# ANALISIS DAN PERANCANGAN *VIRTUAL PRIVATE NETWORK* PADA PT SAMPOERNA TELEKOMUNIKASI INDONESIA

Sinta Tridian Galih1, Satrio Agung Prakoso2
Fakultas Ilmu Komputer,Universitas AKI
sinta.tridian@unaki.ac.id

***Abstrak***

*PT. Sampoerna Telekomunikasi Indonesia adalah perusahaan yang bergerak di bidang Internet Service Provider yang selalu memperhatikan kebutuhan konsumen akan keamanan di internet. Pihak yang tidak berwenang dapat dengan leluasa menggunakan dan menyalahgunakan data untuk kepentingan mereka sendiri. Pernah ada gangguan pada remote access CPE di pelanggan, tidak bisa melakukan remote secara langsung maka harus dengan mengaktifkan fasilitas port forwarding dahulu di Router Mikrotik, baru bisa melakukan remote access pada pelanggan. Teknologi VPN memungkinkan setiap orang untuk dapat mengakses jaringan lokal dari luar menggunakan internet. Dengan menggunakan VPN, maka user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada. Dengan analisis dan perancangan sistem tersebut, dapat menerapkan sistem jaringan VPN di PT. Sampoerna Telekomunikasi indonesia. Jaringan VPN diletakkan di server maupun client dengan kebutuhan jalur khusus dengan melakukan koneksi dari client ke server sehingga terbentuk koneksi point to point. Dengan adanya sistem VPN akan mempermudah perluasan konektivitas jaringan komputer secara geografis (Skalabilitas). Peningkatan keamanan dalam komunikasi data dan menyederhanakan topologi jaringan.*

***Keyword**: Network VPN*

## 1. Pendahuluan

Kemajuan teknologi informasi serta kebutuhan untuk mendapatkan informasi dalam waktu yang singkat dan tepat dalam jumlah yang besar mendorong peningkatan kebutuhan akan jaringan komputer dan internet di berbagai sektor kehidupan masyarakat saat ini.

Teknologi *Virtual Private Network* (VPN) memungkinkan setiap orang untuk dapat mengakses jaringan lokal dari luar menggunakan internet. Dengan menggunakan VPN, maka user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada. Keamanan data dan ketertutupan transmisi data dari akses yang tidak berhak dalam transmisinya pada internet menjadi standart utama dalam VPN, sehingga dalamVPN selalu disertakan akan fitur utama yaitu enkripsi dan tunneling.

Jaringan komputer menjadi pilihan yang tepat baik itu perusahaan maupun personal untuk menyediakan informasi dan menghubungkann LAN ke internet. Hal ini dapat dilihat dari penggunaan internet yang terus meningkat. PT. Sampoerna Telekomunikasi Indonesia adalah perusahaan yang bergerak di bidang Internet Service Provider yang selalu memperhatikan kebutuhan konsumen akan keamanan di internet. Namun ketika konsumen melakukan pertukaran informasi, ada pihak yang melakukan pencurian data selama ditransmisikan di internet. Pihak yang tidak berwenang dapat dengan leluasa menggunakan dan menyalahgunakan data untuk kepentingan mereka sendiri. Pernah ada gangguan pada *remote access* CPE di pelanggan, tidak bisa melakukan remote secara langsung maka harus dengan mengaktifkan fasilitas port forwarding dahulu di *Router* Mikrotik, baru bisa melakukan *remote access* pada pelanggan. Dengan adanya kejadian tersebut maka untuk membangun keamanan komunikasi data dalam jaringan internet adalah dengan menggunakan jaringan *Virtual Private Network* (VPN).

Berdasarkan latar belakang masalah di atas maka perumusan masalah dalam penelitian ini adalah bagaimana membuat jaringan VPN agar dapat menghubungkan jaringan private menggunakan jaringan internet dengan menggunakan *router* mikrotik RouterBoard CRS125-24G-1S-IN dan untuk *client* memakai komputer dengan sistem operasi windows.

Tujuan dari penelitian ini adalah merancang sistem jaringan internet baru yang diharapkan dapat mengatasi kelemahan yang ada pada sistem lama terutama di bidang

jaringan privat yang bisa di akses melalui jaringan internet.

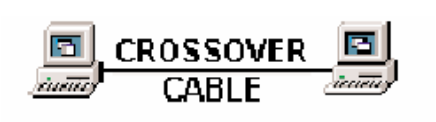
## 2. Kajian Pustaka

### Membangun Jaringan LAN

Dalam membangun jaringan LAN, hal-hal yang harus diperhatikan sebagai berikut :

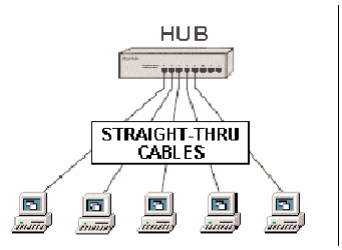
### Pemasangan Kabel

Dalam penyambungan kabel pada konektor RJ-45 ada dua jenis model. Yang pertama dinamakan dengan jenis sambungan *Crossover Cable* yang kegunaannya untuk menghubungkan dua komputer membentuk LAN tanpa melalui *hub* dan untuk menghubungkan antara *hub* ke sebuah *hub* lainya (Wahana Komputer, 2005: 53).




**Gambar 1 : Crossover Cable**

Yang kedua dinamakan dengan jenis sambungan *Straight- Through Cable* yang dipakai untuk menghubungkan komputer kesebuah *hub.*




**Gambar 2 : Straight - Through Cable**

Urutan penyambungan kabel UTP ke konektor RJ-45 untuk metode *straight cable* :

**Tabel 1 Metode Straight Cabel**

| | | |
|---|---|---|
| Putih Orange | 1 | Putih Orange |
| Orange | 2 | Orange |
| Putih Hijau | 3 | Putih Hijau |
| Biru | 4 | Biru |
| Putih Biru | 5 | Putih Biru |
| Hijau | 6 | Hijau |
| Putih Coklat | 7 | Putih Coklat |
| Coklat | 8 | Coklat |

Urutan kabel *Straigh* dipakai untuk menghubungkan komputer ke *switch* atau *hub*.


**Gambar 3 : Pengkabelan Straight - Through Cable**

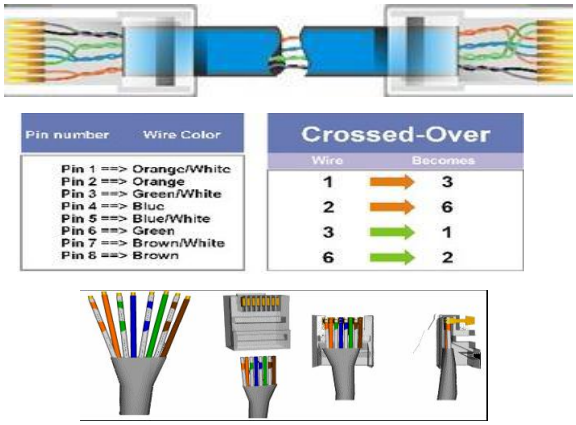
*Untuk* penyambungan kabel UTP ke konektor RJ-45 untuk metode *Cross Cable*, dengan urutan kabelnya :

**Tabel 2 Metode Cross Cabel**

| | | |
|---|---|---|
| Putih Orange | 1 | Putih Hijau |
| Orange | 2 | Hijau |
| Putih Hijau | 3 | Putih Orange |

| | | |
|---|---|---|
| Biru | 4 | Biru |
| Putih Biru | 5 | Putih Biru |
| Hijau | 6 | Orange |
| Putih Coklat | 7 | Putih Coklat |
| Coklat | 8 | Coklat |

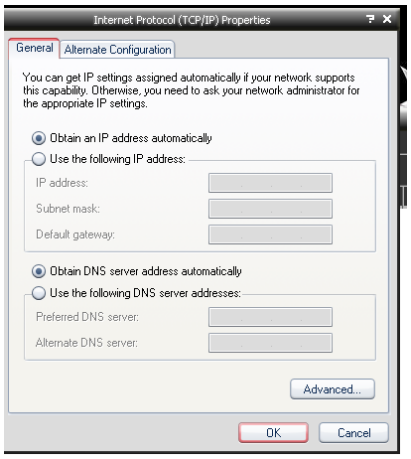
*Urutan Cross Cable* digunakan untuk menghubungkan PC to PC dan HUB to HUB.




