PERANCANGAN JARINGAN KOMPUTER BERBASIS *VIRTUAL PRIVATE NETWORK* (VPN) PADA PT. TIKI JALUR NUGRAHA EKAKURIR

Bambang Mulyatno, Sulistiyo
Fakultas Teknik Program Studi Teknik Informatika Universitas Islam Attahiriyah
Jl. Melayu Kecil III No. 15, Tebet, Jakarta
bangmul@gmail.com

Abstrak

Latar Belakang PT. Tiki Jalur Nugraha Ekakurir (PT Tiki JNE)merupakan perusahaan yang melayani pengiriman cepat, kepabeanan serta distribusi di Indonesia. Dengan banyaknya bidang usaha yang digelutinya, maka Pt. Tiki Jalur Nugraha Ekakurir memiliki banyak cabang sehingga diperlukan suatu mekanisme pendistribusian data jarak jauh antara kantor pusat dengan kantor cabang. Perusahaan juga ingin memberikan fasilitas kepada pegawainya yang memiliki hak akses untuk terhubung ke jaringan lokal perusahaan dimanapun mereka berada. Untuk memenuhi kebutuhan tersebut, diperlukan suatu jaringan lokal yang jangkauannya luas dan tidak bisa diakses oleh sembarang orang, tetapi hanya orang yang memiliki hak akses saja yang dapat terhubung ke jaringan lokal perusahaan tersebut. Tujuan dari penelitian ini adalah untuk merancang suatu jaringan antara kantor pusat dengan kantor cabang serta *mobile user* pada PT. TIKI JALUR NUGRAHA EKAKURIR yang dapat dimanfaatkan untuk meningkatkan kinerja dan efektifitas perusahaan dalam melaksanakan proses bisnisnya. Hasil yang dicapai ini, diharapkan agar sistem yang baru dapat mendukung dan melengkapi sistem yang sudah berjalan dimana informasi akan dapat disampaikan dengan lebih efektif dan efisien. Sistim baru ini juga mampu mengurangi biaya komunikasi antar kantor cabang, mempunyai akses jarak jauh dari luar kantor atau kantor cabang ke kantor pusat, dan tersedia jaringan khusus dalam dunia maya atau internet. Simpulan dari penelitian ini, Teknologi VPN mampu memenuhi kebutuhan tersebut dengan menggunakan metode *authentifikasi user* serta memberi kemudahan bagi pegawai yang memiliki hak akses untuk mengakses jaringan lokal perusahaan dari mana saja, karena VPN terhubung ke internet, dapat mereduksi biaya operasional PT. TIKI JALUR NUGRAHA EKAKURIR karena tidak perlu membayar biaya sewa bulanan kabel (*leased line*) yang mahal. VPN menggunakan internet sebagai media komunikasinya.

Kata kunci: jaringan, topologi, *vitual private network*

Pendahuluan

Pada tahun 2009-an sekarang ini, setiap perusahaan atau organisasi harus dinamis dan mampu bergerak cepat serta mampu menghasilkan suatu informasi yang cepat dan akurat untuk menunjang pengambilan keputusan bagi pihak manajemen. Data dan informasi perlu dikelola secara baik dan profesional agar tujuan perusahaan dapat tercapai secara efektif dan efisien.

Untuk memenuhi kebutuhan tersebut, diperlukan teknologi informasi yang merupakan teknologi yang menggabungkan komputasi atau komputer dengan jalur komunikasi berkecepatan tinggi yang membawa data, suara dan video. Salah satu dukungan Teknologi Informasi adalah internet atau jaringan internet yang berperan sebagai jalur distribusi informasi. Internet telah sangat mengurangi batasan jarak dan waktu. Kini, seorang karyawan yang sedang berada jauh dari kantornya tidak perlu lagi untuk kembali ke kantor untuk sekedar mengambil data yang tersimpan pada *database* kantor.

Virtual Private Network (VPN) merupakan suatu cara untuk membuat sebuah jaringan yang bersifat *private* dan aman untuk mengakses jaringan lokal dengan menggunakan sarana jaringan publik (internet). Dengan menggunakan jaringan publik ini, maka *user* dapat mengakses fitur-fitur yang ada di dalam jaringan lokalnya, mendapatkan hak dan pengaturan yang sama bagaikan secara fisik kita berada di tempat dimana jaringan lokal itu berada.

PT. Tiki Jalur Nugraha Ekakurir (PT Tiki JNE)merupakan perusahaan yang melayani pengiriman cepat, kepabeanan serta distribusi di Indonesia. Dengan banyaknya bidang usaha yang digelutinya, maka Pt. Tiki Jalur Nugraha Ekakurir memiliki banyak cabang sehingga diperlukan suatu mekanisme pendistribusian data jarak jauh antara kantor pusat dengan kantor cabang. Perusahaan juga ingin memberikan fasilitas kepada pegawainya yang memiliki hak akses untuk terhubung ke jaringan lokal perusahaan dimanapun mereka berada. Untuk memenuhi kebutuhan tersebut, diperlukan suatu jaringan lokal yang jangkauannya luas dan tidak bisa diakses oleh sembarang orang, tetapi hanya orang yang memiliki hak akses saja yang dapat terhubung ke jaringan lokal perusahaan tersebut.

