

## BAB II

### LANDASAN TEORI

#### 2.1. Tinjauan Jurnal

Penggunaan VPN ini sebagai solusi efektifitas dan keamanan data sudah banyak diterapkan pada berbagai perusahaan yang memiliki banyak kantor cabang. VPN biasa disebut jaringan pribadi karena hanya pemilik saja yang dapat mengakses jaringan tersebut. Seperti yang sudah diimplementasikan di PT. Mega Tirta Alami yang memiliki banyak kantor cabang yang tersebar di seluruh Indonesia. Penerapan VPN di kantor ini untuk menunjang kegiatan pengiriman data-data penting dari kantor cabang ke kantor pusat ataupun sebaliknya (Supriono dkk, 2013:89).

Ada berbagai metode VPN yang dapat diterapkan seperti L2TP, PPTP dan OpenVPN. Tiap metode memiliki keunggulan dan kelemahan masing-masing. Pada penulisan skripsi ini penulis akan menerapkan metode L2TP/IPsec karena penulis rasa metode inilah yang aman dan mudah dalam konfigurasinya.

L2TP merupakan *tunneling* protokol yang memadukan dua buah protokol yaitu *Layer 2 Forwarding* milik Cisco dan PPTP milik Microsoft. Umumnya digunakan untuk membuat *Virtual Private Dial Network* (VPDN) yang biasanya menggunakan port 1702 dengan protokol UDP.

IPsec adalah pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan *layer* yang berada di atasnya. IPsec berada pada *layer* 3 OSI yaitu *network layer*. IPsec terdiri dari dua buah *security protocol* yaitu AH (*Authentication Header*), protokol yang melakukan autentikasi datagram untuk identifikasi pengirim data tersebut. Dan juga ESP (*Encapsulation Security Header*) yang melakukan enkripsi dan layanan autentikasi.

Oktivasari dan Budi Utomo (2016:92) menjelaskan:

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalu-lintas yaitu *Authetication Header (AH)* dan *Encapsulating Security Payload (ESP)*.

## **2.2. Konsep Dasar Jaringan**

Madcoms (2010) dalam bukunya menjelaskan, jaringan komputer adalah hubungan antara 2 komputer atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data atau informasi, berbagi *resource* yang dimiliki, seperti: *file*, *printer*, media penyimpanan (*harddisk*, *floppy disk*, *cd-rom*, *flash disk*). Data yang berupa teks, audio maupun video, bergerak melalui media kabel atau tanpa kabel (*wireless*) sehingga memungkinkan pengguna komputer dalam jaringan komputer dapat saling bertukar *file*, mencetak pada *printer* yang sama dan menggunakan *hardware* atau *software* yang terhubung dalam jaringan bersama-sama.

### 2.2.1. Jenis Jaringan Komputer

Jenis jaringan komputer menurut Madcoms (2010) secara umum dibagi menjadi empat jenis, yaitu:

#### 1. *Local Area Network*

*Local Area Network* (LAN) dapat didefinisikan sebagai kumpulan komputer yang saling dihubungkan bersama didalam satu area tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung. LAN dapat juga didefinisikan berdasarkan pada penggunaan alamat IP komputer pada jaringan. Suatu komputer atau *host* dapat dikatakan satu LAN bila memiliki alamat IP yang masih dalam satu alamat jaringan, sehingga tidak memerlukan *router* untuk berkomunikasi.

Jaringan LAN dapat juga dibagi menjadi dua tipe, yaitu jaringan *peer to peer* dan jaringan *client-server*. Pada jaringan *peer to peer*, setiap komputer yang terhubung dapat bertindak baik sebagai *workstation* maupun *server*, sedangkan pada jaringan *client-server*, hanya satu komputer yang bertindak sebagai *server* dan komputer lain sebagai *workstation*.

#### 2. *Metropolitan Area Network*

*Metropolitan Area Network* (MAN) merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN.

MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

### 3. *Wide Area Network*

*Wide Area Network* (WAN) adalah jaringan yang biasanya sudah menggunakan media *wireless*, sarana satelit ataupun kabel serat optik, karena jangkauannya yang lebih luas, bukan hanya meliputi satu kota atau antar kota dalam suatu wilayah, tetapi mulai menjangkau area atau wilayah otoritas negara lain.

WAN biasanya lebih rumit dan sangat kompleks bila dibandingkan LAN maupun MAN. WAN menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN kedalam komunikasi global seperti internet, meski demikian antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.

