BAB II

LANDASAN TEORI

2.1. Tinjauan Jurnal

Untuk mendukung penelitian yang penulis lakukan, berikut penulis sajikan dua jurnal ilmiah yang terkait dengan penelitian yang penulis bahas.

> Menurut Aziz dan Purnama (2012:8) Keamanan jaringan saat ini menjadi isu yang penting dan terus berkembang.beberapa kasus yang menyangkut keamanan sistem saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan proteksi yang sedemikian besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan dan sistem-sistem setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini disebabkan karena kemajuan bidang jaringan komputer dengan konsep open sistemnya sehingga siapapun, dimanapun, dan kapanpun, mempunyai kesempatan untuk mengaksesnya.
>
> Menurut Pribadi (2013:1) VPN adalah sebuah koneksi *Virtual* yang bersifat *private* mengapa disebut *virtual* karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan *virtual* dan mengapa disebut *private* karena jaringan ini merupakan jaringan yang sifatnya *private* yang tidak semua orang bisa mengaksesnya. *VPN* menghubungkan PC dengan jaringan publik atau internet namun sifatnya *private*, karena bersifat *private* maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya. Oleh karena itu diperlukan keamanan data.

Dari kedua pendapat pakar tersebut maka dapat disimpulkan bahwa jaringan komputer merupakan media bertukar data dan *VPN* sebagai keamanan untuk melindungi dalam transfer data.

2.2. Konsep Dasar Jaringan

Teknologi jaringan komputer mengalami perkembangan yang sangat pesat hal ini terlihat pada era tahun 80-an jaringan komputer masih merupakan teka-teki. Tapi sekarang jaringan komputer sudah menguasai semua aspek yang ada sehingga mempermudahkan dalam hal pengiriman data. Selain itu, perangkat

keras dan perangkat lunak jaringan telah benar-benar berubah, di awal perkembangannya hampir seluruh jaringan dibangun dari kabel koakxial, kini banyak telah diantaranya dibangun dari serat optik atau komunikasi tanpa kabel.

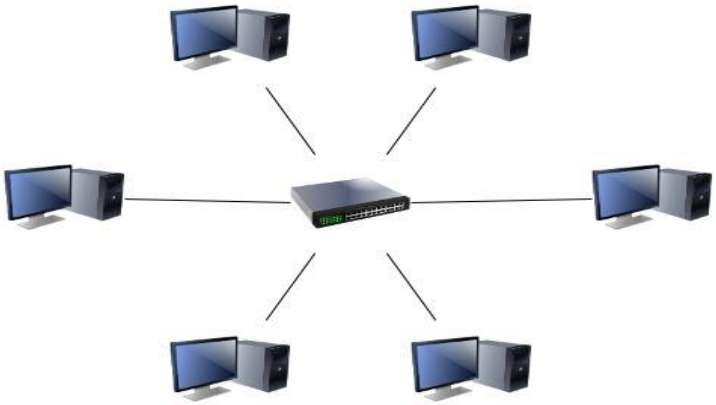
> Menurut Kurnia Trisna Somantri (2007:1) Jaringan komputer merupakan sejumlah komputer yang dapat saling berkomunikasi. Dalam komunikasi ini dapat terjadi perpindahan data maupun berbagi sumber daya. Adapun dalam skala luas, internet juga merupakan jaringan komputer. Jadi secara umum jaringan komputer didefinisikan sebagai perangkat yang terhubung bersama-sama untuk berbagi informasi dan layanan. Adapun layanan data yang dapat dibagi di jaringan ini tidak ada habisnya, misalnya dokumen, musik, *e-mail*, situs *web*, *database*, *printer*, *faks*, telepon, konferensi *video*, dan lain-lain.

2.2.1. Tipe Jaringan Komputer

Tipe jaringan komputer dibagi menjadi empat tipe jaringan komputer dalam hubungannya dengan luas area yang mencakup yaitu :

1. Local Area Network (LAN)

   Lan adalah jaringan komputer yang menghubungkan komputer satu dengan komputer lainya yang mencakup area dalam satu ruang, satu gedung, atau beberapa gedung yang berdekatan sehingga setiap komputer dapat berkomunikasi dan berbagi perangkat keras, seperti harddisk, cd-room, dan printer secara bersama-sama.



