VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Juuso Erkinheimo

DSL-tekniikan päätelaitteet Vaasan kaupungin tietoliikenneverkossa

Liiketalous ja matkailu
2013

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

TIIVISTELMÄ

Tekijä	Juuso Erkinheimo
Opinnäytetyön nimi	DSL-tekniikan päätelaitteet Vaasan kaupungin tietoliikenneverkossa
Vuosi	2013
Kieli	suomi
Sivumäärä	48
Ohjaaja	Antti Mäkitalo

Tämän työn tarkoituksena oli tutkia DSLn-teknologiaa ja Vaasan kaupungin ATK-osastolle tulevia uusia Actelis ML622n-päätelaitteita. Päätelaitteita tutkin testiympäristössä ja olin mukana rakentamassa käyttöön tulevaa DSL-yhteyttä.

Laitteiden testauksessa käytin kahta Actelis ML622n-päätelaitetta, joiden välille loin yhteyden. Testasin laitteessa olevia ominaisuuksia. Tein Vaasan kaupungin ATK-osastolle peruskonfiguraation, jota siellä voidaan käyttää uusissa yhteyksissä.

Tässä työssä on myös asennusohje Actelis ML622n-laitteelle. Ohjeen avulla pystyy luomaan toimivan dsl-yhteyden ja näkee, mitä kaikkia tietoturvallisuusmenetelmiä laitteessa on.

Lisäksi tutkin päätelaitteen eri tietoturvallisuusmenetelmiä ja opastan, kuinka niitä voidaan ottaa käyttöön. Tutkin työssäni DSL-teknologiaa. Perehdyn verkon toimintaan ja tietoturvallisuuteen. Tutkin, mitä verkon hallinta on ja kerron, mitä siinä tulee ottaa huomioon.

Avainsanat dsl, tietoturva, verkon hallinta, päätelaite

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittelyn koulutusohjelma

ABSTRACT

Author	Juuso Erkinheimo
Title	DSL-technology Terminals in the Data Network of the City of Vaasa
Year	2013
Language	Finnish
Pages	48
Name of Supervisor	Antti Mäkitalo

The aim of this thesis was to research DSL-technology and Actelis ML622 terminals that are coming to use in the IT-department of Vaasa city. The terminals were studied in test environment and one DSL-connection that was coming to use was built.

To test the devices two Actelis ML622 terminals were used and between them DSL-connection was created. In addition, different options were tested. A default configuration was made to the IT-department of Vaasa city so that they can use in their new DSL-connections.

An Installation guide to Actelis ML622 device was also made. With this guide a working dsl-connection can be created. I also studied about the different ways of information security were studied and a guide on how they can be used. I studied about the functioning of networks and information security was still examined. I studied of network management and what you should know about it.

Keywords dsl, data security, network managing, terminal

KÄSITELUETTELO

ADSL	Asymmetric Digital Subscriber Line, laajakaistatekniikka
CAP	Carrierless Amplitude Phase, ADSL-tekniikassa käytetty modulointitapa
DMT	Discrete Multi-Tone, Diskreetti monitaajuus, ADSL-tekniikassa käytetty modulointitapa.
DSLAM	Digital Subscriber Line Access Multiplexer, laajakaistakeskitin
DSL	Digital Subscriber Line, laajakaistatekniikka
IP	Internet Protocol, internetprotokolla
OSI-MALLI	Open Systems Interconnection Reference Model, seitsenkerroksinen tiedonsiirtomalli
RADIUS	Remote Authentication Dial In User Service. Käytetään keskitettyyn autentikointiin.
SDSL	Symmetric Digital Subscriber Line, laajakaistatekniikka
SSH	Secure Shell. Suojattu etäkäyttöohjelma
VDSL	Very High Speed Digital Subscriber Line, laajakaistatekniikka
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko

SISÄLLYS

1 JOHDANTO

Tietoliikenneyhteydet ovat vuosien varrella kehittyneet nopeasti, ja nykyisin on käytössä nopeita kuituverkkoja. Kuituverkkojen rakentaminen on kallista, ja täydellinen siirtyminen kuituverkkoon vaatisi todella suuria yhteiskunnallisia investointeja.

Tästä syystä DSL-verkkoja tullaan käyttämään vielä useita vuosia. Niiden rakentaminen on halpaa ja helppoa, koska ne voivat käyttää puhelinkaapeleita. DSL-yhteydet ovat yleisiä peruskuluttajilla, mutta toimivat myös hyvin yrityskäytössä. Ne ovat hyvä ratkaisu, kun ei ole järkevää lähteä rakentamaan kuituverkkoa.

Työssäni kerron DSL-teknologiasta, OSI-mallista, verkon hallinnasta ja tietoturva-asioista. Olen pyrkinyt kirjoittamaan aiheesta niin, että lukija saisi hyvän kuvan DSL-teknologiasta yleisellä tasolla.

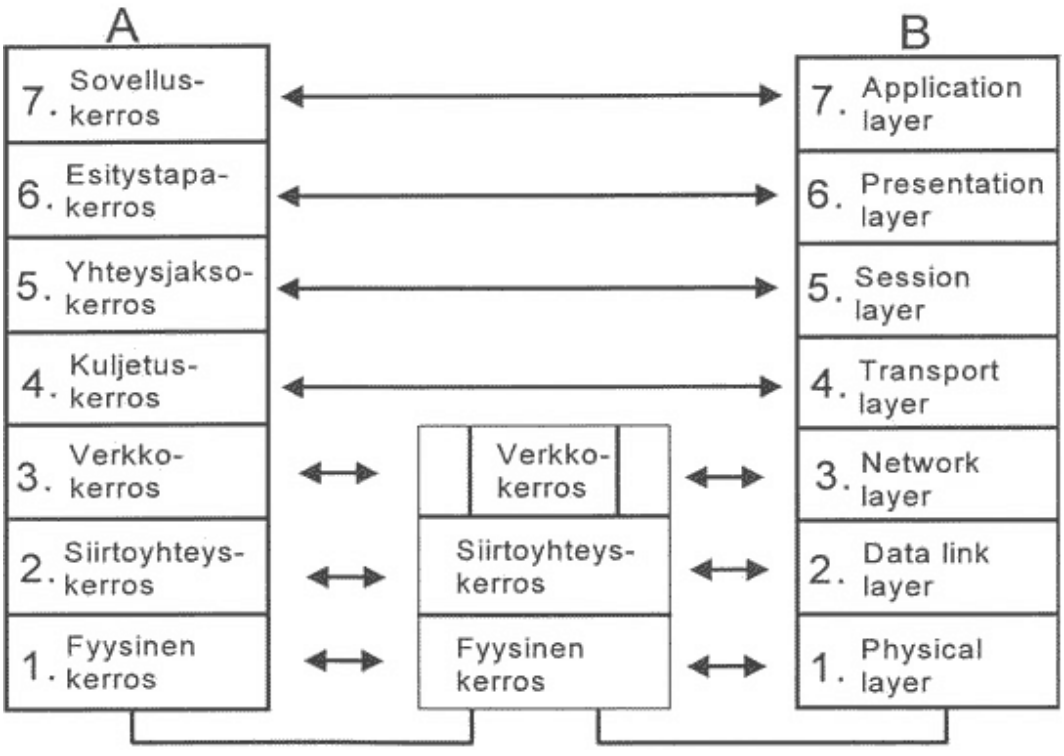
Actelis ML622-konfiguroinnista tein yksityiskohtaisen oppaan, jota pystyy soveltamaan mihin tahansa verkkoon, jossa kyseisiä laitteita käytetään.

Työni toimeksiannon sain Vaasan kaupungin ATK-osastolta, josta toivottiin, että voisin perehtyä heille tuleviin uusiin DSL-yhteyksissä käytettäviin päätelaitteisiin. Työssäni tutkin laitteen ominaisuuksia ja esittelen yksityiskohtaisesti, kuinka asennus tapahtuu.

2 OSI-MALLI

OSI-malli (Open Systems Interconnection Reference Model) on tietojärjestelmien kuvauksissa käytettävä standardi. Mallia käytetään tieto-ja tietoliikennejärjestelmien toiminnan kuvaamisen. Täysin OSI-mallin mukaisia tietojärjestelmiä ei käytännössä ole. OSI-mallin tunteminen kuitenkin helpottaa hahmottamaan, kuinka monimutkaisten järjestelmien eri osat toimivat yhdessä.

OSI-mallin mukaisesti tietojärjestelmälle on määritetty seitsemän perustehtävää. OSI-malli kuvaa näitä seitsemällä eri kerroksella. Alimmat kerrokset 1 - 3 määrittelevät lähinnä laitteistojen ja niihin liittyvien protokollien toimintaa. Ylemmät kerrokset 4 - 7 määrittelevät asiakas-palvelin-sovelluksen ohjelmallista toimintaa. Esittelen tässä luvussa tarkemmin OSI-mallin 7 kerrosta. OSI-malli esitetty kuvassa 3. (Hakala, Vainio 138)



Kuva 3. OSI-malli (Ratol)

2.1 Fyysinen kerros

OSI-mallin alin kerros on fyysinen kerros (Physical Layer). Fyysinen kerros määrittelee kaapelointiin sekä signaalinsiirtoon liittyviä sähköisiä ja mekaanisia arvoja. Fyysisellä tasolla määritellään muun muassa liitin- ja kaapelintyypit, signaalien jännitetasot, vaimennus, ylikuuluminen sekä heijastukset.

Käytettävä johtokoodaus (Encoding) kuuluu myös fyysiseen kerrokseen. Johtokoodauksessa lähetettävät bitit muutetaan erilaisiksi signaalimuodoiksi. Verkon aktiivilaitteet kuuluvat fyysiseen kerrokseen. Aktiivilaitteita ovat keskittimet, toistimet ja mediamuuntimet. (Hakala, Vainio 139)

2.2 Siirtoyhteyskerros

Siirtoyhteyskerroksessa (Data Link Layer) määritellään, miten lähetettävästä datasta muodostetaan kaapelointijärjestelmässä siirrettäviä yksiköitä. Näitä yksiköitä ovat kehykset (frame) sekä solut (cell). Siirtoyhteyskerroksessa määritellään lähettävien ja vastaanottavien laitteiden fyysiset osoitteet (MAC-osoitteet).

Lähiverkoissa käytettävät Ethernet- ja Token Ring -kehysmääritykset ovat siirtoyhteyskerroksessa käytettäviä protokollia. Laajaverkoissa käytettyjä protokollia ovat mm. PPP (Point to Point Protocol, HDLC (High Level Data link Control Protocol) ja Frame Relay. Siirtoyhteyskerroksessa toimivia aktiivilaitteita ovat verkkokortit, sillat ja kytkimet. Nämä laitteet kuuluvat myös fyysiseen kerrokseen (Hakala, Vainio 139.)

Siirtoyhteyskerroksen tehtäviin kuuluu kahden pisteen välisen yhteyden ylläpito, siirtovirheiden havainnointi ja korjaus fyysisellä kerroksella. Lisäksi tietovuon hallinta kuuluu siirtoyhteyskerroksen tehtäviin. Tietovuon hallinnassa seurataan, että fyysiselle kerrokselle ei tarjota enempää dataa kuin vastaanottaja tai siirtotie pystyy käsittelemään.

Siirtoyhteyskerros on jakautunut vuosien varrella kahteen eri kerrokseen. MAC (Medium Access Control) -kerroksessa varataan siirtoyhteys datan siirtoa varten

sekä hoidetaan tietovuon hallinta. LLC (Logical Link Control) -kerroksessa huolehditaan virheiden havaitsemisesta, niiden toipumisesta sekä tietovuon hallinnasta. (Granlund. 8)

2.3 Verkkokerros

Verkkokerroksessa (Network Layer) määritellään verkkojen tietoliikenteessä tarvittavien reititysten ja eri liikennöintimuotojen välillä käytävä priorisointi (Hakala, Vainio 139).

Verkkokerroksen (Network Layer) tehtävänä on tarjota sellainen yhteys tietoverkon yli, joka ei ota kantaa verkossa käytettyyn rakenteeseen ja kytkentätekniikkaan. Yhteyden muodostaminen tällä tyylillä vaatii muutamia toimenpiteitä, jotka seuraavaksi esitän.

Yhteydessä käytettävien eri laitteiden loogiset osoitteet täytyy konvertoida fyysisiksi osoitteiksi ja käytettävät nimet täytyy muuttaa loogisiksi osoitteiksi. Näitä tehtäviä hoidetaan internetverkon DNS- (Domain Name Server) sekä ARP-palvelujen (Address Resolution Protocol) avulla. DNS-palvelussa muutetaan selväkielinen nimi IP-osoitteeksi (Internet Protocol) ja ARP-palvelussa laiteosoite muutetaan IP-osoitteeksi.

Tietoliikennesanomien (nk. pakettien) reitityksessä etsitään paras yhteys lähettäjän ja vastaanottajan välillä. Reitityksellä hoidetaan ruuhkanhallintaa. Verkossa tasataan eri siirtoteiden kuormaa, jotta siirtotien kapasiteetti olisi optimaalisimmin käytössä.

Verkkokerroksessa sovitetaan siirrettävä sanoma siirtotielle sopivaksi. Tämä on tärkeä ominaisuus, koska erilaisilla siirtoyhteyksillä on rajoituksia, kuinka suuri siirrettävä tieto saa olla. Sanoman lähettäjä ei voi tuntea näitä rajoituksia, siksi verkkokerroksessa huolehditaan siitä, että siirtoyhteyskerroksen suurinta sanomapituutta ei ylitetä. Verkkokerros jakaa käyttäjän lähettämät sanomat sellaisiin osiin, että ne mahtuvat siirtoyhteyskerroksen pakettiin ja sanoma saadaan perille. (Granlund 8 - 9)

2.4 Kuljetuskerros

Kuljetuskerros (Transport Layer) on ohjelmallinen kerros. Kuljetuskerroksessa tehtävistä huolehtivat kuljetusprotokollat (Transport Protocol). Lähiverkoissa käytetään muun muassa TCP- (Transmission Control Protocol), Novellin SPX- (Sequential Packet Exchange) ja NetBIOS-protokollia. Näillä protokollilla pilkotaan sovellusten lähettämä datavirta käsittelykokoisiin yksiköihin. Näistä yksiköistä käytetään nimitystä segmentti (Segment) tai paketti (Packet).

