:n tuotteen testiympäristö oli hyvin samanlainen kuin Tosiboxilla. Tuotteessa ei ollut tiedossa olevaa VPN yhteysmekanismia, mutta sellainen on eittämättä rakennettavissa. Myös Indagonin tuote siis tukee yhtä 3G yhteyttä ja yhtä @450 yhteyttä (kuva 23). Indagonin laitteessa yhteydet ovat kuitenkin Tosiboxista poiketen rakennettu yksiin kuoriin ilman Tosiboxissa tarvittavia USB ja RJ45 liityntöjä.



Kuva 23 Indagon Oy:n reitittimen testiasetelma

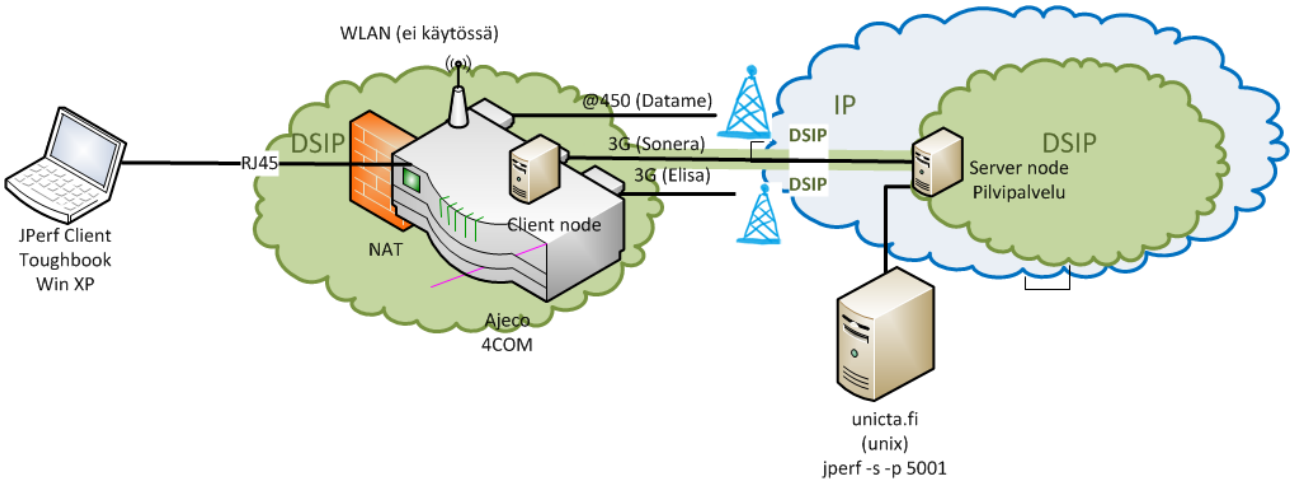
Ajeco

Ajeco Oy:n 4COM laite voidaan konfiguroida tukemaan hyvin monenlaisia liityntöjä. Testitapauksessamme laitteessa oli 2*3G ja @450. Työasema liitettiin laitteeseen RJ45 johdolla kuten kaikissa muissakin laitteissa. Ensimmäisessä konfiguraatiossa (kuva 24) yhteyden toinen pää oli Laurea AMK:n palvelimessa Espoossa. Tässä yhteydessä rajoittavana tekijänä oli palvelinyhteyden rajalliset kaistat jotka kuristivat nopeuden keinotekoisesti verrattuna esimerkiksi suoraan internetiin reitittyviin konfiguraatioihin.



Kuva 24 Ajeco Oy:n 4Com reitittimen alkuperäinen testiasetelma

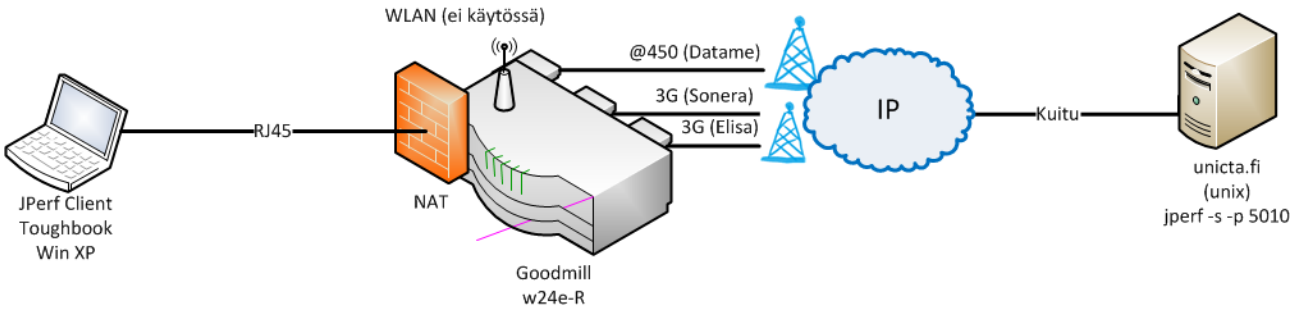
Ajecon laitteen testitapausta muutettiin myöhemmin siten että palvelinpää siirrettiin "väljemmille vesille" eli pilvipalveluun (kuva 25). Näin testeistä saatiin poistettua tuloksia vääristävät "pullon kaulat".



Kuva 25 Ajeco Oy:n 4Com reitittimen toinen testiasetelma

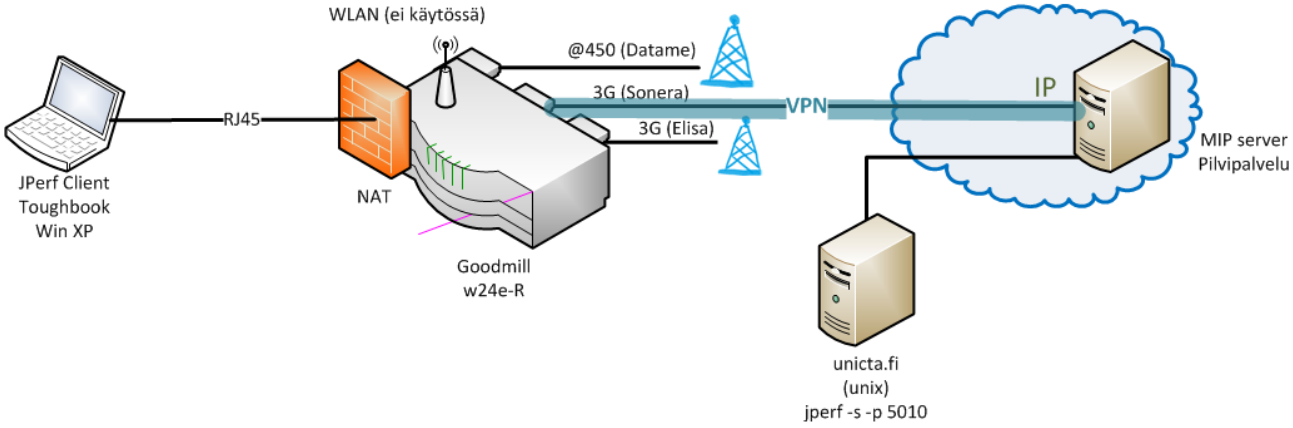
Goodmill Systems

Myös Goodmill Systemsin järjestelmää testattiin kahdella eri toteutuksella. Ensimmäisessä toteutuksessa (kuva 26) liikenne reitittyi suoraan julkiseen internetiin, mikä antoi luonnollisesti hyvän suorituskyvyn kaistanleveyden ja viiveiden osalta, mutta ei luonnollisestikaan toteuta IP istuntojen pysyvyyttä reitittimen vaihtaessa verkkoa. Tällöin avoimena olevat jatkuvaa yhteyttä tarvitsevat sovellukset (esim. videokuva, VoiP) kadottavat yhteytensä.



