BAB II

LANDASAN TEORI

2.1. Pengertian Jaringan Komputer

Menurut Iwan sofana (2008:3), yang dimaksud dengan jaringan komputer (*computer networks*) adalah suatu himpunan interkoneksi sejumlah komputer *autonomus*. Dalam bahasa yang popular dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *printer, hub*, dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (nirkabel). Informasi berupa data akan mengalir dari satu komputer ke komputer lainya atau dari satu komputer ke perangkat lain, sehingga masing – masing komputer yang terhubung tersebut bisa saling bertukar data atau berbagi perangkat keras.

Untuk memudahkan memahami jaringan komputer, para ahli kemudian membagi jaringan komputer berdasarkan klasifikasi, diantaranya :

2.1.1. Berdasarkan Area atau Skala

Berdasarkan skala atau area, jaringan komputer dapat dibagi menjadi empat (4) jenis, yaitu :

1. LAN (*Local Area Network*)

Local Area Network merupakan jaringan lokal yang dibuat pada area tertutup. Misalkan dalam satu gedung atau dalam satu ruangan. Kadangkala jaringan lokal

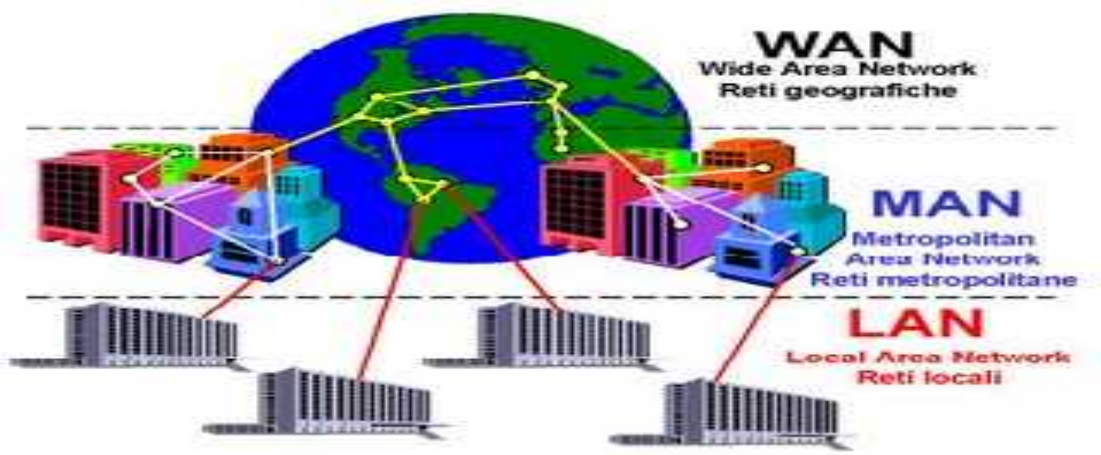
disebut juga jaringan *privat*. LAN biasa digunakan untuk jaringan kecil yang menggunakan *resource* bersama-sama, seperti penggunaan *printer* secara bersama, penggunaan media penyimpanan secara bersama (Iwan sofana, 2008:4).

2. MAN (*Metropolitan Area Network*)

Metropolitan Area Network menggunakan metode yang sama dengan LAN namun daerah cakupanya lebih luas. Daerah cakupan MAN bisa satu RW, beberapa kantor yang berbeda dalam komplek yang sama, satu kota bahkan satu provinsi. Dapat dikatakan MAN merupakan pengembangan dari LAN (Iwan sofana, 2008:4)

3. WAN (*Wide Area Network*)

Wide Area Network cakupanya lebih luas daripada MAN. Cakupan WAN meliputi satu kawasan, satu Negara, satu pulau, bahkan satu benua. Metode yang digunakan WAN hampir sama dengan LAN dan MAN (Iwan sofana, 2008:4).



Sumber: https://aiiumirror.com/2013/04/20/jaringan-komputer (20 april 2016)

Gambar II.1
Jenis Jaringan Komputer Berdasarkan Area

4. Internet

Internet merupakan interkoneksi jaringan-jaringan komputer yang ada di dunia. Sehingga cakupanya sudah mencapai satu planet, bahkan tidak menutup kemungkinan mencangkup antarplanet. Koneksi antar jaringan komputer dapat dilakukan berkat dukungan protokol yang khas, yaitu *Internet Protocol (IP)* (Iwan sofana, 2008:5).

Tabel di bawah dapat digunakan untuk sekedar memberikan gambaran kira-kira luas area LAN, MAN, WAN dan Internet.

Tabel II.1.

Jangkauan Jaringan Komputer Berdasarkan Area

Jarak / Cakupan (meter)	**Contoh**	**Jenis**
10 s/d 100	Ruangan	LAN
100 s/d 1000	Gedung	LAN
1000 s/d 10.000	Kampus	LAN
10.000 s/d 100.000	Kota	MAN
100.000 s/d 1.000.000	Negara	WAN
1.000.000 s/d 10.000.000	Benua	WAN
>10.000.000	Planet	*Internet*

Sumber : Membangun Jaringan Komputer (Iwan sofana, 2008:5)

Istilah seperti SAN, PAN, CAN secara garis besar, jenis – jenis jaringan tersebut masih dapat dikelompokan dalam LAN, MAN, WAN dan Internet. Hanya saja layanan yang disediakan bermacam – macam, sehingga dibuat istilah – istilah tertentu untuk membedakanya dengan yang lain.

2.1.2. Berdasarkan Media Penghantar

Berdasarkan media penghantar, jaringan komputer dapat dibagi menjadi dua (2) jenis, yaitu :

1. Wire Network

Wire Network merupakan jaringan komputer yang menggunakan kabel sebagai media penghantar. Jadi, data mengalir pada kabel. Kabel yang umum digunakan pada jaringan komputer biasanya menggunakan bahan dasar tembaga. Ada juga jenis kabel lain yang menggunakan bahan jenis fiber optik atau serat optik. Biasanya bahan tembaga banyak digunakan pada LAN. Sedangkan untuk MAN atau WAN menggunakan gabungan kabel tembaga dan serat optik (Iwan sofana, 2008:6).

2. Wireless Network

Wireless Network merupakan jaringan tanpa kabel yang menggunakan media penghantar gelombang radio atau cahaya *infrared.* Saat ini sudah semakin banyak outlet atau lokasi tertentu yang menyediakan layanan *wireless network*. Sehingga pengguna dapat dengan mudah melakukan akses *Internet* tanpa kabel. Frekuensi yang digunakan pada radio untuk jaringan komputer biasanya menggunakan frekuensi tinggi, yaitu 2.4 GHz dan 5.8 GHz. Sedangkan penggunaan *infrared* umumnya hanya terbatas untuk jenis jaringan yang hanya melibatkan dua buah komputer saja atau disebut *point to point*. Hal ini menyebabkan *infrared* tidak sepopuler gelombang radio (Iwan sofana, 2008:6).

2.1.3. Berdasarkan Fungsi

Berdasarkan fungsinya, jaringan komputer dapat dibagi menjadi dua (2) jenis, yaitu :

1. *Client Server*

Client Server merupakan jaringan komputer yang salah satu (boleh lebih) komputer difungsikan sebagai *server* atau induk bagi komputer lain. Server melayani komputer lain yang disebut client. Layanan yang diberikan bisa berupa akses *Web, e-mail,* file, atau yang lain. *Client server* banyak dipakai pada *Internet.* Namun LAN atau jaringan lain pun bisa mengimplementasikanya *client server*. Hal ini sangat bergantung pada kebutuhan masing-masing (Iwan sofana, 2008:6).

2. *Peer to Peer*

Peer to peer merupakan jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client.* Setiap komputer dapat menerima dan memberikan *acces* dari atau ke komputer lain. *Peer to peer* banyak diimplementasikan pada LAN. Walaupun dapat juga diimlementasikan pada MAN, WAN, atau *Internet*, namun hal ini kurang lazim. Salah satu alasanya adalah masalah manajemen dan *security*. Sulit sekali menjaga *security* pada jaringan *peer to peer* manakala pengguna komputer sudah sangat banyak (Iwan sofana, 2008:6).

