BAB 2
TINJAUAN PUSTAKA

2.1 Teori Yang Berkaitan Dengan Jaringan

Teori – teori yang berkaitan dengan jaringan akan di bahas pada bab ini :

2.1.1 Pengertian Jaringan Komputer

Tanenbaum (2011, pp. 2) mengatakan bahwa jaringan komputer merupakan koleksi komputer otonom yang saling terhubung oleh teknologi tunggal. Dua komputer dapat dikatakan saling terhubung jika dapat saling bertukar informasi. Koneksi pada jaringan dapat melalui kabel tembaga, serat optik, gelombang mikro, inframerah, dan satelit komunikasi. Tujuan dari jaringan komputer antara lain sebagai berikut:

- Membagi sumber daya. Contohnya berbagi pemakaian *printer,* CPU, memori, *harddisk, software* dan data.
- Komunikasi: contohnya *email, instant messaging, chatting.*
- Akses informasi: contohnya *web browsing.*

Kinerja jaringan komputer mempunyai berbagai jenis masalah, diakibatkan oleh unsur-unsur dalam jaringan komputer contohnya, *bandwidth, latency, and jitter* yang dapat membuat efek yang cukup besar bagi banyak aplikasi dalamsuatu jaringan.

Contoh, komunikasi suara (seperti *VoIP* atau *IP Telephony*) serta *video streaming* dapat membuat pengguna frustasi ketika paket data aplikasi tersebut dijalankan di atas jaringan komputer dengan *bandwidth* yang tidak memadai, atau dengan *latency* yang tidak stabil.

2.1.2 Model-model Topologi Jaringan Komputer

Topologi jaringan adalah sebuah desain jaringan komputer yang akan dibentuk serta menggambarkan bagaimana komputer dalam jaringan tersebut bisa saling terhubung satu sama lain. Topologi Jaringan juga menjelaskan tentang hubungan geometris antara unsur-unsur dasar penyusun jaringan diantaranya, *node*, *link* dan *station*. Untuk membangun jaringan komputer baik

yang berskala kecil atau besar, terlebih dahulu kita harus merancang topologinya. Dari topologi kita bisa menganalisa kebutuhan perangkat keras jaringan yang akan digunakan dan cara akses setiap komputer yang tergabung dalam jaringan tersebut. Dalam definisi topologi terbagi menjadi dua, yaitu :

1. Topologi logika (*logical topology*), menggambarkan cara akses yang digunakan oleh setiap komputer/*device* yang terhubung kedalam jaringan.
   Jenis Topologi Logik :
   a. Topologi *Broadcast*

      Suatu *host* mengirimkan paket data ke seluruh *host* dalam jaringan melalui media komunkasi.

   b. Topologi *Token Passing*

      Mengatur pengiriman data pada *host* melalui media dengan menggunakan *token* yang secara teratur berputar pada seluruh *host*. *Host* hanya dapat mengirimkan data hanya jika *host* tersebut memiliki *token*. Dengan *token* ini, *collision* atau tabrakan data bisa dicegah.

      Topologi fisik (*physical topology*), menunjukan secara fisik tata letak atau kedudukan setiap komputer/*device* yang terhubung menggunakan media komunikasi. Di bawah ini akan dijelaskan empat topologi dasar yang digunakan untuk membangun *LAN* menurut Comer (2009:229-231).

2. Jenis Topologi Fisik :
   a. Topologi *Bus*

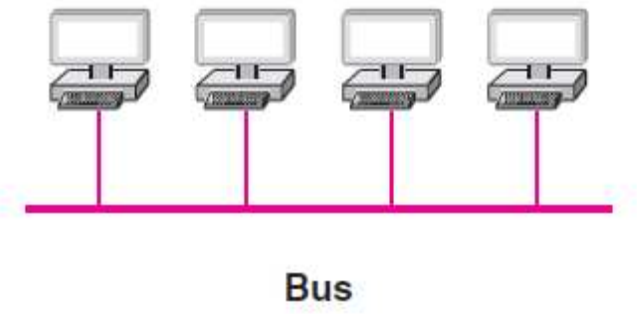
      Topologi *bus* mengguanakan *single backbone segment* sebagai penghubung semua komputer yang ada pada jaringan. Semua komputer langsung terhubung ke komputer tersebut.

      Adapun kelebihan dari Jaringan topologi *bus* adalah:

      - Penggunaan kabel yang sedikit sehingga terlihat sederhana.
      - Pengembangan Jaringannya mudah.

Kekurangan Jaringan bertopologi bus adalah:

- Membutuhkan *repeater* untuk jarak jaringan yang terlalu jauh.
- Jaringan akan terganggu apabila salah satu komputer mengalami kerusakan.
- Apabila terjadi gangguan yang serius maka jaringan tidak dapat digunakan dan pengaruhnya adalah proses pengiriman data akan menjadi lambat dikarenakan lalu-lintas jaringan penuh dan padat akibat tidak adanya pengontrolan *user*.
- Deteksi kesalahan sangat kecil, sehingga apabila terjadi gangguan maka sulit sekali mencari kesalahan tersebut.



Gambar 2.1 Topologi *Bus*

(Computer Networks and Internets 5th edition, Douglas E. Comer, 2008)

b. Topologi *Ring*

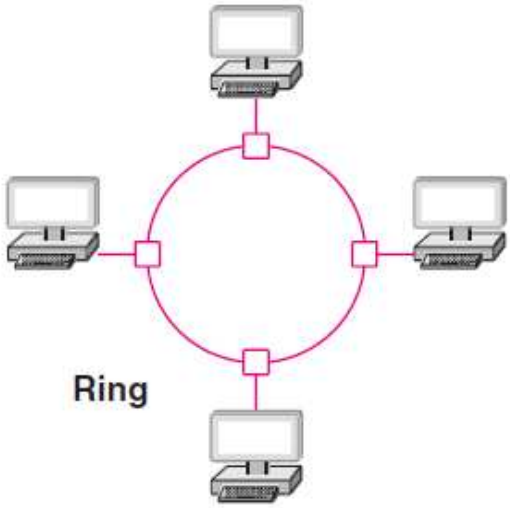
Topologi *Ring* berbentuk rangkaian *workstation* yang masing-masing terhubung ke dua *workstation* lainnya, sedemikian sehingga membentuk jalur melingkar membentuk cincin. Pada topologi *ring*, komunikasi dapat terganggu jika suatu titik mengalami gangguan.

Kelebihan dari jaringan topologi ini adalah:

- Hemat Kabel
- Dapat mengisolasi kesalahan dari suatu *workstation*

Kekurangan dari jaringan topologi ini adalah:

- Sangat peka terhadap kesalahan jaringan walaupun sekecil apapun.
- Sukar untuk mengembangkan jaringan, sehingga jaringan tersebut tampak statis.
- Biaya pemasangan lebih besar.



Gambar 2.2 Topologi *Ring*

(Computer Networks and Internets 5th edition, Douglas E. Comer, 2008)

c. Topologi *Star*

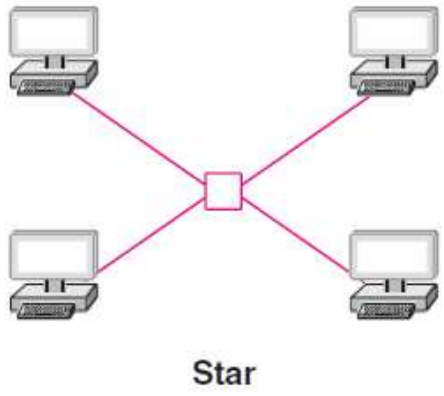
Topologi star menghubungkan semua *workstation* ke satu buah titik pusat. Titik pusat ini biasanya berupa *hub* atau *Switch* sehingga seolah-olah komputer yang terhubung berbentuk seperti bintang.

Kelebihan jaringan Topologi *Star*:

- Mudah dalam mendeteksi kesalahan jaringan karena control jaringan terpusat.
- Fleksibel dalam hal pemasangan jaringan baru, tanpa mempengaruhi jaringan yang lain.
- Apabila salah satu kabel koneksi *user* terputus, maka hanya *user* yang bersangkutan saja yang tidak akan berfungsi dan tidak mempengaruhi *user* yang lain.

Kekurangan jaringan bertopologi *Star*:

- Boros dalam pemakaian kabel jika kita hubungkan dengan jaringan yang lebih besar dan luas;
- Kontrol hanya terpusat pada *hub*/*Switch* sehingga operasionalnya perlu ditangani secara khusus.



Gambar 2.3 Topologi *Star*

(Computer Networks and Internets 5th edition, Douglas E. Comer, 2008)

d. Topologi *Mesh*

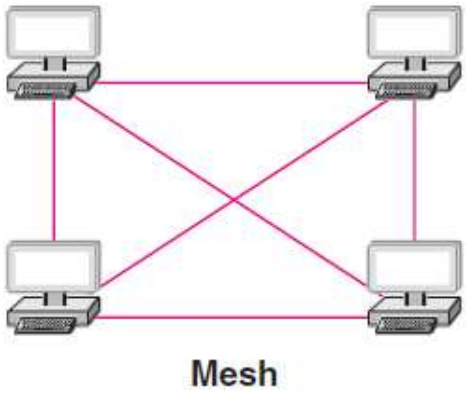
Topologi *Mesh* adalah suatu bentuk hubungan antar perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada di dalam jaringan. Akibatnya, dalam topologi *mesh* setiap perangkat dapat berkomunikasi langsung dengan perangkat yang dituju (*dedicated links*). Topologi *mesh* digunakan ketika dibutuhkan jaringan yang tidak boleh ada kesalahan sedikitpun dalam komunikasi, contohnya pada *System control* pembangkit tenaga nuklir.

Kelebihan Topologi *Mesh* :

- Keamanan dapat dikatakan baik
- Besar *bandwidth* yang cukup lebar
- Tidak perlu khawatir mengenai tabrakan data
- Pengiriman dan pemrosesan data yang terbilang cepat

Kekurangan Topologi *Mesh* :

- Biaya pemasangan yang mahal
- Instalasi dan konfigurasi yang rumit dan sulit



Gambar 2.4 Topologi *Mesh*

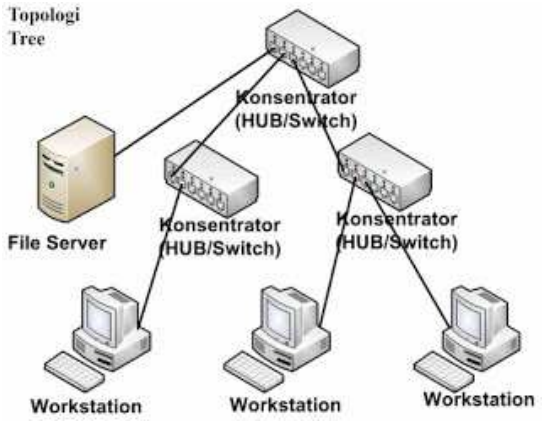
(Computer Networks and Internets 5th edition, Douglas E. Comer, 2008)

e. Topologi *Tree*

Jaringan topologi ini disebut juga sebagai topologi jaringan bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antar sentral dengan hirarki yang berbeda. Untuk hirarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin ke atas mempunyai hirarki semakin tinggi. Topologi jaringan jenis ini cocok digunakan pada sistem jaringan komputer.

