

BAB II

LANDASAN TEORI

2.1. Tinjauan Jurnal

Dalam penulisan skripsi ini penulis menggunakan beberapa research diantaranya jurnal, adapun kutipan jurnal yang penulis gunakan sebagai berikut,

Menurut Supriyono dkk (2013:88-101) PT. Mega Tirta Alami menggunakan email untuk mengirimkan data penting perusahaan termasuk data keuangan. Dengan menggunakan *email*, data yang ditransmisikan melalui jaringan komunikasi publik rentan terhadap berbagai ancaman keamanan. Masalah ini bisa diselesaikan dengan menggunakan *Virtual Private Network* (VPN), sebagai saluran transmisi data. Jurnal ini membahas desain dan implementasi VPN untuk PT Mega Tirta alami yang menghubungkan kantor pusat untuk dua cabang kantor, yaitu cabang 1 di Bandung dan cabang 2 di Bekasi. VPN diimplementasikan dengan titik ke titik protokol *tunneling* (PPTP) dengan menggunakan tiga *router* mikrotik. Hanya beberapa perubahan dalam konfigurasi jaringan komputer untuk meminimalkan kedua biaya, pelaksanaan dan waktu. Sebelum membuat komunikasi data ke kepala kantor, pengguna di cabang 1 atau cabang 2 harus memberikan *username* dan *password* sebagai bagian dari verifikasi dan proses validasi. VPN baru dikembangkan diuji pada berbagai aspek teknis untuk memastikan kehandalan dan pengoperasian. Hasil tes menunjukkan bahwa VPN terhubung antara kantor pusat untuk cabang 1 dan dari kantor pusat ke cabang 2. Untuk menjaga keamanan, hubungan langsung antara cabang 1 dan cabang 2 melalui VPN.

Menurut Riadi (2011:71-80) pengguna jaringan komputer harus mengeluarkan investasi yang tidak sedikit untuk mengakses *internet*. *Internet* telah memberikan pengaruh yang sangat besar pada penyebaran informasi, sehingga semakin banyak orang yang mengakses data melalui *internet*. Permasalahan tersebut dapat diatasi menggunakan mikrotik sebagai pengatur lalu lintas data internet serta melakukan pemfilteran beberapa aplikasi yang dapat mengganggu konektifitas jaringan komputer sesuai dengan aturan yang telah ditetapkan. Penelitian ini dilakukan menggunakan beberapa tahapan antara lain : analisis proses untuk menentukan alur lalu lintas yang melewati proses pemfilteran menggunakan *firewall*, desain untuk mendapatkan cara yang paling efektif dan efisien mengimplementasikan *router*, implementasi serta pengujian yang dilakukan dengan metode *stress test*. Berdasarkan penelitian yang telah dilakukan aplikasi *router* menggunakan mikrotik yang di hasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna.

2.2. Konsep Dasar Jaringan

2.2.1. Jaringan Komputer

Menurut Arul (2010:28) jaringan komputer adalah suatu kumpulan atau beberapa komputer yang dihubungkan sehingga dapat berkomunikasi, termasuk juga *printer* dan peralatan lainnya yang saling terhubung. Data atau informasi ditransfer melalui kabel maupun *wireless* sehingga orang yang menggunakan komputer dapat saling bertukar dokumen dan data, mencetak pada *printer* yang sama dan bersama-sama menggunakan *hardware* atau *software* yang terhubung dengan jaringan.

Menurut Sopandi (2008:2), jaringan komputer merupakan gabungan antara teknologi komputer dan teknologi telekomunikasi atau suatu himpunan interkoneksi sejumlah komputer *autonomous*. Gabungan teknologi ini melahirkan pengolahan data yang data didistribusikan, mencakup pemakaian *database*, *software* aplikasi dan peralatan *hardware* secara bersamaan, sehingga penggunaan komputer yang sebelumnya berdiri sendiri, kini telah diganti dengan sekumpulan komputer yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya, sistem seperti inilah yang disebut jaringan komputer. Dalam bahasa populer dapat di jelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer yang saling berhubungan satu sama lain melalui media perantara.

Jaringan komputer merupakan suatu PC (*Personal Computer*) untuk melakukan komunikasi dengan PC yang lain dengan menggunakan media transmisi sebagai jalur komunikasi.

Media perantara ini bisa berupa kabel atau tanpa kabel (*nirkabel*). Informasi berupa data dapat mengalir dari satu komputer ke komputer lainnya atau dari satu perangkat ke perangkat yang lainnya sehingga masing-masing komputer terhubung tersebut bisa saling bertukar data.

2.2.2. Jenis-jenis Jaringan Komputer

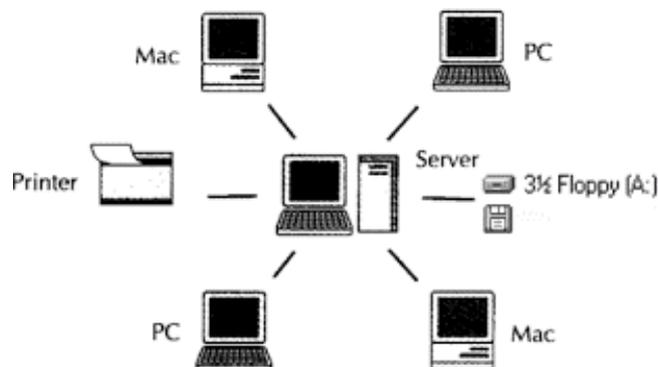
Yudianto (2007:10) mengatakan bahwa pada dasarnya, jaringan komputer merupakan suatu bentuk interkoneksi atau hubungan antar komputer, yang pada dasarnya memiliki beberapa jenis.

1. LAN (*Local Area Network*)

Menurut Sopandi (2008:2) LAN merupakan jaringan yang bersifat internal dan biasanya milik pribadi di dalam sebuah perusahaan kecil atau menengah dan biasanya berukuran sampai beberapa kilometer.

LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam suatu perusahaan atau pabrik-pabrik untuk pemakaian sumber daya (*resource*) bersama baik *hardware* maupun *software* serta sarana untuk saling bertukar informasi. Ada beberapa ciri LAN, yaitu :

- a. Jarak antar terminal tidak terlalu jauh
- b. Pada umumnya LAN tersebut milik satu organisasi atau perusahaan
- c. Umumnya tidak menggunakan fasilitas jaringan telepon, sehingga pengiriman data juga tidak bergantung pada jaringan tersebut
- d. Menggunakan media transmisi berupa kabel khusus untuk komunikasi



Sumber : Yani (2008:7)