### 4. Internet dan Intranet

Internet yang merupakan gabungan dari LAN, MAN, dan WAN, adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia. Setiap komputer dan jaringan terhubung secara langsung maupun tidak langsung ke beberapa jalur utama yang disebut internet *backbone* dan dibedakan satu dengan yang lainnya menggunakan alamat unik yang biasa disebut dengan alamat *Internet Protocol* (IP).

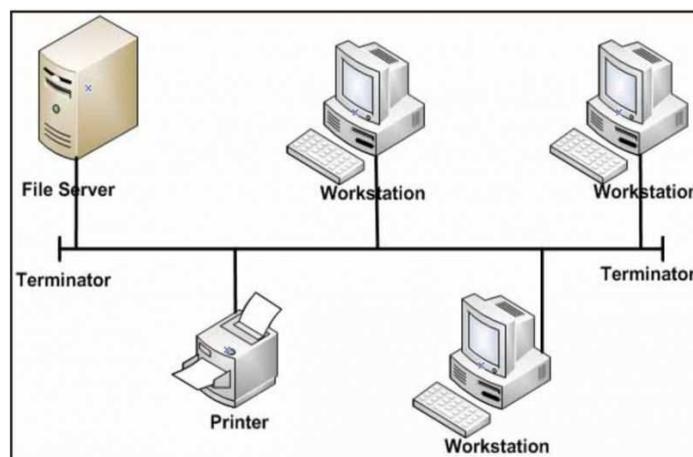
Aplikasi pada jaringan internet dapat juga diterapkan pada sebuah LAN yang memiliki *server*. Sebagai contoh di perusahaan yang memiliki jaringan *client-server*. Bila aplikasi yang ada pada internet, seperti *mail server*, diterapkan pada perusahaan tersebut, maka jaringan ini dapat disebut sebagai intranet. *Client* dapat mengakses *server* tersebut seperti mengakses internet pada umumnya. *Client* juga dapat mengakses aplikasi lain di luar *server* perusahaan (internet).

## 2.2.2. Topologi Jaringan Komputer

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Menurut Madcoms (2010) ada beberapa jenis topologi yaitu:

### 1. Topologi *Bus*

Pada topologi *bus* digunakan sebuah kabel tunggal atau kabel pusat di mana seluruh *workstation* dan *server* dihubungkan. Keunggulan topologi *bus* adalah pengembangan jaringan atau penambahan *workstation* baru dapat dilakukan dengan mudah tanpa mengganggu *workstation* lain. Kelemahan dari topologi ini adalah bila terdapat gangguan di sepanjang kabel pusat maka keseluruhan jaringan akan mengalami gangguan.



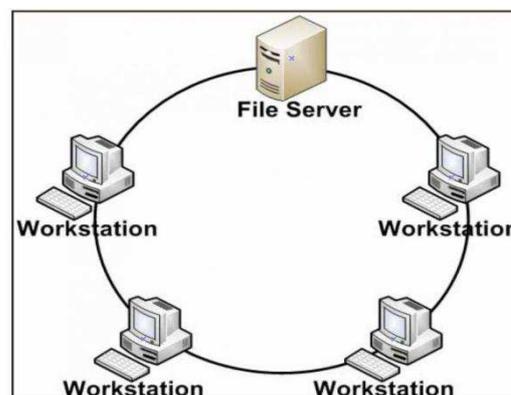
Gambar 2.1. Topologi *Bus*

### 2. Topologi *Token-Ring*

Pada topologi *ring*, semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila

alamat-alamat yang dimaksud sesuai maka informasi diterima dan bila tidak informasi akan dilewatkan.

Kelemahan dari topologi ini adalah setiap node dalam jaringan akan selalu ikut serta mengelola informasi yang dilewatkan dalam jaringan, sehingga bila terdapat gangguan di suatu *node* maka seluruh jaringan akan terganggu. Keunggulan topologi ring adalah tidak terjadinya *collision* atau tabrakan pengiriman data seperti pada topologi *bus*, karena hanya satu *node* dapat mengirimkan data pada suatu saat.

