Satakunnan ammattikorkeakoulu

Samuli Huhtamäki

AUTENTIKOINTI RADIUS-PALVELINTA KÄYTTÄEN

Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

2007

TIIVISTELMÄ

AUTENTIKOINTI RADIUS-PALVELINTA KÄYTTÄEN
Samuli Huhtamäki

SATAKUNNAN AMMATTIKORKEAKOULU
Tekniikan Porin Yksikkö
Tekniikantie 2
28600 Pori

Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
Työn tilaaja: Satakunnan ammattikorkeakoulu
Työn valvoja: Juha Aromaa, DI
Päättötyö: 38 sivua
Tammikuu 2007
UDK: 004.7, 621.39

Asiasanat: RADIUS, autentikointi, pakettiverkko

Tässä opinnäytetyössä otettiin käyttöön RADIUS-palvelin Satakunnan ammattikorkeakoulun GPRS-verkossa. Työssä esiteltiin RADIUKSEEN liittyvä teoria, ja sovellettiin sitä älyverkkolaboratorion verkkoympäristössä. Tavoitteena oli asentaa RADIUS-ohjelmisto laboratorion serverille, ja sitä käytettiin GPRS-verkon palvelujen yhteydessä (GGSN tukee RADIUSTA). Radius-palvelimen avulla autentikoidaan verkon palvelujen käyttäjät.

ABSTRACT

AUTHENTICATION USING RADIUS
Samuli Huhtamäki

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: 38 pages
January 2007
UDK: 004.7, 621.39

Keywords: RADIUS, Authentication, Packet Network

RADIUS server was taken into service in the GPRS Network of Satakunta University of Applied Sciences in this thesis work. Theory of RADIUS was presented and applied in the laboratory network. The main task was to install RADIUS server software to PC and use it with GPRS services (GGSN supports RADIUS). RADIUS is used for authenticating users of network services.

SISÄLLYS

LYHENTEET

AAA	Authentication, Authorization, and Accounting
APN	Access Point Name
CHAP	Challenge-handshake authentication protocol
DNS	Domain Name System, Nimipalvelu
EIR	Equipment Identification Register
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Ragister
IETF	Internet Engineering Task Force
IMEI	Internaional Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP-osoite	Internet Protocol address
MD5	Message-Digest algorithm 5
MSC	Mobile Switching Centre, Matkapuhelinkeskus
MTU	Maximum transmission unit
NAS	Network Access Server
PAP	Password Authentication Protocol
PC	Personal Computer
PDP	Packet Data Protocol
PHP	Hypertext Preprocessor
PKI	Public key infrastructure
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial In User Service, Autentikointipalvelu
RFC	Request for Comments
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SLIP	Serial Line Internet Protocol
TCP	Transmission Control Protocol
TMSI	Temporary Mobile Subscriber Id

UDP	User Datagram Protocol
WAP	Wireless Application Protocol

1 JOHDANTO

Pakettiverkoissa on tarpeen autentikoida palvelujen käyttäjiä ulkoisen autentikointipalvelimen RADIUKSEN avulla. RADIUSTA voidaan hyödyntää myös GPRS-sovellutuksissa. RADIUKSELLA tehtävä autentikointi kuuluu olennaisesti GPRS-yhteyden muodostamiseen. Tosin se ei ole pakollinen ominaisuus ja GPRS-yhteyden muodostaminen toimii ilman sitäkin. Autentikointi, eli käyttäjän tunnistaminen, on kuitenkin tarpeellista, jos GPRS-verkko halutaan turvata ei-toivotuilta käyttäjiltä. Jos RADIUSTA ei ole, verkkoon pääse kirjautumaan ilman salasanaa. Käyttäjä-salasana -yhdistelmä estää ei-toivotun henkilön kirjautumisen verkon palveluun. Autentikointi on tarpeen esimerkiksi, jos joku yrittää päästä kirjautumaan verkkoon vartioimatta jätetyltä päätelaitteelta. Satakunnan ammattikorkeakoulun GPRS-verkkoon ei vielä ole otettu RADIUS-palvelinta käyttöön, joten tämä opinnäytetyö täytti puuttuvan osan GPRS-verkosta.

2 AAA

Kehys, jonka ympärille RADIUS (Remote Authentication Dial In User Service) on rakennettu, tunnetaan AAA-prosessina (Authentication, Authorization, and Accounting). Prosessi sisältää autentikaation, valtuutuksen ja tilastoinnin. Toisaalta AAA-mallissa ei ole mitään RADIUKSELLE ominaista, mutta tarvitaan silti yleinen tausta oikeuttamaan RADIUKSEN toiminta. RADIUS luotiin ennen kuin AAA-malli kehitettiin, mutta se oli ensimmäinen oikea AAA:han perustuva protokolla. Sisältäen AAA toiminnallisuuden se hyväksyttiin laajasti yleiseen käyttöön. [1]

Seuraavat kysymykset kuvaavat hyvin AAA:n toimintaa:

- Kuka sinä olet?
- Mitä palveluja voin antaa sinulle?
- Mitä teit palveluillani kun käytit niitä? [1]

2.1 Autentikointi

Autentikointi, eli todentaminen, on prosessi, joka varmistaa henkilön tai koneen identiteetin. Yleisin autentikointitapa on käyttää käyttäjänimeä ja salasanaa, joka varmentaa käyttäjän aitouden. Internetin liiketoiminta tarvitsee silti varmemman autentikoinnin ja salasanan välittäminen ei ole paras tapa siihen. PKI-infrastuktuuri (Public key infrastructure), osana digitaalista allekirjoitusta, tulee olemaan käytetympi. [1]

2.2 Valtuutus

Valtuutus käyttää sääntöjä, joilla se päättää mitä autentikoitu käyttäjä voi tehdä järjestelmässä. Esimerkiksi internetin palvelun tarjoaja voi päättää antaako se käyttäjälle staattisen IP-osoitteen (Internet Protocol address) vai dynaamisen. Järjestelmänvalvoja määrittelee nämä säännöt. [1]

2.3 Tilastointi

Tilastoinnilla pidetään kirjaa mitä resursseja käyttäjä on käyttänyt yhteyden aikana. Kirjaa pidetään muun muassa kulutetusta ajasta ja kuinka paljon käyttäjä on siirtänyt dataa. Tilastointi tapahtuu lokien avulla. Lokiin tallennetaan tilastoinnit ja käyttötiedot. Sitä käytetään valtuutuksen kontrollointiin, laskutukseen, kehityssuunnan analysointiin, resurssien käyttöasteeseen ja kapasiteetin suunnitteluun. [1]

Tilastoinnin datalla järjestelmänvalvoja voi analysoida onnistuneiden pyyntöjen perusteella kapasiteetin ja ennustaa tulevaisuuden järjestelmän kuormituksen. Palvelun tarjoaja voi laskuttaa käytetyistä palveluista ajan perusteella. Tietoturvan analysoija näkee torjutut autentikointipyynnöt, ja näiden avulla voi miettiä jos jokin tietty kuvio esiintyy usein ja näin mahdollisesti pystyä estämään murtautumisen. [1]

3 RADIUS

RADIUS, kuten muutkin innovatiiviset tuotteet, rakennettiin tarpeeseen. Tässä tapauksessa tarve oli saada tapa autentikointiin, valtuutukseen ja tilastointiin käyttäjille erilaisiin tietokoneresursseihin. RADIUS-protokolla on aikoinaan suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen, jossa se on nykyäänkin laajassa käytössä. RADIUS -protokollan pääasiallinen käyttökohde on operaattorin sisäisessä verkossa, jolloin verkkoa voidaan pitää kohtuullisen luotettavana ja yhden tahon ylläpitämänä. [1] [2]

RADIUS-protokolla määritellään IETF:n (Internet Engineering Task Force) julkaisemissa RFC:eissä (Request for Comments). Ne ovat joukko asiakirjoja, jotka kuvaavat lähinnä teknisten menettelyjen järjestelmiä eli protokollia. Nykyiset määrittelyt ovat RADIUKSEN osalta RFC2865:ssa ja RADIUS-tilastoinnin osalta RFC2866:ssa [3] [4]

3.1 RADIUKSEN ominaisuudet

RFC-dokumentit määrittelevät, että RADIUS:

- On yhteydetöntä UDP-protokollaa (User Datagram Protocol) käyttävä protokolla, joka ei käytä suoria yhteyksiä
- Käyttää hop-by-hop turvallisuusmallia
- On tilaton
- Tukee PAP (Password Authentication Protocol) ja CHAP (Challenge-handshake authentication protocol) autentikointia PPP:n (Point-to-Point Protocol) kautta
- Käyttää MD5-algoritmia (Message-Digest algorithm 5) salasanan suojaukseen
- Sisältää yli 50 attribuutti/arvo-paria ja sillä on valmius luoda valmistajakohtaisia pareja
- Tukee AAA-mallia [1]

Lisäksi, RADIUS tukee melkein kaikkia kaupallisia NAS-laitteita (Network Access Server), joten tulevaisuus on taattu seuraavaksi 10 vuodeksi. [1]

3.1.1 RADIUKSEN pääpiirteet

RADIUS toimii asiakas/palvelin periaatteella. NAS toimii RADIUS-palvelimen asiakkaana. Asiakas toimittaa käyttäjätiedot palvelimelle ja toimii sitten palvelimelta tulleen vastauksen mukaisesti. [5]

RADIUS-palvelimet ovat vastuussa käyttäjäkytkentäpyyntöjen vastaanotosta ja käyttäjän tunnistuksesta. Palvelin palauttaa sitten kaikki tiedot, jotka tarvitaan asiakkaan palvelujen toimittamiseen. [5]

RADIUS-palvelin voi toimia välitysasiakkaana toisille RADIUS-servereille tai toisenlaisille autentikointipalvelimille. [5]

Verkon turvallisuus hoidetaan jaetulla salaisuudella (shared secret) RADIUS-serverin ja asiakkaan välillä. Jaettua salaisuutta ei koskaan lähetetä verkon yli. Lisäksi käyttäjän salasana lähetään salattuna asiakkaan ja palvelimen väillä, jotta vältyttäisiin salakuuntelulta suojaamattomassa verkossa. [5]

RADIUS-palvelimella on joustavat autentikointimekanismit. Palvelin tukee monta tapaa tunnistaa käyttäjä. Kun annetaan käyttäjänimi ja alkuperäinen salasana, palvelin tukee PPP PAP tai CHAP, UNIX-kirjautumista, tai muita autentikointimekanismeja. [5]

RADIUS-protokolla on ”laajeneva” protokolla. Kaikki tapahtumat koostuvat muuttuvan pituisista attribuutti-pituus-arvo -parametreista (Attribute-Length-Value 3-tuples). Uusia attribuutti-arvoja voidaan lisätä ilman, että häiritään alkuperäisiä protokollan toteutuksia. [5]

3.2 RADIUKSEN rajoitteet

RADIUS-protokollalla on myös joitain rajoitteita. Turvallisuudella on joissakin toteutuksissa puutteita. Kun käytetään proxy (välitys) RADIUS-palvelimia, niin kaikki tieto näkyy joka hypyssä, olivat ne salattuja tai ei. Se ei ole riittävän turvallista salasanojen ja sertifikaattien siirtämiselle. [1]