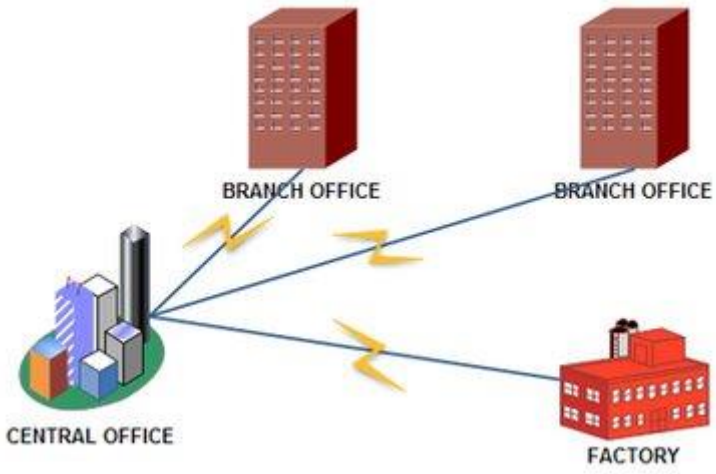
Sumber : http://www.webopedia.com/TERM/L/local_area_network_LAN.html

Gambar II.1

Jaringan LAN

2. Metropolitan Area Network (MAN)

MAN pada prinsipnya sama dengan LAN. Akan tetapi luas wilayah jaringannya lebih besar bila dibandingkan LAN, MAN sangat cocok diterapkan untuk membangun jaringan antar kantor yang letaknya berdekatan dan berada dalam kota yang sama. Jaringan ini umumnya menggunakan media transmisi berupa gelombang mikro atau gelombang radio.



Sumber : http://ecomputernotes.com/computernetworkingnotes/computer-network/metropolitan-area-network

Gambar II.2

Jaringan MAN

3. Wide Area Network (WAN)

WAN adalah suatu jaringan yang memiliki jarak jangkauan yang sangat luas yang mencangkup wilayah antarkota, antarprovinsi, antarnegara, bahkan antarbenua. WAN biasanya dihubungkan dengan menggunakan satelit atau kabel bawah laut. Dengan menggunakan saran WAN, sebuah bank yang ada di Jakarta dapat menghubungi kantor cabangnya yang ada di hongkong dalam waktu yang sangat singkat.

Sumber : https://www.manageengine.com/network-monitoring/images/Topology-Mapping.jpg

Gambar II.3

Jaringan WAN

4. Internet

Internet merupakan gabungan dari LAN, MAN, dan WAN yang ada di seluruh dunia. Oleh sebab itu internet juga merupakan sebuah jaringan komputer. Jika kamu sedang berinternet, berarti kamu terkoneksi ke semua komputer di dunia yang menggunakan internet juga. Jaringan-jaringan tersebut terhubung dalam sebuah jaringan internet yang sangat besar. Oleh karena itu diperlukan jaringan kabel serat optik yang menghubungkan satu benua lain dan dibangun melalui dasar laut.

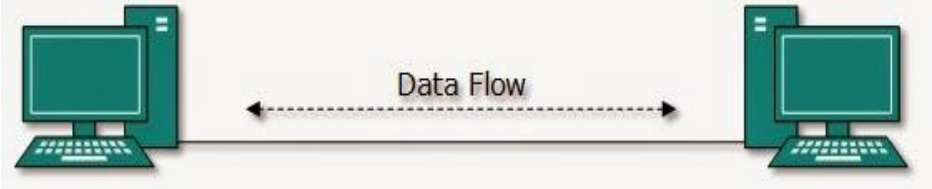
2.2.2. Jaringan Berdasarkan Fungsi

Pada dasarnya setiap jaringan komputer ada yang berfungsi sebagai *client* dan ada juga yang berfungsi sebagai *server*. Tetapi jaringan yang memiliki komputer khusus yang bertugas sebagai server sedangkan komputer lainya

sebagai client. Menurut Sofana (2012:110) Jaringan komputer di bagi menjadi dua jenis jaringan komputer, yaitu :

1. Peer-to-Peer Networks

   Peer to peer adalah jenis jaringan komputer di mana setiap komputer bisa menjadi server sekaligus client. Setiap komputer dapat menerima dan meberikan access dari/ke komputer lain.



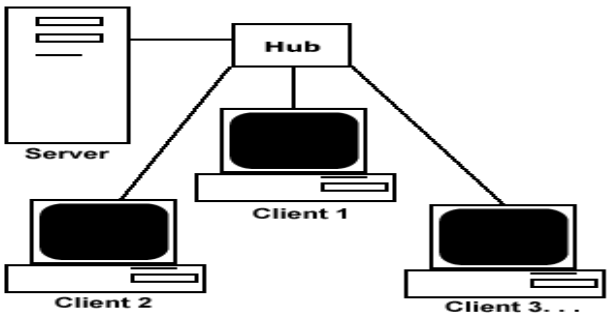
Sumber : http://www.nesabamedia.com/topologi-jaringan-komputer/

Gambar II.4

Ilustrasi Peer to peer

2. Client/Server Networks

   Menurut Sofana (2012:110) Client/Server adalah jaringan komputer yang salah satu(boleh lebih) komputernya difungsikan sebagai server untuk melayani komputer lain. Komputer yang dilayani oleh server disebut client. Layanan yang diberikan bisa berupa akses web, e-mail, file, atau yang lainya.