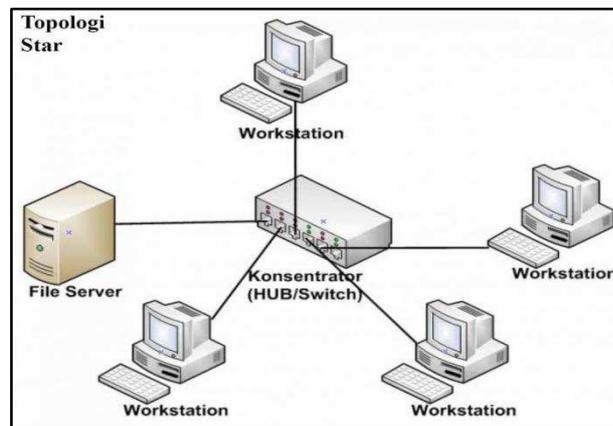


Gambar 2.2. Topologi *Ring*

### 3. Topologi *Star*

Pada topologi *star*, masing-masing *workstation* dihubungkan secara langsung ke *server* atau *hub*. Keunggulan dari topologi *star* adalah dengan adanya kabel tersendiri untuk setiap *workstation* ke *server*, maka *bandwidth* atau lebar jalur komunikasi dalam kabel akan semakin lebar sehingga akan meningkatkan unjuk kerja jaringan secara keseluruhan. Bila terdapat gangguan di suatu jalur kabel maka gangguan hanya akan terjadi dalam komunikasi antara *workstation* yang bersangkutan dengan *server*, jaringan secara keseluruhan tidak

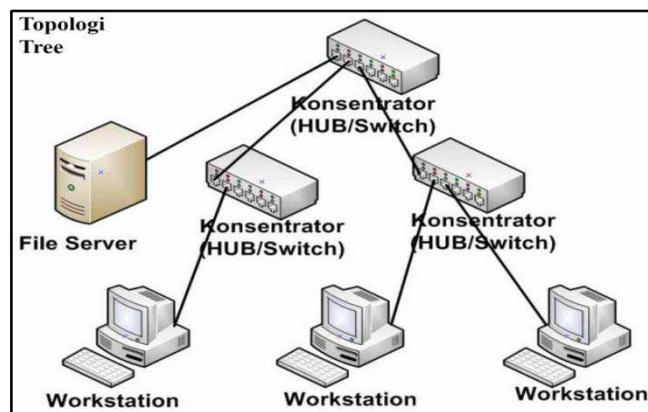
mengalami gangguan. Kelemahan dari topologi *star* adalah kebutuhan kabel yang lebih besar dibandingkan dengan topologi lainnya.



Gambar 2.3. Topologi *Star*

#### 4. Topologi *Tree*

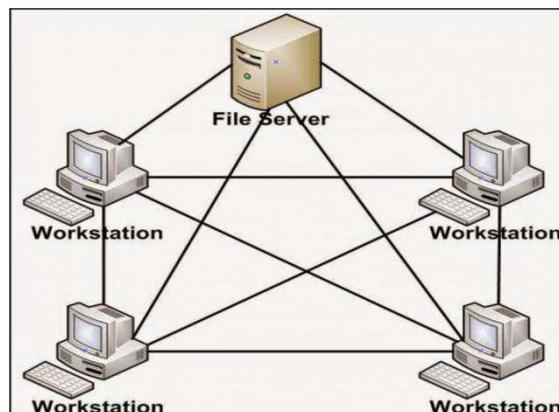
Topologi *tree* merupakan gabungan dari topologi *star* dengan topologi *bus*.



Gambar 2.4. Topologi *Tree*

#### 5. Topologi *Mesh*

Topologi *mesh* digunakan pada kondisi di mana tidak ada hubungan komunikasi terputus secara absolut antar *node* komputer. Topologi ini merefleksikan desain internet yang memiliki *multi path* ke berbagai lokasi.



Gambar 2.5. Topologi *Mesh*

### 2.2.3. Perangkat Jaringan

Masih dalam bukunya, Madcoms (2010) menjelaskan tentang perangkat jaringan adalah semua komputer, *peripheral*, *interface card*, dan perangkat tambahan yang terhubung ke dalam suatu sistem jaringan komputer untuk melakukan komunikasi data. Perangkat jaringan komputer terdiri dari:

#### 1. *Server*

*Server* merupakan pusat kontrol dari jaringan komputer. *Server* berfungsi untuk menyimpan informasi dan untuk mengelola suatu jaringan komputer. *Server* akan melayani seluruh *client* atau *workstation* yang terhubung ke jaringan. Sistem operasi yang digunakan pada *server* adalah sistem operasi yang khusus yang dapat memberikan layanan bagi workstation.

