Satakunnan ammattikorkeakoulu

Jarkko Rahkola

GPRS-YHDYSLIIKENNE

Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

2007

TIIVISTELMÄ

GPRS-YHDYSLIIKENNE
Jarkko Rahkola

SATAKUNNAN AMMATTIKORKEAKOULU
Tekniikan Porin Yksikkö
Tekniikantie 2
28600 Pori

Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
Työn tilaaja: Satakunnan ammattikorkeakoulu
Työn valvoja: Juha Aromaa, DI
Päättötyö: 46 sivua, 2 liitettä
Kesäkuu 2007
UDK: 004.738, 621.395

Asiasanat: GPRS, Virtual Private Network, pakettikytkentä, tietoturva

Tässä opinnäytetyössä otettiin käyttöön IP – tunneli Satakunnan ammattikorkeakoulun GPRS – verkosta oululaiseen Octopus – verkkoon. Tavoitteena oli selvittää erilaiset mahdollisuudet VPN – yhteyden toteuttamiseksi ja saada yhteys toimintakuntoon aikataulussa. Tietolähteenä käytettiin Internet – julkaisuja, kirjallisuutta ja Nokian GGSN:n mukana toimitettuja materiaaleja.

Työssä perehdyttiin ensisijaisesti VPN:n (Virtual Private Network) eri toteutus vaihtoehtoihin. Tämän lisäksi teoriaosuudessa tutustuttiin GPRS – verkon elementteihin ja toimintaan.

ABSTRACT

GPRS INTERCONNECTION
Jarkko Rahkola

SATAKUNTA UNIVERSITY OF APPLIED SCIENCES
Unit of Technology in Pori
Tekniikantie 2
28600 Pori

Degree Program of Information Technology
Telecommunication Technology
Commissioned by: Satakunta University of Applied Sciences
Supervisor: Juha Aromaa, M.Sc
Bachelor's Thesis: 46 pages, 2 annexes
June 2007
UDC: 004.738, 621.395

Keywords: GPRS, Virtual Private Network, packet network, data security

IP –tunnel was taken into service from GPRS network of Satakunta University of Applied Sciences to Octopus network in Oulu. The goal was to figure out different possibilities to carry out VPN connection and to get the connection working as was planned. Sources of information were Internet releases, literature and the material delivered with Nokia GGSN.

The primary target in this thesis was to find out the different kinds of solutions to accomplish Virtual Private Network. Besides this the theory of the network elements and the GPRS network operation was introduced.

SISÄLLYS

LYHENTEET

AH	Authentication Header
AP	Access Point
APN	Access Point Name, GPRS – yhteysosoite
ATM	Asynchronous Transfer Mode, Asynkroninen tiedonsiirtotapa
BSC	Base Station Controller, Tukiasemaohjain
BSS	Base Station Subsystem, Tukiasema – alijärjestelmä
BTS	Base Transceiver Station, Tukiasema
CA	Certification Authority
CHAP	Challenge – Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server, Nimipalvelin
ESP	Encapsulating Security Payload
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service, GSM – pakettidatapalvelu
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol, GPRS – tunnelointiprotokolla
HLR	Home Location Register, Kotirekisteri
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMSI	International Mobile Subscriper Identity, Kansainvälinen matkaviestin tilaajan tunnus
IP	Internet Protocol
IPSec	IP Security Architecture
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
ISP	Internet Service Provider, Internet – palveluntarjoaja
L2TP	Layer 2 Tunneling Protocol

MAC	Message Authentication Code
MAP	Mobile Application Part
MD5	Message – Digest algorithm 5
MM	Mobile Management
MPLS	MultiProtocol Label Switching
MS	Mobile Station, Liikkuva päätelaite
MSC	Mobile Switching Centre, Matkapuhelinkeskus
MVPN	Mobile Virtual Private Network
NAS	Network Access Server
NAT	Network Address Translation, Verkko – osoitemuunnos
NSAPI	Network Service Access Point Identifier
PAP	Password Authentication Protocol
PCU	Packet Control Unit, Paketinohjausyksikkö
PDN	Packet Data Network
PKI	Public Key Infrastructure
PPP	Point – to – Point Protocol
QOS	Quality Of Service, Palvelunlaatu
RADIUS	Remote Authentication Dial – In User Service, Autentikointipalvelu
RAS	Remote Access Server
SA	Security Association
SAD	Security Association Database
SGSN	Serving GPRS Support Node
SPI	Security Parameter Index
SSL	Secure Sockets Layer
TID	GPRS Tunnel ID
TLS	Transport Layer Security
TLLI	Temporary Logical Link Identifier
TCP	Transmission Control Protocol
TRX	Transceiver, Lähetinvastaanotin
UDP	Universal Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless Local Area Network
VLR	Visitor Location Register, Vierailijarekisteri
VPN	Virtual Private Network

1 JOHDANTO

Nykyajan työympäristössä on tärkeätä, että yrityksen työntekijät pääsevät hyödyntämään parhaalla mahdollisella tavalla yrityksen verkossa olevia resursseja oli aika tai paikka mikä tahansa. Yksi mahdollisuus, mikä aina on saatavilla, on matkapuhelin ja sen kautta muodostettu turvallinen VPN – yhteys yrityksen sisäverkon palveluihin. Etätyön tekemisen suosiota on kasvattanut GPRS ja vieläkin enemmän sen suosiota tulee kasvattamaan nykyinen 3G – verkko ja sen tuoma parannus tiedonsiirtonopeuksissa.

Tämä opinnäytetyö on tehty Satakunnan ammattikorkeakoulun älyverkkolaboratoriolle. Opinnäytetyön tavoitteena on selvittää mitä eroa on eri VPN - tunnelointiprotokollien välillä ja valita niistä sopivin toteuttamaan yhteys SAMK:n GPRS – verkon ja oululaisen Octopus – verkon välille.

Työn alussa kappaleessa 2 esitellään GPRS – verkon eri elementit ja käydään läpi GPRS – yhteyden toiminta aina verkkoon ilmoittautumisesta yhteyden sulkemiseen asti.

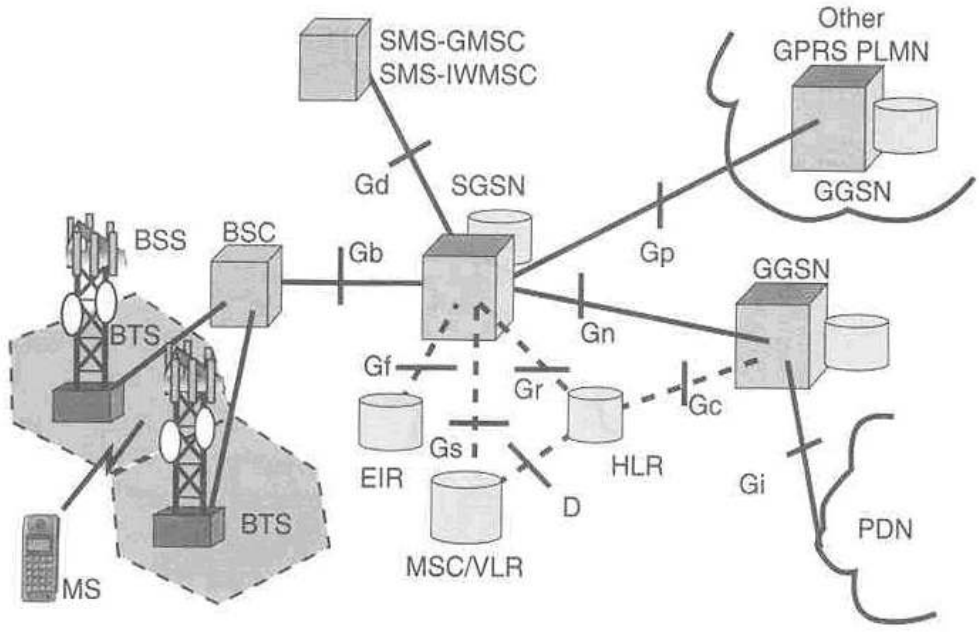
Kappaleissa 3 ja 4 käydään läpi yleistä VPN:stä, eri yhteysmuodoista ja – tyypeistä. Yhtenä tärkeänä asiana käydään läpi VPN:n tunnelointiprotokollat ja niiden hyvät ja huonot puolet.

Viimeiset kappaleet käsittelevät SAMK:a ja Octopusia yleisesti ja niiden välisen yhteyden suunnittelua protokollan valinnasta aina itse IP – tunnelin toteutukseen ja testaamiseen asti.

2 GPRS

2.1 Yleistä

GPRS (General Packet Radio Service) on European Telecommunications Standards Institute (ETSI) määrittelemä GSM – verkon laajennus, jonka mahdollistamana käyttäjä saa muodostettua pakettivälitteisen yhteyden verkkoon. Pakettivälitteinen yhteys tehdään päätelaitteen ja verkossa olevan AP (Access Point) välille. Pakettivälitteisyys tarkoittaa, että GPRS:n radioresursseja käytetään vain kun dataa ollaan siirtämässä tai vastaanottamassa. GPRS tuo mukanaan monikertaisen datansiirtonopeuden verrattuna GSM:n piirikytkentäisillä tekniikoilla saavuttamiin datansiirtonopeuksiin. Muita parannuksia on laskutus joka tapahtuu ainoastaan siirretyn datan mukaan, eikä kuten GSM – verkossa käytetyn ajan mukaan. GPRS:tä puhuttaessa moni on ottanut käyttöönsä termin 2.5G, mikä kuvaa hyvin sitä että käytössä oleva tekniikka on jo hyvin lähellä 3G – verkoissa käytettävää tekniikkaa. Jo nyt GPRS:n avulla käyttäjät voivat saada samoja palveluja kuin 3G – verkossa, kuten esim. lukea sähköpostin, ladata videoita ja saada pääsyn oman työpaikan intranettiin VPN:n avulla. [1] [2] [4]



Kuva 1 GPRS – verkon laitteet ja niiden väliset rajapinnat [1]

2.2 GPRS:n verkkoelementit

GPRS – verkko pohjautuu suurelta osin GSM – verkkoon. Tärkeimpinä uusina elementteinä GPRS tuo verkkoon SGSN (Serving GPRS Support Node) ja GGSN (Gateway GPRS Support Node). Muilta osin GPRS – verkon arkkitehtuuri on sama kuin GSM – verkossakin. Uusien verkkoelementtien johdosta käyttöön tulee myös muutama uusi rajapinta, joita ovat Gb, Gn, Gi, Gr, Gs, Gd ja Gc. [6]

SGSN huolehtii GPRS:n liikkuvuuden hallinnasta, toteuttaa autentikointi proseduurin, datan pakkauksen, salauksen ja reitittää päätelaitteelle menevän ja tulevan liikenteen. SGSN toimii solmuna mihin päätelaitteet tekevät GPRS – liittymisen (attach) tukiaseman kautta. [3]

GGSN on yhdyskäytävänä GPRS – verkon ja ulkoisen pakettiverkon (PDN) välille. Muina ominaisuuksina GGSN tarjoaa, reitityksen, osoitteiden hallinnan, laskutustietojen keräämisen ja palomuurina toimimisen. [3]

BSS koostuu tukiasemista BTS (base transceiver station) ja niitä hallitsevista tukiasemaohjaimista BSC (base station controller). Tukiasema koostuu TRX – elementeistä. TRX:n peittoaluetta kutsutaan soluksi. TRX välittää liikennettä yhdellä taajuudella, joka on jaettu kahdeksaan aikaväliin joita pitkin puhelut ja GPRS yhteydet liikkuvat. Osa aikaväleistä on voitu varata puheluiden käyttöön ja osa kanavista on varattu GPRS – liikenteen käyttöön. Koska puhelu – ja dataliikenne käyttävät samoja kanavia on GSM – puheluille annettu korkeampi prioriteetti ja jäljelle jääneet kanavat palvelevat GPRS – käyttäjiä. Tukiasemaohjaimen BSC tärkein tehtävä on huolehtia oman alueensa radioresurssien hallinnasta. Tukiasemaohjaimen alueella on tyypillisesti useita tukiasemia, joita ryhmittelemällä muodostetaan sijaintialueita. Tukiasemaohjaimeen kuuluu myös lisäelementti paketinohjausyksikkö PCU, joka ohjaa GPRS – yhteydet erilliseen GPRS – runkoverkkoon.[3, 4]

Kotirekisteriin (HLR) on tallennettu tilaaja – ja laskutustiedot ja muuttuvana tietona tilaajan sijaintitiedot.[3, 4]

DNS (Domain Name System) on nimipalvelu, jonka tehtävä on vastata SGSN:n pyytämiin kyselyihin. Eräs tärkeä tapaus on kun SGSN kysyy toisen SGSN IP – osoitetta, johon DNS löytää vastaavuuden ja palauttaa tiedon takaisin. Toinen vaihtoehto on kun GPRS – yhteyttä ollaan aloittamassa ja MS pyytää APN – nimen avulla haluttua kohdeverkkoa. SGSN ei tiedä pelkän APN – nimen perusteellla mitä GGSN:ää tulisi käyttää, ja tämän takia se tekee kyselyn DNS:ltä mitä kyseinen APN – nimi edustaa. DNS vastaa SGSN:lle mitä IP – osoitetta kyseinen APN – nimi edustaa. [5]

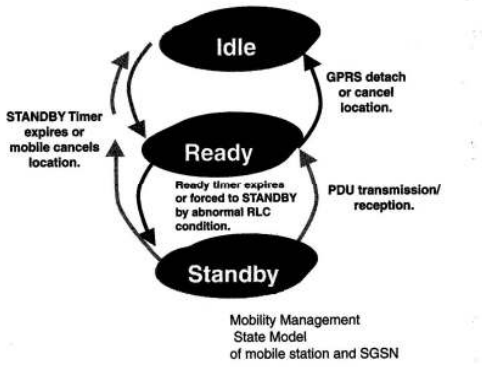
2.3 Elementtien väliset rajapinnat

- Gb, BSC:ssä olevan PCU:n ja SGSN:n välillä, käyttää Frame Relay:tä, nykyisin myös IP:tä
- Gr, SGSN:n ja HLR:n välillä, jonka kautta SGSN noutaa liittymää koskevia tietoja. Tämän rajapinnan kautta kulkevat sanomat käyttävät MAP3 – protokollaa
- Gn, SGSN:n ja GGSN:n välillä, GPRS – runkoverkko jossa käytetään GTP protokollaa
- Gi, GGSN:n ja PDN:n välinen rajapinta
- Gs, SGSN:n ja MSC/VLR:n välinen rajapinta
- Gd, käytetään SMS – viestien kuljettamiseen GPRS:n avulla
- Gc, GGSN:n ja HLR:n välinen rajapinta, jonka kautta GGSN saa liikkuvan aseman sijaintiedot HLR:stä [1, 2, 6]

2.4 GPRS – yhteyden muodostus

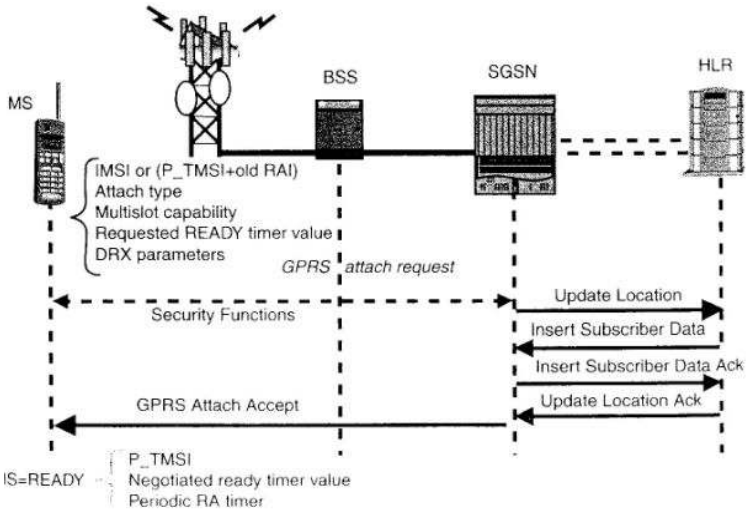
MS ei ole yhteydessä GPRS – verkkoon ennen kuin se on ilmoittautunut sinne, eli tehnyt GPRS – attach:n ja vaihtanut tilakseen ready. Muita mahdollisia tiloja ovat idle ja standby. Idle tilassa MS ei ole tavoitettavissa ja sen sijainti on verkolle tuntematon. Ready tilassa MS on tehnyt GPRS – attach:n ja sen sijainti tiedetään solun tarkkuudella. Datan lähettäminen on mahdollista ready tilassa. Standby tilassa