**Gambar 4 : Pengkabelan Cross Cable**

**TCP/IP**

TCP/IP (*Transmision Control Protokol/Internet Protokol*) adalah sekelompok protokol yang dipakai dalam lingkungan sistem operasi *UNIX* untuk mengatur komunikasi data di *internet* dengan berbagai jenis komputer tanpa mempertimbangkan jarak, kualitas dan banyaknya data yang dialihkan (Wahana Komputer, 2005: 443).




**Gambar 5 : Propertis TCP/IP**

Sumber : Melwin Syafrizal, 2006:29.

**IP Address**

Alamat IP (*IP Address*) merupakan pengenal yang digunakan untuk memberi alamat suatu *host* dalam jaringan komputer. Format alamat IP adalah bilangan 32 bit yang tiap 8 bit-nya dipisahkan oleh tanda titik untuk mempermudah distribusinya. Alamat IP dibagi dalam kelas-kelas A, B, C, D, dan E. (Wahana Komputer, 2006)

Agar lebih mudah dibaca dan ditulis, alamat IP sering ditulis sebagai 4 bilangan desimal yang masing-masing dipisahkan oleh titik. Format penulisan ini disebut *"dotted-decimal notation"*. Setiap bilangan desimal tersebut merupakan nilai dari satu oktet (delapan bit) alamat IP.

| Dotted Decimal | Binary |
|---|---|
| 207.21.32.12 | 11001111<br>00010101<br>00100000 |

| | |
|---|---|
| | 00001100 |
| 192.168.4.1 | 11000000<br>10101000<br>00000100<br>00000001 |

*IP address* terdiri atas dua bagian yaitu *network* ID dan *host* ID, dimana *network* ID menentukan alamat jaringan komputer, sedangkan *hos*t ID menentukan alamat *hos*t (komputer, *router*, *switch*). Oleh sebab itu IP *address* memberikan alamat lengkap suatu *host* beserta alamat jaringan di mana *host* itu berada.

Contoh pengalokasian *IP Address*, misalnya akan dibuat sebuah jaringan yang menghubungkan tiga buah komputer, maka langkah yang harus dilakukan adalah menentukan *network* ID dan *hos*t ID.

*Network* ID digunakan digunakan untuk menunjukkan *host* TCP/IP yang terletak pada jaringan yang sama. Semua *host* pada satu jaringan harus memiliki *network* ID yang sama.

Misalnya jaringan ini diberi *network* ID = 192.168.5.xxx. Sedangkan *host* ID digunakan untuk menunjukkan suatu *host* dalam jaringan. Setiap antarmuka jaringan harus memiliki *host* ID yang unik. Sebagai contoh masing-masing alamat IP, ditentukan *host* ID sebagai berikut : 192.168.5.1, 192.168.5.2, 192.168.5.3.

***Netmask/Subnetmask***

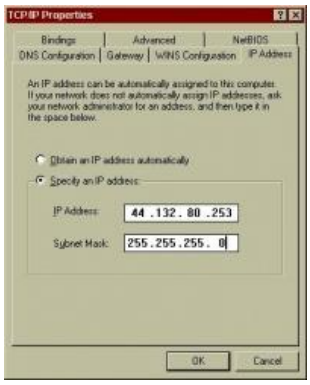
*Subnetmas*k adalah angka biner 32 bit yang digunakan untuk membedakan *network* ID dan *host* ID serta menunjukkan letak suatu *host*, apakah berada pada jaringan lokal atau jaringan luar. (Wahana Komputer, 2006).

Sebuah *subnetmask* biasanya diekspresikan di dalam notasi desimal bertitik (*dotted decimal notation*), seperti halnya alamat IP. Setelah semua *bit* diset sebagai bagian *network identifier* dan *host identifier*, hasil nilai 32-*bit* tersebut akan dikonversikan ke notasi desimal bertitik. Perlu dicatat, bahwa meskipun direpresentasikan sebagai notasi desimal bertitik, *subnet mask* bukanlah sebuah alamat IP.

Contoh :

| | |
|---|---|
| IP Address | 192.168.1.2 |
| Subnet Mask | 255.255.255.0 |

Pada contoh *IP Address* di atas yang disebutkan sebagai w adalah 192, x adalah 168. y adalah 1 dan z adalah 2. Dalam hal ini yang difungsikan sebagai *Net-ID* (alamat jaringan adalah w.x.y yang bernilai 192.168.1. Karena *subnetmask*nya 255. Sedangkan z yang bernilai 2 difungsikan sebagai *host* ID karena *subnet mask*nya 0.




Gambar 6 Memasukkan nomor *IP Address* dan *Subnet Mask*

***Gateway/Router***

*Gateway* adalah sebuah mekanisme yang menyediakan akses ke sebuah sistem lain yang terhubung dalam sebuah *network* (Wahana Komputer, 2005: 207). Di *Internet* suatu alamat bisa ditempuh lewat *gateway-gateway* yang memberikan jalan/*rute* ke arah mana yang harus dilalui supaya paket data sampai ke tujuan. Kebanyakan *gateway* menjalankan *routing daemon* (program yang meng-update secara *dinamis* tabel *routing*). Karena itu *gateway* juga biasanya berfungsi sebagai *router*. *Gateway/router* bisa berbentuk *Router box* seperti yang di produksi Cisco, 3COM, dll atau bisa juga berupa komputer yang menjalankan *Network Operating System plus routing daemon*. Misalkan PC yang dipasang Unix FreeBSD dan menjalankan program *Routed* atau *Gated*. Namun dalam pemakaian Natd, *routing daemon* tidak perlu dijalankan, jadi cukup dipasang *gateway* saja. Karena *gateway/router* mengatur lalu lintas paket data antar jaringan, maka di dalamnya bisa dipasangi mekanisme pembatasan atau pengamanan (*filtering*) paket-paket data.

**DNS**

DNS atau *Domain Name System* adalah Sistem pemberian alamat yang digunakan dalam lingkungan *internet*. Intinya memberi nama lain pada alamat *internet* protokol yang terdiri dari dua bagian yaitu identitas organisasi (nama organisasi tersebut) dan jenis organisasi itu sendiri (Wahana Komputer, 2005: 101).

**Keamanan Jaringan**

Saat ini hampir perusahaan berskala kecil, menengah, apalagi besar telah mengimplementasikan jaringan komputer untuk menghubungkan semua jaringan diperusahaan karena keuntungan yang dirasakan dalam penerapan jaringan komputer sangat besar. Seiring dengan berkembangnya TI dewasa ini perkembangan ancaman terhadap jaringan komputerpun terus meningkat, berbagai serangan dan ancaman dapat saja secara tiba-tiba menyerang jaringan komputer yang terkoneksi ke jaringan .

