

## BAB 2

### TINJAUAN PUSTAKA

#### 2.1 Jaringan Komputer

##### 2.1.1 Pengertian Jaringan Komputer

Jaringan dapat diartikan sebagai interkoneksi dari beberapa komputer. Komputer-komputer ini dapat dihubungkan secara bersama-sama untuk kepentingan yang berbeda dan menggunakan berbagai jenis kabel yang terpisah. Sehingga mengarah ke pengurangan pemakaian waktu dan meningkatnya produktifitas. (Pavani, Chandrika, Krishna, Vol.1, 2012)

Menurut Forouzan (2008,p7) Jaringan adalah seperangkat *devices* (biasanya disebut sebagai *nodes*) yang dihubungkan melalui *communication links*. Pada dasarnya tujuan daripada pembuatan jaringan adalah untuk:

1. Dapat menghemat *hardware* seperti berbagi pemakaian *printer* dan *CPU*.
2. Melakukan komunikasi, contohnya surat elektronik, *instant messaging*, *chatting*.
3. Mendapatkan akses informasi dengan cepat, contohnya *web browsing*.
4. Melakukan *sharing* data

Secara sederhana Jaringan Komputer mempunyai gambaran seperti berikut ini. Dua buah komputer atau lebih yang masing-masing memiliki kartu jaringan (*NIC=Network Interface Card*), kemudian dihubungkan dengan menggunakan kabel atau nirkabel sebagai media transmisi data. Dalam jaringan tersebut terdapat sebuah perangkat lunak (*software*) sistem operasi jaringan yang dapat menghubungkan komputer-komputer tersebut. Rangkaian sederhana seperti di atas sudah bisa dikatakan sebagai sebuah jaringan komputer, tentunya sebuah jaringan komputer yang sederhana. Setiap komputer atau perangkat jaringan yang terhubung dengan jaringan disebut *node*. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan *node*. Apabila ingin membuat

jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan seperti *Hub*, *Bridge*, *Switch*, *Router*, *Gateway* sebagai peralatan interkoneksinya.

Dengan adanya jaringan komputer ini banyak keuntungan yang akan kita dapatkan, contohnya pertukaran data antar komputer atau perangkat dalam sebuah jaringan, *sharing* perangkat, *sharing* program, dan lain sebagainya. Selain beberapa contoh di atas tentu masih banyak lagi kegunaan dari sebuah jaringan komputer.

### 2.1.2 Penggunaan Jaringan Komputer

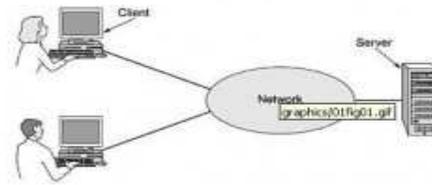
Menurut Tanenbaum (2006, p3, 9 Oktober 2013)

- **Aplikasi Bisnis**

Banyak perusahaan memiliki sejumlah besar komputer. Sebagai contoh, perusahaan mungkin memiliki komputer yang terpisah untuk memonitor produksi, melacak persediaan, dan melakukan daftar gaji. Awalnya, masing-masing komputer ini mungkin telah bekerja di isolasi dari yang lain, tetapi pada beberapa titik, manajemen mungkin telah memutuskan untuk menghubungkan mereka untuk dapat mengekstrak dan mengkorelasikan informasi tentang seluruh perusahaan.

Dalam istilah sederhana, seseorang dapat membayangkan sistem informasi perusahaan sebagai terdiri dari satu atau lebih *database* dan beberapa jumlah karyawan yang membutuhkan untuk mengaksesnya dari jarak jauh. Dalam model ini, data yang disimpan pada komputer yang kuat bernama *server*. Sebaliknya, karyawan yang memiliki mesin sederhana di meja mereka, disebut klien. Para mesin klien dan *server* dihubungkan oleh jaringan, seperti yang diilustrasikan pada Gambar. 2.1.

Figure 1-1. A network with two clients and one server.

**Gambar 2.1 Client – Server**

(Computer Networks, Andrew S. Tanenbaum, 2006, p4)

Pengaturan ini secara keseluruhan disebut model *client-server*. Hal ini banyak digunakan dan membentuk dasar penggunaan jaringan banyak. Hal ini berlaku ketika klien dan *server* keduanya di gedung yang sama (misalnya, berasal dari perusahaan yang sama), tetapi juga ketika mereka jauh terpisah. Sebagai contoh, ketika seseorang di rumah mengakses halaman di *World Wide Web*, model yang sama digunakan, dengan *Web server remote* sebagai *server* dan komputer pribadi pengguna menjadi klien. Dalam kondisi yang paling, satu *server* dapat menangani sejumlah besar klien.