MS on GPRS – verkossa ja sen sijainti tiedetään reititysalueen tarkkuudella. PDP – kontekstin voi aktivoida tai purkaa standby tilassa. [1, 2]



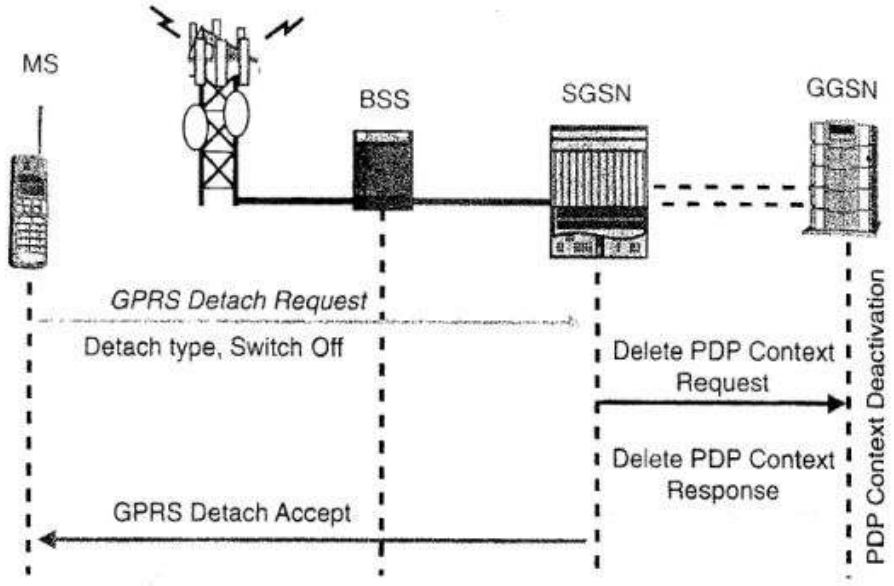
Kuva 2, MM:n tilat.[1]

Verkkoon/SGSN:ään ilmoittauduttaessa MS tarjoaa omat tietonsa ja indikoi minkä tyyppinen ilmoittautumisproseduuri tulee tehdä. Mahdollisuuksia attach:n tekoon ovat GPRS – attach ilman GSM – verkkoon kytkeytymistä, GPRS – attach kun GSM – verkkoon on jo kytkeydytty ja yhdistetty IMSI/GPRS – attach. Attach proseduuri alkaa kun MS haluaa aloittaa pakettivälitteisen yhteyden verkkoon. Ensimmäiseksi MS lähettää Attach request sanoman tilastaan SGSN:lle. Tämän jälkeen MS vahvistetaan, autentikoidaan ja tehdään sijainnipäivitys. Seuraavaksi SGSN lähettää attach accept sanoman jonka MS kuittaa sanomalla attach complete. Nyt on luotuna liikkuvuuden hallintatila eli verkko tietää reititysalueiden tarkkuudella laitteiden sijainnin. Seuraavaksi voidaan aloittaa loogisen yhteyden luonti päätelaitteen ja verkon välille. [1, 2]



Kuva 3, GPRS – attach proceduuri. [1]

Kun halutaan siirtyä ready tilasta idle tilaan, niin täytyy aloittaa GPRS – detach proseduuri. Proseduurin voi aloittaa niin MS kuin verkkokin. MS aloittaa proseduurin lähettämällä SGSN:lle GPRS – detach Request:n. Detach:n tyyppiin voi sisältyä GPRS – detach, IMSI – detach tai molemmat. Tämän jälkeen SGSN lähettää GGSN:lle Delete PDP Context Request:n johon GGSN vastaa Responsella. Seuraavaksi SGSN lähettää GPRS Detach Accept viestin MS:lle, jonka jälkeen MS siirtyy idle tilaan. [1, 2, 6]



Kuva 4, MS:n aloittama GPRS – detach. [1]

Kun verkon on ”irroitettava” MS, SGSN informoi MS:ä että se on ”irroitettu” lähettämällä MS:lle Detach Request:n. Seuraavaksi SGSN lähettää GGSN:lle Delete PDP Context Request:n johon GGSN vastaa Responsella. Lopuksi MS lähettää GPRS Detach Accept viestin SGSN:lle jolla se hyväksyy Detach:n. Mikäli detach:n tyyppiin sisältyy IMSI attach, niin SGSN informoi VLR:ää, joka hoitaa päätelaitteen päivityksen ilman SGSN:ää.[1, 2, 6]

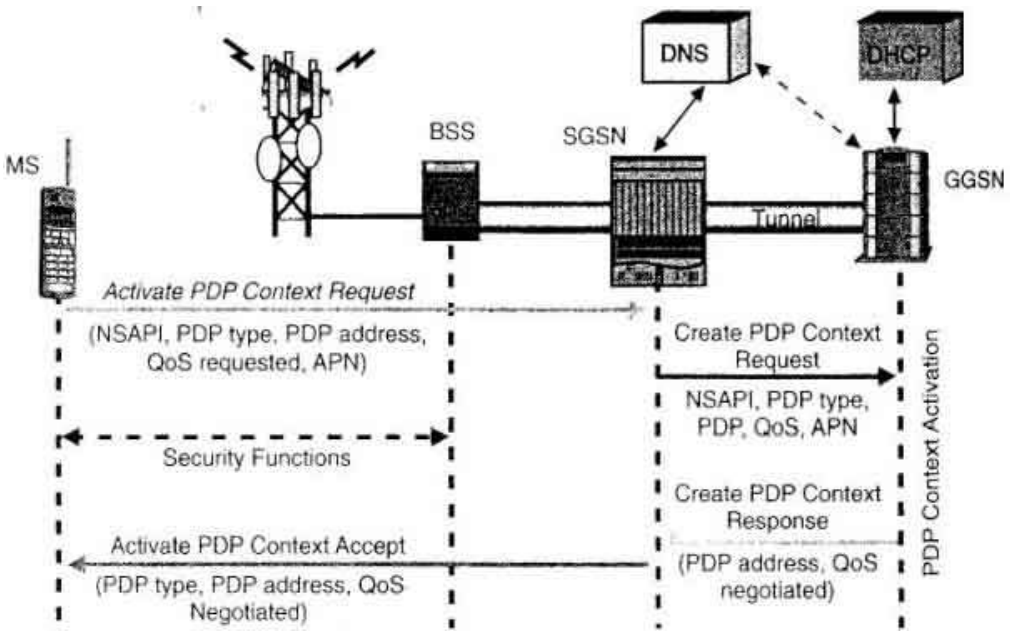
2.5 PDP – kontekstin aktivointi

Ennen kuin dataa voidaan lähettää tai vastaanottaa on aktivoitava PDP – konteksti. PDP – kontekstia käytetään reititystarkoituksiin GPRS – verkon sisällä. GPRS – liittymä sisältää kuvauksen yhdestä tai useammasta PDP – osoitteesta. Jokainen PDP – osoite on kuvattu omalla PDP – kontekstilla MS:ssa, SGSN:ssa ja GGSN:ssa. PDP – konteksti määrittää IP – tunnelin MS:n ja GGSN:n välille. GGSN:n liitäntä ”internetiin” on APN (Access Point Name). PDP – kontekstia luotaessa voidaan määritellä seuraavanlaisia parametreja: NSAPI/TLLI (The Network layer Service Access Point Identifier/Temporary Logical Link Identity), PDP – tyyppi, PDP – osoite, QoS (Quality of Service), TID ja APN. [1, 6]

- **NSAPI/TLLI,** SGSN:n ja MS:n välinen PDP – konteksti on osoitettu TLLI ja NSAPI tunnisteparin avulla.
- **PDP – tyyppi,** ilmaisee PDP – kontekstia luodessa, että minkä tyyppistä protokollaa matkapuhelimen tulee käyttää vaadittavaan palveluun
- **PDP – osoite,** eli verkkokerroksen osoite on GPRS – tilaajan käytössä PDP – kontekstin aktivoinnin jälkeen
- **QoS,** tarkoitetaan palvelunlaatua eli miten tietoliikennettä voidaan luokitella ja projisoida
- **TID,** on käytössä GPRS:n tunnelointiprotokollan apuna GSN:en välissä yksilöimään PDP – konteksti. TID sisältää IMSI:n ja NSAPI:n
- **APN,** on GPRS runkoverkossa viittauksena käytetystä GGSN:stä. APN sisältää kaksi osaa: operaattoritunnuksen ja verkkotunnuksen [6]

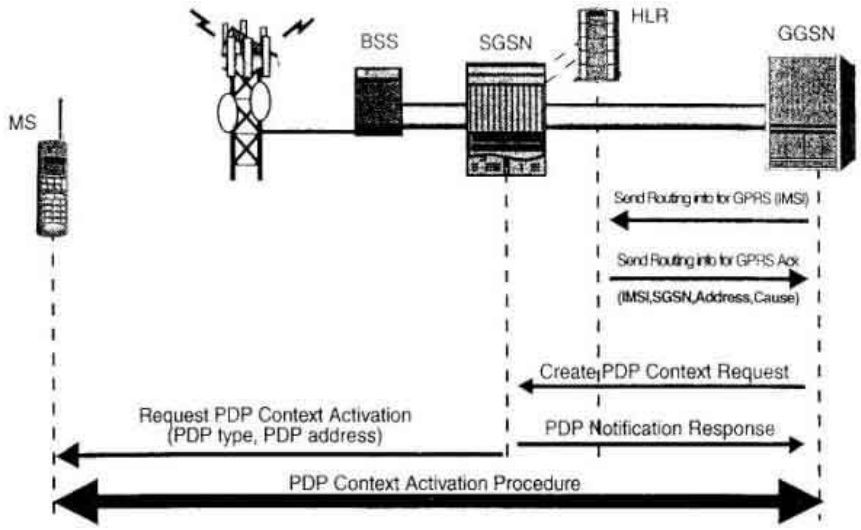
Jokainen PDP – konteksti voi olla joko Active tai Inactive. Inactive tila tarkoittaa, että data palvelu tilaajan PDP – osoitteelle ei ole aktiivinen. Konteksti ei sisällä reititys tietoja, eikä sijainnin vaihto aiheuta päivityksiä PDP – kontekstiin, vaikka tilaaja olisi ilmoittautunut GPRS MM:n. Siirtyminen Inactive tilasta Active tilaan vaatii PDP – kontext:n aktivointiproseduurin aloittamista. Active tilassa PDP – kontext:n käytössä olevalle PDP – osoitteelle on aktivoitu MS:ssa, SGSN:ssa ja GGSN:ssa. Nyt PDP – konteksti sisältää sijainti – ja reititystietoja pakettien lähettämiseen MS:n ja GGSN:n välillä. Active tila on sallittu ainoastaan, kun tilaajan

MM:n tila on standby tai idle. Inactive tilaan siirrytään takaisin kun PDP – konteksti deaktivoidaan. Ennen PDP – kontekstin aloittamista MS on ”ilmoittanut” itsensä SGSN:ään eli tehnyt GPRS – attach:n. Koska GGSN ei vielä tiedä MS:n olemassaolosta on aloitettava PDP – kontekstin aktivointi. PDP – kontekstin aktivoinnin voi aloittaa joko MS tai verkko (GGSN). MS:n aloittaessa aktivointi proseduurin se lähettää Activate PDP Context Request sanoman SGSN:lle. Sanoma sisältää NSAPin, PDP – tyypin, PDP – osoitteen QoS:n ja APN:n. Seuraavaksi SGSN valitsee GGSN:n MS:n lähettämän informaation (APN) avulla. SGSN tekee DNS – kyselyn löytääkseen APN:a vastaavaa GGSN:n. DNS palauttaa GGSN:n IP – osoitteen. Tämän jälkeen SGSN reitittää PDP Context Activation Request:n GGSN:lle joka vastaa APN:ää. Tunneli SGSN:n ja GGSN:n välille on identifioitu käyttämällä TID:tä (Tunnel Identifier). GGSN:n päivitettyä PDP – konteksti taulukkonsa, se lähettää Create PDP Context Response sanoman SGSN:lle, joka sisältää TID – informaation ja MS:n käyttämän IP – osoitteen. SGSN lähettää MS:lle sanoman Activate PDP Context Accept ja päivittää omat taulukkonsa TID:llä ja GGSN:n IP – osoitteella mihin GTP – tunneli on muodostettu. [1, 6]



Kuva 5, MS:n aloittama PDP – kontekstin aktivointi. [1]

PDP – kontekstin aktivointi proseduuriin voi aloittaa spesifikaatioiden mukaan myös verkko, tarkemmin GGSN joka aloittaa aktivoinnin, mikäli MS ei ole vielä sitä vaadittavalle osoitteelle tehnyt. Ennen aktivoinnin aloittamista GGSN vastaanottaa PDP PDU:n (Protocol Description Unit) ja tarkistaa onko PDP – konteksti jo luotuna vaaditulle osoitteelle. Aktivointi alkaa kun GGSN lähettää HLR:lle Send Routing Information sanoman. HLR tarkistaa voidaanko pyyntöä palvella ja jos voidaan niin HLR vastaa Ack:lla joka sisältää SGSN:n osoitteen, mikäli ei voida palvella vastaus sisältää syyn virheeseen. Seuraavaksi GGSN lähettää PDU Notification Request sanoman SGSN:lle joka vastaa GGSN:lle Response:lla, joka sisältää tiedon, että SGSN informoi MS:ää aloittamaan PDP – kontekstin aktivoinnin. MS:n saatua pyynnön se voi aloittaa edellä esitellyn MS:n aloittaman PDP – kontekstin aktivointi proseduurin. [1, 6]

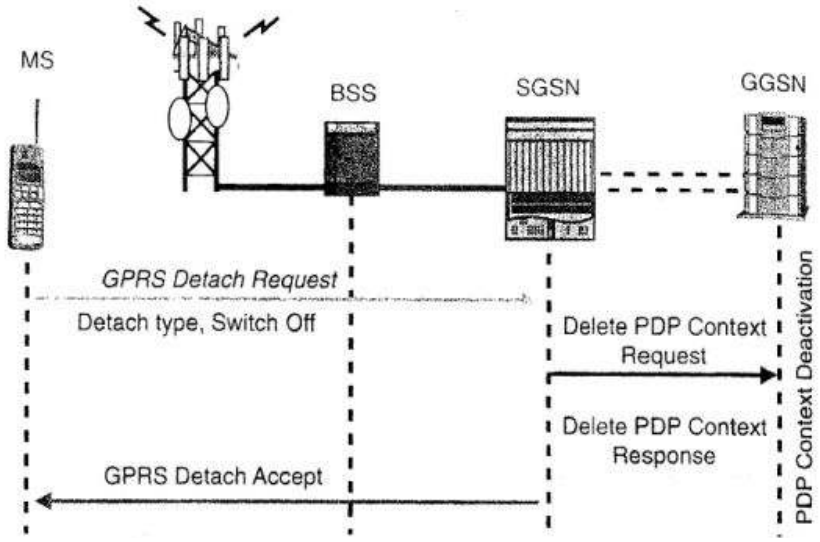


Kuva 6, Verkon aloittama PDP – kontekstin luonti. [1]

