HÄLYTYKSENSIIRTO GPRS-YHTEYDELLÄ

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2008
Marko Ahola

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

AHOLA, MARKO: Hälytyksensiirto GPRS-yhteydellä

Tietoliikennetekniikan opinnäytetyö, 88 sivua, 12 liitesivua

Kevät 2008

TIIVISTELMÄ

Tässä opinnäytetyössä tutkitaan GPRS-palvelun hyödyntämistä TeliaSoneran Sonera Alerta -palveluiden tiedonsiirtoyhteytenä. GPRS-palvelun pakettikytkentäisillä tiedonsiirtoyhteyksillä hyödynnetään GSM-verkon resursseja tehokkaammin kuin GSM-verkon piirikytkentäisillä tiedonsiirtoyhteyksillä. GPRS-yhteyden muodostaminen on nopeampaa ja saavutettava tiedonsiirtonopeus suurempi kuin GSM-yhteyden. GSM-yhteyden soittosarjatekniikat ja -laitteistot ovat ns. vanhenevaa tekniikka, joista pyritään luopumaan. Laitteistoja uusittaessa kustannustehokkaamman tekniikan käyttäminen on taloudellisesti kannattavaa.

Työssä tutustutaan hälytysjärjestelmiin sekä niiden ilmoituksensiirtojärjestelmänä käytettäviin Sonera Alerta -palveluihin. Sonera Alerta -palveluista käsitellään TeliaSoneran yrityksille tarjoamat palvelut sekä Sonera Alerta -palveluihin liittyvät tiedonsiirtopalvelut ja -laitteet. Työn teoriaosassa käsitellään GPRS-palvelun toimintaa ja esitellään GPRS-verkon rakenne ja tärkeimmät verkkoelementit. Modbus-protokollan toiminta kuvataan yleisellä tasolla ja esitellään Modbus-protokollan tiedonsiirtoon käytettävät Modbus-protokollan eri versiot. Teoriaosassa käydään myös lyhyesti läpi TCP/IP-viitemalli sekä TCP-, IP- ja PPP-protokollan toiminta. Työn tutkimusongelman muodostavat Modbus-protokollan käyttämä asiakas/palvelin-malli ja GPRS-yhteyden tiedonsiirrossa esiintyvät viiveajat.

Työssä suunniteltiin ratkaisumalli hälytyksensiirron toteuttamiseksi GPRS-yhteydellä. Suunniteltu ratkaisumalli täyttää pääosin pelastusviranomaisen sekä CEA 4039 -standardin hälytysjärjestelmän ilmoituksensiirtojärjestelmälle asettamat vaatimukset GPRS-yhteydellä välitettäväksi sovellustason protokollaksi valittiin Modbus-protokolla, jota käytetään Sonera Alerta -palveluissa Alerta-palveluverkon päätelaitteen ja palohälytysjärjestelmän välisessä tiedonsiirrossa. GPRS-palvelun ja Modbus-protokollan tutkimiseksi ja testaamiseksi rakennettiin testiympäristö. Lisäksi työssä tarkasteltiin suunnitellun ratkaisumallin linjavalvonnan synnyttämän tiedonsiirron määrää.

Työn tuloksena todettiin hälytyksensiirron toteuttamisen GPRS-yhteydellä olevan mahdollista, mutta luotettavan hälytyksensiirron GPRS-yhteydellä vaativan tiedonsiirron priorisoinnin sekä radiorajapinnan priorisoinnin käyttöönottamisen TeliaSoneran GPRS-verkossa. Lisäksi todettiin hälytyksensiirron toteuttamisen käyttämällä pelkästään GPRS-palvelua vaativan GPRS-verkolta tuen PDP-kontekstin aktivointiin päätelaitteelta GPRS-verkon pyynnöstä.

Avainsanat: Alerta, GPRS, hälytyksensiirto, hälytysjärjestelmä, Modbus

Lahti University of Applied Sciences
Faculty of Technology

AHOLA, MARKO: Implementing GPRS Technology in Alarm Transfer

Bachelor's Thesis in Telecommunications Technology, 88 pages, 12 appendices

Spring 2008

ABSTRACT

The objective of this thesis was to examine the implementation of GPRS technology as a data transfer technique in TeliaSonera's Sonera Alerta services. GPRS technology offers a packet-switched data service, which provides more effective resource usage of the GSM network than circuit-switched data service of the GSM network. Also, GPRS technology is designed for fast reservation to begin the transmission of packets, and attainable data transfer rates are higher. TeliaSonera's aim is to resile from declining dial-up techniques and equipment of the GSM network. Upon the renewal of these techniques it is financially profitable to use more cost-effective techniques.

The thesis familiarizes with alarm systems and Sonera Alerta services, which are used to provide an alarm transmission system for alarm systems. Those Sonera Alerta services, which are provided to business customers, are discussed. Also, related data transfer services and data transmission devices used in Sonera Alerta services are discussed. In the theory part of the thesis, GPRS technology and its functions are clarified, also a structure of the GPRS network and the main network elements are introduced. The functionality of Modbus protocol is clarified, and different versions of the Modbus protocol are introduced. In addition, a brief introduction of the TCP/IP Reference Model, TCP, IP and PPP protocols is included. Research problems of the thesis consist of the client/server model used by Modbus protocol and delay times of the GPRS data service.

Within the thesis a solution to implement GPRS technology in alarm transfer was designed. The solution mostly fullfils the demands set to alarm transfer systems by rescue authorities and the CEA 4039 standard. The Modbus protocol was chosen for the application layer protocol, because it is already used in Sonera Alerta services for data transfer between terminal equipment and fire alarm systems. An experimental alarm transfer system was built to test and study GPRS data service and functions of the Modbus protocol. Also, the amount of data traffic generated by monitoring the data transmission connection was studied.

As a conclusion, it can be said that it is possible to implement GPRS technology in alarm transfer, but to provide a reliable alarm transfer, priorisation must be used in data transfer, and the priorisation of radio interface must be deployed in TeliaSonera's GPRS network. Furthermore, it was clarified that Network-Requested PDP Context Activation procedure must be supported in a GPRS network, if alarm transfer is implemented using only GPRS data service.

Key words: alarm system, alarm transfer, Alerta, GPRS, Modbus

SISÄLLYS

LYHENNELUETTELO

AAA	Authentication, Authorization, Accouting eli tunnistus, valtuutus ja tilastointi
AAS	Alerta Application Server, Alerta-palveluverkon virtuaalisten Modbus TCP/IP -orjalaitteiden sovelluspalvelin
APN	Access Point Name, GPRS-yhdyskäytäväsolmuun määritettävä ulkoisen pakettidataverkon yksilöivä yhteyspisteen nimi
ADU	Application Data Unit, sovellustasolla tiedonsiirtoon käytettävä kehysrakenteinen sovellustietoyksikkö
ASCII	American Standard Code for Information Interchange, Amerikkalainen tietokoneiden merkistöstandardi tekstitiedon esittämiseen
AT	ATtention, modeemien asetusten määrittämiseen ja ohjaukseen tarkoitetun komentokielen etuliite
ADSL	Asymmetric Digital Subscriber Line, asymmetrinen digitaalinen tilaajalinja
BSC	Base Station Controller, radioresurssien hallintaa suorittava tukiasemaohjain
BSS	Base Station System, mobiililaitteet radiotien kautta GSM-verkon keskusjärjestelmään yhdistävä tukiasemajärjestelmä
BTS	Base Transmitter Station, tukiasemalaitteiston sisältävä fyysinen laitteistotila
CEA	Comité Européen des Assurances, kansallisten vakuutusyhtiöiden keskusjärjestöjen yhteenliittymä Euroopan talousalueella
CHAP	Challenge Handshake Authentication Protocol, haaste/vastausmenetelmää päätelaitteen todentamiseen käyttävä protokolla
CID	Connection IDentifier, tiedonsiirtotapahtumiin liitettävä TCP/IP-yhteyden yksilöivä yhteystunniste
CRC	Cyclical Redundancy Check, synkronisessa tiedonsiirrossa käytettävä syklinen summaustarkistus
DHCP	Dynamic Host Configuration Protocol, IP-verkon laitteiden verkkoasetusten määrittämiseen käytettävä protokolla
EIA	Electronic Industries Associates, Yhdysvaltain kansallinen ammattijärjestö, joka edustaa USA:n elektroniikkavalmistajia

EN	EuropeaN standard, eurooppalaisen standardisoimisjärjestön laatima Euroopan talousalueella käytettävä standardi
GGSN	Gateway GPRS Support Node, tiedonsiirron ulkoisiin pakettidataverkkoihin mahdollistava GPRS-yhdyskäytäväsolmu
GMSC	Gateway MSC, ulkoisesta verkosta tai keskuksesta matkapuhelinkeskukselle puheluita tai lyhytsanomia välittävä kauttakulkukeskus
GPRS	General Packet Radio Service, GSM-verkon pakettikytkentäinen tiedonsiirtopalvelu
GR	GPRS Register, HLR:n GPRS-tilaaja- ja reititystiedot sisältävä GPRS-rekisteri
GSM	Global Standard for Mobile Communication, maailmanlaajuisesti matkapuhelinviestinnässä käytettävä joukko standardeja
GTP	GPRS Tunneling Protocol, GPRS-runkoverkossa tiedonsiirron ja merkinannon tunnelointiin käytettävä GPRS-tunnelointiprotokolla
HDLC	High-Level Data Link Control, OSI-mallin siirtoyhteyskerroksen bittiorientoitunut synkroninen tietoliikenneprotokolla
HLR	Home Location Register, GSM-verkon tilaaja- ja laskutustietoja sekä numeroon liittyvät lisäpalvelut sisältävä kotirekisteri
ICMP	Internet Control Message Protocol, IP-pohjaisen tietoliikenneverkon erilaisten virhetilanteiden havaitsemiseen käytettävä protokolla
IETF	Internet Engineering Task Force, Internet-standardeja kehittävä avoin kansainvälinen standardointijärjestö
IMEI	International Mobile Equipment Identity, mobiililaitteen yksikäsitteisesti yksilöivä kansainvälinen mobiililaitetunnus
IMSI	International Mobile Subscriber Identity, GSM-verkon tilaajan yksikäsitteisesti yksilöivä kansainvälinen mobiilitilaajatunnus
IP	Internet Protocol, tietoliikenneprotokolla päätelaitteiden osoitteistamista ja pakettien reitittämisestä varten.
ISO	International Standards Organization, kansainvälisiä ja kaupallisia standardeja tuottava standardointiorganisaatio
ITU-T	International Telecommunications Union - Telecommunications standardisation sector, kansainvälinen telealan standardointijärjestö
IWMSC	InterWorking MSC, ulkoisten verkkojen datayhteyksien yhteensovitustoimintoja suorittava matkapuhelinkeskus

LCP	Link Control Protocol, linkkiyhteyden muodostamiseen, konfigurointiin ja testaukseen käytettävä protokolla
LLC	Logical Link Control, OSI-mallin siirtoyhteyskerroksen ylemmän alikerroksen vuonohjaus- ja kanavointiprotokolla
LRC	Longitudinal Redundancy Check, asynkronisessa tiedonsiirrossa käytettävä pitkittäinen pariteettitarkistus
MAC	Medium Access Control, radiokanavien pääsymerkinannon ohjaus sekä LLC-kehyksien sovitustoimenne
MAP	Manufacturing Automation Protocol, General Motorsin kehittämä teollisuusautomaation vuoroväylä lähiverkkoarkkitehtuuri
MBAP	ModBus Application Protocol, Modbus TCP/IP -protokollassa kapselointiin käytettävä otsikkokenttä
ME	Mobile Equipment, fyysinen mobiililaitteisto GSM-verkon palveluiden käyttämiseen
MM	Mobility Management, tilaajan sijainnin seurannasta, tietokannoista ja turvallisuusasioista huolehtiva liikkuvuuden hallintataso
MMS	Multimedia Messaging Service, multimediasisällön ei reaaliaikaiseen välittämiseen käytettävä multimediaviestipalvelu
MS	Mobile Station, fyysisestä laitteistosta GSM-verkon palveluiden käyttämiseen ja tilaajamoduulista koostuva mobiililaite
MSC	Mobile services Switching Center, puheluiden ja liikkuvuuden hallintaa suorittava matkapuhelinkeskus
MSISDN	Mobile Subscriber ISDN Number, mobiilitilaajan kansainvälinen ISDN-numero
MT	Mobile Termination, radiorajapinnan toimintoja tukeva ja informaatiovirran sovitusta suorittava mobiilipäätelaite
NAS	Network Access Server, etäyhteyksien verkkoon pääsyn hallintaa suorittava verkkoyhteyspalvelin
NCP	Network Control Protocol, verkkokerroksen protokollien konfigurointiin käytettävä protokolla
NSAPI	Network layer Service Access Point Identifier, PDP-kontekstin yksilöimiseen käytettävä verkkokerroksen liityntäpisteen tunniste
OSI	Open Systems Interconnection, ISO (International Standards Organization) kehittämä tietoliikennejärjestelmien viitemalli

PAP	Password Authentication Protocol, yksinkertainen päätelaitteen todentamiseen käyttävä protokolla
PDP	Packet Data Protocol, pakettikytkentäisten verkkojen tiedonsiirrossa käytettävä protokolla esim. IP-protokolla
PDU	Protocol Data Unit, yhteyskäytännön kontrolli- ja käyttäjätietoja sisältävä protokollatietoyksikkö
PPP	Point to Point Protocol, verkkolaitteiden väliseen pisteestä pisteeseen -yhteyden muodostamiseen käytettävä protokolla
QoS	Quality of Service, tietoliikenteen luokittelua ja priorisointia kuvaava termi, palvelunlaatu
RADIUS	Remote Authentication Dial In User Service, käyttäjän todentamiseen, valtuuttamiseen sekä tilastointiin käytettävä protokolla
RFC	Request For Comments, IETF-organisaation (Internet Engineering Task Force) julkaisema Internetiä koskeva standardi
RLC	Radio Link Control, datalohkojen siirtoa ja virheenkorjausta suorittava radiolinkin ohjaustoimenne
RTU	Remote Terminal Unit, fyysisten liitäntöjen rajapintana tietoliikenneverkkoon toimiva hajautetun järjestelmän alakeskus
SGSN	Serving GPRS Support Node, pakettidataa mobiililaitteiden ja GPRS-verkon välillä suorittava GPRS-operointisolmu
SIM	Subscriber Identity Module, tilaajan tunnistetietoja ja salausalgoritmit sisältävä älykortti
SME	Short Message Entity, lyhytsanoman lähettävä tai vastaanottava lyhytsanomaolio
SMS	Short Message Service, lyhyiden tekstimuotoisten sanomien välittämiseen käytettävä lyhytsanomapalvelu
SM-SC	Short Message - Service Centre, lyhytsanomien välittämiseen käytettävä palvelukeskus
SNAP	SafeNet Applicaton Protocol, TeliaSoneran Alerta-palveluverkossa käytettävä sovelluskerroksen protokolla
SSL	Secure Sockets Layer, yhteyskäytäntö Internet-sovellusten tietoliikenteen salaamiseksi
SVK	Suomen Vakuutusyhtiöiden Keskusliitto, Suomessa toimivien vakuutusyhtiöiden etu- ja yhteistoimintajärjestö

TCP	Transmission Control Protocol, tietoliikenneprotokolla yhteyden luomiseksi tietokoneiden välille
TDMA	Time Division Multiple Access, GSM-verkossa käytettävä aikajakoinen monipääsytekniikka.
TA	Terminal Adaptor, päätelaitteiston ja mobiililaitteiston yhteensovittamiseen käytettävä päätesovitin
TE	Terminal Equipment, mobiililaitteiston ohjaukseen ja hallintaan käytettävä päätelaitteisto
TIA	Telecommunications Industry Association, teleteollisuutta edustava Yhdysvaltalainen tietoliikenteen standardointielin
TID	Tunneling Identifier, GPRS-runkoverkon tunnelointiyhteyden yksilöivä tunnelointitunniste
UPS	Uninterruptible Power Source, järjestelmä tai laite, jonka tehtävä on taata virransyöttö lyhyissä katkoksissa ja tasata syöttöjännitettä.
VLR	Visitor Location Register, GSM-verkon tilaaja- ja sijaintitietoja sisältävä dynaaminen vierailijarekisteri

1 JOHDANTO

Tiedonsiirtoyhteyksien kehitys on siirtynyt piirikytkentäisistä yhteyksistä pakettikytkentäisiin yhteyksiin. Suomessa langattoman tiedonsiirron parhaan maantieteellisen peittoalueen tarjoaa GPRS-palvelu (General Packet Radio Service), jonka pakettikytkentäisillä tiedonsiirtoyhteyksillä hyödynnetään GSM-verkon (Global Standard for Mobile Communication) resursseja tehokkaammin kuin GSM-verkon piirikytkentäisillä tiedonsiirtoyhteyksillä. GPRS-palvelun tiedonsiirtoyhteyden muodostaminen on nopeampaa ja saavutettava tiedonsiirtonopeus suurempi kuin GSM-yhteyden. GPRS-palvelua käytettäessä ei radiorajapinnan fyysisen siirtotien aikaväliä varata kiinteästi yhdelle käyttäjälle vaan aikaväliä jaetaan samanaikaisesti useille käyttäjille. GPRS-yhteys käyttää GSM-verkon resursseja vain tarvittaessa, joten GPRS-yhteyttä voidaan ylläpitää ilman kiinteää GSM-verkon resurssien varaamista.

Tässä opinnäytetyössä tutkitaan GPRS-palvelun hyödyntämistä TeliaSonera Finland Oyj:n Sonera Alerta -palveluissa. TeliaSonera Finland Oyj toimii Suomessa Sonera-brandin alla ja on osa TeliaSonera-konsernia. TeliaSonera on Pohjoismaiden ja Baltian johtava televiestintäyritys, jolla on kansainvälisesti vahva asema myös Euraasian matkaviestinmarkkinoilla. TeliaSoneran yrityksille tarjoamia palveluja ovat mm. verkottuneet tietotekniikkapalvelut, puhe- ja dataratkaisut, järjestelmäintegraatio ja yhdentyvät palvelut sekä pitkälle vakioidut ratkaisut pienille ja keskisuurille yrityksille.

Sonera Alerta -tuoteperhe rakentuu erilaisista yrityksille tarjottavista hälytys- ja ohjauspalveluista, joilla voidaan parantaa yrityksen kiinteistö- ja henkilöturvallisuutta. Nykyisissä Sonera Alerta -palveluiden hälytyksensiirtoratkaisuissa käytetään piirikytkentäisiä GSM-yhteyksiä hälytystietojen välittämiseen hälytyskohteesta Alerta-palveluverkkoon. GSM-yhteyden soittosarjatekniikat ja -laitteistot ovat ns. vanhenevaa tekniikka, joiden käyttämisestä pyritään luopumaan. Laitteistojen vanhentuessa tulee väistämättä eteen laitteistojen uusimistarve, jolloin on taloudellisesti kannattavaa siirtyä käyttämään uusia kustannustehokkaampia tekniikoita.

Työn tavoitteena on suunnitella ratkaisumalli Sonera Alerta -palveluiden hälytyksensiirron toteuttamiselle GPRS-yhteydellä. Työssä suunniteltavan ratkaisumallin lähtökohtana käytetään paloilmoitinjärjestelmään liitetyn ilmoituksensiirtojärjestelmän tiedonsiirron toteutusta GPRS-yhteydellä. Paloilmoitinjärjestelmän ilmoituksensiirtojärjestelmälle asetetaan vaatimuksia viranomaistaholta. Ratkaisumallin täyttäessä paloilmoitustensiirrolle asetetut vaatimukset täyttyvät pääsääntöisesti myös muille ilmoituksensiirtojärjestelmille asetetut vaatimukset.

Ratkaisumallin suunnittelulle asetettavat lähtövaatimukset:

- palo- ja rikosilmoitustensiirtojärjestelmille asetettujen vaatimusten täyttyminen
- soveltuvuus Alerta-palvelutuotantojärjestelmään
- hälytyskohteen päätelaitteen määrittelyjen vakiointi
- pieni tiedonsiirron määrä
- keskitetty hallinta.

Hälytysjärjestelmien ilmoituksensiirtojärjestelmien tiedonsiirrossa käytetään useita eri protokollia, joista valittiin tarkasteltavaksi Modbus-protokollan välittäminen GPRS-yhteydellä. Modbus-protokolla on yleisesti teollisuuden kenttäväylien tiedonsiirrossa käytettävä protokolla, joka on tuettuna useiden eri laitevalmistajien teollisuusautomaatiolaitteistoissa. Lisäksi Sonera Hälytys- ja ohjauspalveluissa käytetään Modbus-protokollan Modbus RTU -tiedonsiirtotapaa (Remote Terminal Unit) paloilmoitinjärjestelmän ja Alerta-palveluverkkoon liitetyn hälytyskohteen päätelaitteen välisessä tiedonsiirrossa.

Työn tutkimusongelman muodostavat Modbus-protokollan käyttämä asiakas/palvelin-malli sekä GPRS-yhteyden tiedonsiirrossa esiintyvät vaihtelevat viiveajat. Työ aloitetaan tutustuttamalla lukija hälytyksensiirtojärjestelmiin ja esittelemällä Sonera Alerta -tuoteperheen palvelut sekä niihin liittyvät Soneran tiedonsiirtopalvelut. Työn teoriaosassa perehdytään Modbus-protokollan ja GPRS-palvelun toimintaan sekä käydään lävitse Modbus-protokollan eri versiot ja GPRS-verkon tärkeimmät verkkoelementit. Teoriaosassa esitellään lyhyesti myös TCP/IP-viitemalli (Transmission Control Protocol / Internet Protocol) sekä TCP-, IP- ja PPP-protokollat (Point to Point Protocol).

Työn käytännönosuudessa rakennettiin testiympäristö Modbus-protokollan ja GPRS-yhteyden toiminnan sekä GPRS-palvelun viiveaikojen ja tiedonsiirron määrän tutkimiseksi. Testiympäristössä saadut tulokset esitetään työn liitteissä. Työssä käsiteltävät asiat pyritään esittämään yleisellä tasolla ja lukijalta edellytetään GSM-verkon toiminnan perustuntemusta.

Työssä tehtävät käsittelyn rajaukset:

- radiorajapinnan priorisoinnin toteutus, radiorajapinnan priorisointia ei käytetä Soneran GPRS-verkossa
- GPRS-verkon liikkuvuuden hallinnan ja solunvaihdon tarkastelu, hälytyskohteet ovat kiinteästi paikkaan sidottuja.
- GPRS-palvelun tietoturva, GPRS-palvelun tietoturva on vastaavanlainen kuin GSM-verkon tietoturva
- Modbus-protokollan funktiokoodien tarkempi käsittely, Modbus-protokollan funktiokoodeja on useita kymmeniä eikä niiden läpikäymistä pidetty työn toteutuksen kannalta tarpeellisena.

2 HÄLYTYSJÄRJESTELMÄT

2.1 Paloilmoitinjärjestelmät

Paloilmoitinjärjestelmiä käytetään kohteissa, joissa sammutusvoimien aikainen ja luotettava hälyttäminen parantaa henkilöturvallisuutta ja vähentää omaisuusvahinkoja. Paloilmoitinjärjestelmän käyttäminen voi perustua vapaaehtoisuuteen, rakennusten paloturvallisuusmääräys- ja ohjeosiin tai pelastusviranomaisen pelastuslakiin pohjautuvaan määräykseen. Paloilmoitinjärjestelmä on pakollinen yli 50 majoituspaikan majoitustiloissa, yli 25 vuodepaikan hoitolaitoksissa ja yli 25 hoidettavan henkilön päivähoitolaitoksissa. Majoitustiloissa ja hoitolaitoksissa paloilmoitinjärjestelmän käyttämisellä ei voida kasvattaa palo-osastokokoa. Tuotanto- ja varastorakennuksissa paloilmoitinjärjestelmän käyttämisellä saadaan lievennyksiä rakennuksen kerrosalaa ja palo-osastokokoa koskeviin määräyksiin. (Sähkötieto ry 2004, 36 - 37.)

Paloilmoitinjärjestelmä koostuu varakäyntiakusta, prosessoripohjaisesta keskusyksiköstä ja siihen liittyvistä erilaisista ilmaisimista. Ilmaisimet liitetään paloilmoitinkeskukseen hälytyssilmukoilla, jotka voivat olla osoitteettomia tai osoitteellisia. Keskusyksikön tulee täyttää standardin EN54-2 (EuropeaN standard) asettamat vaatimukset. Keskusyksikön toiminnalliset osat ovat valvonta-, käyttö-, näyttö-, liitäntä- ja ilmoituksensiirtoyksikkö. Keskusyksikkö kerää ja käsittelee järjestelmän ja ilmaisimien tilatietoja, joiden perusteella keskusyksikkö suorittaa valvontaa, toteuttaa sille annetut käskyt ja välittää tietoa käyttö-, näyttö- ja ilmoitustensiirtoyksikölle sekä ulkoisille ohjauksille. Suurialaisissa kohteissa voidaan käyttää ns. hajautettua järjestelmää, jossa on useita keskusyksiköitä. Yksi keskusyksiköistä toimii pääkeskuksena ja muut keskukset toimivat siihen liitettyinä alakeskuksina. Pääkeskuksesta hallinnoidaan koko järjestelmää ja nähdään kaikki järjestelmän tapahtumat. Alakeskuksesta hallinnoidaan ja nähdään vain kyseisen alakeskuksen tapahtumia. Ilmoituksensiirto keskuksilta toteutetaan joko keskuskohtaisilla erillisillä järjestelmävälittimillä tai yhdellä yhteisellä järjestelmäkohtaisella välittimellä. Keskuskohtaisia välittimiä käytettäessä alakeskukset voivat toimia täysin itsenäisinä yksiköinä. (Sähkötieto ry 2004, 54 - 57.)

Paloilmoitinjärjestelmät ryhmitellään käytetyn tekniikan perusteella kolmeen ryhmään: konventionaalinen, osoitteellinen ja osoitteellinen älykäs paloilmoitinjärjestelmä. Konventionaalisessa eli perinteisessä paloilmoitinjärjestelmässä yksi fyysinen hälytyssilmukka muodostaa yhden paloryhmän. Yhteen hälytyssilmukkaan liitetään yksi tai useampia ilmaisimia, joista hälytystieto välitetään kosketintietona. Ilmaisimien toiminta on mekaaninen tai elektroninen ja ilmaisimelta saatava kosketintieto on avautuva tai sulkeutuva. Nykyisin käytettävät ilmaisimet ovat sulkeutuvatoimisia ja ilmaisimissa käytetään sisäistä vastusta, jolloin hälytyssilmukan oikosulku ja hälytystila erotetaan toisistaan. Vanhempien järjestelmien ilmaisimissa ei ole sisäistä vastusta vaan hälytyssilmukka on päätetty pelkästään päätevastukseen. Ilmaisimen toiminta aiheuttaa oikosulun hälytyssilmukassa, joka tulkitaan hälytystiedoksi. Erillistä oikosulkua ei pystytä havaitsemaan vaan se tulkitaan virheellisesti hälytystiedoksi. Konventionaalisessa paloilmoitinjärjestelmässä hälytystieto ilmaisimilta saadaan paloilmoitinkeskukseen hälytyssilmukan tarkkuudella ja vikatiedoista saadaan välitettyä silmukkakatkos, silmukkavika ja silmukan oikosulku. (Sähkötieto ry 2004, 47 - 52.)

Osoitteellisissa paloilmoitinjärjestelmissä silmukka rakenne voi vaihdella eri järjestelmissä tai niiden sisällä. Yleensä käytetään ns. suursilmukkaa, joka lähtee paloilmoitinkeskuksesta ja päättyy takaisin paloilmoitinkeskukseen. Suursilmukka varustetaan oikosulkusuojauksella, ja suursilmukan kattaessa useita paloalueita erotetaan paloalueet toisistaan oikosulkuerottimilla. Suursilmukkaan liitetään useita ilmaisimia, jotka on varustettu osoitepiirillä. Paloilmoitinkeskus tekee tilakyselyitä jokaiseen suursilmukkaan liitettyyn ilmaisimeen ja saa ilmaisimelta vastauksena tilatiedon, joka on palo-, vika- tai normaalitila. Ilmaisimilta hälytystieto saadaan kosketintietona. Osoitteellisessa paloilmoitinjärjestelmässä hälytys- ja vikatieto saadaan paloilmoitinkeskukseen ilmaisimen tarkkuudella. Ilmaisimet ryhmitellään ohjelmallisesti paloryhmiin, ja niiden osoitteet ja hälytysjärjestys tallennetaan tapahtumarekisteriin, jolloin palon kehittymisestä saadaan tarkempaa tietoa kuin konventionaalisessa järjestelmässä. Osoitteelliseen paloilmoitinjärjestelmään voidaan liittää osoitteettomia laitteita ja konventionaalisia hälytyssilmukoita käyttämällä sovitusyksikköä. Sovitusyksiköllä järjestelmään liitetty osoitteeton laite tai kaikki konventionaalisen hälytyssilmukan ilmaisimet näkyvät paloilmoitinkeskuksessa sovitusyksikön osoitteella. (Sähkötieto ry 2004, 47 - 48.)

Osoitteellisen paloilmoitinjärjestelmän ja osoitteellisen älykkään paloilmoitinjärjestelmän erona on ilmaisimilta saatava tieto. Osoitteellisessa paloilmoitinjärjestelmässä saadaan ilmaisimilta vain raja-arvotieto, onko hälytys päällä tai pois päältä. Osoitteellisessa älykkäässä paloilmoitinjärjestelmässä ilmaisimilta saadaan mitta-arvotieto, jolla saadaan tarkempi vaste palotilanteessa ja vältetään virheellisiä palohälytyksiä. Keskuslaitteistot ja ilmaisimet ovat mikroprosessoripohjaisia ja sisältävät valmistajakohtaisia ohjelmistoja, joka mahdollistaa monipuoliset asettelu- ja säätömahdollisuudet. Silmukkaliikennöinnissä hälytystiedon siirtämiseen käytetään liikennöintiprotokollia, jotka ovat analogisia tai digitaalisia. Fyysiset silmukkarakenteet ovat vastaavanlaiset kuin osoitteellisessa paloilmoitinjärjestelmässä ja vastaavasti ilmaisimet ovat varustettu osoitepiirillä. Paloilmoitinkeskukseen välitettävään signaaliin voidaan sisällyttää ilmaisimen tekemää palopäättelyä ja mittavirhepiikkien suodatusta. Osoitteellisessa älykkäässä paloilmoitinjärjestelmässä ilmaisimilta saadaan paloilmoitinkeskukseen osoitekohtainen hälytystieto, ennakkovaroitus sekä vika- ja huoltohälytys. (Sähkötieto ry 2004, 48.)

Paloilmoitinjärjestelmän ilmoituksensiirtojärjestelmällä välitetään paloilmoittimien palo- ja vikailmoitukset hätäkeskukseen tai muuhun viranomaisen ja kiinteistön haltijan hyväksymään jatkuvasti valvottuun paikkaan. Ilmoituksensiirtojärjestelmän ja sen tiedonsiirtoyhteyden on oltava jatkuvasti käytettävissä. Tiedonsiirtoyhteyden linjavikatieto on välitettävä vastaanottajalle 100 sekunnin kuluessa, mikäli tiedonsiirtoyhteyttä ei ole kahdennettu. Linjavikatiedon vastaanottaja ilmoittaa linjaviasta teleoperaattorille tai muulle palvelun tuottajalle korjaavien toimenpiteiden käynnistämiseksi. Paloilmoittimien hälytystiedot ilmoituksensiirtojärjestelmän on välitettävä eteenpäin 10 sekunnin kuluessa ja hälytystietojen on oltava vastaanottajalla 100 sekunnin kuluessa. Pelastusviranomaisen määräyksestä hälytystietoon on voitava liittää tieto tarkemmasta sijaintipaikasta. Yleensä ilmoituksensiirtojärjestelmän tiedonsiirtoyhteyden siirtolaite sijoitetaan paloilmoitinkeskuksen sisälle ja kytketään sen sähkönsyöttöön. Tarvittaessa voidaan käyttää ulkopuolista siirtolaitetta ja sähkönsyöttöä, jolloin siirtolaitteen yhteyden paloilmoitinkeskukseen ja sähkönsyötön on oltava paloilmoitinkeskuksen vikavalvonnan piirissä. Välitettäessä palo- ja vikailmoituksia muuhun jatkuvasti valvottuun paikkaan hälytystietojen on oltava edelleen siirrettävissä hätäkeskukseen luotettavia tiedonsiirtoyhteyksiä käyttäen. (Sähkötieto ry 2004, 64 - 65.)

Paloilmoitinjärjestelmän sähkönsyöttö toteutetaan paloilmoitinkeskuksen sisään asennettavalla teholähteellä tai ulkoisella teholähteellä. Ulkoinen teholähde liitetään paloilmoitinkeskuksen vikavalvontaan ja tarvittaessa käytetään useampia teholähteitä. Paloilmoitinkeskuksissa käytettävissä teholähteissä on oltava ylivirtasuoja ja kaksi erillistä sähkönsyöttöä, jotka ovat yleensä sähköverkko ja varakäyntiakku. Varakäyntiakun varakäyntiajan minimivaatimus on 72 tuntia valvontatilassa sisältäen 30 minuutin hälytysjakson. Akkukapasiteetin laskennassa huomioidaan paloilmoitinkeskuksen ja kaikkien siihen liittyvien laitteiden sekä ilmaisimien virrankulutus. (Sähkötieto ry 2004, 62 - 64.)

2.2 Rikosilmoitinjärjestelmät

Rikosilmoitinjärjestelmiä käytetään kiinteistön tai muun omaisuuden suojaamiseen ilkivallalta, vahingoittamiselta ja anastamiselta. Rikosilmoitinjärjestelmät eivät tarjoa varsinaista fyysistä suojausta vaan niiden suojausvaikutus perustuu ennaltaehkäisyyn ja kiinnijäämisriskin nostamiseen. Rikosilmoitinjärjestelmillä omaisuuden suojaamiseksi toteutettava valvonta jaetaan neljään tasoon: kehä-, kuori-, tila- ja kohdevalvonta. Kehävalvonnalla valvotaan kiinteistön ulkoisia alueita ja kuorivalvonnalla sisäänpääsyreittejä tunkeutumisyritysten varalta. Tilavalvonnalla valvotaan kiinteistön sisätiloja ja kohdevalvonnalla sisätiloissa sijaitsevia yksittäisiä kohteita. Valvontatapojen lisäksi käytetään ryöstöilmoitusta, joka annetaan painikkeella tai vastaavalla laitteella. (Sähkötieto ry 2002, 73 - 75.)

Rikosilmoitinjärjestelmä koostuu varakäyntiakusta, prosessoripohjaisesta keskusyksiköstä ja siihen liittyvistä erilaisista ilmaisimista, lisäksi keskusyksikköön voidaan liittää hälytin-, käyttö-, ohitus- ja ohjauslaitteita. Ilmaisimet liitetään rikosilmoitinkeskukseen hälytyssilmukoilla, jotka voivat olla osoitteettomia tai osoitteellisia. Yhteen hälytyssilmukkaan voidaan liittää useita ilmaisimia. Osoitteettomista hälytyssilmukoista saadaan hälytystieto silmukan ja osoitteellisista ilmaisimen tarkkuudella. Rikosilmoitinjärjestelmään voidaan liittää lisätoimintoja ja laitteita, kuten paloilmoitin ja rikosilmoitinjärjestelmä voidaan integroida kulunvalvontajärjestelmään. Tärkeä osa rikosilmoitinjärjestelmää ovat ilmoituksensiirtolaitteet. (Sähkötieto ry 2002, 77 - 83.)

SVK (Suomen Vakuutusyhtiöiden Keskusliitto) luokittelee rikosilmoitinkeskukset A, B, C ja langaton -tasoluokkiin. Tasoluokissa määritellään mm. keskuksen ilmoitukset, silmukkatyypit ja -määrät. Vakuutusyhtiöt ovat myös ohjeistaneet millaisia rikosilmoitinkeskuksia erityyppisissä kohteissa tulee käyttää ja asettaneet minimivaatimukset rikosilmoitinkeskusten varakäyntiakkujen mitoitukselle. Rikosilmoitinkeskuksen varakäyntiakun varakäyntiajan minimivaatimus on 24 tuntia sisältäen 5 minuutin hälytysjakson. Akkukapasiteetin laskennassa huomioidaan rikosilmoitinkeskuksen ja kaikkien siihen liittyvien ilmaisimien virrankulutus. Rikosilmoitinkeskus sijoitetaan suojattuun tilaan, johon on rajoitettu pääsy. Käytettäessä paikallista valvomoa rikosilmoitinkeskus sijoitetaan valvomon kanssa samaan tilaan tai valvomon laitehuoneeseen. (Sähkötieto ry 2002, 77.)