Sumber : http://www.mindpride.net/root/Extras/client_server_network.htm

Gambar II.5

Ilustrasi Client/Server

b.2.3. Perangkat Pendukung

1. Switch

Switch adalah *device* yang mampu menghubungkan beberapa segment atau kelompok LAN". Switch bekerja di layer 2 dari model referensi Osi. Switch memiliki kemapuan lebih dibandingkan dengan repeater atau hub. Tidak hanya menghubungkan antar jaringan LAN tetapi juga mampu mengatasi masalah *collision* yang dihadapi oleh *device* hub atau repeater. Switch sering digunakan pada *topologi star* dan *extended star*. Berikut ini adalah gambar Switch :

Sumber: www.dlink.com//media/Images/Products/DES/DES1016DF1Image%20LSide.png

Gambar II.6

Switch

2. Router

Router berasal dari akar kata *to route* yang berarti menelusuri. *Router* adalah perangkat khusus yang digunakan untuk mendeteksi dan mengirimkan paket data ke suatu jaringan tertentu yang dituju, yang menggunakan jenis *protocol* yang sama. *Router* pada dasarnya merupakan piranti pembagi jaringan secara logical bukan fisikal. *Router* biasanya digunakan untuk menghubungkan minimal 2 jaringan, misalnya antara dua buah jaringan LAN, jaringan WAN, atau antara jaringan LAN dan ISP (*Internet Service Provider*) atau penyedia layanan internet. Berikut ini adalah gambar *Router* :

Sumber: networkequipment.net/wpcontent/2012/02/router_cisco_1800.jpg

Gambar II.7

Router

3. Modem

Modem berasal dari kata *modulate-demodulate*. Secara teknis, modem merupakan alat yang digunakan untuk mengubah sinyal analog menjadi sinyal digital (*modulate*) atau sebaliknya mengubah sinyal digital menjadi analog (*demodulate*) agar dapat dipahami oleh semua perangkat yang terlibat dalam sebuah proses komunikasi. Berikut ini adalah gambar Modem :

Sumber: http://www.tp-link.co.id/resources/images/products/gallery/TD-8840T-01.jpg

Gambar II.8

Modem

2.3. Manajemen Jaringan

2.3.1. Topologi Jaringan komputer

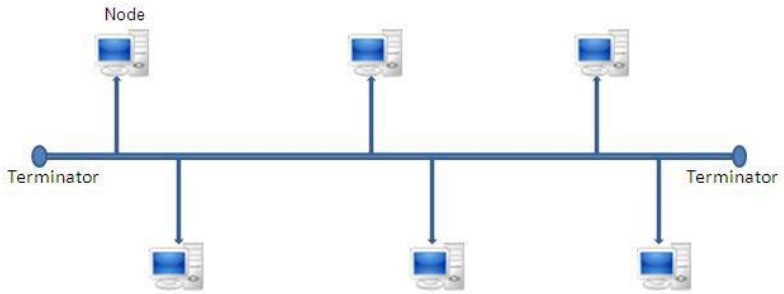
Menurut Kustanto (2013:9) “Topologi jaringan adalah infrastruktur fisik jaringan komputer yang digunakan untuk mengimplementasikan LAN”.

Topologi adalah sesuatu hubungan *node* (terminal komputer) yang satu dengan yang lainya menggunakan jalur (*path*). Semua design network diambil dari tiga topologi dasar yaitu *Bus*, *Star*, *Ring*, *Mesh dan Tree*. Berikut ini adalah beberapa topologi yang digunakan oleh beberapa perusahaan.

1. Topologi Bus (Garis Lurus)

Topologi Linear Bus terdiri dari satu jalur kabel utama dimana pada masing-masing ujungnya diberikan sebuah terminator. Semua nodes pada jaringan (file server, workstation, dan perangkat lainya) terkoneksi sebuah kabel utama

(*backbone*). Jaringan-jaringan *Ethernet* dan Local Talk menggunakan topologi linear ini. Berikut ini adalah gambar topologi *bus* **:**



Sumber: eridesktop.com/wp-content/uploads/2012/10/topologi-jaringan-bus.jpg

Gambar II.9

Topologi Bus

a. Keuntungan topologi *bus*

Hemat kabel, karena pada topologi *bus* hanya menggunakan kabel tunggal dan terpusat sebagai media transmisi sehingga tidak membutuhkan banyak kabel. *Layout* kabel sederhana, pada pemasangan topologi bus rancangan dan skema kabel yang digunakan sangat sederhana sehingga mudah dalam pemasangannya. Pengembangan jaringan komputer atau penambahan komputer baru baik sebagai *server* maupun *client* dapat dilakukan dengan mudah tanpa mengganggu komputer yang lain.

