# BAB II
# TEORI PENDUKUNG

## 2.1 Jaringan Komputer

Jaringan komputer merupakan sejumlah komputer yang dapat saling berkomunikasi. Dalam komunikasi ini dapat terjadi perpindahan data ataupun berbagi sumber daya. Dalam skala luas, internet juga merupakan jaringan komputer. Jadi, suatu jaringan komputer tidak hanya terjadi pada sejumlah komputer yang terdapat pada suatu ruangan ataupun suatu gedung atau perusahaan.

Pada dasarnya teknologi jaringan komputer itu sendiri merupakan perpaduan antara teknologi komputer dan juga teknologi komunikasi.

**Pengenalan Jaringan Komputer**

Untuk bisa membangun sebuah jaringan komputer, anda perlu memahami tipe dan dasar arsitektur jaringan komputer yang sesuai dengan kondisi di tempat anda. Hal ini penting karena tipe dan arsitektur sebuah jaringan menentukan perangkat apa yang harus disediakan untuk membangun jaringan tersebut.

### 2.1.1 JENIS JARINGAN KOMPUTER

Secara umum jaringan komputer dibagi atas lima jenis, yaitu;

1. Local Area Network (LAN)

Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya printer) dan saling bertukar informasi.

2. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN), pada dasarnya 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 (WAN)

Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

4. Internet

Sebenarnya terdapat banyak jaringan didunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kompatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet.

5. Jaringan Tanpa Kabel (Nirkable)

Jaringan tanpa kabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapat informasi atau melakukan komunikasi walaupun sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan

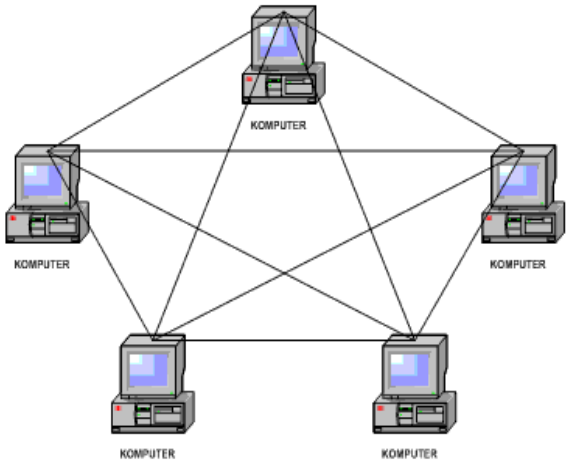
memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel.

### 2.1.2 Tipe Jaringan Komputer

Menurut fungsi komputer pada sebuah jaringan, maka tipe jaringan computer dapat dibedakan menjadi dua tipe, yaitu :

1. Jaringan Peer to Peer atau Point to Point

   Pada jaringan peer to peer, setiap komputer yang terhubung pada jaringan dapat langsung berkomunikasi dengan komputer-komputer lain secara langsung tanpa melalui komputer perantara.

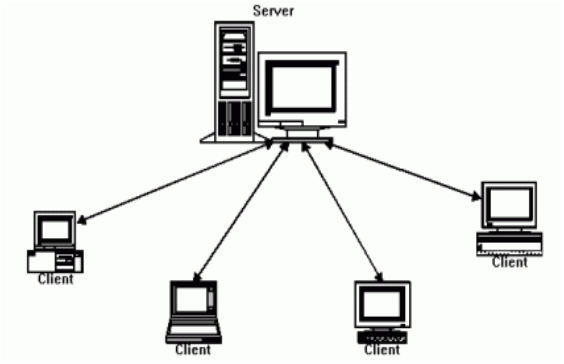



Gambar Jaringan Peer to Peer

   Gambar diatas menunjukkan bahwa masing-masing komputer dalam sebuah jaringan peer to peer terhubung secara langsung ke seluruh komputer yang terdapat dalam jaringan tersebut.

2. Jaringan Client-Server

   Pada jaringan client-server terdapat sebuah jaringan komputer yang berfungsi sebagai server sedangkan komputer-komputer yang lain berfungsi sebagai client.



Gambar Jaringan Client Server

Pada gambar diatas dapat dilihat bahwa komputer-komputer dalam jaringan (client) dapat saling berkomunikasi melalui perantara komputer server. Jika komputer server tidak aktif, maka komputer-komputer client tidak akan dapat berkomunikasi.

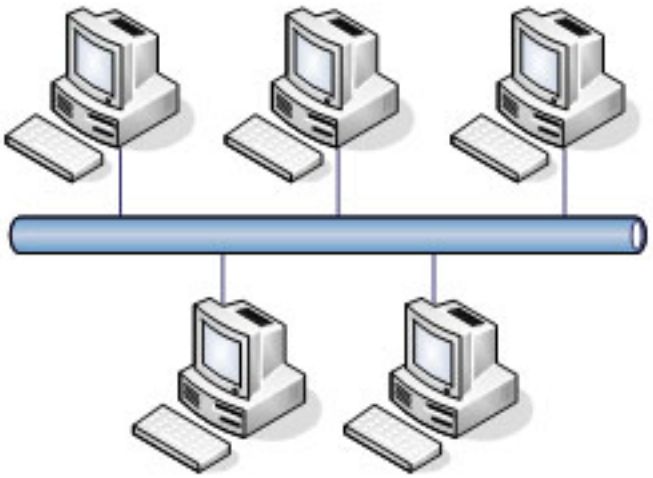
### 2.1.3 Arsitektur Jaringan Komputer

Selain tipe jaringan, hal lain yang berkaitan dengan bentuk jaringan komputer adalah arsitektur jaringan tersebut. Arsitektur jaringan komputer dibedakan menjadi arsitektur fisik (tipe jaringan komputer berdasarkan topologi) dan Tipe jaringan komputer berdasarkan ruang lingkup dan jangkauan.

Bentuk-bentuk arsitektur komputer secara fisik (berdasarkan topologi) sebagai berikut :

1. Topologi Bus

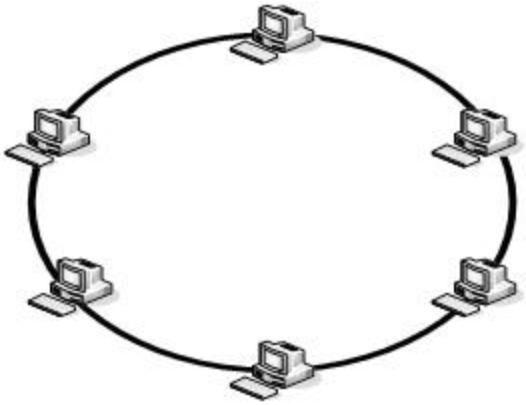
   Pada topologi bus, seluruh komputer dalam sebuah jaringan terhubung pada sebuah bus atau jalur komunikasi data (kabel) yang mana kedua ujung jaringan harus diakhiri dengan sebuah terminator. Komputer-komputer tersebut berkomunikasi dengan cara mengirim dan mengambil data di sepanjang bus tersebut. Topologi ini merupakan topologi jaringan paling sederhana dan biasanya jaringan ini menggunakan media yang berupa kabel coaxial.