Cara untuk mengamankan jaringan adalah menggunakan *firewall. Firewall* dapat

berupa sebuah komputer, *router* atau peralatan komunikasi yang menyaring akses untuk melindungi jaringan dari kejahatan, misalnya untuk melindungi jaringan perusahaan dari pengacau ilegal saat pengguna komputer perusahaan mengakses ke layanan *internet* seperti *email* (Deris Setiawan, 2005: 123).

Sebelum kita memutuskan untuk membuat atau membeli suatu produk *firewall*, terlebih dahulu kita perlu mempertimbangkan beberapa hal agar *firewall* yang kita bangun dapat optimal dan tepat sasaran.

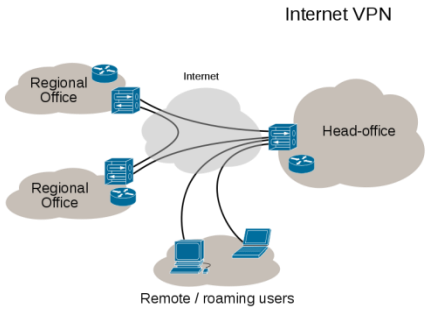
a. Apa yang akan diproteksi
   Jika hanya memproteksi dua atau tiga buah komputer, tidak perlu menggunakan produk *firewall* yang kompleks dan mahal.
b. Memilih, membeli, atau membangun *firewall* sendiri
   Sejumah organisasi dapat membangun sendiri *firewall* atau membeli pada sebuah *vendor* yang menawarkan jasa layanan pembuatan *firewall* baik perangkat keras maupun perangkat lunak.
c. Berapa biaya yang diperlukan
   Semakin canggih teknologinya akan semakin mahal produk tersebut.
d. User Policy
   Bagaimanapun hebatnya sistem yang kita buat tetapi tidak didukung dari sisi usernya akan sangat percuma. Disinilah perlu disusun *policy* yang baik antara sistem dan *user*.
e. Berapa besar efek jika terjadi serangan
   Kita harus dapat memastikan berapa besar efek dan resiko jika kita telah menetapkan metode dan arsitektur dari *firewall* yang akan kita buat.

**Virtual Private Network**

VPN merupakan suatu cara untuk membuat sebuah jaringan bersifat private dan aman dengan menggunakan jaringan *public* atau internet VPN dapat mengirim data antara dua komputer yang melewati jaringan public yang melewati jaringan *public*, sehingga seolah-olah terhubung secara *point-to point* (Mairs, John, 2002:1).

VPN dikembangkan untuk membangun sebuah *intranet* dengan jangkauan yang luas melalui jaringan internet. *Intranet* sudah menjadi komponen penting dalam suatu perusahaan dewasa ini. Dengan kata lain, semakin besar permasalahan ini akan semakin kompleks apabila perusahaan tersebut mempunyai banyak kantor cabang yang tersebar di berbagai kota dengan jarak yang jauh. Sedangkan di lain pihak seluruh kantor tersebut memerlukan suatu metode untuk berhubungan misalnya untuk transfer dan sinkronisasi data. Pada mulanya sistem intranet dikembangkan dengan mengunakan sistem *dedicated line*. Sistem ini menawarkan

kecepatan transfer data yang tinggi namun membutuhkan investasi yang mahal system ini tidak efektif untuk perusahaan kelas menengah ke bawah serta perusahaan yang tersebar di berbagai wilayah yang saling berjauhan.




**Gambar 7 Virtual Private Network**

**Analisis Sistem**

Analisis sistem adalah penguraian dari suatu sistem informasi yang utuh kedalam bagian-bagian komponennya dengan maksud untuk meng-identifikasikan dan mengevaluasi permasalahan-permasalahan, kesempatan, hambatan-hambatan yang terjadi dan kebutuhan-kebutuhan yang diharapkan, sehingga dapat diusulkan perbaikan-perbaikannya (Jogiyanto H.M, 2005:130).

Dalam melakukan analisis sistem terdapat langkah-langkah dasar yang harus dilakukan oleh analis sistem, sebagai berikut:

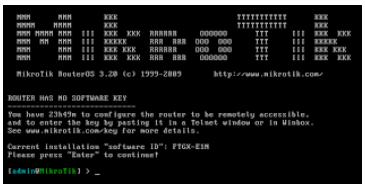
1. *Identifity*, yaitu mengidentifikasi masalah.
2. *Understand*, yaitu memahami kerja dari sistem yang ada.
3. *Analyze*, yaitu menganalisa sistem.
4. *Report*, yaitu membuat laporan hasil analisis.

**Mikrotik**

Mikrotik adalah sebuah perusahaan yang bergerak di bidang produksi perangkat keras (hardware) dan perangkat lunak (Software) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan router dan sistem ISP (Internet Service Provider) nirkabel.

Mikrotik dibuat oleh MikroTikls sebuah perusahaan di kota Riga, Latvia. Latvia adalah sebuah negara yang merupakan "pecahan" dari negara Uni Soviet dulunya atau Rusia sekarang ini. Mikrotik awalnya ditujukan untuk perusahaan jasa layanan Internet (PJI) atau *Internet Service Provider* (ISP) yang melayani pelanggannya menggunakan teknologi nirkabel atau *wireless*. Saat ini MikroTikls memberikan layanan kepada banyak ISP nirkabel untuk layanan akses Internet dibanyak negara di dunia dan juga sangat populer di Indonesia. MikroTik sekarang menyediakan hardware dan software untuk konektivitas internet di sebagian besar negara di seluruh dunia. Produk hardware unggulan Mikrotik berupa

Router, Switch, Antena, dan perangkat pendukung lainnya. Sedangkan produk Software unggulan Mikrotik adalah MikroTik RouterOS.




**Gambar 8 : Mikrotik RouterOS**

MikroTik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot. Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.

RouterBoard adalah router *embedded* produk dari mikrotik. Routerboard seperti sebuah pc mini yang terintegrasi karena dalam satu board tertanam prosesor, ram, rom, dan memori flash. Routerboard menggunakan os RouterOS yang berfungsi sebagai router jaringan, bandwidth management, *proxy server*, dhcp, dns server dan bisa juga berfungsi sebagai hotspot server.

Ada beberapa seri routerboard yang juga bisa berfungsi sebagai wifi. sebagai wifi access point, bridge, wds ataupun sebagai wifi client. seperti seri RB411, RB433, RB600. dan sebagian besar ISP wireless menggunakan routerboard untuk menjalankan fungsi wirelessnya baik sebagai AP ataupun Client. Dengan routerboard Anda bisa menjalankan fungsi sebuah router tanpa tergantung pada PC lagi, karena semua fungsi pada router sudah ada dalam routerboard. Jika dibandingkan dengan pc yang diinstal routerOS, routerboard ukurannya lebih kecil, lebih kompak dan hemat listrik karena hanya menggunakan adaptor. untuk digunakan di jaringan wifi bisa dipasang diatas tower dan menggunakan PoE sebagai sumber arusnya.


**Gambar 9 RouterBoard Mikrotik CRS125**

Mikrotik pada standar perangkat keras berbasiskan Personal Computer (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute atau lebih dikenal dengan istilah routing. Mikrotik yang dibuat sebagai *router* berbasiskan PC banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal

yang paling ringan hingga tingkat lanjut. Contoh aplikasi yang dapat diterapkan dengan adanya Mikrotik selain *routing* adalah aplikasi kapasitas akses (*bandwidth*) manajemen, *firewall*, *wireless access point (WiFi)*, *backhaul link*, sistem *hotspot*, *Virtual Private Netword* (VPN) *server* dan masih banyak lainnya.