Saat ini PT TIKI JALUR NUGRAHA EKAKURIR menggunakan jaringan publik (internet) dan jaringan khusus (*leased line*) untuk koneksi antara kantor pusat dengan kantor cabang. Terhubungnya jaringan lokal ke internet tentunya memudahkan proses distribusi data antara kantor pusat dengan kantor cabang,sehingga penggunaan jaringan khusus pada perusahaan membutuhkan biaya yang besar untuk membangun infrastruktur jaringan perusahaan yang luas.

Analisa Sistem yang Berjalan

Berdasarkan hasil analisis yang telah dilakukan, dapat disimpulkan bahwa saat ini perusahaan mengalami permasalahan sebagai berikut :

1. Belum adanya teknologi *internet* yang dipisahkan secara khusus tanpa dapat diakses oleh orang yang tidak berkepentingan.
2. Penggunaan jaringan khusus *leased line* membutuhkan biaya yang besar untuk pembangunan infrastruktur jaringan perusahaan yang luas.
3. Belum tersedianya koneksi jaringan ke kantor pusat bagi *mobile user* untuk mengakses maupun mengirimkan data. Kebutuhan koneksi ke jaringan pusat bagi *mobile user* ini seperti Direktur dan Manajer yang ingin senantiasa melakukan pemeriksaan laporan keuangan pada perusahaan. Kesulitan yang dihadapi adalah kebutuhan untuk melakukan pemeriksaan keuangan saat berada di luar kantor baik di dalam maupun di luar kota.

Usulan Pemecahan Masalah

Dengan adanya beberapa permasalahan pada sistem jaringan komputer yang digunakan saat ini, PT. TIKI JNE memerlukan solusi untuk mengatasi masalah-masalah tersebut. Tujuan dari solusi ini diusulkan untuk merancang jaringan WAN menggunakan teknologi *virtual private network* (VPN) dengan pertimbangan-pertimbangan sebagai berikut :

1. Authentifikasi user VPN mengijinkan client dan server membangun identitas dalam jaringan dengan benar.
2. Teknologi VPN adalah teknologi yang mampu membuat data yang dikirim lebih dahulu dibungkus (*tunnel*) dan diacak (*encrypt*) sehingga sulit diakses dan dilihat oleh orang yang tidak berkepentingan.
3. Penggunaaan VPN dapat mereduksi biaya operasional karena tidak perlu membayar biaya sewa bulanan kabel (*leased line*) yang mahal. VPN menggunakan internet sebagai media komunikasinya.
4. VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga Direktur, Manajer, dan pegawai yang memiliki hak akses dapat mengakses jaringan lokal perusahaan di manapun dia berada.
5. Tersedianya aplikasi yang memungkinkan perusahaan untuk melakukan layanan pengiriman Data, VoIP, Video Conference, Audio Conference, Intranet dan Ekstranet.

Implementasi

Untuk mengimplementasikan sistem yang diusulkan, perlu memperhatikan kebutuhan *hardware* dan *software* baik pada server maupun klien. Setelah itu baru kita mengkonfigurasi VPN server dan VPN client. Setelah semuanya selesai dikonfigurasi, baru kita evaluasi. Karena keterbatasan akses pada ruang server yang tidak terbuka untuk umum, implementasi yang dilakukan

hanya meliputi penginstalasian sistem, sedangkan evaluasi akan dilakukan dengan simulasi jaringan menggunakan *software* simulator *Packet Tracer 5.0.*

Kebutuhan sistem pada server

Untuk mengkonfigurasi sebuah PC menjadi server kita harus memperhatikan kebutuhan *hardware* dan *software* PC untuk dapat menjalankan sistem operasi yang dipilih. Oleh karena itu dibutuhkan hal-hal seperti:

Hardware

Spesifikasi *hardware* yang dianjurkan untuk mengkonfigurasi PC menjadi sebuah server adalah sebagai berikut :

a. Processor : Pentium IV
b. Memory RAM : 1 GB
c. Hard disk : 40 GB

Software

Standarisasi *software* yang diperlukan pada server adalah sebagai berikut :

a. Sistem Operasi : Microsoft Windows Server 2003 Standar Edition atau Enterprise Edition (*licensed*).
b. Microsoft Office 2003
c. Adobe Acrobat Reader V.5.0 or later
d. Internet Explorer V.6.0 or later
e. Antivirus Symantec Client
f. JINIT 1.3.1.13 & JINIT 1.3.1.22

Kebutuhan sistem pada client

Rancangan sistem jaringan VPN yang diusulkan akan membutuhkan komputer untuk berlaku sebagai klien dengan spesifikasi sebagai berikut atas dasar kebutuhan untuk menjalankan kegiatan operasional perusahaan:

