UNIVERSITAS INDONESIA

ANALISA PERBANDINGAN KINERJA MOBILE VPN MENGGUNAKAN PROTOKOL PPTP DENGAN JARINGAN 3G

SKRIPSI

ARYADI PRAKOSO
0706199136

FAKULTAS TEKNIK
PROGRAM TEKNIK ELEKTRO

DEPOK
DESEMBER, 2009

UNIVERSITAS INDONESIA

ANALISA PERBANDINGAN KINERJA MOBILE VPN MENGGUNAKAN PROTOKOL PPTP DENGAN JARINGAN 3G

SKRIPSI

Diajukan sebagai salah satu syarat memperoleh gelar sarjana

ARYADI PRAKOSO
0706199136

FAKULTAS TEKNIK
PROGRAM TEKNIK ELEKTRO
DEPOK
DESEMBER, 2009

HALAMAN PERNYATAAN ORISINALITAS

Skripsi/Tesis/Disertasi ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama : ARYADI PRAKOSO

NPM : 0706199136

Tanda Tangan: .....

Tanggal : 28 Desember 2009

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : Aryadi prakoso
NPM : 0706199136
Program Studi : Teknik Elektro
Judul Skripsi :Analisa Perbandingan Kinerja Mobile VPN menggunakan Protokol PPTP Dengan Jaringan 3G

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar SarjanaTeknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Muhammad Salman, ST, MIT ( )

Penguji : Ir Endang Sriningsih MT.,Si ( )

Penguji : Dr Ir Anak Agung Putri Ratna M.Eng ( )

Ditetapkan di : Depok

Tanggal : 28 Desember 2009

KATA PENGANTAR / UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Teknik Elektro pada Fakultas Teknik, Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

(1) Bapak Muhammad Salman, ST,MIT , selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini;

(2) Orang tua saya Bpk Suharjono& Siti Rokayah beserta keluarga besar yang telah memberikan bantuan dukungan material dan moral;

(3)Sdri Angie Ayunda ,ST yang menyediakan waktu dan tenaga untuk membantu menemukan solusi dalam menyelesaikan skripsi ini.;

(4) Teman teman jurusan teknik elektro serta sahabat yang telah banyak membantu saya dalam menyelesaikan skripsi ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 28 Desember 2009

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Aryadi Prakoso
NPM : 0706199060
Program Studi : Teknik Elektro
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis karya : Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty- Free Right*)** atas karya ilmiah saya yang berjudul :

ANALISA PERBANDINGAN KINERJA MOBILE VPN
MENGGUNAKAN PROTOKOL PPTP
DENGAN JARINGAN 3G

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.
Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 28 Desember 2009
Yang menyatakan

(Aryadi Prakoso)

ABSTRAK

Nama : Aryadi Prakoso

Program Studi : Teknik Elektro

Judul : Analisa Perbandingan Kinerja Mobile VPN menggunakan Protokol PPTP Dengan Jaringan 3G

Skripsi ini membahas mengenai kemampuan dari VPN Mobile

Dalam era globalisasi saat ini, kemudahan akses terhadap informasi merupakan salah satu kunci untuk dapat bersaing dan memenangkan kompetisi,.Karena dengan adanya informasi yang cepat dan akurat dapat meningkatkan kinerja suatu organisasi atau instansi yang menggunakan sistem tersebut.

Salah satu system informasi tersebut adalah VPN.VPN atau *Virtual Private Network* adalah suatu jaringan private yang mempergunakan sarana jaringan komunikasi publik (dalam hal ini Internet) dengan memakai *tunnelling protocol* dan prosedur pengamanan. Dengan memakai jaringan publik, dalam hal ini Internet, maka biaya pengembangan yang dikeluarkan akan jauh relatif lebih murah daripada harus membangun sebuah jaringan *leased line* sendiri.

Namun, pemakaian Internet sebagai sarana jaringan publik juga menmpunyai resiko sendiri karena Internet terbuka untuk umum maka masalah kerahasiaan dan authentifikasi atas data yang dikirim pun juga terbuka. Oleh karena itu, VPN menjaminnya dengan suatu protocol untuk enkripsi data.

Kata kunci :

VPN, VPN Mobile,PPTP,3G

ABSTRACT

Name : Aryadi Prakoso
Study Program: Elecrical Engineering
Title : Comparison Analysis Performance of Mobile VPN Technology Between PPTP Protocol Based and 3G Network Based

Newdays, simple accessibility to get information is one of the greatest key to win the competition, because with this information which fast and accurate can improve performance of organization when we use this system.

One of the information system is VPN. VPN as known as Virtual Private network is a private network

That using public network communication, in this case was the internet using tunneling protocol and security procedure. Choosing public network communication had several benefit such as lower cost system for development rather than we created own leased lined network.

In other hands, choosing this network have their own risk, cause this network basically is an open network system. This make the secret and authentication problem of sending data also open. Base on this fact VPN play role to guarantee data encryption with some kind protocol

Key words:
VPN, VPN Mobile,PPTP,3G

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Dalam era globalisasi saat ini, kemudahan akses terhadap informasi merupakan salah satu kunci untuk dapat bersaing dan memenangkan kompetisi, karena dengan adanya informasi yang cepat dan akurat dapat meningkatkan kinerja suatu organisasi. Akses informasi yang cepat dan akurat salah satunya bisa didapatkan melalui Internet.

Pemakaian Internet sebagai sarana jaringan publik untuk mendapatkan maupun mengirimkan suatu informasi mempunyai resiko tersendiri karena Internet terbuka untuk umum, maka masalah kerahasiaan dan authentifikasi atas informasi yang diterima dan dikirim pun juga terbuka. Oleh karenanya teknologi VPN dapat menjawab kebutuhan tersebut , menjaminnya dengan suatu protokol untuk enkripsi data.

Salah satu jenis dari VPN adalah *Mobile* VPN.Dengan *Mobile* VPN kita dapat mengakses internal sumber daya suatu organisasi melalui *mobile devices* seperti *Handphone*,PDA, *Smartphone* maupun *Notebook*.

1.2 TUJUAN PENULISAN

Tujuan pembuatan skripsi ini adalah untuk membandingkan kemampuan dari Mobile VPN, dimana Mobile VPN tersebut untuk jalur datanya menggunakan Jaringan 3G dan protokol yang digunakan adalah PPTP, dan akan dibandingkan ketika hanya menggunakan Jaringan 3G.Yang akan dibandingkan yaitu dari sisi Throughput dan Waktu Transfernya

1.3 BATASAN MASALAH

Agar masalah yang akan dibahas menjadi jelas dan tidak banyak menyimpang dari topik yang akan dibahas, maka dalam penulisan proyek akhir ini penulis menekankan, bahwa hal yang akan dibahas adalah perbandingan Throughput dan Waktu Tranfer dari Mobile VPN dengan Jaringan 3G

1.4 METODOLOGI PENELITIAN

Metode penelitian yang akan dilakukan yaitu studi literatur, analisa sistem, uji coba dan perbandingan.

1.5 METODE PENULISAN

Sistematika penulisan skripsi ini terdiri dari bab-bab yang memuat beberapa sub-bab. Untuk memudahkan pembacaan dan pemahaman maka skripsi ini dibagi menjadi beberapa bab yaitu:

BAB I PENDAHULUAN

Bab ini membahas mengenai latar belakang, tujuan penulisan, batasan masalah, metodologi penelitian dan metode penulisan dari skripsi ini.

BAB II *MOBILE* VPN DAN TEKNOLOGI JARINGAN 3G

Bab ini membahas mengenai dasar teori dari VPN, Mobile VPN, Protokol PPTP dan Jaringan 3G

BAB III PERANCANGAN PENGUJIAN *MOBILE* VPN

Bab ini membahas mengenai metode yang digunakan untuk pengujian dan pengambilan data

BAB IV ANALISA HASIL UJICOBA DAN PERBANDINGAN

Bab ini akan membahas mengenai Analisa hasil uji coba dan perbandingan kemampuan dari Mobile VPN menggunakan protokol PPTP dengan Jaringan 3G, yaitu dari sisi Throughput dan waktu transfer yang dibutuhkan untuk mengirimkan data

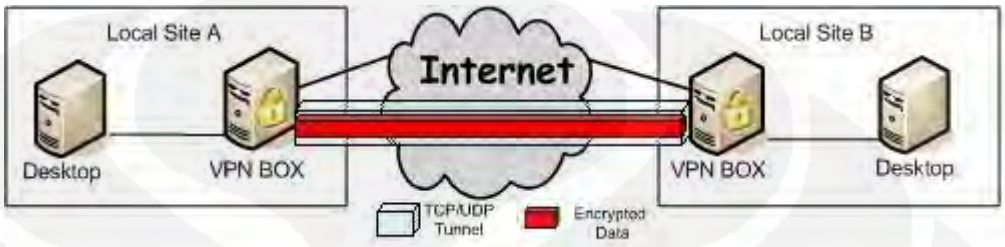
BAB V KESIMPULAN

Penutup berisi kesimpulan dan saran

BAB II

Mobile VPN dan Teknologi Jaringan 3G

2.1 *VPN (Virtual Private Network)*



Gambar 2.1 *Virtual Private Network* (VPN)

VPN dapat diartikan suatu jaringan *private* yang mempergunakan sarana jaringan komunikasi publik yaitu Internet dengan memakai *tunnelling protocol* dan prosedur pengamanannya.

VPN dapat digunakan pada jaringan yang telah ada, seperti internet, maka VPN dapat memfasilitasi transfer data yang bersifat sensitif secara aman melalui jaringan public.VPN juga dapat menyediakan solusi yang fleksibel seperti pengamanan komunikasi antara *remote user* dengan *server* sebuah organisasi tanpa harus memikirkan di mana letak remote user tersebut

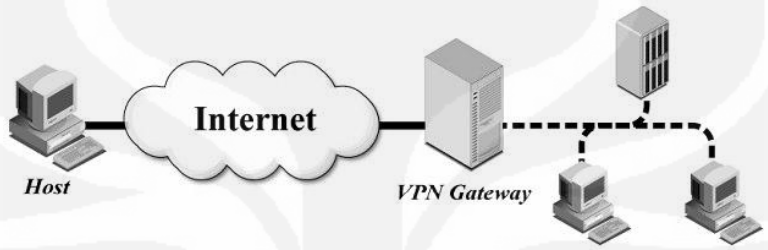
VPN dapat menggunakan kedua bentuk kriptografi, yaitu kriptografi kunci simetris dan kriptografi kunci publik. Kriptografi kunci simetris biasanya lebih efisien dan membutuhkan ongkos pemrosesan yang lebih murah bila dibandingkan dengan kriptografi kunci publik. Oleh karena itu, kriptografi kunci simetri lebih sering digunakan untuk mengenkripsi bagian terpenting dari data yang akan dikirimkan melalui VPN

Algoritma yang umumnya digunakan untuk mengimplementasi kriptografi kunci simetris meliputi *Digital Encryption Standard* (DES),*Triple DES* (3DES), *Advanced Encryption Standard* (AES), *Blowfish, RC4, International Data Encryption Algorithm* (IDEA), dan Hash *Message Authentication Code* (HMAC) versi *Message Digest* 5

(MD5) dan *Secure Hash Algorithm* (SHA-1). Sedangkan algoritma yang umumnya digunakan untuk algoritma kunci publik adalah meliputi RSA, *Digital Signature Algorithm* (DSA), dan *Elliptic Curve DSA* (EDBSA).[2]

2.1.1 Jenis - Jenis VPN

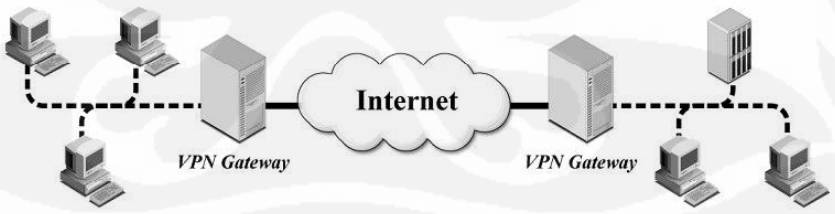
2.1.1.1 *Remote Access*VPN



Gambar 2.2 *Remote Access* VPN

Model *Remote Access VPN* banyak digunakan ketika menghubungkan host pada jaringan yang tidak aman kepada resource pada jaringan yang aman, contohnya menghubungkan pegawai yang sedang berada di lokasi *remote* kepada kantor pusat melalui internet [7]

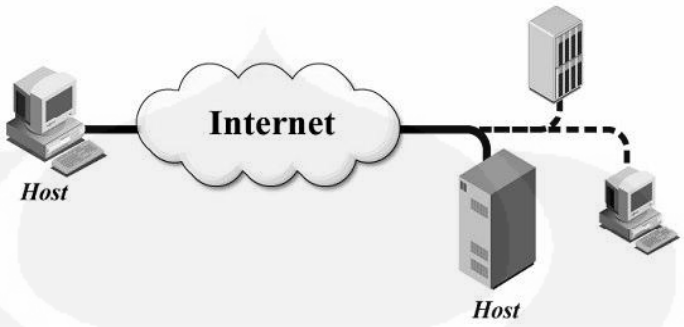
2.1.1.2 *Site to Site* VPN



Gambar 2.3 Site to Site VPN

Arsitektur *Site to Site* biasanya paling banyak digunakan ketika menghubungkan dua jaringan yang aman, seperti menghubungkan sebuah kantor cabang ke pusat melalui internet. Arsitektur model ini menggantikan *wide area network* (WAN) privat yang relative mahal [7]

2.1.1.3 *Host to Host* VPN



Gambar 2.4 Host to Host VPN

Model ini biasa digunakan ketika sejumlah kecil user atau administrator pada sistem remote membutuhkan protokol yang tidak aman dan dapat di*update* untuk menyediakan servis VPN. Arsitektur ini tidak transparan terhadap user karena harus melakukan otentikasi sebelum menggunakan VPN. Selain itu, semua pihak yang terkait harus meng-install perangkat lunak VPN *client* yang telah dikonfigurasi.[7]

2.1.2 Fungsi Utama VPN

VPN harus mampu menyediakan tiga fungsi utama untuk penggunaannya. Ketiga fungsi utama tersebut antara lain sebagai berikut.

2.1.2.1 *Confidentially* (Kerahasiaan)

Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melauinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak.

2.1.2.2 Data *Integrity* (Keutuhan Data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak,

ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

2.1.2.3 *Origin Authentication* (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain

2.1.3 Teknologi VPN

Virtual Private Network adalah perpaduan dari teknologi *tunneling* dengan teknologi enkripsi. Kedua teknologi tersebut saling melengkapi.

2.1.3.1 Teknologi Tunneling

Teknologi *tunneling* merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringa umum, namun koneksi tersbut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya.Hal ini sama dengan seperti penggunaan jalur *busway* yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus.

Koneksi *point-to-point* ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point*.

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan *IP Addressing* dan *IP Routing* yang sudah matang. Maksudnya, antara sumber *tunnel* dengan tujuan *tunnel* telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun.

Apabila *tunnel* tersebut telah terbentuk, maka koneksi *point-to-point* palsu tersebut dapat langsung digunakan untuk mengirim dan menerima data. Namun, di dalam teknologi VPN, *tunnel* tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. *Tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati *tunnel* tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi aman dan bersifat pribadi.

2.1.3.2 Teknologi Enkripsi

Teknologi enkripsi menjamin data yang berlalu-lalang di dalam *tunnel* tidak dapat dibaca dengan mudah oleh orang lain yang bukan merupakan komputer tujuannya. Semakin banyak data yang lewat di dalam *tunnel* yang terbuka di jaringan publik, maka teknologi enkripsi ini semakin dibutuhkan. Enkripsi akan mengubah informasi yang ada dalam *tunnel* tersebut menjadi sebuah *ciphertext* atau teks yang dikacaukan dan tidak ada artinya sama sekali apabila dibaca secara langsung. Untuk dapat membuatnya kembali memiliki arti atau dapat dibaca, maka dibutuhkan proses dekripsi. Proses dekripsi terjadi pada ujung-ujung dari hubungan VPN. Pada kedua ujung ini telah menyepakati sebuah algoritma yang aka digunakan untuk melakukan proses enkripsi dan dekripsinya. Dengan demikian, data yang dikirim aman sampai tempat tujuan, karena orang lain di luar *tunnel* tidak memiliki algoritma untuk membuka data tersebut.

2.2 Mobile VPN

Mobile VPN adalah konfigurasi jaringan di mana perangkat mobile seperti notebook,ponsel maupun personal digital assistant (PDA) dapat mengakses virtual private network (VPN) ketika bergerak dari satu lokasi ke lokasi lainnya.Mobile VPN yang efektif menyediakan pelayanan yang berkesinambungan bagi pengguna dan dapat secara mulus beralih dari teknologi akses dan berbagai jaringan publik. Fungsi mobile VPN yang efektif adalah transparan kepada pengguna akhir tanpa mengorbankan keamanan atau privasi.

2.3 *Point to Point Tunneling Protocol* (PPTP)

PPTP merupakan protokol yang mengizinkan hubungan Point-to Point Protocol (PPP) melewati jaringan IP, dengan membuat Virtual Private Network (VPN)

Teknologi jaringan PPTP merupakan pengembangan dari *remote access Point-to-Point protocol* yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan *private* LAN-to-LAN.

PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan private network sebagai klien dengan *remote access* melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya *public-switched telephone network* (PSTNs) untuk membangun VPN.

Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk *remote users* dan *mobile users* karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

Akan tetapi tidak diperlukan *network access server* dalam membuat PPTP *tunnel* saat menggunakan klien PPTP yang terhubung dengan LAN untuk dapat terhubung dengan server PPTP yang terhubung pada LAN yang sama.

2.3.1 Arsitektur PPTP

Komunikasi yang aman dibuat dengan menggunakan protokol PPTP melewati tiga proses, dimana setiap proses tersebut membutuhkan selesainya proses yang sebelumnya. Ketiga proses tersebut berjalan dengan cara sebagai berikut.

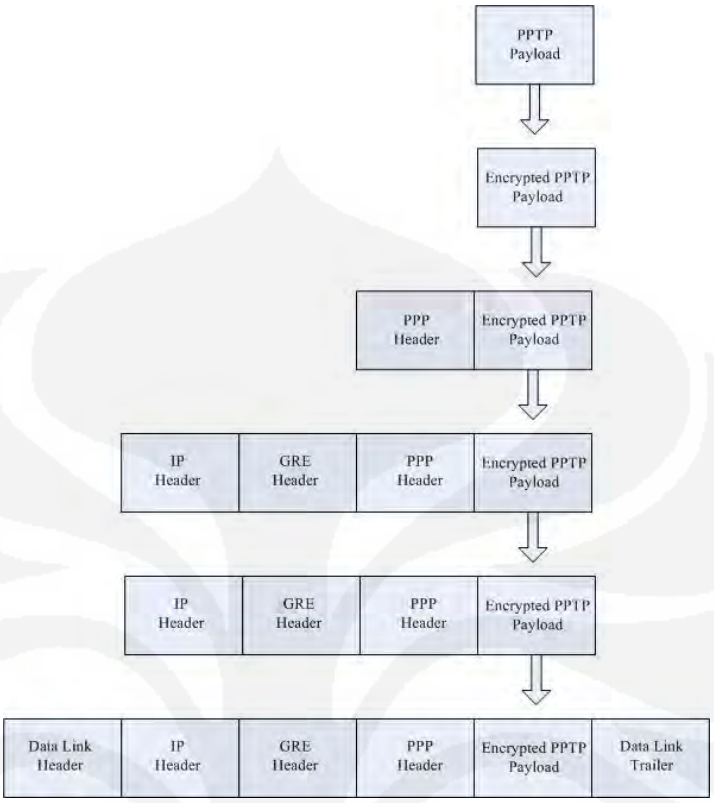
- ***PPTP Connection and Communication***. Klien PPTP menggunakan PPP untuk terhubung ke ISP dengan menggunakan jalur telepon standar atau ISDN line. Koneksi tersebut menggunakan protokol PPP untuk membangun koneksi dan enkripsi paket data.[3]
- ***PPTP Control Connection***. Menggunakan koneksi ke internet yang telah dibangun oleh protokol PPP, protokol PPTP membuat sebuah *control connection* dari klien PPTP ke server PPTP di internet. Koneksi tersebut menggunaka TCP untuk membagun koneksi dan ini disebut dengan PPTP *tunnel*.
- ***PPTP Data Tunneling***. Akhirnya protokol PPTP membuat IP datagrams yang di dalamnya terdapat enkripsi paket PPP yang kemudian dikirim melalui PPTP *tunnel* ke server PPTP. Server PPTP membongkar IP datagram dan mendekripsi paket PPP dan kemudian merutekan paket yang telah didekripsi ke jaringan *private*.

2.3.2 Cara Kerja Protokol PPTP

PPTP mengerjakan tiga proses untuk pengamanan PPTP melalui media yang tidak aman. Proses ini adalah :

- Koneksi berbasis PPP
- Pengendalian Koneksi PPTP
- PPTP Tunneling dan transfer data

Setelah suatu koneksi berbasis PPP dibentuk antara klien PPTP dan Server PPTP, pengendalian koneksi PPTP dijalankan. Pengendalian koneksi PPTP dibentuk berdasarkan pada alamat IP pada klien PPTP dan server , dimana menggunakan port TCP 1723.Setelah pengendalian koneksi PPTP dibentuk, pengendalian dan manajemen pesan bertukar pesan antara Klien dan Server.Pesan ini bertanggung jawab untuk pemeliharaan, manajemen dan penghentian tunnel PPTP.Pesan ini meliputi transmisi berkala dari “PPTP Echo Request” dan “PPTP Echo Replay” pesan yang membantu mendeteksi suatu kegagalan konektifitas antara klien dan server PPTP.Pesan pengendalian PPTP dienkapsulasi TCP Datagrams. Oleh karena itu, setelah pembentukan dari suatu koneksi PPP dengan server remote atau klien, suatu koneksi TCP dibentuk. Koneksi ini digunakan untuk menukar pesan pengendalian PPTP.



Gambar 2.5 Proses tunneling Data Protokol PPTP dari pengirim

Suatu data paket PPTP mengalami berbagai langkah-langkah enkapsulasi, yaitu:

- Enkapsulasi Data

  Informasi yang asli, dienkripsi dan kemudian dienkapsulasi di dalam suatu frame PPP. Suatu header dimasukan dalam frame tersebut.