2.2. Topologi

Topologi merupakan suatu aturan/rules bagaimana menghubungkan komputer (*node*) satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi melalui media/peralatan jaringan, seperti *server, workstation,*

hub/switch dan pengkabelanya (media transmisi data). Ketika kita memutuskan untuk memilih suatu topologi maka kita perlu mengikuti beberapa speseifikasi tertentu (Iwan sofana, 2008:7).

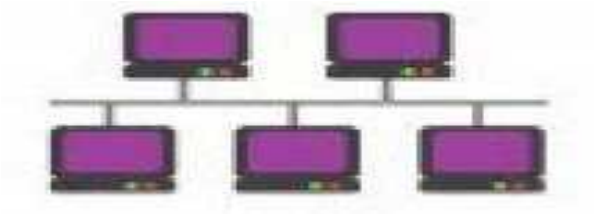
Ada dua jenis topologi, yaitu *physical topology* (topologi fisik) dan *logical topology* (topologi logika). Topologi fisik berkaitan dengan *layout* atau bentuk jaringan, seperti bagaimana memilih perangkat dan melakukan instalasi perangkat jaringan. Sedangkan topologi logika berkaitan dengan bagaimana data mengalir di dalam topologi fisik. Jika topologi fisik bagaikan tubuh maka topologi logika dapat diibaratkan seperti darah yang mengalir dalam tubuh.

2.2.1. Topologi Fisik (*Physical Topology*)

Topologi (fisik) komputer dapat juga digunakan untuk mempermudah memahami jaringan komputer. Beberapa jenis topologi jaringan fisik antara lain :

1. Topologi *Bus*

Topologi *bus* sering disebut juga *daisy chain* atau *Ethernet bus topologie*. Sebutan terakhir diberikan karena pada topologi *bus* digunakan perangkat jaringan atau *network interface card* (NIC) bernama *Ethernet*. Jaringan yang menggunakan topologi *bus* dapat dikenali dari penggunaan sebuah kabel *backbone* (kabel utama) yang menghubungkan semua peralatan jaringan (*device*). Karena kabel *backbone* menjadi satu-satunya jalan bagi lalulintas data maka apabila kabel *backbone* rusak atau terputus akan menyebabkan jaringan mati total (Iwan sofana, 2008:9).



Sumber : http://kelipet.com/2015/09/macam-macam-topologi-jaringan-komputer/ (20 april 2016)

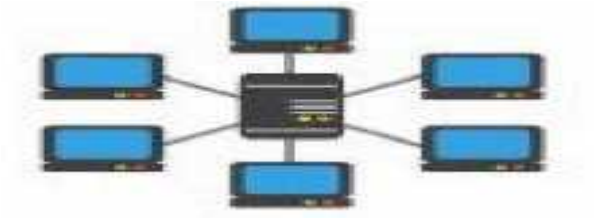
Gambar II.2
Topologi *Bus*

Beberapa karakteristik jaringan topologi *bus* antara lain :

a. Menggunakan sebuah kabel *backbone* untuk transmisi data;
b. Kabel yang digunakan berjenis *coaxial* dan berpelindung menggunakan shield. Ada juga yang mengembangkan jaringan bus menggunakan kabel *twisted pair*;
c. Ujung – ujung kabel *backbone* harus ditutup dengan terminator;
d. Jika satu atau lebih *node crash* tidak akan menyebabkan jaringan lumpuh;
e. Sering terjadi banjir data dan *collision* (tabrakan data) sehingga dapat menurunkan performa jaringan;
f. Sederhana, hemat biaya, serta mudah diimplementasikan pada jaringan berskala kecil.

2. Topologi *Star*

Topologi *star* dikenali dengan keberadaan sebuah sentral berupa *hub* yang menghubungkan ke semua *node*. Setiap *node* menggunakan sebuah kabel UTP atau STP yang dihubungkan dari *Ethernet card* ke *hub* (Iwan sofana, 2008:31).



Sumber : http://kelipet.com/2015/09/macam-macam-topologi-jaringan-komputer/ (20 april 2016)

Gambar II.3
Topologi *Star*

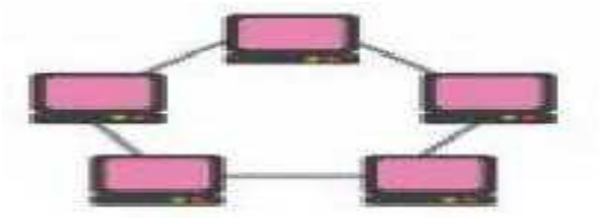
Beberapa karakteristik jaringan topologi *star* antara lain :

a. Menggunakan sentral berupa *hub* atau *switch*;
b. Kabel yang digunakan berjenis STP atau UTP;
c. Jika salah satu segmen kabel putus maka hanya segmen itu saja yang lumpuh, sementara yang lainya dapat berfungsi;
d. Jika *hub* atau sentral rusak maka jaringan akan lumpuh;
e. Data mengalir pada kabel secara bolak-balik;
f. Sering terjadi banjir data dan *collision* (tabrakan data) sehingga dapat menurunkan performa jaringan. Namun hal ini dapat diantisipasi oleh *switch* yang dapat mengatur lalulintas data sehingga kecepatan maksimal dapat tercapai;
g. Relative lebih mahal dibandingkan topologi *bus*, namun proses instalasi mudah dan cocok diimplementasikan pada jaringan berskala kecil maupun besar.

3. Topologi *Ring*

Topologi *ring* sangat berbeda dengan topologi *bus*. Sesuai dengan namanya, jaringan yang menggunakan topologi ini dapat dikenali dari kabel *backbone* yang

membentuk cincin. Setiap komputer terhubung dengan kabel *backbone*. Setelah sampai pada komputer terakhir maka ujung kabel akan kembali disambungkan dengan komputer pertama (Iwan sofana, 2008:21).



Sumber : http://kelipet.com/2015/09/macam-macam-topologi-jaringan-komputer/ (20 april 2016)

Gambar II.4
Topologi *Ring*

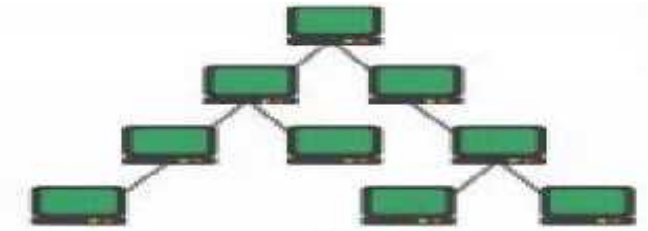
Beberapa karakteristik jaringan topologi *ring* antara lain :

a. Menggunakan sebuah kabel *backbone* untuk transmisi data;
b. Kabel yang digunakan jenis *twisted pair*;
c. Ujung-ujung kabel *backbone* akan dihubungkan dengan node pertama sehingga membentuk cincin atau lingkaran tertutup;
d. Jika kabel putus atau node rusak maka jaringan akan lumpuh;
e. Pengiriman data menggunakan metode *token passing scheme* dan dilakukan secara bergantian pada satu arah saja;
f. Rumit dan relative mahal jika diimplementasikan pada jaringan kecil;

4. Topologi *Tree*

Topologi *tree* disebut juga topologi *star-bus* atau *star/bus hybrid*. Topologi *tree* merupakan gabungan beberapa topologi *star* yang dihubungkan dengan topologi *bus*. Topologi *tree* digunakan untuk menghubungkan beberapa LAN dengan LAN lain. Hubungan antar LAN dilakukan via *hub*. Masing – masing hub dapat dianggap

sebagai akar *(root*) dari masing-masing pohon (*tree*). Topologi *tree* dapat mengurangi kekurangan topologi *bus* yang disebabkan persoalan *broadcast traffic*, dan kekurangan topologi *star* yang disebabkan oleh keterbatasan kapasitas *port hub* (Iwan sofana, 2008:53).