Jika dilihat pada model *client-server* secara detail, bahwa dua proses yang terlibat, satu di mesin klien dan satu di mesin *server*. Komunikasi mengambil bentuk proses klien mengirim pesan melalui jaringan ke *server* proses. Proses klien kemudian menunggu pesan balasan. Ketika proses *server* mendapatkan permintaan tersebut, ia melakukan pekerjaan diminta atau mendongak data yang diminta dan mengirimkan kembali jawaban.

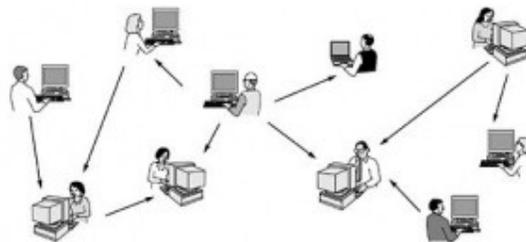
- **Home Aplikasi**

Mengapa komputer digunakan di rumah? Awalnya, untuk pengolah kata dan permainan, tetapi dalam beberapa tahun terakhir bahwa gambar telah berubah secara radikal.

Mungkin alasan terbesar sekarang adalah untuk akses Internet. Beberapa menggunakan lebih populer dari Internet untuk pengguna rumahan adalah sebagai berikut:

- Akses ke informasi jarak jauh.
- Komunikasi orang-ke-orang.
- Interaktif hiburan.
- *Electronic commerce*.

Tipe lain dari komunikasi orang-ke-orang sering disebut dengan nama komunikasi *peer-to-peer*, untuk membedakannya dari model *client-server*. Dalam bentuk ini, individu-individu yang membentuk kelompok longgar dapat berkomunikasi dengan orang lain dalam kelompok, seperti yang ditunjukkan pada Gambar. 2.2. Setiap orang pada prinsipnya dapat berkomunikasi dengan satu atau lebih orang lain, tidak ada pembagian tetap menjadi klien dan *server*.



**Gambar 2.2. Dalam sistem *peer-to-peer* tidak ada *client* dan *server* tetap.**

(Computer Networks, Andrew S. Tanenbaum, 2006, p7)

Kategori lainnya adalah perdagangan elektronik dalam arti luas. Belanja *online* sudah populer dan memungkinkan pengguna untuk memeriksa katalog *online* dari ribuan perusahaan. Beberapa katalog ini segera akan memberikan kemampuan untuk mendapatkan video instan pada produk apapun dengan hanya mengklik nama produk. Setelah pelanggan membeli produk elektronik tetapi

tidak tahu bagaimana menggunakannya, *online* dukungan teknis dapat dikonsultasikan.

Daerah lain di mana *e-commerce* sudah terjadi adalah akses ke lembaga keuangan. Banyak orang sudah membayar tagihan, mengelola rekening bank, dan menangani investasi secara elektronik. Ini pasti akan tumbuh sebagai jaringan yang lebih aman.

### 2.1.3 Manfaat Jaringan Komputer

Manfaat dari jaringan komputer itu sendiri adalah sebagai berikut :

1. *Resource sharing* , dapat menggunakan sumberdaya yang secara bersama-sama. Misalnya seorang pengguna yang berada di 100 Km jauhnya dari suatu data, tidak mendapatkan kesulitan dalam menggunakan data tersebut dan seolah olah data tersebut berada di dekatnya. Hal ini sering diartikan bahwa jaringan komputer mengatasi masalah jarak.

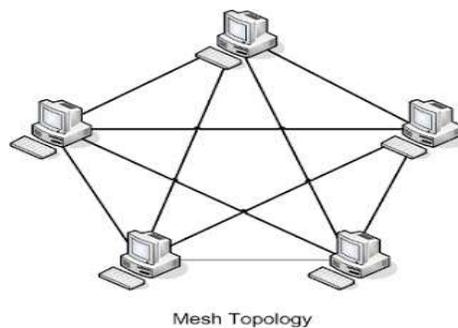
2. Reliabilitas tinggi, dengan jaringan komputer kita akan mendapatkan reliabilitas yang tinggi dengan memiliki sumber-sumber alternatif persediaan. Misalnya semua *file* dapat disimpan atau di *copy* ke dua, ketiga , atau lebih komputer yang terkoneksi ke jaringan. Sehingga bila satu mesin rusak maka salinan di mesin lain bisa digunakan.

3. Menghemat uang. Komputer berukuran kecil mempunyai rasio harga/kinerja yang lebih baik dibandingkan dengan komputer yang besar. Komputer besar seperti mainframe memiliki kecepatan kira – kira sepuluh kali lebih kecepatan komputer kecil/pribadi. Akan tetapi harga mainframe seribu kali lebih mahal dari komputer pribadi. Ketidak seimbangan rasio harga/kinerja inilah membuat para perancang sistem untuk membangun sistem yang terdiri dari komputer – komputer pribadi.