Kuva 26 Goodmill Systems Oy:n w24e-R reitittimen alkuperäinen testiasetelma

Toisessa testitapauksessa yhteys rakennettiin pilvessä olevaan MIP (Mobile IP) palvelimeen VPN (Virtual Private Network) yhteytenä (kuva 27). Pilvipalvelu luonnollisesti tuottaa oman viiveensä pakettien matkaan, mutta kaistan leveys on hyvä. Sinällään koettu viive ei juurikaan haittaa tavanomaisessa käytössä. MIP palvelimen tuominen maantieteellisesti lähemmäs käyttökohteita riittävän suorituskykyiseen palvelinympäristöön ja kohtuullisen tietoliikenneyhteyden ulottuville pudottaa viiveet hyvin pieniksi.



Kuva 27 Goodmill Systems Oy:n w24e-R reitittimen toinen testiasetelma

Kenttätestien tulokset

Kenttätesteillä pyrittiin hakemaan tuntumaa eri laitevalmistajien tuotteisiin niiden käyttöönoton, käytettävyyden, luotettavuuden ja suorituskyvyn osalta. Testit tehtiin olemassa olevien aika- ja henkilöstöresurssien puitteissa siten että niissä koetettiin mallintaa kenttäkäyttöä mahdollisimman todenmukaisesti. Testeissä ei kuitenkaan ollut mahdollista luoda täysin vakioitua testiympäristöä, eikä tätä nähty tarpeelliseksikaan. Vakioitu ympäristö antaisi kuvan laitteiden edellä mainituista ominaisuuksista vain kyseisessä ympäristössä ja testitulosten yleistettävyys jäisi joka tapauksessa kyseenalaiseksi.

Testimenettelyt muotoutuivat näin ollen suhteellisen heterogeenisiksi ja tulosten perusteella ei voi yleisesti muodostaa käsitystä laitteiden "paremmuudesta". Tulokset ovat siis hyvin suuntaa antavia, mutta niistä voi vetää varovaisia johtopäätöksiä, kun testimenettelyjen kuvatut rajoitukset pidetään mielessä.

Luotettavuus

Testissä havaitut luotettavuusongelmat näyttivät olevan kahta päätyyppiä: Joko laite ei havainnut käytössä olleen ilmarajapinnan menevän pois kuuluvuusalueelta ja jatkoi toimimattoman rajapinnan käyttöä tai rajapinnan vaihtuminen kesti sen verran pitkään että tiedonsiirtosessio ehti katketa.

Erityisen ongelman tuntui aiheuttavan @450 verkossa käytettäessä Datame Oy:n toimittamaa erillistä reititintä CDMA yhteyden luomiseen. Reitittimen toiminta sen mennessä kuuluvuusalueen ulkopuolelle ei ilmeisesti ollut aivan ennakoitua ja tämä aiheutti reitittimen "jumimisen" @450 yhteyteen vaikkei sen kautta saatu minkäänlaista tiedonsiirtoa. Ongelma on korjattavissa kun se otetaan huomioon reitittimen softassa.

Käytännössä kaikki testissä olleet laitteet joko osoittivat nykyisellään hyvää luotettavuustasoa tai edellä mainittujen @450 ongelmien korjaamisen jälkeen voidaan sellaiselle saattaa. Olennaisena osana luotettavuuden rakentamista ja tietoliikenneseisokkien minimoimista on reitittimien ilmarajapintojen oikea priorisointi. Tähän vaikuttaa esim. 3G/4G yhteyksien kuuluvuusalueet operaattoreittain. Operaattoreiden valintaa ajatellen lieneekin syytä hahmottaa reitittimen pääasiallinen käyttöalue ja tutkia sen jälkeen kuuluvuusaluekarttoja.

Luonnollisesti kahden 3G yhteyden käyttö yhden sijaan parantaa järjestelmän luotettavuutta, koska aina löytyy katvealueita joissa jonkin operaattori on heikommalla.

Helppokäyttöisyys

Loppukäyttäjän näkökulmasta käytännössä laitteesta joko saa tai ei saa yhteyden tarvittaviin palveluihin. Kentällä laitteen käyttämisessä ainoa "järkevä" toimenpide ongelmatapauksessa on laitteen uudelleen käynnistäminen. Laitteen konfigurointiin liittyvistä käyttöliittymistä on kerrottu laitteiden esittelyn yhteydessä.

Kaistan leveys

Tiedonsiirtonopeuden osalta laitteissa ei havaittu merkittäviä eroavaisuuksia. Hetkittäiset erot selittynevät lähinnä käytössä olleella rajapinnalla. Toisen 3G yhteyden merkitys näkyy pidemmän aikavälin keskiarvoissa kun kahdesta voidaan valita nopeampi. Kenttätestien datamäärä ei kuitenkaan ollut mielestämme riittävän kattava vetää tästä pitkälle vietyjä johtopäätöksiä.

Samalla yhteyden salaaminen (VPN) luonnollisesti nakertaa hyötykuormaa tiedonsiirrosta. Näin on luonnollista että salaamattoman yhteyden nopeus näyttää loppukäyttäjälle paremmalta kuin salatun. Johtopäätösten vetäminen vaatisi huomattavan kattavat testit vakioidummassa ympäristössä.

Pilottikohteet ja pilottien tulokset

Projektissa päädyttiin kolmeen pilottikohteeseen. Kohteet valikoituivat lähinnä osanottajien halukkuuden ja sopivan ajoneuvoalustan löytymisen perusteella. Pilottikohteista kahteen (Keski-Suomi ja Pohjois-Savo) asennettiin Goodmill Oy:n toimittama reititinlaite ja yhteen (Keski-Pohjanmaa ja Pietarsaari) Ajeco Oy:n toimittama laite. Laitteet hankittiin projektin määrärahalla ja yhteydet laitteisiin tulivat Erillisverkot Oy:ltä.

Laitteistojen asennus ajoittui kevääseen 2013 ja syksyyn 2013. Kaikkia laitteita ei asennettu keväällä, jotta kenttätestit voitiin suorittaa alkukesästä. Laitteet jäävät projektin päätyttyä laitosten käyttöön ja niiden käytöstä kerätään jatkuvasti kokemuksia joita voidaan jatkossa hyödyntää palvelun rakentamisessa.

Keski-Suomen pelastuslaitos

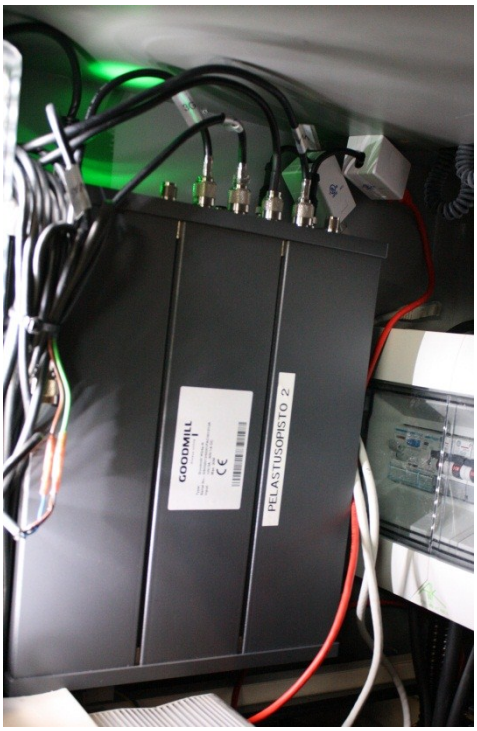
Keski-Suomen pelastuslaitoksella reititin asennettiin uuteen johtoautoon (kuva 28), joka otettiin käyttöön keväällä 2013. Projektin puitteissa käytiin koritehtaalla tutustumassa reitittimen sijoitukseen ja antennikalustukseen.