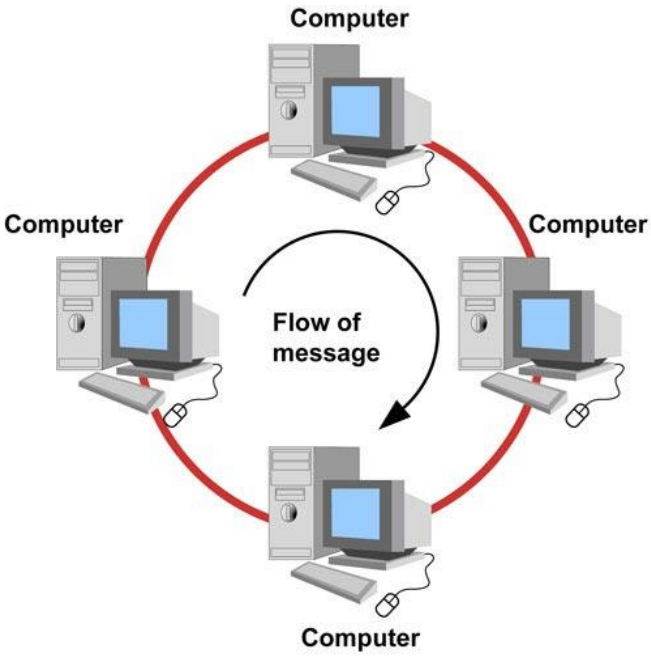
b. Kerungian topologi *bus*

Deteksi dan isolasi kesalahan sangat kecil sehingga jika jaringan mengalami gangguan, maka akan lebih sulit untuk mengidentifikasi kesalahan yang ada. Kepadatan lalu lintas pada jalur utama, karena

topologi *bus* menggunakan kabel terpusat sebagai media transmisi maka lalu lintas data akan sangat padat pada kabel utama. Jika kabel utama mengalami gangguan maka seluruh jaringan akan mengalami gangguan pula. Diperlukan *repeater* sebagai penguat sinyal jika akan menambahkan *workstation* dengan lokasi jauh.

2. Topologi Ring

Metode *token-ring* adalah cara menghubungkan komputer sehingga berbentuk *ring* (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai *loop*, data dikirimkan ke setiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya dan itu untuknya atau bukan. Berikut ini adalah gambar topologi *ring* :



Sumber: eridesktop.com/wp-content/uploads/2012/10/topologi-jaringanring.jpg

Gambar II.10

Topologi Ring

a. Kelebihan topologi *Ring*

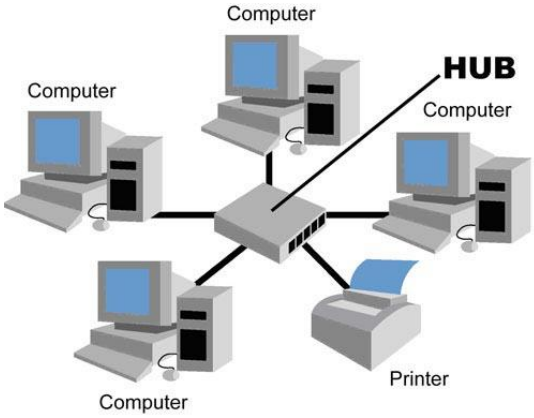
Kelebihan topologi ini adalah tidak terjadinya *Collision* atau tabrakan pegiriman data seperti pada topologi *bus*, karena hanya satu node dapat mengirim data pada suatu saat.

b. Kekurangan topologi *Ring*

Kekurangan dari topologi ini adalah setiap node dalam jaringan akan selalu ikut serta mengelola informasi yang dilewatkan dalam jaringan, sehingga jika terdapat gangguan di suatu node maka seluruh jaringan akan terganggu.

3. Topologi Star

Kontrol terpusat, semua *link* harus melewati pusat yang menyalurkan data tersebut ke semua simpul atau client yang di pilihnya. Simpul pusat dinamakan stasiun primer atau *server* dan lainnya dinamakan stasiun sekunder atau *client.* Setelah hubungan jaringan dimulai oleh *server* maka setiap *client* sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari *server*. Berikut ini gambar topologi *Star* :



Sumber: erideskto p.com/wp-content/uploads/2012/10/topologi-jaringan-star.jpg

Gambar II.11

Topologi Star

a. Keuntungan topologi *star*

1) Cukup mudah untuk mengubah dan menambah komputer ke dalam jaringan yang menggunakan topologi *star* tanpa menggangu aktifitas jaringan yang sedang berlangsung.