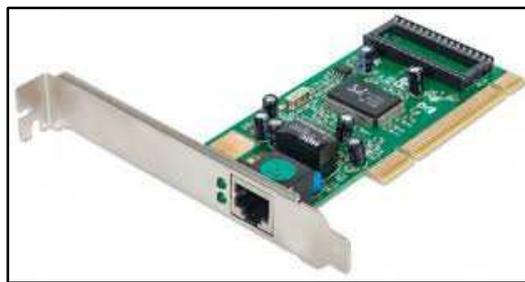
#### 2. *Workstation*

*Workstation* adalah komputer yang terhubung dengan sebuah LAN. Semua komputer yang terhubung dengan jaringan dapat dikatakan sebagai

*workstation*. Komputer ini yang melakukan akses ke *server* guna mendapat layanan yang telah disediakan oleh *server*.

### 3. *Network Interface Card*

*Network Interface Card* (NIC) adalah *expansion board* yang digunakan supaya komputer dapat dihubungkan dengan jaringan. Sebagian besar NIC dirancang untuk jaringan, protokol, dan media tertentu. NIC biasa disebut dengan LAN card.



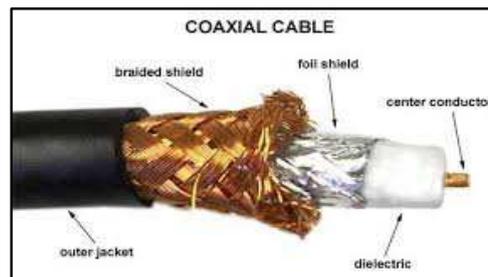
Gambar 2.6. NIC

### 4. Kabel

Kabel adalah saluran yang menghubungkan antara 2 *workstation* atau lebih. Jenis-jenis kabel yang digunakan dalam jaringan antara lain kabel *coaxial*, *fiber optic*, dan *Twisted Pair*.

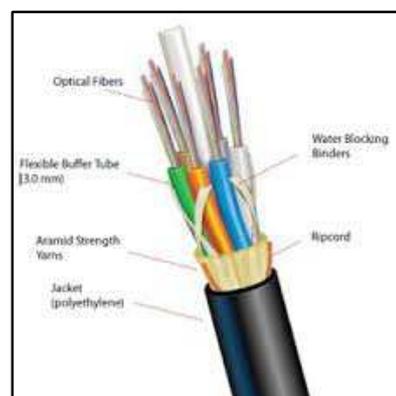
Kabel *coaxial* hanya memiliki satu konduktor yang berada di pusat kabel. Kabel ini memiliki lapisan plastik yang berfungsi untuk pembatas konduktor dengan anyaman kabel yang ada pada lapisan berikutnya. Kabel *coaxial* memiliki kecepatan transfer sampai 10 Mbps. Kabel *coaxial* sering digunakan untuk kabel TV, ARCnet, *thick ethernet* dan *thin ethernet*. *Thick coaxial/10Base5/RG-8* sering digunakan untuk *backbone*, untuk instalasi jaringan antar gedung. Kabel ini secara fisik berat dan tidak fleksibel, namun ia mampu menjangkau jarak 500

m bahkan lebih. *Thin coaxial*/10Base2/RG-58 sering digunakan untuk jaringan antar *workstation*. Kabel ini secara fisik lebih mudah ditangani daripada RG-8 karena lebih fleksibel dan ringan. *Thick coaxial* mempunyai diameter rata-rata 12 mm sedangkan *thin coaxial* mempunyai diameter rata-rata berkisar 5mm. Setiap perangkat dihubungkan dengan BNCT-*connector*.



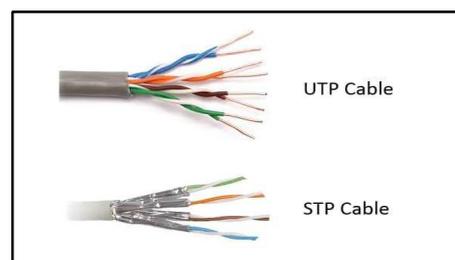
Gambar 2.7. Kabel *Coaxial*

Kabel fiber optik memiliki inti kaca yang dilindungi oleh beberapa lapisan pelindung. Pengiriman data pada kabel ini menggunakan sinar. Kabel fiber optik memiliki jarak yang lebih jauh daripada *twisted pair* dan *coaxial*. Kabel ini juga memiliki kecepatan transfer data yang lebih baik dalam pengiriman data, yaitu mencapai 155 Mbps. Kabel fiber optik memiliki dua tipe, yaitu *single mode* dan *multi mode*. Tipe kabel *single mode* memiliki diameter *core* 9 micron, sedangkan kabel *multi mode* memiliki diameter *core* sebesar 62,5 micron.



