TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Tutkintotyö

Eero Koskiranta

TRANSMISSIOVERKON VALVONTAJÄRJESTELMÄ

Työn valvoja: Yliopettaja, Jorma Punju
Työn ohjaaja: Insinööri, Pekka Ylinikkilä
Tampere 2007

Tekijä: Eero Koskiranta
Työn nimi: TRANSMISSIONVERKON VALVONTAJÄRJESTELMÄ

Päivämäärä: 18.4.2007
Sivumäärä: 27
Hakusanat: transmissio, verkonvalvonta
Koulutusohjelma: Tietotekniikka
Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn valvoja: Jorma Punju, yliopettaja

Työn ohjaaja: Pekka Ylinikkilä, insinööri

Tietoliikenneverkkojen valvontajärjestelmät ovat hyvin merkittävissä rooleissa nykypäiväisissä työympäristöissä. Verkkojen kapasiteettien ja nopeuksien kasvaessa on pystyttävä valvomaan ja hallinnoimaan verkon liikennöintiä. On tärkeätä tietää mitä verkoissa tapahtuu, että voidaan paikallistaa ja sen myötä eliminoida mahdollisesti syntyneet viat.

Järjestelmän myötä verkkojen ylläpidolliset tehtävät ovat huomattavasti helpottuneet ja lisäksi nopeutuneet. Tarkoituksena on, että voidaan hallinnoida verkon jokaista yhteyttä parhaalla mahdollisella tavalla ja sen myötä nopeuttaa tarvittavia huoltotoimenpiteitä. Tärkeintä järjestelmässä on, että työntekijä pääsee itse tutkimaan verkon toimintaa ja hallinnoimaan sitä.

Tässä tutkintotyössä tutkittiin järjestelmän toteuttamismahdollisuudet, suunniteltiin ja rakennettiin valvontaverkko radiopuhelintukiasemien välille. Koko projektin tavoitteena on rakentaa toiminnallinen järjestelmä työympäristön käyttöön tulevaksi. Toimialueellamme sijaitseviin POP:eihin asennettiin tarvittava valvontakortti, joka valvoo kyseisen alueen yhteyksiä. Kaikkiaan kortteja asennettiin kymmenelle eri POP-alueelle, jotka nykyisin tutkivat verkossa tapahtuvaa liikennöintiä. Kortit hälyttävät tarvittaessa käyttäjän tietokoneelle virheistä ja niiden aiheuttamista syistä. Parhaimmillaan yhdellä kortilla voidaan hallita jopa 100 kappaletta POP:eista lähteviä DSL-yhteyksiä.

Tavoitteena oli hyödyntää jo käytössä olevia verkkoja ja niiden laitteistoja. POP:ien väliset yhteydet ovat toteutettu valokaapeliverkoin, verkon kapasiteetti riittää nykypäivän käyttötarpeille. Kuituyhteyksiä hyödyntäen ja virtuaalista lähiverkkoa käyttäen voitiin kyseinen järjestelmä toteuttaa toimivaksi työkaluksi.

Työssä käsitellään tarkoituksellisesti kahta tietoliikenteen osa-aluetta, transmissio- eli siirtojärjestelmäyhteyksiä ja niiden rakennetta ja toimintaa sekä dataverkon yhteyksiä ja sen toiminnallista rakennetta. Ilman näitä kahta osa-aluetta ei olisi verkkoa voitu toteuttaa. Pääpaino työssä kuitenkin on transmissiojärjestelmissä, koska työ tehtiin niiden yhteyksien valvomiselle. Liikennöinti valvontakorteille kuitenkin tapahtuu dataverkon kautta.

Työ koskettaa valtaosin valvontajärjestelmää, jolla siirtoverkkoja hallitaan. Työssä edetään vaiheittain työn etenemisjärjestyksessä eli verkon suunnittelusta aina testaukseen sekä järjestelmän lopulliseen käyttöönottoon.

Verkon rakentaminen kuvataan yhtenä kappaleena, jossa käydään lävitse koko järjestelmän eri asennustoimenpiteet vaihe vaiheelta. Verkon rakenne ja toiminta kuvataan yhdessä, jotta saadaan kuvattu asia lukijalle helpommin ymmärrettävässä muodossa.

Kokonaisen järjestelmän toiminnallinen selostus ja sen muu tekninen dokumentointi jää Tampereen Puhelin Oy:n käyttöön.

TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka, tietoliikennetekniikka

Author: Eero Koskiranta
Title: CONTROL SYSTEM OF TRANSMISSION NETWORK

Date: 18.4.2007
Number of pages: 27
Keywords: transmission, network control
Program: Information technology
Specialization: Telecommunications

Supervisor: Jorma Punju, principal lecturer

Instructor: Pekka Ylinikkilä

The control systems of telecommunication networks are in very significant roles in present-days working environment. It must be possible to control networks traffic when the capacities and speed increase. It is important to know what in the networks takes place so that can be located and the faults which have been possibly created can be eliminated with it.

With the system the maintenance tasks of network have been considerably facilitated and also accelerated. The purpose is that every connection of the network can be governed whit the best way as possible and with it the necessary service operations can be accelerated. In the system it is the most important that the employee is able self to explore the operation of the network and to govern it.

In this thesis the feasibility of the system was examined it was designed and a control network was built between the mobile phone base stations. The objective of the whole project is to build a functional system to come into use of the working environment. The necessary control card which controls the connections of the area was installed in the centre's which are located in our territory. Altogether the cards were installed in ten different centre areas which control the communication in network. The cards give an alarm to the user's computer from the faults and for the reasons caused by them. In the best situation card can be used to command as many as 100 pieces of DSL connections which leaves the centre.

The objective was to utilize networks already in use and their equipment. The connections between the centres are executed with fiber optic cables that the capacity of the network is sufficient to the present-days demands. It was possible utilizing the fiber optic cable connections in question and using a virtual local area network to implement the system in question as a functioning tool.

In the work the two sectors of the telecommunications, the transmission, in other words the transmission system connections and their structure and operation and connections of the data network and its functional structure are intentionally dealt with. It would not have been possible to carry out a network without these two sectors. However, the main stress in the work is in the transmission systems because the work was done their connections for the controlling. The communication to the control cards is performed through the data network.

The work mainly concerns a control system with which the transfer networks are commanded. In the work it is proceeded in progress order of the work phase by phase in other words from the planning of the network to the testing and to the final inauguration of the system.

The building of the network is described as one piece to which the separate installation of the whole system is gone through from the stage to stage. The structure and operation of the network are described together so that a described matter will be obtained to the reader in a more easily understandable form.

The functional commentary of the whole system and other technical documentation stays in the use of Tampereen Puhelin Oy.

ALKUSANAT

Kiitokset Tampereen Puhelin Oy:n henkilökunnalle mahdollisuudesta tehdä tämä tutkintotyö näytteeksi opintojen suorittamisesta työnantajan tarpeiden mukaisesti.

Erityinen kiitos siitä, että tutkintotyön kartoitukseen ja tekemiseen käytetty aika oli joustavaa ja näin ollen työ oli hyvin sopiva opintojen ohessa tehtäväksi.

Kiitokset kuluneista opiskeluvuosista Tampereen ammattikorkeakoulun hallinnolle ja koulutushenkilökunnalle. Teidän kanssanne on ollut ilo ja kunnia tehdä yhteistyötä opintojeni edetessä.

Erityinen kiitos Pekka Ylinikkilälle, Pertti Orsamalle ja Jaakko Lehtimäelle, jotka ovat olleet apuna tämän tutkintotyön teknisen työosuuden ohjauksessa. Lisäksi erityinen kiitos Markku Nymanille ja Jorma Punjulle, jotka ovat olleet apuna kirjoitusasun tarkastuksessa työn ohjaajan, Pekka Ylinikkilän lisäksi.

Tampereella 18. huhtikuuta 2007

Eero Koskiranta

KÄYTETYT TERMIT JA LYHENTEET

Konfiguronti	Asetusten tekeminen
Cisco Pix 501	Cisco Systemsin valmistama palomuuri
IP-Osoite	Internet Protokolla on numerosarja, jonka perusteella IP-paketit löytävät perille Internetissä
Harmaa IP-osoite	Osoitteet, jotka ovat 192.168.0.0 – 192.168.255.255 väliltä
Metro-kytkin	Cisco Systemsin valmistama runkokytkin
WEM	Watson Element Manager Schmid, Telecomin valmistama verkonvalvontaohjelmisto
CMU	Schmid Telecomin valmistama valvonta-agenttikortti käyttäen SNMP-protokollaa
LTU	Schmid Telecomin valmistama linjakortti, joka mahdollistaa neljän SHDSL kupariyhteyden luomisen
DSL	Digital subscriber line, laajakaistainen kupariyhteys
SHDSL	Symmetric High-Bitrate Digital Subscriber Loop, symmetrinen laajakaista-yhteys, joka käyttää kupariyhteyttä
ADSL	Asymmetric digital subscriber line, epäsymmetrinen laajakaistayhteys
SNMP	Simple Network Management Protocol, verkon hallintaprotokolla
PCM	Pulse code modulation, analogisesta signaalista otetaan tasaisin väliajoin näytteitä, jotka ilmaistaan numeerisesti
POP	Toimialueen keskitin
ITU	International Telecommunication Union, Kansainvälinen televiestintäliitto
VLAN	Virtual local area network, virtuaalinen lähiverkko
RS-232	Yleisesti käytetty sarjaliikenneväylän standardi
LED	Light emitting diode, valodiodi

SISÄLLYSLUETTELO

ALKUSANAT iv
KÄYTETYT TERMIT JA LYHENTEET v
SISÄLLYSLUETTELO vi
SISÄLLYSLUETTELO vi
1 JOHDANTO 1
2 TOIMINNALLINEN MÄÄRITTELY 2
2.1 Toimintaperiaate ja työn tavoite 2
2.2 Laitteiston vaatimukset 2
2.3 Toiminnalliset vaatimukset 2
3 VERKON SUUNNITTELU YLEISESTI 3
3.1 Verkon rakenne 3
3.1.1 Dataverkon toteutus valo- ja kuparikaapelein 3
3.1.2 Transmissioverkon toteutus 4
3.1.3 PCM-yhteys 5
3.1.4 SDSL ja SHDSL 5
3.1.5 Watson 5 SHDLS-modeemi 6
3.1.6 Linjakoodauksen perustekniikat 6
3.1.6.1 2B1Q 6
3.1.6.2 QAM 7
3.2 Verkon toiminta 8
3.3 Verkon komponentit 9
3.3.1 Datalaitteet 9
3.3.2 Transmissiolaitteet 9
3.3.3 Ohjelmisto 9
4 VERKON RAKENTAMINEN 10
4.1 IP-osoitteiden määrittely 10
4.2 Palomuurin konfigurointi 10
4.3 Palvelin koneen asentaminen 11
4.4 Valvontaohjelmiston asentaminen 12
4.5 Valvontakorttien asentaminen 12
4.6 Valvontakorttien konfigurointi 13
4.7 Dokumentointi 18
5 OHJELMISTON TOIMINTA 19
5.1 Toimintaperiaate 19
5.2 Hälytykset 21
6 SNMP 23
6.1 SNMP:n toimintaperiaate 23
6.2 Viestien yleinen rakenne 24
6.3 Hälytysryhmä 25
6.4 SNMP:n rajoituksia 25

7 TESTAUS JA KÄYTTÖÖNOTTO 26
8 Päätelmät ja yhteenveto 27
LÄHDELUETTELO 28
LIITELUETTELO 29

1 JOHDANTO

Tämä opinnäytetyö on tehty Tampereen Puhelin Oy:n tarpeisiin syksyn 2006 ja kevään 2007 aikana.

Nykyisin tietoliikenneverkkojen toimivuuteen ja niiden ylläpitoon kiinnitetään huomiota entistäkin tarkemmin, sekä lisäksi verkkojen tuottavuuteen, nopeuksiin ja korjaus toimenpiteisiin. Nopeuksien lisääntyessä myös verkkojen kapasiteetit joutuvat ahtaalle ja vaativat tästä johtuen hyvälaatuisia kaapeleita. Nopean kasvun myötä myös yhteyksien määrät ovat kasvaneet huomattavasti. Ilman valvontajärjestelmää olisi vaikea hallita verkkoa. Yhteyksien määrällinen kasvaminen johtaa myös vikojen valitettavaan kasvuun.

Tarpeiden kasvaessa on myös tarvetta kehittää uusia mahdollisuuksia pysyä tämän päivän teknologian kärjessä, ottaen huomioon asiakaslähtöisyyden. Jos ei ole asiakkaita, ei ole tarvetta kehittää palveluita, eikä myöskään menestyvää liiketoimintaa. Yrityksen tärkeimpänä pääpilarina ovat asiakkaat ja niiden tarpeiden tyydyttäminen. Jos tarjotaan palveluita asiakkaille, on niiden myös toimittava ja tilapäiset viat ovat pystyttävä eliminoimaan mahdollisimman joutuisasti välttäen pitkiä huoltokatkoksia. Kilpailun kasvaessa ja koventuessa on pidettävä huolta asiakkaille tarjottavista tuotteista ja palveluista, jotta saadaan pidettyä heidät tyytyväisinä ja jatkamaan yhteistyötä. Nykyisin palveluntarjoajia on lähes joka alalla useita, mikä antaa asiakkaalle hyvän houkutuksen vaihtaa yritystä paremman palvelun pariin, joka taas lisää paineita pystyä suoriutumaan toiveiden täyttämisistä.

Työn idean yhtenä tärkeänä tavoitteena on juurikin yllä mainittujen tavoitteiden säilyttäminen. Tarkoituksena on päästä hallitsemaan ja ennen kaikkea valvomaan toimialueen transmissio- eli siirtoverkkoja. Näin ollen voidaan nopeuttaa ja tietyllä tapaa helpottaa mahdollisien vikojen korjaamista. Järjestelmän myötä päästään työpaikan verkosta seuraamaan liikennöintiä parhaalla mahdollisella tavalla tietokoneen välityksellä, ja pystytään korjaamaan mahdollisia vikatapauksia etähallinnan kautta.