- Enkapsulasi Frame

  Frame PPP kemudian dienkapsulasi di dalam sebuah Generic Routing Encapsulation (GRE). GRE header yang dimodifikasi berisi suatu 4 byte Acknowledgement field dan suatu Acknowledgement bit yang bersesuaian memberitahu kehadiran dari Acknowledgement bit yang bersesuaian memberitahu kehadiran dari Acknowledgement field. Sebagai tambahan, Key field di dalam frame GRE digantikan

dengan suatu 2 byte long field yang dinamakan Call ID. Klien PPTP menetapkan field ini ketika menciptakan PPTP tunnel.

- Enkapsulasi Paket GRE

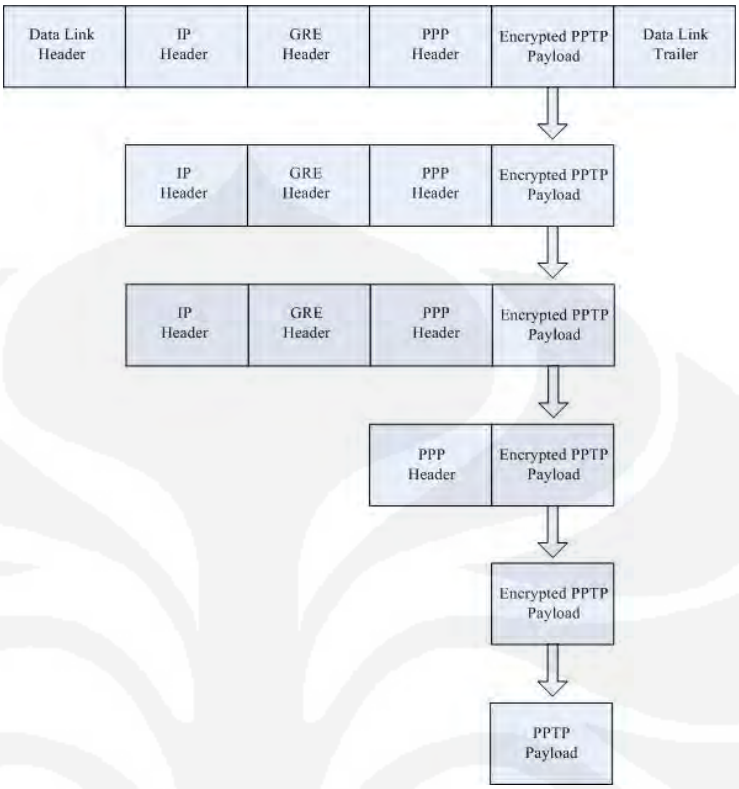
  Berikutnya, suatu IP Header ditambahkan kepada PPP frame, dimana dienkapsulasi di dalam paket GRE. IP header ini berisi alamat IP dari sumber klien PPTP dan server tujuan.

- Enkapsulasi Data Link Layer

  PPTP merupakan potokol tunneling layer 2.Data link header dan trailer memiliki peranan penting dalam tunneling data.Sebelum ditempatkan pada medium transmisi, data link layer menambahkan header dan trailer miliknya ke dalam datagram tersebut.Jika datagram harus berjalan sepanjang suatu PPTP tunnel lokal, datagram dienkapsulasi dengan suatu teknologi LAN header dan trailer.Pada sisi lain, jika tunnel dibawa melalui sebuah hubungan WAN, header dan trailer ditambahkan kembali ke dalam datagram.

  Setelah data PPTP ditranfer dan diterima dengan sukses kepada penerima yang dituju, pada sisi penerima harus memproses paket yang diterima untuk mendapatkan data yang asli.Pemrosesannya merupakan kebalikan dari tunneling data PPTP.Untuk mendapatkan data asli kembali, pada sisi penerima melakukan langkah berikut ini.

  - Sisi penerima memproses Data link header dan trailer yang ditambahkan pengirim.
  - Berikutnya memproses GRE header
  - Memproses IP header
  - Memproses PPP header
  - Terakhir mendekripnya.



Gambar 2.6 Pemrosesan data Protokol PPTP pada penerima

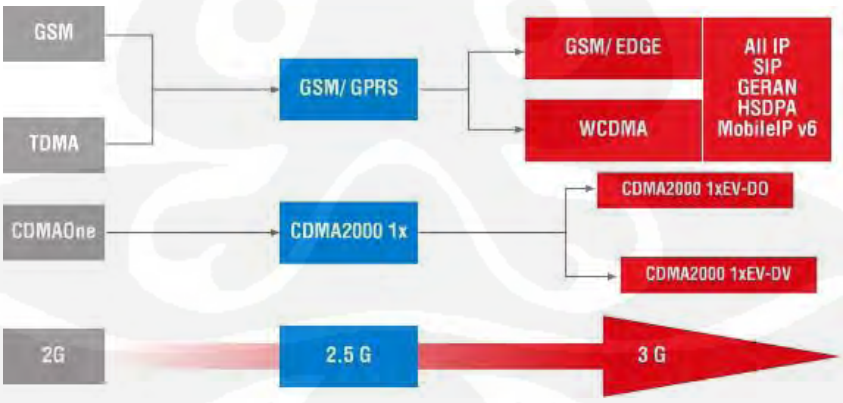
2.4 Teknologi 3G

3G adalah singkatan dari Third Generation atau Generasi Ketiga, yaitu generasi ketiga dalam teknologi telepon selular. 3G merupakan nama yang umum digunakan untuk menyebutkan teknologi lanjutan dari sistem komunikasi mobile, dimana kita bisa mendapatkan layanan data berkecepatan tinggi untuk aplikasi multimedia seperti download musik, nonton TV lewat handphone, internet berkecepatan tinggi, video call, streaming video klip, dan sebagainya.[9]

Secara umum, ITU-T, sebagaimana dikutip oleh FCC mendefinisikan 3G sebagai sebuah solusi nirkabel yang bisa memberikan kecepatan akses Sebesar 144 Kbps untuk kondisi bergerak cepat (mobile), Sebesar 384 Kbps untuk kondisi berjalan (pedestrian), Sebesar 2 Mbps untuk kondisi statik di suatu tempat.

Berdasarkan definisi di atas, perangkat 3G secara umum mempunyai kemampuan transmisi yang besar, baik dalam kecepatan maupun kapasitas dari pendahulunya. Sebagai perbandingan, GSM mampu mengirimkan data hingga 14,4 Kbps, dan GPRS berkisar 53,6 Kbps dengan kecepatan maksimum secara teoritis hingga 171,2 Kbps dengan menggunakan kedelapan timeslotnya secara bersamaan. Sementara itu EDGE(Enhanced Data Rates for Global Evolution) yang sering disebut-sebut sebagai generasi 2,5 dan 2,75 (2,5G dan 2,75G) juga dengan kondisi kedelapan timeslotnya aktif mampu melaju dengan 473,6 Kbps. Dan dalam prakteknya kecepatan yang diperoleh dari GPRS berkisar 50 Kbps dan EDGE mencapai 115 Kbps.

Layanan 3G berada pada frekuensi 1.900 Mhz. ITU-T mendefinisikan layanan 3G untuk GSM pada frekuensi 1.900 Mhz dengan lebar pita sebesar 60 Mhz. Namun, pada umumnya, teknologi berbasis CDMA2000 menggunakan spektrum di frekuensi 800 Mhz, atau yang biasa dikenal sebagai spektrum PCS (Personal Communication System).[9]



Gambar 2.7 Evolusi Jaringan Seluler

2.4.1 Kelebihan 3G dari generasi-generasi sebelumnya :

a. Kualitas suara yang lebih bagus.
b. Keamanan yang terjamin.
c. Kecepatan data mencapai 2 Mbps untuk lokal/Indoor/slow-moving access dan384 kbps untuk wide area access.
d. Support beberapa koneksi secara simultan, sebagai contoh, pengguna dapat browse internet bersamaan dengan melalukan call (telepon) ke tujuan yang berbeda.
e. Infrastruktur bersama dapat mensupport banyak operator dilokasi yang sama.
f. Roaming nasional dan internasional.
g. Bisa menangani packet-and circuit-switched service termasuk internet (IP) dan videoconferencing. Juga high data rate communication services dan asymmetric data transmission.
h. Efiensi spektrum yang bagus, sehingga dapat menggunakan secara maksimum bandwidth yang terbatas.
i. Support untuk multiple cell layer.
j. Co-existance and interconnection dengan satellite-based services.
k. Mekanisme billing yang baru tergantung dari volume data, kualitas service dan waktu.

2.4.2 Varian Teknologi 3G

a. W-CDMA (Wideband - Coded Division Multiple Access) atau UMTS (Universal Mobile Telecommunication System).

   Universal Mobile Telecommunication System (UMTS) merupakan salah sistem generasi ketiga yang dikembangkan di Eropa dan mualai diperkenalkan tahun 2004. Standarisasi dari UMTS ini dilakukan oleh European Telecommunication Standard Institution (ETSI), selain itu Intertational Telecommunications Union Telecommunication Standardisation

Sector (ITU-T) mengerjakan sistem yang sama dinamakan International Mobile Telecommunation System 2000 (IMT 2000). Kedua badan standarisasi ini dapat melakukan kerjasama sehingga terbentuk satu sistem untuk masa yang akan datang. UMTS dirancang sehingga dapat menyediakan bandwith sebesar 2 Mbits/s. Layanan yang dapat diberikan UMTS diupayakan dapat memenuhi permintaan pemakai dimanapun berada, artinya UMTS diharapkan dapat melayani area yang seluas mungkin, jika tidak ada cell UMTS pada suatu daerah dapat di route-kan melalui satelit. UMTS dapat digunakan oleh perkantoran, rumah dan kendaraan. Layanan yang sama dapat diberikan untuk pemakai indoors dan outdoors, public areas dan private areas, urban dan rural. Frekeunsi radio yang dialokasikan untuk UMTS adalah 1885-2025 MHz dan 2110-2200 MHz. Pita tersebut akan digunakan oleh cell yang kecil (pico cell) sehingga dapat memberikan kapasitas yang besar pada UMTS. Multiple akses yang digunakan dapat mengalokasikan bandwith secara dinamis sesuai dengan kebutuhan pelanggan. Research and Technology Development in Advanced Communications Technologies in Europe (RACE) telah mengembangkan dua jenis multiple akses yakni Code Division Multiple Acces (CDMA) dan Time Division Multiple Acces (TDMA), dari keduanya ini belum diputuskan yang akan digunakan. W-CDMA sudah di implentasikan di Japan, Eropa dan Asia, dan akan dikembangkan di 55 negara pada tahun 2006.

b. CDMA2000-1X EV/DV (Evolution/Data/Voice) dan CDMA2000-1X EV-DO (Data Only)/ (Data Optimized) atau IS-856.

   Merupakan teknologi yang didukung oleh komunitas CDMA Amerika Utara,dipimpin oleh CDMA Development Group

(CDG). CDMA2000-1X EV(Evolution) dan CDMA2000-1X EV-DO ini merupakan pengembangan dariteknologi CDMA2000 1x Release 0/RTT atau CDMA2000 (2.5G). Pada awalnya CDMA2000 1xEV-DO (Rev. 0) hanya bisa mengirim data sampai 2,4 Mbps, tetapi kemudian berkembang sehingga CDMA2000 1xEV-DO (dataonly) yang dibagi menjadi 3 berdasarkan kecepatan tranfer datanya, yaitu :

1) CDMA2000 1xEV-DO Revisi A (T-1 speeds) bisa mengirimkan data sampai 2,45 Mbps sampai 3.1 Mbps dan mendukung aplikasi seperti konferensi video.
2) CDMA2000 1xEV-DO Revisi B ini mampu melakukan transmisi data maksimal sampai 73,5 Mbps.Varian lainnya adalah CDMA2000 1xEV-DV yang mengintegrasikan layanan suara dan layanan multimedia data paket berkecepatan tinggi secara simultan pada kecepatan sampai 3,09 Mbps namun keduannya umumnya hanya mempunyai kecepatan transfer pada 300 Kbps.
3) CDMA2000 1xEV-DO Revisi C dikenal dengan nama UMB (Ultra Mobile Broadband) dapat mendukung kecepatan data hingga 280 Mbps pada kondisi puncak (275 Mbps downstream dan 75 Mbps upstream) sehingga dapat dikategorikan kedalam 4G (Fourth-Generation), dapat melayani layanan Ipbased Voice (VOIP), multimedia, broadband, Teknologi informasi, entertainment dan jasa elekronik komersial juga mendukung penuh jaringan jasa wireless pada lingkungan mobile sehingga tidak beda dengan jaringan Wi-Fi, WiMAX, UWB, dll.

c. TD-CDMA (Time Division Code Division Multiple Access) atau UMTS-TDD (Universal Mobile Telecommunication System - Time Division Duplexing) di Eropa.

   Merupakan jaringan data mobile standar teknologi 3G yang dibangun pada jaringan selular telepon mobile standar UMTS/WCDMA dimana keduanya baik UMTS/WCDMA maupun TD-CDMA/UMTS-TDD tidak saling mendukung dikarenakan perbedaan cara kerja, desain, teknologi dan frekuensi yang dipakai. Di Eropa frekuensi yang dipakai UMTS-TDD ada pada 2010-2020MHz yang dapat mentransfer data pada kecepatan 16 Mbps (pada saat kecepatan maksimum baik Downlink maupun Uplink).

d. GAN (Generic Access Network) atau UMA (Unlicensed Mobile Access)

   Teknologi ini di adopsi oleh 3GPP pada bulan April 2005. GAN di tujukan agar system telekomunikasi dapat berjalan secara roaming dan dapat menangani jaringan LAN (WLAN) dan WAN dalam telepon mobile secara bersamaan.

e. HSPA (High-Speed Packet Access)

   HSPA merupakan teknologi dari penyatuan dari protocol teknologi mobile sebelumnya, sehingga memperluas dan menambah kemampuan (terutama dari sisi kecepatan transfer data) dari protokol UMTS yang telah ada sebelumnya. Karena adanya perbedaan kemapuan (downlink dan uplink) tersebut HSPA di bagi menjadi 2 standar, yaitu :

   1) HSDPA (High Speed Downlink Packet Access)
      Merupakan standar HSPA dengan kemampuan dari sisi

kecepatan transfer downlinknya (dari jaringan ke handset), dimana HSDPA dapat mencapai kecepatan downlink 7.2 Mbps dan secara teori dapat ditinggkatkan sampai kecepatan 14.4 Mbps dengan maksimum uplink 384 kbps. HSDPA selain dapat digunakan oleh handphone tetapi dapat pula digunakan oleh Notebook untuk mengakses data dengan kecepatan tinggi.

2) HSUPA (High Speed Uplink Packet Access)

Merupakan standar HSPA dengan kemampuan dari sisi kecepatan transfer uplinknya (dari handset ke jaringan), dimana HSUPA dapat mencapai kecepatan uplink secara teori sampai kecepatan 5.76 Mbps, tetapi HSUPA ini tidak implentasikan (dikomersialkan) dan handsetnya tidak dibuat

f. HSPA+ (HSPA Evolution)

Merupakan teknologi pengembangan dari HSPA terutama pada kecepatan transfer data yang dapat mencapai kecepatan 42 Mbit/s pada downlink dan 11 Mbit/s pada uplink

g. FOMA (Freedom of Mobile Multimedia Access) di Jepang.

FOMA merupakan jaringan 3G pertama di dunia yang mengimplentasikan WCDMA, diluncurkan pada tahun 2001. FOMA merupakan penamaan layanan 3G oleh operator NTT DoCoMo

h. HSOPA (High Speed OFDM Packet Access)

Merupakan teknologi pengembangan dari UMTS terutama pada teknologi antena yang menggunakan Orthogonal Frequency Division Multiplexing (OFDM) dan multiple-input multiple-

output (MIMO). HSOPA dikenal juga sebagai Super 3G dapat mentransfer data sampai kecepatan 100 Mbit/s untuk downlink dan 50 Mbit/s untuk uplink

i. TD-SCDMA (Time Division Synchronous Code Division Multiple Access).

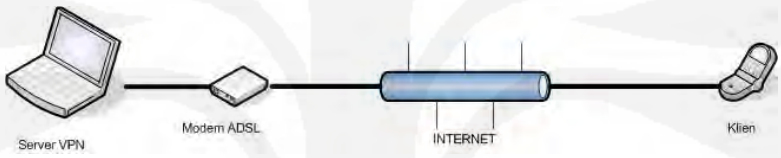
   Merupakan teknologi generasi ketiga ini masih dikembangkan China oleh Chinese Academy of Telecommunications Technology (CATT), Datang dan Siemens AG atas proposal dari China Wireless Telecommunication Standards group (CWTS) kepada ITU (badan PBB untuk telekomunikasi) pada tahun 1999. Teknologi yang dikembangkan untuk menghilangkan ketergantungan pada teknologi barat, tetapi kurang banyak diminati para operator di Asia dikarenakan memerlukan perangkat keras (hardware) yang benar-benar baru dan tidak bisa menggunakan teknologi sebelumnya (CDMA2000 1x). TDSCDMA menggunakan frekuensi 2010 MHz - 2025 MHz (khusus di China), dengan kecepatan transfer data dari 9.6 kbits/s sampai 2048 kbits/s

BAB III

PERANCANGAN METODE PENGUJIAN

Pada bab ini akan dibahas mengenai perancangan metode pengujian yang akan digunakan untuk membandingkan Mobile VPN menggunakan protokol PPTP dengan Jaringan 3G.Perancangan dimulai dengan perencanaan topologi jaringan,software dan hardware yang digunakan, instalasi dan konfigurasi jaringan serta persiapan pengujian.

3.1 Perencanaan Topologi jaringan



Gambar 3.1 Topologi Jaringan

Model topologi jaringan yang digunakan pada pengujian kali ini adalah dengan satu buah Laptop berfungsi sebagai server, Ponsel sebagai Klien,Modem ADSL yang dikonfigurasi agar bisa dilewatkan data VPN PPTP, akses internet baik fixed line dari sisi Server maupun Wireless dari sisi Klien.Pengukuran akan dilakukan dari sisi server.

3.2 Perlengkapan pendukung yang dibutuhkan

Untuk mendukung pelaksanaan pengujian, memerlukan perlengkapan pendukung dimana perlengkapan pendukung tersebut dibagi menjadi 2 yaitu Perangkat keras dan Perangkat lunak yang keduanya saling mendukung.

3.2.1 Perangkat Keras

Perangkat keras yang digunakan untuk melakukan pengujian ini yaitu :

a. Laptop Acer Travelmate 4720

Laptop Acer Travelmate 4720 mempunyai spesifikasi Processor Intel Core 2 duo T 7500 2.2 Ghz (800 Mhz FSB, 4 MB L2 Cache) Memori 1 GB DDR2,160 GB HDD dengan NIC (Network Interface Card) Broadcom Netlink.Laptop ini digunakan sebagai VPN Server yaitu sebagai gerbang antara Server VPN dengan klien.

b. Ponsel Nokia E 71

Ponsel Nokia E 71 mempunyai spesifikasi dimensi 114 x 57 x 10 mm, berat 127 gram, dengan frekuensi operasi Quad-band EGSM 850/900/1800/1900 WCDMA 850/1900 HSDPA,system operasi symbian S60 3rd Edition FP 1, firmware 200.21.118 27-11-2008, IMEI 351940031325360.Ponsel ini digunakan sebagai Klien VPN

c. Jalur data

Jalur data yang digunakan ada 2 yaitu fixed line pada sisi server dan wireless pada sisi klien.Untuk yang fixed line pada sisi server menggunakan produk ADSL (Asymmetric Digital Subscriber Line) Telkomspeedy Dengan kecepatan 384 kbps *downstream* dan 96 kbps *upstream.*Untuk yang wireless pada sisi klien menggunakan jaringan 3G Operator Telkomsel dengan kartu Simpati.

d. Modem ADSL D-LINK DSL-2540T

Modem ini mempunyai spesifikasi maksimum 24Mbps downstream, 1Mbps upstream, Device Interfaces satu RJ-11 untuk Port Input ADSl dan empat RJ-45 untuk port

output.Modem ADSL ini berfungsi untuk menyambungkan jalur data dari ISP ke Server VPN.

3.2.2 Perangkat Lunak

Ada beberapa Perangkat lunak yang digunakan pada pengujian ini yaitu:

a. Windows XP

Windows XP merupakan merupakan sistem operasi berbasis grafis (gambar) dengan berbagai fasilitas, dan kemudahan dalam pengoperasiannya.Microsoft Windows XP ini merupakan salah satu produk unggulan dari Microsoft Corporation yang secara resmi dikeluarkan pada tanggal 25 Oktober 2001. Microsoft Windows XP yang selanjutnya yang disingkat dengan Windows XP ini merupakan kelanjutan dari dari Windows versi sebelumnya.Windows XP dipilih untuk pengujian ini karena sudah terdapat Protokol PPTP di dalamnya dan pengkonfigurasiannya yang mudah untuk digunakan sebagai VPN Server.Windows XP yang digunakan adalah Windows XP Versi 2002 Profesional SP 2 Build 2600.

b. SymNC

SymNC merupakan perangkat lunak berbayar buatan Telexy Networks.Perangkat lunak ini ditujukan untuk pengguna Ponsel dengan Sistem operasi Symbian S60 3rd edition.Perangkat lunak ini berfungsi sebagai perangkat lunak pada klien untuk menghubungkan Ponsel ke server VPN.SymNC yang digunakan untuk pengujian adalah versi 1.00 Build 51.Versi trialnya dapat didownload di pada website www.telexy.com

c. Wireshark

Wireshark merupakan perangkat lunak yang digunakan untuk melakukan analisa jaringan komputer, wireshark dapat menganalisa beberapa parameter QoS seperti bandwidth, delay, throughput, dan packet loss dan lain lain serta dapat mengcapture protokol yang sedang berjalan dalam jaringan tersebut, wireshark yang digunakan untuk pengujian adalah *wireshark versi* 1.2.4 rev 30978 buatan dari Gerald Combs dan dapat didownload secara gratis pada website www.wireshark.org.

d. Trafmeter

Trafmeter merupakan perangkat lunak berbayar yang juga digunakan untuk melakukan analisa jaringan komputer.Trafmeter yang digunakan untuk pengujian adalah trafmeter versi 9.3.546 buatan lastBit Software.Versi trialnya dapat di download pada website www.trafmeter.com

3.3 Instalasi dan Konfigurasi

Setelah menyiapkan perlengkapan pendukung untuk pengujian, maka diperlukan instalasi dan konfigurasi agar pengujian dapat berjalan dengan baik dan sesuai dengan tujuan akhir

3.3.1 Instalasi

Sesuai dengan perlengkapan yang dibutuhkan untuk pengujian, maka yang perlu diinstalasi baik dari sisi server, klien maupun koneksi internet.