Kuva 28 Keski-Suomen pelastuslaitoksen johtoauto koritehtaalla

Varsinainen laitteen asennus ja käyttöönotto tehtiin Jyväskylässä projektin toimesta. Laite asennettiin koritehtaalla asennettuun asennusalustaan, joten lähinnä kyseessä oli kytkentöjen tekeminen ja laitteen testaaminen. Antennien liittimet tosin jouduttiin vaihtamaan asennuksen yhteydessä alkuperäisten ollessa sopimattomia (kuva 29).

Pilotissa testattiin aluksi konfiguraatiota jossa laite oli yhteydessä Erillisverkot Oy:n Jyväskylän toimipisteeseen sijoitettuun MIP palvelimeen. Palvelimen tarkoituksena on tuottaa salattu yhteys reitittimestä (VPN) palvelimeen ja samalla ylläpitää IP istuntoja niissä tilanteissa joissa reititin vaihtaa käyttämäänsä verkkoa. Tällaisessa tilanteessa normaalisti IP-osoite reitittimessä vaihtuu, mikä aiheuttaa VPN-yhteyden katkeamisen, ellei tähän ole erikseen järjestelmässä varauduttu.

Reitittimestä riippumattomista verkko-ongelmista johtuen konfiguraatio muutettiin siten, että MIP palvelin asennettiin pilvipalveluksi, jolloin IP istuntojen pysyvyys saatiin turvattua. Alkuperäisen yhteyden kaistaa myös rajoitti MIP palvelimen sijainti ADSL liittymän takana. Pilvipalveluun perustuvassa konfiguraatiossa VPN yhteys luonnollisesti päättyy pilvessä olevaan MIP palvelimeen ja pilvipalvelun käyttö luo pieniä viiveitä. Viiveet ovat kuitenkin niin pieniä, ettei niitä loppukäyttäjä normaalikäytössä havaitse, eikä yhteyttä rajoittava ADSL pullon kaulaa esiinny. Edellä mainittujen konfiguraatioiden välissä testattiin järjestelmän toimintaa ilman MIP palvelinta, jolloin liikenne reitittyi suoraan julkiseen internetiin.



Kuva 29 Reititin valmiiksi asennettuna

Käyttökokemukset

Edellä raportoitujen alkuhankaluuksien jälkeen käyttäjät ovat olleen hyvin tyytyväisiä yhteyksien laatuun ja luotettavuuteen. Käyttökatkoja ei ole havaittu, eikä laitteisto ole vaatinut aktiivista ylläpitoa. Myös yhteyden suorituskyky on ollut riittävä käyttäjien tarpeisiin. (Puhelinkeskustelu 20.8.2013)

Keski-Pohjanmaan ja Pietarsaaren alueen pelastuslaitos

Keski-Pohjanmaan ja Pietarsaaren aluepelastuslaitoksen johtoautoon, KP30, asennettiin Ajecon 4Com monikanavareititin. Asennus tehtiin magneettiantenneilla "puolipysyväksi". Reititin kiinnitettiin ajoneuvon ohjaamossa olevaan laitekaapin oveen (kuva 30). Virran syöttö otettiin ajoneuvon omasta järjestelmästä (220 v), jossa asemalla virta tulee sähköverkosta ja ajossa invertteristä.

Kuva 30 Pilottiasennus Keski-Pohjanmaan ja Pietarsaaren aluepelastuslaitos, KP30.

Reitittimen tietoliikenne kytkettiin pilvipalveluun, jonka kautta yhteydet muualle reitittyvät. Jatkossa tietoliikenne kannattanee kytkeä siten, että se reitittyy jo laitteelta suoraan joko kuntaverkkoon, TUVEen tai julkiseen internetiin. Ajecon DSiP tuoteperheessä tämä saavutetaan asentamalla verkon solmusovellukset (node) tarvittaviin paikkoihin.

Pelastustoimen langaton laajakaista palveluna

Hankkeen aikana pelastuslaitosten edustajien kanssa käydyn keskustelun ja Suomen Erillisverkot konsernin saaman asiakaspalautteen perusteella on käynyt ilmi, että suuri osa liikkuvaa laajakaistaista dataratkaisua tarvitsevista organisaatioista haluaisi ostaa sen palveluna kuukausimaksua vastaan. Tällöin palveluntuottaja, eli Erillisverkot, vastaisi palvelun tuottamiseen tarvittavien osakokonaisuuksien hankinnasta tai niiden tuottamisesta itse. Tällainen "yhden luukun" periaate on houkutteleva ympäristössä jossa halutaan keskittyä varsinaiseen työhön, eli pelastustoimintaan. Reititinlaitteet tulisivat jatkuvan valvonnan piiriin, kuten VIRVE verkko on tällä hetkellä.

Palvelukuvaus

Palveluntuottaminen vaatisi muun muassa kaupallisten radioverkkojen (Sonera 3G, Datame CDMA jne.) sekä päätelaitteiden (kts. Reititinvalmistajat) kilpailuttamista. Näiden ympärille Erillisverkojen tulee luoda nykyisillä, VIRVEssä käytössä olevilla prosesseilla toimiva Langaton IP –palvelu (LIP) –palvelukokonaisuus, joka sisältää muun muassa asiakaspalvelun sekä palvelunvalvonta ja -hallinta –toiminnot. LIP –palvelun avulla käyttäjä voi liikennöidä viranomaisten yhteisiin tietojärjestelmiin (Esim. KEJO) tai organisaation omiin tietojärjestelmiin Erillisverkkojen kiinteän IP –liittymän (KIP) avulla.

LIP –palveluun liittyminen

LIP –palvelun kohderyhmiä ovat muun muassa:

- Kansalaisten turvallisuutta ja terveyttä sekä yhteiskunnan järjestystä varmistavat viranomais- ja siviiliorganisaatiot
- Turvallisuuskriittiset organisaatiot
- Kriittistä infrastruktuuria ylläpitävät organisaatiot

Palvelun tilaus tapahtuu Erillisverkot konsernissa kustakin asiakkuudesta vastaavan henkilön kautta, eli saman henkilön kautta kuin VIRVEen liittyvät asiat. Kullekin asiakkaalle parhaan kokonaisratkaisun löytämisessä avustavat lisäksi tarvittaessa kyseisestä asiakasratkaisusta vastaava asiantuntija sekä LIP palvelusta vastaava tuotepäällikkö.