2.6 PDP – kontekstin deaktivointi

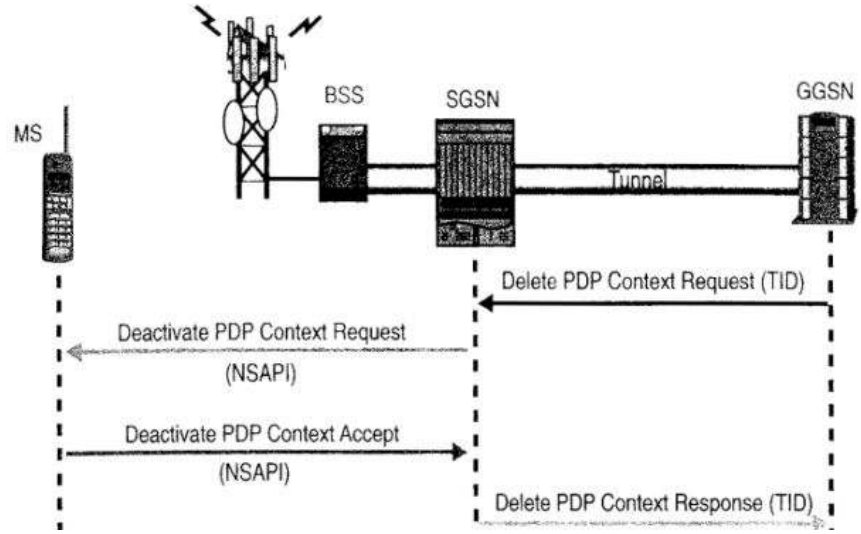
PDP – kontekstin deaktivointi tulee ajankohtaiseksi, kun yhteys halutaan lopettaa. Deaktivointi proseduurin voi aloittaa MS tai verkko. MS:n aloittama deaktivointi alkaa, kun MS lähettää Deactive PDP Context Request sanoman SGSN:lle. SGSN lähettää Delete PDP Context Request sanoman GGSN:lle, joka sanoman saatuaan poistaa PDP – kontekstin ja lähettää Delete PDP Context Response sanoman ta-

kaisin SGSN:lle. Jos MS käytti dynaamista PDP – osoitetta GGSN vapauttaa sen seuraavan MS:n käyttöön. Lopuksi SGSN lähettää accept sanoman MS:lle. GPRS detach:llä kaikki MS:n PDP – kontekstit deaktivoituvat. [1, 6]



Kuva 7, MS:n aloittama PDP – kontekstin deaktivointi. [1]

Verkon aloittama deaktivointi proseduuri alkaa, kun GGSN pyytää SGSN:ltä PDP – kontekstin tuhoamista Delete PDP Context Request sanomalla. SGSN pyytää MS:n deaktivoimaan PDP – kontekstin Deactive PDP Context Request sanomalla. PDP – kontekstin deaktivoituaan MS lähettää Accept:n SGSN:lle, joka vastaa GGSN:lle Delete PDP Context Response sanomalla. Näin konteksti on tuhottu ja GGSN voi vapauttaa PDP – osoitteen muiden käyttöön. [1, 6]



Kuva 8, Verkon aloittama PDP – kontekstin deaktivointi. [1]

3 VPN

3.1 Yleistä

VPN (Virtual private network) on tekniikka, jolla organisaation yksityinen sisäverkko voidaan ulottaa yli julkisen verkon (Internet), tekemällä turvallinen/salattu yhteys tunnelin läpi. Tekniikkaa hyödynnetään esim. liittämällä yrityksen kaukana toisistaan olevien toimipaikkojen sisäverkkoja toisiinsa, tai mahdollistamalla etätyöntekijän pääsy yrityksen sisäverkkoon riippumatta siitä missä verkossa etätyöntekijä kulloinkin on. [1, 3]

VPN – tekniikkaa käytettiin alun perin hyödyntämällä Frame Relay – ja ATM – verkkojen tekniikoita. VPN – yhteydet toteutettiin vuokraamalla yksityinen siirtojohto puhelinyhtiöltä yrityksen käyttöön, joka oli kallista toteuttaa ja näin ollen esti VPN – tekniikan nopean leviämisen käyttäjien keskuudessa. Nykyään VPN – palvelut pohjautuvat IP:aan ja internetin käyttö on tehnyt VPN:stä kiinnostavan palvelun niin yrityksille kuin yksityisillekin. VPN:n yleistymisen myötä on markkinoille tullut paljon uusia laite – ja ohjelmistovalmistajia, jotka ovat omalta osaltaan helpottaneet VPN:n käyttöönottoa. VPN – palvelut ovat siirtymässä langallisista verkoista langattomiin verkkoihin. Langattomissa verkoissa käytössä olevasta tunnelointi VPN – palveluista puhutaan usein nimellä MVPN (Mobile Virtual Private Network). MVPN tuo VPN – palvelun työntekijöille, jotka nykyään kannettavien tietokoneiden sijaan kantavat mukanaan taskukokoisia laitteita. Laitteet voivat olla matkapuhelimia tai PDA – laitteita, joiden avulla työntekijä voi käyttää toimisto – ohjelmia, ottaa yhteyden sähköpostipalvelimeen tai työpaikan sisäverkkoon. Yhteys muodostetaan avaamalla salattu tunneli GPRS – tai WLAN – verkon kautta työpaikalle. VPN – palvelun hyödyntäminen on muodostunut erittäin suosituksi juuri paljon etätyötä tekevien työntekijöiden parissa. [1, 3]

3.2 VPN yli GPRS:n

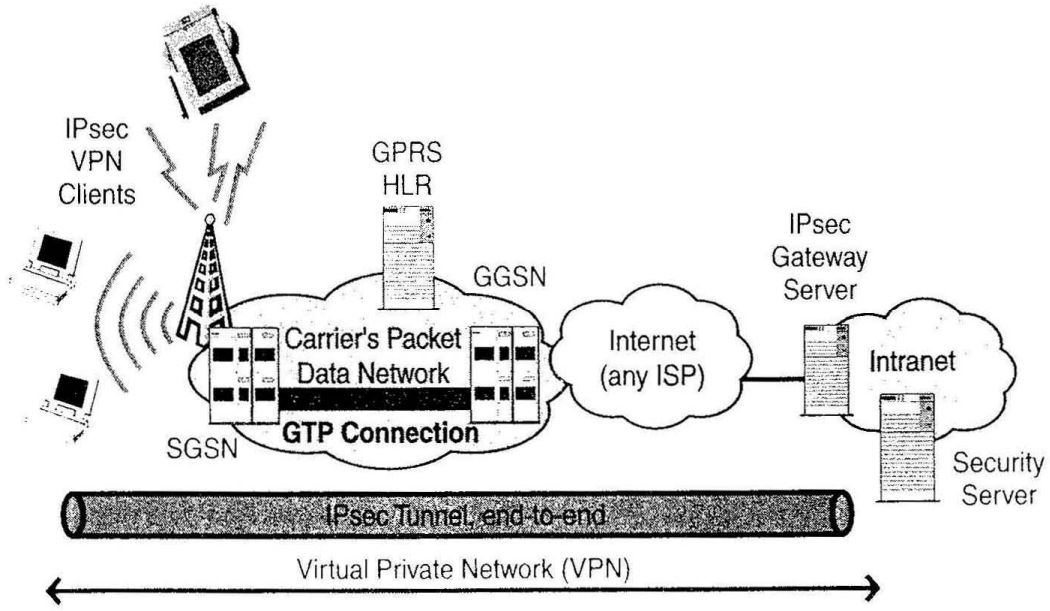
GPRS VPN jakaa suurimman osan vaatimuksista, mitä VPN:lle yleisesti on määritelty. Tärkeimpiä vaatimuksia ovat autentikointi, tiedon eheys, päästä – päähän turvallisuus, ja luottamuksellisuus. MVPN:n käyttäjän autentikointi langattomiin verkkoihin hoidetaan jo liityttäessä GSM – verkkoon (HLR), kun taas otetaan GPRS – yhteys IP – verkkoon autentikointi voidaan suorittaa RADIUS – protokollaa (Remote Authentication Dial In User Service) käyttämällä. Liikenteen suojaus on GSM – verkossa hoidettu ilmatien salauksella ja yleisen IP – verkon puolella liikenne voidaan salata käyttämällä esim. IPSec – protokollaa. GPRS – pohjaiset VPN:t ovat kombinaatioita GPRS:n tunnelointiprotokollasta (GTP) mobiiliverkon puolelta ja IETF:n määrittelemistä tunnelointiprotokollista ulkoisen verkon puolelta. [3, 7]

Puhuttaessa VPN:stä voidaan puhua myös IP – tunneloinnista. IP – tunnelit ovat polkuja, joissa IP liikenne kapseloidaan IP – paketin sisään. Kapseloidut paketit lähetetään lähettäjän alkupisteestä kohteen loppupisteeseen käyttämällä yleisiä (suojaamattomia) kanavia. Tunnelit voivat sijaita myös siirtoyhteyskerroksella, tarjoten kapseloinnin käyttämällä ei reititettäviä protokollia kuten L2TP (Layer 2 Tunneling Protocol) ja PPP (Point – to – Point Protocol). IP VPN:n tekemiseen käytetään kahta perus tunnelointimetodia: päästä – päähän ”vapaaehtoinen” ja verkkopohjainen ”pakollinen”. [3, 7]

3.3 Päästä – päähän VPN

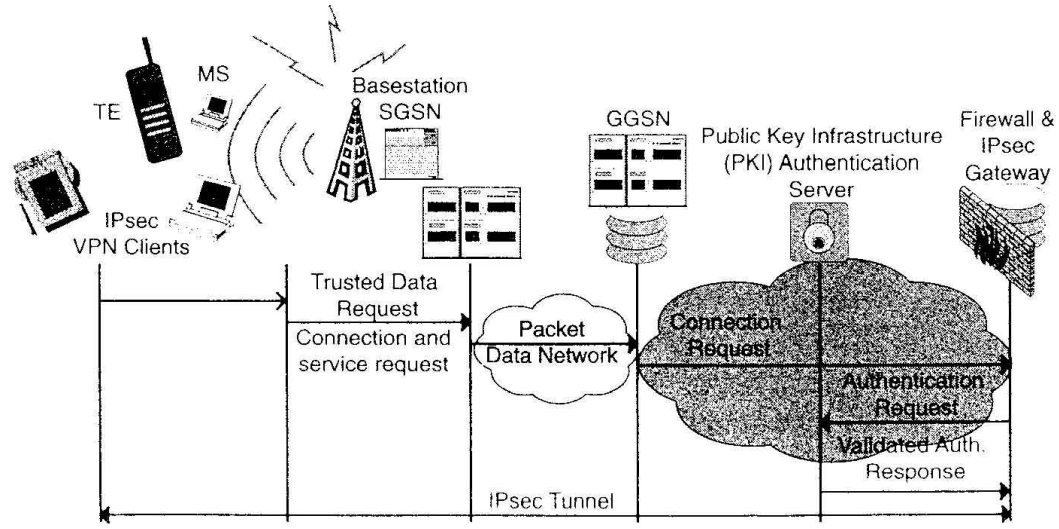
Päästä – päähän tunneli tarjoaa yksinkertaisen ja turvallisen ratkaisun yhteyden ottamiseen yksityisiin verkkoihin. Varsinkin tilaajan näkökulmasta päästä – päähän VPN – yhteys tarjoaa parhaan turvallisuuden. Liikenne salataan lähetettäessä VPN client – ohjelmalla, joka on tilaajan päätelaitteessa. Salatun liikenteen saavuttaessa yrityksen VPN – serverin pakettien salaus puretaan. Näin ollen liikenne meni salattuna koko VPN – yhteyden yli. Päästä – päähän mallissa autentikointi on käyttäjästä ja yrityksestä kiinni, eikä palveluntarjoajasta kuten ”pakollinen” mallissa. Hyvänä esimerkkinä päästä – päähän VPN – tekniikoista on IPSec,

IETF:n standardi. IPSec teknologia tarjoaa salatun tunnelin tilaajilta käyttäen GPRS ”backbonea”, yli internetin, kohti yrityksen yhdyskäytävää käyttäen TCP/IP protokollaa. [1, 9]



Kuva 9, Päästä – päähän VPN - yhteys. [1]

Päästä – päähän VPN – yhteys voidaan toteuttaa myös käyttämällä kolmannen osapuolen PKI – järjestelmää (Public Key Infrastructure). Julkisen avaimen järjestelmän avulla voidaan tehdä, ylläpitää ja käyttää varmenteita. MVPN:ssä PKI:tä käytettään autentikointiin. PKI:n tapauksessa käyttäjälle annetaan yleinen/yksityinen avainpari joita käyttämällä autentikointi tapahtuu. Yksityinen avain on vain omistajan hallussa ja julkinen avain voidaan jakaa kaikille osapuolille. Yksityisen avaimen pitäminen salaisena on parasta tehdä avainpari mobiili laiteelle itselleen ja antaa CA:n (Certification Authorities) sertifioida yleinen avain. Tällä tavoin yksityinen avain pysyy aina samalla laitteella, mikä parantaa turvallisuutta. Avainpari on matemaattisesti luotu, joten jos salataan käyttäen yksityistä avainta niin siihen kuuluva julkinen avain purkaa salauksen ja päinvastoin. PKI:tä käytetään sen jälkeen varmistamaan osapuolten identiteetti ja luomaan salaus avaimet jokaiseen istuntoon. PKI:tä hallinnoi palveluntarjoaja/operaattori joka toimii varmentaja mihin kumpikin VPN – yhteyden osapuolista luottavat. [1, 9]



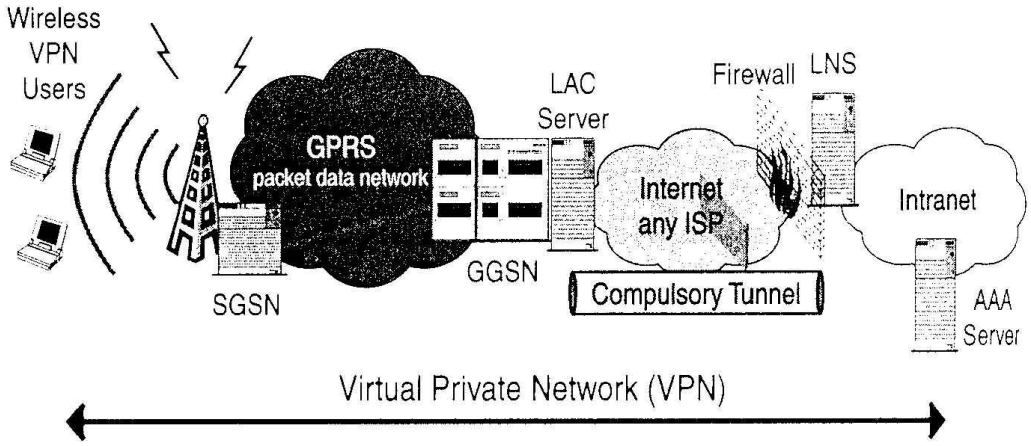
Kuva 10, Päästä – päähän VPN - yhteys, PKI käytössä [1]

Yksi suurimmista päästä – päähän yhteyden ongelmista tulee kun käytössä on NAT (Network Address Translation) eli dynaaminen osoitteiden hallinta. NAT:a käytetään yleisesti GGSN:ssä ja mahdollisesti vielä toisen kerran yhteyden muodostamisen aikana, kun siirrytään julkisen verkon puolelle. Salauksen aikana IP-Sec luo paketille uudet osoitekentät jotka GGSN:n NAT muuttaa. Tästä seuraa, että eheys tarkistus ei onnistu ja paketti pudotetaan pois liikenteestä. Vastaavasti paketin osoitteen muuttuminen voi johtaa IP tarkistussumman menemiseen väärin jolloin paketti hylätään korruptoituneena. Yhtenä ratkaisuna ongelmaan on kapseloida IPSec paketit UDP:n (User Datagram Protocol) sisään ennen lähettämistä. UDP:tä voidaan käyttää ilman, että pakettien eheyttä tarkistetaan vastaanottajan toimesta käyttäen tarkistussummia. UDP kapselointi hidastaa yhteyttä johtuen kapselointi prosessista. Jopa salausprosessi voi hidastua, mikäli käytetään MS:ä. Kannettavan tietokoneen kanssa ongelma ei ole niin suuri johtuen sen paremmasta laskentatehosta. Tekniikoita joilla NAT – ongelma voidaan ratkaista ovat NAT – Traversal tai Ciscon yhteydessä IPSec NAT – Transparency. Yhtenä ratkaisuna NAT – ongelmaan on IPv6:n käyttöönotto, joka mahdollistaa staattisten IP – osoitteiden käytön päätelaitteilla. Näin ollen NAT:n käyttö ja siitä johtuvat ongelmat vähenevät. [3, 7, 8,10]