TAULUKKO 1. Rikosilmoitinkeskusten luokitukset (Sähkötieto ry 2002, 78)

Kohteen riskiluokka	Luokka 4	Luokka 3	Luokka 2	Luokka 1
Keskus	A-luokka	B-luokka	C-luokka	C-luokka/ langaton
Valvontatapa	Kuori ja tila	Ovet ja tila	Kuori tai tila	Kuori tai tila
Ilmoituksen siirto	Valvottulinja ja paikallishälytys	Robottipuhelin tai radiotaajuus ja paikallishälytys	Robottipuhelin tai radiotaajuus ja paikallishälytys	Robottipuhelin tai radiotaajuus ja paikallishälytys
Ilmoituksen vastaanotto	Poliisi tai SVK:n hyväksymä hälytyskeskus	SVK:n hyväksymä hälytyskeskus tai vartiointiliike	Vartiointiliike tai muu 24h/vrk päivystyspaikka	Kotinumerot
Kohteeseen hälytettävät	Poliisi ja vartiointiliike	Vartiointiliike	Vartiointiliike tai yksityishenkilöt	Yksityishenkilöt
Asennus	SVK:n hyväksymä liike	SVK:n hyväksymä liike	Vakuutusyhtiön hyväksymä liike	Vakuutusyhtiön hyväksymä liike
Huolto	Vähintään kerran vuodessa	Vähintään joka toinen vuosi	Tarvittaessa	Tarvittaessa
Siirrettävät tiedot	Murto, päälle/pois ryöstö, sabotaasi vika	Murto, päälle/pois sabotaasi	Murto, sabotaasi	Murto, sabotaasi
Käyttö	Viive ja alfanumero koodi, min. 6/4 merkkiä	Viive tai alfanumero koodi, min. 6/4 merkkiä	Avain tai koodi	Avain tai koodi
Paloilmaisimet	Suositellaan paloilmoitin-järjestelmää	Oma silmukka Oma hälytyslähtö	Oma silmukka Oma hälytyslähtö	
Ilmaisimet radioteitse	Ei sallita	Ei sallita kuin kohdevalvontaan		

2.3 Videovalvontajärjestelmät

Videovalvontajärjestelmiä käytetään jonkin alueen tai tilan valvontaan sekä sisään- ja uloskäyntien tarkkailuun tai prosessin ohjaukseen ja valvontaan. Videovalvontajärjestelmät jaetaan käyttötarkoituksen mukaan erilaisiin järjestelmätyyppeihin: aluevalvonta, tilavalvonta, prosessivalvonta ja erilaiset erityiskäyttösovellukset. Aluevalvonnalla tarkoitetaan laajan alueen valvontaa kokonaisuutena ja tilavalvonnalla jonkin tietyn kohteen yksityiskohtaista valvontaa. Useissa videovalvontajärjestelmissä alue- ja tilavalvonta on yhdistetty, jolloin laajemman alueen tietyt kohteet määritellään kriittisiksi ja niitä valvotaan tarkemmin.
(Sähkötieto ry 2003, 31 - 33.)

Videovalvontajärjestelmällä voidaan toteuttaa laajojen alueiden ja useiden eri kohteiden valvonta ja valvontatietojen tallennus yhteen keskitettyyn valvontapisteeseen. Alue- ja tilavalvontajärjestelmät voidaan liittää hälytys- ja kulunvalvontajärjestelmiin, jolloin valvontaa ja valvontatiedon tallennusta voidaan automatisoida. Teollisuudessa videovalvontajärjestelmiä hyödynnetään osana teollisuusprosessin valvontaa ja ohjausta. Videovalvontajärjestelmällä tarkkaillaan samanaikaisesti tuotantoprosessin eri vaiheita ja kohteita, joiden tarkkaileminen on muutoin mahdotonta. Videovalvontajärjestelmä voidaan liittää osaksi prosessinohjaus- tai automaatiojärjestelmää. Videovalvontajärjestelmien erityiskäyttösovelluksia ovat mm. storoboskooppi-, infapuna- ja mikrokamerat. (Sähkötieto ry 2003, 31 - 34.)

Digitaali- ja tiedonsiirtotekniikan kehittyminen sekä lähiverkkojen ja Internetin käyttäminen ovat monipuolistaneet videovalvontajärjestelmien käyttömahdollisuuksia. IP-kamerat, TCP/IP-pohjaiset tiedonsiirtoyhteydet, palvelimet ja selainpohjaiset graafiset käyttöliittymät ovat osa nykyaikaista videovalvontajärjestelmää. Videovalvontajärjestelmien IP-kameroiden tuottama digitaalinen kuvamateriaali siirretään TCP/IP-pohjaisella tiedonsiirtoyhteydellä valvomoon ja tallennetaan palvelimelle tietokantaan, josta kuvamateriaalia voidaan hakea myöhempää käyttöä varten. Digitaaliset videovalvontajärjestelmät ovat integroitavissa paloilmoitin-, rikosilmoitin- ja kulunvalvontajärjestelmiin. (Sähkötieto ry 2003, 73.)

2.4 Kulunvalvontajärjestelmät

Kulunvalvontajärjestelmiä käytetään alue- ja tilavalvontaan kiinteistön turvallisuuden parantamiseksi, omaisuuden suojaamiseksi ja luvattoman kulun rajoittamiseksi. Kulunvalvontajärjestelmissä kulkutiedot kerätään keskitetysti keskusyksikön muistiin, josta kulkutietoja voidaan tarkastella ja tuottaa erilaisia raportteja. Tarkastelu- tai raportointikriteereinä käytetään mm. tietyn kohteen tai henkilön kulkutapahtumia, kellonaikaa tai epäonnistuneita kulkuyrityksiä. Laittomasta kulusta saadaan hälytystieto kulunvalvontajärjestelmään, josta se voidaan tarvittaessa siirtää kontaktitietona rikosilmoitinjärjestelmään. Hälytystiedon laittomasta kulusta aiheuttaa mm. oven avaaminen avaimella tai hätäpoistumistien vääntönupilla. Kulunvalvontajärjestelmällä voidaan korvata mekaaniset avaimet sähköisillä tunnisteilla, jolloin lukkojen sarjoitus yksinkertaistuu, uudelleen sarjoitustarve ja siihen liittyvät kustannukset pienenevät. (Sähkötieto ry 2002, 33.)

Kulunvalvontajärjestelmä koostuu keskusyksiköstä, keskittimistä, kulunvalvontapäätteistä ja lukituslaitteista. Kulunvalvontajärjestelmän keskusyksikkönä toimii tietokone tai palvelin, jolla hallinnoidaan koko järjestelmän toimintaa. Yleensä kulunvalvontajärjestelmän keskusyksikkö sisältää varmistusaseman, käyttöliittymän, kirjoittimen ja liitännän lähiverkkoon. Tietyn alueen kulunvalvontapäätteet ja lukituslaitteet yhdistetään keskusyksikköön keskittimillä, jotka sisältävät niihin liitettyjen kulunvalvontapäätteiden ja lukituslaitteiden kulkuoikeus- ja ohjaustiedot sekä välittävät kulkutapahtumatiedot keskusyksikköön. Keskittimet yhdistetään keskusyksikköön tähtimäisesti tai väylällä. Keskittimet toimivat itsenäisinä yksiköinä vaikka yhteys keskusyksikköön katkeaisi. (Sähkötieto ry 2002, 35 - 36.)

Kulunvalvontajärjestelmän keskusyksikön sähkönsyöttö varmistetaan hallitun alasajon tarvitsemaksi ajaksi UPS-laitteella (Uninterruptible Power Source). Keskittimet varustetaan akkuvarmennetulla virtalähteellä, jolla varmistetaan keskittimien, kulunvalvontapäätteiden ja lukituslaitteiden sähkönsyöttö. Akkukapasiteetti mitoitetaan kahden tunnin normaalikäytölle. Kulunvalvontajärjestelmän keskusyksikkö ja keskittimet sijoitetaan tilaan, johon on rajoitettu pääsy. Keskusyksikkö sijoitetaan tekniseen laitetilaan tai pääkäyttäjän huoneeseen. Keskittimet sijoitetaan tekniseen laitetilaan tai sähkötiloihin. (Sähkötieto ry 2002, 36 - 37.)

2.5 Valvomojärjestelmät

Valvomojärjestelmä on yksi tärkeimmistä hälytyksensiirtoon liittyvistä osatekijöistä. Valvomojärjestelmän antaman tiedon perusteella reagoidaan hälytystapahtumiin ja päätetään tarvittavat jatkotoimenpiteet, joko automaattisesti tai valvomohenkilöstön toimesta. Valvomojärjestelmää käytetään paikallisesti tai etäyhteydellä. Valvomot ovat kehittyneet internetpalvelimiksi, jolloin niitä voidaan etähallita mm. normaalilla internetselaimella. Etäkäyttö ja laaja käyttäjäkunta edellyttävät hyvää käyttöoikeuksien hallintaa ja tietoturvaa. (Sähkötieto ry 2001, 113 - 115.)

Nykyaikaiset valvomojärjestelmät ovat rajapinnoiltaan avoimia, PC-pohjaisia ja sisältävät graafisen käyttöliittymän. Valvomojärjestelmän rajapintojen ollessa avoimia voidaan samaan valvomoon liittää eri laitevalmistajien ja eri protokollia käyttäviä laitteita tai vaihtaa valvomo-ohjelmisto. Vanhemmissa valvomojärjestelmissä rajapinnat olivat suljettuja, jolloin valvomojärjestelmä ei toiminut kuin tietyn laitevalmistajan laitteistolla ja ohjelmistolla. (Sähkötieto ry 2001, 113 - 114.)

Valvomojärjestelmään voi olla liitettynä paloilmoitin-, rikosilmoitin-, kulunvalvonta- ja videovalvontajärjestelmät, joita kaikkia hallitaan ja tarkkaillaan yhden monitasoisen graafisen käyttöliittymän avulla. Graafisen käyttöliittymän tulee olla looginen ja helppokäyttöinen. Hälytystyyppien erottaminen väreillä ja hälyttävän kohteen havainnollistaminen esim. rakennuksen pohjakuvassa helpottaa hälytystiedon tulkintaa ja nopeuttaa tarvittavien toimenpiteiden aloittamista.
(Sähkötieto ry 2002, 108.)

2.6 Ilmoituksensiirtojärjestelmille asetettavat vaatimukset

Pelastusviranomaisen paloilmoitinjärjestelmien ilmoituksensiirtojärjestelmille asettamien vaatimusten lisäksi SVK asettaa vaatimuksia palo- ja rikosilmoitinjärjestelmien ilmoituksensiirrolle. SVK:n määrittelemät vaatimukset perustuvat CEA 4039 -standardiin (Comité Européen des Assurances), jonka vaatimukset täyttäville ilmoituksensiirtojärjestelmille sekä niissä käytettäville siirtolaitteille SVK myöntää CEA 4039 -standardin vaatimustenmukaisuustodistuksen.

SKV on määritellyt CEA 4039 -standardin sääntöihin lisäyksiä ja tarkennuksia, joilla otetaan huomioon maamme paikalliset erityisolosuhteet. Televerkkojen ja käytettävyysasteen mittaustapa vaihtelee Euroopassa, joten EN50136-1-1-standardissa määriteltyjä arvoja ei voida käyttää. Ilmoitusten välittämisen jälkeisiin tapahtumiin, kuten hälytystiedon käsittely, hälytystietoon vastaaminen tai hälytystiedon oikeellisuuden tarkistaminen, ei CEA 4039 -standardissa oteta kantaa. (CEA 2002, 2 - 4.)

Ilmoituksensiirtojärjestelmän käytettävyydelle asetetaan sama käytettävyysvaatimus kuin itse palo- tai rikosilmoitinjärjestelmälle. Palo- ja rikosilmoitinjärjestelmille asetettavat vaatimukset määritellään CEA 4038 -standardissa. Paloilmoitinjärjestelmän käytettävyys on oltava vähintään 98,5 % vuodessa ja rikosilmoitinjärjestelmän 95 % vuodessa. Ilmoituksensiirtojärjestelmän vikaantumisesta on välitettävä tieto ilmoitinjärjestelmälle ja/tai hälytysten vastaanottokeskukseen. Ilmoituksensiirtojärjestelmän tiedonsiirrossa informaatio ei saa muuttua tai hävitä. Ilmoituksensiirtojärjestelmän tiedonsiirtotapa ei saa olla tunnistettavissa eikä luvattomilla henkilöillä saa olla pääsyä tiedonsiirtotapaan. Tarvittaessa tiedonsiirtopa on salattava, jolloin tietoturva säilyy tiedonsiirtotavan joutuessa luvattomien henkilöiden käsiin. (CEA 2002, 4 - 5.)

TAULUKKO 2. CEA 4039 -standardin vaatimukset (CEA 2002, 4 - 5)

Ilmoituksensiirtojärjestelmä	**Palo**	**Rikos**		
		Luokka 3	Luokka 2	Luokka 1
Maksimi siirtoaika [s]				
Linjavikatieto	100[1)]	20[1)]	180[2)]	180
Hälytystiedon siirto	10	10	10	180
Vika-, tila- ja muun tiedon siirto	180	180	180	180
1) Ellei mahdollista, voidaan lisäksi käyttää toista hälytyksensiirtojärjestelmää, joka on erillinen itsenäisesti toimiva ilmoituksensiirtolaite. 2) Ellei mahdollista, voidaan lisäksi käyttää toista hälytyksensiirtojärjestelmää				
Tiedonsiirto				
Lähettäjän todentaminen		X	X	
Tietojen salaus		X		
Linjavikatiedon välittäminen				
Ilmoitinjärjestelmä	X	X	X	X
Hälytysten vastaanottokeskus	X	X	X	

Samanaikaisesti hälytysten vastaanottokeskukseen saapuvien hälytysten esittäminen on priorisoitava hälytyskeskuksessa sanomatyypin mukaan. Hälytysten priorisoinnille ilmoituksensiirtojärjestelmän tiedonsiirrossa ei aseteta vaatimuksia. Hälytyssanomat on esitettävä hälytysten vastaanottokeskuksessa selkeästi ja yksiselitteisesti. Kaikki hälytyssanomat on tallennettava ja säilytettävä vähintään vuoden ajan. Tallennetusta tiedosta on hälytyssanoman lisäksi käytävä ilmi hälytyskohteen tiedot sekä hälytyssanoman vastaanottamisen tarkka päiväys ja kellonaika. (CEA 2002, 4 - 5.)

3 SONERA ALERTA -PALVELUT

3.1 Sonera Alerta -palveluiden yleiskuvaus

Työntekijöiden turvallinen työympäristö, turvallisuustekniikka ja tietoturva ovat osa yrityksen liiketoimintaa. Sonera Alerta -palveluilla yrityksen toimipisteiden palo-, rikos-, video-, kulunvalvonta-, henkilöturva- ja muut tekniset valvontajärjestelmät yhdistetään etähallittavaksi kokonaisuudeksi, jolloin yrityksen oman turvahenkilöstön ja ulkoisten palveluntuottajien yhteistoiminta helpottuu. Eri järjestelmien keräämät tiedot ovat käytettävissä ja tallennettavissa keskitetysti eikä tietojen saatavuus ole paikkaan sidottu, jolloin paikallisen järjestelmähallinnan tarve pienenee ja ulkoiset palveluntuottajat voivat hoitaa kohteita laajemmalta alueelta. Sonera Alerta -palvelukokonaisuus sisältää kolme pääpalvelua, jotka ovat hälytys- ja ohjauspalvelut, valvomopalvelu ja kulutusmittauspalvelu.
(TeliaSonera Finland Oyj 2003, 1.)

Sonera Alerta -palveluiden keskeinen ominaisuus on tiedon verkottaminen tiedonsiirtoyhteyksiä ja tietotekniikkaa hyväksi käyttäen. Tiedonsiirtoyhteyksissä hyödynnetään yrityksen omaa tietoliikenneverkkoa, Soneran tarjoamia tietoliikenneyhteyksiä sekä Sonera Alerta -runkoverkkoa. Sonera Alerta -palvelut eivät ole järjestelmätoimittaja tai palveluntuottaja sidonnaisia, joten yritys voi tarvittaessa vaihtaa järjestelmätoimittajan tai palveluntuottajan. Sonera Alerta -palvelut ovat yhteensopivia yleisimpien Suomessa käytettävien turvajärjestelmien kanssa.
(TeliaSonera Finland Oyj 2003, 2.)

Sonera Alerta -palvelut tarjoavat keinon yritysturvallisuuden kustannusten vakioimiseen, hallitsemiseen ja lisäkustannussäästöihin. Yrityksen oman tietoliikenneverkon hyödyntäminen lisää kustannustehokkuutta ja järjestelmien etähallittavuus vähentää turhia käyntejä kohteissa, jolloin saadaan säästöjä henkilöstön työ- ja matkakustannuksissa. Sonera Alerta -palvelun toimintamallit pystytään vakioimaan palveluntuottajasta riippumatta, jolloin lisäkustannussäästöjä voidaan saada kilpailuttamalla eri palveluntuottajia ja keskittämällä palveluita yhdelle palveluntuottajalle. (TeliaSonera Finland Oyj 2003, 2 - 3.)

3.2 Sonera Hälytys- ja ohjauspalvelut

Sonera Hälytys- ja ohjauspalvelut on palveluratkaisu palo-, rikos-, kamera-, ja/tai kiinteistövalvontalaitteistojen antamien hälytysten siirtämiseksi varmistetusti halutuille vastaanottajille jatkotoimenpiteitä varten. Hälytystapahtuman vastaanottajana voi olla mm. kiinteistön omistaja, huoltomies, hätäkeskus, yrityksen oma tai vartiointiliikkeen valvomo. Hälytystapahtumasta voidaan lähettää tieto useisiin valvomoihin sekä ennalta määritetyille vastaanottajille samanaikaisesti ja välitettävään sanomatietoon voidaan liittää paikka-, osoite- ja nimitietoa. Hälytystapahtumiin voidaan liittää kuittausvaatimus, jonka tilatietoa voidaan seurata reaaliaikaisesti. (TeliaSonera Finland Oyj 2003, 2.)

3.2.1 Alerta Lite

Sonera Hälytys- ja ohjauspalvelu Alerta Lite on hälytysten- ja ilmoitustensiirtopalvelu, jolla voidaan toteuttaa etävalvottavan kohteen hälytys- ja tapahtumatietojen vastaanotto, tallennus ja edelleensiirto Alerta-palvelutuotantojärjestelmään liitettyyn valvomoon ja/tai suoraan muuhun määriteltyyn viestivälineeseen. Hälytystiedon ilmaisemiseen viestivälineessä voidaan käyttää puhe-, teksti-, telefax- tai sähköpostiviestiä. Etävalvottavaan kohteeseen voidaan tehdä ohjauksia ja kyselyitä puhelimitse, jos käytettävässä päätelaitteessa on tuki tälle ominaisuudelle. Palveluun sisältyy selainpohjainen hallinnointityökalu, jolla kohteet voidaan nimetä, määritellä hälytysketjut, seurata ja tulostaa tallentuneita tapahtumatietoja sekä tehdä kaksisuuntaisten laitteiden ohjauksia ja kyselyitä.
(TeliaSonera Finland Oyj 2005d, 1.)

Alerta Lite -palvelu soveltuu kiinteisiin ja liikkuviin kohteisiin, joissa tiedonsiirtoyhteydelle ei ole asetettu linjavalvontavaatimuksia. Joidenkin valmistajien päätelaitteisiin tai niihin liittyviin valvontalaitteisiin on mahdollista määrittää vastaanottajalle välittyvä elossaoloviesti. Elossaoloviesti on tarkistettavissa palvelun tapahtumalokista, ja se voidaan edelleen siirtää ennalta määritettyyn vastaanottopisteeseen. Tiedonsiirtoyhteytenä palvelussa käytetään joko GSM-datayhteyttä tai kiinteän puhelinverkon yhteyttä. Valitusta verkkoyhteyden toteutustavasta

riippuen päätelaitteena käytetään joko GSM-modeemia tai robottipuhelinta. Alerta Lite -palvelussa käytettävä tiedonsiirtoyhteys ei ole operaattorisidonnainen. (TeliaSonera Finland Oyj 2005d, 1.)

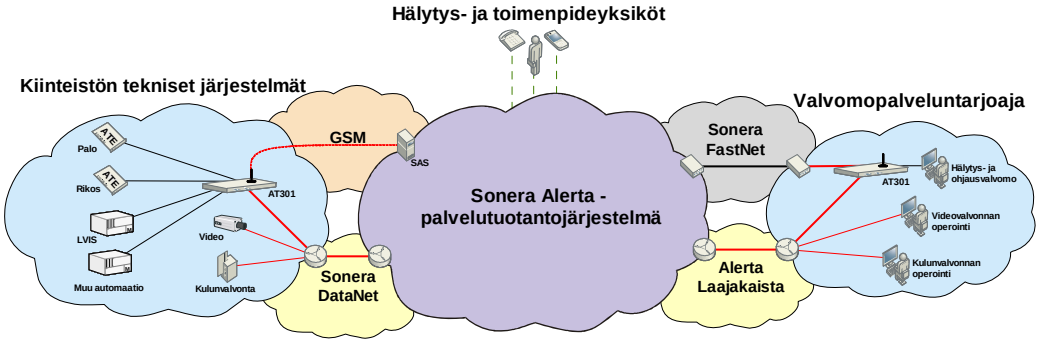
3.2.2 Alerta Prime

Sonera Hälytys- ja ohjauspalvelu Alerta Prime on ilmoitinjärjestelmien hälytysilmoitusten siirtopalvelu, jolla siirretään ja reititetään kiinteistöjen ilmoitusjärjestelmien hälytystietoa Alerta-palvelutuotantojärjestelmään liitettyyn viranomaisen, ulkoisen palveluntuottajan tai yrityksen omaan valvomoon. Hälytystiedot voidaan reitittää tietokohtaisesti usealle eri valvomopalveluntuottajalle sekä erillisen hälyttämispalvelun avulla muuhun määriteltyyn viestivälineeseen. Hälytystiedon ilmaisemiseen viestivälineessä käytetään puhe-, teksti-, telefax- tai sähköpostiviestiä. Hälyttämispalvelussa voidaan määritellä hälytysketjut siten, että eri viestivälineet ja henkilöt toimivat toistensa varmistuksena. Hälyttämispalveluun sisältyy selainpohjainen hallinnointityökalu, jolla määritellään hälytysketjut tai tilataan määrittelyt Soneran asiakaspalvelusta. (TeliaSonera Finland Oyj 2007a, 1, 4.)

Alerta Prime -palvelu soveltuu kiinteisiin kohteisiin, joissa tiedonsiirtoyhteydelle asetetaan linjavalvontavaatimuksia. Alerta Prime -palvelussa Sonera toimittaa käytettävän päätelaitteen ja palvelu sisältää päätelaitteen, kahdennetun tiedonsiirtoyhteyden ja niiden valvonnan. Päätelaitteena käytetään Prime T3 -siirtolaitekorttia, jolla on Vakuutusyhtiöiden keskusliiton 4(A)-luokan hyväksyntä sekä CEA 4039 -standardin vaatimustenmukaisuustodistus. Alerta Prime -palvelun tiedonsiirtoyhteyksinä käytetään GSM-datayhteyttä ja kiinteän puhelinverkon yhteyttä, joista GSM-datayhteys on palvelun pääyhteys ja kiinteän puhelinverkon yhteys toimii varayhteytenä. Molemmat käytetyistä tiedonsiirtoyhteyksistä ovat linjavalvottuina Alerta-palvelutuotantojärjestelmässä. Alerta Prime -palvelun hälytyskohteen on oltava Soneran GSM-verkon kuuluvuusalueella. Hälytyskohteen sijaitessa Soneran kiinteän puhelinverkon palvelualueen ulkopuolella voidaan kiinteän puhelinverkon yhteys toteuttaa toisen operaattorin puhelinliittymällä edellyttäen, että lankapuhelinliittymä sisältää samat lisäominaisuudet kuin Alerta-puhelinliittymä. (TeliaSonera Finland Oyj 2007a, 2 - 5.)

3.2.3 Alerta Pro

Sonera Hälytys- ja ohjauspalvelu Alerta Pro on hälytysten- ja ilmoitustensiirtopalvelu, jolla siirretään etävalvottavan kohteen paloilmoitin- ja rikosilmoitinjärjestelmien hälytystietoa sekä rakennusautomaatiojärjestelmien hälytys- ja ohjaustietoja Alerta-palvelutuotantojärjestelmään liitettyyn viranomaisen, ulkoisen palvelun-tuottajan tai yrityksen omaan valvomoon. Hälytystiedot voidaan reitittää tietokohtaisesti usealle eri valvomopalveluntuottajalle sekä erillisen hälyttämispalvelun avulla muuhun määriteltyyn viestivälineeseen. Hälytystiedon ilmaisemiseen viestivälineessä käytetään puhe-, teksti-, telefax- tai sähköpostiviestiä. Hälyttämispalvelussa voidaan määritellä hälytysketjut siten, että eri viestivälineet ja henkilöt toimivat toistensa varmistuksena. Hälyttämispalveluun sisältyy selainpohjainen hallinnointityökalu, jolla määritellään hälytysketjut tai tilataan määrittelyt Soneran asiakaspalvelusta. Alerta Pro -palvelulla voidaan myös muodostaa suora tiedonsiirtoyhteys eri hälytyskohteissa sijaitsevien järjestelmien tai laitteiden välille. Suoralla tiedonsiirtoyhteydellä voidaan mittaus- ja ohjaustietoja siirtää järjestelmien ja laitteiden välillä sekä niitä voidaan etähallita. Alerta Pro -palvelusta on kaksi toteutusvaihtoehtoa: Alerta Pro One ja Alerta Pro Multi -toteutus. Toteutusvaihtoehdot eroavat toisistaan vain käytettävien eri kiinteistöjärjestelmien lukumäärän osalta. Alerta Pro One -toteutusta käytetään yhden ja Alerta Pro Multi -toteutusta useamman kiinteistöjärjestelmän hälytyksensiirtoon samassa kiinteistössä. (TeliaSonera Finland Oyj 2007b, 1, 5.)



KUVIO 1. Alerta Pro Multi -toteutus (TeliaSonera Finland Oyj 2007b, 2)

Alerta Pro -palvelu soveltuu kiinteisiin kohteisiin, joissa tiedonsiirtoyhteydelle asetetaan linjavalvonta- ja salausvaatimuksia. Alerta Pro -palvelussa Sonera toimittaa käytettävät päätelaitteet ja kahdennetun tiedonsiirtoyhteyden. Alerta Pro -palvelu sisältää päätelaitteiden sekä kahdennetun tiedonsiirtoyhteyden valvonnan. Päätelaitteina käytetään Alerta Pro One -toteutuksessa AT101-reititinkorttia ja Alerta Pro Multi -toteutuksessa AT301-reititintä ja ATE-siirtolaitekorttia. Alerta Pro -palvelulla ja käytettävillä päätelaitteilla on Vakuutusyhtiöiden keskusliiton 4(A)-luokan hyväksyntä sekä CEA 4039 -standardin vaatimustenmukaisuustodistus. Alerta Pro -palvelun tiedonsiirtoyhteyksinä käytetään kiinteänverkon yhteyttä ja GSM-datayhteyttä, joista kiinteänverkon yhteys on palvelun pääyhteys ja GSM-datayhteys toimii varayhteytenä. Tiedonsiirrossa käytetään ensisijaisesti TPC/IP-protokollaa, joka tarvittaessa salataan käyttämällä SSL-salausta (Secure Sockets Layer). Molemmat käytetyistä tiedonsiirtoyhteyksistä ovat linjavalvottuina Alerta-palvelutuotantojärjestelmässä. Alerta Pro -palvelun hälytyskohteen on sijaittava Soneran GSM-verkon kuuluvuusalueella ja Soneran kiinteänverkon palvelualueella. (TeliaSonera Finland Oyj 2007b, 3 - 4, 7.)

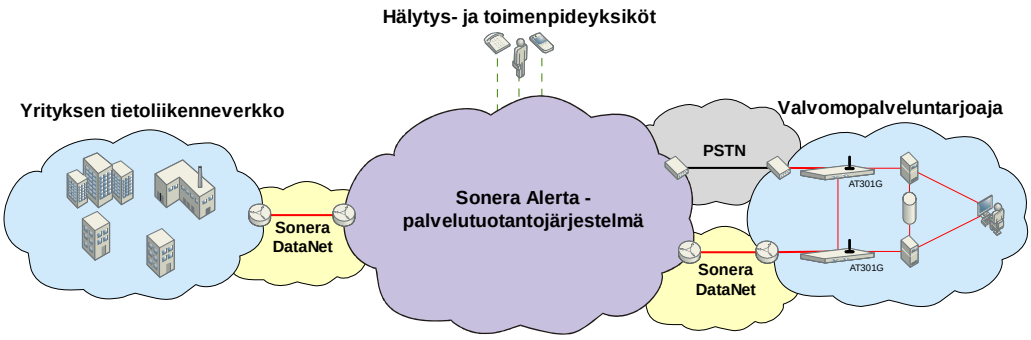
Alerta Pro -palvelu jaetaan kolmeen eri osaan: palo-, rikos-, ja kiinteistöturvapalvelut. Paloturvapalvelulla siirretään paloilmoitinjärjestelmän silmukka tai osoitteellisia palohälytyksiä, palon ennakkovaroituksia, ilmaisimien vika ja irtikytkentätietoja sekä laite- ja yhteysvikatietoja vastaanottavaan valvomoon. Päätelaitteina paloturvapalvelussa käytetään Alerta Pro One -toteutuksessa AT101-reititinkorttia ja Alerta Pro Multi -toteutuksessa AT301-reititintä ja ATE-siirto-laitekorttia. AT101-reititin- ja ATE-siirtolaitekortti asennetaan paloilmoitinkeskuksen sisälle ja kytketään paloilmoitinkeskuksen varmennettuun sähkönsyöttöön. AT301-reititin asennetaan tietoliikennetilaan ja kytketään varmennettuun sähkönsyöttöön. (TeliaSonera Finland Oyj 2007b, 5.)

Rikosturvapalvelulla siirretään rikosilmoitinjärjestelmän keskuksen linjahälytyksiä, silmukka- ja ryhmähälytyksiä ja muita laitehälytyksiä vastaanottavaan valvomoon. Päätelaitteina rikosturvapalvelussa käytetään AT301-reititintä tai AT101-reititinkorttia. Tarvittaessa lisälaitteena käytetään ATE-siirtolaitekorttia. (TeliaSonera Finland Oyj 2007b, 5.)

Kiinteistöturvapalvelulla siirretään rakennusautomaatiojärjestelmän hälytyksiä valvovaan kohteeseen ja ohjaustietoja rakennusautomaatiojärjestelmän laitteiden välillä. Päätelaitteina kiinteistöturvapalvelussa käytetään AT301-reititintä tai AT101-reititinkorttia. Tarvittaessa lisälaitteena käytetään ATE-siirtolaitekorttia. (TeliaSonera Finland Oyj 2007b, 5.)

3.3 Valvomopalvelu

Sonera valvomopalvelu on ratkaisu, jolla vastaanotetaan hälytyssanomia turvallisuusjärjestelmistä ja valvontakuvaa valvottavista kohteista sekä etähallitaan kohdejärjestelmiä valvomojärjestelmällä. Valvomopalvelulla eri palveluntarjoajat kuten aluehätäkeskukset, vartiointi- ja kiinteistöhuoltoliikkeet sekä konsernien päivystyspisteet saavat tietoa Alerta-palvelutuotantojärjestelmän välityksellä paikallisista teknisistä järjestelmistä valvomojärjestelmiinsä. Valvomopalvelulla hälytystapahtumat voidaan edelleen siirtää toiseen valvomoon, muuhun yksittäiseen viestintävälineeseen tai hälytysryhmälle. Edelleen siirrettyihin hälytystapahtumiin voidaan liittää kuittausvaatimus, jonka tilatietoa voidaan seurata reaaliaikaisesti. Hälytystiedon ilmaisemiseen viestivälineessä käytetään puhe-, teksti-, telefax- tai sähköpostiviestiä. (TeliaSonera Finland Oyj 2003, 2.)



KUVIO 2. Valvomopalvelun periaate (TeliaSonera Finland Oyj 2003, 4)

Valvomojärjestelmään välitetään kohteesta hälytysilmoituksia, täydentäviä sijaintitietoja, pohja- ja tilannekuvia, toimintaohjeita sekä muuta tarpeellista informaatiota. Hälytystilanteessa kokonaiskuvaa tilanteesta voidaan täydentää lisätietokyselyillä hälytyskohteen järjestelmään tai valvomojärjestelmään liitettyihin tietokantoihin. Hälytystilanteen vaatiessa hälytys- tai huoltoyksikön kohteessa käyntiä valvomojärjestelmä suorittaa tarvittavien yksiköiden hälytykset ja toimittaa yksiköille toimintaohjeita. (TeliaSonera Finland Oyj 2006c, 1.)

Valvomopalvelukokonaisuus sisältää valvomon fyysisen liittymän, fyysisen liittymän rajapinnat ja tiedonsiirronvarmistuksen, valvomon tietojärjestelmän ja käyttöliittymät sekä Alerta-palveluiden valvomojärjestelmälle tarjoamat palvelut. Fyysinen liittymä on tiedonsiirtoyhteys valvomojärjestelmän ja Alerta-palvelutuotantojärjestelmän välillä. Valvomopalvelun tiedonsiirtoyhteydelle asettamat vaatimukset ovat korkea käytettävyys ja lyhyet vasteajat verkkopalveluihin. Tiedonsiirtoyhteyksinä käytetään kiinteitä datayhteyksiä tai TCP/IP-yhteyksiä. Käytettävyyden varmistamiseksi tiedonsiirtoyhteydet ovat linjavalvottuja ja kahdennettuja. (TeliaSonera Finland Oyj 2006c, 3.)

Kahdennetuissa tiedonsiirtoyhteyksissä pyritään käyttämään erityyppisiä tiedonsiirtoyhteyksiä. Tiedonsiirtoyhteydet ja niiden päätelaitteet ovat valvottuina Alerta-palvelutuotantojärjestelmässä. Tiedonsiirtoyhteyden vikaantuminen aiheuttaa linjavikahälytyksen Alerta-palvelutuotantojärjestelmään ja käytettävään valvomojärjestelmään. Linjavikahälytys voidaan lähettää määritettyyn viestivälineeseen automaattisesti Alerta-palvelutuotantojärjestelmästä tai edelleen siirtona valvomojärjestelmästä. Päätelaitteena valvomopalvelussa käytetään AT301-reititintä, joka toimii valvomojärjestelmän edustapalvelimena ja tarjoaa yhtenäisen liitäntärajapinnan valvomon tietojärjestelmille. Tarvittaessa edustapalvelin ja valvomon tietojärjestelmät voidaan kahdentaa. Edustapalvelimet asennetaan aina valvomotilaan tai sen välittömään läheisyyteen ja liitetään tietojärjestelmään joko sarja- tai Ethernet-liitännällä. (TeliaSonera Finland Oyj 2006c, 3 - 4.)

Valvomoiden tietojärjestelmät ja valvomo-ohjelmistot suunnitellaan usein toimialakohtaisesti, koska toimintatavat ja käsitteet eroavat toisistaan eri toimialoilla. Tiedonsiirron ja viestinnän osalta tarpeet ovat kuitenkin yhtenevät. Valvomopalvelun toiminnallisena rajapintana valvomon tietojärjestelmille toimii palvelukirjasto, jonka avulla valvomopalvelua voidaan hyödyntää eri tarkoituksiin suunniteltuilla tietojärjestelmillä. Palvelukirjastorajapinnassa Alerta-toiminnot ovat määritetty palvelufunktioittain. Palvelufunktiot sisältävät Alerta-toimintojen käyttöön liittyvät muuttujat ja parametrit. Valvomon tietojärjestelmän toimittaja toteuttaa käyttöliittymäänsä tarvittavat palvelufunktiot ja palvelukirjaston Alerta-toiminnot sovitetaan valvomon tietojärjestelmään yhteistyössä Soneran kanssa. Palvelukirjaston Alerta-toimintojen ulkoasu tietojärjestelmän käyttöliittymässä jää tietojärjestelmätoimittajan ratkaistavaksi. (TeliaSonera Finland Oyj 2006c, 5 - 6.)

3.4 Kuvavalvontapalvelu

Sonera Kuvavalvontapalvelu on ratkaisu, jolla yksittäisestä kamerasta tai videovalvontajärjestelmästä saatava kuvainformaatio tallennetaan Alerta-palvelutuotantojärjestelmään ja tarvittaessa edelleen siirretään määriteltyihin viestivälineisiin. Kuvainformaation lähetyksen Alerta-palvelutuotantojärjestelmään aktivoi kameran liikeilmaisin tai rikosilmoitinkeskuksen hälytysilmoitus. Tiedonsiirtoyhteytenä Alerta-palvelutuotantojärjestelmään käytetään GPRS-, GSM- tai muuta IP-pohjaista datayhteyttä. Tiedonsiirtoyhteyden tyyppi on vapaasti valittavissa eikä tiedonsiirtoyhteys ole operaattorisidonnainen. (TeliaSonera Finland Oyj 2004, 1 - 2.)

Kuvavalvontapalvelu vastaanottaa valvottavan kohteen kuvainformaation sekä tapahtumatiedot ja tallentaa ne palvelimelle, joka sijaitsee kohteesta riippumattomassa ja tietoturvallisessa ympäristössä. Yhdestä tapahtumasta tallennettavien kuvien lukumäärään vaikuttaa kohteessa käytettävän videovalvontajärjestelmän ominaisuudet, yksittäinen kamera tuottaa vain yhden kuvan yhdestä tapahtumasta. Palvelimelle tallennettuja tietoja voidaan tarkastella selainpohjaisella hallinnointityökalulla. (TeliaSonera Finland Oyj 2004, 2.)