1. *Hardware*

Spesifikasi *hardware* yang dianjurkan untuk mengkonfigurasi PC menjadi sebuah client adalah sebagai berikut :

a. Processor : Pentium IV
b. Memory RAM : 512 MB
c. HDD : 10 GB

2. *Software*

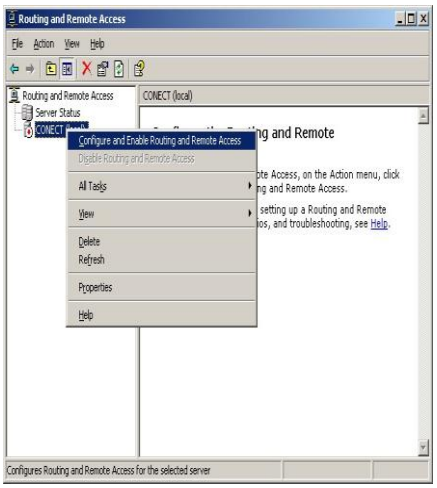
Standarisasi *software* yang diperlukan pada client adalah sebagai berikut :

a. Sistem Operasi : Microsoft Windows XP SP2 (*licensed*).
b. Microsoft Office 2003
c. Adobe Acrobat Reader V.5.0 or later
d. Internet Explorer V.6.0 or later
e. Antivirus Symantec Client
f. JINIT 1.3.1.13 & JINIT 1.3.1.22

Konfigurasi VPN Server

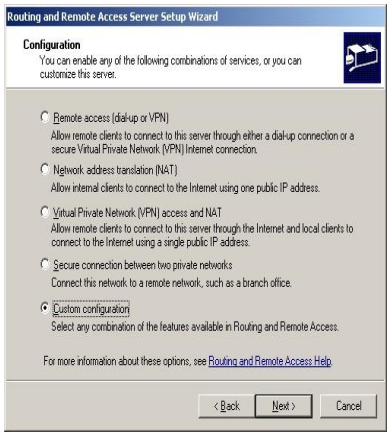
Proses konfigurasi VPN server dengan system operasi Windows Server 2003 adalah sebagai berikut :

1. Pastikan semua koneksi ke internet dan jaringan lokal sudah berjalan dengan baik.
2. Klik menu *Start>Programs>Administrative Tools>Routing and Remote Access*.
3. Pada bagian kiri window, klik kanan pada nama server yang ditampilkan, kemudian pilih *Configure andEnable Routing and Remote Access.*



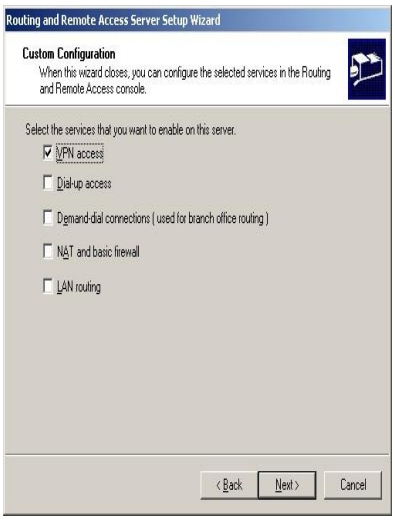
Gambar 1
Mengkonfigurasi *server*

4. Pilih *Custom configuration*, kemudian klik Next.



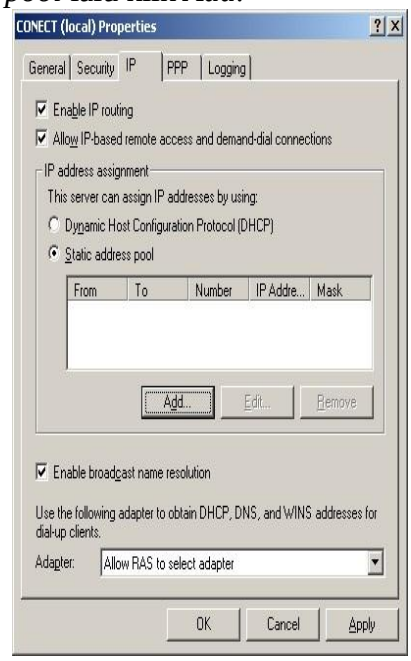
Gambar 2
Pemilihan *custom configuration*

5. *Check list VPN Access*, kemudian klik *Next*. Setelah itu klik tombol *Finish*.



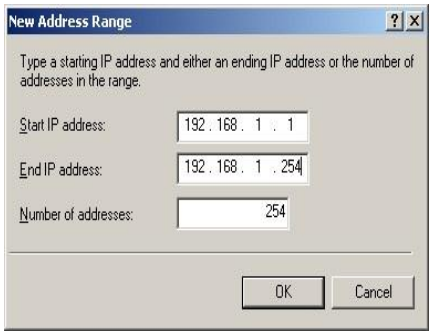
Gambar 3
Pemilihan *service* yang diinginkan pada *server*

6. Setelah selesai, lakukan pengaturan umum server dengan cara klik kanan pada nama server lalu pilih *Properties*.
7. Klik tab IP. Bagian ini mengatur akses data VPN klien. Perhatikan pada bagian *IP Address Assigment*, pilih *static address pool* lalu klik *Add*.



Gambar 4
Pengaturan akses data

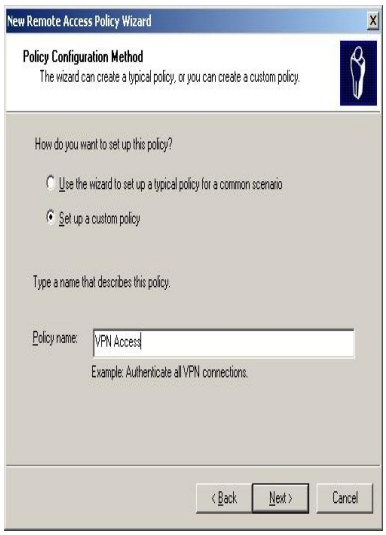
8. Setelah itu masukkan IP range yang akan dialokasikan oleh VPN server kepada kliennya. Setelah selesai klik OK.