## 2.1.4 Topologi Jaringan

### 1. Topologi Jaringan *Mesh*

Topologi jaringan ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran harus disediakan untuk membentuk jaringan *Mesh* adalah jumlah sentral dikurangi 1 ( $n-1$ ,  $n$  = jumlah sentral). Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang. Dengan demikian disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.

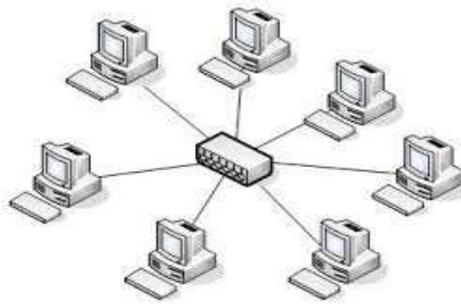


**Gambar 2.3 Topologi *Mesh***

<http://www.cs.umd.edu/cmssc411/proj01/pub/figure4.jpg>

### 2. Topologi Jaringan Bintang (*Star*)

Dalam topologi jaringan bintang, salah satu sentral dibuat sebagai sentral pusat. Bila dibandingkan dengan sistem *mesh*, sistem ini mempunyai tingkat kerumitan jaringan yang lebih sederhana sehingga sistem menjadi lebih ekonomis, tetapi beban yang dipikul sentral pusat cukup berat. Dengan demikian kemungkinan tingkat kerusakan atau gangguan dari sentral ini lebih besar.

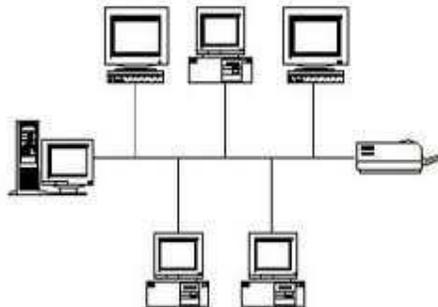


**Gambar 2.4 Topologi Star**

<http://4.bp.blogspot.com/-jUqOam1auw/T10yj2G9SkI/s320/topologi-star.jpg>

### 3. Topologi Jaringan *Bus*

Pada topologi ini semua sentral dihubungkan secara langsung pada media transmisi dengan konfigurasi yang disebut *Bus*. Transmisi sinyal dari suatu sentral tidak dialirkan secara bersamaan dalam dua arah. Topologi jaringan *bus* tidak umum digunakan untuk interkoneksi antar sentral, tetapi biasanya digunakan pada sistem jaringan komputer.

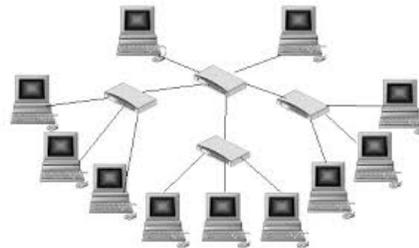


**Gambar 2.5 Topologi Bus**

[www.mattytv.com](http://www.mattytv.com)

#### 4. Topologi Jaringan Pohon (*Tree*)

Topologi jaringan 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 keatas mempunyai hirarki semakin tinggi.

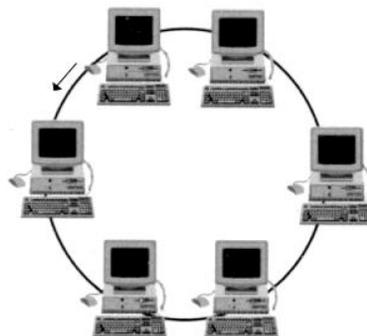


**Gambar 2.6 Topologi Jaringan Pohon(*tree*)**

(<http://jujex.files.wordpress.com/2012/03/topologi-tree.jpg>)

#### 5. Topologi Jaringan Cincin (*Ring*)

Untuk membentuk jaringan cincin, setiap sentral harus dihubungkan seri satu dengan yang lain dan hubungan ini akan membentuk *loop* tertutup. Dalam sistem ini setiap sentral harus dirancang agar dapat berinteraksi dengan sentral yang berdekatan maupun berjauhan. Dengan demikian kemampuan melakukan *switching* ke berbagai arah sentral.



**Gambar 2.7 Topologi Cincin (*Ring*)**

(<http://www.rudinazar.com/wp-content/uploads/2013/09/topologijaringanwarnet.jpg>)

## 2.2 OSI Layer

### 2.2.1 OSI Model

Menurut Iwan Sofana (2012,p92) Model OSI menjadi semacam referensi atau acuan bagi siapa saja yang ingin memahami cara kerja jaringan komputer. Walaupun OSI merupakan sebuah model yang diakui di sunia saat ini, namun tidak ada paksaan bagi pengembang *hardware/software* dan *user* untuk menggunakannya. Sedikit cerita terbentuknya OSI, pada tahun 1977 suatu *subcommittee* dari *International Organization for Standardization (ISO)* mulai bekerja untuk membuat beberapa set standart untuk memfasilitasi komunikasi jaringan. Pekerjaan ini selesai pada tahun 1984 dan dikenal sebagai model referensi OSI – *Open System Interconnection*. Model OSI ini merupakan metoda yang paling luas digunakan untuk menjelaskan komunikasi jaringan. Seksi berikut mencakup topik-topik: Model OSI membagi tugas-tugas jaringan kedalam 7 *layer*.