Hallinnointityökalulla määritellään kuvainformaation edelleen siirto halutuille vastaanottajille, tapahtumatietojen seuranta ja raporttien tulostus. Hallinnointityökalun tapahtumat ja tehdyt muutokset kirjautuvat erilliseen tapahtumalokiin. Tarvittaessa kuvainformaatio edelleen siirretään MMS- (Multimedia Messaging Service) tai sähköpostiviestinä ennalta määriteltyyn viestivälineeseen tai käytettävään valvomojärjestelmään yhteen sovitettuna sanomaviestinä valvomopalveluntarjoajalle. Kuvainformaatiosta voidaan myös muodostaa tapahtumatieto, joka välitetään puheena tai SMS-viestinä (Short Message Service) ennalta määritettyyn hälytysketjuun. Tapahtumatiedon vastaanottaminen edellyttää vastaanottajalta viestin kuittausta. (TeliaSonera Finland Oyj 2004, 2 - 3.)

4 ALERTA-HÄLYTYKSENSIIRTOLAITTEET

4.1 AT101-reititinkortti

AT101-reititinkortti on tiedonsiirtolaite, jolla paikallinen kiinteistö- tai valvomojärjestelmä yhdistetään Alerta-palvelutuotantojärjestelmään. AT101-reititinkortilla siirretään hälytys-, mittaus- ja ohjaustietoja kiinteistöjärjestelmästä paikalliseen valvomojärjestelmään tai Alerta-palveluverkkoon. Tiedonsiirtoyhteys Alerta-palveluverkkoon on linjavalvottu ja kahdennettu. Tiedonsiirtoyhteytenä käytetään TCP/IP-, GSM- tai kiinteää modeemiyhteyttä. AT101-reititinkortti on osa Alerta-palveluverkkoa, joten AT101-reititinkortti on Alerta-palvelutuotantojärjestelmän verkonvalvonnan ja -hallinnan piirissä. AT101-reititinkorttia voidaan etähallita tai operoida paikallisesti. AT101-reititinkortti voidaan liittää mihin tahansa kosketintietoa välittävään kiinteistöjärjestelmään ja sellaisiin osoitteellisia hälytystietoja välittäviin kiinteistöjärjestelmiin, joille on tehty protokollatason sovitus. (TeliaSonera Finland Oyj 2005a, 1.)

AT101-reititinkortti on yhden kortin koteloimaton mikrotietokone, joka sisältää GSM-modeemin, kaksi RS232-sarjaliitäntäporttia, neljä kosketinsisäänmenoa, kaksi kosketinulostuloa ja kaksi Ethernet-liitäntäporttia. AT101-reititinkortin Ethernet-liitäntäportit ovat itsenäisiä, ja jokaiselle Ethernet-liitäntäportille voidaan määrittää kiinteä tai dynaaminen IP-osoite. Ethernet-liitäntäporttien välillä ei ole fyysistä yhteyttä. AT101-reititinkortin kosketinsisäänmenot ja ulostuloreleen kosketintieto releen vetäessä voidaan ohjelmallisesti määritellä avautuvaksi tai sulkeutuvaksi. Kiinteistö- tai valvomojärjestelmä liitetään suoraan AT101-reititinkortin RS232-sarjaliitäntäporttiin, Ethernet-porttiin tai kosketinsisäänmenoon. AT101-reititinkortti asennetaan kiinteistöjärjestelmän sisälle ja kytketään kiinteistöjärjestelmän sähkönsyöttöön tai ulkoiseen virtalähteeseen. Tiedonsiirtoyhteys Alerta-palveluverkkoon liitetään AT101-reititinkortin Ethernet-porttiin ja varayhteys toteutetaan GSM-modeemiyhteydellä. (TeliaSonera Finland Oyj 2005a, 1 - 3.)

4.2 AT301-reititin

AT301-reititin on tiedonsiirtolaite, jolla paikalliset kiinteistö- tai valvomojärjestelmät yhdistetään Alerta-palvelutuotantojärjestelmään. AT301-reitittimellä siirretään hälytys-, mittaus- ja ohjaustietoja kiinteistöjärjestelmistä paikalliseen valvomojärjestelmään tai Alerta-palveluverkkoon. Tiedonsiirtoyhteys Alerta-palveluverkkoon on linjavalvottu ja kahdennettu. Tiedonsiirtoyhteytenä käytetään TCP/IP-, GSM- tai kiinteää modeemiyhteyttä. AT301-reititin on osa Alerta-palveluverkkoa, joten AT301-reititin on Alerta-palvelutuotantojärjestelmän verkonvalvonnan ja -hallinnan piirissä. AT301-reititintä voidaan etähallita tai operoida paikallisesti. AT301-reititin voidaan liittää mihin tahansa kosketintietoa välittävään kiinteistöjärjestelmään ja sellaisiin osoitteellisia hälytystietoja välittäviin kiinteistöjärjestelmiin, joille on tehty protokollatason sovitus.
(TeliaSonera Finland Oyj 2005b, 3 - 5.)

AT301-reititin on yhden kortin koteloitu mikrotietokone, joka sisältää GSM-modeemin, kolme RS232-sarjaliitäntäporttia, kaksi RS485-sarjaliitäntäporttia, neljä kosketinsisäänmenoa, kaksi kosketinulostuloa ja neljä Ethernet-liitäntäporttia, joista yksi on laitteen kotelon sisäpuolella. AT301-reitittimeen voidaan liittää lisäkortti, joka sisältää neljä RS232-sarjaliitäntäporttia. AT301-reitittimen Ethernet-liitäntäportit ovat itsenäisiä ja jokaiselle Ethernet-liitäntäportille voidaan määrittää kiinteä tai dynaaminen IP-osoite. Ethernet-liitäntäporttien välillä ei ole fyysistä yhteyttä, ja RS485-sarjaliitäntäportit ovat sähköisesti erotettu toisistaan. AT301-reitittimen kosketinsisäänmenot ja ulostuloreleen kosketintieto releen vetäessä voidaan ohjelmallisesti määritellä avautuvaksi tai sulkeutuvaksi.
(TeliaSonera Finland Oyj 2005b, 10 - 11.)

Kiinteistö- tai valvomojärjestelmät liitetään AT301-reitittimen sarjaliitäntäportteihin joko suoraan tai lähiyhteysmodeemien välityksellä. Lähiyhteysmodeemien käyttäminen on suositeltavaa haitallisten potentiaalierojen välttämiseksi, etenkin AT301-reitittimen ja kiinteistö- tai valvomojärjestelmien sähkönsyötön tapahtuessa eri virtalähteistä. AT301-reittimen Ethernet-liitäntäportteihin kiinteistö- tai valvomojärjestelmät liitetään joko suoraan tai muun verkkolaitteen esimerkiksi kytkimen välityksellä. (TeliaSonera Finland Oyj 2005b, 8.)

Paloilmoitinjärjestelmät liitetään AT301-reitittimeen aina ATE-siirtolaitekortin välityksellä, ja liikennöinti tapahtuu Modbus-protokollalla. ATE-siirtolaitekortti liitetään AT301-reitittimen RS485-sarjaliitäntäporttiin. Tiedonsiirtoyhteys Alerta-palveluverkkoon liitetään AT301-reitittimen Ethernet-porttiin ja varayhteys toteutetaan GSM-modeemiyhteydellä. (TeliaSonera Finland Oyj 2005b, 8.)

AT301-reititin pyritään aina asentamaan tietoliikennetilaan, jolloin tiedonsiirtoyhteyksien päättäminen sekä kiinteistö- ja valvomojärjestelmien kaapeloinnin ja AT301-reitittimen sähkönsyötön järjestäminen on helpompaa. AT301-reitittimen sähkönsyöttö voidaan toteuttaa kolmella eri tavalla: akkuvarmentamaton tehonlähde, kiinteistöjärjestelmän akkuvarmennettu ulkoinen jänniteotto tai erillinen akkuvarmennettu tehonlähde tai UPS-laite. Sähkönsyötön toteutustapaan vaikuttaa AT301-reitittimen käyttötarkoitus. Siirrettäessä kriittistä informaatiota, kuten palo- ja rikosilmoitushälytykset, AT301-reititin kytketään aina varmennettuun sähkönsyöttöön. (TeliaSonera Finland Oyj 2005b, 6.)

4.3 ATE-siirtolaitekortti

ATE-siirtolaitekortti on AT301-reitittimen RS485-sarjaliitäntäporttiin liitettävä laajennuskortti, joka sisältää RS232-sarjaliitäntäportin, kaksi RS485-sarjaliitäntäporttia, neljä kosketinsisäänmenoa ja kaksi kosketinulostuloa. ATE-siirtolaitekorttia käytetään pääsääntöisesti paloilmoitinkeskuksien ilmoituksensiirtojärjestelmän siirtolaitteena, jolloin ATE-siirtolaitekortti asennetaan paloilmoitinkeskuksen sisälle ja kytketään paloilmoitinkeskuksen varmistettuun sähkönsyöttöön. ATE-siirtolaitekorttia voidaan käyttää myös itsenäisenä osoitteellisten ja silmukkahälytysten siirtolaitteena. Paloilmoittimen tai muun ilmoitinlaitteen osoitteelliset hälytykset liitetään ATE-siirtolaitekorttiin RS232-sarjaliitännällä ja silmukkahälytykset liitetään kosketintietona. ATE-siirtolaitekortti liitetään linjavalvotulla RS485-yhteydellä tietoliikennetilassa olevaan AT301-reitittimeen, joka on liitetty linjavalvotulla tiedonsiirtoyhteydellä Alerta-palvelutuotantojärjestelmään.
(TeliaSonera Finland Oyj 2005b, 16 - 17.)

4.4 Prime T2-3 -siirtolaitekortti

Prime T2-3 -siirtolaitekortti on valvontapääte, jolla paikallinen paloilmoitin-, rikosilmoitin- tai rakennusautomaatiokeskus yhdistetään Alerta-palvelutuotantojärjestelmään. Prime T2-3 -siirtolaitekortilla siirretään kiinteistöjärjestelmien hälytys-, mittaus- ja ohjaustietoa SNAP-protokollalla (SafeNet Applicaton Protocol) Alerta-palvelutuotantojärjestelmän välityksellä valvomojärjestelmään. Tiedonsiirtoyhteys Alerta-palveluverkkoon on linjavalvottu ja kahdennettu. Tiedonsiirtoyhteyksinä käytetään GSM-datayhteyttä ja varmentavaa kiinteän puhelinverkon modeemiyhteyttä. Prime T2-3 -siirtolaitekortti on osa Alerta-palveluverkkoa, joten Prime T2-3 -siirtolaitekortti on Alerta-palvelutuotantojärjestelmän verkonvalvonnan ja -hallinnan piirissä. Prime T2-3 -siirtolaitekorttia voidaan etähallita tai operoida paikallisesti. (Computec Oy 2004, 1 - 2.)

Prime T2-3 -siirtolaitekortti sisältää kahdeksan digitaalituloa, kaksi analogiatuloa, kaksi relelähtöä, GSM- ja analogiamodeemin sekä kuumalinja-toiminnon. Prime T2-3 -siirtolaitekortin digitaali- ja analogiatulojen sekä relelähtöjen toimintaa voidaan muuttaa ohjelmallisesti. Kiinteistöjärjestelmien hälytys-, mittaus- ja ohjaussilmukat liitetään Prime T2-3 -siirtolaitekorttiin kosketintietona. Prime T2-3 -siirtolaitekortti asennetaan kiinteistöjärjestelmän keskuksen sisälle tai teknisen tilan laitekaappiin. Asennettaessa Prime T2-3 -siirtolaitekortti kiinteistöjärjestelmän sisälle kytketään Prime T2-3 -siirtolaitekortti keskuksen varmennettuun sähkönsyöttöön. Laitekaappiin asennettaessa Prime T2-3 -siirtolaitekortti kytketään erilliseen akkuvarmennettuun virtalähteeseen. (Computec Oy 2004, 1 - 2.)

5 KÄYTETTÄVÄT TIEDONSIIRTOPALVELUT

5.1 Alerta Laajakaista

Alerta Laajakaista on suljettu IP-pohjainen kiinteistöjärjestelmien tiedonsiirtoon suunniteltu laajakaistayhteys. Alerta Laajakaistaa käytetään pelkästään kiinteistöjen hälytyksensiirtoon ja valvomokäyttöön liittyvien teknisten järjestelmien ja laitteiden välisiin tiedonsiirtoyhteyksiin tai tiedonsiirtoyhteytenä Alerta-palveluverkkoon. Alerta Laajakaistaa ei käytetä muun tietoliikenteen välittämiseen eikä liittymästä ole yhteyttä Internettiin. Alerta Laajakaistalla ei voida toteuttaa hallinnollisen tai muun monisovelluskäytön tiedonsiirtotarpeita. Alerta Laajakaistan tiedonsiirtoyhteys ja käytettävä päätelaite ovat liitetty Soneran verkon valvontaan ja ylläpitoon. Ylläpitoluokaksi voidaan valita kaksi vaihtoehtoa vakio (A12) tai täysi (A4h) ylläpito. (TeliaSonera Finland Oyj 2005c, 1 - 3.)

Palo- ja rikosilmoitinjärjestelmät sekä rakennusautomaatiojärjestelmät liitetään Alerta Laajakaista -yhteyden reitittimeen Alerta-päätelaitteiden välityksellä. Videovalvonta- ja kulunhallintajärjestelmät tarvitsevat vain kahden pisteen välisen tiedonsiirtoyhteyden, jolloin ne voidaan liittää suoraan Alerta Laajakaista -yhteyden reitittimeen. Reitittimeen suoraan IP-yhteydelle tai Alerta-päätelaitteiden välityksellä liitetyt järjestelmät käyttävät tiedonsiirrossa samaa Alerta Laajakaista -yhteyttä. Alerta Laajakaista -yhteyden tiedonsiirtokapasiteetiksi voidaan valita 256, 512 tai 2048 kb/s. Hälytystietojen ajantasaisen siirron varmistamiseksi ruuhkatilanteessa tiedonsiirtokapasiteetista 5 % on priorisoitu hälytysliikenteelle. (TeliaSonera Finland Oyj 2005c, 1 - 3.)

5.2 Sonera Talotekniikkayhteys Plus -liittymä.

Sonera Talotekniikka Plus -liittymä on eristetty osa Soneran asuinkiinteistöihin toimittamaa kuituyhteyttä Sonera Kiinteistöyhteys Plus tai Sonera Kiinteistöyhteys Kuitu. Sonera Talotekniikkaa Plus -liittymällä toteutetaan avoin IP-pohjainen laajakaistainen Internet-yhteys, jota käytetään pelkästään kiinteistön teknisten järjestelmien tiedonsiirtoon, kuten rakennusautomaatiojärjestelmien etähallinta, energiakulutuksen mittaus ja paikallisten turvajärjestelmien hälytysten siirto. Sonera Talotekniikka Plus -liittymällä ei voida toteuttaa hallinnollisen tai muun monisovelluskäytön tiedonsiirtotarpeita. Sonera Talotekniikka Plus -liittymän valvonta ja ylläpitoluokka määräytyvät käytettävän kuituyhteyden palvelusopimuksen mukaisesti. Sonera Talotekniikka Plus -liittymää käyttävät tekniset järjestelmät ja niistä vastaavat palveluntuottajat ovat asiakkaan vapaasti valittavissa. (TeliaSonera Finland Oyj 2005e, 2 - 3.)

Kiinteistön tekniset järjestelmät liitetään kiinteistön sisäverkon kaapeloinnin perusteella joko suoraan Soneran toimittaman kuituyhteyden liitäntäpisteeseen tai erillisen päätelaitteen välityksellä. Sisäverkon kaapeloinnin ollessa laatuluokan 5 (CAT5) mukainen tai parempi voidaan kiinteistön tekniset järjestelmät liittää suoraan kuituyhteyden liitäntäpisteen Ethernet-liitäntään. Sisäverkon kaapeloinnin ollessa laatuluokan 3 (CAT3) mukainen tai huonompi tulee asiakkaan hankkia siltaava RFC 1483 -standardia (Request For Comments) tukeva ADSL (Asymmetric Digital Subscriber Line) tai ADSL2+ päätelaite kiinteistön teknisten järjestelmien liittämistä varten. Päätelaitetta varten Sonera Talotekniikka Plus -liittymä sisältää yhden kiinteän julkisen IP-osoitteen, jota käytetään tiedonsiirtoyhteyden luomiseen. Yhdelle kuituyhteydelle voidaan toteuttaa kaksi Sonera Talotekniikka Plus -liittymää. Sonera Talotekniikka Plus -liittymän tiedonsiirtokapasiteetti on symmetrinen 512/512 kb/s. (TeliaSonera Finland Oyj 2005e, 2, 4 - 5.)

5.3 TeliaSonera DataNet

TeliaSonera DataNet on yritys- ja yhteisöasiakkaille tarjottava tiedonsiirtopalvelu, jolla yhdistetään asiakkaan eri toimipaikkojen lähiverkot ja muut verkkoratkaisut yhdeksi kokonaisuudeksi. TeliaSonera DataNet -palvelulla muodostetaan asiakaskohtainen monipalveluverkko, johon voidaan liittää yrityksen etätyöntekijät ja yhteistyökumppanit, lisäksi TeliaSonera DataNet -palvelua käytetään tiedonsiirtoalustana muille TeliaSoneran tarjoamille asiakasverkkoon liitettäville IP-pohjaisille palveluille. TeliaSonera DataNet -palvelun kolme pääelementtiä on asiakasverkon vakiopalvelut, eri liittymätavat ja lisäpalvelut.
(TeliaSonera Finland Oyj 2006a, 3 - 4.)

TeliaSonera DataNet on tietoturvallinen ja suljettu verkkoarkkitehtuuri, johon asiakkaalle luodaan oma looginen virtuaalinen asiakasverkko tai useampia asiakaskohtaisia verkkoja. Asiakasverkot erotetaan muista loogisista verkoista tietoturvalliseksi, yksityiseksi ja suojatuksi loogiseksi verkkokokonaisuudeksi, jonka liikennöintiä asiakasverkosta sisään ja ulospäin on rajoitettu. Asiakasverkon toiminnallisuus suunnitellaan asiakkaan tarpeiden pohjalta huomioimalla verkossa käytettävien palveluiden käyttötarpeet ja niiden tiedonsiirrolle asettamat vaatimukset. Asiakkaan lähiverkon liityntänä TeliaSonera DataNet -verkkoon käytetään kolmea liittymätapaa: Multi, Trust tai Flex. Liittymätapa valitaan asiakkaan lähiverkon käyttötarkoituksen, tietoliikennetarpeiden ja maantieteellisen sijainnin perusteella. (TeliaSonera Finland Oyj 2006a, 3, 8.)

TAULUKKO 3. Liittymätapojen ominaisuudet (TeliaSonera Finland Oyj 2006a, 7)

Liittymätapa	**Liikenneluokittelu**	**Päästä-päähän hallinta**	**Kokonaan verkotettu topologia**	**Tähtimäinen topologia**
Multi	Kyllä	Kyllä	Kyllä	Valinnainen
Trust	Ei	Kyllä	Valinnainen	Kyllä
Flex	Ei	Ei	Ei	Kyllä

5.4 Sonera FastNet

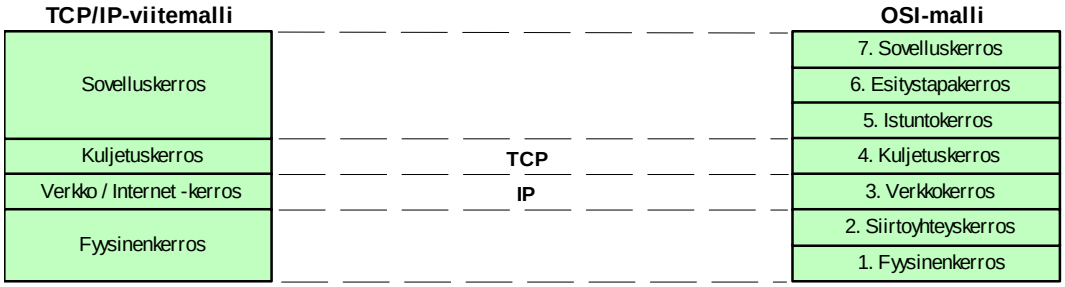
Sonera FastNet -palvelu (Flexible Access System for Tele NETwork) on pienille, keskisuurille sekä konsernitason yrityksille tarjottava tietoliikenneratkaisu, jolla yhdistetään asiakkaan eri toimipaikkojen lähiverkot yhtenäiseksi verkoksi. Sonera FastNet -palvelussa käytetään lähiverkkojen yhdistämiseen kiinteitä yhteyksiä ja palvelulla voidaan toteuttaa yhteydet yleiseen puhelinverkkoon. Sonera FastNet -palvelu toimii myös alustana muille TeliaSonera Finland Oyj:n tarjoamille palveluille ja tukee ITU-T (International Telecommunications Union - Telecommunications) standardien mukaisia liityntärajapintoja käyttävien tietoliikennelaitteiden verkottamista. (TeliaSonera Finland Oyj 2006b, 3 - 5.)

Sonera FastNet -palvelu pohjautuu Tellabs Oy:n MartisDXX™ teknikkaan ja palveluun voidaan liittyä kahdella eri tavalla, joko asiakassolmu Telegate-liittymänä tai modeemiliittymänä. Telegate-liittymiä on neljä eri perustyyppiä mini-, midi-, single- tai doublesolmuja, joista käytettävä solmutyyppi valitaan asiakkaan tarpeen mukaan. Modeemiliittymissä asiakkaan päätelaitteille on tarjolla useita erilaisia ITU-T standardin mukaisia liitäntöjä sekä kantataajuusliitäntöjä. Sonera FastNet -palvelulla toteutettavia yhteyksiä ovat: kiinteät kaksipisteyhteydet, lähiverkkojen yhdistäminen sillatuin yhteyksin, haaroitetut yhteydet, yksisuuntaiset haaroitetut yhteydet, kompressoidut puheyhteydet, kiinteät vaihdeverkot, yhteydet yleiseen puhelinverkkoon ja asiakaskohtaiset varmennukset.
(TeliaSonera Finland Oyj 2006b, 3 - 6.)

6 TCP/IP-PROTOKOLLAPERHE

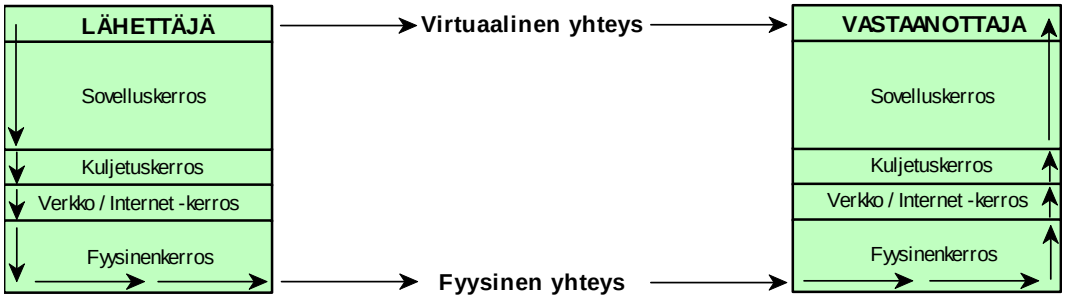
6.1 TCP/IP-pino

TCP/IP on kokoelma tiedonsiirtoprotokollia, joiden käyttämiseen kaikki Internetin tiedonvälitys pohjautuu. Tiedonsiirrossa käytettävät protokollat muodostavat protokollapinon, jonka toiminnallisuus kuvataan TCP/IP-viitemallilla. TCP/IP-viitemalli on yksinkertaistettu kerroksittainen malli, jonka eri kerrokset tarjoavat palveluita toisilleen tiedonvälittämiseksi. TCP/IP ei määrittele mitä välitettävä tietosisältö tarkoittaa tai miten tietosisältöä tulkitaan. (Acromag Inc. 2005, 9.)



KUVIO 3. TCP/IP-viitemalli verrattuna OSI-malliin (Acromag Inc. 2005, 8)

Lähetettäessä tietoa TCP/IP-viitemallin alempi kerros kapseloi ylemmältä kerrokselta vastaanottamansa tietosisällön oman kehysrakenteensa sisälle ja välittää näin muodostamansa sanoman alapuolellaan olevalle kerrokselle. Vastaanotettaessa tietoa alempi kerros poistaa oman kehysrakenteensa ja välittää jäljelle jäävän tietosisällön ylemmälle kerrokselle. (Acromag Inc. 2005, 10.)



KUVIO 4. TCP/IP-pinon toiminta (Acromag Inc. 2005, 10)

6.2 TCP-protokolla

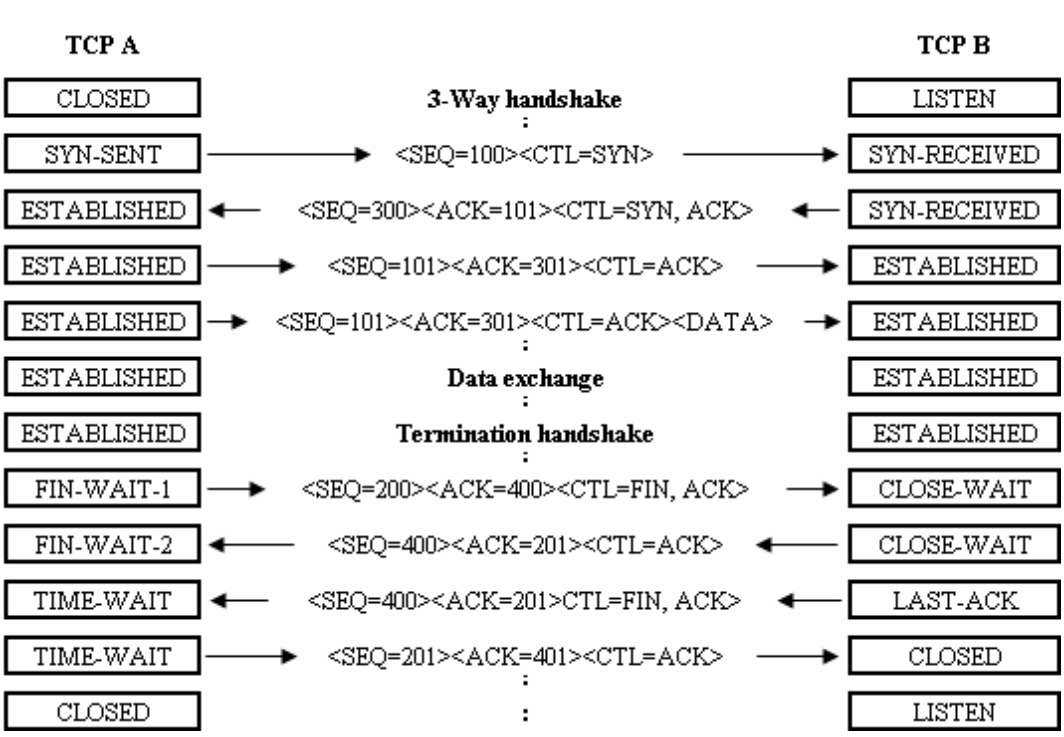
TCP-protokolla on yhteydellinen protokolla, joka sijaitsee TCP/IP-viitemallin kuljetuskerroksella. TCP-protokolla tarjoaa sovelluskerrokselle luotettavan virtuaalisen päästä päähän yhteyden kahden verkossa toimivan laitteen välille. TCP-protokolla muodostaa sovelluskerroksen tietovirrasta segmenttejä, suorittaa kanavointia sekä vuon- ja yhteyksienhallintaa. Vaihtelevan kokoisten segmenttien välittämiseen TCP-protokolla käyttää verkkokerroksen tarjoamaa epäluotettavaa välityspalvelua. Segmenttien pilkkominen tai uudelleen kokoaminen sekä osoitteistus jätetään verkkokerroksen tehtäväksi. Yleensä TCP-protokolla käyttää verkkokerroksen protokollana IP-protokollaa. (Postel 1981b, 1 - 3.)

Tarjotakseen luotettavaa palvelua TCP-protokollan on hallittava tilanteet, joissa vastaanotettu tieto on virheellistä, kadonnut, kahdentunut tai vastaanotettu väärässä järjestyksessä. Luotettavuuden toteuttamiseksi TCP-protokollassa käytetään järjestysnumerointia, vahvistuskuittauksia ja tarkisteita. Lähetettäviin segmentteihin sisällytetään järjestysnumero, jonka perusteella järjestetään vastaanotetut segmentit oikeaan järjestykseen ja tunnistetaan kahdentuneet segmentit. Vahvistuskuittauksilla varmistetaan lähetettyjen segmenttien onnistunut vastaanotto. Lähettäjä odottaa tietyn aikavälin vahvistuskuittausta lähetettyyn segmenttiin, jonka jälkeen segmentti lähetetään uudelleen. Tarkisteilla tunnistetaan tiedonsiirrossa tapahtuneet virheet. Lähetettävästä segmentistä lasketaan tarkiste, joka sisällytetään segmenttiin. Vastaanotetusta segmentistä lasketaan tarkiste, jota verrataan segmentin sisältämään tarkisteeseen. Tarkisteiden erotessa toisistaan segmentti hylätään eikä lähetä vahvistuskuittausta, jolloin segmentti lähetetään uudelleen. TCP-protokollassa vuonhallintaa toteutetaan ikkunoinnilla, jolla määritetään, kuinka monta oktettia voidaan lähettää ennen vahvistuskuittausta. (Postel 1981b, 4.)

Lähde-portti	Kohde-portti	Järjestys-numero	Kuittaus-numero	Otsikon pituus	Varattu	Liput	Ikkunan koko	Tarkiste	Kiire-osoitin	Optiot	Täyte	Tietosisältö

KUVIO 5. TCP-segmentti (Postel 1981b, 15)

Tiedonsiirtotapahtuma osapuolten välillä edellyttää TCP-yhteyden muodostamista. TCP-protokollassa alustetaan ja ylläpidetään tilatietoja sovelluskerroksen tietovirroista. TCP-yhteys käsitetään tilatietojen yhdistelmänä mukaan lukien soketit, järjestysnumerot ja ikkunointi. TCP-yhteys alustetaan käyttämällä kättely-mekanismia. Tiedonsiirtotapahtuman päätyttyä TCP-yhteys puretaan resurssien vapauttamiseksi. (Postel 1981b, 5.)



KUVIO 6. TCP-tiedonsiirtotapahtuma (Postel 1981b, 31, 39)

Tietovirtojen kanavointi ja samanaikaisten yhteyksien hallinta toteutetaan TCP-protokollassa soketeilla. Sovelluskerroksen eri tietovirrat erotetaan toisistaan porttinumeroilla, jotka yhdessä verkkokerroksen osoitteen kanssa muodostavat soketin. Lähde- ja kohdesoketit muodostavat sokettiparin, joka yksilöi käytettävän yhteyden. Paikallista lähdesokettia voidaan käyttää useisiin yhteyksiin eri kohdesoketteihin. Sokettiparin määrittelemällä yhteydellä voidaan siirtää tietoa molempiin suuntiin. (Postel 1981b, 10.)

TAULUKKO 4. TCP-porttinumeroiden jaottelu (Acromag Inc. 2005, 30)

Tunnettu	Rekisteröity	Yksityinen / Dynaaminen
0 - 1023	1024 - 49151	49152 - 65535

6.3 IP-protokolla

IP-protokollaa käytetään yhteen liitettyjen pakettikytkentäistenverkkojen tiedonvälityksessä. IP-protokolla on epäluotettava yhteydetön protokolla, jossa ei muodosteta yhteyttä lähde- ja kohdelaitteiden välille eikä varmisteta tiedon oikeellisuutta tai onnistunutta vastaanottoa. IP-protokolla sijaitsee TCP/IP-viitemallin verkkokerroksella tarjoten kuljetuskerrokselle tiedonvälityspalvelun. IP-protokollassa muodostetaan kuljetuskerrokselta vastaanotetuista segmenteistä datagrammeja, joita kutsutaan IP-paketeiksi. IP-pakettien välittämiseen lähteestä kohteeseen käytetään IP-osoitteita, joiden perusteella verkon laitteet välittävät IP-paketteja verkossa eteenpäin. Laitteiden suorittamaa IP-osoitteeseen pohjautuvaa reitinvalintaa kutsutaan reititykseksi. Jokainen IP-paketti on itsenäinenyksikkö, jonka välittämiseen ei vaikuta muiden IP-pakettien reititys. (Postel 1981a, 1 - 2.)

Välitettäessä IP-paketteja verkoissa, joissa käytettävä pakettikoko on pienempi kuin välitettävän IP-paketin alkuperäinen koko suorittaa IP-protokolla pakettien pilkkomista ja uudelleen kokoamista. IP-paketti voidaan määritellä ei-pilkottavaksi, jolloin IP-pakettia ei pilkota vaan IP-paketti hylätään. (Postel 1981a, 8.)

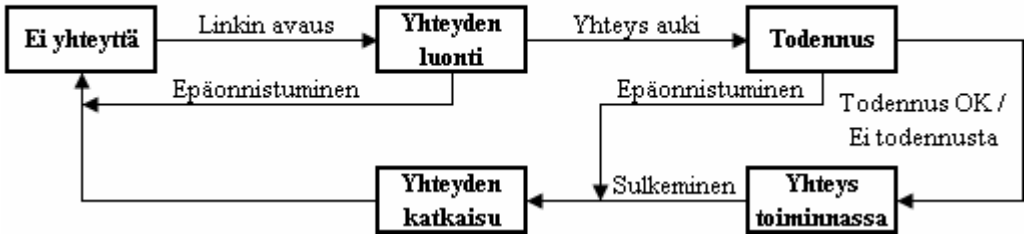
Versio	Otsikon pituus	Palvelun tyyppi	Paketin koko	Tunniste	Liput	Osion koko	Elinaika	Protokolla	Otsikon tarkiste	Lähde-osoite	Kohde-osoite	Optiot	Täyte	Tietosisältö

KUVIO 7. IP-paketti (Postel 1981a, 11)

IP-protokollan välityspalvelun toteuttamiseen käytetään neljää mekanismia: palvelun tyyppi, elinaika, optiot ja otsikon tarkiste. Palvelun tyyppillä määritellään haluttu palvelunlaatu. Palvelun tyyppi on kokoelma parametrejä, joilla määritetään IP-pakettia reititettäessä verkossa käytettävät lähetysparametrit, seuraavana käytettävä verkko tai yhdyslaite. Elinajalla määritetään IP-paketin voimassaoloaika. Reititettäessa IP-pakettia verkon laiteet pienentävät elinajan arvoa, jonka nollautuessa IP-paketti hylätään. Optiolla määritetään tarvittaessa kontrollifunktiota, kuten aikaleimat, turvallisuus ja reitityksen erikoismääreet. Otsikon tarkisteella varmistetaan IP-paketin otsikkotiedon virheettömyys. Otsikontiedon ollessa virheellinen IP-paketti hylätään. (Postel 1981a, 2 - 3.)

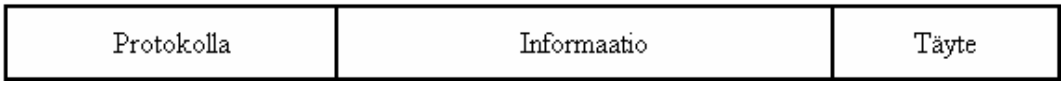
6.4 PPP-protokolla

PPP-protokolla on TCP/IP-viitemallin fyysisellä kerroksella sijaitseva yhteydellinen protokolla, jolla muodostetaan verkkolaitteiden välille kaksisuuntainen pisteestä pisteeseen -yhteys. PPP-protokolla tarjoaa verkkokerrokselle palvelun, jolla voidaan välittää samanaikaisesti verkkokerroksen eri protokollien datagrammeja. PPP-protokolla muodostuu kolmesta komponentista: kapselointi, LCP- (Link Control Protocol) ja NCP-protokolla (Network Control Protocol). Kapseloinnilla toteutetaan verkkokerroksen eri protokollien kanavointi samalle PPP-yhteydelle. LCP:tä käytetään PPP-yhteyden muodostamiseen, testaamiseen ja sulkemiseen. LCP neuvottelee kapselointi asetukset, käsittelee pakettikoon vaihtelut, tunnistaa yhteyssilmukan ja muita yleisiä konfigurointi virheitä. PPP-yhteyttä muodostettaessa voidaan tarvittaessa suorittaa osapuolten todentaminen. NCP:tä käytetään sitä vastaavan verkkokerroksen protokollan hallintaan ja asetuksien neuvottelemiseen. (Simpson 1994, 1 - 2.)



KUVIO 8. PPP-yhteyden tiladiagrammi (Simpson 1994, 6)

PPP-protokollassa verkkokerroksen datagrammi kapseloidaan PPP-kehykseen. PPP-kehys sisältää kolme kenttää, jotka ovat protokolla-, informaatio- ja täytekenttä. Protokollakentän arvolla ilmaistaan PPP-kehykseen kapseloitu verkkokerroksen protokolla, jonka datagrammi sisällytetään informaatiokenttään. Täytekenttää käytetään PPP-kehyksen pituuden vakiointiin. (Simpson 1994, 4 - 5.)

