TURVAJÄRJESTELMIEN ETÄHALLINTA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2006
Keijo Kokko

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

KOKKO, KEIJO: Turvajärjestelmien etähallinta

Tietoliikennetekniikan opinnäytetyö, 49 sivua, 6 liitesivua

Kevät 2006

TIIVISTELMÄ

Tämän opinnäytetyön aiheena oli kiinteistöjen hajautettujen turvajärjestelmien keskitetyn hallinnan suunnittelun mallinnus. Lisäksi tutkittiin hallintajärjestelmien ja siirtomedioiden luotettavuutta.

Mikäli järjestelmien suunnittelusta ei laadita dokumentointia, päädytään tilanteeseen, jossa ainoastaan asennustyön suorittaneella henkilöllä on riittävä kokonaiskuva turvajärjestelmistä sekä niiden hallinnasta. Turvallisuuden kannalta tämä on tietysti hyvä asia, mutta hallittavuus ja huollettavuus heikentyvät selkeästi kyseisen henkilön sairastuessa tai vaihtaessa työpaikkaa. Selkeästi dokumentoidulla suunnittelulla voidaan selkeyttää hajautettujen järjestelmien hallintaa sekä hyödyntää mallia uusien kohteiden tarjouslaskennassa ja toteutuksessa.

Järjestelmien keskitetty hallinta vaatii tiedon siirtämistä julkisen TCP-IP verkon yli. Siirtotien turvallisuus on tällöin ensiarvoisen tärkeää. Hallintajärjestelmien tietoturvallisuuden tasoa tutkittiin analysoimalla testikäyttöön rakennetun turvajärjestelmän ohjausliikennettä. Suunnittelun ja dokumentoinnin siirtäminen sähköiseen muotoon edellytti työkaluja, jotka helpottavat suunnitteluprosessia. Hälytinkeskusten liittäminen TCP-IP- verkkoon toteutetaan erillisten IP-osoitepäätteiden kautta. Kiinteistö IP-osoiteavaruuden ja vapaiden osoitteiden määrittäminen on turvalaiteasentajalle vieras ympäristö. Aliverkotuksen määrittämiseksi kehitettiin helppokäyttöinen Excel-pohjainen työkalu.

Hallintajärjestelmien tietoturvassa havaittiin tietty kahtiajako. Yhteydessä IP-osoitepäätteeseen ei käytetä mitään salausta, kun taas varsinainen liikenne hälytinkeskukseen kulkee salattuna. Tämän vuoksi sisäverkon ulkopuoliset yhteydet pitää aina muodostaa vahvasti salattuna VPN-yhteytenä. Lähitulevaisuudessa nykyiset modeemi-ja ISDN-yhteydet tulevat vaihtumaan laajakaistayhteyksiksi. Tämä saattaa johtaa turvallisuuden tason heikkenemiseen, mikäli yhteyksien tietoturvaan ei kiinnitetä riittävästi huomiota. Turvajärjestelmien suunnittelutyökaluna käytetään cad-perustaista turvasovellusta, josta voidaan tulostaa tarvittavat osaluettelot tarjouslaskentaan sekä toteutukseen. Suunnittelun mallinnukseen tarvitaan dokumentointijärjestelmä, jota voidaan kehittää ja muokata projektikohtaisesti. Tässä opinnäytetyössä laaditut työkalut helpottavat mallinnuksen hahmottamista ja antavat polttoainetta yrityksen oman kehitystyön jatkumiselle.

Asiasanat: turvajärjestelmä, etähallinta, suunnittelukonsepti, mallinnus

Lahti University of Applied Sciences
Faculty of Technology

KOKKO, KEIJO: The remote controlling of security systems

Bachelor's Thesis in Telecommunications Technology, 49 pages, 6 appendices

Spring 2006

ABSTRACT

The topic of this thesis was to create a model for controlling the distributed security systems of real estates. In addition, the reliability of controlling systems and transporting media was examined.

If system development is not properly documented, there is a risk that only a few persons have a clear idea or explicit information of the security systems and of how to control them. From the point of view of security this situation is good but system controlling and service could suffer if the persons are unavailable.
With distinctly documented planning it is possible to clarify the controlling of distributed security systems and exploit this model in calculating and executing new projects.

Centralized administration of security systems requires transporting information over a public TCP-IP network. The security of the network is therefore extremely important. The level of the data protection was examined by analyzing the controlling data transportation of the test security system. Exporting the system planning and documenting into the electronic format required tools that could help the planning process. Connecting the alarm central points to the TCP-IP network was executed by separate IP address terminals. Specifying the IP addressing space of the existing networks is a strange topic for security system installers. An easy-to- use Excel-based tool was developed to help to determine the subnet.

There was a certain division in two in the data security of the control systems. The connection to the IP addressing terminal does not use any kind of data encryption whereas the actual data communication to the security centre is encrypted. This is the reason why external connections to the intranet must always be established with a strong encrypted VPN connection. In the near future the current modem and ISDN connections will be changed to broadband connections. This could lead to weakening of security levels if not enough attention is paid to the data security of the connections. The planning tool for security systems is a CAD-based security application, from where you can print the required part lists for bidding calculations and actual execution. A documentation system that can be developed and edited for separate projects is needed. The tools that were developed in this thesis help to understand the model and make it easier for the company to do further system development in the future.

Keywords: security system, remote controlling, design concept, modelling

SISÄLLYS

LYHENNELUETTELO

ACK Acknowledgement, kuittauspaketti
ADSL Asymmetric Digital Subscriber Line, digitaalinen internet-yhteystekniikka
AP Access Point, langaton tukiasema
ARP Address Resolution Protocol, selvittää IP-osoitetta vastaavan laiteosoitteen
AT Auxillary Tone, Hayes komentokieli
ATM Asynchronous Transfer Mode, asynkroninen toimintamuoto
B-ISDN Broadband Integrated Services Digital Network, laajakaistainen digitaalinen piirikytkentäinen puhelinverkko
BRI Basic Rate Interface, ISDN perusliittymä
CAD Computer Aided Design, tietokoneavusteinen suunnittelu
CAP Carrierless Amplitude & Phase modulation, modulointimenetelmä
CHAP Challenge Handshake Authentication Protocol, yhteyden muodostamisprotokolla
CLNP ConnectionLess Network Protocol, yhteydetön verkkoprotokolla
CR (Configure Request), kantoaallon tunnussignaali
CRC Cyclic Redundancy Check, tarkistussumma.
CSMA/CA Carrier Sense Multiple Access with Collision Avoidance, liikennöintiprotokolla
CTS Clear To Send, ohjaussignaali
DES Data Encryption Standard, salausalgoritmi
DHCP Dynamic Host Configuration Protocol, verkkoprotokolla
DMT Discrete Multitone, diskreetti modulointimenetelmä
DPSK Differential Phase Shift Keying, nelivaiheinen vaihemodulaatio
DSR Data Set Ready**,** siirtolaite valmiina
DSSS Direct Sequence Spread Spectrum, suorasekvenssihajaspektri
DTR Data Terminal Ready, päätelaite toimintavalmis
ESP Encapsulating Security Payload, salausprotokolla
ETSI European Telecommunications Standards Institute
FHSS Frequency Hopping Spread Spectrum, taajuushyppely
FTP File Transfer Protocol, tiedonsiirtoprotokolla
GHz Gigahertsi
HDLC High-Level Data Link Control, tahdistettuun siirtoon sopivan yhteyskäytännön ohjausmenettely
HDSL High bitrate DSL / High-speed Digital Subscriber Line, nopea DSL-yhteys
ICMP Internet Control Message Protocol, sanomaviestien välitys
IEEE Institute of Electrical and Electronics Engineers, yhdysvaltalainen sähkö-, tietokone- ja tietoliikenneinsinöörien yhdistys
IPsec IP Security Architecture, tietoliikenneprotokolla Internet-yhteyksien turvaamiseen
IPX Internet Packet Exchange, yhteydetön liikennöintitapa työaseman ja palvelimen välillä
ISDN Integrated Services Digital Network, digitaalinen piirikytkentäinen puhelinverkko
ISM-kaista Industrial, Sientific and Medical band, 2,4 gigahertsin vapaa taajuuskaista
ITU-T International Telecommunications Union – Telecommunications, standardisointijärjestö
L2F Layer 2 Forwarding, Ciscon tunnelointiprotokolla
L2F Layer 2 Forwarding, tunnelointiprotokolla

L2TP Layer 2 Tunneling Protocol, tunnelointiprotokolla
L2TP Layer 2 Tunneling Protocol, tunnelointiprotokolla
LAN Local Area Network, lähiverkko.
LCP Link Control Protocol, protokolla, jota käytetään PPP yhteyden luomiseen
LVIS Lämpö Vesi Ilma Sähkö
MAC Medium Access Control, fyysisen tason hallintamenettely.
Mbps Megabits per second, megabittiä sekunnissa
MD5 message-digest, viestitiivistealgoritmi
MNP5 Microcom Network Protocol 5, tiedonpakkausprotokolla
NAT Network Address Translation, IP-osoitteen muunnosprotokolla
NCP Network Control Protocol, päästä päähän protokolla
NRZ No Return to Zero, kaksitasoinen nollaan palaamaton signalointimenetelmä
PAP Password Authentication Protocol, autentikointiprotokolla
PCM Pulse Coded Modulation, pulssikoodimodulaatio
PPP Point-to-Point Protocol, suora yhteys protokolla
PPTP Point-to-Point Tunneling Protocol, tunnelointiprotokolla
QAM Quadrature Amplitude Modulation, amplitudi- ja vaihemodululaatio
RARP Reverse Address Resolution Protocol, kysytään IP-osoitetta tunnetulle MAC-osoitteelle
RC4 salausalgoritmi
RIPE-MD Race Integrity Primitives Evaluation Message Digest, yksisuuntainen tiivistefunktio
SDSL Symmetric Digital Subscriber Line, symmetrinen DSL-yhteys
SHA 1 Secure Hash Algorithm 1, salausalgoritmi
SIP Session Initiation Protocol, avoin signalointiprotokolla
SMTP Simple Mail Transfer Protocol, sähköpostiprotokolla
SYN SYNc character**,** yhteyden avauspyyntö
TA Terminal Adapter, sovittaa ei ISDN laitteita ISDN verkkoon
TCM Trellis Coded Modulation, modulointitekniikka
TCP Transmission control protocol, Internet-verkkojen tietoliikenneprotokolla
TDM Time Division Multiplexing, aikajakokanavointi
UDP-User Datagram Protocol, yhteydetön protokolla.
WAN Wide Area Network, laajoja alueita yhdistävä tietokoneverkko.
VDSL Very high rate Digital Subscriber Line, nopea DSL-yhteys
WEP Wired Equivalent Privacy, salausprotokolla
WLAN Wireless Local Area Network, langaton lähiverkko
WPA Wi-Fi Protected Access, suojattu langaton yhteysratkaisu.
VPN Virtual Private Network, virtuaalinen yksityisverkko
xDSL x-type Digital Subscriber Line, x-tyypin DSL
XNS Extensible Name Service, autentikointiprotokolla

1 JOHDANTO

1.1 Työn tausta

Asumiseen liittyvien palvelujen kehittymisessä korostetaan yksilön huomioonottamista, hyvinvoinnin teknologiaa sekä turvallisuutta. Suuntaus tulee heijastumaan myös turvallisuuspalvelujen lisääntyvänä kysyntänä. Asiakaslähtöinen turvajärjestelmien suunnittelu mahdollistaa yksilöllisten turvaratkaisujen lisäksi asiakasryhmille valmiiksi tuotteistettujen ratkaisujen rakentamisen. Tuotteistaminen selkeyttää kokonaisuuden hallintaa ja osaltaan helpottaa asiakasta järjestelmien hankinnassa.

Kiinteistöjen talotekniikan integrointi rakenteisiin tulee olemaan tulevaisuuden haaste rakennustekniikalle. Turva-, valvonta- ja LVIS-tekniikka (Lämpö, Vesi, Ilma, Sähkö) pyritään automatisoimaan sekä liittämään keskitettyyn ohjausjärjestelmään. Asumiseen ja kiinteistöihin liittyvät turvapalvelut mielletään osaksi nykyaikaista kiinteistönpitoa.

Suomen väestörakenteen ikääntyminen tulee lisääntymään oleellisesti muutamassa vuosikymmenessä. Vuonna 2020 arvioidaan yli 65 vuotiaiden osuuden olevan 25 % koko väestöstä (Hyvä asuminen 2010 kehitysohjelma/Tilastokeskus). Palvelujen läheisyyteen muuttavien ikäihmisten vuoksi rakennusten kehittäminen turvallisemmiksi sekä helppokulkuisemmiksi tulee olemaan lähitulevaisuuden suuntaus.

Kiinteistöjen turvajärjestelmien tuotekehitys on ollut viime vuosina voimakasta. Kehitystä on tapahtunut tunnistinlaitteiden lisäksi myös järjestelmien hallinnassa. Keskitetty hallinta sekä automatisointi mahdollistavat kulkuoikeuksien sekä kiinteistöjen turvallisuuden valvonnan tehostamisen. Näin voidaan kohdistaa arvokkaita henkilöstöresursseja sellaisten työvaiheiden hoitoon, joita automatisointi ei voi korvata. Keskitetty hallinta lisää järjestelmien luotettavuutta sekä helpottaa niiden huoltoa ja päivitysten suorittamista. Kaupungit ja kunnat omistavat kiinteistöjä, jotka sijaitsevat usein kymmenien kilometrien päässä toisistaan. Kiinteistöjen eri käyttäjäryhmillä on erilaisia kulkuoikeuksia. Tilapäisille käyttäjille on pystyttävä järjestämään kulkuoikeudet sekä ohjaamaan

hälytysten poiskytkentä käyttövuoron ajaksi ja uudelleenkytkentä vuoron päätyttyä. (Hakala, Vainio 2005.)

1.2. Tavoitteet

Turvajärjestelmien hallinta on toteutetuissa kohteissa järjestetty käyttämällä modeemi- tai ISDN)-pohjaisia (Integrated Services Digital Network päästä päähän yhteyksiä. Kiinteistöissä olevat ADSL)-yhteydet (Asymmetric Digital Subscriber Line mahdollistavat nykyaikaisten salaus- ja tunnelointijärjestelmien avulla etähallinnan yhteyksien siirtämisen julkiseen TCP/IP-verkkoon (Transmission control protocol / Internet Protocol).

Tämän opinnäytetyön tarkoitus on tutkia teknisiä ratkaisuja, jotka voivat mahdollistaa etähallinnan siirtämisen kiinteistöissä jo mahdollisesti oleviin laajakaistayhteyksiin. Lisäksi tavoitteena on laatia suunnittelutyökaluja, joiden avulla konseptin monistaminen muihin kiinteistöympäristöihin helpottuu. Järjestelmästä tulisi muodostua joustava ja hallittava tuote. Hälytinjärjestelmien suunnittelussa on mahdollista hyödyntää CADS-turvasovellusta, jonka avulla sähköisiin pohjapiirroksiin voidaan sijoittaa tunnistimet, johdotukset sekä keskukset. Turvasovelluksesta voidaan tulostaa osaluettelot, joiden avulla tarjouslaskennan sekä varsinaisen toteutusvaiheen tilausten laatiminen helpottuu.

Järjestelmien rakentaminen kehittyy yleensä osatekijöistä, joihin vaikuttavat tilojen käyttäjät ja heidän vaatimuksensa. Kaupungin tai kunnan omistuksessa on lukuisia kiinteistöjä, joissa saattaa olla hyvinkin erilaisia turvavaatimuksia, käytettävyysvaatimuksia ja käyttäjiä. Järjestelmien yhteinen hallinta vaatii eri komponenttien soveltumista käytettävissä olevaan siirtomediaan. Mallinnus ja dokumentointijärjestelmä auttavat suunnittelua, kustannuslaskentaa, asennusta ja ylläpitoa.

Lahden Kiinteistöturvallisuus kuuluu valtakunnalliseen Turvaykköset-ketjuun. Yrityksen laajamittaisena projektina on ollut rakentaa Orimattilan kaupungin kulunvalvonta-, hälytys- ja valvontaverkosto, jota voidaan hallinnoida keskitetysti normaalia tietoverkkoa käyttäen. Järjestelmää on rakennettu Suomalaisen Hedpro Oy:n kehittämillä ja valmistamilla tuotteilla. Keskitetylle järjestelmälle on ollut kiinnostusta myös muissa kaupungeissa ja kunnissa. Tavoitteena on kehittää

suunnittelu- ja dokumentointimalli, jota voidaan helposti monistaa erikokoisten projektien vaatimuksiin.

1.3 Tutkimusongelma

Kuinka voidaanrakentaa IP-pohjainen turvallinen turvajärjestelmä? Miten kehitetään maantieteellisesti hajallaan olevien järjestelmien keskitetty ja luotettava hallintajärjestelmä? Dokumentointityökalujen kehittäminen suunnittelun ja ylläpidon helpottamiseksi. Siirtomedioiden luotettavuuden tutkiminen ja vertailu.

1.4 Rajaukset

Valmistajien omat ohjelmistot ja käyttö- sekä asennusohjeet ovat järjestelmäkohtaisia. Tämän vuoksi varsinaiset turvajärjestelmien hallintaohjelmistot ja niiden käyttö rajattiin tämän opinnäytetyön ulkopuolelle.

1 TCP/IP JÄRJESTELMÄ

2.1 Protokolla

TCP/IP on reitittävä protokolla, joka koostuu useista Internet-protokollista. Protokollat määrittävät standardit tietokoneiden väliselle tiedonsiirrolle, verkkojen kytkennälle sekä reititykselle. TCP/IP:n keskeiset protokollat ovat seuraavat:

- TCP-Transmission Control Protocol: ylemmän tason yhteydellinen protokolla
- IP-Internet Protocol: Internet-osoitteen kuljettaminen reitittimelle
- UDP-User Datagram Protocol, yhteydetön protokolla
- ARP-Address Resolution Protocol, jossa kysytään MAC osoitetta tunnetulle IP-osoitteelle
- RARP-Reverse Address Resolution Protocol, jossa kysytään IP-osoitetta tunnetulle MAC-osoitteelle (Medium Access Control)
- ICMP- sanomaviestien (Internet Control Message Protocol) välitys

Internet-verkko perustuu Internet Protocol eli IP-paketteihin. Siirrettävien pakettien otsikkokentissä sijaitsevat lähettäjän ja vastaanottajan IP-osoitteet. IP-osoitteet yksilöivät lähettäjän ja vastaanottajan. Osoitetietojen perusteella reitittimet siirtävät paketteja mahdollisuuksien mukaan lähemmäs kohdeosoitetta olevalle reitittimelle. Sanoman lähettäjälle on yhdentekevää, mitä reittiä paketti kulkee, kunhan se vain saapuu vastaanottajalle. IP-protokolla ei kuitenkaan huolehdi eikä pidä kirjaa pakettien perillepääsystä. Datan eheys ja virheettömyys pitää hoitaa verkkoprotokollan ylemmillä tasoilla. (Comer 2002, 107.)