3.3.1.1 Instalasi Server

Pada sisi server yang perlu diinstalasi adalah sistem operasi Windows XP versi 2002 Profesional Service Pack 2 Build 2600.

Sedangkan untuk pengukuran data pengujian maka perangkat lunak Wireshark dan Trafmeter berikutnya diinstal pada server.Untuk menginstalasi kedua perangkat lunak tersebut, terlebih dahulu untuk mendownloadnya pada website www.wireshark.org untuk perangkat lunak Wireshark, dan www.trafmeter.com untuk trafmeter. Setelah didownload, double click file wireshark-win32-1.2.4.exe dan file TrafMeter93.exe untuk memulai instalasi Wireshark dan Trafmeter, lalu ikuti instruksi selanjutnya sampai selesai penginstalasian

3.3.1.2 Instalasi Klien

Pada sisi Klien, yang perlu diinstalasi adalah perangkat lunak SymNC.Untuk menginstalasinya, terlebih dahulu di download di website www.telexy.com untuk mendapatkan versi trialnya.Untuk mendownloadnya bisa langsung dari ponsel maupun dari PC baru dikirimkan ke Ponsel baik melalui kabel data maupun koneksi lainnya seperti Bluetooth.setelah dikirimkan ke ponsel, klik file SymNC_v1_0_B51.sis lalu ikuti instruksi selanjutnya sampai selesai penginstalasian.

3.3.1.3 Instalasi Koneksi Internet

Agar Server dan Klien dapat berkomunikasi maka dibutuhkan koneksi internet pada kedua sisi baik pada sisi Server maupun sisi Klien.Untuk sisi klien yang dibutuhkan hanya koneksi dari jaringan operator dimana koneksi tersebut bersifat wireless dan jaringan yang digunakan adalah jaringan 3G.Sedangkan pada sisi server, menggunakan fixed line dari ISP sehingga membutuhkan instalasi seperti modem ADSL dan kabel RJ-45 untuk menyambungkan koneksi internet dari ISP ke Laptop yang pada pengujian ini berfungsi sebagai Server.

3.3.2 Konfigurasi

Agar koneksi VPN dapat dilakukan, setelah selesai penginstalasian diperlukan konfigurasi baik dari sisi server, klien dan koneksi internet

3.3.2.1 Konfigurasi Server

Konfigurasi pada sisi server adalah konfigurasi pada system operasi Windows XP dimana pada system operasi tersebut bisa menjadi sebagai Server VPN maupun Klien VPN tergantung dari konfigurasi yang diinginkan, tanpa harus menginstal perangkat lunak tambahan.Untuk pengujian ini, Windows XP dikonfigurasi sebagai Server VPN berikut langkah – langkahnya.

1. Klik start ⟶ Control Panel ⟶ Network Connection
2. Klik Create a new Conection ⟶ Next ⟶ Pilih Setup Andvanced Connection ⟶ Next

Gambar 3.2 Jendela Network Connection Type

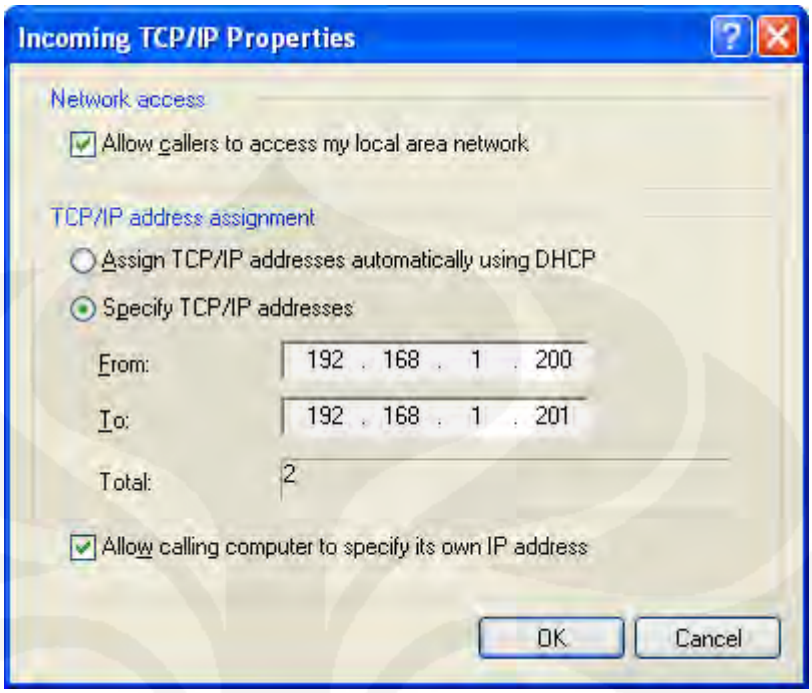
3. Pilih Accept incoming connection ⟶ Next ⟶ Next pilih Allow Virtual Private Connections ⟶ Next

Gambar 3.3 Daftar user

Gambar 3.4 Form untuk menambah user

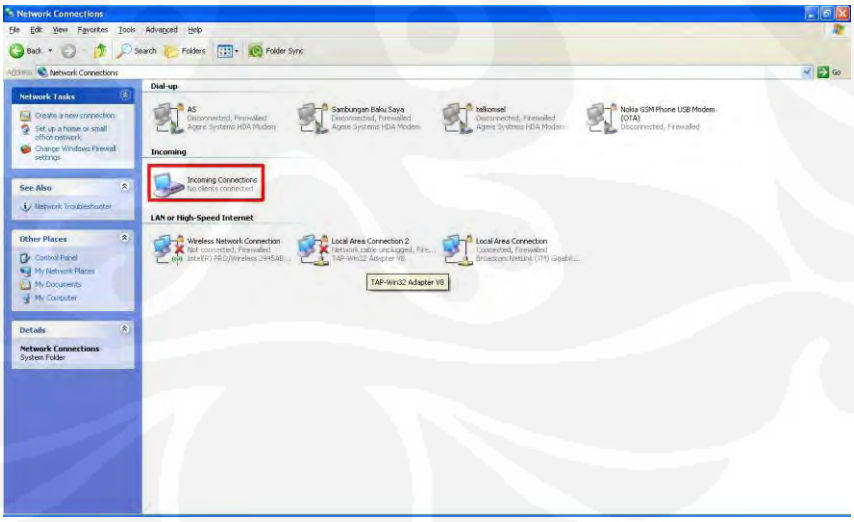
4. Lalu buat user baru untuk autentikasi VPN dengan memilih add lalu isi user name dan password yang diinginkan,misalnya username VPN password elektro, klik OK lalu Next.

5. Pada jendela berikutnya Pilih Internet Protocol klik Properties.pada jendela ini adalah untuk memberikan IP kepada klien agar bisa berkomunikasi dengan server.Klik OK ⟶ Next lalu klik Finish.



Gambar 3.5 Pengaturan IP pada klien

6. Setelah ini maka konfigurasi pada sisi Server sudah selesai dan akan muncul Ikon Incoming Connection pada Jendela Network Connections.



Gambar 3.6 Ikon VPN

7. Setelah selesai mengkonfigurasi pada Server,kita juga perlu untuk mengkonfigurasi pada Modem ADSL agar bisa dilewatkan data Mobile VPN .Langkah – langkahnya adalah sebagai berikut.

    a. Buka Browser Mozilla lalu ketikan alamat IP yang merupakan IP DNS dari Modem yaitu 192.168.1.1

    b. Lalu masukan username dan password

    c. Pilih Advanced, virtual server, VPN tambahkan Rules PPTP.

    d. Pilih Apply, restart Modem.

Gambar 3.7 Konfigurasi Modem ADSL

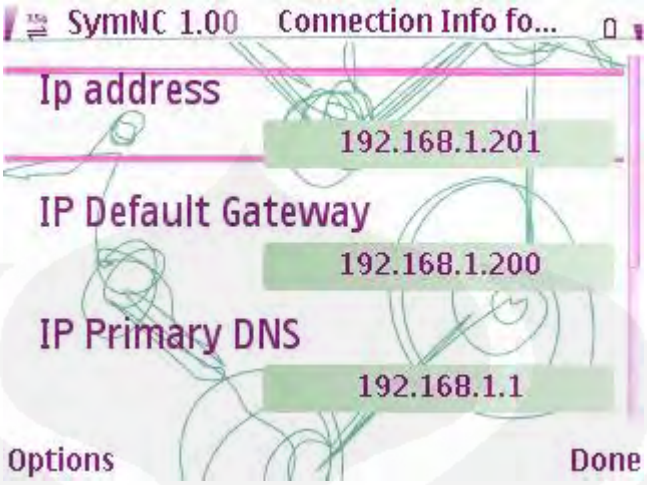
3.3.2.2 Konfigurasi Klien

Konfigurasi pada klien yaitu konfigurasi pada Ponsel.Yang dikonfigurasi adalah perangkat lunak SymNC.Ada beberapa langkah untuk pengkonfigurasiaan SymNC sebagai klien VPN

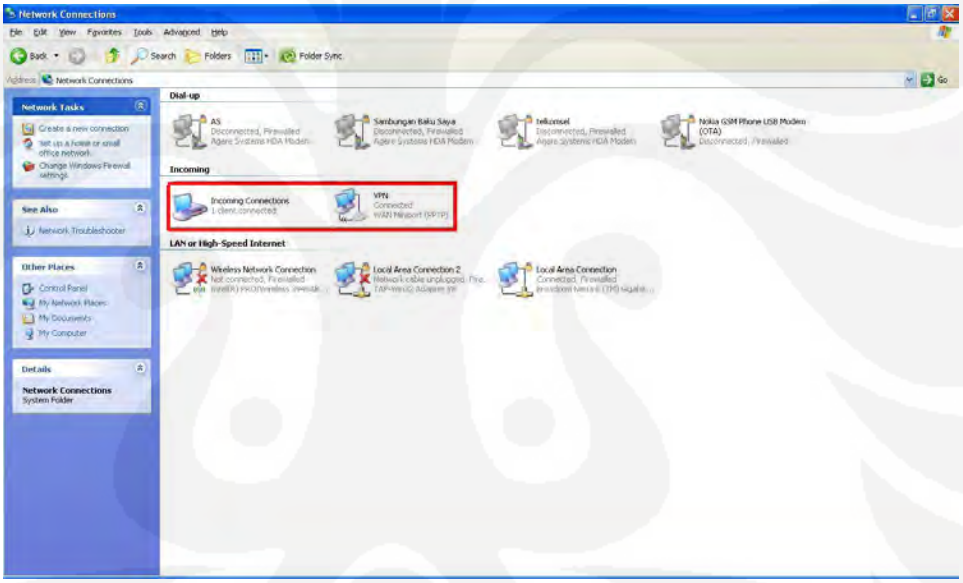
1. Klik ikon SymNC pada Ponsel ⟶ Settings.

2. Langkah berikutnya adalah kita membuat Accounts dimana Accounts tersebut adalah merupakan Accounts yang akan digunakan untuk autentikasi sebagai user yang diijinkan untuk berkomunikasi dengan server VPN.Oleh karena itu, Accounts yang akan dibuat harus sama dengan Accounts yang dibuat pada saat pengkonfigurasiaan Server VPN.Account nya adalah dengan username VPN dan password nya elektro.

3. Setelah selesai membuat accounts, berikutnya adalah membuat access point yaitu dengan memilih ikon PPTP VPN.Access point ini dibuat untuk sebagai jalur data VPN.setelah memilih ikon PPTP pilih options lalu add new.Terdapat beberapa kolom yang harus diisi.Pada kolom name diisi PPTP, lalu Access point diisi yang merupakan operator yang digunakan pada ponsel yaitu Telkomsel.Untuk kolom host merupakan alamat IP Public dari server yaitu 125.160.142.174.Sedangkan kolom terakhir yaitu kolom Account diisi sama dengan Accounts yang dibuat sebelumnya yaitu VPN, lalu pilih Done.Akan meuncul ikon PPTP yang tadi kita buat.Selanjutnya kita test koneksi tersebut dengan memilih options lalu verify.Tunggu beberapa saat, setelah berhasil akan muncul notifikasi seperti gambar 3.7 Berikut.Pada server juga terdapat ikon baru pada jendela Network Connections seperti pada gambar 3.8 itu artinya Acces Point VPN sudah berhasil dikonfigurasi.



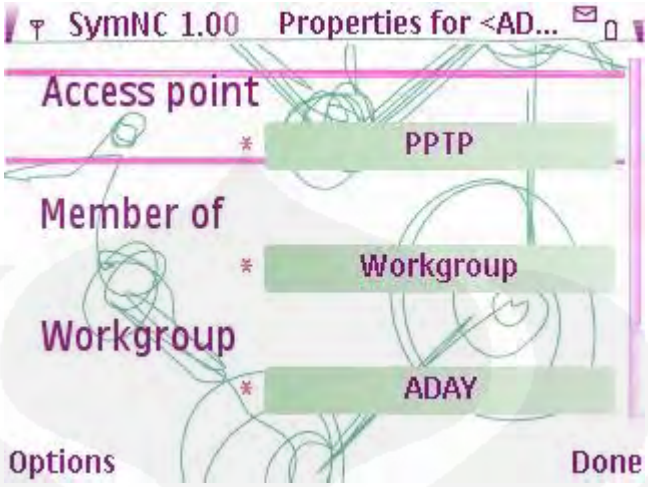
Gambar 3.8 Notifikasi Keberhasilan Test Koneksi VPN



Gambar 3.9 Sambungan VPN PPTP

4. Langkah berikutnya adalah mengkonfigurasi NAS.NAS dikonfigurasi agar server bisa mengakses folder yang di share dan terdapat pada ponsel.Untuk memulai konfigurasi pertama klik ikon NAS.Lalu pilih Network jack.Terdapat form yang akan diisi seperti pada gambar 3.10

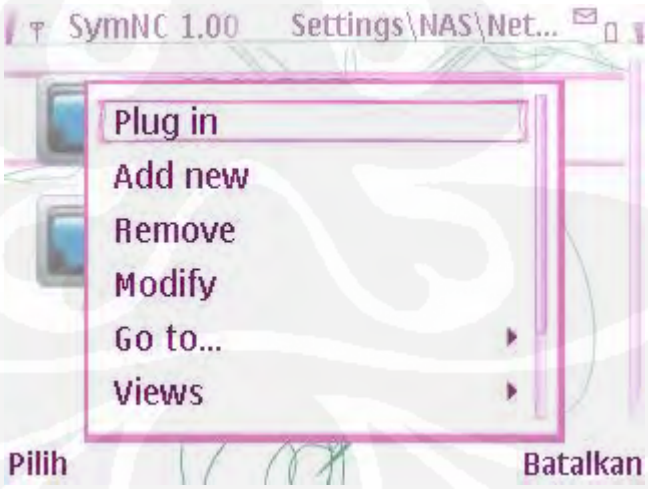
5.



Gambar 3.10 Form Konfigurasi NAS

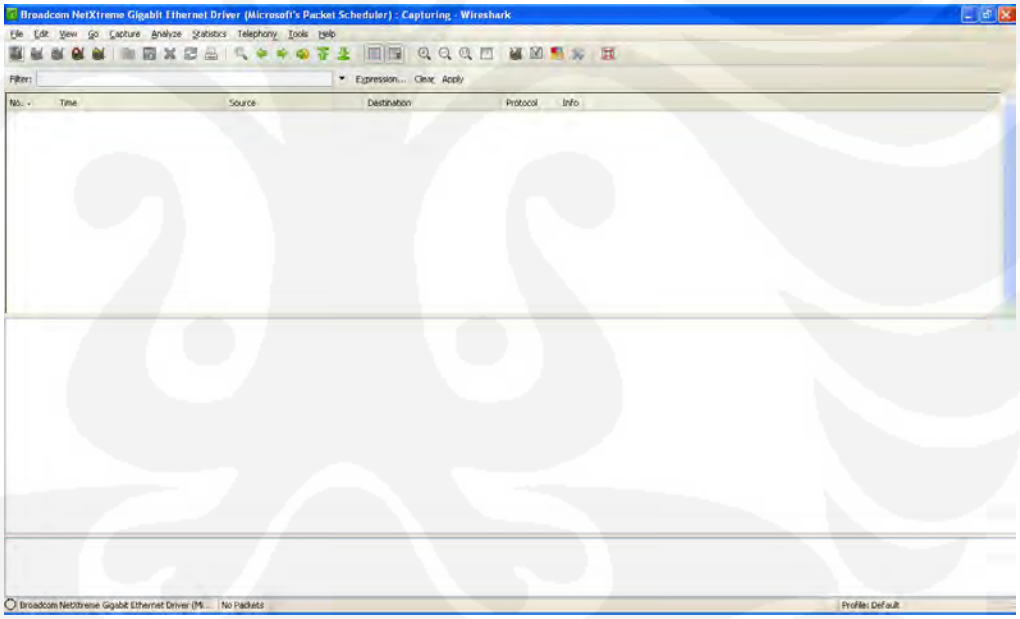
Pada bagian Acces Point, diisi PPTP sama dengan nama yang dibuat pada saat membuat Access point.Lalu pada bagian Member of dan Workgroup disesuaikan dengan server yaitu Workgroup dan nama workgroupnya yaitu ADAY

Setelah selesai mengisi form yang ada, lalu kita bisa memulai untuk menyambungkan Klien dengan server seperti gambar 3.11 dan 3.12

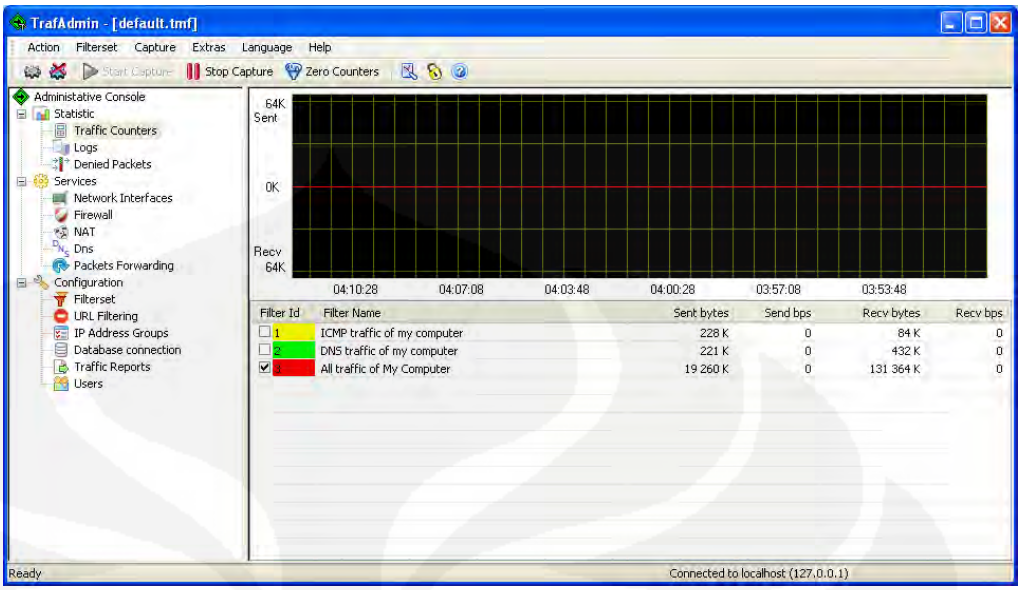


Gambar 3.11 Memulai koneksi ke server

Gambar 3.12 Koneksi Klien dengan Server



Gambar 3.13 Wireshark Versi 1.2.4



Gambar 3.14 Trafmeter versi 9.3

BAB IV

ANALISA HASIL UJICOBA

Pada Bab ini akan dilakukan analisa dan perbandingan terhadap hasil pengujian dari Mobile VPN yaitu Jaringan 3G menggunakan Protokol PPTP dan ketika hanya menggunakan Jaringan 3G saja, dimana parameter yang akan dibahas adalah dari sisi performansi yaitu throughput dan waktu transfer yang dibutuhkan untuk mengirimkan suatu paket dari Klien ke Server maupun sebaliknya dari Server ke Klien.

Throughput merupakan banyaknya bit yang diterima pada suatu node per satuan waktu.sedangkan waktu transfer adalah waktu yang dibutuhkan untuk mengirimkan suatu data dari satu node ke node yang lain.

Pengambilan data dilakukan pada saat klien yang berupa Ponsel melakukan hubungan dengan server VPN yaitu sebuah Laptop.Paket yang dikirimkan berupa Gambar dengan format JPEG dengan ukuran 1024 x 768 besarnya 1.11 MB, dan file Suara dengan format MPEG Layer 3 (mp3) berukuran 2.70 MB dengan bitrate 96 kbps.Selanjutnya data yang lewat di tangkap oleh perangkat lunak Wireshark dan Trafmeter dimana nanti akan bisa dilihat Throughput yang dihasilkan ketika menggunakan Mobile VPN dan Throughput yang hanya menggunakan jaringan 3G saja, serta waktu transfer yang dibutuhkan untuk menstransfer suatu file baik dari Klien ke Server maupun dari Server ke Klien.Khusus untuk file suara, pengujian hanya dilakukan dari Klien ke Server dimana filenya terdapat pada Klien dan dimainkan dengan menggunakan perangkat lunak Winamp di Server.

4.1 Analisa Pengukuran dengan data berupa Gambar dari Klien ke Server

Pada pengukuran ini, data yang dilewatkan berupa gambar dengan format JPEG dengan ukuran 1024 x 768 besarnya 1.11 MB.Pengujian dan pengukuran dilakukan sebanyak 5 kali.Pada pengukuran ini, data yang diamati

pada wireshark yaitu data PPP pada pengujian Mobile VPN dan data TCP pada pengujian Jaringan 3G

Tabel 4.1 Data Throughput dari Klien ke Server

NO	Data Pengujian	Throughput (Mbit/sec)	
		Mobile VPN	Jaringan 3G
1	Pengujian 1	0.065	0.277
2	Pengujian 2	0.097	0.276
3	Pengujian 3	0.207	0.297
4	Pengujian 4	0.071	0.245
5	Pengujian 5	0.174	0.197
6	Rata-rata Pengujian	0.122	0.258

Tabel 4.2 Data Waktu Transfer dari Klien ke Server

NO	Data Pengujian	Waktu Transfer (sec)	
		Mobile VPN	Jaringan 3G
1	Pengujian 1	174	37
2	Pengujian 2	117	37
3	Pengujian 3	53	36
4	Pengujian 4	163	42
5	Pengujian 5	63	52
6	Rata-rata Pengujian	114	40.8

Dari hasil pengukuran terlihat bahwa ketika menggunakan Mobile VPN throughput yang dihasilkan selalu lebih lambat bila dibandingkan dengan throughput menggunakan Jaringan 3G. Rata – rata throughput yang didapatkan dari 5 kali pengujian ketika menggunakan Mobile VPN yaitu 0.122 Mbit/sec sedangkan throughput rata – rata dari jaringan 3G yaitu 0.258 Mbit/sec.Ini berarti throughput Jaringan 3G lebih cepat 111.47 % dibandingkan dengan Mobile VPN ketika menstransfer data dari Server ke Klien.