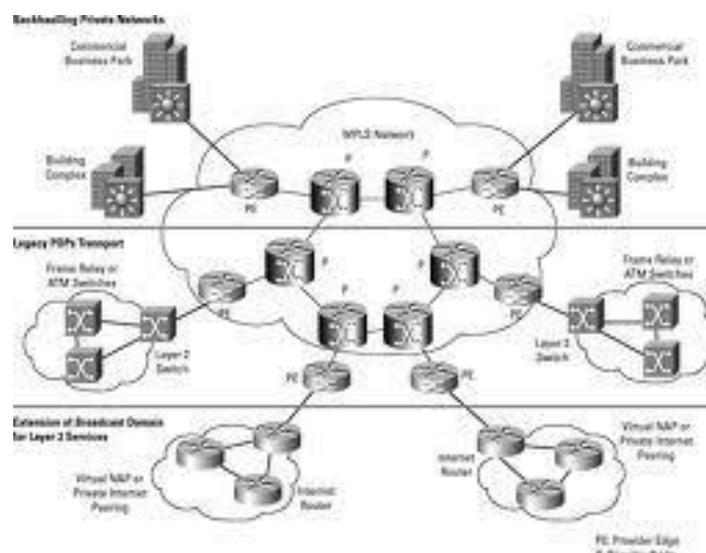
Gambar II.1 Contoh Tampilan Jaringan LAN

Seperti contoh gambar II.1 dengan menggunakan model jaringan LAN, maka seluruh komputer dan *printer* dalam satu ruangan tersebut dapat terkoneksi satu sama lain dengan komputer yang di tengah digunakan menjadi *server* yang mengatur semua sistem di dalam jaringan tersebut.

2. MAN (*Metropolitan Area Network*)

Menurut Ardiyansah (2009:2) MAN dapat mencangkup 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.

MAN dapat dikatakan pengembangan dari LAN namun relatif lebih besar skala jangkauannya bila dibandingkan dengan LAN, misalnya antar wilayah dalam satu provinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yang lebih besar.



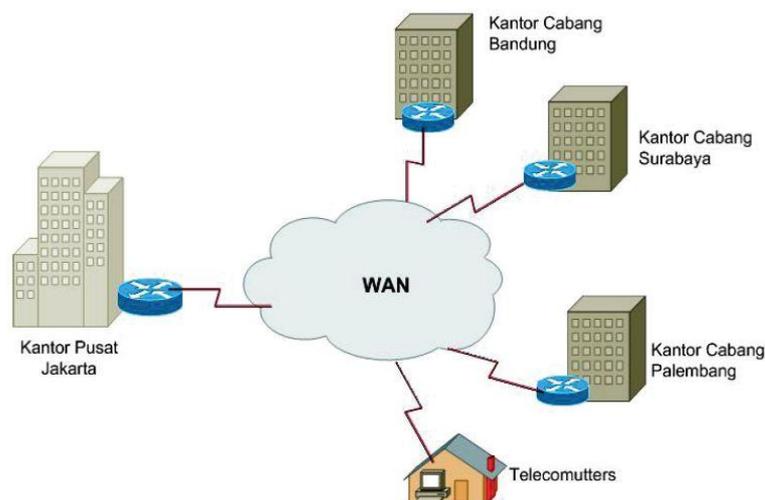
Sumber : Yani (2008:10)

Gambar II.2 Contoh Tampilan Jaringan MAN

Seperti contoh gambar II.2 jaringan komputer MAN ini lebih efisien untuk cakupan yang lebih luas, dengan menggunakan tipe jaringan MAN ini para user akan lebih mudah mengakses data dari user lainnya meski lokasi mereka tidaklah dekat. Walaupun berbeda gedung tetapi dalam satu provinsi dengan menggunakan jaringan MAN maka masih terkoneksi untuk mengakses data perusahaan.

3. WAN (*Wide Area Network*)

Menurut Ardiyansah (2007:3) WAN adalah kumpulan LAN atau *workgroup* yang dihubungkan dengan menggunakan alat komunikasi modern dan jaringan internet dari kantor pusat ke kantor cabang atau pun sebaliknya, maupun antar kantor cabang. Dengan sistem ini, pertukaran data antar kantor dapat dilakukan cepat serta dengan biaya yang relatif lebih murah. Sistem jaringan ini dapat menggunakan jaringan internet yang sudah ada, untung menghubungkan kantor pusat dan kantor cabang atau dengan *PC Stand Alone/Notebook* yang berada di lain kota atau negara.



Sumber : Yani (2008:17)

Gambar II.3 Contoh Tampilan Jaringan WAN

Seperti contoh gambar II.3 walaupun antara kantor pusat dan beberapa kantor cabang berbeda provinsi tetapi tetap bisa terkoneksi dengan kantor pusat

yang menggunakan jaringan WAN. Jaringan WAN ini mencakup area yang lebih luas lagi dibanding jaringan LAN dan MAN.

Diantara jaringan LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda antara satu dengan yang lainnya. LAN mencakup area yang lebih kecil MAN mencakup area yang sedang dan WAN mencakup area yang lebih besar atau luas.

2.2.3. Internet VPN

Menurut Athailah (2013:104) VPN (*Virtual Private Network*) suatu cara untuk membuat sebuah jaringan *private* (pribadi) secara aman dengan menggunakan jaringan publik, VPN dapat melewati jaringan publik seakan akan terhubung secara *point to point*, yang berisi informasi *routing* untuk mendapatkan koneksi *point to point* sehingga dapat melalui jaringan publik sampai ke tujuan.

Sedangkan untuk mendapatkan hubungan yang bersifat *private*, data yang dikirim harus di enkripsi terlebih dahulu untuk menjaga kerahasiannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi, proses enkapsulasi data ini disebut dengan *tunneling*.

VPN merupakan salah satu cara untuk membuat sebuah jaringan bersifat *private* dan aman dengan memanfaatkan jaringan publik seperti *internet*. Data dalam jaringan tersebut tidak dapat diketahui oleh pengguna lain di jaringan publik karena data tersebut dilewatkan pada *tunnel* yang dibentuk oleh VPN.

Menurut Setiawan dan Rini (2009:57) VPN salah satu solusi yang bisa digunakan untuk interkoneksi jaringan pada skala luas WAN, saat ini banyak para

provider menawarkan solusi VPN sebagai komunikasi data perusahaan bisnis untuk interkoneksi ke kantor-kantor cabangnya.

Secara umum VPN dikelompokkan menjadi dua, yaitu :

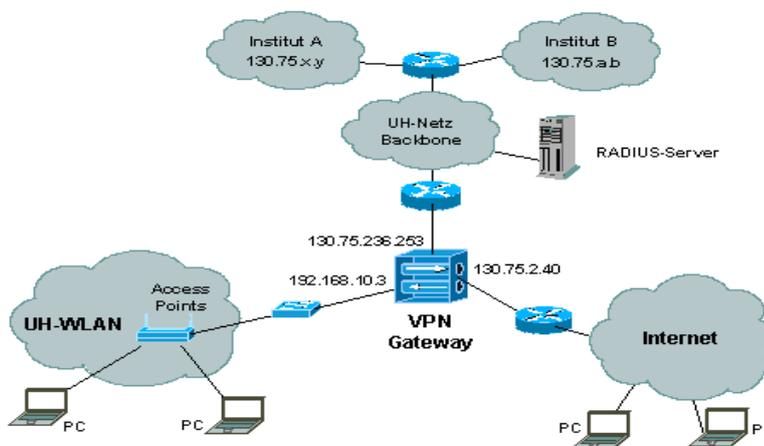
1. *Remote Access* VPN

Remote Access VPN disebut juga *Virtual Private Dial-up Network* (VPDN).