Ciri-ciri jaringan *Tree/hybrid* :

- Merupakan pengembangan dari topologi jaringan *star*.
- Jaringan topologi *Tree* digunakan untuk mendukung algoritma *searching* dan *sorting*
- Setiap tangkai (*node*) dalam *Tree* akan dihubungkan dengan pusat hub yang berada pada awal trafik rangkaian.



Gambar 2.5 Topologi *Tree*

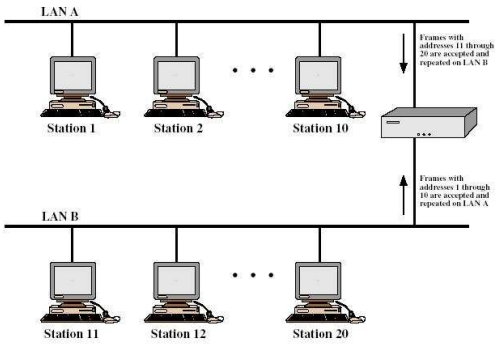
Sumber: (Computer Networks and Internets 5th edition, Douglas E. Comer, 2008)

2.1.3 Jenis Jaringan Komputer

Menurut Chandrika, Rama Krishna, & Velaga Pavani (2012) mengatakan bahwa berdasarkan skala atau area, jaringan komputer dapat dibagi menjadi 4 jenis, yaitu:

1. *LAN*

   Local Area Network adalah suatu jaringan lokal yang dibuat pada area terbatas, misalkan dalam suatu gedung atau dalam suatu ruangan. Kadang kala jaringan lokal disebut juga jaringan personal atau privat. *LAN* biasa digunakan pada sebuah jaringan kecil yang mengunakan *resource* secara bersama seperti pengunaan printer secara bersama, pengunaan media penyimpanan secara bersama dan sebagainya.

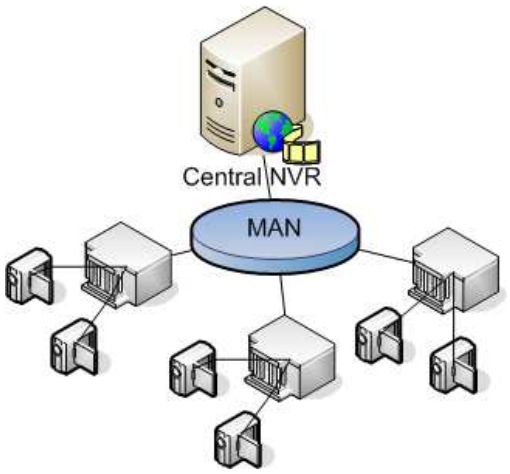


Gambar 2.6 Dua *LAN* yang Terpisah (*workgroup*)

Sumber: (Computer Networks and Internets 5th edition, Douglas E. Comer, 2008)

2. *MAN*

Metropolitan Area Network mengunakan metode yang sama dengan *LAN* namun daerah cakupannya lebih luas. Daerah cakupan *MAN* bisa satu RW, beberapa kantor yang berada dalam komplek yang sama, satu/beberapa desa, satu/beberapa kota. Dapat dikatakan *MAN* pengembangan dari *LAN*.



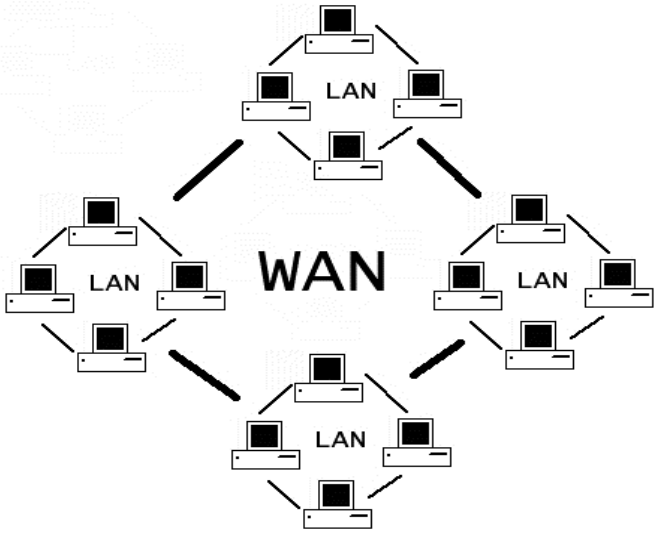
Gambar 2.7 *Metoropolitan Area Network*

Sumber: (Computer Networks and Internets 5th edition, Douglas E. Comer, 2008)

3. *WAN*

Wide Area Network cakupannya lebih luas dari pada *MAN*. Cakupan *WAN* meliputi satu kawasan, satu negara satu pulau, bahkan, satu dunia. Metode yang digunakan *WAN* hampir sama dengan *LAN* dan *MAN*.

Umumnya *WAN* dihubungkan dengan jaringan telepon digital. Namun media transmisi lain pun dapat digunakan.



Gambar 2.8 *Wide Area Network*

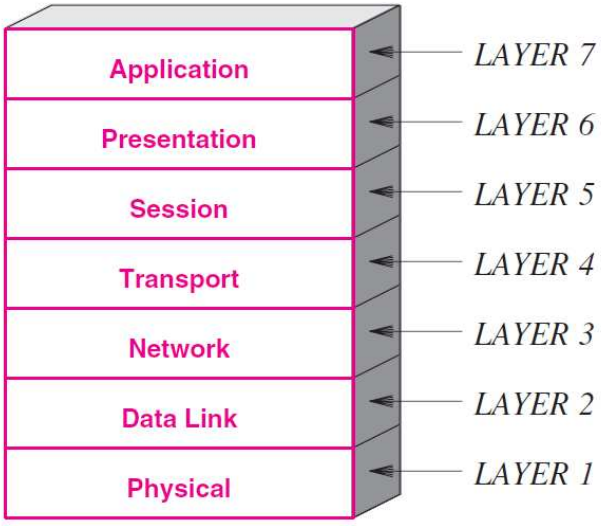
Sumber: (Computer Networks and Internets 5th edition, Douglas E. Comer, 2008)

4. Internet

   Internet adalah interkoneksi jaringan komputer skala besar (mirip *WAN*), yang dihubungkan mengunakan protokol khusus. Jadi sebenarnya internet merupakan bagian dari *WAN*. Cakupan adalah satu dunia bahkan tidak menutup kemungkinan antar planet. Koneksi antar jaringan komputer dapat dilakukan berkat dukungan protokol yang khas, yaitu *TCP/IP* (*Transmission Control Protoco / Internet Protocol*).

2.1.4 *Open System Interconnection* (OSI) Layer

Menurut Tanenbaum (2011:41-45), model *OSI Layer* didasarkan pada pengajuan yang dikembangkan oleh *International Standard Organization (ISO)* sebagai langkah pertama menuju standardisasi internasional protokol yang digunakan dalam berbagai lapisan (*Day* dan *Zimmermann*, 1983) yang setelah itu direvisi pada tahun 1995 (*Day*, 1995). Model ini disebut *ISO OSI (Open System Interconnection) Reference Model* karena berhubungan dengan koneksi sistem terbuka yaitu, sistem yang terbuka untuk berkomunikasi dengan sistem lain. Berikut ini merupakan gambaran dari tabel *OSI Layer* beserta penjelasannya:



Gambar 2.9 *OSI Layer Model*

(Computer Networks and Internets 5th edition, Douglas E. Comer, 2008, p13)

a. *Physical Layer*

Physical layer berkaitan dengan transmisi *bit* di dalam sebuah *channel* komunikasi. Masalah desain yang utama adalah memastikan bahwa ketika di satu sisi mengirimkan sebuah *bit*, nantinya akan diterima oleh sisi lain sebagai 1 *bit*, bukan sebagai 0 *bit*. Lapisan ini

sebagian besar berurusan dengan mekanik, listrik, dan waktu, serta media transmisi fisik, yang terletak dibawah *physical layer*.

b. *Data Link Layer*

Tugas utama dari lapisan ini adalah untuk mengubah transmisi mentah menjadi sebuah garis yang bebas dari kesalahan transmisi yang seharusnya terdeteksi, caranya adalah dengan menutupi kesalahan yang sebenarnya sehingga *Network layer* tidak melihatnya. Lapisan ini menyelesaikan tugasnya dengan cara pengirim memecah data *input* menjadi data *frame* (yang berjumlah ratusan atau ribuan byte) dan mengirimkan *frame* secara berurutan. Jika sudah terkirim, penerima akan mengkonfirmasi penerimaan yang benar dari setiap *frame* dengan mengirimkan kembali *frame* pemberitahuan.

c. *Network Layer*

Lapisan ini mengontrol operasi dari subnet. Masalah desain utama dari lapisan ini adalah menentukan bagaimana paket diarahkan dari sumber ke tujuan. Rutenya dapat berdasarkan tabel statis yang terhubung dengan jaringan dan jarang diubah, atau tabel tersebut dapat di *update* secara otomatis untuk menghindari komponen yang gagal. Selain itu, rute juga dapat ditentukan pada awal setiap percakapan, misalnya, sesi terminal, seperti *login* ke sebuah *remote machine*. Pada akhirnya, desain ini dapat bersifat sangat dinamis, dengan ditentukan lagi untuk masing-masing paket untuk mencerminkan beban jaringan saat itu.

d. *Transport Layer*

Fungsi dasar dari lapisan ini adalah menerima data dari lapisan atasnya, membaginya kedalam unit yang lebih kecil jika diperlukan, mengirimkan data ini ke *Network layer*, dan memastikan bahwa semua bagian sampai dengan benar di ujung lainnya. Selain itu, semua ini

harus dilakukan secara efisien dan dalam cara yang mengisolasi lapisan atas dari perubahan teknologi perangkat seiring waktu berjalan.

e. *Session Layer*

Lapisan ini memungkinan pengguna pada mesin yang berbeda untuk memulai sesi diantara pengguna tersebut. Sesi menawarkan berbagai layanan, termasuk pengendalian dialog (menjaga giliran pengiriman data), manajemen *token* (mencegah kedua pihak menjalankan operasi yang sama secara bersamaan), dan sinkronisasi (membuat *checkpoint* transmisi panjang yang memungkinkan transmisi untuk memulai dari posisi terakhir dimana terjadi *crash* dan melakukan pemulihan).

f. *Presentation Layer*

Tidak seperti lapisan sebelumnya, yang sebagian besar berkaitan dengan pergerakan *bit*, lapisan ini lebih berkaitan dengan sintaks dan semantik dari informasi yang dikirimkan. Untuk memungkinkan komputer dengan perbedaan internal representasi data untuk berkomunikasi, struktur data yang akan dipertukarkan dapat didefinisikan secara abstrak, bersama dengan standar *encoding* yang digunakan pada jaringan. *Presentation layer* mengelola struktur data abstrak dan memungkinkan struktur data tingkat tinggi (misalnya, catatan perbankan) untuk didefinisikan dan dipertukarkan.