### 2.2.2 Tujuh Layer OSI

OSI model dibuat dengan tujuan agar komunikasi data dapat berjalan melalui langkah langkah yang jelas, langkah-langkah ini biasa disebut dengan nama “*layer*” dan Model OSI terdiri dari tujuh *layer* dengan pembagian tugas yang jelas, ke tujuh *layer* itu adalah:

7. *Aplication*

6. *Presentation*

5. *Session*

4. *Transport*

3. *Network*

2. *Data-Link*

1. *Physical*

### 2.2.3 Fungsi Layer

Struktur tujuh lapis model OSI, bersamaan dengan *protocol data unit* pada setiap lapisan :

1. *Physical Layer*

Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti *ethernet*), topologi jaringan dan pengabelan. Selain itu, *level* ini juga mendefinisikan bagaimana *Network Interface Card (NIC)* dapat berinteraksi dengan media kabel atau radio.

2. *Data/Link Layer*

Berfungsi untuk menentukan bagaimana *bit-bit* data dikelompokkan menjadi format yang disebut sebagai *frame*. Selain itu, pada *level* ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya *Media Access Control Address (MAC Address)*), dan menentukan bagaimana perangkat-perangkat jaringan seperti *hub*, *bridge*, *repeater*, dan *switch layer 2* beroperasi. Spesifikasi *IEEE 802*, membagi *level* ini menjadi dua *level* anak, yaitu lapisan *Logical Link Control (LLC)* dan lapisan *Media Access Control (MAC)*

3. *Network Layer*

*Network Layer* berfungsi mengontrol operasi dari subnet dan untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan *routing* melalui *internet working* dengan menggunakan *router*.

4. *Transport Layer*

Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada *level* ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (*acknowledgement*), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.

#### 5. *Session Layer*

Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di *level* ini juga dilakukan resolusi nama.

#### 6. *Presentation Layer*

Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam *level* ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam *Windows NT*) dan juga *Network shell*.

#### 7. *Application Layer*

Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.

### 2.2.4 Tujuan Paket Data

Berdasarkan tujuan paket data pada jaringan komputer, maka ada 3 macam pembagian, yaitu :

#### 1. *Broadcast*

*Broadcast* pada jaringan komputer, merupakan jenis paket yang berasal dari satu titik, dan memiliki tujuan ke semua titik lain yang ada di jaringan. Biasanya jenis paket *broadcast* akan dikirimkan untuk menyatakan suatu berita, atau pencarian sebuah titik pada jaringan.

## 2. *Unicast*

*Unicast* merupakan jenis paket yang berasal dari satu titik, dan memiliki tujuan hanya satu titik yang lain (titik bisa berarti komputer, atau peralatan jaringan lainnya). *Unicast* memiliki satu *MAC address* pengirim, dan satu *MAC address* penerima. Dalam kehidupan sehari – hari, pada saat *browsing* Internet, hal ini sudah melakukan proses *unicast*.

## 3. *Multicast*

*Multicast* merupakan jenis paket yang berasal dari satu buah titik dan bertujuan ke sebuah alamat khusus (bukan titik khusus), di mana alamat khusus ini dapat diketahui oleh titik-titik lain di jaringan yang berkepentingan untuk mengetahuinya.

### **2.2.5 Broadcast Domain dan Collision Domain**

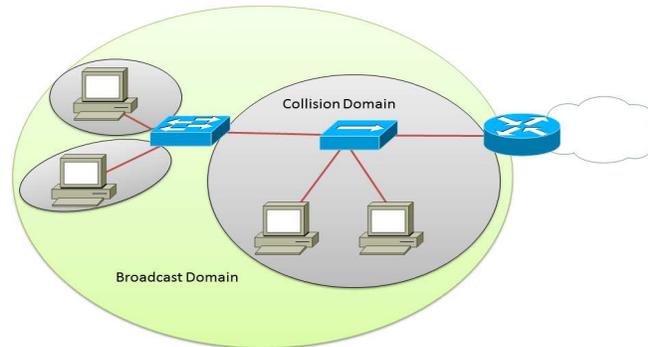
#### a. *Broadcast Domain*

*Broadcast Domain* secara umum dapat didefinisikan sebagai daerah atau wilayah dimana semua *device* atau perangkat di dalamnya dapat mengetahui sinyal yang berasal dari perangkat network tertentu yang berada dalam satu segmen. Sebuah divisi logis dari sebuah jaringan komputer, di mana semua *node* dapat mencapai atau terhubung satu sama lain dengan *broadcast* pada lapisan *data link layer*.