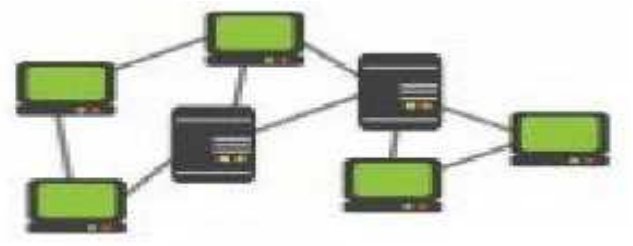
Sumber : http://kelipet.com/2015/09/macam-macam-topologi-jaringan-komputer/ (20 april 2016)

Gambar II.5
Topologi *Tree*

Karakteristik yang dimiliki topologi *tree* mirip dengan topologi *bus* dan *star*. Begitu juga dengan peralatan, kabel dan teknik pemasangan. Apabila kabel penghubung antar hub putus, maka jaringan star masih tetap dapat berfungsi, hanya saja hubungan dengan jaringan *star* yang lain akan terganggu.

5. Topologi *Mesh*

Topologi *mesh* dapat dikenali dengan hubungan *point to point* atau satu-satu ke setiap komputer. Setiap komputer terhubung ke komputer lain melalui kabel, bisa menggunakan kabel *coaxial*, *twisted pair*, bahkan serat optik. Topologi *mesh* sangat jarang diimplementasikan. Selain rumit juga sangat boros kabel. Apabila jumlah komputer semakin banyak maka instalasi kabel jaringan akan semakin rumit juga (Iwan sofana, 2008:54).



Sumber : http://kelipet.com/2015/09/macam-macam-topologi-jaringan-komputer/ (20 april 2016)

Gambar II.6
Topologi *Mesh*

Sebagian ahli menyebutkan bahwa topologi *mesh* sebenarnya termasuk dalam kategori *point to point*. Karena data dapat langsung dikirim ke komputer tujuan tanpa harus melibatkan komputer lain. Hanya saja bentuk jaringan rumit. Namun, ketika salah satu kabel putus maka pengiriman data akan melalui rute lain. Sehingga *mesh* tidak cocok dikelompokan dalam kategori *point to point*.

2.2.2. Topologi Logika (*Logical Topology*)

Topologi logika atau *logical topology* merupakan *rules communication* yang dipakai setiap *node* untuk berkomunikasi dalam jaringan. Sebagai contoh, bagaimana melakukan pengiriman data, bagaimana menerima data, bagaimana mengatur kecepatan transfer data, bagaimana mendeteksi kemungkinan *error*, lalu melakukan pengiriman data ulang dan hal-hal lain (Iwan sofana, 2008:55).

Terdapat dua (2) jenis topologi logika, antara lain :

1. *Shared Media Topologi*

Pada topologi *shared media*, semua *node* atau *network device* yang terhubung ke jaringan dapat mengakses *layout* (media jaringan) kapan saja manakala diperlukan. Akses ke media jaringan dapat dilakukan setiap saat dan tidak dibatasi. Ini merupakan

salah satu keuntungan dari topologi ini namun sekaligus juga merupakan kelemahanya. Karena setiap peralatan dapat mengakses media jaringan kapanpun maka kemungkinan terjadi tabrakan data (*collision*) akan cukup besar. Contoh jaringan yang menggunak*an topologi ini adalah semua varian jaringan yang menggunkan* Ethernet card seperti : topologi *bus, star dan tree* (Iwan sofana, 2008:58).

2. Token Based Topologi

Topologi *token based* menggunakan sebuah *frame* data bernama *token* yang mengalir mengelilingi jaringan. *Token* merupakan kendaraan setiap paket data yang hendak dikirim. Data mengalir pada media jaringan, melewati setiap komputer satu-persatu, hanya satu arah saja (Iwan sofana, 2008:60).

Akses setiap *node* ke media fisik jaringan diatur oleh *token*. Karena pengiriman data dilakukan secara bergantian dan setiap *node* harus menunggu giliran, maka tidak akan pernah terjadi *collision*. Namun, waktu tunggu atau delay dapat terjadi apabila banyak *node* yang ingin mengirim data.

2.3. Perangkat Keras Jaringan

2.3.1. Komponen Jaringan Komputer

Pada pembahasan tentang topologi fisik telah disinggung beberapa peralatan jaringan atau network device standar, seperti NIC (*Ethernet card*), hub, kabel jaringan dan peralatan lain. Beberapa peralatan *network* standar yang sering digunakan adalah NIC, Repeater, Hub, Bridge, Switch (Iwan sofana, 2008:64).

Peralatan – peralatan jaringan tersebut dapat dikaitkan dengan arsitektur standar jaringan yang disebut OSI (*Open system Interconnection*) *reference model* yang dikeluarkan oleh ISO (*International Standars Organization*). *OSI reference model* telah dibuat sejak 1977. OSI dapat dipandang seperti panduan umum atau "*abstract model*", bagaimana protokol-protokol jaringan dan peralatanya saling berkomunikasi dan bekerja sama.

1. NIC

NIC atau *Network Interface Card* merupakan peralatan yang berhubungan langsung dengan komputer dan didesain agar komputer-komputer jaringan dapat saling berkomunikasi. NIC juga menyediakan akses ke media fisik jaringan. Bagaimana bit-bit data (seperti tegangan listrik, arus. Gelombang elektromagnetik, dan besaran fisik lainya) dibentuk akan ditentukan oleh NIC. NIC merupakan contoh perangkat yang bekerja pada layer pertama OSI atau *layer physical* (Iwan sofana, 2008:66).

Sumber : https://commons.org/File:NIC-FA312.jpg (20 april 2016)

Gambar II. 7
Kartu Jaringan

2. HUB

HUB merupakan peralatan yang dapat menggadakan *frame data* yang berasal dari salah satu komputer ke semua *port* yang ada pada *hub* tersebut. Sehingga semua

komputer yang terhubung dengan *port hub* akan menerima data juga. *Hub* digunakan pada jaringan *star* (Iwan sofana, 2008:67).

Sumber : https://www.tokopedia.com/scratchconnect/hub-switch-24-port-3com (19 April 2016)

Gambar II. 8
HUB

Ada beberapa kategori hub yaitu :

a. *Passive Hub* atau *Concentrator*

   Hub biasa yang hanya meneruskan sinyal keseluruh *node. Passive hub* tidak akan memperkuat sinyal yang dating, sehingga tidak dapat digunakan untuk menjangkau area yang lebih besar. *Hub* semacam ini bekerja pada *layer physical.*

b. *Active Hub* atau *Multiport Repeater*

   Berfungsi mirip dengan *passive hub* namun dapat memperkuat sinyal datang, sehingga dapat digunakan untuk menjangkau area yang lebih besar. Hub semacam ini juga bekerja pada *layer physical*.

c. *Intelegent Hub*

   Intelegent hub umumnya dapat digabungkan atau ditumpuk (kadangkala disebut *stackable hub*). Hub jenis ini juga dapat melakukan seleksi alamat paket data tujuan, sehingga hanya *node* yang tertentu yang dapat menerima data. *Hub* semacam ini bekerja pada *layer data link.*

3. Repeater

Repeater merupakan salah satu contoh *active hub*. *Repeater* merupakan peralatan yang dapat menerima sinyal, kemudian memperkuat dan mengirim kembali sinyal tersebut ke tempat lain. Sehingga sinyal dapat menjangkau area yang lebih jauh. Karena *repeater* bekerja pada besaran fisis seperti tegangan listrik, arus listrik atau gelombang elektromagnetik, maka *repeater* termasuk dalam kategori peralatan yang bekerja pada *layer physical* (Iwan sofana, 2008:68).