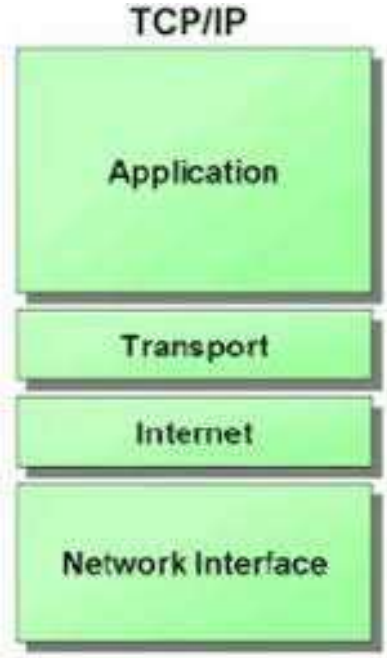
g. *Application Layer*

Lapisan ini berisi berbagai protokol umum yang dibutuhkan oleh pengguna. Salah satu protokol yang banyak digunakan adalah HTTP (*Hypertext Transfer Protocol*), yang merupakan dasar dari *World Wide Web*. Ketika sebuah *browser* ingin membuka halaman web, dia akan mengirimkan nama halaman ke *server* yang menghosting halaman tersebut menggunakan *HTTP*. *Server* itu lalu mengirimkan kembali

halaman tersebut. Protokol aplikasi lainnya digunakan untuk *transfer file*, surat elektronik, dan jaringan berita.

2.1.5 *Transmission Control Protocol/Internet Protocol (TCP/IP)*

TCP/IP merupakan pengembangan *protocol* yang merujuk pada *protocol OSI*, sebagai *protocol* standar umum yang digunakan pada jaringan komunikasi data dalam berbagai perangkat keras dan sistem operasi. Lapisan *TCP/IP* terdiri dari empat lapisan seperti terlihat pada Gambar.



Gambar 2.10 Model *TCP/IP*

sumber : https://hubpages.com/

Fungsi lapisan-lapisan yang terlihat pada gambar model *TCP/IP* adalah:

1. Lapisan Aplikasi (*Application Layer*)

   Lapisan ini berisi bermacam-macam protokol tingkat tinggi. Protokol-protokol terdahulu terdiri dari *terminal virtual (TELNET)*, *transfer file* (FTP), surat elektronik *(SMTP)*. Pada lapisan ini berisikan logik yang dibutuhkan untuk mendukung berbagai aplikasi *user*.

2. Lapisan *Host to Host* (*Transport Layer*)

   Pada lapisan ini menyediakan layanan transfer data ujung ke ujung, lapisan ini meliputi mekanisme kehandalan, menyembunyikan detail-detail jaringan dari lapisan aplikasi. Pada lapisan ini terdapat dua protokol, yaitu *TCP* (*Transmission Control Protocol*) dan *UDP* (*User DatagramProtocol*).

3. Lapisan Internet (*Internet Layer*)

   Lapisan internet berfungsi untuk menghubungkan dua perangkat ke jaringan yang berbeda, diperlukan prosedur-prosedur tertentu agar data dapat melalui yang bermacam-macam. Pada lapisan ini dipergunakan *Internet Protocol (IP)* untuk menyediakan fungsi *routing* melintasi jaringan yang bermacam-macam. Protokol ini diterapkan tidak hanya pada ujung sistem namun juga pada jalur-jalurnya. Tugas lapisan internet adalah untuk mengirimkan paket-paket *IP* ke tempat tujuan seharusnya.

4. Lapisan Akses Jaringan (*Network Access Layer*)

   Lapisan ini bertanggungjawab untuk menyediakan akses ke jaringan komunikasi. Lapisan ini juga bertanggungjawab untuk mengirimkan data ke *node-node* yang terletak pada jaringan yang sama.

2.1.6 Teori Protokol

IPv4 Address

Tanenbaum dan Wetherall mengatakan bahwa IP address adalah sekumpulan bilangan biner sepanjang 32 *bit*, yang dibagi atas 4 segmen dan setiap segmen terdiri atas 8 *bit*. *IP address* merupakan identifikasi setiap *host* pada jaringan internet. Secara teori, tidak boleh ada 2 *host* atau lebih yang tergabung ke internet menggunakan *IP address* yang sama. Hal ini tidak sepenuhnya benar karena kasus-kasus “pencurian” *IP address* seringkali terjadi.

Untuk memudahkan pembacaan dan penulisan, *IP address* telah direpresentasikan dalam bilangan *decimal* yang dipisahkan oleh titik atau disebut *dotted-decimal* format. Nilai *decimal* dari *IP address* inilah yang dikenal dalam pemakaian sehari-hari. Apabila setiap segmen dikonversikan ke bilangan *decimal* berarti nilai yang mungkin antara 0 hingga 255.

Contoh IP address sebagai berikut :

01000100 10000001 11111111 00000001

Jika dikonversikan ke bilangan decimal menjadi :

68.129.255.1

Jangkauan alamat *(range address)* yang bisa digunakan adalah dari

00000000 00000000 00000000 00000000

atau

0.0.0.0

Sampai dengan

11111111 11111111 11111111 11111111

atau

255.255.255.255

Dengan demikian, secara teori ada sebanyak 232 kombinasi *IP address* yang bisa dipakai di seluruh dunia. Jadi, jaringan *TCP/IP* dengan 32 *bit address* mampu menampung sebanyak lebih dari 4 milyar *host*. Pada kenyataannya ada sejumlah *IP address* yang digunakan untuk keperluan khusus. Contoh *IP address* khusus :

- *Network address*
- *Broadcast address*
- *NetMask address*
- *Multicast address*
- *Loopback (localhost) address*
- *Default route address*

Selain itu ada beberapa *IP address* yang tidak bisa digunakan untuk *host-host* internet. *IP address* ini hanya digunakan untuk *host-host* di *LAN*. Kita bebas menggunakan *IP address* di atas untuk keperluan jaringan *local*.

Inilah yang disebut dengan *private IP address (non-routeable IP address)*. Daftar *IP address private* dapat dilihat pada tabel.

Class	Subnet Mask decimal	No. of Hosts per Network	No. of Networks	Start -End Address
A	255.0.0.0	16 Million	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255
D	Reserved for multicast groups			224.0.0.0 - 239.255.255.255
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 - 254.255.255.254

Gambar 2.11 *IP Address*

Sumber: *http://mreze.vigimnazija.edu.rs/wp-content/uploads/2014/02/ip-class*

IP address dapat dipisahkan menjadi 2 bagian, yaitu:

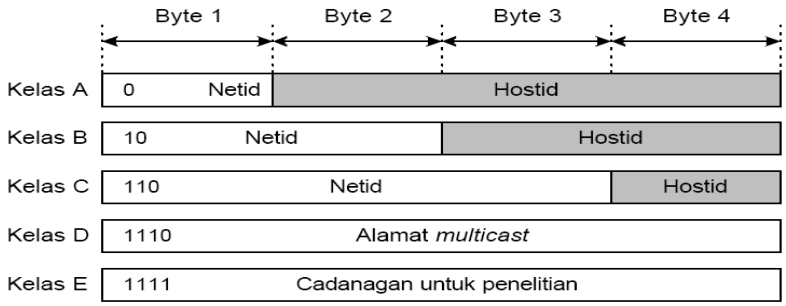
- Bagian *Network (bit-bitNetwork/Network bit)* atau disebut *Network ID.*
- Bagian *host (bit-bit host/host bit)* atau disebut *host ID.*

Bit Network berperan sebagai identifikasi *Network.* Pada jaringan *TCP/IP*, perbedaan antar *Network* tidak ditentukan dari jenis topologi, media fisik jaringan, luas area, jenis sistem operasi, aplikasi, dan sebagainya. Perbedaan jaringan dilihat dari perbedaan *bit-bit Network*-nya. Manakala ada 2 buah jaringan, yang satu menggunakan topologi bus, sedangkan yang lain menggunakan topologi ring, sepanjang *Network bit*-nya sama maka kedua topologi tersebut dikatakan berada pada satu *Network.* Sebaliknya, walaupun sama-sama berbeda pada topologi bus, manakala suatu *host* memiliki *Network bit* yang berbeda dengan *host-host* lain, maka kita katakan *host* tersebut tidak satu *Network.*

Sedangkan *bit host* berperan dalam identifikasi *host* pada suatu *Network.* Jadi, seluruh *host* yang tersambung dalam jaringan yang sama memiliki *bit Network* yang sama namun *bit host*-nya pasti berbeda. Panjang bit *Network* tidak selalu tetap, sangat bergantung kepada kelas *Network* dan kondisi lain, seperti subnetting.

Untuk memudahkan pengaturan *IP address* seluruh komputer pengguna jaringan internet, dibentuklah suatu badan yang mengatur pembagian *IP address.*

Badan tersebut bernama *InterNIC* (Internet *Network* Information Center). *InterNIC* membagi-bagi *IP address* menjadi beberapa kelas. Kelas-kelas tersebut meliputi :



Gambar 2.12 Definisi Kelas *IP Address*

Sumber: *http://s1080.photobucket.com/user/sruntul2/media/p5-1.png.html*

1. Kelas A

   Jika *bit* pertama dari *IP address* adalah 0 maka *IP address* termasuk dalam *Network* kelas A. *Bit* ini dan 7 *bit* berikutnya (8 *bit* pertama) merupakan *bit-bit Network* (*Network bit*) dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 24 *bit* terakhir merupakan *bit host*.

   IP address harus dikonversikan dari bentuk biner ke bentuk desimal. Dengan demikian, hanya ada 128 *Network* kelas A, yakni dari nomor 0.xxx.xxx.xxx sampai 127.xxx.xxx.xxx. Setiap *Network* dapat menampung lebih dari 16 juta (2563) host (xxx adalah variabel, nilainya dari 0 sampai dengan 255).

2. Kelas B

   Jika 2 *bit* pertama dari *IP address* adalah 10, maka *IP address* termasuk dalam *Network* kelas B. 2 *bit* ini dan 14 *bit* berikutnya (16 *bit* pertama) merupakan *bit Network* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 16 *bit* terakhir merupakan *bit host*.

   Jika bentuk biner dikonversikan ke bentuk desimal maka akan terdapat lebih dari 16 ribu *Network* kelas B, yakni dari *Network*

128.0.xxx.xxx hingga 191.125.xxx.xxx. Setiap *Network* kelas B mampu menampung lebih dari 65 ribu *host* (2562).

3. Kelas C

   Jika 3 *bit* pertama dari *IP address* adalah 110, maka *IP address* termasuk dalam *Network* kelas C. 3 *bit* ini dan 21 *bit* berikutnya (24 *bit* pertama) merupakan *bit Network* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 8 *bit* terakhir merupakan bit host.

   Jika bentuk biner dikonversikan ke bentuk desimal maka akan terdapat lebih dari 2 juta *Network* kelas C, yakni dari nomor 192.0.0.xxx hingga 223.255.255.xxx. Setiap *Network* kelas C hanya mampu menampung sekitar 256 *host.*

4. Kelas D

   Jika 4 *bit* pertama adalah 1110, maka *IP address* termasuk dalam kelas D. *IP address* kelas D digunakan untuk *multicast address*, yakni sejumlah komputer yang memakai bersama suatu aplikasi (bedakan dengan pengertian *Network address* yang mengacu kepada sejumlah komputer yang memakai bersama suatu *Network*).

