IMPLEMENTASI *WIDE AREA NETWORK* MENGGUNAKAN TEKNOLOGI VPN BERBASISKAN *IP MULTI PROTOCOL LABEL SWITCHING* (MPLS) : STUDI KASUS PADA KAMPUS BINA SARANA INFORMATIKA

Oleh : **H. Mochamad Wahyudi**

ABSTRAK

Wide Area Network (WAN) dipergunakan untuk menghubungkan jaringan-jaringan *Local Area Network (LAN)* satu dengan lainnya yang berdekatan maupun yang berjauhan dan menggunakan protokol yang sama atau berbeda-beda.

Teknologi yang dapat dipergunakan untuk dapat menghubungkan *WAN,* antara lain: *Dial Up, Leased Line, VSAT, X.25, Frame Relay, Virtual Private Network (VPN)* dan lain-lain. Sedangkan teknologi terbaru yang saat ini sedang dikembangkan untuk membangun jaringan *WAN* yang baik *(realible)* dan permanen adalah *Virtual Private Network* (*VPN*) berbasis *IP Multi Protocol Label Switch* (*VPN IP MPLS*).

VPN IP MPLS ini adalah suatu layanan komunikasi data *any to any connections* berbasis *IP Multi Protocol Label Switch* dengan menggunakan peralatan *(hardware)* dari perusahaan *Cisco* (berupa *Cisco Router* dan *Cisco Switch Catalist*).

Kampus Bina Sarana Informatika (BSI) menggunakan teknologi *VPN IP MPLS* untuk menghubungkan seluruh kampusnya yang terdiri dari 35 lokasi yang tersebar dibeberapa kota yang ada di Indonesia.

Kampus BSI menerapkan sistem domain berbasis sistem Operasi Windows Server 2003 untuk semua untuk yang ada dan menjalankan aplikasi *online* yang disebut dengan *intranet.bsi.ac.id* serta beberapa aplikasi lain.

Untuk menghubungkan seluruh Kampus BSI jaringan global *(internet),* semua Kampus BSI terhubung melalui saluran *Leased Line* sebesar 2.048 Kbps yang terdapat pada Kampus BSI Menara Salemba yang berfungsi sebagai *Backhole*.

I. PENDAHULUAN

Wide Area Network (WAN) dipergunakan untuk menghubungkan jaringan-jaringan *Local Area Network (LAN)* satu dengan lainnya yang berdekatan maupun yang berjauhan dan menggunakan protokol yang sama atau berbeda-beda. Jika pada *LAN* hubungan jaringan komputer dapat dilakukan dengan perantara kabel-kabel milik internal perusahaan seperti : Kabel Koaksial, Kabel UTP / RJ-45, Serat Optik dan lain-lain, maka pada jaringan *WAN* pada umumnya jaringan komputer dihubungan melalui jaringan milik perusahaan telekomunikasi sebagai media perantara. Perusahaan telekomunikasi yang menyediakan sambungan untuk *WAN* tersebut antara laian : PT. Telekomunikasi Indonesia, PT. Indosat, PT. Lintas Arta, PT. Excelcomindo Pratama (XL) dan lain-lain.

WAN dipergunakan untuk menghubungi jaringan-jaringan LAN satu dengan yang lainnya yang berdekatan maupun yang berjauhan dan menggunakan protokol yang sama atau berbeda.

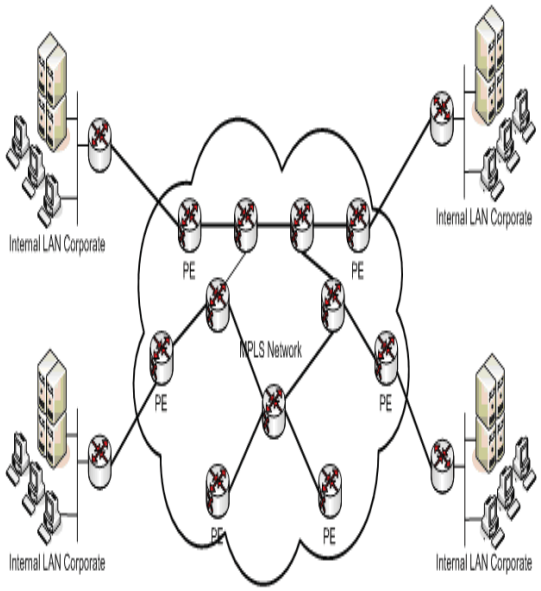
Menurut Hendra Wijaya [2004, Hal. 154] beberapa teknologi yang dapat dipergunakan untuk dapat menghubungkan WAN, antara lain : *Dial Up, Leased Line, VSAT, X.25, Frame Relay, Virtual Private Network (VPN),* dan lain-lain.

Adapun teknologi terbaru yang saat ini sedang dikembangkan untuk membangun jaringan *WAN* yang baik *(realible)* dan permanen adalah *Virtual Private Network* (*VPN*) berbasis *IP Multi Protocol Label Switch* (*VPN IP MPLS*). Menurut tulisan yang berjudul *Solusi Enterprise - IP Virtual Network* yang diambil dari *website* http://www.telkom.co.id/produk-layanan/korporat/data-internet/solusi-enterprise-ip-virtual-network.html, *VPN IP MPLS* disebutkan sebagai suatu layanan komunikasi data *any to any connections* berbasis *IP Multi Protocol Label Switch* dengan menggunakan peralatan *(hardware)* dari perusahaan *Cisco* (berupa *Cisco Router* dan *Cisco Switch Catalist*). Layanan ini memiliki kelebihan dibandingkan dengan layanan komunikasi data melalui *Leased Line* maupun *Frame Relay* yang menggunakan teknologi yang lebih tua.

Teknologi *VPN IP MPLS* merupakan suatu layanan yang dibangun di atas *Integrated Network Architecture* yang secara dinamis dapat mengenali jenis aplikasi *enterprice* untuk memperoleh layanan *end to end security*, *performance* dan *aviability.* Teknologi *VPN IP MPLS* ini merupakan solusi yang sangat praktis bagi suatu institusi yang menginginkan komunikasi secara terus menerus (intensif) antara kantor-kantor cabang dengan kantor pusatnya. *VPN IP MPLS* digunakan untuk merealisasikan *Class of Service* (CoS), dimana suatu institusi dapat mengimplementasikan aplikasinya baik berupa aplikasi yang memiliki *Delay Time Sensitive*, *Mission Critical* maupun *Non Mission Critical* pada satu *platform* jaringan *private IP MPLS*.

a. Karakteristik dan Konfigurasi layanan *VPN IP* MPLS.

Pada gambar bawah ini penulis akan jelaskan mengenai konfigurasi yang diberikan oleh Telkom untuk produk layanan *VPN IP* MPLS.