#### b. *Collision Domain*

*Collision Domain* adalah segmen jaringan fisik (*physical*) di mana paket data dapat bertabrakan dengan satu sama lain ketika dikirim pada medium bersama, khususnya, bila menggunakan protokol jaringan *Ethernet*. Sebuah tabrakan data pada jaringan terjadi ketika lebih dari satu untuk mengirim paket pada segmen jaringan pada waktu yang sama.

Situasi ini biasanya ditemukan dalam lingkungan *hub* dimana setiap *segmen host* terhubung ke sebuah *hub* yang merepresentasikan hanya satu *collision domain* dan hanya satu *broadcast domain*.



**Gambar 2.8 Daerah *Broadcast* dan *Collision Domain***

<http://systemstechblog.files.wordpress.com/2011/02/broadcast-domain.png>

### 2.3 Network Devices

- *Modem*

*Modem* berasal dari singkatan *Modulator Demodulator*. *Modulator* merupakan bagian yang merubah sinyal informasi ke dalam sinyal pembawa (*currier*), dan siap untuk dikirimkan, sedangkan *demodulator* merupakan bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik



**Gambar 2.9 *Modem***

([http://4.bp.blogspot.com/-fwSWy9H6S\\_0/TD-W8901G-02.jpg](http://4.bp.blogspot.com/-fwSWy9H6S_0/TD-W8901G-02.jpg))

- *Hub*

*Hub* merupakan suatu perangkat pada jaringan yang beroperasi pada *layer 1* (*Physical Layer*). *Hub* tidak menyaring dan menerjemahkan sesuatu, hanya mengetahui kecepatan *transfer* data. *Hub* juga melakukan penguatan sinyal.



**Gambar 2.10 Hub**

[http://www.anugrahpratama.com/published/tp-link-switch-hub-tl-sg1008d-gigabit\\_enl.jpg](http://www.anugrahpratama.com/published/tp-link-switch-hub-tl-sg1008d-gigabit_enl.jpg)

- *Switch*

*Switch* merupakan suatu perangkat pada jaringan yang berada pada *layer 2* (*Data Link Layer*) dan sebagian berada pada *layer 3* (*Network Layer*) juga. *Switch* yang mampu melakukan manajemen *transfer* data yaitu hanya meneruskan data ke segmen yang dituju. *Switch* tidak melakukan konversi format data. Ketika paket data dikirimkan melalui salah satu *port* pada *switch*, maka pengiriman paket data tersebut tidak akan terlihat dan tidak terkirim ke setiap port lainnya. Sehingga masing-masing port mempunyai *bandwidth* yang penuh. Ini menyebabkan kecepatan transfer data lebih terjamin. Dengan terjadinya perkembangan teknologi sekarang ini *switch* tidak hanya dapat beroperasi pada *layer 2* saja. *Switch* dapat beroperasi pada *layer 3* yaitu *manageable switch*. *Manageable switch* memiliki *web-based interface* untuk memonitoring dan akses yang aman untuk setiap port yang ada dalam *switch* tersebut. *Manageable port* dapat menggunakan *VLAN*, dimana dapat membuat banyak port yang berbeda dalam satu *switch* yang sama atau *switch* yang berbeda. *Manageable switch* juga

dapat digunakan untuk mengaktifkan atau menonaktifkan port tertentu tanpa harus mencabut kabel. Switch tersebut dapat berfungsi seperti router.



**Gambar 2.11 Switch**

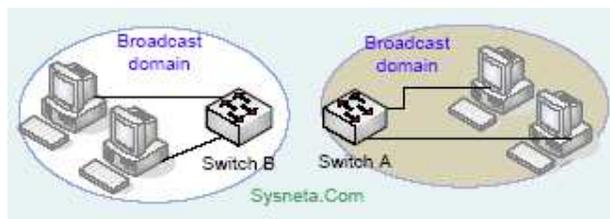
<http://uk.tp-link.com/resources/images/products/large/TL-SF1008D-4.jpg>

## **2.4 VLAN**

### **2.4.1 Pengertian VLAN**

#### **Virtual Local Area Network**

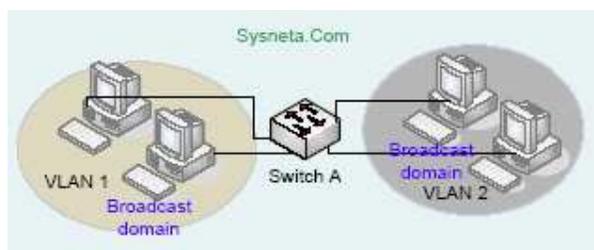
Menurut Iwan Sofana (2008,p174) VLAN disebut “mirip” dengan *subnetwork* karena tujuannya sama, yaitu membuat kelompok atau grup yang terdiri atas beberapa komputer atau perangkat jaringan. VLAN (Virtual Local Area Network) adalah suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN ,hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel karena dapat dibuat segmen yang bergantung pada organisasi, tanpa bergantung lokasi workstations. Dengan kata lain VLAN mengurangi collision dan mempermudah menejemen network.