Gambar 2.8. Fiber Optik

Kabel *twisted pair*, secara umum dibagi menjadi 2 tipe, *Shielded Twisted Pair* (STP) dan *Unshielded Twisted Pair* (UTP). Sepasang kabel yang ditwist (pilin), yang jumlah pasangannya dapat terdiri dari dua, empat atau lebih. Fungsi *twist* bertujuan untuk mengurangi interferensi elektromagnetik terhadap kabel lain atau terhadap sumber eksternal. Kecepatan transfer data yang dapat dilayani sampai 10 Mbps. Konektor yang biasa digunakan adalah RJ-11 atau RJ-45. Dari kedua tipe ini, tipe UTP adalah tipe yang sering digunakan pada jaringan LAN. UTP memiliki 4 pasang kabel terpilin (8 buah kabel) dan hanya 4 buah kabel yang digunakan dalam jaringan. Perangkat yang berkenaan dengan penggunaan jenis kabel ini adalah konektor RJ45 dan *Hub* atau *Switch*.



Gambar 2.9. Kabel UTP dan STP

##### 5. *Hub* dan *Switch*

Pada jaringan bertopologi *star*, *hub* adalah perangkat dengan banyak *port* yang memungkinkan beberapa titik (dalam hal ini komputer yang sudah memasang NIC) bergabung menjadi satu jaringan. Pada jaringan sederhana, salah satu *port* pada *hub* terhubung ke komputer *server*. Bisa juga *hub* tak langsung terhubung ke *server* tetapi juga ke *hub* lain, ini terutama terjadi pada jaringan yang cukup besar. *Hub* bekerja dengan metode *broadcast*, sehingga semua *port* yang ada akan dikirim sinyalnya. Ini berarti, jika lebih dari satu komputer mengirim data ke jaringan secara bersamaan, maka tidak satupun komputer yang

dapat memanfaatkan 100% *bandwidth* jaringan yang tersedia. *Hub* berada pada *physical layer*.



Gambar 2.10.Hub

*Switch* adalah perangkat yang juga berfungsi untuk menghubungkan *multiple* komputer. *Switch* secara fisik sama dengan *hub* tetapi logikalnya sama dengan barisan *brigde*. Peningkatan kecerdasan dibandingkan *hub*, yaitu memiliki pengertian terhadap alamat MAC (*Medium Access Control*) atau pada *link layer model OSI* sehingga hanya mengirimkan data pada *port* yang dituju (*unicast*). Hal ini berbeda dengan *hub* yang mengirimkan data ke semua *port* (*broadcast*). Proses kerjanya adalah apabila paket data datang, *header* dicek untuk menentukan di segmen mana tujuan paket datanya. Kemudian data akan dikirim kembali (*forwarded*) ke segmen tujuan tersebut.



Gambar 2.11.Switch

## 6. Bridge

*Bridge* adalah piranti yang meneruskan lalu lintas antara segmen jaringan berdasar informasi pada lapisan *data link*. Segmen ini mempunyai alamat lapisan jaringan yang sama. *Bridge* bekerja dengan mengenali alamat MAC asal yang

mentransmisi data ke jaringan dan secara otomatis membangun sebuah tabel internal. Tabel ini berfungsi untuk menentukan ke segmen mana paket akan di *route* dan menyediakan kemampuan *filtering*. *Bridge* membagi satu buah jaringan besar kedalam beberapa jaringan kecil. *Bridge* juga dapat di gunakan untuk mengkoneksi diantara *network* yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula.



Gambar 2.12. *Bridge*

## 7. *Router*

*Router* adalah perangkat yang berfungsi menghubungkan suatu LAN ke suatu *internetworking* atau WAN dan mengelola penyaluran lalu-lintas data di dalamnya. *Router* akan menentukan jalur terbaik untuk komunikasi data. *Router* bekerja pada *layer network* dari model OSI untuk memindahkan paket-paket antar jaringan menggunakan alamat logikanya. *Router* memiliki tabel *routing* yang melakukan pencatatan terhadap semua alamat jaringan yang diketahui dan lintasan yang mungkin dilalui serta waktu tempuhnya. *Router* bekerja hanya jika protokol jaringan yang dikonfigurasi adalah protokol yang *routable* seperti TCP/IP atau IPX/SPX. Ini berbeda dengan *bridge* yang bersifat *protocol independent*.