Yrityksen tuottavassa liiketoiminnassa on otettava tarkasti huomioon taloudelliset varat ja niiden käyttökohteet. Järjestelmän myötä viat, jotka voidaan korjata hallintaohjelmiston kautta, säästää kuluja turhien polttoainekustannuksien ja työaikojen osalta merkittäviä määriä.

Tutkintotyössä kuvataan valvontajärjestelmäverkon suunnittelu, toteutus ja sen toiminta.

2 TOIMINNALLINEN MÄÄRITTELY

2.1 Toimintaperiaate ja työn tavoite

Järjestelmä tulee valvomaan transmissio- eli siirtoverkkojen yhteyksiä matkapuhelinten käyttämien tukiasemien välille. Siirtojohtona on käytössä tavallinen 2/2 Mbit/s kuparijohto. Tämän työn tarkoituksena on rakentaa valvontaverkko, jota voidaan hallita yrityksen sisäverkosta sekä vähentää ja helpottaa työkustannuksia. Valvontalaitteisto ja ohjelmisto ovat Schmid Telecomin (Schmid) valmistamia tuotteita. Ohjelmistolla voidaan valvoa kaikkia sen toimialueen siirtojohtoyhteyksiä, joihin valvontalaitteistot on asennettu.

Mahdollisien vikojen sattuessa ohjelma hälyttää kyseisistä ongelmista ja niiden aiheuttamista syistä. Valvontakortit, jotka asennetaan POP:eihin, ovat Schmidin valmistamia CMU-SNMP-agenttikortteja. Niitä asennetaan kymmeneen eri POP:iin ympäri toimialuetta. Palvelinkoneen pystyttäminen on myös yksi osa-alue, jonka kautta kortit kommunikoivat keskenään. Tietoturvariskin välttämiseksi on palvelinkone suojattava haitalliselta liikennöinniltä, joten myös palomuurin konfigurointi kuuluu osana tähän työhön. Kaiken tämän lisäksi työhön kuuluu myös paljon muuta suunnittelua, sekä rakentamista että testausta, joihin paneudutaan vielä syvällisemmin tulevissa luvuissa.

2.2 Laitteiston vaatimukset

1. Järjestelmä on yhteensopiva Windows-käyttöjärjestelmän kanssa.
2. Järjestelmä on yhteensopiva vanhan valvontaohjelmiston kanssa.
3. Järjestelmä voidaan käyttää samanaikaisesti eri toimialueiden sisäverkoista.

2.3 Toiminnalliset vaatimukset

1. Järjestelmä toimii itsenäisesti ilman erillisiä toimenpiteitä.
2. Järjestelmä hälyttää mahdollisista vioista ja ilmoittaa niiden mahdolliset syyt.
3. Järjestelmä voidaan ohjata ja valvoa tietokoneen välityksellä.
4. Laitteistolla voidaan selvittää mahdollisien vikojen syyt.
5. Laitteiston kaikkia ominaisuuksia voidaan muuttaa myös etäältä, kuten itse paikaltakin.
6. Laitteiston on toivuttava mahdollisista katkoksista (esim. sähkökatkos) itsenäisesti.

3 VERKON SUUNNITTELU YLEISESTI

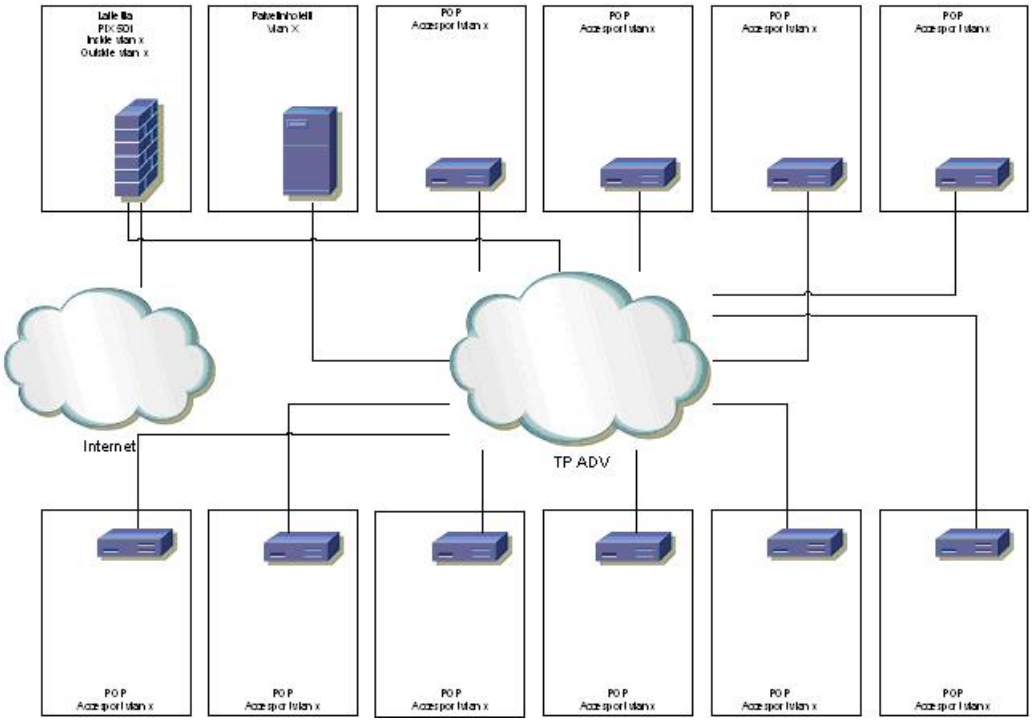
Luvussa 3 käsitellään yleisesti valvontaverkon suunnitteluun liittyviä seikkoja ja sitä millaisia asioita on otettava huomioon sellaista verkkoa rakennettaessa. Aluksi tarkastellaan hieman, millainen on kyseisen verkon rakenne ja miten se on päätetty toteuttaa. Lisäksi katsotaan vielä verkon toiminallista puolta eli sitä millaiseen käyttöön tätä verkkoa käytetään ja minkälaisilla komponenteilla kyseinen verkko on varustettu.

3.1 Verkon rakenne

3.1.1 Dataverkon toteutus valo- ja kuparikaapelein

Rakenteeltaan verkko hyödyntää jo käytössä olevia verkkoja ja niiden ominaisuuksia, joten tälle työlle ei ole varsinaisesti rakennettu omaa fyysistä verkkoa. Transmissioverkkoa hallinnoidaan Tampereen Puhelin Oy:n data-verkon kautta. Kaapeleina käytetään sekä valokaapeleita että kuparikaapeleita. Karkeasti jaotellen, pitkillä matkoilla hyödynnetään valokuitua ja kuparia taas lyhemmillä ja hitaammilla yhteyksillä.

Verkon niin sanottu sydän tai keskipiste sijoittuu palvelinhuoneeseen ja sen kokonaisuuden ympärille, missä serveri ja palomuuri sijaitsevat. Sen kautta kulkeutuu verkon kaikki liikenne, ilman sitä verkko ei voisi toimia. Kuvassa 1 on esitetty verkon fyysinen rakenne.



Kuva 1. Valvontaverkon rakennekuva

Kuvasta 1 nähdään, miten kaapelointi on suoritettu verkossa. Kuvan keskellä oleva pilvi kuvaa työpaikan sisäverkkoa, josta on ainoastaan pääsy palvelimelle kahden muun puhelinyhtiön lisäksi. Yhteys sisäverkosta palvelimelle on toteutettu valokaapeliyhteydellä. Toimiston ja palvelinhuoneen molemmissa päissä ovat metrokytkimet, jotka muuntavat kuituyhteyden Ethernet-yhteydeksi joka sopii täten tietokoneisiin. Yhteys palvelinhuoneessa sijaitsevaan palomuuriin tuodaan runkokytkimestä normaalilla Ethernet-johdolla, josta yhteys jatkuu samaisen kytkimen kautta palvelimelle. Kuvassa 1 olevat 10 POP-laatikkoa kuvaavat paikkoja, joihin valvontakortit on asennettu. Yhteydet jokaiseen POP:iin on rakennettu valokaapeliyhteyksillä. Yhteys palvelinhuoneesta siirtyy suoraan POP:iin lukuun ottamatta muutamia yhteyksiä, jotka kierrätetään toisen POP:in kautta. Valokaapelit on päätetty POP:eissa sijaitseviin runkokytkimiin. Runkokytkimistä yhteys valvontakortille tuodaan Ethernet- eli lähiverkkokaapelia pitkin. Omistajayhtiöiden sisäverkkoihin yhteydet kulkevat valokuidussa, missä yhteys muunnetaan runkokytkimen kautta kupariyhteydeksi, ja siitä se jaetaan kytkimien kautta sisäverkkoon.

3.1.2 Transmissioverkon toteutus

Kuten aiemmin on kuvattu, transmissio- eli siirtoverkoilla tarkoitetaan tukiasemien välisiä yhteyksiä. Yhteydet tällaisessa verkossa kuljetetaan normaalisti kuparikaapelein. Tämä työ koskee juuri tällaisen verkon valvomista ja hallintaa, mutta jotta voitaisiin valvoa kyseistä verkkoa, tarvitaan fyysinen dataverkkokin jota aiemmassa luvussa käsiteltiin. Sen verkon kautta valvotaan tätä verkkoa. Transmissio on kuitenkin aivan oma lukunsa eikä sitä voida rinnastaa dataverkkoon.

Luvussa 4.5 kerrotaan hieman POP:eissa sijaitsevista transmissiolaitteista valvontakorttien asennusten yhteydessä. Jokaisessa popissa, johon CMU-kortti on asennettu, löytyy myös Schmidin kehikko, jossa kortti on kiinni. Kehikkoon mahtuu valvontakortin lisäksi 12 kappaletta LTU- eli linjakorttia, joista DSL-yhteys muodostetaan tukiasemalle. Yhteen korttiin mahtuu maksimissaan 4 yhteyttä, joten kehikossa voi olla käytössä parhaimmillaan 48 DSL-yhteyttä. Yhteyksien määrä riippuu myös siitä käytetäänkö yhtä- vai kahta kaapeliparia. Yhdellä CMU-kortilla voidaan hallita kahta Schmidin kehikkoa, joten kehikon ollessa täynnä voi valvottavia yhteyksiä olla jopa 100 kappaletta.

Linja- eli LTU-kortin yhteys toteutetaan kuparisella SHDSL-yhteydellä. Yhteys eroaa tavallisesta kotikäyttöisestä ADSL- eli laajakaistayhteydestä siten, että SHDSL-yhteys on symmetrinen, joten nopeudet molempiin suuntiin ovat samansuuruiset. Yhteyden saapuessa tilaajalle on siellä vastassa SHDSL-modeemi, joka luo symmetrisen yhteyden. Nopeutta voidaan muuttaa mutta normaalisti nopeusluokkana käytetään suurinta 2/2Mbit/s.

3.1.3 PCM-yhteys

PCM eli pulssikoodimodulaatio on yksi sähköisistä menetelmistä, jolla voidaan koodata ääni-informaatiota. Siinä analogisesta signaalista otetaan tasaisin väliajoin näytteitä, jotka ilmaistaan numeerisesti. Näytteen taso voidaan ilmaista joko lineaarisesti tai logaritmisesti.

Digitaalisessa puhelinverkossa käytettävä PCM-koodaus on määritelty ITU:n suosituksessa. Euroopassa käytettävä *A-law* on logaritminen, sen näytteenottotaajuus on 8000 hertsiä ja kussakin näytteessä on 8 bittiä. Näytteiden logaritmisuus laajentaa dynamiikkaa 36 dB:iin saakka. Tärkein syy erilaisiin näytteenottolakeihin oli runkoverkossa käytetty linjakoodaus, joka toimii erittäin huonosti, jos lähetettävänä on pelkkiä nollia.

Nyquistin teoreeman mukaan taajuuksia, jotka ovat korkeampia kuin puolet näytteenottotaajuudesta ei saada tallennettua, joten 8000 hertsin näytteenottotaajuudella voidaan tallentaa teoriassa korkeintaan 4000 hertsin taajuuksia. Käytännössä raja kulkee 3400 hertsissä.

Perinteisessä PCM:n määritelmässä äänisignaalia voidaan käsitellä ennen sen digitoimista, mutta pakattu digitaalinen ääni ei enää ole PCM-muodossa. PCM:stä on monia muunnelmia, jotka nykyaikainen äänenpakkaus on paljolti syrjäyttänyt. Sellaisia ovat mm. differentiaalinen PCM (DPCM) ja adaptiivinen DPCM (ADPCM).

3.1.4 SDSL ja SHDSL

SDSL tarjoaa symmetrisen tiedonsiirron samoilla nopeuksilla kuin HDSL. Erona on, että SDSL käyttää vain yhtä kupariparia, kun HDSL tarvitsee niitä kaksi tai kolme (poikkeuksena HDSL-II). SDSL:n maksimi toimintaetäisyys on noin 7 km. Transmissioverkoissa käytetään kahta johdinparia, joten sen vuoksi meidän käytössämme on ainoastaan SHDSL-yhteyksiä.

SDSL mahdollistaa äänen ja datan siirron samaan aikaan samassa siirtotiessä, joskaan perustoteutuksessa tämä ei yleensä ole mahdollista. SDSL käyttää linjakoodaukseen 2B1Q-tekniikkaa. Sen vuoksi äänen ja datan siirto samanaikaisesti on mahdollista ainoastaan, jos käytetään jakosuodinta. Symmetrisen luonteensa vuoksi SDSL on luonteva valinta sovelluksiin, joissa dataa siirtyy molempiin suuntiin suunnilleen yhtä paljon. Yksi mahdollinen käyttökohde SDSL:lle voisivat olla videoneuvottelut. Pienten käyttöönottokustannusten ansiosta SDSL on varteen otettava vaihtoehto myös kodeissa ja pienissä yrityksissä. Yksi suosittu SDSL:n käyttökohde ovat kiinteistöliittymät. Niissä hyödynnetään taloyhtiön sisällä olevaa tavallista puhelinverkkoa. Kiinteistöliittymän runkoliittymä on kytketty ulkomaailmaan SDSL-tekniikalla. SDSL-tekniikkaa ei ole kansainvälisesti standardoitu.