   Salah satu penggunaan *multicast address* yang sedang berkembang saat ini di internet adalah aplikasi untuk *real-time* video *conference* yang melibatkan lebih dari 2 *host (multipoint),* menggunakan *multicast backbone (MBone).* Pada *IP address* kelas D tidak dikenal *bit-bit Network* dan *host.*

5. Kelas E

   Kelas terakhir adalah kelas E. *IP address* kelas E masih bersifat percobaan. Jika 4 *bit* pertama adalah 1111 (atau sisa dari seluruh kelas) maka *IP address* termasuk dalam kategori kelas E. Pemakaian *IP address* kelas E dicadangkan untuk kegiatan eksperimental.

2.1.7 Perangkat *Network*

Menurut Hartpence (2011:80-90) perangkat jaringan atau *Network Device* adalah alat yang digunakan untuk menghubungkan *end-user device* ke jaringan, memperluas jangkauan jaringan, melakukan konversi format data, mengatur transfer data, dan banyak fungsi jaringan lainnya :

1. *Switch*

Switch merupakan *Network device* yang bekerja pada *Layer* 2 model *OSI*, yang mampu melakukan manajemen transfer data yaitu hanya meneruskan data ke segmen yang dituju. *Switch* tidak melakukan konversi format data.

Switch mempelajari *host* mana saja yang terhubung kesuatu *port* dengan membaca *MAC address* asal yang ada di dalam *frame* kemudian *Switch* membuka sirkuit *virtual* antara *node* sumber dengan *node* tujuan. Dengan demikian komunikasi dua *port* tersebut tidak mempengaruhi *traffic* dari *port* lain. Hal tersebut membuat *LAN* lebih efisien.

Switch terbagi menjadi dua jenis, yaitu *manageable Switch* dan *unmanageable Switch* . Secara umum fungsi kedua jenis *Switch* sama yaitu sebagai media penghubung dalam jaringan yang sama, memperbesar skala jaringan.

a. Manageable Switch

Manageable Switch mempunyai *IP address* tersendiri dan memiliki fitur telnet dan mungkin juga *web-based interface* untuk memonitoring dan akses yang aman untuk setiap *port* yang ada di dalam *Switch*. *Port* pada *Manageable Switch* dapat dikonfigurasi menggunakan *VLAN* tertentu, dimana dapat membuat banyak *port* yang berbeda dalam *Switch* yang sama. *Manageable Switch* juga dapat digunakan untuk mengaktifkan atau menonaktifkan *port* tertentu tanpa harus mencabut kabel. *Manageable Switch*, memiliki fitur monitoring yang fungsinya dapat melakukan konfigurasi *IP address* bahkan juga dapat melakukan pengecekan transfer data melalui *IP address*, atau melakui *protocol SNMP* atau program monitoring lainnya.

Gambar 2.13 *Manageable Switch*

sumber : http://www.cisco.com

b. Unmanageable Switch

Unmanageable Switch sering disebut dengan *glorified hub*, yang berarti bahwa *Switch* dapat dilakukan tanpa interaksi dengan *user.* Pada *Switch unmanaged* tidak dapat melakukan pengaturan prioritas lalu lintas data dimana semua data memiliki prioritas yang sama, baik data yang *urgent* atau tidak.

Pada *Switch unmanage* tidak memiliki fitur monitoring. Artinya *Switch unmanage* yang dipasang pada jaringan tidak bisa dicek melalui *Network* atau jaringan. Dimana pengecekan hanya dapat dilakukan untuk memastikan data yang dikirim telah sampai tujuan.

Gambar 2.14 *Unmanageable Switch*

sumber : http://www.alliedtelesis.com

2. *Router*

Router merupakan perangkat keras jaringan komputer yang dapat digunakan untuk menghubungkan beberapa jaringan yang sama atau berbeda. *Router* adalah sebuah alat untuk mengirimkan paket data melalui jaringan atau internet untuk dapat menuju tujuannya, proses tersebut dinamakan *routing*. *Router* bertugas melakukan *routing* paket data dari *source* ke *destination* pada *LAN*, dan menyediakan koneksi ke *WAN*. Dalam lingkungan *LAN*, *router* membatasi *broadcast domain*, menyediakan

layanan *local address resolution* seperti ARP (*Address Resolution Protocol*) dan RARP (*Reverse Address Resolution Protocol*), dan membagi *Network* dengan menggunakan struktur *subNetwork.*

Gambar 2.15 *Router*

sumber : http://www.cisco.com

3. *Access Point* (AP)

AP disebut juga sebagai *wireless hubs* karena mediumnya terbagi. Seperti sebuah hub, AP membroadcast *traffic* ke semua yang mampu mendengarnya. Tetapi, hal ini terjadi lebih kepada tipe medianya dibandingkan pengoperasian dari AP tersebut. Standar 802.11 mendeskripsikan beberapa tugas utamanya:

- Memberi tahu pengguna jaringan dari keberadaannya dan menegosiasikan koneksi
- Meneruskan *traffic* antara jaringan kabel dan nirkabel
- Mengatur *traffic* dari semua node *wireless* yang terkoneksi
- Mengenkripsi data *traffic*
- Mengatur node dalam mode hemat daya

Node menggunakan tiga langkah proses ketika bergabung dengan jaringan nirkabel. Pertama, jaringan tersebut harus ditemukan dengan pendeteksian aktif atau pasif. Kedua, node harus mengautentikasi dengan jaringan. Ketiga, node telah terasosiasi dengan jaringan.

4. *HUB*

Hub adalah sebuah perangkat yang menyediakan suatu jalur fisik bagi suatu sinyal untuk dapat menyeberang dari satu kabel ke kabel berikutnya. Pada dasarnya, hub merupakan repeater dengan banyak port, maka hub hanya menguatkan sinyal listrik yang masuk ke dalam salah satu portnya, dan meneruskan sinyal itu ke semua port yang lain. Karena hub hanya bekerja menguatkan sinyal tanpa melakukan pemrosesan apapun, maka tiap-tiap port pada hub selalu merupakan bagian dari segmen jaringan (collision domain yang sama).

Gambar 2.16 Hub

Sumber: http://www.patartambunan.com/wp-content/uploads/2014/01/Fungsi-HUB-Pada-Jaringan-Komputer

5. Bridge

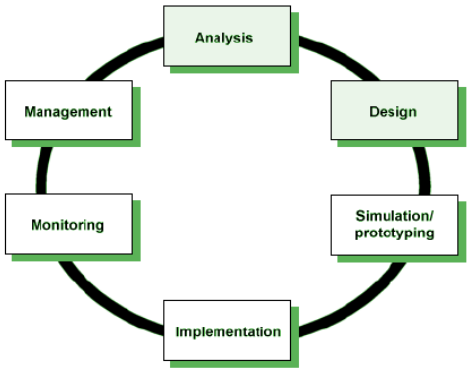
Bridge pada umumnya mirip menyerupai hub. *Bridge* adalah perangkat dengan 2 *port*, yang biasanya digunakan untuk menghubungkan segmen jaringan yang satu dengan segmen jaringan yang lain. Bedanya dengan *hub* adalah *bridge* melaksanakan pemeriksaan terhadap data yang datang, dan membuat keputusan apakah data itu boleh dilewatkan atau tidak. *Bridge* bekerja pada lapisan 2 OSI (misalnya *MAC Address*).

Gambar 2.17 Bridge

Sumber: https://www.ictlounge.com/Images/network_bridge

2.1.8 NDLC Teori Metode

Menurut Goldman (2004:205) *NDLC* merupakan suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus awal dan akhir dalam membangun sebuah jaringan komputer yang mencakup beberapa proses tahapan, yaitu analysis, design, simulation/prototyping, implementation, monitoring, management. Sebuah jaringan baru tentu saja harus bermula dari tahap awalnya, yaitu dengan tahapan analisis. Sedangkan jaringan yang sudah ada terus mengalami perkembangan dari satu tahap ketahap selanjutnya dalam *NDLC*. Berikut ini adalah penjelasan tahapan yang dilakukan dalam metode *NDLC*:



Gambar 2.18 *NDLC*

(Sumber:http://www.technologyuk.net/telecommunications/Networks/images/lifecycle01.gif)

1. Analisis

Pada tahap ini dilakukan analisis kebutuhan dan analisis permasalahan yang muncul, metode yang digunakan adalah:

a. Wawancara

Proses pengajuan pertanyaan dan pencatatan jawaban untuk dokumentasi yang akan digunakan untuk mendapatkan informasi tentang sistem jaringan.

b. Survey Lapangan

Langkah verifikasi atas hasil wawancara sehingga hasil yang didapatkan valid dan dapat digambarkan kedalam bentuk topologi, grafik, atau tabel. Langkah ini dilakukan dengan kunjungan ke perusahaan.

2. Perancangan

Dari hasil analisis permasalahan jaringan kemudian langkah perancangan akan membuat rancangan jaringan dari kebutuhan jaringan yang ada. Konfigurasi untuk instalasi dan implementasi teknologi yang sudah ditentukan pada langkah sebelumnya.

3. Simulasi

Pada tahap ini dilakukan simulasi untuk melihat kinerja awal dari jaringan yang sudah dirancang dan yang akan dibangun. Dari tahap simulasi akan di dapatkan informasi mengenai rancangan jaringan. Jika terdapat kekurangan atau error maka akan segera diperbaiki.

4. Implementasi

Setelah hasil simulasi jaringan telah berhasil dilakukan maka langkah berikutnya adalah penerapan, perancangan, dan teknologi jaringan yang baru pada perusahaan berdasarkan rancangan yang telah dibuat. Diikuti dengan *Test* ing untuk memastikan hasilnya sesuai dengan apa yang di harapkan.

5. Monitoring

Setelah tahapan implementasi berhasil dilakukan dan dapat berjalan dengan baik maka tahapan berikutnya adalah monitoring agar komunikasi dapat berjalan sesuai yang diinginkan dan ketujuan yang tepat.

6. Management Policy

Pada tahap manajemen dilakukan pengaturan kebijakan agar sistem yang dibangun dapat berjalan dengan baik pada kebijakan setiap level yang dibuat sesuai dengan kebutuhan dalam perusahaan tersebut.

2.1.9 Cara Pengetesan yang digunakan

Ping (*Packet Internet Gopher)* adalah sebuah programutilitas yang dapat digunakan untuk memeriksa konektivitas jaringan berbasis teknologi *Transmission Control Protocol/Internet Protocol*(TCP/IP).

Dengan menggunakan utilitas ini, dapat diuji apakah sebuah komputer terhubung dengan komputer lainnya. Hal inidilakukan dengan mengirim sebuah paket kepada alamat IP yang hendak di uji coba konektivitasnya dan menunggu respondarinya.