**Sistem Level Lisensi Mikrotik**

Mikrotik bukanlah perangkat lunak yang gratis jika anda ingin memanfaatkannya secara penuh, dibutuhkan lisensi dari MikroTikls untuk dapat menggunakanya alias berbayar. Mikrotik dikenal dengan istilah Level pada lisensinya. Tersedia mulai dari Level 0 kemudian 1, 3 hingga 6, untuk Level 1 adalah versi Demo Mikrotik dapat digunakan secara gratis dengan fungsi-fungsi yang sangat terbatas. Tentunya setiap level memilki kemampuan yang berbeda-beda sesuai dengan harganya, Level 6 adalah level tertinggi dengan fungsi yang paling lengkap. Secara singkat dapat digambarkan jelaskan sebagai berikut:

1. Level 0 (gratis); tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
2. Level 1 (demo); pada level ini kamu dapat menggunakannya sbg fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.
3. Level 3; sudah mencakup level 1 ditambah dengan kemampuan untuk menajemen segala perangkat keras yang berbasiskan Kartu Jaringan atau *Ethernet* dan pengelolan perangkat wireless tipe klien.
4. Level 4; sudah mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola perangkat wireless tipe akses poin.
5. Level 5; mencakup level 1, 3 dan 4 ditambah dengan kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.
6. Level 6; mencakup semua level dan tidak memiliki limitasi apapun.

Router yang kami gunakan untuk implementasi VPN di PT. Sampoerna Telekomunikasi Indonesia memakai *RouterBoard* CRS125-24G-1S-IN Adalah *Switch Layer* 3 dengan 24 *port gigabit ethernet* + 1 SFP. *Switch* ini Berbasis *RouterOS* sehingga mampu melakukan berbagai fungsi *networking* seperti *Routing/Firewall/VPN Rackmont Case* dengan spesifikasi berikut ini:

**Tabel 4 Spesifikasi RouterBoard CRS125**

| **Spesifikasi CRS125-24G-1S-RM** | |
|---|---|
| Product Code | CRS125-24G-1S-RM |
| Architecture | MIPS-BE |
| CPU | AR9344 600MHz |
| Current Monitor | No |
| Main Storage/NAND | 128MB |
| RAM | 128MB |
| SFP Ports | 1 |
| LAN Ports | 24 |
| Gigabit | Yes |
| Switch Chip | 3 |
| MiniPCI | 0 |
| Integrated Wireless | No |
| MiniPCIe | 0 |
| SIM Card Slots | No |
| USB | 1 (microUSB) |
| Power on USB | Yes |
| Memory Cards | No |
| Power Jack | No |
| 802.3af Support | No |
| POE Input | No |
| POE Output | No |
| Serial Port | Yes |
| Voltage Monitor | Yes |
| Temperature Sensor | Yes |
| Dimentions | 443x142x44mm |
| Operating System | RouterOS |
| Temperature Range | -30C .. +70C |
| RouterOS License | Level5 |

## 3. Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah dengan melakukan studi kepustakaan mengenai teknologi VPN dari jenis, keuntungan, kelemahan, dan teori-teori yang mendukung, melakukan wawancara kepada staff IT PT. Sampoerna Telekomunikasi Indonesia untuk mendapatkan informasi yang berguna untuk penelitian ini, kemudian melakukan observasi dan survei terhadap jaringan perusahaan untuk mendapatkan informasi yang berguna dalam perancangan remote access VPN. Setelah itu menetapkan solusi yang dipakai serta menentukan teknologi yang dipakai beserta alasan pemilihan teknologi tersebut. Tahap selanjutnya adalah dengan melakukan analisa kebutuhan sistem meliputi spesifikasi sistem dan merancang topologi jaringan VPN yang akan dibuat di perusahaan. Dan pada akhirnya melakukan implementasi meliputi konfigurasi VPN Server di Mikrotik router board dan client di windows 7 kemudian melakukan pengujian koneksi VPN yang telah dibuat.

## 4. Pembahasan

### Analisa Permasalahan

Sebagai tahapan awal melakukan analisa terhadap suatu sistem yang sudah ada sehingga dapat mengetahui kelemahan dan kelebihan sistem yang ada dan dengan demikian dapat memudahkan kedalam sistem yang baru. Pada saat ini PT. Sampoerna Telekomunikasi Indonesia menerapkan sistem remote accees ke pelanggan menggunakan sistem manual, yaitu dengan cara menggunakan fitur NAT pada firewall untuk proses *port forwarding*.

Dengan sistem yang demikian, Internet Dedicated PT. Sampoerna Telekomunikasi Indonesia dalam melakukan remote acces ke pelanggan harus di setting satu per satu sehingga kurang efektif. Dengan adanya sisten VPN maka permasalahan diatas dapat teratasi karena jaringan lebih aman dan bisa melakukan remote access dari mana saja pada perangkat yang terhubung internet.

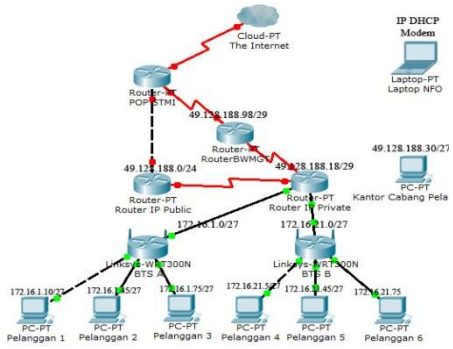
PT. Sampoerna Telekomunikasi Indonesia memiliki pelanggan ribuan yang tersebar di seluruh wilayah Indonesia. Beberapa bulan ini ada permintaan akan layanan VPN. Setiap pelanggan membutuhkan layanan yang berbeda-beda seperti korporasi dan instansi pemerintahan yang membutuhkan layanan dengan kebutuhan jalur khusus. Kegiatan pelanggan instansi pemerintah dan bisnis yang mengirim dan menerima data, yang berarti transaksi data yang terjadi setiap hari. Terutama pelanggan perusahaan yang sedang berkembang dan memiliki banyak kantor cabang dan sering melakukan komunikasi dengan kantor cabangnya tersebut. Komunikasinya bisa berupa pertukaran data, informasi dan lain-lain. Terkadang informasi yang dipertukarkan merupakan informasi yang bersifat rahasia. Data-data transaksi dikirim dengan menggunakan internet melalui *messenger* dan *email*. Dengan hanya menggunakan media tersebut, keamanan data yang dikirim atau diterima rentan terhadap pencurian, rusak, hilang dan serangan hacker.

### Solusi Permasalahan

Berdasarkan hasil permasalahan yang dihadapi, maka diusulkan pemecahan masalah dengan cara membuat *Virtual Private Network* (VPN). Dengan VPN maka pelanggan dan seluruh cabang-cabangnya dapat dihubungkan menjadi satu jaringan internal dengan menggunakan media jaringan publik/ jaringan internet yang ada sebagai media perantara. Selain kantor cabang, semua karyawan dan staff yang kebetulan sedang tidak dapat berada di perusahaan tetapi ingin mengakses data pekerjaan atau data-data yang diinginkan dapat mengaksesnya melalui jalur internet.