Sedangkan untuk hasil pengukuran dari waktu transfer nya, dari 5 kali pengujian didapatkan rata – rata dari Mobile VPN yaitu 114 detik jauh lebih lambat bila dibandingkan dengan waktu transfer dari Jaringan 3G yaitu 40.8 detik.Ini berarti waktu transfer Jaringan 3G lebih cepat 179.4 % bila dibandingkan denganwaktu transfer Mobile VPN.

4.2 Analisa Pengukuran dengan data berupa Gambar dari Server ke Klien

Pada pengukuran berikutnya masih sama yaitu berupa file gambar format JPEG dengan ukuran 1024 x 768 besarnya 1.11 MB dari Server ke Klien. Pada pengukuran ini, data yang diamati pada wireshark yaitu data PPP pada pengujian Mobile VPN dan data TCP pada pengujian Jaringan 3G.

Tabel 4.3 Data Throughput dari Server ke Klien

NO	Data Pengujian	Throughput (Mbit/sec)	
		Mobile VPN	Jaringan 3G
1	Pengujian 1	0.195	0.188
2	Pengujian 2	0.192	0.174
3	Pengujian 3	0.209	0.208
4	Pengujian 4	0.209	0.202
5	Pengujian 5	0.210	0.191
6	Rata-rata Pengujian	0.203	0.176

Tabel 4.4 Data Waktu Transfer dari Server ke Klien

NO	Data Pengujian	Waktu Transfer (sec)	
		Mobile VPN	Jaringan 3G
1	Pengujian 1	106	110
2	Pengujian 2	107	117
3	Pengujian 3	95	94
4	Pengujian 4	97	95
5	Pengujian 5	94	106
6	Rata-rata Pengujian	99.8	104.4

Hasil yang didapatkan ketika mengirimkan data dari Server ke Klien mendapatkan hasil yang berbeda bila dibandingkan ketika mengirimkan data dari Klien ke Server.Throughput yang dihasilkan ketika mengunakan Mobile VPN selalu lebih cepat bila dibandingkan dengan throughput ketika menggunakan Jaringan 3G walaupun perbedaannya sedikit.Throughput rata – rata yang dihasilkan dari 5 kali pengujian untuk Mobile VPN yaitu 203 Mbit/sec sedangkan ketika menggunakan Jaringan 3G yaitu 0.176 Mbit/sec.Berarti throughput Mobile VPN lebih cepat 15.3 % dibandingkan dengan Jaringan 3G

Begitu juga untuk waktu transfer, ketika menggunakan Mobile VPN lebih cepat bila dibandingkan dengan Jaringan 3G.Data rata – rata yang didapatkan dari 5 kali pengujian untuk Mobile VPN yaitu 99.8 detik sedangkan untuk Jaringan 3G yaitu 104.4 detik.Ini berarti waktu transfer Mobile VPN lebih cepat 4.6 % bila dibandingkan dengan Jringan 3G

4.3 Analisa pengukuran dengan data berupa file suara dari Klien ke Server

Pada pengukuran ini, data yang dilewatkan berupa suara dimana filenya berformat MPEG Layer 3 berukuran 2.70 MB ,bitrate 96 kbps, lama waktu bila diputar pada player musik yaitu 3 menit 56 detik.Filenya terdapat pada Ponsel dan dimainkan pada PC menggunakan perangkat lunak Winamp versi 5.541. Pada pengukuran ini, data yang diamati pada wireshark yaitu data PPP pada pengujian Mobile VPN dan data TCP pada pengujian Jaringan 3G

Tabel 4.5 Data throughput Streaming File Suara

NO	Data Pengujian	Throughput (Mbit/sec)	
		Mobile VPN	Jaringan 3G
1	Pengujian 1	0.048	0.135
2	Pengujian 2	0.098	0.151
3	Pengujian 3	0.178	0.141
4	Pengujian 4	0.197	0.154
5	Pengujian 5	0.150	0.136
6	Rata-rata Pengujian	0.134	0.143

Tabel 4.6 Data Waktu Transfer File Suara

NO	Data Pengujian	Waktu Transfer (sec)	
		Mobile VPN	Jaringan 3G
1	Pengujian 1	886	290
2	Pengujian 2	554	251
3	Pengujian 3	270	169
4	Pengujian 4	253	245
5	Pengujian 5	291	279
6	Rata-rata Pengujian	450.8	246.8

Dari data dihasilkan bahwa ketika menggunakan Mobile VPN rata – rata throughput yang didapatkan yaitu 0.134 Mbit/sec sedangkan ketika menggunakan Jaringan 3G yaitu 0.143 Mbit/sec.Ini berarti throughput menggunakan Jaringan 3G lebih cepat 6.7 % bila dibandingkan dengan Mobile VPN

Sedangkan rata – rata lamanya waktu yang dibutuhkan untuk memutar file suara tersebut dari 5 kali pengujian yaitu 450.8 detik. Sedangkan ketika menggunakan jaringan 3G lamanya waktu yang dibutuhkan yaitu 246.8 detik.

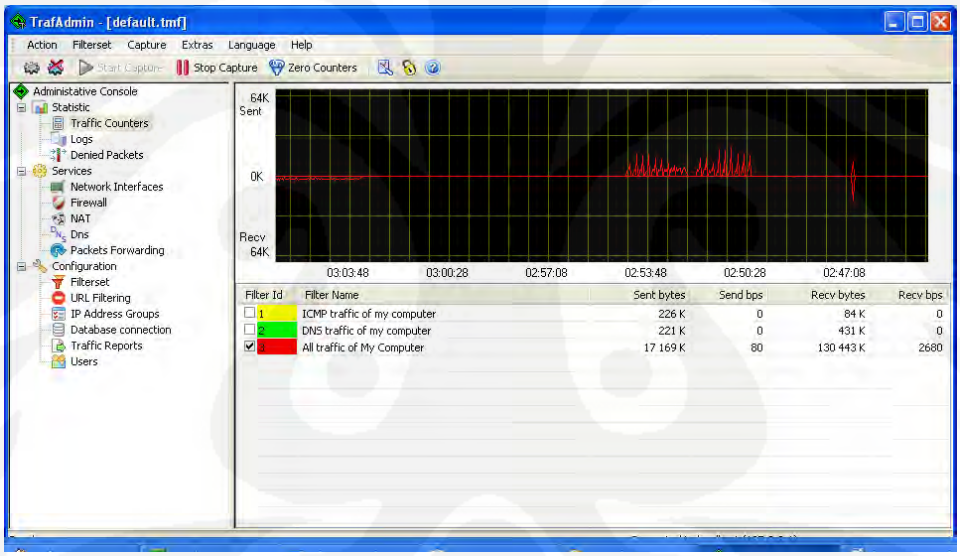
Ketika diputar, suara yang dihasilkan pada pengujian 1, menggunakan Mobile VPN terdengar putus-putus, tidak lengkap sepenuhnya, sedangkan pada saat menggunakan jaringan 3G suara yang terdengar secara utuh tidak putus-putus.Ini disebabkan karena file suara yang digunakan mempunyai bitrate 96 kbps sedangkan pada pengujian 1 menggunakan Mobile VPN didapatkan throughput 48 kbps.Sedangkan pada Jaringan 3G throughput yang didapatkan 136 kbps.

Pada pengujian 2,3,4,dan 5, baik menggunakan Mobile VPN maupun menggunakan Jaringan 3G, suara yang terdengar tidak putus – putus dan terdengan secara utuh ini disebabkan karena throughput yang didapatkan baik Mobile VPN maupun menggunakan Jaringan 3G throughput yang didapatkan lebih besar dari bitrate file suara yang digunakan.

4.4 Hasil pengukuran menggunakan Trafmeter

Pengukuran menggunakan Trafmeter adalah untuk melihat throughput yang didapatkan secara bersamaan pada sisi pengirim maupun penerima.Pada pengukuran ini data yang diambil dari pengukuran pada saat menggunakan Mobile VPN dimana data yang dikirim berupa file gambar format JPEG dengan ukuran 1024 x 768 besarnya 1.11 MB yang dikirim dari PC ke Ponsel maupun sebaliknya dari Ponsel ke PC.

Gambar 4.1 Data hasil pengukuran TrafMeter Dari Server ke Klien



Gambar 4.2 Data hasil pengukuran TrafMeter Dari Klien ke Server

Berdasarkan dari pengukuran Trafmeter terlihat bahwa, ketika mengirimkan data dari Server ke Klien didapat throughput dari sisi pengirim 11416 bps lebih besar bila dibandingkan dengan throughput pada sisi penerima 196.

Sedangkan pada pengukuran berikutnya yaitu dari Klien ke Server justru terjadi sebaliknya, dimana pada sisi pengirim throughput yang dihasilkan 80 bps lebih kecil bila dibandingkan dengan throughput pada sisi penerima 2680 bps.

Ini bisa terjadi karena perbedaan throughput di kedua sisi dimana pada klien jaringan yang digunakan merupakan jaringan dari operator dimana bandwithnya lebih kecil bila dibandingkan dengan jaringan pada Server.

BAB V

KESIMPULAN DAN SARAN

Berdasarkan hasil analisa dan perbandingan yang telah dilakukan, maka dapat diambil kesimpulan bahwa :

1. Pada pengukuran pengiriman data dari Klien ke Server didapatkan bahwa rata – rata Throughput yang dihasilkan ketika menggunakan Mobile VPN yaitu 0.122 Mbit/sec sedangkan dengan jaringan 3G didapatkan Throughput 0.258 Mbit/sec.

   Menggunakan Jaringan 3G dari Klien ke Server,Throughput yang didapatkan lebih besar bila dibandingkan dengan menggunakan Mobile VPN.

2. Pada pengukuran pengiriman data dari Server ke Klien didapatkan bahwa rata – rata Throughput yang dihasilkan ketika menggunakan Mobile VPN yaitu 0.203 Mbit/sec sedangkan dengan jaringan 3G didapatkan Throughput 0.176 Mbit/sec.

   Menggunakan Mobile VPN dari server ke Klien, throughput yang dihasilkan lebih besar bila dibandingkan dengan menggunakan Jaringan 3G.

3. Pada pengukuran pengiriman data dari Klien ke Server didapatkan bahwa rata – rata Waktu Transfer yang dihasilkan ketika menggunakan Mobile VPN yaitu 114 detik sedangkan dengan jaringan 3G didapatkan Waktu transfer 40.8 detik .

   Menggunakan Jaringan 3G dari Klien ke Server,waktu transfer yang didapatkan lebih cepat bila dibandingkan dengan menggunakan Mobile VPN.

4. Pada pengukuran pengiriman data dari Server ke Klien didapatkan bahwa rata – rata Waktu Transfer yang dihasilkan ketika menggunakan Mobile VPN yaitu 99.8 detik sedangkan dengan jaringan 3G didapatkan Waktu transfer 104.4 detik .

   Menggunakan Mobile VPN dari server ke Klien, waktu transfer yang dihasilkan lebih cepat bila dibandingkan dengan menggunakan Jaringan 3G.

5. Pada Hasil pengukuran data menggunakan Trafmeter, dapat dibuktikan bahwa apabila mengirimkan data dari Server ke Klien maka Throughput pada sisi pengirim lebih besar bila dibandingkan dengan sisi penerima.Bila mengirimkan data dari Klien ke Server maka Throughput pada sisi pengirim lebih kecil bila dibandingkan dengan sisi penerima.
6. Untuk mengirim data yang tidak terlalu besar ukurannya (± 1 MB) dari Server ke Klien, lebih efektif menggunakan Protokol VPN karena Throughput yang dihasilkan lebih besar dan Waktu Transfernya lebih cepat bila dibandingkan Jaringan 3G.
7. Untuk mengirim data yang tidak terlalu besar ukurannya (± 1 MB) dari Klien ke Server, lebih efektif menggunakan Jaringan 3G karena Throughput yang dihasilkan lebih besar dan Waktu Transfernya lebih cepat bila dibandingkan Protokol VPN.

Berdasarkan hasil pembuatan dan penulisan skripsi ini maka saran yang dapat diberikan adalah :

1. Selain membandingkan dengan Protokol PPTP dapat juga dibandingkan dengan Protokol VPN yang lain.
2. Selain perbandingan dari sisi Throughput dan Waktu Transfer, dapat juga dibandingkan dari sisi Keamanannya.

DAFTAR ACUAN

[1] Ariyus,Dony.2008.Pengantar Ilmu Kriptografi Teori,Analisis,dan Implementasi.Yogyakarta:Andi Yogyakarta

[2] Thomas,Tom.2005.Network Security First-Step Yogyakarta: Andi Yogyakarta

[3] http://www.ilmukomputer.com

[4] http://www.aventail.com

[5] http://www.arraynetworks.net

[6] http://www.infonetics.com

[7] http://www.sejutablog.com/pengantar-jaringan-komputer-lan/

[8] http://telekomui.org/?p=40

[9] http://ardhiblog.blog.uns.ac.id/2009/07/10/mengenal-teknologi 3g/

[10] Irawan,Budhi.2005. Jaringan Komputer. Yogyakarta : Graha Ilmu

DAFTAR REFERENSI

SymNC 1.00 S60 UserGuide 24 Mei 2009 http://www.symnc.com

Ariyus,Dony.2008.*Pengantar Ilmu Kriptografi Teori,Analisis,dan Implementasi*.Yogyakarta:Andi Yogyakarta

Thomas,Tom.2005.*Network Security First-Step* Yogyakarta. Andi Yogyakarta

Dasar VPN, 27 Nopember 2009 http://www.ilmukomputer.com

PPTP vs L2TP, 19 Oktober 2009 http://www.aventail.com

Network Computer, 17 Oktober 2009 http://www.arraynetworks.net

VPN PPTP, 3 Desember 2009 http://www.infonetics.com

Jaringan Komputer 4 Nopember 2009 http://www.sejutablog.com/pengantar-jaringan-komputer-lan/

Mengenal teknologi 3G,29 Desember 2009 http://ardhiblog.blog.uns.ac.id

Nokia E71 factsheet, 20 Oktober 2009 http://www.nokia.com

DSL-2540T user guide, 12 Oktober 2009 http://www.dlink.co.id

Paper-pptpv2, 16 Agustus 2009 http://www.schneier.com/

SymNC 1.00

User Guide

TABLE OF CONTENTS

1 DOCUMENT INFORMATION

This document is the user guide for the **SymNC 1.00** (S60 3rd & 5th edition) application.

1.1 TERMINOLOGY

Abbreviation	Definition
AP	Access Point
SIS	Symbian OS Installation System
S60	Symbian OS Series 60 platform (3rd or 5th editions)
SymNC	Network Commander for S60 3rd and 5th editions from Telexy Networks Inc. (www.telexy.com)

1.2 REVISION HISTORY

Date	Version	Description
02-Jul-09	0.01	First draft
23-Jul-09	0.10	First full version with all screenshots
25-Sep-09	1.00.044	Corresponds to the build #44
15-Oct-09	1.00.049	Corresponds to the build #49
19-Oct-09	1.00.051	Corresponds to the build #51

2 INTRODUCTION

Telexy **SymNC (Network Commander) 1.00** for S60 (3rd & 5th editions) is an application that brings your phone into real-life computer networking world.

Besides the unique opportunities it brings into Symbian mobile planet, including:

- wirelessly browse computer network (Windows, Mac OS, Linux, UNIX) via standard methods;

- map network shared resources for subsequent instant access (without additional software installation or configuration on the network computer),

- access (open/read/modify) regular files (like text, office files, images, etc.) directly from network;

- control network hosts via shutdown or reboot,

this tool also incorporates the following Telexy networking applications to become reachable from a single place:

- SymSync - easy file synchronization between mobile phones and network computers;

- SymNAS - easy NAS-functionality, that allows sharing phone's folders or drives such that they can be accessed from any computer on network (Windows, Mac OS, Linux, UNIX);

- SymPlayer - easy audio file play back directly from network as well as from local drives;

- SymVPN - PPTP VPN client, that securely connects to your home or corporate network.

- SymRDP – RDP (v.6) client, that allows you to use your S60 phone and connect to a remote computer in a different location (this functionality available ONLY for S60 5th edition phones).

With all these features this application becomes a powerful Network Commander and turns your phone into a fully-functional networking device.

2.1 SUPPORTED PLATFORMS & DEVICES

The application is compatible with the following S60 3rd and 5th edition devices:

- ***Nokia E-Series***: E50, E51, E55, E60, E61, E61i, E62, E63, E63 NAM, E65, E66, E70, E71, E75, E90;
- ***Nokia N-Series***: N73, N76, N77, N78, N79, N80, N80 Internet Edition, N81, N81 8GB, N82, N85, N86, N86 8MP, N91, N91 8GB, N92, N93, N93i, N95, N95 8GB, N95-3 NAM, N96, N97, N97 mini;
- ***Nokia***: 5230, 5530 XpressMusic, 5800 XpressMusic, 5800 Navigation Edition, X6;
- ***Samsung***: G810, i550, i550w, i8510 INNOV8, SGH-i7110, i8910 HD.
- ***Sony Ericson***: Satio(Idou)

It is expected that **SymNC 1.00** will work normally, in general, with any S60 3rd or 5th edition devices with WLAN, 3G or WiMAX support.

2.2 POSSIBLE CHARGES

Connection to and use of the Internet from your cell phone is typically not free. Whether or not you will be charged for using **SymNC 1.00** (namely, for use of Internet via a Data bearer) can be determined from your local service provider.

3 INSTALLATION AND PREPARATION

The **SymNC 1.00** is supplied as a single Symbian OS Installation System (SIS) file. It must be transferred to the phone via any version of SymSync, or through USB cable, memory card, Bluetooth or downloaded from **telexy.com** website directly to you phone. Once transferred, the standard installation process can be applied.

3.1 PRE-REQUISITES

Before installing, ensure that the phone supports any Data bearer (WLAN or 3G is most recommended). Make sure that you are in the range of a bearer through which you are going to connect to Internet (for example WLAN router).

3.2 TRIAL AND REGISTRATION

Telexy Networks offers its products through the following practice. Every product can be used in two stages:

- Trial version is free to download and use. This version is fully functional; however it works only for a limited period of time, starting on the date of installation. The tryout period is long enough to understand whether this product suits your needs or not. Thus, by the expiration date you can decide if you are ready to purchase the product.

- **Final version of a product is fully functional and time-unlimited.** First - a personalized license needs to be purchased on the Telexy website. Then it should be registered on your phone (see section 5.2). These actions legitimize the final version of the product on your device. There is no need to download anything else. Once the license is provided, the trial version becomes fully operational.

Thus, after the first installation the application always finds itself in the trial version state.

4 USING THE TOOL

The basic usage of the system is described in this chapter with corresponding screenshots.

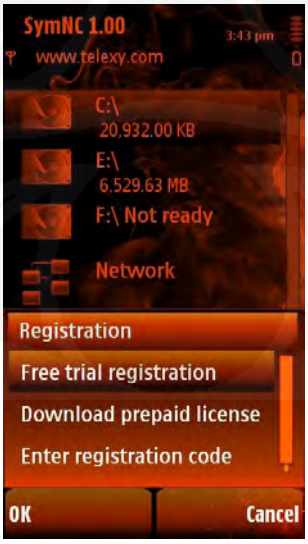
4.1 HOW TO LAUNCH

The tool is launched from the phone's application list by selecting "**SymNC**" icon.

SymNC 1.00 icon can be placed in different application folders on different devices. Usually, it could be "Applications" or "Installed" folder. Please, refer to your phone's manual for more details.

4.1.1 First launch of Trial version

First launch of trial version of the application always causes the "Product registration required!" dialog to appear – in order to use the application in free trial mode you have to go through a simple registration procedure. During this procedure SymNC 1.00 will connect to www.telexy.com and download a trial license for your phone. Thus, select "Register" > "Free trial registration" > <Appropriate access point> in sequence.



When the license is downloaded, select the "Register" option and complete the registration process by pressing "Ok" soft-key.

Right after the trial registration the "End User License Agreement" dialog will appear. Please, read it carefully and indicate your decision by pressing "Accept" or "Decline" button. "Decline" leads to the application closure. "Accept" means that you agree with EULA and therefore can use the application.

4.1.2 Regular appearance

Next application's screen is just a reminder that the current version is a try-out; therefore it will appear on every launch (with number of days decreasing) until trial license expiration or legal registration. Use the "Try" button to enter the application's main page.

4.2 HOW TO USE

4.2.1 Application's main screen overview

The main screen in SymNC application includes the following entries:

- system drives (local and network);

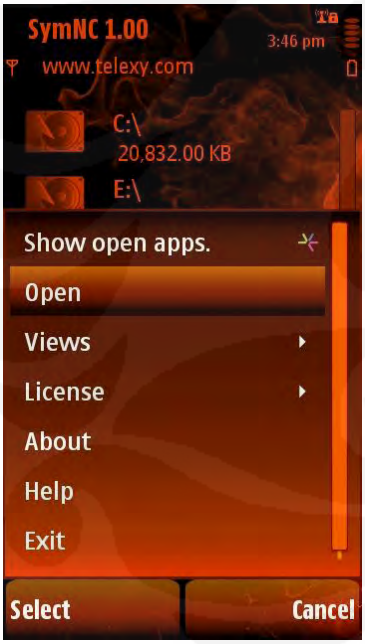
- "Network" - allows browsing the network;

- "RDP Links" – list of pre-arranged RDP session descriptors (this feature available ONLY for S60 5th edition phones);

- "Settings" - allows configuring, viewing and managing the Network Commander setup and the phone's network environment by providing access to the aforementioned Telexy networking applications;

At any data presentation level (from the main application view down to drive-level view or "Settings" view and further), the following menu commands are available:

- "Open" - goes to lower layer (rocker's "Enter" is a shortcut);



- "Go to..." - submenu returns to the Root (main window) of SymNC 1.00 from anywhere below;

- "Views" - switches application views (see 4.2.1.1);

- "Help" - provides help description for a current context;

Additional menu options in the SymNC 1.00 main window are:

- "About" - standard "About" information;

- "License" - groups license-related operations:

  - "Register" - downloads the purchased license to phone and registers it or receives a license via "Registration Code" (not available once the phone is registered);

  - "Properties" - displays registered license content.