LIP palvelun sisältö

Lähtökohtaisesti LIP -palvelu sisältää aina sekä laitteen että tarvittavat radioliittymät sekä niihin liittyvä asiakaskohtainen IP -osoitteistus. Peruspalveluun sisältyy tietoliikenteen reititys asiakkaan omaan virtuaaliverkkoon (L3VPN). Liikennöinti muihin virtuaaliverkkoihin vaatii säännön avaamisen ulkoiseen kytkentäytimeen (UKY) joka on oma tuotteensa. Peruspalvelun tulee todennäköisesti koostumaan monikanavareitittimestä jossa on kaksi 3G/LTE tai yksi 3G/LTe ja yksi 2G -liittymää. Palveluun ei sisälly laitteen asennus. Lisäpalveluina asiakkaille tullaan mahdollisesti tarjoamaan erityyppisiä päätelaitteita (1 radioliittymä ja vain yksiradio) sekä erilaisia liittymiä, kuten satelliitti tai CDMA450. Palvelu sisältää virka-aikaan toimivan asiakaspalvelun sekä 24/7 toimivan vikailmoitus –palvelun. Käyttäjiä tullaan lisäksi tiedottamaan suunnitelluista ja yllättävistä epäkäytettävyystilanteista mahdollisuuksien mukaan.

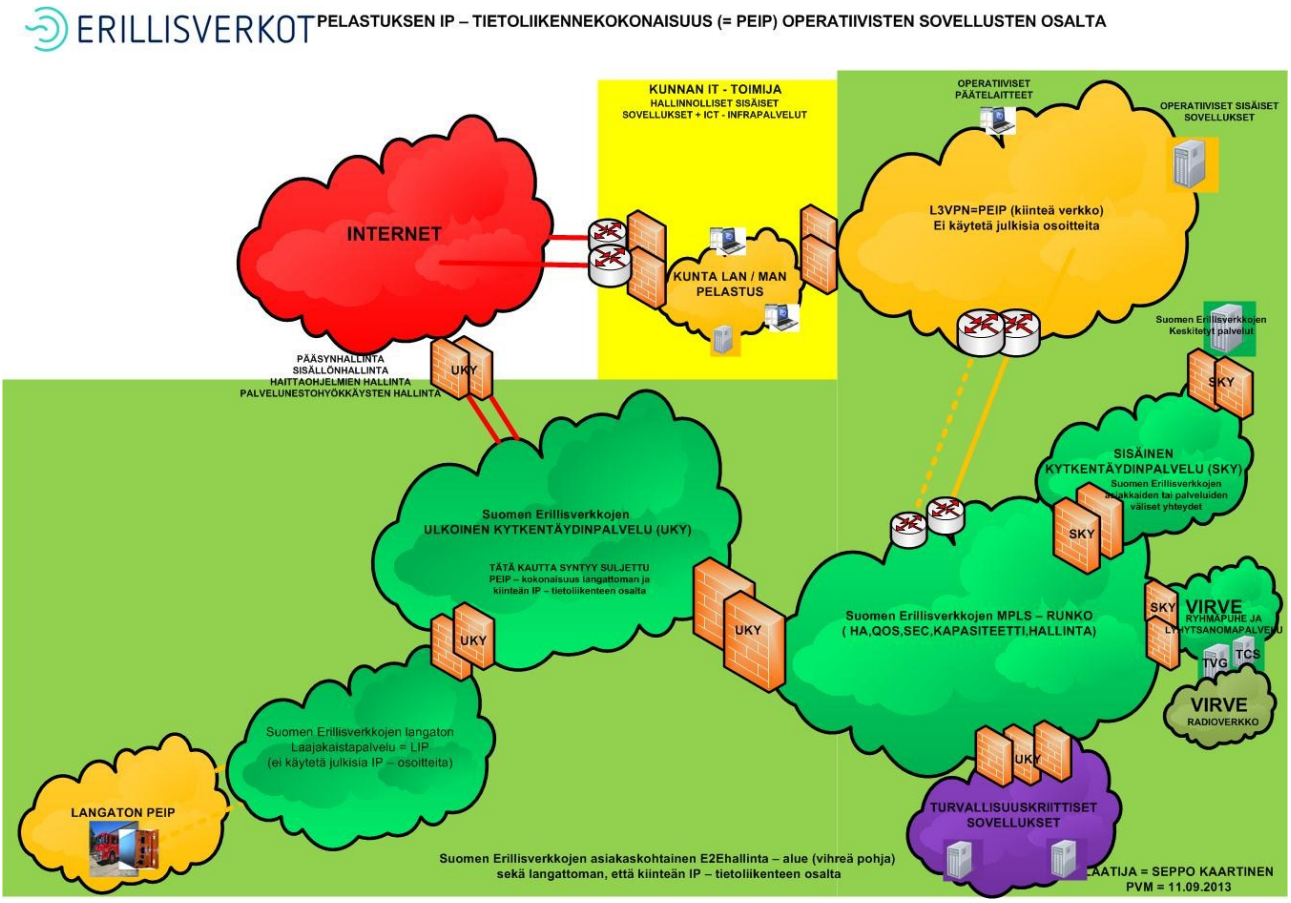
Osalla palvelun käyttäjistä on jo olemassa laite, joka ei ole vielä elinkaaren päässä. Tällaisille käyttäjille voidaan toimittaa vain radioliittymät. Mikäli asiakkaan päätelaite on yhteensopiva hankitun hallintajärjestelmän kanssa, voidaan se lisäksi ottaa Erillisverkkojen etävalvontaan.

Palvelun rakentaminen

Pelastustoimen langatonta laajakaistaa rakennetaan palveluksi parhaillaan. Erillisverkot Oy on lähettänyt useille monikanavareitittimiä tarjoaville yrityksille tarjouspyynnöt alkukesästä 2013 koskien reititinlaitteita ja niihin liittyviä taustajärjestelmiä. Laitetoimittajien laitteistojen kyvykkyyksiä on selvitetty tarjouspyynnössä liitteen 2 kysymyspatterilla.

Palvelu tullaan tarjoamaan asiakkaille niin sanottuna elinkaarimallina, jolloin asiakkaat maksavat Erillisverkoille kiinteää kuukausimaksua sopimuskauden ajan. Kuukausimaksua vastaan Erillisverkot vastaa sekä liittymien, että tuotteeseen sisältyvien laitteiden hankinnasta ja ylläpidosta. Kuukausimaksu sisältää myös liikennöintimaksut.

Palvelun rakentamisvaihe ajoittuu 2013 loppupuolelle ja 2014 alkuvuoteen. Tavoitteena on, että ensimmäiset asiakkaat voisivat ostaa palvelun 2014. LIP palvelun verkkoarkkitehtuuria ja sen liittymistä muuhun, olemassa olevaan verkkoinfrastruktuuriin on kuvattu kuvassa 31. Kuva on suuremmassa koossa paremman luettavuuden vuoksi liitteessä 3.



Kuva 31 Langattoman IP -palvelun (LIP) liittyminen muuhun verkkoinfrastruktuuriin

Yhteenveto

MoniKa hankkeen tavoitteet toteutuivat täysimääräisesti. Tätä raporttia kirjoitettaessa Erillisverkot ovat pyytäneet tarjouksia laitetoimittajilta viranomaisten langattoman laajakaistan toteutusta varten ja tavoitteena on että palvelun tekninen ympäristö on vuoden 2014 alkupuolella valmis. Hankkeen aikana tehtiin paljon työtä laajakaistayhteyden kautta tavoiteltavien palvelujen todellisen saatavuuden eteen. Tästä työstä suuri osa oli tietoturva- ja arkkitehtuurityötä, jonka tavoitteena oli luoda verkkoympäristöstä sellainen, ettei se rajoittaisi pelastustoimessa (tai muussa viranomaistyössä) tarvittavien palvelujen saatavuutta. Tässä yhteydessä yhteistyötä tehtiin TOTI ja etenkin KEJO hankkeiden kanssa.