Symmetriseen tiedonsiirtoon on edelleen kehitetty myös nopeampi SHDSL-tekniikka (Symmetric High-Bitrate Digital Subscriber Loop). SHDSL käyttää siirtotienä yhtä kupariparikaapelia nopeudella 2,3Mbps. Käytettäessä kahta kupariparia päästään nopeuteen 4,6 Mbps. SDSL:aan verrattuna SHDSL käyttää kehittyneempää TC-PAM-linjakoodausta (Trellis-Coded Pulse Amplitude Modulation) ja on paremmin yhteensopiva muiden DSL-tekniikoiden kanssa. Käyttämänsä taajuusalueen vuoksi SHDSL ei mahdollista äänen siirtoa samanaikaisesti datan kanssa. SHDSL on standardoitu kansainvälisesti standardissa ITU-T G.991.2. Lisäksi ovat olemassa ANSI:n ja ETSI:n standardit Pohjois-Amerikalle ja Euroopalle. /1/

3.1.5 Watson 5 SHDLS-modeemi

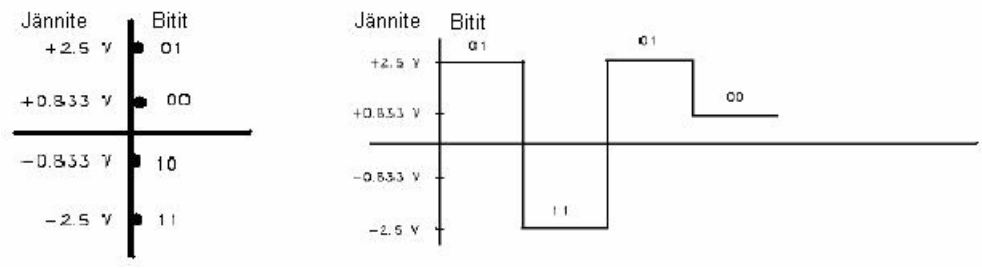
Tässä työssä transmissioverkon toisessa päässä eli tukiasemalla sijaitsee SHDSL-modeemi, joka muuntaa PCM-yhteyden SHDSL-yhteydeksi. Tampereen Puhelin Oy:n käyttämät transmissiolaitteet ovat Schmidin valmistamia tuotteita, kuten tämä Watson 5 laitekin. Modeemi on mallinimeltään Watson 5, ja se mahdollistaa 2/2Mbit/s symmetrisen nopeuden. Alla on kirjattu modeemin tärkeimpiä teknisiä tietoja. /2/

- 1, 2 tai 4 kupariparia
- Linjaimpedanssi 135 Ohm
- Linjaliitin RJ-45, 8 pinniä
- E1 2MBit/s 2.048kBit/s ± 50ppm; HDB3; G.704 transparent
- Paikallinen sarjaporttimonitorointi V.24/V.28, 9.600 Baud, VT100 terminaaliyhteys
- Watson Element Manager + SNMP Agent CMU-kortti
- NTU Kaukosyöttö jänteen yli tai paikkallisyöttö ulkoisen jännitelähteen avulla
- LTU-kortti saa virran kehikosta: 48 VDC
- Minirack LTU: 48VDC tai 220VAC IEC230

3.1.6 Linjakoodauksen perustekniikat

3.1.6.1 2B1Q

2B1Q (2-Binary-1-Quarternary) on yksinkertainen linjakoodausmenetelmä, jota käytetään eräissä DSL-tekniikoissa ja niiden edeltäjässä ISDN:ssä. 2B1Q on nelitasoinen koodi, joka esittää kaksi bittiä yhdellä jännitetasolla kuvan 2 mukaisesti. Lisäksi kuvassa 2 on esimerkki signaalista, jolla esitetään bittijono 01110100.

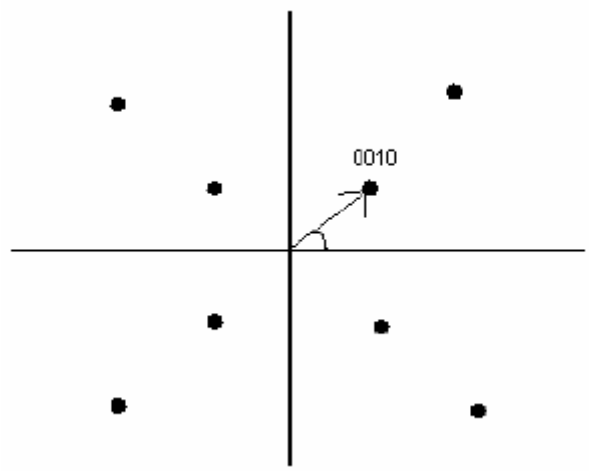


Kuva 2. 2B1Q-jännitetasot ja esimerkki 2B1Q-linjakoodauksen käytöstä

Käytettäessä 2B1Q-linjakoodausta ääntä ja dataa ei voida siirtää samanaikaisesti, koska koodausmenetelmä varaa koko kaistan. 2B1Q-tekniikkaa käytetään HDSL- ja SDSL-tekniikoissa (Single line Subscriber Line). /1/

3.1.6.2 QAM

QAM-linjakoodaus muistuttaa 2B1Q:ta sikäli, että myös siinä useita databittejä koodataan jokaiseen linjalle lähetettyyn symboliin. Muuta yhteistä tekniikoilla ei juuri olekaan. Kun 2B1Q-koodauksessa moduloidaan vain signaalin jännitetasoja, QAM moduloi sekä signaalin amplitudin että vaihekulman. Kuvan 4 koordinaatistossa on esitetty eräs QAM-toteutus. Kaaviosta käytetään nimitystä QAM constellation eli QAM-kuvio. Kukin piste edustaa tiettyä bittijonoa (esim. 0001, 0011, 0100 jne.). Signaalin amplitudi ja vaihe muodostavat vektorin, joka määrittää tietyn pisteen. Amplitudi määrittää kuinka kaukana origosta piste on. Vaihekulma määrittää kuinka suuressa kulmassa ollaan koordinaatiston x-akseliin nähden. Koska kaikkien 4-bittisten kombinaatioiden esittäminen vaatii 16 pistettä, kuvan 4 QAM-kuviosta voidaan käyttää nimitystä 16-QAM.



Kuva 3. Esimerkki QAM-kuviosta

Linjalla, jolla esiintyy vain vähän häiriöitä, voitaisiin käyttää huomattavasti tiheämpää QAM-kuviota, jossa amplituditasoja olisi paljon enemmän ja vaihekulmien välillä olisivat pienemmät erot. QAM-vastaanottimet voivat mukautua taustakohinan ja häiriöiden

aiheuttamiin haittoihin päättämällä, käytetäänkö suurta vai pientä määrää amplitudi- ja vaihetiloja. /1/

3.2 Verkon toiminta

Verkon toiminnassa käydään lävitse, miten valvontayhteys kulkeutuu POP:ista käyttäjän koneelle ja millaisien laitteiden läpi yhteys viedään. Luvussa 3.1 kerrottiin verkon rakenteellisuudesta, joka pohjusti toiminnallista puolta, kuten millaisissa kaapeleissa yhteydet kulkevat eri POP:ien, laitteiden ja käyttäjien välillä. Tässä luvussa keskitytään enemmänkin data-verkon toimintaan, koska valvontajärjestelmää hallitaan kyseisen verkon kautta.

Aluksi otetaan yhteys yrityksen sisäverkkoon, josta on sallittu pääsy palvelinkoneelle. WEM-2-ohjelmiston avulla päästään käsiksi valvontajärjestelmään. Jos kaikki sujuu moitteetta, on yhteys käyttäjällä nyt auki. Tieto käyttäjän koneelta lähtee yrityksen sisäverkon kautta reitittimelle tai tässä tapauksessa kytkimelle. Siitä tieto siirtyy toiselle kytkimelle, josta käytetään nimitystä metro- eli runkokytkin. Runkokytkimessä kuparikaapeliyhteys muunnetaan valokaapeliyhteydeksi, sitten matka jatkuu valokuidussa toiselle samanlaiselle metrokytkimelle, joka sijaitsee palvelinhuoneistossa. Yhteys tässä vaiheessa tulee kyseisen kytkimen inside- eli sisääntulo-puolelle, josta tieto siirretään VLAN:in kautta toiselle metrokytkimelle. Tämän jälkeen yhteys kytketään ristikytkennän avulla palvelinkoneelle. Palvelinkoneelta yhteys jatkaa valokaapelin välityksellä POP:iin jossa valvontakortit sijaitsevat. POP:in päässä on vastassa myös metrokytkin josta yhteys kytketään valvontakortille lähiverkkokaapelin avulla. Jokaiseen POP:iin yhteys ei kulje suoraan palvelinhuoneesta vaan saattaa kiertää jonkun toisen POP:in kautta, mutta pysyy kuitenkin samaisessa VLAN:issa. Periaatteessa verkko on samanlainen kuin tavallinen lähiverkko mutta toimii virtuaalisena lähiverkkona. Tieto käyttäjältä valvontakortille pysyy koko ajan VLAN:in sisällä joten verkko ei kommunikoi lainkaan ulkoverkon kanssa, jos yhteysväli on ainoastaan käyttäjä ja CMU-kortti. Kahden muun puhelinyhtiöiden liikennöinti verkossa tapahtuu samalla lailla paitsi palvelinhuoneelta yhteys jatkaa yhtiöiden omaan sisäverkkoon valokuidun välityksellä.

Verkosta on mahdollisuus päästä ulkomaailman eli Internetiin, mutta silloin yhteys kiertää palomuurin kautta. Sisäverkosta ulospäin liikennöintireitti kulkee seuraavasti. Kun tieto sisäverkosta siirtyy valokaapelilla runkokytkimelle, on yhteys määritelty metrokytkimen inside-porttiin. Kytkimelle on konfiguroitu kaksi porttia tätä järjestelmää varten, inside- eli sisääntulo-portti ja outside- eli ulostulo-portti. Siihen on myös määritelty molempien porttien omat VLAN:it, jotta yhteys kulkeutuu oikeaan paikkaan. Kytkimen inside portista tieto siirtyy palomuurin inside puolelle. Tässä vaiheessa palomuuri varmistaa että sille on sallittu päästää kyseinen IP-osoite sisään. Sen jälkeen tieto lähtee palomuurin outside-puolelta ulos ja jatkaa matkaa takaisin samaiselle metro-kytkimelle outside-porttiin. Ulostulo-portista tieto jatkaa matkaansa maailmalle eli internetiin. Ulkoverkosta tultaessa

tieto kulkee samaa reittiä pitkin mutta pysähtyy palomuuriin, koska sillä estetään kaikki ulkopuolinen liikennöinti verkon sisälle. Transmissioverkon toiminta POP:ista tukiasemalle on melko yksinkertainen. Tieto linjakortilta lähtee tukiasemalle 2/2 Mbit/s-yhteytenä, joka voidaan viedä joko kuparikaapelissa tai valokaapelissa. Yhteys kierrätetään POP:in läpi, jossa suoritetaan ristikytkentä haluttuun tukiasemakohteeseen. Tieto kulkee POP:ista tukiasemalle SHDSL-yhteytenä. Kuten aiemmissa luvuissa jo kerrottiin, SHDSL-modeemina käytetään myös Schmidin valmistamaa tuotetta.

3.3 Verkon komponentit

Seuraavassa käydään lävitse kaikki verkon komponentit. Nämä kaikki alla olevat komponentit esiintyvät verkon rakenteessa yllä mainittuun tapaan. Laitteet on jaoteltu datalaitteisiin ja transmissionlaitteisiin.

3.3.1 Datalaitteet

Datalaitteet ovat seuraavat:

- Cisco Catalyst 6500 Metro-kytkin /Liite 3/
- Cisco Catalyst 2960 Metro-kytkin /Liite 2/
- Cisco Pix 501 palomuuri /Liite 2/
- Pentium 4, 512Mb, Windows XP palvelinkone /Liite 3/

3.3.2 Transmissiolaitteet

Transmissiolaitteet ovat seuraavat:

- Schmid CMU-SNMP agentti-kortti /Liite 1/
- Schmid LTU-linjakortti /Liite 2/
- Schmid kehikko /Liite 2/
- Schmid Watson 5 SHDSL modeemi

3.3.3 Ohjelmisto

Ohjelmistot ovat seuraavat:

- Schmid WEM-2 server
- Schmid WEM-2 client

4 VERKON RAKENTAMINEN

Neljännessä luvussa käydään läpi vaihe vaiheelta, miten verkon rakentaminen on edennyt ja mitä kaikkea on otettava huomioon kyseistä järjestelmää rakennettaessa. Asiat etenevät loogisessa järjestyksessä työn asennusvaiheen suhteen. On hyvin tärkeätä tällaista työtä tehtäessä jaksottaa eri vaiheet, jotta työ etenisi mahdollisimman joustavasti ongelmitta välttäen. Alla olevissa luvuissa 4.1 - 4.6 perehdytään tarkemmin ja syvällisemmin, miten työ on edennyt vaiheittain.

4.1 IP-osoitteiden määrittely

Työn alkuvaiheessa täytyi hankkia jokaiselle valvontakortille oma IP-osoite, joita kaikkiaan oli 20 kappaletta. Valvontakortteja asennettiin aluksi vain 10 kappaletta mutta myöhemmin kun verkko laajenee, niin loput IP-osoitteet ovat valmiina käytettäviksi. IP-osoitteet valittiin tietystä osoiteavaruudesta, ja ne olivat harmaita osoitteita. Osoitteet olivat 20 peräkkäistä osoitetta. Näin ollen osoitteiden paikallistaminen oli helppoa suunnitella, kun vierekkäiset osoitteet määriteltiin vierekkäisille POP-paikoille. Harmaat osoitteet jaettiin POP-alueiden mukaisesti siten että lähellä toisiaan olevat POP:it saisivat vierekkäiset osoitteet. Niin meneteltiin siksi, että on entistä helpompi hahmottaa verkkoa, kun osoitteet eivät ole aivan sekaisin.

Tietoturvariskin vuoksi korttien osoitteet valittiin harmaiksi eikä julkisiksi. Näin ollen jokaisella kortilla on yksi harmaa osoite, johon ei pääse kiinni muualta kuin kolmen puhelinyhtiön verkosta. POP-alueiden kasvaessa valvontaverkkoa laajennetaan luultavasti ympäri toimialuettamme.