Gambar I.1. Konfigurasi Infrastuktur *VPN IP MPLS*

b. Sistem Keamanan *VPN IP MPLS*

VPN IP MPLS diciptakan untuk memenuhi kebutuhan akan layanan data komunikasi yang mempunyai fleksibilitas tinggi seperti *network* berbasis *IP (Internet)* namun tetap bersifat *Privacy/Secure* dan mampu menerapkan *Quality of Service (QoS)* seperti jaringan *Frame Relay*. Cara kerja *MPLS* adalah melewatkan paket *(Forward)* berdasarkan *Label,* dan menggunakan teknologi *Switching* bukan *Routing.*

Teknologi *MPLS* memiliki tingkat keamanan yang sangat tinggi atau baik, tidak kalah dengan keamanan pada jaringan *Frame Relay* maupun *ATM*. Penerapan *VPN IP MPLS* suatu institusi yang sangat mengutamakan keamanan datanya, tingkat keamanan *MPLS* ini masih dapat ditingkatkan lagi dengan menggabungkan teknologi *MPLS* dan teknologi *IPSec* yang menerapkan mekanisme *tunneling* dan enkripsi untuk keamanan serta kriptografi yang secara fleksibel dapat mendukung kombinasi dari autentifikasi, integrasi, akses kontrol dan kerahasiaan.

c. Jenis layanan *VPN IP MPLS*

Standar paket layanan *VPN IP* adalah berdasarkan *Class of Service (CoS) VPN IP* dengan beberapa tipe paket *CoS* yang terdapat pada Telkom adalah :

1). *VPN IP Interactive*

Tabel berikut ini adalah penjelasan mengenai paket *VPN IP Interactive.*

Tabel I.1. *VPN IP Interactive*

Class of Service	Description	Application	SLA Parameter	CPE Services
VPN IP Interactive	Services to support real time communication applications with high sensitivity to delay and jitter. - IP PBX - IP Video Conference - IP Surveillance	Voice Call & Video Conferencing	Network Availability = 99% Latency = 125 ms Jitter = 75 ms Packet Loss <= 0.5%	Managed

2). *VPN IP Gold*

Tabel berikut ini adalah penjelasan mengenai paket *VPN IP Interactive.*

Tabel I.2. *VPN IP Gold*

Class of Service	Description	Application	SLA Parameter	CPE Services
VPN IP Gold	Services to support mission critical which are real time and time dependent: - Intranet - Extranet - Disaster Recovery - Carrier Interconnect	SAP,Siebel,Oracle,Baan,people Soft,Citrix	Network Availability = 99% Latency = 125-150 ms Packet Loss <= 5%	Managed

3). *VPN IP Silver*

Tabel berikut ini adalah penjelasan mengenai pake *VPN IP Interactive.*

Tabel I.3. *VPN IP Silver*

Class of Service	Description	Application	SLA Parameter	CPE Services
VPN IP Silver	Services to support on critical applications which are less sensitive to delay: Internet,Extranet	Microsoft Exchange ,E-mail,FTP,HTTP,SMTP	Network Availability = 99%	Un-managed Managed

Layanan ini terdiri dari enam paket, merupakan paduan dari tiga komposisi yaitu layanan Interaktif, *Gold* dan *Silver* dengan spesifikasi sebagai berikut :

a. Layanan Interaktif

Digunakan untuk komunikasi *Real Time*, sensitif terhadap *Delay Time* dan *Jitter*, misalnya *Voice* atau *Video Conferencing.*

b. Layanan *Gold*

Mendukung aplikasi kritikal yang interaktif dan tergantung waktu, seperti aplikasi *Client/Server* dan aplikasi *Database*.

c. Layanan *Silver*

Ditujukan untuk penggunaan aplikasi non kritikal, seperti *e-mail, http, SMTP*, dan *FTP*.

Telkom menawarkan *Class of Services (CoS)* ini melalui *service packaging* berdasarkan presentasi *bandwidth* yang dialokasikan dan dijaminkan untuk *port* akses yang dibutuhkan. Berikut komposisi CoS masing-masing paket layanan :

Tabel I.4. Komposisi *CoS* masing-masing layanan *VPN IP.*

Paket	Interactive	Gold	Silver
1*	100%		
2	30%	40%	30%
3		100%	
4		70%	30%
5		30%	70%
6			100%

Catatan :
* Khusus bagi operator

Kecuali paket 6, paket-paket layanan yang lain *router* disisi pelanggan harus dikelola oleh Telkom dalam rangka memberikan jaminan kualitas pelayanan.

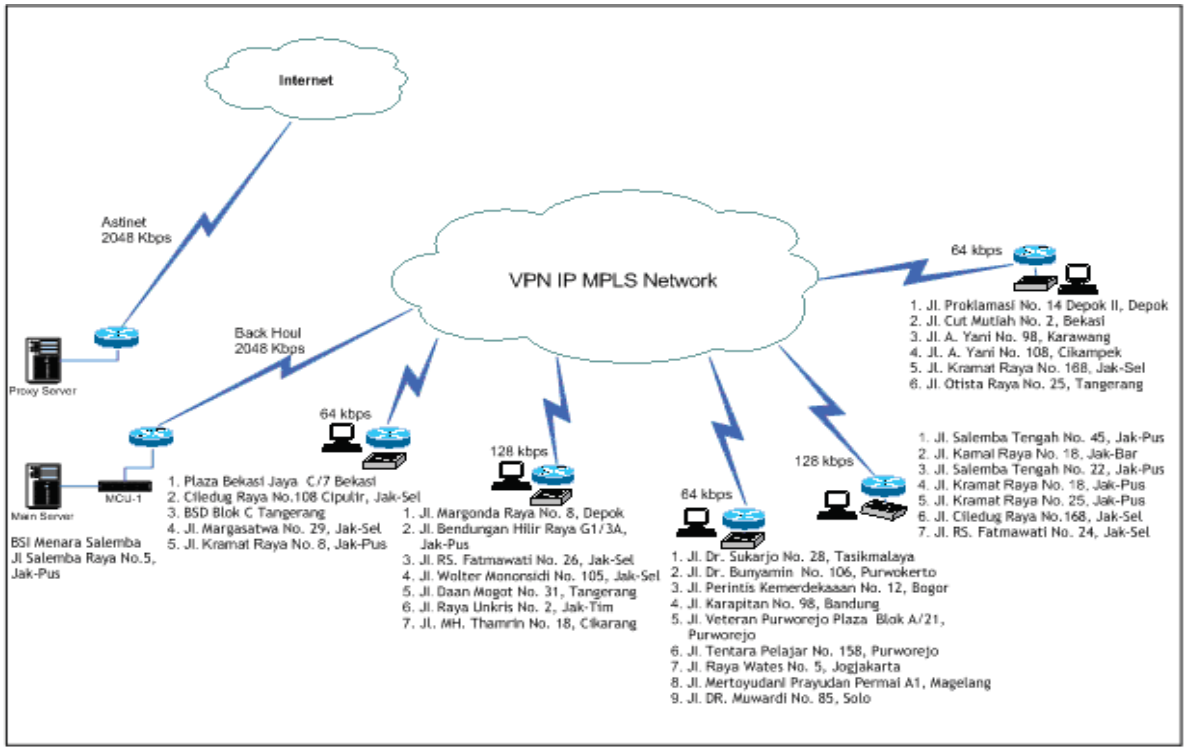
II. PEMBAHASAN

Pada tulisan ini, sebagai studi kasus penulis akan menjelaskan implementasi penggunaan teknologi *VPN IP MPLS* untuk membangun jaringan *VPN* pada Kampus Bina Sarana Informatika (BSI). Saat ini, Kampus BSI memiliki 35 lokasi yang tersebar dibeberapa kota di Indonesia. Secara lengkap, lokasi Kampus BSI, besar *bandwidth* yang digunakan serta konfigurasi *IP Address* jaringan *VPN* Kampus BSI dapat dilihat pada tabel di bawah ini.