VPDN adalah jenis *user-to-LAN connection*. Artinya, *user* dapat melakukan koneksi ke *private network* dari manapun, apabila diperlukan biasanya VPDN digunakan oleh karyawan yang bekerja di luar kantor. Mereka dapat memanfaatkan komputer yang sudah dilengkapi perangkat tertentu untuk melakukan koneksi dengan jaringan LAN di kantor.

2. *Site-to-site* VPN

Site-to-site VPN diimplementasikan dengan memanfaatkan perangkat *dedicated* yang dihubungkan via *internet* *Site-to-site* VPN digunakan untuk menghubungkan berbagai area yang sudah *fixed* atau tetap, misal kantor cabang dengan kantor pusat.



Sumber : Winarno (2013:20)

Gambar II.4 Contoh Tampilan Jaringan VPN.

Seperti contoh gambar II.4 fitur dan fungsi *Virtual Private Network* adalah sebuah sistem yang memungkinkan komputer jaringan luas secara geografis tanpa ada hambatan fisik. VPN dikategorikan sebagai bentuk jaringan dalam cakupan area luas. Karena kebutuhan untuk memberikan akses khusus atau membuat akses khusus untuk karyawan yang harus *mobile* oleh karena VPN adalah jaringan intra global aktif sehingga karyawan dari manapun dapat terhubung ke jaringan *internet* dan *intranet* perusahaan.

2.2.4. Teknologi Tunneling

Menurut Derianto (2006:18) 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 tersebut 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.

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* 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 aman dan bersifat pribadi.

Tunnel merupakan suatu mekanisme enkripsi-deskripsi data. Data yang dikirim melalui jalur publik adalah data terenkripsi yang hanya bisa dibuka oleh ujung dari *tunnel* yang memiliki kunci untuk mendeskripsi data tersebut. Dengan adanya mekanisme *tunneling* VPN dapat dimanfaatkan pada beberapa kondisi, yaitu :

1. *Remote Access Client Connection*, VPN berfungsi untuk mendukung *remote* dari komputer rumah ke komputer atau sebaliknya dengan memanfaatkan jaringan *internet*.
2. LAN to LAN *internet working* dengan memanfaatkan VPN, 2 jaringan atau lebih yang terpisah letak dapat digabungkan menjadi seperti dalam satu jaringan, dengan syarat semua jaringan tersebut tersambung ke jaringan *internet*.
3. Kontrol akses dalam suatu internet VPN dapat dimanfaatkan untuk mengamankan penggunaan suatu jaringan *intranet*, dengan tujuan agar data yang dikirimkan pengguna tersebut tidak diketahui pengguna lain pada jaringan yang sama.

2.2.5. Protokol

Menurut Derianto (2006:15) protokol merupakan kumpulan dari beberapa aturan yang berhubungan dengan komunikasi data antara beberapa alat komunikasi supaya komunikasi data dapat dilakukan dengan benar.

1. *Point to Point Protocol* (PTPP)

Menurut Towidjojo (2013:198) koneksi *point to point* (titik ke titik) dapat digunakan untuk menghubungkan secara langsung satu perangkat dengan perangkat lainnya. Umumnya digunakan untuk menghubungkan jaringan lokal ke internet *service provider*. Tujuan untuk membuat hubungan langsung atau *face to face* antara *provider* dengan klien adalah untuk memudahkan manajemen jaringan dan memisahkan satu klien dengan klien lainnya. Untuk membuat topologi *point to point* ini digunakanlah *Point to Point Protocol*



Sumber : Winarno (2013:25)

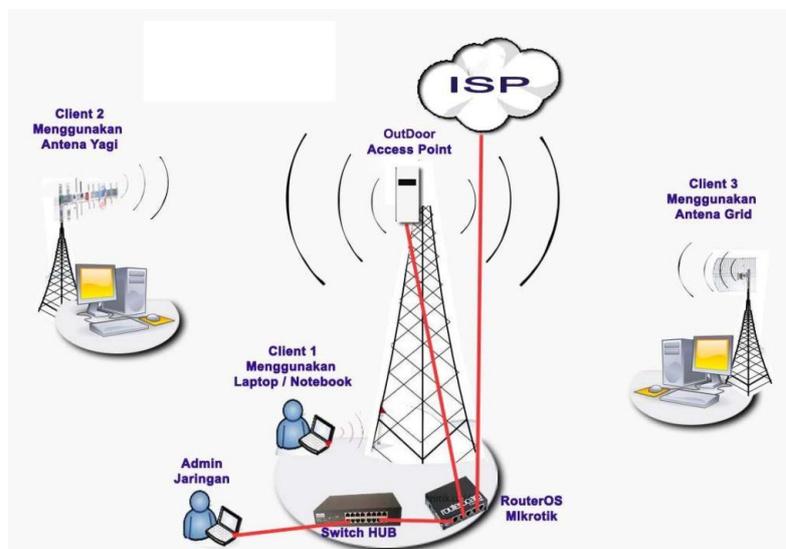
Gambar II.5 Contoh Tampilan Jaringan PTPP

Seperti contoh gambar II.5 sebuah proses pengiriman paket data ke komputer pada jaringan *private* dengan *me-routing* paket data tersebut melalui jaringan LAN. *Router* jaringan yang lain tidak bisa mengakses komputer yang berada pada jaringan *private*. Oleh karena itu, *tunneling* memungkinkan jaringan *routing* untuk mentransmisikan paket data ke jaringan penghubung, seperti PTPP *server*, yang terhubung ke jaringan *routing* dan jaringan *private*. PTPP *client* dan PTPP *server* menggunakan *tunneling* untuk merutekan paket data secara aman ke

komputer yang berada pada jaringan *private* melalui jaringan LAN yang hanya mengetahui alamat *server* penghubung jaringan *private*.

2. *Point To Point Protocol Over Ethernet* (PPPoE)

Menurut Towidjojo (2010:187) PPPoE adalah pengembangan dari PPP. Perbedaan keduanya terletak pada media dimana protocol ini diimplementasikan. Jika PPP digunakan pada jaringan yang menggunakan serial maupun GSM modem, maka PPPoE digunakan untuk membuat topologi *point to point* pada jaringan *Ethernet*.



Sumber : Winarno (2013:28)

Gambar II .6 Contoh Tampilan Jaringan PPPoE

Seperti contoh gambar II.6 Dengan menggunakan PPPoE, pengguna hampir dapat "memanggil" dari satu komputer ke komputer lain melalui jaringan *Ethernet*, membentuk titik ke titik koneksi antara mereka dan kemudian aman transportasi paket data melalui koneksi tersebut.