Yhteydetön protokolla IP sijoittuu OSI-mallin verkkokerrokselle. Ylemmän tason TCP-protokolla huolehtii pakettien pääsystä perille. Reaaliaikasen äänen ja liikkuvan kuvan siirtoon käytetään yleensä yhteydetöntä UDP-protokollaa, joka on nopeutensa vuoksi TCP:tä parempi. Reaaliaikaista kuvaa tai ääntä siirrettäessä kadonneiden pakettien uudelleenlähetys sotkee sanoman ymmärrettävyyttä.
IP:n kanssa samalle Internet-kerrokselle sijoittuvat myös sanomaviestit (ICMP), osoitteen selvitykset (ARP) ja käänteinen osoitteen selvitys (RARP).
(Uotila 1998, 178.)

2.2. IP-tietosähke

IP-tietosähke rakentuu seuraavista otsikkotiedoista:

1. MAC osoite
   Vastaanottajan ja lähettäjän MAC–osoitteetovat valmistajan asettamia yksilöllisiä laitetunnisteita.

2. IP otsikko
   IP kehyksen versionumero ilmaistaan 4 bitin kentällä. Tällä varmistetaan yhtenäinen tulkinta kehystä käsittelevien osapuolten kesken. Käytettävä versio on nykyisin 4.

3. Otsikon pituus
   Otsikon pituus ilmoitetaan 4 bitillä. Otsikkoon voidaan sijoittaa lisätietoja esimerkiksi reitityksen ohjauksesta. Tavallisin otsikko on 20 tavun pituinen, jolloin otsikon pituuskentän arvo on 5.

4. Palvelun tyyppi
   Pituus on 8 bittiä. Ilmoittaa verkolle, minkätyyppistä palvelua IP-paketille halutaan. Palvelua voidaan pyytää prioriteetin asettamiseksi, viivyttämiseksi, läpimenon parantamiseksi sekä luotettavuuden parantamiseksi. Verkko ei kuitenkaan pysty takaamaan kaikkien palveluiden toteutumista.

5. Tietosähkeen pituuden määrittäminen
   Tietosähkeen pituus ilmoitetaan 16 bitin kentässä 8 bitin oktetteina.

6. Tunniste
   Tunnisteena on16 bittinen pilkottujen osien tunnus.

7. Fragmentoinnin eli tiedon pilkkomisen ohjaus
   Kentän pituus on 16 bittiä, joka ilmaisee onko datan pilkkominen sallittua sekä pilkottujen osien sijainnin. Tämän tiedon avulla vastaanottaja pystyy kokoamaan datan oikeaan muotoon.

8. Paketin eliniän määrittäminen

Elinikä ilmoitetaan 8 bitin määrityksenä sallitusta solmujen tai reitittimien määrästä. Tämän tarkoituksena on estää solmulta tai reitittimeltä toiselle loputtomasti kiertävien tietosähkeiden muodostuminen.

9. Protokolla

Protokolla kentässä ilmaistaan 8-bittinen tunniste käytössä olevasta protokollasta.

10. Otsikon tarkistussumma

16-bittinen tarkistussumma määrittää otsikon oikeellisuuden. Tämä lasketaan koko otsikolle.

11. Lähteen IP-osoite

Lähteen tunniste ilmaistaan 32-bittisenä lähettäjän osoiteena.

12. Vastaanottajan IP-osoite

Vastaanottajan tunniste ilmaistaan 32-bittisenä vastaanottajan osoitteena.

13. Lisätiedot

Sisältää valinnaisia lisätietoja turvallisuudesta, käytettävästä reitistä, reitityshistoriasta sekä aikaleimasta. Lisätiedot koostuvat 32 bittisistä sanoista. (Uotila 1998, 178.)

2.3 TCP

TCP- protokolla on yhteydellinen liikennöintikäytäntö kahden solmun välillä. TCP käyttää isääntäkoneiden sovelluksien osoituksissa porttinumeroita 1-65535 (16 bittinen osoitus) Porttinumerot 1 - 255 jaotellaan staattisiksi eli kiinteiksi porteiksi sekä numerot 256 – 65535 dynaamisiksi eli vapaasti käytettäviksi porteiksi.

FTP-tiedostojen siirto suoritetaan dynaamisella portilla numero 20 ja Telnet-yhteys luodaan porttinumerolla 23. FTP-yhteyttä muodostava kone määrittää omaksi portikseen jonkin dynaamisista porteista ja ottaa yhteyden kohdekoneen porttiin numero 20. Tiedonsiirto tapahtuu näiden porttien välityksellä. (Uotila 1998, 187.)

2.3.1 Yhteyden muodostaminen

Kolmivaiheisen kättelyn avulla määritetään sekvenssinumerot, joilla seurataan pakettien lähettämistä ja vastaanottoa. Kättely tapahtuu SYN-ja ACK-bittien lähettämisellä. Yhteyttä muodostava kone lähettää SYN-bitin sisältävän paketin, jossa sekvenssinumeroksi on merkitty x kohdekoneelle, joka vastaanotettuaan sen lähettää takaisin SYN-bitin sekvenssinumerona y ja ACK-bittinä x+1. Yhteyttä muodostava kone vastaanottaa SYN-bitin ja lähettää kohdekoneelle oman ACK-bittinsä, joka on y+1.

Sekvenssinumeroiden avulla kohdekone varmistuu kaikkien pakettien perillepääsystä pyytämällä uudelleenlähetystä, mikäli jokin numeroitu paketti puuttuu. Käytännössä lähdekone lähettää saman paketin uudestaan, ellei se vastaanota kyseisen paketin ACK-bittiä. (Uotila 1998, 189.)

2.3.2 Ikkunointi ja vuonhallinta

Toisin kuin HDLC-(High-Level Data Link Control) ja X.25 protokollissa TCP-ikkunointia ja vuonhallintaa voidaan säätää vastaanottajan kapasiteetin mukaisesti.

Vuonhallinnalla sanoman vastaanottaja pystyy määrittämään lähetettävien sanomien nopeuden säätämällä lähetysjaksojen pituutta eli ikkunakokoa. Ikkunoinnilla määritetään vastaanotettujen pakettien määrä ennen kuin lähetetään kuittaus eli ACK-bitti. Ikkunakokona voi olla esimerkiksi 4 oktettia, joiden vastaanoton jälkeen ACK-bitti lähetetään lähdekoneelle. Mikäli lähdekone ei saa kuittausbittiä, se tietää, että kohdekone ei ole pystynut vastaanottamaan kaikkia paketteja onnistuneesti ja paketit pitää lähettää uudelleen sekä hidastaa lähetysnopeutta. (Uotila 1998, 195.)

2.3.3 Datan eheyden tarkistaminen

Siirtomediassa esiintyy aina sähköisiä häiriöitä, jotka vaikuttavat siirrettävän datan eheyteen. Häiriöt voivat aiheutua siirtomediassa tapahtuvasta ylikuulumisesta tai ulkopuolisesta sähkömagneettisesta säteilystä.

Siirtotiellä tapahtuvien bittivirheiden havaitsemiseksi data pitää tarkistaa. Lähettäjä laskee jokaiselle TCP paketille 16 bittisen tarkistussumman otsikkotiedoista sekä hyötykuormasta. Jokainen siirtotiellä oleva laite laskee vertailuarvon sekä vastaanottaessaan paketin että lähettäessään sen edelleen. Tarkistussummaa verrataan alkuperäiseen arvoon ja pyydetään uudelleenlähetystä, mikäli luku poikkeaa vertailuarvosta. (Granlund 2000, 162-165.)

2 TIETOLIIKENNEYHTEYDET

3.1 Modeemiyhteys

3.1.1 Yleistä

Modeemi muuntaa tietokoneella lähetettävän digitaalisen signaalin puhelinverkossa käytettäväksi analogiseksi signaaliksi. Vastaanottopäässä analoginen signaali muutetaan vastaavasti digitaaliseen muotoon.

Modeemiyhteys luodaan vastaanottajan ja lähettäjän välille istuntokohtaisesti käyttämällä puhelinverkkoon määritettyä soittosarjaa. Yhteyden muodostamiseen käytetään PPP-protokollaa (Point to Point Protocol) joka toimii OSI-mallin siirtoyhteyskerroksella. (Uotila 1998, 112.)

3.1.2 Yhteyden muodostus

Käytännössä modeemin yhteyden muodostus tapahtuu seuraavasti: Tietokoneessa oleva tietoliikenneohjelmisto ilmoittaa DTR)-signaalilla (Data Terminal Ready) modeemille valmiudesta tietojen lähettämiseen. Modeemi vastaa DSR-signaalilla (Data Set Ready) toimintavalmiudesta. Näillä kahdella signaalilla käynnistetään tietoliikenne modeemin välityksellä lankapuhelinverkossa. Tietoliikenneohjelmisto välittää komennot modeemille käyttäen AT-komentotaulukkoa (attention). Ohjelmisto ohjaa modeemia ottamaan yhteyden soittosarjassa määritettyyn puhelinnumeroon, jonka toisessa päässä on vastaanottajan modeemi tai palveluntarjoajan PPP-serveri, johon soittosarjan puhelinnumero on kytketty. Serverissä olevan puhelinnnumeron takana olevassa modeemisarjassa sijaitsee useita modeemeja ketjussa n. 10 - 30 kpl modeemeja/sarja. Mikäli sarjan ensimmäinen modeemi on varattu, niin puhelu ohjataan seuraavaan jne.

Vastaanottavan modeemin vastatessa puheluun ilmaisee lähetyspään modeemi merkkiäänellä kyseessä olevan tiedonsiirtoon tarkoitetun puhelun. Vastaanottava modeemi vastaa merkkiääneen korkeammalla äänellä. Lähettävä modeemi avaa kantoaallon tunnussignaalin CR (Configure Request) tietokoneelle. Ennen lähetyksen alkua tietoliikenneohjelmisto lähettää modeemille RTS-signaalin

(Request To Send) ja odottaa vastaukseksi CTR-signaalia (Clear To Send) modeemilta ennen kuin lähetys voidaan aloittaa. Lähettävä ja vastaanottava modeemi suorittavat nykyisin automaattisesti PPP-protokollan avulla kättelyn, käytettävän protokollan määrittelyn, asetusten tekemisen ja yhteyden päättämisen. (Uotila 1998, 113.)

3.1.3 Kehystäminen ja pakkaus

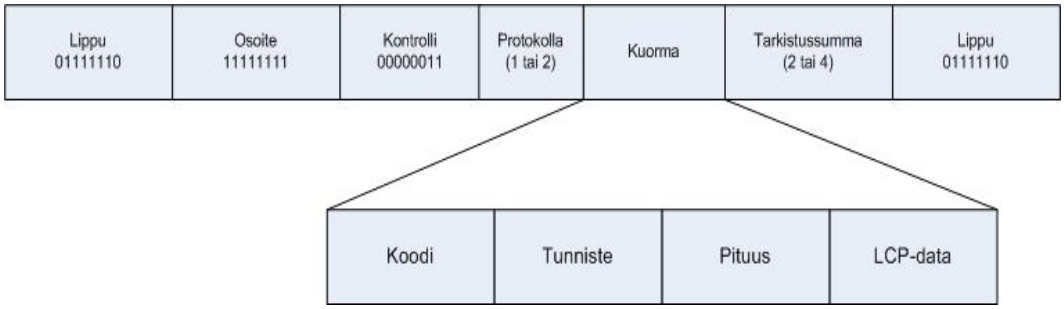
Kantoaaltosignaali modeemien välillä toimii myös yhteyden ylläpidon merkkisignaalina. Kantoaalto moduloidaan vanhempien modeemien DPSK-moduloinnilla (Differential Phase Shift Keying), uusimpien modeemien QAM-moduloinnilla (Quadrature Amplitude Modulation) tai TCM- moduloinnilla (Trellis Coded Modulation).

Virheiden korjaukseen käytetään pariteettitarkistusta (erillinen pariteettibitti even, odd) ja nykyisin uusissa modeemeissa CRC- tarkistussummaa (Cyclic Redundancy Check). CRC-tarkistussumma lisätään kehykseen, josta vastaanottaja tarkastaa onko tiedonsiirrossa tapahtunut virhe. Virheelliset kehykset tuhotaan ja pyydetään uudelleenlähetystä.

Lähetettävä data pyritään pakkaamaan mahdollisimman pieneen tilaan. Bittivirrasta leikataan tarpeettomat bitit pois ja loppu pakataan käyttämällä sopivaa pakkausalgoritmia. Tiedonpakkausstandardeja ovat esimerkiksi V42 bis sekä MNP5. Pakkaussuhteet vaihtelevat 1:2-1:4:n välillä. (Uotila 1998, 117.)

3.1.4 PPP-protokolla

Modeemien kättelyyn käytetään PPP-protokollaa, joka toimii data-link kerroksella (siirtoyhteys). PPP:n kehystyksen muoto perustuu toiminnaltaan HDLC-protokollaan. PPP on kuitenkin merkkipohjainen, eli kehyksen pituus on 8 bitin monikerta. Kehyksessä olevan protokollakentän toimintoina ovat LCP (Link Control Protocol) ja NCP (Network Control Protocol). NCP-kehysten avulla voidaan sopia käytettävän verkkoyhteyskerroksen protokolla, joka mahdollistaa useiden eri verkkoyhteysprotokollien pakettien muodostamisen (enkapsulointi) kuten IP, IPX (Internet Packet Exchange), AppleTalk, CLNP (ConnectionLess Network Protocol) ja XNS (Extensible Name Service).



KUVIO 1. LCP-kehys

Yhteyden muodostaminen ja asetukset neuvotellaan LCP - kehyksillä.

LCP-paketit voidaan jaotella kolmeen ryhmään jotka ovat konfigurointi-, lopetus- ja ylläpitopaketit.

- konfigurointipaketit (Link Configuration)
  (Konfigurointitiedot): yhteyttä luova kone lähettää Configure Request parametrilistan vastaanottavalle koneelle, joka vastaa tilanteesta riippuen seuraavilla vastauspaketeilla:
  Yhteyden luominen ja asetusten tekeminen suoritetaan konfigurointipyynnollä (Configure-Request).
  Yhteyden luominen ja asetusten tekeminen, konfiguraation hyväksyminen, jolloin parametrit ovat olemassa ja ne kelpaavat (Configure-Ack).
  Yhteyden luominen ja asetusten tekeminen, konfiguraation hylkääminen. Parametrit ovat olemassa, mutta niille ilmoitetaan vaihtoehtoiset arvot (Configure-Nak)
  Puutteellisen konfiguraation hylkääminen. Parametreja ei ole olemassa. Sisältää listan kaikista hylätyistä optioista (Configure-Reject)

- lopetuspaketit (Link Termination)
  lopetuspyyntö (Terminate-Request)
  lopetuksen vahvistaminen (Terminate-Ack)

- ylläpitopaketit (link maintenance)
  koodin hylkääminen (Code Reject)
  protokollan hylkääminen (Protocol-Reject)
  kaiutuspyyntö (Echo-Request)

7. kaiutus (Echo-Reply)
8. hylkäyspyyntö (Discard-request)

Yhteyden soveltuvuus ja laatu testataan verkkoyhteyskerroksen protokollille sopivaksi (optio). Datasiirto lopetetaan LCP-, NCP-kehyksillä tai ulkoisella keskeytyksellä. Kuviossa 1 on esitetty LCP-kehyksen rakenne. (CCNA v2.1.4 chapter 4 4 PPP-protocol.)

3.1.5 PAP ja CHAP autentikointi

PAP autentikointi (Password Authentication Protocol) tapahtuu kaksiosaisena kättelynä. Sen jälkeen kun PPP-yhteys on luotu, käyttäjätunnus ja salasana lähetetään vastapuolelle, joka joko hyväksyy tai hylkää yhteyden.

Salasanat lähetetään salaamattomina. Salasanakäytäntö ei anna suojaa toistolle tai toistuville salasanan hyväksyttämisyrityksille. Tämän vuoksi PAP ei ole vahva autentikointiprotokolla.

CHAP-autentikointi (Challenge Handshake Authentication Protocol) suoritetaan kolmivaiheisella kättelyllä käyttäen haaste-vastaus-menetelmää. Viestityyppejä on neljä kappaletta, jotka ovat haaste, vastaus, onnistuminen ja epäonnistuminen. Tunnistamista vaativa osapuoli lähettää ensin haaste-viestin, joka sisältää pyynnön käyttäjätunnuksesta ja salasanasta sekä varsinaisen haasteen. Tunnistus voidaan toistaa myös muodostetun yhteyden aikana. Yhteyden aikainen tunnistus voidaan määrittää toistuvaksi tietyn ajan välein.

Vastaanottava kone vastaa yhdensuuntaisella hash-funktiolla laskemansa arvon, esim MD5. Salausta vaativa kone laskee itse vartailuarvon, vertaa sitä lähetettyyn ja hyväksyy tai hylkää yhteyden. Funktion laskeminen perustuu salaiseen avaimeen, joka on molempien osapuolten käytössä. Autentikointi voidaan tehdä kaksisuuntaisesti siten, että kumpikin osapuoli voi toimia haasteen antajana Salaista avainta ei lähetetä verkon yli. Avaimen pituus pitää olla vähintään hash-arvon pituus MD5 = 16 oktettia. (CCNA v2.1.4 chapter 4 4 PPP-protocol.)