Gambar 2.13. *Router*

## 8. Repeater

*Repeater* bekerja pada level *physical layer* dalam model jaringan OSI. *Repeater* bertugas meregenerasi atau memperkuat sinyal-sinyal yang masuk. Pada ethernet kualitas transmisi data hanya dapat bertahan dalam *range* waktu dan jangkauan terbatas, yang selanjutnya mengalami degradasi. *Repeater* akan berusaha mempertahankan integritas sinyal dan mencegah degradasi sampai paket-paket data menuju tujuan. Kelemahan *repeater* yaitu tidak dapat melakukan filter *traffic* jaringan. Data (bits) yang masuk ke salah satu *port* dikirim ke luar melalui semua *port*. Dengan demikian data akan tersebar ke segmen-segmen LAN tanpa memperhitungkan apakah data tersebut dibutuhkan atau tidak.



Gambar 2.14. Repeater

## 9. Modem

Modem adalah sebuah *device* yang digunakan sebagai penghubung dari sebuah PC atau jaringan ke Penyedia Layanan Internet (*Internet Service Provider* / ISP). Salah satu modem yang biasa dipakai untuk koneksi ke internet ialah modem ADSL.



Gambar 2.15. Modem ADSL

### 2.3. Manajemen Jaringan

Dalam tulisannya, manajemen jaringan adalah sebuah pekerjaan untuk memelihara seluruh sumber jaringan dalam keadaan baik. Sistem manajemen jaringan adalah sekumpulan perangkat untuk memantau dan mengontrol jaringan. Sistem manajemen jaringan terdiri dari tambahan perangkat keras dan piranti lunak yang diimplementasikan di antara komponen-komponen jaringan yang sudah ada (Hikdayah, 2011:12).

#### 2.3.1. IP Addressing

*IP address* adalah alamat logika yang diberikan ke peralatan jaringan menggunakan protokol TCP/IP. *IP address* terdiri dari 32 bit angka *binary*, yang ditulis dalam empat kelompok yang masing-masing kelompoknya terdiri dari 8 bit (oktat) yang dipisah oleh tanda titik. Contohnya:

11000000.00010000.00001010.00000001

Atau dapat ditulis dalam bentuk empat kelompok format desimal (0-255), misalnya:

192.16.10.1

*IP address* yang terdiri dari 32 bit angka dikenal sebagai IP versi 4 (IPv4). *IP address* terdiri dari *network ID* dan *host ID*. Dimana *network ID* menentukan alamat jaringan, sedangkan *host ID* menentukan alamat *host* atau komputer.

Berapa jumlah *network ID* ataupun *host ID* adalah bergantung pada kelas IP *address* yang dipakai.

IP *address* dapat dibedakan menjadi lima kelas, yaitu A, B, C dan D. Dalam hal ini kelas A, B dan C digunakan untuk *address* biasa. Sedangkan kelas D untuk *multicasting*. Berikut penjelasan masing-masing kelas IP *address*:

#### 1. *Class A address*

Kelas ini didesain untuk mensupport *network* yang sangat besar dengan jumlah lebih dari 16 juta *host address* yang tersedia. Kelas ini menggunakan oktet pertama untuk menunjukkan *network address*, tiga oktet berikutnya tersedia untuk *host address*.

Bit pertama dari oktet pertama kelas A adalah 0, dengan demikian maka *range* yang bisa didapatkan adalah 0-127 dalam bilangan biner atau 00000000-01111111. Tetapi untuk angka 0 dan 127 tidak dapat digunakan. Serta IP *address* 127.0.0.0 khusus digunakan untuk *loopback testing*. Maka angka dari oktet pertama yang merupakan nilai dari 1 sampai 126 adalah alamat kelas A.

#### 2. *Class B address*

Kelas ini didesain untuk kebutuhan jaringan skala menengah hingga besar. Kelas ini menggunakan dua oktet pertama untuk menunjukkan *network address*, dua oktet berikutnya tersedia untuk *host address*.

Dua bit pertama dari oktet pertama kelas B adalah 10, dengan demikian maka *range* yang bisa didapatkan adalah 128-191 dalam bilangan biner atau

10000000-10111111. Maka angka dari oktet pertama yang merupakan nilai dari 128 sampai 191 adalah alamat kelas B.

### 3. Class C address

Kelas ini banyak digunakan untuk mensupport jaringan skala kecil dengan jumlah maksimum host per networknya adalah 254 host.

Tiga bit pertama dari oktet pertama kelas C adalah 110, dengan demikian maka *range* yang bisa didapatkan adalah 192-223 dalam bilangan biner atau 11000000-11011111. Maka angka dari oktet pertama yang merupakan nilai dari 192 sampai 223 adalah alamat kelas C.