Gambar Topologi Bus

2. Topologi Ring (Topologi Cincin)

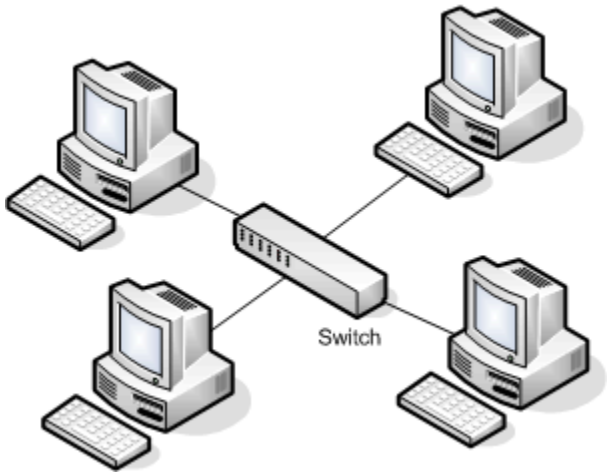
Pada topologi cincin, jaringan ini terhubung pada sebuah jalur data yang menghubungkan komputer satu dengan yang lainnya secara sambung menyambung sedemikian rupa sehingga menyerupai sebuah cincin atau ring. Dalam sistem jaringan ini data dikirim secara berkeliling sepanjang jaringan. Setiap komputer yang mengirim data ke komputer lain dalam jaringan akan menempatkan data tersebut ke dalam ring ini. Selanjutnya komputer yang dituju akan mengambil data tersebut dari ring.



Gambar Topologi Ring

3. Topologi Star (Topologi Bintang)

Pada topologi star (bintang), dimana masing-masing komputer dalam jaringan dihubungkan ke pusat atau sentral dengan mengunakan jalur (bus) yang berbeda. Komunikasi pada jaringan diatur oleh sentral jaringan.

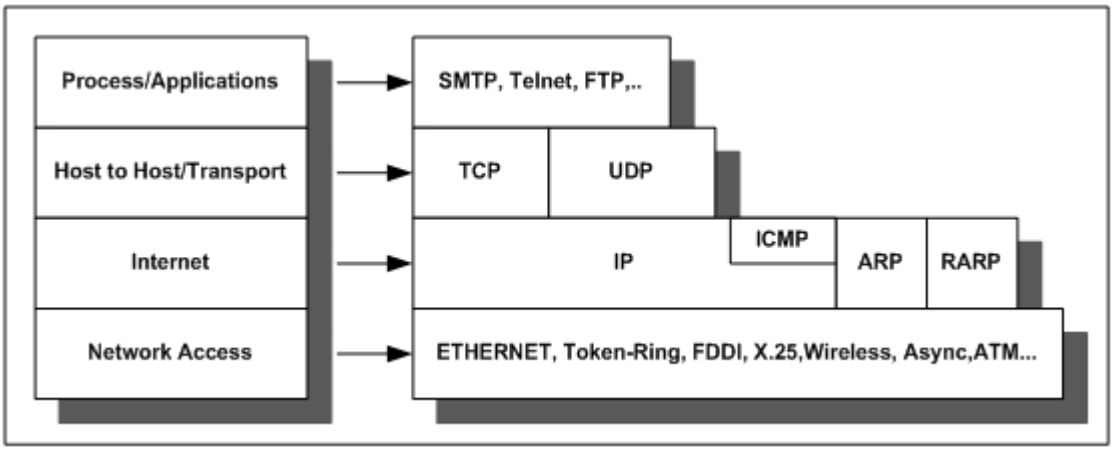



Gambar Topologi Star

Dari gambar diatas tampak bahwa komputer-komputer dalam jaringan tersebut terhubung ke pusat dengan menggunakan jalur masing-masing.

## 2.2 Mekanisme Kerja TCP/IP

*Transfer Control Protocol/Internet Protocol* (TCP/IP) pada dasarnya terdiri dari beberapa protokol yang berbeda, masing-masing dirancang untuk memenuhi tugas-tugas khusus dalam jaringan yang menggunakan TCP/IP. Berkat prinsip ini, tugas masing-masing protokol menjadi jelas dan sederhana. Protokol yang satu tidak perlu mengetahui cara kerja protokol yang lain, sepanjang masih bisa saling mengirim dan menerima data.




**Gambar 2.3 Protokol dan network di dalam model TCP/IP**

Oleh karenanya, TCP/IP menjadi protokol komunikasi data yang fleksibel. Protokol TCP/IP dapat diterapkan dengan mudah di setiap jenis komputer dan *interface* jaringan, karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau jaringan tertentu. Agar TCP/IP dapat berjalan di atas *interface* jaringan tertentu, hanya perlu dilakukan perubahan pada protokol yang berhubungan dengan *interface* saja.

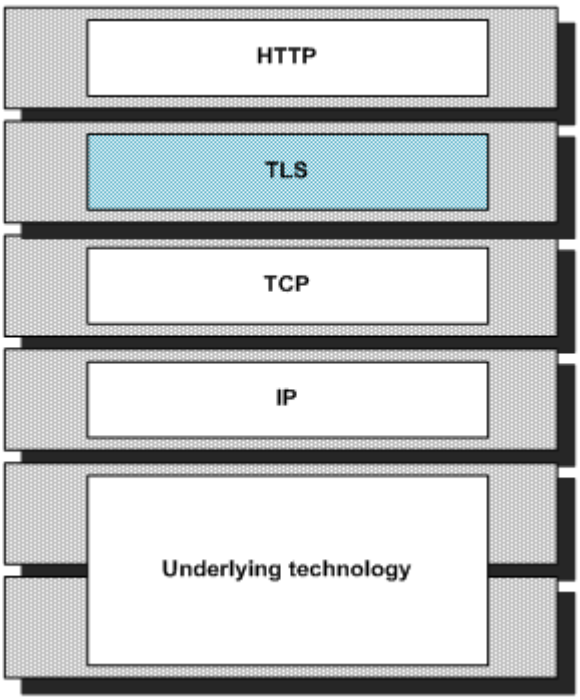
Model referensi TCP/IP yang ditunjukkan pada Gambar 2.3 menunjukkan empat lapisan dalam model TCP/IP yaitu: *Network Access, Internet/IP*, *Host to Host/Transport* dan *Application/process*.yang berhubungan dengan protokol otentikasi hanya terdapat pada lapisan/*layer Application*, *Transport* dan *Internet* saja. Pada setiap lapisan tersebut akan dilihat dari sisi keamanan/*security* ini dikarenakan sistem otentikasi berhubungan erat dengan faktor keamanan.

### 2.2.1 Security Lapisan Aplikasi (Application Layer Security)

Implementasi keamanan pada lapisan aplikasi adalah yang paling mudah dan sederhana, jika komunikasi internet melibatkan dua pihak, seperti kasus komunikasi *email* dan *telnet*. Pengirim dan penerima mempunyai kesepakatan untuk menggunakan protokol yang sama dan jenis layanan keamanan yang diinginkan. Pada bagian lapisan ini terdapat dua protokol yang digunakan, yaitu PGP (*Pretty Good Privacy***)** dan SSH (*secure shell)*.