Kuljetuskerroksen protokollat huolehtivat yhteyden muodostamisesta sekä sen purkamisesta asiakas- ja palvelinohjelmistojen välillä. Protokollat varmistavat lähetetyn datan perille menon sopivalla kuittausmenettelyllä (Acknowledgement Method).

Kehittyneemmät protokollat kuljetuskerroksessa ottavat huomioon laitteiden kuormitustilanteen ja ilmoittavat dataa lähettävälle laitteelle, kuinka paljon se voi ottaa dataa vastaan.

Tehtäväkokonaisuus, jota kutsutaan vuonohjaukseksi (Flow Control), hoitaa datan pilkkomisen, lähetettävän pakettikoon määrityksen ja kuittauksen. (Hakala, Vainio. 139 - 140)

Kuljetuskerros tarjoaa tiedonsiirtoyhteyttä kahden päätepisteen välillä. Nämä yhteydet voivat olla yhteydellisiä (Connection Oriented) tai yhteydettömiä (Connectionless).

Yhteydellisessä yhteys luodaan, kun osapuolet aikovat siirtää dataa toisilleen. Yhteys suljetaan, kun tiedonsiirto päättyy. Yhteydellinen yhteys on luotettava. Siinä data siirtyy lähettäjältä vastaanottajalle virheittä ja verkossa siirrettävien sanomien järjestys ei muutu. TCP (Transmission Control Protocol) on tyypillinen yhteydellinen protokolla.

Yhteydetöntä yhteyttä käytetään, kun tehtävä on niin yksinkertainen, että ei ole tarpeellista ilmoittaa yhteyden perustamisesta jokaisen siirron yhteydessä eikä ole tarpeen valvoa sanoman perille pääsyä. Yhteydettömällä yhteydellä siirrettävä

sanoma lähetetään vastaanottajalle ilman erillistä ilmoitusta. Yhteydettömässä yhteydessä vastaanottaja on varautunut sanoman tulemiseen, mutta ei tiedä, koska sanoma lähetetään. Ei myöskään tiedetä, onko lähetettyjä sanomia kadonnut matkalla. UDP (User Datagram Protocol) on yhteydetön protokolla. (Granlund 9)

2.5 Istuntokerros

Istuntokerros (Session Layer) huolehtii käyttöoikeuksien tarkistuksista ja järjestelmän suojaukseen liittyvistä tehtävistä. Istuntokerroksen ohjelmistojen tehtävänä on tarjota tarvittavat kirjautumisrutiinit ja salausmenetelmät. Ohjelmistot huolehtivat myös tiedosto-, tietue- sekä kenttälukituksista. Ohjelmistot suojaavat myös keskusmuistialueita. (Hakala,Vainio 140)

Istuntokerros huolehtii sovellusten välisistä ohjaustoiminnoista. Lisäksi sen tehtävinä on yhteyden muodostaminen ja sen siirtoyhteyspalvelun varaaminen, yhteyden ominaisuuksien sopiminen osapuolten välillä, tarkistuspisteillä yhteyden varmistaminen, yhteyden päättäminen sekä resurssien vapauttaminen.

Istuntokerroksen tehtävät ovat lisääntyneet tietoliikennettä käyttävien sovellusten muuttuessa. Multimedian mukanaan tuoma tehtävä on erilaisten keskinäisten datavirtojen synkronointi. Nykyisissä järjestelmissä näistä tehtävistä vastaa pääasiassa käyttöjärjestelmä. (Granlund 10)

2.6 Esitystapakerros

Esitystapakerroksessa (Presentation Layer) määritellään, missä muodossa asiakkaan ja palvelimen välinen sanomaliikenne tapahtuu. Esitystapakerroksen määrittelyihin kuuluvat erilaiset koodausjärjestelmät. Tiedon siirtäminen järjestelmien välillä tapahtuu binäärimerkkijonoina (binary string). Siirrossa käytetään vain yhtä tietotyyppiä. Tämän takia sanomarakenteeseen joudutaan määrittämään, miten alkuperäiset tietotyypit koodataan (encode) binäärimerkkijonoksi ja miten ne dekoodataan (decode) takaisin alkuperäisiksi tietotyypeiksi vastaanottavassa sovelluksessa.

Merkkikoodistot ovat kerroksessa käytettäviä määrityksiä. Näitä merkkikoodistoja ovat muun muassa ASCII (American Standard for Character Information Interchange), tietotyypeissä käytettävät esitystavat, kuten ASN1 (Abstract Syntax Notation One) sekä binäärimuotoisen datan käsittelykuvaukset kuten BER (Basic Encoding Rules). Nykyisin lähiverkkojärjestelmissä näistä tehtävistä huolehtii käyttöjärjestelmä. (Hakala, Vainio 140)

2.7 Sovelluskerros

Sovelluskerroksessa (Application Layer) tarjotaan sovelluksille rajapinta OSI-järjestelmään. Tyypillisiä palveluita sovelluskerroksessa ovat tiedonsiirto, sähköposti ja hakemistopalvelut. (Granlund 10)

Sovelluskerroksessa määritellään sovellusten ja käyttöjärjestelmien toiminnasta ne osat, joita ei ole alemmissa kerroksissa määritelty. Nykyisissä lähiverkkojen sovelluksissa ja käyttöjärjestelmissä ei pystytä erottamaan sovellus-, esitystapa- ja istuntokerroksia. Ne muodostavat yhdessä ohjelmallisen kokonaisuuden. (Hakala, Vainio 140 - 141)

3 DSL-TEKNOLOGIA

3.1 Yleistä

DSL (Digital Subscriber Line) on tekniikka, joka syntyi vaihtoehdoksi optiselle kuidulle. Täydellinen siirtyminen kuituun edellyttäisi niin suuria yhteiskunnallisia investointeja, ettei siihen ole ollut mahdollista siirtyä. DSL-tekniikat käyttävät kuparisia puhelinlinjoja, joten tekniikka on soveltunut hyvin käytettäväksi, koska puhelinlinjoja on useimpiin paikkoihin jo vedetty, sekä niitä on halvempi rakentaa kuin kuituverkkoja (Granlund 383.)

DSL-teknologiaan kuuluvat ADSL:n (Assymmetric Digital Subscriber Line), HDSL (High-bit rate Digital Subscriber Line), RADSL (Rate Adaptive Digital Sub-scriber Line), SDSL (Symmetric Digital Subscriber Line) sekä VDSL (Very high speed Digital Subscriber Line). Yhteistä näille kaikille on se, että ne perustuvat parikaapeliyhteyksiin. Useimmat DSL-tekniikoista vaativat, että käytetään erillistä jakosuodinta, jonka avulla voidaan erottaa puhelinliikenne dataliikenteestä (Granlund 383.)

3.2 Modulointi

Digitaalinen tiedonsiirto ei onnistu pitkän matkan kuparijohtimissa ilman signaalin muuntamista digitaalisesta muodosta analogiseen muotoon. Tätä muunnosprosessia kutsutaan moduloinniksi.

Modulointi tehdään modeemissa. Modeemissa muodostetaan kantoaalto sopivalle taajuusalueelle. Muuttamalla tämän kantoaallon ominaisuuksia voidaan viestittää siirrettävistä biteistä. Tällä tavoin siirtotielle lähetettävät signaalit voidaan muotoilla sellaisiksi, että ne sopivat johtimen rajoitteisiin. Tämä on digitaalisen signaalin siirtämistä analogisella siirtotiellä (Granlund 92.)

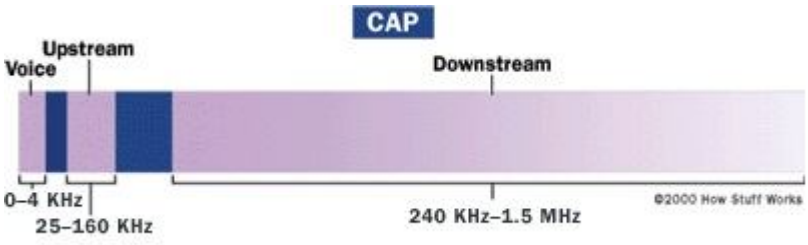
3.2.1 Modulointitekniikoita dsl-yhteyksissä

On olemassa kaksi kilpailevaa ja yhteensopimatonta standardia, joiden avulla signaalin modulointi voidaan tehdä. Nämä tekniikat ovat CAP (Carrierless Amplitude Phase ja DMT (Discrete Multi-Tone). CAP-tekniikka on vanhempi ja sitä käytettiin DSL-asennuksien alkuaikoina. Nykyään DMT-tekniikka on yleisemmin käytetty. (Howstuffworks; Allied Telesis)

3.2.2 CAP-modulointi

CAP-tekniikka on koodausmetodi, joka jakaa puhelinlinjan kolmeen erillään olevaan aallonpituusalueeseen. Puhelinliikenne toimii 0 - 4 KHz (kilohertsin) aallonpituusalueella. Tiedon lähetyskanava käyttäjältä takaisin palvelimelle tapahtuu taajuudella 25 - 160 KHz. Tiedon vastaanottokanava palvelimelta käyttäjälle alkaa 240 kilohertsin taajuudelta ja loppuu noin 1,5 MHz (megahertsiin). Taajuuden loppupäähän vaikuttavia tekijöitä ovat linjan pituus, linjalla oleva häiriöäänten määrä sekä käyttäjien määrä puhelinyhtiön kytkimellä.

CAP-tekniikassa on kolmijakoinen menetelmä, jossa kolme kanavaa on laajasti eroteltu toisistaan. Tämä erottelu on luotu minimoimaan mahdollinen häiriö eri kanavien sekä signaalien välillä. CAP-kolmijako on esitetty kuvassa 1. (Howstuffworks), (Allied Telesis)

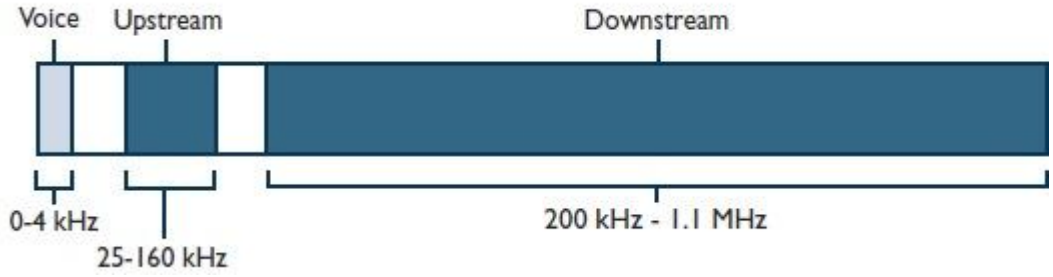


Kuva 1. CAP-kolmijako (Howstuffworks)

3.2.3 DMT-modulointi

DMT-tekniikka on käytetyin modulointimetodi. DMT:n signaali jaetaan 256 erilliseen kanavaan, jotka kaikki ovat 4.3125 KHz levyisiä. Tiedonlähetyskanavia tuosta 256 kanavasta on 224 ja tiedon vastaanotolle on 32 kanavaa. Kaikkia 256

kanavaa valvotaan erikseen, jotta tiedonkulku ei estyisi. DMT-tekniikka vaihtelee signaalin kanavaa jatkuvasti, jotta parhaat kanavat olisivat käytössä tiedonlähetykseen sekä vastaanottamiseen. DMT-tekniikka pystyy hyödyntämään kaikkia spektrin kanavia ja pystyy toimimaan, vaikka kanavilla olisi häiriötä. DMT pystyy myös käyttämään joitakin alempia kanavia kaksisuuntaisesti. Tämä tarkoittaa sitä, että niissä pystytään lähettämään sekä vastaanottamaan tietoa. DMT:n jako esitetty kuvassa 2. (Howstuffworks; Allied Telesis)



Kuva 2. DMT jako (Allied Telesis)

3.3 ADSL

Asymmetric Digital Subscriber Line eli ADSL. ADSL toimii normaalissa kuparikaapelipuhelinverkossa, joten se ei vaadi erillistä kaapelointia. Olemassa olevia kuparikaapeleita pystytään käyttämään tiedonsiirtokanavina.

ADSL on epäsymmetrinen, joka tarkoittaa sitä, että tieto liikkuu eri suuntiin eri nopeudella. Käyttäjälle tämä tarkoittaa sitä, että tietoa voidaan ottaa vastaan selvästi suuremmalla nopeudella kuin lähettää sitä eteenpäin. (FiCom)

ADSL-liittymän rakentaminen on helppoa ja yhteys on kohtuullisen nopea. ADSL-tekniikalla pystytään parhaimmillaan siirtämään dataa alavirtaan nopeudella 28 Mbit/s (megabittiä sekunnissa) ja ylävirtaan nopeudella 3,5 Mbit/s. ADSL onkin tällä hetkellä yleisimmin käytetty laajakaistatekniikka. (Granlund 389)

3.4 SDSL

Symmetrical Digital Subscriber Line eli SDSL-tekniikka syntyi, kun tarvittiin yhteys, jonka avulla voidaan käyttää vakionopeutta puheen ja datan siirron kanssa. Tiedonsiirtonopeudet SDSL-yhteydellä ovat 192 - 2304 kbit/s (kilobittiä sekunnissa). Käyttämällä kahta johdinparia saadaan kapasiteetti kaksinkertaistua. SDSL-tekniikka toimii maksimissaan kolme kilometriä pitkän tilaajajohdon kanssa.