2.1.10 Teori dan Metoda *Fact Finding*

Dalam penulisan skripsi ini, ada beberapa metode digunakan, yaitu :

1. Metode analisa dan pengumpulan data (*Fact Finding*).

   Pengumpulan data yang dilakukan menggunakan *Fact Finding* dengan langkah-langkah sebagai berikut:

   a. Wawancara

      Dilakukan dengan memberikan beberapa pertanyaan secara tatap muka kepada divisi IT BJB. Wawancara dilakukan untuk mendapatkan informasi mengenai apa saja yang dibutuhkan dalam pembuatan skripsi ini.

   b. Analisis sistem yang sedang berjalan

      Pada tahap ini yang akan dilakukan adalah melakukan analisis terhadap sistem jaringan yang sedang berjalan. Langkah ini dilakukan dengan kunjungan ke KCP Simpang Dago dan Kantor Wilayah I.

   c. Studi Pustaka

      Mencari, mempelajari dan mengumpulkan kebutuhan sistem yang sedang berjalan pada KCP Simpang Dago dan Kantor Wilayah I Metode ini digunakan untuk menemukan landasan – landasan teori yang digunakan dalam melakukan penelitian, serta mengadakan studi penelaahan terhadap buku-buku, literatur-literatur, catatan-catatan, dan laporan-laporan yang ada hubungannya dengan masalah yang dipecahkan.

d. Perancangan

Membuat struktur dan desain sistem jaringan baru berdasarkan hasil analisis dan kebutuhan KCP Simpang Dago dan Kantor Wilayah I Bank BJB.

e. Uji Coba

Melakukan pengujian terhadap jaringan yang sudah dibuat apakah sudah sesuai dan berjalan dengan baik.

2. Metode Perancangan Jaringan

Metode perancangan jaringan yang digunakan adalah metode *Network Development Life Cycle* (NDLC). Berikut 6 tahap penting yang kami gunakan:

- *Analysis*
- *Design*
- *Simulation / Prototype*
- *Implementation*
- *Monitoring*
- *Management*

2.1.11 Teori dan Metoda pengukuran

PUTTY adalah sebuah program *Open* source yang dapat Anda gunakan untuk melakukan protokol jaringan *SSH*, Telnet dan Rlogin. Protokol ini dapat digunakan untuk menjalankan sesi remote pada sebuah komputer melalui sebuah jaringan, baik itu *LAN*, maupun internet. Program ini banyak digunakan oleh para pengguna komputer tingkat menengah ke atas, yang biasanya digunakan untuk menyambungkan, mensimulasi, atau mencoba berbagai hal yang terkait dengan jaringan. Program ini juga dapat Anda gunakan sebagai tunnel di suatu jaringan.

Selama ini banyak orang yang menggunakan Putty sebagai aplikasi pilihan untuk menghubungkan antara PC (windows) dengan server yang memiliki sistem operasi Linux, termasuk dalam meremote VPS linux. Putty memang merupakan aplikasi SSH Client yang paling banyak digunakan saat

ini. Selain ramah terhadap sistem operasi windows, putty juga dapat diinstall pada sistem operasi Linux. Tampilan putty memang sederhana, tapi juga memiliki pengaturan serta fitur yang sangat beragam. Diantaranya seperti Disable application cursor keys mode, Disable application keypad mode, Disable arabic text shaping, mengganti warna pada backgroud, text dan lain sebagainya.

Selain mendukung SSH, putty juga mendukung koneksi melalui telnet, raw, rlogin dan serial communications. Putty terkenal sangat ringan dan tidak membebani resource. Fitur yang cukup menarik di putty pada OS Linux Ubuntu adalah adanya fitur penyimpanan profile, ini sangat berguna untuk memudahkan jika nantinya ingin kembali melakukan remote koneksi pada profile yang pernah di gunakan sebelumnya.

2.2 Teori Khusus

Berikut merupakan beberapa teori yang terkait tema penelitian (tematik) adalah sebagai berikut:

2.2.1 Routing

Routing merupakan proses berpindahnya data melalui jaringan denganmelalui beberapa *segmen* jaringan menggunakan peralatan yang disebut router. Router (pengatur *rute*) akan memilihkan jalur data yang tepat sesuai dengan arah tujuan data. Penempatan router di jaringan akan menggabungkan serta mengkoneksikan router-router kecil yang akan membentuk sebuah *entitas* yang disebut antar jaringan atau *interNetwork*.

Router akan mengolah informasi tentang arah jalur data dari sebuah *file* menjadi skema yang disebut tabel *routing*. Tabel ini berisi informasi *interface* router jaringan (atau *port*) yang digunakan untuk mengirim data melalui *segmen* jaringan tertentu. Router tidak akan menjalankan paket-paket *broadcast* yang tidak diketahui tujuannya. Router akan mengatur sebuah paket yang dikirimkan jika mempunyai tujuan yang spesifik. Protokol *routing* pada dasarnya adalah metode-metode yang digunakan oleh router untuk saling mengomunikasikan informasi NLR. Dengan demikian, sebuah router dapat

menginformasikan rute-rute yang diketahuinya kepada router-router lain di dalam jaringan. Tujuan-tujuan penggunaan protokol *routing* adalah:

1. Menyederhanakan proses manajemen jaringan karena alamat-alamat yang dapat dicapai dapat segera diketahui secara otomatis.
2. Menemukan jalur-jalur bebas-loop di dalam jaringan.
3. Menetapkan jalur terbaik di antara beberapa pilihan yang tersedia.
4. Memastikan bahwa semua router yang ada di dalam jaringan ‘menyetujui’ jalur-jalur terbaik yang telah ditetapkan.

Terdapat banyak protokol *routing* yang digunakan dewasa ini, masing-masing dengan kelebihan dan kekurangan relatifnya. Sebagian di antaranya adalah standar terbuka (*Open standard*) yang dikelola oleh badan-badan standar internasional, semisal IETF dan ISO, sedangkan sebagian lainnya adalah standar proprieter (*proprietary standard*) yang dikuasai kepemilikannya oleh perusahaan-perusahaan swasta. Akan tetapi, semua protokol ini menyediakan suatu mekanisme bagi router untuk saling berkomunikasi dengan satu sama lainnya,sehingga NLRI dapat terkumpul secara lengkap dan, selanjutnya, diolah dan digunakan untuk menentukan jalur-jalur terbaik di dalam jaringan serta mengatasi berbagai potensi masalah *looping* .

2.2.2 Static Routing

Static routing merupakan sebuah mekanisme pengisian tabel *routing* yang dilakukan oleh administrator secara manual pada tiap-tiap router. *Static routing* memiliki beberapa keuntungan:

1. Meringankan kerja processor yang terdapat di router.
2. Tidak ada *bandwidth* yang digunakan untuk pertukaran informasi (isidari tabel routing) antar router.
3. Tingkat keamanan lebih tinggi dibanding dengan mekanisme lainnya.

Sedangkan kekurangan yang dimiliki oleh *static routing* antara lain :

1. Administrator harus mengetahui informasi tiap-tiap router yang terhubung dengan jaringan.
2. Jika terdapat penambahan atau perubahan topologi jaringan, administrator harus mengubah isi tabel *routing*.
3. Tidak cocok untuk jaringan router yang besar.

2.2.3 Dynamic Routing

Dynamic routing merupakan sebuah mekanisme pengisian dan pemeliharaan tabel *routing* tidak dilakukan secara manual oleh administrator. Router akan saling bertukar informasi *routing* agar dapat mengetahui alamat tujuan dan memelihara tabel *routing*. Router IP (yang semakin sering disebut sebagai *Gateway*) selalu dihubungkan ke lebih dari satu *Network* fisik, Router IP adalah *host multihome* (*host* yang memiliki banyak rumah atau hubungan antar muka pada lebih dari satu *Network*) yang bisa mengarahkan paket-paket. Pemilihan jalur dilakukan berdasarkan pada jarak terpendek antara *device* pengirim dengan *device* tujuan. Untuk merepresentasikan jarak, *dynamic routing* menggunakan nilai *metric*. Parameter-parameter yang biasa digunakan untuk menghasilkan sebuah nilai *metric*, di antaranya:

1. *Hop count*, berdasarkan pada banyaknya router yang dilewati.
2. *Ticks*, berdasarkan waktu yang diperlukan dengan satuan waktu *ticks*.
3. *Cost*, berdasarkan pada perbandingan sebuah nilai patokan *standard* dengan *bandwidth* yang tersedia.
4. *Compose metric*, berdasarkan hasil perhitungan dari parameter-parameter berikut :
   - *Bandwidth*
   - *Delay*
   - *Load*
   - *Reliability*
   - MTU (*Maximum Transmit Unit*)

Router merupakan perangkat *layer* 3, yang merupakan perangkat yang lebih rumit dan cerdas. Router berfungsi meneruskan paket data dari satu tempat ketempat lain, tergantung nilai alamat jaringan, bukan alamat *hardware* (MAC) seperti *bridge*. Router bekerja dengan membaca protokol seperti IP, untuk membuat keputusan ke mana harus mengirim atau meneruskan data yang diterima.

2.2.4 Routing Protocol

Routed protocol adalah fungsi transportasi yang dilakukan oleh protokol routing dalam melintasi antar jaringan. Secara umum, *routed protocol* beradadalam konteks yang berhubungan dengan *protocol Network*. Protokol ini mempunyai variasi fungsi yang dibutuhkan untuk melakukan komunikasi antar aplikasi pengguna sebagai sumbernya dan peralatan yang menjadi tujuannya.

Fungsi tersebut bervariasi tergantung protokol *suite*-nya. *Routed protocol* adalah protokol yang dirutekan melalui *interNetwork*. Contoh *routed protocol* adalah IP, *DECnet*, *AppleTalk*, *Novell Netware*, OSI, *Banyan VINES*, dan *Xerox Network System* (XNS). *Routing protocol* adalah protokol yang mengimplementasikan algoritma *routing*, contohnya adalah *Interior Gateway Routing Protocol* (IGRP), EIGRP, OSPF, *Exterior Gateway Protocol*(EGP), BGP, *Intermediate System to Intermediate System* (IS-IS), dan RIP.

2.2.5 FHRP (First Hop Redudancy Protocol)

Menurut Dubey, P., Shilpi Sharma, & Aabha Sachdev (2013) *FHRP* merupakan suatu Protocol yang berguna untuk *Network* agar memiliki *Availability* yang baik, dengan cara menyediakan jalur (Link) Redudancy pada dua atau lebih perangkat Phisiccally yang di konfigurasi menjadi satu perangkat virtual, salah satu perangkat akan menjadi jalur active (utama) dan yang lain Standby atau jalur cadangan (Backup Link) apabila jalur utama Down, contohnya dua perangkat menjadi satu interface virtual jadi pada dua perangkat tersebut akan sepakat hanya ada satu *Gateway* pada dua Link (jalur)

dan pada Link tersebut ada yang active dan Backup. Yang masuk pada Protocol FHRP ini adalah VRRP, HSRP, GLBP.

Proses detail pada konfigurasi Protocol FHRP adalah sebagai berikut:

- Forwarding / active router mengirim paket pesan ke standby router tiap beberapa detik.
- Secara default router yang menyala duluan akan menjadi *forwarding* router.
- Apabila active router sedang *down* dan tidak mengirim paket pesan ke standby router maka otomatis standby router active dan menjadi forwarding router.
- Secara default apabila mantan active router *connected* maka router akan menjadi standby router dan posisinya sudah di ambil alih, (kecuali nilai priority masih tertinggi maka router akan menjadi active ruuter).

2.2.6 VRRP (Virtual Router Redundancy Protocol)

Menurut Dubey, P., Shilpi Sharma, & Aabha Sachdev (2013) *VRRP* adalah protokol umum yang secara dinamis menunjuk satu atau beberapa router untuk dapat menggunakan IP *Address* yang sama. Dalam konfigurasi VRRP, sebuah router dipilih menjadi virtual router utama dengan router lainnya sebagai virtual router cadangan jika virtual router utama tersebut *down*. Dikarenakan protokol VRRP adalah protokol umum, maka penggunaan merek perangkat jaringan komputer dapat berbeda. Setiap perangkat jaringan komputer khususnya *Switch manageable* maupun router pasti telah dibekali dengan protokol VRRP.