  - "Buy" – redirects to the developer site where the license can be purchased (not available once the phone is registered);

Navigating up and down the folders/items inside SymNC can be done quickly using the rocker shortcuts "Right" (open/down) or "Left" (up/back).

4.2.1.1 Application's views

SymNC has two views (called "Left" and "Right") in the main application. These are useful when working with two different folders (for example, folders located on two different drives, be it local or network), such as when manually copying or moving files. The third view - "Music Player" - is a Telexy Music Player view (see here for more details).

Submenu "Views..." groups all the commands for switching views ("Music Player" can be used as long as the "Play music" command has been once used);

4.2.1.2 "Volume" submenu

Depending on whether music is playing at the moment or not optional "Volume" submenu may become available. This submenu provides the following volume control options:

- "Up" – increases volume on 10%;
- "Down" – decreases volume on 10%;
- "Quiet" – sets volume to minimal;
- "Medium" – sets average volume;
- "Loud" – sets maximum volume;

Besides these methods for volume control also can be fulfilled with a step of 10%:

- through the standard "Volume Up" and "Volume Down" keys;
- via "Up" and "Down" rocker's keys;

4.2.2 System drives

The list of System Drives presented on the main application window includes local phone drives as well as network drives mapped using SymNC (see 4.2.5.2 for more details).

4.2.2.1 Local and Network drives

Local and network drives have different icons. The second line in the drives presentations displays:

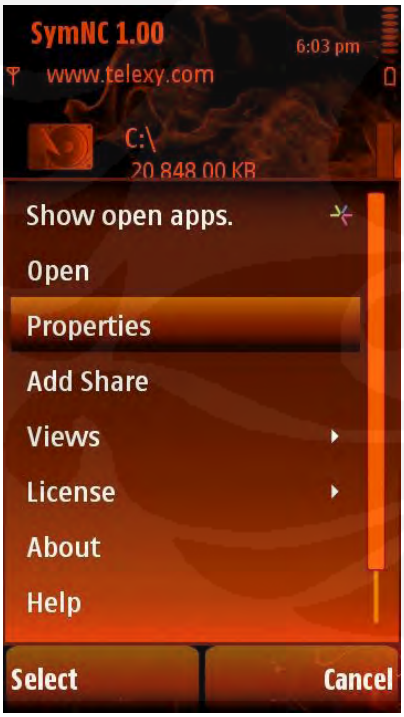
- the free space available for the Local Drive;

- the full path to the mapped location for the mapped Network Drive.

If a local drive is defined as a Share by NAS application (for more details see SymNAS User Guide), a special share symbol appears on its icon.

A network drive can be enabled or disabled (see 4.2.5.2.2). Only enabled network drives appear in the system drives section.

4.2.2.2 System drives menu options



Additional menu option for a system drive is:

- "Properties" - displays this drive's properties.

For local drives, the following commands are possible depending on its state (not shared/shared):

- "Add share" - opens a dialog to create new NAS-Share and user's permission for it where fields' values are preset by the context (see SymNAS User Guide for more details);

- "Remove share" - opens a dialog to cancel sharing at the corresponding location.

4.2.2.3 Drive's properties

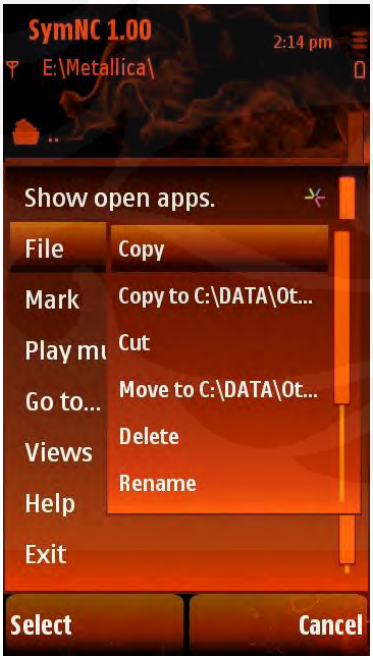
A drive properties form contains the following fields:

- "Name";
- "Size";
- "Free space";

4.2.3 Drives' File System content

Inside System Drives (local or mapped) or inside a Share available through the "Network" (see 4.2.4.3 for more details), the following menu commands are presented:

4.2.3.1 Submenu "Files"



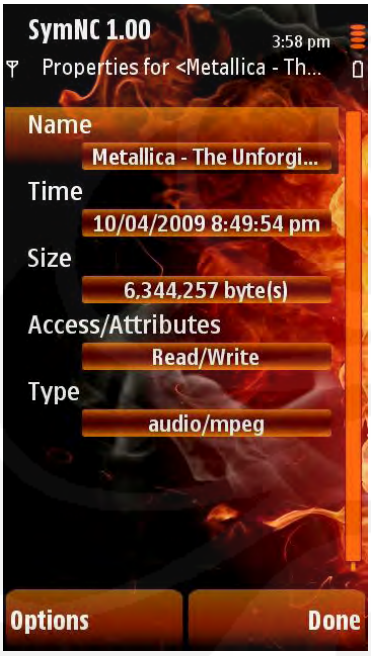
File/folder operations are grouped in the submenu "Files". The following operations are available:

- "Copy" - marks the selected item(s) which can be later inserted using "Files > Paste";
- "Copy To ..." – copies the selected files to a folder that is focused in an opposite view. This command is available ONLY if the folder in the opposite view is a valid file-system folder;
- "Cut" - marks the selected item(s) in order to be later moved using "Files > Paste"
- "Move To ..." – moves the selected files to a folder that is focused in an opposite view. This command is available ONLY if the folder in the opposite view is a valid file-system folder;
- "Paste" - inserts previously marked item(s), into the current folder. This command is only available after "Cut" or "Copy";
- "Delete" - deletes the selected item(s) after a confirmation;

- "Rename" - renames the current item;

- "New folder" - creates a folder with the specified title;

- "Launch" - executes/opens the current file (audio, text, office files, images, installation, etc.) as soon as appropriate application is installed on phone; I.e. if this is a music file then it launches the music player; if this is a LOCAL video file then the video player is launched (VIDEO PLAYBACK IS NOT SUPPORTED FOR NETWORK DRIVES OR SHARES). The same operation is performed using the "Select" button or pressing the rocker.



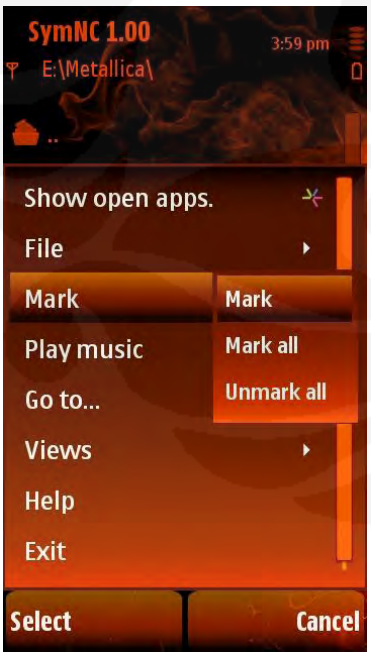
- "Properties" - description of the file/folder attributes;

4.2.3.2 File/folder properties

"File/Folder properties" form displays the properties of the current file or folder. It contains the standard fields:

- "Name";
- "Time" (modification);
- "Size";
- "Access/Attributes";
- "Type";

4.2.3.3 Submenu "Mark"

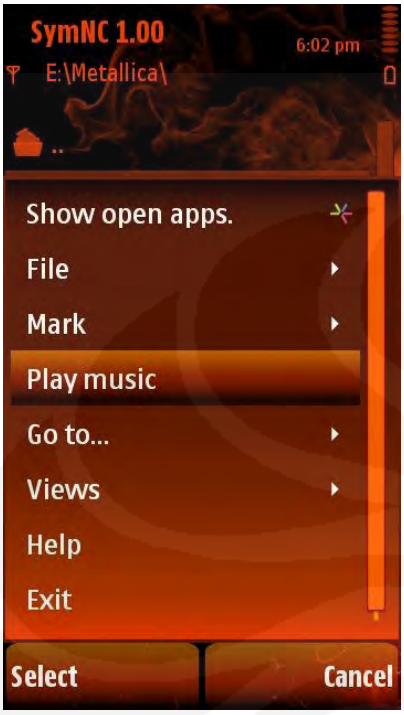


Mark/Unmark operations are grouped in the submenu "Mark". The following operations are available:

- "Mark" - marks the current item;
- "Unmark" - unmarks the current item;
- "Mark all" - marks all files in the current folder;
- "Unmark all" - unmarks all marked files in the current folder;

If some files or folders in the current folder are marked then the file operation is applied to the group (if applicable).

4.2.3.4 "Play music" command

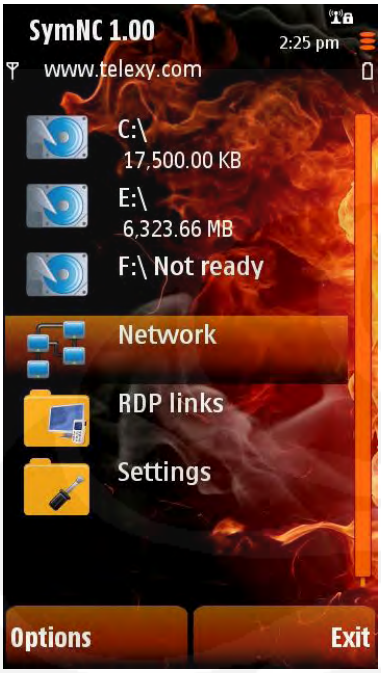


"Play music" command starts playback for the current item (file or folder with music files) via Telexy Music Player (see here for more detail).

4.2.3.5 Search feature

Search feature allows a user to filter only those files or folders that correspond to a search criterion: just start to type the name of the item you interested in and Drives view will reflect only corresponding items.

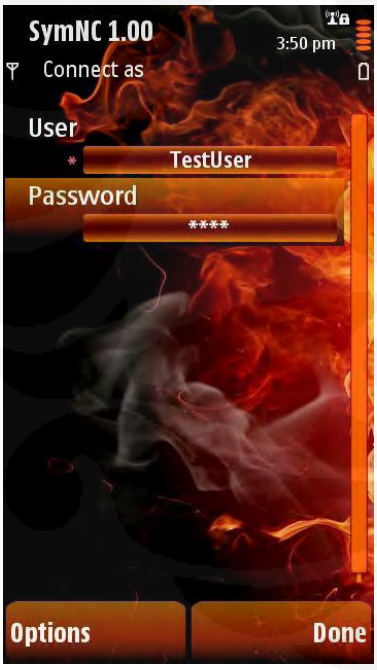
4.2.4 Network Browsing



Entering the "Network" folder results in displaying the list of Internet Access Points registered on the phone.

To begin browsing the network using the desired Access Point, navigate to it and use the "Open" menu option, press the rocker or use rocker's "Right" button.

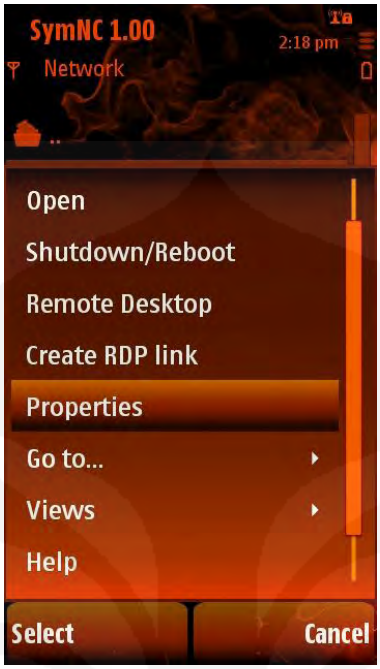
4.2.4.1 Login procedure



If **SymNC** is the only application from Telexy Networks, Inc., installed on your phone, then upon the first network browsing attempt, the system may request the name and password of the account you use to login into the selected network. If the login succeeds, the information entered for the login will be saved in the "Accounts" list automatically (see section 4.2.5.1). Subsequently, the system will use the saved accounts when logging into a network. The system will request the parameters for creating a new account only if none of the existing accounts match the current environment.

4.2.4.2 Network computers

A successful result of entering an Access Point is a list that displays the computer's names which are available over the network using this AP (the Access Point is specified in the window's header).



To view the shared resources of this computer navigate to it and use the "Open" menu option, press the rocker or use rocker's "Right" button.

If you have sufficient permissions to access this computer, you will be permitted entry.

If you do not have sufficient permission you will see an "Access denied" message.

Additional menu options for network hosts are:

- "Properties" - displays the properties of this network computer (see 4.2.4.2.1)

- "Shutdown/Reboot" - allows shutting down or rebooting the selected host (see 4.2.4.2.2).

4.2.4.2.1 Network Drive Properties

"Properties" menu option displays the properties of selected network computer. The form contains the following fields:

- "Name";
- "IP address";

If the computer has multiple IP addresses, all of them will be listed. But only first address will be used by SymNC to access that computer.

4.2.4.2.2 Network host shutdown/reboot control

To initiate shutdown\reboot of the host, the form with the following fields need to be completed:

- "Server name" - automatically preset by the context;

- "Message" - the message would be displayed on the host's screen during shutdown (shutdown/reboot reason);

- "Timeout" - timeout before the action on the host (in seconds);

- "Force application close" - "Yes/No" toggle field ("No" by default);

- "Reboot/Shutdown " - an action mode: "Reboot"/ "Shutdown" toggle field.

4.2.4.3 Network shares

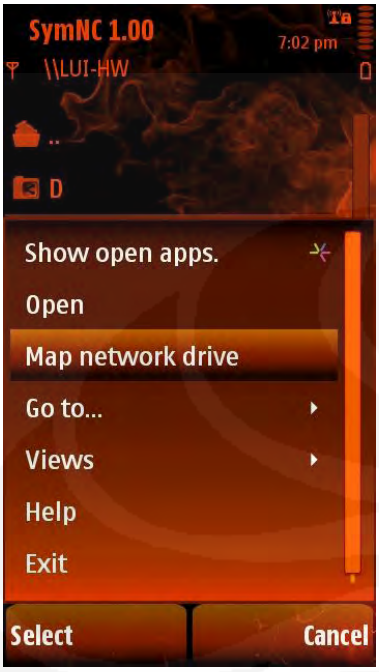
Entering a selected network computer from the computer register (see 4.2.4.2) results into the list of shares defined on this computer (the the network computer is specified in the window's header).

If this Share is already registered in **SymNC 1.00** as a "Network Drive" (see 4.2.4.3.2), this will be marked by a special icon.

To enter the desired Share, navigate to it and use the "Open" menu option, press the rocker or use rocker's "Right" button.

If you have sufficient permissions to access this Share, you will be permitted entry. If you do not have sufficient permission you will see an "Access denied" message.

4.2.4.3.1 Network Share's menu options

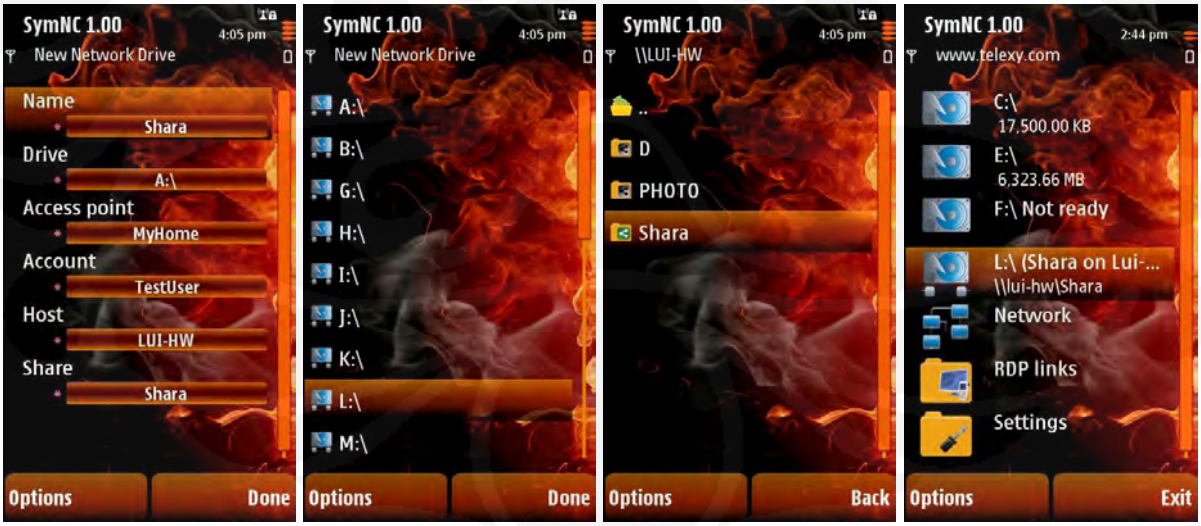


Depending on the state of the network Share (not mapped/mapped) the following additional menu commands are available:

- "Map network drive" – opens the form for creating "Network Drive" entry with values preset by the context (see section 4.2.4.3.2);
- "Disconnect network drive" - opens a request dialog for deletion of the corresponding "Network Drive.

4.2.4.3.2 Network Drive mapping operation

If you use "Map network drive" command, a form describing new Network Drive pre-filled with context values will appear for this share. The only values that can be changed are the drive letter and possibly the "Name" field. As a result, "Settings/Network Drives" will have a record added for this network location. You are able now to access it from "System drives" section just as you would for a local drive.



4.2.4.3.3 Network Share file operations

Inside the Share available through the "Network" the menu commands are almost the same as for System Drives (see section 4.2.3).

4.2.5 "Settings" folder

In addition to configuring **SymNC 1.00** while browsing local drives ("Add Share"/"Remove Share" (see section 4.2.2.2)) and "Network" ("Map network drive"/"Disconnect network drive" (see sections 4.2.4.3.2); automatic user account creation (see section 4.2.4.1)), the network environment can be configured using the "Settings" folder. It consists of five sections:

1) The "Accounts" section contains the user account information that is used to ensure secure access to shared local or network locations.
2) "Network drives" section lists external network locations which can be accessed from this phone.
3) Entry to SymSync configuration;
4) Entry to SymNAS configuration;
5) Entry to SymVPN configuration.

Here only "Accounts" and "Network Folders" sections will be described. To get more details on SymSync, SymNAS and SymVPN – see the corresponding User Guids by links marked above.

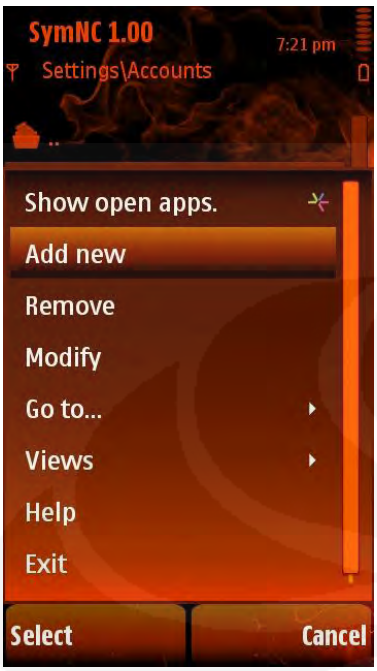
4.2.5.1 "Accounts" section overview.

The "Accounts" section contains the Telexy-specific user account information that is used to ensure secure access between a phone and computer networks (including VPN).

For the case of giving access permissions for the phone to be accessed from a network computer, this register includes the accounts for users that can access the phone's shares (as defined by some Telexy product) from network computers or other phones. For the case of access in the opposite direction (from phone to network computer or VPN), the information to be used to access network locations or VPN networks is listed.

Standard network (or VPN) authentication methods are used to ensure secure access.

The content of this register is your own secret information. Do not share it with others.

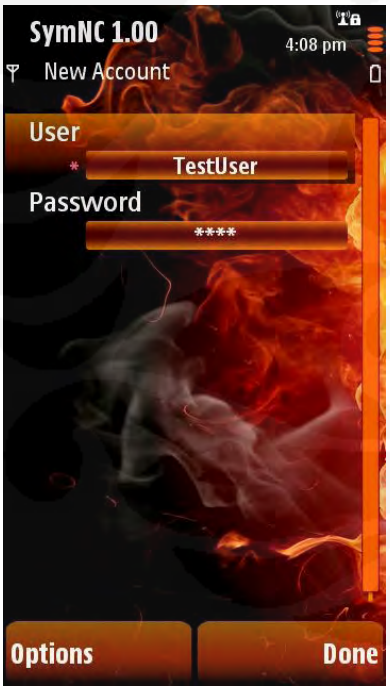


The register can include (if applicable) a pre-defined account "Everyone" that is used by default to assign permissions for local (phones) shares.

The following operations are available in the "Option" menu:

- "Add new" – creates new account (see 4.2.5.1.1);
- "Modify" – edits existing account (see 4.2.5.1.1);
- "Remove" – delete existing account.

4.2.5.1.1 Account creation/editing form.



Accounts are described using the following 2 fields:

1) Username:

- a login name for the person that will access the phone's shares from the computer

OR

- a login name for the person that has permissions to access the network computer or VPN;

2) Password - corresponding password for the username field above;

IMPORTANT: Depending on authentication method of your network extended username format might be required.

The extended username format is:

<**Domain**>\<**Username**>

For example: **telexy\guest**

DOMAIN: A collection of computers on a network that share a common database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.

4.2.5.2 Mapped Network Drives

Network drives section lists external network locations which can be accessed from this phone.

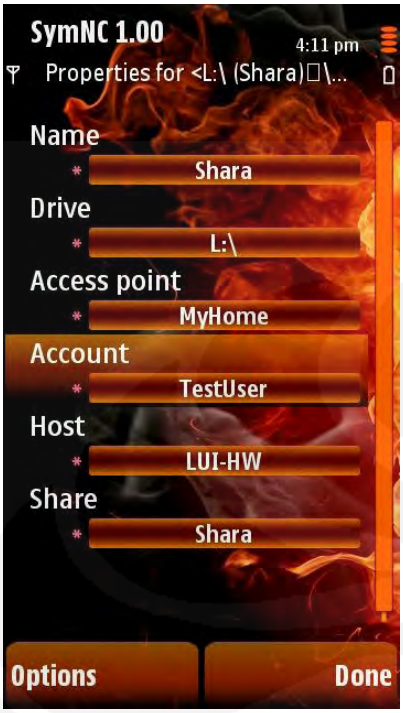
After the new network drive is specified it appears in the "System Drives" section and is ready to use.