Penggunaan internet sebagai media VPN dapat menekan biaya yang dikeluarkan dan lebih mudah untuk diterapkan daripada membuat sebuah jaringan baru menggunakan media kabel ataupun wireless. Pemilihan

jenis VPN yang akan digunakan tentu saja harus memiliki sistem keamanan yang baik agar semua data yang melewatinya tidak jatuh ke orang-orang yang tidak berhak untuk mengakses data tersebut. Selain pada sisi keamanan, VPN yang akan digunakan juga harus menyediakan kemudahan kepada administrator dalam melakukan konfigurasi, administrasi. Secara ringkas topologi VPN dapat dilihat pada gambar 10




**Gambar 10** Topologi Jaringan VPN PT Sampoerna Telekomunikasi Indonesia

Berdasarkan topologi pada gambar 10 diatas dapat ditarik kesimpulan bahwa jaringan internet dibagi antara dua segment yaitu IP Public STMI 49.128.188.0/24 dan IP Private Class B dengan estimasi 172.16.1.0/27, 172.16.21.0/27, 172.16.31.0/27 yang dipakai untuk jaringan local VPN. Untuk sebagai pusat server VPN berada di router CRS 125 dengan dengan mode IP private kemudian di distribusikan melalui transmisi BTS dengan menggunakan Radio Microwave. Setelah dari BTS dipancarkan melalui AP (*access point*) dan diterima pelanggan dengan perangkat CPE (*customise premise equipment*) kemudian bisa langsung dipakai untuk jaringan local atau di routing kembali sesuai jaringan yang digunakan pelanggan.

**Analisa Kebutuhan Sistem**

Dalam pengembangan sistem *virtual private network*, diperlukan analisa kebutuhan *software*, *hardware*, *brainware* dengan perician sebagai berikut:

***Software* Pendukung**

Beberapa perangkat lunak (*software*) yang dibutuhkan untuk mendukung pembuatan sistem *virtual private network* pada PT. Sampoerna Telekomunikasi Indonesia sebagai berikut :

a. Sistem yang digunakan adalah Router OS versi 6.15 yang sudah include pada pada Router CRS125.
b. Untuk client memakai sistem operasi berbasis Windows 7 Home Basic dengan pertimbangan bahwa sistem operasi ini menggunakan *Graphical User Interface* (GUI) yang mudah digunakan.
c. *Utility*, digunakan untuk membantu para pemakai komputer dalam mengoperasikan komputernya dan sebagai pendukung.

   Contoh : Winbox

***Hardware* Pendukung**

*Hardware* atau perangkat keras yang digunakan untuk mendukung *software*. Adapun spesifikasi standar *hardware* yang akan dipergunakan sebagai berikut :

**Analisa Kebutuhan *Hardware* untuk *Server***

*RouterBoard* CRS125-24G-1S-IN Adalah *Switch Layer* 3 dengan 24 *port gigabit ethernet* + 1 SFP. *Switch* ini Berbasis *RouterOS* sehingga mampu melakukan berbagai fungsi *networking* seperti *Routing/Firewall/VPN Rackmont Case* dengan spesifikasi seperti yang ditunjukkan dalam tabel 4.

**Analisa Kebutuhan *Hardware* untuk *Client***

a. *Processor Core i3*

Kelebihan *Processor Core i3* karena kecepatan kerja 2,66 GHz pada CPUnya yang seolah-olah memiliki 4 prosesor yang bekerja sama, tipe tersebut dapat mendukung kerja Sistem Operasi Windows 7 dan *software-software* yang membutuhkan *resource* tinggi. Prosessor tersebut juga bisa menyesuaikan update software yang berkembang begitu pesat yang membutuhkan *source* yang cukup besar, cukup mumpuni untuk pemakaian jangka panjang.

b. *Memory DDR3- 4GB*

*Memory DDR3- 4GB* kerjanya stabil dan memiliki kapasitas yang sesuai dengan perkembangan *software* saat ini yang membutuhkan *source* yang cukup besar.

c. *HDD 500 GB SATA*

*Hardisk 500 GB SATA* selain mudah didapat di toko-toko komputer, merk ini mempunyai kualitas penyimpanan data yang lebih baik dan tahan terhadap goncangan yang tidak terlalu keras serta mempunyai kecepatan putar piringan yang cukup tinggi sehingga kecepatan simpan dan panggil lebih cepat.

d. *DVDRW*

*DVDRW* merupakan media untuk mengcopy data yang cukup terkenal. Media ini sebuah jenis *hardware* untuk *mengcopy* data ke CD atau DVD, kemudian isinya dapat kita hapus jika diinginkan. Alat ini memiliki kecepatan *copy* data yang baik dan cepat.

e. *Monitor LED "20"*

*Monitor LED "20"* ini mempunyai layar yang lebar dan cenderung agak sejuk di mata dan tidak memerlukan tegangan listrik yang tinggi.

f. *Keyboard* dan *Mouse*

*Keyboard* dan *Mouse* ini menggunakan model yang *compatibel* dengan *standart* windows 7 dengan tombol minimal 103 *key* dan untuk mouse menggunakan *optical mouse* atau *scroll mouse* yang kompatibel dengan windows 7.

*g. UPS*

*UPS* ini selain digunakan untuk mencegah terputusnya arus listrik yang mengalir ke komputer *server* dari akibat putusnya aliran listrik. Alat ini juga sangat dibutuhkan untuk keselamatan data. Dengan daya 1200 VA sudah cukup untuk kapasitas server mikrotik dan PC bisa untuk backup kurang lebih dua jam.

**Kebutuhan *Brainware***

Perangkat ini adalah perangkat pelaksana yaitu manusia, tanpa manusia semua yang ada (*Software* dan *Hardware*) tidak akan berjalan dengan baik. Jadi *Hardware*, *Software* dan *Brainware* harus ada dan berfungsi sesuai dengan tempatnya. Masing-masing *Brainware* digolongkan menjadi :

*a. Datacomm*

*Datacomm* diperlukan sebagai petugas yang membuat dan setting program-program aplikasi tertentu sesuai dengan kebutuhan organisasi dan arahan dari sistem operasi.

*b. Network Field Operation* (NFO)

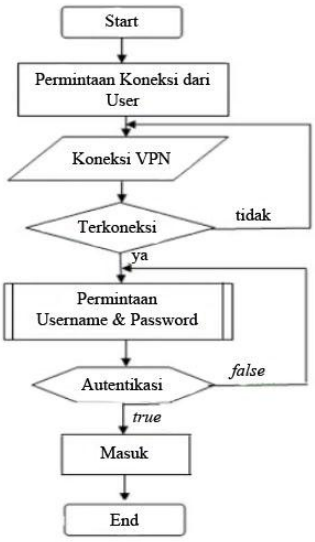
*Network Field Operation* diperlukan sebagai petugas untuk memastikan semua perangkat terkait Layanan Internet *Dedicated* di sisi *network* bekerja dengan semestinya dalam menyediakan layanan sesuai paket yang diambil pelanggan.

c. CRT IT

Teknisi komputer diperlukan sebagai petugas untuk memastikan semua perangkat terkait Layanan Internet *Dedicated* di lokasi pelanggan bekerja dengan semestinya dalam menyediakan layanan sesuai paket yang diambil pelanggan.

**Desain Sistem.**

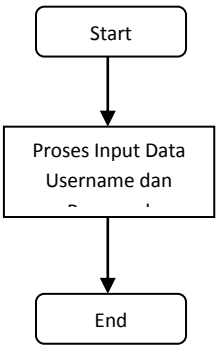
Secara ringkas diagram flowchart implementasi sistem VPN ini ditunjukan pada gambar dibawah ini yaitu :




**Gambar 11** Flowchart Sistem VPN

Keterangan :

Sistem jaringan VPN diawali dengan permintaan koneksi dari user kemudian masuk ke sistem untuk proses koneksi ke jaringan VPN. Jika proses tersebut tidak terkoneksi maka akan kembali ke proses awal. Setelah proses tersebut bisa terkoneksi maka akan ke proses permintaan *username* dan *password* dalam penyimpanan database. Proses selanjutnya terjadi autentikasi jika status *false* maka akan kembali ke proses login *user* dan password. Jika autentikasi dengan status *true* maka akan berhasil masuk ke sistem dan jaringan VPN bisa digunakan.