3.2. ISDN-yhteys

3.2.1 Yleistä

ISDN (Integrated Services Digital Network) on digitaalinen monipalveluverkko, joka hyödyntää puhelinverkon keskusten digitaalisia kytkentäominaisuuksia ja keskusten välisiä digitaalisia siirtoyhteyksiä. Puhelinkeskukset ja niiden väliset siirtoyhteydet käyttävät puheen PCM-koodaustekniikkaa (Pulse Coded Modulation) ja yhdistävät TDM-kanavointia (Time Division Multiplexing) hyväksikäyttäen 64 kbit/s piirikytkentäisiä kanavia 30 kpl saavuttaen 2.048 Mb/s nopeudella toimivan siirtotien. Näiden palvelujen hyödyntämiseen päästään korvaamalla puhelinverkon analoginen tilaajaliitäntä digitaalisella ISDN liitännällä. (Keogh 2001,160.)

ISDN:n tulee käyttää samaa 64 kb/s nopeutta, jotta se olisi yhteensopiva runkoverkon kanssa. Digitalisoitu puhe ja tietokoneen käyttämä digitaalinen tiedonsiirto voivat kumpikin hyödyntää samaa tiedonsiirtokanavaa. (Granlund 2000, 250.)

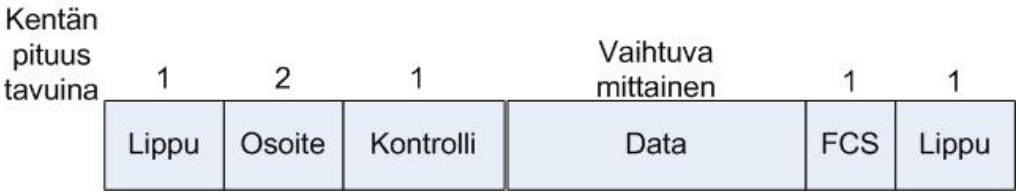
3.2.2 ISDN-liitännät

ISDN:lle on märitelty kaksi tapaa jolla voidaan liittyä digitaaliseen runkoverkkoon. Perusliittymä sisältää kaksi 64 kb/s nopeuksista B-kanavaa ja yhden 16 kb/s D-kanavan. B-kanavat siirtävät joko puhetta tai dataa. D-kanava on varattu merkinantoon. Nämä nopeudet ovat tehollisia nopeuksia, ja niiden lisäksi on varattu takaisin heijastumisen poistamiseksi 16 kb/s sekä kehysrakenteen ylläpitämiseksi 32 kb/s. Kokonaislinjanopeus on täten 192 kb/s. Perusliittymään voidaan liittää 8 kpl joko digitaalisia tai analogisia päätelaitteita. Näihin päätelaitteisiin on mahdollista saada oma erillinen puhelinnumero. Normaalisti kotikäyttöön tarjottavaan perusliittymään kuuluu 2 - 3 puhelinnumeroa.

Järjestelmäliittymä PRI (Primary Rate Interface) sisältää 30 kpl 8-bit B-kanavaa yhden 8-bit D-kanavan ja yhden 8-bit-kehystyskanavan. Kokonaisnopeudeksi saadaan 2.048 Mb/s lähetysnopeuden ollessa 8000 kehystä sekunnissa (32 x 8 x 8000). Järjestelmäliittymä on kehitetty palvelemaan suurempia yrityksiä, joiden puhelinvaiheteet tai datasoittosarjat voidaan liittää digitaaliseen puhelinverkkoon.

Ohjauksesta vastaava D-kanava, jonka kehysrakenne on esitetty kuviossa 2, toimii OSI-mallin siirtoyhteyskerroksella. D-kanavalla on 3-kerroksinen protokollarakenne. Ensimmäinen kerros kuvaa fyysistä yhteyttä TE:n ja NT:n välillä sisältäen liitännän, linjakoodauksen, kehystyksen ja sähköiset ominaisuudet. Toinen kerros kuvaa fyysisen kerroksen virheenkorjausta ja luo loogisen yhteyden päätelaitteen ja verkon välille. Kolmas kerros kuvaa merkinantoa verkon palvelujen käyttämiseksi.

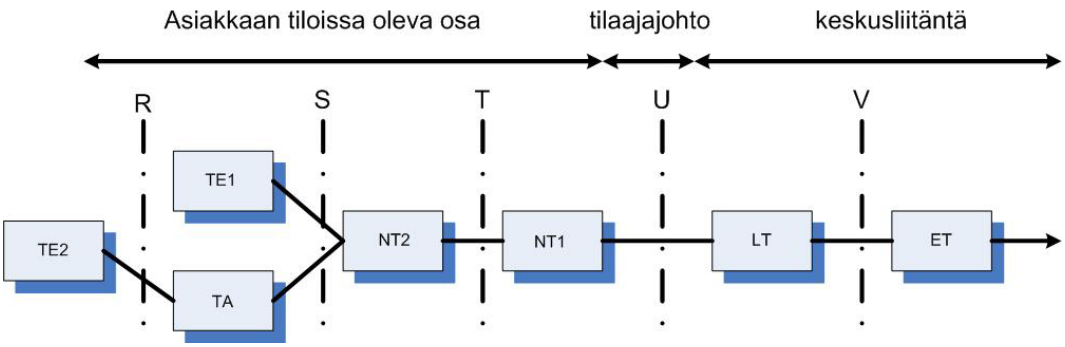
Kehyksen alku ja loppu ilmaistaan erillisillä kehysten erottimilla (lippu, flag), jotka ovat yhden tavun pituisia. Osoitekenttä on kahden tavun mittainen, ja sen tehtävä on virtuaalikanavien osoittaminen ja vuonvalvonnan signalointi. Vaihtuvanmittaisen informaatiokentän pituus voidaan neuvotella yhteydenmuodostuksessa. Tarkistussumman pituus on yksi tavu. (Granlund 2000, 252.)



KUVIO 2. D-kanavan kehystyyppi

3.2.3 ISDN- järjestelmän rajapinnat ja referenssipisteet

.

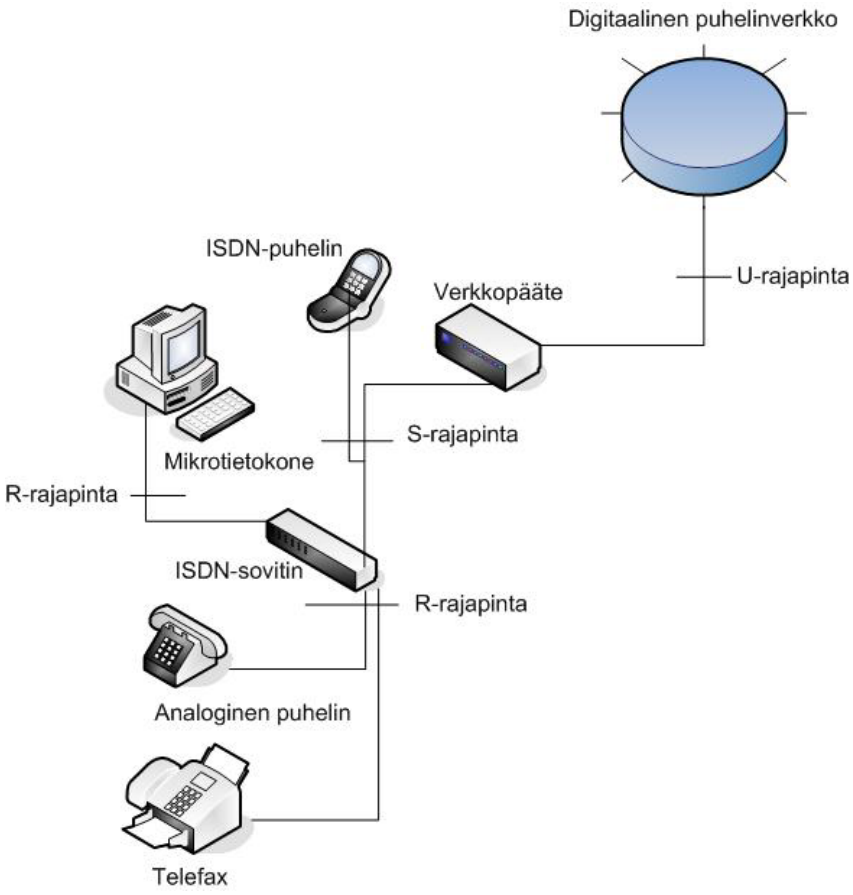


KUVIO 3. ISDN:n referenssipisteet

Kuviossa 3 on esitetty referenssipisteet ISDN liittymälle, jossa

- NT1 on verkkopääte 1
- NT2 on verkkopääte 2
- TA on ISDN-sovitin
- TE1 on aito ISDN-päätelaite
- TE2 on laite ilman ISDN-liitäntää
- LT ja LE ovat vastuussa verkko- ja kytkintoiminnoista.

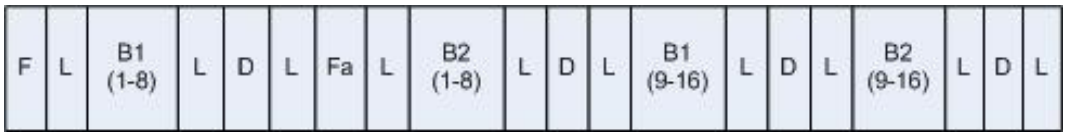
R-rajapinta on kehitetty analogisten laitteiden tai ISDN-yhteensopimattomien digitaalisten laitteiden liittämiseksi järjestelmään Terminal Adapterin (TA) välityksellä. S/T-rajapinta on päätelaitteiden puoleinen rajapinta, joten siihen voidaan liittää suoraan ISDN-yhteensopivat laitteet, kuten esimerkiksi ISDN-puhelimet tai vastaavasti ISDN-sovitin. U-rajapinta on ISDN-verkkopäätteen televerkonpuoleinen liitäntärajapinta. V-rajapinta erottaa keskuksen ja keskuspään siirtojärjestelmät toisistaan. Kuviossa 4 esitetään laitekohtaiset liitymärajapinnat. (Uotila 1998, 125.)



KUVIO 4. ISDN laitekuvaus

3.2.4 ISDN-perusliittymän kehys

Kuviossa 5 on esitetty ISDN-perusliittymän kehys. Kehyksen pituus on 48 bittiä ja siirtoaika 250 µs.
Jokaiseen kehykseen sisältyy kummankin B-kanavan 16-bittinen ja D-kanavan 4-bittinen informaatio.



KUVIO 5.ISDN-kehys

TAULUKKO 1. ISDN-kehyksen bittinumerot (Kuusi. 1999)

Bitin numero	Päätelaitteesta verkkopäätteeseen
1	F=kehyksen aloitusbitti
2	L= tasapainotusbitti
3-10	B= ensimmäisen B-kanavan 1. Oktetti
11	L= tasapainotusbitti
12	D= D-kanavan 1.bitti
13	L= tasapainotusbitti
14	Fa= apukehysbitti (käytetään monikehyksissä)
15	L= tasapainotusbitti
16-23	B= toisen B-kanavan 1. Oktetti
24	L= tasapainotusbitti
25	D= D-kanavan 2.bitti
26	L= tasapainotusbitti
27-34	B= ensimmäisen B-kanavan 2. Oktetti
35	L= tasapainotusbitti
36	D= D-kanavan 3. bitti
37	L= tasapainotusbitti
38-45	B= toisen B-kanavan 2. Oktetti
46	L= tasapainotusbitti
47	D= D-kanavan 4. Bitti
48	L= tasapainotusbitti

Taulukossa 1 on esitetty ISDN-kehyksen bittijaottelu eri kanavien kesken (CCNA v2.1.4 chapter 4, 5 ISDN).

3.3 ADSL-yhteys

ADSL- teknologia (Asymmetric Digital Subscriber line) kuuluu XDSL-teknologioihin (X-type Digital Subscriber line) yhdessä HDSL:n (High bitrate DSL), SDSL:n (Symmetric Digital Subscriber Line) ja VDSL:n (Very high rate Digital Subscriber Line) kanssa. Asymmetrisenä tiedonsiirtona sen

tiedonsiirtonopeus on suurempi verkosta päätelaitteelle kuin päätelaitteelta verkkoon. Normaalissa selainkäytössähän verkosta tulevan tiedon määrä on huomattavasti suurempi kuin sinne lähetetään.

Liikennöintiin käytetään ISDN:n tavoin puhelinverkon kierrettyä parikaapelointia. ADSL-järjestelmän käyttämä taajuuskaista sijoittuu normaalin puhelinliikenteen käyttämää 0 - 4 kHz:n taajuuskaistaa ylemmäksi, joten nämä eivät häiritse toistensa liikennöintiä. Sekä palvelun tarjoaja että käyttäjä liittyvät järjestelmään erillisillä liitäntäyksiköillä. Liitäntäyksiköihin voidaan liittää useita eri laitteita palvelun tarjoajan tai käyttäjän vaatimusten mukaisesti. Puheen ja ADSL-signaalin samanaikainen käyttö parikaapelissa järjestetään käyttämällä erotinta (Splitter) parikaapelin molemmissa päissä. Erotin kykenee sekä yhdistämään signaalit siirtotielle että erottamaan ne toisistaan.

DSL-tekniikoissa käytetään modulointimenetelminä joko CAP-(Carrierless Amplitude Phase) tai DMT- menetelmiä (Discrete Multi-Tone Modulation), jotka molemmat perustuvat QAM linjakoodaukseen, jossa moduloidaan sekä signaalin amplitudi että vaihekulma. CAP-menetelmässä kantoaalto tukahdutetaan ennen siirtoa. Viestisignaalin moduloinnin jälkeen se tallennetaan muistiin ja lopuksi palaset kootaan moduloituun aaltoon. CAP testaa aluksi siirtomedian laadun ja etsii parhaan siirtokyvyn käytettävässä johtimessa. CAP-menetelmässä signaalin huipun suhde keskiarvoon on pienempi kuin DMT:ssä, jolloin sen vaatima teho on pienempi. CAP käyttää puheelle ja datalle erillisiä taajuuskaistoja, jolloin molempien samanaikainen siirto on mahdolista.

DMT-modulaatio jakaa käytettävissä olevan taajuuskaistan 256 erilliseen alikanavaan, joiden kaistanleveys on 4 kHz. Jokaisella kaistalla voidaan siirtää 0-15 bittiä sekunnissa. Liikennöinti taajuuskaistoilla jaetaan siten, että verkosta päätelaitteelle päin käytetään kaikkia 256 kaistaa, joista 32 kpl ovat kaksisuuntaisia mahdollistaen päätelaitteen liikennöinnin verkkoon. Jokaisen kanavan siirtokyky tarkastetaan ennen lähetystä, jonka jälkeen valitaan siirtotielle sopiva QAM-kuvio. DMT on standardoitu merkittävimpien instituutioiden toimesta joten sille voidaan ennustaa laajempaa käyttöä kuin CAP-moduloinnille (Granlund 2000, 102.)

3.4 WLAN-yhteys

WLAN (Wireless Local Area Network) käyttää fyysisen siirtotien asemasta sähkömagneettisia aaltoja tiedon välittämiseen. Siirrettävä data liitetään radioaalloille moduloinnin avulla. Tyypillisesti WLAN korvaa lähiverkkokaapeloinnin, jolloin tukiasema on liitetty perinteiseen verkkoon. IEEE-standardi 802.11 määrittelee OSI:n fyysisen- ja siirtoyhteyskerroksen sovittamisen langattomiin lähiverkkoihin. Tällä hetkellä käytössä on yleisesti 802.11b (max 11 mb/s) ja 802.11g standardit (max 54 Mb/s). IEEE 802.11 määrittelee radiotaajuudelle kaksi hajaspektritekniikkaan perustuvaa DSSS (Direct Sequence Spread Spectrum) ja FHSS- tekniikkaa (Frequency Hopping Spread Spectrum). Siirtotekniikat vaativat vastaanottajan ja lähettäjän synkronointia sekä sovittua menettelyä signaalin käsittelemiseksi. Hajaspektritekniikkaa käytettäessä taajuusalue jaetaan alitaajuuksiin, joilla tietoa lähetetään samanaikaisesti Signaalin taajuutena on 2.4–2.4835 GHz:n ISM-kaista (Industrial, Sientific and Medical) joka on jaettu 14 kanavaan 5 MHz:n porrastuksella. Käytettävä lähetysteho Euroopassa on 100 mW ja Yhdysvalloissa 1 W.

Perusarkkitetehtuureina ovat infrastruktuuripohjainen- ja ad hoc-arkkitehtuuri. Ad hoc-verkot ovat pieniä päätelaitteiden muodostamia tukiasemattomia verkkoja, jossa laitteet kommunikoivat suoraan keskenään. Infrastruktuuriverkoissa on tukiasemia (access point), jotka ovat yhteydessä laajempaan verkkojärjestelmään. Tietoliikenne kulkee tukiasemien kautta langattomasta langalliseen verkkoon ja päinvastoin. Tukiasemat voidaan järjestää siten, että käyttäjät voivat liikkua toisen tukiaseman alueelle yhteyden katkeamatta (roaming).

Siirtoyhteyskerroksella käytetään tietoliikenteen törmäyksien ehkäisyssä CSMA/CA-tekniikka (Carrier Sense Multiple Access with Collision Avoidance), joka tarkastaa ennen lähetystä, onko siirtotie muiden lähettävien laitteiden käytössä. Siirtotien ollessa varattuna lähetyksen aloitusta siirretään, jolloin vältytään törmäyksiltä.

Tietoturva on tähän asti ollut WLAN-verkon heikko lenkki. Käytössä olevan WEP-salauksen (Wired Equivalent Prvacy) purku on helppoa internetistä ladattavilla ohjelmistoilla. 802.11i:n myötä käyttöön tulee WPA- suojaus (Wi-Fi

Protected Access), joka parantaa tietoturvaa huomattavasti. Turvajärjestelmien etähallinnassa on kuitenkin aina käytettävä VPN- yhteyttä (Virtual Private Network)- joka mahdollistaa riittävän tietoturvan. (Granlund 2001, 230.)

3.5 VPN-yhteys

3.5.1 Yleistä

VPN on käsitteenä vanha ja juontuu jo ajalta ennen julkista TCP/IP-verkkoa. Termi on syntynyt puhelinliikenteen piiristä ja kuvannut aikoinaan yksityisissä puhelinverkoissa olevien yksityisten puhelinvaihteiden välisiä yhteyksiä. Datasiirtoon nimitys siirtyi, kun yritykset vuokrasivat teleoperaattoreilta omia yksityisiä linjoja yhdistääkseen maantieteellisesti erillään olevien konttoreiden sisäisiä verkkoja.

