BAB 2

LANDASAN TEORI

2.1 Pengertian Jaringan

Jaringan komputer menurut Andrew S. Tanenbaum (1997, p1) adalah sekumpulan computer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya. Ada dua model koneksi dalam jaringan yaitu:

2.1.1 *Internet*

Pengertian internet memiliki arti yang cukup luas dimana kata internet itu sendiri merupakan singkatan kata dari *interconnection-networking*, bila dijabarkan secara sistem global maka internet merupakan jaringan komputer diseluruh penjuru dunia yang saling terhubung satu sama lain dengan menggunakan standar *Internet Protocol Suite* (**TCP/IP**) sehingga antara komputer dapat saling mengakses informasi dan bertukar data. Internet mencangkup segala sesuatu secara luas baik itu komputerisasi maupun telekomunikasi.

2.1.2 *Protokol*

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras.

2.2 Media Transmisi

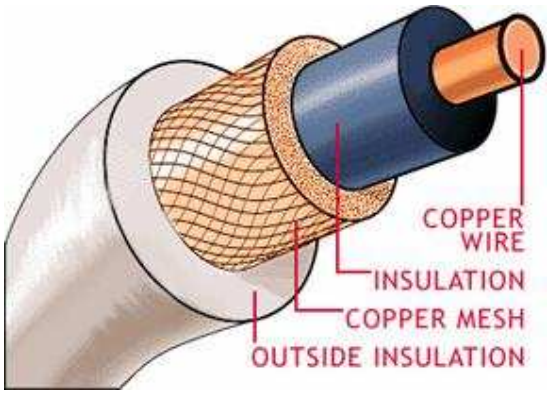
Sesuai dengan fungsinya yaitu untuk membawa aliran bit data dari satu komputer ke komputer lainnya, maka dalam pengiriman data memerlukan media transmisi yang nantinya digunakan untuk keperluan *transmisi*. Media *transmisi* memerlukan suatu jalur fisik antara *transmitter* dan *receiver* dalam sistem *transmisi* data. Media *transmisi* dibagi menjadi dua yaitu:

2.2.1 Media Terarah (*Guided Transmision Data*)

Suatu media yang digunakan untuk mengirimkan data, dimana arah ujung yang satu dengan ujung yang lainnya sudah jelas, sebagai contohnya adalah kabel. Bila sumber data dan penerima jaraknya tidak terlalu jauh dan dalam lokasi tersebut, maka dapat digunakan kabel sebagai media *transmisi*nya. Kabel merupakan komponen fisik jaringan yang paling rentan dan harus diinstalasi secara cermat dan teliti. Kabel sebagai media *transmisi* yang terpadu yang secara umum digunakan untuk *transmisi* data adalah *coaxial*, *twisted pair*, *fiber optic*.

2.2.1.1 *Coaxial*

Coaxial secara umum digunakan sebagai antenna televisi, *transmisi* telepon jarak jauh, link komputer dan LAN. *Coaxial* dapat digunakan untuk signal analog maupun digital. *Coaxial* terdiri dua konduktor, dibentuk untuk beroperasi pada pita frekuensi. Kabel *coaxial* terdiri dari dua penghantar yaitu penghantar dalam yang berupa inti tembaga dan penghantar luar yang berbentuk serabut (*shield*). Berikut contoh dari kabel *coaxial*.



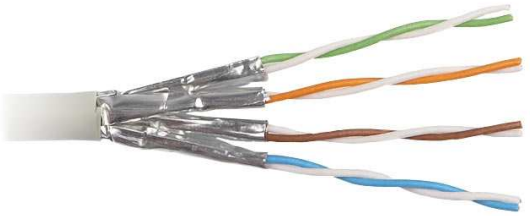
Gambar 2.1 Kabel *Coaxial*

Sumber : http://anangss.blogspot.com/2009/09/macam-macam-kabel-jaringan.html

2.2.1.2 *Twisted Pair*

Kabel *twisted pair* dapat dibagi menjadi dua macam yaitu *shielded* yang memiliki selubung pembungkus dan *unshielded* yang tidak mempunyai selubung pembungkus. Kabel ini merupakan