SDSL:n rakenne mahdollistaa datan ja puheen käsittelyn digitaalisen puhelinverkon tavoin. SDSL moduloi lähettämänsä datan, joka tarkoittaa, ettei se käytä koko siirtotien taajuuskaistaa. SDSL jättää puhekaistan vapaaksi, joka toimii alle 4 000 hertsin taajuudella. (Granlund 385)

3.5 VDSL

Very high speed Digital Subscriber Line eli VDSL on DSL-tekniikoista kaikista nopein. VDSL-tekniikka on kehitetty optisten siirtoteiden jatkeeksi, kun optisella kaapelilla ei ole tarkoituksenmukaista korvata tilaajaliittymää. VDSL-tekniikka toimii lyhyen matkan kupariparikaapeleissa, joita käytetään puhelinlinjoissa. Yhteyden nopeuteen vaikuttaa, kaapelin pituus ja mitä ominaisuuksia yhteydessä käytetään. (Granlund 386), (Pulse Supply)

VDSL-tekniikka pystyy lähettämään tietoa alavirtaan maksimissaan 52 Mbit/s, mutta tällöin kaapelin pituus saa olla maksimissaan 300 metriä. Ylävirtaan tällainen VDSL-yhteys pystyy liikennöimään 12 Mbit/s nopeutta. Kaapelin pituuden pidentyessä yhteyden nopeus laskee.

Symmetrisen VDSL-yhteyden maksiminopeus voi olla enintään 26 Mbit/s. Symmetrinen yhteys tarkoittaa sitä, että yhteys toimii yhtä nopeasti niin ala- kuin ylävirtaan. (Granlund 387)

4 FYYSINEN TASO JA LAITTEET

Käsittelen tässä luvussa tarkemmin DSL-yhteyksissä tarvittavat laitteet ja fyysisen tason. Fyysiseen tasoon kuuluvat siirtotiet, kuten puhelinverkossa käytettävä kuparikaapelointi. Yhteys tarvitsee kaapeloinnin lisäksi toimiakseen modeemeja sekä DSLAM-kytkimen (Digital Subscriber Line Access Mulplexer).

4.1 Fyysiset siirtotiet

DSL-yhteyksien fyysisinä siirtoteinä toimii erilaiset kaapelit, kuten kuparikaapeli, optinen valokuitu ja verkkokaapelit. Kuparikaapelit ovat perinteisiä puhelinkaapeleita, joita pitkin DSL-yhteys perinteisesti tuodaan asiakkaalle asti. Optisia valokuituja käytetään suuremmissa alue- ja runkoverkoissa. (Granlund 40)

4.1.1 Kuparikaapeli

Kuparikaapelin maksimi tiedonsiirtoetäisyys 0,5 mm:n johtimisella kaapelilla on noin kolme ja puoli kilometriä ja 0,4 mm:n johtimisella kaapelilla vähän alle kolme kilometriä (Draka).

Kuparikaapelilla operaattori yleensä toteuttaa liityntäverkon. Liityntäverkko on se televerkon taso, johon asiakkaat liittyvät. Operaattorin tilaajaverkko voi myös olla toteutettuna kuparikaapelilla vaikka nykyisin optisen valokuidun käyttö on lisääntynyt. Tilaajaverkko liittyy kiintöistössä olevaan kuparikaapelilla toteutettuun kiinteistöverkkoon (Helkama Flash Cord.)

4.1.2 Optinen valokuitu

Optisissa valokuiduissa digitaalinen tieto siirretään valopulssien avulla. Optinen kuitu sisältää kolme komponenttiä. Kuidun sisällä kulkevasta ydinjohdosta (Core), jota ympäröi valoverho (Cladding), joka pitää valonsäteet ytimessä, sekä vaipasta, joka suojaa koko rakennetta. (Granlund 48)

Optisia valokuituja käytetään suurikapasiteettisten runko- ja alueverkkojen rakennuksessa (Helkama Flash Cord).

DSL-yhteys tarvitsee toimiakseen modeemin. Modeemin avulla kommunikoidaan operaattorin DSLAM-laitteen kanssa. Modeemi muuntaa korkeataajuuksiset äänet lähetysääniksi, jotka lähetetään operaattorin DSLAM-laitteelle. Modeemi vastaanottaa ja modului DSLAM-laitteelta tulevat äänet sellaisiksi, joita tietokone ymmärtää. (eHow Tech)

4.2 DSLAM

DSLAM-laitteen avulla operaattori pystyy käsittelemään useiden asiakkaiden internet-yhteyksiä samanaikaisesti. DSLAM toimii kanavana, jonka kautta useat asiakkaat voivat luoda nopean yhdyskäytävän internetiin käyttämällä vain yhtä yhteyttä. (WiseGeek)

5 VERKON HALLINTA

Verkonhallinnan tehtävänä on turvata verkon kautta saatavien palveluiden toimivuus. Verkon haltijan on ylläpidettävä palvelinten ja niiden asiakkaiden välisiä yhteyksiä. Verkon haltijan on huolehdittava siirtokapasiteetin riittävyydestä, sekä yhteyksien luotettavuudesta ja turvallisuudesta.

Verkonhallinnassa on pystyttävä havaitsemaan vikatilanteet, joita tulee kaapelointijärjestelmissä, aktiivilaitteissa sekä tietokoneiden liityntälaitteissa, kuten verkkokorteissa ja päätelaitteissa. Niiden havaitseminen suuremmissa verkoissa edellyttää keskitettyyn hallintaan siirtymistä.

Yleisimmät verkon hallinnassa käytettävät työkalut ovat SNMP-protokollaan (Simple Network Management Protocol) perustuvia verkonhallintaohjelmia sekä telnet- tai www-pohjaisia laitteiston laitehallintaohjelmia. Verkon dokumentointi on yksi tärkeä osa verkon hallintaa ja esittelen sen SNMP-protokollan kanssa tarkemmin tässä luvussa. (Hakala, Vainio 322)

5.1 Verkon dokumentointi

Verkon dokumentointi on tärkeää, koska kun tiedetään, kuinka verkon tulisi toimia on vikojen selvittäminen helpompaa. Verkon dokumentointi on järkevää tehdä katselmusten avulla. Katselmuksia on viisi eri tyyppiä, jotka ovat investointikatselmus, tilakatselmus, toiminnallinen katselmus, tehokkuuskatselmus ja tietoturvakatselmus. Esittelen eri katselmukset tarkemmin tässä luvussa. (Ciscon verkkoakatemia 1. vuosi 809)

5.1.1 Investointikatselmus

Investointikatselmuksessa tehdään lista kaikista verkon laitteista ja ohjelmistoista. Verkossa käytettävistä laitteista olisi syytä kirjata ylös sarjanumerot, tyypit ja käyttäjien nimet. Suotavaa olisi kerätä tiedot työasemien ja verkkolaitteiden asetuksista.

Yleisesti pidetään hyödyllisenä investointitietojen säilyttämistä verkkolaitteiden yhteydessä. Toinen tapa on pitää tiedot tallennettuina teksti- tai datatietokantaan,

jolloin tukihenkilöstön on helppo päästä niihin käsiksi. Itse käyttäisin molempia tapoja.

Verkon ohjelmistosovelluksista kerättäviä tietoja on muun muassa käytetyn ohjelmiston tyyppi, kunkin sovelluksen käyttäjien lukumäärä ja sovelluksen vaatima käyttöympäristö. Käyttäjämäärien kirjaamisesta on se hyöty, että nähdään, ettei käyttäjien määrä ylitä ohjelmistolisenssissä sallittua määrää. (Ciscon verkkoakatemia 1. vuosi 810)

5.1.2 Tilakatselmus

Tilakatselmuksessa kirjataan muistiin laitteiden sijainti. Kirjata kuuluisi kaapelointi, työasemat, oheislaitteet ja erilaiset verkkolaitteet, kuten keskittimet, sillat ja reitittimet. Olisi hyödyllistä lisätä kaikki laitteet rakennuksen pohjapiirustukseen, kaikkien on helppo löytää laitteet katsomalla vain pohjapiirrustuksessa, missä laite sijaitsee.

Tilakatselmuksen kirjauksen jälkeen tulisi tietojen pohjalta luoda verkkokartta suoraan pohjapiirustukseen. Karttaan olisi hyvä laittaa kaikkien verkkoon liitettyjen laitteiden fyysinen sijainti ja niissä käytettävät sovellukset. IP- ja MAC-osoitteet ja verkkosolmujen välisten kaapelinvetojen pituudet olisi myös suositeltavaa kirjata ylös. Kattavan tilakatselmuksen tekeminen helpottaa jatkossa vikojen selvittämistä. (Ciscon verkkoakatemia 1. vuosi 810)

5.1.3 Toiminnallinen katselmus

Toiminnallisessa katselmuksessa seurataan, toimiiko verkon päivittäistä toimintaa. Tämän suorittaminen edellyttää erikoisohjelmistoja ja laitteita. Verkkomonitoroinnin lisäksi voidaan käyttää verkkoanalysaattoria, kaapelitutkaa (Time Domain Reflectometer), kaapelihaaroittimia, jännitemittareita ja oskillaattoria. Verkkomonitorointi ja analysaattorit toimivat omissa erikoisohjelmistoissaan.

Näiden laitteiden ja ohjelmistojen avulla voidaan seurata verkon liikennettä laskemalla lähetettyjen pakettien ja tarvittavien uudelleenlähetysten määrää,

pakettien kokoa ja verkon käyttöä. Seuraamalla näitä laitteiden ja ohjelmistojen avulla voidaan helpommin havaita kaapelikatkot, oikosulut, mediassa esiintyvä kohina ja paikallistaa verkossa olevat pullonkaulat. (Ciscon verkkoakatemia 1. vuosi 811)

5.1.4 Tehokkuuskatselmus

Tehokkuuskatselmuksessa seurataan, toimiiko verkko kykyjensä mukaan. Tulisi tehdä kustannusanalyysi siitä, kuinka helposti verkosta on saatavissa informaatiota sekä analysoida verkon kykyä pitää data eheänä. Tulisi arvioida verkon tukemiseen käytettävissä olevasta henkilöstöstä ja arvioida verkon käyttäjiä ja heidän kykyjään käyttää verkon laitteita ja ohjelmistoja. (Ciscon verkkoakatemia 1. vuosi, 814)

5.1.5 Tietoturvakatselmus

Tietoturvakatselmuksessa tutkitaan verkon tietoturvavaatimuksia ja sitä, millä ohjelmisto- ja laiteratkaisuilla se voitaisiin parhaiten hoitaa. Tulisi tehdä luettelo segmenteistä, joihin pääsyä olisi syytä rajoittaa tai joiden data vaatii salausta. Laitteista, tiedostoista ja hakemistoista, jotka tarvitsevat lukitsemista tai salasanasuojausta, kannattaisi myös lisätä tiedot katselmukseen. Varmuuskopioinnista kannattaa miettiä, mitkä tiedostot ja hakemistot tarvitsevat varmuuskopiointia, sekä kuinka usein varmuuskopiot tulisi ottaa.

Verkossa tulee olla käytössä virussuojaus ja verkon valvonta. Valvontaa varten täytyy hankkia verkkoanalysaattori, jonka avulla on helpompi seurata mitä verkossa tapahtuu. (Ciscon verkkoakatemia 1. vuosi, 814 - 815)

5.2 SNMP-pohjainen laitteistonhallinta

TCP/IP-verkoissa on usein suuri määrä palvelimia ja aktiivilaitteita, joissa saattaa tulla toiminnallisia virheitä. Tämän lisäksi verkon toiminnan muuttuessa siihen saattaa tulla suorituskyvyn kannalta vaarallisia pullonkauloja. Oman uhkansa verkon toimivuuteen aiheuttaa vihamieliset käyttäjät organisaation sisällä sekä erityisesti verkon ulkopuolelta tulevien hakkerien ja krakkerien

tunkeutumisyritykset. Huolellinen suunnittelu ja laitteistojen turvamääritykset ovat verkon hallittavuuden ja turvallisuuden takeena.

SNMP-protokollaa käyttävät verkon hallinta-asemat sekä hallittavat laitteet ovat TCP/IP-pohjaisissa verkoissa hallinnan kulmakivenä. Verkon laitteet, työasemat, palvelimet ja aktiivilaitteet kuuluvat periaatteessa kaikki hallinnan piirin. Laitteistovirheiden automaattinen havaitseminen ja kuormituksen laskeminen ovat valvonnan painopisteitä. (Hakala, Vainio 323)

5.2.1 SNMP-protokolla

TCP/IP-pohjaisessa verkonhallinnassa hallittavissa laitteissa on käytössä hallinta-agentti (Management Agent, SNMP-agent). Hallinta-agentti kerää tietoja laitteen toiminnasta. Kerättyjä tietoja kysellään erillisellä hallintaohjelmalla (Management Station). SNMP-protokollaa käytetään hallinta-aseman ja agentin välisessä liikenteessä. SNMP on sovellustason protokolla, joka määrittää, missä muodossa hallinta-asema suorittaa kyselyt agentin MIB-tietokantaan (Management Information Base) ja määrittelee, missä muodossa agentin tulee vastata tehtyyn kyselyyn.

Agentti voi lähettää omaehtoisesti viestejä hallinta-aseman avulla. Agenttiohjelmistossa voidaan määritellä kynnysarvo tietyille tapahtumille. Kynnysarvon ylityttyä agentti lähettää hallinta-asemalle sanoman tästä arvon ylityksestä. Kynnysarvoksi voidaan määritellä esimerkiksi yksittäiset vakavat virheet, kuten virtakatkokset. (Hakala, Vainio 323 – 324)

6 TIETOTURVA

Verkon tietoturvan ylläpitoon kannattaa kiinnittää runsaasti huomiota. Usein ymmärretään varautua ulkopuolelta tuleviin uhkiin, mutta unohdetaan, että suurin osa vakavista tietoturvariskeistä tulee oman organisaation sisältä.

Tieto on nykyaikaisten organisaatioiden arvokkainta omaisuutta ja se on syytä turvata. Tietojen luottamuksellisuus, saatavuus ja oikeellisuus on pystyttävä turvaamaan mahdollisimman hyvin.