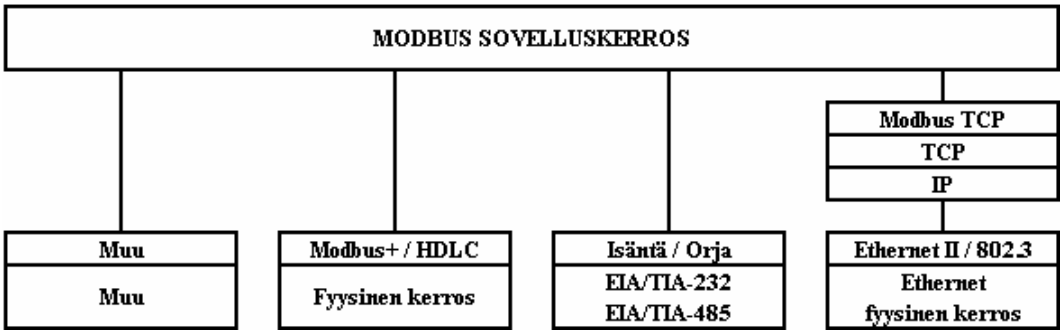


KUVIO 9. PPP-kehys (Simpson 1994, 4)

7 MODBUS-PROTOKOLLA

7.1 Yleiskuvaus

Modbus-protokolla on alun perin vuonna 1979 kehitetty avoin sovellustason sanomanvälitysprotokolla, joka toimii OSI-mallin (Open Systems Interconnection) seitsemännellä kerroksella. Modbus-protokollaa käytetään yleisesti teollisuuden tuotantoympäristöissä mm. kenttäväylien tiedonsiirtoprotokollana, ja siitä on kehittynyt ns. de facto -standardi, joka on tuettuna useiden eri laitevalmistajien sovelluksissa. Modbus-protokolla toimii haaste/vastaus-menetelmällä ja sen tarjoamat palvelut määritellään erilaisilla funktiokoodeilla. Modbus-protokollaa käyttävät laitteet toimivat joko isäntä- tai orjalaitteina, joiden sovellustason sanomanvälitys tapahtuu asiakas/palvelin-malliin pohjautuen, isäntälaitteen toimiessa asiakkaana ja orjalaiteen palvelimena. Modbus-protokolla ei ole siirtomedia riippuvainen vaan sitä voidaan käyttää tiedonvälitykseen erityyppisten väylien ja verkkojen muodostamassa verkkoarkkitehtuurissa. (Modbus-IDA 2006a, 2 - 3.)



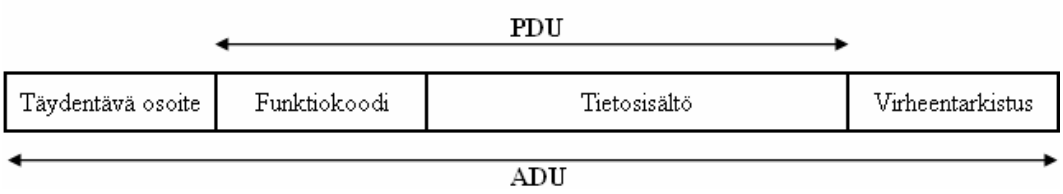
KUVIO 10. Modbus kommunikointiperiaate (Modbus-IDA 2006a, 2)

Modbus-protokolla on yleiskieli, jota käytetään erilaisten laitteiden ja ohjainten väliseen sanomanvaihtoon. Modbus-protokollassa määritetään käytettävä sanomarakenne, jonka laitteet tunnistavat ja käyttävät riippumatta sanomavälitykseen käytettävästä fyysisestä verkkoympäristöstä. Modbus-protokollassa määritetään prosessi, jota laitteet käyttävät pyytäessään pääsyä muihin laitteisiin, kuinka laitteet vastaavat toisilta laitteilta saamiinsa kyselyihin ja kuinka sanomanvälityksessä tapahtuvat virheet havaitaan ja raportoidaan. (Modicon Inc. 1996, 2.)

Modbus-protokollassa määritetään sarjaväyläisten verkkojen tiedonsiirrossa käytettävä tiedonsiirtoprotokolla, joka määrittää, kuinka laitteet tietävät oman laiteosoitteensa, tunnistavat itselleen osoitetut sanomat, päättävät millaisia toimenpiteitä suoritetaan ja kuinka vastaanotetusta sanomasta puretaan tarvittava data tai muu informaatio. Käytettäessä Modbus-protokollaa verkkoissa, joissa tiedonsiirtoon käytetään jotain muuta tiedonsiirtoprotokollaa, konvertoidaan Modbus-protokollan sanomat käytettävän tiedonsiirtoprotokollan kehys- tai pakettirakenteen sisälle. Modbus-protokollan sanomien konvertoiminen muihin tiedonsiirtoprotokolliin tehdään sovellusohjelmistokirjastojen ja ajureiden avulla. Konversiossa muutetaan Modbus-protokollan laiteosoitteet, reititystiedot ja virheentarkistus käytettävän tiedonsiirtoprotokollan mukaisiksi. Yleisimmät muista käytettävistä verkkotyypeistä ovat Ethernet ja token-passing -verkot, joille perinteisestä sarjaväyläliikenteessä käytettävästä Modbus-protokollasta on kehitetty Ethernet-verkoille Modbus TCP/IP -protokolla ja token-passing sekä MAP-verkoille (Manufacturing Automation Protocol) Modbus Plus -protokolla. (Modicon Inc. 1996, 2.)

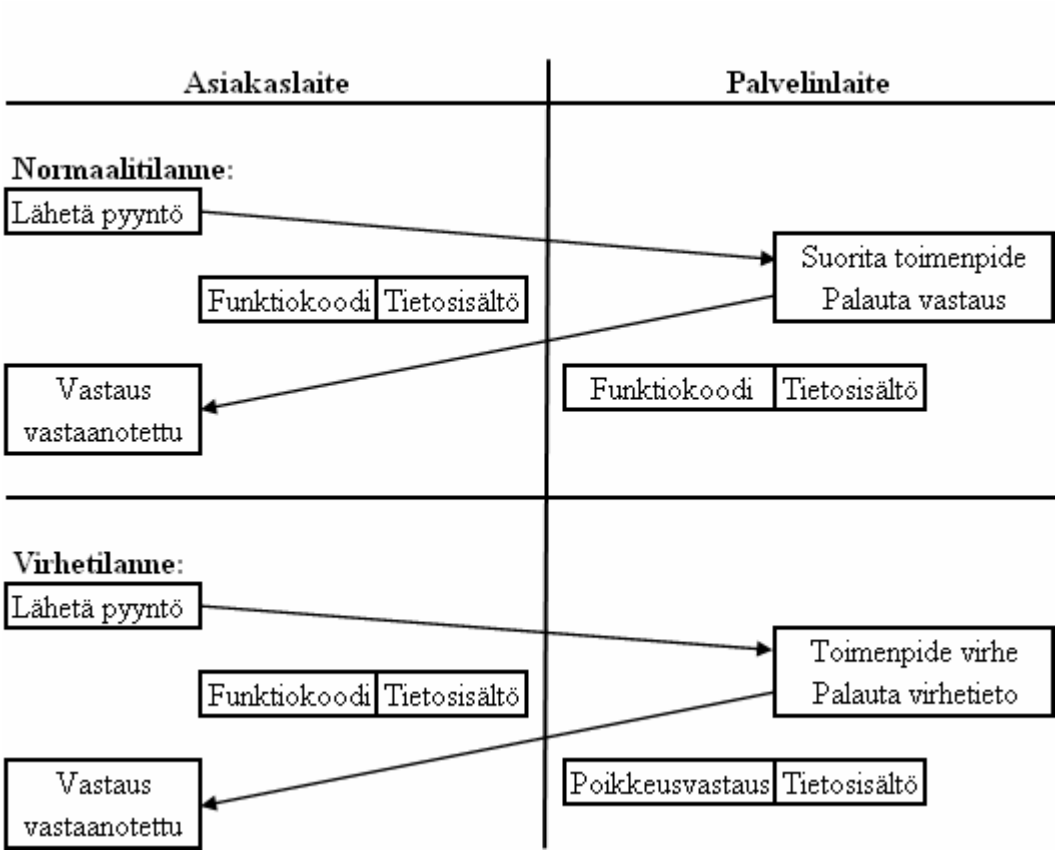
7.2 Modbus-protokollan sanomanvälitys

Modbus-protokollan sanomanvälitykseen käytetään protokollatietoyksikköä PDU (Protocol Data Unit), joka on täysin riippumaton OSI-mallin sovellustason alapuolella toimivista kerroksista. Käytettäessä Modbus-protokollaa tiedonsiirtoon väylillä tai verkoissa lisätään protokollatietoyksikköön lisäkenttiä. Lisäkentät ja protokollatietoyksikkö muodostavat sovellustietoyksikön ADU (Application Data Unit), jonka maksimipituus on 256 tavua. Protokollatietoyksikön maksimipituus määräytyy käytettävän tiedonsiirtoprotokollan osoitetietoon ja virheentarkistukseen käyttämien tavujen perusteella. (Modbus-IDA 2006a, 3 - 5.)



KUVIO 11. Modbus-protokollan kehysrakenne (Modbus-IDA 2006a, 4)

Modbus-protokollan sanomanvälitys aloitetaan aina asiakaslaiteen palvelinlaitteelle tekemällä kyselyllä. Asiakaslaite määrittelee palvelinlaitteelle lähetettävän sovellustietoyksikön sisällön, jonka funktiokoodilla määritetään vastaanottavan palvelinlaitteen suorittamat toimenpiteet. Sovellustietoyksikön tietosisältö sisältää palvelinlaitteen funktiokoodin suorittamiseen tarvitsemia tietoja, kuten käsiteltävien yksiköiden määrän, tietosisällön pituuden tavuissa tai käytettävät rekisteriosoitteet. Palvelinlaite palauttaa asiakaslaitteelle vastauksena sovellustietoyksikön, jonka funktiokoodi on sama kuin asiakaslaitteen lähettämässä kyselyssä. Asiakaslaitteen kyselyssä käytetty funktiokoodi määrittelee palautettavan sovellustietoyksikön tietosisällön. Tietosisällössä palautetaan joko asiakaslaitteen pyytämät tiedot tai tietosisältö jätetään tyhjäksi. Virhetilanteessa palvelinlaite palauttaa vastauksena sovellustietoyksikön, jonka funktiokoodina käytetään asiakaslaitteen lähettämän kyselyn funktiokoodia vastaava poikkeusvastauskoodia ja sovellustietoyksikön tietosisällössä on virhetilanteen käsittelyyn tarvittavaa tietoa. (Modbus-IDA 2006a, 4.)



KUVIO 12. Modbus sanomanvälitys (Modbus-IDA 2006a, 4 - 5)

Modbus-protokollan käyttämät funktiokoodit jaotellaan kolmeen kategoriaan, jotka ovat yleiset, käyttäjän määrittelemät ja varatut funktiokoodit. Funktiokoodi on yhden tavun pituinen, ja käytettävät arvot ovat väliltä 1 - 255, joista 128 - 255 on varattuna poikkeusvastauskoodeille. Funktiokoodin nolla arvoa ei käytetä. Määriteltäessä suoritettavaksi useita toimenpiteitä käytettävään funktiokoodiin lisätään tarvittaessa alifunktiokoodi. Alifunktiokoodien arvot ovat väliltä 1 - 255. (Modbus-IDA 2006a, 4, 10.)

TAULUKKO 5. Funktiokoodien jaottelu (Modbus-IDA 2006a, 11)

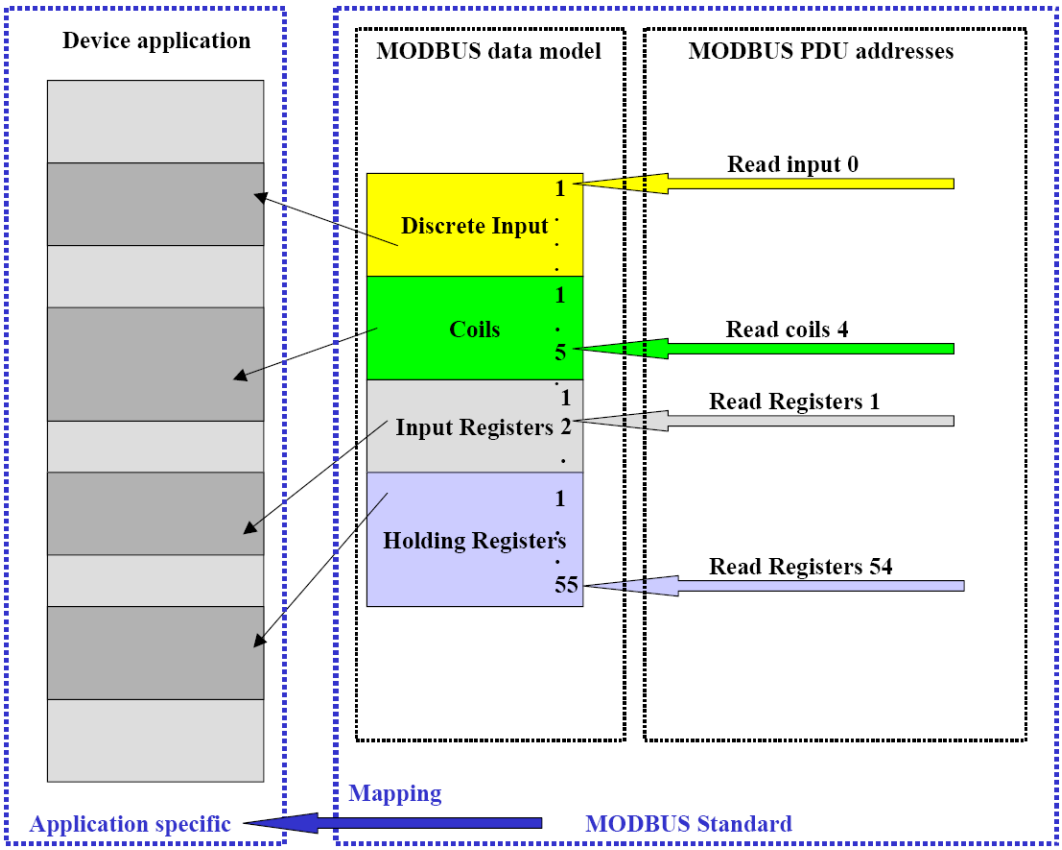
Yleinen	**Käyttäjän määrittelemä**	**Yleinen**	**Käyttäjän määrittelemä**	**Yleinen**
1 - 64	65 - 72	73 – 99	100 - 110	111 - 127

Käsiteltävät tiedot sijoitetaan laitteen sovellusmuistiin, josta tehdään linkitys tietoviittauksilla laitteen fyysisiin osoitteisiin. Protokollatietoyksikössä jokaiselle tiedolle määritetään osoite väliltä 0 - 65535. Osoitteiden ja tietoalkioiden koodaamiseen Modbus-protokollassa käytetään ns. big-Endian esitystapaa, jossa välitettävän tiedon numeerisen määrän ollessa suurempi kuin yksi bitti lähetetään ensimmäisenä eniten merkitsevä tavu. Modbus-protokollan tietomalli rakentuu neljästä lohkosta, jotka käsittävät useita elementtejä. Käytettävän tietomallin toimita perustuu neljään ensisijaiseen tauluun, jotka ovat erilliset tulot (Discretes Input), silmukka (Coils), tulorekisteri (Input Registers) ja pitorekisteri (Holding Registers)-taulut. (Modbus-IDA 2006a, 6 - 7.)

TAULUKKO 6. Ensisijaiset taulut (Modbus-IDA 2006a, 7)

Ensisijaiset taulut	**Objektityyppi**	**Luku / Kirjoitus**	**Kuvaus**
Erilliset tulot	yksi bitti	Luku	Tulojen ja lähtöjen tilatiedot (I/O)
Silmukat	yksi bitti	Luku / Kirjoitus	Sovelluksella muutettava tieto
Tulorekisterit	16-bittinen sana	Luku	Tulojen ja lähtöjen tilatiedot (I/O)
Pitorekisterit	16-bittinen sana	Luku / kirjoitus	Sovelluksella muutettava tieto

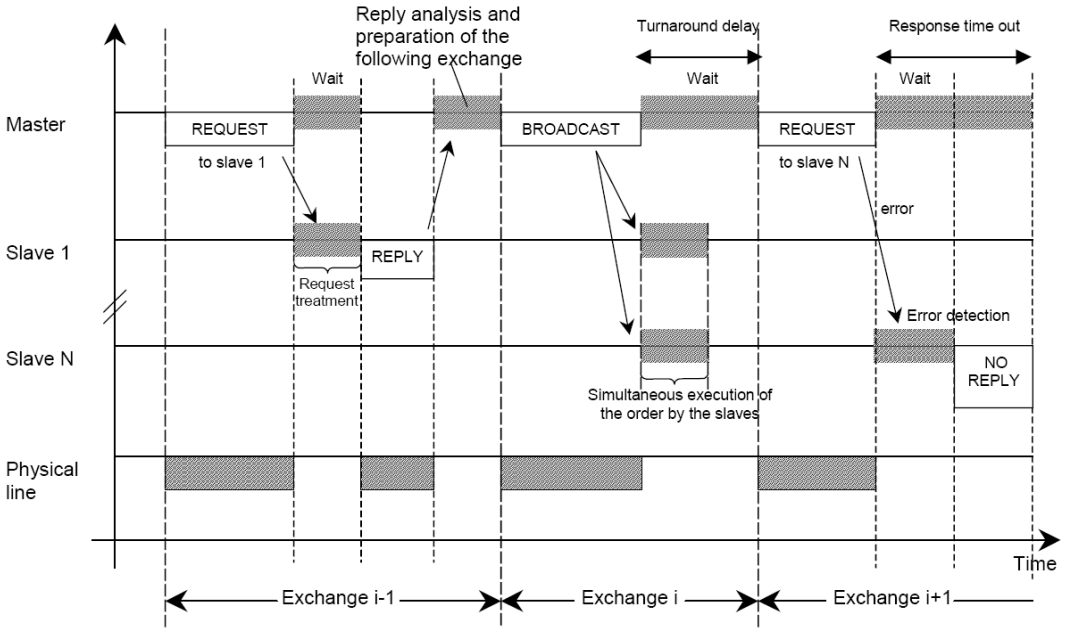
Yhteen ensisijaiseen tauluun voidaan määrittää 65536 erillistä tietoalkiota. Sanomanvälityksessä käytettävä funktiokoodi määrittelee, kuinka monta peräkkäistä tietoalkiota luku- tai kirjoitusoperaatiossa käsitellään. Vaikka Modbus-protokollassa käytetään erillisiä tauluja, ei tulojen ja lähtöjen eikä bitti- ja sana-osoitettavien tietoalkioiden välille ole määritetty rajoja. Tauluja voidaan käsitellä joko erillisinä lohkoina tai yhtenä yhtenäisenä lohkona. Käsiteltäessä tauluja erillisinä lohkoina on kunkin lohkon sisältämiin tietoalkioihin pääsy vain tietyillä määritellyillä funktioilla. Käytettäessä yhtä lohkoa on useilla eri funktiolla pääsy samoihin tietoalkioihin. Modbus-protokollan tietomallin yhdistäminen laitteen käyttämään sovellukseen ja käytettävä lohkomalli ovat täysin laitevalmistajakohtaisia. (Modbus-IDA 2006a, 6 - 8.)



KUVIO 13. Modbus-osoitusmalli (Modbus-IDA 2006a, 8)

7.3 Modbus-protokolla ja sarjaväylät

Modbus-protokollassa määritetään OSI-mallin sovellustason sanomanvälityksen lisäksi sarjaväyläliikenteen tiedonsiirtoprotokolla, joka toimii OSI-mallin toisella kerroksella. Tiedonsiirtoprotokollassa käytetään isäntä/orja-tekniikkaa, jossa yksi verkon laitteista toimii isäntälaitteena, muiden laitteiden toimiessa orjalaitteina. Isäntälaite hallinnoi verkkoa ja alustaa kaikki verkon tapahtumat. Orjalaitteet vain käsittelevät isäntälaitteelta vastaanotettuja sanomia, eivätkä ne alusta verkon tapahtumia. Vastaanotettujen sanomien funktiokoodien ja tietosisällön perusteella orjalaitteet suorittavat halutut toimenpiteet ja palauttavat vastaussanoman isäntälaitteelle. Vastaussanoma on kuittaus pyydetyn toimenpiteen suorittamisesta, kysytyn tietosisällön palautus isäntälaitteelle, virheilmoitus pyydetyn toimenpiteen suorittamisen epäonnistumisesta tai tiedonsiirrossa tapahtuneesta virheestä. Isäntälaite lähettää sanoman joko yksittäiselle orjalaitteelle tai levityssanoman kaikille orjalaitteille. Orjalaite palauttaa vastaussanoman itselleen osoitettuihin sanomiin. Vastaanotettuun levityssanomaan orjalaite ei palauta vastaussanomaa. Orjalaitteet eivät myöskään välitä sanomia toisilleen. Isäntä- ja orjalaitteiden sanomanvälityksessä käytetään kahta tiedonsiirtotapaa, jotka ovat ASCII- (American Standard Code for Information Interchange) ja RTU-tiedonsiirtotavat. Kaikkien verkon laitteiden on käyttävä samaa tiedonsiirtotapaa. (Modicon Inc. 1996, 4 - 6.)



KUVIO 14. Isäntä- ja orjalaitteiden sanomanvälitys (Modbus-IDA 2006c, 11)

OSI-mallin fyysisellä kerroksella kaikki samassa verkossa olevat Modbus-protokollaa käyttävät laitteet on kytketty samaan sarjaliikenneväylään joko suoraan tai modeemin välityksellä. Laitteiden sarjaliikenneväylän liitäntänä käytetään erilaisia fyysisiä liitäntöjä, joista yleisin on TIA/EIA-485-standardin (Telecommunications Industry Association / Electronic Industries Associates) mukainen parijohdin liitäntä, lisäoptiona voidaan käyttää myös TIA/EIA-485-standardin nelijohdinversiota. Tiedonsiirtoyhteyden etäisyyden ollessa lyhyt ja vain kahdenpisteen välinen voidaan fyysisenä liitäntänä käyttää myös TIA/EIA-232-E-standardin liitäntää. Käytettävän fyysisen liitännän standardissa määritellään käytettävä liitintyyppi, nastajärjestys, kaapelointi, signaalitasot, pariteettivarmistus ja päätelaitteen siirtonopeus. (Modbus-IDA 2006c, 5.)

TAULUKKO 7. Modbus sarjaväyläliikenneparametrit (Modbus-IDA 2006c, 34)

	Perus		**Yleinen**	**Oletusarvo**
Osoitteistus	Orjalaite: Konfiguroitava osoite 1 - 247	Isäntälaite: Osoitteiden 1 - 247 osoitus	Sama kuin perus	-
Levitys-sanoma	Kyllä		Kyllä	-
Päätelaitteen siirtonopeus (b/s)	9600 (suositellaan myös 19200)		9600 tai 19200 (+ muita konfiguroitavia nopeuksia)	19200 (jos tuettu, muutoin 9600)
Pariteetti-varmistus	Parillinen		Parillinen, pariton tai ei varmistusta	Parillinen
Tiedonsiirto-tapa	RTU		RTU tai ASCII	RTU
Fyysinen liitäntä	TIA/EIA-485 parijohdin tai TIA/EIA-232-E		TIA/EIA-485 pari/nelijohdin tai TIA/EIA-232-E	TIA/EIA-485 parijohdin
Liitintyyppi	RJ-45 (suositus)		-	-

7.3.1 Modbus ASCII -tiedonsiirtotapa

Modbus-protokollan ASCII-tiedonsiirtotapaa käytettäessä lähetetään jokainen 8-bittinen tavu kahtena ASCII-merkkinä. Lähetettävän sanoman merkkien välinen sallittu maksimi aikaväli on yksi sekunti. Sallitun aikavälin ylittyessä vastaanottava laite olettaa tiedonsiirrossa tapahtuneen virheen ja hylkää sanoman. ASCII-tiedonsiirtotavassa kehyksen alku merkitään kaksoispisteellä (:) ja kehyksen päättyminen rivin-vaihdolla (CRLF). Verkon laitteet tarkkailevat sarjaväylän liikennettä ja havaitessaan kaksoispiste-merkin laitteet käsittelevät kehyksessä seuraavana olevan osoitekentän. Osoitekentän sisältämän osoitteen perusteella laite päättelee, onko kyseinen sanoma osoitettu laitteelle. Osoitekentän sisältäessä laitteen oman osoitteen tai levityssanomaosoitteen laite käsittelee sanoman, muutoin laite hylkää sanoman. (Modicon Inc. 1996, 6 - 8.)

Alku	Osoite	Funktiokoodi	Tietosisältö	LRC-tarkiste	Loppu
1 merkki :	2 merkkiä	2 merkkiä	n merkkiä	2 merkkiä	2 merkkiä CRLF

KUVIO 15. Modbus ASCII -kehysrakenne (Modicon Inc. 1996, 8)

ASCII-tiedonsiirtotavassa sanoman kehysrakenteeseen lisätään kahden ASCII-merkin pituinen virheentarkistuskenttä. Virheentarkistukseen käytetään LRC-menetelmää (Longitudinal Redundancy Check). Ennen ASCII-koodausta lähettävä laite laskee aloitus ja lopetusmerkkien välisistä binaariarvoista LRC-tarkisteen, joka on yhden tavun pituinen 8-bittinen binaariarvo. Laskettu LRC-tarkiste koodataan kahdeksi ASCII-merkiksi, jotka sisällytetään kehyksen virheentarkistuskenttään. Sanoman vastaanottava laite suorittavaa vastaavan LRC-tarkisteen laskennan sanoman sisällöstä ja vertaa saamaansa arvoa virheentarkistuskentän LRC-tarkisteen arvoon. Vastaanotetun sanoman LRC-tarkisteen ja sanoman sisällöstä lasketun LRC-tarkisteen erotessa toisistaan todetaan tiedonsiirrossa tapahtuneen virheen ja sanoma hylätään. (Modbus-IDA 2006c, 18.)

7.3.2 Modbus RTU -tiedonsiirtotapa

Modbus-protokollan RTU-tiedonsiirtotapaa käytettäessä lähetetään jokainen 8-bittinen tavu kahtena 4-bittisenä heksadesimaali-merkkinä. Sanomat lähetetään jatkuvana virtana eikä lähetettävien merkkien aikaväli saa ylittää 1,5 merkinaikaa. Merkinaika sekunneissa määräytyy käytettävän päätelaitteen siirtonopeuden perusteella. Sallitun aikavälin ylittyessä vastaanottava laite olettaa tiedonsiirrossa tapahtuneen virheen ja hylkää sanoman. Sanoman hylkäämisen jälkeen laite olettaa seuraavan vastaanotetun tavun olevan uuden sanoman osoitekenttä. RTU-tiedonsiirtotavassa sanomat erotetaan toisistaan vähintään 3,5 merkinajan pituisilla tyhjillä aikaväleillä, jolloin ei tapahdu lähetystä. Varsinaisen sanoman lähetys alkaa osoitekentällä. Verkon laitteet tarkkailevat sarjaväylän liikennettä ja vastaanottaessaan sanoman laitteet käsittelevät sanoman osoitekentän. Osoitekentän sisältämän osoitteen perusteella laite päättelee, onko kyseinen sanoma osoitettu laitteelle. Osoitekentän sisältäessä laitteen oman osoitteen tai levityssanomaosoitteen laite käsittelee sanoman, muutoin laite hylkää sanoman. Vastaanotettaessa uusi sanoma ennen kuin tyhjä aikaväli on kulunut loppuun, tulkitaan sanoma virheellisesti kuuluvaksi edelliseen vastaanotettuun sanomaan. (Modicon Inc. 1996, 7 - 9.)

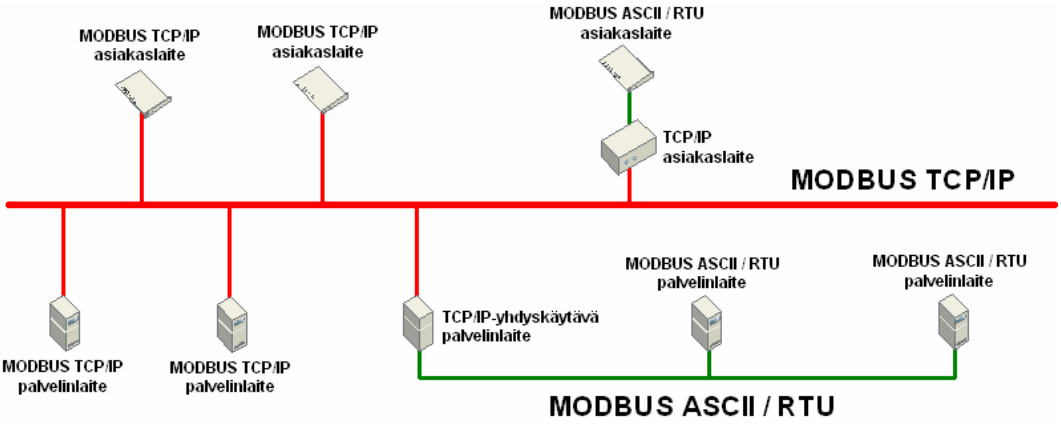
Alku	Osoite	Funktiokoodi	Tietosisältö	CRC-tarkiste	Loppu
≥ 3,5 x merkinaika	8 bittiä	8 bittiä	n x 8 bittiä	16 bittiä	≥ 3,5 x merkinaika

KUVIO 16. Modbus RTU -kehysrakenne (Modicon Inc. 1996, 9)

RTU-tiedonsiirtotavassa sanoman kehysrakenteeseen lisätään 16-bitin pituinen virheen tarkistuskenttä. Virheentarkistukseen käytetään CRC-menetelmää (Cyclical Redundancy Check). Ennen sanoman lähetystä lähettävä laite laskee koko sanoman sisällöstä CRC-tarkisteen, joka sijoitetaan virheentarkistuskenttään. Sanoman vastaanottava laite suorittavaa vastaavan CRC-tarkisteen laskennan sanoman sisällöstä ja vertaa saamaansa arvoa virheentarkistuskentän CRC-tarkisteen arvoon. Vastaanotetun sanoman CRC-tarkisteen ja sanoman sisällöstä lasketun CRC-tarkisteen erotessa toisistaan todetaan tiedonsiirrossa tapahtuneen virheen ja sanoma hylätään. (Modbus-IDA 2006c, 14.)

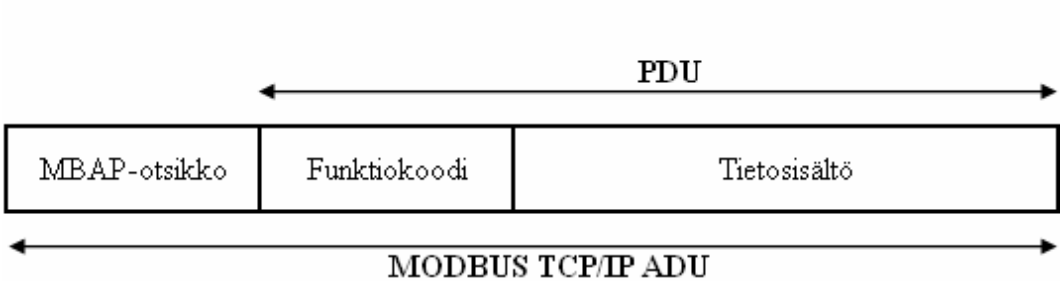
7.4 Modbus TCP/IP -protokolla

Modbus TCP/IP -protokollaa käytetään Modbus-protokollan sanomanvälityksen tiedonsiirtoprotokollana Ethernet TCP/IP -verkoissa. Modbus TCP/IP -protokollan toiminta pohjautuu asiakas/palvelin-malliin. Asiakas/palvelin-mallin tiedonvälityksessä käytetään neljää sanomatyyppiä: pyyntö-, vahvistus-, osoitus- ja vastaussanoma. Asiakaslaite alustaa verkon tapahtuman pyyntösanomalla, jonka palvelinlaite vastaanottaa ja käsittelee osoitussanomana. Vastaanotettuun pyyntösanomaan palvelinlaite palauttaa asiakaslaitteelle vastaussanoman, jonka asiakaslaite käsittelee vahvistussanomana. Modbus TCP/IP -protokollan tiedonvälitysarkkitehtuurissa käytetään asiakas- ja palvelinlaitteiden lisäksi yhteyslaitteita, joiden välityksellä yhdistetään TCP/IP-verkko sarjaväyläliikenteisiin aliverkkoihin. Verkkojen välisinä yhteyslaitteina käytetään silta-, reititin- ja yhdyskäytävälaitteita. (Modbus-IDA 2006b, 2 - 3.)



KUVIO 17. Modbus TCP/IP -verkkoarkkitehtuuri (Modbus-IDA 2006b, 4)

Modbus TCP/IP -verkoissa Modbus-protokollan sanomat kapseloidaan lisäämällä Modbus-protokollatietoyksikköön MBAP-otsikko (ModBus Application Protocol). MBAP-otsikko ja protokollatietoyksikkö muodostavat yhdessä Modbus TCP/IP -sovellustietoyksikön, jonka TCP/IP tunnistaa ja käsittelee MBAP-otsikon sisältämien tietojen avulla. (Modbus-IDA 2006b, 4.)



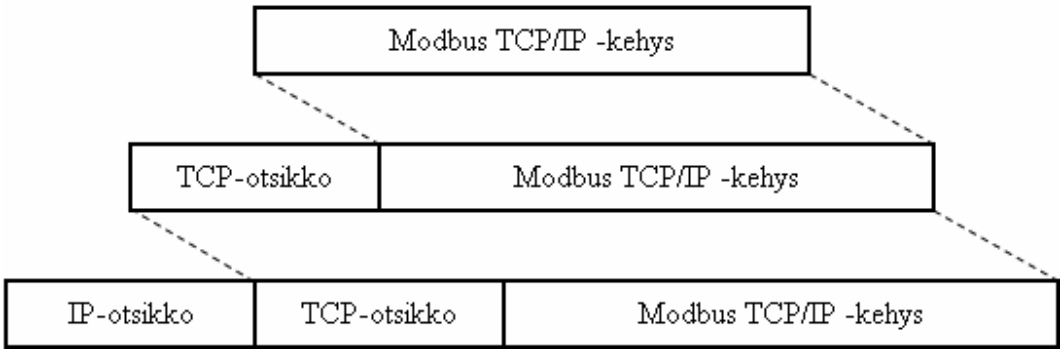
KUVIO 18. Modbus TCP/IP -kehysrakenne (Modbus-IDA 2006b, 4)

MBAP-otsikko sisältää neljä kenttää, jotka ovat tapahtuma-, protokolla- yksikkötunniste ja pituuskenttä. Tapahtumatunnistekenttää käytetään Modbus-protokollan sanomanvälitystapahtuman yksilöimiseen. Asiakaslaite asettaa tapahtumatunnistekentän arvon lähetettävän pyyntösanoman otsikkotietoon, josta palvelinlaite lukee kentän arvon ja asettaa saman arvon asiakaslaitteelle palautettavan vastaussanoman otsikkotietoon. Protokollatunnistekenttää käytetään järjestelmän sisäiseen kanavointiin. Modbus-protokollassa protokollatunnistekentän arvoksi asetetaan 0. Yksikkötunnistekenttää käytetään järjestelmän sisäiseen reititykseen, kentän arvon yksilöidessä asiakaslaitteen. Tyypillisesti yksikkötunnistetta käytetään yhteyslaitteen välityksellä TCP/IP- ja sarjaväyläliikenteisten verkkojen välillä tapahtuvassa tiedonsiirrossa. Protokolla- ja yksikkötunnistekenttien arvot asetetaan samalla tavoin kuin tapahtumatunnistekenttä arvo. Pituuskentän arvo on pituuskentän jälkeisten kenttien tavumäärä, jonka asiakas- ja palvelinlaitteet laskevat ja asettavat ennen sanoman lähettämistä. Pituuskentän arvon avulla sanoman vastaanottaja tunnistaa sanoman rajat, vaikka sanoma olisi pilkottu tiedonsiirrossa useisiin paketteihin. (Modbus-IDA 2006b, 5 - 6.)

Tapahtumatunniste	Protokollatunniste	Pituus	Yksikkötunniste
16 bittiä	16 bittiä	16 bittiä	8 bittiä

KUVIO 19. MBAP-otsikko (Modbus-IDA 2006b, 5)

Modbus TCP/IP -protokolla käyttää TCP/IP-protokollaperhettä Modbus-sanomien välittämiseen laitteiden välillä. Modbus TCP/IP -kehys kapseloidaan sellaisenaan TCP/IP-kehyksen sisälle. Kapseloitaessa Modbus-protokollan kehys TCP/IP-kehykseen sijoitetaan Modbus-protokollan kehyksen lisäosoitekentän sisältämä osoitetieto MBAP-otsikon yksikkötunnistekenttään ja poistetaan Modbus-kehyksen virheentarkistuskenttä. (Acromag Inc. 2005, 4.)