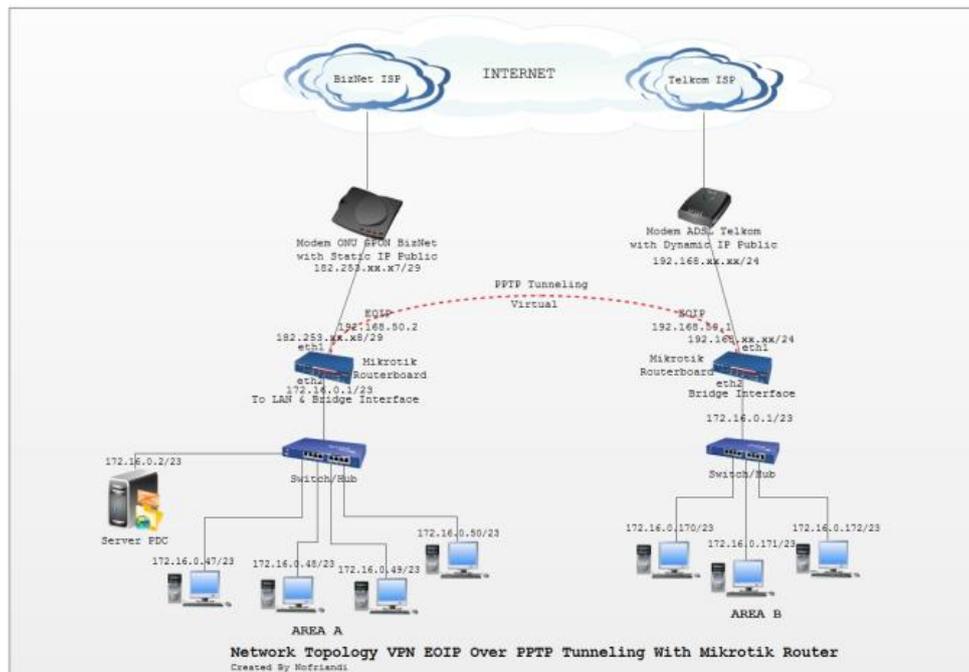
3. PPTP

Menurut Snader (2010:187) PPTP adalah protokol jaringan yang memungkinkan pengamanan transfer data dari *remote client* (*client* yang berada jauh dari *server*) ke *server* pribadi perusahaan dengan menggunakan sebuah VPN melalui TCP/IP.

PPTP adalah salah satu protokol yang digunakan untuk membangun VPN. VPN akan menawarkan tingkat *encryption* yang lebih baik selain menawarkan fitur *authentication*. Inilah yang membuat VPN menjadi pilihan wajib jika anda menuntut level yang lebih baik pada saat akan membuat *tunnel*.

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari *remote client* (*client* yang berada jauh dari *server*) ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Snader, 2008:189).

Protokol ini dikembangkan oleh *Microsoft* dan *Cisco*. Teknologi jaringan PPTP merupakan pengembangan dari *Remote Access Point-to-Point Protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF).



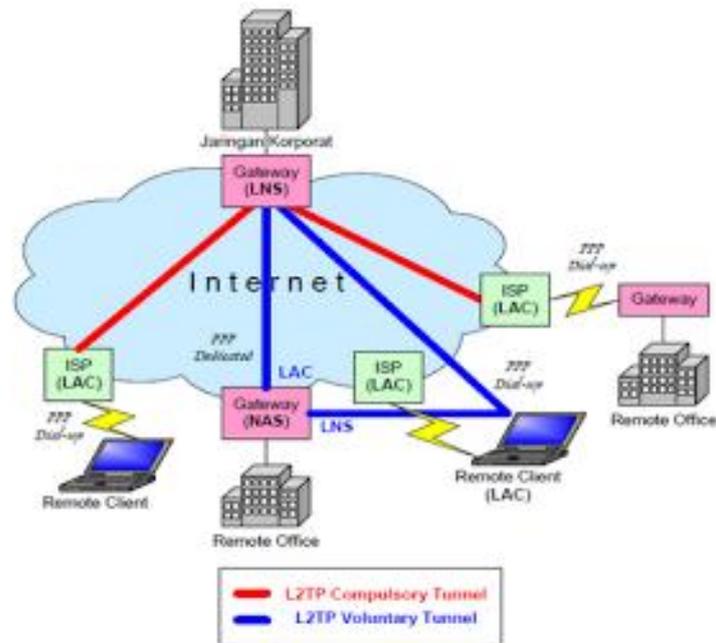
Sumber : Winarno (2013:30)

Gambar II.7 Contoh Tampilan Jaringan PPTP

Seperti contoh gambar II.7 *router* area A dan *router* area B terhubung oleh 2 modem yang berbeda dan masing-masing akan terhubung dengan komputer di areanya masing-masing tetapi masih kedua area tersebut masih bisa terhubung dan diakses dengan PPTP *tunneling*.

4. *Layer 2 Tunneling Protocol (L2TP)*

Menurut Ramdhani dan Sularsa (2010:3) L2TP adalah sebuah *tunneling* protokol yang memadukan dan mengkombinasikan dua buah *tunneling* protokol yang bersifat *proprietary*, yaitu L2F (*Layer to Forwarding*) memiliki *cisco system* dengan PPTP milik *Microsoft*.



Sumber : Winarno (2013:33)

Gambar II.8 Contoh Tampilan Jaringan L2TP

Seperti contoh gambar II.8 terdapat dua model tunnel L2TP yang dikenal, yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint tunnel* nya. Pada *compulsory tunnel*, ujung *tunnel* berada pada ISP. Sedangkan pada *voluntary*, ujung *tunnel* berada pada *client remote*.

2.3. Peralatan Pendukung

Dalam membentuk sebuah jaringan, maka membutuhkan peralatan berupa:

1. *Network Interface Card* (NIC)

Menurut Sopandi (2010:16) *Network Interface Card* (NIC) adalah *card* penghubung PC dengan jaringan, sehingga memungkinkan komputer untuk terkoneksi ke jaringan computer. Bentuk yang paling umum dari NIC adalah *ethernet* metode yang sangat cepat dalam mentransfer data antar komputer. NIC memungkinkan sebuah computer untuk memberi dan mengambil informasi dari komputer lain yang ada di jaringan yang sama dapat berupa internet atau LAN (*Local Area Network*). Pada gambar II.9 merupakan salah satu contoh alat NIC.



Sumber : Yani (2008:9)

Gambar II.9 Network Interface Card (NIC)

2. Switch

Menurut Sopandi (2010:19) switch adalah alat yang digunakan untuk menghubungkan beberapa LAN yang terpisah serta menyediakan *filter* paket antar LAN. Switch adalah peralatan *multi port*, masing-masing dapat mendukung satu *workstation*, Jaringan *ethernet* atau jaringan *token ring*. Meskipun terhubung dengan jaringan yang berbeda pada masing-masing *port*, *switch* dapat memindahkan paket data antar jaringan apabila diperlukan. Dalam hal ini *switch* berlaku seperti *bridge multi port* yang sangat cepat (paket data di *filter* oleh *switch* dengan alamat yang dituju). Pada gambar II.10 merupakan salah satu contoh alat Switch.



Sumber : Yani (2008:36)

Gambar II.10 Switch

3. Router

Menurut Sopandi (2010:19) *router* adalah perangkat jaringan yang digunakan untuk menghubungkan beberapa jaringan, baik jaringan yang sama maupun berbeda dari segi teknologinya seperti menghubungkan jaringan yang menggunakan topologi *bus*, *star* dan *ring*. Pada gambar II.11 merupakan salah satu contoh alat Router.