Toinen rajoite on se, että RADIUKSELLA ei ole tukea resurssien uudelleen kutsumiselle ja vapauttamiselle sen jälkeen kun valtuutus on tehty. On mahdollista, että on olemassa monihyppy (multi-hop) proxy-RADIUS ketju, missä ensimmäinen palvelin hyväksyy pyynnön ja ottaa sen jälkeen yhteyden toiseen laitteeseen toimittaakseen palvelut. Jos jostain syystä palvelu ei olekaan saatavilla, niin RFC:ssä ei ole määräystä kieltää tai katkaista palvelua kun pääsy on estetty. Jotkut valmistajat ovat kehittäneet tuen jälkihylkäämiselle, se sisältää käyttäjän poistamisen ennemmin tietyn ajan perusteella kuin vain pääsyn epäämisen seuraavalla kirjautumisyrityksellä, mutta virallisessa määrittelyssä sitä ei ole. [1]

Kolmanneksi RADIUS on tilaton. Se ei pidä kirjaa kokoonpanoasetuksista, tapahtumatiedoista, tai mistään muusta seuraavan session tiedoista. Kun ohjelma on tilaton, se ei pysty pitämään tietoa edellisestä sessiosta seuraavaan sessioon, kuten siitä mitä käyttäjä teki tai tilanteista, jotka ilmenivät prosessin aikana. [1]

Lopuksi RADIUKSEN käyttäjät ovat huomanneet, että RADIUKSELLA on skaalautuvuusongelmia. Asia ilmenee RFC 2865:ssä heti ensimmäisellä sivulla: RADIUS voi kärsiä huonontuneesta suorituskyvystä ja tietojen menetyksestä kun sitä käytetään isoissa järjestelmissä, koska sitä ei ole varustettu ruuhkanhallinnalla. [1]

3.3 Toiminta

Seuraavaksi on selostettu RADIUKSEN toiminta eli RADIUS-pakettejen tarkoitus. Myöhemmässä vaiheessa paneudutaan pakettien muotoon ja rakenteeseen.

Kun asiakaskone asetetaan käyttämään RADIUSTA, mikä tahansa asiakaskoneen käyttäjä esittää autentikointitiedon asiakaskoneelle. Tämä voi tapahtua muokattavalla sisäänkirjautumiskehotteella, johon annetaan käyttäjänimi ja salasana. Vaihtoehtoisesti voidaan käyttää esim. PPP-protokollaa, jossa autentikointipaketit sisältävät salasanan ja käyttäjänimen. [5]

Kun asiakaskone on saanut tiedot, se voi valita RADIUKSEN autentikoimaan. Tehdäkseen sen asiakaskone luo Access-Request -pyynnön eli pääsypyynnön, joka sisältää attribuutit kuten käyttäjän nimen, käyttäjän salasanan, asiakaskoneen tunnisteen ja portti tunnisteen, johon käyttäjä yrittää päästä. Salasana suojataan MD5-algoritmilla. [5]

Access-Request toimitetaan RADIUS-palvelimelle verkon kautta. Jos ei saada vastausta tietyn ajan kuluessa, pyyntö lähetetään uudelleen. Asiakaskone voi myös välittää pyynnöt toiselle palvelimelle tai palvelimille, jos pääpalvelin ei ole tavoitettavissa. Toissijaista palvelinta voidaan käyttää joko tietyn yritysten epäonnistumisien määrän jälkeen tai kiertovuorottelu periaatteella. [5]

Kun RADIUS-palvelin saa pyynnön, se vahvistaa pyynnön lähettäneen asiakaskoneen. Jos asiakaskoneen lähettämässä viestissä ei ole RADIUS-serverin kanssa samaa jaettua salaisuutta, niin viesti pitää hylätä ilman mitään ilmoitusta. Jos taas asiakaskone on validi, RADIUS-palvelin katsoo käyttäjien tietokannasta kenen nimi täsmää pyyntöön. Käyttäjätietomerkintä tietokannassa sisältää listan vaatimuksista, jotka pitää päteä että voidaan antaa käyttöoikeus käyttäjälle. Tämä sisältää aina salasanan vahvistamisen, mutta siihen voi myös määrittää asiakkaat tai portit joihin käyttäjällä on oikeus. [5]

RADIUS-palvelin voi tehdä pyyntöjä toisille palvelimille tyydyttääkseen pyynnön, jossa se on itse asiakkaana. [5]

Jos Proxy-State attribuutteja on Access-Request-paketissa, niin ne pitää kopioida muuttumattomina ja järjestyksessä vastauspakettiin. Muut attribuutit voidaan sijoittaa ennen, jälkeen tai jopa keskelle Proxy-State attribuuttiin. [5]

Jos mikään ehto ei toteudu, RADIUS-palvelin lähettää Access-Reject eli pääsyevätty -paketin, joka osoittaa että pyyntö on epäkelpo. Palvelin voi myös lisätä viestin Access-

Reject -pakettiin, jonka asiakaskone näyttää käyttäjälle. Access-Reject -paketissa ei sallita muita Attribuutteja (paitsi Proxy-State -paketteja). [5]

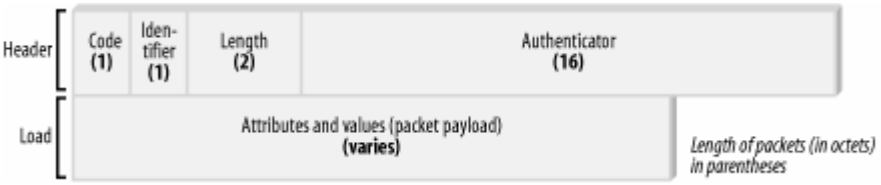
Jos kaikki ehdot toteutuvat, palvelin lähettää Access-Challenge -vastauksen, johon käyttäjän pitää vastata. Se voi sisältää viestin, jonka asiakaskone näyttää käyttäjälle, ja siinä voi myös olla State-attribuutti eli tila-attribuutti. [5]

Jos asiakaskone ottaa vastaan Access-Challenge -paketin, ja mikäli se tukee challenge/response -ominaisuutta, se voi näyttää viestin käyttäjälle. Seuraavaksi näytetään kehote, johon vastataan. Sitten asiakaskone lähettää uudelleen alkuperäisen Access-Request -paketin uudella pyyntötunnuksella, jossa User-Password –attribuuti korvataan vastauskella (salattuna). Myös State-attribuuti sisälletään pakettiin, jos sellaista on. Pyynnössä voi olla vain 0 tai 1 ilmentymää State-attribuutista. Palvelin voi sitten vastata tähän uuteen Access-Request -pakettiin joko Access-Accept, Access-Reject tai uudella Access-Chalenge -paketilla. [5]

Jos kaikki ehdot toteutuvat, asetusarvojen lista käyttäjälle pannaan (pääsy hyväksytty) Access-Accept -vastaukseen. Nämä arvot sisältävät palvelun tyypin (esim. SLIP (Serial Line Internet Protocol), PPP, Login User) ja kaikki muut tarpeelliset arvot palvelulle. SLIP:lle ja PPP:lle arvot sisältävät esim. IP-osoiteen, aliverkonmaskin, MTU:n (Maximum transmission unit), halutun pakkauksen ja halutun pakettisuodatus tunnisteet. Tekstipohjaisille käyttäjille tämä voi sisältää arvoja kuten halutun protokollan ja isäntäkoneen. [5]

3.4 Pakettien rakenne

RADIUS-protokolla käyttää UDP-paketteja sanomien välittämiseen asiakkaan ja palvelimen välillä, kuten sanottu. Protokolla kommunikoi porttinumero 1812:lla, joka eri kuin alkuperäisessä RADIUS RFC -dokumentissa. Ensimmäisessä revisiossa käytettiin porttia 1645, mutta myöhemmin todettiin, että se on ristiriidassa ”Datametrics”-palvelun kanssa. [1]



Kuva 1. Kuvaus RADIUS-paketin rakenteesta [1]

3.4.1 Koodi (Code)

Koodialue on yhden oktetin pituinen ja se erottelee RADIUS-viestien tyypit. Paketit, joilla on väärä koodi, tuhotaan ilman ilmoitusta. Oikeat koodit ovat:

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server (kehityksen alla)
- 13 Status-Client (kehityksen alla)
- 255 Varattu [1]

3.4.2 Tunniste (Identifier)

Tunnistealue on yhden oktetin mittainen ja sitä käytetään säikeistykseen, tai automaattisten alkupyyntöjen ja jälkivastausten linkittämiseen. RADIUS-palvelimet voivat pysäyttää kaksoisviestit tutkimalla tekijöitä kuten lähde IP-osoitetta, lähde UDP porttia, viestin kulunutta aikaa ja tunnistekenttää. [1]

3.4.3 Pituus (Length)

Pituusalue on kahden oktetin mittainen ja sitä käyttetään RADIUS-viestin pituuden määrittämiseen. Arvo tässä kentässä on laskettu analysoimalla koodi-, tunniste-, pituus-, autentikointi- ja attribuuttikenttää, sekä löytämällä niiden summan. Pituuskenttä on tar-

kistettu kun RADIUS-palvelin ottaa vastaan paketin ja varmistaa tiedon eheyden. Pituuden arvot vaihtelevat 20:n ja 4096:n välillä. [1]

RFC:n mukaan RADIUS tarvitsee tiettyjä käyttäytymisiä mitä tulee väärän mittaisiin datan pituuteen. Jos RADIUS-palvelin ottaa vastaan lähetyksen, jossa viestin pituus on pidempi kuin pituuskenttä, se hylkää kaiken datan, joka on pituuskentän määrittämän kohdan jälkeen. Jos puolestaan palvelin ottaa vastaan lyhyemmän viestin mitä kenttä ilmoittaa, se hylkää viestin. [1]

3.4.4 Autentikaattori (Authenticator)

Autentikaattorialue, usein 16 oktettia pitkä, on kenttä, jossa viestin eheys tarkistetaan ja varmistetaan. Tässä kentässä tärkein oktetti lähetetään ennen muita ja arvoa käytetään autentikoimaan vastauksia RADIUS-serveriltä. Tätä arvoa käytetään myös salasanojen piilottamiseen. [1]

On olemassa kaksi tyyppia autentikointiarvoa: pyyntö- ja vastausarvot. Pyyntöautentikaattoreja käytetään ”Autentication-Request” ja ”Accounting-Request”-paketeissa. Pyyntöarvossa kenttä on 16 oktettia pitkä ja generoidaan täysin sattumavaraisesti, jotta vältytään hyökkäyksiltä. Kun RADIUS ei tee mitään suojatakseen kommunikointia salakuuntelulta eli pakettien sieppaukselta, satunnaiset arvot hyvän salasanan kanssa tekevät kuuntelusta vaikeaa. [1]

Vastausautentikaattoria käytetään Access-Accept, Access-Reject ja Access-Challenge -paketeissa. Arvo lasketaan yksisuuntaisella MD5-algoritmillä, mikä generoidaan koodi-, tunniste-, pituus- ja pyyntöautentikaattorialueista, jotka ovat paketin otsakkeessa. Näitä seuraa paketin hyötykuorma ja jaettu salaisuus. [1]

3.5 Pakettien tyypit

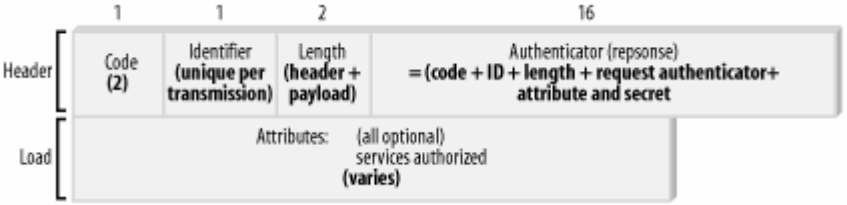
RADIUS-paketteja on neljää tyyppiä, joilla on merkitystä AAA-transaktiolle:

- Access-Request

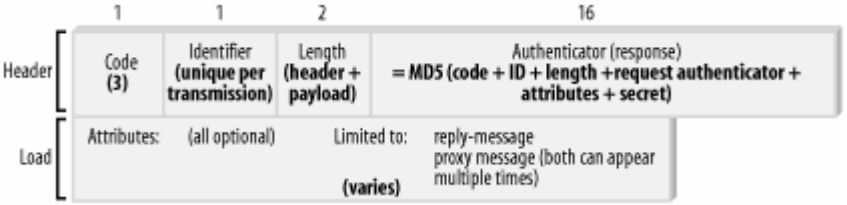
- Access-Accept
- Access-Reject
- Access-Challenge [1]

Seuraavaksi on esitetty pakettien rakennekuvat.