3.4 Network level VPN

Toinen käytettävissä oleva tapa rakentaa VPN on aloittaa tunneli GGSN:ltä kohti intranettiä. Liikenne salataan VPN – serverillä tai reitittimellä, jotka ovat kytketty AP:n (AP:n on määritelty toisen pään VPN – serverin IP – osoite) ja palveluntarjoajan runkoverkon väliin. Salattu liikenne kulkee nyt yli julkisen verkon kohti intranettiä, jossa VPN – server purkaa salauksen. Käyttäjä on autentikoitu siinä vaiheessa kun lupa pääsystä AP:lle on tullut, mikä on erikseen määritelty HLR:ssä. Kaikki muu liikenne mikä ei ole menossa intranettiin lähetään AP:n läpi salaamattomana. Erillistä VPN – serveriä tai reititintä ei operaattorin päässä tarvita, mikäli GGSN on varustettu tarvittavilla ominaisuuksilla liikenteen salaamisen ja VPN – tunnelin avaamiseen. Yleisimpiä tunnelin toteuttamiseen käytetyistä protokollista ovat GRE, L2TP, MPLS ja eniten käytettynä IPSec, joka myös ainoana tarjoaa kunnollisen salauksen. Yleisesti on käytetty GRE – IPSec yhdistelmää joka tarjoaa hyvin toimivan salauksen ja tunnelointiprotokollan. Käyttämällä GGSN:ltä lähtevää VPN – tunnelia voidaan välttää mahdollinen NAT – ongelma mikä oli päästä – päähän yhteyden kanssa. Tosin kummassakin päässä tunnelia vaatimuksena on VPN – serverin sijoittaminen NAT:n ulkopuolella. [3, 7, 8]

”Pakollinen” ratkaisu vaatii sen, että tilaaja käyttää siihen varattua AP:a, joka taas tarkoittaa, että tilaajan on käytettävä operaattorin GPRS verkkoa yhteyden luontiin. Operaattorin verkon käyttö taas tuo tilaajalle lisää kustannuksia, jonka varsinkin paljon dataa siirtävä huomaa nopeasti. Onneksi operaattorit ovat huomanneet kysynnän suuren kasvun ja laskeneet hintojaan huomattavasti. Hyvänä asiana GPRS:n käytössä on se että yhteyden käyttö ajasta ei laskuteta vaan ainoastaan siitä minkä verran dataa siirretään. Yhtenä ongelmana on, että tilaajien on luotettava mobiilioperaattoreihin, koska liikenne kulkee salaamattomana GPRS – runkoverkossa ja altistuu siellä hyökkäyksille. Yhtenä vaihtoehtona on salauksen käyttäminen sovellustasolla. [3, 7, 8]



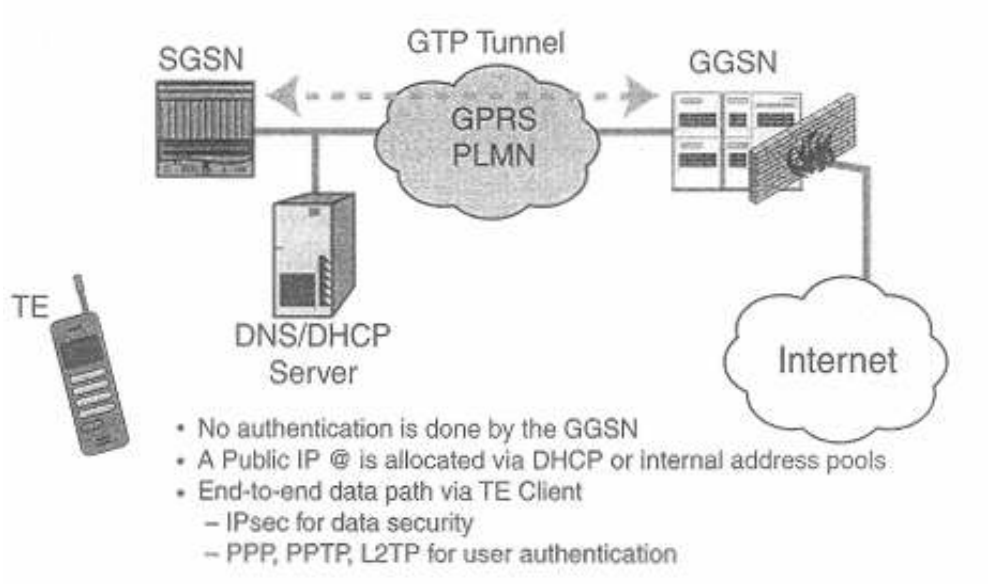
Kuva 11, Network level VPN. [1]

3.5 Transparent vai Non – transparent yhteystyyppi

GPRS:n tekninen spesifikaatio tarjoaa Transparentin ja NON – transparentin yhteysmoodin GPRS – verkon ja ulkoisen IP – verkon yhdistämiselle. Transparent yhteys tukee ainoastaan IP – pohjaista kommunikaatiota ja IP – tyypin PDP – kontekstin luontia GGSN:ään. NON – transparent yhteys tukee niin IP – kuin PPP – moodia operaatioon yhdessä IP – tai PPP – tyypin PDP – kontekstin kanssa joka on luotuna GGSN:ään.

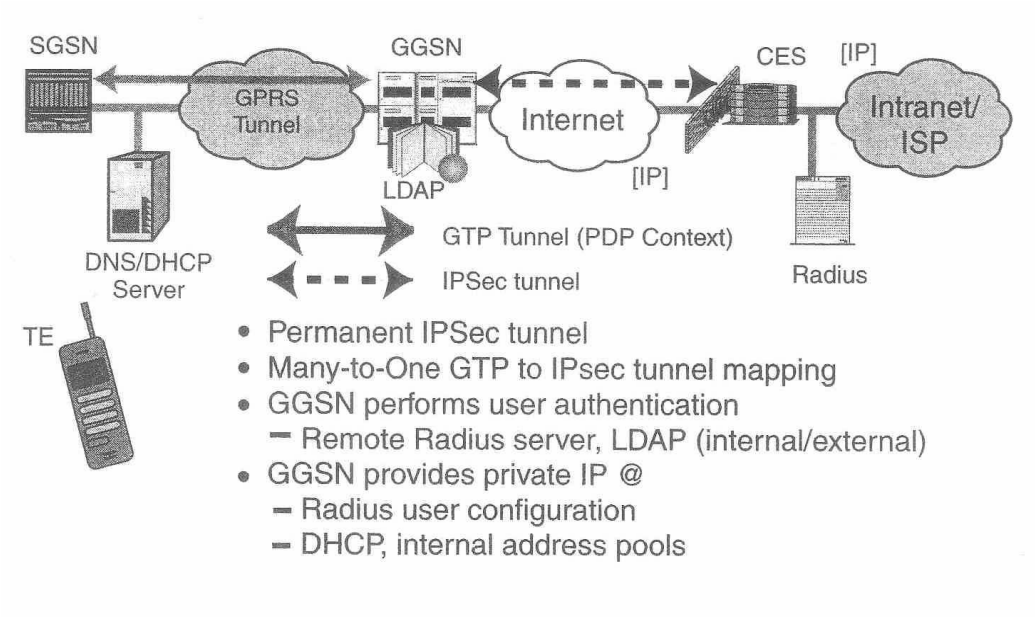
Transparent moodi tarkoittaa, että GGSN ei ota osaa käyttäjän autentikointiin, eli GGSN ei lähetä autentikointi pyyntöä PDP – kontekstin aktivoinnin yhteydessä. Autentikointi on suoritettu MS:n ja SGSN:n välillä käyttäen hyväksi HLR:ää, VLR:ää ja muita fyysisen kerroksen elementtejä. Transparent moodi tarkoittaa yleensä, että operaattori on ISP:na, eli tarjoaa erilaisia palveluja ja yhteyden internetiin suoraan GPRS käyttäjälle. Tästä johtuen MS:lle on annettu IP – osoite operaattorin osoite – avaruudesta, joko staattinen IP – osoite tai PDP – kontekstin luonnin yhteydessä dynaaminen IP osoite käyttämällä paikallista DHCP – serveriä. Transparentin tapauksessa käytetään päästä – päähän tunnelia. Tunneli tehdään MS:stä kohde verkon VPN – serverille. Tunneli salataan käyttämällä IP-Sec:ä, mikäli liikenne menee yli suojaamattoman verkon. Koska päästä – päähän yhteys on salattu MS:n ja kohdeverkon välillä, ei GGSN:n ja kohdeverkon välille

tarvita erillistä salaus protokollaa. Käyttäjän autentikointi voidaan suorittaa joko ISP:llä tai kohdeverkossa käyttämällä RADIUS:sta. [1, 3, 11]



Kuva 12, transparent mode. [1]

Non – transparent:ssa moodissa GPRS – operaattori toimii lähinnä ”bittiputken” luovuttajana, mahdollistaen yhteyden ISP:lle tai intranettiin. MS saa IP – osoitteen joka on ISP:n tai Intranetin osoiteavaruudesta lähettämällä kyselyn RADIUS – palvelimelle tai DHCP – serverille. IP – osoite on joko staattinen tai PDP – kontekstin luonnin yhteydessä dynaaminen. Tunnelointiprotokollina GGSN:n ja ISP:n tai yksityisen verkon välillä voidaan käyttää esim. IPSec:ä, L2TP:tä ja GRE:tä. Kuten protokollista käy ilmi niin VPN – yhteys voi olla myös salaamaton. Valinta protokollasta ja yhteyden salauksesta tehdään molemminpuolisesti lähtö – ja kohdeverkon välillä. VPN – yhteyden avaukseen tarvittavat parametrit GGSN päättelee APN:n perusteella saatuaan SGSN:ltä PDP Context Request – sanoman. Parametreja ovat: osoitteiden jakamiseen ja autentikointiin käytettävä serveri, mitä protokollaa käytetään kyseisen serverin kanssa esim. RADIUS tai DHCP ja kommunikointiin ja turvallisuuteen tarvittavat ominaisuudet jotka tarvitaan keskusteluun serverin kanssa, kuten tunnelin tyyppi tai IPSec SA. GGSN vastaa SGSN:lle Create PDP Context Response sanomalla, jonka jälkeen tunneli kohdeverkkoon on muodostettu. [1, 3, 11]



Kuva 13, Non –transparent access [1]

4 VPN – TUNNELOINTIPROTOKOLLAT

Nykyään on monia eri ratkaisuja kapseloida protokolla toisen protokollan yli. VPN:stä puhuttaessa kapselointiin käytettäviä protokollia/tekniikoita on useita, osa protokollista sisältää turvallisuuteen liittyviä lisäkerroksia protokollan sisäänrakennettuina osatekijöinä ja osa protokollista on keskittynyt kuljettamaan dataa yli toisen verkon. Tunnelointiprotokollista suosituimpia MVPN:n tekemiseen ovat L2TP, GRE, MPLS ja ainoana hyvän turvallisuuden tarjoava ”protokollana” IPSec. Muita käytössä olevia VPN – tekniikoita ovat PPTP ja IP – in – IP. Usein myös yhdistellään kahta eri tekniikkaa esim. GRE – IPSec tai L2TP – IPSec, yhdisteleminen mahdollistaa käyttää hyväksi kummankin protokollan parhaat puolet. Uusi hieman edellisistä poikkeava ratkaisu on SSLVPN, missä tarjotaan pääsy yrityksen tietojärjestelmiin salatun liikenteen kautta, mutta varsinaista pakettiliikennettä ei päästetä yrityksen verkkoihin. [1, 3, 12]

Yleensä tunneli tehdään kapseloimalla alkuperäinen IP – paketti toisen IP – paketin sisälle ja lisäämällä pakettiin kapselointi otsake esim. GRE – otsake. Tunneleita voidaan käyttää myös kapseloimaan ei reititettäviä protokollia, kuten PPP. Kapseloitu paketti lähetetään tunnelin läpi kohdeverkon päätepisteeseen, käyttämällä yleisiä ei turvallisia kanavia. Koska tunneli tehdään usein käyttämällä ei turvallisia kanavia tarvitaan IP – pakettien suojaksi salausta. Ratkaisun tähän turvallisuus ongelmaan tarjoaa IPSec joka lisää paketteihin joko AH – tai ESP – otsakkeen jotka tarjoavat autentikoinnin, salauksen ja tiedon eheyden. Se mitä protokollaa tulisi käyttää VPN:n rakentamiseen yli GPRS:n tai UMTS:n on usein kiinni palveluntarjoajasta, jonka kautta yhteys rakennetaan. MS:ltä lähtevät yhteydet toteutetaan yleensä käyttämällä IPSec:ä, kun taas yritys access yhteydet GGSN:ltä eteenpäin rakennetaan käyttämällä GRE – tai L2TP – protokollaa ilman IPSec:ä tai IPSec:n kanssa datan kuljettamiseen. [1, 3, 12]

Protokollan valintaan vaikuttavat myös verkon eri elementit, onko NAT käytössä, mitä protokollia laitteet tukevat ja protokollissa olevat ominaisuudet. Valittaessa VPN – ratkaisua on hyvä harkita ratkaisua, jossa on sekä datan autentikointi ja

käyttäjän autentikointi mekanismit. Useimmat nykyisistä VPN – ratkaisuista tarjoavat vain toisen autentikointi tavoista. Täydellinen VPN – ratkaisu sisältää kummatkin autentikointi mekanismit ja hyvän datan salauksen. VPN – ratkaisuissa käytetty siirtomuoto määrittää mitkä osat sanomasta on salattu. Jotkin ratkaisut salaavat koko sanoman, IP – otsikon ja datan, kun taas jotkin ratkaistu salaavat ainoastaan datan. Nykyään on käytössä neljä eri siirtomuotoa:

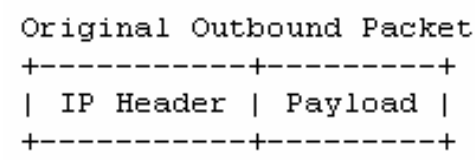
- **”In – place” siirtomuoto,** vain data on salattu ja paketin koko ei ole muuttunut
- **Kuljetusmuoto,** vain data on salattu, ja paketin koko kasvaa
- **Salattu tunnelimuoto,** IP – otsikko ja data on salattu ja uusi IP – osoite on tehty ja reititetty VPN – tunnelin päätepisteeseen
- **Ei salattu tunnelimuoto,** mitään ei ole salattu, eli kaikki kuljetettava data on puhdasta tekstiä [1, 3, 12]

4.1 IPSec

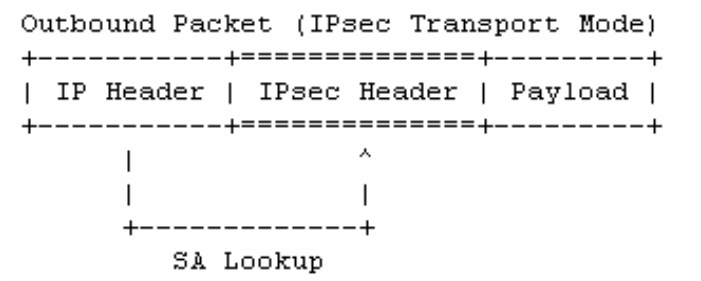
IPSec (IP Security) on IETF:n kehittämä kokoelma protokollia, joiden tarkoituksena on mahdollistaa tietoliikennepakettien turvallinen vaihto verkkokerroksella. Kun IPSec turvaa verkkokerroksen yhteydet, niin IPSec protokollapino takaa niiden sovellusten turvallisuuden jotka käyttävät verkkokerroksen yhteyksiä. IP Security protokollat on suunniteltu toimimaan sekä IPv4:n ja IPv6:n kanssa. Salaus protokollia voidaan käyttää suojaamaan yksi tai useampi ”tunneli” kahden isäntäkoneen (host), kahden turva – gatewayn tai turva – gatewayn ja isäntäkoneen välillä. IPSec:n tarjoamat turvallisuus palvelut mahdollistavat, että järjestelmä pääsee valitsemaan vaadittavat turvallisuus protokollat, määrittämään palveluihin käytetyt alkoritmit ja laittamaan paikoilleen salausavaimet joita tarvitaan mahdollisiin palveluihin. Turvallisuus palveluihin, mitä IPSec tarjoaa, sisältyy pääsynvalvonta, lähettävän pään autentikointi, yhteydetön eheys, tiedon alkuperän todennuksen, suojauksen toistoa vastaan, luottamuksellisuus (salauksen) ja rajoitettu vuon luottamuksellisuus. Kyseisten turvallisuus palveluiden mahdollistamiseen

pakettivirtojen turvaamisessa IPSec käyttää kahta protokollaa: AH (Authentication Header) ja ESP (Encapsulating Security Payload). Kumpikin protokolla tukee kahta eri moodia kuljetus (Transport) ja tunneli (Tunneling). Avaintenvaihtoprotokollana IPSec:n kanssa on suositeltu käytettäväksi IKE:ä (Internet Key Exchange). [3, 13]