Tabel II.1. Daftar lokasi Kampus BSI dan Konfigurasi IP *Address VPN* BSI

No	Alamat	Bandwidth	CP	CID	Interface	IP LAN	IP WAN	IP WAN (Captured from IP Ops)
1	Jl. Salemba Raya No. 5, Jakarta-Pusat	2048	020620517	2035036	Ethernet	172.100.44.0/22	-	172.17.195.25/30
2	Jl. Bendungan Hilir Raya Blok G1/3A, Jakarta-Pusat	128	CP020723309	14110	V.35	172.100.4.0/22	172.17.195.114/30	172.17.195.113/30
3	Jl. RS. Fatmawati No. 26 Pondok Labu, Jakarta-Selatan	128	CP020220549	14041	V.35	172.100.12.0/22	172.17.195.110/30	172.17.195.109/30
4	Jl. Wolter Mongonsidi No. 105 Kebayoran Baru, Jakarta-Selatan	128	CP020220545	14157	V.35	172.100.20.0/22	172.17.195.118/30	172.17.195.117/30
5	Jl. Kramat Raya No. 168, Jakarta-Pusat	64	020620512	20340037	Ethernet	172.100.24.0/22	-	172.17.195.29/30
6	Jl. Kramat Raya No. 18, Jakarta-Pusat	128	020620513	20340038	Ethernet	172.100.28.0/22	-	172.17.195.33/30
7	Jl. Kramat Raya No. 8, Jakarta-Pusat	64	020620514	20340039	Ethernet	172.100.32.0/22	-	172.17.195.37/30
8	Jl. Salemba Tengah No. 45, Jakarta-Pusat	128	020620515	20340040	Ethernet	172.100.36.0/22	-	172.17.195.41/30
9	Jl. Salemba Tengah No. 22, Jakarta-Pusat	128	020620516	20340041	Ethernet	172.100.40.0/22	-	172.17.195.45/30
10	Jl. Otista Raya No. 25, Tangerang	64	020422125	2005707	Ethernet	172.100.48.0/22	-	172.17.195.17/30
11	Jl. Daan Mogot No. 31, Tangerang	128	020422123	2005711	Ethernet	172.100.52.0/22	-	172.17.195.5/30
12	Jl. Proklamasi Blok A No.14 Depok II Tengah - Depok	64	9060014	14506	V.35	172.100.56.0/22	172.17.195.102/30	172.17.195.101/30
13	Jl. Margonda Raya No. 8, Depok	128	CP020220543	14024	V.35	172.100.60.0/22	172.17.195.98/30	172.17.195.97/30
14	Jl. Ir H Juanda Plaza Bekasi Jaya Blk C No.7, Bekasi	64	020821158	2037701	Ethernet	172.100.64.0/22	-	172.17.195.1/30
15	Jl. Raya Unkkris No. 2, Jakarta Timur	128	CP020121132	14103	V.35	172.100.72.0/22	172.17.195.90/30	172.17.195.89/30
16	Jl. Ciledug Raya No. 108 Cipulir, Jakarta-Selatan	64	CP020220546	14217	V.35	172.100.76.0/22	172.17.195.122/30	172.17.195.121/30
17	Jl. Perintis Kemerdekaan C-12 Mall Merdeka, Bogor	64	09060135	2034712	Ethernet	172.100.80.0/22	-	172.17.195.21/30
18	Jl. Ahmad Yani No. 108, Cikampek	64	CP020723315	14126	V.35	172.100.88.0/22	172.17.195.86/30	172.17.195.85/30
19	Jl. MH. Thamrin No. 18 Lippo Cikarang, Bekasi	64	CP020821157	14010	V.35	172.100.92.0/22	172.17.195.82/30	172.17.195.81/30
20	Jl. Kamal Raya No. 18 Ring Road, Jakarta-Barat	128	CP020723315	14173	V.35	172.100.96.0/22	172.17.195.78/30	172.17.195.77/30
21	Jl. Ciledug Raya No. 168, Jakarta-Selatan	128	020220089	13809	V.35	172.100.100.0/22	172.17.195.54/30	172.17.195.53/30
22	Jl. Karapitan No. 98, Bandung	64	23041200069	3024725	Ethernet	172.100.104.0/22	-	172.17.195.57/30
23	Jl. Dr Sukarjo No. 28, Tasikmalaya	64	23041200069	3007720	Ethernet	172.100.108.0/22	-	172.17.195.61/30
24	Jl. Veteran Puworejo Plaza Blok A No. 21, Purworejo	64	149114013008	14093	V.35	172.100.112.0/22	172.17.195.74/30	172.17.195.73/30
25	Jl. Tentara Pelajar No. 158, Purworejo	64	149114013007	14092	V.35	172.100.116.0/22	172.17.195.70/30	172.17.195.69/30
26	Jl. Raya Wates No. 5 Griya Alvita Kalibayem, Yogyakarta	64	CP149114000004	4010703	Ethernet	172.100.120.0/22	-	172.17.195.13/30
27	Jl. Martoyudan, Prayudan Permai A, Magelang	64	149114006002	14082	V.35	172.100.124.0/22	172.17.195.66/30	172.17.195.65/30
28	Jl. Dr. Muwardi No. 85, Solo	64	CP149505000017	40123700	Ethernet	172.100.128.0/22	-	172.17.195.9/30
29	Jl. Kramat Raya No. 25, Jakarta-Pusat	128	020620518	20340042	Ethernet	172.100.132.0/22	-	172.17.195.49/30
30	Jl. RS. Fatmawati No. 24 Pondok Labu, Jakarta-Selatan	128	CP020220547	14521	V.35	172.100.8.0/22	172.17.195.130/30	172.17.195.129/30
31	Jl. Margasatwa No. 29, Jakarta-Selatan	64	CP020220281	14559	V.35	172.100.16.0/22	172.17.195.106/30	172.17.195.105/30
32	Jl. Cut Mutiah No. 2, Bekasi	64	CP020821159	14514	V.35	172.100.68.0/22	172.17.195.94/30	172.17.195.93/30
33	Jl. Ahmad Yani No. 98, Karawang	64	CP020821190	2035704	Ethernet	172.100.84.0/22	-	172.17.195.125/30
34	Jl. Dr. Bunyamin No. 106 Pabuaran, Purwokerto	64	CP149.303.000.055	4045707	Ethernet	172.100.140.0/22	-	172.17.195.133/30
35	Jl. BSD Sektor XIV Blok C1 No. 1 Serpong, Tangerang	64	CP020422174	2075706	Ethernet	172.100.136.0/22	-	172.17.195.137/30

Secara umum koneksi jaringan *VPN* BSI yang menggunakan teknologi *VPN IP MPLS* tersebut dapat di lihat pada gambar di bawah ini.