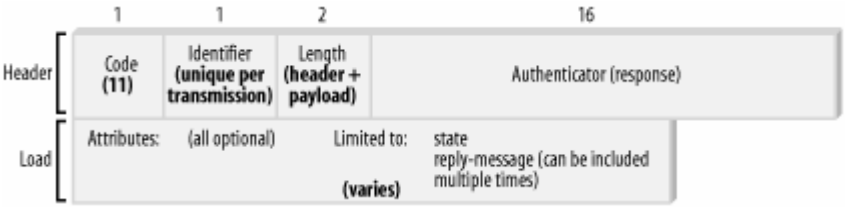
Kuva 2. Access-Request -paketti [1]



Kuva 3. Access-Accept -paketti [1]



Kuva 4. Access-Reject -paketti [1]



Kuva 5. Access-Challenge -paketti [1]

3.6 UDP:n Käyttö

RADIUKSESSA käytetään UDP:tä TCP:n (Transmission Control Protocol) sijasta. Tämä on valittu pääasiassa teknisistä syistä. RADIUS on tapahtumapohjainen protokolla, jolla on seuraavia ominaisuuksia:

1. Jos pyyntö epäonnistuu pääautentikointipalvelimelle, niin pitää tehdä kysely sekundaaripalvelimelle. Tämän vaatimuksen täyttämiseen kopio pyynnöstä täytyy pitää kuljetustason yläpuolella, mikä puolestaan sallii vaihtoehtoisen lähetyksen. Tämä tarkoittaa, että uudelleenlähettämisajastimia tarvitaan silti. [5]

2. Ajastinvaatimukset tälle protokollalle ovat huomattavan erilaiset kuin TCP-protokollalla. RADIUKSEN ei tarvitse huolehtia kadonneen tiedon häviämisestä. Jos käyttäjä suostuu odottamaan autentikointia muutaman sekunnin, niin TCP-protokollan uudelleenlähettämiselle ei ole tarvetta, eikä myöskään sen vahvistussanomille. Jos taas käyttäjä ei suostu odottaa minuutteja autentikointia, niin TCP-protokollan tiedon varmistettua perille pääsyä parin minuutin kuluttua ei tarvita. Vaihtoehtoisen palvelimen nopeampi käyttö antaa käyttäjälle pääsyn ennen luovuttamista. [5]

3. RADIUKSEN tilaton luonne yksinkertaistaa UDP-protokollan käytön. Palvelimet ja asiakkaat tulevat ja menevät, niitä sammutetaan ja käynnistetään uudelleen. Tämä ei kuitenkaan aiheuta välttämättä ongelmia TCP-protokollallekaan, koodia voidaan kirjoittaa siten että se pystyy kestämään nämä tapahtumat. UDP-protokolla puolestaan eliminoi koko asian. Joka asiakas ja palvelin voi avata UDP-yhteyden vain kerran ja jättää sen auki, vaikka verkossa olisi vikatilanteita. [5]

4. UDP-protokolla yksinkertaistaa palvelintoteutuksen. Aluksi RADIUS pystyi prosessoimaan yhden pyynnön kerrallaan, eli palvelin oli yksisäikeinen. Tämän puolestaan todettiin olevan hallitsemattomissa ympäristöissä, joissa taustaturvallisuusmekanismi kesti todellisen ajan (sekunnin tai enemmän). Palvelimen pyyntöjono täyttyi ympäristöissä, joissa oli satoja käyttäjiä, ja käyttäjät eivät enää ha-

lunneet odottaa autentikointia. Järkeenkäypä ratkaisu oli tehdä palvelin monisäikeiseksi. UDP-protokollalla tämä oli yksinkertaista tehdä. Jokaiselle pyynnölle perustettiin oma prosessi, jotka voivat vastata yksinkertaisella UDP-paketilla suoraan asiakas-NAS:lle asiakkaan alkuperäisen tiedon. [5]

Kuten sanottu UDP tarvitsee yhden asian, joka on rakennettu TCP:hen: UDP:n kanssa pitää keinotekoisesti hallita uudelleenlähettämisajastimia samalle palvelimelle. Toisaalta tämä ei tarvitse yhtä tarkkaa huomiota kuin TCP:ssä tehdyt ajastimet. Tämä on kuitenkin pieni hinta UDP:n tuomista eduista. [5]

3.7 Jaetut salaisuudet

Tietoturvan parantamiseksi RADIUS-protokolla käyttää jaettuja salaisuuksia (shared secrets). Molemmat osapuolet, asiakas ja palvelin, tietävät jaetut salaisuudet. Jaetut salaisuudet ovat samat sekä asiakkaalla että palvelimella (huomaa ”jaetut”). Jaettuja salaisuuksia käytetään kaikissa toiminnoissa, jotka tarvitsevat datan piilottamista ja salaamista. Ainoa tekninen rajoite on, että jaetut salaisuudet pitää olla isompia kuin 0 pituudeltaan. RFC kuitenkin suosittelee, että salaisuus pitää olla vähintään 16 oktettia. Niin pitkä salaisuus on käytännössä mahdotonta murtaa ilman raakaa voimaa. Sama käytäntö, joka takaa hyvän salasanan pätee myös RADIUKSEN jaetuille salaisuuksille. Jokaisella asiakas-palvelin -parilla on uniikki jaettu salaisuus. [1]

3.8 RADIUS-tilastointi

Autentikoinnin (joka varmistaa käyttäjän identiteetin) ja valtuutuksen (joka antaa tiettyjä palveluja käyttäjälle) lisäksi tarvitaan tilastointia. Tilastoinnilla kerätään hyödyllistä tietoa käyttäjästä ja käyttäjän toimista. [1]

Tiedot tulevat vielä enemmän hyödyllisiksi kun niitä käytetään käyttäjäryhmien analysoimiseen. Hyödyllisiä tietoja ovat muun muassa: siirretyn datan määrä, keskimääräinen ajan käyttö jne. [1]

RADIUS tukee täysin tilastointiprotokollaa, joka täyttää AAA-mallin vaatimukset. [1]

Tilastoinnin avainseikat

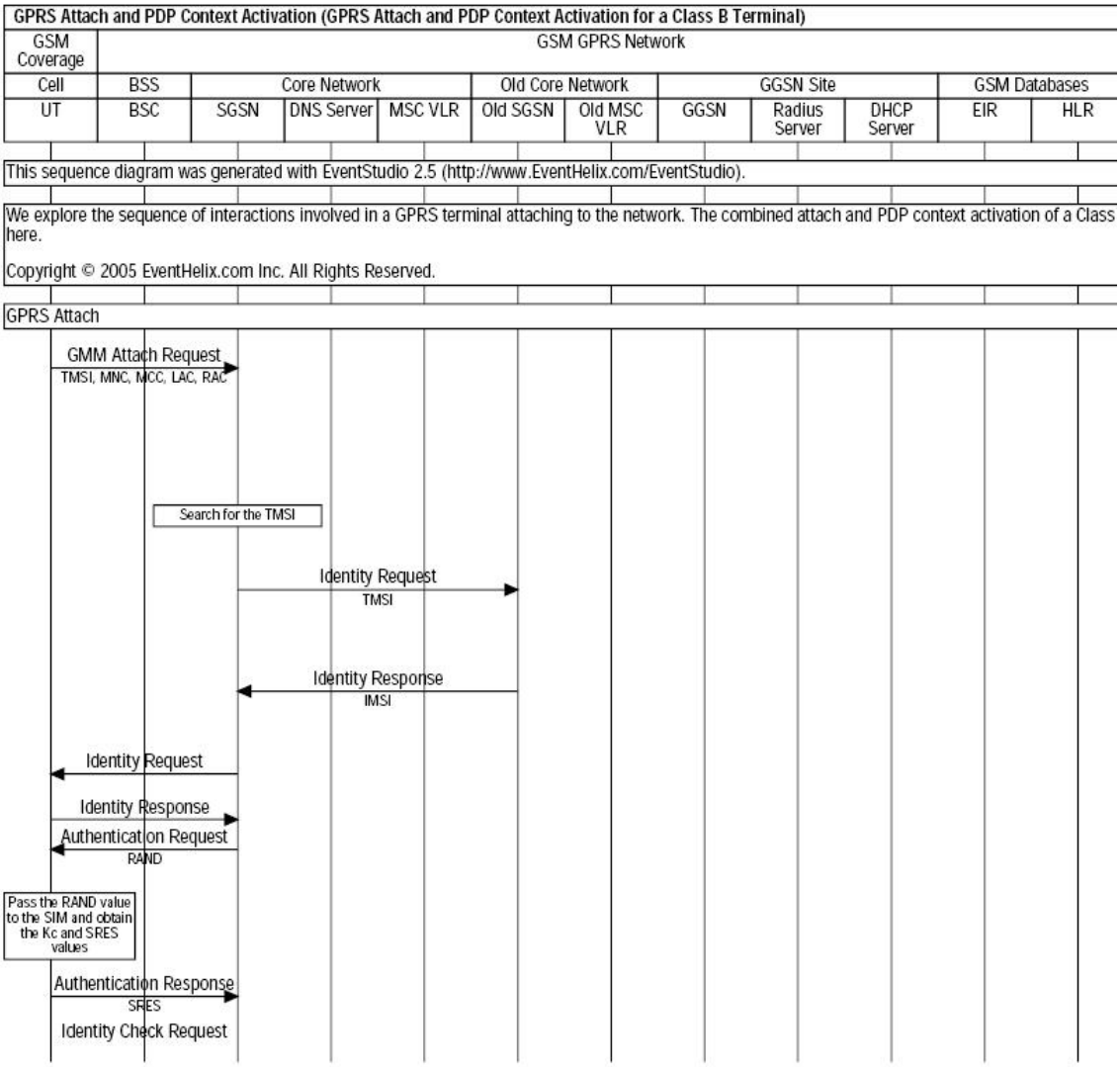
RADIUKSEN tilastointi toimii asiakas/palvelin periaatteella, kuten itse protokollakin. RADIUS-tilastointikone on palvelin RADIUS asiakaslaitteistolle, joka toimii asiakkaana. Asiakas lähettää käyttötiedot RADIUS-palvelimelle prosessointia varten. Palvelin kuittaa onnistuneet tiedon vastaanoton. On myös mahdollista, että Palvelin toimii tilastoinnin välityspalvelimena samalla tapaa kuin autentikoinnissa ja valtuutuksessa. [1]