**Gambar 2.12 Virtual Local Area Network**

<http://www.jaringan-komputer.cv-sysneta.com/2009/10/virtual-lan-trunking.jpg>

Dua buah Switch membentuk dua *broadcast domain* berbeda, tanpa VLAN. Secara alternatif, beberapa *broadcast domain* dapat dibuat dengan menggunakan sebuah *Switch* tunggal. Seperti gambar diatas, gambar dibawah ini menunjukkan dua buah *broadcast domain* yang sama akan tetapi diimplementasikan sebagai dua VLAN yang berbeda pada sebuah *Switch* tunggal.



**Gambar 2.13 Virtual Area Network**

<http://www.jaringan-komputer.cv-sysneta.com/2009/10/virtual-lan-trunking.jpg>

Beberapa *broadcast domain* dapat dibuat dengan menggunakan sebuah *Switch* tunggal. Untuk sebuah jaringan LAN kecil misal dirumahan atau dikantoran kecil, tidak ada alasan untuk membuat VLAN. Akan tetapi ada beberapa motivasi untuk membuat VLAN yang meliputi alasan berikut ini:

1. Untuk mengelompokkan user berdasarkan departemen, atau mengelompokkan suatu group pekerja kolaborasi, ketimbang berdasarkan lokasi.
2. Untuk menurangi *overhead* dengan membatasi ukuran *broadcast domain*
3. Untuk menekankan keamanan yang lebih baik dengan menjaga piranti-piranti sensitif terpisah kedalam suatu VLAN

Untuk memisahkan *traffic* khusus dari *traffic* utama – misalkan memisahkan IP telepon kedalam VLAN khusus terpisah dari *traffic* user.

Virtual LAN atau VLAN memungkinkan para ahli jaringan dan administrator jaringan untuk membuat jaringan *logical network* dari *physical network*. Teknologi ini digunakan untuk segmentasi jaringan yang kompleks kedalam jaringan yang lebih kecil untuk kemampuan manajemen yang lebih baik, meningkatkan performa dan keamanan. VLAN secara *logical* membuat segmen – segmen dengan menggunakan switch berdasarkan fungsi – fungsi organisasi seperti departemen atau letak geografisnya. Oleh karena itu mengimplementasikan VLAN untuk suatu jaringan akan mendapatkan keuntungan sebagai berikut :

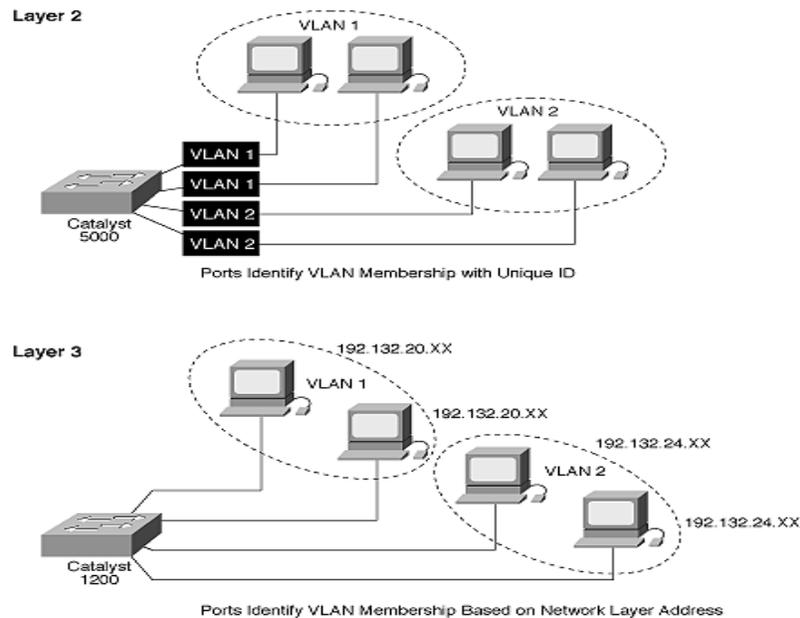
- Mudah merelokasi PC pada LAN
- Mudah menambah atau menghapus host ke LAN atau dari LAN
- Mudah memodifikasi konfigurasi LAN
- Mudah mengontrol lalu lintas jaringan antar LAN
- Meningkatkan keamanan jaringan
- Mudah mengelola administrasi jaringan

(Mohaned Al-Obaidy, JITBM & ARF Vol 4, 2012)

Dengan memanfaatkan berbagai teknik khususnya teknik *subnetting* dan penggunaan hardware yang lebih baik (antara lain *switch*) maka muncullah konsep *Virtual Local Area Network* (VLAN) yang diharapkan dapat memberikan hasil yang lebih baik dibanding *Local Area Network* (LAN).