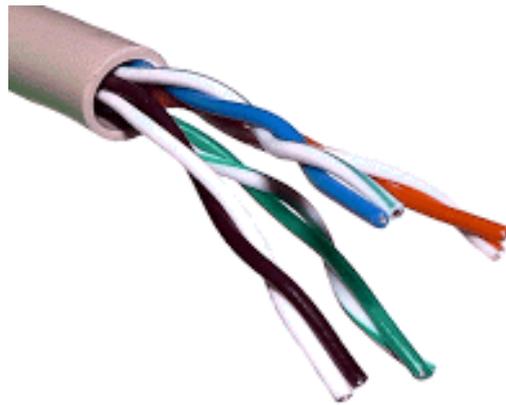


Sumber : Yani (2008:37)

Gambar II.11 Router

4. Kabel UTP

Menurut Sopandi (2010:21) kabel UTP adalah kabel sebagai media transmisi dalam jaringan LAN. Kabel UTP ini termasuk kabel yang tidak memiliki pelindung dan memiliki rangkaian kabel yang saling terpilin satu dengan lainnya. Keberadaan kabel UTP ini membuat antar jaringan komputer dapat terhubung melalui LAN. Pada gambar II.12 merupakan salah satu contoh kabel UTP.



Sumber : Yani (2008:39)

Gambar II.12 Kabel UTP

2.3.1. Topologi Jaringan

Menurut Linto (2010:30) *topologi* atau arsitektur jaringan merupakan pola hubungan antar terminal dalam suatu sistem jaringan komputer. *Topologi* ini akan memengaruhi tingkat efektifitas kinerja jaringan. Ada beberapa jenis topologi yang dapat diimplementasikan dalam jaringan. Namun, bentuk topologi yang utama adalah topologi *bus*, topologi *ring*, dan topologi *star*.

Topologi digunakan sebagai salah satu cara untuk membentuk model jaringan komputer yang digunakan, semua itu ditinjau dari perangkat *hardware*, kabel serta jarak pada model jaringan yang digunakan. Jenis topologi dibagi dua, yaitu :

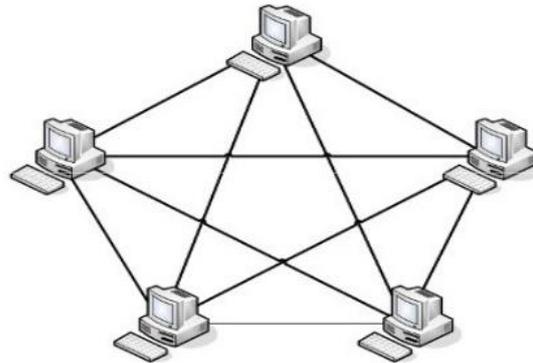
1. Topologi fisik

Topologi fisik merupakan *layout* aktual dari kabel (media) jaringan. Adapun topologi fisik (*Physical topology*) yang umum digunakan dalam membangun sebuah jaringan adalah sebagai berikut :

a. Topologi Mesh

Menurut Linto (2010:38) Topologi ini sering disebut “*peer to peer*”, sebab merupakan suatu implementasi suatu jaringan komputer yang menghubungkan seluruh komputer secara langsung. Topologi ini digunakan pada kondisi dimana tidak ada komunikasi terputus secara absolut antar *node* komputer. Topologi ini

merefleksikan desain yang memiliki *multi path* ke berbagai lokasi. Saat ini sangat jarang digunakan sebab sangat rumit dan tidak praktis.



Sumber : Sopandi (2010:39)

Gambar II.13 Model Topologi Mesh

Seperti contoh gambar II.13 semua komputer dalam suatu kantor saling berhubungan satu sama lainnya. Topologi mesh merupakan bentuk topologi yang sangat cocok dalam hal pemilihan *route* yang banyak. Hal tersebut berfungsi sebagai jalur *backup* pada saat jalur lain mengalami masalah.

b. Topologi Bus

Menurut Linto (2010:40), Topologi *Bus* merupakan topologi yang menghubungkan semua terminal ke satu jalur komunikasi yang kedua ujungnya ditutup dengan terminator. Topologi ini menghubungkan komputer secara berantai (*daisy-chain*), informasi yang dikirim akan melewati semua terminal pada jalur tersebut. Jika alamat yang tercantum atau informasi yang dikirim sesuai dengan alamat terminal yang dilewati, maka data atau informasi tersebut akan diterima dan diproses, jika alamat tersebut tidak sesuai, maka informasi tersebut akan diabaikan oleh terminal yang dilewati.

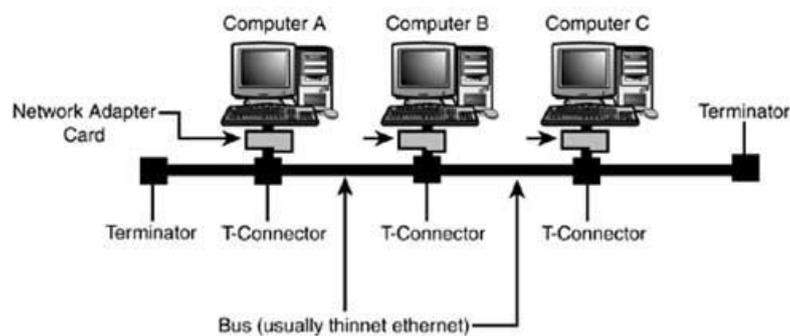
Topologi ini seringkali dijumpai pada sistem *client* atau *server*, dimana salah satu mesin pada jaringan tersebut difungsikan sebagai *File Server*, yang berarti bahwa mesin tersebut dikhususkan hanya untuk pendistribusian data dan biasanya tidak digunakan untuk pemrosesan informasi.

Keuntungan :

- 1) Metode komunikasinya sangat efisien serta hemat kabel
- 2) Releabilitas cukup tinggi
- 3) *Layout* kabel sederhana dan mudah dikembangkan
- 4) Tidak butuh sistem kendali pusat
- 5) Penambahan atau pengurangan terminal dapat dilakukan tanpa mengganggu operasi berjalan

Kelemahan :

- 1) Deteksi dan isolasi kesalahan sangat kecil
- 2) Kepadatan lalu lintas yang tinggi
- 3) Keamanan data kurang terjamin
- 4) Kecepatan akan menurun bila jumlah pemakai bertambah
- 5) Diperlukan repeater untuk jarak jauh



Sumber : Sopandi (2010:40)

Gambar II.14 Model Topologi *Bus*

Seperti contoh gambar II.14 topologi bus bisa dibilang topologi yang cukup sederhana dibanding topologi yang lainnya. Topologi ini biasanya digunakan pada instalasi jaringan berbasis *fiber optic*. Topologi bus hanya menggunakan sebuah kabel jenis *coaxial* disepanjang *node client* dan pada

umumnya, ujung kabel *coaxial* tersebut biasanya diberikan T konektor sebagai kabel *end to end*.