Pelkästään harmailla osoitteilla ei tietenkään voida julkista verkkoa tehdä, vaan tarvitaan myös julkisia osoitteita. Käytännössä olisi riittänyt jopa yksikin julkinen osoite, mutta tässä kohdassa tulevat myös vastaan tietoturva-asiat, joten tarvittiin vielä yksi osoite lisää. Kaiken kaikkiaan kahdella julkisella osoitteella tullaan toimeen. Ensimmäinen julkinen osoite tarvitaan palvelinkoneelle jotta voidaan ottaa yhteys ensinnäkin siihen. Nykyäänhän ei voida julkisia palvelimia jättää ilman mitään suojauksia, joten tarvitaan jonkinlainen palomuuri. Näin ollen toinen julkinen osoite tarvitaan palomuurin käyttöön, jotta voidaan estää haitallinen liikennöinti.

4.2 Palomuurin konfigurointi

Palomuurina on Ciscon Pix 501, joka on ominaisuuksiltaan monipuolinen palomuuri. Palomuuriin ohjelmoitiin, kuten yllä mainittiin, toinen julkisista osoitteista, johon voidaan ottaa yhteys työpaikan sisäverkosta. Sen lisäksi estettiin kaikki muu liikennöinti palomuurille ulkoverkosta, paitsi kolmen puhelinyhtiön sisäverkon osoitteet, joita ovat Tampereen Puhelin Oy, Pohjois-Hämeen Puhelin Oy sekä Ikaalisten-Parkanon Puhelin Oy. Näiden kolmen yrityksien verkosta voidaan valvoa ja hallinnoida verkkoa. Pohjois-

Hämeen Puhelin Oy ja Ikaalisten-Parkanon Puhelin Oy hallinnoivat transmissioverkkoa Tampereen Puhelin Oy:n sisäverkon kautta. Fyysinen yhteys palomuurille toteutettiin 10/10Mbit/s nopeuden yhteydellä. Palomuurissa on NAT- toiminto päällä, jolla julkinen IP-osoite jaetaan harmaiksi osoitteiksi. Siten Pix 501 reitittää julkisen IP:n harmaiksi osoitteiksi, mikä myös johtuu täysin tietoturvariskeistä, ja näin ollen ei tarvitse kuluttaa useita julkisia osoitteita turhaan. Palomuurille määritellään kaikki kymmenen CMU-kortin IP-osoitteet ja palvelinkoneen harmaa osoite. Tämän lisäksi Ciscon Pix 501:een tarvitsee määritellä kaksi VLAN:ia, jotta yhteys voidaan luoda ja toteuttaa metro-kytkimelle. Metro-kytkimeltä kytketään suoraan liitäntäjohto palomuuriin kiinni. Palomuurissa on inside- ja outside-portit eli sisääntulo ja ulostulo. Molemmat portit tarvitsevat oman VLAN:it ja ne pitää määritellä palomuurille. Yhteys sisäverkosta tulee palomuurin inside-puolelle POP:in metro-kytkimestä ja kiertää PIX:in läpi ja tulee outside-puolelta, siitä yhteys jatkaa ulkoverkkoon eli Internetiin.

4.3 Palvelin koneen asentaminen

Kun IP-osoitteet on saatu jaettua ja palomuuri konfiguroitua, niin voidaan alkaa asentaa palvelinkonetta kuntoon. Valvontaohjelmisto WEM ei vaadi suorituskyvyltään mahdottoman tehokasta konetta, joten koneeksi voidaan valita aivan tavallinen nykyaikainen tai jopa muutaman vuoden vanha kone. Tärkeimpiä laitteistovaatimuksia ovat muistinmäärä ja prosessorin tehokkuus sekä jäähdytys, jotta kone ei kuumene liikaa, kun laitteisto sijaitsee palvelinkaapissa. Tosin palvelinkaappi, johon tämä kone tuli on varustettu asiallisin tuulettimin, jotka ovat pitäneet lämpölukemat normaaliarvoissa.

Kun palvelinta eli serverikonetta alettiin rakentaa, niin vastaan tuli muutamia ongelmia. Tarkoituksena oli ensin rakentaa toimiva kone vanhoista ylijääneistä palvelinkoneista. Kone rakennettiin kolmesta eri koneesta, joista yhdistettiin toimivat komponentit, kuten muistit, kovalevy, virtalähde, cd-asema ynnä muut tarvittavat komponentit. Mikään näistä koneista ei toiminut suoraan, vaan jouduttiin vaihtamaan komponentteja useaan kertaan koneiden välillä, kunnes lopulta oli löydetty kaikki toimivat osat. Tämän jälkeen kone lähti toimimaan vallan mainiosti minkä jälkeen voitiin siirtyä käyttöliittymän asennukseen. Käyttöliittymänä käytetään Windows XP Pro-ohjelmistoa sillä tiedettiin sen toimivan jo entuudestaan kyseisen WEM-ohjelmiston kanssa. Ohjelmistona olisi voitu käyttää muidenkin valmistamia käyttöliittymiä, mutta käyttäjäystävällisen ympäristön myötä päädyimme Windowsiin.

Sitten alkoikin tulla vastaan ongelmia kun XP:n asennus ei suostunut toimimaan mitenkään, vaan jumittui aina tietyllä asennushetkellä. Tutkittaessa vikaa huomattiin, että vika oli palvelinkoneen kovalevyssä, joka oli osittain vioittunut. Kun vika oli saatu paikallistamisen jälkeen korjattua, niin XP saatiin asennettua moitteetta koneeseen. Tästä päästyä voitiin asentaa valvonta eli WEM-2-ohjelmisto koneelle. Ohjelmiston asennus

puolestaan sujui moitteetta ja saatiin verkko näkyville. Viat eivät loppuneetkaan tähän, vaan kun muutaman päivän ylhäällä olon jälkeen huomattiin, että sammui aika-ajoin.

Lopulta päädyttiin että uuteen palvelinkoneeseen, jollainen sattui löytymään yrityksestä käyttämättömänä. Tämän myötä viat loppuivat kerralla ja saatiin lopulta toimiva palvelinkone, joka on nyt luotettava. Kone on tälläkin hetkellä käynnissä ja valvoo verkkoa ympäri vuorokauden.

Varsinaisen palvelinkoneen asentaminen verkkoon ei vaadi suuria toimenpiteitä alkuvaikeuksistaan huolimatta. Palomuurilta tuodaan yhteys palvelinkoneelle metrokytkimien kautta. IP-osoitteeksi valittiin kahdenkymmenen harmaan osoitteen joukosta ensimmäinen, eli pienin selkeyden vuoksi. Samainen osoite määriteltiin myös palomuurille. Serverikoneelle määriteltiin kiinteä IP-osoite, joka oli myös samainen harmaaosoite. Sen jälkeen palvelin liitettiin verkkoon, jonka jälkeen siihen voitiin ottaa ensimmäinen testiyhteys.

4.4 Valvontaohjelmiston asentaminen

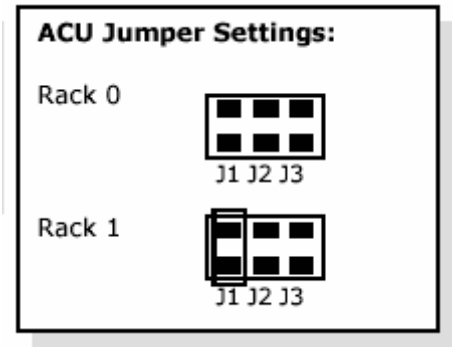
Kun yhteys on saatu kuntoon serverille asti yrityksien sisäverkosta, päästään asentamaan valvontaohjelmisto. Valvontaohjelmistona käytetään Schmidin valmistamaa WEM (Watson Element Manager)-valvontaohjelmistoa. Tämä hallintaverkko toteutettiin uudemmalla WEM-2-ohjelmistolla. Palvelin koneelle asennetaan WEM-2-server eli serverikoneelle tarkoitettu ohjelmisto, joka valvoo ja jonka kautta valvotaan verkkoa. Käyttäjän koneelle asennetaan WEM-2-client, eli käyttäjälle tarkoitettu ohjelmisto, jolla varsinaisesti päästään valvomaan ja konfiguroimaan verkkoa ja sen asetuksia. Client-ohjelmiston asennus suoritettiin koneisiin, joilla voidaan ottaa yhteys yrityksen sisäverkosta. Myöskään tämä ohjelmisto ei vaadi suurenmoisia laitteistovaatimuksia. Asennus tapahtuu normaalisti kuten muillekin Windows-koneille. Kun ohjelmisto on asennettu onnistuneesti, päästään ottamaan yhteys palvelimelle ja testaamaan liikennöintiä. Valvontakorttien asennuksen jälkeen pystytään ottamaan jokaisen POP:in korttiin yhteys ja muuttamaan kyseisen kortin asetuksia läpikotaisin mitä voidaan myös paikanpäällä tehdä.

4.5 Valvontakorttien asentaminen

CMU-kortit asennetaan Schmidin valmistamaan kehikkoon jotka sijaitsevat POP:issa. Kehikkoon voidaan asentaa kaiken kaikkiaan 13 korttia, joista CMU-kortille on varattu paikka 12. Yhdellä CMU:lla voidaan hallita kahta Schmidin kehikkoa, joten yhdellä kortilla voidaan hallita kaikkiaan 25 LTU-korttia. Yhteen LTU-korttiin mahtuu maksimissaan neljä DSL-yhteyttä riippuen yhteyksien nopeuksista sekä käytetäänkö yhtä- vai kahta kaapeliparia. Kaikkiaan valvontakortilla voidaan hallita yhteensä 100 yhteyttä. Kehikko on standardi 19 tuuman laitekaapin levyinen, jolloin se on helppo asentaa tavalliseen laitekaappiin. CMU-kortti ottaa käyttöjännitteensä 48V kehikostaan suoraan kun kortti

työnnetään kehikkoon. Kehikolle sähkö tuodaan tavallisesti suoraan tasasuuntaajalta sulakkeen kautta.

Kehikossa sijaitseva ACU-kortti, eli ohjainkortti sijaitsee CMU-kortin oikealla puolella. Sen kautta päästään hallitsemaan kaikkien korttien asetuksia sarjaliikenneväylän kautta. ACU-kortilla on jumpperilla määriteltävät asetukset, jotka on oltava oikeassa asennossa kortin toiminnan kannalta. Jos asennettavia Schimin kehikoita on vain yksi kappale, jumperointiin ei tarvitse koske. Asentaakseen toisen kehikon rinnalle, tarvitsee jumperointia muuttaa. ACU-kortilla on kuvan 4 mukainen jumperointi, rack 0 tarkoittaa ensimmäistä kehikkoa, rack 1 toista kehikko. Rack 1:n nastat J1 täytyy kytkeä yhteen jotta saadaan molemmat kehikot toimimaan.



Kuva 4. ACU-ohjainkortin jumperointi asetukset /4/

Kun kortti on saatu kiinni paikkaan 12, kytketään kortille datayhteys. Jokaisessa POP:issa on metrokytkin, josta datayhteys tuodaan oikean VLAN:in kautta kytkimelle. Kytkimen vapaaseen porttiin on konfiguroitu tätä järjestelmää varten automaattisesti hakeva nopeus, joka asettuu 100/100Mbit/s, josta saadaan data-yhteys kortille. Kortille yhteys kytketään suoralla lähiverkko johdolla.

4.6 Valvontakorttien konfigurointi

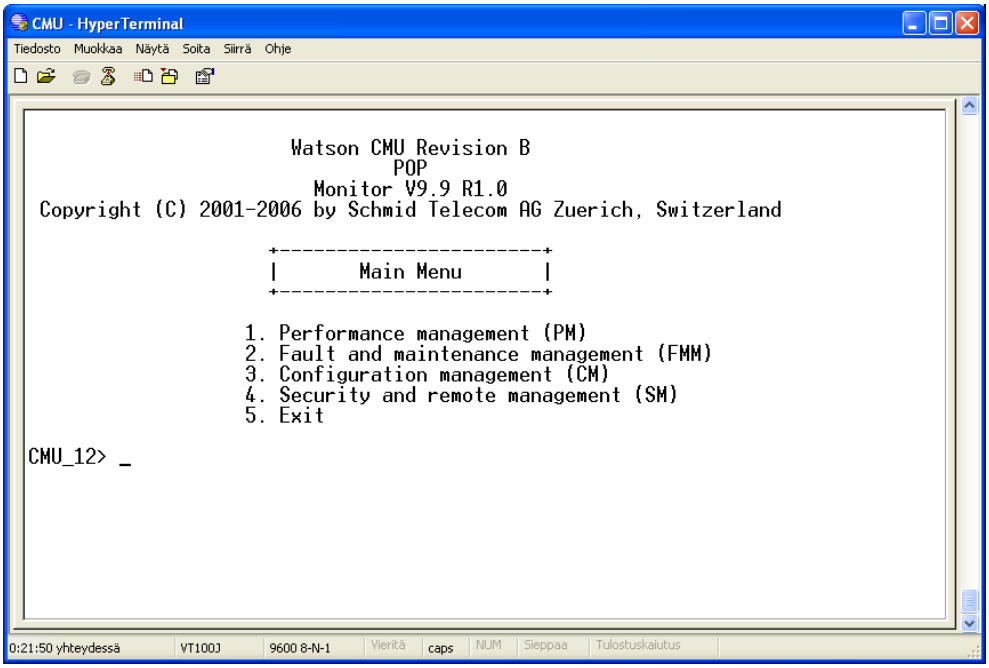
Seuraavaksi katsotaan miten CMU-kortit konfiguroidaan kun ne ovat saatu asennettua paikalleen. Korttien täytyy olla kiinni kehikossa ja sähköjen päällä, jotta korttiin voidaan ottaa yhteys. Korttia konfiguroidaan kehikon 13.sta korttipaikasta kuten muita kehikon kortteja, menemällä sarjakaapelilla kiinni RS 232 väylään jossa lukee ”monitor”. Korttiin otetaan yhteys normaalilla telnet -yhteydellä (esim. hyperterminal-ohjelmistolla). Ohjelmiston käynnistymisen yhteydessä täytyy asettaa seuraavat ominaisuudet kohdalleen jotta yhteydenotto kortille onnistuu:

- Bittejä sekunnissa: 9600
- Databittejä: 8
- Pariteetti Ei mitään

- Stopbittejä 1
- Vuonohjaus Ei mitään

Asetuksien määrittelyn jälkeen avautuu tyhjä ruutu terminaaliohjelmasta. Näppäilemällä tunnuksen %12 päästään kirjautumaan sisään kehikon 12. korttipaikkaan, jossa CMU sijaitsee. Muuttamalla %-merkin perässä olevaa numeroa päästään kirjautumaan halutulle kortille, esimerkiksi %4 kirjautuisi kortille 4, jossa sijaitsee LTU-kortti. Tämän jälkeen avautuu ruudulle CMU-kortin päävalikko, josta voidaan valita halutut toimenpiteet valintanäppäimin 1-5. Seuraavassa on kuvattu päävalikon erilaiset toimenpiteet:

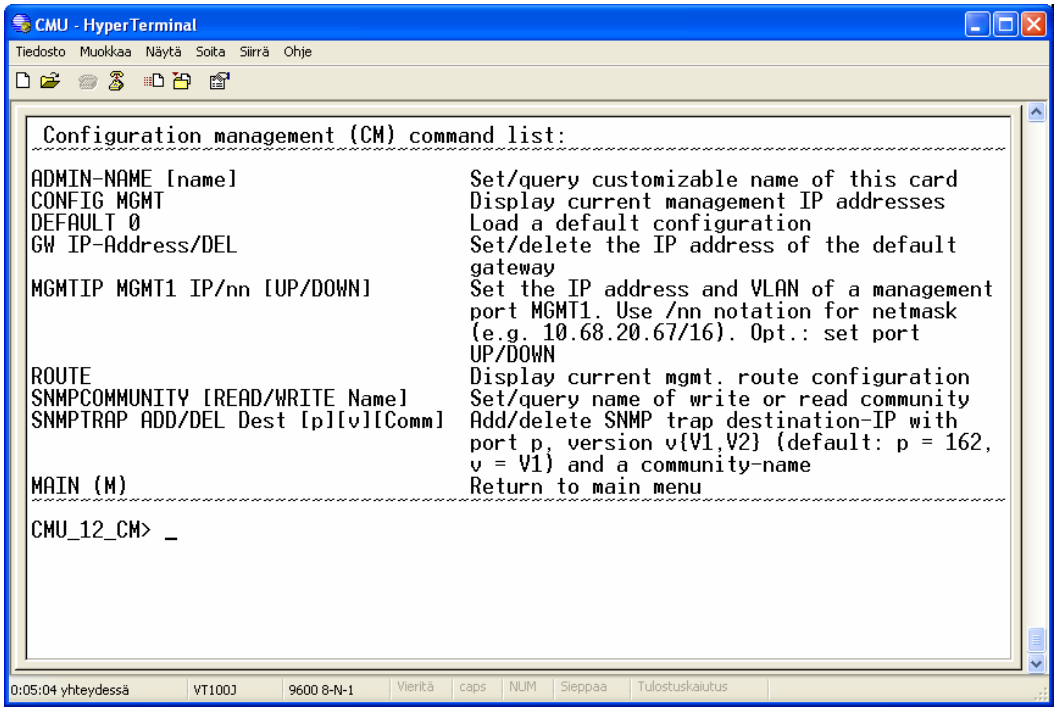
1. Suorituskyvyn hallinta
2. Virheiden ja ylläpidon hallinta
3. Asetusten hallinta
4. Hälytysten hallinta
5. Lopeta



Kuva 5. CMU-kortin päävalikko näkymä

Kuvassa 5 on CMU-kortin päävalikon näkymä, josta päästään kortin eri toimenpiteisiin. Toiseksi ylimmälle riville voidaan asettaa POP-alueen nimi. Päävalikossa voidaan aloittaa

kortin konfigurointi. Valikkoihin päästään sisään näppäilemällä sen valikon numero ja Enter. Kaiken kaikkiaan kortille ei tarvitse asettaa muuta kuin POP-alueen tiedot, yleisesti ottaen paikan nimi sekä tarvittavat IP-osoitteet. Valikosta 1 (suorituskyvyn hallinta) saadaan muutettua paikan tiedot oikeiksi, tässä työssä käytettiin selkeyden vuoksi POP:in nimiä. Lopulta päästään hyödyntämään luvussa 4.1 käsiteltyjä IP-osoitteita. Valikkoon 3 saadaan asetettua myös IP-osoitteet sen POP-alueeseen kuuluviksi osoitteiksi, jotka aiemmin ovat jo määritelty. Kortille määritellään kaksi harmaata osoitetta, jotka ovat kortin osoite sekä palvelimen osoite. Tämä lisäksi asetetaan vielä kortin aliverkonpeite ja yhdyskäytävä.



Kuva 6. Valikon 3 toiminnot

Kuvassa 6 on valikon 3 kaikki toiminnot, joilla kortin asetukset saadaan tehtyä oikeiksi. Tämän työn kaikki tarvittavat tiedot asetettiin valikossa 3. Seuraavaksi käydään läpi kortin konfigurointi vaihe vaiheelta kunnes kortti on valmis käytettäväksi. Kaarisulkuihin on merkitty tämän esitystavan selkeyttämisen vuoksi asetettavat tiedot. Oikeassa konfigurointitilanteessa tietoja ei kirjoiteta kaarisulkujen sisälle. Tekstin syöttöön käytetään normaalisti isoja kirjaimia, tarvittaessa pienet kirjaimet saadaan kirjoittamalla sana lainausmerkkien sisälle.

1. Kortin nimeäminen:

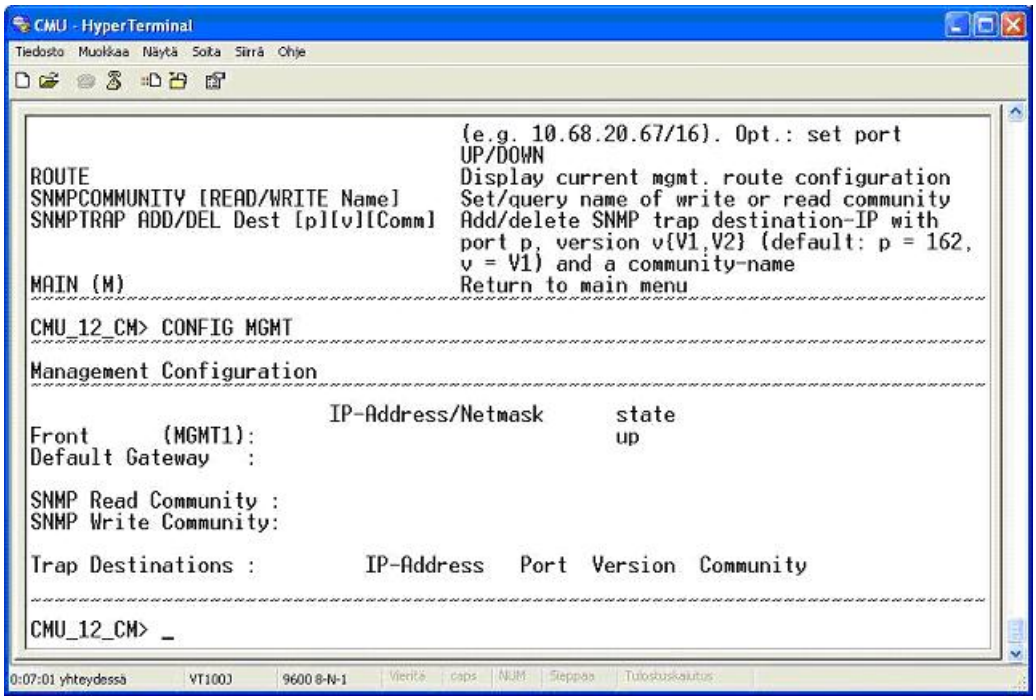
    - ADMIN-NAME (POP:IN NIMI)

2. Kortin IP-osoitteen sekä aliverkonpeitteen (netmask = nn) määrittäminen

    - MGMTIP MGMT1 (XXX.XXX.XXX.XXX/nn)

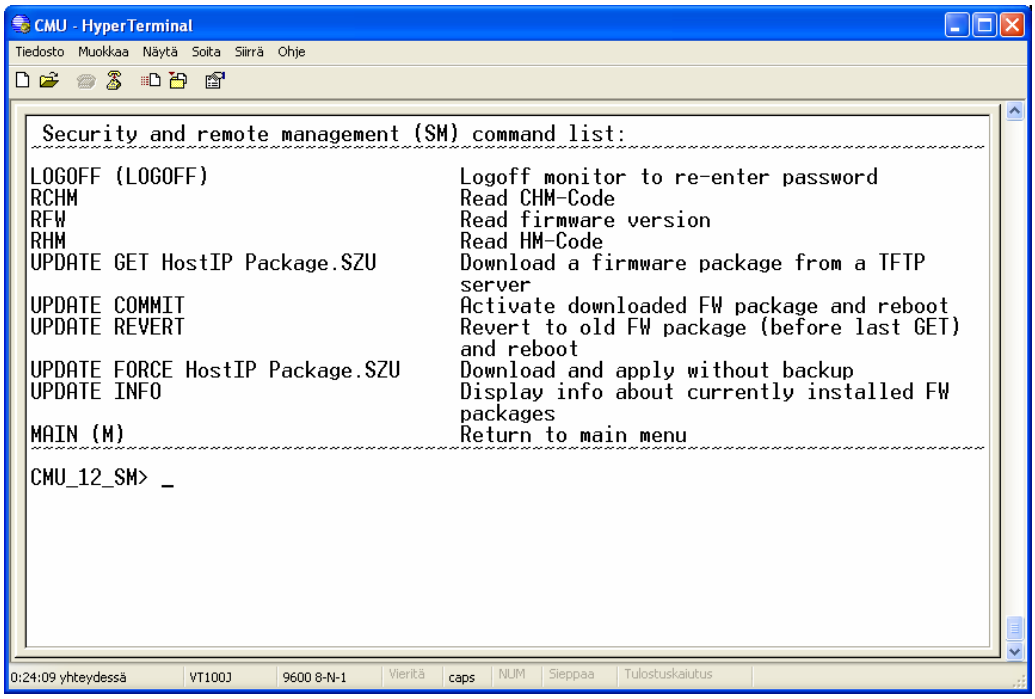
3. Kortin yhdyskäytävän määrittäminen
    - GW (XXX.XXX.XXX.XXX)
4. Palvelinkoneen IP-osoitteen määrittäminen
    - SNMPTRAP ADD (XXX.XXX.XXX.XXX)
5. SNMP-yhteyden asettaminen
    - SNMPCOMMUNITY READ ”(kirjoitetaan pienillä)”
    - SNMPCOMMUNITY WRITE ”(kirjoitetaan pienillä)”

Asetukset tallentuvat automaattisesti muistiin heti kun muutos on tehty. Erillistä tallennuskomentoa kortilla ei lainkaan ole. Varmuuden vuoksi voidaan poistua kortilta ja mennä uudelleen valikkoon 3 ja tarkistaa että asetukset ovat varmasti jääneet muistiin.



Kuva 7. Näkymä konfiguroinnin hallinnasta

Kuvasta 7 voidaan tarkastella, että konfigurointi on onnistunut, eikä virheitä ole sattunut. Yllä olevaan toimintoon päästään valikon 3 takaa näppäilemällä teksti: CONFIG MGMT. Lyhenne tulee suomennettuna sanoista asetusten hallinta. Tässä tilassa on kätevä tarkistaa, että kaikki asetukset ovat menneet oikein. Kuvan 7 valikkoon tulee näkyviin kaikki äskettäin tehdyt muutokset. Kun tiedot ovat tarkistettu oikeiksi, kortti on saatu konfiguroitua onnistuneesti.



Kuva 8. Valikon 4 toiminnot

Kuvassa 8 näytetään mitä valikon 4 takaa löytyy. Tässä työssä ei tarvinnut koskea näihin asetuksiin millään lailla. Pääsääntöisesti täältä valikosta tehdään kortille tarvittavat päivitykset. Lisäksi voidaan muuttaa kortin ohjelmistoa esimerkiksi uudempaan. Korttien asennusvaiheessa ei ollut saatavilla uudempaa ohjelmistoa tai muitakaan päivityksiä, joten keskityttiin ainoastaan vain kortin asetusten tekemiseen.

Kaiken tämän jälkeen kortti on valmis testattavaksi. Nyt päästään ottamaan ensimmäinen testiyhteys kortille. Yhteyttä kortille ei voida testata suoraan pingaamalla eli lähettämällä paketteja IP-osoitteeseen, koska osoitehan on harmaa, jota ei voida pingata. Luvussa 7 käsitellään tarkemmin korttien testausta ja verkon käyttöönottoa.

Ennen järjestelmän varsinaista käyttöönottoa on laitteistoa testattava huolella. On kokeiltava kuinka se suoriutuu työympäristössä, ja onko se valmis jokapäiväiseen käyttöön. Parhaitenhan se tulee testatuksi, kun se otetaan suoraan käyttöön mutta kuitenkin testimielessä, jotta osataan varautua ennalta arvaamattomiin ongelmiin ja sen myötä niiden eliminointiin.

Kun kaikki CMU-kortit olivat saatu asennettua onnistuneesti eri puolille POP-saluetta, niin päästiin vihdoin kokeilemaan lopullisesti järjestelmää ja sen tuomia ominaisuuksia. Ensin kokeiltiin ottaa yhteys palvelimelle työpaikan sisäverkosta ja saada palvelin näkyviin WEM-2-ohjelmistossa. Kun pienien vaikeuksien jälkeen tämä oli suoritettu ja saatu liikennöinti pelaamaan serverille asti oli vuorossa korttien testaus sillä korttien liikennöinti tapahtuu serverin kautta. Kortit saatiin näkyviin ohjelmistossa mutkitta ja liikennöinti alkoi toimia. Kun

kaikkien POP:ien yhteydet olivat testattu toimiviksi, eikä ongelmia esiintynyt, niin oli enää viimeisen vaiheen aika ennen varsinaista käyttöönottoa.

4.7 Dokumentointi

Nykypäivänä dokumentointia tarvitaan lähestulkoon kaikessa yritystoiminnassa. Ilman sitä on lähes mahdotonta toimia monissakaan työtehtävissä. Ilman arkistointia monien asioiden hoitaminen tuottaisi turhia ja ylimääräisiä tunteja, jotka voidaan välttää hyvällä ja täsmällisellä kirjanpidolla. Monesti arkistointi tahtoo jäädä tekemättä, ja näin ollen vaikeuttaa työtehtäviä jatkossa.