Täydellisen tietoturvaan ei ole mahdollista päästä ja tulee muistaa, että siitä tulee ylläpitokustannuksia. Tietoturvallisuus täytyy pyrkiä pitämään hyvänä, mutta kustannukset eivät saa karata käsistä. (Hakala, Vainio 341)

6.1 Luottamuksellisuus, eheys ja käytettävyys

Tietoturvallisuus voidaan jakaa kolmeen keskeiseen tekijään, jotka ovat luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuudessa pyritään siihen, että tiedot ovat käytössä vain niillä henkilöillä, joilla on kyseisten tietojen käyttöoikeus.

Verkoissa luottamuksellisuutta pyritään ylläpitämään salakirjoituksella ja erilaisilla käyttäjäntunnistusmekanismeillä, jotka mahdollistavat verkkoon pääsyn vain auktorisoiduille käyttäjille.

Eheys tarkoittaa sitä, etteivät tietojärjestelmiin tallennetut tiedot pääse muuttumaan virheellisiksi. Eheyden varmistaminen vaatii varautumista tietojen tahalliseen muuttamiseen (Krakkerointi) sekä tietojen tahattomaan muuttumiseen.

Tahaton muuttuminen voi tapahtua ohjelmien virheellisen käytön, ohjelmointivirheen, laitevirheen sekä tiedonsiirtovirheiden takia. Tätä pyritään välttämään käyttämällä yhteydellisiä protokollia.

Salakirjoituksen avulla voidaan estää siirron aikana muuttuneiden tietojen tallentumista tietojärjestelmiin. Tahallista tietojen muuttumista pyritään estämään käyttäjien tunnistamisen ja erilaisten palomuurien avulla.

Käytettävyys tarkoittaa sitä, että tiedot on saatavilla kohtuullisessa ajassa ja ne ovat käyttökelpoisessa muodossa. Käytettävyyttä tietoverkoissa ylläpidetään takaamalla riittävä kaistanleveys ja varayhteydet. (Hakala, Vainio 342)

6.2 Pääsynvalvonta ja kiistämättömyys

Aikaisemmissa kappaleissa olevien tekijöiden lisäksi monet tietoturvallisuusmääritelmät käyttävät termejä pääsynvalvonta ja kiistämättömyys. Pääsynvalvonnalla tarkoitetaan kaikkia niitä mekanismeja, joilla eri käyttäjät tunnistetaan, ja kuinka tietojärjestelmiin pääsyä rajoitetaan.

Kiistämättömyydellä tarkoitetaan sitä, että tietojen käytöstä ja muuttamisesta jää merkintä käyttötietoihin.

Pääsynvalvontaa ja kiistämättömyyttä varmistetaan käyttämällä salausta hyödyntäviä tunnistuspalvelimia ja lokipalveluja. (Hakala, Vainio 342)

6.3 Verkkoihin kohdistuvat uhat

Tiedonsaannin estyminen on yleisin tietoverkkoihin kohdistuva ja useimmin tapahtuva uhka. Tiedonsaannin estyminen tapahtuu, kun verkossa olevat aktiivilaitteet, verkkokortit tai kaapelointi vikaantuu. Tämä estää pääsyn palveluihin ja niiden sisältämiin tietoihin.

Tiedon saanti voi estyä myös tahallisen palvelun tukkivan hyökkäyksen takia. Nykyisin internetissä olevat tietojärjestelmät oon yleensä varustettu palomuureilla, jotka estävät pääsyn sisään tietojärjestelmiin.

Ongelmana on enemmänkin se, että hakkerit tukkivat organisaation julkisia palvelimia ja aktiivilaitteita niin suurilla sanomamäärillä, ettei ne voi enää vastata käyttäjien palvelupyyntöihin. (Hakala, Vainio 342)

6.4 Palomuurit

Palomuuri on käsitteenä hieman epämääräinen. Sillä voidaan tarkoittaa eri tyyppisiä laitteita tai ohjelmistoja, joiden avulla pyritään estämään asiattomien henkilöiden pääsy verkkoon tai tiettyyn verkon palveluun.

Toimintansa puolesta palomuurit voidaan jakaa kolmeen perustyyppiin: pakettisuodattimiin, välityspalvelimiin ja sovellustason yhdyskäytäviin.

Pakettisuodatin on laite, joka hylkää liikennettä lähde- ja kohdeosoitteiden sekä sovellusten käyttämien porttinumeroiden perusteella.

Välityspalvelimet taas avaavat käyttäjän puolesta yhteyden johonkin tiettyyn palveluun. Palveluihin voidaan määritellä etukäteen, mistä laitteista yhteys niihin voidaan muodostaa. Tämän avulla voidaan myös varmistaa käyttäjän luotettava tunnistus eli autentikointi, ennen kuin yhteys avataan. Näitä kutsutaan Proxy-palomuureiksi. Proxy palomuureissa on ongelmana se, että ne jättävät yhteyden palveluun auki, kunnes palvelua tarjoava palvelin sen sulkee.

Tietoturvan kannalta tehokkain palomuuri on sovellustason yhdyskäytävä (Application Level Gateway). Sovellustason yhdyskäytävä välittää liikenteen asiakas- ja palvelinohjelmiston välillä ja tutkii kaikkien pakettien sisällön. Se tutkii kaikki lävitseen kulkevat sallitun liikenteen paketit yksitellen ja analysoi niiden sisällön, ennen kuin ne lähetetään eteenpäin.

Kun se törmää normaalista poikkeaviin paketteihin, niitä ei välitetä eteenpäin, ja niitä voidaan tallentaa myöhempää analyysiä varten. Epäilyttävien pakettien löytyessä se tekee hälytyksen, jonka näkee palomuurista vastaavat henkilöt.

Huolellisesti suunniteltuna pakettiensuodatus on riittävä menetelmä torjumaan ulkopuoliset hyökkäykset. (Hakala, Vainio 347)

6.5 Pääsylistat

Pääsylistoja (Access List) käytetään reitittimien ja siihen liitettyjen verkkojen käyttöoikeuksien määrittämiseen. Pääsylistoja käytetään palomuuritoimintoihin

sekä erilaisten päivitystietojen rajoittamiseen. Pääsylistat voidaan jakaa kahteen ryhmään: vakiolistoihin (IP standard) sekä laajennettuihin listoihin.

Vakiolistoja voidaan käyttää rajoittavana listana. Se määrittelee, mistä osoitteista tulleet päivitykset voidaan hyväksyä. Vakiolistan avulla voidaan määrittää osoitteet, joista tuleva liikenne voidaan joko hyväksyä tai hylätä.

Laajennettuja listoja käytetään silloin, kun halutaan määritellä liikennettä tarkemmin. Voidaan määritellä sekä lähde- että kohdeosoite, protokollantyyppi, lähde- ja kohdeportit sekä yhteyden muodostuksen suunta. (Hakala, Vainio 348)

7 PÄÄTELAITTEEN ESITTELY JA ASENNUS

Vaasan kaupungille tulevat uudet DSL-päätelaitteet ovat Actelis ML622. Laitteiden konfiguraatiot tehdään laitteen omalla MetaASSIST Viewn -ohjelmalla. Tulen esittelemään laitteen ominaisuuksia. Esittelen, kuinka tehdään yleispätevä konfiguraatio, sekä kerron laitteen tietoturvallisuusominaisuuksista. Lisäksi teen Vaasan kaupungin toivomuksesta heille peruskonfiguraation, jota voitaisiin käyttää.

Testiympäristössäni loin linjan ethernet verkkokaapelin avulla kotonani. Tämän lisäksi olen ollut mukana yhteyden asennuksessa, josta näin, kuinka laitteet toimivat kenttäoloissa ja kuinka asennus tapahtuu kuparikaapelin avulla. Actelis ML622-laite edestä ja takaa kuvassa 4.

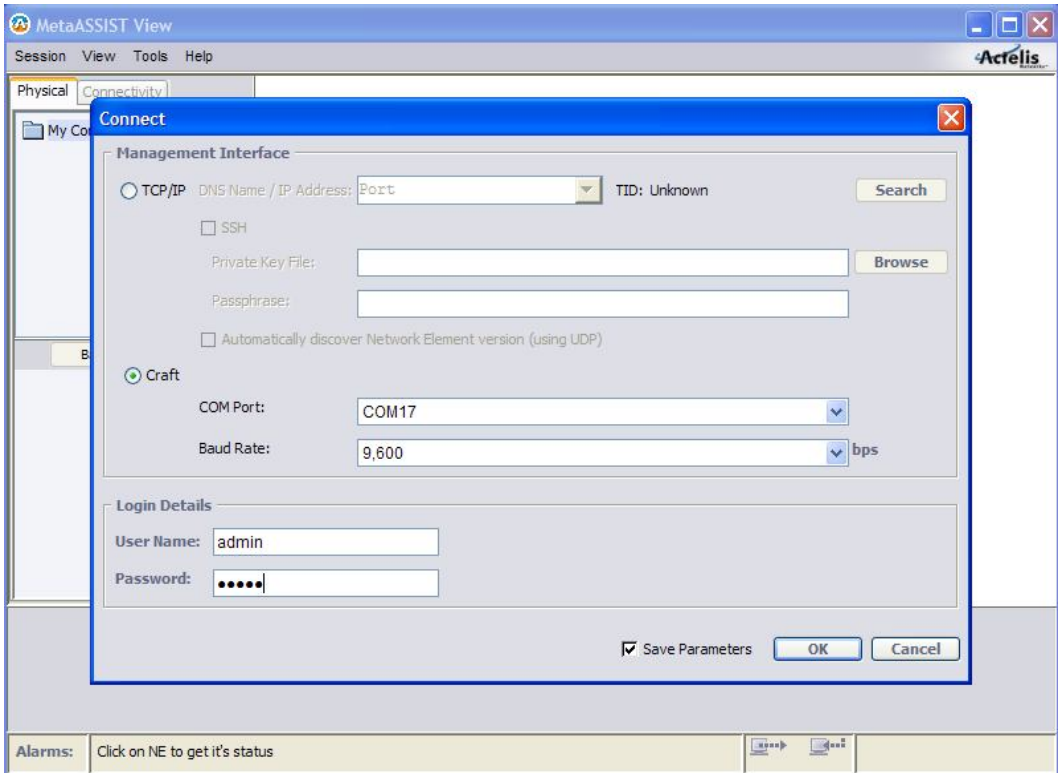
Kuva 4. Actelis ML622-laite edestä ja takaa.

7.1 Actelis ML622-laitteen asennusyhteyden muodostus

Kaikkien Actelis-laitteiden asennus tehdään heidän omalla MetaASSIST Viewn nimisellä -ohjelmalla. Laitteeseen otetaan yhteys ensimmäisen kerran CRAFT-kaapelilla, joka on RS-323 sarjakaapeli. Tämä johtuu siitä, että laitteella ei ole vielä IP-asetuksia.

Tietokoneissa, joissa ei ole sarjaporttia, joudutaan käyttämään USB-adapteria. Tämän lisäksi täytyy asentaa Windows-päivitys, jonka jälkeen tietokone tunnistaa sarjaportin.

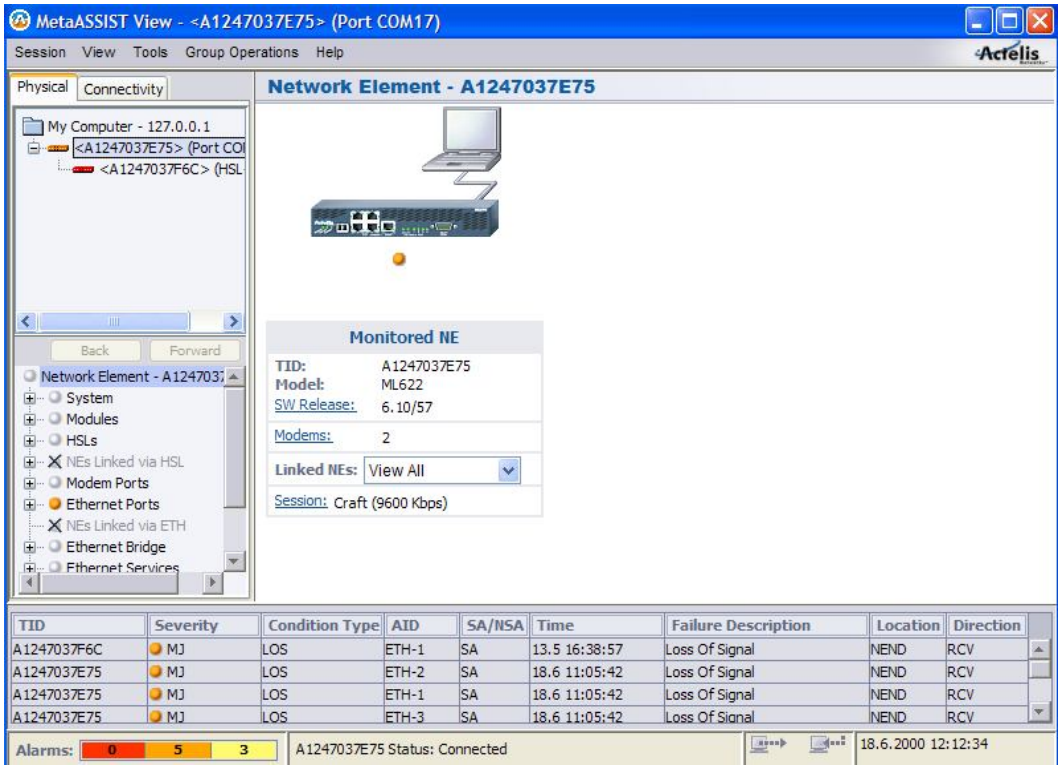
MetaASSIST -ohjelma voidaan avata, kun laite on liitetty CRAFT-kaapelilla. Huomasin, että kannattaa odottaa hetken aikaa, että ohjelma tunnistaa yhteyden. MetaASSIST -ohjelman käynnistyttyä valitaan Management Interfaceksi Craft ja valitaan COM-porttilistasta koneen COM-portti. Tämän voi tarkistaa tietokoneen laitehallinnasta. Yhteysnopeutena käytetään 9 600 bps. Tämän jälkeen laitetaan käyttäjätunnus ja salasana. Oletus käyttäjätunnus ja salasana löytyvät laitteen manuaalista. MetaASSIST View yhteyden muodostus esitetty kuvassa 5.