sepasang kabel yang di *twist* satu sama lain dengan tujuan untuk mengurangi interferensi listrik. Ada dua jenis kabel *twisted pair* yaitu UTP (*Unshielded Twisted Pair*) dan STP (*Shielded Twisted Pair*) yang dapat melewatkan signal sampai 10-100 Mbps dan hanya dapat menangani satu *channel* data (*baseband*). Koneksi pada *twisted pair* biasanya menggunakan konektor RJ-11 atau RJ-45. Kabel STP lebih tahan interferensi daripada UTP dan dapat beroperasi pada kecepatan yang lebih tinggi sampai 100 Mbps, namun lebih sulit ditangani secara fisik. Berikut contoh kabel STP (gambar 2.2) dan kabel UTP (gambar 2.3)



Gambar 2.2 Kabel STP

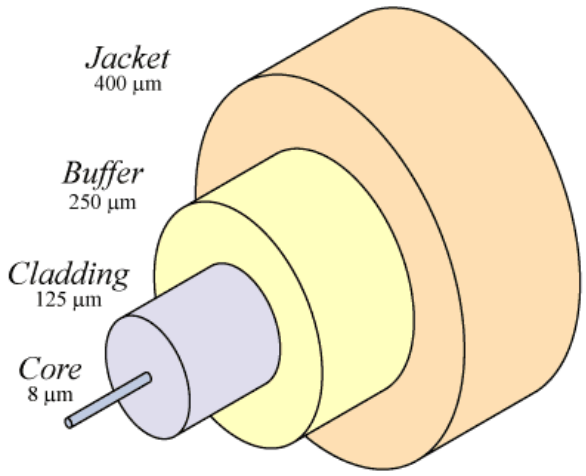
Gambar 2.3 Kabel UTP

Sumber : http://apotas.blogspot.com/2010/10/twisted-pair-ethernet-cable.html

2.2.1.3 *Fiber Optic*

Fiber optic adalah teknologi perkabelan terkini yang memiliki kecepatan sangat tinggi. Kabel *fiber optic* bentuknya sama dengan kabel *coaxial*. Jenis kabel ini tidak menggunakan tembaga (*cooper*), melainkan serat *optic* dimana signal yang

dialirkan berupa berkas cahaya. Kabel *fiber optic* mampu mengirimkan *bandwidth* lebih banyak dan biasanya digunakan untuk komunikasi antar *backbone* atau bisa juga digunakan untuk LAN dengan kecepatan yang tinggi. Pada pusat kabel terdapat inti kaca yang merupakan tempat cahaya akan berpropagasi. Kabel *fiber optic* terdiri dari dua jenis, yang dikenal sebagai *singlemode* dan *multimode*. Kabel *singlemode* dapat menjangkau jarak yang lebih jauh dan hanya mengirim satu signal pada satu waktu. Sedangkan untuk kabel *multimode* dapat mengirim signal yang berbeda dan mengirim data pada sudut *refraksi* yang berbeda pada saat yang bersamaan. Kabel *singlemode* dapat menjangkau ratusan kilometer sedangkan *multimode* biasanya hanya mencapai 550 meter atau kurang.



Gambar 2.4 Kabel *Fiber Optic*

Sumber : http://10110163.blog.unikom.ac.id/sekilas-tentang.4ak

2.2.2 Media Tak Terarah (*Un-Guided Transmission Data*)

Suatu media yang digunakan untuk mengirimkan data, dimana arah ujung yang satu dengan ujung yang lainnya tersebar, contohnya nirkabel (*wireless*). Komunikasi ini mengirimkan signal ke udara berdasarkan spectrum elektromagnetik.

2.2.2.1 Transmisi Radio

Perkembangan teknologi komunikasi radio sangat pesat, penggunaan *wireless* LAN sudah semakin popular. Untuk mengirimkan data menggunakan komunikasi radio ada beberapa cara yaitu memancarkan langsung, sesuai dengan permukaan bumi dan dipantulkan melalui lapisan *atmosfer*. Komunikasi radio ini menggunakan *frekuensi* khusus supaya tidak mengakibatkan *interferensi* dengan pengguna *frekuensi* lainnya. *Frekuensi* yang boleh digunakan disebut ISM band (*Industrial, Scientific and Medical*).