Gambar II.1. Konfigurasi Jaringan *VPN IP MPLS* BSI

Pada gambar II.1 dapat kita perhatikan bahwa setiap kampus BSI terhubung secara langsung menggunakan jaringan *VPN IP MPLS* milik Telkom agar dapat saling terkoneksi dengan kampus BSI Menara Salemba yang dalam hal ini difungsikan sebagai sisi *backhole* (pusat interkoneksi jaringan di Kampus BSI).

Pemanfaatan jaringan *VPN* tersebut dapat dimanfaatkan untuk kebutuhan-kebutuhan internal BSI seperti pembangunan *intranet* yang dapat membuat suatu sisten informasi *online* berbasis *web,* komunikasi data maupun suara menggunkan *Instant Messenger (Net Meeting, Office Communicator / Live Communication System,* dll), *sharing resource (file, software dan hardware)*, bahkan sampai dengan pemanfaatan komunikasi menggunakan teknologi *Voice Over Internet Protocol (VoIP)*. Sedangkan untuk menghubungkan seluruh jaringan komputer di Kampus BSI ke jaringan global *(internet),* seluruh Kampus BSI dapat terkoneksi melalui jalur *Leased Line* dengan *bandwidth* sebesar 2.048 Kbps yang terdapat pada Kampus BSI Menara Salemba *(Backhole)* yang sudah terhubung ke jalur *internet* menggunakan *ASTINet* dari Telkom.

Teknologi *VPN IP MPLS* ini melikiki dua macam *interface* untuk keluaran yang menghubungkan antara *Router PE* yang ada disisi Telkom (Pada masing-masing STO Telkom yang terdekat dengan kampus BSI) dengan *Router CE* yang ada di masing-masing kampus BSI, yaitu :

1. *Standard Ethernet* (10/100 Mbps) yang merupakan keluaran untuk *VPN IP Modem/Router (HDSL Modem).*
2. *Port* V.35 yang merupakan keluaran untuk ke *router* milik BSI.

Pada perangkat *router* yang terdapat disisi kampus BSI (CE) terdapat dua macam merk *router* yang digunakan, yaitu : *Cisco Router* dan *Allied Telesyn (AT) Router*.

Pada sisi *backhoule*, yaitu Kampus BSI Menara Salemba menggunakan *Cisco Router* 2801 tipe Modular. Pada kampus-kampus BSI yang menggunakan *interface* keluaran berupa *Port* V.35 menggunakan *Cisco Router* 2501 untuk dapat terkoneksi dengan Router yang ada pada sisi *backhole*. Pada kampus BSI di Purworejo A, Purworejo B, Magelang & Cikampek menggunakan Router *Allied Telesyn (AT) Router* Tipe AT-AR410 *Multiprotocol Modular Router* 4X10/100TX+1 PIC Slot untuk dapat terkoneksi dengan *Router* yang ada pada sisi *backhole*. Kampus-kampus BSI yang menggunakan *interface* keluaran *Standard Ethernet* menggunakan *VPN IP Modem/Router (HDSL Modem)* dengan Merk ZyXEL Prestige 700 Series untuk dapat terkoneksi dengan *Router* yang ada pada sisi *backhole*.

Adapun tahapan-tahapan untuk mengimplementasikan *VPN* dengan menggunakan Teknologi VPN IP MPLS adalah sebagai berikut :

1. Membangun infrastuktur jaringan *VPN* yang menghubungkan semua lokasi Kampus BSI dengan kampus BSI Menara Salemba sebagai *backhole*.
2. Setelah seluruh infrastruktur jaringan *VPN* selesai dibangun, langkah berikutnya adalah membangun *Server-Server* yang akan digunakan untuk melayani kebutuhan yang ada di internal BSI yang ada pada sisi BSI Menara Salemba yang akan dijadikan pusat untuk pelayanan, misalnya : *Server* untuk pengaturan sistem domain *(Domain Controller Server)*, *Database Server*, *Domain Name System (DNS) Server*, WINS *Server*, DHCP *Server*, Web *Server*, Mail *Server*, Proxy *Server*, dll. Sedangkan pada sisi kampus cabang BSI, buatlah minimal ada satu buah *Server* yang dipergunakan sebagai *Additional Domain Controller Server* yang juga difungsikan sebagai DNS *Server*, WINS *Server*, dan DHCP *Server*.

3. Setelah infrastruktur dan *server-server* yang akan digunakan siap untuk dipergunakan, maka langkah terakhir adalah untuk membangun aplikasi *online* yang dapat secara *multi user* digunakan dari masing-masing kampus BSI seperti : Sistem penerimaan siswa kursus atau mahasiswa baru, Pengolahan data *online* dari, Sistem pemantauan lokasi *online* mengggunakan *Network Camera*, Sistem absensi karyawan *online* dan lain-lain.

Kampus BSI menerapkan sistem domain yang berbasis sistem Operasi *Windows Server* 2003 yang digunakan untuk mengatur sistem komputer yang terdapat diseluruh kampus BSI. Sistem domain yang digunakan sistem *single domain*. Sistem *single domain* pada kampus BSI hanya memiliki satu nama domain yaitu bsi.ac.id yang diatur secara terpusat pada *Domain Controller Server* yang terdapat pada Kampus BSI Menara Salemba. Mesin *Domain Controller Server* ini sendiri sebenarnya adalah *root domain* atau *Domain Controller Server* yang pertama kali dibuat. Sedangkan untuk membantu kerja dari *Domain Controller Server* yang berada pada kampus BSI Menara Salemba, mesin ini dibantu oleh tiga buah mesin *Domain Controller Server* lain yang berfungsi sebagai mesin *Additional Domain Controller Server* serta juga dapat dimanfaatkan sebagai mesin *backup* apabila sewaktu-waktu mesin *Domain Controller Server* mengalami gangguan.

Pembangunan *Domain Controller Server* pada Kampus BSI Menara Salemba ini dimaksudkan untuk melayani semua pengguna komputer *(user)* yang berjumlah sekitar 100-150 orang karyawan yang akan menggunakan komputer *(login)* ke dalam sistem komputer yang ada di BSI dari Kampus BSI Menara Selemba dengan jumlah komputer sekitar 100 unit.

Sedangkan untuk melayani semua pengguna komputer *(user)* yang ada pada kampus cabang BSI yang akan menggunakan komputer *(login)* ke dalam sistem komputer yang ada di BSI dari masing-masing kampus cabang BSI, maka dibangunlah minimal satu buah mesin *Domain Controller Server*. Adapun maksud dari pembangunan mesin *Domain Controller Server* pada masing-masing kampus cabang BSI ini adalah agar semua *user* yang *login* cukup dilayani oleh mesin *Domain Controller Server* yang ada dicabang tersebut dengan kata lain tidak perlu menggunakan *bandwidth* VPN IP dari cabang tersebut yang sangat kecil untuk mendapatkan ijin akses ke komputer dari mesin *Domain Controller Server* yang ada di BSI Menara Salemba.