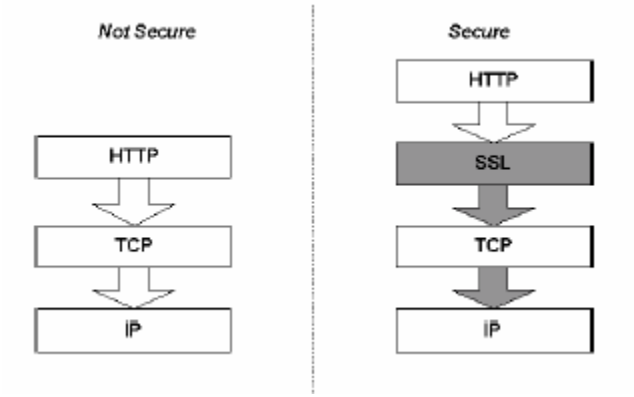
### 2.2.2 Security Lapisan Transport (Transport Layer Security)

*Transport Layer Security* (TLS) berada antara lapisan aplikasi dan lapisan transport. Pada Gambar 2.4 diperlihatkan, bahwa TLS berada diantara lapisan protokol HTTP (aplikasi) dan protokol TCP (transport). Dengan demikian dapat dinyatakan bahwa lapisan aplikasi dalam hal ini HTTP menggunakan TLS dan TLS menggunakan layanan dari lapisan transport dalam hal ini TCP untuk membawa informasi.




**Gambar 2.4 Posisi TLS pada lapisan protokol IP**

TLS dirancang untuk menyediakan keamanan pada lapisan transport. TLS diperoleh dari suatu protokol keamanan yang disebut dengan SSL (*Secure Sockets Layer*) yang dirancang oleh Netscape guna menjamin keamanan WWW. TLS adalah bentuk lain dari SSL, yang dirancang oleh IETF (*Internet Engineering Task Force*) untuk transaksi di internet seperti ditunjukkan oleh Gambar 2.5.




**Gambar 2.5 SSL merupakan lapisan terpisah dalam susunan protokol Internet**

SSL merupakan Protokol berlapis. Dalam tiap lapisannya, sebuah data terdiri dari panjang, deskripsi dan isi. SSL mengambil data untuk dikirimkan, dipecahkan kedalam blok-blok yang teratur, kemudian dikompres jika perlu, menerapkan MAC, dienkripsi, dan hasilnya dikirimkan. Di tempat tujuan, data didekripsi, verifikasi, dekompres, dan disusun kembali. Hasilnya dikirimkan ke klien di atasnya. Cara kerja SSL dapat kita lihat dengan tahapan – tahapan berikut ini:

1. Klien membentuk koneksi awal ke *server* dan meminta koneksi SSL.
2. Bila *server* yang dihubungi telah dikonfigurasi dengan benar, maka *server* ini akan mengirimkan *public key* miliknya kepada klien.
3. Klien membandingkan sertifikat dari *server* ke basisdata *trusted authorities*. Bila sertifikat ini terdaftar, artinya klien mempercayai *server* tersebut dan akan maju kelangkah 4. Bila sertifikat itu terdaftar, maka pemakai harus menambahkan sertifikat ini ke *trusted database* sebelum maju ke langkah 4.
4. Klien menggunakan *public key* yang didapatnya untuk men-*enkrip* sesi dan mengirimkan *session key* ke *server*. Bila *server* meminta sertifikat klien di langkah 2, maka klien harus mengirimkannya sekarang.
5. Bila *server* dikonfigurasi untuk menerima sertifikat, maka *server* akan membandingkan sertifikat yang diterimanya dengan basisdata *trusted authorities* dan akan menerima atau menolak koneksi yang diminta.

Bila kondisi ditolak, suatu pesan kegagalan akan dikirimkan ke klien. Bila koneksi diterima, atau bila *server* tidak dikonfigurasi untuk menerima

sertifikat, maka *server* akan men-*decode session key* yang didapat dari klien dengan *private key* milik *server* dan mengirimkan pesan berhasil ke klien yang sekaligus akan membuka suatu *secure data chanel.*

### 2.2.3 Security Lapisan IP (IPSec)

IP Security (IPSec) merupakan sekumpulan protokol yang dirancang oleh IETF (*Internet Engineering Task Force* ) untuk menyediakan layanan keamanan bagi paket data yang dibawa di internet. IPSec tidak didefinisikan untuk menggunakan berbagai metoda enkripsi atau otentikasi yang spesifik. Tetapi IPSec menyediakan sebuah *framework* dan sebuah mekanisme. IPSec mendefinisikan dua protokol yang digunakan pada IP (lapisan *network*) seperti : Protokol *Authentication Header* (AH) dan protokol *Encapsulating Security Payload* (ESP).

## 2.3 Pengertian *Virtual Private Network*

*Virtual Private Network* (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

VPN dapat terjadi antara dua *end-system* atau dua komputer atau antara dua atau lebih jaringan yang berbeda. VPN dapat dibentuk dengan menggunakan teknologi *tunneling* dan enkripsi. Koneksi VPN juga dapat terjadi pada semua layer pada protocol OSI, sehingga komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan. Dengan demikian, VPN juga dapat dikategorikan sebagai infrastruktur WAN alterbatif untuk mendapatkan koneksi *point-to-point* pribadi antara pengirim dan penerima. Dan dapat dilakukan dengan menggunakan media apa saja, tanpa perlu media *leased line* atau *frame relay*.

### 2.3.1 Fungsi Utama Teknologi VPN

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

**a. *Confidentially* (Kerahasiaan)**

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

**b. *Data Intergrity* (Keutuhan data)**

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

**c. *Origin Authentication* (Autentikasi sumber)**

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

### 2.3.2 Kelebihan VPN Dibandingkan Dengan Teknologi *Leased Line*

Manfaat VPN apabila dibandingkan dengan menggunakan teknologi tradisional seperti *leased line* antara lain sebagai berikut.

a. **Biaya lebih murah**

Pembangunan jaringan *leased line* khusus atau pribadi memerlukan biaya yang sangat mahal. VPN dapat menjadi alternatif yang dapat digunakan untuk dapat mengatasi permasalahan diatas. VPN dibangun dengan menggunakan jaringan internet milik publik tanpa perlu membangun jaringan pribadi. Dengan demikian bila ingin menggunakan VPN hanya diperlukan koneksi internet.

b. **Fleksibilitas**

Semakin berkembangnya internet, dan makin banyaknya *user* yang menggunakannya membuat VPN juga ikut berkembang. Setiap *user* dapat tergabung dalam VPN yang telah dibangun tanpa terbatas jarak dan waktu. Fleksibilitas dapat dicapai apabila u*ser* tersebut terkoneksi dengan internet dan mendapat ijin menggunakan VPN.

c. **Kemudahan pengaturan dan administrasi**

Keseluruhan VPN dapat diatur dalam server VPN sendiri, dan untuk dapat digunakan oleh klien, maka perlu diinstal aplikasi VPN pada klien. Hal ini tentu lebih mudah apabila dibandingkan dengan menggunakan *leased line* yang masih perlu memonitor modem.

*d.* **Mengurangi kerumitan pengaturan dengan teknologi *tunneling***

*Tunneling* atau terowongan merupakan kunci utama pada VPN. Koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat *tunnel* yang menghubungkan pengirim dan penerima data. Dengan adanya *tunnel* ini, maka tidak diperlukan pengaturan-pengaturan lain yang ada di luar *tunnel* tersebut, asalkan sumber dari *tunnel* tersebut dapat menjangkau tujuannya.

### 2.3.3 Perangkat VPN

Pada dasarnya, semua perangkat komputer yang dilengkapi dengan fasilitas pengalamatan IP dan diinstal dengan aplikasi pembuat *tunnel* dan algoritma enkripsi dan dekripsi, dapat dibangun komunikasi VPN di dalamnya.