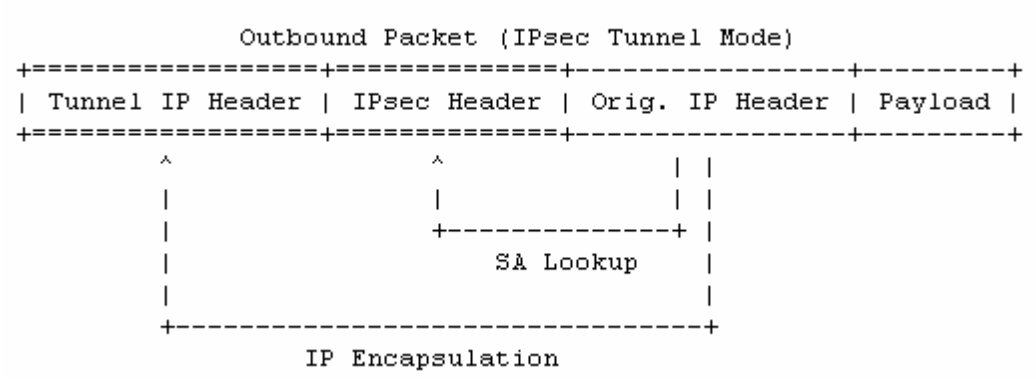
- **Tunnelimoodi** kapseloi ja suojaa koko IP – paketin, mukaan lukien IP – otsakkeen uuden IP – paketin sisään, jotta mikään osa alkuperäisestä IP – paketista ei ole näkyvissä tai muutettavissa, kun paketti ollaan siirtämässä yli verkon.
- **Kuljetusmoodissa** IPSec asettaa turvallisuus protokolla otsakkeen ulosmenevän IP – paketin alkuperäisen IP – otsakkeen ja paketin hyötykuorman (payload) väliin. IPSec otsakkeen sisältö pohjautuu SA:han joka käyttää alkuperäisen IP – otsakkeen sisältöä ja hyötykuormaa paikallistaakseen SA:n SAD:sta eli turvallisuus assosiaation tietokannasta. [13, 14]



Kuva 14, Alkuperäinen lähtevä paketti [15]



Kuva 15, Lähtevän paketin rakenne kuljetusmoodin alla [15]



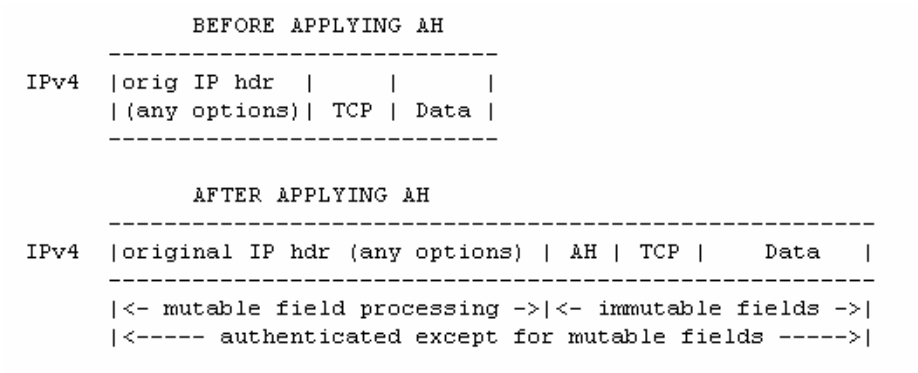
Kuva 16, Lähtevän paketin rakenne tunnelimoodin alla [15]

SA (Security Association) on kahden osapuolen välinen sopimus. SA määrittelee mitä IPSec:n protokollaa käytetään suojaamaan paketit, muunnokset, avaimet ja kuinka kauan määrätyt avaimet ovat voimassa. 32 – bittinen yhteystunnus SPI (Security Parameter Index) on tärkeä elementti SA:lle. Sitä käytetään yksilöllisesti tunnistamaan SA vastaanottopäässä. [23]

AH (Authentication Header) on yksi IPSec:n avainprotokollista, joka tarjoaa yhteydettömän tiedon eheyden todennuksen, tiedon alkuperän tunnistamisen ja tarjoaa suojan paketin uudelleenlähetykseltä. Viimeksi mainittu, valinnainen palvelu, voidaan ottaa käyttöön vastaanottajan toimesta, kun SA (Security Association) on muodostettu. Koska AH ei sisällä tiedon luotettavuuden varmistamista, tätä standardia voidaan käyttää laajalti Internetissä. Tämä on myös suurin syy siihen, että IPSec käyttää kahta eri mekanismia AH ja ESP pakettien salaukseen AH:ssa tiedon eheys ja autentikointi tarjotaan yhdessä, lisäämällä suojattuun viestiin ylimääräinen lohko. Tätä lohkoa kutsutaan nimellä ICV (Integrity Check Value) kehyksen tarkistussumma, yleinen termi jota käytetään kuvaamaan joko MAC:a (Message Authentication Code) tai digitaalista allekirjoitusta. Niiden avulla voidaan varmistaa, että data on pysynyt lähetyksessä muuttumattomana ja että lähettäjä on todella se, joka niin väittää. Salausta (esim. HMAC – MD5) käyttämällä otsikosta saadaan todistuskelpoinen: vaikka datan lähettäjä haluaisi myöhemmin kieltää lähettäneensä jotain tiettyä, lähettäjä voidaan kuitenkin aukottomasti todistaa. Autentikaatiossa käytetty data lasketaan koko IP – datagrammista. [14, 19, 20]

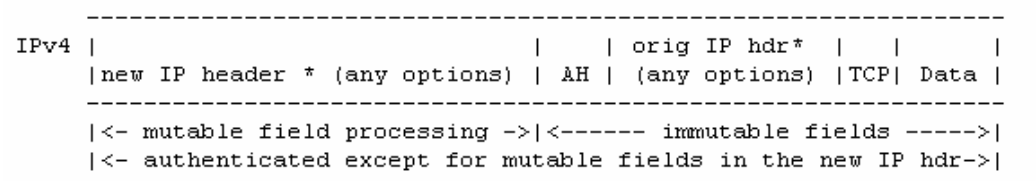
Kuljetusmoodissa datapaketin IP – otsikko on ulommaisin IP – otsikko, jota seuraa AH – otsikko ja sitten datapaketin hyötykuorma. AH autentikoi koko datapa-

ketin, paitsi muuttuvia kenttiä. Kuljetusmoodi vaatii vähemmän prosessointia kuin tunnelimoodi, mutta ei tarjoa niin hyvää turvallisuutta. [19,20]



Kuva 17, datapaketista ennen AH:ta ja kuljetusmoodissa AH:n lisäämisen jälkeen. [19]

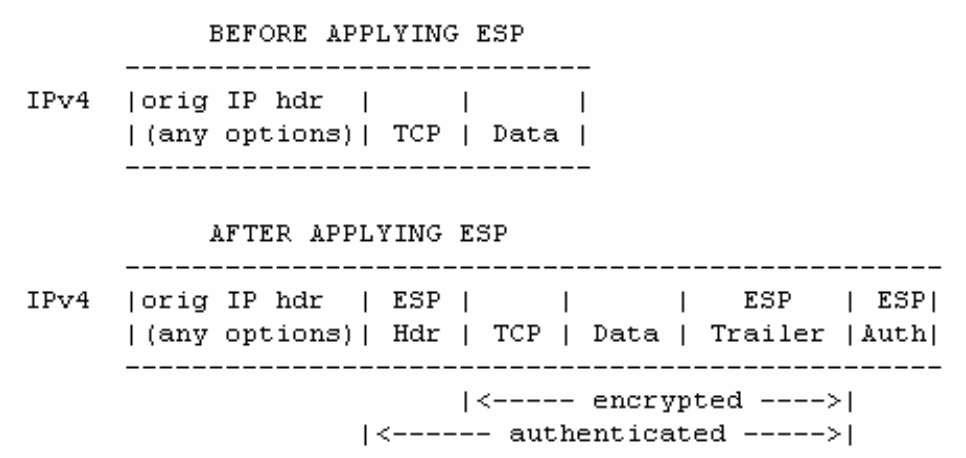
Tunnelimoodi luo uuden IP – otsikon ja käyttää sitä datapaketin ulommaisena IP – otsikkona. AH – otsikko seuraa uutta IP – otsikkoa ja viimeisenä tulee alkuperäinen datapaketti. AH autentikoi koko datapaketin, joka tarkoittaa, että vastaanottaja huomaa jos datapaketti on muuttunut lähetyksen aikana. Tunnelimoodin etu on, että se suojaa koko kapseloidun IP – paketin. [19, 20]



Kuva 18, datapaketista tunnelimoodissa AH:n lisäämisen jälkeen. [19]

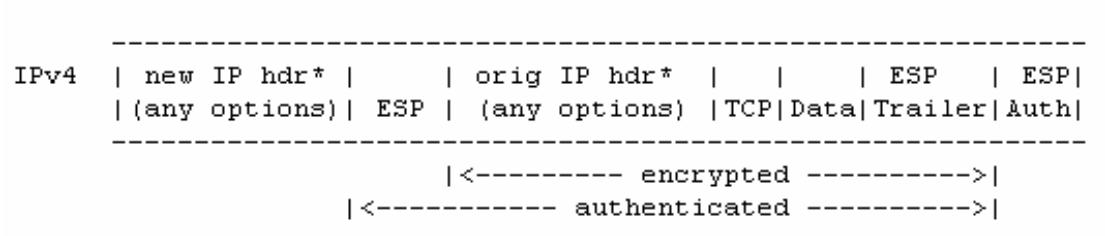
ESP (Encapsulation Security Payload) tarjoaa tiedon luotettavuuden, eheyden ja todennuksen. Lisäksi ESP tarjoaa suojan paketin uudelleenlähetystä vastaan. Jos ESP:tä käytetään todentamaan tiedon eheyttä, se ei käsitä IP – headerin muuttumattomia kenttiä. Kuten AH:ssa autentikointi ja tiedon eheys ovat kaksi palvelua jotka kulkevat käsi kädessä ja on usein koottu yhteen yhden termin ”autentikointi” alle; niiden käyttäminen tapahtuu ICV – lohkon avulla. Suoja paketin uudelleenlähetystä vastaan voidaan valita käyttöön, mikäli autentikointi on myös valittuna. Palvelu tarjotaan käyttämällä erityistä sarjanumeroa, minkä vastaanottaja paketeista tarkistaa. ESP:n yleisimmin käyttämät algoritmit tarjoamaan autentikointi toiminnallisuudet ovat HMAC – MD5 ja HMAC – SHA. [20, 21]

Kuljetusmoodissa ESP – otsikko seuraa alkuperäisen datapaketin IP – otsikkoa, jos datapaketissa on jo valmiiksi IPSec – otsikko niin sitten ESP – otsikko menee ennen sitä. ESP:n traileri – otsake ja valinnainen autentikointi data seuraavat hyötykuormaa. Kuljetusmoodi ei autentikoi tai salaa IP – otsikkoa. Kuljetusmoodi vaatii vähemmän prosessoitavaa ylikuormaa kuin tunnelimoodi, mutta ei tarjoa yhtä paljon turvallisuutta. Useimmissa tapauksissa ”isäntäkoneet” käyttävät ESP:tä kuljetusmoodissa. [20, 21]



Kuva 19, datapaketista ennen ESP:tä ja kuljetusmoodissa ESP:n lisäämisen jälkeen. [21]

Tunnelimoodi luo uuden IP – otsikon ja käyttää sitä datapaketin ulommaisena IP – otsikkona, jota seuraa ESP – otsikko ja alkuperäinen datapaketti. ESP traileri ja valinnainen autentikointi data on lisätty hyötykuormaan. Kun käytetään salausta ja autentikointia, ESP suojaa kokonaan alkuperäisen datapaketin, koska se on nyt uuden ESP – paketin hyötykuorma. ESP ei silti suojaa uutta IP – otsikkoa. Yhdyskäytävien on käytettävä ESP:tä tunnelimoodissa. [20, 21]



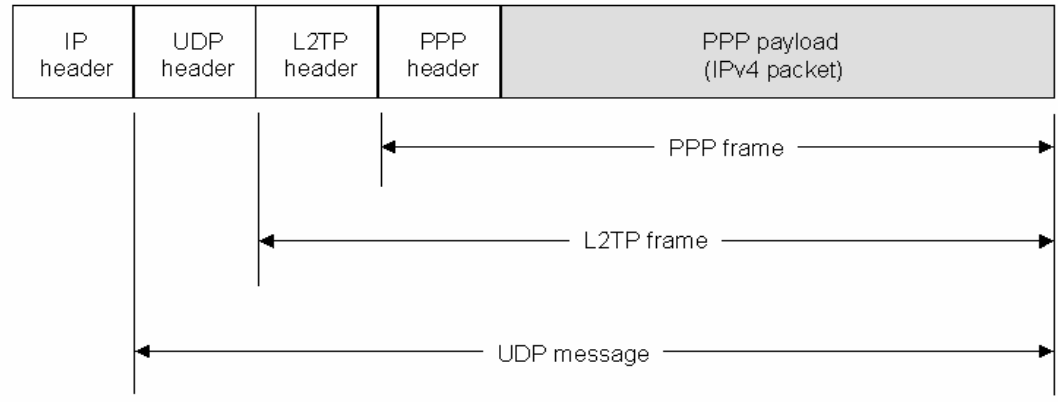
Kuva 20, datapaketista tunnelimoodissa ESP:n lisäämisen jälkeen. [21]

Nykyään on tarjolla monia eri teknologioita, joita voidaan käyttää suojaamaan IP – datan liikenne, kuten SSL/TLS, IPSec tarjoaa silti parhaan kokonaissuojan

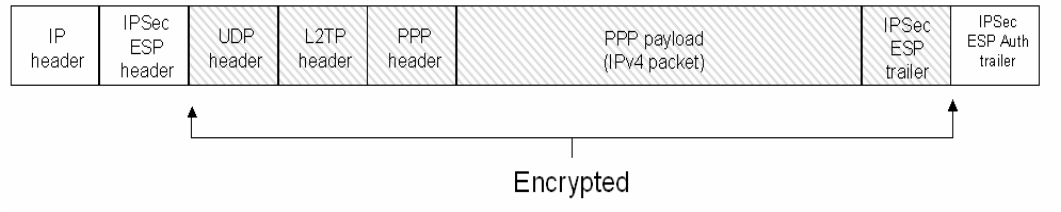
IP:lle. IPSec tarjoaa kolme eri aluetta IP tason turvallisuuteen: autentikoinnin, luottamuksellisuuden ja avainten hallinnan. Käytössä parhaan toimivuuden IP-Sec:n protokollista tarjoaa ESP, joka tarjoaa autentikoinnin ja luottamuksellisuuden, kun taas AH ei tarjoa luottamuksellisuutta. [22]

4.2 L2TP

L2TP on yhdistelmä Ciscon kehittämästä L2F protokollasta ja Microsoftin PPTP protokollasta, joka toimii OSI – mallin 2. kerroksessa ja siten tukee myös ei IP – protokollia. L2TP jättää salauksen ylempien kerrosten protokollien harteille (esim. IPSec) ja hoitaa tiedon kapseloinnin, niin että se voidaan kuljettaa julkisten verkkojen läpi. L2Tp tunneli tehdään kapseloimalla L2TP kehys UDP – paketin sisään, mikä vastaavasti on kapseloitu IP – paketin sisään. Tämän IP – paketin lähde – ja kohdeosoitteet määrittävät yhteyden päätepisteet. Koska uloin kapselointi protokolla on IP, voidaan IPSec:ä käyttää suojaamaan data joka kulkee L2TP tunnelissa. Protokollina IPSec:n kanssa voidaan käyttää AH:ta, ESP:tä (yleisin) ja IKE:ä. ESP:tä käyttämällä saadaan IP – paketille taattua autentikointi, eheyden tarkistus ja salaus. L2TP tarjoaa myös PPP:n autentikointimetodit CHAP (Challenge Handshake Authentication Protocol) ja PAP (Password Authentication Protocol). Näistä CHAP on varmempi menetelmä. CHAP:a käytetään yhteyden aikana vahvistamaan toisen pään ”henkilöllisyys” 3 – osaisella kädenpuristuksella, kun taas PAP käyttää 2 – osaista kädenpuristusta. [20, 24]