New Network Drive can be created manually via "Add New" command. But we recommend using the procedure described in 4.2.4.3.2.

All operation available on Network Drives explained in 4.2.5.2.2.

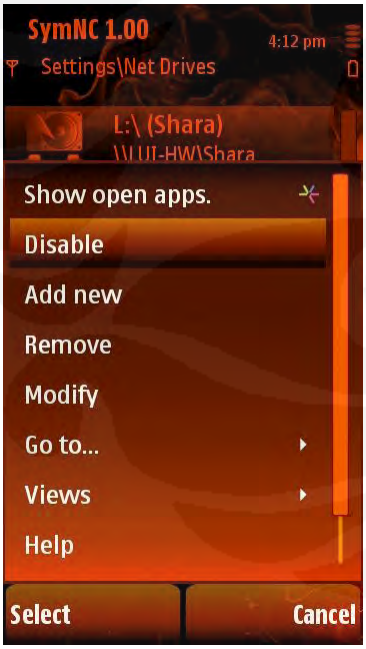
4.2.5.2.1 Network drive properties

Each network location is described using:



- "Name" – short name the user gives to the network location;
- "Drive" – letter for the drive to be used to access;
- "Access point" – access point used to access the network location;
- "Account" – link to the "Accounts" table entry which will be used to access the network location;
- "Host" – URL or IP address of the network computer which hosts the location;
- "Share" – network shared folder name.

4.2.5.2.2 "Network Drives" Menu options



You can disable the Network Drive using the "Disable" command if for some reason it should not be displayed on "System Drives" section. You can later revert this action, using the "Enable" command. The state of "Enabled/Disabled" displays different icons.

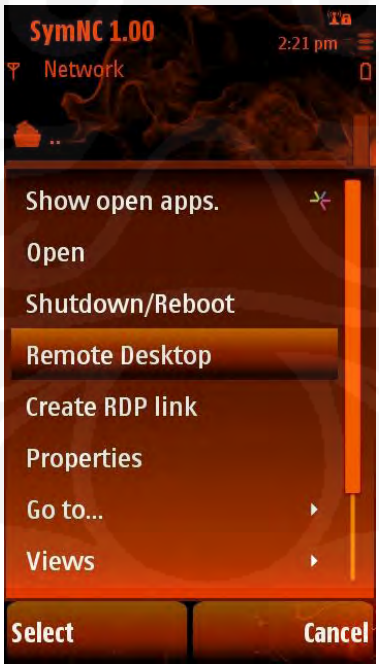
4.2.6 RDP functionality (ONLY for S60 5th edition phones)

This feature available ONLY on S60 5th edition devices!

4.2.6.1 "RDP Links" folder

This folder represents an entry to SymRDP configuration. To get more details on SymRDP – see the referenced User Guide by links marked above.

4.2.6.2 RDP-related menu "Options" for network workstations



If RDP feature is supported for your phone, the additional menu options for network hosts are available:

- "Remote Desktop" - creates an RDP session for the selected network computer;

- "Create RDP Link" - opens the form for creating an RDP link to the selected network computer with values preset for current context. The link will be created and placed in the "RDP Links" folder.

See more details in the SymRDP User Guide.

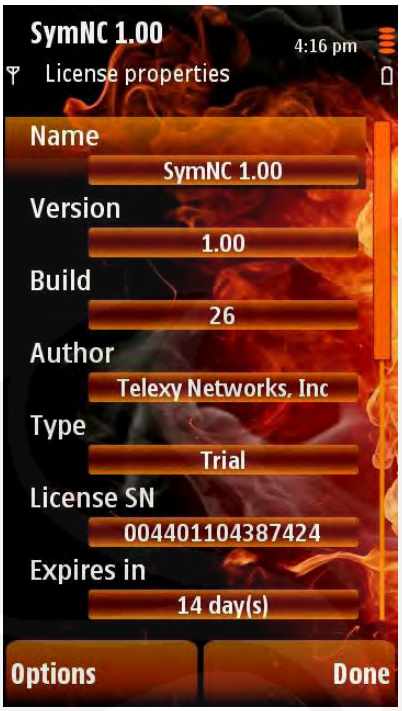
5 LICENSING AND REGISTRATION

As you might remember from the section 3.2 **SymNC 1.00** can be either in "TRIAL" or in "Registered" state.

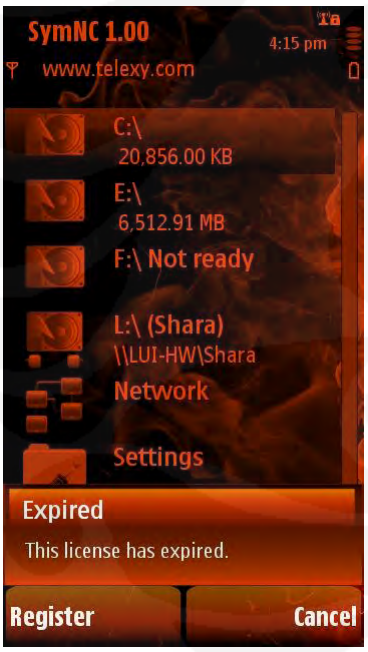
5.1 TRIAL LICENSE

While the application is in "Trial" state, every launch would cause "TRIAL" warning (see section 4.1.2).

At any moment you can check the application license from the root application page via "Menu\Licence\Property". You can find that the type of the licence is "Trial", it is issued to your phone (check the SN), what are the activation and expiration dates. At any moment you can check the EULA.



5.2 HOW TO REGISTER



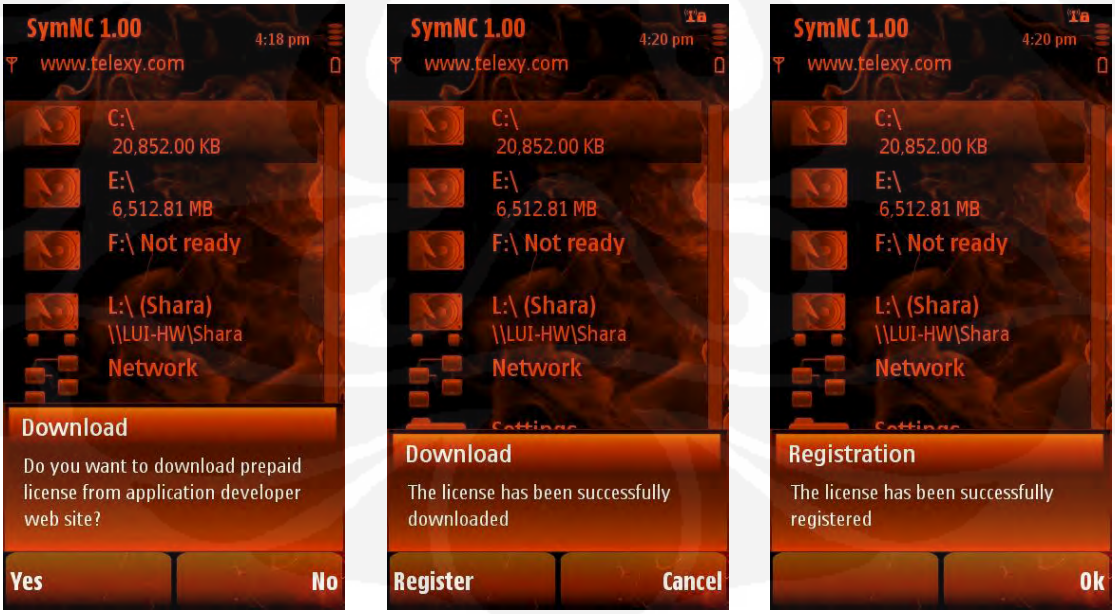
Sooner or later you will face a point when you have to decide whether this application is worth buying. If it is, you have to legalize it on your phone. Of course, you can wait to the uttermost – trial licence expiration but in this situation the only option that remains will be "Register".

Thus, how to register our product? Select "Register" option and then choose "Download prepaid license" command. You will be asked about a licence acquisition first. If you haven't bought a licence yet ("No"), the application instructs you what to do in order to register.

So, you have to go to our web-site www.telexy.com and buy a full licence.

5.3 FINALIZING REGISTRATION

When a licence has been bought, you can finalize the registration process on your phone. Select "Register" and "Download prepaid license" options again and agree to "download" and "register" the license in the following two dialogs.



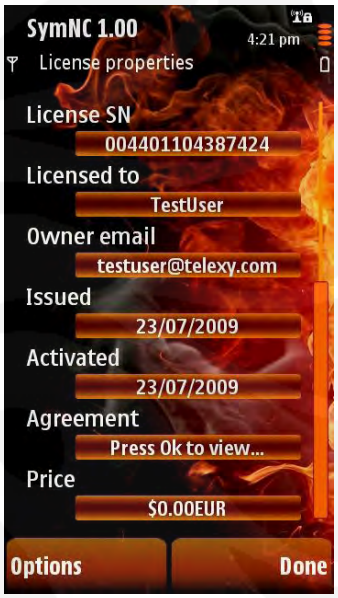
Successful registration will be indicated. Press "Ok" to finish.

5.4 REGISTERED STATUS RESTORATION

It is worthy to note that if a license has once been bought, it is always available for re-registration. Let's say, if for some reason SymNC was re-installed then it will appear in the Trial state. However, it is enough to repeat the registration procedure from section 5.3 to restore the registered status.

5.5 LEGAL LICENSE

You can view the downloaded licence, selecting the "Menu\Licence\Property". New licence is personalized. It also has "Production" type, a proper Serial number and appropriate dates and price fields.



6 UNINSTALL SPECIFICITY (WHAT'S NEEDED TO KNOW WHEN UNINSTALLING SYMNC OR ANY OTHER TELEXY-PRODUCT)

The previous release of Telexy products (July 2009) was based on an approach that is described here. We thought that it is normal that people sometimes will see this quite harmless warning "***Component ... missing. Continue?***" because:

1) It is normal indeed according to Symbian documentation (see the link above for details);

2) It is just a warning that has a part "...Continue?" allowing you to ignore it and proceed with an installation.

However, we met a situation that this warning created a lot of confusion among our customers. And we got feeling that some of them became so confused that they stopped using Telexy products because of that.

Thus, in order to avoid this situation we decided to change Telexy products installation practice and come to a more smooth installation procedure. Now with new Telexy release (starting from October 2009) that warning message will not appear anymore.

On the other hand, this improvement has a cost, since now there is a side effect: if you have several Telexy products installed on your phone and uninstall one of them, sometimes there could be a problem after uninstallation.

For example, you have two Telexy products A and B. A was installed first and then B. Two situations are possible:

1) You decided to uninstall the product B. In this case everything will go normally without problem; Remaining product A is still operational;

2) You decided to uninstall the product A - this is a problematic case. After un-installation of product A, product B becomes out of order and has to be re-installed to resolve the situation.

We are sorry for any inconveniences in advance.

7 CONCLUSION

We are continually trying to improve SymNC. If you have any suggestions that could make the product better in any way, please address them to our business department and we will add your comments to our To Do list.

Please share your opinion, remarks, compatibility issues, possible problems, etc. with us on our forum: http://forum.telexy.com/. Should you have any problem, please feel free to contact our 24/7/365 Customer Support Team.

We hope that this software is of value to you and that it makes your networking requirements simpler and easier to use.

NOKIA
Connecting People

Nokia E71

Smart simplicity

Optimise your e-mail experience with the Nokia E71; built to keep your work and free time as integrated or separate as you like with customisable business and personal modes. Improve efficiency with greater portability, one-touch keys and go places with built-in A-GPS and Nokia Maps.

Features at a glance

- Fast, easy access to messaging, including your business and personal email, without the complexity.
- Trim and fitted with a full keyboard, Nokia E71 is impeccably tailored for business on the move.
- Two home screens let you choose between work and leisure modes. choose application shortcuts to suit your schedule with message notifications on or off.

Size
- Form: Monoblock with full keyboard
- Dimensions: 114 x 57 x 10 mm
- Weight: 127 g (with battery)
- Volume: 66 cc
- Full keyboard
- High quality QVGA display

Display and 3D
- Size: 2.36"
- Resolution: 320 x 240 pixels (QVGA)
- Up to 16 million colours
- TFT active matrix (QVGA)
- Two customisable home screen modes

Email
- Easy email set-up
- Support for Active Sync for Microsoft Exchange via Mail for Exchange
- Supported protocols: IMAP4, Microsoft ActiveSync, POP3, SMTP
- Support for email attachments
- IMAP IDLE support
- Support for Nokia Intellisync Wireless Email
- Integrated Nokia Mobile VPN

Keys and input methods
- Full keyboard
- Dedicated one-touch keys: Home, calendar, contacts, and email
- Speaker dependent and speaker independent voice dialling
- Intelligent input with auto-completion, auto-correction, auto-punctuation, and learning capability
- Accelerated scrolling with Navi™Key
- Notification light in Navi™Key

Colours and covers
- Available in-box colours
- Grey steel
- White steel

Connectors
- Micro-USB connector, full-speed
- 2.5 mm Nokia AV connector

Power
- BP-4L 1500 mAh Li-Po standard battery
- Talk time: GSM up to 10 h 30 min, WCDMA up to 4 h 30 min
- Standby time: GSM up to 17 days, WCDMA up to 20 days, WLAN idle up to 166 hours
- Music playback time (maximum): 18 h

*Operation times vary depending on the network and usage

Memory
- microSD memory card slot, hot swappable, max. 8 GB
- Approximately 110 MB internal dynamic memory

Operating frequency
- E71-1 Quad-band EGSM 850/900/1800/1900, WCDMA 900/2100 HSDPA
- E71-2 Quad-band EGSM 850/900/1800/1900, WCDMA 850/1900 HSDPA
- E71-3 Quad-band EGSM 850/900/1800/1900, WCDMA 850/2100 HSDPA
- Offline mode

Data network
- CSD
- HSCSD
- GPRS class A, multislot class 32, maximum speed 100/60 kbps (DL/UL)
- EDGE class A, multislot class 32, maximum speed 296/177.6 kbps (DL/UL)
- WCDMA 900/2100 or 850/1900 or 850/2100, maximum speed 384/384 kbps (DL/UL)
- HSDPA class 6, maximum speed 3.6 Mbps/384 kbps (DL/UL)
- WLAN IEEE 802.11b/g
- WLAN Security: WEP, 802.1X, WPA, WPA2
- TCP/IP support
- Nokia PC Internet Access (capability to serve as a data modem)
- IETF SIP and 3GPP

Local connectivity and synchronisation
- Infrared, maximum speed 115 kbps
- Bluetooth version 2.0 with Enhanced Data Rate
  - Bluetooth profiles: DUN, OPP, FTP, HFP, GOEP, HSP, BIP, RSAP, GAVDP, AVRCP, A2DP
- MTP (Multimedia Transfer Protocol) support
- Bluetooth (Bluetooth Serial Port Profile. BT SPP)
- Infrared
- File
- Network (Raw). Direct TCP/IP socket connection to any specified port (a.k.a HP JetDirect™)
- Network (LPR). Line Printer Daemon protocol (RFC1179)
- Support for local and remote SyncML synchronisation, iSync, Intellisync, ActiveSync

Call features
- Integrated handsfree speakerphone
- Automatic answer with headset or car kit
- Any key answer
- Call waiting, call hold, call divert
- Call timer
- Logging of dialled, received and missed calls
- Automatic redial and fallback
- Speed dialling
- Speaker dependent and speaker independent voice dialling (SDND, SIND)
- Fixed dialling number support
- Vibrating alert (internal)
- Side volume keys
- Mute key
- Contacts with images
- Conference calling
- Push to talk
- VoIP
- Easy dialling directly from home screen (not available in all countries)

Messaging
- SMS
- Multiple SMS deletion
- Text-to-speech message reader
- MMS
- Distribution lists for messaging
- Instant messaging with Presence-enhanced contacts
- Cell broadcast

Security features
- Device lock
- Remote lock
- Data encryption for both phone memory and microSD card
- Mobile VPN

Web browsing
- Supported markup languages: HTML, XHTML, MP, WML, CSS
- Supported protocols: HTTP, WAP 2.0
- TCP/IP support
- Nokia browser
  - JavaScript version 1.3 and 1.5
  - Mini Map
- Nokia Mobile Search
- Nokia PC Internet Access (capability to serve as a data modem)

GPS and navigation
- Integrated A-GPS
- Nokia Maps application

Photography
- 3.2 megapixel camera (2048 x 1536 pixels)
- Autofocus
- LED flash
- Image formats: JPEG/EXIF
- CMOS sensor
- 4 x digital zoom
- Focal length: 3.8 mm
- Focus range: 10 cm to infinity
- Macro focus: 10-60 cm
- Flash modes: Automatic, On, Red-eye, Off
- Flash operating range: 1 m
- White balance modes: automatic, sunny, incandescent, fluorescent
- Centre weighted auto exposure; exposure compensation: +2 ~ -2EV at 0.7 step
- Capture modes: still, sequence, self-timer, video
- Scene modes: auto, user defined, close-up, portrait, landscape, night, night portrait
- Colour tone modes: normal, sepia, black & white, negative
- Full-screen viewfinder with grid
- Active toolbar
- Share photos with Share on Ovi

Video
- Main camera
- 320 x 240 (QVGA) at 30/15 fps
- 176 x 144 at 15 fps (QCIF)
- Digital video zoom
- Front camera
  - Video recording at up to 128 x 96 pixels (QCIF) and up to 15 fps
  - Up to 2x digital video zoom
- Video recording file formats: .mp4, .3gp; codecs: H.263, MPEG-4 VSP
- Audio recording formats: AMR
- Video white balance modes: automatic, sunny, incandescent, fluorescent
- Scene modes: automatic, night
- Colour tone modes: normal, sepia, black & white, negative
- Clip length (maximum): 1 h
- RealPlayer
- Video playback file formats: .mp4, .3gp; codecs: H.263, H.264 ,Real Video and MPEG-4
- Video streaming: .3gp, .rm, mp4
- Customisable video ring tones

Music and audio playback
- Music player
- Media player
- Nokia Music Manager
- Nokia Music Store support
- Music playback file formats: .mp3, .wma, .aac, AAC+, eAAC+
- Audio streaming formats: .rm, .eAAC+
- FM radio 87.5-108 MHz
- Visual Radio support. Read more: www.visualradio.com
- 2.5 mm Nokia AV connector
- Nokia Podcasting support
- Customisable ring tones
- Synchronise music with Windows Media Player
- Navi™ Key support
- Voice Aid

Voice and audio recording
- Voice commands
- Speaker dependent and speaker independent voice dialling (SIND)
- Voice recorder
- Audio recording formats: AMR-WB, AMR-NB
- Speech codecs: FR, EFR, HRO/1, AMR-HR, and AMR-FR
- Text-to-speech

Personalisation: profiles, themes, ring tones
- Customisable home screen content in Business and Personal modes
- Customisable profiles
- Customisable ring tones
- Customisable video ring tones
- Support for talking ring tones
- Customisable themes

Software platform and user interface
- S60 3.1 Edition, Eseries
- Symbian Os 9.2
- Two home screen modes with customisable active standby views
- Voice commands

Personal information management (PIM): contacts, clock, calendar etc.
- Advanced contacts database: multiple number and e-mail details per contact, contacts with images
- Support for assigning images to contacts
- Support for contact groups
- Closed user group support
- Fixed Dialling Number support
- Clock: analogue and digital
- Alarm clock with ring tones
- Reminders
- Calculator with advanced functions
- Calendar with week and month view
- Converter
- Active Notes
- To-do list
- PIM information viewable during call

Applications
- Windows Live! (not available in all countries)
- WorldMate
- Advanced Call Manager
- Wireless Presenter
- Nokia Sports Tracker
- Global Race
- Top Hits Solitaire Collection
- Nokia Multiscanner
- Yahoo Go! (not available in all countries)
- Java™ MIDP 2.0
- Flash Lite 3.0
- Chat and instant messaging
- Nokia browser
  - JavaScript version 1.3 and 1.5
  - Mini Map
- Dictionary
- Quickoffice (Quickword, Quickpoint, Quicksheet)
- PDF Viewer
- ZIP Manager
- Download!
- File Manager
- Nokia Search
- Nokia Maps
- Adding more applications:
  - Use the Download! client
  - Over-the-air (OTA) downloads

Sales package contents
- Nokia E71
- Nokia Battery BP-4L
- Nokia Charger AC-5
- Nokia Connectivity Cable CA-101
- Nokia Headset HS-47
- Nokia Eseries Wrist-strap
- Nokia Eseries Pouch
- User Guide
- Quick Start Guide and other documention
- 2GM microSD depending on market/channel

Available colors

Grey Steel White Steel Black Red Steel

The availability of the product and its features depends on your area and service providers, so please contact them and your Nokia dealer for further information. These specifications are subject to change without notice.
Music is copyright protected by international treaties and national copyright laws. It may be necessary to obtain permission or a license to reproduce or copy music. Please check the relevant legislation of the applicable country. Please respect copyrighted materials in your use of the Nokia Audio Manager.
Phone specifications mentioned above are based on the latest available information; please visit www.nokia-asia.com for the most recently updated product specifications.

www.nokia-asia.com/e71

ADSL2+ 4-PORT ROUTER

HIGH-SPEED ADSL2/2+ INTERNET CONNECTION

Latest ADSL2/2+ standards provide Internet transmission of up to 24Mbps downstream, 1Mbps upstream

SECURITY PROTECTION

Stateful Packet Inspection (SPI) and Denial of Service (Dos) attack prevention provide firewall protection from Internet attacks

QUALITY OF SERVICE (QoS)

Multiple Diffserv priority queues for smooth VoIP traffic/streaming multimedia

ULTIMATE INTERNET CONNECTION

The DSL-2540T 4-port ADSL router is an affordable high-performance ADSL router for home and the small office. With integrated ADSL2/2+ supporting up to 24Mbps download speed, firewall protection, Quality of Service (QoS) and built-in 4-port switch, this router provides all the essentials that a home or small office needs to establish a secure and high-speed remote link to the outside world.

AFFORDABLE HIGH-SPEED CONNECTION FOR HOME & SMALL OFFICE

Designed as a very affordable high-performance ADSL router for home and SOHO users, the DSL-2540T provides not only the low-cost, high-speed Internet connection, but also the security and Quality of Service (QoS) required by users in today's high-risk and versatile Internet environments.