c. Topologi *Ring*

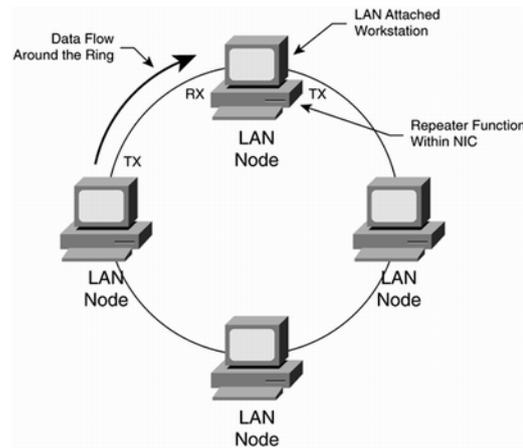
Menurut Linto (2010:41) sesuai dengan namanya, *ring* atau cincin, seluruh komputer dalam jaringan terhubung pada sebuah jalur data yang menghubungkan komputer satu dengan komputer lainnya secara berkesinambungan sedemikian rupa sehingga menyerupai semacam cincin. Topologi ini mirip dengan hubungan seri pada rangkaian listrik, dengan kedua ujung dihubungkan kembali, sehingga jika salah satu komputer mengalami gangguan, maka hal itu akan mempengaruhi seluruh jaringan. Dalam sistem jaringan ini, data dikirim secara berkeliling sepanjang jaringan (*ring*).

Keuntungan :

- 1) Susunan kabel sederhana
- 2) Dapat menjadi lebih murah dengan penggunaan kabel yang sedikit
- 3) Tidak perlu penanganan *bundle* kabel khusus
- 4) Dapat melayani lalu lintas data yang padat

Kelemahan :

- 1) Topologi ini paling rendah kesalahan (*fault*) dan toleransinya
- 2) Kerusakan dan terbukanya ujung kabel dapat menyebabkan matinya keseluruhan jaringan
- 3) Pengembangan jaringan lebih kaku
- 4) Diperlukan *repeater* hubungan jarak jauh



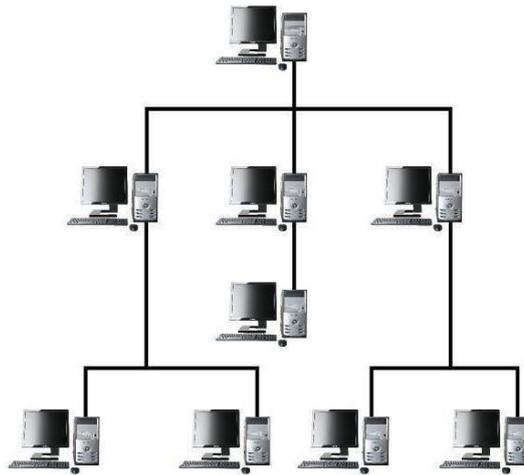
Sumber : Sopandi (2010:41)

Gambar II.15 Model Topologi *Ring*

Seperti contoh gambar II.15 topologi *ring* atau cincin merupakan salah satu topologi jaringan yang menghubungkan satu komputer dengan komputer lainnya dalam suatu rangkaian melingkar, mirip dengan cincin. Biasanya topologi ini hanya menggunakan LAN *card* untuk menghubungkan komputer satu dengan komputer lainnya.

d. Topologi *Tree* (Pohon)

Menurut Linto (2010:42) topologi ini disebut juga topologi jaringan bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antar sentral dengan hierarki yang berbeda. Untuk hierarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin ke atas mempunyai hierarki semakin tinggi.



Sumber : Sopandi (2010:43)

Gambar II.16 Model Topologi *Tree* (Pohon)

Seperti contoh gambar II.16 topologi *tree* atau pohon merupakan topologi gabungan antara topologi *star* dan juga topologi *bus*. Topologi jaringan ini biasanya digunakan untuk interkoneksi antar sentral dengan hirarki yang berbeda-beda. Topologi ini juga jaringan bertingkat.

e. Topologi *Star*

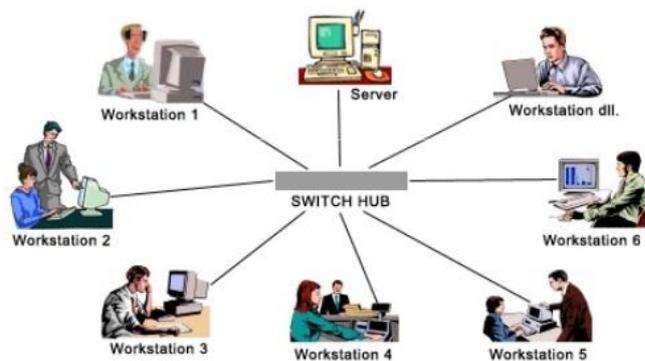
Menurut Linto (2010:42) dalam topologi ini masing-masing komputer dalam jaringan dihubungkan ke sebuah konsentrator atau poin sentral. Poin ini umumnya berupa *hub* atau *switch* dihubungkan dengan menggunakan jalur yang berbeda-beda, sehingga jika salah satu komputer mengalami gangguan, maka jaringan tidak terpengaruh. Hal ini juga memungkinkan pengaturan instalasi jaringan yang lebih fleksibel dan kecepatan komunikasi data yang lebih baik dibanding topologi yang lain.

Keuntungan :

- 1) Mudah melakukan modifikasi tata letak kabel
- 2) Mudah mengembangkan jaringan
- 3) Pemasangan dan perubahan yang terjadi pada salah satu *client* tidak mempengaruhi pada *client* lain pada jaringan

Kelemahan :

- 1) Menggunakan kabel yang banyak karena itu mahal biaya perkabelan
- 2) Membuatkan peralatan tambahan seperti *hub*, *repeater* yang bersaluran banyak (*multiport*)
- 3) Kinerja jaringan sangat di pengaruhi oleh kemampuan sentral atau dari jaringan tersebut dan diperlukan keahlian khusus



Sumber : Sopandi (2010:42)

Gambar II.17 Model Topologi *Star*

Seperti contoh gambar II.17 topologi *star* atau bintang merupakan salah satu bentuk topologi jaringan yang biasanya menggunakan *switch* atau *hub* untuk menghubungkan *client* satu dengan *client* yang lain.

2. Topologi Logik

Topologi logik (*Logical topology*) dari sebuah jaringan yang menggambarkan bagaimana *host host* saling berkomunikasi melalui sebuah media.

Ada dua tipe umum dari topologi logik yaitu :

a. Topologi *Broadcast*

Cukup memberi arti bahwa setiap *host* mengirim datanya ke semua *host* lain dalam media jaringan, dan disana tidak ada bentuk stasiun pemesanan

apapun, didalam *network* berlaku aturan yang pertama datang, pertama dilayani. Konsep ini juga berlaku pada cara kerja *Ethernet*.

b. Topologi *Token Passing*

Token passing mengontrol akses *network* dengan melepas pesan elektronik ke setiap *host* secara berurutan. Saat sebuah *host* menerimanya ini memberi arti bahwa *host* tersebut dapat mengirim data dalam *network*. Jika *host* tidak memiliki data untuk dikirim, ia akan melepas pesan ke *host* berikutnya dan proses similar ini akan terus berulang.