Gambar 5
Address range assignment

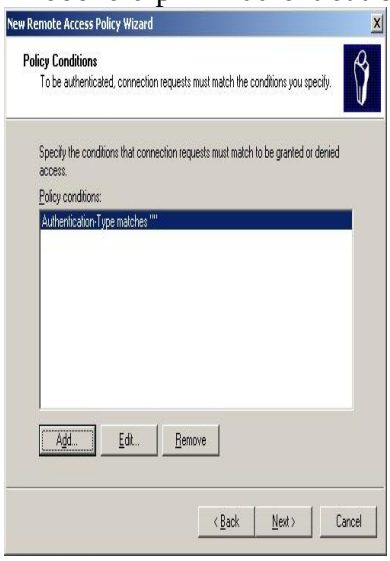
Pada tahap ini konfigurasi VPN server sudah selesai. Namun ada baiknya juga untuk mengatur beberapa pilihan lain sesuai dengan kebutuhan perusahaan, di antaranya membuat sebuah *remote access policy*. Cara membuatnya adalah sebagai berikut :

1. Buka jendela *Routing and Remote Access* seperti langkah sebelumnya. Klik kanan pada *Remote Access Policies*, kemudian pilih *New RemoteAccess Policies.*
2. Pada kotak dialog *Policy Configuration Method*, pilih *set up a custom policy* kemudian masukkan nama yang diinginkan (misalnya VPN Access).



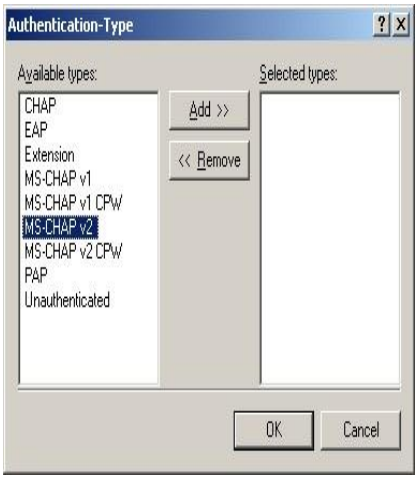
Gambar 6
Konfigurasi Remote Access Policy

3. Pada bagian *policy condition*, klik add lalu pilih *Authentication Type*.



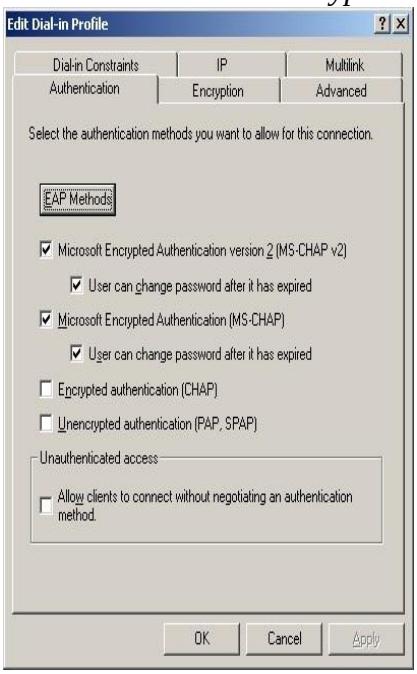
Gambar 7
Policy Condition

4. Pilih MS CHAP v2 dan klik tombol Add kemudian klik OK.



Gambar 8
Authentication Type

1. Klik tombol *Edit Profile*, akan tampil pengaturan-pengaturan yang bisa diatur sesuai dengan kebutuhan. Seperti protokol *authentication* dan *encryption* pada VPN.



Gambar 9
Pengaturan profile VPN

2. Klik tombol OK dan dilanjutkan dengan Next sampai proses konfigurasi selesai.

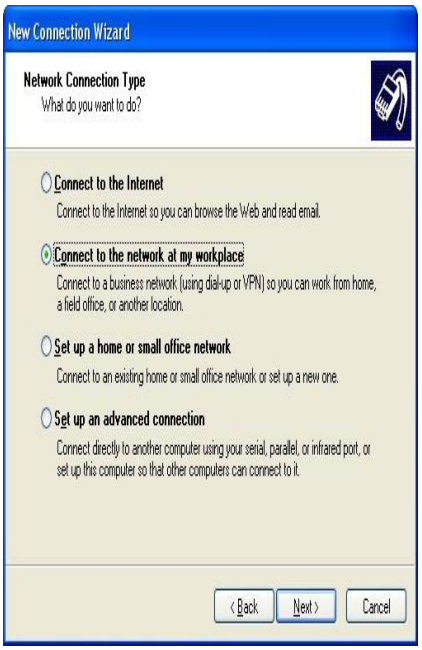
Konfigurasi VPN Client

Setelah konfigurasi pada server VPN selesai dilakukan, selanjutnya dilakukan konfigurasi pada klien VPN. Proses Konfigurasi VPN client dengan sistem operasi Windows XP adalah sebagai berikut :

1. Pastikan internet sudah aktif (*connected*), bisa digunakan untuk akses internet.
2. Buat koneksi baru dengan cara klik menu *Start>Control Panel>Network Connection>Create a new connection*. Jendela *New Connection Wizard* akan ditampilkan.