Ympyrä on sulkeutumassa, sillä VPN-yhteyksiä käytetään nopeasti yleistymässä olevan IP-puheen siirrossa. Aluksi vuokrattuja linjoja käytettiin X-25, Frame Relay ja ATM)-yhteyksiin (Asynchronous Transfer Mode). Nykyisin VPN-yhteys tunneloidaan julkiseen TCP/IP-verkkoon toimintamallista riippuen joko PPP, L2TP (Layer 2 Tunneling Protocol), L2F (Layer 2 Forwarding), IPsec (IP Security Architecture), PPTP- tekniikoilla (Point-to-Point Tunneling Protocol). (Perlmutter&Zarkower 2001, 86.)

3.5.2 VPN-yhteyden muodostaminen

VPN-yhteys voidaan luoda joko VPN-etäyhteytenä tai reitittimien välisenä VPN-yhteytenä. VPN-etäyhteys voidaan luoda yksittäisen työaseman ja esimerkiksi yrityksen VPN-palvelimen välille, jolloin etätyöasema voi käyttää joko palvelimen tai sen takana olevan sisäisen LAN-verkon (Local Area Network) tiedostoja ja ohjelmia samalla tavalla kuin kone olisi fyysisesti sisäverkossa. VPN-yhteydet reitittimien välillä mahdollistavat yrityksen maantieteellisesti erillään olevien LAN-verkkojen yhdistymisen siten, että LAN-verkossa oleva reititin havaitsee toiseen konttoriin osoitetun datagrammin ja luo tällöin VPN-yhteyden kohdekonttorin reitittimeen, jonka kautta kehykset reititetään. Yhteyksissä käytetään sekä 2 ja 3 kerroksen VPN-protokollia.

Tunnelointi on siirrettävän kehyksen sijoittamista salattuna hyötykuormaksi toisen kehyksen sisään, jolloin kaapatusta datasta ei suoraan voida selvittää alkuperäisiä lähde- ja kohdeosoitteita. Jotta yhteyttä voidaan kutsua VPN-yhteydeksi, ei riitä ainoastaan kehysten tunnelointi, vaan yhteyden tulisi täyttää seuraavat vaatimukset:

1. lähettäjän ja vastaanottajan autentikointi

VPN-palvelimen tai -reitittimen tulee tunnistaa asiakas ja asiakkaan oikeudet. Lisäksi asiakkaan on tunnistettava VPN-palvelin tai-reititin. Menetelmällä varmistetaan molempien osapuolten oikeellisuus.

2. datan eheyden varmistus

Lähettäjän on salattava data käyttäen symmetristä salausalgoritmia. Vastaanottaja purkaa sanoman samalla salausalgoritmilla ja laskee tiivistefunktiosta tarkistussumman, jolla todetaan datan eheys.

3. datan salaus

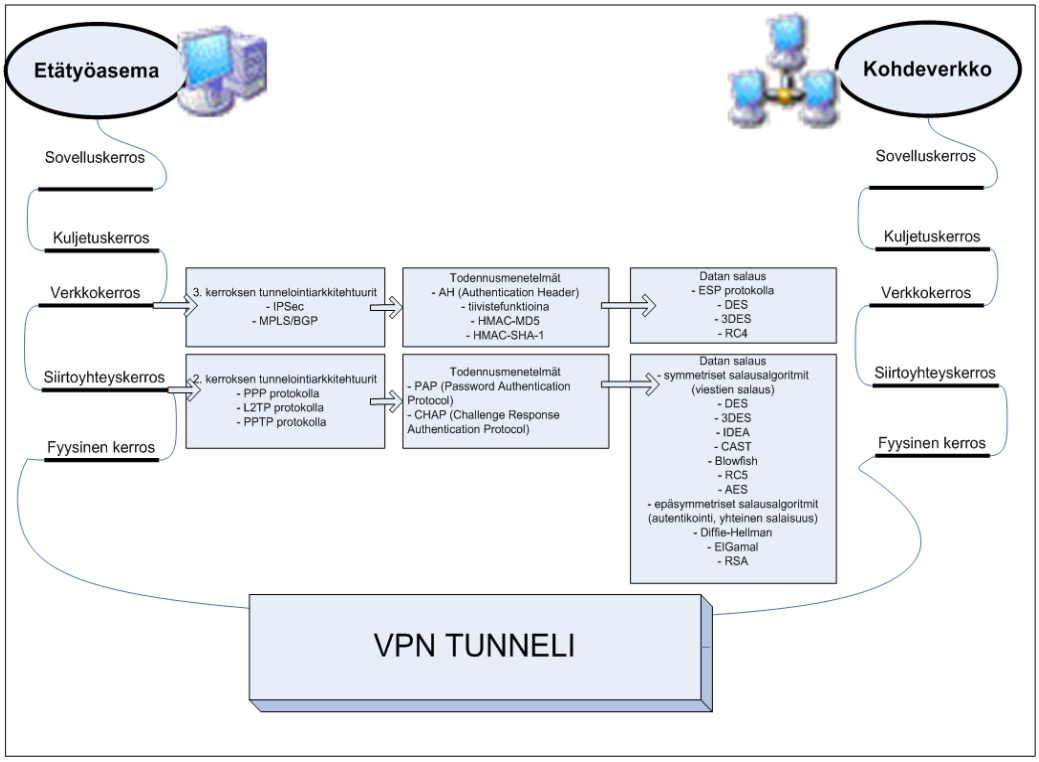
Datagrammi salataan tunneloinnin sisällä käyttäen salausalgoritmeja, esimerkiksi IPSec käyttää salauksessa ESP-salausta (Encapsulating Security Payload). ESP ei määrää käytettävää salausalgoritmia. Usein käytettyjä ovat esimerkiksi DES-(Data Encryption Standard), 3DES-tai RC4-salausalgoritmit.

4. datan uudelleenkäytön suojaus

Mahdollisesti kaapattua ja purettua dataa ei voida käyttää hyödyksi murtautumiseen.
- MDH eli Manipulation Detection Code
- tiivisteen salaus käyttäen esimerkiksi MD5-(Message
Digest 5), SHA-1-(Secure Hash Algorithm) tai RIPE-MD-tiivistefunktioita

5. salausavainten hallinta

Salausavaimina käytetään yleisesti sekoitefunktioita, esimerkiksi MD5 tai SHA-1.



KUVIO 6. VPN-ja OSI-kerrokset

Kuviossa 6 on esitetty eri salausprotokollien sijainti OSI-kerroksilla. Protokollat sijoittuvat verkko- ja siirtoyhteyskerroksille. (Perlmutter 2001, 86.)

3 TURVAJÄRJESELMÄT

4.1. Yleistä

Laajakaistaliittymien sekä kiinteistöjen tietoliikenneverkkojen lisääntymisen myötä tulevat lähivuosina lisääntymään myös kiinteistöjen turva-, valvonta-, seuranta- ja automaatiojärjestelmät sekä niiden etähallintajärjestelmät.

Lisääntyneet valvontasegmentit vaativat kehittyneitä hallintajärjestelmiä. Hallinnan keskittämisellä voidaan lisätä kustannustehokkuutta purkamalla päällekkäisiä ohjausjärjestelmiä.

4.2. Turvajärjestelmät

Turvajärjestelmät voidaan jaotella käyttötarkoituksen mukaisesti henkilöturva-, paloilmoitin-, kulunvalvonta-, työajanseuranta-, rikosilmoitus- sekä videovalvontajärjestelmiin.

Henkilöturvajärjestelmiin kuuluvat eri hoito- ja huoltolaitosten potilasturvallisuuten liittyvät hoitajakutsujärjestelmät sekä henkilöstön turvallisuuden lisäämiseksi suunnatut päällekarkaus-hälytysjärjestelmät. Hoitajien ja vartijoiden mukana kulkevat langattomat hälytin- ja vastaanotinlaitteet toimivat EU-alueella 868 MHz:n radiotaajuudella.

Paloilmoitinjärjestelmien tulee olla viranomaisten hyväksymiä laitteistoja, jotka sisältävät paloilmoitinkeskuksen varavirtalähteineen, hälytinjärjestelmän, jonka kuuluvuus on koko kiinteistön alueelle, hälytyksen siirron paloviranomaisille sekä tarvittava määrä paloilmaisimia ja paloilmoituspainikkeita. Palohälytykset annetaan kohteessa paikallishälytyksinä ja osoitteellisten paloilmoitinkeskusten kautta ne ohjataan hälytyskeskukseen, valtakunnalliseen turvaverkkoon tai PC:n (Personal computer) hälytysgrafiikkaan. paloilmoitinkeskusten ohjelmointi suoritetaan tietokoneella joko paikallisesti tai etäohjelmointina.

Kulunvalvontajärjestelmien avulla kiinteistöjen avainhallinta voidaan järjestää eri käyttäjäryhmien vaatimusten mukaisesti. Kulkuoikeuksiin voidaan tehdä rajoituksia sekä aika- että tilaperusteisesti. Lokitiedostosta voidaan seurata

käyttäjän liikkumista kiinteistön tiloissa. Kulunvalvontajärjestelmää käytetään usein rikosilmoitinten, hissien ilmastoinnin sekä valaistuksen ohjaukseen. Teknisesti järjestelmään kuuluvat sähköiset lukitukset, tunnistinlaitteet sekä kulunvalvontaohjelmisto, joka voi sijaita erillisellä palvelinkoneella tai yrityksen sisäverkon työasemassa. Käyttäjällä on hallussaan joko magneettijuovakortti tai yleisimmin käytössä oleva etätunnistinkortti.

Eri työvaiheiden suorittamiseen kulunut aika on perinteisesti kirjattu tuntilapuille. Työajanseuranta mahdollistaa tuotannon ja kokoonpanon eri työvaiheiden aikamenekkien automatisoinnin. Seurannan raporttien avulla voidaan selvittää työajan jakautuminen kustannuspaikoittain. Näitä tietoja on mahdollista hyödyntää sekä tuotteiden että projektien hinnoittelussa. Esimerkkinä voidaan mainita tasolasiteollisuus, joka pystyy hinnoittelemaan projektikohtaiset tuotehinnat asiakkaan lähettämän yksityiskohtaisen lasiluettelon mukaisesti. Linjaston läpimenoaika ja täyttöaste voidaan ennakoida hyödyntämällä tarkkoja lasimenekkejä sekä toteutuneita työaikaraportteja. Teknisesti työajanseuranta hyödyntää samaa teknologiaa kulunvalvonnan kanssa, mutta työpisteisiin voidaan lisäksi liittää etälukijoita, joihin työvaiheet voidaan yksilöidä. Työajan seurantaohjelmisto voi olla osana kulunvalvontajärjestelmää.

Työajan liukuma on perinteisillä tuntilapuilla lähes mahdotonta toteuttaa virheettömästi. Työajan seurantajärjestelmällä voidaan tuntukirjaukset suorittaa reaaliajassa, jolloin järjestelmän luotettavuus on erittäin hyvä. Yleisimmin työajan liukuma liitetään teknisesti kulunvalvontaan ja työajanseurantaan.
Eri ruokailuvaihtoehdot voidaan hinnoitella sekä liittää laskutustietoihin käyttäjien henkilökohtaisten ostojen erittelyt.

Rikosilmoitinjärjestelmien päätelaitteina käytetään infrapunailmaisimia liikkeen havaitsemiseen, lasirikkoilmaisimia tunnistamaan äänen perusteella lasi rikkoutumisen sekä oviin ja ikkunoihin asennettavia magneettikoskettimia, jotka antavat hälytystiedon kosketintiedon muuttumisen perusteella. Kiinteistöissä työskentelevien henkilöiden turvallisuutta voidaan lisätä langattomilla ryöstöpainikkeilla.

Videovalvontajärjestelmiin kuuluvat perinteiset langalliset kamerat sekä langattomat kamerat. Kuvatallenteet taltioidaan joko video kuvanauhoille tai erillisille kovalevytallentimille. Kuvatallenteet voidaan purkaa tarvittaessa TCP/IP verkon kautta.

4.3 Pääteilmaisimet ja hälytinkeskukset

4.3.1 Yleistä

Hälytinjärjestelmät ovat yleistyneet viime vuosina liike- ja teollisuuskiinteistöistä kerros-, rivi- ja pientalorakentamiseen. Järjestelmien vaatimat johdotukset huomioidaan jollakin tasolla usein jo sähkösuunnitelmissa.

Koska kiinteistön kaikkien huonetilojen lopullista käyttötarkoitusta ei rakentamisvaiheessa vielä voida tietää, jää lopullinen turvajärjestelmien suunnittelu ja toteutus erikoisliikkeen tehtäväksi. Turvallisuussyistä rikosilmoitinjärjestelmiä ei ilmoiteta sähkösuunnitelmissa. Suunnitelmat pidetään salaisina ja luovutetaan ainoastaan valtuutetulle rikosilmoitinliikkeelle.

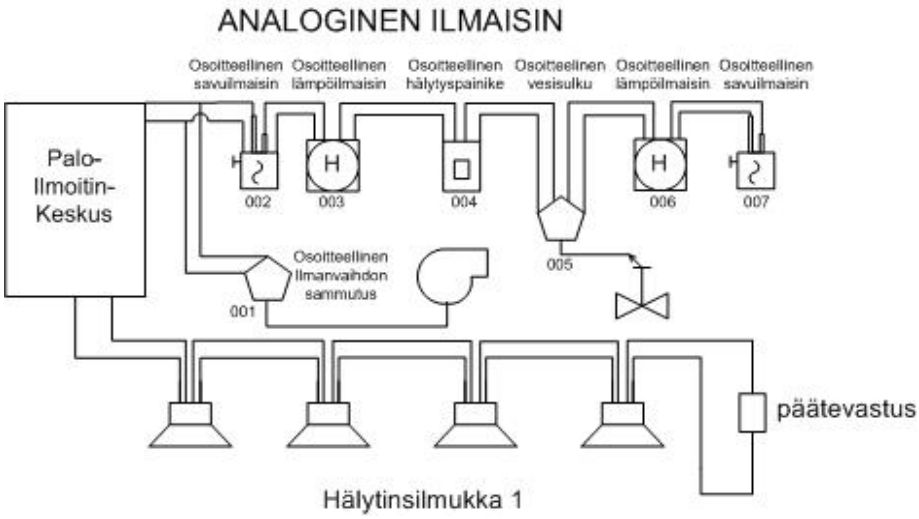
4.3.2 Rikosilmoitinlaitteistojen tiedonsiirto

Rikosilmoitinjärjestelmät toimivat pääteilmaisimen välittämän kärkitiedon avulla. Tällaisia pääteilmaisimia ovat esimerkiksi magneettikoskettimet, lasirikkoilmaisimet, liiketunnistimet, infrapunakennot ja yksinkertaiset kytkimet. Kärkitieto ilmaistaan jännitteen katkeamisena tai kytkeytymisenä.

Usein ilmoitinväylä on varmistettu jännitetunnistimella, joka antaa hälytyksen, mikäli johdin katkeaa. Tällä pystytään havaitsemaan johtimien mahdolliset rikkoutumiset tai tahallinen katkaisu.

4.3.3 Paloilmoitinlaitteistojen tiedonsiirto

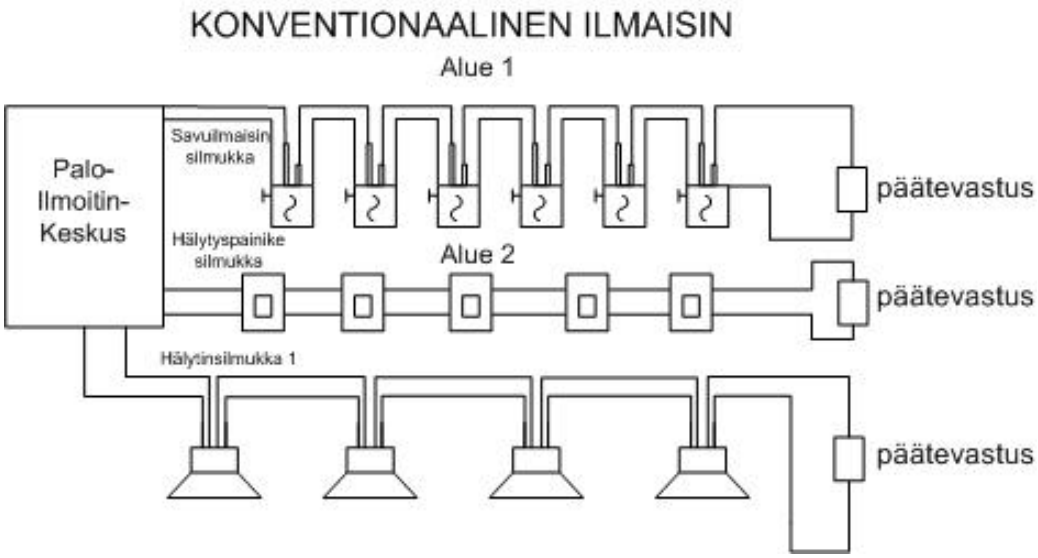
Paloilmoittimet jaetaan analogisiin ja konventionaalisiin ilmaisimiin.



KUVIO 7. Analoginen hälytinjärjestelmä

Osoitteellinen analoginen ilmaisin mahdollistaa useiden toiminnallisesti erilaisten ilmaisimien käytön samassa silmukassa (kuvio 7). Osoitteen avulla tiedonsiirto voi olla kaksisuuntaista, jolloin ilmaisinta voidan tarvittaessa säätää eri olosuhteisiin suoraan keskukselta. Keskus tunnistaa jokaisen ilmaisimen sen yksilöllisen osoitteen perusteella. Varsinainen päätös hälytyksestä tai vikailmoituksesta suoritetaan paloilmoitinkeskuksessa.