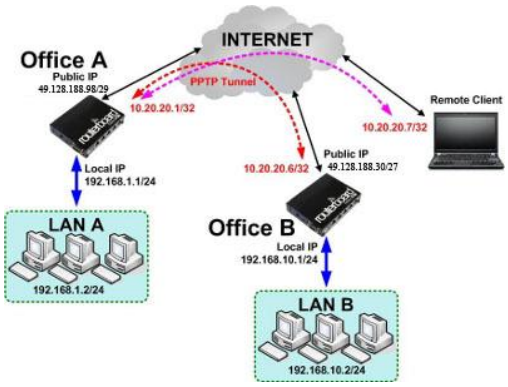



**Gambar 12** Proses Permintaan Username dan Password

Keterangan :

Jadi pada gambar 12 menunjukkan proses sub program permintaan username dan password yang diawali dengan permulaan start kemudian masuk ke proses input data username dan password kemudian ke akhir program end. Setelah selesai dilanjutkan ke proses yang ada pada flowchart yang ditunjukkan pada gambar 11

Pada desain sistem ini akan menghubungkan jaringan dengan menerapkan VPN dengan PPTP. Untuk topologinya bisa dilihat pada gambar 13 di bawah.




**Gambar 13** Topologi Jaringan VPN

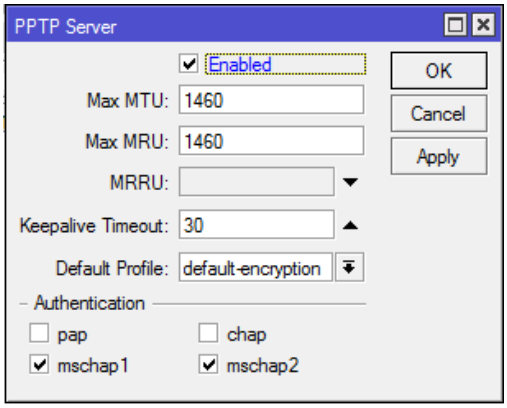
Router Office A dan Router Office B terhubung ke internet via ether 1 dan PC pada masing-masing jaringan lokal terhubung ke Ether 2. Remote client juga sudah terhubung ke internet. Langkah selanjutnya melakukan konfigurasi agar Router A dan jaringan LAN A bisa diakses dari Router B dan jaringan LAN B serta Remote Client. Langkah-langkah setting PPTP dengan Winbox sebagai berikut:

**Konfigurasi PPTP Server**

Berdasar topologi pada gambar 13 di atas, yang menjadi pusat dari link PPTP (konsentrator) adalah Router Office A , maka harus dilakukan setting PPTP Server pada router tersebut.

**Enable PPTP Server**

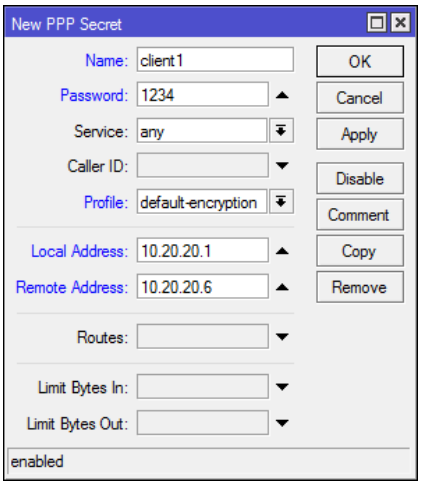
Langkah pertama yang harus dilakukan adalah mengaktifkan PPTP server. Masuk pada menu **PPP->Interface->PPTP Server** . Gunakan profile "Default-encryption" agar jalur VPN terenkripsi.




**Gambar 14** Setting PPTP Server

**Secret**

Pada tahap selanjutnya menentukan **username** dan **password** untuk proses autentikasi Client yang akan terkoneksi ke PPTP server. Penggunaan huruf besar dan kecil akan berpengaruh. Local Address adalah alamat IP yang akan terpasang pada router itu sendiri (Router A / PPTP Server) setelah link PPTP terbentuk. Remote Address adalah alamat IP yang akan diberikan ke Client setelah link PPTP terbentuk. Contoh konfigurasi sebagai berikut. Arahkan agar menggunakan profile "Default-Encryption"



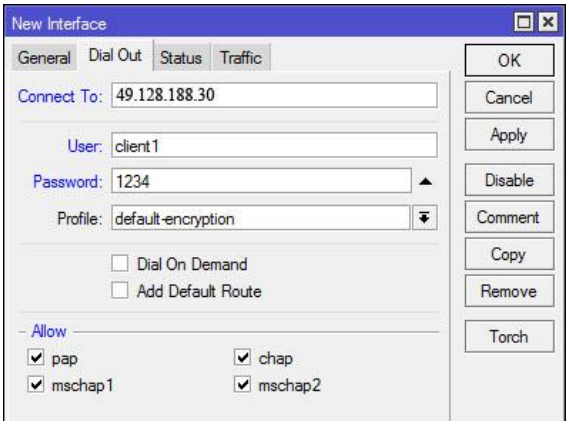

**Gambar 15** Setting Password VPN

Proses untuk konfigurasi Router A (PPTP Server) sudah selesai, tahap selanjutnya melakukan konfigurasi di sisi client.

**Client Router Office B**

Langkah-langkah untuk melakukan konfigurasi Client PPTP pada Router Mikrotik adalah sebagai berikut :

Tambahkan interface baru PPTP Client, lakukan dial ke IP Public Router A (PPTP server) dan masukkan username dan password sesuai pengaturan secret PPTP Server.



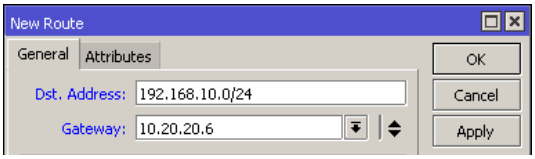

**Gambar 16** Setting Interface VPN

**Catatan** : IP 49.128.188.30 adalah permisalan ip public dari server, Untuk implementasi sebenarnya sesuaikan dengan ip public yang diperoleh dari ISP PT. Sampoerna Telekomunikasi Indonesia. Setelah koneksi PPTP terbentuk, akan muncul IP Address baru di kedua Router dengan flag “D” yang menempel di interface pptp sesuai dengan pengaturan Secret pada PPTP server.

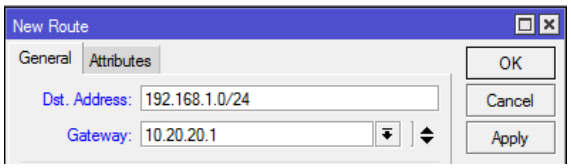
**Static Route**

Proses koneksi VPN antar router sudah terbentuk, akan tetapi antar jaringan lokal belum bisa saling berkomunikasi. Agar antar jaringan local bisa saling berkomunikasi, maka perlu menambahkan routing static dengan konfigurasi.

- **dst-address** : jaringan local Router lawan
- **gateway** : IP PPTP Tunnel pada kedua router.