Sumber : http://xvongola.co.id/2011/10/pengertian-switch-hub-router-bridge-dan.html (19 April 2016)

Gambar II. 9
Repeater

4. Bridge

Bridge merupakan peralatan yang dapat menghubungkan beberapap segmen dalam sebuah jaringn. Berbeda dengan *hub, bridge* dapat mempelajari *mac address* tujuan. Sehingga ketika sebuah komputer mengirim data ke komputer tertentu, *bridge* akan mengirim data melalui *port* yang terhubung ke komputer tujuan saja. Ketika *bridge* belum mengetahui *port* mana yang terhubung dengan komputer tujuan, maka dia akan mencoba mengirim pesan *broadcast* ke semua *port* (kecuali *port* komputer pengirim). Setelah *port* tujuan diketahui maka untuk selanjutnya hanya *port* itu saja yang akan dikirim data. *Bridge* juga dapat memfilter *traffic* di antara dua segmen LAN. *Bridge* bekerja pada *layer data link* (Iwan sofana, 2008:68).

Sumber : https://techbuzzersworld.com/2011/08/10/types-of-networks-and-networking-devices/(19 April 2016)

Gambar II. 10
Bridge

Beberapa karakteristik *bridge*, sebagai berikut :

a. *Bridge* lebih "*intelegent*" dibandingkan *hub* karena mampu menganalisis *incoming frames* dan meneruskanya berdasarkan informasi *address*
b. *Bridge* dapat mengumpulkan (*collect*) dan melalui paket (*pass packet*) diantara dua atau lebih segmen LAN
c. *Bridge* dapat membuat *multiple collision domains*, sehingga beberapa komputer dapat mengirimkan data secara simultan tanpa menyebabkan *collision*
d. *Bridge* dapat menyimpan dan mengelola *MAC address table* pada memorinya

5. *Router*

Router adalah peralatan jaringan yang dapat menghubungkan satu jaringan dengan jaringan lain. Sepintas lalu *router* mirip dengan *bridge*, namun *router* lebih cerdas dibandingkan *bridge. Router* bekerja menggunkan *routing table* yang disimpan di memorinya untuk membuat keputusan tentang kemana dan bagaimana paket dikirimkan. *Router* dapat memutuskan *route* terbaik yang akan ditempuh oleh paket data. *Router* akan memutuskan media fisik jaringan yang disukai dan yang tidak disukai. *Protocol routing* dapat mengantisipasi berbagai kondisi yang tidak

dimiliki oleh peralatan *bridge*. *Router* bekerja pada *layer network* (Iwan sofana, 2008:70).

Sumber : http://www.cisco.com/en/US/products/ps8321/prod_view_selector.html (19 April 2016)

Gambar II. 11
Router

6. *Network Switch*

Disamping *repeater, bridge* dan *router*, terdapat sejumlah peralatan *network switching* yang digunakan dalam membangun *internetwork*. Peralatan *switch* didesain dengan tujuan berbeda dengan *repeater, bridge* dan *router*,. Jika perangkat jaringan yang terhubung pada LAN terlalu banyak maka kebutuhan transmisi meningkat melebihi kapasitas yang mampu dilayani oleh media komunikasi jaringan (Iwan sofana, 2008:71).

Sumber:http://www.ariatech.com.au/index.php?action=module&module=products&page=263 (19 April 2016)

Gambar II. 12
Switch

Kita dapat menggunkan *router* untuk mengisolasikan group fisik jaringan dengan yang lain. Penggunaan *router* cocok pada sistem *internetwork* dengan kelompok-kelompok kerja yang terletak dalam lokasi yang kecil. Untuk kasus

kelompok-kelompok kerja terpisah secara geografis maka penggunaan *router* tidak dapat mengisolasikan lalu lintas data. Lalu lintas data dalam kelompok kerja yang tinggi akan menyebabkan beban di *router* tetap tinggi karena lalu lintas tersebut selalu melewati *router*. Untuk mengatasi hal ini digunakan peralatan *switching* atau *network switch.*

7. Media Transmisi

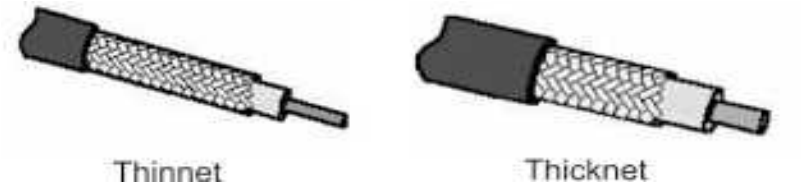
Jenis Media Transmisi Jaringan Komputer. Transmisi di sini diartikan proses perpindahan ataupun pertukaran data dari komputer ke komputer, komputer ke server, ataupun komputer ke media elektronik lainnya. Jadi untuk melakukan pertukaran data tersebut, tidak terjadi begitu saja. Dibutuhkan media yang sebagai perantara untuk proses pengiriman data tersebut :

a. Media trasnmisi dengan menggunakan kabel (*Wire)*

Untuk media ini, kabel yang digunakan terbagi atas 2, yaitu :

1). *Copper* media, yaitu kabel yang digunakan terbuat dari tembaga. Jenis kabel ini memiliki banyak tipe, diantaranya :

a). *Coaxial cable*, karakteristik kabel ini adalah digunakan pada topologi *ring*, terdapat satu inti kabel dan terhadapat lapisan seperti alumunium foil yang bertujuan untuk menghilangkan pengaruh dari luar kabel seperti *elektromagnetik interference (EMI*) dan radio *frequency interference (RFI)*. Jenis kabel ini terdiri dari 2, yaitu : *Thin Ethernet* atau *Thinet*, kabel ini jarak maksimumnya 200 m. *Thick Ethernet* atau *Thicknet*, kabel ini jarak maksimumnya 500 m.



Sumber : http://www.tifkom.net/2015/06/jenis-media-transmisi-jaringan-komputer.html

Gambar II. 13
Kabel coaxial

b). *Twisted Pair cable*, karakteristik : kabel ini berpilin secara berpasangan dan merupakan generasi setelah kabel *coaxial*. Sekarang kabel ini sering digunakan pada saat membangun jaringan. Untuk menghubungkan kabel ini digunakan konektor atau yang disebut dengan *Registered jack (RJ).* Ada 2 jenis kabel ini yaitu : STP (*Shielded Twisted Pair*) *cable* dan UTP (*Unshielded Twisted Pair*) *cable.*

Sumber : http://www.tifkom.net/2015/06/jenis-media-transmisi-jaringan-komputer.html (19 april 2016)

Gambar II. 14
Kabel STP dan UTP

2). Optical media. Pada optical media proses penyaluran data dilakukan dengan melewatkan cahaya (gelap/terang) pada kabel yang berupa serat kaca (*Fiber Optic*). Pada saat ini terdapat 2 jenis fiber optik yang umum digunakan yaitu : *Single-mode* fiber optik dan *multi-mode* fiber optik.

b. Media transmisi tanpa menggunakan kabel (*Wireless)*

Pada media transmisi ini, gelombang radio merupakan alat perantara untuk menghantar data pada jaringan. Pada saat ini trennya disebut wi-fi (*wireless fidelity*).

Ada beberapa standar yang diatur oleh IEEE untuk jenis media yaitu: 1). 802.11a: frekuensi sebesar 5 GHz, *bandwith* sebesar 54 Mbps. 2). 802.11b: frekuensi sebesar 2,4 GHz, *bandwith* sebesar 11 Mbps. 3). 802.11g: frekuensi sebesar 2,4 GHz, *bandwith* sebesar 54 Mbps. Pada media ini *wireless* terdapat kekurangan, yaitu sangat mudah dipengaruhi oleh *Radio Frequency Interface (RFI*) yang mengganggu pengiriman data.

2.4. Perangkat Lunak Jaringan

2.4.1 Mikrotik

Mikrotikls merupakan nama perusahaan pemegang lisensi Mikrotik yang berlokasi di Riga, ibukota Latvia, sebuah negara pecahan Uni soviet yang bersebelahan dengan Rusia. Mikrotikls merupakan produsen *software* dan *hardware* router Mikrotik. Dengan mikrotik maka teknologi *internet* menjadi lebih cepat, handal dan terjangkau untuk pengguna yang lebih luas.

Mikrotik RouterOS adalah sebuah *software* yang berfungsi mengubah PC (komputer) menjadi sebuah *router*. Mikrotik RouterOS layaknya IOS cisco yang diinstall di dalam router cisco, hanya saja IOS cisco tidak bisa di install di dalam komputer kecuali menggunakan emulator seperti GNS3 atau dynamips. Pada dasarnya RouterOS merupakan sistem operasi Mikrotik RouterBOARD yang berbasis kernel Linux v.2.6.