Osoitteellinen analoginen ilmaisin toimii sensorina, joka lähettää tietoja hälytinkeskukselle esimerkiksi lämpötilasta ja savun määrästä. Ilmaisimien herkkyyttä voidaan säätää esimerkiksi päivä- ja yökäytölle, jolloin esimerkiksi tehdastiloissa päivällä suoritettavat normaalit vähän savua tuottavat työvaiheet eivät laukaise hälytystä. Paloilmoitinkeskukseen liitetyn sarjaliikenneulostulon kautta hälytystietoja voidaan jakaa sammutus- ja pelastustöiden suorittamiselle tärkeisiin strategisiin paikkoihin rinnakkaisnäyttötaulujen avulla.



KUVIO 8. Konventionaalinen hälytinsilmukka

Konventionaalinen ilmaisin on yksinkertainen osoitteeton ilmaisin, joka yleensä liitetään omaan konventionaaliseen (kuvio 8) silmukkaan tai analogisen silmukan alasilmukkayksikköön. Ilmaisimella ei tällöin ole osoitetietoa, joten valvottavien alueiden silmukat on johdotettava erikseen paloilmoitinkeskukselle. Osoitetieto voidaan kuitenkin saada lisäämällä ilmaisimeen erillinen osoitepääte.

Konventionaalinen ilmaisin ei ole säädettävissä, eikä se voi mitata lisäinformaatiota keskukselle.

4.3.4 Valvontajärjestelmien dataliikenne

Kulunvalvonta käyttää datasiirrossa lukijan ja keskuksen välillä rinnakkaissiirtoa jossa ykkösellä ja nollalla on molemmilla omat johtimet. Lukijalaitteen ohjausjännitteelle asennetaan myös erilliset johtimet.

Videovalvonta voidaan jakaa analogisiin ja digitaalisiin valvontajärjestelmiin. Analoginen videonauhalle tallentava järjestelmä on väistynyt digitaalisten kovalevytallentimien yleistymisen myötä. Digitaalisen järjestelmän etuna on kuvamateriaalin hakutoimintojen monipuolisuus sekä kuvan laatu. Videokamerat voivat lähettää kuvasignaalia langallisesti koaksikaapelin, kierretyn parikaapelin, valokuidun tai langattomasti esimerkiksi Bluetooth-/ WLAN-yhteyden kautta. Ohjaussignaali ja virransyöttö kuvauksen aloittamiseen saadaan tunnistinlaitteelta tai keskukselta kierretyn parikaapelin (MHS 1x4x0.5) välityksellä

pulssikoodattuna sarjasiirtona. Kuvasignaali taltioidaan kovalevytallentimille. joista materiaalia voidaan tarkastella paikallisesti suoraan tallentimelta tai verkkoyhtyden välityksellä. Kuvamateriaalin autenttisuus varmistetaan aikaleimalla, joka on yksisuuntainen matemaattisen funktion avulla laskettu tarkiste.

4.3.5 Hallintajärjestelmien dataliikenne

Ilmoitinkeskukset keräävät ilmoitinelimistä tulevan hälytintiedon sekä tallentavat datan tai edelleenlähettävät tiedon ennalta määrättyihin valvontapisteisiin. Ilmoitinkeskusten toiminta perustuu osoitteelliseen silmukkatekniikkaan. Silmukoiden määrä on keskuksesta riippuen 16-512 silmukkaa. Jokaiseen silmukkaan voidaan liittää tietty määrä osoitepäätteitä, joilla jokaisella on yksilöllinen osoite. Osoitepäätteen jatkoksi liitetään esimerkiksi magneettikosketin. Koskettimen antama kärkitieto välittyy osoitepäätteen kautta keskukseen.

Rikosilmoitinkeskuksiin voidaan kytkeä lisäsarjaliikennekortteja, joihin voidaan liittää esimerkiksi kulunvalvontaa ja videovaihteita. Kulunvalvontaominaisuudet saadaan yhdistämällä sarjaliikennekorttiin Intre-keskusyksikkö, joka pitää muistissaan käyttäjien kulkuoikeuksien lisäksi 5200 viimeistä kulkutapahtumaa. Keskusyksikköön yhdistetään koko oviympäristön kaikki laitteet: lukijat, avauspainikkeet, magneettikoskettimet sekä moottorilukon ja varmuuslukon ohjaukset. Laajemmissa kokonaisuuksissa vaidaan keskusyksikköön liittää ovielektronikkayksiköitä max 16 kappaletta, joilla voidaan laajentaa ovihallintaa suurempiin kiinteistöihin. Ovielektronikkayksiköiden välisenä liikennöintinä käytetään RS-485 (Recommended Standard) sarjaliikennettä.

4.3.6 RS-485-tekniikka

RS 485 on EIA (Electrinics Industries Association) laatima sarjaliikkennestandardi. Topologialtaan RS-485 on ketju jonka yhteen väyläsegmenttiin voidaan liittää jopa 32 laitetta (taulukko 2).

TAULUKKO 2. RS-485:n lähetin- ja vastaanotinpiiri (Laamanen 2000)

Lähetinpiiri	
Määrä:	maks. 32 lähetintä
Lähtöimpedanssi:	120 ohmia
Vuotovirta:	-100 µA
Diff. lähtöjännite:	1,5-5 V
Lähtövirta:	150 mA nollajännitteeseen, 250 mA -7:stä +12 V:iin
Vastaanotinpiiri	
Tuloimpedanssi:	12 kilo-ohmia
Suurin yhteismuotoinen jännite:	-7:stä +12 V:iin
Herkkyys diff. tulojännitteelle:	±200 mV
Nopeus: maks.	32 Mbps
ESD-suojaus:	2,5 kV

Kaapelina käytetään kierrettyä parikaapelia siten, että jokainen signaali käyttää yhtä paria. Ketjun molempiin päihin asennetaan 100-120 ohmin päätevastus heijastumien eliminoimiseksi. Paras tulos saavutetaan suojatulla parikaapelilla lisättynä Fail safe-vastuksilla, jolloin väylä voidaan pitää halutussa tilassa, mikäli sillä ei ole liikennettä. RS-485:n tiedonsiirtonopeus on 10 Mb/s.

Maksimietäisyydellä 1200 m taataan 100 kb/s. Liikennöinti tapahtuu isäntä-orja-periaatteella, jossa jokaisella orjayksiköllä on oma osoittensa. Vain yksi laite voi lähettää dataa vuorollaan ja isäntäkone huolehtii vuorojen jakamisesta. Varsinaista protokollaa törmäysten käsittelystä ei ole, vaan se suunnitellaan tapaus- ja laitekohtaisesti. Elektroniikkayksiköihin liitetyt päätteet liikennöivät siten, että ykköselle ja nollalle kytketään johtimet. (Laamanen, 2000.)

4.3.7 RS-232-tekniikka

RS-232 on sarjaväylä kahden tietokonelaitteen väliseen liikennöintiin. Data siirretään peräkkäin bitti kerrallaan. Datapaketin mitta on yksi tavu, ja liikenteenä käytetään NRZ-koodausta (No Return to Zero), jolloin kahden bitin välillä jännitetila ei palaa perustilaan. Esimerkiksi bittijonon 0000 aikana jännitetaso on koko ajan samalla tasolla. Looginen 0-taso lähetyksessä on +5 V..+15 V ja vastaanotossa +3 V..+25 V sekä looginen 1-taso lähetyksessä on -5 V..-15 V ja vastaanotossa -3V..-25V. Standardi sisältää ainoastaan pariteettibitin, jolla tunnistetaan tavun virheellisten bittien parittomuus. Virheenkorjausta ei

kuitenkaan pystytä suorittamaan, joten se on tarvittaessa toteutettava ylemmän tason protokollalla. (Laamanen, 2000.)

4 ETÄYHTEYS ILMOITINKESKUKSEEN

5.1 Yleistä

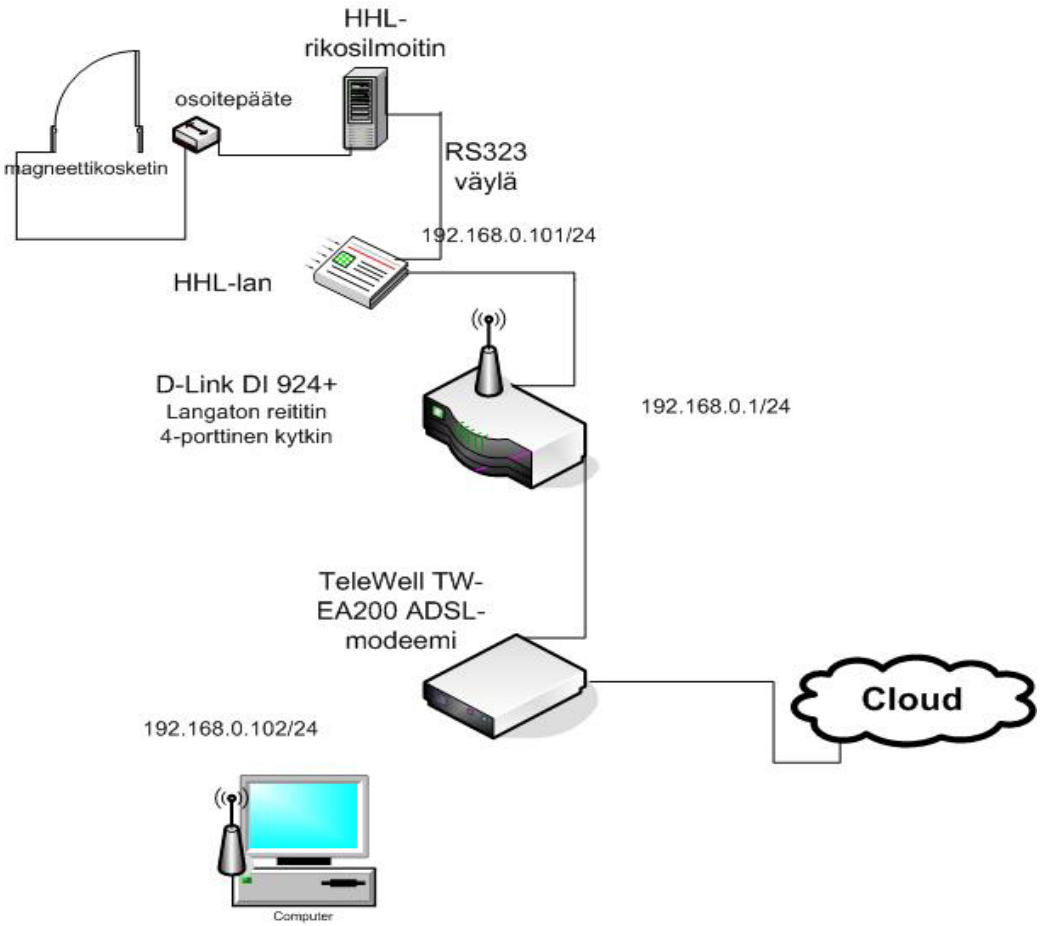
Turvajärjestelmä koostuu tunnistimien ja ilmaisimien muodostamasta verkosta, joka on yhteydessä hälytinkeskukseen. Hälytinkeskuksia voidaan liittää keskuskoneeseen, johon on asennettu järjestelmän mukainen hallintaohjelmisto.

Testikäyttöön rakennetulla laitteistolla pyrittiin selvittämään hallintaan käytettävien ohjelmistojen tietoturvallisuuden tasoa. Suojaamaton yhteys julkisen TCP/IP-verkon kautta on aina riskitekijä, joka pitää huomioida yhteystyyppien valinnassa. Dataliikenteen määrää ja suojauksen tasoa arvioimalla voidaan löytää mahdolliset tietoturvariskit sekä keinot tietoturvan parantamiselle.

5.2 Testilaitteisto

Kuviossa 9 on testikäyttöön rakennettu laitteisto, jonka hallinta suoritetaan pc:llä langattomasti WLAN-yhteydellä. Langattomaan reitittimeen on kytketty HHL-lan kortti. Korttiin on liitetty HHL-keskus RS-232-väylän avulla. Keskuksen hälytinsilmukkaan on kytketty osoitepääte ja magneettikosketin. Osoitepäätteet ovat osoitteellisen silmukkatekniikan peruste. Jokaisella osoitepäätteellä on yksilöllinen kiinteä osoite, jonka avulla järjestelmään kytketty hälytin, magneettikosketin tai ohjattava lukitus voidaan yksilöidä.

Mikäli etäyhteys rikosilmoittimeen otetaan sisäverkon ulkopuolelta, on hallintaa varten muodostettava ensin yhteys esimerkiksi NAT)-muunnoksen (Network Address Translation suorittavaan palomuuriin tai palvelimeen.

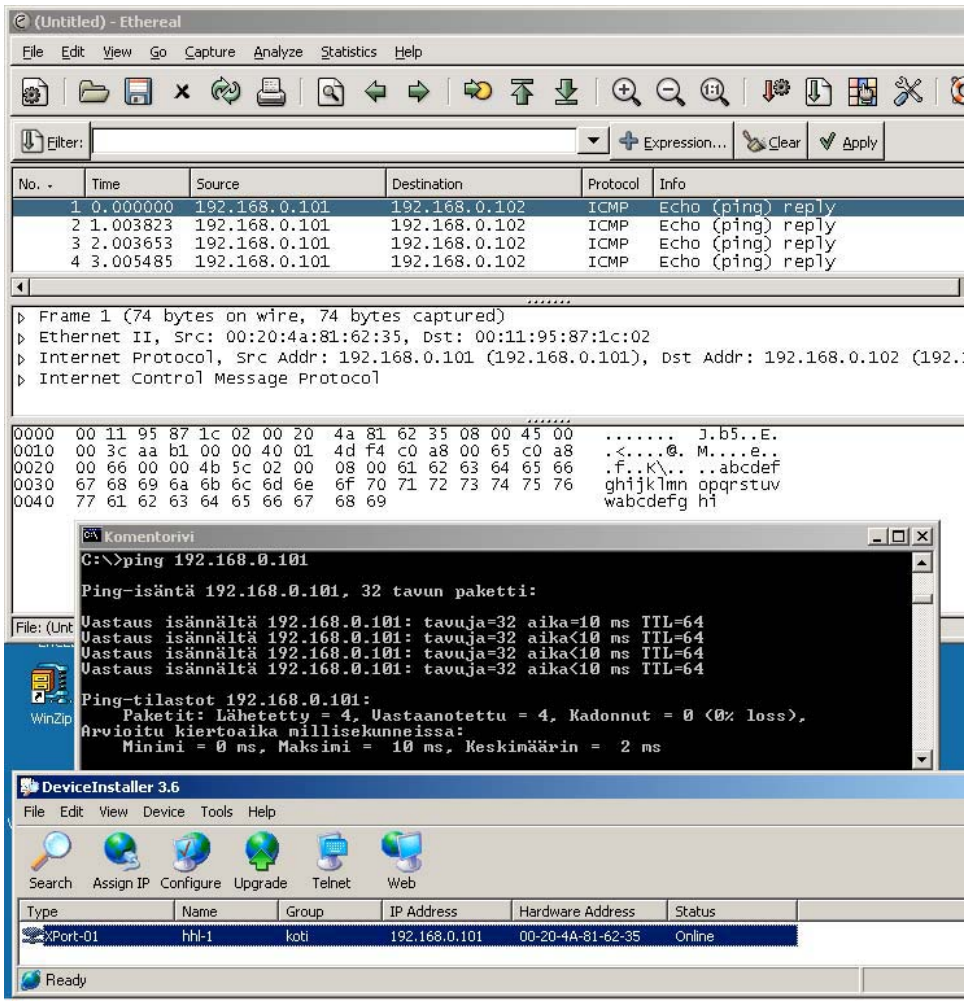


KUVIO 9. Testilaitteisto

5.3 Testiyhteys HHL-laniin

Yhteyden muodostamisen eri vaiheista pyrittiin selvittämään tietoturvallisuuden taso käyttämällä muutamien verkkoanalysaattorien ilmaisversioita. Näin pystyttiin selvittämään sekä yhteyden muodostamisen että varsinaisen ohjausliikenteen tietoturvan taso.

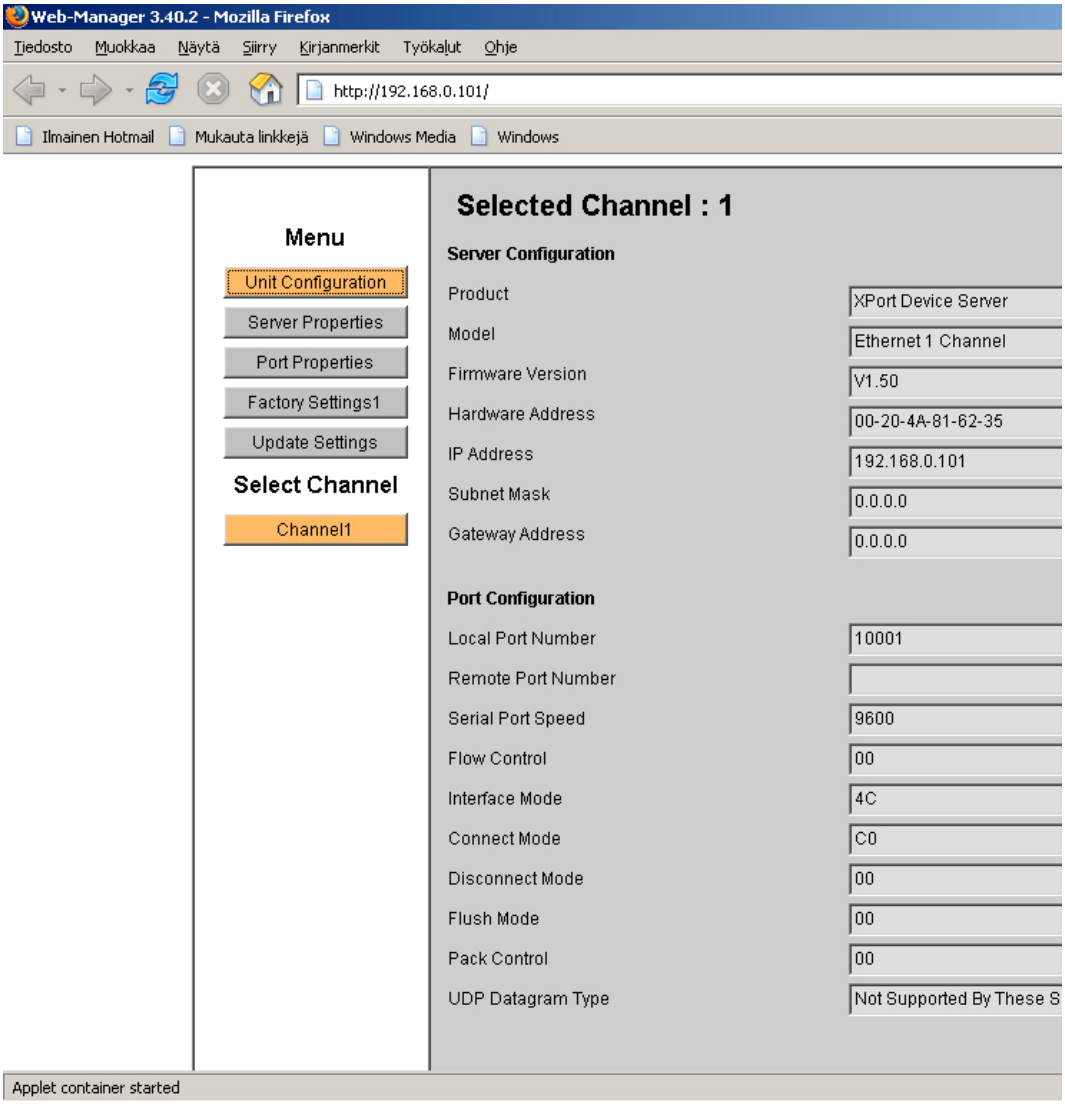
Yhteys HHL-laniin otettiin Lantronix Device Installer -pääteohjelmalla. Tässä tapauksessa IP-osoite otettiin dynaamisesti langattomalta reitittimeltä.