2.3.2. *IP Address*

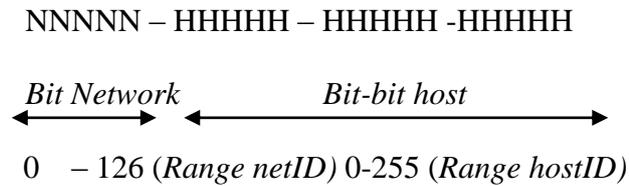
Menurut Herlambang (2008:13), *IP Address (Internet protocol Address)* adalah pengenal yang digunakan untuk memberi alamat pada tiap tiap komputer dalam jaringan. *IP Address* merupakan representasi dari 32 *bit* bilangan *biner* yang ditampilkan dalam bentuk *desimal*, terdiri atas beberapa segmen, dan tiap segmen terdiri atas 8 *bit*.

Menurut Dede (2008:60), *IP Address* dapat dipisahkan menjadi 2 bagian, yakni bagian *network (bit-bit network* atau *network bit)* dan bagian *host (bit-bit host* atau *host bit)*. *Bit network* berperan dalam identifikasi suatu *network* dari *network* yang lain, sedangkan *bit host* berperan dalam identifikasi *host* dalam suatu *network*. Jadi, seluruh *host* yang tersambung dalam jaringan yang sama memiliki *bit network* yang sama. Sebagian dari *bit-bit* bagian awal dari *IP Address* merupakan *network bit* atau *network number*, sedangkan sisanya untuk *host*. Ada 3 kelas *address* yang utama dalam TCP/IP, yakni kelas A, kelas B dan kelas C. Perangkat lunak Internet Protokol menentukan pembagian jenis kelas ini dengan menguji beberapa *bit* pertama dari *IP Address*.

1. *IP Address* Kelas A

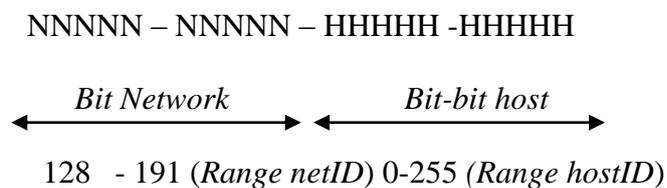
Bit pertama *IP address* kelas A adalah 0, dengan panjang *Net ID* 8 *bit* dan panjang *host ID* 24 *bit*. Jadi *byte* pertama *IP Address* kelas A mempunyai jangkauan dari 0-126. Sedangkan 127 digunakan untuk *reserve*. Jadi pada kelas A terdapat 126 *network* dengan tiap *network* dapat menampung sekitar 16.777.216 *host* (255x255x255). *IP Address* kelas A diberikan untuk jaringan

dengan jumlah *host* yang sangat besar. IP kelas A ini dapat digambarkan seperti berikut.



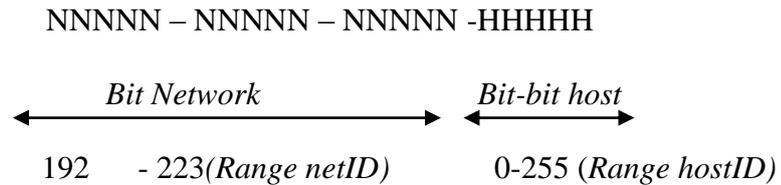
2. IP Address Kelas B

Dua *bit* IP Address kelas B selalu di set 10 sehingga *byte* pertamanya selalu bernilai antara 128-191. *Network ID* adalah 16 *bit* pertama dan 16 *bit* sisanya adalah *host ID* sehingga kalau ada komputer mempunyai IP address 167.205.20.162, maka *network ID* =167.205 dan *host ID* = 20.162. Pada IP Address kelas B ini mempunyai jangkauan IP dari 128.xxx.xxx.xxx sampai 191.255.xxx.xxx, yakni berjumlah 16.384 *network* dengan jumlah *host* tiap *network* 255x255 *host* atau sekitar 65.536 *host*. IP kelas B ini dapat digambarkan seperti berikut :



3. IP Address Kelas C

IP Address kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga *bit* pertama IP address kelas C diset 110. *Network ID* terdiri dari 24 *bit* dan *host ID* 8 *bit* sisanya sehingga dapat terbentuk sekitar 2.097.152 *network* dengan masing – masing *network* memiliki 254 *host*. Berikut gambaran IP kelas C :



4. *Subnetting*.

Menurut Tarigan (2009:5), 32 *bit IP Address* yang tersedia. Teknik *subnetting* membuat skala jaringan *subnetting* adalah membagi suatu *network* menjadi *sub-sub network* yang lebih kecil dengan memanfaatkan lebih luas dan tidak dibatas oleh kelas-kelas IP (*IP Classes*) A, B, dan C yang sudah diatur. Dengan *subnetting*, anda bisa membuat *network* dengan batasan *host* yang lebih realistis sesuai kebutuhan. *Subnetting* menyediakan cara yang lebih fleksibel untuk menentukan bagian mana dari sebuah 32 *bit IP Address* yang mewakili *network ID* dan bagian mana yang mewakili *host ID*. Dengan kelas-kelas IP *Address* standar, hanya 3 kemungkinan *network ID* yang tersedia 8 *bit* untuk kelas A, 16 *bit* untuk kelas B, dan 24 *bit* untuk kelas C. *Subnetting* mengizinkan anda memilih angka *bit* acak (*arbitrary number*) untuk digunakan sebagai *network ID*.

Tujuan dilakukannya *subnetting* adalah untuk :

- a. Membagi satu kelas *network* atas sejumlah *subnetwork* dengan arti membagi suatu kelas jaringan menjadi bagian-bagian yang lebih kecil
- b. Menempatkan suatu *host*, apakah berada dalam satu jaringan atau tidak
- c. Untuk mengatasi masalah perbedaanan *hardware* dengan topologi fisik jaringan
- d. Penggunaan IP *Address* yang lebih efisien

Kita juga harus menguasai konsep *subnetting* untuk mendapatkan IP *Address* baru, dimana dengan cara ini kita dapat membuat *network ID* baru dari suatu *network* yang kita miliki sebelumnya. *Subnetting* digunakan untuk memecah satu buah *network* menjadi beberapa *network* kecil.

Untuk memperbanyak *network* ID dari suatu *network* ID yang sudah ada, dimana sebagian *host* ID dikorbankan untuk digunakan dalam membuat ID tambahan.

Rumus untuk mencari banyak *subnet* adalah 2^n , dimana n = jumlah *binari* 1 pada *oktet* terakhir *subnet mask* pada kelas C dan 2 *oktet* terakhir pada kelas B serta 3 *oktet* terakhir pada kelas A. Sedangkan rumus untuk mencari jumlah *host* per *subnet* adalah $2^m - 2$, dimana m = merupakan kebalikan dari n , yaitu banyaknya *binari* 0 pada *oktet* terakhir. Untuk blok *subnet* dapat dihitung dengan rumus $256 - b$, dimana b = nilai *subnet mask*.