KUVIO 20. Modbus TCP/IP -kehyksen kapselointi (Acromag Inc. 2005, 27)

Modbus TCP/IP -sanomien välittämiseksi Modbus TCP/IP -protokollaa käyttävien laitteiden välille on muodostettava TCP-yhteys. TCP-yhteys muodostetaan asiakas/palvelin-mallilla. Palvelimena toimiva orjalaite kuuntelee TCP-protokollan porttia 502, joka on varattu Modbus sovelluksien käyttöön. Asiakkaana toimiva isäntälaite avaa yhteyden palvelinlaitteen porttiin 502. TCP-yhteyden muodostamisen jälkeen voidaan TCP-yhteydellä lähettää tietoa kumpaankin suuntaan laitteiden välillä. Isäntä- ja orjalaitteiden välille voidaan muodostaa useita samanaikaisia TCP/IP-yhteyksiä. Tiedonsiirtotapahtumiin liitetään yhteystunniste CID (Connection IDentifier), joka yksilöi käytettävän TCP/IP-yhteyden. Lähetettäessä tietoa TCP/IP-yhteydellä kumpaankin suuntaan käytetään kahta yhteystunnistetta. Modbus TCP/IP -protokollan sanomanvälitys yhteydet ovat kahden laitteen välisiä päästä päähän yhteyksiä, joten Modbus TCP/IP -protokollan sanomanvälityksessä käytetään vain unicast-tyyppisiä sanomia. (Acromag Inc. 2005, 27.)

Modbus TCP/IP -protokollan käyttämien TCP-yhteyksien hallinta voidaan toteuttaa ohjelmallisesti sovellustasolla tai automaattisesti TCP-yhteyksien hallintamoduulilla. TCP-yhteyksien hallinta sovellustasolla tarjoaa enemmän joustavuutta sovellusohjelmoinnissa, mutta edellyttää TCP/IP-protokollaperheen toiminnan hyvää tuntemusta. Yleensä TCP-yhteyksien hallinta toteutetaan automaattisesti, jolloin TCP-yhteyksien muodostaminen ja hallinta on täysin piilotettu sovellustasolta. Sovellustasolla ainoastaan lähetetään ja vastaanotetaan Modbus-sanomia. (Modbus-IDA 2006b, 10.)

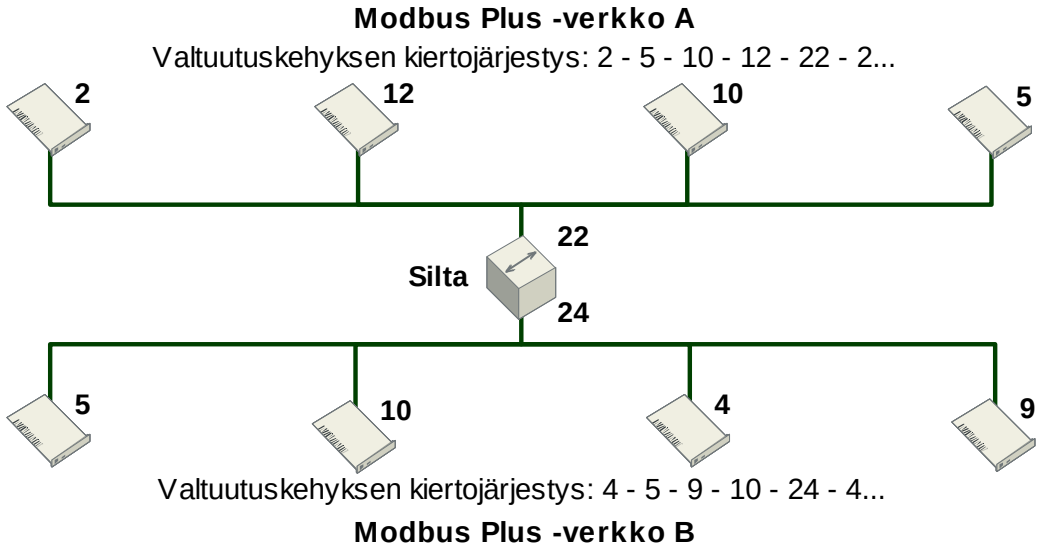
Modbus TCP/IP -protokollan toteutuksen suositukset:

- Ilman selvää käyttäjävaatimusta käytetään automaattista TCP-yhteyksien hallintaa.
- TCP-yhteys etälaitteeseen pidetään avoimena. TCP-yhteyttä ei avata ja suljeta erikseen jokaista Modbus TCP/IP -tapahtumaa varten.
- TCP-yhteyksiä avataan mahdollisimman vähän. Yksi TCP-yhteys yhdelle sovellukselle.
- TCP-yhteydellä voi olla samanaikaisesti aktiivisena useita Modbus-tapahtumia.
- Kaksisuuntaisessa tiedonvälityksessä avataan erilliset TCP-yhteydet asiakas- ja palvelinlaitteiden tietovirroille.
- Yhdessä TCP-kehyksessä kuljetetaan vain yksi Modbus-sovellustietoyksikkö.

(Modbus-IDA 2006b, 10.)

7.5 Modbus Plus -protokolla

Modbus Plus -protokolla on teollisuuden lähiverkoissa käytettävä protokolla, jonka tiedonvälitys toteutetaan valtuudenvälitys-menetelmällä (token-passing). Modbus Plus -verkon laitteet muodostavat vertaisverkon, jossa valtuutuskehys (token) välitetään loogisessa renkaassa laitteelta laiteella. Modbus Plus -protokollaa käyttävät laitteet välittävät tietoa toisilleen vertaisverkko-tekniikalla, jolloin verkon laite voi toimia samanaikaisesti isäntä- ja orjalaitteena. Sanomatasolla käytetään kuitenkin Modbus-protokollan isäntä- ja orjalaite periaatetta. Verkon laitteen toimiessa samanaikaisesti isäntä- ja orjalaitteena on laitteen muodostettava kaksi erillistä sanomanvälitys tapahtumaa, joista toisessa laite toimii isäntälaitteena ja toisessa orjalaitteena. Modbus Plus -protokolla on suljettu protokolla, jonka käyttäminen edellyttää lisenssiä. (Modicon Inc. 1996, 4 - 5.)

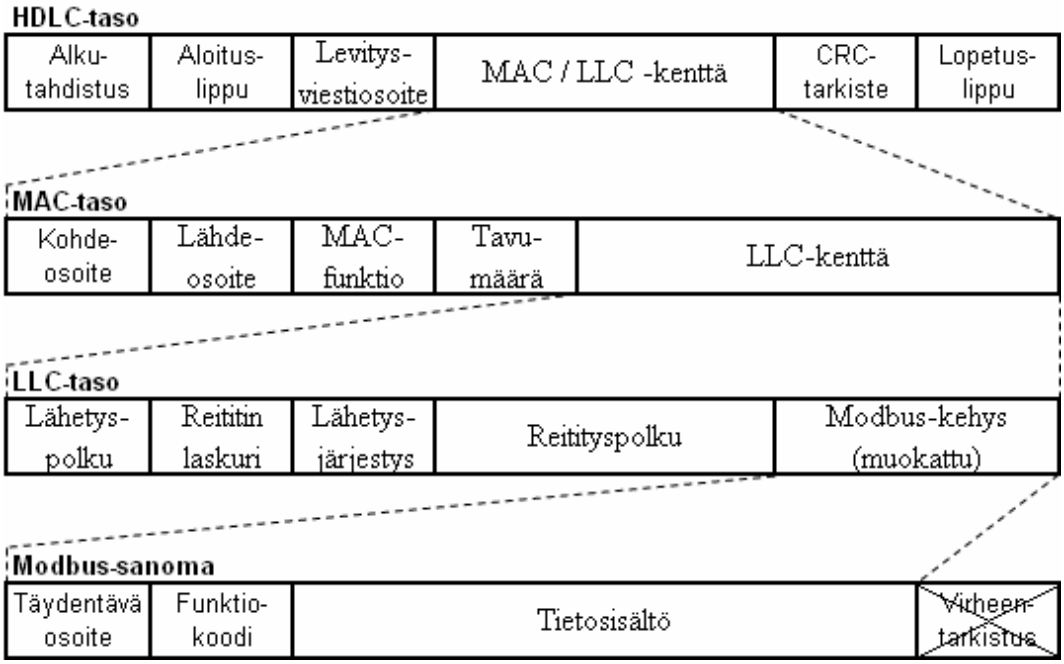


KUVIO 21. Modbus Plus -verkkoarkkitehtuuri (Schneider Electric 2004, 16)

Modbus Plus -verkon laitteille määritetään osoite väliltä 1 - 64. Osoitteen avulla laitteet tunnistetaan ja määritetään valtuutuskehyksen kiertojärjestys verkossa. Valtuutuskehyksen kiertojärjestys on pienimmästä osoitteesta suurimpaan osoitteeseen. Laitteen fyysinen sijainti ei vaikuta osoitteistukseen. Modbus Plus -verkkoja voidaan yhdistää toisiinsa siltalaitteilla. Jokaisella Modbus Plus -verkolla on oma erillinen valtuutuskehyksen kierto eivätkä verkkoja yhdistävät siltalaitteet välitä valtuutuskehystä verkosta toiseen. (Schneider Electric 2004, 16.)

Alustettaessa Modbus Plus -verkko sen laitteet muodostavat itselleen kaikki verkon laitteet sisältävän taulun, minkä jälkeen käynnistetään valtuutuskehyksen kierto. Vastaanottaessaan laitteelle itselleen osoitetun valtuutuskehyksen käynnistää laite Modbus-sanoman välityksen. Lähetettyään kaikki Modbus-sanomat laite välittää valtuutuskehyksen kiertojärjestyksessä seuraavalle laitteelle. Levityssanomat liitetään lähetettävään valtuutuskehykseen, josta verkon laitteet lukevat levityssanoman. Modbus Plus -verkon laitteet käsittelevät valtuutuskehykset, vaikka valtuutuskehys ei olisi osoitettu laitteelle itselleen.
(Schneider Electric 2004, 28 - 29.)

Modbus Plus -protokolla käyttää HDLC-protokollaa (High-Level Data Link Control) Modbus-sanomien välittämiseen. Modbus-protokollan kehys kapseloidaan HDLC-protokollan LLC-kentän (Logical Link Control) sisälle. Modbus-protokollan kehyksen osoitekenttä konvertoidaan Modbus Plus -protokollan reititys-polkukenttään ja virheentarkistuskenttä poistetaan. Virheentarkistukseen käytetään HDLC-protokollan virheentarkistuskenttää. (Modicon Inc. 1996, 20 - 21.)



KUVIO 22. Modbus Plus -kehyksen kapselointi (Modicon Inc. 1996, 21)

8 GPRS-PALVELU

8.1 Yleiskuvaus

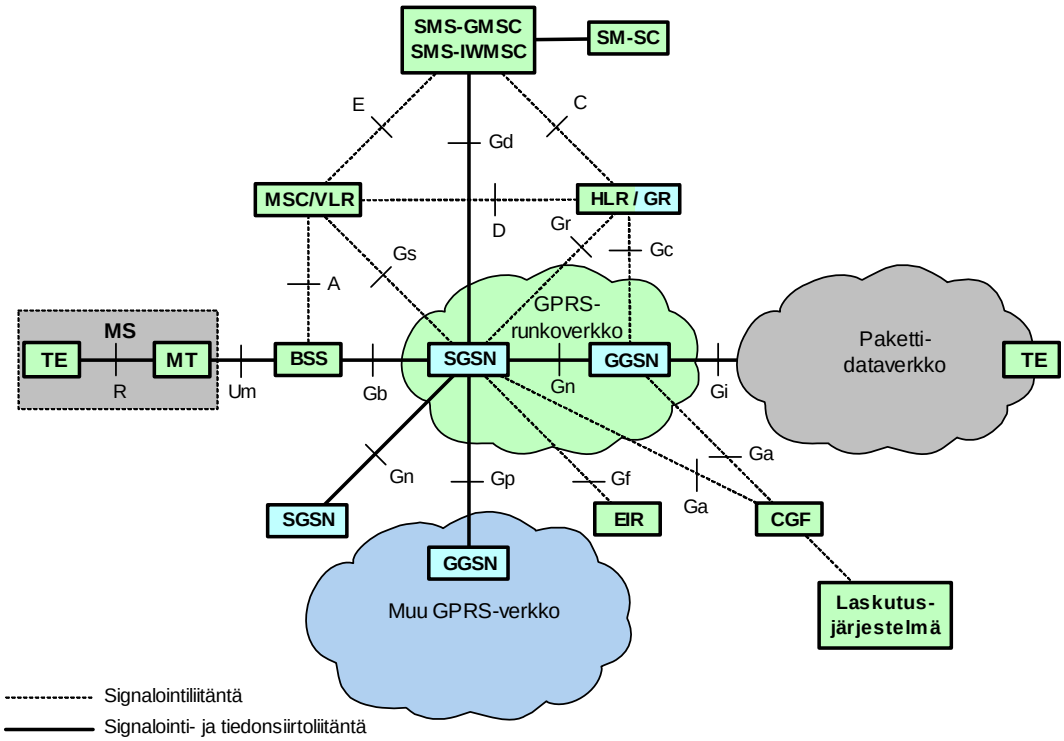
GPRS-palvelulla toteutetaan pakettikytkentäinen tiedonsiirto piirikytkentäisessä GSM-verkossa. GPRS-järjestelmässä radio- ja verkkoalijärjestelmät erotetaan toisistaan, jolloin verkkoalijärjestelmää voidaan käyttää muiden radioverkkotekniikoiden kanssa sekä verkon ja radiorajapinnan resurssien käyttöä voidaan optimoida. GPRS-palvelu ei vaadi muutoksia GSM-verkon matkapuhelinkeskuksien MSC (Mobile services Switching Center) perusrakenteeseen. (ETSI 2000c, 13.)

GPRS-järjestelmässä GSM-verkkoon määritetään uudet GPRS-radiokanavat, joiden jakaminen on tehty joustavaksi. Yhteen TDMA-kehykseen (Time Division Multiple Access) määritetään 1 - 8 radiorajapinnan aikaväliä, jotka jaetaan verkon aktiivisille käyttäjille. Uplink- ja downlink-aikavälit voidaan jakaa erikseen. Radiorajapinnan resursseja jaetaan kiinteästi tai dynaamisesti puhe- ja tiedonsiirtopalveluille, verkon kuormituksen sekä muiden operaattorin asettamien määreiden perusteella. GPRS-järjestelmän radiokanavilla käytetään eri kanavakoodausluokkia, jotka vaikuttavat toteutuvaan tiedonsiirtonopeuteen. GPRS-järjestelmän tiedonsiirtonopeus yhdelle käyttäjälle on välillä 9 - 150 kb/s riippuen käytettävästä kanavakoodausluokasta. Tiedonsiirron lisäksi GPRS-radiokanavia voidaan käyttää SMS-viestien välittämiseen. (ETSI 2000c, 13.)

GPRS-palvelu tukee sovelluksia, jotka perustuvat standardoituihin dataprotokolliin. GPRS-spesifikaatioissa määritetään yhteen liittäminen IP- ja X.25-verkkoihin. GPRS-palvelu on suunniteltu vaihtelevaan ja purskeiseen tiedonsiirtoon sekä satunnaiseen suurten tietomäärien siirtämiseen. GPRS-palvelussa käytetään useita palvelunlaatuprofiileja. GPRS-palvelussa ei käytetä erillistä yhteydenmuodostusta, kuten piirikytkentäisissä yhteyksissä, vaan nopeaa merkinantoa pakettitiedonsiirron aloittamiseksi. Merkinanto on kestoltaan tyypillisesti 0,5 - 1 sekuntia. (ETSI 2000c, 13.)

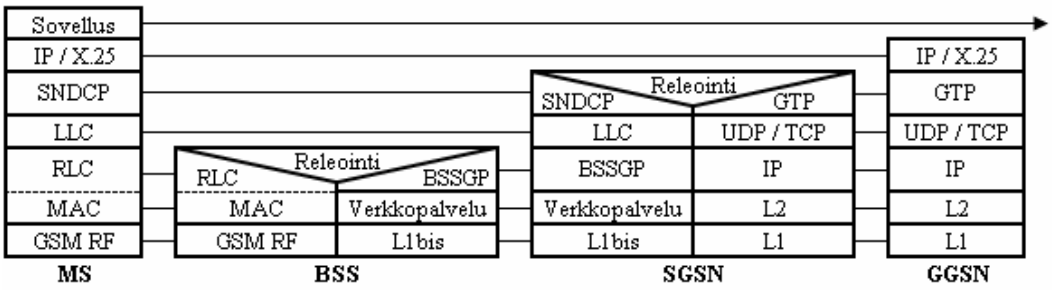
8.2 Verkkoarkkitehtuuri ja -elementit

GPRS-palvelussa GSM-verkkoarkkitehtuuriin lisätään kaksi verkkoelementtiä: GPRS-operointisolmu SGSN (Serving GPRS Support Node) ja -yhdyskäytäväsolmu GGSN (Gateway GPRS Support Node). SGSN sijaitsee samalla verkkohierarkian tasolla kuin MSC. SGSN:n tehtävänä on seurata yksittäisten mobiililaitteiden MS (Mobile Station) sijaintia, suorittaa turvallisuuteen liittyviä toimintoja sekä huolehtia pääsynhallinnasta. SGSN yhdistetään tukiasemajärjestelmään BSS (Base Station System) Frame Relay -yhteydellä. GGSN tarjoaa yhteen liitännän ulkoisiin pakettikytkentäisiin verkkoihin. SGSN ja GGSN ovat yhteydessä toisiinsa IP-pohjaisen GPRS-runkoverkon välityksellä. Kotirekisteriin HLR (Home Location Register) lisätään GPRS-tilaaja- ja reititystiedot sisältävä GPRS-rekisteri GR (GPRS Register). Lyhytsanoman kauttakulku- SMS-GMSC (Gateway MSC) ja yhteensovituskeskus SMS-IWMSC (InterWorking MSC) päivitetään tukemaan SMS-viestien välittämistä SGSN kautta. MSC/VLR (Visitor Location Register) voidaan päivittää GPRS- ja GSM-palveluiden koordinoinnin ja toiminnallisuuden tehostamiseksi, jolloin voidaan mm. puheluita kutsua SGSN kautta ja yhdistää GPRS- ja GSM-sijaintitieto päivitykset. (ETSI 2000c, 13.)



KUVIO 23. GPRS-verkon looginen rakenne (ETSI 2000c, 14, 19)

Toiminnallisuuksiltaan GPRS-verkko jaetaan kahteen tasoon, jotka ovat tiedonsiirto- ja signalointitasot. Tiedonsiirtotaso muodostuu kerroksittaisesta protokollarakenteesta, jossa eri protokollakerrokset suorittavat itsenäisesti käyttäjän tiedonsiirtoon liittyviä toimintoja. Signalointitaso muodostuu protokollista, joilla hallinnoidaan ja tuetaan tiedonsiirtotason toimintoja. (ETSI 2000c, 22 - 23.)



KUVIO 24. GPRS-verkon tiedonsiirtotason kerrosmalli (ETSI 2000c, 22)

GPRS-palvelun turvallisuus toiminnallisuudet ovat vastaavanlaiset kuin GSM-verkon. Todentaminen ja salausasetukset suoritetaan SGSN:ssä samoihin algoritmeihin, avaimiin ja kriteereihin pohjautuen kuin GSM-verkossa. GPRS-palvelun käyttämä salausalgoritmi on optimoitu pakettitiedonsiirrolle. (ETSI 2000c, 13.)

TAULUKKO 8. Verkkoelementtien toiminnot (ETSI 2000c, 21)

	MS	BSS	SGSN	GGSN	HLR
Verkkoon pääsyn hallinta:					
Rekisteröinti					X
Todennus ja valtuutus	X		X		X
Pääsynohjaus	X	X	X		
Viestin seuranta					
Pakettien päätesovitus	X				
Laskutustiedon keräys			X	X	
Pakettien reititys ja siirto:					
Välitys	X	X	X	X	
Reititys	X	X	X	X	
Osoitteenmuunnos ja osoitteistus	X		X	X	
Kapselointi	X		X	X	
Tunnelointi			X	X	
Pakkaus	X		X		
Salaus	X		X		X
Liikkuvuuden hallinta:	X		X	X	X
Loogisen yhteyden hallinta:					
Loogisen yhteyden muodostus	X		X		
Loogisen yhteyden ylläpito	X		X		
Loogisen yhteyden vapautus	X		X		
Radioresurssien hallinta:					
Um hallinta	X	X			
Solunvalinta	X	X			
Um-Tranx	X	X			
Pohn hallinta		X	X		

8.2.1 Mobiililaite (MS)

Mobiililaiteella käsitetään fyysinen laitteisto, jolla käytetään GSM-verkon tarjoamia palveluita. Mobiililaite koostuu mobiililaitteistosta ME (Mobile Equipment) ja tilaajamoduulista SIM (Subscriber Identity Module). Mobiililaitteisto jaetaan toiminnallisuuksiltaan kahteen osaan, jotka ovat mobiilipäätelaite MT (Mobile Termination) ja päätelaitteisto TE (Terminal Equipment). Mobiililaitteissa käytetään eri tunnisteita, joista tärkeimmät ovat kansainvälinen mobiililaitetunnus IMEI (International Mobile Equipment Identity) ja kansainvälinen mobiilitilaajatunnus IMSI (International Mobile Subscriber Identity) (ETSI 2000a, 15; ETSI 2001a, 14.)

GPRS-palvelua tukevat mobiililaitteet jaetaan toiminnoiltaan kolmeen luokkaan:

- Luokka A: Mobiililaite voi kytkeytyä ja käyttää GSM- ja GPRS-palveluita samanaikaisesti.
- Luokka B: Mobiililaite voi kytkeytyä GSM- ja GPRS-palveluihin samanaikaisesti, mutta käyttää vain toista palveluista toisen palvelun odottaessa.
- Luokka C: Mobiililaite kytkeytyy ja käyttää ainoastaan GPRS-palvelua.

(ETSI 2000c, 21.)

TAULUKKO 9. GPRS-mobiililaitteen MM- ja PDP-kontekstit (ETSI 2000c, 84)

Kenttä	**SIM**	**Kuvaus**
IMSI	X	Kansainvälinen mobiilitilaajatunnus
MM-tila		Liikkuvuuden hallinnan tilatieto (idle, standby, ready)
P-TMSI	X	Käyttäjän tilapäistunniste GPRS-verkossa
P-TMSI allekirjoitus	X	Käyttäjän tilapäistunnisteen allekirjoitus GPRS-verkossa
Reititysalue	X	Käytettävä reititysalue
Solutunniste		Käytettävä solu
Kc	X	Käytettävä salausavain
CKSN	X	Käytettävän salausavaimen järjestysnumero
Salausalgoritmi		Käytettävä salausalgoritmi
Päätelaiteluokka		Kertoo verkolle mihin toimintoihin mobiililaite kykenee
DRX-parametrit		Epäjatkuvan vastaanoton parametrit
SMS-radioprioriteetti		RLC/MAC-radiorajapinnan prioriteetti SMS:n lähetyksessä
MM-kontekstin sisältämä PDP-konteksti: (MM-konteksti voi sisältää useita eri PDP-kontekseja)		
PDP-tyyppi		PDP-konteksin tyyppi (esim. X.25, PPP, IP)
PDP-osoite		PDP-osoite esim. X.121-osoite
PDP-tila		Pakettidataprotokollan tilatieto (aktiivinen tai ei-aktiivinen)
Dynaamisen osoitteen sallinta		Määrittää voiko mobiililaite käyttää dynaamista osoitetta
Pyydetty APN		Käytettävä APN
NSAPI		Verkkokerroksen liityntäpisteen tunniste
TI		Tapahtumatunniste
Pyydetty palvelunlaatuprofiili		Käytettäväksi pyydetty palvelunlaatuprofiili
Neuvoteltu palvelunlaatuprofiili		Käytettävä palvelunlaatuprofiili
Radioprioriteetti		RLC/MAC-radiorajapinnan prioriteetti uplink-suunnan tiedonsiirtoon
Lähetettävä N-PDU numero		Seuraavan SGSN:lle lähetettävän N-PDU:n SNDCP-järjestysnumero
Vastaanotettu N-PDU numero		Seuraavaksi SGSN:ltä vastaanotettavan N-PDU:n SNDCP-järjestysnumero

8.2.2 Tukiasemajärjestelmä (BSS)

Tukiasemajärjestelmällä käsitetään fyysinen laitteisto, jolla toteutetaan radiopeitto tietylle maantieteelliselle alueelle. Tukiasemajärjestelmä sisältää mobiililaitteen kanssa radiotiellä tapahtuvaan tiedonvälitykseen tarvittavan laitteiston. Toiminnallisuuksiltaan tukiasemajärjestelmä jaetaan kahteen osaan, jotka ovat tukiasema BTS (Base Transmitter Station) ja tukiasemaohjain BSC (Base Station Controller). Tukiasema suorittaa tiedonvälityksen radiotiellä ja tukiasemaohjain radioresurssien hallinnan. (ETSI 2000a, 15; ETSI 2001a, 15.)

8.2.3 Matkapuhelinkeskus (MSC)

Matkapuhelinkeskus vastaa kiinteän verkon puhelinkeskusta. Matkapuhelinkeskuksessa suoritetaan keskuksen alueella sijaitseviin mobiililaitteisiin liittyviä kytkentä- ja signalointitoimintoja. Kiinteän verkon puhelinkeskuksen toimintojen lisäksi matkapuhelinkeskuksessa suoritetaan liikkuvuuden hallintaa, kuten radioresurssien hallinnointi, sijaintirekisterien päivitykset ja solun vaihtoon liittyvät toiminnot. Matkapuhelinkeskuksen yhteen liittämiseksi ulkoisiin verkkoihin matkapuhelinkeskus sisältää yhteensovitustoimintoja, jotka määritetään ulkoisen verkon tyypin ja käytettävien palveluiden perusteella. (ETSI 2000a, 14; ETSI 2001a, 15.)

8.2.4 Vierailijarekisteri (VLR)

Vierailijarekisteri on matkapuhelinkeskuksen dynaaminen rekisteri, johon tallennetaan matkapuhelinkeskuksen alueella toimiviin mobiililaitteisiin liittyviä tietoja. Vierailijarekisteri sisältää puheluiden ja muiden palveluiden hallinnointitietoja. Mobiililaitteen siirtyessä matkapuhelinkeskuksen alueelle matkapuhelinkeskus välittää mobiililaitteen sijaintialuetunnuksen vierailijarekisterille, joka hakee tarvittaessa mobiililaitteen tilaajatiedot kotirekisteristä. Kotirekisteriin tallennetaan mobiililaitteen käyttämän vierailijarekisterin numero. Tilaajatietojen lisäksi kotirekisteristä voidaan välittää vierailijarekisterille muita eri palveluihin liittyviä tietoja. (ETSI 2000a, 13; ETSI 2001a, 15.)

8.2.5 GPRS-operointisolmu (SGSN)

GPRS-operointisolmu tarjoaa mobiililaitteille GPRS-palvelun muodostamalla mobiililaitteille MM- (Mobility Management) ja PDP-kontekstit (Packet Data Protocol). MM-konteksti sisältää mobiililaitteen liikkuvuuden hallintaan ja turvallisuuteen liittyviä tietoja ja PDP-konteksti sisältää mobiililaitteen reititystiedot. PDP-kontekstin reititystiedoilla radiorajapinnan yli siirrettävät paketit reititetään GPRS-tilaajan käyttämälle GPRS-yhdyskäytäväsolmulle. GPRS-operointisolmu voi myös vastaanottaa kutsupyyntöjä MSC/VLR:ltä ja välittää mobiililaitteiden sijaintitietoja MSC/VLR:lle. (ETSI 2000c, 19.)

TAULUKKO 10. SGSN MM- ja PDP-kontekstit (ETSI 2000c, 82)

Kenttä	**Kuvaus**
IMSI	Kansainvälinen mobiilitilaajatunnus
MM-tila	Liikkuvuuden hallinnan tilatieto (idle, standby, ready)
P-TMSI	Käyttäjän tilapäistunniste GPRS-verkossa
P-TMSI allekirjoitus	Käyttäjän tilapäistunnisteen allekirjoitus GPRS-verkossa
IMEI	Kansainvälinen mobiililaitetunnus
MSISDN	Mobiilitilaajan kansainvälinen ISDN-numero
Reititysalue	Käytettävä reititysalue
Solutunniste	Käytettävä solu
Solutunnisteen ikä	Mobiililaitteen lähettämän LLC PDU:n vastaanottamisesta kulunut aika
VLR-numero	Mobiililaitteen käyttämän MSC/VLR:n numero
Uusi SGSN-osoite	Uuden SGSN:n IP-osoite, johon puskuroidut paketit lähetetään
Todennustripletti	Todennus- ja salausparametrit
Kc	Käytettävä salausavain
CKSN	Käytettävän salausavaimen järjestysnumero
Salausalgoritmi	Käytettävä salausalgoritmi
Radioverkkoluokka	Mobiililaitteen radioverkko-ominaisuudet
SGSN-luokka	Mobiililaitteen verkko-ominaisuudet
DRX-parametrit	Epäjatkuvan vastaanoton parametrit
MNRG	Ilmaisee tarvitseeko mobiililaitteen toiminnosta raportoida HLR:lle
NGAF	Ilmaisee tarvitseeko mobiililaitteen toiminnosta raportoida MSC/VLR:lle
PPF	Ilmaisee voidaanko suorittaa GSM- tai GPRS-palveluiden kutsuminen
SMS-parametrit	SMS välittämiseen liittyvät parametrit esim. operaattorin asettamat estot
Palautus	Ilmaisee suorittaako HLR tai VLR tietokannan palautusta
SMS-radioprioriteetti	RLC/MAC-radiorajapinnan prioriteetti SMS:n lähetyksessä
MM-kontekstin sisältämä PDP-konteksti: (MM-konteksti voi sisältää useita eri PDP-kontekseja)	
PDP-kontektin tunnus	PDP-kontekstin yksilöivä tunnus
PDP-tila	Pakettidataprotokollan tilatieto (aktiivinen tai ei-aktiivinen)
PDP-tyyppi	PDP-konteksin tyyppi (esim. X.25, PPP, IP)
PDP-osoite	PDP-osoite esim. X.121-osoite
Tilattu APN	HLR:ltä vastaanotettu APN
Käytettävä APN	Tällä hetkellä käytettävä APN
NSAPI	Verkkokerroksen liityntäpisteen tunniste
TI	Tapahtumatunniste
Käytettävä GGSN-osoite	Tällä hetkellä käytettävän GGSN:n IP-osoite
VPLMN-osoitteen sallinta	Määrittelee voiko mobiililaite käyttää APN:ää verkkovierailun aikana
Tilattu palvelunlaatuprofiili	Tilaajatietoihin tallennettu palvelunlaatuprofiili
Pyydetty palvelunlaatuprofiili	Käytettäväksi pyydetty palvelunlaatuprofiili
Neuvoteltu palvelunlaatuprofiili	Käytettävä palvelunlaatuprofiili
Radioprioriteetti	RLC/MAC-radiorajapinnan prioriteetti uplink-suunnan tiedonsiirtoon
Lähetettävä N-PDU numero	Seuraavan SGSN:lle lähetettävän N-PDU:n SNDCP-järjestysnumero
Vastaanotettu N-PDU numero	Seuraavaksi SGSN:ltä vastaanotettavan N-PDU:n SNDCP-järjestysnumero
SND	Seuraavan mobiililaitteelle lähetettävän N-PDU:n GTP-järjestysnumero
SNU	Seuraavan GGSN:lle lähetettävän N-PDU:n GTP-järjestysnumero
Laskutustunnus	SGSN:ssä ja GGSN:ssä muodostettavia laskutustietueita yksilöivä tunnus
Uudelleenjärjestäminen	Uudelleenjärjestetäänkö SGSN:ssä N-PDU:t ennen mobiililaitteella lähettämistä

8.2.6 GPRS-yhdyskäytäväsolmu (GGSN)

GPRS-yhdyskäytäväsolmu toimii GPRS-palvelua tukevan GSM-verkon yhteen liityntäpisteenä pakettidataverkkoihin. GPRS-yhdyskäytäväsolmu sisältää verkkoon kytkeytyneiden GPRS-tilaajien reititystietoja, joita käytetään radiorajapinnan yli siirrettävien pakettien tunnelointiin mobiililaitteiden kytkeytymispisteeseen eli GPRS-operointisolmulle. GPRS-yhdyskäytävä- ja operointisolmut sisältävät IP-toiminnallisuuden, joten solmut voidaan yhdistää toisiinsa käyttämällä IP-reitittimiä. GPRS-yhdyskäytävä- ja operointisolmujen toiminnot voidaan myös yhdistää yhdeksi fyysiseksi solmuksi. (ETSI 2000c, 19.)

TAULUKKO 11. GGSN PDP-konteksti (ETSI 2000c, 82)

Kenttä	Kuvaus
IMSI	Kansainvälinen mobiilitilaajatunnus
NSAPI	Verkkokerroksen liityntäpisteen tunniste
MSISDN	Mobiilitilaajan kansainvälinen ISDN-numero
PDP-tyyppi	PDP-konteksin tyyppi (esim. X.25, PPP, IP)
PDP-osoite	PDP-osoite esim. X.121-osoite
Dynaaminen osoite	Määrittelee onko PDP-osoite kiinteä vai dynaaminen
Käytettävä APN	Tällä hetkellä käytettävä APN
Neuvoteltu palvelunlaatuprofiili	Käytettävä palvelunlaatuprofiili
SGSN-osoite	Mobiililaitteen käyttämän SGSN:n IP-osoite
MNRG	Ilmaisee onko mobiililaite merkitty HLR:ssä ei tavoiteta -tilaan
Palautus	Ilmaisee suorittaako SGSN tietokannan palautusta
SND	Seuraavan SGSN:lle lähetettävän N-PDU:n GTP-järjestysnumero
SNU	Seuraavaksi SGSN:ltä vastaanotettavan N-PDU:n GTP-järjestysnumero
Laskutustunnus	SGSN:ssä ja GGSN:ssä muodostettavia laskutustietueita yksilöivä tunnus
Uudelleenjärjestäminen	Uudelleenjärjestetäänkö GGSN:ssä SGSN:ltä vastaanotetut N-PDU:t

8.2.7 Kotirekisteri (HLR)

Kotirekisteri on tietokanta, jota käytetään tilaajatietojen tallentamiseen ja hallinnointiin. Kaikki verkko-operaattorin tilaajatietojen ylläpidolliset toimenpiteet tehdään kotirekisterissä. Kotirekisteri sisältää tilaajatietojen lisäksi sijaintitietoja, joiden perusteella mm. puheluita reititetään matkapuhelinkeskuksille. Käytettäessä GPRS-palvelua kotirekisteri sisältää GPRS-tilaaja- ja reititystiedot.
(ETSI 2000c, 20; ETSI 2001a, 15.)

TAULUKKO 12. HLR GPRS-tilaajatiedot (ETSI 2000c, 81)

Kenttä	**Kuvaus**
IMSI	Kansainvälinen mobiilitilaajatunnus
MSISDN	Mobiilitilaajan kansainvälinen ISDN-numero
SGSN-numero	Mobiililaitteen käyttämän SGSN:n SS7-numero
SGSN-osoite	Mobiililaitteen käyttämän SGSN:n IP-osoite
SMS-parametrit	SMS välittämiseen liittyvät parametrit esim. operaattorin asettamat estot
GPRS-purku	Ilmaisee MM- ja PDP-kontekstien poiston SGSN:ltä
MNRG	Ilmaisee ettei mobiililaitetta tavoiteta SGSN:kautta, ei tavoiteta -tila
GGSN-lista	GGSN:ään liittyvä GSN-numero ja valinnainen IP-osoite
IMSI:in liitettävä PDP-konteksti: (IMSI:lle voidaan määrittää useita eri PDP-kontekseja)	
PDP-kontektin tunnus	PDP-kontekstin yksilöivä tunnus
PDP-tyyppi	PDP-konteksin tyyppi (esim. X.25, PPP, IP)
PDP-osoite	PDP-osoite esim. X.121-osoite
APN:n nimi	Ulkoisen pakettidataverkon DNS-nimeämissääntöjen mukainen nimi
Tilattu palvelunlaatuprofiili	Tilaajan oletus palvelunlaatuprofiili
VPLMN-osoitteen sallinta	Määrittelee voiko mobiililaite käyttää APN:ää verkkovierailun aikana

8.3 GPRS-tiedonsiirto

GPRS-palveluiden käyttämiseksi mobiililaite suorittaa GPRS-verkkoon kytkeytymisen, jolloin GPRS-verkko saa tiedon mobiililaitteen läsnäolosta. GPRS-verkkoon kytkeytymisessä muodostetaan looginen yhteys mobiililaitteen ja SGSN välille, jolloin voidaan välittää SMS-viestejä GPRS-radiokanavilla, kutsua puheluita SGSN kautta sekä ilmoittaa mobiililaitteelle verkosta tulevasta GPRS-datasta. Tiedonsiirtämiseksi mobiililaitteen ja ulkoisten tietoverkkojen välillä on mobiililaitteen suoritettava tiedonsiirtoon käytettävän PDP-osoitteen aktivointi, jolloin PDP-osoitetta vastaava GGSN saa tiedon mobiililaitteesta. (ETSI 2000c, 14.)

Mobiililaitteen ja GGSN:n välisessä ns. läpinäkyvässä tiedonsiirrossa käytetään GPRS-spesifisiä kapselointi- ja tunnelointiprotokollia. Läpinäkyvä tiedonsiirto vähentää tarvetta tulkita eri protokollia GPRS-verkossa ja mahdollistaa joustavamman yhteen liittämisen uusiin tiedonsiirtoprotokolliin. Tiedonsiirrossa voidaan käyttää pakkausta tiedonsiirron tehostamiseksi sekä uudelleenlähetysprotokollia luotettavuuden parantamiseksi. (ETSI 2000c, 14.)