### 4. Class D address

Kelas ini digunakan untuk *multicasting*, yaitu *network address* yang unik yang menunjukkan paket dengan alamat tujuan ke *group predefined* dari sebuah IP *address*. Oleh karena itu *single unit* dapat mentransmit aliran tunggal dari data secara simultan ke lebih dari satu penerima.

Empat bit pertama dari oktet pertama kelas D adalah 1110, dengan demikian maka *range* yang bisa didapatkan adalah 224-239 dalam bilangan biner atau 11100000-11101111. Maka angka dari oktet pertama yang merupakan nilai dari 224 sampai 239 adalah alamat kelas D.

Tabel 2.1. Tabel IP Address

Kelas IP	Range	First Network ID	Last Network ID	Default Subnet Mask	Max Usable Host Per Network ID
Kelas A	1 - 126	1.0.0.0	126.0.0.0	255.0.0.0	16777216
Kelas B	128 - 191	128.0.0.0	191.255.0.0	255.255.0.0	65536
Kelas C	192 - 223	192.0.0.0	233.255.255.0	255.255.255.0	254
Kelas D	224 - 239	Digunakan untuk keperluan Multicasting.			
Kelas E	240 - 255	Digunakan untuk keperluan pengembangan (research and experiment)			

### 2.3.2. Routing

*Routing* dibedakan menjadi dua jenis, yaitu *routing* statis (*static routing*) dan *routing* dinamis (*dynamic routing*) (saputra dkk, 2015:3).

#### 1. *Routing* Statis

*Routing* statis mempunyai pengaturan paling sederhana yang dapat dilakukan pada jaringan komputer. Administrator jaringan hanya mengisi setiap entri dalam *forwarding table* di setiap *router* yang ada di jaringan tersebut.

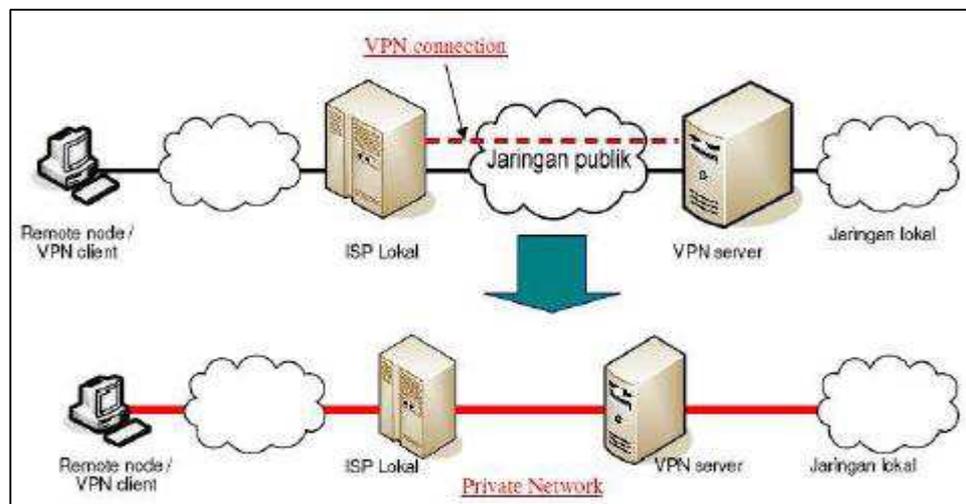
#### 2. *Routing* Dinamis

*Routing* dimana *router* dapat menentukan sendiri rute terbaik yang akan dilaluinya dalam meneruskan sebuah paket dari *network* satu ke *network* lainnya. Administrator jaringan hanya menentukan bagaimana *router* mempelajari paket. Rute pada *routing* dinamis dapat berubah sesuai dengan pelajaran yang didapat oleh *router*.

### 2.3.3. VPN

VPN adalah singkatan dari *virtual private network*, yaitu jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya internet) untuk menghubungkan antar *remote-site* secara aman. Perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi

*traffic* (lalu lintas) antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya ke dalam *remote-site*.



Gambar 2.16. Konsep VPN

VPN adalah sebuah koneksi virtual yang bersifat *private* mengapa disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual dan mengapa disebut *private* karena jaringan ini merupakan jaringan yang tidak semua orang bisa mengaksesnya. VPN menghubungkan PC dengan jaringan publik atau internet namun sifatnya *private*, karena bersifat *private* maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya. Oleh karena itu diperlukan keamanan data.