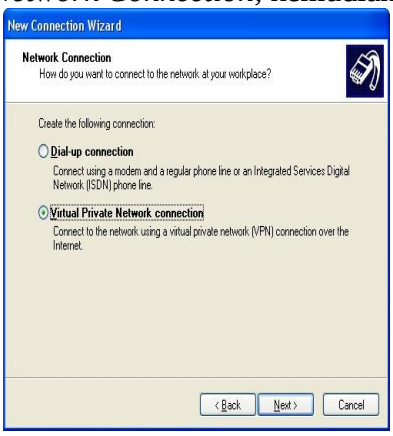
Gambar 10
Jendela *New Connection Wizard*

1. Klik *Next*, kemudian pilih option *Connect to the network at my workplace*. Selanjutnya klik *Next*.



Gambar 11
Memilih tipe koneksi jaringan

2. Pilih option *Virtual Private Network Connection*, kemudian klik *Next*.

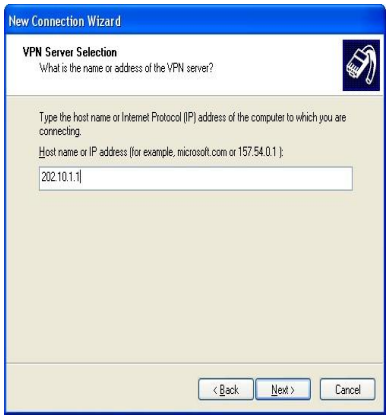


Gambar 12
Membuat koneksi *Virtual Private Network*

3. Masukkan nama perusahaan kemudian klik *Next*.

Gambar 13
Memasukkan nama perusahaan

4. Setelah itu masukkan alamat IP atau nama host VPN Server kemudian klik *Next*.



Gambar 14
Memasukkan alamat IP VPN server

5. Klik Finish.

Gambar 15
Selesai membuat koneksi

6. Setelah konfigurasi selesai, klien dapat login ke server VPN dengan memasukkan Username dan Password yang telah terdapat pada admin.

Gambar 16
Proses otentifikasi *username* dan *password*

Setelah selesai bekerja sebaiknya koneksi VPN Client diputuskan (*disconnect*). Langkah-langkah untuk melakukan proses *disconnect* dari VPN Client adalah sebagai berikut :

1. Buka jendela *Network Connection*.
2. Klik kanan ikon koneksi jaringan *Virtual Provate Network* TIKI JNE.
3. Pilih dan klik *Disconnect*.

Evaluasi dengan Simulasi

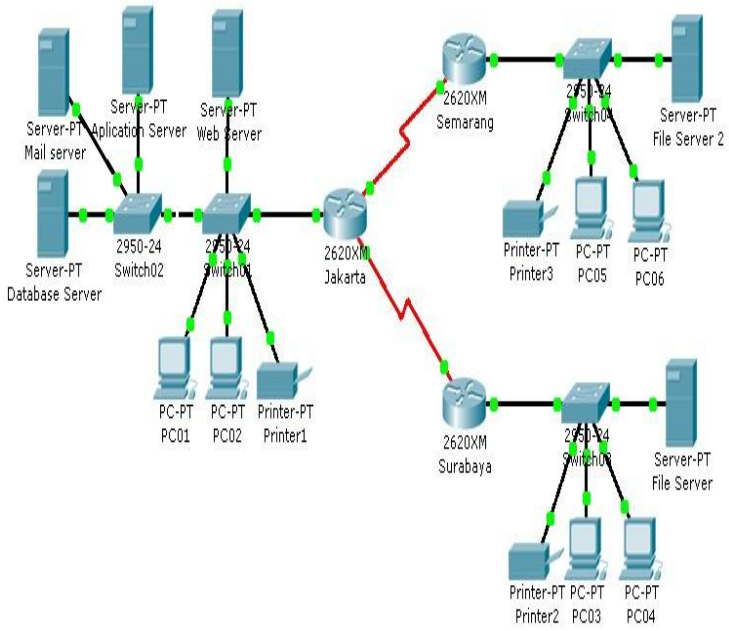
Evaluasi sistem akan dilakukan dengan menggunakan *software* simulasi *Packet Tracer 5.0*. Hal ini disebabkan keterbatasan akses pada jaringan perusahaan yang tidak terbuka untuk umum. Simulasi adalah model dari realitas sehingga tujuan dibuatnya simulasi ini adalah untuk mengetahui apakah jaringan yang dirancang dapat berjalan dengan baik.

Packet Tracer adalah sebuah *software* yang dikembangkan oleh Cisco. imana *software* tersebut berfungsi untuk membuat suatu jaringan komputer atau sering disebut dengan *computer network*. Dalam *software* ini telah tersedia komponen–kompenen atau alat–alat yang sering dipakai atau digunakan dalam *system network* tersebut, seperti kabel LAN (*cross over*, *console*), hub, switch, router dan lain sebagainya, sehingga kita dapat dengan mudah membuat sebuah simulasi jaringan computer di dalam PC. Simulasi ini berfungsi untuk mengetahui cara kerja pada tiap–tiap alat tersebut dan cara pengiriman sebuah pesan / data dari komputer satu ke komputer lain.