Kuva 21, L2TP paketin rakenne [25]

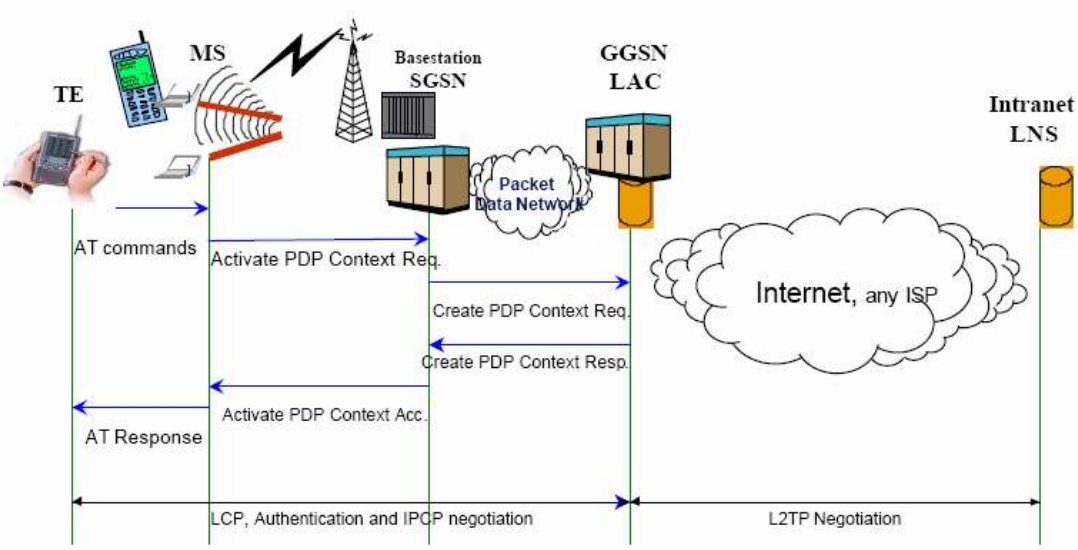


Kuva 22, L2TP liikenteen salaus käyttämällä IPSec:ä ESP:n kanssa. [25]

Kaksi tärkeintä komponenttia, jotka tekevät L2TP:n ovat LAC (L2TP Access Concentrator) ja LNS (L2TP Network Server). LAC kuuluu internet palvelutarjoajan verkkoon ja sen tehtävä on avata L2TP – tunneli itsensä ja LNS:n välille. Tunnelia pitkin kulkee käyttäjän data esim. yrityksen verkkoon. LNS on siis reititin, mikä kuuluu esim. yrityksen verkkoon ja palvelee päätepisteenä L2TP tunneloinnille ja istunnoille. Jos taas PC:ssä tai reitittimessä on L2TP ohjelmisto/toiminnallisuus, niin LAC:a ei tarvita vaan tunnelointi menee RAS:n (Remote Access Server) läpi LNS:lle. RAS ei siis luo tunnelia vaan se ohjaa valmiiksi tunneloidun datan LNS:lle. L2TP hyödyntää kahden tyyppisiä viestejä protokollassaan, kontrolliviestejä ja dataviestejä. Kontrolliviestejä käytetään muodostamaan, ylläpitämään ja purkamaan tunneleita ja puheluita. Kontrolliviestit hyödyntävät luotettavaa kontrollikanavaa L2TP:ssä taatakseen lähetyksen. Dataviestejä käytetään PPP – kehysten kapselointiin ja tunneliin siirtämiseen. Dataviestien pakettien numerointi on mahdollista ja pakettien hukkumistapauksissa ei käytetä uudelleenlähettämistä. [24, 26, 27]

L2TP tukee kahta eri tunnelointimuotoa: ”vapaaehtoinen” (voluntary) ja ”pakollinen” (compulsory) tunneli. Vapaaehtoisen tunnelin muodostaa käyttäjä, käyttämällä L2TP tunnelointiclienttia. Käyttäjä lähettää L2TP paketit NAS:lle (Network Access Server) mikä jatkaa sen eteenpäin LNS:lle. Tunneli on muodostettu käyttäjän koneen/MS:n ja yrityksen verkon välille. Pakollinen tunneli muodostetaan ilman käyttäjän toimia, eikä käyttäjälle myöskään anneta tehdä yhteyteen liittyviä valintoja. Tunnelin muodostuksen hoitaa ISP. Pakollisessa tunneloinnissa isäntäkone avaa/aloittaa yhteyden palveluntarjoalle. MVPN:n käyttäjä ottaa yhteyden yrityksen verkkoon liittymällä ensin GPRS verkkoon ja aloittaa PPP istunnon ja määrittelee käytettävän APN:n. Kun PDP – konteksti on aktiivisena istunnon kontrolli luovutetaan GGSN:n tukemalle LAC:lle, joka hoitaa tunnelin avaamisen yrityksen LNS:lle. LAC kapseloi paketit L2TP:ksi ja tunneloi ne LNS:lle. Näin

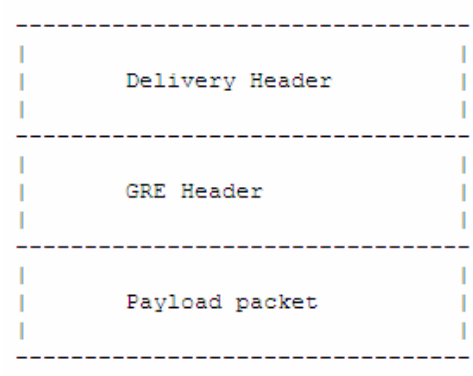
tunneli on muodostettu etäkäyttäjän ja yrityksen verkon välille. LAC hoitaa myös GTP – L2TP tunneli muutoksen. Vaikka ISP muodostaa yhteyden, käyttäjän täytyy hoitaa liikenteen turvaaminen esim. käyttämällä IPSec:ä. Pakollisessa tunneloinnissa ISP:n täytyy tukea L2TP:tä. [3, 20, 26]



Kuva 23, VPN:n toteutus L2TP:tä hyödyntäen. [12]

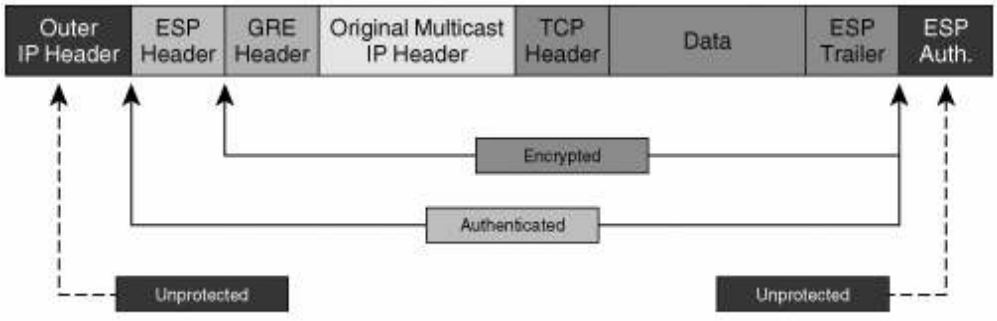
4.3 GRE

GRE on IP – tunnelointiprotokolla, joka on suunniteltu kapseloimaan verkkotason paketteja IP – tunnelointipakettien sisään. Protokollan on kehittänyt Cisco. Useimmissa tapauksissa, järjestelmällä on paketti (Payload packet) joka täytyisi kapseloida ja lähettää määränpäähänsä. Paketti on ensin kapseloitu GRE – paketilla, jäljelle jäänyt GRE – paketti kapseloidaan sen jälkeen jollain toisella protokollalla ja lähetetään eteenpäin. Tätä ulompaa protokollaa kutsutaan kuljetus protokollaksi (Delivery Protocol/Header). GRE – tunneli on suunniteltu kokonaan tilattomaksi, mikä tarkoittaa, että mikään tunnelin päätepisteistä ei pidä minkäänlaista informaatiota etäpään tilasta tai saatavuudesta. Tämä antaa asiakkaille joustavuutta konfiguroida tai uudelleen konfiguroida IP – arkkitehtuuriaan ilman, että täytyy olla huolissaan liitettävyydestä/yhteensopivuudesta. GRE luo virtuaalisen pisteestä pisteeseen – yhteyden reitittimien välille yli IP – verkon. [11, 28]



Kuva 24, GRE – kapseloidun paketin muoto. [28]

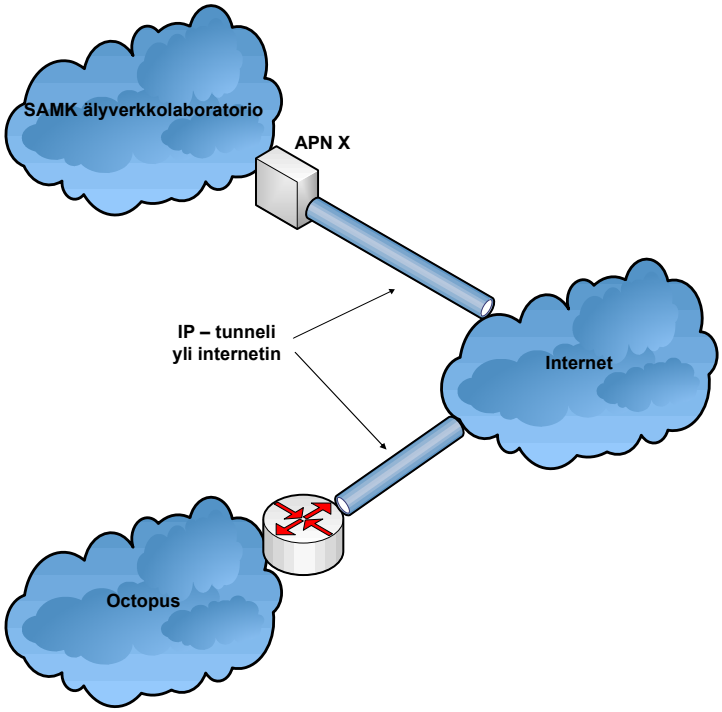
GRE protokolla ei tarjoa itsessään mitään merkittävää turvallisuutta. Ainoa hyvä ratkaisu on käyttää GRE – protokollan kanssa IPSec:n AH:ta tai ESP:tä, jolloin saadaan tarvittava turvallisuus taattua. IPSec + GRE mallia käytetään liikenteen kanssa, joka vaatii hyvän luottamuksellisuuden ja jota ei normaalisti voida käyttää normaalin IPSec päästä – päähän yhteyden kanssa. IP – pohjaiset ryhmälähetys (multicast) – protokollat, kuten ryhmälähetyssovellukset streamatulle äänelle ja videolle yli IP:n sopivat tähän kategoriaan. GRE:tä käyttämällä, ryhmälähetys – liikenne tyypit voidaan esittää sellaisessa muodossa, jotka IPSec:n salaus ”moottori” ymmärtää. [28, 29]



Kuva 25, Multicast dataan lisätty GRE + IPSec:n ESP. [29]

5 IP – TUNNELIN TOTEUTUS SAMK – OCTOPUS

Opinnäytetyöni tarkoituksena on toteuttaa IP – tunneli SAMK:n älyverkkolaboratorion GPRS – verkon ja oululaisen 3G – ja WLAN – verkkoja hyödyntävän testausympäristö Octopus:n välille. Yhteys toteutetaan yli julkisen IP – verkon ja yhteyttä varten täytyy määrittää toimiva tunnelointiprotokolla ja testata yhteyden toiminta.

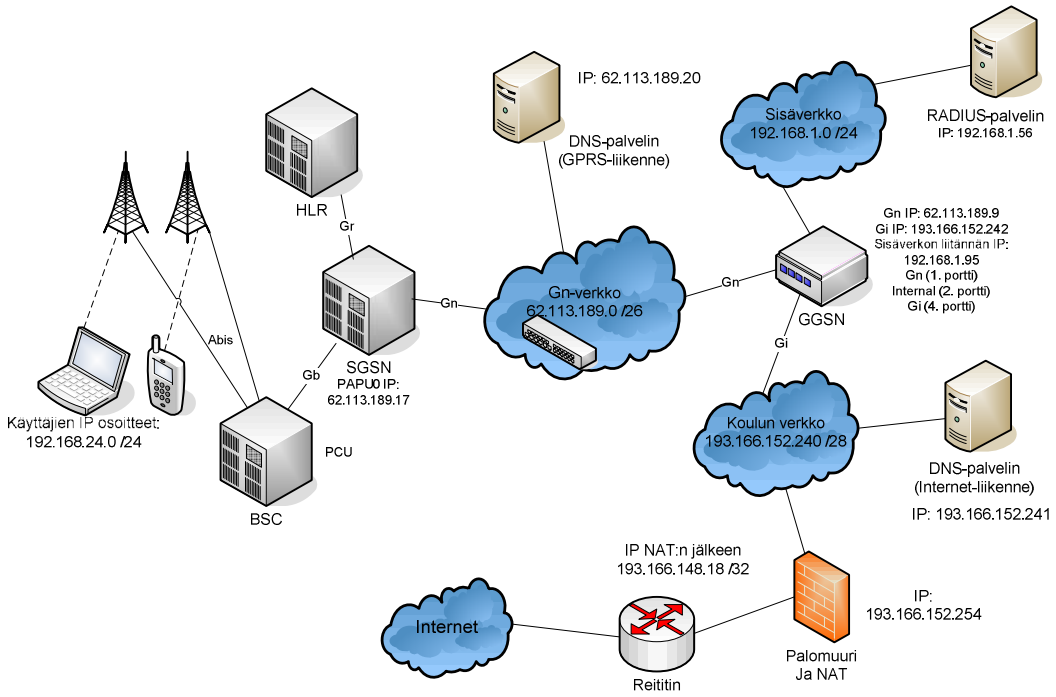


Kuva 26, tarvittava yhteys välillä SAMK – Octopus

5.1 SAMK:n GPRS – verkko

SAMK:n GPRS – verkko pohjautuu Nokian valmistamiin laitteisiin. SGSN perustuu Nokian DX 200 järjestelmään ja GGSN on Nokian IP 650 sarjan laite. DX – käyttöliittymä on myös muissa laboratorion telelaitteissa. Nimipalvelimena verkossa on Linux – pohjainen (MandrakeLinux jakeluversio 10.1) named DNS – palvelin ja Radius – palvelimena toimii Linuxiin asennettu FreeRADIUS ohjelma. Runkoverkon kytkimenä toimii Nortel Networks:n 100 Mbit:n Baystack – kytkin.