8.3.1 GPRS-verkkoon kytkeytyminen

GPRS-verkossa mobiililaitteelle määritetään kolme eri liikkuvuuden hallinnan tilaa, jotka ovat idle-, standby- ja ready-tilat. Liikkuvuuden hallintaan liittyvistä tiedoista muodostetaan mobiililaitteelle MM-konteksti, jota ylläpidetään mobiililaitteessa ja SGSN:ssä. Liikkuvuuden hallinnan tila määrittää mobiililaitteelle tietyn toiminnallisuuden tason ja ylläpidettävien MM-kontekstien sisältämät tiedot. (ETSI 2000c, 26.)

Liikkuvuuden hallinnan tilat:

- Idle: Mobiililaite ei ole kytkeytyneenä GPRS:n liikkuvuuden hallintaan, eikä mobiililaitteelle ole muodostettu MM-kontekstia. GPRS-verkko ei tiedä mobiililaitteen sijaintiin ja reititykseen liittyviä tietoja, joten tiedonsiirto tai mobiililaitteen kutsuminen verkosta eivät ole mahdollisia. Mobiililaite suorittaa vain verkon ja solun valintaa. MM-kontekstin muodostamiseksi mobiililaitteen on suoritettava GPRS-verkkoon kytkeytyminen.
- Standby: Mobiililaite on kytkeytyneenä GPRS:n liikkuvuuden hallintaan, ja mobiililaitteelle on muodostettu MM-konteksti. GPRS-verkko tietää mobiililaitteen sijainnin reititysalueen tarkkuudella, joten mobiililaitetta voidaan kutsua verkosta, mutta tiedonsiirto ei ole mahdollista. Mobiililaite suorittaa solun ja reititysalueen valintaa sekä välittää SGSN:lle reititysalueen päivitystietoja. Mobiililaitteen käynnistäessä PDP-kontekstin aktivoinnin tai vastatessa verkon kutsuun siirtyy mobiililaite ready-tilaan.
- Ready: GPRS-verkko tietää mobiililaitteen sijainnin solun tarkkuudella. Mobiililaite suorittaa solun valintaa tai vaihtoehtoisesti verkko voi tehdä solun valinnan. Tiedonsiirto mobiililaitteen ja GPRS-verkon välillä on mahdollista. Mobiililaite pysyy ready-tilassa siitä huolimatta, onko mobiililaitteelle varattu radioresursseja tai suoritetaanko tiedonsiirtoa. Ready-tilan ylläpitoon käytetään ajastinta, jonka nollantuessa mobiililaite siirtyy standby-tilaan. Idle-tilaan siirtyäkseen mobiililaitteen on suoritettava GPRS-verkosta poistuminen.

(ETSI 2000c, 26 - 27.)

8.3.2 PDP-osoitteet

GPRS-verkossa tiedonsiirtoon käytetään PDP-osoitteita. PDP-osoitteille muodostetaan itsenäinen muista PDP-osoitteista riippumaton PDP-konteksti, jota ylläpidetään mobiililaitteessa, SGSN:llä ja GGSN:llä. PDP-kontekstilla on kaksi tilaa active- ja inactive-tilat. PDP-kontekstin tila määrittää voidaanko PDP-osoitetta käyttää tiedonsiirtämiseen. PDP-kontekstin active-tilassa voidaan PDP-osoitetta käyttää tiedonsiirtoon. Mobiililaitteelle voidaan määrittää useita eri PDP-osoitteita, jotka sisällytetään mobiililaitteen MM-kontekstiin. (ETSI 2000c, 58.)

Verkko-operaattori voi määrittää mobiililaitteen GPRS-tilaajatietoihin PDP-osoitteet kiinteästi tai dynaamisesti. Käytettäessä dynaamisia PDP-osoitteita GGSN suorittaa PDP-osoitteiden määrityksen ja vapauttamisen. Mobiililaitteen PDP-kontekstin aktivoinnin kutsuminen GPRS-verkosta edellyttää kiinteän PDP-osoitteen määrittämistä mobiililaitteelle. Mobiililaitteelle voidaan määrittää samanaikaisesti käyttöön kiinteitä ja dynaamisia PDP-osoitteita. (ETSI 2000c, 59.)

PDP-kontekstin tilat:

- Inactive: Inactive-tilassa PDP-konteksti ei sisällä PDP-osoitteen protokollatietoyksikköjen käsittelyyn tarvittavia reititys- ja osoitetietoja eikä mobiililaitteen sijainnin muuttuessa päivitetä PDP-kontekstia vaikka mobiililaite olisi GPRS-verkkoon kytkeytyneenä. Active-tilaan siirrytään mobiililaitteen suorittamalla PDP-kontekstin aktivoinnilla. Tarvittaessa GGSN voi lähettää mobiililaitteelle pyynnön suorittaa PDP-kontekstin aktivointi edellyttäen, että mobiililaitteen liikkuvuuden hallinnan tila on standby- tai ready-tilassa.
- Active: Active-tilassa PDP-konteksti sisältää PDP-osoitteen protokollatietoyksiköiden käsittelyyn tarvittavat reititys- ja osoitetiedot. Active-tila edellyttää, että mobiililaitteen liikkuvuuden hallinnan tila on standby- tai ready-tilassa. Inactive-tilaan siirrytään mobiililaitteen suorittamalla PDP-kontekstin purkamisella. Mobiililaitteen liikkuvuuden hallinnan tilan vaihtuessa idle-tilaan siirtyvät kaikki mobiililaitteen PDP-kontekstit inactive-tilaan.

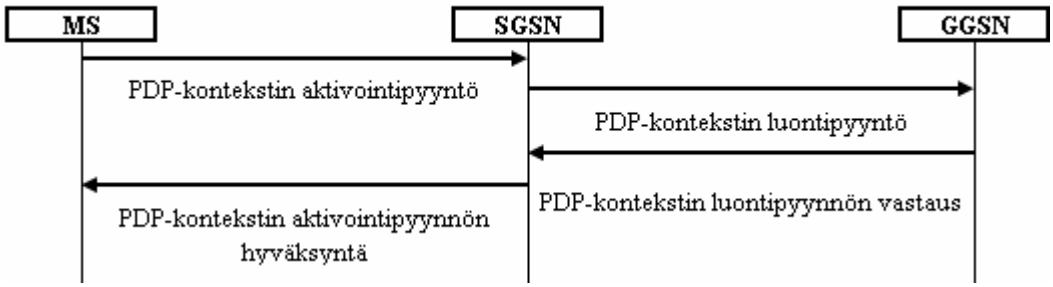
(ETSI 2000c, 58.)

8.3.3 PDP-osoitteen aktivointi

Mobiililaite suorittaa PDP-osoitteen aktivoinnin lähettämällä PDP-kontekstin aktivointipyynnön SGSN:lle, joka vahvistaa aktivointipyynnön vertaamalla PDP-tyyppiä, PDP-osoitetta ja yhteyspisteen nimeä APN (Access Point Name) PDP-kontekstin tilaajatietoihin. Vahvistamisen tai GGSN-osoitteen saannin epäonnistuessa SGSN hylkää aktivointipyynnön. Vahvistamisen ja GGSN-osoitteen saannin onnistuessa SSGN luo PDP-kontekstille tunnelointitunnisteen TID (Tunneling Identifier) yhdistämällä MM-kontekstin sisältämän IMSI:n ja mobiililaitteelta vastaanotetun verkkokerroksen liityntäpisteen tunnisteen NSAPI (Network layer Service Access Point Identifier) ja lähettää PDP-kontekstin luontipyynnön GGSN:lle. (ETSI 2000c, 60 - 61.)

Vastaanottaessaan SGSN:ltä PDP-kontekstin luontipyynnön GGSN luo PDP-kontekstin tauluun uuden tietueen, jota käytetään PDP-tietoyksiköiden reitittämiseen SGSN:n ja ulkoisen pakettidataverkon välillä. GGSN palauttaa SGSN:lle vastauksen PDP-kontekstin luontipyyntöön. GGSN hylkää PDP-kontekstin luontipyynnöt, jotka sisältävät PDP-kontekstille soveltumattoman palvelunlaatuprofiilin. (ETSI 2000c, 61.)

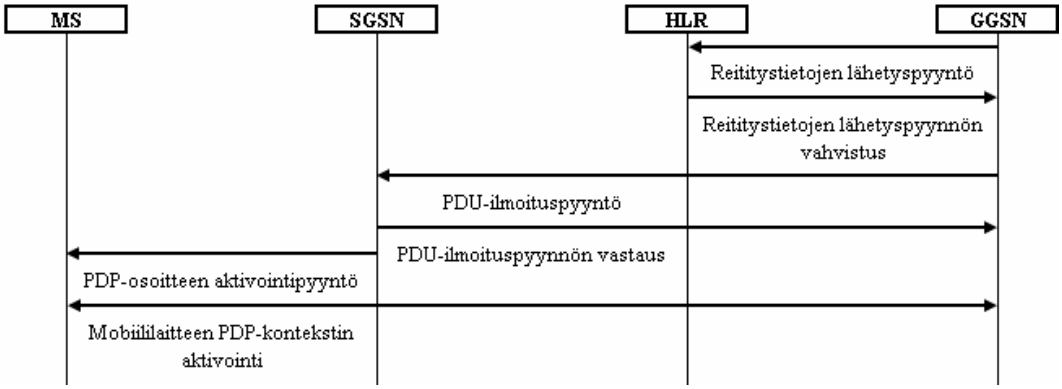
Saatuaan GGSN:ltä vastauksen PDP-kontekstin luontipyyntöön SGSN sisällyttää PDP-kontekstiin NSAPI:n, GGSN-osoitteen ja dynaamisen PDP-osoitteen. SGSN valitsee käytettävän radiotien prioriteetin neuvotellun palvelunlaatuprofiilin perusteella ja palauttaa mobiililaitteelle PDP-kontekstin aktivointipyynnön hyväksynnän. SGSN ilmoittaa mobiililaitteelle myös aktivointipyynnön epäonnistumisesta. (ETSI 2000c, 61.)



KUVIO 25. Mobiililaitteen PDP-kontekstin aktivointi (ETSI 2000c, 60)

PDP-kontekstin aktivointi mobiililaitteelta voidaan käynnistää myös GPRS-verkon pyynnöstä. Vastaanottaessaan ulkoisesta pakettidataverkosta tietylle PDP-osoitteelle osoitetun PDP-tietoyksikön GGSN tarkistaa onko PDP-osoitteelle muodostettu PDP-konteksti. PDP-kontekstin puuttuessa GGSN käynnistää toimenpiteet PDP-kontekstin luomiseksi suorittamalla pyynnön käynnistää PDP-osoitteen aktivointi mobiililaitteelta. (ETSI 2000c, 61.)

GGSN lähettää reititystietojen lähetyspyynnön HLR:lle, joka vastaa pyyntöön vahvistuksella. Vahvistus sisältää mm. mobiililaitteen IMSI:n ja käytettävän SGSN-osoitteen. HLR:n todetessa ettei pyyntöä voida toteuttaa, sisältää vahvistus hylkäyssyyn. Vastaanotettuaan HLR:ltä hyväksytyn vahvistuksen GGSN lähettää HLR:n määrittämälle SGSN:lle PDU-ilmoituspyynnön, johon SGSN lähettää vastauksen GGSN:lle ja lähettää PDP-kontekstissa määritellylle mobiililaitteelle pyynnön käynnistää pyydetyn PDP-osoitteen aktivointi. (ETSI 2000c, 62.)



KUVIO 26. PDP-kontekstin aktivointi verkosta (ETSI 2000c, 62)

8.4 GPRS palvelunlaatu

GPRS-verkossa palvelunlaatu QoS (Quality of Service) toteutetaan palvelunlaatuprofiileilla, jotka määritetään erikseen jokaiselle PDP-kontekstille. Palvelunlaatuprofiili käsitetään yhtenä parametrina, joka sisältää useita tiedonsiirtoon liittyviä ominaisuuksia. Ominaisuudet jaetaan viiteen palveluntasoluokkaan: prioriteetti, viive, luotettavuus, keskimääräinen datan läpäisykyky ja maksimaalinen datan läpäisykyky. (ETSI 2000c, 90 - 91.)

Mobiililaite voi pyytää tietyn arvon jokaiselle palveluntasoluokan ominaisuudelle, mukaan lukien HLR:än tilaajatietoihin tallennetut oletusarvot. Palveluntasoluokkien ominaisuuksista voidaan muodostaa hyvin monenlaisia palvelunlaatuprofiileja, mutta GPRS-verkko ei välttämättä tue kaikkia mahdollisia yhdistelmiä. GPRS-verkko neuvottelee PDP-osoitteen aktivoinnin yhteydessä palveluntasoluokan ominaisuuksille tarjolla olevien GPRS-resurssien mukaiset tasot, joista muodostetaan neuvoteltu palvelunlaatuprofiili. GPRS-verkko palauttaa mobiililaitteelle tiedon neuvotellusta palvelunlaatuprofiilista, jonka mobiililaite joko hyväksyy tai hylkää. GPRS-verkko pyrkii ylläpitämään riittäviä GPRS-resursseja neuvotelluille palvelunlaatuprofiileille. (ETSI 2000c, 91.)

GPRS-verkon RLC/MAC-kerroksella (Radio Link Control / Medium Access Control) tuetaan neljää radiotien prioriteettitasoa tiedonsiirrolle ja erillistä tasoa signalointiviesteille. Uplink-pääsyn yhteydessä mobiililaite voi ilmaista käytettävän radiotien prioriteettitason sekä käytetäänkö uplink-yhteyttä tiedonsiirtoon vai signalointiviestien välittämiseen. Mobiililaitteen ilmaisemien tietojen perusteella BSS määrittelee radiotien pääsyn ja palvelun prioriteetit ruuhkatilanteessa. SGSN määrittelee neuvotellun palvelunlaatuprofiilin perusteella tiedonsiirtoon käytettävän radiotien prioriteetin. (ETSI 2000c, 91.)

8.4.1 Prioriteetti

Normaalissa toimintatilassa GPRS-verkko pyrkii ylläpitämään kaikkien käytössä olevien palvelunlaatuprofiilien asettamat palveluvelvoitteet. Palvelun prioriteetti määrittelee palveluvelvoitteen ylläpitämisen suhteellisen tärkeyden epänormaalissa tilanteessa, kuten rajoittuneet verkon resurssit tai ruuhkatilanne. Palvelun prioriteetti määritellään kolmella eri prioriteettiluokalla. (ETSI 2000c, 91.)

TAULUKKO 13. Prioriteettiluokat (ETSI 2000c, 91)

Prioriteetti-luokka	Prioriteetin nimi	Kuvaus
1	Korkea	Palveluvelvoitteet suoritetaan ennen luokkia 2 ja 3
2	Normaali	Palveluvelvoitteet suoritetaan ennen luokkaa 3
3	Alhainen	Palveluvelvoitteet suoritetaan luokkien 1 ja 2 jälkeen

8.4.2 Viive

GPRS-verkossa käytetään neljää viiveluokkaa, jotka määrittävät suurimman sallitun pakettikohtaisen siirtoviiveen. Viiveluokkien parametrit määritetään maksimiarvona tiedonsiirron keskimääräiselle päästä päähän viiveelle sekä viiveen arvona, jonka 95-prosenttia liikenteestä alittaa. Viive määritellään kahdelle pakettikoolle 128 ja 1024 oktettia ja mittayksikkönä käytetään sekuntia. Liikennöitäessä mobiililaitteen ja ulkoisen pakettidataverkon laitteen välillä viive mitataan mobiililaitteen R- tai S-rajapinnan ja GPRS-verkon Gi-rajapinnan väliltä eikä viive sisällä ulkoisen pakettidataverkon viiveitä. Viive sisältää radiokanavien ja GPRS-verkon siirtoviiveen sekä radiorajapinnan pääsyviiveen uplink-suunnassa tai radiokanavien määritysviiveen downlik-suunnassa. (ETSI 2000b, 18 - 19; ETSI 2000c, 91.)

TAULUKKO 14. Viiveluokat (ETSI 2000b, 19)

Viiveluokka	**Viive** [*s*]			
	Pakettikoko 128 oktettia		Pakettikoko 1024 oktettia	
	Keskimääräinen	95 % liikenteestä	Keskimääräinen	95 % liikenteestä
1	< 0,5	< 1,5	< 2	< 7
2	< 5	< 25	< 15	< 75
3	< 50	< 250	< 75	< 375
4	Ei määritetty (Best Effort)			

8.4.3 Luotettavuus

GPRS-verkossa määritellään viisi luotettavuusluokkaa, joista luokat 1 - 3 on määritetty ei-reaaliaikaiselle ja luokat 4 - 5 reaaliaikaiselle tiedonsiirrolle. Luotettavuusluokka valitaan käytettävän sovelluksen tiedonsiirrolle asettamien vaatimusten perusteella. Luotettavuusluokka määrittelee PDP-kontekstille virhe todennäköisyyksien tavoitetasot tiedon häviämiselle, kahdentumiselle, rikkoutumiselle ja epäjärjestyksessä vastaanottamiselle. Luotettavuusluokka asettaa vaatimuksia useille GPRS-verkon protokollakerroksille. RLC-, LLC- ja GTP-protokollakerrokset (GPRS Tunneling Protocol) tukevat luotettavuusluokkien asettamia suorituskykyvaatimuksia. GPRS-verkon signalointitiedon välittämiseen käytetään luotettavuusluokkaa kolme. (ETSI 2000b, 18; ETSI 2000c, 91 - 92.)

TAULUKKO 15. Ei-reaaliaikaiset luotettavuusluokat (ETSI 2000b, 18)

Luotettavuus-luokka	Todennäköisyys			
	Häviäminen	Kahdentuminen	Epäjärjestys	vikaantuminen
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

8.4.4 Keskimääräinen datan läpäisykyky

Keskimääräisellä datan läpäisykyvyllä määritetään keskiarvo, jolla tietoa oletetaan siirrettävän aktiivisen PDP-kontekstin jäljellä olevana elinaikana. Keskimääräisellä datan läpäisykyvyllä voidaan rajoittaa tiedonsiirtoa GPRS-verkossa tilaajakohtaisesti neuvoteltuun maksimitasoon, jolloin tilaajalle ei anneta lisää resursseja vaikka niitä olisi GPRS-verkossa vapaana. Keskimääräinen läpäisykyky voidaan määrittää myös ns. best effort -periaatteen mukaisesti, jolloin kaikkia mobiililaitteita kohdellaan GPRS-verkossa samanarvoisina ja resursseja jaetaan mobiililaitteen tarpeen ja GPRS-verkon resurssien saatavuuden mukaan. Keskimääräinen datan läpäisykyky mitataan R- ja Gi-rajapintojen väliltä ja yksikkönä käytetään oktettia tunnissa. (ETSI 2000c, 93.)

TAULUKKO 16. Keskimääräinen datan läpäisykykyluokat (ETSI 2000c, 93)

Keskimääräinen datan läpäisykykyluokka	Keskimääräinen datan läpäisykyky	
	oktettia/tunti	~bit/s
1	100	0,22
2	200	0,44
3	500	1,11
4	1000	2,2
5	2000	4,4
6	5000	11,1
7	10000	22
8	20000	44
9	50000	111
10	100000	220
11	200000	440
12	500000	1110
13	1000000	2200
14	2000000	4400
15	5000000	11100
16	10000000	22000
17	20000000	44000
18	50000000	111000
31	Best Effort	

8.4.5 Maksimaalinen datan läpäisykyky

Maksimaalisella datan läpäisykyvyllä määritetään yksittäiselle PDP-kontekstille oletus maksimitaso, jolla tietoa voidaan siirtää. Maksimaaliseen datan läpäisykykyyn vaikuttavat käytettävä mobiililaite ja vapaana olevat radiotien resurssit, joten ei ole takeita voidaanko maksimaalinen datan läpäisykyky saavuttaa tiedonsiirrossa tai ylläpitää tietyn aikajakson. Maksimaalisella datan läpäisykyvyllä voidaan myös rajoittaa tiedonsiirtoa GPRS-verkossa tilaajakohtaisesti neuvoteltuun maksimitasoon, jolloin tilaajalle ei anneta lisää resursseja vaikka niitä olisi GPRS-verkossa vapaana. Maksimaalinen datan läpäisykyky mitataan R- ja Gi-rajapintojen väliltä ja yksikkönä käytetään oktettia sekunnissa. (ETSI 2000c, 92.)

TAULUKKO 17. Maksimaalinen datan läpäisykykyluokat (ETSI 2000c, 92)

Maksimaalinen datan läpäisykykyluokka	**Maksimaalinen datan läpäisykyky**	
	oktettia/sekunti	kbit/s
1	1000	8
2	2000	16
3	4000	32
4	8000	64
5	16000	128
6	32000	256
7	64000	512
8	128000	1024
9	256000	2048

8.5 RADIUS-protokolla

GPRS-verkon mobiililaitteiden todentamiseen, pääsyn hallintaan, tilastointiin sekä verkkoasetusten määrittämiseen ja hallintaan voidaan käyttää RADIUS-protokollaa (Remote Authentication Dial In User Service) tukevaa AAA-palvelinta (Authentication, Authorization, Accouting). GGSN:llä ulkoisen pakettidatanverkon yksilöivälle APN:lle määritetään käytettävä AAA-palvelin, johon RADIUS-protokollan kyselyt ohjataan. Käytettäessä RADIUS-protokollaa GGSN toimii RADIUS-asiakkaana ja AAA-palvelin RADIUS-palvelimena. Mobiililaitteen yksilöivänä tietona käytetään mobiililaitteen kansainvälistä ISDN-numeroa MSISDN (Mobile Subscriber ISDN Number) tai IMSI:ä. (ETSI 2005, 26.)

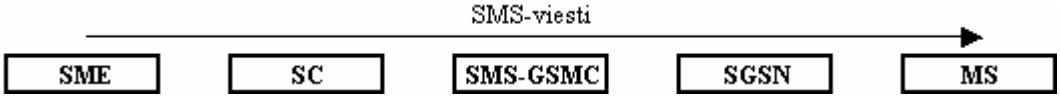
Käytettäessä AAA-palvelinta ulkoisen pakettidataverkon pääsyn hallintaan suoritetaan mobiililaitteen todentaminen PDP-osoitteen aktivoinin yhteydessä. Vastaanottaessa GGSN:llä PDP-kontekstin luontipyyntö lähetetään GGSN:ltä AAA-palvelimelle pääsy pyyntö -sanoma, joka sisältää mobiililaitteen todentamiseen tarvittavat tiedot. AAA-palvelimella todennetaan mobiililaite, tarkistetaan mobiililaitteen verkkoon pääsylle asetettujen vaatimusten täyttyminen ja palautetaan vastaus GGSN:lle. Hyväksyttäessä mobiililaitteen verkkoon pääsy palautetaan AAA-palvelimelta GGSN:lle pääsy hyväksytty -sanoma, joka voi sisältää PDP-kontekstin luomisessa käytettäviä verkkoasetuksia, kuten mobiililaitteelle määritettävän IP-osoitteen. Hylättäessä mobiililaitteen verkkoon pääsy palautetaan AAA-palvelimelta GGSN:lle pääsy hylätty -sanoma. Vastaanotettaessa GGSN:llä pääsy hyväksytty -sanoma luodaan pyydetty PDP-konteksti. Vastaanotettaessa pääsy hylätty -sanoma tai vastausta pääsy pyyntö -sanomaan ei saada hylätään GGSN:llä PDP-kontekstin luontipyyntö. (Rigney, Rubens, Simpson & Willens 2000, 5 - 7; ETSI 2005, 26.)

RADIUS-tilastointi aloitetaan AAA-palvelimen onnistuneen mobiililaitteen todentamisen jälkeen tai AAA-palvelinta voidaan käyttää pelkästään tilastointiin, jolloin mobiililaitetta ei todenneta AAA-palvelimella vaan luotetaan GPRS-verkon suorittamaan mobiililaitteen todentamiseen. Käytettäessä AAA-palvelinta tilastointiin lähetetään GGSN:ltä AAA-palvelimelle tilastoinnin aloituspyyntö -sanoma, johon AAA-palvelin palauttaa vastauksena tilastoinnin aloitus -vastaussanoman. Tilastoinnin aloituspyyntö -sanoma sisältää mm. mobiililaitteen yksilöivän tiedon ja mobiililaitteelle määritetyn IP-osoitteen. Mobiililaitteen IP-osoitetta käytetään sovelluspalvelimilla mobiililaitteen tunnistamiseen. Ulkoisten sovellusten vaatiessa tilastoinnin aloitus -vastaussanoman, GGSN:llä joko hylätään mobiililaitteelta vastaanotettu data kunnes AAA-palvelimelta saadaan tilastoinnin aloitus -vastaussanoma tai GGSN:ltä palautetaan SGSN:lle vastaus PDP-kontekstin luontipyyntöön vasta tilastoinnin aloitus -vastaussanoman jälkeen. Purettaessa PDP-konteksti lähetetään GGSN:ltä AAA-palvelimelle tilastoinnin lopetuspyyntö -sanoma, johon AAA-palvelin palauttaa vastauksena tilastoinnin lopetus -vastaussanoman. PDP-kontekstin purku suoritetaan GGSN:llä välittömästi eikä GGSN jää odottamaan AAA-palvelimen tilastoinnin lopetus -vastaussanomaa. (ETSI 2005, 26 - 28.)

8.6 SMS-viestin välittäminen GPRS-radiokanavilla

GSM-verkon lyhytsanomapalvelulla lähetetään ja vastaanotetaan SMS-viestejä. SMS-viestien välittämiseen käytetään lyhytsanoman palvelukeskusta SM-SC (Short Message - Service Centre), jossa suoritetaan verkkojen yhteen liittämiseen ja viestinvälitykseen liittyviä toimintoja. Lyhytsanoman lähettäjästä ja vastaanottajasta käytetään termiä lyhytsanomaolio SME (Short Message Entity), joka voi sijaita kiinteässä verkossa, mobiililaitteessa tai SM-SC:ssä. GPRS-verkkoon kytkeytyneelle mobiililaitteelle voidaan välittää SMS-viestejä GPRS-radiokanavilla, jolloin SMS-viestit välitetään mobiililaitteelle SGSN:ltä eikä MSC:ltä. Välitettäessä SMS-viestejä SGSN:ltä hyödynnetään radiorajapinnan resursseja tehokkaammin kuin välitettäessä SMS-viestejä MSC:ltä. SMS-viestin välittämisen epäonnistuessa SGSN:ltä yritetään SMS-viestin välitystä MSC:een kautta.
(ETSI 2000c, 93 - 94; ETSI 2001b, 11.)

Lähetettäessä mobiililaitteelle lyhytsanoma muodostetaan SME:llä SMS-viesti ja lähetetään se SM-SC:n kautta SMS-GMSC:lle, joka lukee SMS-viestistä vastaanottavan mobiililaitteen osoitteen. SMS-GMSC pyytää osoitetta vastaavan mobiililaitteen reititystiedot HRL:ltä lähettämällä lähetä lyhytsanoman reititystiedot -sanoman. HLR palauttaa lähetä lyhytsanoman reititystiedot -sanoman vastauksena lähetä lyhytsanoman reititystiedot tulos -sanoman, joka sisältää joko mobiililaitetta palvelevan SGSN:n tai MSC:n numeron tai molempien numerot. Lähetä lyhytsanoman reititystiedot tulos -sanoman sisältäessä SGSN:n osoitteen välittää SMS-GMSC SMS-viestin osoitetta vastaavalle SGSN:lle, joka lähettää SMS-viestin mobiililaitteelle GPRS-radiokanavilla. SGSN lähettää tiedon onnistuneesta SMS-viestin välittämisestä SMS-GMSC, joka välittää tiedon SM-SC:lle.
(ETSI 2000c, 93.)



KUVIO 27. SMS-viestin välittäminen mobiililaitteelle (ETSI 2001b, 24.)

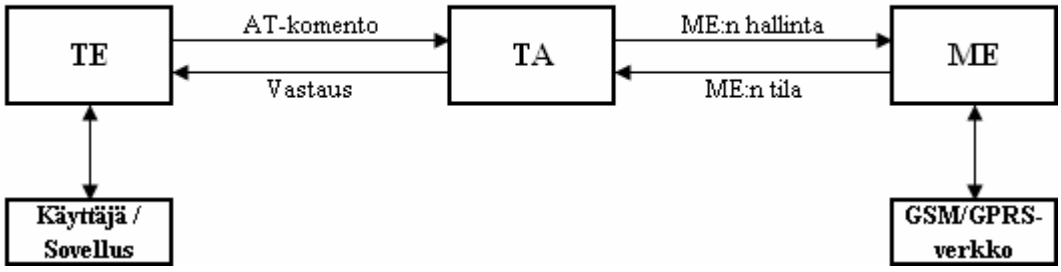
8.7 AT-komennot

Mobiililaitteiston toimintojen ja GSM-verkon palveluiden hallintaan päätelaitteistolta käytetään AT-komentoja (ATtention). GSM-verkon AT-komennot määritellään ITU-T suosituksessa V.25ter, jonka +C-sarja on varattu digitaalisille mobiililaitejärjestelmille. GPRS-palvelun AT-komennot on määritelty ETSI:n toimesta. AT-komentojen välittämiseen käytetään päätesovitinta TA (Terminal Adaptor), jolla mobiililaitteisto ja päätelaitteisto yhdistetään toisiinsa. Päätelaitteiston ja päätesovittimen välinen rajapinta voidaan toteuttaa ITU-T suosituksen V.24 mukaisella sarjakaapelilla, infrapunalinkillä tai muulla vastaavanlaisella menetelmällä. AT-komentojen oikean toiminnan varmistamiseksi päätelaitteiston ja päätesovittimen väliselle linkille suositellaan 8-bittistä datansiirtoa. (ETSI 2003, 8.)

Fyysisen toteutuksen vaihtoehdot:

- Mobiililaitteisto, päätesovitin ja päätelaitteisto ovat erilliset yksiköt.
- Mobiililaitteisto ja päätesovitin on yhdistetty samaan kuoreen, päätelaitteiston ollessa erillinen yksikkö.
- Päätesovitin ja päätelaitteisto on yhdistetty samaan kuoreen, mobiililaitteiston ollessa erillinen yksikkö.
- Mobiililaitteisto, päätesovitin ja päätelaitteisto on yhdistetty samaan yksikköön.

(ETSI 2003, 8.)



KUVIO 28. Mobiililaitteiston hallinta (ETSI 2003, 8)

9 HÄLYTYKSENSIIRRON TOTEUTUS GPRS-YHTEYDELLÄ

9.1 Ratkaisumallin valinta

GPRS-yhteydellä käytetään IP-pohjaista tiedonsiirtoyhteyttä, jonka tiedonsiirrossa voi esiintyä jopa usean sekunnin mittaisia viiveitä. GPRS-yhteydellä käytettäväksi protokollaksi valittiin Modbus TCP/IP -protokolla, joka on suunniteltu IP-pohjaisille tiedonsiirtoyhteyksille. Modbus TCP/IP -protokollan tiedonsiirrossa käytetään vahvistuskuittaus-menetelmää, joten lähetettyyn Modbus-pyyntösanomaan saadaan periaatteessa aina vastaus edellyttäen että TCP-yhteys on toiminnassa. Modbus TCP/IP -protokollassa ei ole määritelty lainkaan vaatimuksia viiveajalle, joten Modbus TCP/IP -protokolla soveltuu myös viiveaikojen osalta GPRS-yhteydellä käytettäväksi.

Ratkaisumallin valinnassa päädyttiin käyttämään toteutusta, jossa hälytyskohteen päätelaite toimii Modbus TCP/IP -isäntälaitteena ja Alerta-palveluverkon palvelin Modbus TCP/IP -orjalaitteena. Tehtyyn valintaan vaikuttivat Modbus TCP/IP -protokollan käyttämä asiakas/palvelin-malli ja GPRS-verkon asettamat rajoitukset. Modbus TCP/IP -protokollassa verkon tapahtuma alustetaan aina asiakkaana toimivalta isäntälaiteelta ja GPRS-yhteys on aina muodostettava mobiililaitteelta verkkoon. ETSI:n standardeissa määritellään GPRS-yhteyden muodostaminen mobiililaitteelta GPRS-verkon pyynnöstä, mutta laitevalmistajat eivät kuitenkaan ole ominaisuutta toteuttaneet laitteistoihinsa, tietoturvaan liittyvien ongelmien vuoksi. Haluttaessa muodostaa verkon pyynnöstä GPRS-yhteys on käytettävä erillistä herätettä. Herätteenä voidaan käyttää SMS-viestiä tai GSM-puhelua.

Jatkuvaa ns. Always-On GPRS-yhteyttä, jossa PDP-kontekstia pidetään jatkuvasti päällä, ei voida käyttää taloudellisista syistä. Laitevalmistajille maksetaan lisenssimaksuja mm. samanaikaisesti voimassa olevien GPRS-yhteyksien lukumäärän mukaan. Hälytyskohteiden määrän ollessa muutamia satoja kohteita kustannukset olisivat vielä siedettävät, mutta suuremmissa hälytyskohde määrissä kustannukset nousevat liian korkeiksi. Teknisiä esteitä jatkuvan GPRS-yhteyden käyttämiselle ei ole.

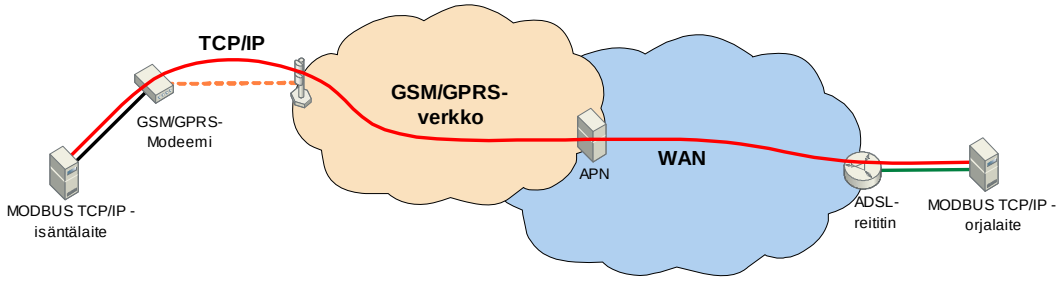
Toisena ratkaisumallina tutkittiin toteutusta, jossa Alerta-palveluverkon palvelin toimii Modbus TCP/IP -isäntälaitteena ja hälytyskohteen päätelaite Modbus TCP/IP -orjalaitteena. Ratkaisumallissa palvelimelta lähetetään päätelaitteelle toistuvia Modbus TCP/IP -pyyntösanomia, joilla luetaan päätelaitteen rekisterien tilatiedot. Ratkaisumallin todettiin edellyttävän käytännössä jatkuvan GPRS-yhteyden. Ratkaisumallin todettiin myös synnyttävän huomattavasti enemmän tiedonsiirtoa GPRS-yhteydellä kuin toteutukseen valitun ratkaisumallin, joten ratkaisumalli päätettiin hylätä.

Kolmantena ratkaisumallina tutkittiin toteutusta, jossa hälytyskohteen siirtolaitekortti toimii Modbus RTU -isäntälaitteena ja Alerta-palveluverkon palvelin Modbus RTU -orjalaitteena. Ratkaisumallissa hälytyskohteen päätelaite toimii siltalaitteena ja Modbus RTU -sanomat kapseloidaan IP-protokollan datagrammin sisään. Modbus RTU -protokollan käyttäminen edellyttää tiedonsiirtoverkolta lyhyitä vasteaikoja eikä Modbus RTU -protokollan tiedonsiirrossa käytetä vahvistuskuittausmekanismia. Lähetettyyn Modbus RTU -kyselysanomaan on saatava vastaussanoma oletuksena yhden sekunnin sisällä, muutoin kyselysanoman lähettäjä tulkitsee lähetyksen epäonnistuneen ja kyselysanoma lähetetään uudelleen. GPRS-verkon tiedonsiirrossa esiintyvien viiveaikojen ja GPRS-yhteyden muodostamiseen käytettävän merkinannon kestoajan todettiin olevan sellaiset, ettei toteutus toimisi luotettavasti, joten ratkaisumalli päätettiin hylätä.

9.2 Testiympäristö

Modbus TCP/IP -protokollan sanomanvälityksen ja GPRS-yhteyden tutkimiseksi ja testaamiseksi rakennettiin testiympäristö. Testiympäristö toteutettiin kahdella tietokoneella, joista toiseen asennettiin virtuaalinen Modbus TCP/IP -orjalaite. Orjalaitteen sisältävä tietokone liitettiin operaattorin verkkoon ADSL-reitittimen välityksellä. Toiseen Modbus TCP/IP -isäntälaitteena toimivaan tietokoneeseen liitettiin GSM/GPRS-modeemi, jota ohjattiin tietokoneelta AT-komennoilla.

GSM/GPRS-modeemin ja GGSN:n välille muodostettiin PPP-yhteys, jolla välitettiin Modbus TCP/IP -protokollan sanomia. Modbus TCP/IP -isäntälaitteelta kirjoitettiin ja luettiin orjalaitteen muistirekisterien tietoja. Testiympäristön toteutuksen todettiin toimivan ja Modbus TCP/IP -protokollan sanomanvälitys onnistuneeksi. PPP-yhteyden avaaminen ja sulkeminen, protokolla-analysaattorin kaappaukset Modbus TCP/IP -sanomista, testiympäristön päästä päähän viiveajat sekä GPRS-yhteyden linjavalvonnan tiedonsiirron määrä esitetään liitteissä 1 - 4.