Mesin *Domain Controller Server* yang ada pada setiap kampus cabang BSI, secara *realtime* akan melakukan sinkrosisasi data dengan mesin *Domain Controller Server* yang ada pada Kampus BSI Menara Salemba atau kampus-kampus BSI yang lainnya. Dalam sistem *Domain Name Sistem (DNS),* untuk mengakses komputer yang berada dalam satu *Network* ID yang sama, *user* dapat melakukan perintah *Computer_Name* atau *NetBIOS Name* atau \\IP *Address Computer*. Misalnya anda akan mengakses komputer dengan nama PROGRAMMER01 yang berada pada *IP Address* 172.16.40.100, maka perintah yang harus ada lakukan adalah \\PROGRAMMER01 atau \\172.16.40.100. Hal yang seperti ini dapat anda lakukan lagi ketika anda sudah berada pada suatu jaringan *WAN* yang memiliki konsep *IP Address* yang di-*subnetting*.

Untuk mengatasi hal tersebut, maka dibangunlah suatu mesin yang disebut dengan *WINS Server* di kampus BSI Menara Salemba. Mesin *WINS Server* ini juga bangun pada seluruh kampus cabang.

Mesin-mesin *WINS Server* ini nantinya akan selalu melakukan sinkronikasi dengan mesin-mesin *WINS Server* yang lain ketika terjadi sinkroniksai antar mesin *Domain Controller Server*. Tugas dari mesin ini adalah untuk menterjemahkan *Computer Name* atau *NetBIOS Name* menjadi *IP Address* agar dapat diakses dari lokasi lain yang memiki *IP Address* yang berbeda *segment*.

IP Address yang di-*subnetting* disini adalah jaringan komputer yang ada pada suatu instutitusi tersebut menggunakan *IP Address Private*. Kemudian *IP Address Private* tersebut yang tadinya hanya memiliki satu buah *Network ID* dan hanya bisa digunakan satu jaringan komputer yang terdapat pada satu cabang, maka *IP Address Private* tadi dipecah-pecah lagi dengan mengorbankan beberapa *Host ID*-nya untuk membentuk beberapa *Network ID* yang baru. Dengan memiliki beberapa *Network ID* yang baru tadi, maka setiap cabang yang memiliki *IP Address* yang berbeda *segment* (Karena sudah di-*subnetting* tadi), maka sekarang masing-masing *IP Address* tersebut sudah dapat saling berkomunikasi dengan cabang lain yang memiliki *IP Address* yang berbeda dengan bantuan perangkat *Router*. Sebagai contoh, misalkan anda mempunyai *Network ID* 172.16.0.0/16. Maka *range IP Address* yang dapat anda gunakan adalah 172.16.0.0 sampai dengan 172.16.255.254 dengan *subnet mask* 255.255.0.0 (/16). Dengan kata lain, dalam satu cabang pada instritusi anda hanya boleh memiliki maksimal 65.534 *host*. Sementara seperti Kampus BSI misalnya, memiliki 35 lokasi yang semua jaringan komputernya terhubung melalui *VPN IP MPLS*.

Secara teori memang bisa saja anda memberikan *IP Addrress* yang berbeda untuk setiap cabang, misalnya : IP Adress 172.16.0.0/16 untuk BSI Cengkareng, IP Adress 172.17.0.0/16 untuk BSI Jatiwaringin, IP Adress 172.18.0.0/16 untuk BSI Purwokerto dan seterusnya. Hal ini dalam konsep *intranet* kurang tepat. Dalam konsep *intranet* lebih baik anda menggunakan *Network ID* 172.16.0.0/16 yang *subneting* menjadi beberapa *Netwok ID* baru. Daftar hasil *subnetting IP Address* 172.16.0.0/16 tersebut dapat dilihat pada tabel di bawah ini.

Tabel II.2. Contoh *Subnetting IP Address*

No	Network ID	Range IP Address	IP Address Broadcast	No	Network ID	Range IP Address	IP Address Broadcast
1	172.16.4.0	172.16.4.1 - 172.16.7.254	172.16.7.255	32	172.16.128.0	172.16.128.1 - 172.16.131.254	172.16.131.255
2	172.16.8.0	172.16.8.1 - 172.16.11.254	172.16.11.255	33	172.16.132.0	172.16.132.1 - 172.16.135.254	172.16.135.255
3	172.16.12.0	172.16.12.1 - 172.16.15.254	172.16.15.255	34	172.16.136.0	172.16.136.1 - 172.16.139.254	172.16.139.255
4	172.16.16.0	172.16.16.1 - 172.16.19.254	172.16.19.255	35	172.16.140.0	172.16.140.1 - 172.16.143.254	172.16.143.255
5	172.16.20.0	172.16.20.1 - 172.16.23.254	172.16.23.255	36	172.16.144.0	172.16.144.1 - 172.16.147.254	172.16.147.255
6	172.16.24.0	172.16.24.1 - 172.16.27.254	172.16.27.255	37	172.16.148.0	172.16.148.1 - 172.16.151.254	172.16.151.255
7	172.16.28.0	172.16.28.1 - 172.16.31.254	172.16.31.255	38	172.16.152.0	172.16.152.1 - 172.16.155.254	172.16.155.255
8	172.16.32.0	172.16.32.1 - 172.16.35.254	172.16.35.255	39	172.16.156.0	172.16.156.1 - 172.16.159.254	172.16.159.255
9	172.16.36.0	172.16.36.1 - 172.16.39.254	172.16.39.255	40	172.16.160.0	172.16.160.1 - 172.16.163.254	172.16.163.255
10	172.16.40.0	172.16.40.1 - 172.16.43.254	172.16.43.255	41	172.16.164.0	172.16.164.1 - 172.16.167.254	172.16.167.255
11	172.16.44.0	172.16.44.1 - 172.16.47.254	172.16.47.255	42	172.16.168.0	172.16.168.1 - 172.16.171.254	172.16.171.255
12	172.16.48.0	172.16.48.1 - 172.16.51.254	172.16.51.255	43	172.16.172.0	172.16.172.1 - 172.16.175.254	172.16.175.255
13	172.16.52.0	172.16.52.1 - 172.16.55.254	172.16.55.255	44	172.16.176.0	172.16.176.1 - 172.16.179.254	172.16.179.255
14	172.16.56.0	172.16.56.1 - 172.16.59.254	172.16.59.255	45	172.16.180.0	172.16.180.1 - 172.16.183.254	172.16.183.255
15	172.16.60.0	172.16.60.1 - 172.16.63.254	172.16.63.255	46	172.16.184.0	172.16.184.1 - 172.16.187.254	172.16.187.255
16	172.16.64.0	172.16.64.1 - 172.16.67.254	172.16.67.255	47	172.16.188.0	172.16.188.1 - 172.16.191.254	172.16.191.255
17	172.16.68.0	172.16.68.1 - 172.16.71.254	172.16.71.255	48	172.16.192.0	172.16.192.1 - 172.16.195.254	172.16.195.255
18	172.16.72.0	172.16.72.1 - 172.16.75.254	172.16.75.255	49	172.16.196.0	172.16.196.1 - 172.16.199.254	172.16.199.255
19	172.16.76.0	172.16.76.1 - 172.16.79.254	172.16.79.255	50	172.16.200.0	172.16.200.1 - 172.16.203.254	172.16.203.255
20	172.16.80.0	172.16.80.1 - 172.16.83.254	172.16.83.255	51	172.16.204.0	172.16.204.1 - 172.16.207.254	172.16.207.255
21	172.16.84.0	172.16.84.1 - 172.16.87.254	172.16.87.255	52	172.16.208.0	172.16.208.1 - 172.16.211.254	172.16.211.255
22	172.16.88.0	172.16.88.1 - 172.16.91.254	172.16.91.255	53	172.16.212.0	172.16.212.1 - 172.16.215.254	172.16.215.255
23	172.16.92.0	172.16.92.1 - 172.16.95.254	172.16.95.255	54	172.16.216.0	172.16.216.1 - 172.16.219.254	172.16.219.255
24	172.16.96.0	172.16.96.1 - 172.16.99.254	172.16.99.255	55	172.16.220.0	172.16.220.1 - 172.16.223.254	172.16.223.255
25	172.16.100.0	172.16.100.1 - 172.16.103.254	172.16.103.255	56	172.16.224.0	172.16.224.1 - 172.16.227.254	172.16.227.255
26	172.16.104.0	172.16.104.1 - 172.16.107.254	172.16.107.255	57	172.16.228.0	172.16.228.1 - 172.16.231.254	172.16.231.255
27	172.16.108.0	172.16.108.1 - 172.16.111.254	172.16.111.255	58	172.16.232.0	172.16.232.1 - 172.16.235.254	172.16.235.255
28	172.16.112.0	172.16.112.1 - 172.16.115.254	172.16.115.255	59	172.16.236.0	172.16.236.1 - 172.16.239.254	172.16.239.255
29	172.16.116.0	172.16.116.1 - 172.16.119.254	172.16.119.255	60	172.16.240.0	172.16.240.1 - 172.16.243.254	172.16.243.255
30	172.16.120.0	172.16.120.1 - 172.16.123.254	172.16.123.255	61	172.16.244.0	172.16.244.1 - 172.16.247.254	172.16.247.255
31	172.16.124.0	172.16.124.1 - 172.16.127.254	172.16.127.255	62	172.16.248.0	172.16.248.1 - 172.16.251.254	172.16.251.255