SGSN, GGSN ja DNS – nimipalvelin ovat kiinni Gn – verkon Baystack kytkimessä ja samassa aliverkossa 62.113.189.0 /26. GGSN:stä on yhteydet myös laboratorion omaan aliverkkoon IP – osoitteella 192.168.1.95 /24 ja SAMK:n omaan julkiseen verkkoon osoitteella 193.166.152.254 /28 (Gi – rajapinta). Radius – palvelin on kiinni laboratorion omassa aliverkossa osoitteella 192.168.1.56 /24. Päätelaitteet ovat koulun osoiteavaruudesta varatussa aliverkossa 192.168.24.0 /24. [5]



Kuva 27, SAMK:n GPRS - verkko [16]

5.2 IP – tunnelointiprotokollan ja yhteystyypin valinta

Ensimmäiseksi asiaksi yhteyttä määriteltäessä ja protokollaa valittaessa tuli eteen yhteystyypin valinta, eli mikä yhteystyyppi sopii parhaiten SAMK:n tapauksessa, käytetäänkö päästä – päähän yhteyttä vai aloitetaanko IP – tunneli vasta GGSN:ltä tai erilliseltä VPN – laitteelta. Päästä päähän yhteys jätettiin pois vaihtoehdoista, koska koulussa on käytössä useita päätelaitteita joihin täytyisi asentaa ensin pääteohjelma jonka avulla yhteys voitaisiin muodostaa. Toinen syy oli koulussa käytössä oleva NAT osoitemuunnos, mikä on usein tuonut ongelmia VPN – yhteyden (IPSec) toimivuudelle. Erillisen VPN – laitteen kautta tehtävä yhteys tulisi kysee-

seen ainoastaan siinä tapauksessa, että yhteys täytyisi salata IPSec:ä käyttäen. Koska tarvittava yhteys tulee opetuskäyttöön, eikä siinä tulla lähettämään mitään arkaluontoista tietoa ei salaus ole tällä hetkellä tarpeellinen. Seuraavaksi täytyi tutkia mahdollisuutta voisiko yhteyden aloittaa GGSN:ltä. GGSN:n asetuksia tutkiessani havaitsin, että APN määrittelyissä tuetaan IPv4:sen lisäksi IP tunnelin muodostamista. Vaihtoehtoina tunneloinnin muodostamiselle APN:ssä ovat GRE, L2TP ja IP – in – IP. Koska IP – tunneli tullaan tekemään Octopus:iin Oulun ammattikorkeakoulun kautta, täytyi yhteyden valinnassa konsultoida myös heidän teknistä henkilökuntaansa ja Octopus:n henkilökuntaa. Puhelinneuvottelussa OAMK:n ja Octopus:n henkilöstön kanssa päädyimme protokollan valinnassa GRE – tunneliin. Valintaa helpotti OAMK:n henkilöstön hyvät kokemukset GRE – tunnelin käytöstä vastaavissa tilanteissa. Vaikka GRE – tunnelia käytettäessä ei pakettiliikennettä pystytä salaamaan, voidaan silti käyttäjien autentikointi suorittaa RADIUS palvelinta hyväksi käyttäen. GRE – tunnelia käytettäessä on käytössä non – transparent moodi. [17]

5.3 GRE – tunneloinnin toteutus

GRE – tunneloinnin määrittely aloitettiin GGSN:stä konfiguroimalla yhteyttä varten oma APN. APN:n nimeksi tuli ”octopus”. Seuraavaksi määriteltiin käytettävä tunnelointitapa eli GRE. Tämän jälkeen täytyi määritellä tunnelin eri päiden (SAMK – OAMK/Octopus) IP – osoitteet. SAMK:n (Tunnel Local IP Address) pään IP – osoitteeksi määriteltiin Gi rajapinnan IP – osoite 193.166.152.242 ja OAMK/Octopus pään IP – osoitteeksi määriteltiin 82.128.161.242. Vastaavasti OAMK/Octopus:ssa tehtiin tarvittavat määritykset heidän reitittimeensä tunnelin muodostamiseksi. [18]

IPv4 Access Point

Identification			
Name	octopus	Numeric ID	1
Description	octopus apn	Row Status	Active
Connection Type			
Type	GRE tunnel	Virtual Mobile Address	
Tunnel Local IP Address	193.166.152.242	Tunnel Remote IP Address	82.128.161.242
Redistribute to RIP	Disabled	Redistribute to OSPF External	Disabled
OSPF	Disabled		
DHCP Servers			
IP address 1		IP Address 2	
IP Address 3		IP Address 4	
Release Message Sending	Enabled		
RADIUS Servers			
Primary Authentication Server IP Address		Port Number	
Primary Authentication Server Key		Description	
Secondary Authentication Server IP address		Port Number	
Secondary Authentication Server Key		Description	
Primary Account Server IP address		Port Number	
Primary Account Server Key		Description	
Secondary Account Server IP address		Port Number	
Secondary Account Server Key		Description	
Client IP Address		Account Server Operation	Not used
Retransmission Timeouts			
Limitations			
Max. Active PDP Contexts	16382	Max. Dynamic IP addresses	10
Methods			
IP Address Generation Method	GGSN	User Authentication Method	None
Security			
Intermobile Traffic	Disabled	Inter-AP Traffic	Disabled
Unverified Mobile Acceptance	Enabled		
Mobile's IP Addresses			
Dynamic IP Address	192.168.24.0	Mask Length	25
Static IP Address	192.168.24.0	Mask Length	25
Toll Free Network			
Toll FreeNetwork	0.0.0.0	Mask Length	0
DNS			
DNS 1		DNS 2	
Session Timeouts			
Session Timeout		Idle Timeout	
Quality of Service			
DSCP Mark uplink packets	Disabled		

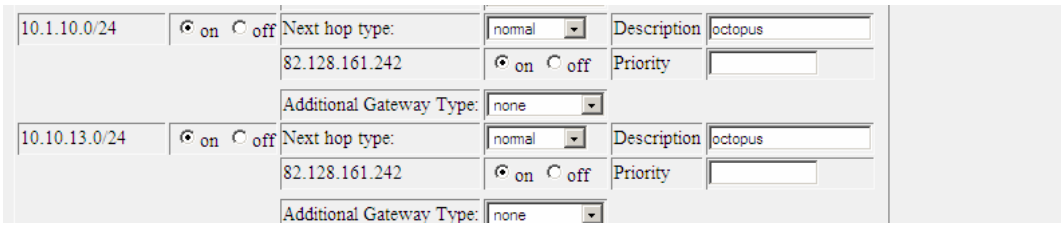
Kuva 28, GGSN:ään konfiguroitu Octopus APN

```
interface Tunnel1
 ip unnumbered FastEthernet0/0.2
 ip tcp adjust-mss 1436
 tunnel source FastEthernet0/0.2
 tunnel destination 193.166.152.242
 tunnel path-mtu-discovery

ip route 192.168.24.0 255.255.255.0 Tunnel1
```

Kuva 29, OAMK/Octopusissa tehdyt tunnelointi määritykset [18]

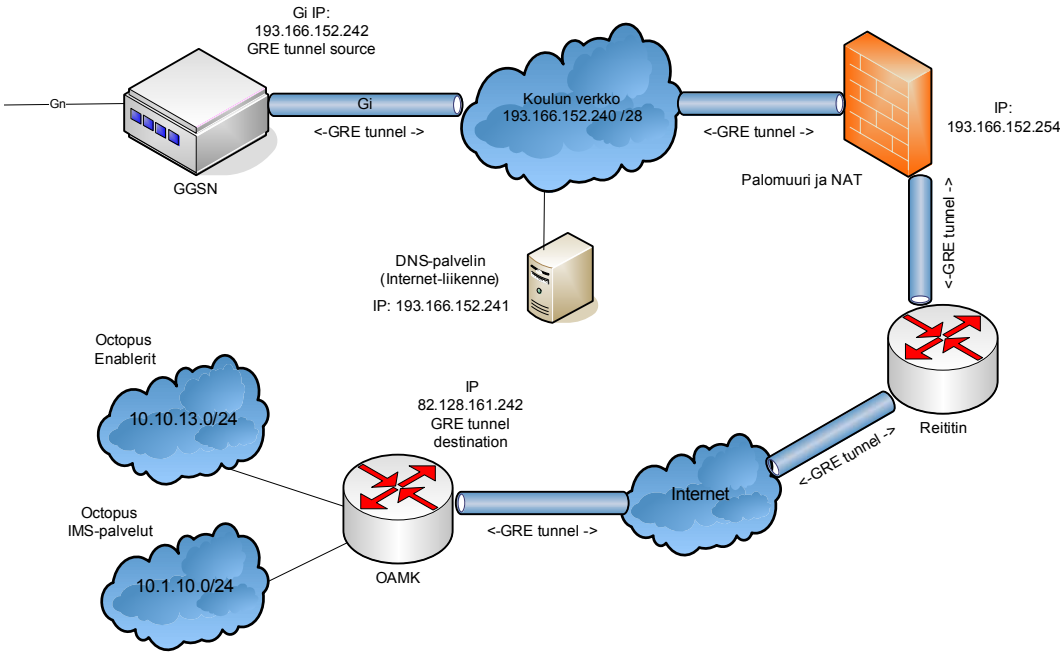
Nämä määritykset koskivat vasta GRE – tunnelia ja vielä täytyi tehdä reitit Octopus:n verkkoihin 10.10.13.0 /24 (Enablerit) ja 10.1.10.0 /24 (IMS – palvelut). SAMK:n GGSN:ään konfiguroitiin staattiset reitit siten, että kaikki liikenne edellä mainittuihin verkkoihin kulkee aina IP – osoitteen 82.128.161.242 kautta. Vastaavasti OAMK:ssa tehtiin määritykset jotta liikenne saataisiin kulkemaan GRE – tunnelin jälkeen eteenpäin haluttuihin verkkoihin. Näiden määritysten avulla saadaan GRE – tunneli muodostettua GGSN:ltä OAMK:n verkon kautta Octopus:n verkkoihin. (Yhteys toimii myös ilman staattisia reittejä SAMK:n päässä. Staattiset reitit takasivat testausvaiheessa, että liikenne ohjautuu oikeaan osoitteeseen.)



Kuva 30, GGSN:ään konfiguroidut staattiset reitit

Yhteyden toimivuus testattiin lähettämällä päätelaitteelta ping – ohjelman avulla testipaketti (ICMP Echo Request) GRE – tunnelin osoitteeseen 82.128.161.242 ja saamalla sieltä vastaus (ICMP Echo Reply). Saatuamme varmuuden GRE – tunnelin toimivuudesta, ”pingasimme” myös Octopus:n verkoissa 10.10.13.0 /24 (Enablerit) ja 10.1.10.0 /24 (IMS – palvelut) olevia IP – osoitteita. Tällä varmistimme, että reititys toimii kuten halusimme. OAMK:n päästä ”pingattiin” vastaavasti päätelaitteitamme. Etherealin kanssa tehty liikenteen monitorointi Gi rajapinnalta varmisti GRE – kapseloinnin toimivuuden. Etherealista saadut tulosteet GRE – paketeista ovat liitteenä 1.

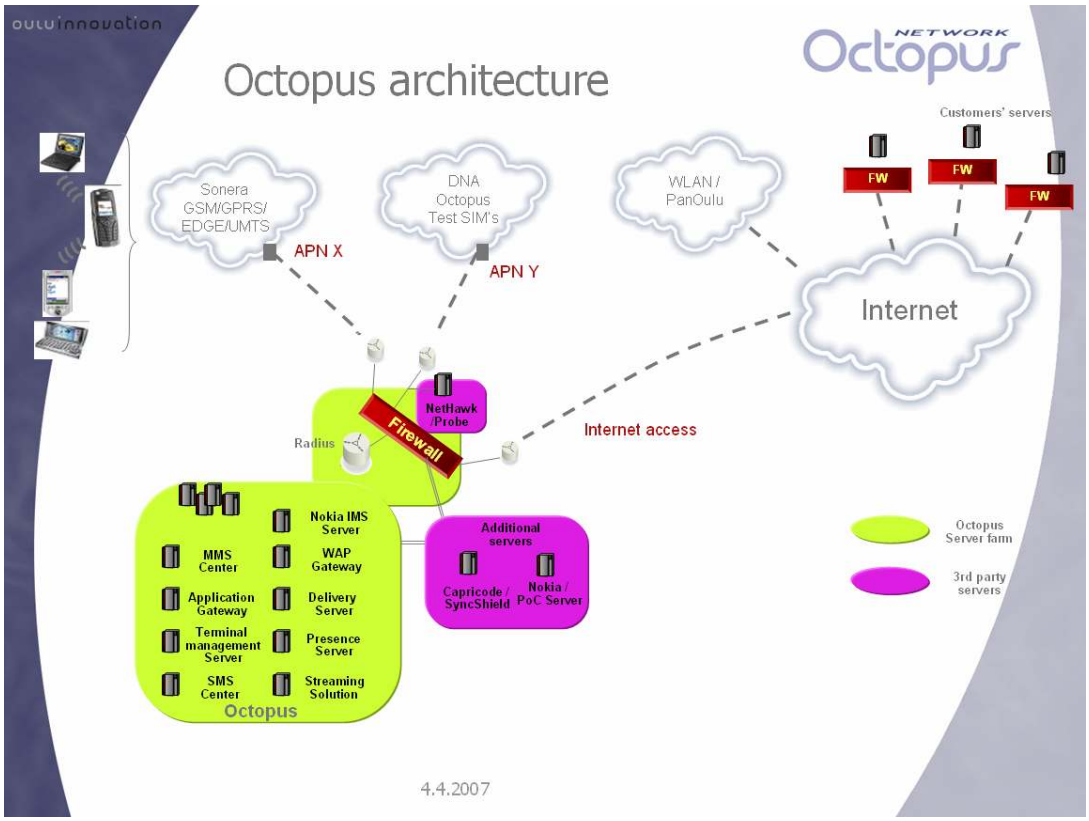
GPRS – yhteys Octopus verkkoon avataan valitsemalla päätelaitteen GPRS asetuksista octopus APN käyttöön ja avaamalla GPRS – yhteys auki. Kontekstin luonninjälkeen data liikenne menee päätelaitteelta SGSN:lle, jonka kautta se menee GTP – tunnelia pitkin GGSN:lle. GGSN pakkaa IP – paketit GRE – protokollan sisään ja lähettää paketit tunnelia pitkin OAMK:n reitittimelle, jossa GRE – kapseloitujen pakettien purku tapahtuu. Tämän jälkeen puretut IP – paketit jatkavat matkaa Octopus:n verkossa oleviin palveluihin.



Kuva 31, GRE – tunneli SAMK:n GGSN:ltä OAMK:n reitittimelle

6 OCTOPUS

Octopus on GPRS –, 3G – ja WLAN – verkkoja hyödyntävä testausympäristö. Ympäristön sovellus – ja teknologiamahdollistajat (ks. liite 2, Lyhyt kuvaus Octopus – ympäristön palvelimista) tarjoavat edellytykset uusien tuotteiden ja palvelujen kehittämiseen ja testaamiseen. Testausalustan ympärille rakentuvat Octopusin asiantuntijapalvelut tähtäävät mobiilipalveluiden ja – sovellusten ideointiin, innovointiin ja lopulta viemiseen markkinoille. Koko prosessin ajan Octopus tarjoaa asiakkailleen koulutusta ja liiketoimintatukea. Lisää tietoa Octopus:sta: http://www.octo.fi/ . [30]



Kuva 32, Octopus arkkitehtuuri. [31]

7 YHTEENVETO

Opinnäytetyössä toteutin yhteyden SAMK:n GPRS – verkon ja oululaisen Octopus – verkon välille. Työ sopi minulle hyvin, koska olin aikaisemmassa työharjoittelussani älyverkkolaboratoriossa keskittynyt GPRS – verkon toimintaan. Itse yhteyden päätin toteuttaa GRE – protokollaa käyttämällä. GRE – protokollaan päätyminen oli loppujen lopuksi helppo ratkaisu, koska OAMK:n henkilökunnalla oli hyvä kokemus siitä aikaisemmissa yhteyksissään ja se että Nokian GGSN:n APN:n määrittelyissä oli tuki sille eikä näin ollen investointeja uusiin laitteisiin tarvittu.

Työssäni kävin läpi VPN:n teoriaa ja esittelin eri mahdollisuuksia miten tunnelointi voidaan toteuttaa GPRS – verkosta toiseen verkkoon. Havaitsin, että tunneloinnin toteuttamiseen voidaan käyttää monia eri protokollia. Mikäli tunneloinnin toteutuksen ehdottomana edellytyksenä on riittävä salaus, niin vaihtoehtoja on vain yksi, IPSec. Kun taas yhteyttä käytetään ei niin arkaluontoisten tietojen siirtämiseen kuten SAMK:n tapauksessa voidaan käyttää jotain muutakin protokollaa kuten GRE.

Työn tavoite saavutettiin juuri oikeaan, koska seuraava oppilas oli jo aloittamassa omaa opinnäytetyötään, jossa hän tulee hyödyntämään yhteyttä Octopus:iin. Yhteyttä voidaan myös hyödyntää opetuksessa, kun halutaan demonstroida 3G – verkon palveluita, esim. IMS:n käyttöä.

LÄHDELUETTELO

[1] Bates, R. GPRS. McGraw-Hill TELECOM. 2002. 380 s.