Keutungan menggunakan program simulasi ini adalah lebih hemat waktu dalam bekerja menggunakan *software* / *hardware*, kemampuan untuk mencoba berbagai macam skenario dari *hardware* dan *software*, dan kemampuan untuk memprediksi masalah yang potensial dari *software* dan *hardware* yang digunakan sebelum penggunaan sebenarnya. Ada beberapa batasan yang terdapat pada program simulasi ini, antara lain :

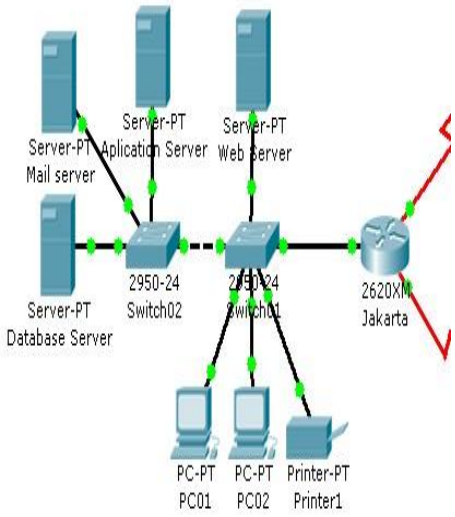
1. Tidak adanya konfigurasi mendetail tentang spesifikasi komputer
2. Keterbatasan jenis *hardware* yang digunakan

Struktur simulasi jaringan PT. TIKI JALUR NUGRAHA EKAKURIR adalah sebagai berikut :



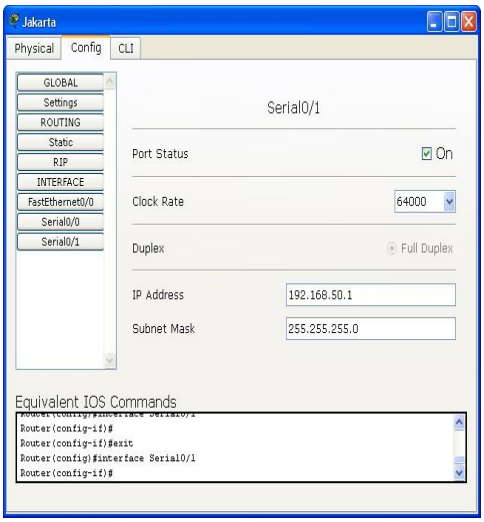
Gambar 17
Struktur simulasi jaringan perusahaan

Pada gambar 17. menunjukkan hubungan antar kantor pusat di Jakarta dengan kantor cabang di Semarang dan Surabaya yang digambarkan dengan 3 buah router yang saling terhubung melalui jaringan internet. Bila struktur jaringan pada kantor pusat dilihat lebih dalam, maka akan terlihat seperti gambar 4.20. Gambar di bawah merupakan gambaran umum struktur jaringan yang ada pada kantor pusat yang disimulasikan.



Gambar 18
Struktur simulasi jaringan pada kantor pusat

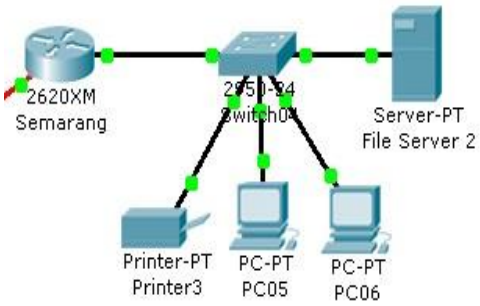
Pada router kantor pusat perlu diberi pengaturan *clock rate* ke kantor cabang agar router-router tersebut dapat saling terhubung sehingga dapat melakukan komunikasi dan transfer data. Klik router yang berada di kantor pusat tersebut untuk dilakukan berbagai pengaturan oleh *user* seperti yang ditunjukkan pada gambar 19.



Gambar 19
Pengaturan router pada kantor pusat

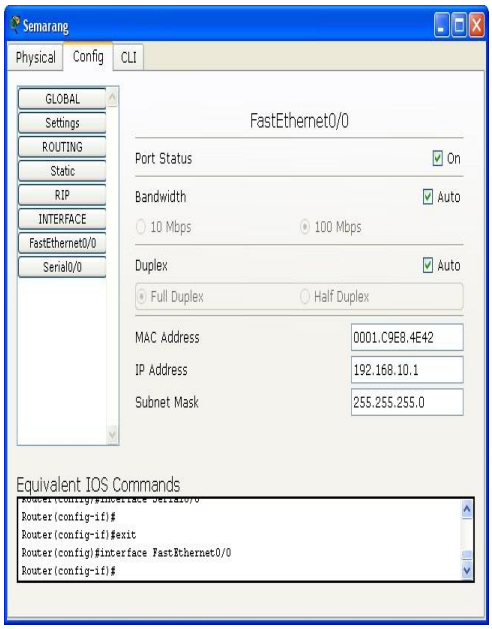
Pada konfigurasi FastEthernet0/0, masukkan *IP Address* 192.168.40.1 dan *Subnet Mask* 255.255.255.0. Pada konfigurasi Serial0/0, masukkan *IP Address* 192.168.20.1 dan *Subnet Mask* 255.255.255.0 serta beri pengaturan *Clock Rate* 64000. Pada konfigurasi Serial0/1, masukkan *IP Address* 192.168.50.1 dan *Subnet Mask* 255.255.255.0 serta beri pengaturan *Clock Rate* 64000.