Kommunikaatio laitteiden välillä on turvattu. Kaikki tieto, joka kulkee palvelimen ja asiakkaan välillä turvataan jaetulla salaisuudella. Jaettua salaisuutta ei koskaan kuljeteta verkon yli. [1]

RADIUS-tilastointi on laajennettavissa. Tilastoinnin attribuuttien formaatti on melkein samanlainen kuin autentikoinin ja valtuutuksen. Useimmat tarjotut palvelut voidaan määrittää käyttämällä attribuutti-arvo pareja (attribute-value pairs). Näitä pareja voidaan lisätä ja muokata olemassa olevaan toteutukseen ilman, että häiritään jo käytössä olevia toimintoja.[1]

4 GPRS liityntä ja PDP-kontekstin avaus

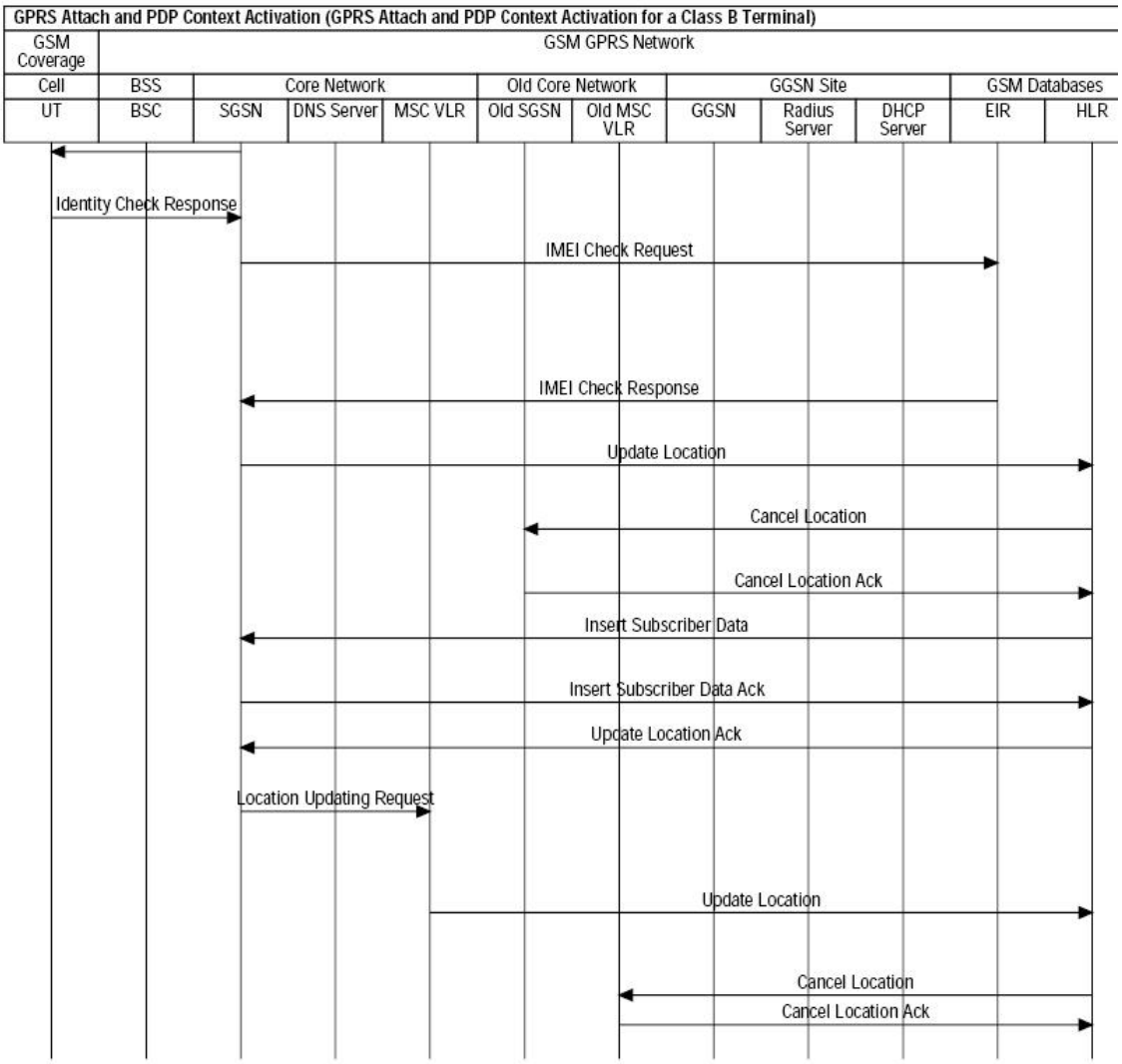
Koska GPRS-liityntä (General Packet Radio Service) (GPRS Attach) ja PDP-kontekstin avaus (Packet Data Protocol) (PDP Context Activation) liittyvät olennaisesti RADIUK-SEEN ts. RADIUS-autentikointi on osa GPRS-yhteyden avaamista, on hyvä katsastaa miten yhteys luodaan. Ilman RADIUS-autentikointiakin yhteys muodostuu. GGSN:n (Gateway GPRS Support Node) APN-konfiguroinnissa (Access Point Name) tehdään määrittely käytetäänkö autentikointia (ja myös tilastointia.)



Kuva 6. GPRS liityntä ja PDP-kontekstin avaus. 1. Osa [6]

Kuvan selitykset ylhäältä alas numerojärjestyksessä kohtakohdalta (GPRS Attach):

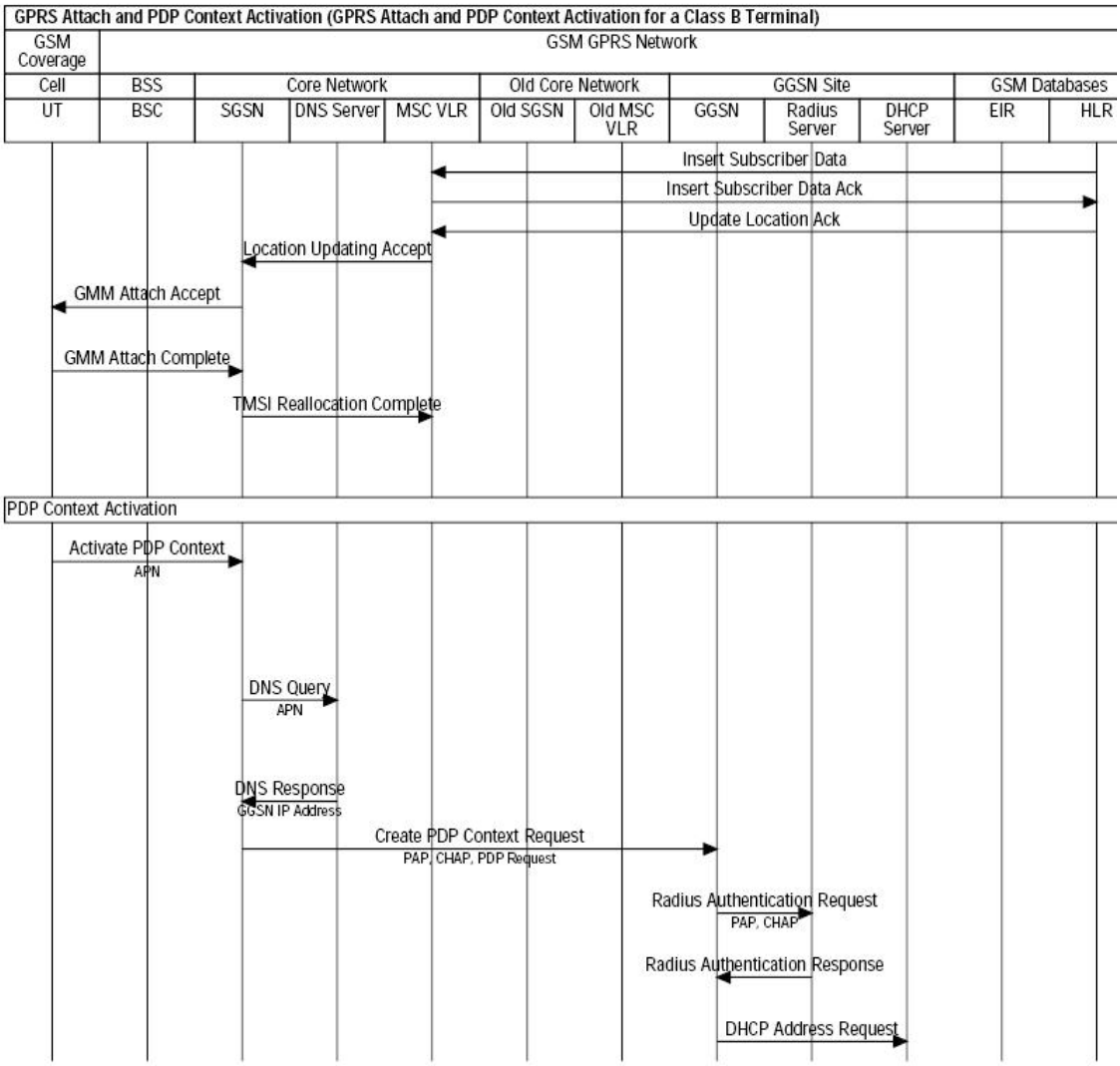
1. Päätelaite aloittaa liityntäprosessin kun laite kytketään päälle. Sanoma sisältää aikaisemmin käytetyn TMSI (Temporary Mobile Subscriber Id). Mobiilin verkkotunnus, sijaintialue ja reititysalue ovat myös sanomassa.
2. SGSN (Serving GPRS Support Node) etsii tietokannastaan TMSI:n.
3. Jos tietoa ei löydy TMSI:lle, niin SGSN käyttää vanhaa sijaintialuetietoa tunnistaakseen vanhan SGSN, jossa tätä päätelaitetta palveltiin.
4. Vanha SGSN vastaa GPRS päätelaitteen IMSI:llä (International Mobile Subscriber Identity) SGSN:lle.
5. SGSN pyytää päätelaitetta tunnustautumaan.
6. Päätelaite vastaa takaisin.
7. SGSN autentikoi GPRS-päätelaitteen lähettämällä RAND-arvon (Random value).
8. SIM (Subscriber Identity Module) käyttää salaisia GSM-algoritmejä (Global System for Mobile Communications)RAND-arvoon ja salaiseenavaimeen (Ki) hankkiakseen istuntoavaimen (Kc) ja SRES:n.
9. Laskettu SRES-arvo lähetetään SGSN:lle.