FIREWALL PROTECTION & QoS

Security feature prevents unauthorized access to the home and office network from Internet intruders. The router provides firewall security using Stateful Packet Inspection (SPI) and hacker attack logging for Denial of Service (DoS) attack protection. SPI inspects the contents of all incoming packet headers before deciding what packets are allowed to pass through. Router access control is provided with packet filtering based on port and source/destination MAC/IP addresses.
For Quality of Service (QoS), the router supports multiple priority queues to enable a group of home or office users to experience the benefit of smooth network connection of inbound and outbound data without concern of traffic congestion. This QoS support allows users to enjoy high ADSL transmission for applications such as VoIP, streaming multimedia and on-line games over the Internet.

D-Link®

HIGH-SPEED ADSL BROADBAND

DSL-2540T

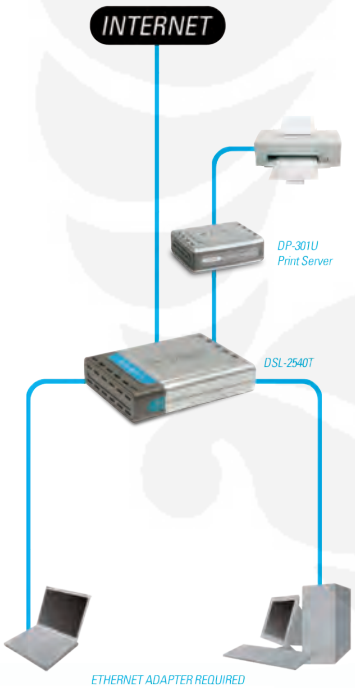
WHAT THIS PRODUCT DOES

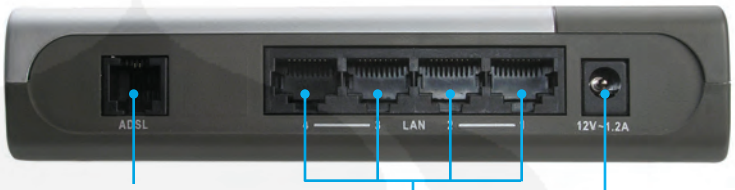
This 4-port ADSL router connects to the Internet using an integrated high-speed ADSL2/2+ interface. Multiple computers at home or the office can share the high-speed Internet connection. The router provides firewall protection and QoS for secure and smooth on-line games, voice communication and download of photos, files, music and video over the Internet. 4 built-in LAN ports provide ready connection to 4 computers through the Ethernet cables.

GET HIGH-SPEED ADSL SPEED

Ready ADSL connection with up to 24Mbps downstream and 1Mbps upstream. Watch TV, listen to live music and broadcast on the Internet, play games and experience clear Internet phone calls. Now, smooth streaming multimedia and VoIP voice are possible at home and in the office through a simple connection to this router.

YOUR NETWORK SETUP





RJ-11 ADSL Port
To Phone Line

4 RJ-45
10/100 BASE-TX Ethernet Ports
To Computers, Print Sever, Wireless AP

Power Socket
To Power Adapter

TECHNICAL SPECIFICATIONS

DEVICE INTERFACES
- RJ-11 ADSL port
- 4 RJ-45 10/100BASE-TX Ethernet ports with auto MDI/MDIX
- Factory reset button

ADSL STANDARDS
- ADSL standards: Multi-mode, ANSI T1.413 Issue 2, ITU G.992.1 (G.dmt) Annex A, ITU G.992.2 (G.lite) Annex A, ITU G.994.1 (G.hs)
- ADSL2 standards: ITU G.992.3 (G.dmt. bis) Annex A/L/M, ITU G.992.4 (G.lite.bis) Annex A
- ADSL2+ standards: ITU G.992.5 Annex A/L/M

ADSL DATA RATES
- G.dmt: 8Mbps downstream, 832Kbps upstream
- G.lite: 1.5Mbps downstream, 512Kbps upstream
- ADSL2: 12Mbps downstream, 1Mbps upstream
- ADSL2+: 24Mbps downstream, 1Mbps upstream

ATM & PPP PROTOCOLS
- ATM Adaptation Layer Type 5 (AAL5)
- Bridged or routed Ethernet encapsulation
- VC and LLC based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- Classical IP over ATM (RFC 1577)
- OAM F4/F5

ROUTER FEATURES & NETWORK PROTOCOLS
- NAT, Static Routing, RIP v1, v2
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server & DMZ
- SNTP, DNS proxy and IGMP proxy

FIREWALL/ACCESS SECURITY
- Built-in NAT firewall
- Stateful Packet Inspection (SPI)
- DoS attacks prevention (IP Spoofing, Land Attack, Smurf Attack, Ping of Death, TCP SYN flooding)
- Packet filtering based on port, source IP address, destination IP address, MAC address (ICMP/TCP/UDP)

VIRTUAL PRIVATE NETWORK (VPN)
PPTP/IPSec pass-through

CONFIGURATION/MANAGEMENT
- Quick installation wizard
- Web-based GUI for remote/local management
- Firmware upgrade, configuration data upload/download via Web-based GUI
- Telnet server for remote/local management
- Syslog monitoring
- SNMP v1, v2c support with built-in MIB-II (RFC 1213)
- Remote management TR-069 (optional)
- DHCP server/client/relay

QoS CONTROL
- LAN to WAN traffic prioritization/ bandwidth management
- 802.1p traffic prioritization (4 queues)

\

SECURITY/BANDWIDTH MANAGEMENT
- IGMP Snooping with 32 Multicast groups
- PVC/VLAN port mapping (4 VLANs)
- Bandwidth management based-on IP protocol, port number, MAC address

POWER INPUT
Through 12VAC 1.2A external power adapter

DIMENSIONS
142 x 109 x 31 mm
(5.59 x 4.29 x 1.22 inches)

WEIGHT
235.8 grams (0.52 lb)

OPERATING TEMPERATURE
0˚ to 40˚ C (32˚ to 104˚ F)

STORAGE TEMPERATURE
-20˚ to 70˚ C (-4 ˚ to 158˚ F)

OPERATING HUMIDITY
5% to 95% non-condensing

EMISSION (EMC/EMI)
- FCC Part 15 Class B
- CE (EN55022/EN55024/EN300 328/ EN301 489)

Safety
- CSA
- LVD

BROADBAND

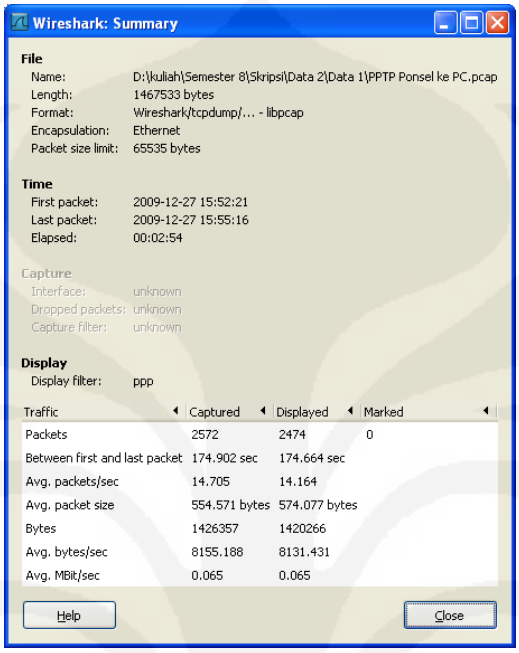
D-Link Worldwide Offices

U.S.A.	TEL: 1-800-326-1688	FAX: 1-866-743-4905	Spain	TEL: 34-93-4090770	FAX: 34-93-4910795	Turkey	TEL: 90-312-473-40-55	FAX: 90-312-473-40-58
Canada	TEL: 1-905-8295033	FAX: 1-905-8295223	Portugal	TEL: 351-21-8688493		Egypt	TEL: 202-291-9035	FAX: 202-291-9051
Europe (U. K.)	TEL: 44-20-8955-9000	FAX: 44-20-8955-9001	Czech Republic	TEL: 420-(603)-276-589		Israel	TEL: 972-9-9715700	FAX: 972-9-9715601
Germany	TEL: 49-6196-77990	FAX: 49-6196-7799300	Switzerland	TEL: 41-(0)-1-832-11-00	FAX: 41(0)-1-832-11-01	LatinAmerica	TEL: 56-2-232-3185	FAX: 56-2-232-0923
France	TEL: 33-1-30238688	FAX: 33-1-30238689	Greece	TEL: 30-210-9914 512	FAX: 30-210-9916902	Brazil	TEL: 55-11-218-59300	FAX: 55-11-218-59322
Netherlands	TEL: 31-10-282-1445	FAX: 31-10-282-1331	Luxemburg	TEL: 32-(0)2-517-7111	FAX: 32-(0)2-517-6500	South Africa	TEL: 27-12-665-2165	FAX: 27-12-665-2186
Belgium	TEL: 32(0)2-517-7111	FAX: 32(0)2-517-6500	Poland	TEL: 48-(0)-22-583-92-75	FAX: 48-(0)-22-583-92-76	Russia	TEL: 7-495-744-0099	FAX: 7-495-744-0099 #350
Italy	TEL: 39-02-2900-0676	FAX: 39-02-2900-1723	Hungary	TEL: 36-(0)-1-461-30-00	FAX: 36-(0)-1-461-30-09	Japan	TEL: 81-3-5781-0963	FAX: 81-3-5781-0965
Sweden	TEL: 46-(0)8564-61900	FAX: 46-(0)8564-61901	Singapore	TEL: 65-6774-6233	FAX: 65-6774-6322	China	TEL: 86-10-58635800	FAX: 86-10-58635799
Denmark	TEL: 45-43-969040	FAX: 45-43-424347	Australia	TEL: 61-2-8899-1800	FAX: 61-2-8899-1868	Taiwan	TEL: 886-2-6600-0123	FAX: 886-2-6600-8168
Norway	TEL: 47-99-300-100	FAX: 47-22-309580	India	TEL: 91-022-26526741	FAX: 91-022-26528914	Headquarters	TEL: 886-2-6600-0123	FAX: 886-2-6600-9898
Finland	TEL: 358-9-270 5000	FAX: 358-9-2707 5001	Middle East (Dubai)	TEL: 971-4-3916480	FAX: 971-4-3908881			

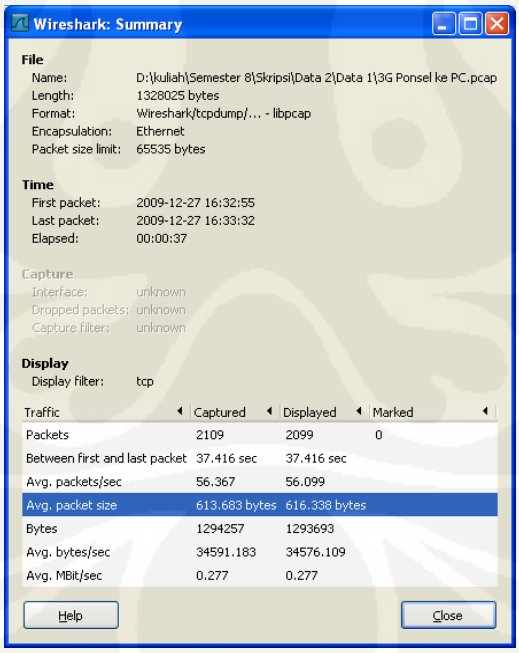
Release 01 (Aug. 2006)