Kuva 5. MetaASSIST View yhteyden muodostus.

7.2 MetaASSIST Viewn- päävalikko

Seuraavassa kuvassa nähdään MetaASSIST View kirjautuneena sisään päävalikkoon. Päävalikossa on neljä eri osaa. Pienessä laatikossa vasemmassa yläreunassa näkyvät laitteet ja niiden suhteet toisiinsa. Tämän alapuolella olevassa laatikossa näkyy lista asetuksista, joita laitteelle voidaan määritellä. Asetuksia tulee enemmän kun painetaan + -merkkiä. Oikealla oleva laatikko on alue, jossa itse asetukset määritellään. Alareunassa näkyvät hälytykset. MetaASSIST Viewn- päävalikko on esitelty kuvassa 6.

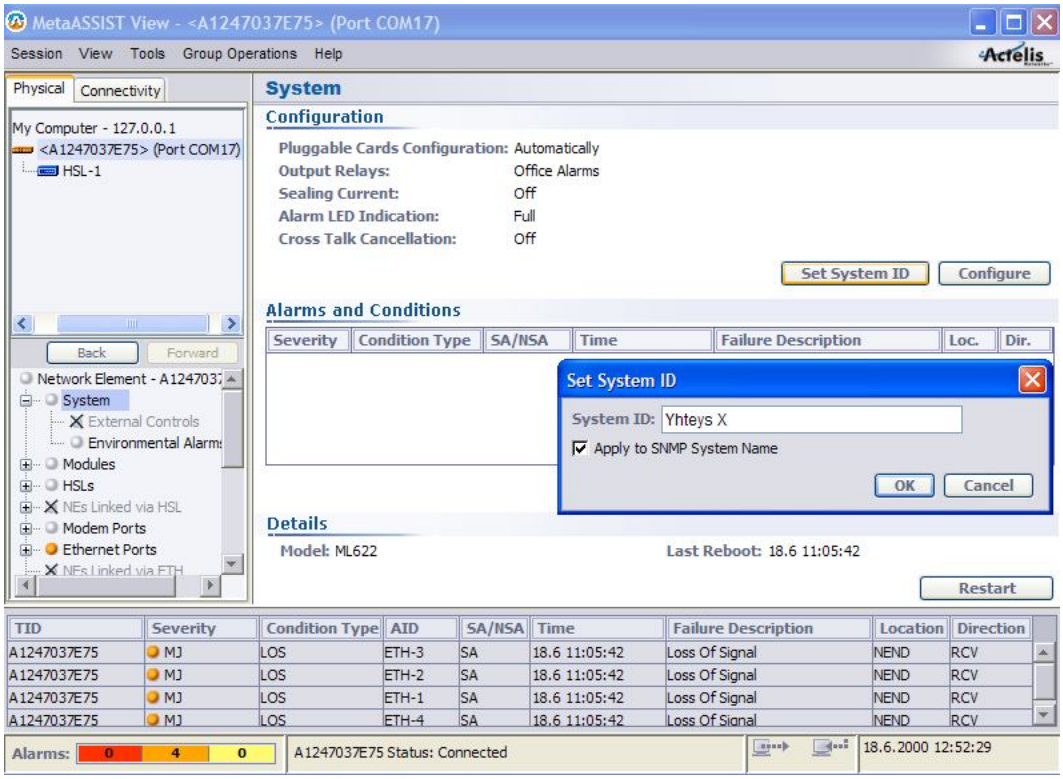


Kuva 6. MetaASSIST View päävalikko

7.3 Laitteen nimeäminen ja käyttäjätunnusten hallinta

Ensimmäisenä konfiguraationa suosittelisin laitteen nimeämistä ja käyttäjätunnusten salasanojen vaihtoa. Laitteen nimeksi kannattaa laittaa kyseistä yhteyttä kuvaava nimi. Nimessä voisi tulla ilm,i missä laite sijaitsee. Tämä helpottaa jatkossa vianselvitystä.

Laitteen nimen antaminen tapahtuu System-valikossa. Siellä valitaan Set System ID, jota painamalla ilmestyy pieni ikkuna, johon nimi laitetaan. Täällä voidaan myös valita Apply to SNMP System name. Tämä ikkuna kannattaa valita, koska se mahdollistaa kyselyjen tekemisen laitteen tilasta sekä laite voi lähettää itse hälytyksiä. MetaASSIST Viewn- laitteen nimeäminen on esitelty kuvassa 7.

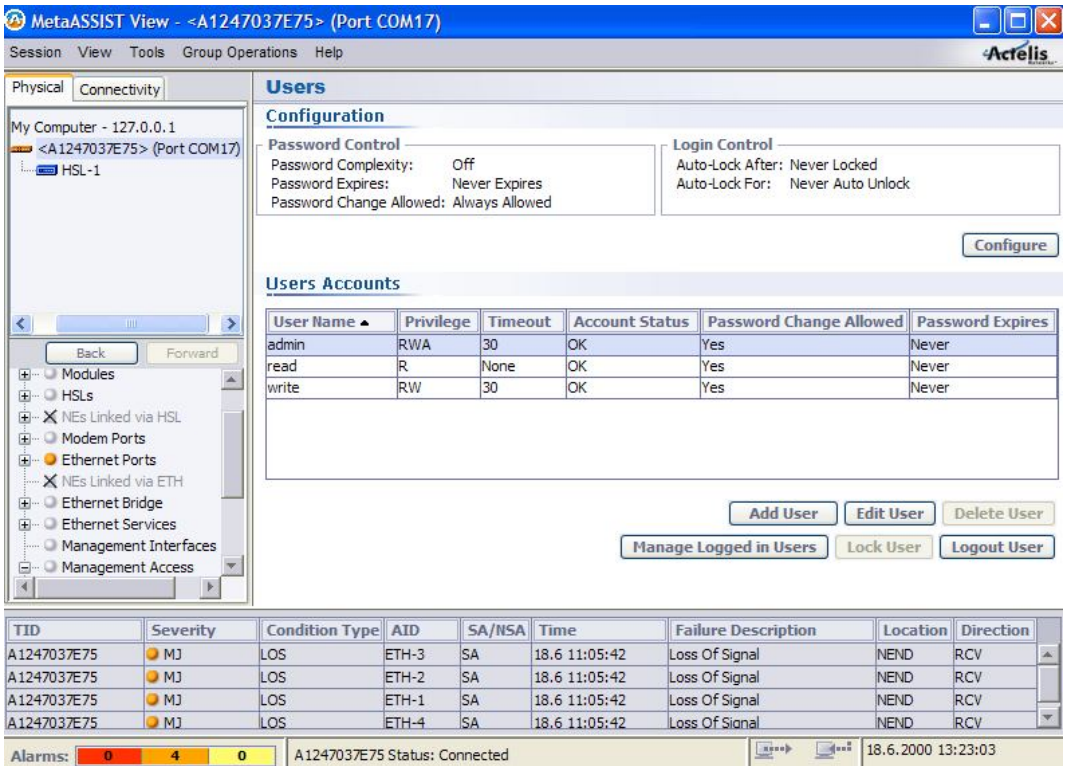


Kuva 7. Laitteen nimeäminen MetaASSIST Viewillä.

Käyttäjätunnusten hallinta tapahtuu Management Access -valikossa olevassa User -alavalikosta. Laitteessa on kolme oletustunnusta: admin, read ja write. Laitteeseen voidaan maksimissaan luoda 100 eri käyttäjätunnusta, joille voidaan antaa erilaisia käyttöoikeuksia.

Salasanan voi määrittää valitsemalla tunnus, jolle salasana valitaan ja painamalla Edit user. Itse suosittelisin tekemään uudet tunnukset ja poistamaan laitteessa valmiiksi olevat tunnukset tietoturvasyistä.

Users- valikossa olevasta Configure- valikosta voidaan määrittää, kuinka usein salasana tulee vaihtaa tai kuinka nopeasti viime vaihdosta sen voi vaihtaa. Lisäksi voidaan määrittää, kuinka monta kertaa salasanan voi laittaa väärin, ennen kuin tunnus menee lukkoon. Samassa valikossa voidaan määrittää, kuinka kauaksi aikaa tunnus lukkiutuu, kun salasana on laitettu väärin liian monta kertaa. Käyttäjätunnusten hallinta on esitetty kuvassa 8.



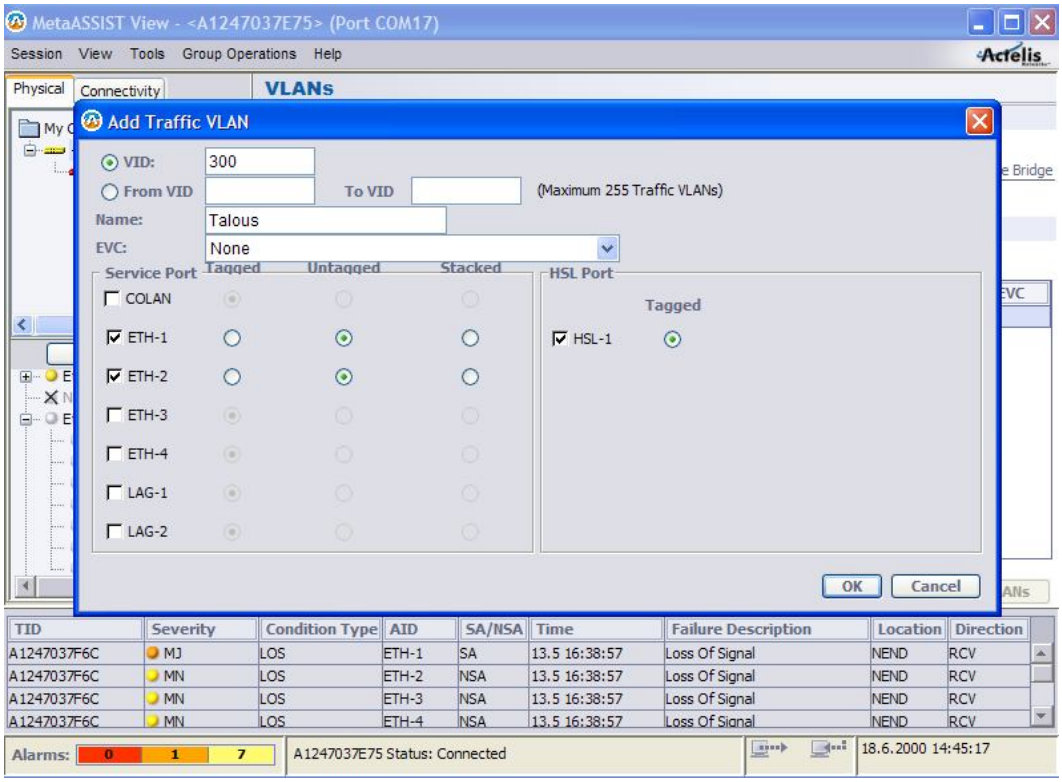
Kuva 8. Käyttäjätunnusten hallinta

7.4 Virtuaalilähiverkkojen ja IP-asetusten määrittäminen

Virtuaalilähiverkkojen määritys tapahtuu Ethernet Bridge -valikon alla olevasta VLANs -alavalikosta. Laitteessa on vakiona hallinnalle oma virtuaalilähiverkko, jota voidaan muokata omaan käyttötarkoitukseen sopivaksi. Virtuaalilähiverkkojen muokkaaminen tapahtuu valitsemalla haluttu VID Virtual Lan ID ja painamalla Edit VLAN -painikkeesta. Täällä voidaan määritellä, mitkä portit kuuluvat tiettyyn virtuaalilähiverkkoon.

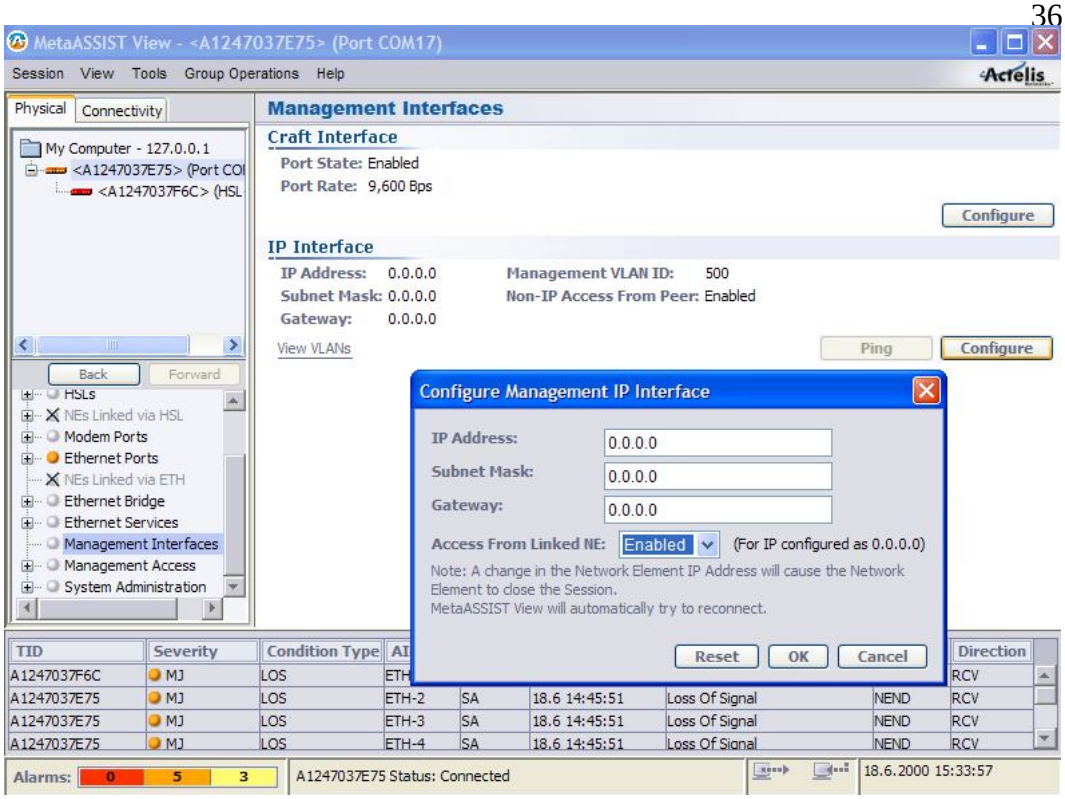
Porteille voidaan määrittää ovatko ne tagged vai untagged. Tagged -määritystä käytetään esimerkiksi reitittimille, jotka tukevat virtuaalilähiverkkoja. Untagged -määritystä taas käytetään laitteille, jotka eivät tue virtuaalilähiverkkoja.