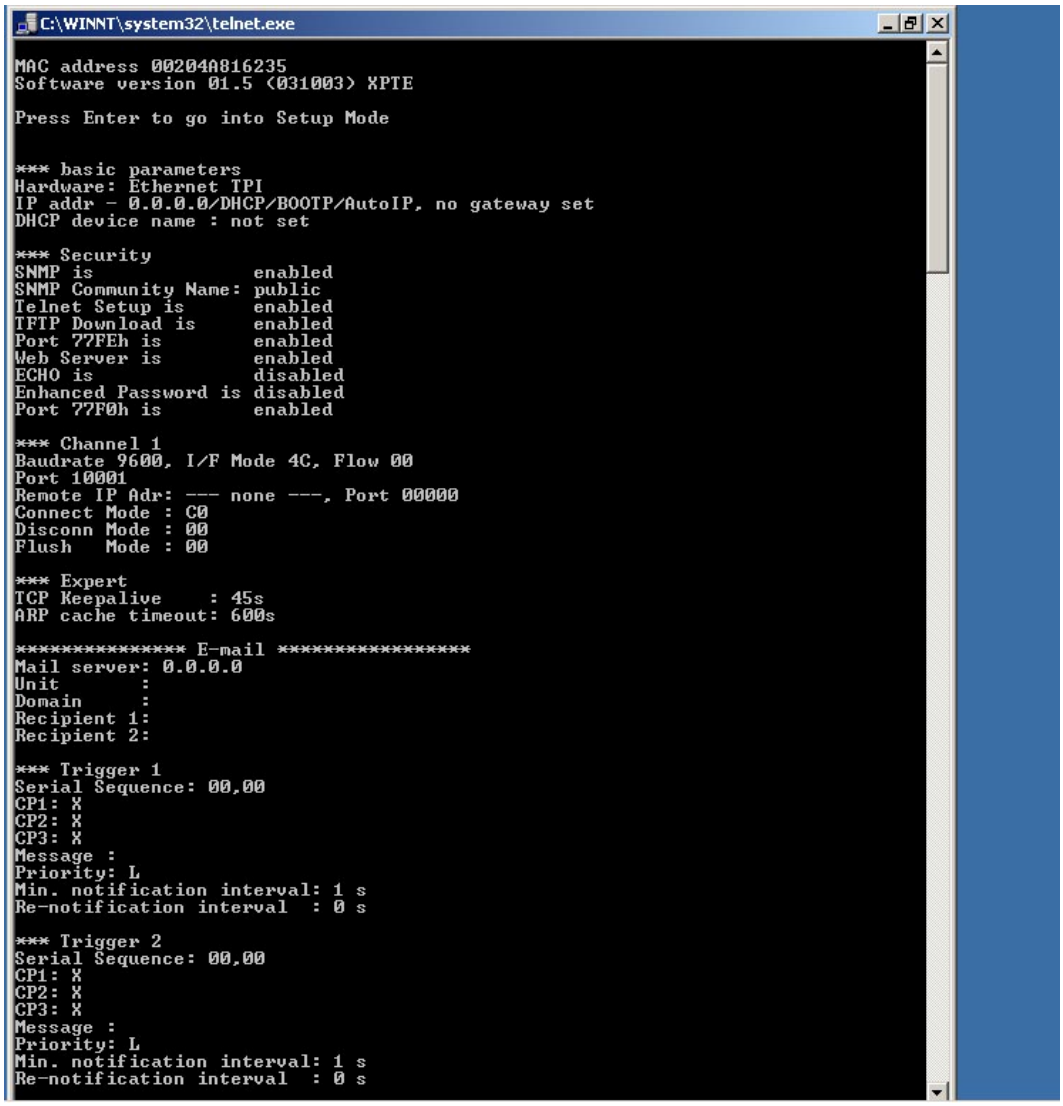
KUVIO 10. Yhteyden muodostaminen

Device Installer-ohjelmalla haettiin HHL-lanille IP-osoite käyttämällä Assign IP -toimintoa. Langaton reititin antoi osoitteen dynaamisesti, ja yhteys saatiin välttömästi toimimaan. Yhteyden muodostuminen varmistettiin lähettämällä kaiutuspaketti (ping) HHL-lanille. Ethereralilla voitiin todentaa, että vastauspingi saapui takaisin oikealta mac-osoitteelta (kuvio 10). Samalla voitiin todeta, että yhteys kulkee salaamattomana ja mitään salasanoja yhteyden autentikoimiseksi ei vaadita.

Yhteyden konfigurointiin voidaan käyttää joko selainpohjaisesti Web Manager -ohjelmaa (kuvio 11) tai Telnet-yhteyttä (kuvio 12) tekstipohjaisesti. Telnet liikenne kulkee aina selväkielisenä, joten tietoturvasyistä sitä ei tulisi käyttää muuta kuin sisäverkossa tapahtuviin yhteyksiin.



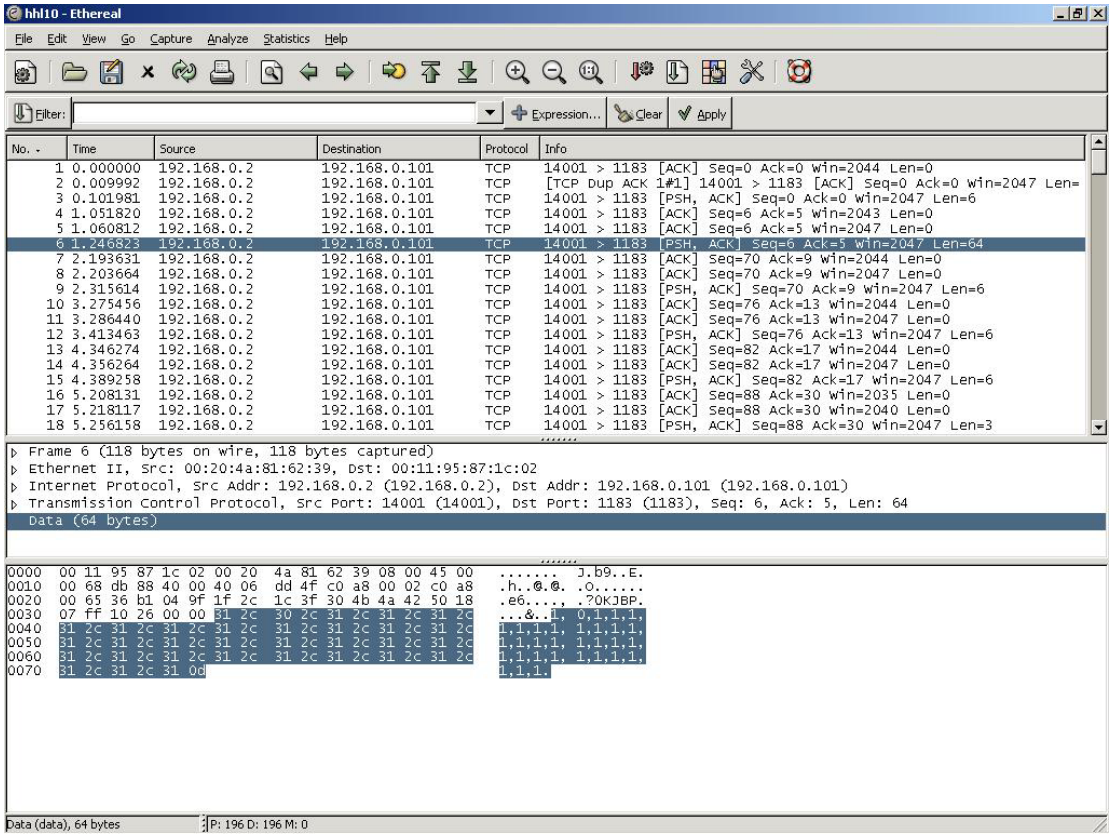
KUVIO 11. Graafinen käyttöliittymä



KUVIO 12. Telnet-liittymä

5.4 Testiyhteys HHL-keskukseen

Varsinainen yhteys HHL-keskukseen otetaan erillisillä Hs-Setup-, Netfront- ja Main-ohjelmilla. Näiden avulla asetetaan kaikki valvontaan liittyvät aika- ja kulkuoikeusparametrit.



KUVIO 13. Verkkoanalysaattorin kaappaus datasta

Ohjausdataa hallintatietokoneen ja keskuksen välisestä liikenteestä kaapattiin kolmella eri verkkoanalysaattorilla. Testattavat ohjelmat olivat Ethereal, Softperfect Network Protocol Analyzer sekä ZxSniffer. Kuviossa 13 esitetty kuvaruutukaappaus Ethereal-analysaattorista osoittaa, että salasanat ja ohjausdata siirtyvät salattuna, joten ainakin tavallisimmat analysointiohjelmat eivät pysty näyttämään dataa selväkielisenä. Testissä ei pyritty murtamaan HHL-keskuksen salausta, vaan tarkoituksena oli selvittää salauksen olemassaolo, sillä useilla turvalaiteasentajilla on ollut mielikuva HHL-keskuksen salaamattomasta ohjausliikenteestä.

Mikäli ulkopuolinen taho pääsee kaappaamaan verkkoliikennettä joko sisäverkosta tai julkisesta TCP/IP-liikenteestä esimerkiksi yrityksen palvelimen

välityksellä, voi pääsy HHL-keskukseen olla mahdollista. Kevyesti salatun datan purkaminen ei ole mahdoton tehtävä, ja mitä enemmän datatietoa voidaan kerätä, sitä helpompaa on selvittää käytettävät salausmenetelmät. Murtautuminen voi olla jopa tahatonta hakkeritoimintaa, jolla voi olla kiinteistön turvallisuuden kannalta tuhoisia vaikutuksia. Keskuksen kautta voidaan hälytyksiä kytkeä pois päältä sekä avata esimerkiksi kiinteistössä olevia sähkölukituksia. Mikäli samaan järjestelmään on liitetty taloteknisiä laitteistoja, saattaa esimerkiksi kiinteistön lämmitysjärjestelmä olla manipuloitavissa.

Turvajärjestelmälaitteiston valmistajan tulisi huomioida ohjausliikenteen siirtymisen julkiseen TCP/IP-verkkoon laatimalla riittävä ohjeistus turvallisista hallintajärjestelmiin muodostetuista yhteystyypeistä. Turva- ja taloteknisten järjestelmien yhdistyminen luo paljon mahdollisuuksia mutta myös lisääntyvää haavoittuvuutta, mikäli tietoturva-asioihin ei paneuduta riittävän tehokkaasti.

6 JÄRJESTELMÄKOKONAISUUDEN LUOMINEN

6.1 Nykyiset dokumentointijärjestelmät

Hallintajärjestelmien rakentamisessa ei nykyisin ole käytössä dokumentointijärjestelmää vaan järjestelmäkokonaisuudet ovat lähinnä asennushenkilökunnan ja käyttäjien muistissa. Laitteistoista vastuussa olevien työntekijöiden sairastuessa tai siirtyessä toisiin työtehtäviin ei korvaavilla henkilöillä ole välttämättä riittävää kuvaa kokonaisuuden hallinnasta. Lisäksi järjestelmän monistaminen muihin ympäristöihin on vaikeaa. Puuttuva dokumentointi estää myös kokonaisuuden tuotteistamisen.

Turvajärjestelmien suunnittelu suoritetaan arkkitehtisuunnitelmien pohjapiirroksiin, jotka yleensä toimitetaan paperikopioina. Osaluettelot ja kaapelimäärät laaditaan käsin pohjapiirroksiin merkittyjen suunnitelmien perusteella. Mikäli suunnitelmiin tulee muutoksia suunnittelu- tai toteutusvaiheessa, aiheuttavat ne kohtuuttomasti ylimääräisiä piirustus- ja kopiointikuluja.

6.2 Järjestelmät erillisinä kokonaisuuksina

Turvajärjestelmät toimivat itsenäisinä yksiköinä ja niiden käyttämiseen ei välttämättä tarvita erillisiä verkkoon tai muuhun siirtomediaan sidottuja keskitettyjä hallintapisteitä. Hälytysten siirto esimerkiksi vartiointiliikkeeseen voidaan toteuttaa joko matkapuhelin- tai lankapuhelintekniikalla. Valvontakameroiden nauhoitukset tallennetaan kovalevytallentimille, jotka sijaitsevat keskuksen läheisyydessä. Kulunvalvonnan ja hälytysjärjestelmien keskuksen konfigurointi ja asetusten muuttaminen voidaan suorittaa valikkopohjaisen käyttölaitteen välityksellä. Muutosten tekeminen kuitenkin vaatii aina käyntiä käyttölaitteen luona.

Valvottavien kiinteistöjen lukumäärän kasvaessa keskitetty hallinta saattaa nousta varteenotettavaksi vaihtoehdoksi. Valvontakameroiden tallentimien ohjaus ja purku voidaan suorittaa IP-verkon välityksellä selainpohjaisesti. Ovien kulkuoikeuksien muutokset pystytään hallitsemaan keskitetysti. Hälytystietojen

ohjaukset voidaan osoittaa työaikana henkilökunnalle ja työajan ulkopuolella vartiointiliikkeeseen.

6.3 Vaihtoehdot järjestelmien väliseksi yhteydeksi

Yksittäisen kiinteistön hallinta voidaan suorittaa keskitetysti, mikäli kiinteistössä on riittävän laaja sisäverkko, johon voidaan liittää ilmoitinkeskuksia HHL-lanien välityksellä. Tällä tavalla rakennettu järjestelmä on tarvittaessa helppo liittää laajempaan keskitettyyn hallintajärjestelmään.

Useiden kiinteistöjen hallintaan tarvittava yhteys voidaan muodostaa analogisesti modeemin välityksellä piirikytkentäistä puhelinverkkoa hyödyntäen. Tällöin yhteyden molemmissa päissä pitää olla modeemi sekä soittosarjat. ISDN-yhteys tarjoaa digitaalisen vaihtoehdon, jos liittymän vaihto digitaaliseen ISDN -liittymään on mahdollista. Kiinteistöjen ADSL-liittymät mahdollistavat hallinnan ilman erillisiä liittymä- ja puhelinkustannuksia. Mikäli rakennukset sijaitsevat lähekkäin, yhteys voidaan muodostaa myös langattoman WLAN-verkon välityksellä.

6.4 Vaihtoehdot järjestelmien suunnitteluun

Järjestelmien suunnitteluun tarvitaan kiinteistöistä laaditut rakennuspiirustukset. Vanhoissa kiinteistöissä on usein käytettävissä ainoastaan piirustusten paperikopiot, jolloin suunnittelumerkintöjen piirtämistä varten niistä voidaan ottaa kopiot muoville tai kuultopaperille. Suunnittelu suoritetaan tällöin piirtämällä tarvittavat muutokset rakennuspiirustuksiin sekä laatimalla osaluettelot käsin luetteloimalla. Toinen vaihtoehto on skannata kuvat tietokoneelle ja muodostaa CAD-yhteensopiva formaatti käyttäen vektorointiohjelmaa.

Uudemmista kiinteistöistä on mahdollista saada suunnitelmat suoraan sähköisessä muodossa joko dwg- tai dxf-formaatissa. Sähköisiin suunnitelmiin piirretyistä kuvista voidaan tulostaa paperiversiot työmaakäyttöön sekä kiinteistön arkistoon. Toteuttamalla suunnittelu CAD-pohjaisella turvasovelluksella digitalisoituihin rakennuspiirustuksiin voidaan osaluettelointi saada ohjelmallisesti.

6.5 Tavoitteet kokonaisuuden hallintaan

Kokonaisuuden hallittavuudessa voidaan kulkea useampaa eri tietä. Mikäli kaikki keskitetään yhdelle hallintatyöasemalle, saattaa ongelmaksi tulla toiminnan turvaaminen, jos hallintatyöasema jostakin syystä rikkoutuu tai ei pääse verkkoon. Hallintaohjelmiston käyttö usealta työasemalta on varmempaa, mutta tietojen päivitys on tällöin saatava jotenkin hallintaan, jotta vältytään päällekäisiltä operoinneilta.

Hallintaohjelmistojen sijoittaminen palvelimelle ja niiden käyttäminen esimerkiksi VPN-tunneloinnin välityksellä mahdollistaisi etäkäytön useista eri toimipisteistä. Tällä järjestelmällä voitaisiin estää päällekkäiset kirjautumiset sekä turvata lokitiedot keskitettyyn tallennuspaikkaan. Vaihtoehtojen pitää soveltua asiakkaan vaatimuksiin ja toimintaympäristöön.

6.6 Tavoitteet dokumentointiin

Dokumentoinnin pitää olla helppokäyttöinen ja selkeä ylläpitää. Järjestelmän osien muutosten, korjausten sekä päivitysten kirjaaminen selkeään ja havainnolliseen muotoon pitäisi olla riittävän vaivatonta. Myöskään dokumentoinnin tekeminen ei saisi kuluttaa tarpeetonta resurssia eikä muodostua rasitteeksi. Mikäli järjestelmästä tulee liian kankea, se ei palvele varsinaista tarkoitustaan.