2.4. Manajemen Jaringan

2.4.1. Pengertian Manajemen Jaringan

Menurut Derianto (2007:15) manajemen jaringan adalah sebuah fungsi pengawasan terhadap unjuk kerja jaringan komputer dan pengambilan tindakan untuk mengendalikan aliran trafik agar diperoleh kapasitas jaringan dengan pengoperasian yang maksimum pada berbagai situasi.

Menurut Ardiyansyah (2008:22) pengertian lain manajemen jaringan yaitu upaya mengkoordinasikan dan mendistribusikan sumber daya untuk merencanakan, menganalisa, mengevaluasi, mendesain, mengadministrasikan dan mengembangkan jaringan komputer sehingga diperoleh kualitas pelayanan yang baik pada seluruh waktu dengan seluruh ongkos yang proposional dan kapasitas yang optimal.

Jadi secara umum manajemen jaringan komputer merupakan kemampuan untuk mengontrol dan memonitor sebuah jaringan komputer dari sebuah lokasi.

2.4.2. Faktor Manajemen Jaringan

Perkembangan teknologi telekomunikasi mengakibatkan semakin kompleksnya jaringan telekomunikasi. Hal ini memerlukan suatu sistem pengoperasian dan pemeliharaan jaringan yang efisien, ketersediaan yang optimum dan keandalan yang maksimal. Terminal operasi dan pemeliharaan (*Operation and Maintenance Terminal - OMT*) terhubung langsung kepada perangkat dan disediakan pada setiap perangkat (*mandatory*). Dengan bertambahnya jumlah perangkat sejenis, akan lebih efisien jika semua perangkat itu dioperasikan dari suatu pusat operasi dan pemeliharaan (*Operation and Maintenance Center – OMC*).

Pada mulanya setiap vendor membuat sendiri-sendiri OMT-nya, hal ini membuat operator harus mengeluarkan investasi yang besar untuk pengadaan OMT dan infrastrukturnya. Untuk mendapatkan OMC yang mampu menjadi OMT bagi semua vendor diperlukan suatu aturan interkoneksi, antarmuka dan protokol yang berlaku bagi semua vendor (*standard*).

2.4.3. Pemeliharaan Manajemen Jaringan

Pemeliharaan manajemen jaringan bertujuan untuk menjaga tetap beroperasinya jaringan. Maka dari itu pemeliharaan manajemen jaringan dibagi menjadi dua, yaitu :

1. Pemeliharaan Tidak Terencana

Pemeliharaan darurat yang perlu segera dilakukan tindakan untuk pencegahan akibat yang serius Contoh : Hilangnya produksi, kerusakan yang berat pada alat, keselamatan kerja.

2. Pemeliharaan Terencana

Pada dasarnya proses pemeliharaan bertujuan untuk menjaga tetap beroperasinya jaringan serta menjamin kelangsungan *service* kepada pelanggan.

Dilihat dari prosesnya, kegiatan pemeliharaan jaringan dapat dibagi dua:

a. Pemeliharaan kuratif

Pemeliharaan kuratif dilakukan bila terjadi atau terdapat pengaduan gangguan pelanggan, laporan kerusakan, atau alarm dari jaringan. Kegiatan yang dilakukan meliputi pengukuran untuk lokalisasi gangguan dan tindakan perbaikan/penggantian elemen jaringan yang mengalami kerusakan.

b. Pemeliharaan Preventif

Pemeliharaan preventif dilakukan sebelum terjadinya gangguan pada sistem sehingga sistem terjaga kelangsungan operasinya.

Langkah/aktifitas yang dilakukan dalam pemeliharaan preventif adalah sebagai berikut:

- 1) Monitoring unjuk kerja
- 2) *Periodic test* yang terjadwal dan otomatis
- 3) *Periodic Backup* Administrasi
- 4) Pengarsipan *Alarms Log file* dan *Historical Alarms file*

2.4.4. Tujuan Manajemen Jaringan

Tujuan dari manajemen jaringan yaitu menyediakan pelayanan jaringan telekomunikasi yang terbaik untuk sebuah perusahaan dan karyawannya pada biaya yang serendah mungkin dengan melakukan beberapa hal sebagai berikut:

1. Melaksanakan *Ongoing Operation* dalam sistem telekomunikasi

2. Menyiapkan dan melaksanakan *budget* telekomunikasi.
3. Mengikuti perubahan/pergantian perangkat, pelayanan, struktur industri, dan tarif
4. Implementasi strategi dalam pengendalian dan instruksi karyawan
5. perusahaan sesuai prosedur yang efisien
6. Membantu *top management* dalam mengembangkan kebijaksanaan telekomunikasi perusahaan
7. Mengurangi atau menghilangkan gangguan pada elemen jaringan atau keseluruhan jaringan
8. Mencegah menjalarnya gangguan ke elemen/jaringan yang lain
9. Memelihara performa jaringan, sehingga memberikan peluang keberhasilan panggilan yang lebih besar
10. Merencanakan layanan manajemen
11. Mengelola panggilan masuk secara optimal, baik dalam keadaan normal maupun tidak normal.

2.4.5. Fungsi Manajemen Jaringan

Fungsi-fungsi manajemen jaringan, yaitu :

1. Manajemen Kesalahan (*Fault Management*)

Menyediakan fasilitas yang memungkinkan administrator jaringan untuk mengetahui kesalahan (*fault*) pada perangkat yang dikelola, jaringan, dan operasi jaringan, agar dapat segera menentukan apa penyebabnya dan dapat segera mengambil tindakan (perbaikan). Untuk itu, manajemen kesalahan memiliki mekanisme untuk melaporkan terjadinya kesalahan, mencatat

laporan kesalahan (*logging*), melakukan diagnosis, mengoreksi kesalahan (dimungkinkan secara otomatis).

2. Manajemen Konfigurasi (*Configuration Management*)

Memonitor informasi konfigurasi jaringan sehingga dampak dari perangkat keras atau pun lunak tertentu dapat dikelola dengan baik. Hal tersebut dapat dilakukan dengan kemampuan untuk inisialisasi, konfigurasi ulang, pengoperasian dan mematikan perangkat yang dikelola.

3. Pelaporan (*Accounting*)

Mengukur utilisasi jaringan dari pengguna atau grup tertentu untuk menghasilkan informasi tagihan (*billing*), mengatur pengguna atau grup, membantu dalam menjaga performa jaringan pada level tertentu yang dapat diterima.

4. Manajemen Performa (*Performance Management*)

Mengukur berbagai aspek dari performa jaringan termasuk pengumpulan dan analisis dari data statistik sistem sehingga dapat dikelola dan dipertahankan pada level tertentu yang dapat diterima. Untuk itu, manajemen performa memiliki kemampuan untuk memperoleh utilisasi dan tingkat kesalahan dari perangkat jaringan, mempertahankan performa pada level tertentu dengan memastikan perangkat memiliki kapasitas yang mencukupi.

5. Manajemen Keamanan (*Security Management*)

Mengatur akses ke sumber daya jaringan sehingga informasi tidak dapat diperoleh tanpa izin. Hal tersebut dilakukan dengan cara membatasi akses ke sumber daya jaringan memberi pemberitahuan akan adanya usaha pelanggaran dan pelanggaran keamanan.