Dari tabel di atas dapat disimpulkan bahwa sebuah *Network ID* 172.16.0.0 dengan *default subnet mask*-nya 255.255.0.0 (/16) setelah dilakukan *subnetting* sebanyak 6-*bit* menghasikan 62 *Network ID* baru dan pada setiap *Network ID* maksimal ada sebanyak 1.022 *host*. Kalau anda memiliki sebanyak 62

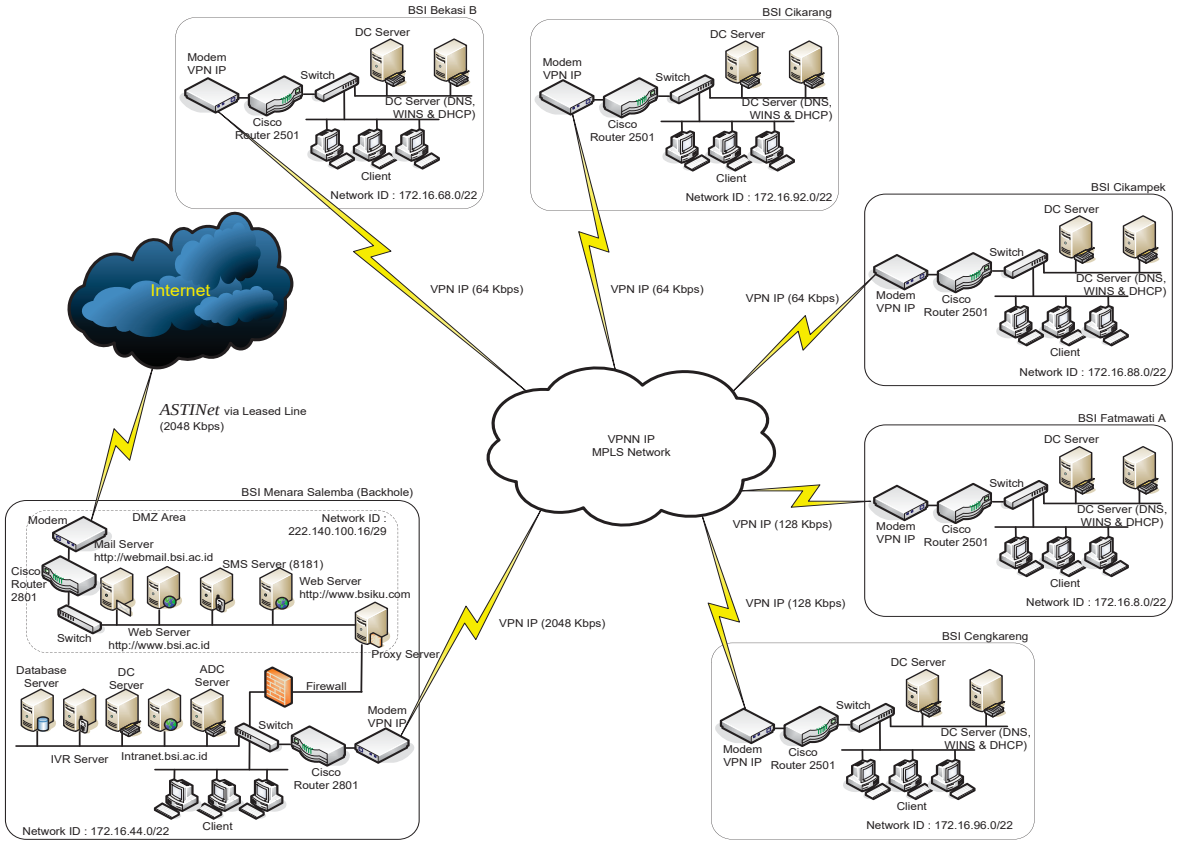
Network ID, berarti anda dapat menghubungkan maksimal 62 kantor anda ke dalam jaringan komputer *(WAN)*. Adapun ke-62 *Netwok ID* baru tersebut adalah 172.16.4.0, 172.16.8.0, 172.16.12.0, ..., 172.16.248.0 dengan *subnet mask* yang baru yaitu 255.255.252.0 (/22).

Dalam menentukan *IP Address* yang akan digunakan oleh suatu institusi yang akan menghubungkan semua jaringan komputer yang terdapat pada kantor cabang dengan kantor pusatnya *(WAN)*, sebaiknya anda menggunakan *IP Address Private*. Hal ini dimaksudkan, apabila suatu saat, instritusi anda akan melakukan koneksi juga ke dunia luar *(internet)* maka institusi anda tidak perlu repot-repot untuk merubah konfigurasi *IP Address* lagi (karena kemungkinan besar *IP Address* yang anda gunakan sudah ada yang menggunakannya di *internet*). Pada tabel berikut ini adalah rincian daftar *IP Address Private* yang dapat anda pergunakan.