Komunikasi VPN dengan *tunneling* dan enkripsi ini dapat dibangun antara sebuah *router* dengan *router* yang lain, antara sebuah *router* dengan beberapa *router*, antara PC dengan *server* VPN *concentrator*, antara *router* atau PC dengan *firewall* berkemampuan VPN, dan masih banyak lagi.

### 2.3.4 Jenis-jenis VPN

VPN memang telah menjadi sebuah teknologi alternatif sejak lama. Dunia bisnis juga telah menggunakan VPN sebagai kunci dari proses bisnisnya. Seperti misalnya dipergunakan untuk melayani pemesanan tiket perjalanan, transaksi perbankan, transaksi informasi keuangan, dan berbagai sektor penting lain juga telah mempercayakan penggunaan VPN. Berdasarkan *user* yang terkoneksi dengan VPN dan bentuk fasilitas yang diperoleh oleh *user* yang terkoneksi dengan VPN, maka VPN dapat dibedakan menjadi dua jenis, yaitu sebagai berikut.

#### 2.3.4.1 *Intranet* VPN

Intranet merupakan koneksi VPN yang membuka jalur komunikasi pribadi menuju ke jarinan lokal yang bersifat pribadi melalui jaringan publik seperti internet. Dengan melalui VPN jenis ini, *user* dapat langsung mengakses file-file kerja dengan leluasa tanpa terikat tempat dan waktu. Apabila dianalogikan pada sebuah perusahaan, koneksi ke kantor pusat dapat dilakukan dari mana saja, dari kantor pusat menuju ke kantor cabang dapat pula dibuat koneksi pribadi, dan juga dari kantor juga memungkinkan untuk dibuat jalur komunikasi pribadi yang ekonomis.

#### 2.3.4.2 *Ekstranet* VPN

*Ekstranet* VPN merupakan fasilitas VPN yang diperuntukkan bagi pihak-pihak dari luar anggota organisasi atau perusahaan, tetapi masih memiliki hak dan kepentingan untuk dapat mengakses data dalam kantor. Pada umumnya *user* dari VPN dari jenis ini merupakan *customer, vendor, partnet* dan *supplier* dari suatu perusahaan.

#### 2.3.4.3 Model *Remote Access* VPN

VPN merupakan sebuah proses *remote access* yang bertujuan mendapatkan koneksi ke jaringan *private* tujuannya. Proses *remote accsess* VPN tersebut dibedakan menjadi dua jenis berdasarkan oleh siapa proses *remote access* VPN tersebut dilakukan. Kedua jenis tersebut antara lain sebagai berikut.

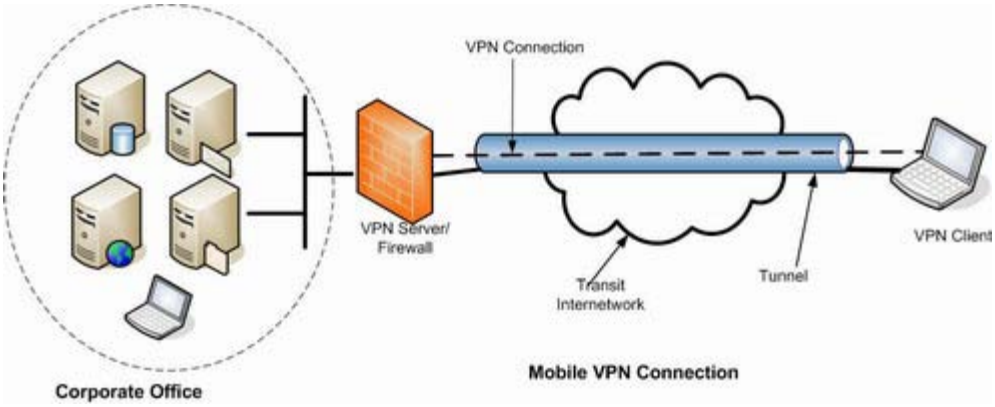
#### 2.3.4.4 *Client-initiated*

Secara harfiah, *client-initiated* merupakan pihak klien yang berinisiatif untuk melakukan sesuatu. Pada VPN jenis ini, ketika sebuah komputer ingin membangun koneksi VPN maka PC tersebutlah yang berusaha membangun *tunnel* dan melakukan proses enkripsi hingga mencapai tujuannya dengan aman. Namun, proses ini tetap mengandalkan jasa dari jaringan *Internet Service Provider* (ISP) yang dapat digunakan untuk umum. *Clien-initiated* digunakan oleh komputer-komputer umum dengan mengandalkan VPN *server* atau VPN *concentrator* pada jaringan tujuannya.

#### 2.3.4.5 *Network Access Server-initiated*

Berbeda dengan *clien-initiated*, VPN jenis *network access server-initiated* ini tidak mengharuskan clien untuk membuat *tunnel* dan melakukan enkripsi dan dekripsi sendiri. VPN jenis ini hanya mengharuskan *user* melakukan *dial-in* ke *network access server* (NAS) dari ISP. Kemudian, NAS tersebut yang membangun *tunnel* menuju ke jaringan *private* yang dituju oleh klien tersebut. Dengan demikian, koneksi VPN dapat dibangun dan dipergunakan oleh banyak klien dari manapun, karena pada umumnya NAS milik ISP tersebut memang dibuka untuk umum.

## 2.4 Teknologi VPN




**Gambar 3.1 Teknologi VPN**

*Virtual Private Network* merupakan perpaduan dari teknologi *tunneling* dengan teknologi enkripsi. Berikut penjelasan menganai kedua teknologi tersebut.

### 2.4.1 Teknologi *Tunneling*

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

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

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

Apabila *tunnel* tersebut telah terbentuk, maka koneksi *point-to-point* palsu tersebut dapat langsung digunakan untuk mengirim dan menerima data. Namun,

di dalam teknologi VPN, *tunnel* tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. *Tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati *tunnel* tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi mana dan bersifat pribadi.

### 2.4.2 Teknologi Enkripsi

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

## 2.5 *Point to Point Tunneling Protocol* (PPTP)

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari *remote client* ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP.

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

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

internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya *public-switched telephone network* (PSTNs) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk *remote users* dan *mobile users* karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

Umumnya terdapat tiga komputer yang diperlukan untuk membangun PPTP, yaitu sebagai berikut.

- Klien PPTP
- *Network access server* (NAS)
- Server PPTP

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

### 2.5.1 Klien PPTP

Komputer yang mendukung PPTP dapat terhubung ke server PPTP dengan dua cara, antara lain sebagai berikut.

- Dengan menggunakan *Network access server* (NAS) milik ISP yang mendukung koneksi PPP.
- Dengan menggunakan *physical* TCP/IP pada LAN sendiri untuk terhubung ke server PPTP.

Klien PPTP yang menggunakan NAS milik ISP harus disetting dengan menggunakan modem dan peralatan VPN untuk membuat koneksi sendiri ke ISP dan server PPTP. Koneksi pertama adalah *dial-up* menggunakan protokol PPP melalui modem ke ISP. Koneksi kedua adalah VPN dengan menggunakan PPTP, melalui modem dan koneksi ISP, ke tunnel melalui koneksi pertama karena *tunnel* antar peralatan VPN telah dibangun dengan menggunakan modem dan koneksi PPP ke internet.