Järjestelmien suunnittelu aloitetaan lähtötietojen kartoituksella, jossa määritellään asiakkaan tarvitsema toiminnallinen turvallisuus, kiinteistön kulkujärjestelyt ja turvatekniset ratkaisut. Kohteen turvajärjestelmistä pitää pystyä tuottamaan taso- ja järjestelmäpiirustukset CAD-tiedostoina, laiteluettelot sekä käyttöohjeet henkilöstölle. Etähallinnan yhteyksien suunnittelussa on huomioitava eri siirtomedioiden tietoturvariskit. Dokumentointijärjestelmä laitteistojen IP-osoitteista sekä fyysisestä sijainnista rakennetaan selkeäksi. Asentajien sekä järjestelmän huollosta vastaavien on pystyttävä hyödyntämään järjestelmätietoja tehokkaasti. Asentajilla tulee olla selkeät ohjeistukset ja apuohjelmat, jotta esimerkiksi sisäverkkoon liittyminen ja verkon IP-avaruuden määrittäminen voidaan suorittaa ilman TCP/IP-aliverkotuksen perusteellista tuntemista (LIITTEET 2 ja 3).

7 JÄRJESTELMÄN MALLINNUS

7.1 Järjestelmien väliset yhteydet ja suunnittelutyökalut

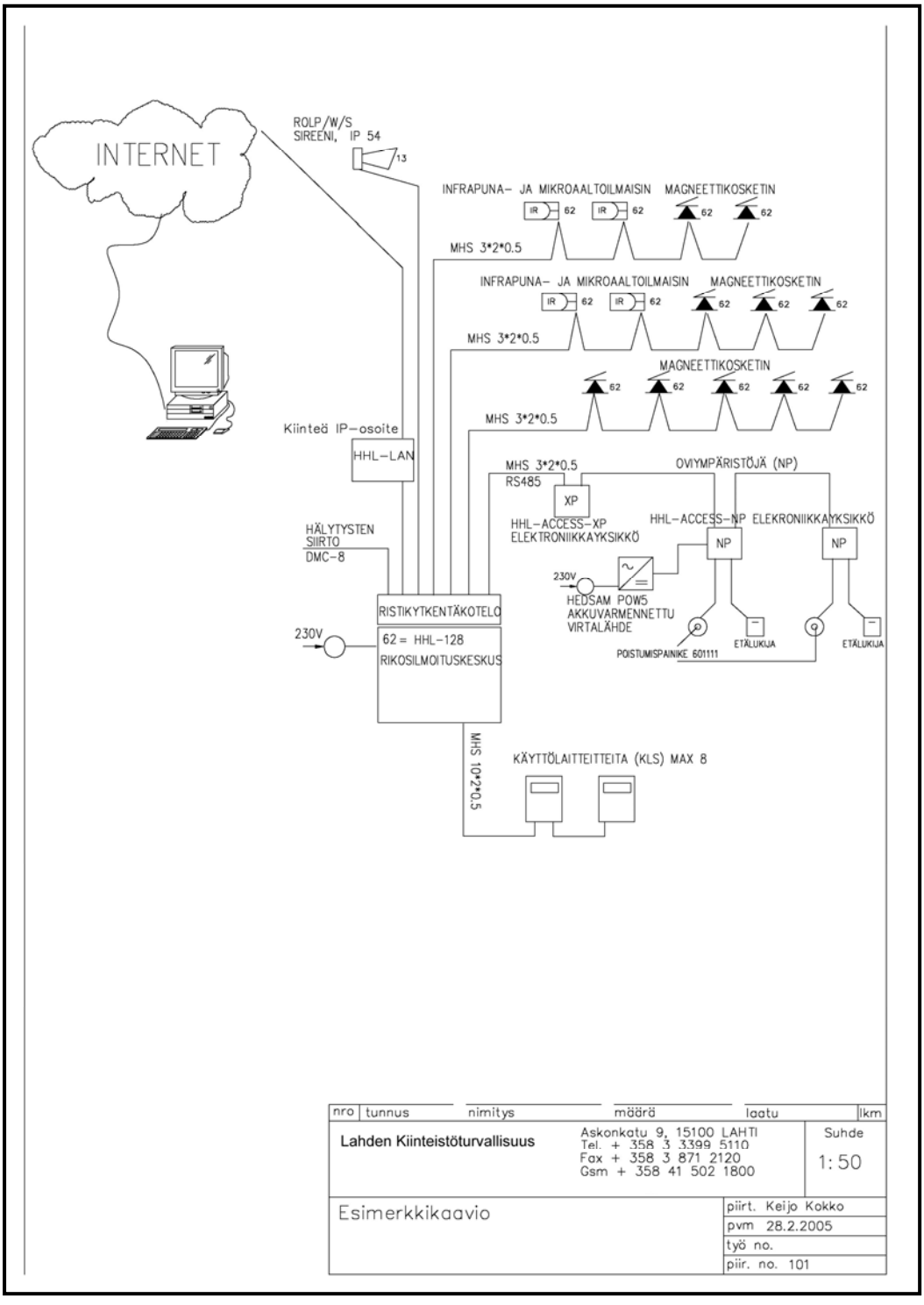
Koska lähes kaikki kiinteistöt on varustettu ADSL-yhteydellä, on järkevää hyödyntää tätä mahdollisuutta myös etähallinnan yhteystyypiksi. Etäyhteys on muodostettava aina VPN-yhteytenä. Mikäli kiinteistöön on liitetty ainoastaan puhelinlinja, voidaan yhteys muodostaa modeemilla tai ISDN-yhteytenä.

Suunnittelutyökaluna käytetään Kymdadan CADS-ohjelmaa ja sen turvasovellusta. Kiinteistöjen paperille tulostetuista ark-kuvista tehdään vektorointiohjelmalla dwg-kuvia, joihin suunnitellaan kiinteistökohtaiset laitekuvaukset. Mikäli kiinteistön ark-suunnitelmat ovat jo valmiiksi dwg-muodossa, voidaan niitä hyödyntää suoraan. Yrityksen käytössä on 3 kpl CADS-lisenssejä, joihin kaikkiin on asennettu turvasovellus. Laitevalmistaja pystyy myös tarjoamaan ohjelmistolaajennusta, jonka avulla voidaan havainnollistaa hälytysjärjestelmä ja nopeasti paikallistaa hälytyksen tehnyt valvontaelin. Suunnittelussa olisi hyvä voida käyttää valmistajan omaa suunnittelusovellusta, joka tarjoaisi riittävän päivitettävyyden sekä ohjelmien että komponenttien osalta.

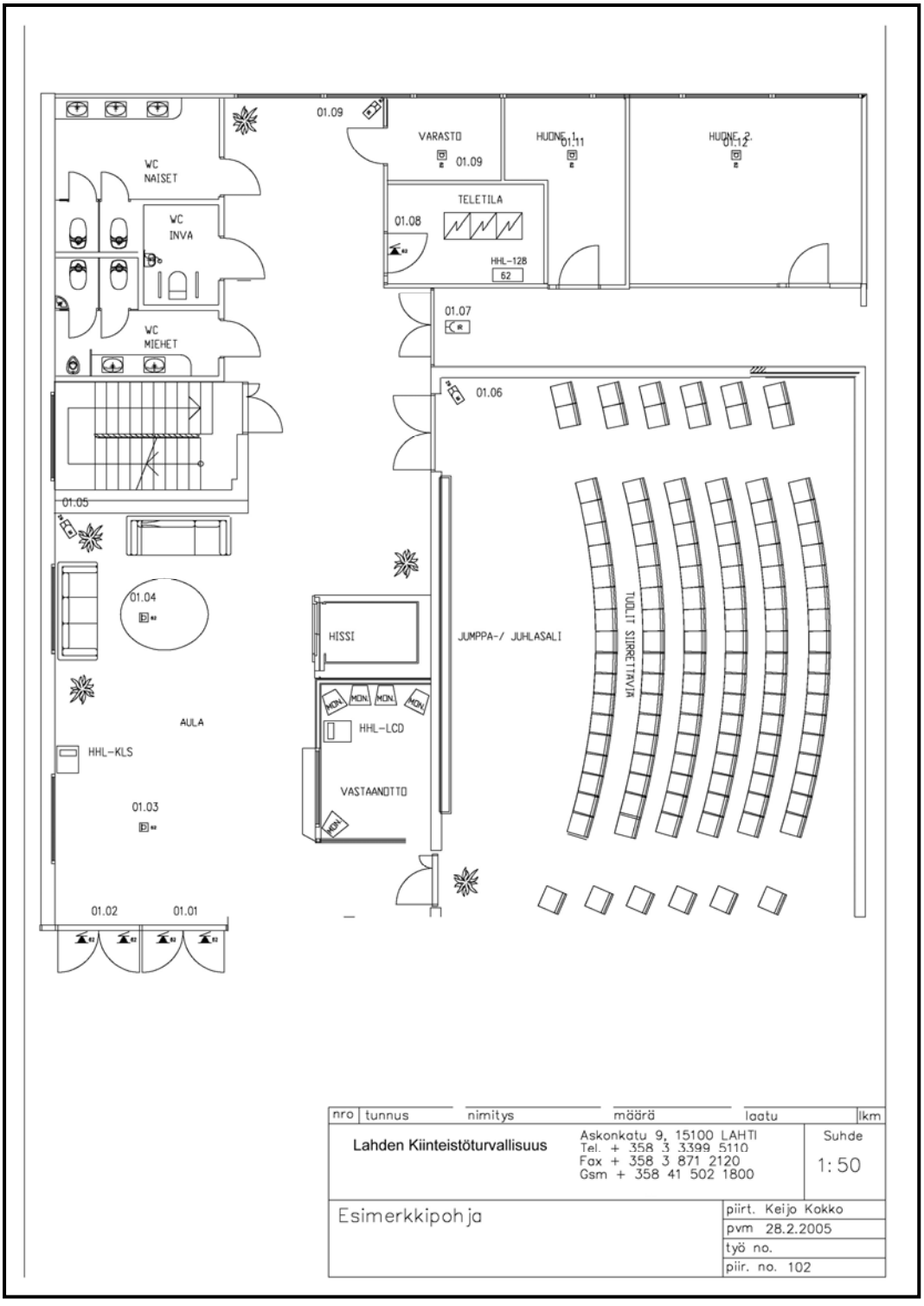
7.2 Dokumentoinnin mallinnus

Kuviossa 14 on esitetty linjakaavio kiinteistön rikosilmoitin- ja kulunvalvontajärjestelmästä. Nykyaikaisella ilmoituskeskuksella voidaan hallita varsinaisten rikosilmoitusjärjestelmien lisäksi kulunvalvontaa, talotekniikkaa, kameravalvontaa sekä ovijärjestelmiin liittyvää automatiikkaa. Ilmoituskeskuksen hallinta voidaan suorittaa keskitetysti TCP/IP-tekniikalla esimerkiksi yritykseen liitetyn laajakaistayhteyden välityksellä.

Kuviossa 15 on rikosilmoitin- ja kulunvalvontalaitteet sijoitettu kiinteistön pohjapiirrokseen. Sähköisiin piirustuksiin voidaan helposti tehdä muutoksia tai lisäyksiä, mikäli kiinteistön käyttötarkoitus vaihtuu.



KUVIO 14. Esimerkkikaavio linjapiirroksesta



KUVIO 15. Esimerkkipohja rikosilmoittimista ja kulunvalvonnasta

CAD-pohjaisen suunnittelujärjestelmän avulla turvalaitteistot voidaan sijoittaa suoraan sähköisiin arkkitehtipiirroksiin. Sovelluksesta voidaan tulostaa osaluettelot tarjouslaskennan ja asennuksen käyttöön. Asennusta varten tulostetaan vain suoritettavan työvaiheen asennus- ja kytkentäpiirustukset (LIITE 4). Kaapelointien asennuksessa tarvitaan ainoastaan tasopiirustukset, joihin on merkitty kaapelityypit ja niiden sijainti. Laiteluettelot ja niiden sijoituspiirustukset esitetään erillisessä kuvassa.

Järjestelmäkaavioissa ei saa olla päätepalvelimien IP-osoitteita näkyvissä. IP-osoitteet saadaan tarvittaessa näkyviin ohjelmallisesti. IP-verkkojen segmentit nimetään jokaisen osaston ja kiinteistön osalta. Kaavioissa esitetään valvottavat ovet, tilat, hissit, ym. kohteet silmukoittain sekä osoitepäätteiden numerointi, osoitteet ja tieto, mihin valvontalaitteeseen ne on kytketty. Nämä tiedot luetteloidaan jokaisen HHL-keskuksen osalta. IP-verkkoon kytkettävät päätepalvelimet nimetään ja ilmoitetaan, minkä nimiseen segmenttiin ne kuuluvat. Järjestelmiin määritetään, miten niitä etähallitaan ja kenellä on oikeus suorittaa hallintatehtäviä. Järjestelmä on voitava esittää graafisesti A4-tai A3-muodossa kiinteistökohtaisesti sekä lisäksi hallinnan osalta tärkeimmät toiminnot koko järjestelmästä.

7.3 Lähtötietojen määritys

Järjestelmän suunnitteluun tarvittavat lähtötiedot määriteltiin seuraavan jaottelun mukaisesti (LIITE 1):

- järjestelmään liitettävät kiinteistöt
- pohjapiirustukset kiinteistöistä ja tiloista
- tarvittavat toiminnot (kulunvalvonta, murtohälytys, tilojen ohjaus, palohälytys, videovalvonta, työaikaseuranta, ruokalaseuranta, kiinteistöjen kuorisuojaus ja henkilöstön turvallisuus)
- siirtomediat keskusten ja hallintajärjestelmän välillä:
    - modeemiyhteys
    - ISDN-yhteys
    - sisäverkkoyhteys
    - yhteys julkisen TCP/IP-verkon yli (VPN, muut suojatut yhteydet)

- hallintaoikeudet (keskitetty hallinta vai hajautettu kiinteistökohtaisesti)
- laajennettavuus (ja laajennuksien helppo päivitettävyys dokumentointijärjestelmään.)
- päivitettävyys
- vikailmoitusten lähetysosoite
- turvatasot
- olemassa olevat laitteistot joita voidaan hyödyntää
- olemassa olevat, hyödynnettävät siirtomediat
- mahdolliset turvauhat.

Dokumentointi muodostuu suunnittelun ja projektin toteutuksen aikana valmistuneista piirroksista ja suunnittelutiedoista. Projektin aikana tapahtuneet muutokset ja lisäykset kirjataan suunnitelmiin. Muutostietosarakkeisiin kirjataan kuvaus muutoksesta sekä päiväys. Muutostiedot ja päivitetyt suunnitteludokumentit toimitetaan tilaajalle kohteen luovutuksen yhteydessä.

8 YHTEENVETO JA JOHTOPÄÄTÖKSET

Kiinteistöjen turvajärjestelmät sekä automaattiset talotekniikan hallinta- ja säätöjärjestelmät tulevat yleistymään. Lähes kaikkiin uudisrakennuksiin laaditaan turvasuunnitelma, jonka avulla turvajärjestelmät voidaan asentaa. Kiinteistöjen kunnostustöiden yhteydessä toteutetaan yleensä tietoverkon yleiskaapeloinnin asennus sekä turvatasojen kartoitus sekä mahdollinen turvatason nosto.

Nykyisin turvajärjestelmien kaapelointi toteutetaan omana runkoverkkona, joka ei hyödynnä kiinteistöön mahdollisesti asennettavaa sisäverkon yleiskaapelointia. Tässä suhteessa turva-alalla vallitsee selkeä kahtiajako. Osa turvasuunnittelijoista haluaa pitää turvajärjestelmien kaapelointiverkon kokonaan erillään yleiskaapelointiverkosta ja osa suunnittelijoista pyrkii löytämään mahdollisuuksia yleiskaapelointiverkon hyödyntämiselle.

Turvalaitevalmistajilla on tuotteistossaan komponentteja joilla turvajärjestelmä voidaan liittää osaksi sisäverkkoa. Osoitepäätteiden avulla kärki- ja ohjaustietoja voidaan siirtää turvallisesti kiinteistössä. Valitettavasti turvajärjestelmien komponentit ja ohjelmistot ovat valmistajakohtaisia eivätkä näin ollen ole toisten valmistajien komponenttien kanssa yhteensopivia. Yhteinen standardointi ja ohjelmistot mahdollistaisivat yhteisen kehitystyön, jonka avulla tietoturvan tason kohottaminen olisi kustannustehokkaampaa. Tämä helpottaisi järjestelmien siirtämistä osaksi kiinteistön sisäverkkoa.

Kaupunkien ja kuntien omistuksessa on lukuisia kiinteistöjä, joissa päiväkäyttäjien lisäksi on iltakäyttäjiä sekä satunnaisia käyttäjiä. Esimerkkinä mainittakoon liikuntatilat, joiden päiväkäyttö on lähinnä koulujen hallinnassa, mutta iltakäyttäjinä ovat urheiluseurat sekä yritykset. Ovien avaaminen ja sulkeminen hoidetaan pääasiassa vahtimestarien tai huoltomiesten toimesta.

Nykyaikaisten kulunvalvontajärjestelmien ansiosta avainhallinta ja kulkuoikeudet voidaan määrittää käyttäjä- sekä aikaperusteisesti. Esimerkiksi koulun liikuntatilojen käyttö voidaan automatisoida siten, että varsinaista jatkuvaa päivystystä ei enää tarvita. Tarvittavat kulkuoikeuksien muutokset voidaan suorittaa keskitetysti yhteisen hallintajärjestelmän avulla. Vastaavasti kiinteistön

muut turva- ja taloteknisten järjestelmien valvonta voidaan siirtää keskitettyyn valvomoon. Tämä säästää resursseja sekä vapauttaa henkilökuntaa muihin huolto- ja kunnostustehtäviin.

Tekniset valmiudet järjestelmien etähallinnalle ovat olemassa, mutta vain harvassa kaupungissa tai kunnassa on ryhdytty toimiin keskitetyn hallinnan toteuttamiseksi. Markkinoilla ei ole ollut valmista tuotetta ja ratkaisumallia etähallinnan järjestämiseksi.