Pengertian VLAN Merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN , hal ini mengakibatkan suatu network dapat dikonfigurasi secara *virtual* tanpa harus menuruti lokasi fisik peralatan.

Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi *workstation* seperti pada gambar pada halaman selanjutnya :



**Gambar 2.14 VLAN**

<http://emulanetwork.files.wordpress.com/2011/01/vlan-subnet-based.gif>

## 2.4.2 Inter VLAN

Menurut Iwan Sofana (2012,p536) VLAN tanpa menggunakan inter VLAN routing masih belum terlalu bermanfaat sebab masing-masing VLAN tidak dapat berkomunikasi dengan VLAN lain. Di sinilah peranan router. Router dapat menghubungkan beberapa *subnet* yang berbeda.

### *InterVLAN routing*

*InterVLAN routing* adalah proses mem-forward traffic network dari satu VLAN ke VLAN lain menggunakan router. VLAN diasosiasikan dengan ip subnet yang unik pada network. Konfigurasi subnet akan memfasilitasi proses routing pada lingkungan beberapa VLAN. Ketika kita menggunakan router untuk memfasilitasi inter-VLAN routing, interface pada router dapat

dihubungkan dengan VLAN yang berbeda. Setiap *device* pada VLAN tersebut mengirimkan *traffic* melalui *router* untuk mencapai VLAN lain.

Inter-VLAN *routing* secara tradisional mengharuskan beberapa *interface physical* pada kedua *router* dan *switch*. Bagaimanapun juga, tidak semua konfigurasi inter-VLAN *routing* mengharuskan beberapa *physical interface*. Beberapa *router software* memperbolehkan konfigurasi *router* sebagai link *trunk*. Hal ini membuka kemungkinan terjadinya inter-VLAN *routing*. *Router on a stick* adalah salah satu jenis konfigurasi *router* yang mana sebuah *interface physical* me-*routing traffic* antara beberapa VLAN pada *network*. *Router interface* dikonfigurasi untuk beroperasi sebagai *link trunk* dan terhubung dengan sebuah *port switch* dalam mode *trunk*. *Router* menunjukkan inter-VLAN *routing* dengan menerima *traffic* VLAN yang telah di tag pada *interface* trunk dari *switch* dan secara internal me-*routing* antar VLAN menggunakan *sub-interface*. Kemudian *router* akan mem-*forward traffic* VLAN yang di tag menuju VLAN tujuan pada *interface physical* yang sama. *Sub-interface* adalah beberapa *interface virtual* yang diasosiasikan dengan *interface physical*. *Sub-interface* ini dikonfigurasi dengan *software* pada *router* yang secara independent dikonfigurasi dengan *ip address* dan VLAN untuk beroperasi pada VLAN tertentu. *Sub-interface* dikonfigurasi untuk beberapa subnet yang berbeda namun berhubungan dengan VLAN lain yang memfasilitasi *routing* secara *logical* sebelum *frame data* di tag VLAN dan dikirimkan ke *physical interface*

### 2.4.3 Jenis – jenis VLAN

Keanggotaan dalam suatu VLAN dapat di klasifikasikan berdasarkan *port* yang di gunakan, *MAC address*, tipe protokol.

#### 1. Berdasarkan *Port*

Keanggotaan pada suatu VLAN dapat di dasarkan pada *port* yang di gunakan oleh VLAN tersebut. Sebagai contoh, pada *switch* dengan 4 *port*, *port* 1, 2, dan 4 merupakan VLAN 1 sedang *port* 3 dimiliki oleh VLAN 2, lihat tabel: Tabel *port* dan VLAN.

*Port 1 2 3 4*

*VLAN 2 2 1 2*

Kelemahannya adalah *user* tidak bisa untuk berpindah pindah, apabila harus berpindah maka Network administrator harus mengkonfigurasi ulang.

## 2. Berdasarkan MAC Address

Keanggotaan suatu VLAN didasarkan pada MAC *address* dari setiap *workstation*/komputer yang dimiliki oleh *user*. *Switch* mendeteksi/mencatat semua MAC *address* yang dimiliki oleh setiap Virtual LAN. MAC *address* merupakan suatu bagian yang dimiliki oleh NIC (*Network Interface Card*) di setiap *workstation*.

Kelebihannya apabila *user* berpindah pindah maka dia akan tetap terkonfigurasi sebagai anggota dari VLAN tersebut. Sedangkan kekurangannya bahwa setiap mesin harus di konfigurasi secara manual, dan untuk jaringan yang memiliki ratusan *workstation* maka tipe ini kurang efisien untuk dilakukan.