Persyaratan kedua koneksi diatas tidak dapat dilakukan pada saat komputer menggunakan PPTP untuk membuat VPN diantara komputer yang

secara fisik terhubung ke jaringan *private* perusahaan. Pada skenario tersebut, klien PPTP telah siap untuk terhubung ke jaringan dan hanya menggunakan jaringan *dial-up* dengan peralatan VPN untuk membuat koneksi ke server PPTP pada LAN.

Paket PPTP dari klien *remote access* PPTP dan klien lokal LAN PPTP di proses secara berbeda-beda. Paket PPTP dari klien *remote access* PPTP ditempatkan pada media fisik peralatan komunikasi, saat Paket PPTP dari klien LAN PPTP ditempatkan pada media fisik *network adapter* seperti dijelaskan pada gambar di bawah ini.

### 2.5.2 *Network Access Server* (NAS) pada ISP

ISP menggunakan NAS untuk mendukung klien yang *dial in* menggunakan sebuah protokol, seperti SLIP atau PPP, untuk mendapatkan akses ke internet. Bagaimanapun untuk mendukung PPTP yang dapat digunakan klien, NAS harus memiliki fasilitas PPP.

NAS milik ISP didesain dan dibangun untuk mengakomodasi klien *dial in* yang sangat banyak. NAS dibuat oleh perusahaan seperti 3Com, Ascend, ECI telematics, dan U.S. Robotics, yang menjadi anggota dari forum PPTP.

ISP yang memberikan pelayanan PPTP dengan memperbolehkan klien menggunakan NAS untuk PPTP dapat mendukung Windows +95, Windows NT versi 3.5 dan 3.51, sama baiknya seperti pada klien PPP, seperti Apple Macintosh atau UNIX. Klien tersebut dapat menggunakan koneksi PPP ke server ISP. Server ISP bertugas sebagai klien PPTP dan terhubung ke server PPTP pada jaringan *private*, membuat PPTP *tunnel* dari server ISP ke server PPTP.

### 2.5.3 Server PPTP

Server PPTP merupakan server dengan kemampuan *routing* yang terhubung ke jaringan *private* dan internet. Dalam hal ini, server PPTP diartikan sebagai komputer yang menjalankan windows NT server versi 4.0 dan RAS. PPTP di*install* sebagai protokol jaringan. Dengan instalasi tersebut, PPTP disetting dengan menambahkan *virtual device* layaknya VPN ke RAS dan *dial-up networking*.

## 2.6 Arsitektur PPTP

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

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

## 2.7 PPTP *Control Connection*

Protokol PPTP menspesifikasikan seri pengiriman dari *control message* antara PPTP-*enabled client* dan server PPTP. *Control message* membangun, memelihara dan mengakhiri PPTP tunnel. Berikut ini merupakan daftar yang dibuat oleh *control message* dasar yang digunakan untuk membuat dan memelihara PPTP *tunnel.*

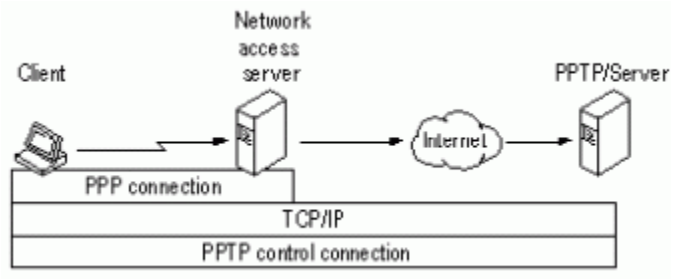
**Tabel 3.1 PPTP Control Message Type**

| Tipe *Message* | Manfaat |
|---|---|
| PPTP_START_SESSION_REQUEST | Permintaan untuk memulai Session |
| PPTP_START_SESSION_REPLY | Untuk menjawab *start session* |
| PPTP_ECHO_REQUEST | *Maintain session* |
| PPTP_ECHO_REPLY | Untuk menjawab *Maintain session* |
| PPTP_WAN_ERROR_NOTIFY | Laporan *error* pada koneksi PPP |
| PPTP_SET_LINK_INFO | Merubah setting koneksi antara klien dan server PPTP |
| PPTP_STOP_SESSION_REQUEST | Mengakhiri *session* |
| PPTP_STOP_SESSION_REPLY | Untuk menjawab *stop session* |

*Control message* ditransmisikan pada paket kontrol pada TCP datagram. Satu koneksi TCP dibangun antara klien PPTP dan server PPTP. Koneksi tersebut digunakan untuk menukar *control message*. *Control messages* dikirim dengan TCP datagram. Datagram terdiri dari PPP *header*, TCP *header*, PPTP *control message* dan *trailer*.


**Gambar 3.2 PPTP TCP Datagram dengan *Control Messages***

Penukaran *message* antara klien PPTP dan server PPTP melalui koneksi TCP digunakan untuk membuat dan memelihara PPTP *tunnel*.




**Gambar 3.3 PPTP *Control Connection* ke server PPTP melalui PPP *Connection* menuju ISP**

Catatan pada ilustrasi di atas, *control connection* merupakan skenario dimana klien *remote access* adalah klien PPTP itu sendiri. Pada skenario tersebut dimana klien *remote access* bukanlah PPTP-*enabled* dan tidak menggunakan PPTP-*enabled* NAS milik ISP, PPTP *control connection* dimulai di server ISP.

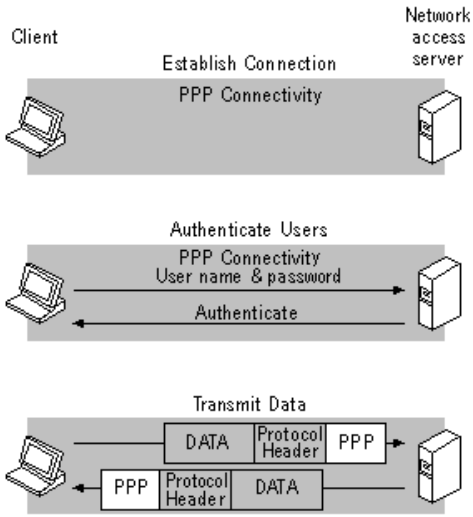
### 2.8 Protokol PPP (*Point to Point Protocol*)

PPP merupakan *remote access protocol* yang digunakan oleh PPTP untuk mengirim *multi-protocol data* melewati TCP/IP. PPP meringkas IP, IPX, dan NetBEUI *packet* antara PPP *frames* dan mengirim ringkasan paket tersebut dengan membuat hubungan *point-to-point* antara komputer pengirim dan penerima.

Umumnya PPTP dimulai saat klien melakukan *dial-up* ke NAS milik ISP. Protokol PPP digunakan untuk membuat koneksi *dial-up* antara klien dan NAS dan memberikan tiga fungsi berikut ini.

- **Memulai dan mengakhiri *physical connection***. Protokol PPP menggunakan urutan yang didefinisikan pada RFC 1661 untuk membangun dan menjaga koneksi antar *remote computers*.
- ***Authenticates users***. Klien PPTP diautentikasi dengan oleh protokol PPP. Menjelaskan text, mengenkripsi, ataupun *Microsoft encryption authentication* dapat digunakan oleh protokol PPP.
- **Membuat PPP datagrams yang terdiri dari enkripsi IPX, NetBEUI, atau TCP/IP packets**. PPP membuat datagrams yang terdiri dari satu atau lebih enkripsi, TCP/IP, IPX, atau NetBEUI data packet. Karena paket tersebut terenkripsi, semua trafik antara klien PPP dan NAS akan aman.