Selain bisa di install di dalam PC, mikrotik RouterOS juga bisa diinstall pada sebuah *hardware* khusus yang bernama *RouterBoard*. Ketika kita membeli mikrotik *RouterBoard* biasanya sudah terinstall RouterOS didalamnya.

Sebagai sebuah *router*, mikrotik memiliki fitur – fitur yang tidak kalah dengan *router – router* mahal seperti cisco. Beberapa fitur mikrotik antara lain :

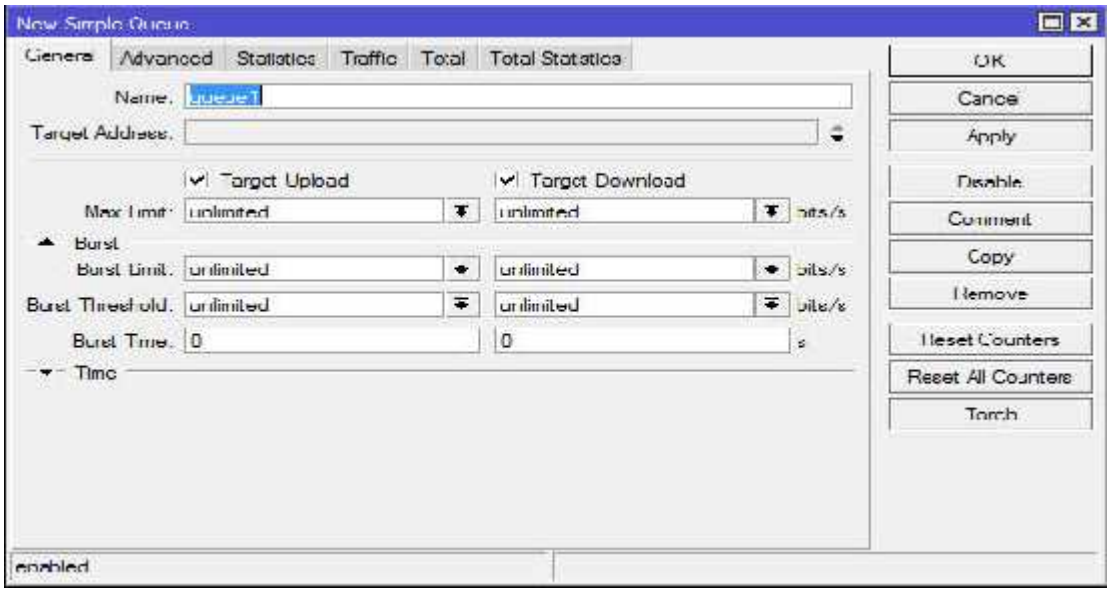
1. *Interface Fisik : Ethernet, FO. Wireless* : 900Mhz, 2.4 Ghz, 5.8 Ghz. Virtual : *Bridge, Bonding, Vlan. Tunnel* : EoIP, PPTP, L2TP, MPLS, PPPoE.
2. *Routing : Policy Routing, statik routing, dinamis routing* (OSPF, BGP, RIP)
3. *Firewall : Filter Rule, TTL, Address list, Network Address Translation* (NAT)
4. *Bandwidth Management* : HTB, PFIFO, BFIFO, RED, SFQ, PCQ
5. *Service :Hotspot, Web Proxy*, DHCP, DNS
6. *Management User : Radius, User manager,* PPP *user*.
7. *Tools : Graph, MAC-ping, Torch, Ping.*

Mikrotik management bandwidth pada dasarnya mempunyai 2 sistem management *bandwidth* yaitu *simple queue* dan *queue tree. Simple queue* sering digunakan sebagai management *bandwidth* dengan *limit IP address (simple limit*) sedang *queue tree* lebih spesifik lagi yaitu *content website* misalnya *extention* dan alamat website dan lain sebagainya.

1. Simple Queue

Simple queue merupakan menu pada routerOS untuk melakukan manajemen *bandwidth* untuk jaringan yang sederhana. Untuk menggunakan *simple queue*, pekerjaan *packet classification* dan *marking packet* tidak wajib untuk dilakukan. Meskipun semikian, *simple queue* sebenarnya juga bisa melakukan manajemen

bandwidth terhadap *packet-packet* yang sudah di*marking* (Rendra towidjojo, 2014;120).



Sumber : dokumntasi pribadi (19 April 2016)

Gambar II. 15

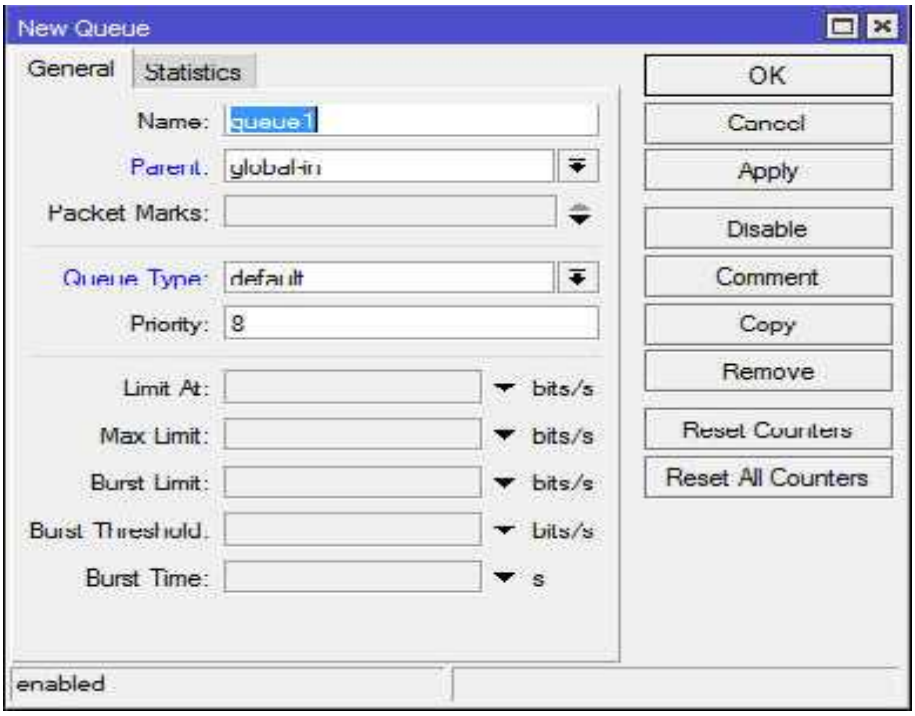
Menu pada *simple queue*

Konfigurasi *queue* yang dilakukan oleh *simple queue* tetap menggunakan *Hierarchical Token Bucket* sebagai metode utama. Namun *queue* tersebut tidak dilakukan pada *interface* fisik. *Simple queue* akan melakukan *queue pada interface virtual.*

2. Tree Queue

Secara garis besar, *queue tree* masih memiliki beberapa persamaan dengan *simple queue*. Keduanya tetap menggunakan *Hierarchical Token Bucket* untuk menyusun konfigurasi-konfigurasi *queue*. Sehingga nantinya *queue tree* juga dikenal adanya *inner queue* dan *leaf queue*. *Queue tree* juga dapat dikombinasikan dengan metode *queu*e lainya seperti FIFO maupun PCQ (Rendra towidjojo, 2014;170).

Berbeda dengan *simple queue* sebelumnya, *queue tree* adalah konfigurasi yang bersifat *one way* (satu arah), ini berarti sebuah konfigurasi hanya akan mampu melakukan *queue* terhadap satu arah jenis *traffic*. Jika sebuah konfigurasi queue pada *queue tree* ditunjukan untuk melakukan terhadap *bandwidth*, maka konfigurasi tersebut tidak akan melakukan *queue* untuk *bandwidth upload*, demikian pula sebaliknya. Sehingga untuk melakukan *queue* terhadap trafik *upload* dan *download* dari sebuah komputer *client*, harus dibuat 2 konfigurasi *queue*.