Pelastustoimen tiedonsiirron tarpeita analysoitiin kartoittamalla pelastustoimen käyttämiä palveluita ja niiden kriittisyyttä pelastustoiminnassa. Palvelukartoitusta hyödynnetään jatkossa TUPO- ja VOTI hankkeissa, joissa määritellään pelastustoiminnan työasemien kokoonpano ja tietoturvakäytänteet. Tässä palvelukartoitus saumattomasti nivoutuu MoniKa hankkeeseen siten että tiedonsiirron priorisointi toteutetaan työasemavakioinnin yhteydessä.

Tarjolla olevista monikanavareitittimistä kerättiin tietoa sekä dokumentaatioiden ja yritysvierailujen muodossa, että omin kenttätestein ja pilottien kautta. Pilottikohteet jäävät toimintaan hankkeen päätyttyäkin ja niistä saatavaa kokemusta tullaan hyödyntämään palvelun rakentamisessa.

Kenttätesteistä kerättiin verraten laaja ja yksityiskohtainen data jota analysoitiin hankkeen aikana. Analyysin perusteella voidaan todeta että kaikki koekäytössä olleet laitteet ovat joko sellaisenaan suoraan käyttökelpoisia viranomaisten langattoman laajakaistan toteutukseen tai pienin muutoksin ja parannuksin. Kenttätestin osoittamat ongelmakohdat on kommunikoitu suoraan laitetoimittajille ja osa ongelmista on jo hankkeen aikana korjattukin laitetoimittajien toimesta. Kenttätestien ympäristöä ei kuitenkaan saatu niin hyvin vakioitua, että yksityiskohtaisia tuloksia voisi tasapuolisesti käsitellä tässä raportissa. Toisaalta oppimisprosessi on ollut molemmin puolinen sekä testauksen suorittamisen suhteen hankkeen henkilöstölle että myös laitevalmistajien suhteen tällaiseen testiin valmistautumisessa ja laitteiston testikuntoon saattamisessa.

Kaikki laitevalmistajat olivat kotimaisia toimijoita joilta jokaiselta löytyy riittävä osaaminen omasta takaa muokata ja räätälöidä laitteistoa ja sen toimintaa viranomaiskäyttöön soveltuvaksi.

Kaiken kaikkiaan hanketta voi luonnehtia onnistuneeksi tulosten ollessa näkyvissä enemmän kentällä kuin tässä raportissa. Langattoman laajakaistapalvelun rakentaminen on hyvässä vauhdissa ja reititinlaitteiden osalta kilpailutus on käynnissä. Osana kilpailutusta on reitittimien ohella niiden hallinnointi ja monitorointijärjestelmät. MoniKa hankkeessa näihin järjestelmiin ei paneuduttu, vaan hallinnoinnin ja monitoroinnin järjestelyjen kartoitus jätettiin palvelun tarjoajan tehtäväksi. Luonnollisesti nämä palvelut ja niiden tuottamisen sujuvuus ovat ensisijaisen tärkeitä palvelun tarjoajan näkökulmasta. On helposti nähtävissä, että yhdellä palvelun tarjoajalla on useita satoja reitittimiä tuotannossa yhtä aikaa, jolloin laitteiden etävalvonta ja etenkin etähallinta nousevat erityisen tärkeiksi.

Suositukset

Viranomaisten varmennettu liikkuva laajakaista on monen tekijän summa. Järjestelmää rakennettaessa on otettava huomioon useita seikkoja joista itse monikanavareititin on vain yksi. Laitteiston hallintajärjestelmä tulee hyvin tärkeään rooliin, kun laitteita alkaa olla satoja. Laajamittaisessa kaupallisessa toiminnassa myös toimitusvarmuus korostuu ja toimituksissa mahdollisesti ilmeneviin ongelmiin tulee varautua.

Laitteistojen ja hallintajärjestelmien source escrow

Laajakaistapalvelu tarvitsee ohjelmistoja sekä reitittimen käyttöjärjestelmässä että reitittimien hallinnan taustajärjestelmässä. Lisäksi tietoliikenteessä tarvitaan yleensä palvelinsovelluksia ja VPN tai vastaavia sovelluksia. Näiden sovellusten ylläpitomahdollisuuksien varmistaminen on nähtävissä ensiarvoisen tärkeäksi riskienhallintamenettelyksi laajakaistan tuotteistamisessa.

Mikäli ratkaisut perustuvat avoimen lähdekoodin tuotteisiin, täytyy varmistaa että joko toimittajalla tai omassa organisaatiossa todella on kyky kehittää ja ylläpitää järjestelmää jos avoimen lähdekoodin tuotetta kehittävä yhteisö jostain syystä lakkaa toimimasta tai tuotteen ylläpito muutoin "jää heitteille".

Silloin, kun sovellukset perustuvat toimittajan omaan sovellustuotantoon, on syytä varmistua siitä, että kaikelle hankittujen tuotteiden lähdekoodille on olemassa ns. source escrow sopimus. Tämä tarkoittaa sitä, että tuotteiden lähdekoodit ovat luotetun kolmannen osapuolen hallussa, ja mikäli toimittajan kyky toimittaa tuotteita tai ylläpitää ohjelmistoja jostain syystä katoaa, ostaja saa tuotteiden lähdekoodit haltuunsa. Tällöin luonnollisesti on olennaista että ostajalla on kyky hyödyntää lähdekoodia, eli osaaminen sen ylläpitoon ja jatkokehitykseen.

Laitteistojen ja tietoliikennejärjestelyjen tietoturva ja auditoinnit

Laitteistotoimittajat luonnollisesti ovat valmiita kehumaan oman laitteistonsa tietoturvatasoa ja käyttämiensä kommunikaatiomenettelyjen ylivertaisuutta. Pelkät toimittajien kertomaan perustuvat arviot ovat kuitenkin riski rakennettaessa laajamittaista palvelua viranomaiskäyttöön. Kilpailutusvaiheessa olisi hyvä käydä jonkinlainen tekninen dialogi tietoturva-asiantuntijoiden avustuksella jotta eri ratkaisuvaihtoehdoissa mahdollisesti piilevät tietoturvaan tai muuhun toiminnallisuuteen liittyvät uhat ja potentiaaliset ongelmat saataisiin selville. Tässäkin raportissa esitettyjen laitteistojen toimintatavat ja kommunikaatiotavat eroavat hyvin selkeästi toisistaan ja niiden haavoittuvuudet trenditermiksi nousseen kyberuhkan osalta tulisi tutkia. Viranomaisten varmennettu laajakaista ei voi perustua järjestelmään, jonka vieras valtio tai riittävän tietämyksen osaava rikollisjärjestö voi lamaannuttaa halutessaan. Minimissään laite-hallintajärjestelmä kokonaisuuden tulee olla luotettavan ja osaavan tahon auditoima.

Auditointeja on monenlaisia ja monentasoisia. Hyvin usein auditoinneissa tyydytään ns. penetraatiotestauksiin ja dokumentteihin perustuvaan auditointiin. Huomioiden viranomaisten varmennetun langattoman laajakaistan toimintakriittisyyden, on perusteltua, että laitteistojen ja taustajärjestelmien lähdekoodit auditoidaan kooditasolla (koodikatselmus) valittavasta järjestelmästä. Koodikatselmus voidaan toteuttaa joko automaattisin työkaluin tai manuaalisesti, asiaan perehtyneen ekspertin toimesta. Manuaalinen vaihtoehto luonnollisesti kalliimpi toteuttaa, mutta siten löydetään sellaiset ongelmat (myös tietoturvaan liittyvät) joita automaattisin työkaluin ei voi havaita.