Kuva 7. GPRS liityntä ja PDP-kontekstin avaus. 2. Osa [6]

10. SGSN pyytää sitten GPRS-päätelaitteen identiteettiä.
11. GPRS päätelaite vastaa identiteetin kanssa.
12. Tarkistetaan, että päätelaite ei ole varastettu. IMEI (Internaional Mobile Equipment Identity) lähetetään EIR:lle (Equipment Identification Register).
13. EIR hyväksyy tilaajan ja vastaa tilanteesta taikaisin SGSN:lle.
14. SGSN ilmoittaa HLR:lle (Home Location Ragister) uudesta GPRS-laitteen sijainnista.
15. HLR ilmoittaa vanhalle SGSN:lle siitä, että GPRS-laite on siirtynyt uudelle alueelle.
16. Vanha SGSN kuittaa.
17. HLR päivittää kaikki tilaajatiedot uuteen SGSN:ään.

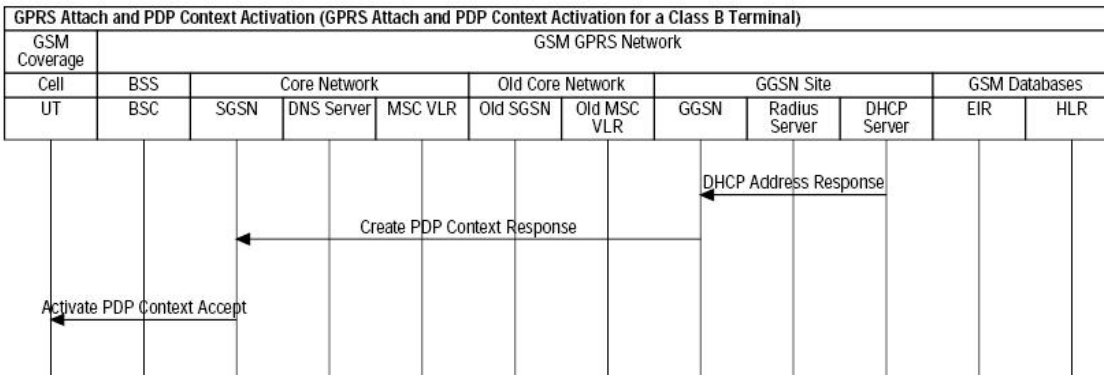
18. SGSN kuittaa takaisin HLR:lle.
19. HLR vastaa SGSN:n ”Päivitä sijainti” -sanomaan.
20. Päätelaite aloitti yhdistetyn liittymisen, joten SGSN päivittää myös sijaintitiedot MSC-VLR välillä, joka käsittelee äänipuhelut.
21. MSC (Mobile Switching Centre) myös aloittaa päivityksen HLR:ssä. Toimintojen sarja on identtinen SGSN:n HLR päivityksen kanssa.
22. MSC ilmoittaa SGSN:lle sen, että se lopetti sijainninpäivityksen.
23. SGSN vastaa Päätelaitteen alkuperäiseen GPRS yhdistettyyn liityntä pyyntöön.
24. Attach Complete viestittää liityntäprosessin valmistumisen. Tämä välitetään MSC-VLR:lle: ”TMSI uudelleenjakaminen valmis”.



Kuva 8. GPRS liityntä ja PDP-kontekstin avaus. 3. Osa [6]

PDP-kontekstin avaus:

1. GPRS-laite käynnistää nyt PDP-kontekstinaktivointiprosessin. Tämän avulla Laite saa IP-osoitteen. Yhteydentarjoajan määrittelemä APN välitetään parametrinä.
2. SGSN aloittaa DNS-kyselyn (Domain Name System) etsiäkseen GGSN:ää vastaavan APN:n, joka on myös määritetty päätelaitteessa.
3. DNS antaa GGSN:n IP-osoitteen.
4. SGSN reitittää GGSN:ää vastaavan PDP-kontekstin avauspyynnön.
5. GGSN autentisoi GPRS-tilaajan RADIUS-serverillä.
6. RADIUS-serveri autentikoi tilaajan onnistuneesti ja vastaa takaisin GGSN:lle.
7. GGSN pyytää nyt DHCP-serveriltä dynaamisen IP-osoitteen GPRS-tilaajalle (SAMK:in verkossa GGSN antaa IP-osoitteen kts. kuva 15 kohta IP Address Generation Method).



Kuva 9. GPRS liityntä ja PDP-kontekstin avaus. 4. Osa [6]

8. DNS-serveri antaa IP-osoitteen.
9. GGSN vastaa takaisin SGSN:lle, mikä merkitsee sitä, että PDP-kontekstin avaus -prosessi on valmis.
10. SGSN vastaa takaisin GPRS-laitteelle. Tämä signaloi sitä, että PDP-kontekstin avaus onnistui.

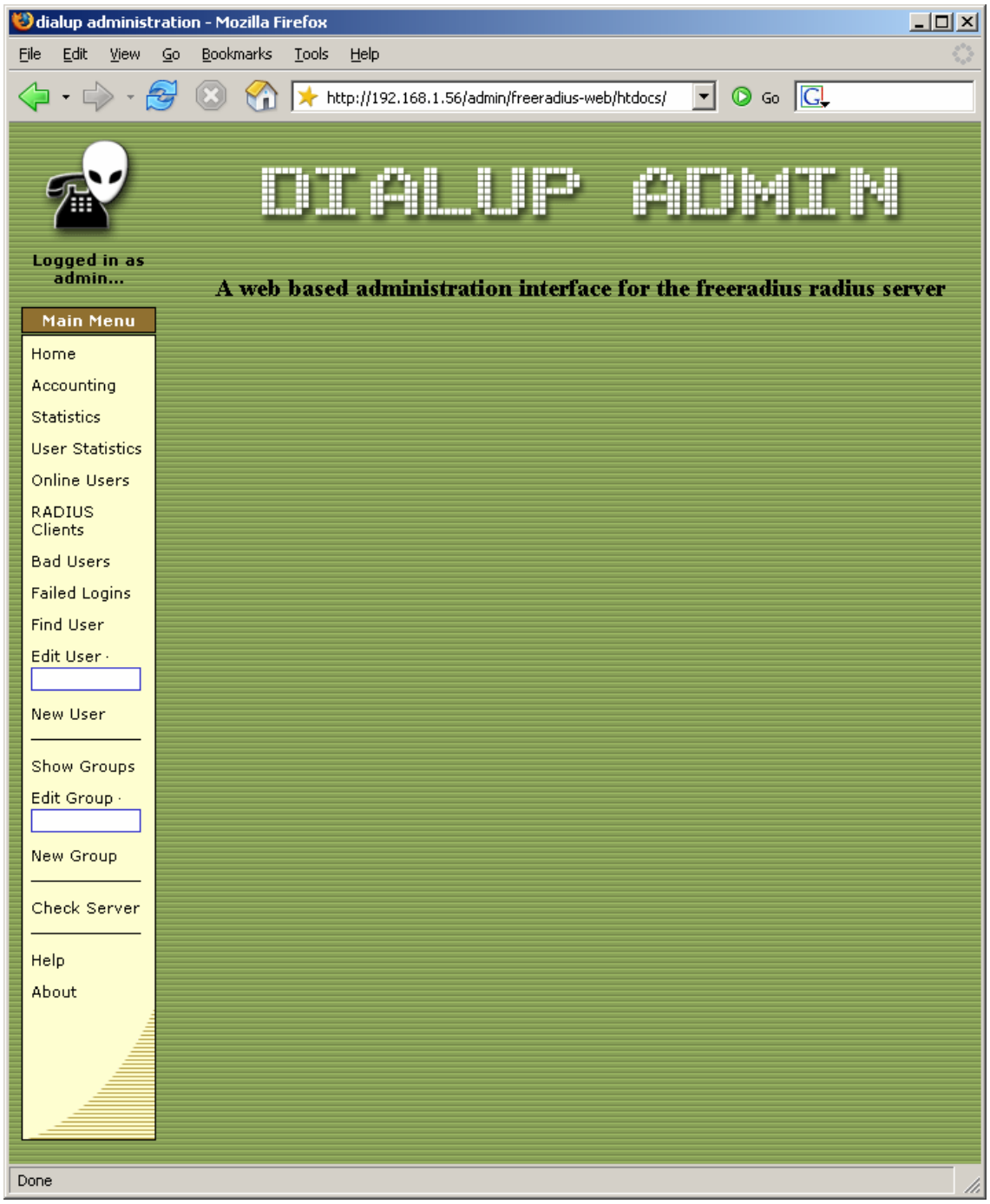
5 RADIUKSEN KÄYTTÖÖNOTTO SAMK:N GPRS-VERKOSSA

RADIUS otettiin käyttöön jo muilta osin valmiiseen SAMK:in GPRS-verkkoon. RADIUS palvelinkoneena käytettiin uudehkoa PC:tä (Personal Computer), jossa on AMD Athlon 64 3400+ -prosessori ja 1,5 Gt muistia, Windows Server 2003 Standard Edition -käyttöjärjestelmällä varustettuna. Palvelimeen asennettiin ilmainen VMware Server -ohjelmisto, versiota 1.0.1. Tätä ohjelmistoa käytetään virtuaalikoneiden luontiin ja käyttöön. Ohjelmistoon asennettiin virtuaalikoneeksi Mandriva Linux 2006. Mandrivan järjestelmäversio oli: 2.6.12-12mdksmp

RADIUS ohjelmistoksi valittiin FreeRADIUS. Se on myös ilmainen, avoimeen lähdekoodiin perustuva, ja hyvin dokumentoitu ohjelmisto. Lisäksi siinä on Web-käyttöliittymä Dialup Admin, jonka takia palvelimen konfiguraatio on nopeampaa ja helpompaa, kuin tekstitiedoston konfigurointi. FreeRADIUKSEN saa kaikkiin Linuxeihin kääntämällä se lähdekoodista. Mandrivaan puolestaan sen saa paketinhallinnan kautta asennettuna valmiina pakettina.

Virtuaalikoneeseen asennettiin myös Ethereal -protokolla-analysaattori, jotta pystyttiin testaamaan RADIUS protokollan toiminta. Liitteessä 1 on Etherealin luomaa analyysia. Ethereal pitää käynnistää komennolla sudo ethereal tai su ensin ja ethereal. Käyttäjänimi Mandriva-virtuaalikoneeseen on samuli ja salasana on inlabra%. Super userin (tai substitute user) salasana on inlabra%. Dialup Adminin käyttäjänimi on admin ja salasana inlabra% ja samat ovat myös GGSN:ssä. Windows koneen käyttäjänimi on administrator ja salasana inlabra%.