Sumber : dokumntasi pribadi (19 April 2016)

Gambar II. 16
Menu pada *queue tree*

2.5. TCP/IP dan *Subnetting*

Model referensi DARPA atau DARPA *Refence Model* adalah sebuah *referensi protokol* jaringan yang diusulkan oleh department pertahanan Amerika

Serikat atau DOD (*Deartement of Defense*). Model ini dimnamai begitu karena lembaga yang mengembangkan TCP/IP adalah DARPA (*United States Defence Advanced Research Project Agency*) pada decade 1970-an hingga 1980-an. Pada mulanya TCP/IP digunakan pada jaringan ARPANET. Namun, saat ini telah menjadi protokol standar bagi jaringan yang lebih umum yang disebut *internet* (Iwan sofana, 2008:88).

Sejauh ini kita sering menjumpai kata protokol. Cukup sulit untuk mendefinisikan protokol, karena protokol memiliki banyak variasi dan banyak tujuan penggunaan. Secara sederhana dapat dijelaskan protokol merupakan sekumpulan aturan dalam komunikasi data. Protokol mengatur bagaimana terjadinya hubungan dan perpindahan data antara dua atau lebih komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi keduanya. Pada tingkat yang terendah, protokol mendefinisikan koneksi perangkat keras. Kebanyakan protokol memiliki salah satu atau beberapa karakteristik sebagai berikut :

1. Melakukan deteksi apakah ada koneksi fisik atau tidak, yang dilakukan oleh komputer atau mesin lain;
2. Melakukan *handshaking*;
3. Menjadi negosiator berbagai macam karakteristik koneksi;
4. Mengatur bagaimana mengawali dan mengakhiri suatu pesan;
5. Menentukan format pesan;
6. Melakukan *error detection* dan *error correction* saat terjadi kerusakan pesan;
7. Mengakhiri suatu koneksi;

Berbeda dengan model referensi OSI yang memiliki 7 layer, model referensi DARPA hanya memiliki 4 lapisan yaitu : *Application layer, host to host layer (transport layer), internetworking layer (internet layer)* dan *network interface layer (physical layer).*

Tabel II. 2

Model DARPA

Layer	Keterangan
4 (*Application)*	Berfungsi menyediakan akses aplikasi terhadap jaringan TCP/IP. Layer ini menangani *high level protokol*, masalah *representasi data*, proses *encoding*, dialog control yang memungkinkan terjadinya komunikasi antar aplikasi jaringan. Protokol aplikasi pada layer ini diantaranya : Telnet, DHCP, DNS, HTTP, FTP, SMTP, SNMP dan lain-lain.
3 (*Host to host*)	Berfungsi membuat komunikasi antardua *host*. Layer ini menyediakan layanan pengiriman dari sumber data menuju ke tujuan data dengan cara membuat *logical connection* diantara keduanya. Layer ini bertugas memecah data dan menyatukan kembali data yang diterima dari *application layer* ke dalam aliran data yang sama antara sumber dan mengirim data. Ada dua cara pengiriman data, *connection oriented* (TCP) atau *connectionless oriented* (UDP). Protokol TCP memiliki orientasi terhadap reliabilitas data sedangkan UDP lebih berorientasi kepada kecepatan pengiriman data. Protokol pada layer ini adalah : TCP dan UDP
2 *(Internetworking*)	Berfungsi untuk melakukan *routing* dan pembuatan paket IP menggunkan teknik *encapsulation*. Layer ini memiliki tugas untuk memilih *rule* terbaik yang akan dilewati oleh sebuah paket data dalam sebuah jaringan. Selain itu juga bertugas melakukan *paket switching* untuk mendukung tugas utama tersebut. Protokol yang menggunakan layer ini yaitu : IP, ICMP, ARP, RARP.
1 (*Network Interface*)	Berfungsi meletakan *frame-frame* data yang akan dikirim ke media jaringan. Layer ini bertugas mengatur semua hal yang diperlukan sebuah paket IP. Protokol yang berjalan pada layer ini adalah : *Ethernet, Token ring*, POTS, ISDN, *Frame Relay* dan ATM

Sumber : Membagun Jaringan Komputer (Iwan sofana, 2008:90)

2.5.1. IP (*Internet Protocol*)

Internet protocol (IP) berada pada *layer internetwork* atau *internet*. IP merupakan kunci dari jaringan TCP/IP, agar dapat berjalan dengan baik maka semua aplikasi jaringan TCP/IP pasti bertumpu kepada *Internet Protocol*. IP merupakan protokol yang mengatur bagaimana suatu data dapat dikenal dan dikirim dari satu komputer ke komputer lain. IP bersifat *connectionless protocol*. Ini berarti IP tidak melakukan *error detection* dan *error recovery*. IP tidak dapat melakukan *handshake* (pertukaran control informasi) saat membangun sebuah koneksi, sebelum data dikirim. Padahal handshake merupakan salah satu syarat agar sebuah koneksi baru dapat terjadi. Dengan demikian, IP bergantung pada layer lainya untuk melakukan *handshake* (Iwan sofana, 2008:93).

Protokol IP memiliki lima fungsi utama, yaitu :

1. Mendefinisikan paket yang menjadi unit satuan terkecil pada transmisi data di *Internet*;
2. Memindahkan data antara *transport layer* dan *network interface layer*;
3. Mendefinisikan skema pengalamatan *internet* dan *IP address*;
4. Menentukan *routing paket*;
5. Melakukan *fragmentasi* dan penyusunan ulang paket.

Protokol IP juga dikenal sebagai "*Best effort" protocol*. Hal ini karena IP tidak memberi jaminan bahwa suatu datagram akan sampai ketujuan dengan selamat. IP hanya memberi jaminan untuk melakukan usaha terbaik (*best effort*) agar *datagram* dapat sampai ke tujuan.

2.5.2. TCP

Transmission Control Protocol (TCP) merupakan protokol penting dalam *layer transport*, TCP merupakan protokol yang bersifat *connection oriented*. TCP menyediakan layanan pengiriman data yang *connection oriented, reliable, byte stream service. Connection oriented* berarti dua aplikasi pengguna TCP harus melakukan pembentukan hubungan dalam bentuk pertukaran kontreol informasi *(handshaking*), sebelum transmisi data terjadi. *Reliable* berarti TCP menerapkan proses deteksi kesalahan paket dan retransmisi. Byte stream berarti paket dikirimkan dan sampai ke tempat tujuan secara berurutan (Iwan sofana, 2008:97).

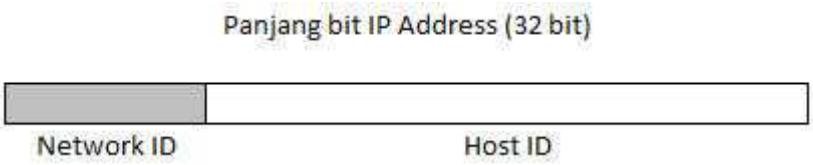
Protokol TCP sangat cocok digunakan untuk koneksi yang membutuhkan kehandalan tinggi, seperti telnet, ssh, FTP, HTTP dan beberapa layanan lain yang bersifat kritis.

2.5.3. *IPv4 Address*

IP address merupakan sekumpulan bilangan binner 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 dua host atau lebih yang tergabung ke i*nternet* menggunkan *IP address* yang sama. Hal ini tidak sepenuhnya benar karena kasus-kasus pencurian *IP address* seringkali terjadi (Iwan sofana, 2008:103).