Myös tässä valvontaverkon rakennuksessa täytyy dokumentoida asiat. Kaikki mitä kappaleessa 4 on käsitelty ja aikanaan tehty, on täytynyt merkata talteen. Ilman niitä tietoja olisi vaikeata lähteä korjaamaan vikoja, esimerkiksi missä POP:issa mikäkin IP-osoite on ja mitä yhteyksiä POP:ista lähtee maailmalle.

Se, miksi tässä luvussa käsitellään dokumentointia ja sen merkityksellisyyttä, johtuu siitä että WEM-2 ohjelmisto kaikkien teknillisten ominaisuuksien lisäksi on myös hyvä dokumentointijärjestelmä. Kun varsinainen fyysinen työ oli suoritettu ja testattu että yhteydet ovat kunnossa ja päästään jokaiseen CMU-korttiin kiinni niin sen jälkeen suoritettiin dokumentointi. Ohjelmistoon kirjataan ylös jokaisen LTU-kortin jokainen DSL-yhteys. Aikasemmin puhuttiin että yhteen LTU-korttiin saadaan maksimissaan neljä yhteyttä, joten nämä kaikki kirjataan talteen. Kun kaikki yhteydet ovat kirjattu talteen, silloin on helppo tarkistaa ohjelmasta missä POP:issa, millä kortilla ja missä portissa ovat kyseiset yhteydet. Vaikka tämä järjestelmä on tarkoitettu käytettäväksi valvomista ja hallintaa varten, voidaan siihen dokumentoida yhteydet kätevästi, josta on helppo ja vaivaton tarkastaa tarvittavat dokumentit. Yhteyksien kasvaessa ohjelmistoon on helppo lisätä sekä poistaa tietoja ja näin ollen kirjanpito pysyy selkeänä ja ajan tasalla.

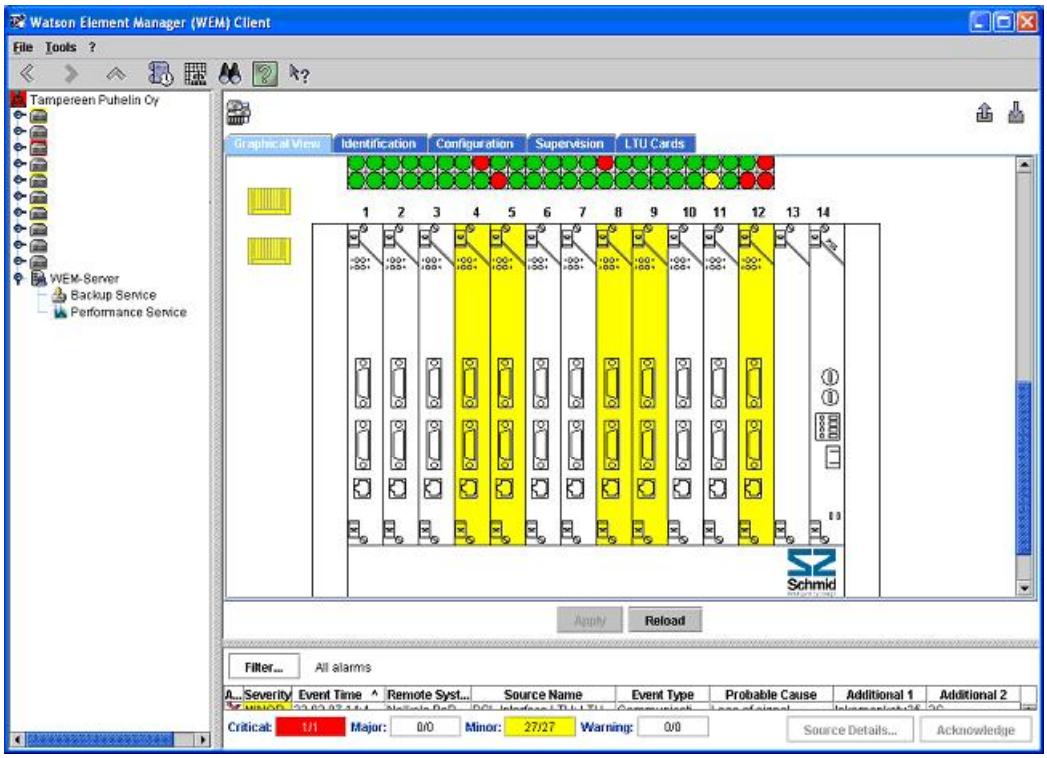
5 OHJELMISTON TOIMINTA

Valvontaverkon valmistuttua työnkuva muuttui hyödyllisempään suuntaan, välttämättä aina ei tarvitse lähteä paikanpäälle tutkimaan ja paikallistamaan vikaa, koska nyt liikennöintiä voidaan seurata työpisteeltä. Näin ollen voidaan välttää turhia edestakaisia työmatkoja POP:eille ja säästää matkakustannuksissa sekä työajassa. Vian ilmettyä voidaan ohjelmiston avulla saada alustavaa tietoutta millaisesta viasta mahdollisesti olisi kyse ja miten vika tulisi eliminoida. Joskus vian korjaus saattaa hoitua esimerkiksi pelkällä kortin uudelleen käynnistämisellä, jos kortti on mahdollisesti mennyt jumiin. Tällaisissa vikatöissä voidaan säästää yllättävän paljon aikaa ja näin ollen myös rahaa. Tietenkään ohjelmisto ei ole mikään robotti, joka pystyisi korjaamaan kaikkia vikoja etähallinnan kautta. POP:ien väliset puhelinjohdot ovat vuokrajohtoja, joten niiden ylläpitotehtävät eivät kuulu Tampereen Puhelin Oy:n toimenkuvaan. Valvontajärjestelmällä pystytään todentamaan kaapeliviat vuokranantajalle, jotka hoitavat viat itse kuntoon.

Tämän alustuksen jälkeen voidaankin syventyä hieman tarkastelemaan mitä kaikkea kortilla voidaan valvoa ja hallita. Lisäksi katsotaan, miltä ohjelmisto näyttää ja miten ohjelmisto ilmoittaa mahdollisista vioista ja niiden syistä.

5.1 Toimintaperiaate

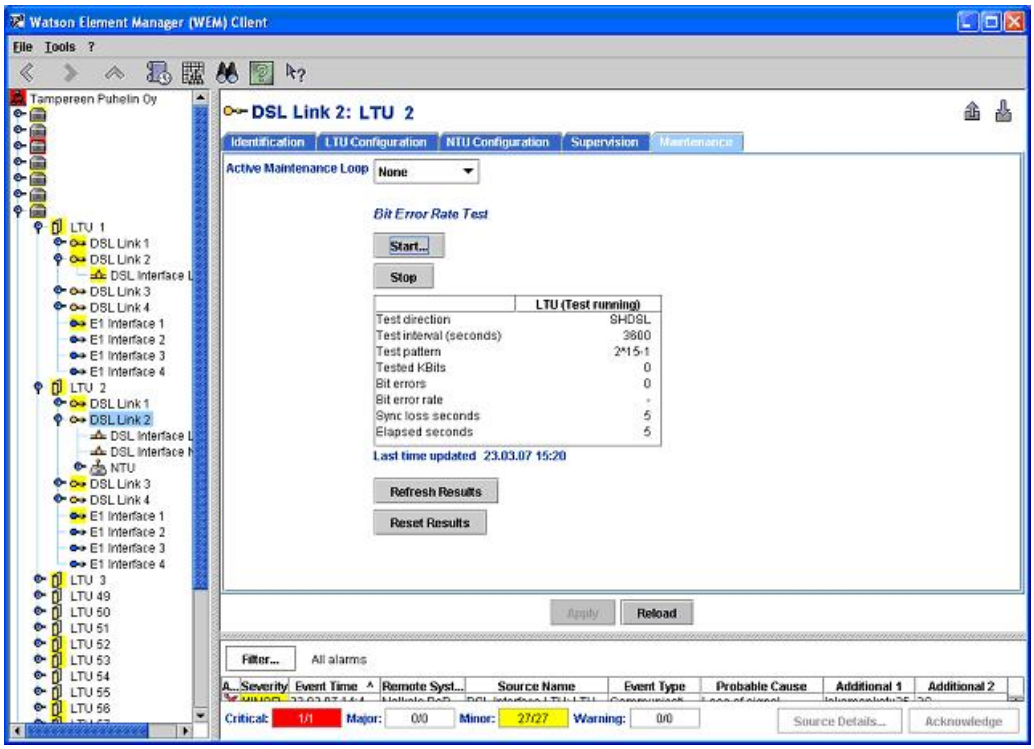
Kuvassa 9 on esitetty graafinen kuva satunnaisen POP:in Schmid-kehikosta. Ohjelmistolla voidaan käytännössä katsoen tehdä kaikki samat operaatiot kuin paikanpäältäkin. Erona ohjelmistossa on se, että siinä on graafinen käyttöliittymä joka helpottaa ja havainnollistaa paremmin laitteistoa. Kuvassa 9 näkyy samanlainen näkymä kuin POP:issakin, 12. korttipaikka on varattu valvontakortille ja paikat 1-11 sekä 13 linjakorteille. Vasemmalla näkyy palvelinkoneen tiedot WEM-2 server sekä yläpuolella kaikki 10 POP:ia joissa CMU-kortit ovat asennettu paikoilleen. Yhteyden ollessa kunnossa POP:iin asti, saadaan yhteys poimittua valikkoon. Korttien näyttäessä punaista, on yhteydenotossa jotain häiriötä. Voidaan havaita että kolmas kortti ylhäältä näyttäisi olevan punaisella joten siihen poppiin ei yhteys jostain syystä ole kunnossa. Klikkaamalla kehikossa näkyvää korttia, päästään tutkimaan kortin sisälle yhteyksien tiloja ja niiden ominaisuuksia.



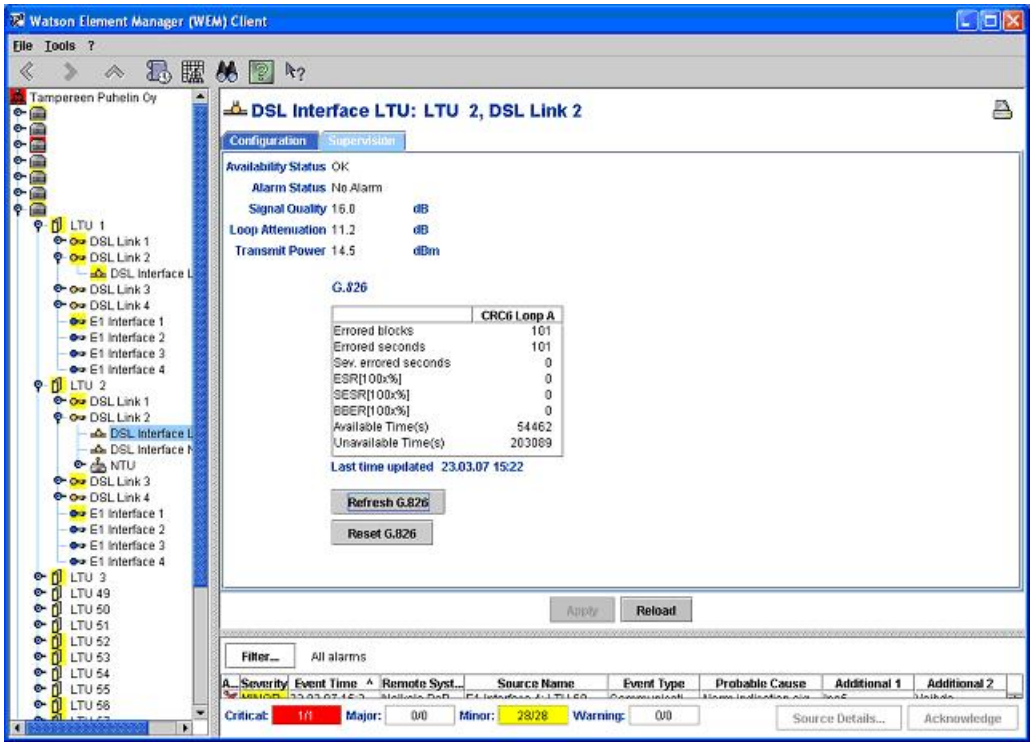
Kuva 9. Graafinen näkymä Schmidin kehikosta

Kuvassa 10 on menty satunnaiseen korttiin kiinni. Ylhäältä nähdään että kyseessä on DSL Link 2: LTU 2 eli toisen linjankortin toinen yhteys. Tässä tilassa voidaan esimerkiksi testata kyseisen yhteyden linja-arvoja tekemällä (Bit Error Rate Test) testi. Vasemmalla reunassa näkyy poppien alla olevat LTU-kortit ja niiden jokaisen alla DSL-yhteydet. Jokaisessa kortissa on neljä yhteyttä, kuten aiemmin jo mainittiin kyseisestä asiasta. Tarvittaessa kyseinen yhteys voidaan katkaista ohjelmiston avulla jos kortti on vaikka mennyt jumiin.

Kuvassa 11 on mitattu samaisen linjakortin kaapeliarvot. Ohjelma mittaa kaapelin signaalikohina suhteen eli miten paljon kaapelissa esiintyy häiriöitä joka ilmoitetaan desibelisenä arvona. Ohjelma näyttää myös linjan vaimennusarvot eli kuinka paljon kaapelissa kulkeva signaali vaimenee tilaajan ja linjakortin välillä desibeleinä. Lisäksi mitataan vielä signaalin voimakkuus kaapelissa joka ilmoitetaan dBm-arvona. Linja-arvojen mennessä raja-arvojen alapuolelle, ilmoittaa ohjelmisto kaapelien huonolaatuisuudesta. Lisäksi voidaan tarkastella mm. jaksonaikana tapahtuneita virheitä sekä sekunnissa tapahtuneita virheitä. Tästä valikosta voidaan linja resetoida eli ns. käyttää linja alhaalla ja käynnistää se uudelleen.