2.2.2.2 Komunikasi Satelit

Komunikasi ini digunakan untuk komunikasi jarak jauh dimana menghubungkannya diperlukan teknologi satelit. Menurut jaraknya satelit bias dikategorikan menjadi *geostationary*, *medium-earth orbit*, *low-earth orbit*. Untuk menghubungi site yang lain, bisa dilakukan dengan *Very Small Aperture Terminal* (VSAT). VSAT adalah sebuah stasiun bumi kecil yang bekerja pada satelit geostationer dan digunakan untuk berbagai aplikasi di dunia telekomunikasi, termasuk data interaktif pelayanan komunikasi suara, data, video digital serta dapat diaplikasikan untuk jaringan WAN (*Wide Area Network*). Jaringan VSAT sendiri dapat digabungkan dengan jaringan lain yang sudah ada misalnya jaringan telepon dan jaringan internet.

2.2.2.3 *Frame Relay*

Frame relay merupakan suatu layanan data paket yang memungkinkan beberapa pengguna menggunakan satu jalur transmisi pada waktu yang bersamaan. Untuk lalu lintas komunikasi yang padat, *frame relay* jauh lebih efisien daripada *leased line* yang disediakan khusus untuk satu pelanggan (*dedicated*). Dalam teknik telekomunikasi, paket *switching* dikembangkan untuk memenuhi komunikasi data yang sifatnya cepat dan akurat. Pada paket data ada istilah *frame* yang menyatakan batas bingkai sebuah paket. Batas *frame* ditandai

dengan *flag*. Dan data akan dibawa sepanjang jalur komunikasi dalam bentuk *frame-frame*.

2.2.2.4 *Wireless*

Wireless atau *wireless network* merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Pada dasarnya *wireless* dengan LAN merupakan sama-sama jaringan komputer yang saling terhubung antara satu dengan lainnya, yang membedakan antara keduanya adalah media jalur lintas data yang digunakan, jika LAN masih menggunakan kabel sebagai media lintas data, sedangkan *wireless* menggunakan media gelombang radio/udara. Penerapan dari aplikasi wireless network ini antara lain adalah jaringan nirkabel diperusahaan, atau mobile communication seperti handphone, dan HT.

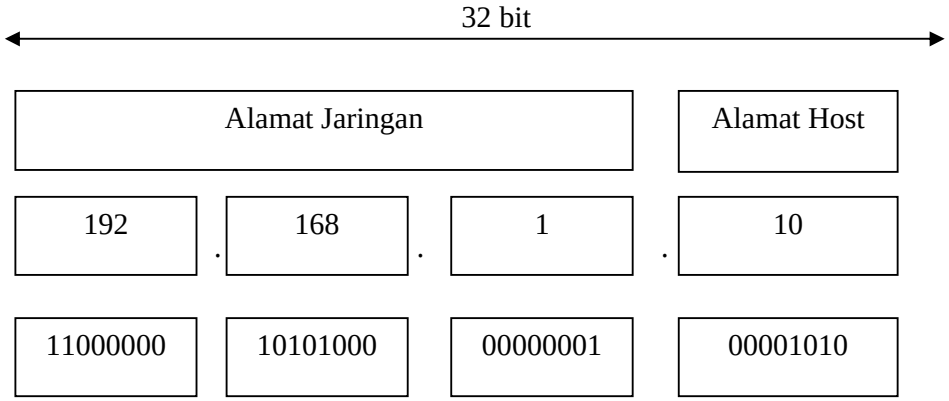
2.3 IP *Address (Internet Protocol Address)*

IP *Address* menurut Rendra Towidjojo (2012, p13) adalah metode pengalamatan pada jaringan komputer dengan memberikan sederetan angka pada komputer (*host*), router atau peralatan jaringan lainnya. IP Address sebenarnya bukan diberikan kepada komputer (host) atau router, melainkan pada interface jaringan dari host / router tersebut.

Jika sebuah host / router memiliki 2 interface jaringan maka host tersebut bisa saja menggunakan 2 IP Address sebagai alamatnya. Angka yang digunakan adalah bilangan biner (bilangan yang hanya mengenal angka 1 dan 0). Pengalamatan IP Address merupakan pengalamatan yang memungkinkan alamat-alamat komputer diatur secara logika oleh Administrator jaringan (Admin).