Laitteeseen voi myös luoda uusia virtuaalilähiverkkoja. Tämä tapahtuu Add VLAN -painikkeesta. Seuraavassa kuvassa luodaan virtuaalilähiverkko Talous, johon liitetään Ethernet -portit yksi ja kaksi. Virtuaalilähiverkon lisääminen on kuvassa 9.



Kuva 9. Virtuaalilähiverkon lisääminen

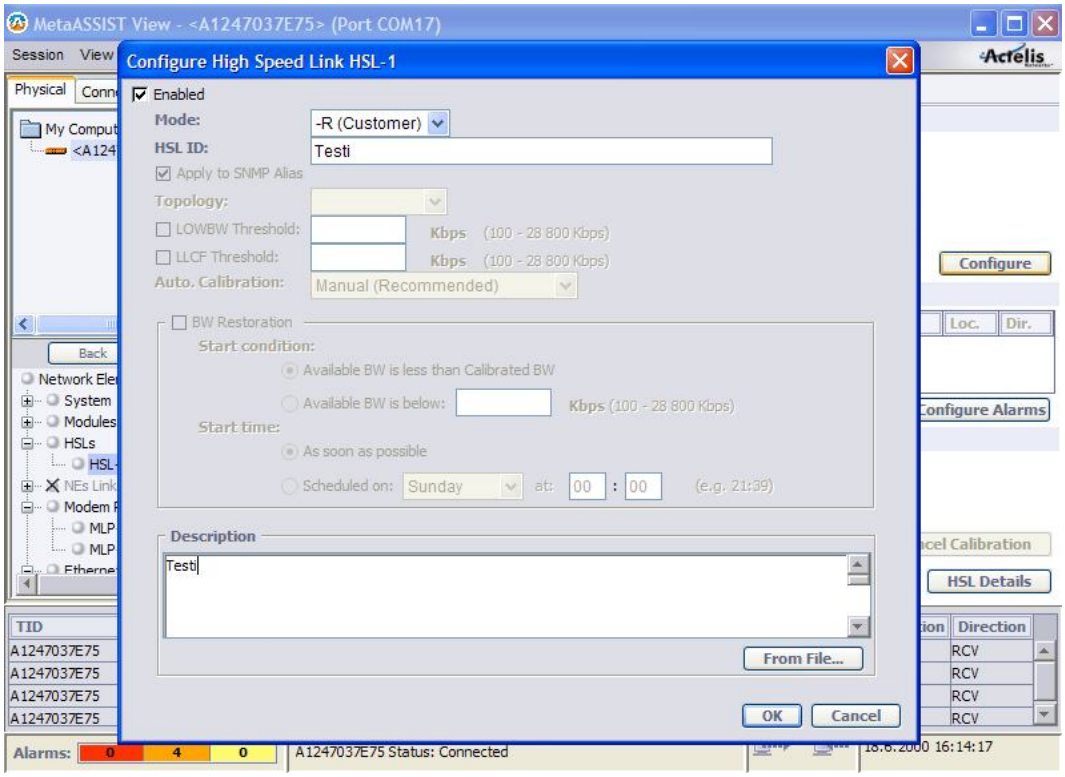
Laitteen IP-osoitteen voi muuttaa Management Interfaces -valikosta. IP Interface-kohdasta löytyy Configure -näppäin, sitä painamalla aukeaa valikko, jossa määritetään IP-osoite, maski ja yhdyskäytävä. Kun IP-osoite on määritetty, voidaan laitteeseen ottaa yhteys käyttämällä sitä. IP-osoitteen määrittely on kuvassa 10.



Kuva 10. IP-osoitteen määrittäminen

7.5 HSL-yhteyden luonti

Edellä olevien määritysten jälkeen luodaan HSL-yhteys. HSL-yhteys luodaan HSLs -valikon Configure- näppäimellä. Mode- kohdassa määritellään laite joko hallitsevaksi O (Office) tai vastaanottavaksi R (Customer). HSL ID- kohtaan voidaan syöttää HSL-yhteydelle nimi. Description- kohtaan voidaan kirjoittaa tai ladata tiedostosta kuvaus yhteydestä. Muita asetuksia ei tarvitse muuttaa. HSL-yhteyden luonti on kuvassa 11.



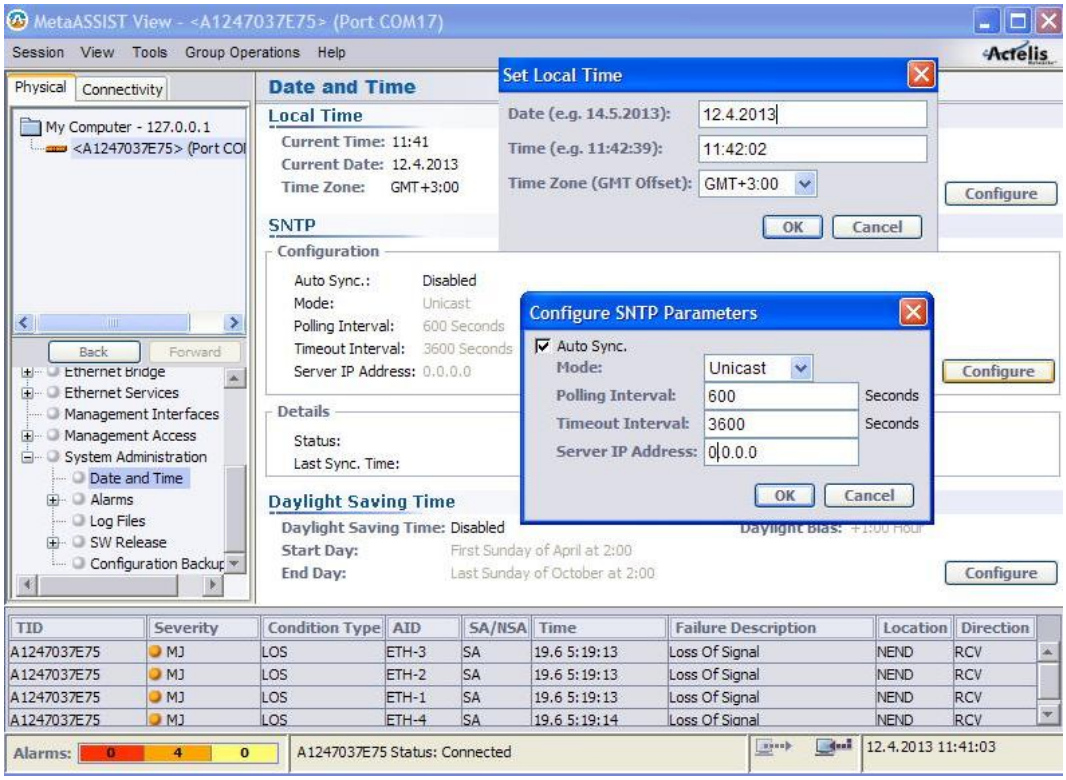
Kuva 11. HSL-yhteyden luonti.

7.6 Laitteen kellonajan määritys

Laitteelle kannattaa asettaa oikea kellonaika, koska tämä helpottaa vianselvityksessä . Vikaa on helpompi selvittää, kun tiedetään, koska se on ilmaantunut. Kellonajat voidaan määritellä joko käsin tai se voidaan myös hakea SNTP-palvelimen kautta. Käsin määrittelyssä tulee ottaa huomioon aikavyöhyke sekä kesä- ja talviaikojen oikeellisuus, muuten kellonaika tulee vääräksi, kun kesä- tai talviaika vaihtuu. Kellonaika määritellään laitteen System administration -valikon Data and Timen- alavalikossa.

Käsin määrittely tehdään Local Time kohdan Configure -näppäimen kautta. Tässä valikossa määritetään Date (Päivä), Time (Aika) ja Time Zone (Aikavyöhyke. Suomen aikavyöhyke on kesäaikana GMT +3 ja talviaikana GMT +2.

SNTP-palvelimen kautta määrittely tehdään SNTP -kohdan Configure -näppäimen kautta. Tänne määritetään käytössä olevan SNTP-palvelimen IP-osoite. Muita asetuksia ei tarvitse muuttaa. Tämän jälkeen laite hakee kellonaika -asetuksensa SNTP-palvelimen kautta. Kellonajan määrittäminen on kuvassa 12.



Kuva 12. Kellonajan määrittäminen.

Kuvassa olevat ikkunat eivät voi olla auki samaan aikaan, vaan olen tilan vuoksi leikannut toisen ikkunan ja liittänyt kuvaan.

7.7 Yhteyden muodostaminen päätelaitteilla

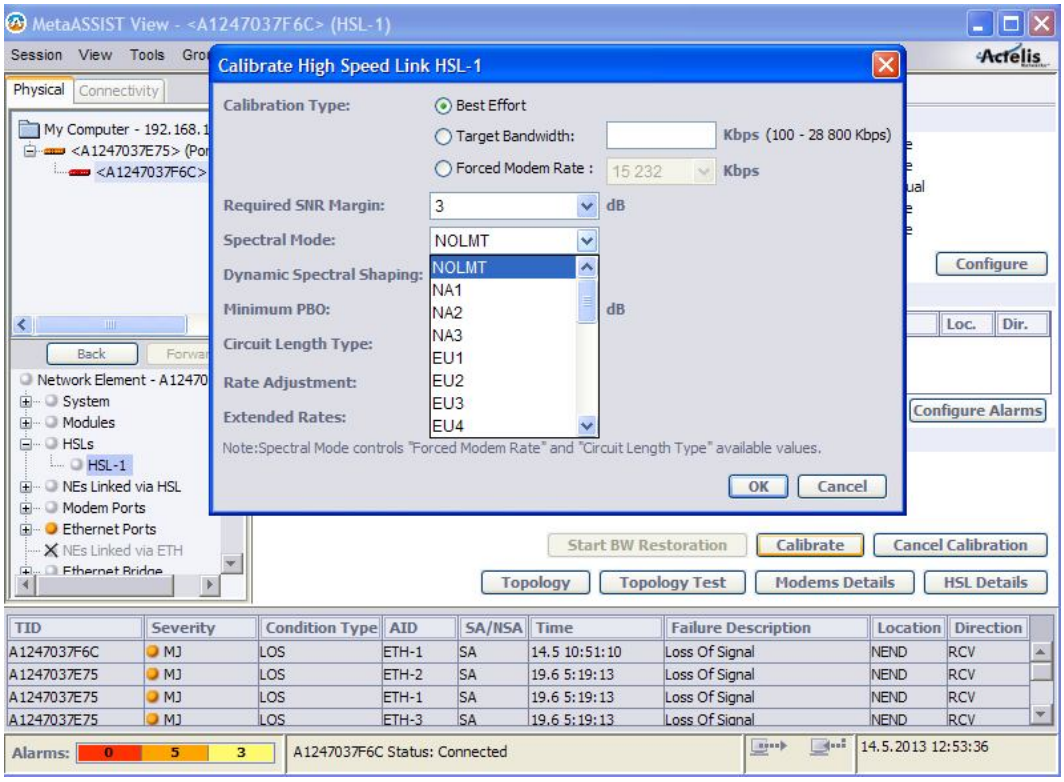
Edellä olevien asetusten määrittämisen jälkeen voidaan yhteyslaitteet liittää toisiinsa. Laitteet liitetään toisiinsa niiden takana olevien Copper Pairs (Kupariportit) -porttien avulla. Näitä portteja laitteessa on kaksi, joka tarkoittaa sitä, että laitteissa voidaan käyttää kahta kuparilinjaa. Käyttämällä kahta kuparilinjaa yhteydennopeus lisääntyy.

Kun laitteet on liitetty toisiinsa täytyy niiden välinen yhteys kalibroida. Laitteiden kalibrointi tehdään HSL-1n -laitteessa.

MetaASSIST Viewn -ohjelmassa valitaan vasemman ylänurkan laatikosta HSL-1 laite. Tämän jälkeen aukaistaan HSLs -valikon alta HSL-1 -alavalikko, ja sieltä painetaan Calibrate -näppäintä. Kalibrointityypiksi voidaan valita Best Effort tai

määritellä itse, kuinka nopeana yhteys pyritään saamaan. Linjan nopeuteen vaikuttaa kuparikaapelien pituus ja laatu. Minun ja Vaasan kaupungin asiantuntijoiden pystyttämät linjat ovat yhtä lukuunottamatta toimineet Best Effortn - automaattisella kalibroinnilla.

Käsin tehty kalibrointi tehdään muuttamalla Spectral Modea. Toiminnosta löytyy useita eri vaihtoehtoja linjan kalibrointiin. Vaihtoehdoissa pakotetaan linja toimimaan tietyllä nopeudella. Käsin kalibroimalla yhteyksien nopeutta voidaan saada paremmaksi, mutta se on herkempi häiriötilanteissa. Yhteyden nopeus voi olla maksimissaan 15 Mbit/s, käyttämällä kahta kuparikaapelia. Yhteyden kalibrointi kuvassa 13.



Kuva 13. Yhteyden kalibrointi

Kalibrointi kestää muutaman minuutin. Kalibroinnin jälkeen yhteys on valmiina käytettäväksi. Tämän jälkeen parantaisin laitteiden tietoturvallisuutta. Kerroin jo aluksi käyttäjätunnusten ja salasanojen vaihtamisesta. Tämän lisäksi on useita keinoja, joilla laitteen tietoturvallisuutta voidaan parantaa. Kerron tästä seuraavassa luvussa.