Tabel II.3. *IP Address Private*

No	Kelas	Network ID Private	Subnet Mask	Range IP Address
1	A	10.0.0.0	255.0.0.0	10.0.0.1 - 10.255.255.254
2	B	172.16.0.0	252.240.0.0	172.16.0.1 - 172.16.255.254
3	C	192.168.0.0	255.255.0.0	192.168.0.1 - 192.168.255.254

Implementasi lengkap jaringan *WAN* menggunakan *VPN IP MPLS* pada Kampus BSI ini dapat dilihat pada Gambar II.2 berikut ini.



Gambar II.2. Spesifikasi jaringan *VPN* Kampus BSI

Pada gambar tersebut dapat anda lihat bahwa setiap Kampus BSI dapat terhubung ke BSI Menara Salemba di Jakarta menggunakan media *VPN IP MPLS*, dimana seluruh komputer yang ada dapat terhubung secara langsung antara satu dengan lainnya seolah-olah berada dalam satu jaringan LAN. Prinsip kerja dari *VPN IP MPLS* tersebut adalah menghubungkan masing-masing Kampus BSI yang ada dicabang dengan Kampus BSI Menara Salemba yang berada di Jakarta yang disebut dengan *Backhole*. *Router-router* disini berfungsi untuk melewatkan paket-paket data yang datangnya dari *IP Address* yang berbeda *segment*. Sedangkan agar masing-masing kampus cabang BSI dapat terkoneksi ke jaringan global *(internet)*, maka pada konfigurasi *Cisco Router* 2801 yang terdapat pada Kampus BSI Menara Salemba *(Backhole)* harus diberikan pengaturan agar setiap komputer yang akan akses ke *internet* harus menuju ke *Proxy Server (Squid)* yang ada di *Backhole* dengan *IP Address* 172.16.44.254. Jadi komputer yang boleh langsung terhubung ke *internet* adalah komputer *Proxy Server* yang memiliki dua *Ethernet Card*, yaitu : 172.16.44.254/22 dan 222.140.100.22/29 yang mana *IP Address* 222.140.100.22/29 berada pada area *Demilitary Zone (DMZ)* yang dilindungi oleh *Firewall*. *DMZ ini* meskipun kedengarannya sangat menyeramkan, sebenarnya ini hanya area yang berada diambang luar dari *firewall*. Asumsikanlah bahwa *DNZ* ini adalah halaman depan rumah anda, halaman ini masih milik anda. Anda juga bisa meletakan barang-barang tertentu disana, sementara juga memiliki barang-barang yang harus dijaga didalam rumah.

Menurut Rafiudin [2006, Hal. 10], dalam kontek *firewall, DMZ* dapat didefinisikan "Sebagai bagian dari jaringan namun bukan bagian dari jaringan internal kita dan tidak secara langsung menjadi bagian dari *internet.* Secara tipikal, area ini berada diantara *router* akses *internet* kita dan *Host Bastian* ("Benteng") kita meskipun dapat juga berada diantara dua komponen pembentukl *policy* arsitektur kita".

Area DMZ dapat anda buat menggunakan cara mengkonfigurasi *router* pada sisi BSI Menara Salemba (*Backhole*) dengan cara memberikan perintah *"access control-lists (ACL)".*

Berikut ini contoh konfigurasi *Cisco Router* yang ada pada sisi *backhole.* Adapun contoh dari konfigurasi *router* pada *Cisco Router* 2801 adalah sebagai berikut :

```
--- IP Adress dari Router Astinet (ISP) untuk akses ke internet ---
BSI (config)# ip route 0.0.0.0 0.0.0.0 192.168.2.177

--- Mengijinkan IP Address 172.16.4.0 s/d 172.16.140.0 melewati Fast Ehernet 0/1 (IP LAN) ---
BSI (config)# ip route 172.16.4.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.8.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.12.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.16.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.20.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.24.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.28.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.32.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.36.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.40.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.44.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.48.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.52.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.56.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.60.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.64.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.68.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.72.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.76.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.80.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.84.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.88.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.92.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.96.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.100.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.104.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.108.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.112.0 255.255.252.0 FastEthernet0/1
```

```
BSI (config)# ip route 172.16.96.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.100.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.104.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.108.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.112.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.116.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.120.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.124.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.128.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.132.0 255.255.252.0 FastEthernet0/1
BSI (config)# ip route 172.16.140.0 255.255.252.0 FastEthernet0/1
```

```
--- Mengijinkan IP Address tersebut Fast Ehernet 0/0 (IP VPN) ---
BSI (config)# ip route 172.17.195.52 255.255.255.252 FastEthernet0/0
BSI (config)# ip route 172.17.195.64 255.255.255.252 FastEthernet0/0
BSI (config)# ip route 172.17.195.68 255.255.255.252 FastEthernet0/0
BSI (config)# ip route 172.17.195.72 255.255.255.252 FastEthernet0/0
BSI (config)# ip route 172.17.195.76 255.255.255.252 FastEthernet0/0
BSI (config)# ip route 172.17.195.80 255.255.255.252 FastEthernet0/0
```

```
--- Mengijinkan IP Address 172.16.4.0 s/d 172.16.140.0 untuk akses ke internet hanya melalui
IP Address 172.16.44.254 (IP Address Proxy Server) ---
BSI (config)# access-list 1 permit 172.16.4.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.8.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.12.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.16.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.20.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.24.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.28.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.32.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.36.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.40.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.44.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.48.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.52.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.56.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.60.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.64.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.68.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.72.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.76.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.80.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.84.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.88.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.92.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.96.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.100.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.104.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.108.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.112.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.116.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.120.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.124.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.128.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.132.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.140.0 0.0.3.255
BSI (config)# access-list 1 permit 172.16.0.0 0.0.0.255
BSI (config)# access-list 100 permit ip host 172.16.44.254 any
```

Pada gambar II.2 di atas terlihat terdapat satu buah mesin *Web Server* yang bernama http://www.bsi.ac.id dan satu buah mesin *Mail Server* dengan nama http://webmail.bsi.ac.id.

Agar setiap pengguna yang berada di dalam internal jaringan BSI dapat mengakses ke alamat http://www.bsi.ac.id dan http://webmail.bsi.ac.id, maka pada mesin *DNS Server* anda harus di definisikan juga sebuah *zone* baru untuk *DNS Server* anda dengan nama bsi.ac.id dengan nama *host* "*www*" dan "*webmail*" ke alamat mesin *Web Server* dan *Mail Server* yang ada pada dareah DMZ di atas. Misalnya, ketika pengguna mengakses *website* http://www.bsi.ac.id dari *web browser*-nya yang berada dari internal jaringan Kampus BSI maka *IP Address*-nya akan di arahkan ke 222.140.100.18 sedangkan untuk http://webmail.bsi.ac.id akan diarahkan ke IP Address 222.140.100.19. Akan tetapi untuk menghemat penggunan *bandwidth* di jaringan internal Kampus BSI, sebaiknya ada lakukan pengaturan lagi pada sisi *router* yang terdapat di BSI Menara Salemba yaitu apabila ada yang mengkases ke http://www.bsi.ac.id dan http://webmail.bsi.ac.id atau http://www.bsiku.com, maka yang seharusnya akan masuk ke *IP Address* Statik *(IP Address Public)* di *internet* (Misalnya : 222.140.100.18, 222.140.100.19 dan 222.140.100.20) tetapi dapat diakses

hanya melalui *Proxy Server* yang menggunakan *IP Address* Lokal *(IP Address Private)* yang terdapat pada internal jaringan Kampus BSI. Hal ini akan sangat membantu untuk mempercepat akases ke alamat-alamat tersebut.