Lampiran 4

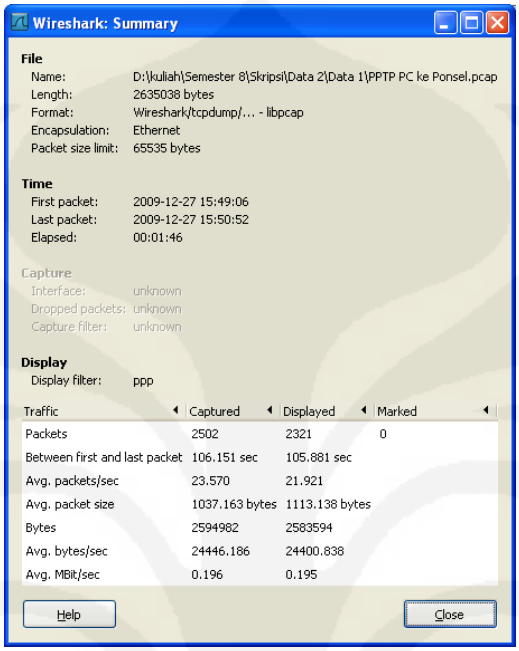
Data Pengujian 1



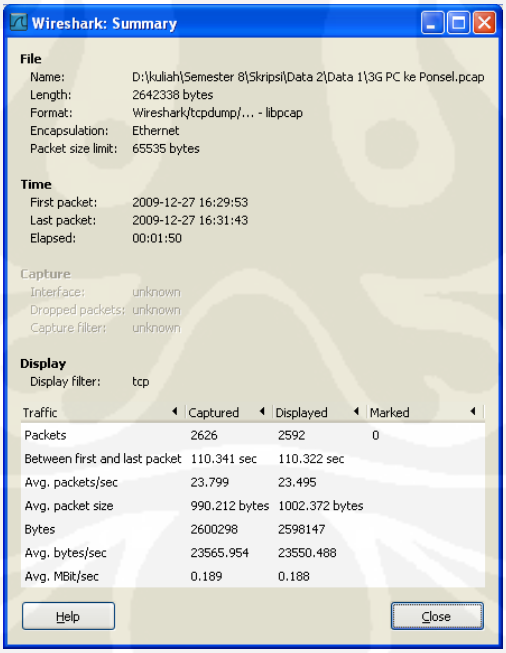
Data Mobile VPN dari Klien ke Server



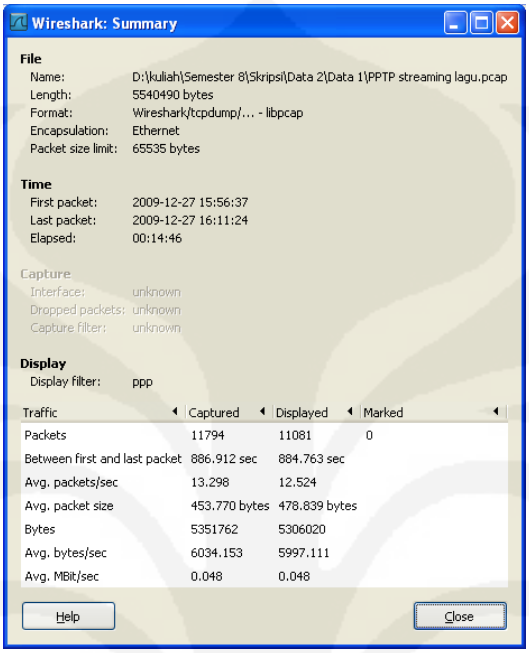
Data Jaringan 3G dari Klien ke Server



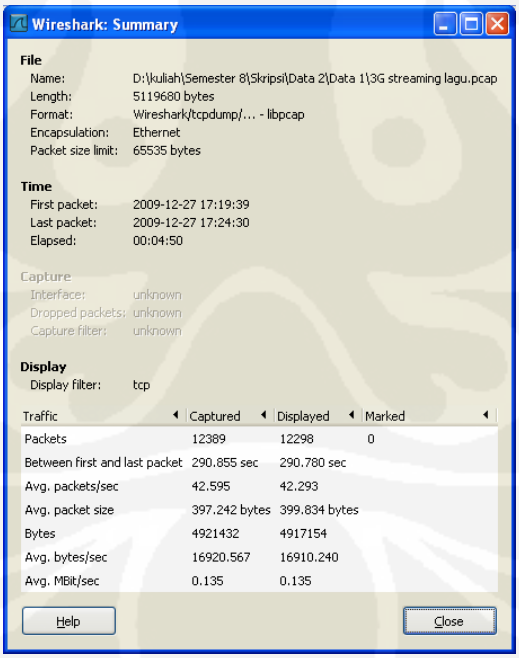
Data Mobile VPN dari Server ke Klien



Data 3G dari Server ke Klien



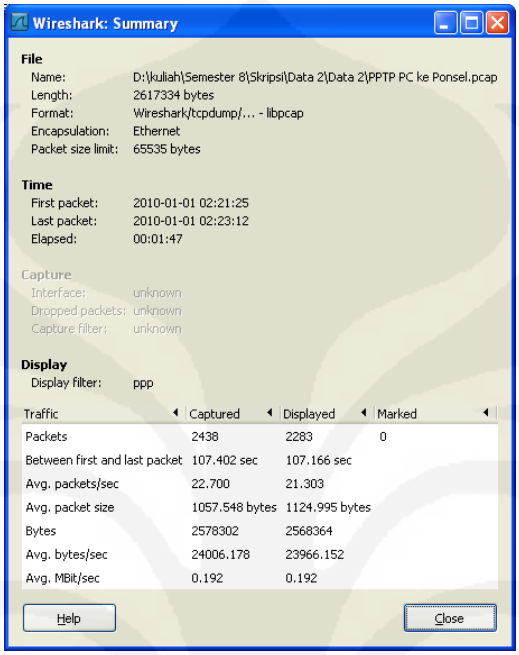
Data Mobile VPN Streaming File Suara



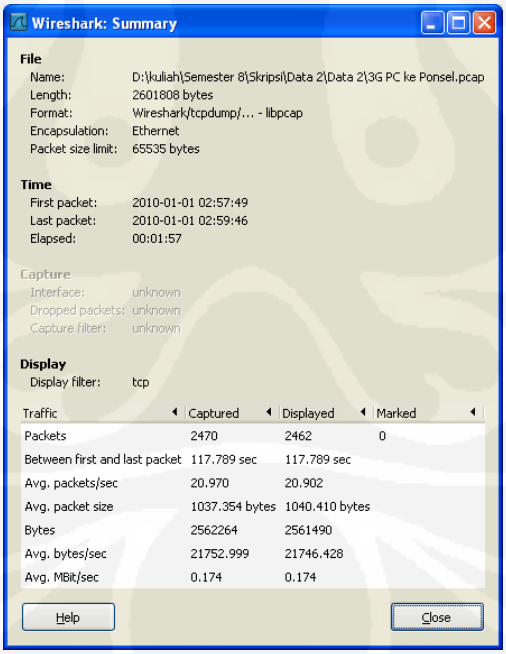
Data 3G Streaming File Suara

Lampiran 5

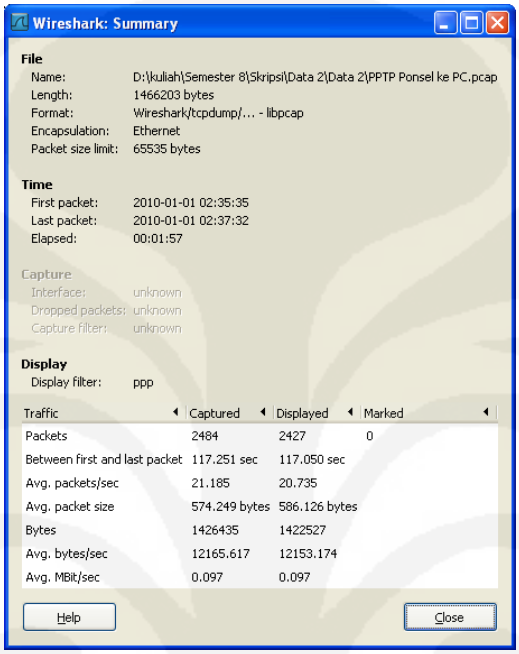
Data Pengujian 2



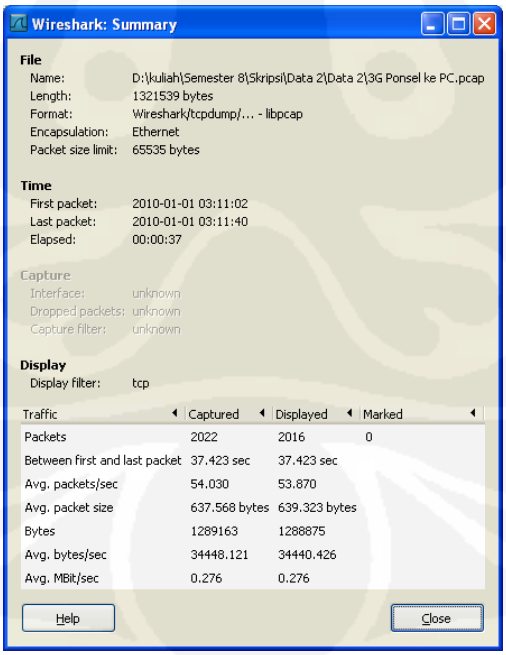
Data Mobile VPN dari Server ke Klien



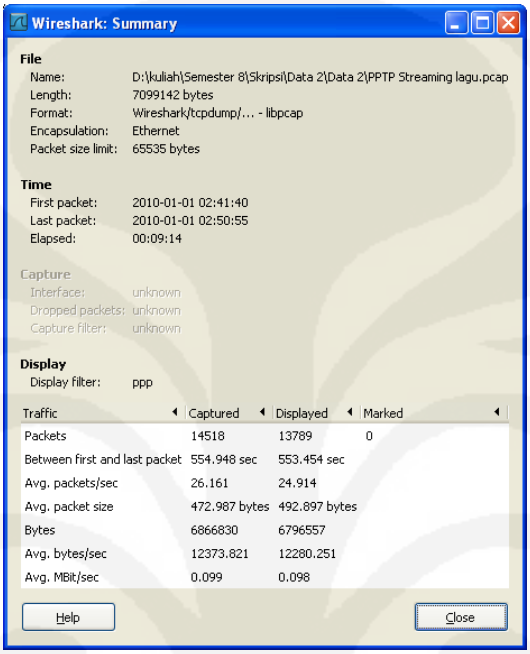
Data 3G dari Server ke Klien



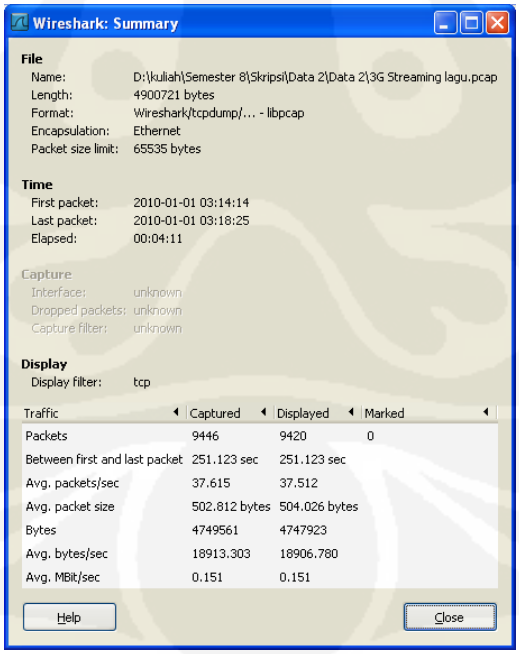
Data Mobile VPN dari Klien ke Server



Data 3G dari Klien ke Server



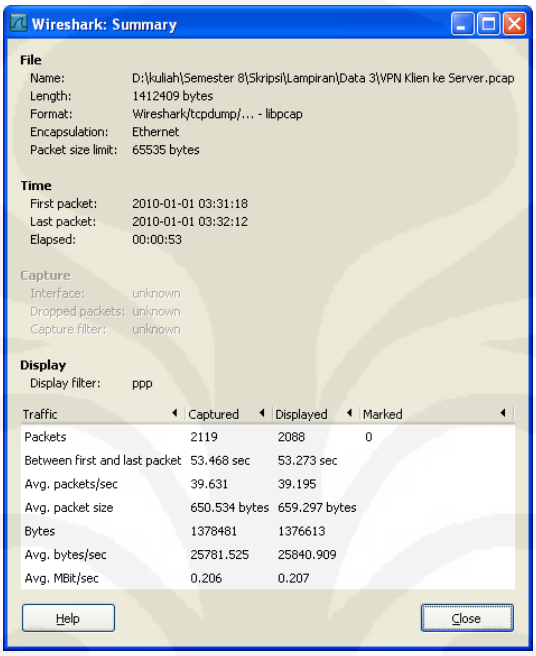
Data Mobile VPN Streaming File Suara



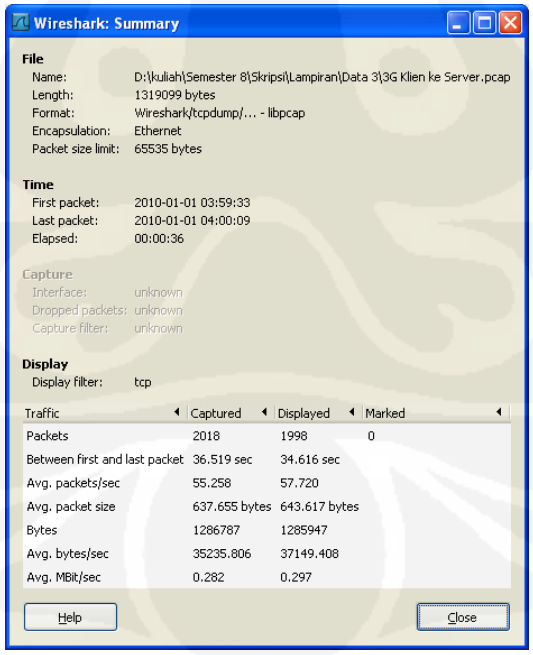
Data 3G Streaming File Suara

Lampiran 6

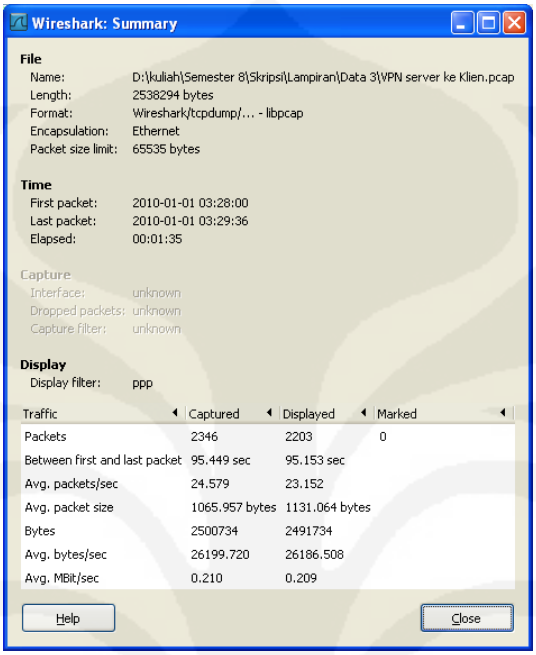
Data Pengujian 3



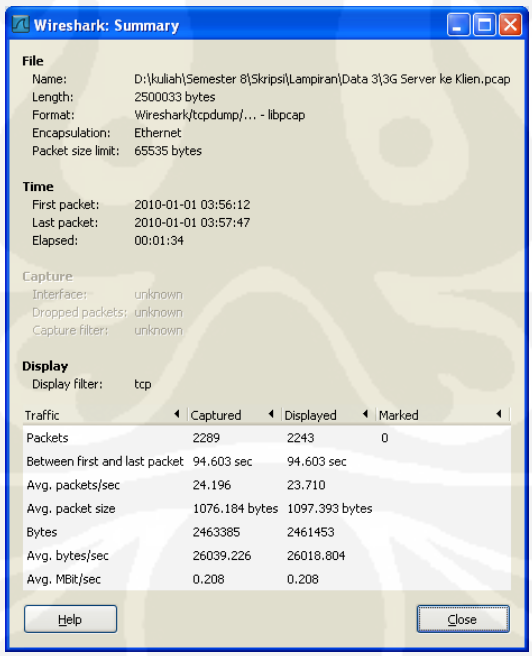
Data Mobile VPN dari Klien ke Server



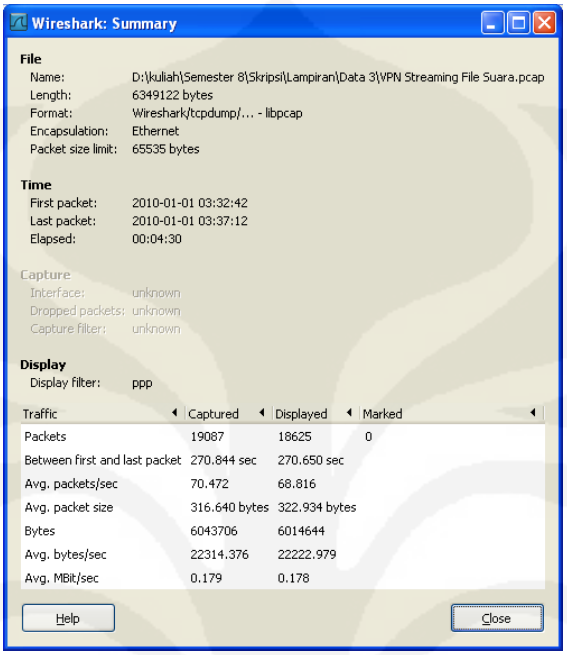
Data Jaringan 3G dari Klien ke Server



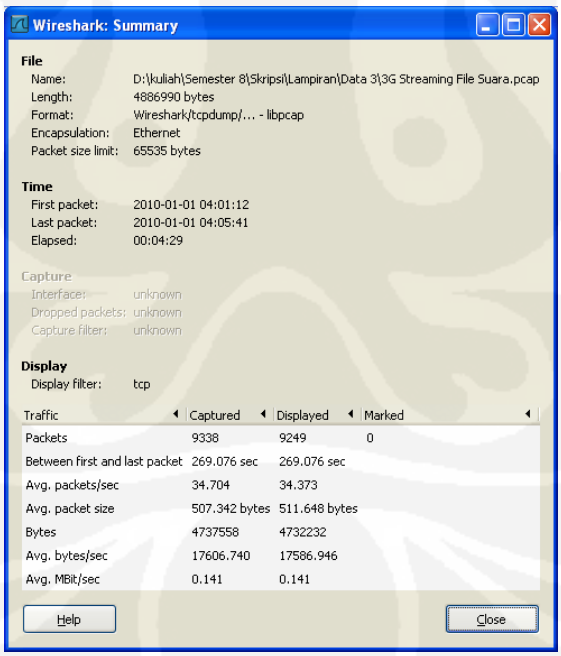
Data Mobile VPN dari Server ke Klien



Data 3G dari Server ke Klien



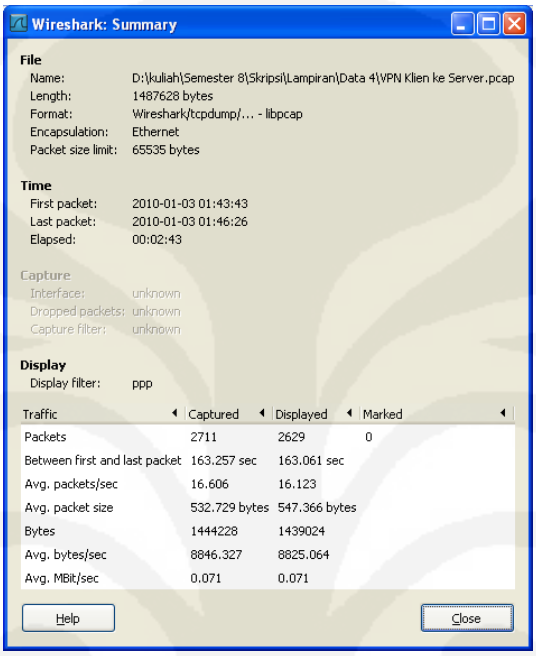
Data Mobile VPN Streaming File Suara



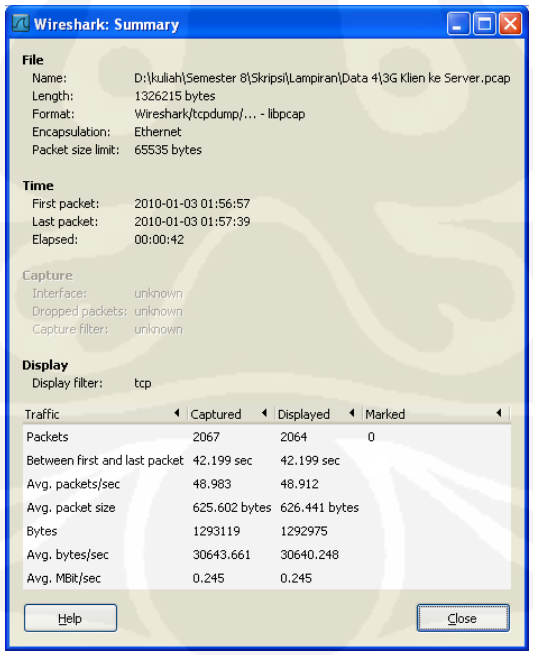
Data 3G Streaming File Suara

Lampiran 7

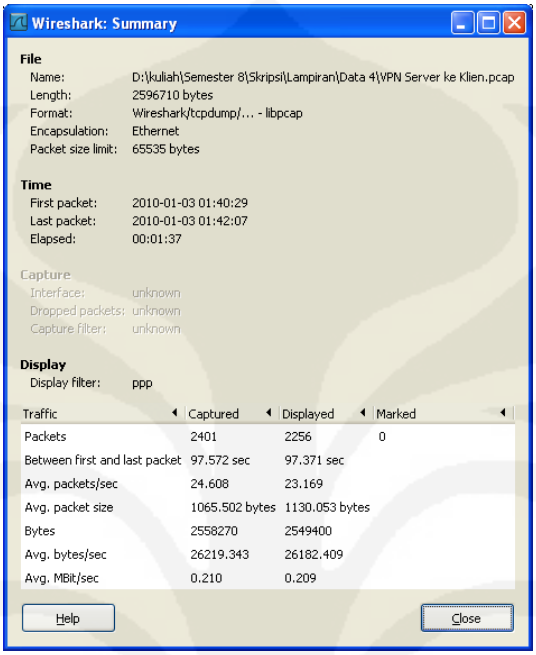
Data Pengujian 4



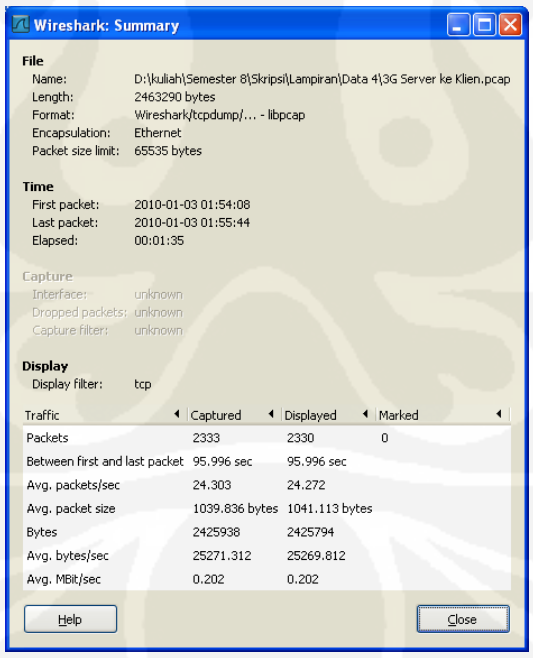
Data Mobile VPN dari Klien ke Server



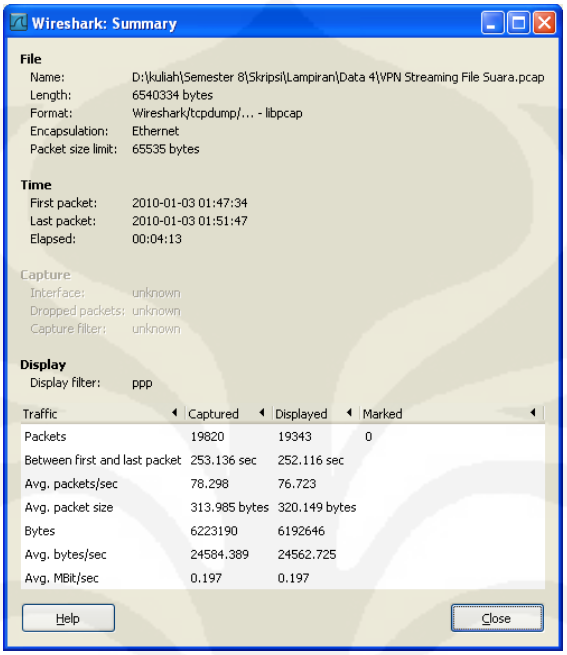
Data Jaringan 3G dari Klien ke Server



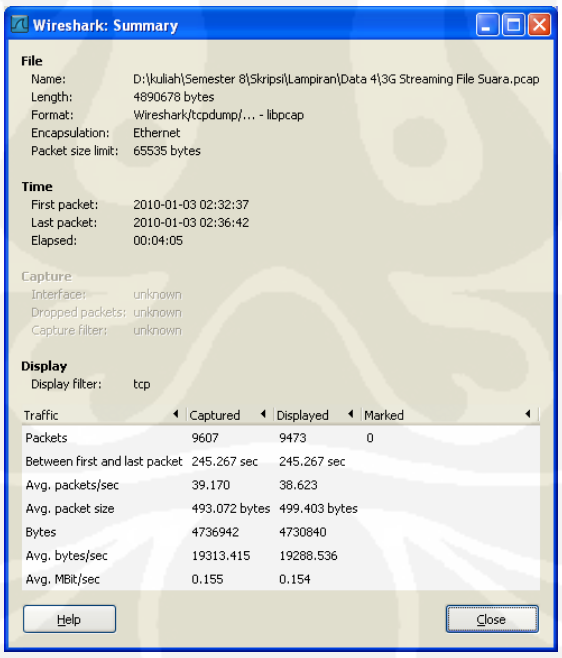
Data Mobile VPN dari Server ke Klien



Data 3G dari Server ke Klien



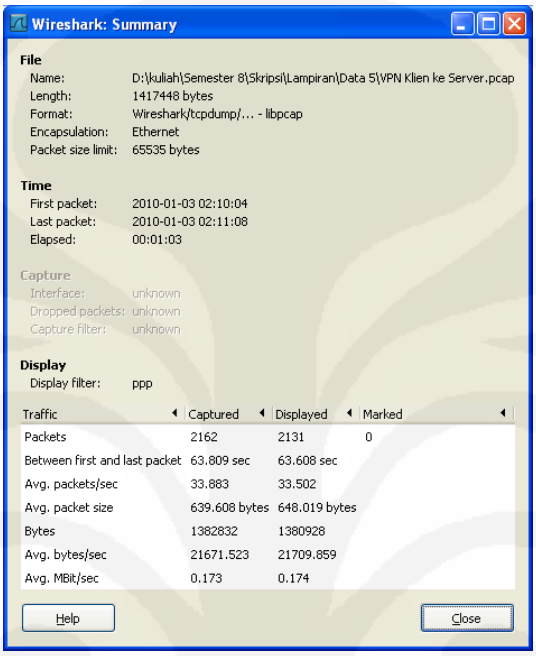
Data Mobile VPN Streaming File Suara



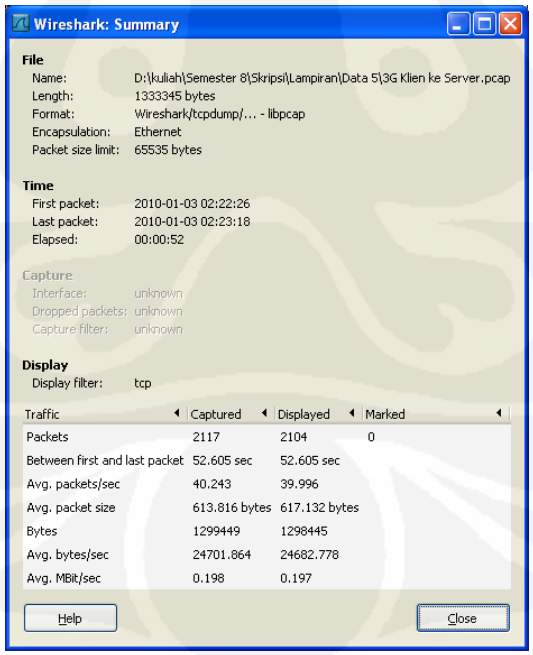
Data 3G Streaming File Suara

Lampiran 8

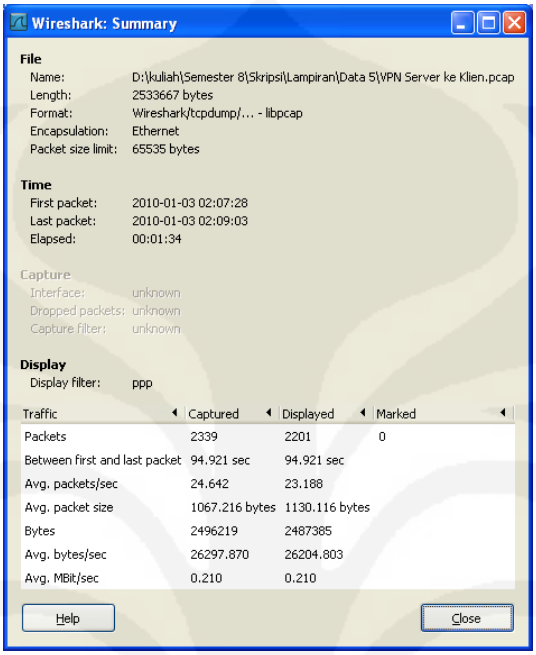
Data Pengujian 5



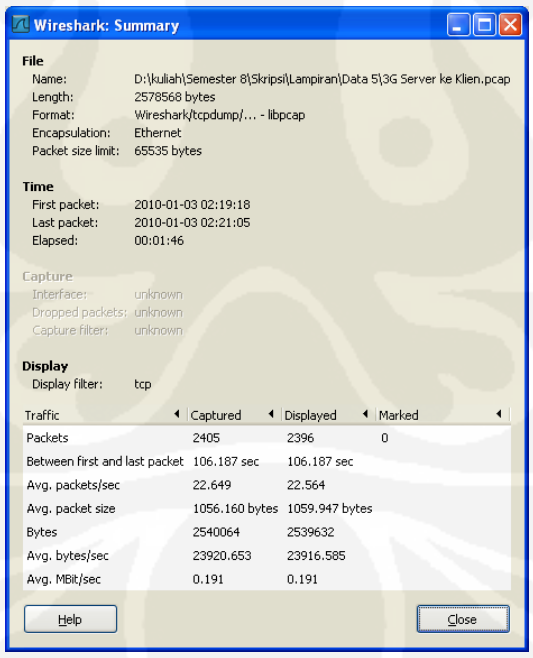
Data Mobile VPN dari Klien ke Server



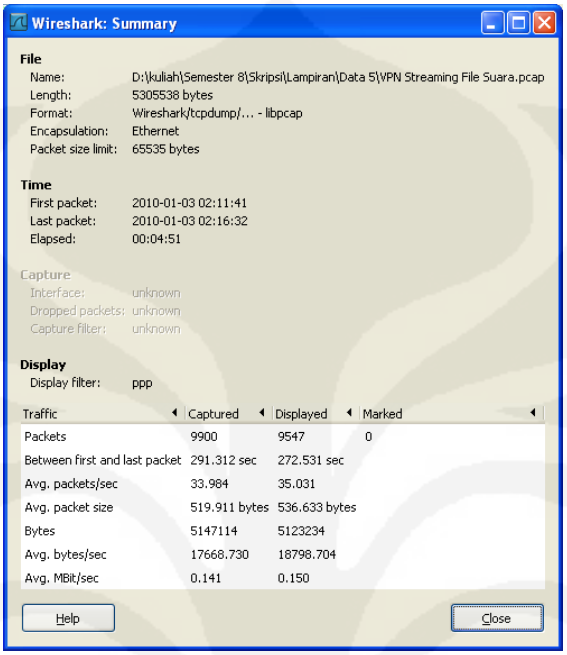
Data Jaringan 3G dari Klien ke Server



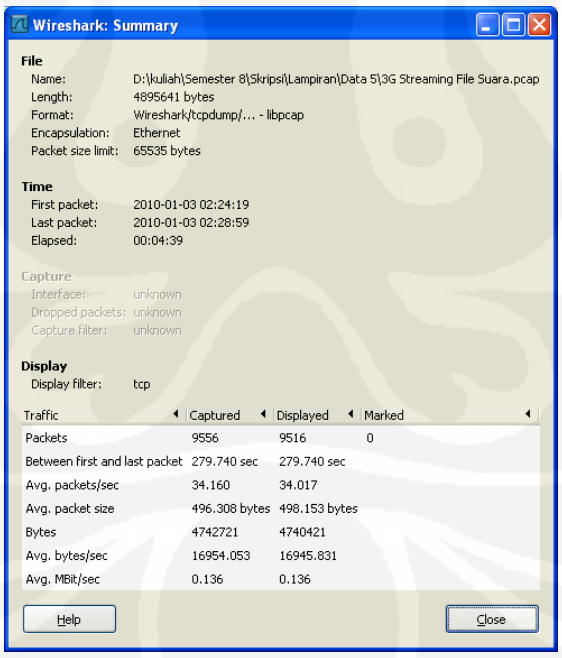
Data Mobile VPN dari Server ke Klien



Data 3G dari Server ke Klien



Data Mobile VPN Streaming File Suara



Data 3G Streaming File Suara