7.8 Tietoturvallisuuden parantaminen

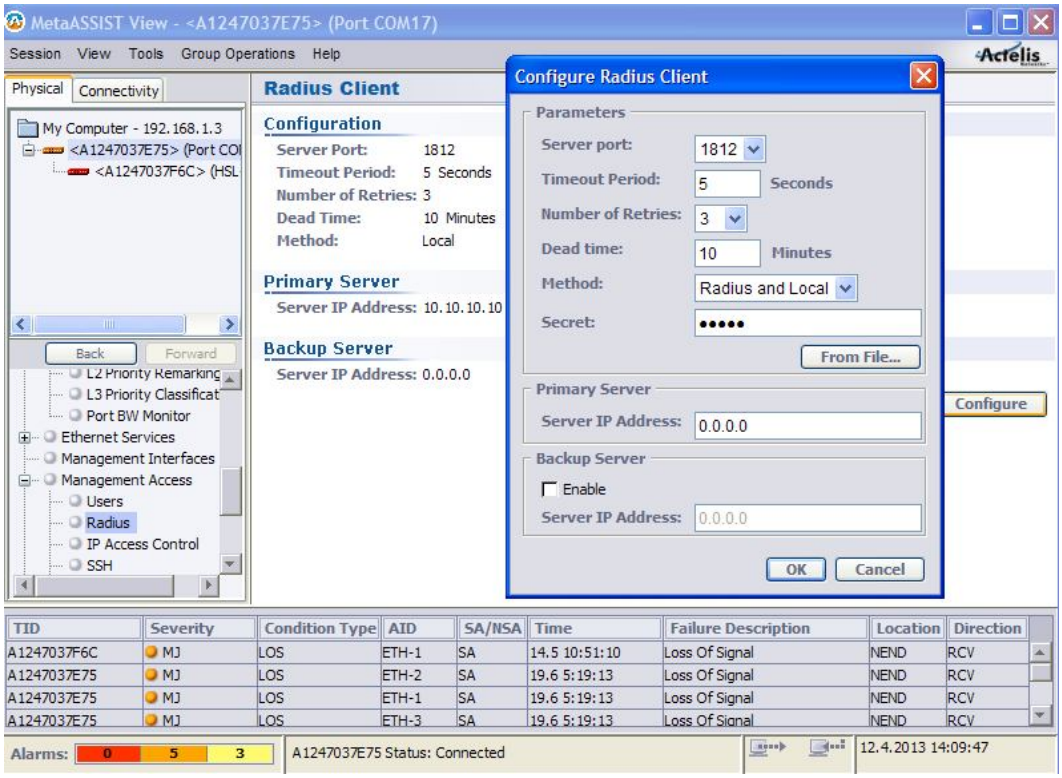
Actelis ML622n -laitteissa tietoturvallisuutta voidaan parantaa eri keinoilla. Käyttäjätunnusten ja salasanojen vaihtamisten lisäksi voidaan kirjautuminen laitteeseen hoitaa RADIUS (Remote Authentication Dial-In User Service) -palvelun avulla. Lisäksi kirjautuminen voidaan rajata vain tiettyihin IP-osoitteisiin. Laitteeseen otettavana yhteytenä voidaan käyttää myös salattua SSH (Secure Shell) -yhteyttä.

7.8.1 Radius-palvelun käyttöönotto

RADIUS-palvelun käyttöönotto vaatii sen, että verkossa on toiminnassa erillinen RADIUS-palvelin. RADIUS-palvelimella hoidetaan käyttäjätunnuksia ja salasanoja keskitetysti. Tässä Actelis ML622 on RADIUS-palvelimen asiakkaana, johon lähetetään tunnistuspyyntö.

RADIUS-palvelu voidaan ottaa käyttöön Management Access -valikon alta löytyvästä Radius -alavalikosta painamalla Configure näppäintä. Tässä ikkunassa täytyy valita palvelimen portti, metodi ja salasana, jota käytetään palvelimen ja Actelis ML622n -laitteen väliseen yhteyteen. Lisäksi täytyy antaa RADIUS-palvelimen IP-osoite sekä varmuuspalvelimen IP-osoite, jos sellainen on käytössä.

Metodina käyttäisin Radius and Local, koska jos käytetään vain Radius-metodia, yhteyttä ei voida muodostaa sarjakaapelin avulla. Radius-palvelun käyttöönotto kuvassa 14.



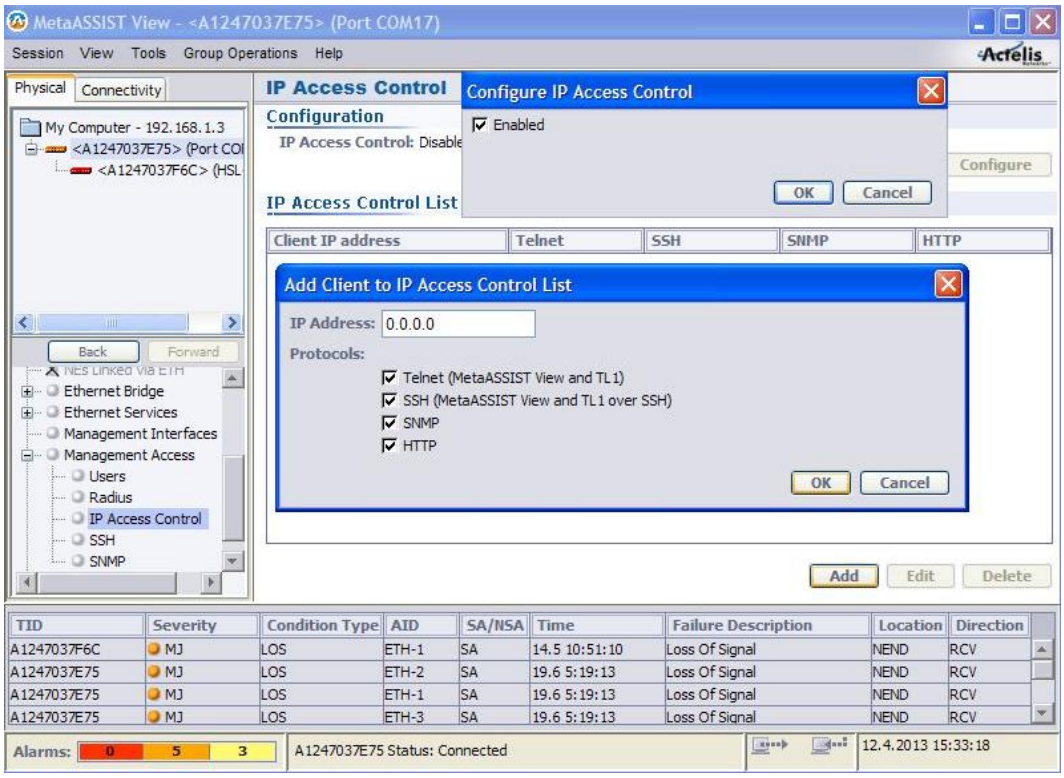
Kuva 14. Radius-palvelun käyttöönotto.

7.8.2 Kirjautumisen hallinta IP-osoitteilla

Laitteeseen voidaan määritellä, mistä IP-osoitteista siihen voidaan ottaa yhteyttä. Tämän toiminnon avulla voidaan rajata, miltä koneilta tai palvelimilta voidaan kirjautua laitteen hallintaan. Jos käytetään tätä suojausmekanismia, olisi mielestäni järkevintä antaa pääsy vain vaikka tietyiltä palvelimilta. Tämä tarkoittaisi sitä, että ensin täytyy pystyä kirjautumaan palvelimeen siihen vaadittavilla tunnuksilla. Tämän jälkeen täytyy vielä tietää itse laitteen kirjautumistunnus ja salasana.

IP-osoitteilla toimivan kirjautumisen voi ottaa käyttöön Management Accessn -valikon alta löytyvästä IP Access Control -alavalikosta. Ensin täytyy lisätä haluttu IP-osoite IP Access Control -listaan. Tämä tapahtuu painamalla Add -painiketta. Tästä aukeavaan ikkunaan annetaan sallittava IP-osoite ja valitaan, millä protokollilla yhteys voidaan ottaa. Näitä protokollia on Telnet, SSH, SNMP sekä HTTP.

Tämän jälkeen täytyy IP Access Control vielä sallia. Tämä tapahtuu Configuration -kentässä olevasta Configuration näppäimestä. Tästä aukeavaan ikkunaan täytyy vain laittaa rasti Enabled -kohtaan. Kirjautumisen hallinta IP-osoitteilla on esitetty kuvassa 15.



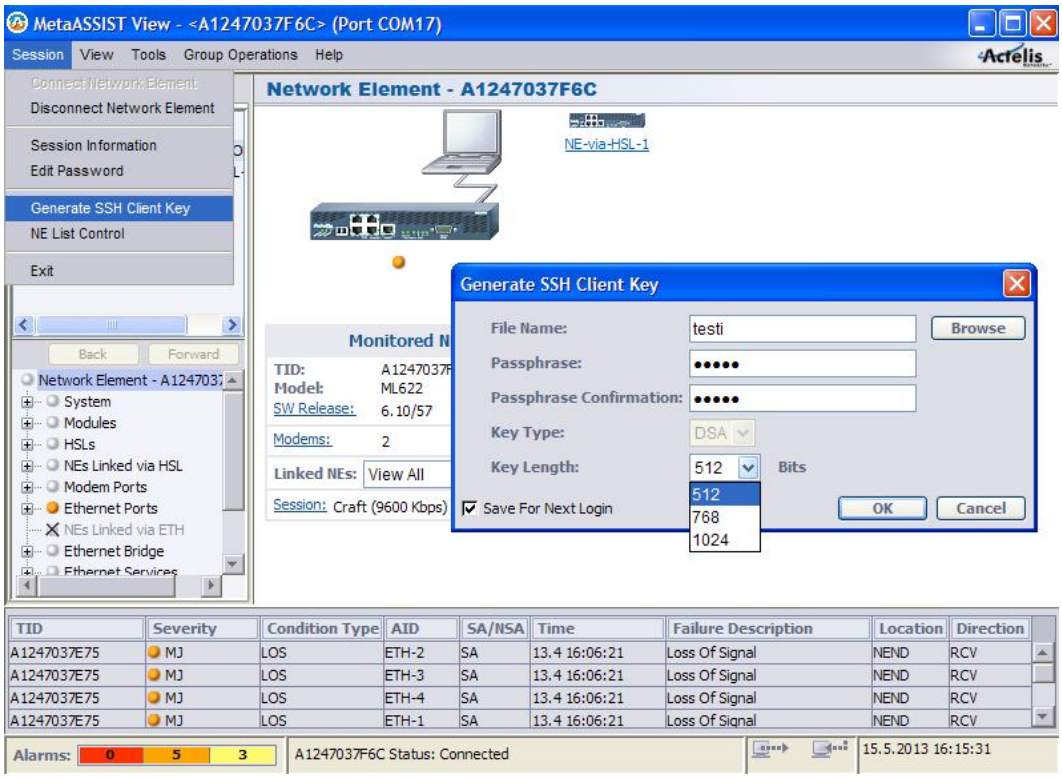
Kuva 15. Kirjautumisen hallinta IP-osoitteilla.

Kuvassa olevat ikkunat eivät voi olla auki samaan aikaan, vaan olen tilan vuoksi leikannut toisen ikkunan ja liittänyt kuvaan.

7.8.3 Salattu SSH-yhteys

Actelis ML622n -laitteeseen voidaan ottaa yhteys myös salatulla SSH-yhteydellä. SSH-tekniikan avulla laitteeseen kirjautuminen ja tiedon siirto MetaASSIST Viewn -ohjelman ja yhteyden ottavan laitteen välillä voidaan salata. Laite tukee 512-, 768- ja 1024-bittisiä DSA-kirjautumisavaimia. Laite käyttää AES-, DES-, 3DES- ja Blowfish algoritmeja salauksessa.

SSH-salauksen käyttöönotto vaatii muutamia toimenpiteitä. Ensin täytyy generoida SSH-asiakasavain. Se luodaan Session -ylävalikon kautta. Valitaan kohta Generate SSH Client Key, johon annetaan avaimelle nimi, salasana ja valita avaimen bittikoko. File Name kohdassa kannattaa valita Browse ja tallentaa avain haluamaansa paikkaan. Rastimalla Save For Next Login -kohta generoitua avainta käytetään seuraavan kirjautumisen yhteydessä. SSH-asiakasavaimen luonti esitetty kuvassa 16.



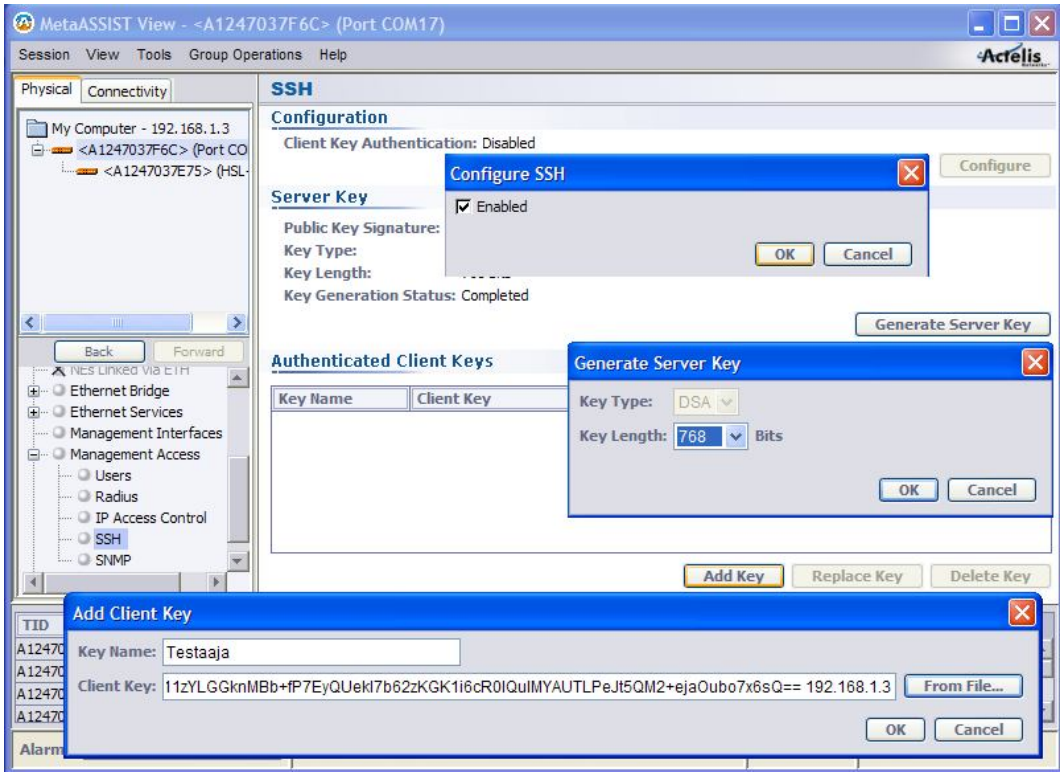
Kuva 16. Asiakasavaimen luonti

Avaimen luonnin jälkeen siirrytään seuraavaan vaiheeseen, joka on laitteessa olevan SSH-palvelimen konfigurointi. Tämä vaatii Admin -oikeuksia. SSH-palvelimen konfiguraatio tapahtuu Management Access valikon alla olevassa SSH alavalikossa.