Ilustrasinya sepeti gambar berikut ini.




**Gambar 3.4 Dial-Up Networking PPP Connection ke ISP**

Untuk beberapa situasi, *remote clients* mungkin memiliki akses langsung ke TCP/IP network, seperti internet. Misalnya, sebuah laptop dengan *network card* dapat menggunakan hotspot internet pada ruang rapat. Dengan koneksi IP secara langsung tersebut, inisial koneksi PPP ke ISP tidak diperlukan. Klien tersebut dapat menginisialisasikan koneksi ke server PPTP tanpa membuat koneksi pertama ke ISP.

## 2.9 RADIUS (Remote Access Dial In User Service)

Radius mempunyai 802.1x STANDAR IEEE, yang berguna untuk menghasilkan untuk menghasilkan kontrol akses, Konsep AAA (Autentikasi, authorization, and accounting) dan manajemen kunci untuk *wireless* LANs berbasis UDP Protocol. Tapi kelemahan RADIUS adalah lambat. Tidak ada keamanan jaringan yang benar – benar secure.

Apabila pelanggan konek ke suatu netwotk menggunakan wireless, maka RADIUS akan bekerja dengan metode 3 konsepnya tersebut. Dengan metode Autentikasi, yaitu memastikan apakah pelanggan tersebut benar telah terdaftar pada sebuah jaringan wireless tersebut, autentikasi merupakan keaslian, dapat melihat keaslian pelanggan dengan menggunakan user name dan password. RADIUS menggunakan RAS Secure ID untuk membuat autentikasi yang kuat dalam pengontrolan akses. Terdapat port di RADIUS autentikasi, yaitu port 1812.

Terdapat vendor – vendor hardware dan software yang mengimplementasikan RADIUS sebagai solusi autentikasi user, jadi keaslian dalam suatu network dapat benar – benar terjaga apabila menggunakan RADIUS.

RADIUS juga meng-authorization, yaitu untuk mengetahui hak akses dia sebagai apa, apakah hanya sebagai pelanggan, administrator (yang bekerja untuk meng-insert, update, delete), atau sebagai pimpinan. Ini digunakan agar kemananan jaringan lebih terkontrol karena telah di bagi hak – haknya masing – masing. Konsep lainnya adalah accounting, accounting ini merupakan pendaftaran account, apakah pelanggan ini sah sebagai pelanggan atau tidak. RADIUS accounting menggunakan port 1813 namun ada juga vendor yang menggunakan port 1645/1646 (cisco) dan 1645/1646 (juniper)

2.9.1 Paket Data RADIUS

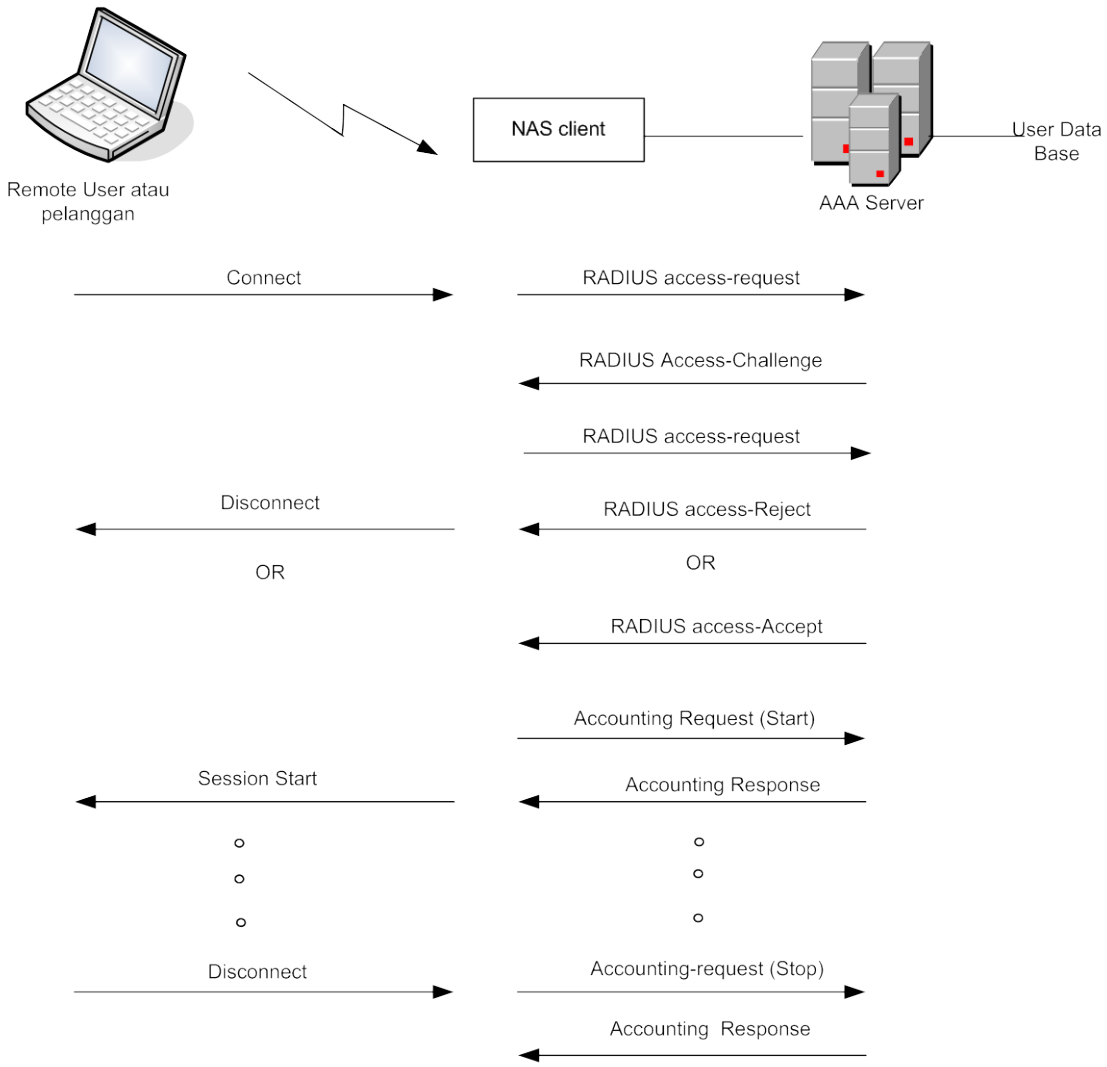
Radius mempunyai struktur paket data. Di sinilah tugas protocol RADIUS, Paket – paket data tersebut di encapsulation. Paket data tersebut terdiri dari 5 bagian dan memiliki pengertian masing – masing. Antara lain :

*1. Code*

Code digunakan untuk membedakan tipe pesan RADIUS yang dikirimkan pada paket. Code memiliki panjang adalah satu octet. Kode-kode tersebut (dalam desimal) ialah:

1 Access-Request
2 Access-Accept
3 Access-Reject
4 Accounting-Request
5 Accounting-Response
11 Access-Challenge
12 Status-Server
13 Status-Client
255 Reserved

Berikut gambar dari penjelasan di atas :