2) Apabila satu komputer yang mengalami kerusakan dalam jaringan maka komputer tersebut tidak akan membuat mati seluruh jaringan *star*.

3) Kita dapat menggunakan beberapa tipe kabel di dalam jaringan yang sama dengan *hub*/*switch* yang dapat mengakomodasi tipe kabel yang berbeda.

b. Kerugian topologi *star*

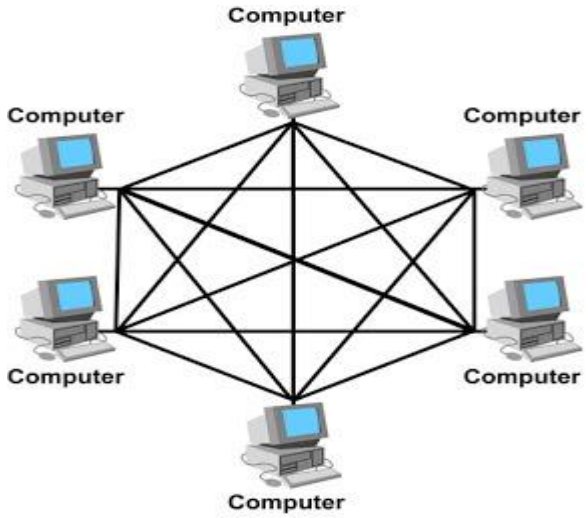
1) Memiliki satu titik kesalahan, terletak pada *hub/switch*. Jika *hub/switch* pusat mengalami kegagalan, maka seluruh jaringan akan gagal.

2) Membutuhkan lebih banyak kabel karena semua kabel jaringan harus ditarik ke satu *central point,* jadi lebih banyak membutuhkan kabel daripada topologi jaringan lain.

3) Jumlah terminal terbatas, tergantung dari *port* yang ada di *hub/switch*. Lalu lintas data yang padat dapat menyebabkan jaringan bekerja lebih lambat.

4. Topologi Mesh

Berikut ini adalah gambar dari topologi mesh :



Sumber: eridesktop.com/wp-content/uploads/2012/10/topologi-jaringan-mesh.jpg

Gambar II.12

Topologi *Mesh*

a. Karakteristik Topologi *Mesh*

1) Topologi *mesh* memiliki hubungan yang berlebihan antara peralatan-peralatan yang ada.

2) Susunannya pada setiap peralatan yang ada didalam jaringan saling terhubung satu sama lain.

3) Jika jumlah peralatan yang terhubung sangat banyak, tentunya ini akan sangat sulit sekali untuk dikendalikan dibandingkan hanya sedikit peralatan saja yang terhubung.

b. Keuntungan Topologi *Mesh*

1) Keuntungan utama dari penggunaan topologi *mesh* adalah *fault tolerance*

2) Terjaminnya kapasitas channel komunikasi, karena memiliki hubungan yang berlebih.

3) Relatif lebih mudah untuk di lakukan troubleshoot.

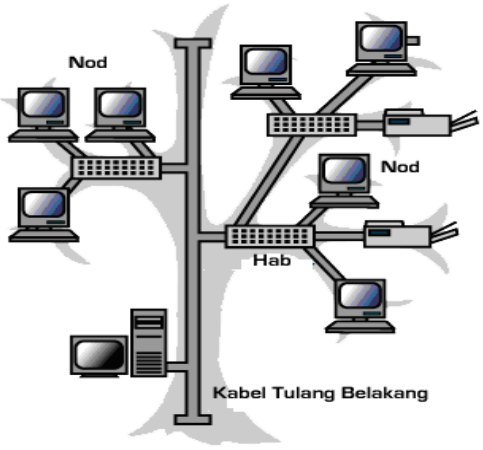
c. Kerugian Topologi *mesh*

1) Sulitnya pada saat melakukan instalasi dan melakukan konfigurasi ulang saat jumlah komputer dan peralatan-peralatan yang terhubung semakin meningkat jumlahnya.

2) Biaya yang besar untuk memelihara hubungan yang berlebihan.

5. Topologi Tree

Berikut ini adalah gambar topologi *tree :*



Sumber: erideskto p.com/wp-content/uploads/2012/10/topologi-jaringan-tree.jpg

Gambar II.13

Topologi *Tree*

1. Kelebihan Topologi *Tree*

   1) Seperti topologi star perangkat terhubung pada pusat pengendali *hub*, tetapi *hub* dibagi menjadi dua : *central hub* , dan *secondary hub.*

   2) Topologi *tree* ini memiliki keunggulan lebih mampu menjangkau jarak yang lebih jauh dengan mengaktifkan fungsi *Repeater* yang dimiliki oleh *hub*.