Laitteistojen käyttöjärjestelmien osalta koodiaudit myös löytää sellaiset sinänsä hyvässä tarkoituksessa esimerkiksi testausta ja tuotekehitystä varten tehdyt ja mahdollisesti koodiin jääneet root salasanat ja muut takaovet, joita ei ole valmiista tuotteesta poistettu. Yhdestä testatusta tuotteesta tällainen havaittiin testivaiheessa ilman koodikatselmustakin. Lienee selvää, että loppukäyttäjän täytyy viranomaistoiminnassa olla tietoinen kaikista tällaisista tuotteessa olevista piilevistä ominaisuuksista.

Pelastustoimen käytössä olevia palveluita

LIITE 1

	Kuvaus	Tuotantopaikka	Tuot. paikka 2	Reititys tulevaisuudessa	Käyttöliittymä (nyt)	Käyttöliittymä 2 (nyt)	Käyttöliittymä tulevaisuudessa	Operatiivinen luokittelu	Kuka omistaa	Järjestelmä Lisätietoja
Väestöhälyttimet	Väestöhälyttimien käynnistys- ja valvontasov. Pelastuslaitos		Radioverkko (VIRVE, VHF)	Kuntaverkko		VIRVE päätelaite	Paikallinen sovellus, HÄKE	KEJO, ERICA	1. Kiireellinen operatiivinen	Kunta
Varotieto	Uhkaavan henkilön, kohteen ja välineen tieto Insta ja tuotetaan ERICAssa		TUVE			ei ole		KEJO, ERICA	1. Kiireellinen operatiivinen	HÄKE
JOTKE	Pelastustoimen ylemmän tason tilannekuvajärjestelmä Tieto & SM/PEO/MJ		Yksityinen palvelun tarjoaja	(PEIP tulevaisuudessa)		WWW			2. Kiireetön operatiivinen	SM/PEO
PetoMedia	Mediatiedotteiden jakelukanava		TUVE			ei ole	sähköpostijakelulista		1. Kiireellinen operatiivinen	SM/PEO
Vaaratiedote	Kansalaisten varoittamisjärjestelmä		TUVE			ei ole	sähköposti/sanelu häkeen	KEJO	1. Kiireellinen operatiivinen	HÄKE
PEKE	Pelastustoimen kenttäjohtamisjärjestelmä Haltik ja SM/PEO		TUVE			Sovellus		KEJO Korvaa	1. Kiireellinen operatiivinen	SM/PEO
Lomakkeet	Pelastustoiminnan johtajan apuvälineet Nykyisin tuotanto pelastuslaitoksilla		TUVE	KEJO (tulevaisuudessa)		ei ole	Paperi	KEJO ?	1. Kiireellinen operatiivinen	
Kohdekortti	Kuvaus kohteesta pelastustoiminnan johtamisen näkökulmasta		PEIP	Varanto		Sovellus	MERLOT / Paperi	KEJO ?	1. Kiireellinen operatiivinen	
Turvallisuussää	Ilmatieteen laitoksen viranomaissääpalvelu		Yksityinen palvelun tarjoaja	FMI (PEIP tulevaisuudessa)	PEIP	WWW		WWW	2. Kiireetön operatiivinen	
Häiriöt tieliikenteessä	Tieliikenteen häiriöiden tiedotusjärjestelmä		Yksityinen palvelun tarjoaja	Trafi (PEIP tulevaisuudessa)	PEIP	WWW			2. Kiireetön operatiivinen	Liikennevirasto
LUOVA operatiivinen	Luonnon onnettomuuksien varoitusjärjestelmä Ilmatieteen laitos		Yksityinen palvelun tarjoaja	Ilmatieteen laitos (PEIP tulevaisuudessa)		PEIP	WWW	sähköposti / tekstiviesti		2. Kiireetön
USVA lähettä VIRVEN yli tiedot STUKiin	Ulkoinen säteilyn valvonta	Yksityinen palvelun tarjoaja	STUK (PEIP tulevaisuudessa)	PEIP	WWW			2. Kiireetön operatiivinen	STUK	250 mittausasemaa
Videokuva	Live tilannekuvan välitys	Yksityinen palvelun tarjoaja	Useita (PEIP tulevaisuudessa)	PEIP			KEJO?	1. Kiireellinen operatiivinen		
Tiepuomit, portit ja liikennevalot operatiivinen	Kunta	Moottoriteiden kauko-ohjattavat puomit		Yksityinen palvelun tarjoaja	Trafi (PEIP tulevaisuudessa)	PEIP	PEKE		KEJO, ERICA	1. Kiireellinen
Liikennevalo-ohjaus	Ajoneuvon paikannukseen perustuva liikennevalo-ohjaus		Yksityinen palvelun tarjoaja	PEIP tulevaisuudessa	PEIP	PEKE		KEJO, ERICA	1. Kiireellinen operatiivinen	Kunta
KETU	Kemikaalituoterekisteri	Yksityinen palvelun tarjoaja	Tukes (PEIP tulevaisuudessa)		www		WWW ?	1. Kiireellinen operatiivinen	Tukes	www.ketu.fi
TOKEVA	Toimintaohjeet vaaarallisten aineiden onnettomuudessa http://www.ttl.fi		Yksityinen palvelun tarjoaja	PeO Varanto/PEIP		ei ole	Paperi	PDF	1. Kiireellinen operatiivinen	Työterveyslaitos
OVA	Onnettomuuden vaaraa aiheuttavat aineet http://www.ttl.fi		Yksityinen palvelun tarjoaja	Työterveyslaitos /PEIP		ei ole	Paperi	PDF	1. Kiireellinen operatiivinen	Työterveyslaitos
Kansainväliset kemikalikortit	http://kappa.ttl.fi/kemikaalikortit/	Yksityinen palvelun tarjoaja	Työterveyslaitos / PEIP		WWW	Ladattava html sovellus		1. Kiireellinen operatiivinen	WHO	
WWW	Julkinen internet	Julkinen internet			www		www	1. Kiireellinen operatiivinen	ei kukaan	