Tässä opinnäytetyössä pyrittiin laatimaan työkaluja, joiden avulla järjestelmien etähallinnan dokumentointi olisi helpompi ja yksiselitteisempi toteuttaa. Hallintaan käytettävien siirtomedioiden vertailu ja turvallisuusnäkökohtien tutkiminen mahdollisesti auttaa kumoamaan turva-alalla vallitsevan käsityksen siitä, että TCP/IP-verkon käyttäminen osana turvajärjestelmiä ei tarjoa riittävää turvatasoa. Järjestelmien laajeneminen johtaa siihen, että rinnakkaisia kaapelointeja ei ole enää taloudellisesti perusteltua käyttää. Mikäli kiinteistöön on asennettu yleiskaapelointi, sen hyödyntäminen kannattaa tutkia huolellisesti.

Suunnittelutyökalun valinta oli tässä yritysympäristössä helppoa, sillä yrityksen käytössä on tarvittavat suunniteluohjelmistot, jolloin yhteisen dokumentointimallin puuttuminen on ollut ainoa hidaste suunnittelutyökalujen hyödyntämiselle. Dataliikenteen suojaustyyppejä ja -tasoja ei laitevalmistajien taholta turvallisuussyistä haluttu paljastaa, ja siksi niiden sisäisiin turvallisuusvaatimuksiin ei ole ollut mahdollisuutta puuttua. Etähallinnan dataliikenteen turvallisuuteen voidaan kuitenkin oleellisesti vaikuttaa käyttämällä vahvasti suojattuja yhteysprotokollia.

Keskeisimmät ongelmat järjestelmän rakentamisessa ovat olleet riittävän dokumentoinnin puute sekä sisäverkkojen vapaiden IP-osoitteiden määrittäminen. CAD-pohjaisen suunnitteluun ja dokumentointiin on ollut tekniset mahdollisuudet, mutta yhteistä menettelytapaa ei ollut rakennettu. Haastavinta työssä on ollut omaksua eri turvajärjestelmien keskeiset tiedonsiirtoperiaatteet sekä CAD-suunnittelun perusteet.

Työssä laaditut määritykset ja työkalut ovat hyödyksi vain siinä tapauksessa, että niitä käytetään. Käytännön työssä huomataan varmaankin monia kehityskohteita, joita ei tässä opinnäytetyössä tullut esiin. Järjestelmä tulee muotoutumaan ajan kuluessa käyttäjiensä näköiseksi, jolloin se toivottavasti palvelee tarkoitustaan entistä paremmin.

Kohdeyrityksen tavoitteena on hallintajärjestelmän tuotteistaminen. Tämä selvitystyö antaa komponentteja, joiden avulla tuotteistaminen voidaan selkeyttää, jolloin myyntityö asiakkaalle tulee helpottumaan. Mikäli tuote osoittautuu riittävän hyväksi, erottuu yritys muista kilpailijoista ja riski joutumisesta ankaraan hintakilpailuun vähenee.

LÄHTEET

Comer, D, J. 2002. TCP/IP. Gummerus, Jyväskylä.

Cisco CCNA kurssimateriaali v2.1.4 [verkkodokumentti]. [viitattu 11.12.2005] Saatavissa: http//www.cisco.com

Granlund, K. P. 2000. Tietoliikenne 2. painos. Gummerus, Jyväskylä.

Granlund, K. P. 2001. Langaton tiedonsiirtoWSOY, Jyväskylä.

Hakala, M, Vainio, M, P. 2005. Tietoverkon rakentaminen. WSOY, Helsinki.

Hyvä asuminen 2010 kehitysohjelma/Tilastokeskus [verkkodokumentti]. Helsinki [viitattu 12.12.2005] Saatavissa:http://www.kiinteistoliitto.fi/attachements/2005-03-15T15-51-0467.pdf

Keogh, J, P. 2001. Verkkotekniikat – tehokas hallinta. Edita Oyj, Helsinki.

Kuusi, P. Esitelmä [verkkodokumentti]. Helsinki: Teknillinen korkeakoulu, 1999 [viitattu 28.2.2005]. Saatavissa: http: //netlab.tkk.fi / opetus / s38117 / k99 / Esitelmat / pyry_kuusi.pdf

Laamanen, T. esitelmä [verkkodokumentti], Jyväskylä: Jyväskylän yliopisto tietotekniikan laitos 2000 [viitattu 15.1.2005]. Saatavissa: http://www.cc.jyu.fi/~laamanen/datasiirto

Perlmutter, P., Zarkower J. 2001. Virtuaaliset yksityisverkot. Edita Oyj, Helsinki.

Puska, M. J. 2000. Lähiverkkojen tekniikka. Gummerus, Jyväskylä.

LIITTEET:

LIITE 1. Lähtötietokaavake

LIITE 2. Aliverkon osoiteavaruuden määrittäminen

LIITE 3. Aliverkotuslaskuri

LIITE 4 tasopiirustus rikosilmoitin ja johdotuskaavio

LIITE 1. Lähtötietokaavake

Päiväys	24.02.2005
Kohde	Esimerkkikonttori
Kiinteistö	toimistotalo

tarvittavat toiminnot

	kerros	**tila**	**krs**	**tila**	**kerros**	**tila**	**kerros**	**tila**
	1	Konttori 1	**2**					
murtohälytys		**x**						
kulunvalvonta		**x**						
ohjaus								
palohälytys		**x**						
videovalvonta								
työaikaseuranta		**x**						
ruokalaseuranta								
kuorisuojaus								
henkilöstön turvallisuus								

LÄHIVERKON TIEDOT (C-luokan aliverkko)
Selvitä IP-laskurin avulla mihin aliverkkoon HHL-lan kuuluu.
Aseta vapaa IP-osoite staattisesti laniin

Sisäverkon hallintakoneen IP-osoite	**192**	**168**	**0**	**101**
Aliverkon peite	**255**	**255**	**255**	**0**
Aliverkkojen lukumäärä	**8**			
käytettävissä oleva IP-osoitealue	**192.168.0.96 - 192.168.0.127**			

HHL-LANIN OSOITE	**192.168.0.120**

Siirtomediat keskusten ja hallintajärjestelmien välillä

		Modeemi	**ISDN**		**LAN**	**ADSL**	**VPN**	**yhteystiedot**
Kiinteistö	**Keskus**							

Toimistotalo	konttori1/HHL128	**x**							

Hallintaoikeudet

	nimi	Käyttöikeustaso
pääkäyttäjä	Jaakko Toimisto	laaja
sivukäyttäjä 1	Pekka Paperi	rajoitettu
sivukäyttäjä 2		
sivukäyttäjä 3		
sivukäyttäjä 4		
sivukäyttäjä 5		
sivukäyttäjä 6		

VARTIOINTI: Securitas

VIIVEET (s)
SISÄÄN:
ULOS:

SIREENIT:

ROBOTTI:
PUH.NRO:
KOHDETUNNUS:

KANAVAT:

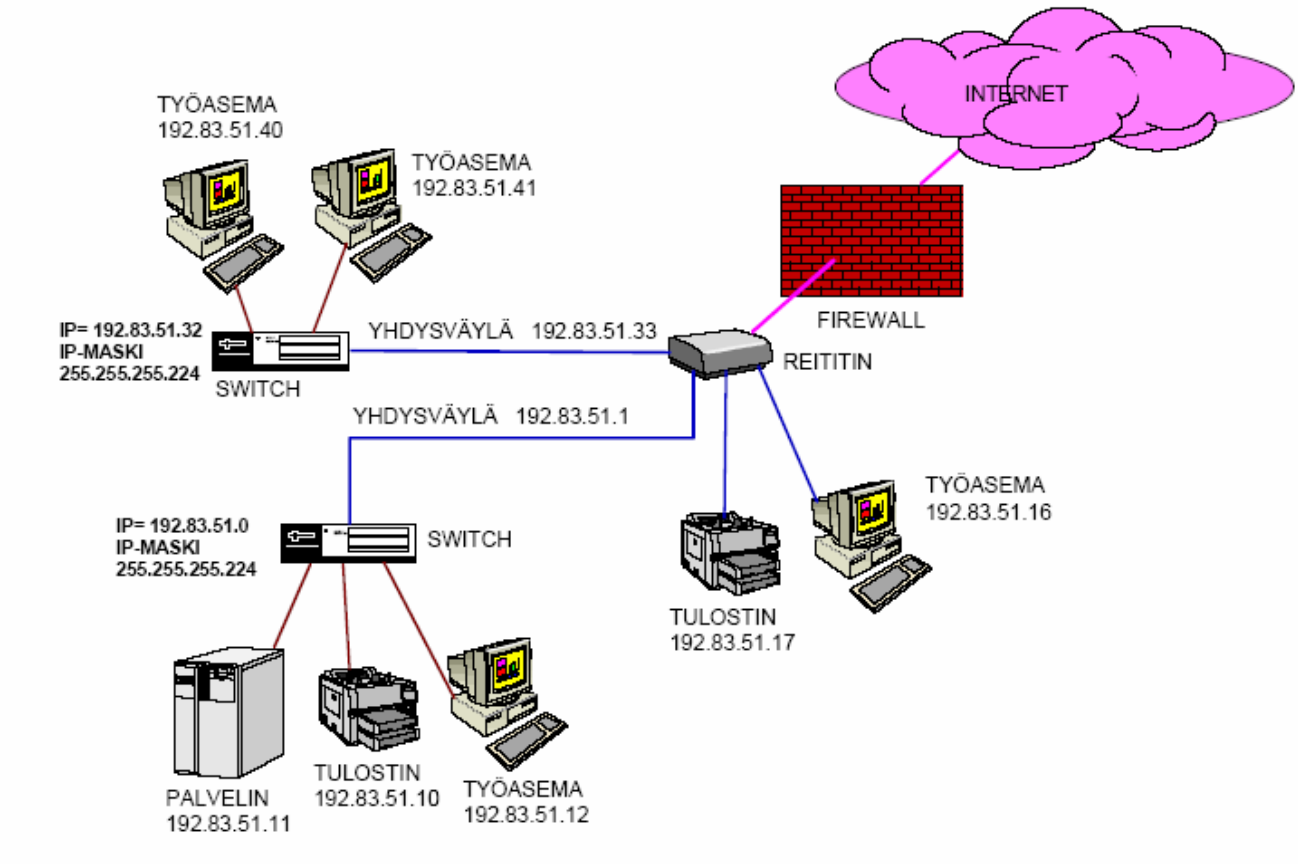
1.	aula murto	**2.**	tsto murto	**3.**	yö/päivä
4.		**5.**		**6.**	

7.	**8.**	**9.**
10.	**11.**	**12.**

SILMUKKATIEDOT:

1.	wc aula	**2.**	varasto	**3.**	teletila
4.	Huone1.	**5.**	Huone2.	**6.**	Huone3.
7.		**8.**		**9.**	
10.		**11.**		**12.**	
13.		**14.**		**15.**	

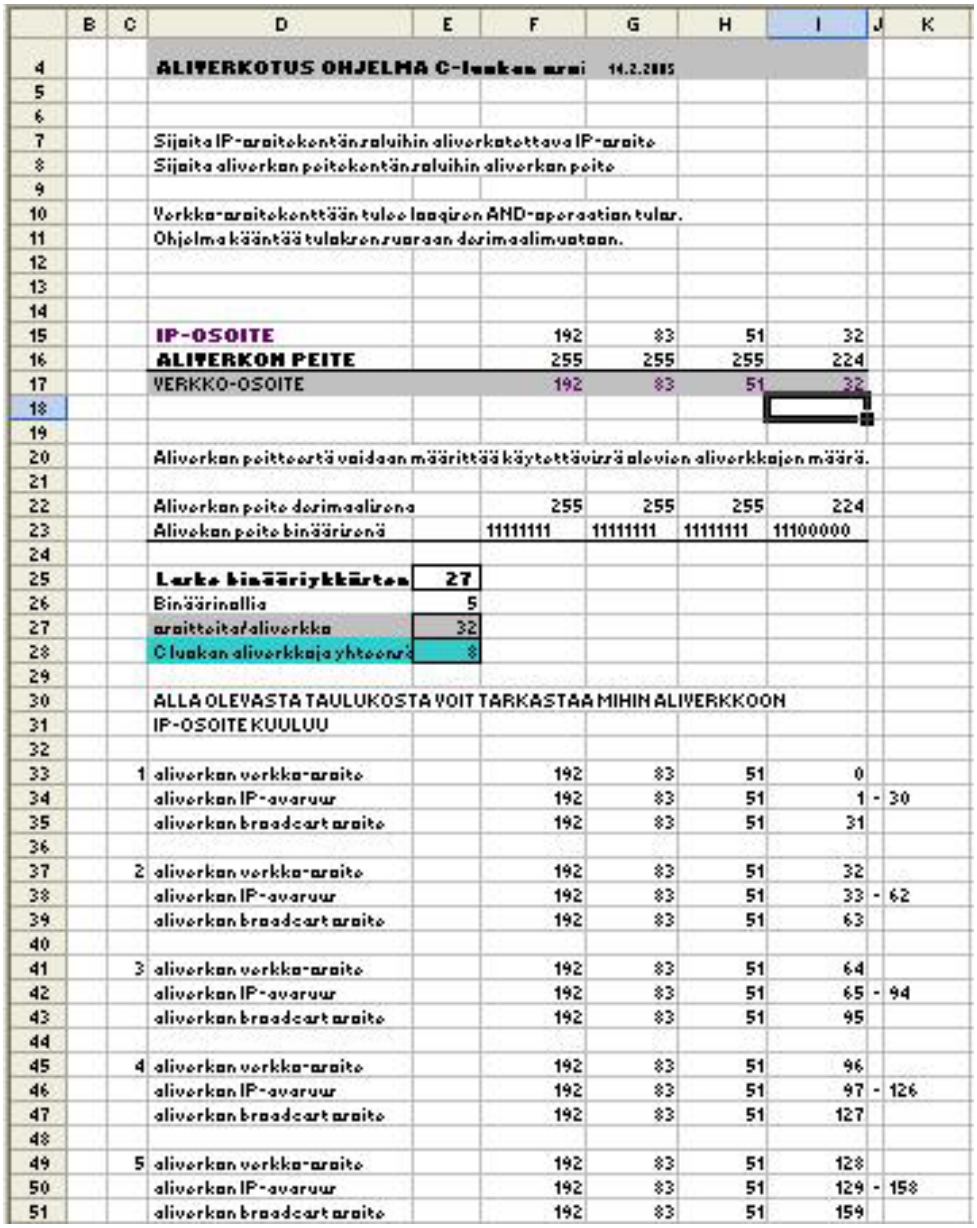
LIITE 2. Aliverkon osoiteavaruuden määrittäminen



segmentoitu sisäverkko (Luentomoniste v.3.1, Osa I
Mikko Lipponen, M.Sc.)

HHL-lanien liittämiseksi sisäverkkoon on pystyttävä selvittämään kyseisen sisäverkon osoiteavaruus. Riittääkö esimerkiksi aliverkossa 192.83.51.32 / 27 vapaita osoitteita jos työasemien osoitteet ovat väliltä 192.83.51.40 – 192.83.51.57? Selvitystyö on aloitettava aliverkon osoiteavaruuden määrittämisellä. Selvittämiseen voidaan käyttää exel-pohjaista aliverkkolaskuria jonka avulla voidaan helposti selvittää minkä verran vapaita osoitteita on jäljellä. Laskuri antaa osoiteavaruudeksi 192.83.51.32-192.83.51.63 joista ensimmäinen on aliverkon verkko-osoite ja jälkimmäinen aliverkon broadcast osoite. Vapaat osoiteet löytyvät väliltä 192.83.51.33-192.83.51.39 ja 192.83.51.58-192.83.51.62.

LIITE 3. Aliverkotuslaskuri (excel-ohjelma)



	B	C	D	E	F	G	H	I	J	K
4			**ALIVERKOTUS OHJELMA C-luokan arvi** 14.2.2005							
5										
6										
7			Sijoita IP-osoitekentän paluihin aliverkotettava IP-osoite							
8			Sijoita aliverkon peitekentän paluihin aliverkon peite							
9										
10			Verkko-osoitekenttään tulee loogisen AND-operaation tulos.							
11			Ohjelma kääntää tuloksen suoraan desimaalimuotoon.							
12										
13										
14										
15			**IP-OSOITE**		192	83	51	32		
16			**ALIVERKON PEITE**		255	255	255	224		
17			VERKKO-OSOITE		192	83	51	32		
18										
19										
20			Aliverkon peitteestä voidaan määrittää käytettävissä olevien aliverkkojen määrä.							
21										
22			Aliverkon peite desimaalisena		255	255	255	224		
23			Aliverkon peite binäärisenä		11111111	11111111	11111111	11100000		
24										
25			**Luku binääriykkösten**	27						
26			Binäärinollia	5						
27			osoitteita/aliverkko	32						
28			C luokan aliverkkoja yhteensä	8						
29										
30			ALLA OLEVASTA TAULUKOSTA VOIT TARKASTAA MIHIN ALIVERKKOON							
31			IP-OSOITE KUULUU							
32										
33		1	aliverkon verkko-osoite		192	83	51	0		
34			aliverkon IP-avaruus		192	83	51	1	-	30
35			aliverkon broadcast osoite		192	83	51	31		
36										
37		2	aliverkon verkko-osoite		192	83	51	32		
38			aliverkon IP-avaruus		192	83	51	33	-	62
39			aliverkon broadcast osoite		192	83	51	63		
40										
41		3	aliverkon verkko-osoite		192	83	51	64		
42			aliverkon IP-avaruus		192	83	51	65	-	94
43			aliverkon broadcast osoite		192	83	51	95		
44										
45		4	aliverkon verkko-osoite		192	83	51	96		
46			aliverkon IP-avaruus		192	83	51	97	-	126
47			aliverkon broadcast osoite		192	83	51	127		
48										
49		5	aliverkon verkko-osoite		192	83	51	128		
50			aliverkon IP-avaruus		192	83	51	129	-	158
51			aliverkon broadcast osoite		192	83	51	159		

LIITE 4. Tasopiirustus: rikosilmoitin ja johdotuskaavio