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 seahri-hari. *IP address* dapat dipisahkan menjadi 2 bagian yaitu : bagian *network (Network ID*) dan bagian *host (Host ID).*



Sumber : Membangun Jaringan Komputer (Iwan sofana, 2008:104)

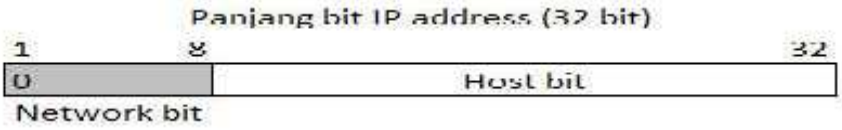
Gambar II. 17
Ilustrasi *IP address*

1. Kelas *IP Address*

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*nya menjadi beberapa kelas, meliputi :

a. Kelas A

IP address kelas A memiliki struktur sebagai berikut :



Sumber : Membangun Jaringan Komputer (Iwan sofana, 2008:106)

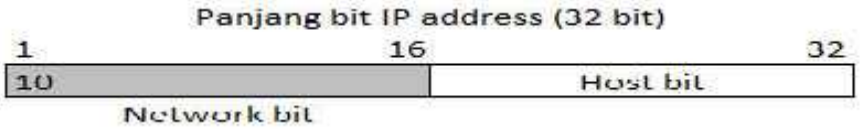
Gambar II. 18
Ilustrasi *IP address* kelas A

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) merupakanbit-bit *network (network bit)* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 24 bit terakhir merupakan *bit host* (Iwan sofana, 2008:106).

Dengan demikian, hanya ada 128 network kelas A, yakni dari 0.xxx.xxx.xxx sampai 127.xxx.xxx.xxx. Setiap network dapat menampung lebih dari 16 juta host (xxx adalah variable, nilainya dari 0 s.d. 255).

b. Kelas B

IP addres kelas B memiliki struktur sebagai berikut :



Sumber : Membangun Jaringan Komputer (Iwan sofana, 2008:106)

Gambar II. 19

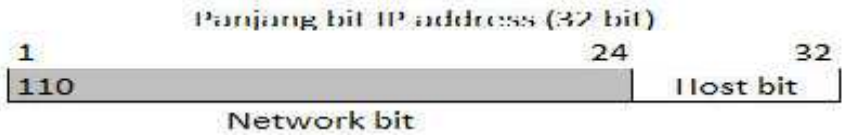
Ilustrasi *IP address* kelas B

Jika 2 bit pertama dari *IP address* adalah 10, maka *IP address* termasuk dalam *network* kelas B. Dua bit ini dan 14 bit berikutnya (16 bit pertama) merupakan *bit network*, sedangkan 16 bit terakhir merupakan *bit host* (Iwan sofana, 2008:106).

Akan terdapat lebih dari 16 ribu *network* kelas B, yakni dari *network* 128.0.xxx.xxx hingga 191.255.xxx.xxx. Setiap network kelas B mampu menampung lebih dari 65 ribu *host.*

c. Kelas C

IP address kelas C memiliki struktur sebagai berikut :



Sumber : Membangun Jaringan Komputer (Iwan sofana, 2008:106)

Gambar II. 20

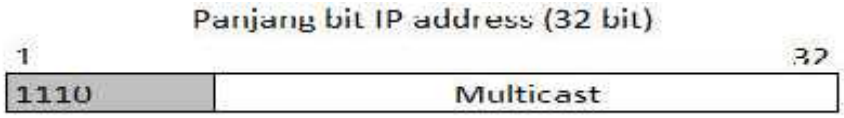
Ilustrasi *IP address* kelas C

Jika bit pertama *IP address* adalah 110, maka *IP address* termasuk dalam *network* kelas C. Tiga bit ini dan 21 bit berikutnya (24 bit pertama) merupakan *bit network*, sedangkan 8 bit terakhir merupakan *bit host*.

Terdapat lebih dari 2 juta *network* kelas C, yakni dari 192.0.0.xxx hingga 223.255.255.xxx. Setiap *network* kelas C hanya mampu menampung sekitar 256 *host* (Iwan sofana, 2008:107).

d. Kelas D

Selain ke tiga kelas diatas, ada 2 kelas lagi yang ditunjukan untuk pemakaian khusus, yakni kelas D dan kelas E. *IP address* kelas D memiliki struktur sebgai berikut :



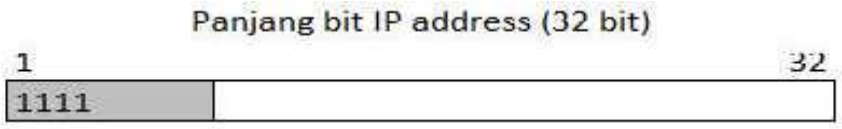
Sumber : Membangun Jaringan Komputer (Iwan sofana, 2008:107)

Gambar II. 21
Ilustrasi *IP address* kelas D

Jika 4 bit pertama adalah 1110, maka *IP address* termasuk kelas D. *IP address* kelas D digunakan untuk *multicast address*, yakni sejumlah komputer yang memakai bersama suatu aplikasi. Salah satu penggunaan *multicast address* adalah sedang berkembang saat ini di internet adalah untuk aplikasi *realtime video conference* yang meibatkan lebih dari dua host (*multi point*), menggunakan *Multicast Backbone* (MBone). Pada IP address kelas D tidak dikenal *bit network* dan *host.*

e. Kelas E

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



Sumber : Membangun Jaringan Komputer (Iwan sofana, 2008:108)

Gambar II. 22
Ilustrasi *IP address* kelas E

2. Network Address

Kita sudah melihat bahwa *IP address* kelas A, B, dan C selalu dapat dibagi menjadi dua bagian, yaitu bagian *network* dan *host*. Dalam prakteknya, sebuah host tidak pernah berdiri sendiri namun memerlukan host lain dan bergabung membentuk sebuah *network*. Setiap network yang tergabung di internet haruslah memiliki ID yang unik, yang disebut alamat *network* atau *network address* (Iwan sofana, 2008:109).

Network address juga dapat menyederhanakan proses *routing internet*. *Router* cukup melihat *network address* untuk menentukan ke router mana suatu *datagram* harus dikirimkan. Selanjutnya *datagram* akan diteruskan oleh router jaringan lokal ke host tujuan.

3. Broadcast Address

Broadcast address merupakan *IP address* khusus yang digunakan untuk mengirim atau menerima informasi yang harus diketahui oleh seluruh *host* pada suatu

network. Setiap *datagram IP* memiliki *header* berisi *IP address* alamat tujuan. Dengan adanya alamat ini, maka hanya host tujuan saja yang memproses *datagram* tersebut, sedangkan host lain akan mengabaikanya (Iwan sofana, 2008:110).

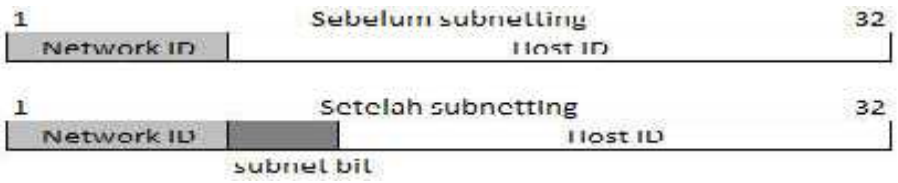
Seluruh *host* pada suatu *network* harus memiliki *broadcast address* yang sama pula. Dengan demikian, broadcast address tidak boleh digunakan sebagai *IP address* untuk host tertentu. Jadi sebenarnya setiap host memiliki 2 *address* untuk penerimaan *datagram*, yaitu : *IP address* yang bersifat unik, *broadcast address* yang selalu sama untuk setiap host satu network.

4. Netmask Address

Netmask address merupakan *IP address* khusus yang digunakan untuk menentukan pembagian panjang *bit network* dengan *bit host* . *Netmask* juga digunakan untuk mencari *network address* (Iwan sofana, 2008:113).

2.5.4. *Subnetting*

Subnetting adalah proses membagi atau memecah sebuah *network* menjadi beberapa *network* yang lebih kecil (*subnet-subnet*). Esensi dari subnetting adalah memindahkan garis pemisah bagian *network* sehingga beberapa bit host digunakan untuk bit tambahan bagian network (Iwan sofana , 2008:114).