Tabel MAC *address* dan VLAN

MAC <i>address</i>	132516617738	272389579355	536666337777	24444125556
VLAN	1	2	2	1

## 3. Berdasarkan tipe protokol yang digunakan

Keanggotaan VLAN juga bisa berdasarkan protokol yang digunakan, lihat table. Tabel Protokol dan VLAN

Protokol	IP	IPX
VLAN	1	2

#### 4. Berdasarkan Alamat Subnet IP

Subnet IP *address* pada suatu jaringan juga dapat digunakan untuk mengklasifikasi

suatu VLAN. Tabel IP Subnet dan VLAN

IP subnet	22.3.24	46.20.45
VLAN	1	2

Konfigurasi ini tidak berhubungan dengan routing pada jaringan dan juga tidak memperlakukan fungsi *router*. IP *address* digunakan untuk memetakan keanggotaan VLAN. Keuntungannya seorang *user* tidak perlu mengkonfigurasi ulang alamatnya di jaringan apabila berpindah tempat, hanya saja karena bekerja di layer yang lebih tinggi maka akan sedikit lebih lambat untuk meneruskan paket di banding menggunakan MAC *addresses*.

#### 5. Berdasarkan aplikasi atau kombinasi lain

Sangat dimungkinkan untuk menentukan suatu VLAN berdasarkan aplikasi yang dijalankan, atau kombinasi dari semua tipe di atas untuk diterapkan pada suatu jaringan. Misalkan: aplikasi FTP (*file transfer protocol*) hanya bias digunakan oleh VLAN 1 dan Telnet hanya bisa digunakan pada VLAN 2.

### 2.4.5 Perbandingan VLAN dan LAN

Penggunaan LAN telah memungkinkan semua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Kerjasama ini semakin berkembang dari hanya pertukaran data hingga penggunaan peralatan secara bersama (*resource sharing* atau disebut juga *hardware sharing*).<sup>10</sup> LAN memungkinkan data tersebar secara *broadcast* keseluruh jaringan, hal ini akan mengakibatkan mudahnya pengguna yang tidak dikenal (*unauthorized user*) untuk dapat mengakses semua bagian dari *broadcast*.

Semakin besar *broadcast*, maka semakin besar akses yang didapat, kecuali hub yang dipakai diberi fungsi kontrol keamanan.

VLAN yang merupakan hasil konfigurasi *switch* menyebabkan setiap *port switch* diterapkan menjadi milik suatu VLAN. Oleh karena berada dalam satu segmen, *port-port* yang bernaung dibawah suatu VLAN dapat saling berkomunikasi langsung. Sedangkan *port-port* yang berada di luar VLAN tersebut atau berada dalam naungan VLAN lain, tidak dapat saling berkomunikasi langsung karena VLAN tidak meneruskan *broadcast*.

VLAN yang memiliki kemampuan untuk memberikan keuntungan tambahan dalam hal keamanan jaringan tidak menyediakan pembagian/penggunaan media/data dalam suatu jaringan secara keseluruhan. *Switch* pada jaringan menciptakan batas-batas yang hanya dapat digunakan oleh komputer yang termasuk dalam VLAN tersebut. Hal ini mengakibatkan administrator dapat dengan mudah mensegmentasi pengguna, terutama dalam hal penggunaan media/data yang bersifat rahasia (*sensitive information*) kepada seluruh pengguna jaringan yang tergabung secara fisik.

Keamanan yang diberikan oleh VLAN meskipun lebih baik dari LAN, belum menjamin keamanan jaringan secara keseluruhan dan juga belum dapat dianggap cukup untuk menanggulangi seluruh masalah keamanan .VLAN masih sangat memerlukan berbagai tambahan untuk meningkatkan keamanan jaringan itu sendiri seperti *firewall*, pembatasan pengguna secara akses perindividu, *intrusion detection*, pengendalian jumlah dan besarnya *broadcast* domain, enkripsi jaringan, dsb.

Dukungan Tingkat keamanan yang lebih baik dari LAN inilah yang dapat dijadikan suatu nilai tambah dari penggunaan VLAN sebagai sistem jaringan. Salah satu kelebihan yang diberikan oleh penggunaan VLAN adalah control administrasi secara terpusat, artinya aplikasi dari manajemen VLAN dapat dikonfigurasi, diatur dan diawasi secara terpusat, pengendalian *broadcast* jaringan, rencana perpindahan, penambahan, perubahan dan pengaturan akses khusus ke dalam jaringan serta mendapatkan media/data yang memiliki fungsi penting dalam perencanaan dan administrasi di dalam grup tersebut semuanya

dapat dilakukan secara terpusat. Dengan adanya pengontrolan manajemen secara terpusat maka administrator jaringan juga dapat mengelompokkan grup-grup VLAN secara spesifik berdasarkan pengguna dan *port* dari *switch*. Yang digunakan, mengatur tingkat keamanan, mengambil dan menyebar data melewati jalur yang ada, mengkonfigurasi komunikasi yang melewati *switch*, dan memonitor lalu lintas data serta penggunaan *bandwidth* dari VLAN saat melalui tempat-tempat yang rawan di dalam jaringan.