Selanjutnya apabila struktur jaringan pada kantor cabang dilihat lebih dalam, maka akan terlihat seperti gambar 20. Gambar 20 merupakan gambaran umum struktur jaringan yang ada pada setiap kantor cabang yang disimulasikan.



Gambar 20
Struktur simulasi jaringan pada kantor cabang

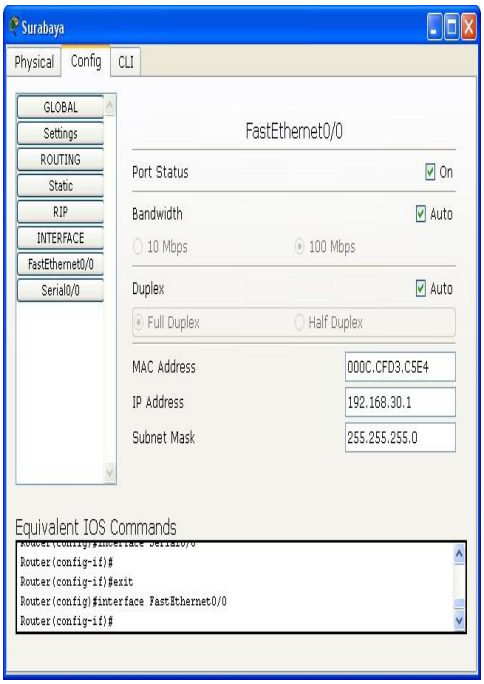
Pada *router* kantor cabang Semarang perlu diberi pengaturan. Klik router yang berada di kantor cabang tersebut untuk dilakukan berbagai pengaturan oleh *user* seperti yang ditunjukkan pada gambar 21.



Gambar 21
Pengaturan router pada kantor cabang Semarang

Pada konfigurasi FastEthernet0/0, masukkan *IP Address* 192.168.10.1 dan *Subnet Mask* 255.255.255.0. Pada konfigurasi Serial0/0, masukkan *IP Address* 192.168.20.2 dan *Subnet Mask* 255.255.255.0.

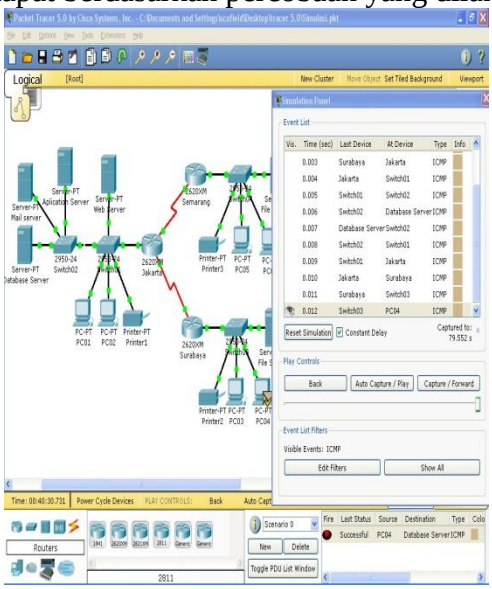
Pada router kantor cabang Surabaya juga perlu diberi pengaturan. Klik router yang berada di kantor cabang tersebut untuk dilakukan berbagai pengaturan oleh *user* seperti yang ditunjukkan pada gambar 22.



Gambar 22
Pengaturan router pada kantor cabang Surabaya

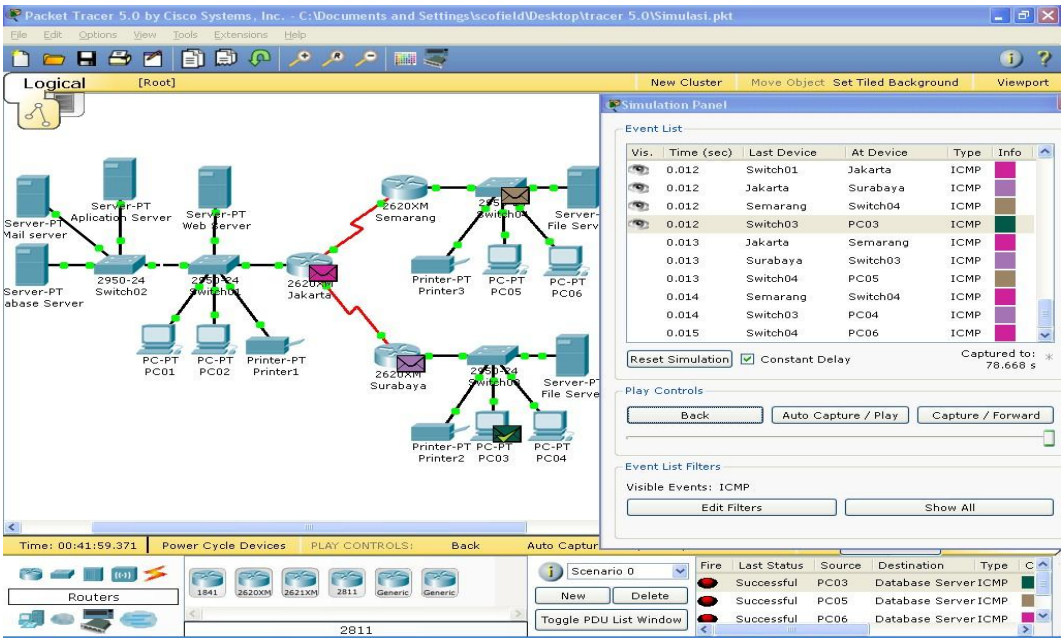
Pada konfigurasi FastEthernet0/0, masukkan *IP Address* 192.168.30.1 dan *Subnet Mask* 255.255.255.0. Pada konfigurasi Serial0/0, masukkan *IP Address* 192.168.50.5 dan *Subnet Mask* 255.255.255.0.