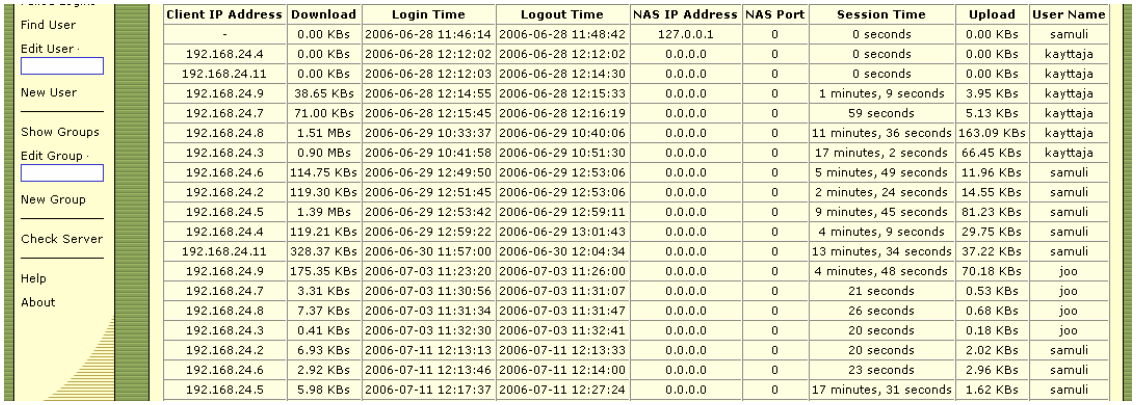
5.1 Dialup Admin



Kuva 10. Dialup Admin

Dialup Admin on Web-käyttöliittymä FreeRADIUS-palvelinohjelmalle. Dialup Adminia varten asennettiin myös Apache Web-palvelin ja siihen PHP-tuki (Hypertext Preprocessor), sekä MySQL-serveri. Dialup Admin tarvitsee MySQL:n, koska se käyttää

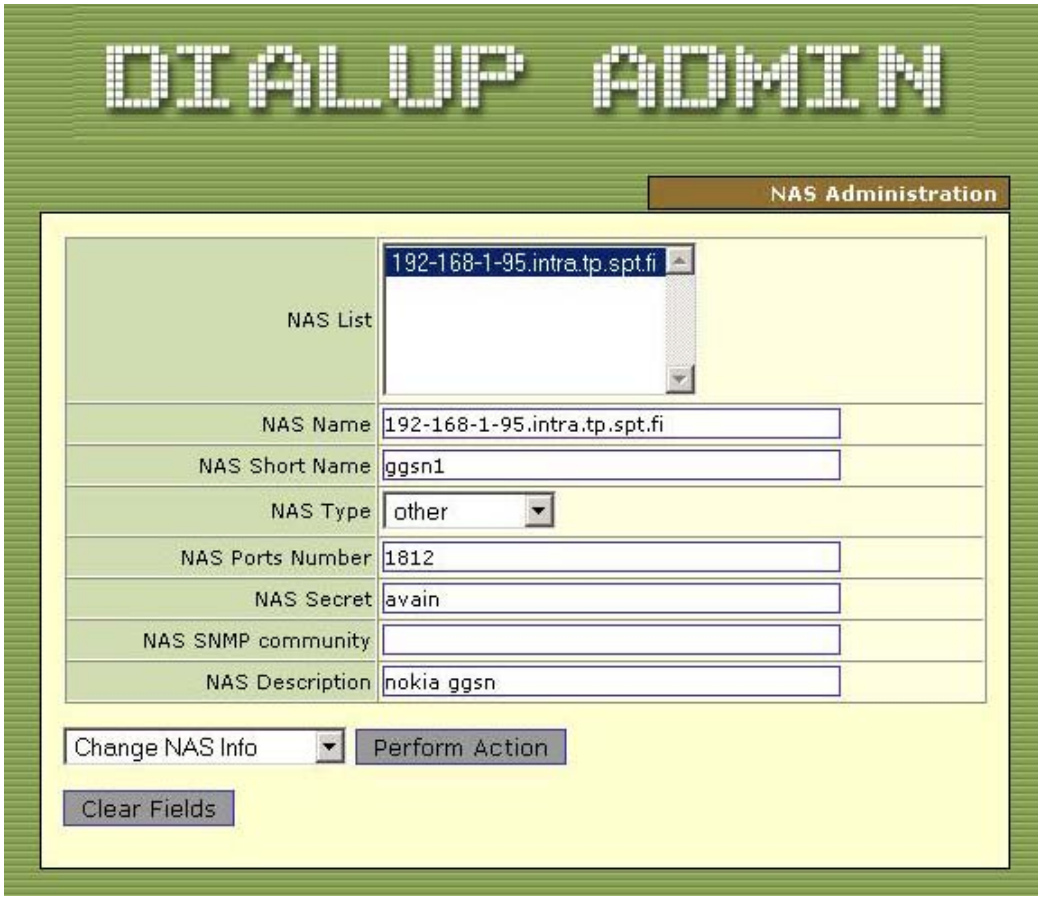
tietokantaa tallentaakseen konfiguraatiot. Myös PHP-tuki tarvitaan, koska Dialup Amin on kirjoitettu PHP:llä. Nämä asennettiin Mandriva-virtuaalikoneeseen.



Client IP Address	Download	Login Time	Logout Time	NAS IP Address	NAS Port	Session Time	Upload	User Name
-	0.00 KBs	2006-06-28 11:46:14	2006-06-28 11:48:42	127.0.0.1	0	0 seconds	0.00 KBs	samuli
192.168.24.4	0.00 KBs	2006-06-28 12:12:02	2006-06-28 12:12:02	0.0.0.0	0	0 seconds	0.00 KBs	kayttaja
192.168.24.11	0.00 KBs	2006-06-28 12:12:03	2006-06-28 12:14:30	0.0.0.0	0	0 seconds	0.00 KBs	kayttaja
192.168.24.9	38.65 KBs	2006-06-28 12:14:55	2006-06-28 12:15:33	0.0.0.0	0	1 minutes, 9 seconds	3.95 KBs	kayttaja
192.168.24.7	71.00 KBs	2006-06-28 12:15:45	2006-06-28 12:16:19	0.0.0.0	0	59 seconds	5.13 KBs	kayttaja
192.168.24.8	1.51 MBs	2006-06-29 10:33:37	2006-06-29 10:40:06	0.0.0.0	0	11 minutes, 36 seconds	163.09 KBs	kayttaja
192.168.24.3	0.90 MBs	2006-06-29 10:41:58	2006-06-29 10:51:30	0.0.0.0	0	17 minutes, 2 seconds	66.45 KBs	kayttaja
192.168.24.6	114.75 KBs	2006-06-29 12:49:50	2006-06-29 12:53:06	0.0.0.0	0	5 minutes, 49 seconds	11.96 KBs	samuli
192.168.24.2	119.30 KBs	2006-06-29 12:51:45	2006-06-29 12:53:06	0.0.0.0	0	2 minutes, 24 seconds	14.55 KBs	samuli
192.168.24.5	1.39 MBs	2006-06-29 12:53:42	2006-06-29 12:59:11	0.0.0.0	0	9 minutes, 45 seconds	81.23 KBs	samuli
192.168.24.4	119.21 KBs	2006-06-29 12:59:22	2006-06-29 13:01:43	0.0.0.0	0	4 minutes, 9 seconds	29.75 KBs	samuli
192.168.24.11	328.37 KBs	2006-06-30 11:57:00	2006-06-30 12:04:34	0.0.0.0	0	13 minutes, 34 seconds	37.22 KBs	samuli
192.168.24.9	175.35 KBs	2006-07-03 11:23:20	2006-07-03 11:26:00	0.0.0.0	0	4 minutes, 48 seconds	70.18 KBs	joo
192.168.24.7	3.31 KBs	2006-07-03 11:30:56	2006-07-03 11:31:07	0.0.0.0	0	21 seconds	0.53 KBs	joo
192.168.24.8	7.37 KBs	2006-07-03 11:31:34	2006-07-03 11:31:47	0.0.0.0	0	26 seconds	0.68 KBs	joo
192.168.24.3	0.41 KBs	2006-07-03 11:32:30	2006-07-03 11:32:41	0.0.0.0	0	20 seconds	0.18 KBs	joo
192.168.24.2	6.93 KBs	2006-07-11 12:13:13	2006-07-11 12:13:33	0.0.0.0	0	20 seconds	2.02 KBs	samuli
192.168.24.6	2.92 KBs	2006-07-11 12:13:46	2006-07-11 12:14:00	0.0.0.0	0	23 seconds	2.96 KBs	samuli
192.168.24.5	5.98 KBs	2006-07-11 12:17:37	2006-07-11 12:27:24	0.0.0.0	0	17 minutes, 31 seconds	1.62 KBs	samuli

Kuva 11. Dialup Adminin Accounting -sivu

Dialup Adminin avulla voidaan seurata käyttäjien tilastointitietoja Accounting -sivulla. Sieltä näkee muun muassa asiakkaan, tässä tapauksessa mobiililaitteen, IP-osoitteen, latauksien kilotavumäärän jne.

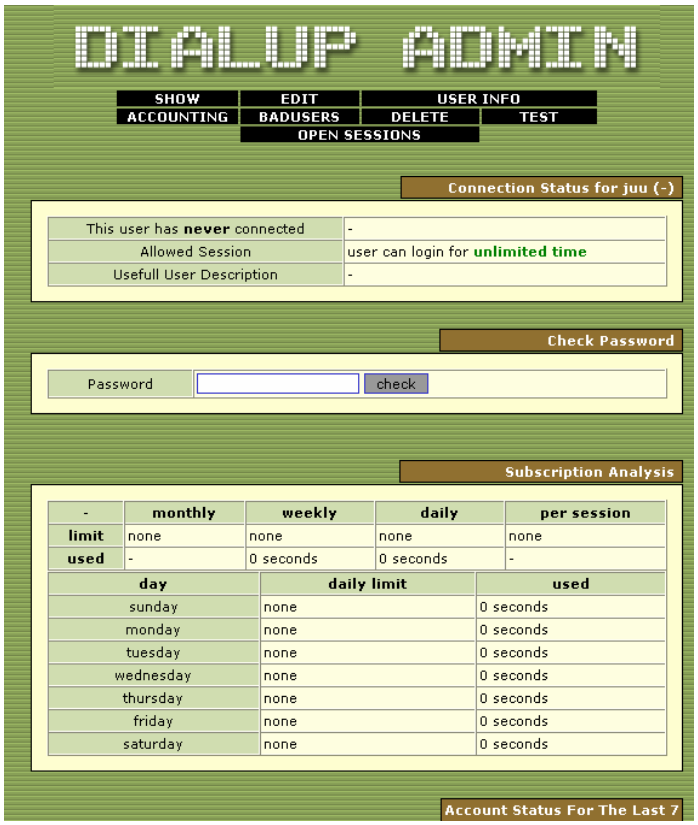


Kuva 12. NAS-määrittely Dialup Adminin RADIUS Clients -sivu

RADIUS Clients -kohdasta aukeaa NAS Admnistration -sivu. Tätä sivua käytetään NAS:ien määrittelyyn. NAS Name pitää olla DNS-muotoisena, pelkkä IP-osoite ei kelpaa. NAS Secret, eli jaettu salaisuus, pitää olla samaksi määritetty kuin GGSN:n APN-konfiguraatiossa.