Kuva 10. Virheiden testaus kaapelille



Kuva 11. DSL-yhteyden mitatut kaapeliarvot

5.2 Hälytykset

Aikaisemmin kerrottiin että WEM-2:n graafisesta käyttöliittymästä on hyötyä selkeyden vuoksi. Hälytyksissä voidaan havaita graafisuuden kätevyys ja selkeys. Jos verkossa

ilmenee jotain vikaa, niin ohjelmisto hälyttää vioista eri väreillä riippuen kuinka kriittinen vika on kyseessä. On helppo havaita ongelmat jos joku yhteyksistä on muuttunut esimerkiksi punaiseksi. Eri hälytysvärejä on yhteensä neljä, jotka muuttuvat vikojen mukaan. Seuraavassa käydään lävitse eri värit ja niiden tärkeys asteet.

- Punainen tarkoittaa kriittistä vikaa
- Oranssi ilmaisee merkittävää vikaa
- Keltainen tarkoittaa merkityksetöntä vikaa
- Valkoinen ilmaisee kaikkien olevan kunnossa

Ohjelmistohan valvoo verkkoa eli toisin sanoen kupariyhteyksiä, joten yleisesti ottaen hälytykset johtuvat transmissioverkosta eli kaapeleista, mutta muitakin mahdollisia vian syitä voi olla. Alla olevaan listaan on merkattu yleisimmät viat, joista ohjelmisto voi hälyttää:

- Huonojen kaapeleiden takia häiriöt kasvavat liian suuriksi.
- Ulkoisten rasitusten takia kaapeli on mennyt poikki.
- Linjakortti on jumittunut tai hajonnut
- SHDSL modeemi on jumittunut tai hajonnut

Näiden lisäksi voi tietysti olla sellaisia vikoja joista ohjelmisto ei pysty hälyttämään, kuten:

- WEM-palvelin on kaatunut
- CMU-kortti on hajonnut
- Data liikennöinti ei toimi CMU-kortille

Kuvassa 9 linjakorttien yläpuolella olevat pallot kuvaavat kortilla olevia ledejä jotka merkkaavat kortilla olevien yhteyksien tilaa. Esimerkiksi neljännen kortin toinen yhteys on punaisella joten silloin yhteydessä saattaa olla jotain vikaa tai kyseinen paikka voi olla tyhjä jolloin siellä ei kulje mitään liikennettä.

6 SNMP

SNMP (Simple Network Management Protocol) on tämän hetken yleisin verkonhallintaprotokolla. Se on suunniteltu yksinkertaiseksi, helposti toteutettavaksi verkonhallintatyökaluksi verkon komponenttien hallintaan. Termi SNMP viittaa joukkoon verkonhallintastandardeja, jotka kuvaavat itse protokollan (SNMP, Simple Network Management Protocol), hallintatietokantojen määrittelyn (MIB, Management Information Base) sekä joukon tieto-olioita (SMI, Structure of Management Information). SNMP on hyvin keskeinen osa-alue tämän valvontaverkon toiminnan kannalta. WEM-2-ohjelmisto ilmoittaa palvelimen kautta käyttäjän koneelle verkon tapahtumista. /3/

6.1 SNMP:n toimintaperiaate

TCP/IP-verkonhallintamallissa on neljä perusosaa:

- Hallinta-asema (Management station)
- Hallinta-agentti (Management agent)
- Hallintatietokanta (Management Information Base, MIB)
- Verkonhallinan yhteyskäytäntö (Network-management protocol)

Hallinta-asemassa ajetaan verkonhallintajärjestelmää, jonka avulla voidaan suorittaa tiedon analysointia, vioista toipumista jne. Kyseiseen järjestelmään kuuluu myös ohjelmisto varsinaista verkon valvontaa ja hallintaa varten. Verkonhallintaohjelmistoon on toteutettu myös tietokanta, jossa voidaan säilyttää ja käsitellä hallittavista laitteista saatua tietoa.

Hallinta-agentti on ohjelma, joka on toteutettu verkon laitteisiin. SNMP:n avulla voidaan hallita laitteita hallinta-asemasta käsin. Hallinta-agentti vastaa hallinta-asemasta tulleisiin kyselyihin ja pyyntöihin mutta voi myös oma-aloitteisesti kertoa hallinta-asemalle verkon merkittävistä tapahtumista.

Hallittavia resursseja kuvataan olioina (object). Tarkkaan ottaen kyse ei ole olioista, vaan jokainen olio on muuttuja, joka kuvaa hallinta-agentin jotain ominaisuutta. Joukkoa tällaisia olioita kutsutaan hallintatietokannaksi (Management Information Base). Nämä oliot on standardoitu siten, että kaikki samantyyppiset laitteet tukevat samaa joukkoa olioita. Hallinta-asema voi kysellä hallinta-agentin tietokannan jonkin olion arvoa tai asettaa sen ja siten toteuttaa verkon valvontaa ja hallintaa.

Hallinta-asemat ja hallinta-agentit liitetään toisiinsa verkonhallinnan yhteyskäytännön avulla. Verkon komponenttien hallintaan tarkoitetulla yksinkertaisella verkonhallintaprotokollalla (SNMP:llä) on seuraavat perusoperaatiot:

- Lukeminen (Get), jonka avulla hallinta-asema voi hakea hallinta-agentin olioiden arvoja.

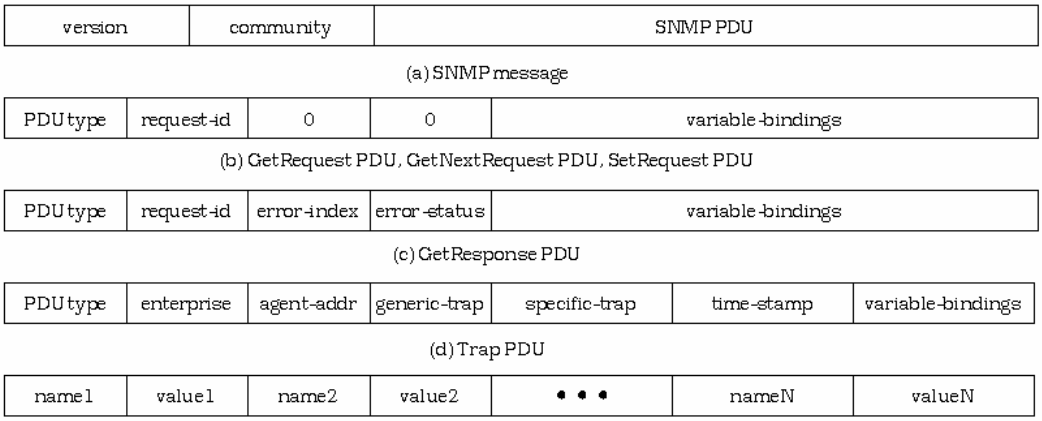
- Kirjoittaminen (Set), jonka avulla hallinta-asema voi asettaa hallinta-agentin olioiden arvoja.

- Ilmoitus (Trap), jonka avulla hallinta-agentti voi kertoa hallinta-asemalle standardissa määritellyistä merkittävistä verkon tapahtumista. /3/

6.2 Viestien yleinen rakenne

SNMP:ssä hallinta-asema ja hallinta-agentti kommunikoivat SNMP-viestien avulla. Jokainen viesti sisältää versionumeron, joka osoittaa mitä SNMP-versiota käytetään, yhteisötunnuksen ja yhden operaatioviestin viidestä mahdollisesta.

Kuvassa 12 on esitetty SNMP-viestin perusrakenne, eri operaatioviestien rakenne sekä näihin viesteihin sisältyvän olioinformaation yleisrakenne. Voidaan huomata, että kaikki luku- ja kirjoituspyynnöt ovat rakenteeltaan samanlaisia ja eroavat pyyntöihin lähetettävästä vastauksesta ainoastaan siinä, että niissä on virheilmoituksia varten varatut kentät nollia.



Kuva 12 SNMP-viestien osien rakenne /3/

SNMP-viesteissä on mahdollista sisällyttää yhteen viestiin useampia olioita käsitteleviä toimenpiteitä, mikäli niille suoritettavat operaatiot ovat samoja. Jos siis hallinta-asema haluaa lukea joltain hallinta-agentilta tietyn joukon olioita, se voi lähettää viestin, jossa on listattu kaikki halutut olioiden ilmentymät, ja saada vastauksen, jossa on kaikki kyseiset ilmentymät ja niiden arvot. Tämä tekniikka voi huomattavasti vähentää SNMP-viestien aiheuttamaa kuormaa verkossa. /3/

6.3 Hälytysryhmä

CMU-kortti lähettää trap-viestejä palvelimen kautta käyttäjän koneelle mahdollisista vioista tai ylipäätään verkon tilasta. Trap-viesti on hallinta-agentin oma-aloitteisesti hallinta-asemalle lähettämä viesti, jolla se ilmoittaa jostain merkittävästä tapahtumasta. Se eroaa rakenteeltaan huomattavasti.

Hälytyksille voidaan määritellä, mitä laskuria seurataan, minkä mittaiselta ajanjaksolta tietoa kerätään ja onko hälytyksen perusteena absoluuttinen vai arvon muutokseen perustuva hälytys. Lisäksi voidaan määritellä raja, jonka perusteella hälytys suoritetaan, sekä raja, jonka yli tai alle tarkkailtavan arvon on mentävä, ennen kuin suoritetaan uusi hälytys. /3/

6.4 SNMP:n rajoituksia

Suurin ongelma SNMP:n käytössä verkonhallintaan on sen varsin yksinkertainen autentikointimekanismi. Sen takia useimmat laite- ja ohjelmistovalmistajat rajaavat mielellään vahvat hallintamekanismit muiden tekniikoiden kuin SNMP:n ulottuville. Tämä johtaa siihen, että SNMP:tä voidaan lähinnä käyttää verkon valvontaan eikä niinkään verkon hallintaan.

SNMP- pohjaisen järjestelmän toteutuksessa tarvittava tieto on se, kuinka montaa hallinta-agenttia yksi hallinta-asema voi hallita. Tällöin on määriteltävä, kuinka usein laitteille halutaan esittää kyselyitä ja mikä on verkon aiheuttama keskimääräinen viive. Yksinkertaistamalla ongelmaa siten, että ainoastaan yhdelle laitteelle kerrallaan tehdään kyselyitä, voidaan muodostaa seuraavanlainen yhteys valvottavien laitteiden määrän (N), halutun kyselyvälin (T) ja yhteen kyselyyn kuluvan ajan välille (delta)

Kyselyyn kuluva aika (delta) riippuu useista tekijöistä: /3/

- Hallinta-aseman kyselyn muodostamiseen ja vastauksen käsittelyyn kuluva aika.
- Verkon aiheuttama viive sekä kyselyn että vastauksen lähettämiseen.
- Hallinta-agentin kyselyn käsittelyyn ja vastauksen muodostamiseen kuluva aika.
- Kyselyiden ja niihin saatavien vastausten lukumäärä.

7 TESTAUS JA KÄYTTÖÖNOTTO

Ennen järjestelmän varsinaista käyttöönottoa on laitteistoa testattava huolella. On kokeiltava eri ominaisuuksia työympäristössä ja onko se valmis jokapäiväiseen käyttöön. Järjestelmää on testattava huolella ennen käyttöönottoa, jotta vikoja ei ilmene. Jos vikoja ilmenee, aiheuttavat ne mahdollisesti katkoksia asiakkaille.

Tässä työssä, kun kaikki CMU-kortit olivat saatu asennetuksi onnistuneesti eri puolille POP-aluetta, päästiin vihdoin kokeilemaan lopullisesti järjestelmää ja sen tuomia ominaisuuksia. Ensin kokeiltiin pingata eli ottaa yhteys palvelimelle työpaikan sisäverkosta. Kun tämä toiminto oli suoritettu onnistuneesti, päästiin kokeilemaan yhteyttä Schmidin WEM-2-ohjelmistolla. Ohjelmistolle syötettiin palvelinkoneen julkinen osoite, johon yritettiin ottaa yhteyttä. Kun pienien vaikeuksien jälkeen tämä oli suoritettu ja saatu liikennöinti toimimaan serverille asti, oli vuorossa korttien asennus ohjelmistoon. Jokainen kortti täytyi tallentaa ohjelmistoon tuomalla se päävalikkoon näkyville. Kortit saatiin näkyviin ohjelmistossa kuitenkin mutkitta ja liikennöinti alkoi toimia välittömästi. Tämän jälkeen ohjelmisto otettiin käyttöön työympäristössä ja testattiin ohjelmiston eri ominaisuuksia ja niiden toimivuutta. Kun kaikkien POP:ien yhteydet olivat testattu toimiviksi eikä ongelmia esiintynyt, oli enää viimeisen vaiheen eli käyttöönoton aika. Nykyisin laite on jokapäiväisessä käytössä ja on helpottanut ja varsinkin auttanut huomattavasti työntekijöiden työtehtäviä. Pieniä ongelmia laitteen toimivuuden kanssa on havaittu, kun laite on ollut muutaman kuukauden käytössä. Ongelmia tutkitaan parhaillaan ja yritetään selvittää mahdollisien vikojen syyt, jotta päästään hyödyntämään ohjelmistoa parhaansa mukaan.

Kaikin puolin järjestelmä on havaittu toimivaksi ja hyödylliseksi jokapäiväisenä työkaluna. Vain muutaman kuukauden käyttöönotossa on jo ollut todellista hyötyä laitteiston toiminnoista ja sen tuomista eduista. Järjestelmä on kuitenkin valvontaohjelmisto, joka valvoo verkkoa jatkuvasti, näin ollen sen tulee toimia ympäri vuorokauden eikä saa katkoa eikä jumittaa yhteyksiä.

Jatkossa valvontaverkko tulee laajenemaan toimialueella uusien POP-alueiden voimin. Kun järjestelmä on havaittu toimivaksi ratkaisuksi ja yhteydet ovat lisääntyneet POP:eihin, voidaan alkaa suunnittelemaan verkon laajennustoimenpiteitä ja laitteistoiden lisähankintoja.

8 Päätelmät ja yhteenveto

Työn haasteellisuus oli huomattavan suuri, johtuen siitä että en ole ollut aikaisemmin tekemisissä kyseisten laitteiden kanssa. Aluksi tuntui hieman mahdottomalta aloittaa työn tekemistä, kun ei ollut minkäänlaista alkutietoutta eikä taitoa miten ja mistä tulisi aloittaa tämän projektin työskentely. Kysymällä vanhemmilta työntekijöiltä ja tutustumalla itse järjestelmän materiaaleihin, aloin pääsemään hieman jyvälle mistä oikein olikaan kyse.