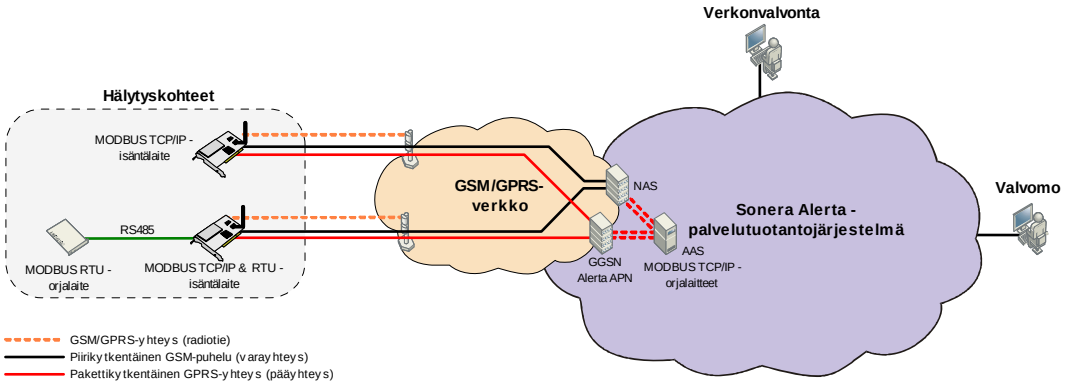


KUVIO 29. Testiympäristö

9.3 Valitun ratkaisumallin yleiskuvaus

Hälytyskohteen päätelaitteessa hälytystietojen välittämiseen käytetään Modbus RTU ja TCP/IP -protokollia. Päätelaite yhdistetään palo-, rikos- tai kiinteistöjärjestelmän keskusyksikköön. Tarvittaessa käytetään erillistä siirtolaitekorttia, joka liitetään TIA/EIA-485-standardin mukaisella sarjaväyläliitännällä päätelaitteeseen. Päätelaite toimii Modbus-isäntälaitteena, josta välitetään Modbus-sanomat GPRS-yhteydellä Alerta-palveluverkon palvelimelle. Palvelimella päätelaitteelta vastaanotettu Modbus-sanoma osoitetaan päätelaitteen hälytyskohdetta vastaavalle virtuaaliselle Modbus-orjalaitteelle. Hälytyskohteen hälytys- ja reititystietojen määrittelyt tehdään virtuaalisessa Modbus-orjalaitteessa. Hälytystietojen yhteensovittamiseksi Alerta-palvelutuotantojärjestelmään suoritetaan palvelimella protokollasovitus Alerta-palveluverkossa käytettävään SNAP-protokollaan, jolloin palvelin toimii GPRS-yhteydellä toteutetun hälytyksensiirron ja Alerta-palveluverkon välisenä rajapintana.

GPRS-yhteyden linjavalvonta toteutetaan Alerta-palveluverkon palvelimella käyttämällä Modbus-orjalaitteessa laskurirekisteriä, jolle asetetaan raja-arvo. Hälytyskohteen päätelaitteelta lähetetään palvelimelle toistuvia Modbus-sanomia, joilla nollataan Modbus-orjalaitteen laskurirekisterin arvo. Laskurirekisterin raja-arvon ylittyminen aiheuttaa linjavikahälytyksen, joka välitetään palvelimelta SNAP-protokollan sanomana Alerta-palveluverkon verkonvalvontaan ja valvomopalvelun-tarjoajan valvomoon. Päätelaitteen hallintayhteyden muodostamiseen sekä asetusten muuttamiseen tarvittavan GPRS-yhteyden herätteenä käytetään SMS-viestiä.



KUVIO 30. Valitun ratkaisumallin periaate

9.4 Hälytyskohteen päätelaite

Hälytyskohteen päätelaitteeseen muodostetaan piiri- ja pakettikytkentäisiä yhteyksiä. Piirikytkentäinen yhteys ei saa estää pakettikytkentäisen yhteyden toimintaa, joten päätelaitteessa käytetään A-luokan mobiililaitteistoa. Yhdistettäessä päätelaite hälytyksensiirtojärjestelmään toimii päätelaite Modbus TCP/IP -isäntälaitteena. Hälytyksensiirtojärjestelmän osoitteelliset hälytykset liitetään päätelaitteeseen TIA/EIA-232-E-sarjaväyläliitännällä ja silmukkahälytykset liitetään kosketintietona. Päätelaitteen varayhteys toteutetaan GSM-modeemiyhteydellä. Hälytyssilmukoiden tilatietoja ylläpidetään päätelaitteen muistirekistereissä, joiden tilatiedon muuttuessa käynnistetään toimenpiteet muuttuneen tilatiedon edelleen siirtämiseksi Alerta-palveluverkkoon. Päätelaite kytketään hälytyksensiirtojärjestelmän varmennettuun sähkönsyöttöön tai erilliseen akkuvarmennettuun virtalähteeseen.

Päätelaite voidaan myös liittää hälytyksensiirtojärjestelmään siirtolaitekortin välityksellä. Siirtolaitekortti liitetään päätelaiteeseen TIA/EIA-485-sarjaväyläliitännällä, jonka tiedonsiirrossa käytetään Modbus RTU -protokollaa. Yhdistettäessä päätelaite siirtolaitekortin välityksellä hälytyksensiirtojärjestelmään toimii päätelaite sekä Modbus RTU että Modbus TCP/IP -isäntälaitteena siirtolaitekortin toimiessa Modbus RTU -orjalaitteena. Päätelaiteelta lähetetään siirtolaitekortille toistuvia Modbus RTU -kyselysanomia, joilla luetaan siirtolaitekortin muistirekisterien tilatiedot. Siirtolaitekortilta luettuja tilatietoja verrataan päätelaitteen muistirekisterien tilatietoihin, joiden erotessa toisistaan käynnistää päätelaite vastaavat toimenpiteet muuttuneen tilatiedon edelleen siirtämiseksi kuin toimiessaan itsenäisenä yksikkönä.

Päätelaitteen ominaisuudet:

- protokollatuki: TCP/IP, Modbus TCP/IP, Modbus RTU
- A-luokan GSM/GPRS-modeemi
- neljä kosketinsisäänmenoa
- kaksi kosketinulostuloa
- TIA/EIA-232-E- ja TIA/EIA-485-sarjaliitäntäportit.

9.4.1 Päätelaitteen asetusten määrittäminen

Hälytyskohde yksilöidään IMEI-, IMSI- sekä GSM/GPRS-verkon HLR:n tilaajatietoihin IMSI-tunnisteelle määritetyllä MSISDN-tunnisteella. Hälytyskohteessa päätelaite voidaan käyttöönottaa tai siirtää toiseen hälytyskohteeseen ilman päätelaitteen asetusten manuaalista määrittelyä. Päätelaite voidaan siirtää toisen asiakkaan käyttöön vaihtamalla tilaajamoduuli eli SIM-kortti. Päätelaitteen rekisteröityessä ensimmäistä kertaa GSM-verkkoon tunnistetaan hälytyskohde päätelaitteen IMEI- ja IMSI-tunnisteesta, jolloin päätelaitteelle välitetään SMS-viestillä GPRS-verkon APN sekä Alerta-palveluverkon palvelimen IP-osoite. SMS-viestin sisältämä APN ja IP-osoite tallennetaan päätelaitteen muistirekisteriin, jonka jälkeen päätelaitteelta muodostetaan GPRS-yhteys Alerta-palveluverkon palvelimelle. Palvelimelta luetaan Modbus TCP/IP -sanomilla virtuaaliselle Modbus-orjalaitteelle määritetyt hälytyskohteen asetukset.

Päätelaitteen lähettämä Modbus TCP/IP -sanoma sisältää aina saman yksikkötunnisteen eikä yksikkötunnistetta käytetä hälytyskohteen tunnistamiseen. Hälytyskohde tunnistetaan palvelimella hälytyskohteesta muodostetun TCP/IP-yhteyden lähdeosoitteesta, jolloin Modbus TCP/IP -protokollan yksikkötunniste voidaan vakioida eikä yksikkötunnistetta tarvitse erikseen määritellä päätelaitekohtaisesti.

Päätelaitteen IP-osoitetta ei määritetä kiinteästi päätelaiteeseen, vaan päätelaitteelle jaetaan dynaaminen IP-osoite PDP-osoitteen aktivoinnin yhteydessä. Päätelaitteelle jaettava IP-osoite on sidottu päätelaitteen MSISDN-tunnisteeseen ja päätelaitteelle annetaan yleensä käyttöön sama IP-osoite. Päätelaitteen ollessa pidemmän aikaa poissa GPRS-verkosta voi IP-osoite kuitenkin vaihtua. IP-osoitteen vaihtumiseen tarvittava aika määritellään Alerta-palveluverkon AAA-palvelimella. Vaihdettaessa pääteläitteen tilaajamoduuli vaihtuu myös päätelaitteen IP-osoite.

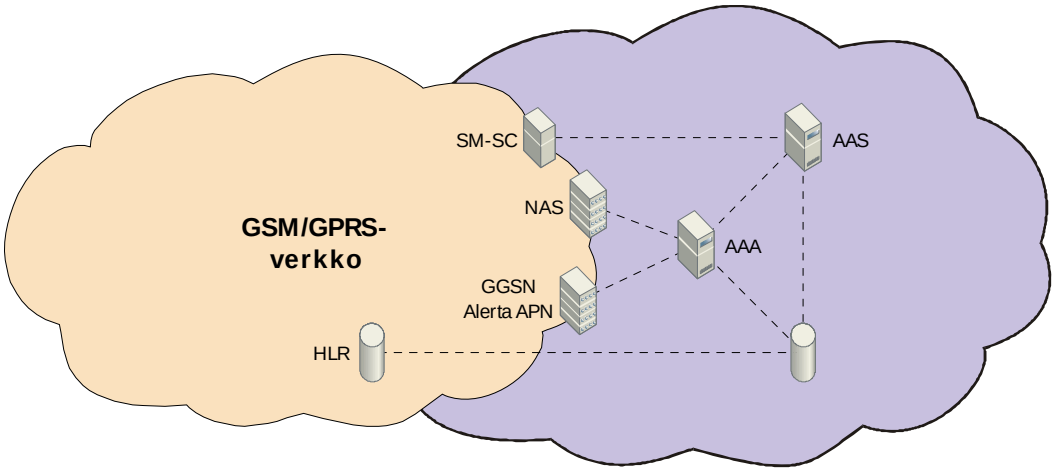
9.4.2 Hälytystiedon välittäminen päätelaitteelta

Normaalissa toimintatilassa päätelaite on GPRS-verkon liikkuvuuden hallinnan standby-tilassa. Päätelaitteen muistirekisterin tilatiedon muuttuessa siirrytään liikkuvuuden hallinnan ready-tilaan suorittamalla PDP-osoitteen aktivointi. PDP-osoitteen aktivoinnissa päätelaite saa GPRS-verkosta tiedonsiirtoon tarvittavat asetustiedot. Päätelaitteelta muodostetaan TCP/IP-yhteys Alerta-palveluverkon palvelimelle. TCP/IP-yhteyden luomisen jälkeen rakennetaan Modbus TCP/IP -protokollan pyyntösanoma, jolla kirjoitetaan muuttuneet tilatiedot palvelimen hälytyskohdetta vastaavalle virtuaaliselle Modbus TCP/IP -orjalaitteelle. Vastaanotettuaan virtuaaliselta orjalaitteelta vastaussanoman lähetettyyn Modbus TCP/IP -protokollan pyyntösanomaan päätelaite sulkee TCP/IP-yhteyden, purkaa PDP-kontekstin ja palaa takaisin GPRS-verkon liikkuvuuden hallinnan standby-tilaan.

Päätelaitteen asetuksiin voidaan määritellä toissijainen APN. GPRS-yhteyden muodostamisen epäonnistuessa ensisijaiseen APN:n yritetään GPRS-yhteyden muodostamista toissijaisen APN:n kautta. GPRS-yhteyden muodostamisen epäonnistuessa myös toissijaisen APN:n kautta tai päätelaitteelle ei ole määritelty toissijaista APN:ää siirrytään käyttämään piirikytkentäistä GSM-varayhteyttä.

9.5 Alerta-palveluverkon palvelimet

Ratkaisumallissa käytetään kolmea Alerta-palveluverkon palvelinta. Virtuaaliset Modbus TCP/IP -orjalaitteet toimivat sovelluspalvelimella AAS (Alerta Application Server). GPRS-verkon mobiililaitteiden pääsynhallintaan, IP-osoitteiden hallintaan ja yhteyksien tilastointiin käytetään AAA-palvelinta. Ratkaisussa varayhteytenä käytettävien GSM-yhteyksien verkkoon pääsyn hallintaan käytetään soittosarjajärjestelmänä toimivaa verkkoyhteyspalvelinta NAS (Network Access Server). AAA- ja AAS-palvelimet sekä GPRS-verkon HLR käyttävät yhteistä tietokantaa orjalaitteisiin liittyvien tietojen ylläpitoon. AAS-palvelimelta välitetään SM-SC:n kautta SMS-viestejä, joita käytetään herätteenä hälytyskohteen päätelaitteelle Modbus-orjalaitteen asetusten lukemiseksi AAS-palvelimelta ja päätelaitteen hallintayhteyden muodostamisen käynnistämiseksi päätelaitteelta.



KUVIO 31. Alerta-palvelutuotantojärjestelmän hallinta- ja ohjaustiedon välitys

Ratkaisumallissa AAA-palvelimen tehtävänä on hallinnoida hälytyskohteiden päätelaitteille jaettavia IP-osoitteita ja suorittaa tilastointia. Tarvittaessa päätelaite voidaan todentaa AAA-palvelimella käyttämällä PAP- (Password Authentication Protocol) tai CHAP-protokollaa (Challenge Handshake Authentication Protocol). Ratkaisumallissa ei kuitenkaan pääsääntöisesti käytetä AAA-palvelinta päätelaitteen todentamiseen, vaan luotetaan GPRS-verkon suorittamaan päätelaitteen todentamiseen.

AAA-palvelimella käytetään DHCP-protokollaa (Dynamic Host Configuration Protocol) IP-osoitteiden jakamiseen päätelaitteille. Päätelaitteen IP-osoite määritetään GGSN:ltä vastaanotetun pääsy pyyntö -sanoman sisältämän MSISDN-tunnisteen perusteella. Hälytyskohteen päätelaite saa käyttöönsä saman IP-osoitteen, ellei DHCP-pitoaika ole ylittynyt. Käytettävä DHCP-pitoaika on vapaasti määriteltävissä. Tarvittaessa AAA-palvelimella voidaan määrittää päätelaitteen MSISDN-tunnisteelle pysyvä IP-osoite, jolloin IP-osoite ei vaihdu, vaikka päätelaite olisi pidemmän aikaa poissa GPRS-verkosta.

Hälytyskohdetta käyttöön otettaessa määritetään GPRS-verkon HLR:n tilaajatiedot mm. IMSI- ja MSISDN-tunnisteet, jotka kirjoitetaan AAA- ja AAS-palvelimien käyttämään tietokantaan. Tietokannasta ei lueta tietoja HLR:lle. Määritettäessä virtuaalisen Modbus TCP/IP -orjalaitteen tila-, hälytys- ja reititystietoja luetaan tietokantaan HLR:ltä kirjoitetut tilaajatiedot IMSI-tunnisteen perusteella. Hälytyskohteen tietojen määrittelyn jälkeen tiedot tallennetaan tietokantaan.

9.5.1 AAA-palvelin

AAA-palvelin toimii RADIUS-protokollan isäntänä, ja GGSN asiakkaana. Käytettäessä GSM-varayhteyttä asiakkaana toimii NAS-palvelin vastaavalla tavoin kuin GGSN käytettäessä GPRS-yhteyttä. Vastaanotettaessa PDP-kontekstin luontipyyntö GGSN:llä lähetetään AAA-palvelimelle RADIUS-protokollan pääsy pyyntö -sanoma, joka sisältää päätelaitteen yksilöivän MSISDN-tunnisteen. AAA-palvelimelta palautetaan pääsy hyväksytty -sanoma, joka sisältää päätelaitteelle määritettävän IP-osoitteen. Vastaanotettaessa AAA-palvelimelta pääsy hyväksytty -sanoma GGSN:ltä lähetetään AAA-palvelimelle tilastoinnin aloituspyyntö -sanoma, joka sisältää päätelaitteen MSISDN-tunnisteen ja päätelaitteelle määritettävän IP-osoitteen. AAA-palvelimelta pyyntö välitetään AAS-palvelimelle. AAS-palvelimella IP-osoite määritetään MSISDN-tunnistetta vastaavan Modbus TCP/IP -orjalaitteen tietoihin ja palautetaan vastaus AAA-palvelimelle. AAA-palvelimella käynnistetään RADIUS-tilastointi ja palautetaan GGSN:lle tilastoinnin aloitus -vastaussanoma, jonka vastaanotettuaan GGSN:ltä palautetaan SGSN:lle vastaus PDP-kontekstin luontipyyntöön.

IP-osoitteen määrittämisen epäonnistuessa AAS-palvelimella esim. AAS-palvelimella ei ole MSISDN-tunnistetta vastaavaa Modbus TCP/IP -orjalaitetta palautetaan AAA-palvelimelle hylkäystieto, jolloin AAA-palvelimelta palautetaan GGSN:lle tilastoinnin hylkäys -sanoma. GGSN:llä keskeytetään PDP-kontekstin luonti ja palautetaan SGSN:lle PDP-kontekstin luontipyynnön hylkäys. Purettaessa PDP-konteksti GGSN:ltä välitetään AAA-palvelimelle tilastoinnin lopetuspyyntö -sanoma, jolloin AAA-palvelimella lopetetaan RADIUS-tilastointi.

9.5.2 AAS-palvelin

AAS-palvelimella ylläpidetään hälytyskohteiden virtuaalisia Modbus TCP/IP -orjalaitteita. AAS-palvelimella toimiva virtuaalinen Modbus TCP/IP -orjalaite on sovellus, johon on ohjelmallisesti toteutettu Modbus TCP/IP -orjalaitteen toiminnallisuudet sekä vastaavia toiminnallisuuksia kuin AT101- ja AT301-laitteissa. Hälytyskohteen määritellyt tehdään virtuaaliselle Modbus TCP/IP -orjalaitteelle vastaavasti kuin AT101- ja AT301-laitteisiin. Virtuaaliseen Modbus TCP/IP -orjalaitteeseen määritellään hälytyspisteet ja -lajit sekä valvomotaulukkoon Alerta-palveluverkon reititysmääritykset. Alerta-palveluverkon näkökulmasta virtuaalinen Modbus TCP/IP -orjalaite on yksi hälytyskohde muiden fyysisten hälytyskohteiden joukossa.

AAS-palvelimella käytetään hälytyskohteen yksilöivänä tunnisteena TCP/IP-yhteyden lähdeosoitetta, jonka perusteella päätelaitteelta vastaanotetut Modbus TCP/IP -pyyntösanomat ohjataan hälytyskohdetta vastaavalle virtuaaliselle Modbus TCP/IP -orjalaitteelle. Modbus TCP/IP -pyyntösanoma sisältää aina saman yksikkötunnisteen eikä sitä käytetä hälytyskohteen tunnistamiseen. Modbus TCP/IP -pyyntösanomalla kirjoitetaan virtuaalisen Modbus TCP/IP -orjalaitteen muistirekisteriin hälytyskohteen muuttunut tilatieto. Virtuaalisen Modbus TCP/IP -orjalaitteen hälytysmääritysten perusteella muodostetaan Alerta-palvelutuotantojärjestelmään yhteensopiva SNAP-protokollan sanoma, joka välitetään AAS-palvelimelta virtuaalisen Modbus TCP/IP -orjalaitteen reititysmääritysten mukaisesti Alerta-palveluverkkoon.

9.6 GPRS-yhteyden linjavalvonta

Hälytyskohteen päätelaitteen GPRS-yhteyden linjavalvonta toteutetaan Alerta-palveluverkon AAS-palvelimella virtuaalisen Modbus TCP/IP -orjalaitteen laskurirekisterillä, jolle asetetaan raja-arvo. Laskurirekisterin arvo nollataan säännöllisin väliajoin lähettämällä hälytyskohteen päätelaitteelta Modbus TCP/IP -pyyntösanoma, jolla kirjoitetaan laskurirekisteriin nolla-arvo. Laskurirekisterin raja-arvon ylittyessä käynnistetään AAS-palvelimella toimenpiteet linjavikatiedon välittämiseksi verkonvalvontaan ja valvomopalvelutarjoajan valvomoon. Valvomopalveluntarjoajan valvomoon linjavikatieto välitetään Alerta- palvelutuotantojärjestelmään yhteensopivana SNAP-protokollan sanomana, joka sisältää tiedon vikaantuneesta hälytyskohteesta. Toteutus linjavikatiedon välittämiseksi verkonvalvontaan on vapaasti toteutettavissa.

Pelastusviranomaisvaatimuksissa asetetaan paloilmoituksensiirron linjavikatiedon välittämiselle valvomoon 100 sekunnin maksimiaika, joten laskurirekisterin arvo on nollattava tämän aikajakson sisällä. GPRS-yhteyden tiedonsiirrosta syntyy taloudellisia kustannuksia, joten Modbus TCP/IP -pyyntösanomien lähetysväli on pidettävä mahdollisimmin suurena kustannusten minimoimiseksi. Ratkaisumallissa Modbus TCP/IP -pyyntösanomien lähetysväliksi valittiin 80 sekuntia.

Modbus TCP/IP -protokollan tiedonsiirrossa käytetään vahvistuskuittaus-menetelmää, joten lähetettyyn Modbus TCP/IP -pyyntösanomaan saadaan periaatteessa aina vastaus edellyttäen, että TCP-yhteys on toiminnassa. Ratkaisumallissa odotetaan lähetetyn Modbus TCP/IP -pyyntösanoman vahvistussanomaa Modbus TCP/IP -orjalaitteelta 80 sekunnin ajan, jonka jälkeen Modbus TCP/IP -pyyntösanoman lähetystä pidetään epäonnistuneena ja pienennetään pyyntösanomien lähetysväli viiteen sekuntiin. Modbus TCP/IP -pyyntösanomien lähetysväli pidetään viidessä sekunnissa, kunnes Modbus TCP/IP -pyyntösanomaan saadaan vahvistussanoma, jolloin palataan takaisin 80 sekunnin lähetysväliin. Toteutuksella pyritään ehkäisemään aiheettoman linjavikahälytyksen syntyminen tilanteessa, jossa yksittäisen Modbus TCP/IP -pyyntösanoman välittäminen on epäonnistunut. Epäonnistuneista Modbus TCP/IP -pyyntösanoman lähetyksistä kerätään lokitietoa, jota voidaan hyödyntää vianselvityksessä.

9.7 Hälytysliikenteen priorisointi ja palvelunlaatu

Käytettäessä dynaamista radiorajapinnan resurssien hallintaa GPRS-tiedonsiirto on radiokanavilla alemmalla prioriteetille kuin piirikytkentäiset GSM-puhelut, joten ruuhkatilanteessa GPRS-palvelun käyttö voi estyä. GPRS-palvelun saatavuuden varmistamiseksi mobiililaitetta palvelevaan soluun on määritettävä kiinteästi vähintään yksi TDMA-aikaväli GPRS-tiedonsiirrolle. Hälytysliikenne on ns. kriittistä liikennettä, joten hälytyksensiirtoon liittyvä GPRS-yhteyden tiedonsiirto on priorisoitava radiorajapinnassa korkeammalle prioriteetille kuin muu tiedonsiirto. Radiorajapinnan priorisointia ei kuitenkaan ole toteutettu Soneran GPRS-verkossa. Teknistä estettä radiorajapinnan priorisoinnille ei ole.

GPRS-yhteydellä välitettävä Modbus TCP/IP -protokolla ei aseta vaatimuksia GPRS-verkon viiveajoille, mutta pelastusviranomaisvaatimuksissa asetetaan paloilmoitinjärjestelmän hälytystiedon välittämiselle valvomoon 10 sekunnin maksimiaika. Pelastusviranomaisvaatimusten täyttämiseksi määritellään GPRS-tiedonsiirto viiveluokkaan yksi, jota myös suunnitellun ratkaisumallin GPRS-yhteyden linjavalvonnan toteutus edellyttää käytettäväksi. Hälytyksensiirron onnistuminen GPRS-verkon ruuhkatilanteessa varmistetaan määrittelemällä GPRS-tiedonsiirto prioriteettiluokkaan yksi, jonka käyttäminen myös pienentää tiedonsiirron maksimiviiveaikaa GPRS-verkon normaalissa toimintatilassa.

Modbus TCP/IP -protokollassa käytetään vahvistuskuittaus-menetelmää tiedonsiirrossa tapahtuneiden virheiden havaitsemiseen ja tiedonsiirron aikana korruptoituneen datan korjaamiseen, joten GPRS-yhteydellä voidaan käyttää luotettavuusluokkaa kolme. Luotettavuusluokka kolme on nimenomaan tarkoitettu ei-reaaliaikaiselle tiedonsiirrolle, joka sisältää menetelmän tiedonsiirrossa tapahtuneiden virheiden havaitsemiseksi ja tiedonsiirron aikana korruptoituneen datan korjaamiseksi.

Suunnitellussa ratkaisumallissa GPRS-yhteydellä välitettävän tiedonsiirron määrä on vähäistä, joten keskimääräinen datan läpäisykyky määritellään best effort -periaatteella. Prioriteettiluokan yksi käyttäminen parantaa keskimääräistä datan läpäisykykyä, koska korkeammalle prioriteetille määritetylle GPRS-yhteydelle

tarjotaan GPRS-verkon resursseja ennen alemman prioriteetin GPRS-yhteyksiä. GPRS-yhteydelle määritetyn maksimaalisen datan läpäisykykyluokan toteutumiselle ei anneta takeita, joten maksimaalinen datan läpäisykykyluokka jätetään määrittelemättä.

Käytettäessä piirikytkentäistä GSM-varayhteyttä tiedonsiirrolle ei tarvitse määritellä palvelunlaatua tai priorisoida tiedonsiirtoa. Hälytyskohteen päätelaitteelta muodostetulle GSM-yhteydelle varataan GSM-verkosta kiinteä resurssi, jota ei jaeta muiden GSM-verkon käyttäjien kanssa. Hälytyskohteen päätelaitteen GSM-yhteyden muodostaminen voidaan määritellä muita GSM-yhteyksiä korkeammalle prioriteetille. Soneran GSM-verkon estotodennäköisyyttä kiiretunnin aikana pidettiin riittävän pienenä, joten GSM-yhteyden muodostamisen priorisointia ei nähty tarpeelliseksi. Ratkaisumallissa tilannetta, jossa on siirrytty käyttämään GSM-varayhteyttä, pidetään virhetilanteena. Hälytyskohteen päätelaitteen tiedonsiirtoyhteyteen suhtaudutaan kuin tiedonsiirtoyhteyttä ei olisi lainkaan ja hälytyksensiirtoa hälytyskohteen päätelaitteelta pidetään estyneenä.

10 YHTEENVETO

Työtä pidetään pääosin onnistuneena. Työssä suunniteltu ratkaisumalli hälytyksensiirron toteuttamiseksi GPRS-yhteydellä täyttää asetetut lähtövaatimukset. Työstä on kuitenkin todettava sen olevan osittain teoreettinen tarkastelu. Nykyisissä Sonera Alerta -palveluiden päätelaitteissa ei ole GPRS-palvelua tuettuna, joten ratkaisumallin toimivuuden testaamiseen ei voitu käyttää käytössä olevia päätelaitteita. Hälytyksensiirron testaamiseksi rakennettiin testiympäristö, jossa käytettiin GPRS-palvelua tukevaa päätelaitetta. Käytetyssä päätelaitteessa ei kuitenkaan ole vastaavanlaisia toiminnallisuuksia kuin Sonera Alerta -palveluissa käytettävissä päätelaitteissa. Sonera Alerta -palveluiden päätelaitteet sisältävät Alerta-spesifisiä ratkaisuja, joten testiympäristön päätelaitteen ohjelmistoon olisi tarvinnut tehdä muutoksia. Sovellusohjelmointi ei sisälly työntekijän osaamisalueen eikä työn varsinaisen aihealueeseen. Modbus-protokollaa käytetään jo olemassa olevissa ratkaisuissa hälytyskohteen päätelaitteen ja hälytysjärjestelmän välisessä tiedonsiirrossa. Lisäksi päätelaitteisiin on toteutettu protokollamuunnos Modbus-protokollasta SNAP-protokollaan, jonka sanomien välittämiseen kiinteillä tiedonsiirtoyhteyksillä käytetään TCP/IP-protokollaa. Tarvittava tieto protokollamuunnoksesta ja TCP/IP-protokollan käyttämisestä hälytyksensiirtoon on jo olemassa, joten sovellusohjelmointia ei pidetty tarpeellisena työn toteutuksen kannalta.

Ilmoituksensiirtojärjestelmille asetettavien vaatimusten osalta on todettava, ettei ratkaisumalli täytä CEA 4039 -standardissa luokan kolme rikosilmoitinjärjestelmän ilmoituksensiirtojärjestelmän linjavikatiedon välittämiselle asetettua 20 sekunnin maksimiaikaa. Ratkaisumallissa linjavalvonnan toteutuksessa käytettävien Modbus TCP/IP -pyyntösanomien lähetysvälinä käytetään 80 sekuntia. Rikosilmoitinjärjestelmän ilmoituksensiirtojärjestelmän linjavikatiedon välittämiselle asetettu vaatimus voidaan täyttää pienentämällä Modbus TCP/IP -pyyntösanoman lähetysväliä. Lähetysvälin pienentäminen kuitenkin moninkertaistaa linjavalvonnan synnyttämän tiedonsiirron määrän, joka vastaavasti kasvattaa taloudellisia kustannuksia. Käytettäessä suunniteltua ratkaisumallia kiinteän tiedonsiirtoyhteyden varmentavana yhteytenä on linjavalvonnan Modbus TCP/IP -pyyntösanoman lähetysväli vapaasti määriteltävissä tai linjavalvonta voidaan jättää kokonaan pois.

Suunniteltua ratkaisumallia ei voitu toteuttaa pelkästään GPRS-palvelua käyttämällä, vaan jouduttiin käyttämään erillistä SMS-viestillä tehtävää herätettä GPRS-yhteyden muodostamiseksi päätelaitteelta. Ongelman aiheutti PDP-kontekstin aktivointi päätelaitteelta GPRS-verkon pyynnöstä. ETSI:n standardeissa määritellään menetelmä PDP-kontekstin aktivoimiseksi päätelaitteelta GPRS-verkon pyynnöstä, mutta menetelmälle ei ole tällä hetkellä tukea Soneran GPRS-verkon laitteistoissa. On hyvin todennäköistä, että GPRS-verkon laitteistoihin tulee tulevaisuudessa tuki PDP-kontekstin aktivoinnille GPRS-verkon pyynnöstä. Osalla laitevalmistajista on jo olemassa ratkaisuja edeltävän toteuttamiseksi. GPRS-verkon laitteistojen tukiessa PDP-kontekstin aktivointia GPRS-verkon pyynnöstä voidaan hälytyksensiirto GPRS-yhteydellä toteuttaa käyttämällä vain GPRS-palvelua.

GPRS-verkon tukiessa PDP-kontekstin aktivointia GPRS-verkon pyynnöstä linjavalvonta voidaan toteuttaa GPRS-verkosta päätelaitteelle tehtävillä kyselyillä ja erottaa varsinaisesta hälytyksensiirtoon käytettävästä ratkaisusta omaksi erilliseksi kokonaisuudekseen. Linjavalvonta voidaan toteuttaa esim. GPRS-verkon takana olevalta palvelimelta tehtävillä ICMP-kyselyillä (Internet Control Message Protocol), jolloin linjavalvonnan synnyttämän tiedonsiirron määrä on n. 40 % pienempi verrattuna työssä suunnitellun ratkaisumallin linjavalvonnan synnyttämään tiedonsiirron määrään. TeliaSonera DataNet mobiili varayhteys -palvelussa käytetään tähän tarkoitukseen soveltuvaa ratkaisua. Linjavalvonnan toteuttamista GPRS-verkosta päätelaitteelle tehtävillä kyselyillä pidetään parempana ratkaisuna kuin suunnitellun ratkaisumallin linjavalvonnan toteutusta.

Työssä käytetty Modbus-protokolla ei itsessään tarjoa lisäarvoa jo olemassa oleviin ratkaisuihin. Hälytyksensiirron toteuttamiseen voidaan käyttää myös muita protokollia, jotka sietävät GPRS-yhteyden tiedonsiirrossa esiintyviä vaihtelevia ja pitkiä viiveaikoja. Modbus-protokolla käyttäminen myös osittain rajoittaa ratkaisumallissa esitetyn toteutuksen käytettävyyttä. Ratkaisumallia voidaan käyttää hälytyskohteissa, joiden hälytysjärjestelmä tukee Modbus-protokollaa. Työssä esitetyt GPRS-palveluun liittyvät asiat ovat yleispäteviä, joten ne pätevät myös muilla protokollilla toteutettaviin ratkaisuihin.

Nykyisissä ratkaisuissa hälytyskohteen hälytys- ja reititysmäärittelyt määritellään päätelaitteeseen, lisäksi päätelaitteessa tehdään protokollasovitus Alerta-palveluverkossa käytettävään SNAP-protokollaan. Suunnitellussa ratkaisumallissa pyrittiin vakioimaan päätelaitteen määrittelyt ja toteuttamaan päätelaitteiden hallinnointi keskitetysti, joten protokollamuunnosta SNAP-protokollaan ei voida tehdä päätelaitteessa. Hälytyskohteen hälytys- ja reititysmäärittelyt sekä protokollamuunnos SNAP-protokollaan tehdään Alerta-palveluverkon AAS-palvelimella.

Jatkotoimenpiteenä on selvitettävä suunnitellun ratkaisumallin soveltuvuus suurempiin kokonaisuuksiin. Suunnitellussa ratkaisumallissa AAS-palvelimella pidetään hälytyskohteiden virtuaalisia Modbus TCP/IP -orjalaitteita jatkuvasti päällä, joka synnyttää AAS-palvelimelle kuormitusta. Palvelimen kuormitusta voidaan pienentää toteutuksella, jossa virtuaalinen Modbus TCP/IP -orjalaite käynnistetään AAS-palvelimella vain tarvittaessa. Suunnitellun ratkaisumallin linjavalvonta on kuitenkin toteutettu virtuaalisessa Modbus TCP/IP -orjalaitteessa, joten AAS-palvelimen kuormituksen pienentyessä vastaavasti AAS-palvelimelta tehtävien tietokanta kyselyiden määrä kasvaa. AAS-palvelimen kuormituksen pienentämiseksi on linjavalvonnan toteutus erotettava hälytyksensiirtoratkaisusta, jolloin virtuaalinen Modbus TCP/IP -orjalaite käynnistetään palvelimella vain hälytystilanteessa tai muutettaessa virtuaalisen Modbus TCP/IP -orjalaitteen tai hälytyskohteen päätelaitteen määrityksiä. Linjavalvonnan erottaminen kuitenkin edellyttää GPRS-verkolta tuen PDP-kontekstin aktivoinnille GPRS-verkon pyynnöstä.

Hälytystiedon välittämiselle hälytyskohteesta valvomoon asetetaan 10 sekunnin maksimiaika. GPRS-yhteyden tiedonsiirrossa esiintyy viiveitä, jolloin hälytystiedon välittämiselle asetettu maksimiaika voi ylittyä. Lisäksi GSM-verkon ruuhkatilanteessa GPRS-palvelun käyttö voi estyä kokonaan. Hälytystiedon välittämiselle asetetun maksimiaika vaatimuksen täyttämiseksi on GPRS-palvelulle varattava kiinteä resurssi GSM-verkosta ja GPRS-tiedonsiirrossa käytettävä priorisointia. Hälytyksensiirron toteuttaminen GPRS-yhteydellä vaatii radiorajapinnan priorisoinnin käyttöönottamisen Soneran GPRS-verkossa.

LÄHTEET

Acromag Inc. 2005. Introduction to Modbus TCP/IP, Technical Reference [verkkojulkaisu]. Acromag Inc. [viitattu 9.2.2008]. Saatavissa: http://www.acromag.com/pdf/intro_modbusTCP_765a.pdf

CEA. 2002. CEA 4039: 2002-08 (fi) - Tavoitteelliset vaatimukset ilmoitusten siirtojärjestelmille (ISJ) [verkkojulkaisu]. CEA [viitattu 9.2.2008]. Saatavissa: http://www.fkl.fi/asp/ida/download.asp?pgid=3079&pgmain=fkl-www&prm1=wwwuser_fkl&docid=1143&sec=&ext=.pdf

Computec Oy. 2004. T2-3 asennus- ja testausohje.