**Gambar 17** Penambahan static route di Router A



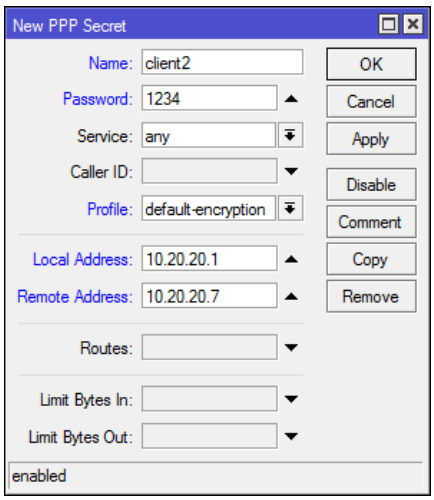

**Gambar 18** Penambahan static route di router B

**Mobile Client**

Client PPTP tidak harus menggunakan Router. Seperti pada topologi jaringan gambar 13 di atas, ada sebuah Remote Client (Laptop) yang akan melakukan koneksi VPN ke Router A. Maka harus membuat Secret baru pada PPTP server untuk autentikasi remote client tersebut.

**Secret**

username = **client2** ; password = **1234** ; Local Address = **10.20.20.1** ; Remote Address = **10.20.20.7**

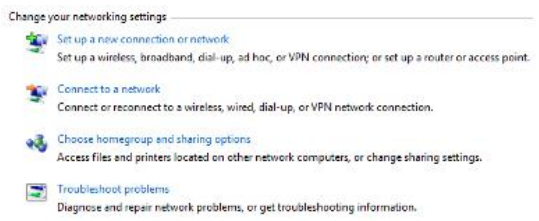



**Gambar 19** Setting PPP Client

Proses selanjutnya perlu melakukan konfigurasi PPTP Client pada Laptop. Langkah-langkahnya akan berbeda pada tiap OS. Berikut tutorial konfigurasi PPTP Client untuk OS Windows 7.

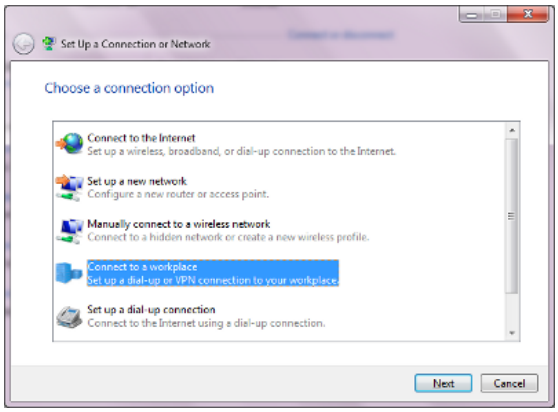
**Konfigurasi PPTP Client Windows 7**

Pastikan laptop sudah terkoneksi dengan internet. Masuk pada menu Network and Sharing Center, kemudian create koneksi baru dengan memilih **Set up new connection or network**.



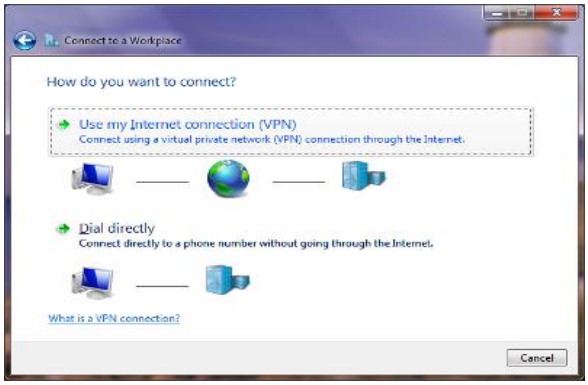

**Gambar 20** Setting Connection

Pada tampilan window selanjutnya, pilih **Connect to a workplace** , lalu klik next.



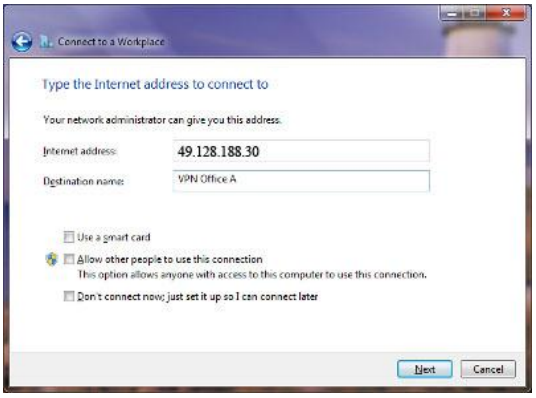

**Gambar 21** Connect Workplace

Kemudian, pilih **Use My Internet Connection (VPN)**



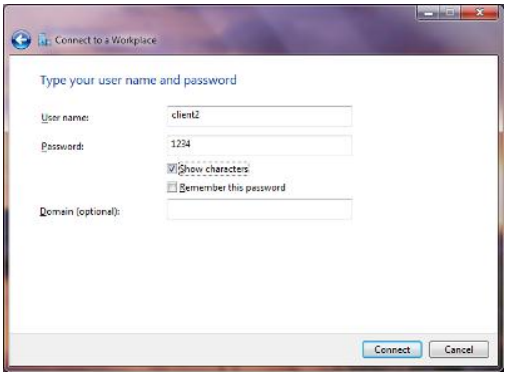

**Gambar 22** Connection VPN

Pada langkah berikutnya, koneksi ke jaringan VPN masukkan ke IP Address yang akan akan melakukan koneksi. Sesuai topologi , maka kita masukkan IP address public Router A. Destination name adalah parameter untuk memberikan nama pada interface VPN yang sedang dibuat.



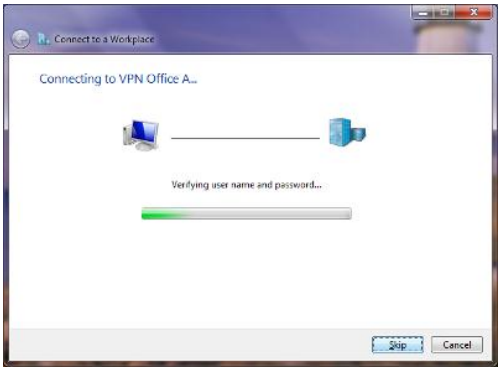

**Gambar 23** Setting Connection IP Public

Selanjutnya masukkan username dan password sesuai pengaturan Secret yang ada di PPTP server. Lalu klik Connect.




**Gambar 24** Inputan user dan password

Akan ada proses autentikasi, tunggu sampai selesai.



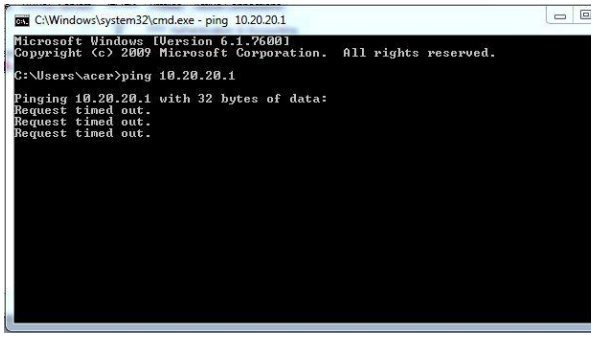

**Gambar 25** Dial ke sistem VPN

Jika proses setting telah selesai, dibagian network laptop akan muncul interface baru dengan nama VPN Office A dan terpasang IP address yang mengambil dari ip-pool Remote Address sesuai dengan pengaturan profile dan Secret pada PPTP Server. Koneksi VPN dari Laptop ke Router A sudah terbentuk. Laptop sudah bisa akses ke Router A dan Jaringan LAN A. Untuk melakukan remote ke Router A tinggal memasukkan IP address Router yang terpasang setelah link VPN terbentuk, yaitu IP address 10.20.20.1.