Gambar di atas ini merupakan paket data , terdapat remote user pelanggan yang benar – benar sah untuk mengakses wireless tersebut. Terdapat juga NAS server, NAS Server itu yang biasa disingkat Network-Attached Storage (NAS) device adalah sebuah *sistem penyimpanan* yang mempunyai tujuan khusus yaitu untuk diakses dari jauh melalui *data network.* Dari gambar tesebut terlihat terdapat hubungan antara Remote user (pelanggan) dengan AAA (Autentikasi, authorization, and accounting ) melalui NAS (Network-Attached Storage)

NAS menyediakan jalan yang cocok untuk setiap komputer dalam sebuah LAN untuk saling berbagi pool penyimpanan dengan kemudahan yang sama

seperti menamai dan menikmati akses seperti HAS lokal. Tetapi kelemahan dari NAS ini adalah umumnya cenderung untuk lebih tidak efisien dan memiliki peforma yang lebih buruk dari penyimpanan *direct-attached.* SCSI adalah protokol NAS terbaru. Protokol ini menggunakan protokol IP *network* untuk membawa protokol SCSI. *Host* dapat memperlakukan penyimpanannya seperti *direct-attached*, tapi *storage*-nya sendiri dapat berada jauh dari *host*.

Ketika Terkoneksiterdapat kode – kode yang di gunakan untuk membedakan tipe pesan RADIUS, misal paket data yang di kirimkan oleh kode RADIUS access-requst menuju ke AAA Server, di AAA Server tersebut terdapat user database, pengertian dari database itu sendiri adalah sekumpulan data-data atau file yang saling berhubungan satu sama lain dalam satu media penyimpanan, dimana pemakai dapat mengakses dan memanipulasi data. Data base yang terdapat pada AAA Server merupakan data base yang terdistribusi. Jadi di dalam database AAA Server tersebut berisi Autentikasi yang bisa berupa user name dan password atau authorization yang berisi hak akses pelanggan untuk menggunakan network tersebut dan membatasi kekuasaan, sedangkan accounting berisikan account – account pelanggan yang menggunakan network tersebut. Dari paket data yang berisikan kode – kode tersebut di AAA Server akan di kembalikan lagi ke NAS Client yang mempunyai tujuan khusus yang dapat di akses dari jauh melalui data network.

2. Identifier

Identifier juga berguna untuk mengidentifikasikan dan untuk mencocokkan permintaan, apabila permintaan itu cocok maka akan terjadi RADIUS access Request. Identifier memiliki panjang satu oktet.

3. Length

Memiliki panjang dua oktet, memberikan informasi mengenai panjang paket.

4. Authenticator

Memiliki panjang 16 oktet, digunakan untuk membuktikan balasan dari

RADIUS server, selain itu digunakan juga untuk algoritma password.

5. Attributes

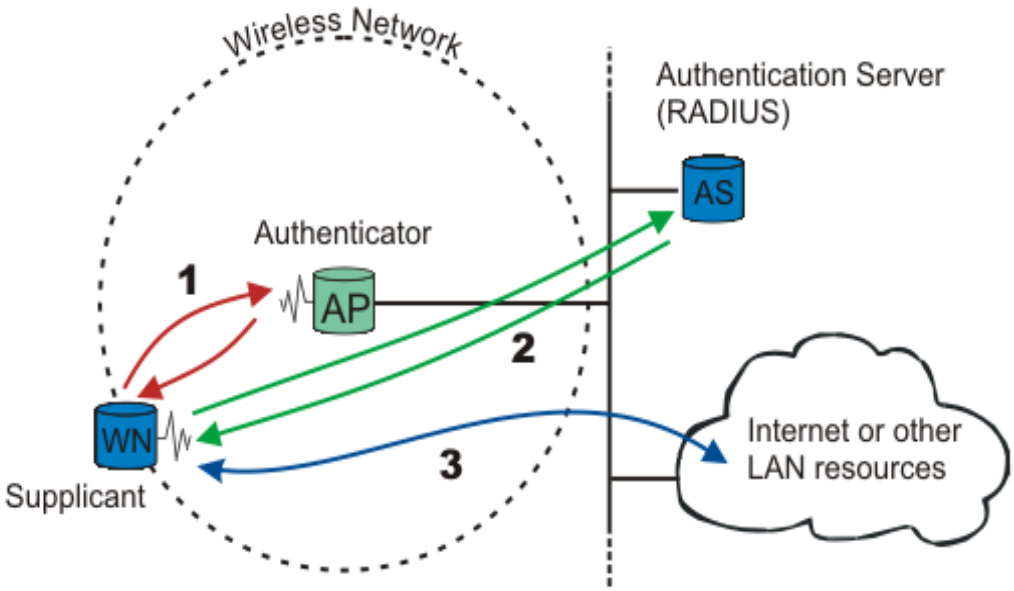
Berisikan informasi yang dibawa pesan RADIUS, setiap pesan dapat membawa satu atau lebih atribut. Contoh atribut RADIUS: nama pengguna, password, CHAP-password, alamat IP access point(AP), pesan balasan. Tujuan standar 802.1x IEEE adalah untuk menghasilkan kontrol akses, autentikasi, dan manajemen kunci untuk wireless LANs. Standar ini berdasarkan pada Internet Engineering Task Force (IETF) Extensible Authentication Protocol (EAP), yang ditetapkan dalam RFC 2284. Standar 802.1x IEEE juga mendukung beberapa metode autentikasi, seperti smart cards, password yang hanya bisa digunakan oleh satu pengguna pada satu waktu, dan yang lebih baik lagi adalah biometrics.

### 2.9.2 **Tujuan standar 802.1x IEEE**

Tujuan standar 8021x IEEE adalah untuk menghasilkan kontrol akses, autentikasi, dan manajemen kunci untuk wireless LANs. Standar ini berdasarkan pada *Internet Engineering Task Force* (IETF) *Extensible Authentication Protocol* (EAP), yang ditetapkan dalam RFC 2284. Standar 802.1x IEEE juga mendukung beberapa metode autentikasi, seperti *smart cards*, *password* yang hanya bisa digunakan oleh satu pengguna pada satu waktu, dan yang lebih baik lagi adalah *biometrics*.

802.1x terdiri dari tiga bagian, yaitu wireless node *(*supplicant), access point (autentikator), autentikasi server. Autentikasi server yang digunakan adalah *Remote Authentication Dial-In Service* (RADIUS) server dan digunakan untuk autentikasi pengguna yang akan mengakses *wireless* LAN. EAP adalah protokol layer 2 yang menggantikan PAP dan CHAP.