ETSI. 2000a. ETSI TS 100 522 V7.1.0 (2000-02) - Digital cellular telecommunications system (Phase 2+); Network architecture (GSM 03.02 version 7.1.0 Release 1998) [verkkojulkaisu]. ETSI [viitattu 9.2.2008]. Saatavissa: http://webapp.etsi.org/exchangefolder/ts_100522v070100p.pdf

ETSI. 2000b. ETSI TS 101 113 V7.5.0 (2000-07) - Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1 (GSM 02.60 version 7.5.0 Release 1998) [verkkojulkaisu]. ETSI [viitattu 9.2.2008]. Saatavissa: http://webapp.etsi.org/exchangefolder/ts_101113v070500p.pdf

ETSI. 2000c. ETSI EN 301 344 V7.4.1 (2000-09) - Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2 (GSM 03.60 version 7.4.1 Release 1998) [verkkojulkaisu]. ETSI [viitattu 9.2.2008]. Saatavissa: http://webapp.etsi.org/exchangefolder/en_301344v070401p.pdf

ETSI. 2001a. ETSI TS 101 622 V6.0.1 (2001-02) - Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network (PLMN) (GSM 01.02 version 6.0.1 Release 1997) [verkkojulkaisu]. ETSI [viitattu 9.2.2008]. Saatavissa: http://webapp.etsi.org/exchangefolder/ts_101622v060001p.pdf

ETSI. 2001b. ETSI TS 100 901 V7.5.0 (2001-12) - Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) (3GPP TS 03.40 version 7.5.0 Release 1998) [verkkojulkaisu]. ETSI [viitattu 9.2.2008]. Saatavissa: http://webapp.etsi.org/exchangefolder/ts_100901v070500p.pdf

ETSI. 2003. ETSI TS 100 916 V7.8.0 (2003-03) - Digital cellular telecommunications system (Phase 2+); AT Command set for GSM Mobile Equipment (ME) (3GPP TS 07.07 version 7.8.0 Release 1998) [verkkojulkaisu]. ETSI [viitattu 9.2.2008]. Saatavissa: http://webapp.etsi.org/exchangefolder/ts_100916v070800p.pdf

ETSI. 2005. ETSI TS 101 348 V7.10.1 (2005-06) - Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN) (3GPP TS 09.61 version 7.10.1 Release 1998) [verkkojulkaisu]. ETSI [viitattu 9.2.2008]. Saatavissa: http://webapp.etsi.org/exchangefolder/ts_101348v071001p.pdf

Modbus-IDA. 2006a. Modbus Application Protocol Specification V1.1b [verkkojulkaisu]. Modbus-IDA [viitattu 9.2.2008]. Saatavissa: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

Modbus-IDA. 2006b. Modbus Messaging on TCP/IP Implementation Guide V1.0b [verkkojulkaisu]. Modbus-IDA [viitattu 9.2.2008]. Saatavissa: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

Modbus-IDA. 2006c. Modbus over Serial Line Specification and Implementation Guide V1.02 [verkkojulkaisu]. Modbus-IDA [viitattu 9.2.2008]. Saatavissa: http://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

Modicon Inc. 1996. Modicon Modbus Protocol Reference Guide [verkkojulkaisu]. Modicon Inc [viitattu 9.2.2008]. Saatavissa: http://www.modbus.org/docs/PI_MBUS_300.pdf

Postel, J. 1981a. RFC 791 - Internet Protocol [verkkojulkaisu]. IETF [viitattu 9.2.2008]. Saatavissa: http://tools.ietf.org/html/rfc791

Postel, J. 1981b. RFC 793 - Transmission Control Protocol [verkkojulkaisu]. IETF [viitattu 9.2.2008]. Saatavissa: http://tools.ietf.org/html/rfc793

Rigney, C., Rubens, A., Simpson, W. & Willens, S. 2000. RFC 2865 - Remote Authentication Dial In User Service (RADIUS) [verkkojulkaisu]. IETF [viitattu 9.2.2008]. Saatavissa: http://tools.ietf.org/html/rfc2865

Schneider Electric. 2004. Modicon Modbus Plus Network Planning and Installation Guide, Version 6.0 [verkkojulkaisu]. Schneider Electric [viitattu 9.2.2008]. Saatavissa: http://download.telemecanique.com/85256D9800508A23/all/852566B70073220C85256AAA004B9FB6/$File/31003525_k03_000_03.pdf

Simpson, W. 1994. RFC 1661 - The Point-to-Point Protocol (PPP) [verkkojulkaisu]. IETF [viitattu 9.2.2008]. Saatavissa: http://tools.ietf.org/html/rfc1661

Sähkötieto ry. 2002. Kulunvalvonta- ja rikosilmoitinjärjestelmät. Sähkötekniset tietojärjestelmät: ST-käsikirja 11. 3. uusittu painos. Espoo: Sähköinfo Oy.

Sähkötieto ry. 2001. Rakennusautomaatiojärjestelmät. Sähkötekniset tietojärjestelmät: ST-käsikirja 17. 2. uusittu painos. Espoo: Sähköinfo Oy.

Sähkötieto ry. 2003. Videovalvontajärjestelmät. Sähkötekniset tietojärjestelmät: ST-käsikirja 13. 3. uudistettu painos. Espoo: Sähköinfo Oy.

Sähkötieto ry. 2004. Paloilmoitinjärjestelmät. Sähkötekniset tietojärjestelmät: ST-käsikirja 10. 4. tarkistettu painos. Espoo: Sähköinfo Oy.

TeliaSonera Finland Oyj. 2003. Sonera Alerta -konserniratkaisu. Esite.

TeliaSonera Finland Oyj. 2004. Sonera Kuvavalvontapalvelu. Palvelukuvaus.

TeliaSonera Finland Oyj. 2005a. AT101. Asennusohje.

TeliaSonera Finland Oyj. 2005b. AT301 ja ATE. Asennusohje.

TeliaSonera Finland Oyj. 2005c. Alerta Laajakaista. Palvelukuvaus.

TeliaSonera Finland Oyj. 2005d. Sonera Hälytys- ja ohjauspalvelut, Lite. Palvelukuvaus.

TeliaSonera Finland Oyj. 2005e. Sonera Talotekniikkayhteys Plus. Palvelukuvaus.

TeliaSonera Finland Oyj. 2006a. TeliaSonera DataNet. Palvelukuvaus.

TeliaSonera Finland Oyj. 2006b. Sonera FastNet. Palvelukuvaus.

TeliaSonera Finland Oyj. 2006c. Sonera Valvomopalvelu. Palvelukuvaus.

TeliaSonera Finland Oyj. 2007a. Sonera Hälytys- ja ohjauspalvelut, Prime. Palvelukuvaus.

TeliaSonera Finland Oyj. 2007b. Sonera Hälytys- ja ohjauspalvelut, Pro. Palvelukuvaus.

LIITTEET

PPP-yhteyden avaaminen:

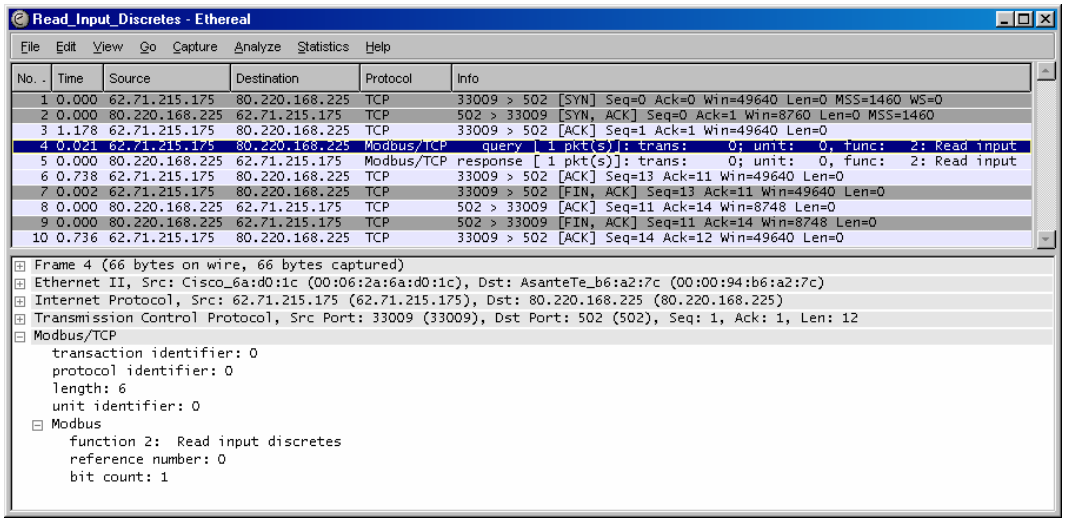
```
serial speed set to 115200 bps
AT
OK
connect option: '/etc/ppp/connect' started (pid 1665)
ATH
OK
ATE1
OK
AT+CGDCONT=1,"IP","prointernet","0.0.0.0",0,0
OK
ATD*99#
CONNECT
Serial connection established.
serial speed set to 115200 bps
Using interface sppp1
Connect: sppp1 <--> /dev/term/0
sent [LCP ConfReq id=0x14 <asyncmap 0xa0000> <magic 0x5a6b3cb5>]
rcvd [LCP ConfRej id=0x14 <magic 0x5a6b3cb5>]
sent [LCP Ident id=0x15 magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Nov
6 2006 21:53:17)"]
sent [LCP ConfReq id=0x16 <asyncmap 0xa0000>]
rcvd [LCP CodeRej id=0x0 0c 15 00 42 00 00 00 00 70 70 70 2d 32 2e 34 2e 30
62 31 20 28 53 75 6e 20 4d 69 63 72 6f 73 79 ...]
LCP: Rcvd Code-Reject for Identification id 21
rcvd [LCP ConfAck id=0x16 <asyncmap 0xa0000>]
rcvd [LCP ConfReq id=0x0 <auth pap> <mru 1500> <asyncmap 0xa0000>]
sent [LCP ConfAck id=0x0 <auth pap> <mru 1500> <asyncmap 0xa0000>]
LCP: Peer has rejected Identification; not sending another
Authenticating to peer with PAP
sent [PAP AuthReq id=0x1 user="********" password="********"]
rcvd [PAP AuthAck id=0x1 ""]
sent [IPCP ConfReq id=0x54 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns2
0.0.0.0>]
rcvd [IPCP ConfReq id=0x0 <addr 10.6.6.6>]
sent [IPCP ConfAck id=0x0 <addr 10.6.6.6>]
sent [IPCP ConfReq id=0x54 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns2
0.0.0.0>]
rcvd [IPCP ConfNak id=0x54 <addr 62.71.218.100> <ms-dns1 192.89.123.230>
<ms-dns2 192.89.123.231>]
sent [IPCP ConfReq id=0x55 <addr 62.71.218.100> <ms-dns1 192.89.123.230>
<ms-dns2 192.89.123.231>]
rcvd [IPCP ConfAck id=0x55 <addr 62.71.218.100> <ms-dns1 192.89.123.230>
<ms-dns2 192.89.123.231>]
local  IP address 62.71.218.100
remote IP address 10.6.6.6
primary   DNS address 192.89.123.230
secondary DNS address 192.89.123.231
```

PPP-yhteyden sulkeminen:

Terminating on signal 2.
sent [LCP TermReq id=0x18 "No network protocols running"]
rcvd [LCP TermAck id=0x18]
Connection terminated.
Connect time 0.3 minutes.
Sent 555 bytes (12 packets), received 581 bytes (10 packets).
serial speed set to 115200 bps

Sending break to the modem
disconnect option: '/etc/ppp/disconnect' started (pid 1667)
Serial link disconnected.

Erillisen tulon tilatiedon lukeminen (Funktiokoodi 0x02: Read Discrete Inputs)



No. Time Source Destination Protocol Info
1 0.000 62.71.215.175 80.220.168.225 TCP 33009 > 502 [SYN] Seq=0 Ack=0 Win=49640 Len=0 MSS=1460 WS=0
Frame 1 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33009 (33009), Dst Port: 502 (502), Seq: 0, Ack: 0, Len: 0

No. Time Source Destination Protocol Info
2 0.000 80.220.168.225 62.71.215.175 TCP 502 > 33009 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1460
Frame 2 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c), Dst: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c)
Internet Protocol, Src: 80.220.168.225 (80.220.168.225), Dst: 62.71.215.175 (62.71.215.175)
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 33009 (33009), Seq: 0, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
3 1.178 62.71.215.175 80.220.168.225 TCP 33009 > 502 [ACK] Seq=1 Ack=1 Win=49640 Len=0
Frame 3 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33009 (33009), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 0

No. Time Source Destination Protocol
4 0.021 62.71.215.175 80.220.168.225 Modbus/TCP
Info: query [1 pkt(s)]: trans: 0; unit: 0, func: 2: Read input discretes.

Frame 4 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33009 (33009), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
Modbus/TCP
transaction identifier: 0
protocol identifier: 0
length: 6
unit identifier: 0
Modbus
function 2: Read input discretes
reference number: 0
bit count: 1

No. Time Source Destination Protocol
5 0.000 80.220.168.225 62.71.215.175 Modbus/TCP
Info: response [1 pkt(s)]: trans: 0; unit: 0, func: 2: Read input discretes.

Frame 5 (64 bytes on wire, 64 bytes captured)
Ethernet II, Src: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c), Dst: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c)
Internet Protocol, Src: 80.220.168.225 (80.220.168.225), Dst: 62.71.215.175 (62.71.215.175)
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 33009 (33009), Seq: 1, Ack: 13, Len: 10
Modbus/TCP
transaction identifier: 0
protocol identifier: 0
length: 4
unit identifier: 0
Modbus
function 2: Read input discretes
byte count: 1
Data

No. Time Source Destination Protocol Info
6 0.738 62.71.215.175 80.220.168.225 TCP 33009 > 502 [ACK] Seq=13 Ack=11 Win=49640 Len=0
Frame 6 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33009 (33009), Dst Port: 502 (502), Seq: 13, Ack: 11, Len: 0

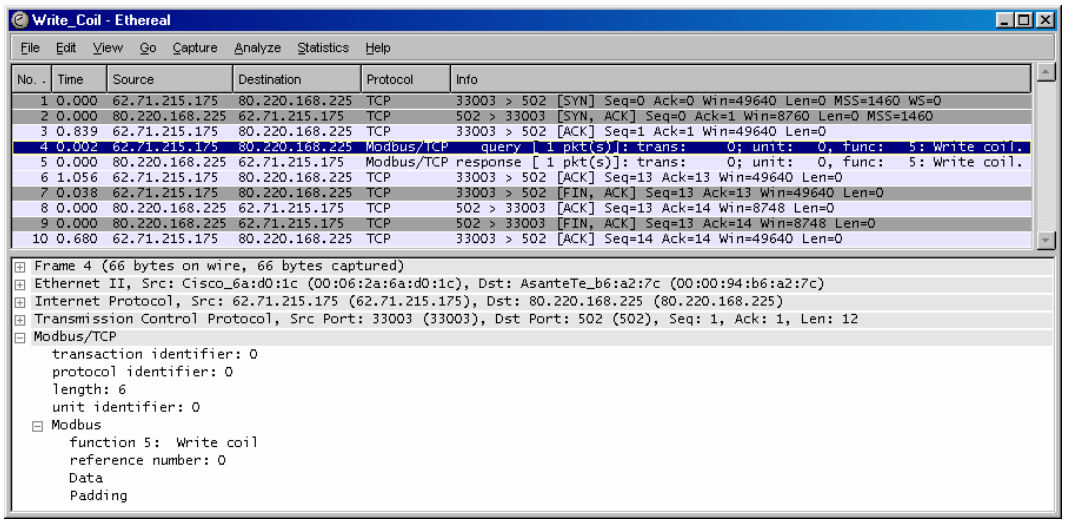
No. Time Source Destination Protocol Info
7 0.002 62.71.215.175 80.220.168.225 TCP 33009 > 502 [FIN, ACK] Seq=13 Ack=11 Win=49640 Len=0
Frame 7 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33009 (33009), Dst Port: 502 (502), Seq: 13, Ack: 11, Len: 0

No. Time Source Destination Protocol Info
8 0.000 80.220.168.225 62.71.215.175 TCP 502 > 33009 [ACK] Seq=11 Ack=14 Win=8748 Len=0
Frame 8 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c), Dst: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c)
Internet Protocol, Src: 80.220.168.225 (80.220.168.225), Dst: 62.71.215.175 (62.71.215.175)
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 33009 (33009), Seq: 11, Ack: 14, Len: 0

No. Time Source Destination Protocol Info
9 0.000 80.220.168.225 62.71.215.175 TCP 502 > 33009 [FIN, ACK] Seq=11 Ack=14 Win=8748 Len=0
Frame 9 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c), Dst: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c)
Internet Protocol, Src: 80.220.168.225 (80.220.168.225), Dst: 62.71.215.175 (62.71.215.175)
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 33009 (33009), Seq: 11, Ack: 14, Len: 0

No. Time Source Destination Protocol Info
10 0.736 62.71.215.175 80.220.168.225 TCP 33009 > 502 [ACK] Seq=14 Ack=12 Win=49640 Len=0
Frame 10 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33009 (33009), Dst Port: 502 (502), Seq: 14, Ack: 12, Len: 0

Silmukan tilatiedon kirjoittaminen (Funktiokoodi 0x05: Write Single Coil)



No.	Time	Source	Destination	Protocol	Info
1	0.000	62.71.215.175	80.220.168.225	TCP	33003 > 502 [SYN] Seq=0 Ack=0 Win=49640 Len=0 MSS=1460 WS=0

Frame 1 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33003 (33003), Dst Port: 502 (502), Seq: 0, Ack: 0, Len: 0

No.	Time	Source	Destination	Protocol	Info
2	0.000	80.220.168.225	62.71.215.175	TCP	502 > 33003 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1460

Frame 2 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c), Dst: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c)
Internet Protocol, Src: 80.220.168.225 (80.220.168.225), Dst: 62.71.215.175 (62.71.215.175)
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 33003 (33003), Seq: 0, Ack: 1, Len: 0

No.	Time	Source	Destination	Protocol	Info
3	0.839	62.71.215.175	80.220.168.225	TCP	33003 > 502 [ACK] Seq=1 Ack=1 Win=49640 Len=0

Frame 3 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33003 (33003), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 0

No.	Time	Source	Destination	Protocol
4	0.002	62.71.215.175	80.220.168.225	Modbus/TCP

Info: query [1 pkt(s)]: trans: 0; unit: 0, func: 5: Write coil.

Frame 4 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33003 (33003), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
Modbus/TCP
transaction identifier: 0
protocol identifier: 0
length: 6
unit identifier: 0
Modbus
function 5: Write coil
reference number: 0
Data
Padding

No.	Time	Source	Destination	Protocol
5	0.000	80.220.168.225	62.71.215.175	Modbus/TCP

Info: response [1 pkt(s)]: trans: 0; unit: 0, func: 5: Write coil.

Frame 5 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c), Dst: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c)
Internet Protocol, Src: 80.220.168.225 (80.220.168.225), Dst: 62.71.215.175 (62.71.215.175)
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 33003 (33003), Seq: 1, Ack: 13, Len: 12
Modbus/TCP
- transaction identifier: 0
- protocol identifier: 0
- length: 6
- unit identifier: 0
- Modbus
  - function 5: Write coil
  - reference number: 0
  - Data
  - Padding

No.	Time	Source	Destination	Protocol	Info
6	1.056	62.71.215.175	80.220.168.225	TCP	33003 > 502 [ACK] Seq=13 Ack=13 Win=49640 Len=0

Frame 6 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33003 (33003), Dst Port: 502 (502), Seq: 13, Ack: 13, Len: 0

No.	Time	Source	Destination	Protocol	Info
7	0.038	62.71.215.175	80.220.168.225	TCP	33003 > 502 [FIN, ACK] Seq=13 Ack=13 Win=49640 Len=0

Frame 7 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33003 (33003), Dst Port: 502 (502), Seq: 13, Ack: 13, Len: 0

No.	Time	Source	Destination	Protocol	Info
8	0.000	80.220.168.225	62.71.215.175	TCP	502 > 33003 [ACK] Seq=13 Ack=14 Win=8748 Len=0

Frame 8 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c), Dst: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c)
Internet Protocol, Src: 80.220.168.225 (80.220.168.225), Dst: 62.71.215.175 (62.71.215.175)
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 33003 (33003), Seq: 13, Ack: 14, Len: 0

No.	Time	Source	Destination	Protocol	Info
9	0.000	80.220.168.225	62.71.215.175	TCP	502 > 33003 [FIN, ACK] Seq=13 Ack=14 Win=8748 Len=0

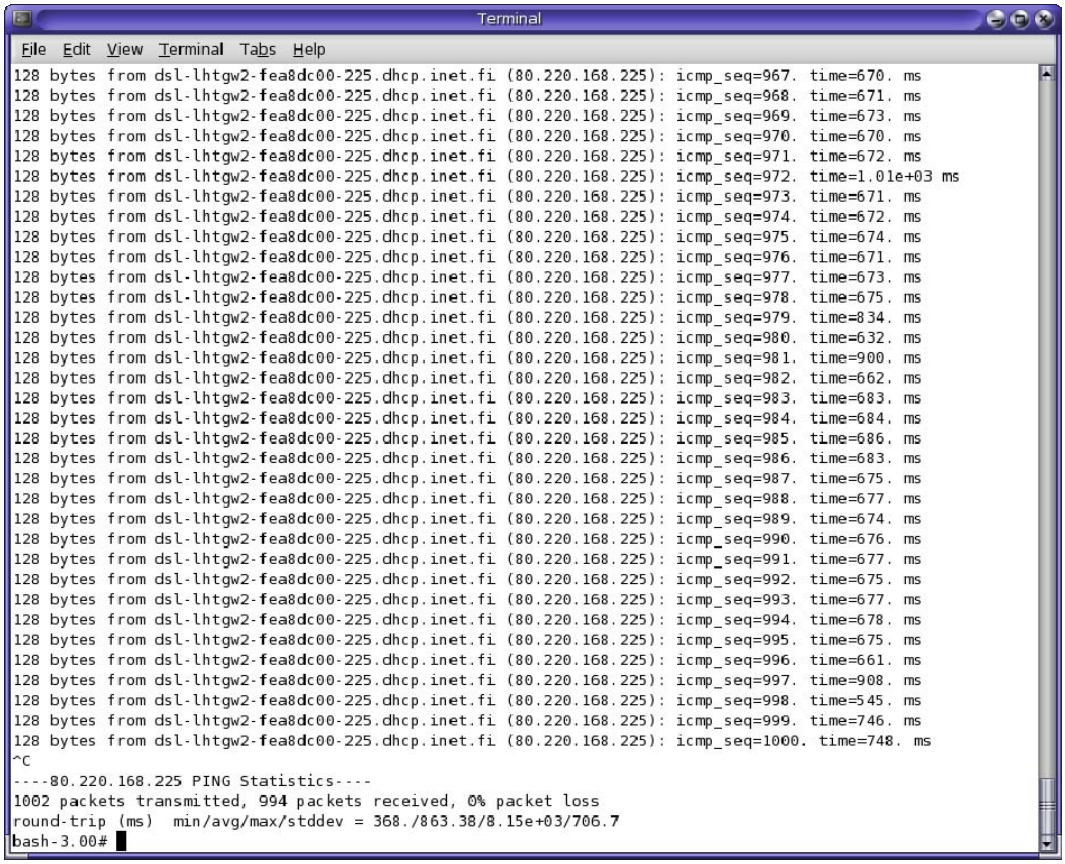
Frame 9 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c), Dst: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c)
Internet Protocol, Src: 80.220.168.225 (80.220.168.225), Dst: 62.71.215.175 (62.71.215.175)
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 33003 (33003), Seq: 13, Ack: 14, Len: 0

No.	Time	Source	Destination	Protocol	Info
10	0.680	62.71.215.175	80.220.168.225	TCP	33003 > 502 [ACK] Seq=14 Ack=14 Win=49640 Len=0

Frame 10 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_6a:d0:1c (00:06:2a:6a:d0:1c), Dst: AsanteTe_b6:a2:7c (00:00:94:b6:a2:7c)
Internet Protocol, Src: 62.71.215.175 (62.71.215.175), Dst: 80.220.168.225 (80.220.168.225)
Transmission Control Protocol, Src Port: 33003 (33003), Dst Port: 502 (502), Seq: 14, Ack: 14, Len: 0

Päästä päähän viiveaika, viiveluokka 4 (best effort)

IP-paketin koko 128 tavua



Lähetetyt paketit: 1002 kpl

Vastaanotetut paketit: 993 kpl

Pakettihäviö: 0,90 %

Päästä päähän viiveaika:

Minimi = 358 ms

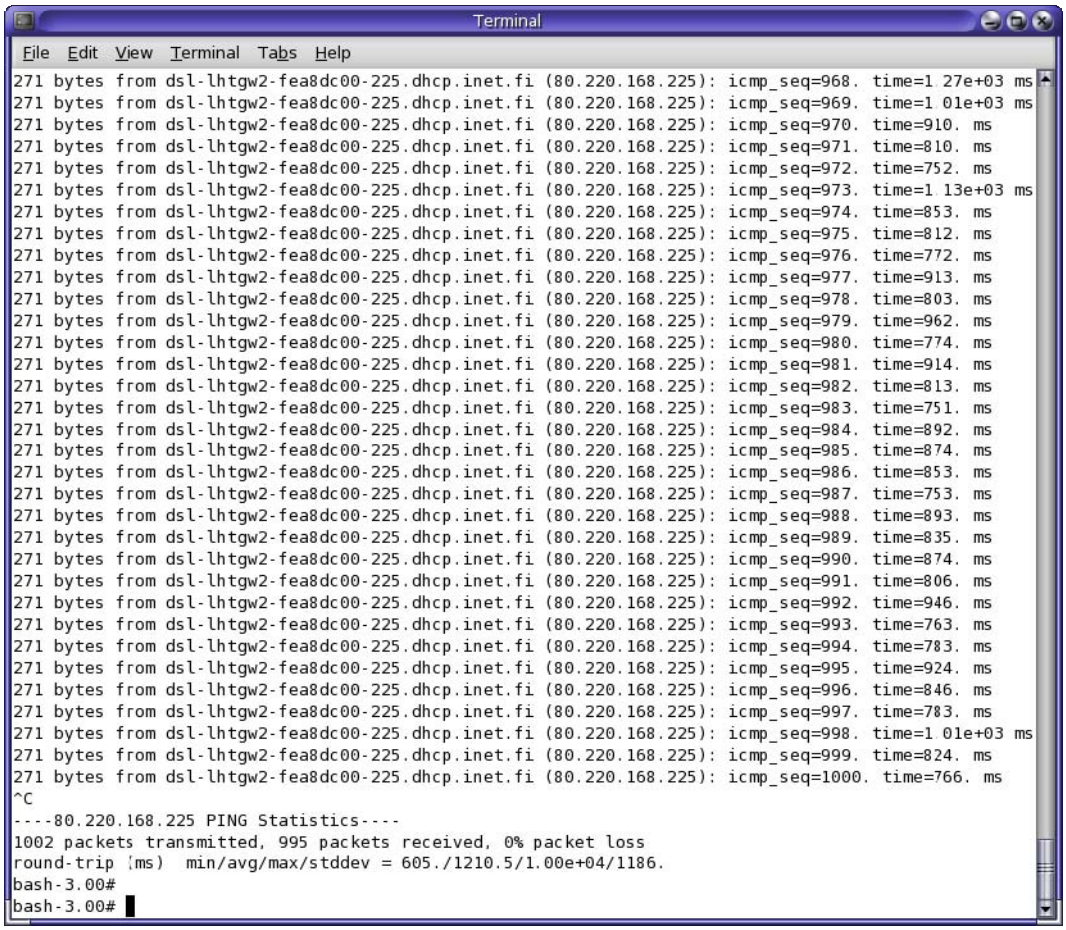
Maksimi = 8150 ms

Keskiarvo = 863 ms

Keskihajonta = 708 ms

Päästä päähän viiveaika, viiveluokka 4 (best effort)

IP-paketin koko 271 tavua, TCP-otsikko + MBAP-otsikko + Modbus PDU (max.)



Lähetetyt paketit: 1002 kpl

Vastaanotetut paketit: 995 kpl

Pakettihäviö: 0,70 %

Päästä päähän viiveaika:

Minimi = 605 ms

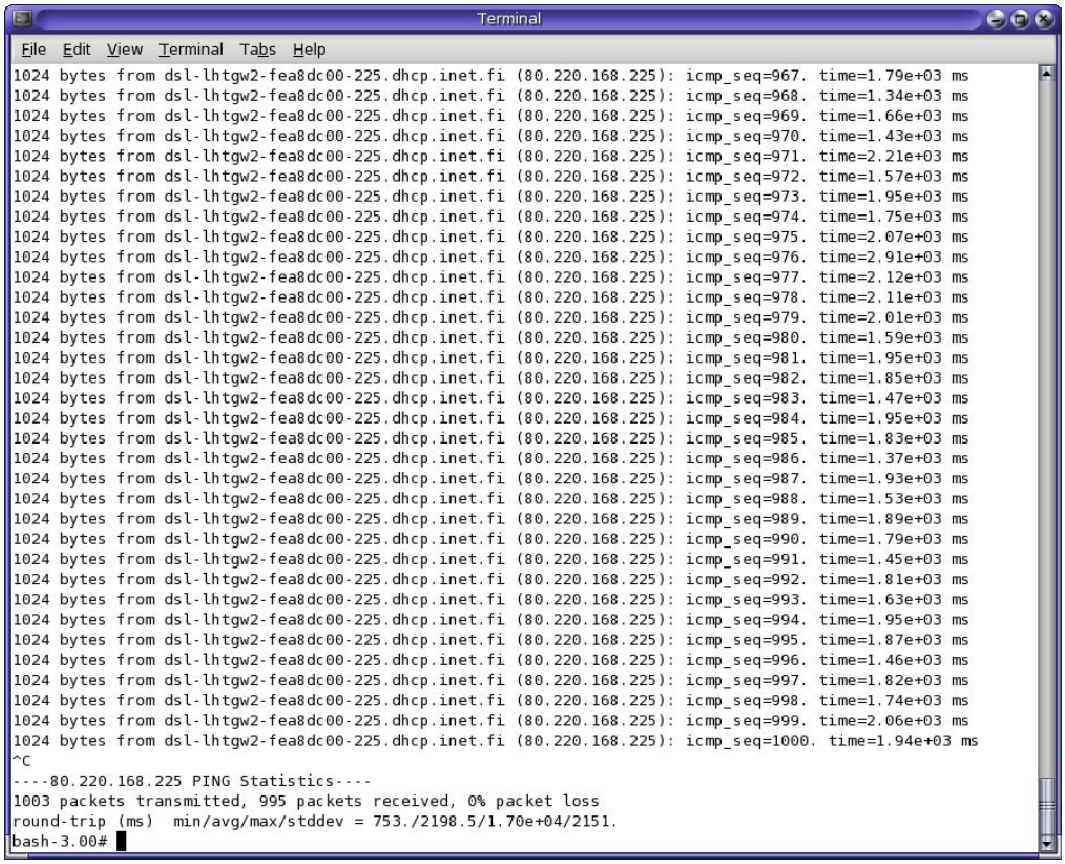
Maksimi = 10000 ms

Keskiarvo = 1211 ms

Keskihajonta = 1186 ms

Päästä päähän viiveaika, viiveluokka 4 (best effort)

IP-paketin koko 1024 tavua



Lähetetyt paketit: 1003 kpl

Vastaanotetut paketit: 995 kpl

Pakettihäviö: 0,80 %

Päästä päähän viiveaika:

Minimi = 753 ms

Maksimi = 17000 ms

Keskiarvo = 2199 ms

Keskihajonta = 2151 ms

GPRS-yhteyden linjavalvonnan tiedonsiirron määrä, ratkaisumalli

	Paketit [kpl]		**Tiedonsiirto [tavua]**		
	Lähetetty	Vastaanotettu	Lähetetty	Vastaanotettu	Yhteensä
1	14	12	595	490	1085
2	15	12	596	488	1084
3	14	12	595	488	1083
4	14	12	603	488	1091
5	15	13	679	576	1255
6	14	12	598	487	1085
7	15	13	681	574	1255
8	14	12	607	498	1105
9	14	12	597	488	1085
10	15	13	678	574	1252
11	14	12	594	490	1084
12	14	12	597	488	1085
13	14	12	593	490	1083
14	14	12	596	489	1085
15	16	13	757	642	1399
16	14	12	593	491	1084
17	14	12	593	490	1083
18	14	12	595	488	1083
19	14	12	593	488	1081
20	14	12	596	490	1086
21	17	15	827	940	1767
22	14	12	594	489	1083
23	14	12	598	493	1091
24	14	12	594	489	1083
25	14	12	594	488	1082
26	17	15	833	944	1777
27	15	13	678	574	1252
28	15	12	678	488	1166
29	14	12	594	489	1083
30	14	12	593	489	1082
31	14	12	601	489	1090
32	17	15	828	944	1772
33	14	12	598	487	1085
34	14	12	591	489	1080
35	14	12	593	492	1085
36	14	12	594	494	1088
37	14	12	592	491	1083
38	14	12	591	492	1083
39	14	12	597	493	1090
40	15	13	683	578	1261
41	14	12	598	493	1091
42	17	15	836	940	1776
43	14	12	595	494	1089
44	14	12	597	489	1086
45	15	12	677	488	1165
46	14	12	600	489	1089
47	15	13	685	575	1260
48	14	12	594	489	1083
49	14	12	595	493	1088
50	14	12	595	493	1088
Minimi	14	12	591	487	1080
Maksimi	17	15	836	944	1777
Keskiarvo	14	12	631	539	1171
Keski-hajonta	0,89	0,85	70	125	192

GPRS-yhteyden linjavalvonnan tiedonsiirron määrä, ICMP-kysely

	Paketit [kpl]		**Tiedonsiirto [tavua]**		
	Lähetetty	Vastaanotettu	Lähetetty	Vastaanotettu	Yhteensä
1	9	9	319	313	632
2	11	10	485	468	953
3	12	12	558	765	1323
4	9	9	322	313	635
5	9	9	322	311	633
6	9	9	322	311	633
7	9	9	319	312	631
8	9	9	323	313	636
9	9	9	322	314	636
10	9	9	320	312	632
11	9	9	320	310	630
12	12	12	559	764	1323
13	9	9	321	314	635
14	9	9	320	313	633
15	9	9	323	312	635
16	9	9	319	311	630
17	10	9	404	312	716
18	12	11	556	615	1171
19	9	9	320	314	634
20	9	9	323	314	637
21	9	9	322	314	636
22	10	10	405	399	804
23	9	9	320	311	631
24	9	9	323	312	635
25	10	9	405	310	715
26	9	9	319	313	632
27	9	9	320	313	633
28	9	9	324	315	639
29	9	9	321	311	632
30	9	9	323	312	635
31	9	9	322	311	633
32	9	9	319	311	630
33	10	9	406	313	719
34	9	9	320	310	630
35	9	9	319	313	632
36	9	9	323	311	634
37	9	9	322	311	633
38	9	9	318	310	628
39	9	9	321	311	632
40	12	11	567	552	1119
41	9	9	325	311	636
42	9	9	318	311	629
43	11	11	495	952	1447
44	9	9	321	312	633
45	9	9	321	310	631
46	9	9	321	311	632
47	9	9	322	311	633
48	9	9	322	313	635
49	10	10	404	396	800
50	9	9	320	315	635
Minimi	9	9	318	310	628
Maksimi	12	12	567	952	1447
Keskiarvo	9	9	355	360	716
Keski-hajonta	0,91	0,76	73	135	201

Modbus TCP/IP -pyyntösanoman lähetysvälin vaikutus tiedonsiirron määrään

Lähetysväli [s]	Keskimääräinen tiedonsiirto				
	tavua/min	tavua/h	tavua/d	tavua/kk (30 d)	tavua/a (365 d)
10	7026	421560	10117440	303523200	3692865600
15	4684	281040	6744960	202348800	2461910400
20	3513	210780	5058720	151761600	1846432800
25	2810	168624	4046976	121409280	1477146240
30	2342	140520	3372480	101174400	1230955200
35	2007	120446	2890697	86720914	1055104457
40	1757	105390	2529360	75880800	923216400
45	1561	93680	2248320	67449600	820636800
50	1405	84312	2023488	60704640	738573120
55	1277	76647	1839535	55186036	671430109
60	1171	70260	1686240	50587200	615477600
65	1081	64855	1556529	46695877	568133169
70	1004	60223	1445349	43360457	527552229
75	937	56208	1348992	40469760	492382080
80	878	52695	1264680	37940400	461608200
85	827	49595	1190287	35708612	434454776
90	781	46840	1124160	33724800	410318400
95	740	44375	1064994	31949811	388722695
100	703	42156	1011744	30352320	369286560

ICMP-kyselyn lähetysvälin vaikutus tiedonsiirron määrään

Lähetysväli [s]	Keskimääräinen tiedonsiirto				
	tavua/min	tavua/h	tavua/d	tavua/kk (30 d)	tavua/a (365 d)
10	4296	257760	6186240	185587200	2257977600
15	2864	171840	4124160	123724800	1505318400
20	2148	128880	3093120	92793600	1128988800
25	1718	103104	2474496	74234880	903191040
30	1432	85920	2062080	61862400	752659200
35	1227	73646	1767497	53024914	645136457
40	1074	64440	1546560	46396800	564494400
45	955	57280	1374720	41241600	501772800
50	859	51552	1237248	37117440	451595520
55	781	46865	1124771	33743127	410541382
60	716	42960	1031040	30931200	376329600
65	661	39655	951729	28551877	347381169
70	614	36823	883749	26512457	322568229
75	573	34368	824832	24744960	301063680
80	537	32220	773280	23198400	282247200
85	505	30325	727793	21833788	265644424
90	477	28640	687360	20620800	250886400
95	452	27133	651183	19535495	237681853
100	430	25776	618624	18558720	225797760