CODEA	Ensihoidon kenttäjärjestelmä	Kuntaverkko	Radioverkko		Sovellus		Sovellus	1. Kiireellinen operatiivinen	Codea Oy	www.codea.fi
MERLOT Mobile	Kenttäjohtamisen järjestelmä (liikkuvassa kalustossa) http://www.logica.fi		Kuntaverkko	Pelastuslaitos		Sovellus			1. Kiireellinen operatiivinen	Logica
MERLOT Office	Valvomojärjestelmä	Kuntaverkko	Pelastuslaitos/PEIP		Sovellus			1. Kiireellinen operatiivinen	Logica	http://www.logica.fi
MERLOT Opto	Operatiivinen toiminta toimintaohjeet ja -muistio http://www.logica.fi		Kuntaverkko	Pelastuslaitos/PEIP		Sovellus			1. Kiireellinen operatiivinen	Logica
MERLOT Medi	Ensihoidon kenttäjärjestelmä	Yksityinen palvelun tarjoaja	HUS / Logica		Sovellus			1. Kiireellinen operatiivinen	Logica	http://www.logica.fi
MERLOT Palotarkastus	Palotarkastusjärjestelmä	Kuntaverkko	Pelastuslaitos / PEIP Varanto		Sovellus			2. Kiireetön operatiivinen	Logica	http://www.logica.fi
E-Beam, Smart Board	Älytaulujärjestelmä tilannekuvan ylläpitämiseen		Kuntaverkko	Pelastuslaitos / PEIP		Sovellus	Älytaulu		2. Kiireetön operatiivinen	useita
Lync, etc. Kokonaisviestintäratkaisut operatiivinen	useita	Unified Communication, chat, pikaviesti, email, mediajako		Kuntaverkko	PEIP		Sovellus	www		1. Kiireellinen
Intranet, extranet	Sisäverkot	Kuntaverkko	Pelastuslaitos / PEIP			Käyttöjärjestelmä ?		2. Kiireetön operatiivinen	useita	
Sosiaalinen media	Sosiaalinen media, Facebook, twitter, Google+, Linked-In… esim. facebook, twitter,vkontakt		Julkinen internet	Useita		www		www	2. Kiireetön operatiivinen	useita
Virve-verkon tilannekuva	Virve-valvomon tilannekuva	TUVE	PEIP (Kejo ?)					2. Kiireetön operatiivinen		
Energiayhtiöiden tilannekuva operatiivinen	Energiaverkon tilannekuva, useita toimijoita useita	Tieto ja Savon Voima Verkko: GridWise-tilannekuvajärjestelmä	Yksityinen palvelun tarjoaja	Useita (reititys tulevaisuudessa PEIP)						2. Kiireetön
Valvontakamerat operatiivinen	Kuntien, yritysten, viranomaisten valvontakamerat useita	CCTV	Kuntaverkko	yksityisiä palvelun tarjoajia PEIP			Sovellus			2. Kiireetön
Kaksisuuntainen hälytysjärjestelmä operatiivinen	ei vielä kukaan?	Itsenäinen, luotettava erillinen hälytysjärjestelmä Järjestelmää ei vielä ole olemassa (tiedossa)		Radioverkko (VIRVE, VHF)	IP PEIP		Sovellus	Mobiilisovellus	Sovellus/mobiili (KEJO?)	1. Kiireellinen
KEJO	Kenttäjohtamisen järjestelmä	TUVE			Sovellus		KEJO	1. Kiireellinen operatiivinen		
TUKA	Turvallisuuskarttapalvelu	TUVE	KEJO		ei ole		KEJO	1. Kiireellinen operatiivinen	ei vielä kukaan	
Wisemaster	Palotarkastusjärjestelmä	Yksityinen palvelun tarjoaja	Tulevaisuudessa Varanto (PEIP)		Sovellus		Varanto ?	2. Kiireetön operatiivinen		
Escape	Vaarallisten aineiden leviämisennusteet ja -mallit			Paikallinen sovellus (PEIP)		Sovellus		Sovellus	2. Kiireetön operatiivinen	Ilmatieteen laitos
HESU / Rescue Planner, STORE, Promeron, etc.	3. Hallinnolliset/Tukipalvelut	Operatiivisen henkilöstön suunnittelu Useita		Kuntaverkko	Pelastuslaitos, tulevaisuudessa Varanto			Sovellus		Sovellus
Virve hallinnointi	Puheryhmien ja laitteiden hallinta, DWS käyttöpaikka		PEIP						3. Hallinnolliset/Tukipalvelut	
Virve puheryhmätallennus	Puheliikenteen audiotallennus	TUVE	ERVE konesali					2. Kiireetön operatiivinen		
Aineistopankki	PEIPissä laitosten yhteinen tiedostojen tallennus ja jako		PEIP	Varanto					2. Kiireetön operatiivinen	

Tiedoston hallinta	Sisäverkon tiedostojen jako ja hallinta	Kuntaverkko	Tulevaisuudessa PEIP					2. Kiireetön operatiivinen	
Varareittijärjestelmä	Tieliikenteen häiriöiden sähköinen varareittijärjestelmä	Yksityinen palvelun tarjoaja		PEIP	WWW		KEJO?	1. Kiireellinen operatiivinen	Trafi
HAKA rekisteri jne. Tuntikirjanpito	Yksityinen palvelun tarjoaja	Agenteq Oy	PEIP	WWW		Varanto ?	3. Hallinnolliset/Tukipalvelut	SPEK	VPKt, nuoriso-osastot
Saku laskutus	Sairaankuljetuksen laskutusjärjestelmä	Kuntaverkko						3. Hallinnolliset/Tukipalvelut	
Kalustorekisteri	Materiaalin hallinta (Ajoneuvot, tarvikkeet, varusteet…)	Kuntaverkko	PEIP ja Varanto		Sovellus	www ?		2. Kiireetön operatiivinen	
KEMU	Tietojärjestelmä vaarallisia aineita sisältävistä laitoksista SM, AVI ja EU valvoo, www.tukes.fi	Yksityinen palvelun tarjoaja	PEIP		www	kemuextra.tukes.fi	KEJO ?	1. Kiireellinen operatiivinen	Tukes
Pronto korvaa tulevaisuudessa	Yksityinen palvelun tarjoaja	PEIP tulevaisuudessa		WWW		Varanto?	1. Kiireellinen operatiivinen	Pelastusopisto	Varanto mahdollisesti
Virve IP viestintä	VIRVE pakettidata (hidas, huono kapasiteetti)	TUVE	PEIP						

LIITE 2: Tarjouspyynnön hankinnan järjestelmävaatimukset

Päätelaitteen vähimmäisvaatimukset

1. Kaksi GSM- modeemia, jotka kykenevät 3G -tekniikkaan. Vähintään toisen modeemeista tulee lisäksi tukea 2G -verkkoa ja toisen LTE -tekniikkaa. Modeemien tulee tukea Suomessa käytössä olevia taajuusalueita, 900, 1800, 2100 ja tulevia, 700-800MHz:n taajuusalueita.

2. Ajoneuvoon asennettavissa, (ruggeroitu) yleiset ajoneuvoasennusta koskevat ympäristövaatimukset, IP65

3. Verkkorajapinnan raja-arvojen määrittely etänä (OTA) tilaajan toimesta (vrt. tietoliikennevuon siirtyminen paremmalle yhteydelle)

4. Ethernet -rajapinta

5. WAN -rajapinta ulkoisille modeemeille

6. Pystyy toimimaan langattoman verkon (802.11b/g) tukiasemana

7. Monikanavareititin tunnistautuu isäntäjärjestelmään saadakseen palvelua

8. Käyttäjästä riippumaton tietoliikenteen salakirjoitus isäntäjärjestelmään

9. Sisäinen tai ulkoinen GPS

10. Etähallittavissa ja etäpäivitettävissä (konfiguraatio ja ohjelmisto)

11. Ulkoiset antennit modeemeille

12. Automaattinen elpyminen toissijaiseen isäntäjärjestelmään ensisijaisen isäntäjärjestelmän vikaantuessa

13. Laitehuoltoon toimitettava laite on asentajan palautettavissa tehdasasetuksille

14. Laite ei lisää merkittävästi mobiilien verkkojen viivettä, viiveen vaihtelua tai pakettihäviötä.

Päätelaitteen lisäominaisuudet (optiot)