Keamanan dengan konsep demikian maka jaringan VPN ini menawarkan keamanan dan *untraceable*, tidak dapat terdeteksi sehingga IP kita tidak diketahui karena yang digunakan adalah IP publik milik *VPN server*. Dengan ada enkripsi dan dekripsi maka data yang lewat jaringan internet ini tidak dapat diakses oleh orang lain bahkan oleh *client* lain yang terhubung ke *server* VPN yang sama

sekalipun. Karena kunci untuk membuka enkripsinya hanya diketahui oleh *server* VPN dan *client* yang terhubung.

#### 2.3.4. L2TP/IPsec

L2TP merupakan *tunneling* protokol yang memadukan dua buah protokol yaitu *Layer 2 Forwarding* milik Cisco dan PPTP milik Microsoft. Umumnya digunakan untuk membuat *Virtual Private Dial Network* (VPDN) yang biasanya menggunakan port 1702 dengan protokol UDP.

Metode L2TP ini bisa diaplikasikan dalam dua jenis koneksi yaitu *site-to-site* VPN atau *remote-access* VPN.

*Site-to-site* VPN adalah koneksi *tunelling* antara dua buah jaringan yang berbeda yang dihubungkan melalui internet. Dalam VPN jenis ini menggunakan sebuah VPN *server* pada masing-masing jaringan yang saling terhubung. Dibutuhkan konfigurasi di kedua VPN *server* tersebut agar dapat bisa saling terkoneksi.

*Remote-access* VPN adalah koneksi *tunelling* antara satu perangkat pengguna dengan VPN server melalui jaringan internet. Dibutuhkan konfigurasi pada VPN *server* untuk dapat diakses oleh perangkat pengguna diluar kantor dengan otentikasi *username* dan *password*.

L2TP/IPsec mempunyai keunggulan dalam hal kemudahan konfigurasi dan juga keamanan transmisi data.

## 2.4. Konsep Penunjang Usulan

Dalam sub-bab ini penulis akan menjelaskan beberapa hal yang diperlukan dalam perancangan jaringan usulan VPN ini. Sebagian besar adalah perangkat lunak atau aplikasi pendukung untuk melakukan testing dan monitoring jaringan VPN yang akan dibuat.

### 1. VMware Workstation

VMware *workstation* adalah sebuah perangkat lunak mesin virtual untuk arsitektur x86 dan x86-64 dari VMware, sebuah bagian dari EMC *corporation*. Dengan VMware *workstation* ini kita dapat menjalankan satu atau banyak sistem operasi secara simultan menggunakan satu mesin fisik. Dalam penelitian kali ini penulis menggunakan VMware *workstation* sebagai pengganti *router* fisik mikrotik untuk menjalankan *server* VPN.

### 2. Winbox

Winbox adalah sebuah perangkat lunak atau utilitas yang digunakan untuk *remote* sebuah *server* mikrotik kedalam mode GUI (*Graphical User Interface*) melalui sistem operasi Windows. Penulis menggunakan Winbox ini untuk mempermudah dalam konfigurasi *server* VPN berbasis mikrotik yang digunakan.

### 3. Wireshark

Wireshark merupakan salah satu tools atau aplikasi *network analyzer* atau penganalisa jaringan. Penganalisaan kinerja jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang

berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk *sniffing* (memperoleh informasi penting seperti *password email*, dll).

Wireshark sendiri merupakan *free tools* untuk *Network Analyzer* yang ada saat ini. Dan tampilan dari Wireshark ini sendiri terbilang sangat bersahabat dengan *user* karena menggunakan tampilan grafis atau GUI (*Graphical User Interface*).

#### 4. Packet Tracer

Packet Tracer adalah simulator alat-alat jaringan Cisco yang sering digunakan sebagai media pembelajaran dan pelatihan, dan juga dalam bidang penelitian simulasi jaringan komputer. Program ini dibuat oleh Cisco *Systems* dan disediakan gratis untuk fakultas, siswa dan alumni yang telah berpartisipasi di *Cisco Networking Academy*.

Fungsinya adalah untuk merancang sebuah sistem atau topologi jaringan yang akan di terapkan pada dunia nyata, karena kalau kita merancang topologi jaringan komputer tanpa bantuan aplikasi seperti ini membutuhkan biaya yang mahal. Untuk itu dibuat aplikasi seperti ini agar semua orang dapat belajar tanpa membutuhkan biaya yang mahal.

#### 5. GNS3

Adalah *software* simulasi jaringan berbasis GUI yang mirip dengan Packet Tracer. Namun pada GNS3 memungkinkan simulasi jaringan yang kompleks, karena menggunakan sistem operasi asli dari perangkat-perangkat jaringan seperti *router* dan *switch*.