Kuva 13. New User -sivu

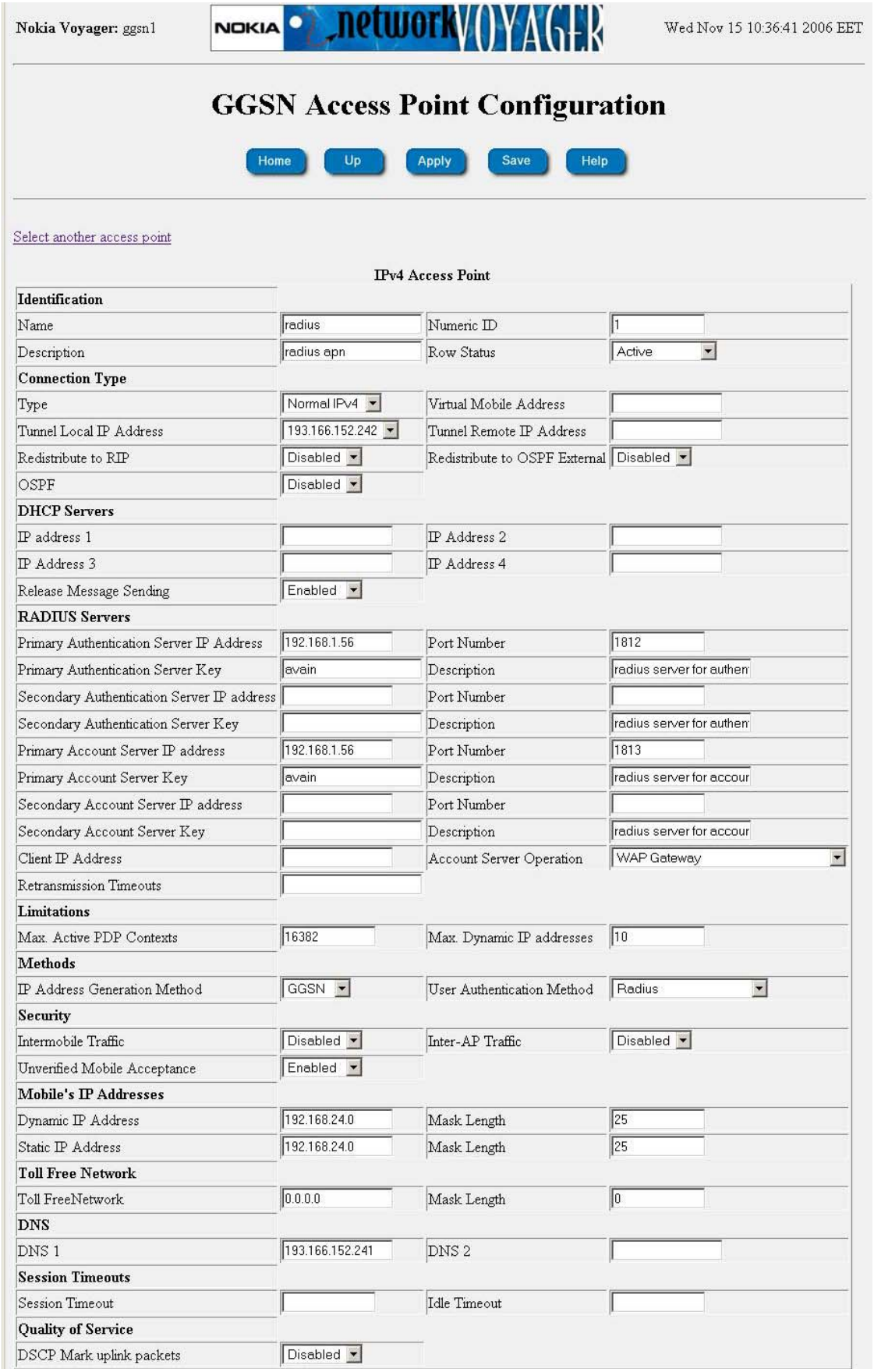
Uusi käyttäjä luodaan New User -sivulla. Username ja Password -kohdat ovat pakollisia. Sen lisäksi voidaan lisätä käyttäjän tietoja muun muassa etu- ja sukunimi. Kun Daily Limittiin ja Weekly Limittiin lisää none arvon, sessiosta tulee rajaton. Käyttäjän tietoja voi editoida jälkeenpäin Edit User -sivulla.



Kuva 14. Edit User -sivu

5.2 GGSN

GGSN on Nokian valmistama Nokia IP650. Laite oli käyttövalmiina ja laitteeseen piti määrittää pelkästään APN. Radius apn:n pohjana käytettiin valmiiksi määritettyä internet apn:ää. APN:ään lisättiin RADIUS palvelimen IP-osoitteet ja portti numerot. Server key on sama kuin dialup adminissa määritetty. User Authentication Method muutettiin Radiukseksi ja Account Server Operation WAP Gatewayksi (Wireless Application Protocol). Jotta APN toimisi, täytyy myös nimipalvelimeen lisätä radius APN:ää vastaava IP-osoite. SAMK:n nimipalvelimen konfiguraatiosta on lisää Ari Rosun opinnäytetyössä ”GPRS-noden käyttöönotto.”



Nokia Voyager: ggsn1 — networkVOYAGER — Wed Nov 15 10:36:41 2006 EET

GGSN Access Point Configuration

Home | Up | Apply | Save | Help

Select another access point

IPv4 Access Point

Identification			
Name	radius	Numeric ID	1
Description	radius apn	Row Status	Active
Connection Type			
Type	Normal IPv4	Virtual Mobile Address	
Tunnel Local IP Address	193.166.152.242	Tunnel Remote IP Address	
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	192.168.1.56	Port Number	1812
Primary Authentication Server Key	avain	Description	radius server for authen
Secondary Authentication Server IP address		Port Number	
Secondary Authentication Server Key		Description	radius server for authen
Primary Account Server IP address	192.168.1.56	Port Number	1813
Primary Account Server Key	avain	Description	radius server for accour
Secondary Account Server IP address		Port Number	
Secondary Account Server Key		Description	radius server for accour
Client IP Address		Account Server Operation	WAP Gateway
Retransmission Timeouts			
Limitations			
Max. Active PDP Contexts	16382	Max. Dynamic IP addresses	10
Methods			
IP Address Generation Method	GGSN	User Authentication Method	Radius
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	193.166.152.241	DNS 2	
Session Timeouts			
Session Timeout		Idle Timeout	
Quality of Service			
DSCP Mark uplink packets	Disabled		

Kuva 15. GGSN:ään määritetty radius-APN

5.3 Tilaajan luonti

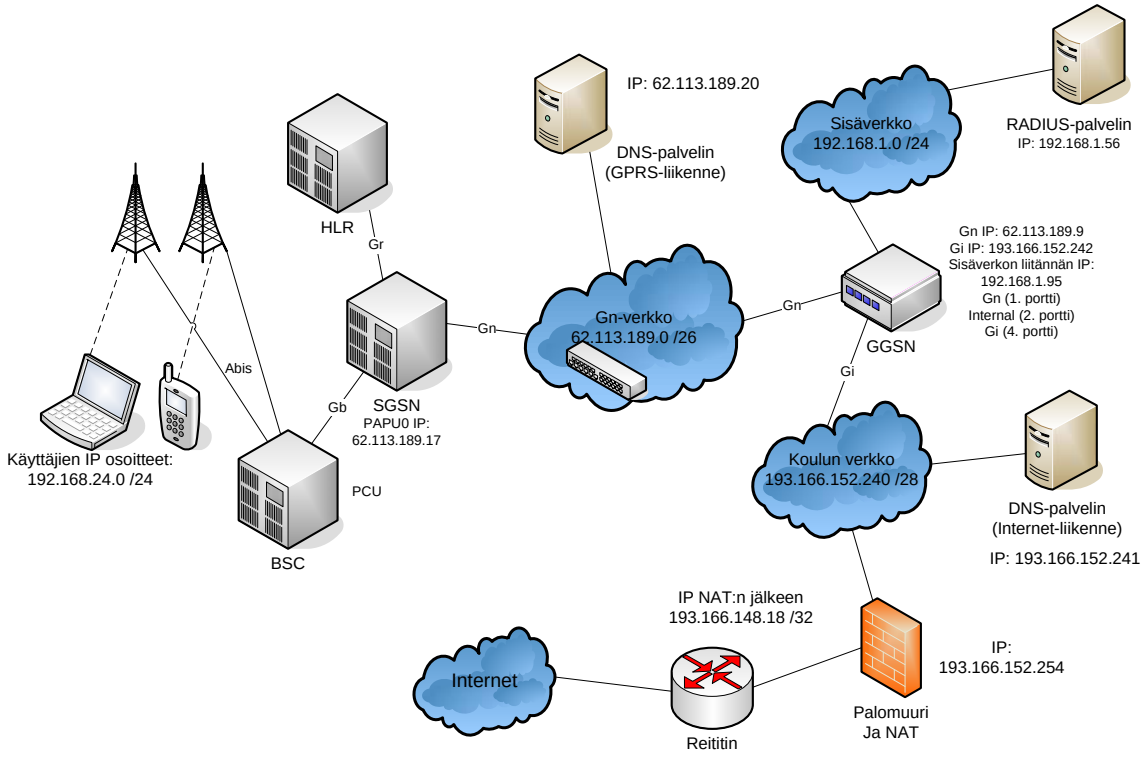
Seuraavaksi luodaan mobiilitilaaja. Tämä tehdään kahdella komennolla.

Tilaaja luodaan HLR:ään seuraavalla komennolla:
“MIC:IMSI=244151111110035,MSISDN=35826479935:SAM=ALL,;”

Tilaajan PDP-kontekstin luodaan HLR:ssa seuraavalla komennolla:
”MNC:IMSI=244151111110035:PDPID=1,APN="RADIUS",;”

Jokaisella tilaajalla on oma IMSI. Se on tallennettu SIM-korttiin. APN on sama kuin GGSN:ään määritetty APN. Tilaajalla voi olla monta APN:ää, eli jokaisella palvelulla vaikka omansa. Kyseisellä IMSI:llä olikin kaksi APN:ää määritettynä tekohetkellä: toinen ilman RADIUS-autentikointia ja toinen sen kanssa. Tämä oli lähinnä testaussyistä.

5.4 RADIUS-palvelin GPRS-verkossa



Kuva 16. SAMK:n GPRS-runkoverkko (RADIUS-palvelin lisättynä) [7]

Radius-palvelin voi olla missä tahansa aliverkossa, johon GGSN on kytketty. Verkolla ei ole merkittävästi väliä: riittää vain, että GGSN saa yhteyden RADIUS-palvelimeen. Yleisen käytännön mukaan RADIUS-kannattaisi asentaa backbone eli Gn-verkkoon, mutta palvelin laitettiin GGSN:n sisäverkkoon, koska koneella, Windows-server isäntä-koneella, oli reitti Internetiin, ja näin tiedonhaku ja työskentely helpottuivat. Loppujen lopuksi RADIUS-palvelin ehkä kannattaisi siirtää Gn-verkkoon lähinnä tietoturvasyistä.