1. Neljä yhtäaikaista tietoliikennerajapintaa (esim. 3G, LTE, CDMA, WIFI)
2. Ulkoinen CDMA -modeemi (@450)
3. Ulkoinen tai sisäinen TETRA-modeemi
4. Ulkoinen satelliittimodeemi
5. USB-liitäntä ja siihen kytketyn laitteen virransyöttö (esim. valvontakamera)
6. Päätelaite osaa automaattisesti siirtyä parempilaatuiselle yhteydelle. (vrt. verkko tarjoaa palvelua, sen kapasiteetti ei välttämättä täytä vaatimuksia.)
7. Päätelaite on tietoinen kaikkien tuettujen tietoliikennerajapintojen tilasta samanaikaisesti ja kykenee raportoimaan siitä reaaliaikaisesti hallintajärjestelmään
8. Verkonvaihto ei katkaise tiedonsiirtoa, (vrt. Oper. A to Oper. B) ja mahdollista VPN -tunnelia ei tarvitse uudelleenmuodostaa tietoliikennerajapinnan vaihdon aikana tai sen jälkeen
9. Ohjelmistopohjainen laadunseuranta-agentti (voi olla sisäänrakennettu isäntä- tai hallintajärjestelmään)
10. Useita Ethernet -rajapintoja
11. Pystyy toimimaan langattoman verkon 802.11n tukiasemana
12. Pystyy liittymään langattomaan verkkoon (802.11b/g/n)
13. Ad Hoc / Mesh tyylinen päätelaitteiden välinen liikennöinti isäntäjärjestelmän kautta*
14. Tietovuopohjainen liikenteen kuormanjako useammalle tietoliikennerajapinnalle yhtäaikaisesti (vrt. useamman verkkorajapinnan yhtäaikainen käyttö)
15. Sensori- / ohjauskäyttäjä (RS232 -portti, I/O-portti)
16. Akku/kondensaattorivarmennus lyhyelle (alle 20 s.) sähkökatkokselle
17. IP -liikenteen tunnelointi SDS viesteihin TETRA-modeemin avulla
18. Graafinen käyttöliittymä

19. Tietoliikenteen luokittelu ja priorisointi (laitteeseen sisään tulevaan liikenteeseen, verkon ei oleteta ottavan kantaa liikenteen prioriteettimerkintöihin)

Isäntäjärjestelmän vähimmäisvaatimukset

1. Monikanavareititin tunnistautuu järjestelmään saadakseen palvelua
2. Valvottavissa ja hallittavissa etänä
3. Tietoliikenne kulkee keskitetysti isäntäjärjestelmän kautta
4. Isäntäjärjestelmä kahdennettavissa kahteen tai useampaan laitetilaan.
5. Käyttäjästä riippumaton tietoliikenteen salakirjoitus monikanavareitittimeen

Isäntäjärjestelmän lisäominaisuudet (optiot)

1. SNMP -valvonta
2. Graafinen käyttöliittymä
3. Tietoliikenteen luokittelu ja priorisointi

Hallintajärjestelmän vähimmäisvaatimukset

1. Graafinen käyttöliittymä
2. ilmaisee selkeästi laitteiden tilan kuvan (ja äänen avulla)
3. Tuottaa lokitietoa vikatapauksista
4. Tuottaa lokitietoa laitteen ja siihen kytkettyjen rajapintojen käytettävyydestä, saatavuudesta
5. Konfiguraatiopäivitys päätelaitteeseen (OTA)

6. Ohjelmistopäivitys päätelaitteeseen (OTA)

7. Monikanavareititin voidaan kytkeä pois palvelusta / isäntäjärjestelmästä helposti

Hallintajärjestelmän lisäominaisuudet (optiot)

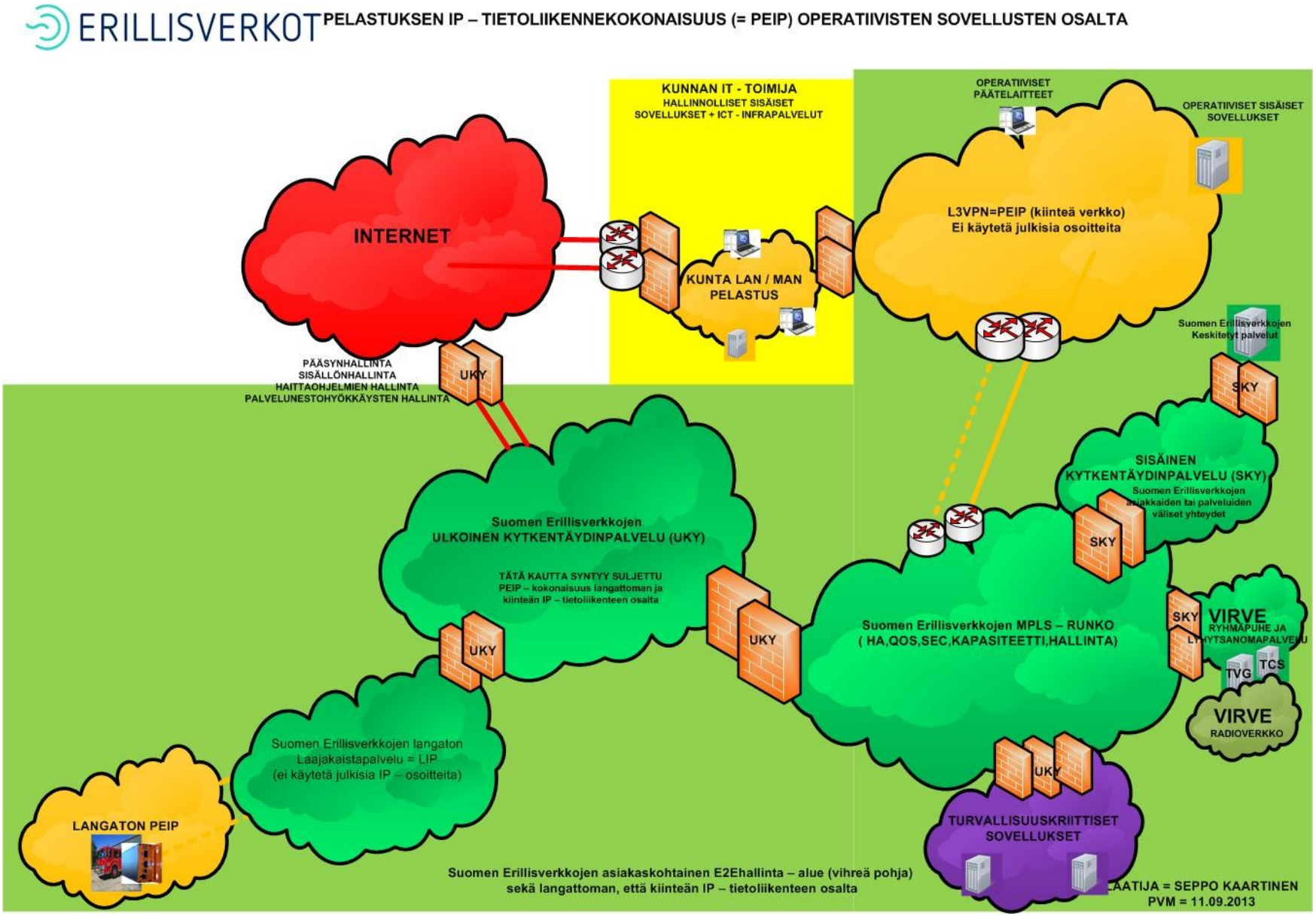
1. Useiden päätelaitteiden (MKR) yhtäaikainen konfigurointi / hallinta

2. Asennettavissa virtuaalipalvelinalustalle

3. SNMP- valvonta

4. Raportointikyvykkyys

5. Tuottaa lokatiotiedolla olevaa lokitietoa

6. Rollback mahdollisuus aiempaan päätelaitteen ohjelmistoversioon

LIITE 3 Langattoman IP -palvelun (LIP) liittyminen muuhun verkkoinfrastruktuuriin