Setelah seluruh proses konfigurasi selesai, selanjutnya akan dilakukan percobaan simulasi. Percobaan simulasi ini dilakukan dengan dua skenario, pada skenario pertama terdapat 1 *client* yang mengakses VPN. *Client* ini melakukan proses pengiriman data dari kantor cabang ke kantor pusat. Pada skenario kedua terdapat 4 *client* yang secara bersama-sama melakukan proses pengiriman data ke kantor pusat. Hasil yang didapat berdasarkan percobaan yang dilakukan adalah sebagai berikut :



Gambar 23
Proses pengiriman data satu *client*

Pada gambar 24 menunjukkan lamanya *delay* proses pengiriman data 1 *client*, yaitu selama 79,552 detik.



Gambar 24
Proses pengiriman data empat client

Pada gambar 25 menunjukkan lamanya *delay* proses pengiriman data 4 client, yaitu selama 78,668 detik. Setelah dilakukan 3 kali percobaan pengiriman data pada masing-masing skenario tersebut maka dapat dilihat nilai perbandingannya sebagai berikut :

Tabel 1
Perbandingan delay proses pengiriman data

Percobaan	Proses delay 1 client (Sec)	Proses delay 4 client (sec)
1	79.552	78.668
2	77.869	78.142
3	78.903	78.116

Berdasarkan percobaan 1 dan 3 pada tabel 1, dapat dilihat bahwa proses *delay time* pengiriman data 4 *client* lebih cepat dibandingkan proses *delay time* pengiriman data 1 *client*. Hal ini menunjukkan bahwa proses *delay time* dari server VPN tidak dipengaruhi oleh perbedaan jumlah *client* yang mengirimkan data.

Kesimpulan

Berdasarkan hasil analisa dan perancangan sistem jaringan yang diusulkan, maka dapat diambil beberapa kesimpulan sebagai berikut : (1) Dalam melakukan pengiriman dan penerimaan data melalui internet, PT. TIKI JALUR NUGRAHA EKAKURIR memerlukan teknologi internet yang dipisahkan secara khusus tanpa dapat diakses oleh orang yang tidak berkepentingan. Teknologi VPN mampu memenuhi kebutuhan tersebut dengan menggunakan metode *authentifikasi user*. Metode enkripsi mengijinkan data yang bersifat sensitif untuk disembunyikan dari publik; (2) Penggunaan teknologi VPN memberi kemudahan bagi pegawai yang memiliki hak akses untuk mengakses jaringan lokal perusahaan dari mana saja, karena VPN terhubung ke internet; (3) Penggunaan teknologi VPN dapat mereduksi biaya operasional PT. TIKI JALUR NUGRAHA EKAKURIR karena tidak perlu membayar biaya sewa bulanan kabel (*leased line*) yang mahal. VPN menggunakan internet sebagai media komunikasinya; (4) Sistem yang diusulkan masih memiliki kelebihan yakni Tidak perlu perombakkan struktur jaringan yang sudah ada, sehingga dapat memanfaatkan struktur yang sudah ada, jadi implementasinya lebih mudah dan murah. Kemudahan dalam penggunaan sistem yang baru. Namun ada pula kekurangannya yaitu Perfoma

VPN sangat tergantung pada jaringan internet karena traffic yang terjadi di internet melibatkan semua pihak pengguna internet di seluruh dunia.

Daftar Pustaka

Deris, "Jenis-Jenis Jaringan Komputer", www.ilkom.unsri.ac.id /deris/akademik/files/2009 /jarkom_IF diakses tanggal 5 Nopember 2009.

M. Gupta, "Authentication/Confidentiality for OSPFv2", Juniper Network, Tahun 2009.

M. Gupta, "Elliptic Curve *Cryptography*: The Next Generation of Internet Security", Sun Labs white paper released at SunNetwork, Tahun *2003.*

Microsoft, "How To Configure IPSec Tunneling in Windows Server 2003", http://support.microsoft.com/kb/816514, diakses tanggal 17 Nopember 2009.

Shedtya, "Tutorial dan Ebook windows server 2003", http://blog.shedtya.web.id/2008/06/instalasi-windows-server-2003.html, diakses tanggal 29 Nopember 2009.

Tanenbaum, Andrew S., "Jaringan Komputer", jilid 1-2, Prenhallindo, Jakarta, tahun 2000.

Telkomlink, "VPN IP MPLS", http://main.telkom.net/index.php?option=com_content&task=view&id=28&Itemid=59 , diakses tanggal 18 Nopember 2009