2. Kekurangan Topologi *Tree*

   Kabel yang digunakan menjadi lebih banyak sehingga perencanaannya yang matang dalam pengaturannya, termasuk didalamnya adalah tata letak ruang.

2.2.2. TCP / IP Subnetting

1. Pengetian TCP/IP

Menurut Kustanto (2008: 42),” IP atau *Internet Protocol* adalah sederetan angka biner 32 bit yang terbagi menjadi 4 kelompok, masing-masing kelompok terdiri atas biner 8 bit yang di pisahkan dengan tanda titik (dot)”.

Menurut Sofana (2010:43), “IP (*Internet Protocol*) *Address* merupakan alamat yang diberikan kepada komputer-komputer yang terhubung dalam suatu jaringan. *IP Address* terdiri dari 2 bagian , yaitu : *Network ID* dan *Host ID*”. *Network ID* menentukan alamat dalam jaringan (*Network Address*), sedangkan *host ID* menentukan alamat dari peralatan jaringan yang sifatnya unik untuk membedakan antara satu mesin dengan mesin yang lain. Ibarat sebuah alamat rumah, *Network ID* seperti alamat rumah dan *Host ID* seperti nomor rumah.

IP Address berdasarkan perkembangannya dibagi menjadi dua jenis :

a. IPv4 (*Internet Protocol* versi 4), merupakan *IP Address* yang terdiri dari 32 bit yang dibagi menjadi 4 segmen berukuran 8 bit.
b. IPv6 (*Internet Protocol* versi 6), merupakan *IP Address* yang terdiri dari 128 bit yang digunakan untuk mengatasi permintaan *IP Address* yang semakin meningkat.

2. Pengertian Subnetting

Menurut Wahidin (2008:47), “subnetting adalah teknik memecah suatu jaringan besar menjadi jaringan yang lebih kecil dengan cara mengorbankan bit Host ID pada subnet mask untuk dijadikan Network ID baru”. Berikut ini adalah tabel subnetting beserta kelas ip address:

Tabel II.1

Subnetting berserta Kelas IP Address

Mask Length	Host Length	Math	Max Host	Subnet Mask	Mask Octet	Binary Mask	Subnet Length
/32	0	2^0	1	255.255.255.255	4	11111111	0
/31	1	2^1	2	255.255.255.254	4	11111110	1
/30	2	2^2	4	255.255.255.252	4	11111100	2
/29	3	2^3	8	255.255.255.248	4	11111000	3
/28	4	2^4	16	255.255.255.240	4	11110000	4
/27	5	2^5	32	255.255.255.224	4	11100000	5
/26	6	2^6	64	255.255.255.192	4	11000000	6
/25	7	2^7	128	255.255.255.128	4	10000000	7
/24	8	2^8	256	255.255.255.0	4	11111111	8
KELAS C							
/23	9	2^9	512	255.255.254.0	3	11111110	9
/22	10	2^10	1,024	255.255.252.0	3	11111100	10
/21	11	2^11	2,048	255.255.248.0	3	11111000	11
/20	12	2^12	4,096	255.255.240.0	3	11110000	12
/19	13	2^13	8,192	255.255.224.0	3	11100000	13
/18	14	2^14	16,384	255.255.192.0	3	11000000	14
/17	15	2^15	32,768	255.255.128.0	3	10000000	15
/16	16	2^16	64,536	255.255.0.0	2	11111111	16
KELAS B							
/15	17	2^17	131,072	255.254.0.0	2	11111110	17
/14	18	2^18	262,144	255.252.0.0	2	11111100	18
/13	19	2^19	524,28	255.248.0.0	2	11111000	19

			8				
/12	20	2^20	1,048,576	255.240.0.0	2	11110000	20
/11	21	2^21	2,097,152	255.224.0.0	2	11100000	21
/10	22	2^22	4,194,304	255.192.0.0	2	11000000	22
/9	23	2^23	8,388,608	255.128.0.0	2	10000000	23
/8	24	2^24	16,777,216	255.0.0.0	1	11111111	24
KELAS A							

Sumber : http://www.diarypc.com/2013/11/tabel-subnet-mask-untuk-kelas-a-kelas-b-dan-c.html

2.3.3. Sistem Keamanan Jaringan

Menurut Kustanto (2013:12), "sistem keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer". Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer. Tujuannya adalah untuk mengantisipasi risiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung atau pun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Jika diamati mengenai keamanan, maka keamanan jaringan komputer dapat ditinjau dari segi bentuknya, yaitu sebagai berikut :

1. Keamanan *Hardware*

Keamanan *hardware* berkaitan dengan perangkat keras yang digunakan dalam jaringan komputer. Keamanan *hardware* sering dilupakan padahal merupakan hal utama untuk menjaga jaringan dari agar tetap stabil. Dalam keamanan *hardware, server* dan tempat penyimpanan data harus menjadi perhatian utama. Akses secara fisik terhadap *server* dan data-data penting harus dibatasi semaksimal mungkin.