Sumber : Membangun Jaringan Komputer (Iwan sofana, 2008:115)

Gambar II. 23
Ilustrasi IP perubahan panjang bit network dan host karena subnetting

Pada ilustrasi diatas dapat dilihat bagaimana bagian *network* bertambah panjang. *Subnetting* akan mengakibatkan beberapa perubahan sebagai berikut : Panjang *bit network* bertambah dan *bit host* berkurang, *Network address* berubah, *Netmask address* berubah, *Broadcast address* berubah, Jumlah *network (subnet*) bertambah, Jumlah *host* maksimal setiap berkurang.

Subnetting dilakukan dengan beberapa alasan, diantaranya :

1. Untuk efisiensi *IP address*, alokasi *IP address* berdasarkan pembagian kelas kurang efisien;
2. Untuk menjembatani perbedaan topologi fisik seringkali digunakan *router*. *Router* bekerja dengan cara meneruskan paket antar *network* berbeda. Perbedaan *network* dalam TCP/IP ditentukan dari *network* address-nya. Sehingga untuk mengatasi kita harus membagi sebuah *network* menjadi beberapa subnet yang kemudian dihubungkan oleh *router*.
3. Untuk memudahkan proses manajemen atau pengaturan *security network*.
4. Untuk mengisolasi *traffic*. Manakala suatu host berkomunikasi dengan host lain pada *subnet* yang sama, pesan broadcast cukup disebarkan di antara anggota dan tidak akan diteruskan ke *subnet* lain.

2.6. Sistem Keamanan Jaringan

2.6.1. Firewall dan Pendahuluan Security

Mengingat pentingnya perlindungan informasi yang ada pada komputer, maka telah dikembangkan berbagai teknik untuk melindungi komputernya dari berbagai

serangan seperti enkripsi data, pengembangan metode *otentifikasi, proteksi biometri*, *firewalling*, dan sebagainya (Iwan sofana, 2008:162).

1. Security

Menurut garfinkel, seorang pakar security, keamanan komputer atau komputer security mencangkup empat aspek yaitu :

a. Privacy

Aspek *privacy* berhubungan dengan kerahasiaan informasi. Inti utama aspek *privacy* adalah bagaimana menjaga informasi dari orang yang tidak berhak mengaksesnya. Sebagai contoh, email seorang pemakai tidak boleh dibaca oleh orang lain, bahkan *administrato*r sekalipun. Beberapa usaha telah dilakukan untuk melindungi aspek *privac*y, diantaranya penggunaan *enkrips*i.

b. Integrity

Aspek *integrity* berhubungan dengan keutuhan informasi. Inti utama aspek *integrity* adalah bagaimana menjaga informasi agar tidak diubah tanpa izin pemilik informasi. *Virus*, *Trojan horse*, atau pemakai lain dapat mengubah informasi tanpa izin, ini merupakan contoh serangan pada aspek ini. Sebuah email dapat saja ditangkap di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju. Penggunaan *enkripsi* dan *digital signature* dapat mengatasi masalah ini.

c. Athentication

Aspek *authentication* berhubungan dengan identitas atau jati diri atau kepemilikan yang sah. Sistem harus mengetahui bahwa suatu informasi dibuat atau diakses oleh pemilik yang sah. Ada dua masalah yang terkait dengan

aspek ini, yang pertama pembuktian keaslian informasi atau dokumen, yang kedua adalah *acces control.*

Salah satu usaha untuk memenuhi masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan *digital signature. Watermarking* dapat digunakan untuk menjaga "*intellectual property*", dengan menandai dokumen atau hasil karya dengan tanda tangan pembuat. Masalah kedua, yaitu *acces control*, berkaitan dengan pembatasan hak akses orang yang dapat mengakses informasi. Cara standar yang digunakan untuk acces control yaitu dengan *login* dan *password.*

d. Availabilitiy

Aspek *availability* berhubungan dengan ketersediaan informasi. Contoh serangan terhadap aspek ini yaitu "*denial of service attack*", di mana *server* dikirimi permintaan palsu yang bertubi-tubi sehinga tidak dapat melayani permintaan lain. Contoh lain adalah mailbomb, dimana seorang pemakai dikirim email bertubi-tubi (hingga ribuan email), sehingga tidak dapat membuka emailnya. Kondisi ini menyebabkan informasi tidak dapat diakses ketika dibutuhkan.

2. Serangan

Serangan terhadap *security* atau *security attack* merupakan segala bentuk gangguan terhadap keamanan sistem informasi. Menurut W. Stalings, ada beberapa kemungkinan serangan terhadap aspek-aspek *security* :

a. Interruption

Serangan jenis ini ditunjukan terhadap ketersediaan (aspek *availability*) informasi. Sistem dapat dirusak, baik software maupun *hardware*, sedemikian rupa sehingga informasi tidak dapat diakses lagi.

b. Interception

Serangan jenis ini ditunjukan terhadap aspek *privacy* dan *authentication*. Pihak yang tidak berwenang dapat mengakses informasi. Contoh dari serangan ini adalah "*wiretapping*"

c. Modification

Serangan jenis ini ditunjukan terhadap aspek *privacy*, *authentication* dan *intergrity*. Pihak yang tidak berwenang dapat mengakses dan mengubah informasi.

d. Fabrication

Serangan jenis ini ditunjukan terhadap asek *privacy*, *authentication*, dan *integrity*. Pihak yang tidak berwenang dapat menyisipkan objek palsu ke dalam sistem seperti jaringan komputer.

3. Firewall

Sebuah *firewall* digunakan untuk melindungi jaringan komputer, khususnya LAN dari berbagai serangan (*intrusions)* yang dapat menyebabkan data *corrupt* atau *service* menjadi macet. Sebuah *firewall* dapat berupa komputer biasa yang telah dikonfigurasi menggunakan *software* tertentu, bisa juga *hardware/device* khusus. Sekurang-kurangnya *firewall* memiliki dua buah *interface*. Salah satu *interface* dihubungkan dengan jaringan *private* (yang akan dilindungi, biasanya LAN),

sedangkan *interface* yang lain dapat dihubungkan dengan jaringan *public* (biasanya internet) (Iwan sofana, 2008:164).

Umumnya *firewall* menjadi satu dengan *router* atau NAT *router*, namun *firewall* memiliki fitur-fitur lebih lengkap dibandingkan *router* biasa. *Firewall* dapat menyeleksi setiap data yang keluar/masuk, kemudian membandingkanya dengan kriteria atau *policy* tertentu. Manakala sesuai dengan *policy* maka data akan diteruskan. Jika tidak sesuai, data akan di *block* atau di *drop.*

Firewall umumnya dibuat dengan menggunakan satu atau beberapa metode proses *control akses*, yang meliputi :

a. *Packet filtering*, paket – paket dianalisis dan disaring menggunakan sekumpulan aturan. Setiap paket yang disaring akan dilihat *header*nya. Karena informasi *IP address* asal/tujuan, port, ada pada *header* ini. Paket-paket yang sesuai dengan aturan akan diteruskan ke tujuanya, sedangkan yang tidak sesuai akan dimusnahkan.
b. *Proxy service*, *proxy* tidak melakukan penyeringan paket-paket. *Proxy* bekerja pada tingkat aplikasi, sehingga *proxy* dapat menyaring isi paket-paket melalui *firewall*. Informasi berasal dari *internet* akan ditampung sementara di suatu tempat tertentu yang disebut *proxy server*. Kemudian *host-host* pada LAN akan mengaksesnya dari *proxy server*, demikian pula sebaliknya. Pengguna pada jaringan lokal tidak menyadari bahwa mereka tidak terhubung langsung dengan *internet. Proxy* dapat dianalogikan seperti bak air yang menampung air dari sumur. Untuk mandi, orang tidak langsung terjun ke sumur namun menggunaakan air yang ada di bak.

c. *Stateful inspection*, merupakan metode terbaru yang bekerja bukan dengan menyeleksi isi setiap paket, melaikan membandingkan *key* yang menjadi bagian paket ke suatu *database* yang berisi informasi terpercaya. Informasi yang melalui *firewall* dimonitor secara spesifik, untuk kemudian dibandingkan dengan *database*. Jika dianggap “bersih” maka informasi boleh melalui *firewall*, jika “tidak bersih” informasi akan dimusnahkan.