Työ eteni täsmälleen siinä järjestyksessä miten se luvussa 4 on esitetty. Pieniä alkukankeuksia oli matkan varrella, mutta niistä selviydyttiin kuitenkin melko pienillä vaivoilla eteenpäin. Se mikä jäi laitteistoasennuksista mieleen päällimmäisenä ja hyvänä vinkkinä on, että ei kannata asentaa vanhoja käytöstä poistuneita laitteita uudelleen työkäyttöön, vaikka siinä säästäisikin loppukustannuksien osalta. Monesti mitä ihmeellisimmät viat saattavat johtua juurikin vanhoista, osittain rikkinäisistä laitteista.

Dataverkot ja niiden laitteistot olivat jo entuudestaan tuttuja tietyltä osin mutta sain silti paljon uutta ja hyödyllistä tietoa. Transmissioverkot ja laitteet olivatkin aivan uutta ja mielenkiintoista asiaa, johon tuskin ilman tätä työtä olisin päässyt edes tutustumaan ainakaan näin paljolti. Kuten edellisessä luvussa kerrottiin, verkkojen laajentuessa myös valvonnan määrä tulee lisääntymään. Tästä johtuen pääsen varmasti vielä tekemään lisäasennuksia ja näin ollen laajentamaan valvontaverkostoa toimialueellamme. Tämän työnpohjalta on helpompi lähteä laajentamaan verkkoa, kun tietää jälkikäteen mitä ja miten täytyy toimia, ja näin ollen asennukset saadaan suoritettua nopeammalla ajanjaksolla.

Oli mielenkiintoista päästä rakentamaan sellaista järjestelmää joka tulee työympäristön joka päiväseen käyttöön. Tästä johtuen oli mukava asentaa laitteistoja, kun tiesi että tekemästäni työstä olisi jotain hyötyä yritykselle, ja pääsee itse testaamaan järjestelmää ja olemaan mukana käyttöönotossa. Oli luontevampaa aloittaa dokumentointi tähän kirjalliseen raportointiin, kun oli päässyt itse suunnittelemaan, asentamaan, testaamaan ja ottamaan käyttöön kyseistä järjestelmää.

Tässä opintotyössä suurin pääpaino painottuu laitteistoiden asennukseen ja testaukseen sekä lisäksi järjestelmän toiminnalliseen osuuteen. Työ käsittelee pitkälti koko projektin viemistä vaiheittain alusta loppuun saakka. Työ on kuitenkin jaoteltu verkon rakenteelliseen, toiminnalliseen ja lisäksi asennukselliseen osuuteen. Sen pohjalta on luotu tämä dokumentointi omien kokemusten ja havaintojen pohjalta.

Valvontajärjestelmä jää tarpeelliseksi työkaluksi tämän teknisen dokumentoinnin lisäksi Tampereen Puhelin Oy:lle.

LÄHDELUETTELO

Sähköiset lähteet

1. http://www2.lut.fi/~tjaakkol/xDSL_Seminaari.pdf [Viitattu 24.3.2007]

2. http://www.kandk.fi/tuotteet/dsl-tuotteet_ja_jarjestelmat/watson_5_g_shdsl/ [Viitattu 31.3.2007]

3. http://users.tkk.fi/~hau/thesis/SNMP.html [Viitattu 24.3.2007]

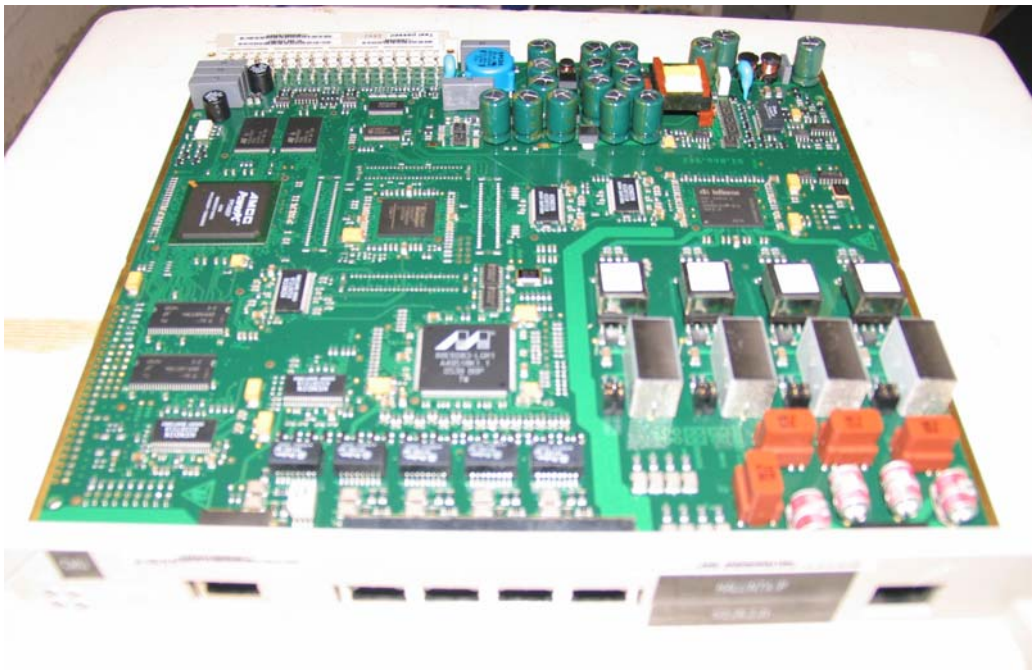
4. http://www.kandk.fi/mp/db/file_library/x/IMG/10740/file/CMU-Installation.pdf [Viitattu 24.3.2007]

LIITELUETTELO

1. Schmidin valmistama CMU-agent-valvontakortti paikalleen asennettuna

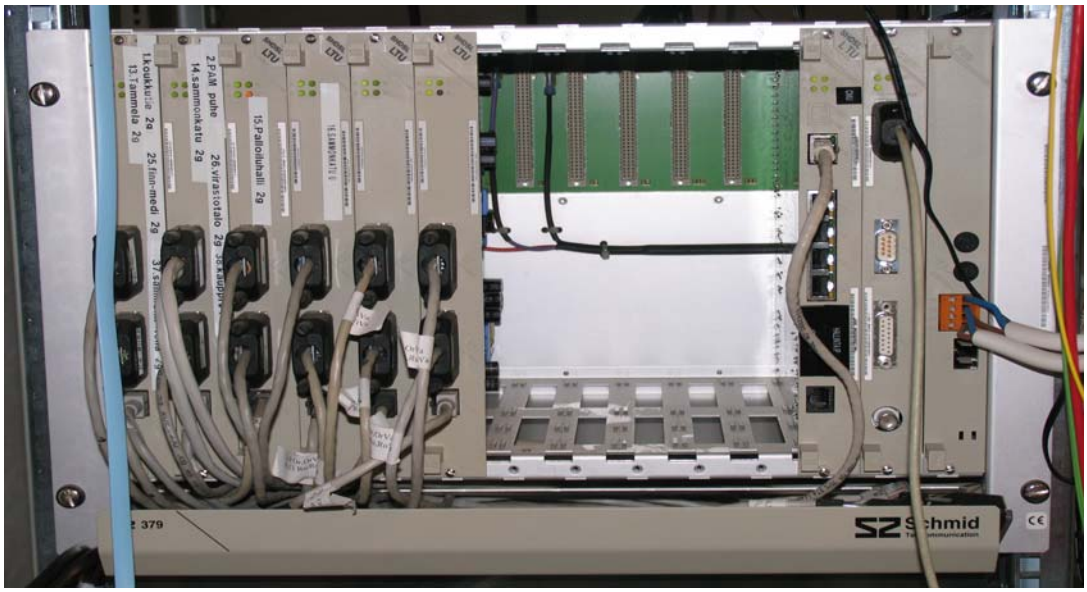
2. Schmidin kehikko, Ciscon valmistama metrokytkin ja palomuuri

3. Ristikytkentä Ciscon valmistamalta metrokytkimeltä palvelinkoneelle

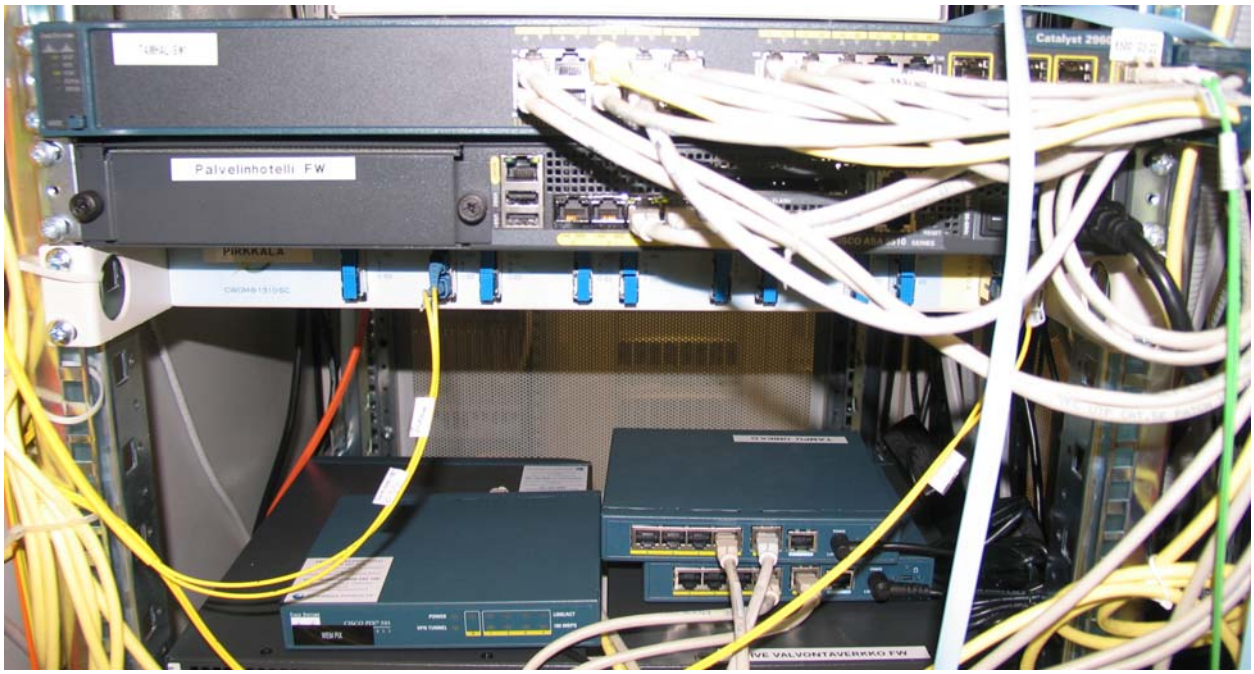


Kuva 1. Schmidin valmistama CMU-agent valvontakortti

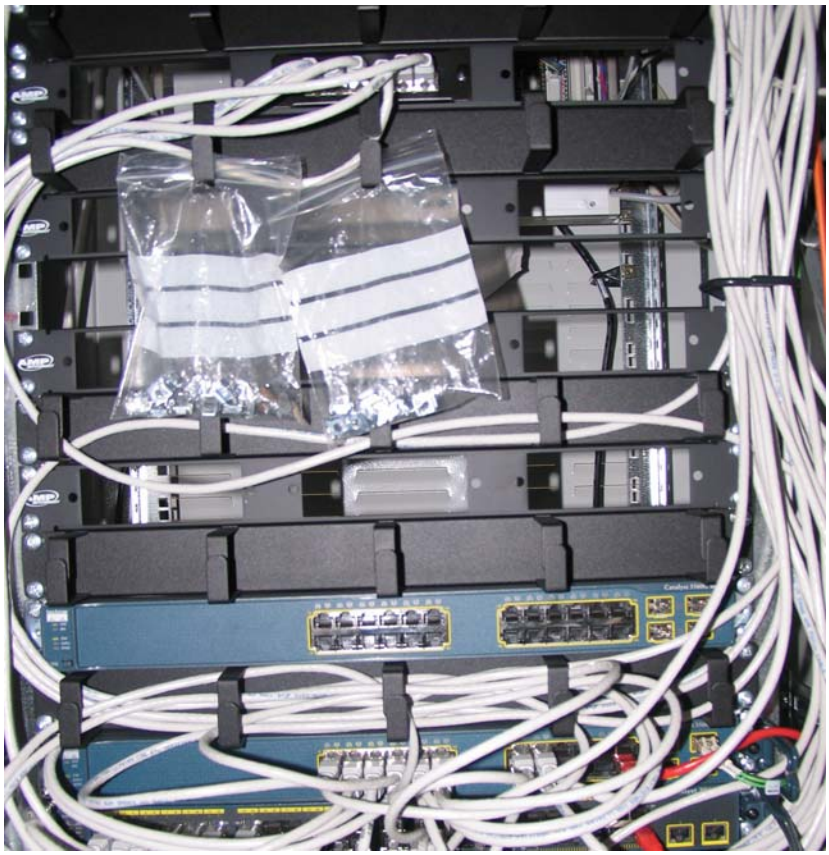
Kuva 2. CMU-agent valvonttakortti paikalleen asennettuna



Kuva 1. Schmidin valmistama 19” kehikko johon CMU- ja LTU-kortit asentuvat. Kuusi vasemmanpuoleista korttia ovat Schmidin LTU-linjakortteja. Paikassa 12 on asennettuna CMU-agent valvontakortti.



Kuva 2. Ylhäällä oleva laite on Ciscon valmistama Catalyst 2950 metrokytkin. Kuvan alareunassa näkyy kolme kappaletta Ciscon valmistamia PIX 501 palomuureja.



Kuva 1. Ristikytkentä kaapissa sijaitseva Ciscon valmistama catalyst 6500 metrokytkin, josta yhteys on kytketty ristikytkennän avulla palvelinkoneelle

Kuva 2. Ristikytkennän toinen pää palvelinkaapissa, josta yhteys tuodaan lähiverkkokaapelilla serverille