**Mekanisme Autentikasi menggunakan RADIUS server**




Penjelasan :

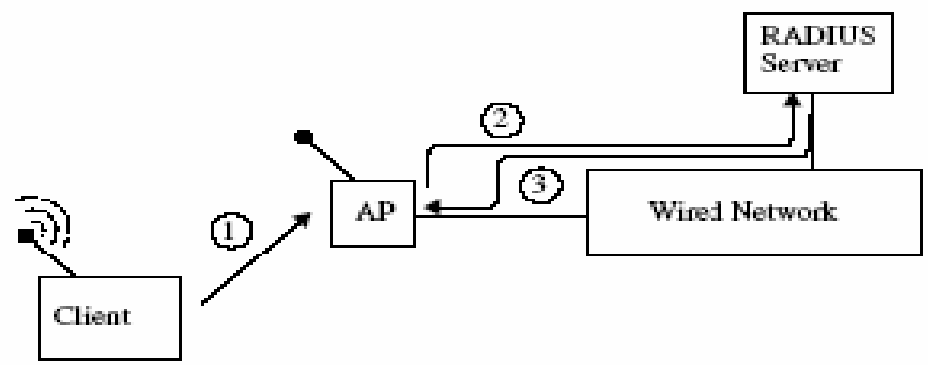
1. Wireless Node (WN) / Supplicant akan meminta akses ke wireless network Akses Point atau disebut dengan AP akan menanyakan identitas Supplicant. Tidak ada trafik data selain EAP yang di perbolehkan sebelum Supplicant terautentikasi. Access Point bukanlah sebuah autentikator, tetapi akses point berisi autentikator
2. Setelah nama-pengguna dan password di kirim, proses autentikasi dimulai. Protokokol yang di gunakan antara Supplicant dan Autentikator adalah EAP. Protocol over LAN (EAPoL) Autentikator mengencapsulasi kembali pesan EAP ke dalam format RADIUS, dan mengirimnya ke RADIUS server. Selama proses autentikasi, autentikator hanya menyampaikan paket antara Supplicant dan RADIUS server. Setelah proses autentikasi selesai, RADIUS server mengirimkan pesan sukses ( atau gagal, apabila proses autentikasi gagal)
3. Apabila proses autentikasi sukses, *Supplicant* diperbolehkan untuk mengakses *wireless* LAN dan/atau internet.

### 2.9.3 Pemfilteran alamat MAC

MAC address merupakan alamat setiap computer. Setiap computer (PC), server, laptop pasti mempunyai NIC, NIC itu berupa hardware. Di dalam NIC itu terdapat nomor MAC. Pengguna *wireless* LAN dapat difilter berdasarkan alamat MAC *wireless card* yang dimiliki pengguna.Hampir semua *access point* telah mempunyai fiturpemfilter alamat MAC.

Administrator jaringan dapat memprogram *access point*, program ini yang berisi daftar alamat-alamat MAC yang dapat mengakses *access point* tersebut. Memprogram *access point* untuk memasukkan alamat-alamat MAC akan sangat merepotkan, terutama apabila jumlah alamat MAC yang ingin terhubung ke *access point* sangat banyak. Pemfilteran alamat MAC dapat diimplementasikan pada RADIUS server, alamat MAC beserta identitas pengguna dimasukkan ke dalam RADIUS server. Hal ini tentu akan mempermudah administrator untuk mengelola *wireless* LAN.

**Pemfilteran alamat MAC dengan menggunakan RADIUS Server**




Berikut ini penjelasan dari mengenai pemfilteran alamat MAC dengan RADIUS server:

1. *Client* (*Wireless Node*) meminta akses ke *Access Point* (AP).
2. AP meneruskan permintaan *client* ke RADIUS Server, di RADIUS Serveralamat MAC *client* diperiksa apakah ada di *database*.

3. RADIUS memberikan tanggapan ke AP, apabila autentikasi di RADIUS Server berhasil maka *client* diperbolehkan untuk mengakses AP, dan apabila gagal maka *client* tidak diijinkan untuk mengakses AP tersebut.

Autentikasi menggunakan RADIUS Server yang dibarengi dengan pemfilteran alamat MAC diharapkan dapat menambah keamanan wireless LAN dari orang orang yang tidak mempunyai hak akses ke *wireless* LAN. Sistem ini cocok di terapkan disuatu instansi, baik itu swasta maupun pemerintahan. Karena alamat MAC yang dapat mengakses wireless LAN dibatasi, maka sistem ini kurang cocok apabila diterapkan pada hotspot yang terpasang di tempat-tempat umum, seperti kafe, mal, bandara. Alasan orang menggunakan *hotspot* yang berada di tempat-tempat umum adalah karena kemudahan yang ditawarkan oleh teknologi *wireless*. Apabila sistem ini diterapkan pada *hotspot* yang terdapat di tempattempat umum, ada kemungkinan para pelanggan yang menggunakan *hotspot* tidak tertarik lagi karena merasa repot.

### 2.9.4 Keamanan RADIUS Server

Protokol RADIUS yang digunakan sebagai salah satu sistem keamanan wireless LAN melalui autentikasi pengguna wireless LAN, ternyata memiliki beberapa lubang keamanan.

Mekanisme proteksi menggunakan nama pengguna dan password ternyata tidak cukup aman untuk diterapkan. Hal ini diperparah dengan penerapan teknik enkripsi dan kriptografi yang tidak benar. Paket access-request yang tidak diautentikasi oleh RADIUS server. Metode shared secret sudah sangat berisiko apabila diterapkan untuk proses autentikasi dari client ke RADIUS server.

Beberapa lubang keamanan protokol RADIUS:

• MD5 dan shared secret

Seperti yang sudah disebutkan diatas bahwa metode shared secret sudah sangat berisiko untuk diterapkan, hal ini dikarenakan lemahnya MD5 hash yang menyimpan tanggapan autentikator. Hacker / penyusup dapat dengan mudah mengetahui paket access-request beserta tanggapannya. Penyusup dapat dengan mudah mengetahui shared secret dengan cara melakukan penghitungan awal terhadap perhitungan MD5.

• Paket access-request

Tidak adanya autentikasi dan verifikasi terhadap paket access-request merupakan salah satu kelemahan dari protokol RADIUS. Paket access-request harus berisi atribut alamat IP access point (AP), nama pengguna beserta password atau CHAP-password, port yang digunakan oleh access point [6]. Nama pengguna beserta password disembunyikan dengan memakai metode RSA Message Digest Algorithm MD5. RADIUS server akan memeriksa dan memastikan bahwa pesan yang dikirim oleh alamat IP adalah salah satu dari client yang terdaftar. Penyusup dapat mengetahui dan menggunakan alamat IP yang menjadi client dari RADIUS server ini. Hal ini merupakan salah satu keterbatasan dari rancangan protokol RADIUS.

• Pemecahan password

Skema proteksi password yang dipakai adalah stream-chiper, dimana MD5 digunakan sebagai sebuah ad hoc pseudorandom number generator (PRNG). 16 oktet pertama bertindak sebagai sebuah synchronous stream chiper. Yang menjadi masalah adalah keamanan dari cipher ini masih menjadi suatu pertanyaan, protokol RADIUS tidak dengan jelas menyebutkan apa yang menjadi kebutuhan dari cipher tersebut. MD5 hash secara umum digunakan untuk crypthographic hash, bukan stream chiper. Ada kemungkinan masalah keamanan yang ditimbulkan dari penggunaan MD5 hash tersebut.

Seperti yang telah dijelaskan diatas bahwa atribut password diamankan dengan metode stream chiper. Hal ini memungkinkan penyusup mendapatkan informasi shared secret apabila mereka melakukan sniffing ke jaringan wireless dan mencoba masuk ke RADIUS server

• Serangan menggunakan Request Authenticator

Keamanan RADIUS bergantung pada pembangkitan Request Authenticator. Request Authenticator ini harus unik dan tidak dapat diprediksi untuk menjamin keamanan. Protokol RADIUS tidak menekankan pada pentingnya Pembangkitan Request Authenticator, sehingga banyak implementasi yang menggunakan PRNG yang jelek untuk membangkitkan Request Authenticator. Apabila client menggunakan PRNG yang mempunyai short circle, maka protokol tidak menyediakan proteksi.