Contoh penerapan VRRP yaitu di dalam sebuah jaringan ketika terdapat 1 *Gateway* ketika internet *down* atau putus maka semua *user* tidak bisa tersambung ke internet, oleh karena itu dibuat 2 buah *Gateway*. Tetapi dengan 2 buah *Gateway* masih tidak effisien karena admin harus melakukan reset satu-persatu di tiap PC untuk menentukan *Gateway* mana yang akan digunakan, apalagi jika salah satu *Gateway* mati maka akan ada beberapa PC yang tidak bisa tersambung ke internet. Metode *failover*

VRRP bisa dibuat seolah olah ada satu IP *Gateway* virtual, sehingga walaupun salah satu *Gateway* mati PC *client* tetap bisa tersambung ke internet.

2.2.7 HSRP (Hot Standby Router Protocol)

Menurut Singh, A. Kumar, & Abhay Kothari (2011) *HSRP* adalah protokol paten milik Cisco yang dibuat pada tahun 1994 untuk mengijinkan *failover* secara cepat dan transparan dari *hop* pertama perangkat IP *address*. Salah satu cara untuk meningkatkan waktu *uptime* hingga mendekati 100 persen, HSRP dapat digunakan pada jaringan komputer dengan *Availability* yang tinggi dengan menyediakan redundansi IP *address Network* pada hop pertama *routing* untuk *host* dan jaringan komputer yang telah dikonfigurasi menggunakan sebuah IP *Address default Gateway*.

1. Dasar Operasi HSRP

   Salah satu cara untuk mencapai *Network uptime* hingga mendekati 100% adalah menggunakan HSRP. HSRP menyediakan redundansi untuk Jaringan IP, memastikan bahwa lalu lintas data dari user dapat dipulihkan secara cepat dan transparan dari kegagalan hop pertama (*Gateway*) pada perangkat jaringan komputer.

   Melalui *sharing* IP Address dan MAC Address (Layer 2 OSI), dua atau lebih router dapat bertindak sebagai sebuah single “virtual” Router. Anggota lain dari grup virtual router secara berkala salinng bertukar informasi status. Dengan Cara ini, satu router dapat mengasumsikan tanggung jawab atas proses *routing* pada router lain, jika memang terdapat kendala baik direncakan maupun tidak. *Client* yang ada di bawahnya secara terus-menerus meneruskan IP *Packets* ke IP dan MAC *Address* yang konsisten, dan perubahan *routing* dilakukan secara transparan.

2. Operasional HSRP

Operasinal HSRP ialah sekumpulan router yang dapat bertindak sebagai single virtual router terhadap host yang ada di LAN. Sekumpulan router tersebut dikenal sebagai HSRP *group* atau standby group. Sebuah *single* router dipilih dari sebuah group router bertanggung jawab untuk mem-forward paket data yang dikirimkan host ke virtual router. Router tersebut dikenal dengan *Active* Router. Router lainnya bertindak sebagai *standby* router. Pada saat active router terjadi masalah, *standby* router akan mengambil alih proses *forwarding packet* data yang sebelumnya merupakan tanggung jawab dari *Active* Router.

penjelasan operasi HSRP di atas, Berikut ini adalah beberapa istilah dalam HSRP.

Tabel 2. 1. Istilah dalam HSRP

Term (Istilah)	Definition (Definisi)
Active Router	Router yang meneruskan paket-paket untuk virtual router
Standby Router	Router cadangan Bila Active Router *Down*
Standby Group	Kelompok router yang telah dikonfigurasi HSRP untuk menjadi virtual router

3. Pengalamatan HSRP

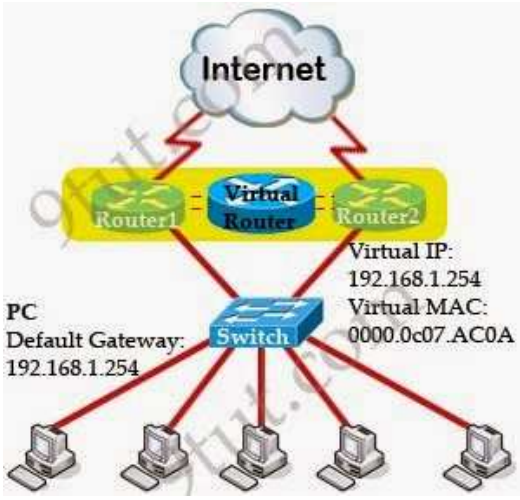
Dalam kebanyakan kasus ketika mengkonfigurasi router-router untuk menjadi bagian dari HSRP Group, mereka menggunakan Mac address khusus yang digunakan pada grup HSRP tersebut dan Mac Address bawaan pabrik. Router yang berada pada HSRP tersebut menggunakan MAC Address HSRP ketika menjadi Active Router, pada saat menjadi standby router MAC Address yang digunakan adalah MAC Address bawaan pabrik.

HSRP menggunakan Mac Address di bawah ini pada semua media kecuali Token Ring:

0000.0c07.ac** (dimana ** adalah nomor dari HSRP Group)

4. Cara Kerja HSRP

Gambar di bawah ini menjelaskan tentang bagaimana cara kerja dari metode HSRP.



Gambar 2.19 HSRP

Sumber: http://www.9tut.com

Gambar di atas terdapat 2 router fisik, 1 router virtual, 1 *Switch* , dan 5 *client* PC. Cara kerjanya adalah kedua router di atas dianggap sebagai satu router (virtual) saja, HSRP menggunakan sebuah IP dan MAC *Address* virtual dari dua router fisik yang berguna untuk mempresentasikan hanya satu *Gateway* untuk semua Host, sebagai contoh: Virtual IP:192.168.1.254 dan Virtual Mac *Address* 0000.0C07.AC0A jadi semua *host* akan mengarahkan *Gateway*-nya pada IP dan Mac tersebut.

Pada protokol HSRP seluruh router yang tergabung dalam HSRP *group* saling bertukan informasi status dengan mengirimkan pesan *Hello Packet* sesama router tersebut. Setiap router meingirimkan pesan *Hello Packet* tersebut ke alamat spesifik. Pada protokol HSRP versi 1 pesan *Hello Packet* dikirimkan ke alamat IP 224.0.0.2 port UDP 1985, sedangkan untuk HSRP versi 2 pesan *Hello Packet* dikirimkan ke alamat IP 224.0.0.102 pada versi IOS 12.2(46)SE ke atas.

Setiap versi dari protokol HSRP memiliki struktur pesan *Hello Packet* yang berbeda, sekelompok router yang menjalankan HSRP harus berkomitmen untuk menggunakan versi protokol HSRP yang sama, jika tidak maka komunikasi

protokol HSRP tidak akan berjalan, karena format *hallo packet* yang berbeda. Default *hello-timer* pada HSRP adalah 3 detik dan hold time adalah 10 detik

HSRP memiliki fitur *preemption* dimana memungkinkan sebuah router yang ada pada group HSRP yang memiliki prioritas tertinggi dapat secara cepat menjadi Active Router. Nilai prioritas tersebut diurutkan berdasarkan nilai yang telah ditentukan pada saat konfigurasi awal HSRP, selanjutnya prioritas ditentukan berdasarkan IP Address. Pada beberapa kasus nilai tertinggi merupakan prioritas terbesar untuk menentukan router mana yang akan menjadi *Active* Router.

2.2.8 GLBP (*Gateway* Loadbalancing Protocol)

Pada Protocol GLBP ini berbeda dengan yang VRRP DAN HSRP, GLBP sudah tidak menggunakan *redundancy* tetapi menggunakan *load balancing* sesuai dengan namanya, Load balancing adalah sebuah konsep yang gunanya untuk menyeimbangkan beban atau muatan. Seperti itulah prinsip kerja dari GLBP. Intinya adalah membagi kerja Router yang besarnya sama atau seimbang/balance. GLBP melindungi trafik data dari kerusakan router atau jalur data. GLBP melindungi trafik dengan cara router-routernya diberi sebuah default *Gateway* yang sama sedangkan yang membedakan pada virtual MACnya dari masing-masing router.

2.3 VLAN

Menurut Lammle (2007:552), VLAN adalah pengelompokan logikal dari pengguna jaringan dan sumber daya yang terhubung ke administratif yang didefinisikan ke dalam *port* pada *Switch* . Pada saat VLAN dibuat, jaringan akan membuat *broadcast domain* yang lebih kecil pada *layer 2* intrajaringan dengan menetapkan *port* yang berbeda pada *Switch* ke subjaringan yang berbeda. VLAN bekerja seperti subnet atau *broadcast domain* sendiri, yang berarti bahwa *frame* disiarkan hanya ke jaringan aktif antara *port* logikal yang dikelompokkan dalam VLAN yang sama.

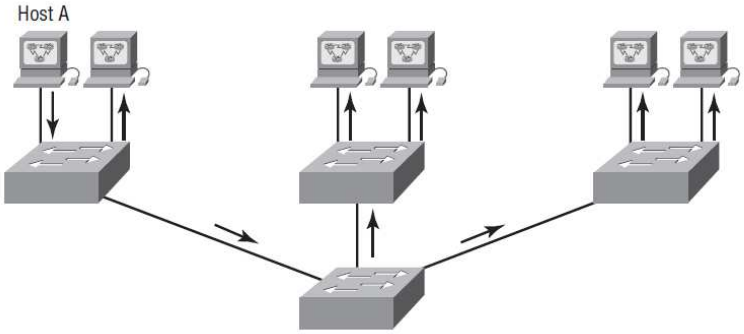
Secara *default, host* di VLAN tertentu tidak dapat berkomunikasi dengan *host* yang merupakan anggota dari VLAN lain, jadi jika komputer ingin dapat berkomunikasi antar-VLAN, masih diperlukan router.

Menurut Shaffi dan Al-Obaidy (2012:1), Virtual LAN atau VLAN memungkinkan para insinyur jaringan dan *administrator* jaringan untuk membuat jaringan logikal berdasarkan jaringan fisik. Teknologi ini digunakan untuk membuat segmentasi jaringan yang kompleks menjadi jaringan yang lebih kecil untuk pengelolaan yang lebih baik, meningkatkan kinerja dan keamanan. VLAN secara logikal membuat segmen dalam *Switch* berdasarkan fungsi organisasi seperti departemen atau lokasi geografis. Oleh karena itu, menerapkan VLAN untuk setiap jaringan akan mencapai manfaat sebagai berikut:

- Kemudahan pemindahan lokasi PC pada *Local Area Network.*
- Mudah menambahkan atau menghapus *host* ke atau dari suatu LAN.
- Mudah mengubah konfigurasi LAN.
- Mudah mengontrol lalu lintas jaringan antara LAN.
- ACL menyediakan *access* atau *denied services*.
- Meningkatkan keamanan jaringan.
- Mudah mengelola administrasi jaringan.
- Mengurangi biaya.