6 YHTEENVETO

Työssäni piti ottaa käyttöön RADIUS-palvelin SAMK:n GPRS-verkkoon. Verkko oli muuten toimintakunnossa, siitä puuttui vain RADIUS-palvelin. Valitsin FreeRADIUS-ohjelmiston, koska sen väitetään olevan yksi maailman käytetyimmistä. Se on myös ilmainen ja näin ollen koulu säästi rahaa. Esimerkiksi Ciscon valmistama Cisco Secure ACS 3.3 for Windows kaupallinen hinta on noin 4600 €. FreeRADIUKSESSA on silti sama toiminnallisuus kuin kaupallisissakin.

Työssäni esittelin RADIUS-protokollan teoriaa ja selitin miten RADIUS-ohjelmistoa käytetään. Työni vaati Linux tuntemusta, toisaalta kaupallinen ohjelmisto olisi ollut helppo asentaa Windowsin päälle paria nappia painamalla. Se olisi vaatinut vain tutustumista itse ohjelmaan. Minun piti konfiguroida muun muassa tekstitiedostoja ja asentaa lisäksi MySQL, kuten olen jo maininnut, jotta RADIUS-serveri käyttäisi tietokantaa käyttäjien tallentamiseen.

Nyt kun älyverkkolaboratoriossa on RADIUS-serveri GPRS-käytössä, sitä voi hyödyntää IP- ja matkapuhelinverkkojen opetuksessa.

LÄHTEET

[1] Hassell, J. RADIUS. O'Reilly & Associates. E-book. 2002.

[2] Verkkodokumentti, viitattu 13.7.2006
Saatavissa: http://fi.wikipedia.org/wiki/RADIUS

[3] Verkkodokumentti, viitattu 13.7.2006
Saatavissa: http://en.wikipedia.org/wiki/RADIUS

[4] Verkkodokumentti, viitattu 13.7.2006
Saatavissa: http://www.cs.tut.fi/~jkorpela/rfct.html

[5] Verkkodokumentti, viitattu 18.7.2006
Saatavissa: http://www.freeradius.org/rfc/rfc2865.html

[6] Verkkodokumentti, viitattu 7.11.2006
Saatavissa:
http://www.eventhelix.com/RealtimeMantra/Telecom/gprs_attach_pdp_sequence_diagram.pdf

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

LIITTEET

LIITE 1 Etherealiin tulleet RADIUS-paketit yhteyden luomisessa

```
No.     Time        Source                Destination           Protocol Info
     25 6.033222    192.168.1.95          192.168.1.56          RADIUS   Access-Request(1) (id=109, l=96)

Frame 25 (138 bytes on wire, 138 bytes captured)
    Arrival Time: Oct 31, 2006 11:23:22.712065000
    Time delta from previous packet: 6.033222000 seconds
    Time since reference or first frame: 6.033222000 seconds
    Frame Number: 25
    Packet Length: 138 bytes
    Capture Length: 138 bytes
    Protocols in frame: eth:ip:udp:radius
    Coloring Rule Name: UDP
    Coloring Rule String: udp
Ethernet II, Src: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1), Dst: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
    Destination: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
        Address: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT address
    Source: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
        Address: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT address
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.95 (192.168.1.95), Dst: 192.168.1.56 (192.168.1.56)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 124
    Identification: 0x46fa (18170)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xaf8f [correct]
        Good: True
        Bad : False
    Source: 192.168.1.95 (192.168.1.95)
    Destination: 192.168.1.56 (192.168.1.56)
User Datagram Protocol, Src Port: radius (1812), Dst Port: radius (1812)
    Source port: radius (1812)
    Destination port: radius (1812)
    Length: 104
    Checksum: 0xaad6 [correct]
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x6d (109)
    Length: 96
    Authenticator: 2F6A57325B010120A908612CC0320CB7
    Attribute Value Pairs
        AVP: l=7  t=NAS-Identifier(32): ggsn1
            NAS-Identifier: ggsn1
        AVP: l=5  t=User-Name(1): joo
            User-Name: joo
        AVP: l=18  t=User-Password(2): Encrypted
            User-Password: \360\276X2\233\375&\244\231\2471K\216xe\332
        AVP: l=6  t=NAS-IP-Address(4): 0.0.0.0
            NAS-IP-Address: 0.0.0.0 (0.0.0.0)
        AVP: l=6  t=NAS-Port-Type(61): Virtual(5)
            NAS-Port-Type: Virtual (5)
        AVP: l=13  t=Calling-Station-Id(31): 35826479835
            Calling-Station-Id: 35826479835
        AVP: l=3  t=Called-Station-Id(30): 1
            Called-Station-Id: 1
        AVP: l=18  t=Acct-Session-Id(44): 09bd713e580a0f00
            Acct-Session-Id: 09bd713e580a0f00
No.     Time        Source                Destination           Protocol Info
     26 6.039719    192.168.1.56          192.168.1.95          RADIUS   Access-Accept(2) (id=109, l=26)

Frame 26 (68 bytes on wire, 68 bytes captured)
    Arrival Time: Oct 31, 2006 11:23:22.718562000
    Time delta from previous packet: 0.006497000 seconds
    Time since reference or first frame: 6.039719000 seconds
    Frame Number: 26
    Packet Length: 68 bytes
    Capture Length: 68 bytes
    Protocols in frame: eth:ip:udp:radius
    Coloring Rule Name: UDP
    Coloring Rule String: udp
Ethernet II, Src: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d), Dst: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
    Destination: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
        Address: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT address
    Source: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
        Address: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
```

```
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT address
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.56 (192.168.1.56), Dst: 192.168.1.95 (192.168.1.95)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 54
    Identification: 0x0002 (2)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xb6cd [correct]
        Good: True
        Bad : False
    Source: 192.168.1.56 (192.168.1.56)
    Destination: 192.168.1.95 (192.168.1.95)
User Datagram Protocol, Src Port: radius (1812), Dst Port: radius (1812)
    Source port: radius (1812)
    Destination port: radius (1812)
    Length: 34
    Checksum: 0x643b [correct]
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x6d (109)
    Length: 26
    Authenticator: A925615166E4C85A18D927A3C73523C8
    Attribute Value Pairs
        AVP: l=6  t=Session-Timeout(27): 100000
            Session-Timeout: 100000
No.     Time        Source                Destination           Protocol Info
     27 6.040658    192.168.1.95          192.168.1.56          RADIUS   Accounting-Request(4) (id=110, l=124)

Frame 27 (166 bytes on wire, 166 bytes captured)
    Arrival Time: Oct 31, 2006 11:23:22.719501000
    Time delta from previous packet: 0.000939000 seconds
    Time since reference or first frame: 6.040658000 seconds
    Frame Number: 27
    Packet Length: 166 bytes
    Capture Length: 166 bytes
    Protocols in frame: eth:ip:udp:radius
    Coloring Rule Name: UDP
    Coloring Rule String: udp
Ethernet II, Src: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1), Dst: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
    Destination: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
        Address: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT address
    Source: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
        Address: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT address
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.95 (192.168.1.95), Dst: 192.168.1.56 (192.168.1.56)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 152
    Identification: 0x46fc (18172)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xaf71 [correct]
        Good: True
        Bad : False
    Source: 192.168.1.95 (192.168.1.95)
    Destination: 192.168.1.56 (192.168.1.56)
User Datagram Protocol, Src Port: radius (1812), Dst Port: radius-acct (1813)
    Source port: radius (1812)
    Destination port: radius-acct (1813)
    Length: 132
    Checksum: 0x2fd5 [correct]
Radius Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0x6e (110)
    Length: 124
    Authenticator: ECB11013472ECADEF2F560432991656E
    Attribute Value Pairs
        AVP: l=7  t=NAS-Identifier(32): ggsn1
            NAS-Identifier: ggsn1
        AVP: l=5  t=User-Name(1): joo
            User-Name: joo
        AVP: l=6  t=Acct-Status-Type(40): Start(1)
            Acct-Status-Type: Start (1)
        AVP: l=6  t=NAS-IP-Address(4): 0.0.0.0
            NAS-IP-Address: 0.0.0.0 (0.0.0.0)
        AVP: l=6  t=NAS-Port-Type(61): Virtual(5)
            NAS-Port-Type: Virtual (5)
        AVP: l=13  t=Calling-Station-Id(31): 35826479835
```

```
            Calling-Station-Id: 35826479835
        AVP: l=3  t=Called-Station-Id(30): 1
            Called-Station-Id: 1
        AVP: l=18  t=Acct-Session-Id(44): 09bd713e580a0f00
            Acct-Session-Id: 09bd713e580a0f00
        AVP: l=6  t=Framed-IP-Address(8): 192.168.24.3
            Framed-IP-Address: 192.168.24.3 (192.168.24.3)
        AVP: l=10  t=X-Ascend-IPX-Alias(224): 4761453869081374965
            X-Ascend-IPX-Alias: 4761453869081374965
        AVP: l=6  t=X-Ascend-Metric(225): 985688
            X-Ascend-Metric: 985688
        AVP: l=6  t=X-Ascend-PRI-Number-Type(226): 8
            X-Ascend-PRI-Number-Type: 8
        AVP: l=6  t=X-Ascend-Dial-Number(227): >q\275\t
            X-Ascend-Dial-Number: >q\275\t
        AVP: l=6  t=X-Ascend-Route-IP(228): 1047641361
            X-Ascend-Route-IP: 1047641361
No.     Time        Source                Destination           Protocol Info
     28 6.044120    192.168.1.56          192.168.1.95          RADIUS   Accounting-Response(5) (id=110, l=20)

Frame 28 (62 bytes on wire, 62 bytes captured)
    Arrival Time: Oct 31, 2006 11:23:22.722963000
    Time delta from previous packet: 0.003462000 seconds
    Time since reference or first frame: 6.044120000 seconds
    Frame Number: 28
    Packet Length: 62 bytes
    Capture Length: 62 bytes
    Protocols in frame: eth:ip:udp:radius
    Coloring Rule Name: UDP
    Coloring Rule String: udp
Ethernet II, Src: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d), Dst: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
    Destination: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
        Address: NokiaInt_0c:0e:f1 (00:a0:8e:0c:0e:f1)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT address
    Source: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
        Address: Vmware_b9:cd:9d (00:0c:29:b9:cd:9d)
        .... ...0 .... .... .... .... = Multicast: This is a UNICAST frame
        .... ..0. .... .... .... .... = Locally Administrated Address: This is a FACTORY DEFAULT address
    Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.56 (192.168.1.56), Dst: 192.168.1.95 (192.168.1.95)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 48
    Identification: 0x0002 (2)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xb6d3 [correct]
        Good: True
        Bad : False
    Source: 192.168.1.56 (192.168.1.56)
    Destination: 192.168.1.95 (192.168.1.95)
User Datagram Protocol, Src Port: radius-acct (1813), Dst Port: radius (1812)
    Source port: radius-acct (1813)
    Destination port: radius (1812)
    Length: 28
    Checksum: 0x1da9 [correct]
Radius Protocol
    Code: Accounting-Response (5)
    Packet identifier: 0x6e (110)
    Length: 20
    Authenticator: 72527E26B938F2859930E5916658C927
```