Akan lebih mudah bagi pencuri data untuk mengambil *harddisk* atau *tape backup* dari *server* dan tempat penyimpanannya daripada harus menyadap data secara software dari jaringan. Sampah juga harus diperhatikan karena banyak sekali *hacker* yang mendatangi tempat sampah perusahaan untuk mencari informasi mengenai jaringan komputernya. Salah satu cara mengamankan *hardware* adalah menempatkan di ruangan yang memiliki keamanan yang baik. Lubang saluran udara perlu diberi perhatian karena dapat saja orang masuk ke ruangan server melaui saluran tersebut. Kabel-kabel jaringan harus dilindungi agar tidak mudah bagi *hacker* memotong kabel lalu menyambungkan ke komputernya.

Akses terhadap komputer juga dapat dibatasi dengan mengeset keamanan di level BIOS yang dapat mencegah akses terhadap komputer, memformat *harddisk*, dan mengubah isi *Main Boot Record* (tempat informasi partisi) *harddisk*. Penggunaan *hardware* autentifikasi seperti *smart card* dan *finger print detector* juga layak dipertimbangkan untuk meningkatkan keamanan.

2. Keamanan *Software*

Sesuai dengan namanya, maka yang harus diamankan adalah perangkat lunak. Perangkat lunak yang kita maksud disini bisa berupa sistem operasi, sistem aplikasi, data dan informasi yang tersimpan dalam komputer jaringan terutama pada *server*. Contohnya, jika *server* hanya bertugas menjadi *router*, tidak perlu *software web server* dan *FTP server* diinstal. Membatasi *software* yang dipasang akan mengurangi konflik antar *software* dan membatasi akses, contohnya jika *router* dipasangi juga dengan *FTP server*, maka orang dari luar dengan login *anonymous* mungkin akan dapat mengakses *router* tersebut.

Software yang akan diinstal sebaiknya juga memiliki pengaturan keamanan yang baik. Kemampuan enkripsi (mengacak data) adalah spesifikasi yang harus dimilki oleh *software* yang akan digunakan, khusunya enkripsi 128 bit karena enkripsi dengan sistem 56 bit sudah dapat dipecahkan dengan mudah saat ini. Beberapa *software* yang memiliki lubang keamanan adalah *mail server sendmail* dan aplikasi telnet. *Sendmail* memiliki kekurangan yaitu dapat ditelnet tanpa *login* di *port* (25) dan pengakses dapat membuat email dengan alamat palsu. Aplikasi telnet memiliki kekurangan mengirimkan data tanpa mengenkripsinya (mengacak data) sehingga bila dapat disadap akan sangat mudah untuk mendapatkan data.

Hal kedua yang perlu diperhatikan adalah *password*. Sebaiknya diset panjang *password* minimum untuk mempersulit *hacker* memecahkan *password*. *Password* juga akan semakin baik jika tidak terdiri huruf atau angka saja, huruf kecil atau kapital semua, namun sebaiknya dikombinasi. Enkripsi dapat menambah keamanan jaringan dengan cara mengacak *password* dan *username*,

baik dalam *record* di *host* maupun pada saat *password* dan *username* itu dilewatkan jaringan saat melakukan *login* ke komputer lain.

Routing tidak terlepas pula dari gangguan keamanan. Gangguan yang sering muncul adalah pemberian informasi palsu mengenai jalur *routing* (*source routing* pada *header IP*). Pemberian informasi palsu ini biasanya dimaksudkan agar datagram-datagram dapat disadap. Untuk mencegah hal seperti itu, *router* harus diset agar tidak mengijinkan *source routing* dan dalam *protokol routing* disertakan autentifikasi atau semacam *password* agar informasi *routing* hanya didapat dari *router* yang terpercaya.

2.3.4. Virtual Private Network (VPN)

Menurut Sofana (2012:228) VPN boleh jadi termasuk ke dalam salah satu kandidat WAN. Namun, VPN menggunakan WAN sebagai media transportasi data.

VPN atau *Virtual Private Network* adalah teknologi jaringan komputer yang memanfaatkan media komunikasi publik seperti internet, untuk menghubungkan beberapa jaringan lokal. Informasi yang berasal dari *node-node* VPN akan "dibungkus" (*tunneled*) dan kemudian mengalir melalui jaringan publik. Sehingga informasi menjadi aman dan tidak mudah dibaca oleh yang lain.