1. Perbandingan LAN dan VLAN

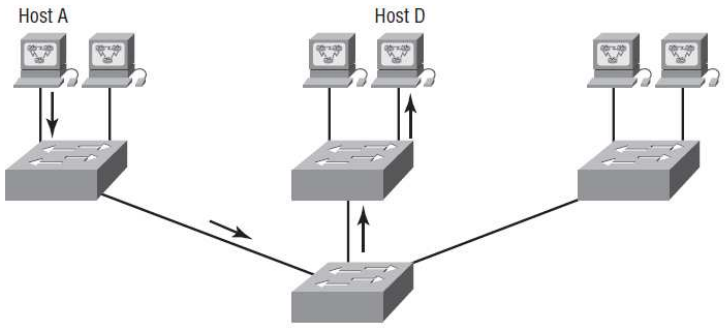
Menurut Lammle (2007:552), jaringan yang terhubung pada switch pada *layer* 2 biasanya dirancang sebagai *flat-network*. Dengan konfigurasi ini, setiap paket *broadcast* ditransmisikan ke setiap perangkat yang ada dalam jaringan tanpa melihat apakah perangkat harus menerima data itu atau tidak. Jaringan disebut *flat* karena hanya memiliki satu *broadcast domain.*



Gambar 2.20 Struktur *Flat-network*

(Cisco ® Certified Network Associate Study Guide - Sixth Edition, Lammle, 2007, p553)

Gambar 2.10 menunjukkan ketika *host* A mengirimkan *frame* menuju *host* D sebagai tujuan. *Frame* yang diteruskan hanya keluar pada *port* di mana *host* D berada. Salah satu manfaat yang diperoleh dengan memiliki jaringan switch *layer 2* adalah untuk membuat segmen *collision domain* individu untuk setiap perangkat terhubung ke setiap *port* pada switch. Namun seringkali, semakin besar jumlah pengguna dan perangkat, semakin banyak *broadcast* dan paket yang harus ditangani switch.



Gambar 2.21 Struktur Jaringan Dengan Switch

(Cisco ® Certified Network Associate Study Guide - Sixth Edition, Lammle, 2007, p553)

Salah satu masalah serius yang terjadi pada kebanyakan jaringan switch *layer* 2 adalah masalah keamanan. Semua pengguna dapat melihat semua perangkat secara *default*. *Broadcast* akan disiarkan ke seluruh perangkat, sehingga berisiko jika *password* disimpan pada *server* dan perangkat lainnya.

Dengan menggunakan VLAN, banyak masalah dapat dipecahkan terkait dengan jaringan switch *layer* 2. Berikut adalah daftar singkat cara VLAN dalam menyederhanakan manajemen jaringan:

- Kemudahan dalam menambahkan, memindahkan, dan mengubah jaringan dengan hanya mengkonfigurasi *port* ke VLAN yang sesuai.
- Sekelompok pengguna yang membutuhkan tingkat keamanan yang tinggi dapat dimasukkan ke dalam VLAN tertentu, sehingga pengguna di luar VLAN tidak dapat berkomunikasi dengan yang di dalam VLAN tersebut.
- Pengelompokan logikal dari pengguna berdasarkan fungsi, VLAN bersifat independen dan tidak bergantung dari lokasi fisik atau geografis.
- VLAN meningkatkan keamanan jaringan.
- VLAN meningkatkan jumlah *broadcast domain* sekaligus mengurangi ukurannya.

a. Broadcast

Semua perangkat dalam VLAN adalah anggota dari *broadcast domain* yang sama dan menerima semua *broadcast*. Secara *default*, siaran ini disaring dari semua *port* pada switch yang bukan anggota VLAN yang sama. Hal ini membuat permasalahan yang terjadi bila suatu jaringan hanya memiliki hanya satu buah *broadcast domain* dapat teratasi.

b. Security

Pada VLAN, ketika banyak grup *broadcast* dibuat, maka *administrator* akan memiliki kontrol penuh terhadap setiap *port* dan pengguna. Maka, pengguna tidak dapat lagi menghubungkan perangkatnya secara sembarang ke dalam switch *port* dan mendapatkan *resource* dari jaringan karena setiap

perangkat baru yang terhubung harus terkonfigurasi dengan benar sesuai VLAN *port* yang ada.

Selain itu, VLAN dapat dibuat sesuai dengan sumber daya jaringan dan kebutuhan pengguna tertentu, ditambah switch dapat dikonfigurasi untuk menginformasikan stasiun manajemen jaringan dari akses yang tidak sah ke sumber daya jaringan. Dan jika dibutuhkan komunikasi antar VLAN, maka dapat diterapkan sebuah pembatasan pada router, alamat perangkat keras, protokol, dan aplikasi.

c. Flexibility and Scalability

Layer 2 switch hanya membaca *frame* untuk disaring. Secara *default*, switch meneruskan semua *broadcast*. Tetapi jika ingin membuat dan menerapkan VLAN, pada dasarnya akan memecah *broadcast domain* menjadi lebih kecil pada *layer* 2.

Hal ini berarti bahwa *broadcast* yang dikirimkan dari sebuah node dalam satu VLAN tidak akan diteruskan ke *port* konfigurasi milik VLAN yang berbeda. Jadi dengan menetapkan *port* switch atau pengguna untuk kelompok VLAN pada switch atau sekelompok switch yang terhubung, akan diperoleh fleksibilitas untuk menambahkan pengguna yang diinginkan ke dalam domain *broadcast* terlepas dari lokasi fisiknya. Pengaturan ini juga berfungsi untuk memblokir *broadcast storm* yang disebabkan oleh kesalahan *Network Interface Card* (NIC) serta mencegah perangkat perantara dalam menyebarkan *broadcast storm* di seluruh intrajaringan.

2. VLAN *Memberships*

Keanggotaan VLAN dibagi menjadi dua model yaitu *Static* VLAN dan *Dynamic* VLAN.

a. *Static* VLAN

VLAN statis adalah cara yang paling umum untuk membuat VLAN, dan salah satu alasan untuk itu adalah karena VLAN statis adalah yang paling aman. Keamanan ini berasal dari fakta bahwa

setiap *port* switch yang ditetapkan, akan selalu terpelihara sesuai dengan VLAN yang terhubung.

Konfigurasi VLAN statis cukup mudah untuk diatur dan diawasi, dan bekerja dengan sangat baik dalam lingkungan jaringan dimana setiap gerakan pengguna dalam jaringan perlu dikontrol.

b. *Dynamic* VLAN

Di sisi lain, VLAN dinamis menentukan VLAN tugas node secara otomatis. Dengan menggunakan *intelligent management software*, tugas VLAN dapat dibagi sesuai dengan alamat perangkat keras (MAC), protokol, atau bahkan aplikasi yang membuat VLAN dinamis.

Sebagai contoh, katakanlah alamat MAC telah dimasukkan ke dalam aplikasi manajemen VLAN terpusat dan terhubung ke node yang baru. Jika sebuah PC terpasang ke sebuah *port* switch yang belum ditetapkan, VLAN database manajemen akan mencari alamat perangkat keras dan menetapkan dan mengkonfigurasi *port* switch ke VLAN yang benar. Hal ini membuat manajemen dan konfigurasi lebih mudah karena jika pengguna berpindah tempat, switch akan menempatkannya ke VLAN yang benar secara otomatis.

Dalam pengalamatan pada VLAN dinamis, dapat digunakan VLAN *Management Policy Server* (VMPS) yaitu layanan untuk membuat sebuah *database* alamat MAC yang akan digunakan untuk pengalamatan dinamis VLAN. *Database* VMPS otomatis memetakan alamat MAC ke VLAN.

3. *Identifying* VLANs

Ketahuilah bahwa *port* switch hanya sebuah *interface layer* 2 yang berhubungan dengan *port* fisik. Sebuah *port* switch hanya bisa

tergabung pada suatu VLAN jika terhubung pada *port* akses atau port *trunk*.

Ada dua jenis link dalam jaringan switch yaitu *access port* dan *trunk port*. *Access port* hanya memiliki dan membawa *traffic* satu VLAN saja. *Traffic* yang diterima dan dikirim terdiri dalam format asli tanpa VLAN *tagging*.

Setiap perangkat yang terpasang ke *access link* tidak mengetahui tentang keanggotaan VLAN. Perangkat hanya berasumsi bahwa ia berada pada *broadcast domain* yang sama. Selain itu, switch menghapus informasi VLAN apapun dari *frame* sebelum diteruskan ke perangkat *access link*. Perangkat *access link* tidak bisa berkomunikasi dengan perangkat luar VLAN kecuali paket dihubungkan menggunakan router. Setiap *port* switch hanya bisa dikonfigurasikan antara *access port* atau *trunk port* dan bukan keduanya sekaligus.

Sedangkan istilah *trunk port* terinspirasi oleh sistem batang telepon yang membawa beberapa percakapan telepon sekaligus. Artinya bahwa *trunk port* dapat membawa beberapa VLAN pada satu waktu.

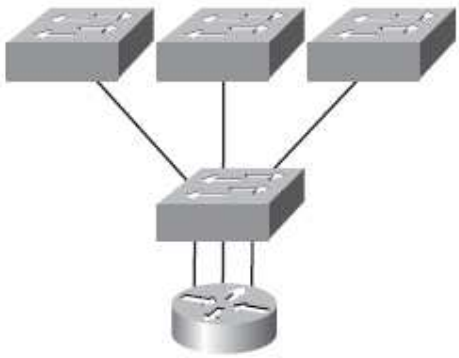
Trunk link merupakan sebuah *link* dengan kecepatan 100-1000Mbps *point-to-point* antara dua switch, antara switch dan router, atau bahkan antara switch dan *server*, dan membawa lalu lintas dari beberapa VLAN antara 1-4094 pada satu waktu.

Dengan menggunakan *trunk port*, dapat dibuat sebuah *single-port* yang terhubung kepada beberapa VLAN yang berbeda. *Trunk* membawa berbagai informasi VLAN melalui *link* apabila *link* antar switch telah dikonfigurasi pada mode *trunk*.

4. Inter-VLAN *Routing*

Host di dalam VLAN bekerja di dalam broadcast domainnya sendiri dan berkomunikasi secara bebas. VLAN membuat partisi jaringan dan pembagian traffic dalam layer 2 OSI. Jika ingin berkomunikasi antar VLAN, maka dibutuhkan perangkat dari layer 3, yaitu router.

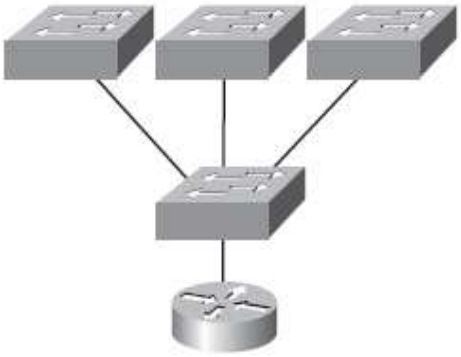
Router yang dapat digunakan harus memiliki *interface* untuk setiap VLAN atau sebuah router yang mendukung ISL atau 802.1Q *routing*. Seperti ditunjukkan pada gambar 2.11, jika hanya memiliki sedikit VLAN (dua atau tiga), maka dapat menggunakan router dengan dua atau tiga koneksi *Fast Ethernet*.



Gambar 2.22 Router Mengkoneksikan Tiga VLAN Secara Bersamaan.
(Cisco ® Certified Network Associate Study Guide - Sixth Edition, Lammle, 2007, p567)

Setiap *interface* router terhubung dengan sebuah *access link*. Ini berarti alamat IP setiap *interface* dari router akan menjadi alamat *default gateway* untuk setiap *host* di setiap VLAN.