Ensimmäiseksi generoidaan Server Key painamalla Generate Server Keyn -näppäintä. Valitaan avaimen pituus listasta ja painetaan OK, jonka jälkeen tulee varoitusikkuna, jossa kerrotaan, että uusi Server key generoidaan. Ohjelma kysyy Haluatko jatkaa. Tähän valitaan Yes.

Nyt voidaan lisätä tekemämme asiakasavain Authenticated Client Keys -listaan painamalla Add Key. Aukeavaan ikkunaan annetaan avaimelle nimi ja etsitään tallentamamme avain painamalla From File -näppäintä. Tämän jälkeen painetaan OK.

Tämän jälkeen täytyy ottaa käyttöön Client Key Authentication painamalla Configure näppäintä, josta aukeavaan ikkunaan rastitaan Enabled kohta päälle ja painetaan OK. SSH-palvelimen käyttöönotto on kuvassa 17.

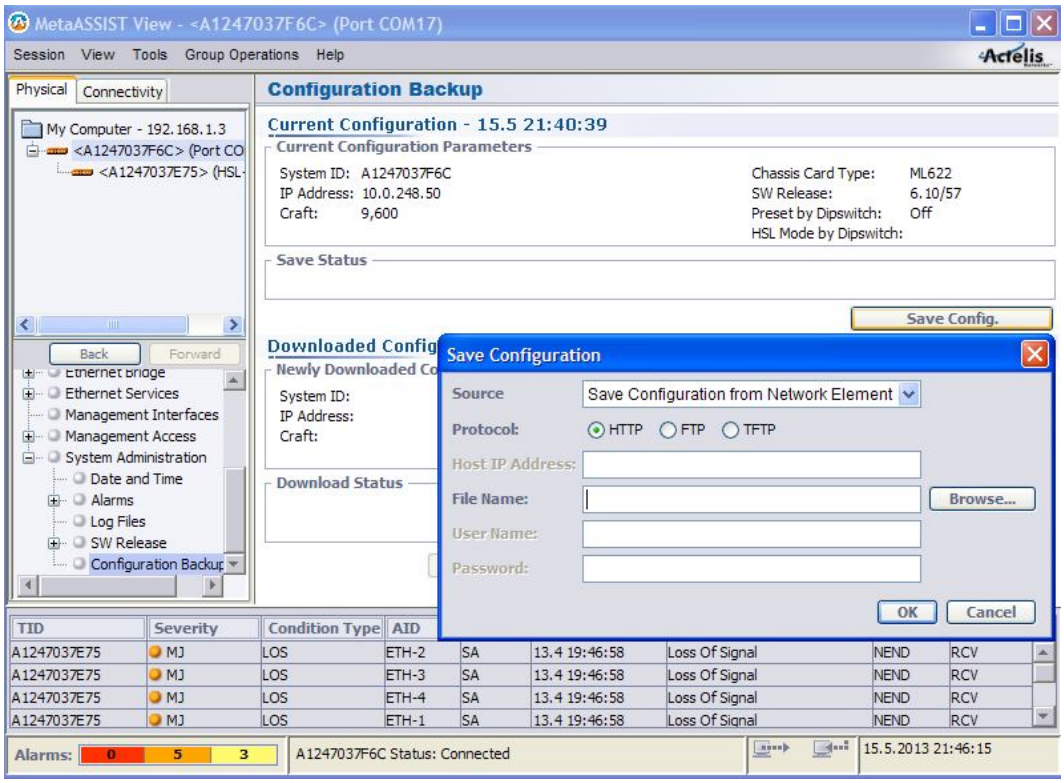


Kuva 17. SSH-palvelimen käyttöönotto

7.9 Varmuuskopion ottaminen konfiguraatiosta

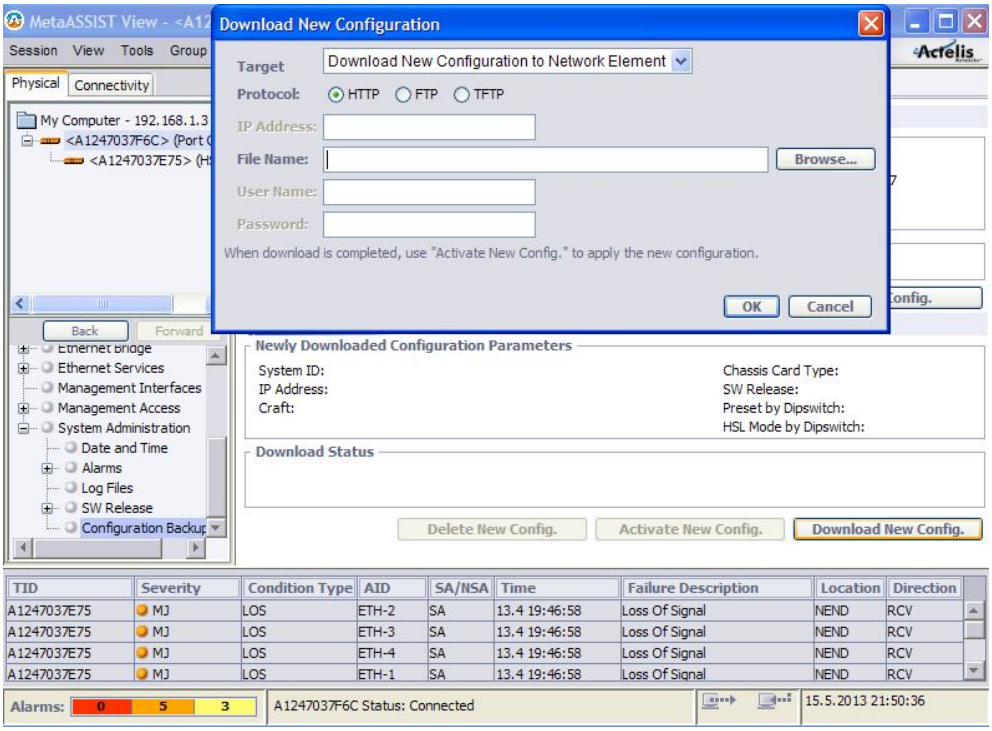
Laitteen konfiguraatiosta on mahdollista ottaa varmuuskopio, joka voidaan palauttaa ja aktivoida laitteeseen. Suosittelen varmuuskopiotoiminnon käyttöä. Varmuuskopiota ei pysty ottamaan craft-sarjakaapeliyhteydellä, vaan laitteeseen täytyy olla yhteydessä IP-osoitteen kautta.

Varmuuskopion ottaminen tapahtuu System Administration -valikon alta löytyvästä Configuration Backup -alavalikosta painamalla Save Config -näppäintä. Tässä ikkunassa täytyy valita protokolla, jonka avulla tiedosto tallennetaan. Lisäksi tiedostolle täytyy antaa nimi ja valita, mihin se tietokoneelle tallennetaan. Varmuuskopion tallentaminen kuvassa 18.



Kuva 18. Varmuuskopion tallentaminen.

Varmuuskopion palauttaminen ja aktivointi tapahtuu samassa valikossa painamalla Download New Config. Ensin haetaan palautettava konfiguraatio ja tämän jälkeen, jos se halutaan ottaa käyttöön, painetaan Activate New Config -näppäintä. Varmuuskopion palauttaminen ja aktivointi kuvassa 19.



Kuva 19. Varmuuskopion palauttaminen ja aktivointi.

8 YHTEENVETO

Opinnäytetyöni tarkoituksena oli perehtyä DSL-teknologiaan ja tutkia Vaasan kaupungin ATK-osastolle tulevien Actelis ML622n -laitteiden ominaisuuksia. Lisäksi tein yksityiskohtaisen esityksen itse laitteen asennuksesta.

Olen ollut kiinnostunut tietoliikenteeseen liittyvistä aiheista. Työtä tehdessä oma tietotaitoni ja osaamiseni aihepiiriin kasvoi. Työn tilaajan hyötynä oli se, että he saavat lisää hyödyllistä tietoa laitteesta ja sen eri ominaisuuksista.

Testasin laitetta testiympäristössä ja kenttäoloissa. Laite vaikutti mielestäni todella hyvältä DSL-yhteyden käyttötarkoituksiin. Laitteesta löytyi paljon hyödyllisiä ominaisuuksia ja tietoturvallisuutta pystytään lisäämään monilla eri tavoilla.

Laitteessa pystytään käyttämään virtuaalisia lähiverkkoja, jota pidin todella hyvänä ominaisuutena, koska ei tarvitse hankkia erillisiä kytkimiä hoitamaan tätä asiaa. Laitemäärä voi mahdollisesti vähentyä ja säästetään kustannuksissa.

Uskon, että DSL-yhteydet tulevat olemaan käytössä vielä useita vuosia. Ne ovat halpoja toteuttaa ja yhteysnopeudet saadaan tarpeeksi nopeiksi nykyajan tarpeisiin. Yrityskäytössä niitä on käytössä paljon pienissä toimipisteissä, joissa yhteysnopeuden ei tarvitse olla kovin nopea. DSL-yhteys riittää myös puhelujen soittoon ja vastaanottoon varsin hyvin.

Työssäni eniten aikaa käytin laitteen tutkimiseen ja testaukseen. Laitteen manuaalia täytyi tutkia, jotta ymmärsi, mitä eri ominaisuudet tekevät ja tarkoittavat. Konfiguraatioon käytettävä MetaASSIST Viewn -ohjelma oli looginen ja helppokäyttöinen. Konfiguraatiota tehdessä ei tarvinnut välittää siitä, että tekisi jotain peruuttamatonta, koska sen pystyi resetoimaan. Laitteen tutkiminen ja testaaminen oli mielenkiintoista ja siihen oli mukava perehtyä.

Kirjallisen osan tekeminen tapahtui aika nopeasti, kunhan vain pääsin alkuun. Vaikein osa oli löytää luotettavia lähteitä. Varsinkin elektronisten lähteiden käyttäminen oli vaikeaa, koska luotettavia sivustoja ei meinannut löytyä. Tästä syystä käytinkin enimmäkseen kirjallisia lähteitä. Kirjallisuutta aiheestani löytyi vanhemmista 2000-luvun kirjoista. Tähän varmasti vaikutti, että aiheeni oli iäkkäästä tekniikasta.

Kaiken kaikkiaan olen tyytyväinen työn lopputulokseen. Henkilökohtaisella tasolla sain työtä tehdessä paljon uutta tietoa DSL-tekniikoista ja tietoverkoista. Vaasan kaupungin ATK-osasto hyötyi työstäni siltä osin, että voivat käyttää tekemääni peruskonfiguraatiota ja saivat laitteesta paljon tietoa.

LÄHTEET

Kirjat

Cisco Press – Suom. Holttinen, Jarmo 2002, Cisco Verkkoakatemia Ensimmäinen vuosi. Helsinki. Edita.

Granlund, Kaj 2007. Tietoliikenne 1.painos. Jyväskylä. WSOY/Docendo

Hakala, Mika. Vainio, Mika 2005. Tietoverkon rakentaminen 1. painos. Jyväskylä. WSOY/Docendo

Elektroniset julkaisut

Allied Telesis, DSL White Paper. [verkkodokumentti]. [viitattu 15.4.2013]. Saatavissa:
http://www.alliedtelesis.fi/media/pdf/dsl_wp.pdf

Draka uutinen, Kuparikaapelit hoitavat oman osansa laajakaistaverkossa. [www-sivu]. [viitattu30.4.2013]. Saatavissa:
http://www.draka.fi/draka/Countries/Draka_Finland/Languages/suomi/navigaatio/Uutiset/Arkisto/KuparikaapelitLaajakaistaverkossa.html

eHow tech, How Do DSL Modems Work?, [www-sivu]. [viitattu 30.4.2013]. Saatavissa:
http://www.ehow.com/how-does_4570094_dsl-modems-work.html

FiCom, ADSL. [www-sivu]. [viitattu 17.4.2013]. Saatavissa:
http://www.ficom.fi/tietoa/tietoa_4_1.html?Id=1045051770.html

Helkama Flash Cord 2001, Valokaapelit tele-ja tietoverkoissa. [verkkodokumentti]. [viitattu 30.4.2013]. Saatavissa:
http://helkamabica.fi/pdf/FlashCord-fi.pdf

Pulse Supply, ADSL and VDSL basics. [www-sivu]. [viitattu 19.4.2013]. Saatavissa:
http://www.pulsewan.com/data101/adsl_vdsl_basics.htm

Ratol. OSI-MALLI. [www-sivu]. [viitattu 24.5.2013] Saatavissa:
http://www.ratol.fi/opensource/lahiverkot/fin/yleista/osi_malli.htm

wiseGEEK, What is DSLAM?. [www-sivu]. [viitattu 30.4.2013]. Saatavissa: http://www.wisegeek.org/what-is-dslam.htm