Umumnya VPN diimplementasikan oleh lembaga/perusahaan besar. Biasanya perusahaan ini memiliki kantor cabang yang lokasinya cukup jauh dari kantor pusat. Sehingga diperlukan solusi yang tepat untuk mengatasi keterbatasan LAN. VPN dapat menjadi sebuah pilihan yang cukup tepat. Tentu saja VPN boleh diimplementasikan oleh pengguna rumah atau siapapun yang membutuhkannya.

Menurut Sofana (2012:229) VPN sendiri memiliki beberapa jenis, dan penulis menggunakan metode EzVPN :

1. EzVPN

EzVPN adalah VPN yang mudah diimplementasikan karena semua parameter dibuat diisi concentrator (VPN Server), sehingga mengurangi konfigurasi yang lebih kompleks pada client, EzVPN menyederhanakan proses instalasi karena ketika client EzVPN inisialisasi tunnel, server EzVPN melakukan push parameter policy IPSec terhadap client dan membentuk komunikasi tunnel VPN.

Menurut Sofana (2012:31) untuk mengamankan informasi yang berasal dari jaringan internal, VPN menggunakan beberapa metode keamanan, seperti :

a. *Firewall*

Firewall menyediakan penghalang antara jaringan lokal dengan internet. Pada firewall dapat ditentukan port-port mana saja yang boleh dibuka, paket apa saja yang boleh melalui *firewall*, dan *protocol* apa saja yang diperbolehkan.

b. *Enkripsi*

Enkripsi merupakan metode yang umum untuk mengamankan data. Informasi akan diacak sedemikian rupa sehingga sukar dibaca oleh orang lain. Secara umum ada dua metode enkripsi, yaitu:

1. Symmetric-key encryption

Pada metode ini, masing-masing komputer pengirim dan penerima harus memiliki "*key*" yang sama.

2. Public-key encryption

Pada metode ini, komputer pengirim menggunakan *public-key* milik komputer penerima untuk melakukan enkripsi.

c. IPSec

Internet Protocol Security Protocol (IPSec) menyediakan fitur security yang lebih baik. Seperti algoritma enkripsi yang lebih bagus. *IPSec* menggunakan dua mode enkripsi, yaitu :

1) Tunnel

Tunnel melakukan enkripsi pada *header* dan *payload* pada masing-masing paket.

2) Transport

Transport hanya melakukan enkripsi pada *payload* masing-masing paket.

Secara umum ada dua asumsi yang digunakan untuk menentukan *security* pada VPN, yang pertama yaitu dengan mempercayai bahwa network yang digunakan aman dan dapat dipercaya. Ini yang disebut sebagai trusted model, yang kedua adalah sebaliknya, diasumsikan network tidak aman sehingga diperlukan mekanisme *security* tertentu, ini yang disebut *secure* model.

2. AAA

AAA (Authentication, Authorization dan Accounting) merupakan nama yang diambil berdasarkan pada fungsi yang dapat dilakukannya yakni sistem melakukan kegiatan otentikasi, otorisasi dan akunting terhadap setiap orang yang mengakses jaringan secara remote. AAA terdiri dari:

a. Authentication : sebuah metode untuk memverifikasi user, berbasiskan pada username dan password, Token card atau respon Challenge.

b. Authorization : menyediakan access control terhadap resource atau operasi yang dapat dilakukan oleh user.

c. Accounting : untuk menelusuri tindakan user, resource yang diakses dan lamanya mengakses suatu resource.

2.4. Konsep Penunjang Usulan

2.4.1. GNS3

GNS3 (Graphic Network Simulator) adalah software simulasi jaringan komputer berbasis GUI yang mirip dengan Cisco Packet Tracer. Namun pada GNS3 memungkinkan simulasi jaringan yang komplek, karena menggunakan operating system asli dari perangkat jaringan seperti cisco dan juniper. Sehingga kita berada kondisi lebih nyata dalam mengkonfigurasi router langsung daripada di Cisco Packet Tracer. GNS3 adalah alat pelengkap yang sangat baik untuk laboratorium nyata bagi network engineer.

2.4.2. Wireshark

Wireshark merupakan salah satu tools atau aplikasi “Network Analyzer” atau Penganalisa Jaringan. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan, sampai pada digunakan pula untuk sniffing (memperoleh informasi penting seperti password email, dll). Wireshark sendiri

merupakan free tools untuk Network Analyzer yang ada saat ini. Dan tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan user karena menggunakan tampilan grafis atau GUI (Graphical User Interface).