Satu *interface Fast Ethernet* sudah cukup dibandingkan harus menggunakan sebuah *interface* untuk setiap VLAN dengan menjalankan ISL atau 802.1Q *trunking*. Gambar 2.12 menunjukkan sebuah *interface Fast Ethernet* dari sebuah router yang terkonfigurasi dengan ISL atau 802.1Q *trunking*. Ini memungkinkan semua VLAN untuk berkomunikasi melalui satu *interface*. Cisco menyebut istilah ini "router *on a stick*."



Gambar 2.23 Router Mengkoneksikan Semua VLAN Bersamaan
Melalui Satu *Interface* (*Router on a Stick*).
(Cisco ® Certified Network Associate Study Guide - Sixth Edition, Lammle, 2007, p568)

5. VLAN *Trunking Protocol* (VTP)

Tujuan dasar dari VLAN *Trunking Protocol* (VTP) adalah untuk mengelola semua VLAN yang dikonfigurasi di sebuah switch intrajaringan dan untuk menjaga konsistensi di seluruh jaringan, VTP memungkinkan untuk menambah, menghapus, dan mengubah nama VLAN yang informasinya kemudian disebarkan ke semua switch lain dalam VTP *domain*.

Berikut daftar dari beberapa fitur VTP yang ditawarkan:

- Konfigurasi VLAN yang konsisten di semua switch dalam jaringan.
- VLAN *trunking* melalui jaringan campuran, seperti *Ethernet* ke ATM LANE atau bahkan FDDI.
- Pelacakan dan pemantauan VLAN yang akurat.
- Pelaporan secara dinamis mengenai VLAN yang ditambahkan, ke semua switch dalam VTP *domain*.
- *Plug and Play* dalam penambahan VLAN.

Sebelum dapat menggunakan VTP untuk mengelola VLAN di seluruh jaringan, harus dibuat *server* VTP terlebih dahulu. *Server* yang dibutuhkan untuk berbagi informasi VLAN harus menggunakan nama

domain yang sama, dan switch harus terdapat di *domain* yang sama pada satu waktu. Jadi pada dasarnya, ini berarti bahwa switch hanya dapat berbagi informasi VTP *domain* dengan switch lain jika switch tersebut dikonfigurasi ke dalam *domain* VTP yang sama. Informasi VTP dikirim antara switch hanya melalui *trunk port*. Selain *server*, terdapat sebuah mode lain yang disebut mode transparan VTP. Di dalamnya, switch dapat dikonfigurasi untuk meneruskan informasi VTP melalui *port trunk* namun tidak menerima *update* informasi atau memperbarui *database* VTP.

Terdapat 3 persyaratan VTP untuk mengkomunikasikan informasi VLAN antara switch yaitu:

- Nama *domain* VTP manajemen dari kedua switch harus diatur sama.
- Salah satu switch harus dikonfigurasi sebagai VTP *server*.
- Tidak diperlukan sebuah router.

6. VTP *Modes of Operation*

- ***Server***: ini adalah mode *default* untuk semua switch Catalyst. Diperlukan setidaknya satu *server* di *domain* VTP untuk menyebarkan informasi VLAN di seluruh *domain* tersebut. Switch harus dalam mode *server* untuk dapat membuat, menambah, dan menghapus VLAN dalam *domain* VTP. Informasi VTP yang diubah pada mode *server*, dan setiap perubahan yang dibuat ke switch dalam mode *server* akan diperlihatkan ke seluruh *domain* VTP.

- ***Client***: dalam mode klien, switch tidak hanya menerima informasi dari *server* VTP, tetapi switch juga mengirim dan menerima *update*, sehingga dengan cara ini, switch berperilaku seperti *server* VTP. Perbedaannya adalah bahwa switch tidak dapat membuat, mengubah, atau menghapus VLAN. *Port* pada switch klien tidak dapat ditambahkan ke VLAN baru sebelum *server* VTP memberitahukan switch klien VLAN baru tersebut. Informasi VLAN yang

dikirim dari *server* VTP tidak disimpan pada NVRAM, yang berarti bahwa jika switch direset atau dimuat ulang, informasi VLAN akan dihapus. Jadi pada dasarnya, switch dalam mode klien VTP akan meneruskan ringkasan informasi VTP dan memprosesnya. Switch ini akan mempelajari informasi tanpa menyimpan konfigurasi VTP dalam konfigurasi berjalan, dan tidak akan menyimpannya pada NVRAM. Switch yang berada dalam mode klien VTP hanya akan mempelajari dan menyampaikan informasi VTP.

Transparan: Switch dalam mode transparan tidak turut serta dalam VTP *domain* atau berbagi *database* VLAN, namun switch akan meneruskan VTP *Advertisements* melalui konfigurasi *link trunk*. Mode ini dapat membuat, memodifikasi, dan menghapus VLAN karena terdapat *database* sendiri yang bersifat rahasia dari switch lain. Meskipun disimpan di NVRAM, *database* VLAN dalam mode transparan sebenarnya hanya berarti secara lokal. Seluruh tujuan dari mode transparan adalah agar memungkinkan *remote* switch untuk menerima *database* VLAN dari VTP *server* melalui switch yang tidak berpartisipasi dalam VLAN yang sama. VTP hanya mengetahui *normal-range* VLAN, yaitu ID VLAN 1-1005. VLAN dengan ID lebih besar dari 1005 disebut *extended-range* VLAN dan tidak disimpan dalam *database* VLAN. Switch harus dalam mode transparan VTP ketika membuat ID VLAN 1006-4094, sehingga akan sangat jarang penggunaan VLAN tersebut.

2.4 Pengukuran Kinerja *Sistem*

Parameter-parameter sistem yang akan dianalisis pada penelitian ini adalah sebagai berikut:

1. *Throughput*

   Throughput adalah kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data yang diukur dalam bps. Persamaan untuk menghitung *Throughput:*

$$Throughput = \frac{\text{Jumlah data yang dikirim } (bits)}{\text{Jumlah waktu pengiriman data } (sec)}$$

Nilai *Throughput* dari suatu jaringan dapat dikategorikan berdasarkan standarisasi TIPHON seperti pada tabel 2.1.

Tabel 2.1 Kategori Jaringan Berdasarkan Nilai *Throughput*

Kategori	Keberhasilan
Sangat Bagus	76 s/d 100 %
Bagus	51 s/d 75 %
Sedang	26 s/d 50 %
Buruk	< 25 %

2. *Latency* (*Delay*)

Latency (*Delay*) adalah lama waktu suatu paket yang diakibatkan oleh proses transmisi dari suatu titik ke titik lain yang menjadi tujuannya. Waktu tunda ini bisa dipengaruhi oleh jarak (misalnya akibat pemakaian satelit), atau kongesti (yang memperpanjang antrian), atau bisa juga akibat waktu olah yang lama (misalnya untuk *digitizing* dan kompresi data). Satuan yang digunakan pada perhitungan *delay* adalah *mili second* (ms).

Persamaan untuk menghitung *Delay:*

$$Delay = \frac{\text{Jumlah waktu pengiriman data (sec)}}{\text{Jumlah packet}}$$

Nilai *delay* dari suatu jaringan dapat dikategorikan berdasarkan standarisasi TIPHON seperti pada Tabel 2.2.

Tabel 2.2 Kategori Jaringan Berdasarkan Nilai *Delay*

Kategori	Besar *Delay*
Sangat Bagus	<150ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Buruk	> 450 ms

3. *Packet Loss*

Packet Loss adalah kegagalan transmisi paket data mencapai tujuannya. Umumnya perangkat *Network* memiliki *buffer* untuk menampung data yang diterima. Jika terjadi *kongesti* yang cukup lama, *buffer* akan penuh, dan data baru tidak diterima. Satuan yang digunakan pada perhitungan *packet loss* adalah persen. Persamaan untuk menghitung *Packet Loss:* Nilai *packet loss* dari suatu jaringan dapat dikategorikan berdasarkan standarisasi TIPHON seperti pada Tabel 2.3.

Tabel 2.3 Kategori jaringan berdasarkan nilai *packet loss*

Kategori	*Packet Loss*
Sangat Bagus	0 %
Bagus	3 %
Sedang	15 %
Buruk	25

2.5 Hasil Penelitian atau Produk Sebelumnya

Menurut Nurul Fadilah Zamzami dengan judul jurnal “IMPLEMENTASI LOAD BALANCING DAN FAILOVER MENGGUNAKAN MIKROTIK ROUTER OS BERDASARKAN MULTIHOMED *GATEWAY* PADA WARUNG INTERNET “DIGA” ” mengatakan bahwa tujuan penelitian ialah melakukan implementasi terhadap teknik penggabungan Load Balancing dan Failover dalam Multihomed *Gateway* menggunakan sistem operasi Mikrotik. Metode penelitian yang digunakan meliputi metode analisis (studi literatur), metode perancangan sistem, metode implementasi, metode pengujian, serta metode pembuatan laporan.

Hasil yang dicapai adalah apabila ip tersebut memakai jaringan lokal maka selanjutnya kita akan memutus jaringan yang ia gunakan. Apabila ip tersebut menggunakan jaringan isp yang lain atau dengan kata lain jaringan internasional maka hal tersebut dinyatakan telah sesuai begitupun sebaliknya. Kemudian setelah kita memutuskan jaringan sebaliknya maka setelah ditraceroute, jaringan akan kembali kepada salah satu jaringan yang up. Dan itu membuktikan bahwa hal ini telah berhasil. Simpulan dari penelitian ini adalah pada pengujian routing telah membuktikan bahwa *Gateway* kedua isp telah berhasil dipisahkan berdasarkan kebutuhan bandwidth lokal ataupun internasional. Dengan demikian tujuan penulis untuk memperoleh pemisahan jalur internet antara isp pertama dan kedua sesuai kebutuhan client dan dapat saling mem-backup antar isp telah tercapai.

Menurut Yogi Osadhani, Ibrahim Wijaya, dan Akhmad Sudomo Pratama dengan judul jurnal "Analisis dan Implementasi Teknik Failover dan Filtering Content pada PT. Budiman Sejahtera Development" mengatakan bahwa Tujuan penelitian ialah menganalisis dan mengimplementasikan teknik failover dan filtering content pada jaringan PT. Budiman Sejahtera Development menggunakan router mikrotik, sehingga jaringan pada PT. Budiman Sejahtera Development dapat bekerja lebih baik. Metode penelitian meliputi analisis berupa survei dan observasi terhadap sistem yang sedang berjalan, studi literatur serta melakukan interview kepada IT Engineer PT. Budiman Sejahtera Development. Hasil yang dicapai dari penelitian ini adalah rancangan topologi jaringan baru, penerapan teknik failover untuk memberikan backup link terhadap ISP utama, jika terjadi putus koneksi dan filtering content untuk membatasi akses terhadap situs tertentu. Simpulan dari penelitian ini adalah dengan menggunakan teknik failover terhadap dua jaringan internet, akan memberikan backup pada jalur koneksi internet utama. Sehingga saat jalur koneksi utama terputus, jalur cadangan akan langsung mem-backup secara otomatis, serta penerapan filtering content terhadap situs tertentu akan memberikan kinerja yang baik terhadap pegawai PT. Budiman Sejahtera Development.