Untuk keperluan internal Kampus BSI, pada kampus BSI Menara Salemba terdapat mesin *server intranet* yang dapat diakses dari seluruh Kampus BSI pada alamat https://intranet.bsi.ac.id.

III. PENUTUP

3.1. Kesimpulan

Wide Area Network (WAN) dipergunakan untuk menghubungkan jaringan-jaringan *Local Area Network (LAN)* satu dengan lainnya yang berdekatan maupun yang berjauhan dan menggunakan protokol yang sama atau berbeda-beda. Jika pada *LAN* hubungan jaringan komputer dapat dilakukan dengan perantara kabel-kabel milik internal perusahaan seperti : Kabel Koaksial, Kabel UTP/RJ-45, Serat Optik dan lain-lain, maka pada jaringan *WAN* pada umumnya jaringan komputer dihubungan melalui jaringan milik perusahaan telekomunikasi sebagai media perantara. Teknologi yang dipergunakan untuk menghubungkan WAN, antara lain: *Dial Up, Leased Line, VSAT, X.25, Frame Relay, Virtual Private Network (VPN),* dll. Sedangkan teknologi terbaru yang saat ini sedang dikembangkan untuk membangun jaringan *WAN* yang baik *(realible)* dan permanen adalah *Virtual Private Network* (*VPN*) berbasis *IP Multi Protocol Label Switch* (*VPN IP MPLS*).

Standar paket layanan *VPN IP* adalah berdasarkan *Class of Service (CoS) VPN IP* dengan beberapa tipe paket *CoS* yang terdapat pada Telkom adalah: *VPN IP Interactive, VPN IP Gold* dan *VPN IP* Silver. Layanan ini terdiri dari enam paket, merupakan paduan dari tiga komposisi yaitu layanan *Interaktif, Gold* dan *Silver* dengan spesifikasi sebagai berikut :

1. Layanan Interaktif, digunakan untuk komunikasi *Real Time*, sensitif terhadap *Delay Time* dan *Jitter*, misalnya *Voice* atau *Video Conferencing.*
2. Layanan *Gold, m*endukung aplikasi kritikal yang interaktif dan tergantung waktu, seperti aplikasi *Client/Server* dan aplikasi *Database*.
3. Layanan *Silver, d*itujukan untuk penggunaan aplikasi non kritikal, seperti *e-mail, http, SMTP*, dan *FTP*.

3.2. Saran

Dalam rangka untuk meningkat kinerja dan kompatibilitas dari perangkat infrastruktur jaringan *WAN* yang ada pada Kampus BSI, idealnya semua perangkat yang ada berasal dari satu *vendor*, misalnya *Cisco*. Hal ini juga untuk lebih memudahkan manajemen perangkat serta perawatannya *(maintenance)*.

Adapun perangkat-perangkat tersebut adalah : *Router, Switch* dan *Firewall*. Sedangkan untuk perangkat *Switch* yang ada sebaiknya menggunakan tipe perangkat *Switch Manageble* semua. Hal ini dimaksudkan agar memudahkan pengaturan terhadap setiap *port* pada perangkat *Switch* tersebut yang nantinya akan berkaitan dengan layanan *(service)* apa saja yang dapat diberikan terhadap pengguna komputer yang terhubung pada *Port Switch Manageble* tersebut. Misalnya : *SMTP, POP3, HTTP, Telnet dan lain-lain*.

Untuk mempercepat proses *login user* yang ada pada masing-masing cabang Kampus BSI, sebaiknya pada setiap Kampus Cabang BSI minimal menggunakan dua buah *server* yang berfungsi sebagai *Additional Domain Controler*. Hal ini dimaksudkan apabila mesin utama *Additional Domain Controler* yang ada pada cabang tersebut mengalami gangguan, maka mesin *Additional Domain Controler* yang

kedua akan berfungsi sebagai *backup* unit dan melayani *user* yang akan *login* ke sistem komputer yang ada di kampus BSI. Serta semua *user* yang ada harus melakukan proses *login* ke dalam sistem *domain* untuk menghindari hal-hal yang tidak diinginkan serta aktivitas dari *user* yang *login* tersebut dapat selalu tercatat pada berkas *log* dari sistem.

Agar penggunaan *bandwidth* yang ada lebih hemat dan tidak menggangu *user* yang sedang melakukan aktivitasnya melalui jaringan *intranet*-nya, sebaiknya proses *replikasi* baik *database, DNS, WINS*, dan lain-lain dari semua mesin *Additional Domain Controler* yang ada, sebaiknya diatur untuk melakukan proses replikasi pada saat jam-jam tidak sibuk, yaitu antara pukul 22.00 s/d 06.00.

Untuk menghindari hilangnya data-data yang ada pada setiap mesin server *Additional Domain Controler*, sebaiknya semua *server* yang ada dilengkapi dengan minimal satu buah *disk mirror*. Serta pelaksanaan *disk mirror* tersebut harus benar-benar selalu diperhatikan, jangan sampai proses *disk mirror* mengalami gangguan.

DAFTAR PUSTAKA

Anoname. 2007. *International IP-VPN MPLS*. Diambil dari : http://www.xl.co.id/Business_Solutions/Layanan_Komunikasi_Data/International_IP-VPN_MPLS/.

Anoname. 2007. *Solusi Enterprise - IP Virtual Network*. Dimabil dari : http://www.telkom.co.id/produk-layanan/korporat/data-internet/solusi-enterprise-ip-virtual-network.html.

Anoname. 2007. *TELKOMLink VPN IP*. Diambil dari : http://www.telkom.net/pojok_telkomlink_vpnip.php.

Anoname. 2007. *VPN Multiservice.* Diambil dari : http://www.lintasarta.net/tabid/83/Default.aspx.

Rafiudin, Rahmat. 2006. Membangun *Firewall* dan *Traffic Filtering* Berbasis *Cisco.* Penerbit Andi. Yogyakarta.

S'to. 2004. Menguasai *Windows Server* 2003. Elek Media Komputindo. Jakarta.

Wijaya, Hendra. Ir. 2004. Belajar Sendiri *Cisco Router*. Edisi Baru untuk mengambil Sertifikat CCNA (640-801). Elek Media Komputindo. Jakarta.

_____. Ir. 2006. Belajar Sendiri *Cisco ADSL Router, PIX Firewall* dan *VPN.* Elek Media Komputindo. Jakarta.

Wirija, Sudantha. Ir. 2005. *Microsoft Windows Server* 2003. Elek Media Komputindo. Jakarta.