[2] Granlund, K. Langaton tiedonsiirto. Docendo Finland Oy. 2001. 399s.

[3] Shneyderman, A. Mobile VPNs for Next Generation GPRS and UMTS Networks. Lucent Technologies. 2000. [verkkodokumentti]. [viitattu 19.2.2007]. Saatavissa: http://esoumoy.free.fr/telecom/tutorial/3G-VPN.pdf

[4] Penttinen, J. Tietoliikennetekniikka.Werner Söderström Osakeyhtiö. 2006. 234s.

[5] Rosu, A. Opinnäytetyö: GPRS-noden käyttöönotto. Pori: Satakunnan ammattikorkekoulu. 2005. 51s.

[6] EN 301344 V7.4.1. Digital cellular telecommunications system (phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2. European Telecommunication Standard. 1998.

[7] rfc 2764, A Framework for IP Based Virtual Private Networks. IETF. 2000. [verkkodokumentti]. [viitattu 19.2.2007]. Saatavissa: http://www.ietf.org/rfc/rfc2764.txt

[8] Rautpalo, J. GPRS Security - Secure Remote Connections over GPRS [verkkodokumentti]. [viitattu 19.2.2007]. Saatavissa: http://users.tkk.fi/~jrautpal/gprs/gprs_sec.html

[9] The Evolution of MobileVPN and its Implications for Security. Nokia. 2006. [verkkodokumentti]. [viitattu 20.2.2007]. Saatavissa: http://www.nokiaforbusiness.com/documents/WhitePaper_TheEvolutionofVPN.pdf

[10] Negotiation of NAT-Traversal in the IKE. IETF. 2003. [verkkodokumentti]. [viitattu 20.2.2007]. Saatavissa:
http://www3.ietf.org/proceedings/03nov/I-D/draft-ietf-ipsec-nat-t-ike-07.txt

[11] The Nokia Gateway GPRS Support Node Release 2, Product Description

[12] Kopeikin, R. Sommars, S. Wireless GPRS Access to Virtual Private Networks For Carriers and ESPs. Lucent Technologies. 2000. [verkkodokumentti]. [viitattu 1.2.2007]. Saatavissa:
http://www.3gamericas.org/pdfs/access.pdf

[13] rfc 2401, Security Architecture for the Internet Protocol. IETF. 1998. [verkkodokumentti]. [viitattu 19.2.2007]. Saatavissa:
http://www.ietf.org/rfc/rfc2401.txt

[14] IPSec. Hervé Schauer Consultants.1998-2000. [verkkodokumentti]. [viitattu 7.3.2007]. Saatavissa:
http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en#11

[15] rfc 3884, Use of IPsec Transport Mode for Dynamic Routing. IETF. 2004. [verkkodokumentti]. [viitattu 8.3.2007]. Saatavissa:
http://www.ietf.org/rfc/rfc3884.txt

[16] Huhtamäki, S. Opinnäytetyö: Autentikointi RADIUS-palvelinta käyttäen. Pori: Satakunnan ammattikorkeakoulu. 2007. 38s.

[17] Puhelinneuvottelu, SAMK Jarkko Rahkola – OAMK Jukka Orajärvi – Octopus Kari Lampela pe 26.1.2007 14.30.

[18] Orajärvi, J. gre-parametrit (octopus). [sähköpostiviesti]. Vastaanottaja: japerahk@tp.spt.fi. Lähetetty ma 12.3.2007 19:59.

[19] rfc 4302, IP Authentication Header. IETF. 2005. [verkkodokumentti]. [viitattu 11.4.2007]. Saatavissa: http://www.ietf.org/rfc/rfc4302.txt

[20] Encapsulation Security Payload, Authentication Header ja L2TP. IBM.2002, 2005. [verkkodokumentti]. [viitattu 11.4.2007]. Saatavissa: http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzaja/rzajaesp.htm

[21] rfc4303, IP Encapsulating Security Payload (ESP). IETF. 2005. [verkkodokumentti]. [viitattu 12.4.2007]. Saatavissa: http://www.ietf.org/rfc/rfc4303.txt

[22] Shawn W. Toderick. Encapsulating Security Payload: Strengths and Weaknesses. 2004. [verkkodokumentti]. [viitattu 7.3.2007]. Saatavissa: http://www.infosecwriters.com/text_resources/pdf/ESP_Strengths_and_Weaknesses.pdf

[23] Pehrsson Å. Wireless VPN: IPSec vs SSL/TLS. [verkkodokumentti]. [viitattu 7.3.2007]. Saatavissa: http://www.it.kth.se/courses/2G1330/2G1330_asa_pehrsson-20050712.pdf

[24] Nokkonen J, Partanen J, Salonen R ja Jokiniemi J. PPTP ja L2TP perusteet. [verkkodokumentti]. [viitattu 23.4.2007]. Saatavissa: http://www.ac.tut.fi/aci/courses/7601010/2003_audi/pdf/PPTP_L2TP.pdf

[25] TCP/IP Fundamentals for Microsoft Windows. Microsoft. 2005. [verkkodokumentti]. [viitattu 23.4.2007]. Saatavissa: http://www.microsoft.com/technet/network/evaluate/technol/tcpipfund/tcpipfund_ch14.mspx

[26] Layer 2 Tunneling Protocol (L2TP) Overview. IBM Corporation. 1999. [verkkodokumentti]. [viitattu 23.4.2007]. Saatavissa: http://www03.ibm.com/servers/eserver/iseries/tcpip/vpn/redbooks/l2tppres/pdf/l2tppres.pdf

[27] rfc2661, Layer Two Tunneling Protocol "L2TP". IETF. 1999. [verkkodokumentti]. [viitattu 23.4.2007]. Saatavissa:
http://www.ietf.org/rfc/rfc2661.txt

[28] rfc1702, Generic Routing Encapsulation over IPv4 networks. IETF. 1994. [verkkodokumentti]. [viitattu 1.5.2007]. Saatavissa:
http://www.ietf.org/rfc/rfc1702.txt

[29] Carmouche, J. Basic IPsec VPN Topologies and Configurations. Cisco. 2006. [verkkodokumentti]. [viitattu 2.5.2007]. Saatavissa:
http://www.ciscopress.com/articles/article.asp?p=606584&seqNum=2&rl=1

[30] Octopus verkkosivusto. [verkkodokumentti]. [viitattu 4.4.2007]. Saatavissa:
http://www.octo.fi/

[31] Octopus asiakasmateriaali. Octopus Network 20070223_tiivis.ppt. [viitattu 4.4.2007].

[32] Octopus asiakasmateriaali. Octopus_liittymä_asetukset_2_0.pdf. [viitattu 4.4.2007].

LIITTEET

LIITE 1 Gi rajapinnalta monitoroidut GRE – kapseloidut ping request ja response paketit Etherealilla avattuna. Ping IP – osoitteesta **192.169.24.8** GRE – tunnelin kautta **193.166.152.242 – 82.128.161.242** Octopus:n verkon IP – osoitteeseen **10.10.13.100**.

No.	Time	Source	Destination	Protocol	Info
2	0.081249	**192.168.24.8**	**10.10.13.100**	**ICMP**	**Echo (ping) request**

Frame 2 (71 bytes on wire, 71 bytes captured)
Arrival Time: Mar 19, 2007 11:04:19.024620000
Time delta from previous packet: 0.081249000 seconds
Time since reference or first frame: 0.081249000 seconds
Frame Number: 2
Packet Length: 71 bytes
Capture Length: 71 bytes
Protocols in frame: eth:ip:gre:ip:icmp:data
Coloring Rule Name: ICMP
Coloring Rule String: icmp
Ethernet II, Src: NokiaInt_0c:0e:f3 (00:a0:8e:0c:0e:f3), Dst: 3Com_14:c1:44 (00:04:76:14:c1:44)
Destination: 3Com_14:c1:44 (00:04:76:14:c1:44)
Source: NokiaInt_0c:0e:f3 (00:a0:8e:0c:0e:f3)
Type: IP (0x0800)
Internet Protocol, Src: 193.166.152.242 (193.166.152.242), Dst: 82.128.161.242 (82.128.161.242)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 57
Identification: 0xeb08 (60168)
Flags: 0x00

Fragment offset: 0

Time to live: 255

Protocol: GRE (0x2f)

Header checksum: 0x8181 [correct]

Source: 193.166.152.242 (193.166.152.242)

Destination: 82.128.161.242 (82.128.161.242)

Generic Routing Encapsulation (IP)

Flags and version: 0000

Protocol Type: IP (0x0800)

Internet Protocol, Src: 192.168.24.8 (192.168.24.8), Dst: 10.10.13.100 (10.10.13.100)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 33

Identification: 0x78f1 (30961)

Flags: 0x00

Fragment offset: 0

Time to live: 128

Protocol: ICMP (0x01)

Header checksum: 0xd1cc [correct]

Source: 192.168.24.8 (192.168.24.8)

Destination: 10.10.13.100 (10.10.13.100)

Internet Control Message Protocol

No.	Time	Source	Destination	Protocol	Info
3	0.111436	**10.10.13.100**	**192.168.24.8**	**ICMP**	**Echo (ping) reply**

Frame 3 (71 bytes on wire, 71 bytes captured)

Arrival Time: Mar 19, 2007 11:04:19.054807000

Time delta from previous packet: 0.030187000 seconds

Time since reference or first frame: 0.111436000 seconds

Frame Number: 3

Packet Length: 71 bytes

Capture Length: 71 bytes

Protocols in frame: eth:ip:gre:ip:icmp:data

Coloring Rule Name: ICMP

Coloring Rule String: icmp

Ethernet II, Src: 3Com_14:c1:44 (00:04:76:14:c1:44), Dst: NokiaInt_0c:0e:f3 (00:a0:8e:0c:0e:f3)

Destination: NokiaInt_0c:0e:f3 (00:a0:8e:0c:0e:f3)

Source: 3Com_14:c1:44 (00:04:76:14:c1:44)

Type: IP (0x0800)

Internet Protocol, Src: 82.128.161.242 (82.128.161.242), Dst: 193.166.152.242 (193.166.152.242)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 57

Identification: 0x34a7 (13479)

Flags: 0x04 (Don't Fragment)

Fragment offset: 0

Time to live: 239

Protocol: GRE (0x2f)

Header checksum: 0x07e3 [correct]

Source: 82.128.161.242 (82.128.161.242)

Destination: 193.166.152.242 (193.166.152.242)

Generic Routing Encapsulation (IP)

Flags and version: 0000

Protocol Type: IP (0x0800)

Internet Protocol, Src: 10.10.13.100 (10.10.13.100), Dst: 192.168.24.8 (192.168.24.8)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 33

Identification: 0x33d3 (13267)

Flags: 0x04 (Don't Fragment)

Fragment offset: 0

Time to live: 254

Protocol: ICMP (0x01)

Header checksum: 0x58ea [correct]

Source: 10.10.13.100 (10.10.13.100)

Destination: 192.168.24.8 (192.168.24.8)

Internet Control Message Protocol

LIITE 2 Lyhyt kuvaus Octopus – ympäristön palvelimista [32]

SMSC (Short Message Service Centre)

SMSC eli lyhytsanomakeskus toimii tekstiviestien välittäjänä ja SMS -palvelun käyttö vaatii vain Octopus -lyhytsanomakeskuksen numeron päivittämisen puhelimen asetuksiin.

MMSC (Multimedia Service Centre)

MMSC toimii multimedia viestien välittäjänä ja palvelun käyttö vaatii ainoastaan puhelimessa olevat MMS -asetukset.

WAP-GW (WAP Gateway)

WAP-GW on palvelin, joka toimii yhdyskäytävänä langattoman verkon ja Inter- tai intranetissä sijaitsevien WAP -palveluiden välillä. WAP-palvelun käyttöön riittää oikeat asetukset puhelimessa.

AGW (Application Gateway)

AGW:n avulla laajennetaan multimediapalvelu myös ei MM-puhelimen omistajien käyttöön. Perinteisen puhelimen omistajat saavat tekstiviestin heille saapuneesta MM-viestistä. Tämä tekstiviesti sisältää web-osoitteen ja tilapäisen tunnuksen viestin lukemista varten. AGW toimii yhdyskäytävänä myös sähköpostien välittämisessä Internetin ja MM-puhelimien välillä. AGW mm. muuntaa multimediaa sisältävät sähköpostit puhelimien ymmärtämään formaattiin. Lisäksi AGW mahdollistaa viestien lähettämisen web-selaimen avulla ja viestien varastoimisen Personal albumiin.

NAP (Nokia Artuse Profiler)

Nokia Artuse Profile Directory (NAP) on tietokanta, jonka avulla operaattori/tilaajat voivat hallita tilaajakohtaisia multimedia-asetuksia. Multimediapalvelun yhteydessä NAP tukee seuraavia ominaisuuksia:

• MM-palveluun liittyvät asetukset (palvelun esto, tukeeko puhelin MM ominaisuuksia jne.)
• MM-viestien siirto tai kopiointi toiseen numeroon tai osoitteeseen.
• MM-viestien lähettämisen ja/tai vastaanottamisen esto.

MSG (Messaging Gateway) ent. NAMP

Nokia Messaging Gateway on palvelin, joka toimii yhdyskäytävänä langattoman mobiiliverkon ja Inter/intranetissä sijaitsevien sovellusten välillä. Nokia NMG:n avulla tuotetaan tilaajille HTML, WML, Nokia Smart Messaging, ja multimedia sisältöisiä lisäarvopalveluita.

DLS (Delivery Server)

Nokia Delivery Server mahdollistaa sisällön lataamisen Octopus GPRS-verkon kautta mobiilipäätelaitteeseen. DLS hoitaa käyttäjän tunnistamisen, hakee käyttäjän tilaaman sisällön, toimittaa sen päätelaitteeseen ja generoi laskutusinformaation. Jaettava sisältö voi olla esim. Java-sovelluksia, kuvia, musiikkia yms. Ladattavan tiedoston koolle ei ole rajoitusta.

Streaming Solution

Nokia Streaming Solution on järjestelmä, jonka kautta voidaan reaaliaikaisesti tuoda videokuvaa ja ääntä internetissä sijaitsevalta palvelimelta käyttäjän päätelaitteeseen. Streaming solution koostuu Streaming serveristä ja proxysta. Proxy välittää päätelaitteen pyynnön serverille, joka tunnistaa käyttäjän ja varmistaa, että pyydetty videotiedosto on saatavilla. Streaming server lähettää videostreamin proxylle, joka monistaa ja lähettää sen kullekin yhtäaikaiselle käyttäjälle. Nokia Streaming Solution koostuu RealNetworks Helix Universal Serveristä ja Proxy:stä.

Nokia Terminal Management Server

Nokia Terminal Management Server mahdollistaa puhelimien konfiguraatioiden jakamisen päätelaitteisiin, esim. WAP ja MMS -asetukset, OTA -viestinä (Over The Air).

Nokia Presence Server

Presencen avulla käyttäjät voivat luoda ja käyttää dynaamisia profiileja, sisältäen mm. tietoa tavoitettavuudesta, sijainnista, sen hetkisistä aktiviteeteista sekä päätelaitteen ominaisuuksista. Presence mahdollistaa uusia palveluja sekä tuo uusia mahdollisuuksia olemassa oleviin palveluihin.

SIP proxy

SIP (Session Initiation Protocol) serveri mahdollistaa langattomat IP yhteydet. SIP:n avulla pystytään luomaan palvelujen käytettävissä oleva IP – yhteys kahden päätelait-

teen välille, oli sitten kyseessä kännykkä, PC, kämmentietokone, videokamera tai jokin muu laite. SIP – yhteys mahdollistaa uudenlaisia IP-pohjaisia palveluja, kuten PoC (Push-to-Talk), multiplayer-pelit ja multimediasisällön jakaminen.

Nokia IMS (IP Multimedia Subsystem)

Nokia IMS on ns. operaattori SIP. Se lisää SIP proxyyn ulottuvuuksia joita kaupallisessa ympäristössä toimittaessa tarvitaan. Mukana on mm. sessioiden hallinta, autentikointi, palvelun tavoittaminen, yhteensopivuus, laskutus sekä toiminta muiden palvelumahdollistajien kanssa kuten esimerkiksi Presence.