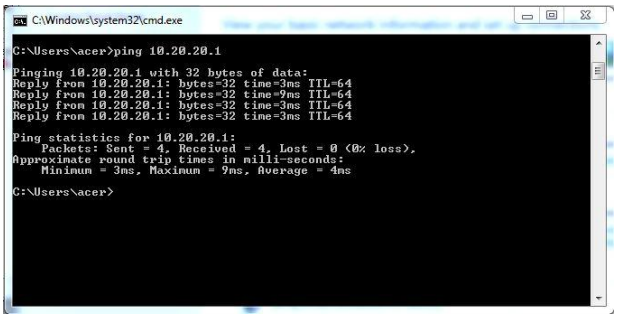
**Hasil Implementasi Sistem VPN**

Dalam melakukan pengujian terhadap sistem VPN yang sudah dibuat menggunakan tahap sebagai berikut :

1. Melakukan pengujian VPN server melalui tunneling yaitu dengan menggunakan ping dari client ke server sebelum dan sesudah diaktifkan VPN server.

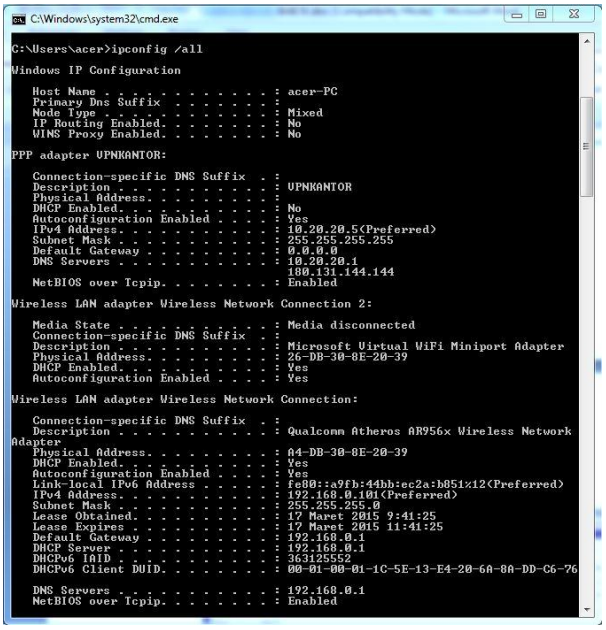



**Gambar 26** Sebelum diaktifkan VPN server




**Gambar 27** Sesudah diaktifkan VPN server

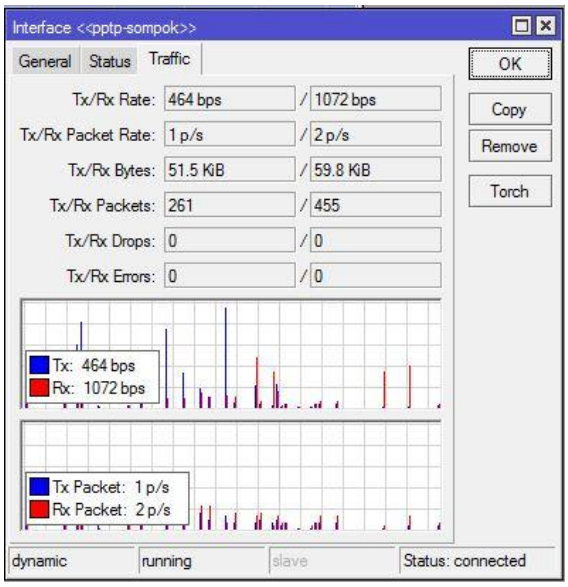
2. Melihat status konfigurasi interface client, untuk melihat konfigurasi pada client windows dengan perintah ipconfig /all setelah terhubung ke VPN server




**Gambar 28** Ethernet Adapter

Pada gambar 26 dan 27 terlihat pada saat proses transfer data tipe paket data ketika sebelum mengaktifkan VPN yang ditransfer adalah berupa protocol TCP yang lebih mementingkan keakuratan. Sedangkan ketika sesudah diaktifkan VPN protocol yang digunakan adalah Protokol UDP dipilih karena prinsipnya yang

mementingkan kecepatan akan menambah kecepatan transfer data melewati VPN.




**Gambar 29** Grafik Traffic Data

Dari gambar 29 diatas terlihat tranfer rate data pada jaringan VPN yang telah dibuat. Dari proses tersebut terjadi ketika client melakukan transfer file maka digrafik tersebut terlihat kecepatan transfernya. Untuk kecepatan transfer data tergantung dari ukuran data yang ditransfer dan kecepatan bandwith internet yang digunakan.

## 5. Kesimpulan

Berdasarkan penelitian yang dilakukan mengenai analisa dan perancangan VPN, kesimpulan yang dapat diambil dari hasil pembahasan bab – bab sebelumnya pada PT. Sampoerna Telekomunikasi Indonesia sebagai berikut, untuk merancang dan menerapkan sistem jaringan VPN di PT. Sampoerna Telekomunikasi Indonesia adalah sebagai berikut :

a. Perangkat router yang dipakai untuk membuat jaringan VPN tersebut menggunakan mikrotik dengan sistem operasi RouterOS.
b. Jaringan VPN diletakkan di server dengan kebutuhan jalur khusus dengan melakukan koneksi dari client ke server sehingga terbentuk koneksi point to point.
c. Untuk client memakai Router maupun PC yang disetting koneksi secara dial up sehingga terbentuk koneksi point to point.

## 6. Daftar Pustaka

Anhar, http://www.ilmukomputer.org, *Flowchart*, diakses tanggal 18 Februari 2015

Anonim, http://id.wikipedia.org, *Virtual Private Network*, diakses tanggal 22 Januari 2015.

Anonim, http://www.mikrotik.co.id, *Virtual Private Network Artikel*, diakses tanggal 22 Januari 2015.

Arikunto Suharsimi, 2005, *Manajemen Penelitian*, Yogyakarta : Penerbit Andi.

Deris Setiawan, 2005, *Sistem Keamanan Komputer*, Jakarta : Elex Media Komputindo.

EM Zulfajri, Ratu Aprilia Senja, 2008, *KLBI*, Jakarta: Difa Publisher.

Fathansyah, 2001, *Basis Data*, Bandung : Informatika.

Febrian Jack, 2004, *Pengetahuan Komputer dan Teknologi Informasi*, Bandung : Informatika Bandung.

Jogiyanto, 2005, *Analisis dan Desain Sistem Informasi*, Yogyakarta: Andi Offset.

Kadir Abdul, 2003, *Pengenalan Teknologi Informasi*, Yogyakarta : Andi Offset.

Mairs, J. 2002. VPNs: *A Beginner's Guide*.

Mulyono Hasyim, 2008, *Buku Pintar Komputer*, Jakarta : Kriya Pustaka.

Sutabri Tata, 2003, *Analisa Sistem Informasi*, Yogyakarta : Penerbit Andi.

Sugiyono, 2014, *Metode Penelitian Kuantitatif, Kualitatif dan Kombinasi*, Bandung : Alfabeta.

Syafrizal Melwin, *Pengantar Jaringan Komputer*, Yogyakarta : Andi Offset, 2005.

Wahana Komputer, 2005, *Kamus Lengkap Dunia Komputer*, Yogyakarta : Andi Offset.

Wahana Komputer, 2006, *Seri Penuntun Praktis Menginstalasi Perangkat Jaringan Komputer*, Yogyakarta : Andi Offse