Baik host dan router yang berada dalam jaringan harus menggunakan IP Address yang unik. Unik artinya tidak boleh ada dua host yang memiliki IP Address yang sama dalam satu broadcast domain. Karena nomor tersebut

merupakan alamat atau pengenal bagi host tersebut dalam jaringan maka pengiriman data tentu akan kacau jika ada dua komputer yang memiliki alamat yang sama.



Gambar 2.5 IP *Address* dengan representasi dalam biner

IPv4 memiliki 5 jenis kelas yaitu, A, B, C, D, dan E. Tetapi umumnya yang digunakan hanya kelas A, B, dan C. Berikut skema kelas pada IPv4.

Tabel 2.1 IPv4

Kelas	Format	*Range* Alamat	Jumlah *Host* Maksimal
A	N.H.H.H	1.0.0.0 – 126.0.0.0	$2^{24} – 2$
B	N.N.H.H	128.1.0.0 – 191.254.0.0	$2^{16} – 2$
C	N.N.N.H	192.0.1.0 – 223.255.254.0	$2^{8} – 2$
D	-	224.0.0.0 – 239.255.255.255	-
E	-	240.0.0.0 – 254.255.255.255	-

Keterangan: N = Alamat Jaringan ; H = Alamat Host

2.4 Subnet Mask dan Subnetting

Subnetting menurut Rendra Towidjojo (2012, p34) adalah teknik memecah sebuah jaringan *(network)* menjadi beberapa jaringan baru. Hasil dari subnetting adalah beberapa jaringan kecil yang disebut sub jaringan atau sub network.

Subnet mask digunakan untuk menentukan bagian manakah dari sebuah alamat yang merupakan alamat jaringan dan bagian manakah yang merupakan alamat *host.* Subnet mask direpresentasikan dengan nilai 1 dan 0 dimana bagian dengan angka 1 merepresentasikan alamat jaringan dan bagian dengan angka 0

merepresentasikan alamat *host*, akan tetapi untuk lebih mudah maka biasanya direpresentasikan dengan bilangan desimal.

Tidak semua jaringan membutuhkan subnet, dalam hal ini berarti sebuah jaringan menggunakan *subnet mask default*. *Subnet default* untuk masing-masing kelas tidak dapat diubah. Maksudnya adalah kita tidak bisa menggunakan sebuah subnet 255.255.0.0 untuk kelas A, jika kita mencobanya maka alamat tersebut menjadi tidak *valid* bahkan biasanya tidak diperbolehkan mengetikkan *subnet mask* yang salah tersebut.

Tabel 2.2 Subnet Mask Default

Kelas	Format	Subnet Mask Default
A	N.H.H.H	255.0.0.0
B	N.N.H.H	255.255.0.0
C	N.N.N.H	255.255.255.0

Subnetworks atau *subnet* adalah sekelompok komputer dan peralatan jaringan yang memiliki routing *prefix* IP *address* yang sama. Dengan menggunakan *subnetting*, sebuah jaringan yang besar bisa dipecah dan dibentuk menjadi sebuah jaringan-jaringan yang lebih kecil. Proses tersebut dinamakan dengan *subnetting*. Tanpa adanya *subnetting* di jaringan besar, lalu lintas paket bisa mencapai nilai rata-rata yang cukup tinggi. *Subnetting* juga membantu dalam mengatasi keterbatasan jumlah *host* pada IPv4. Oleh karena itu, jika dilihat dari posisinya di dalam sebuah jaringan, alamat IP dibagi menjadi 2 golongan, yaitu:

a. IP *public* yaitu IP *address* yang langsung terhubung ke dalam internet dan bersifat unik.
b. IP *private* yaitu IP *address* yang bersifat tidak umum yang hanya dikenali oleh jaringan lokal saja.

Tabel 2.3 IP Private

Kelas	*Range* IP
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Ketika sudah diputuskan untuk memilih sebuah *subnet mask*, maka kita perlu menentukan beberapa hal yaitu, jumlah *subnet*, alamat *network*, *host* yang valid, dan alamat *broadcast*. Berikut ini adalah contoh perhitungan *subnet* untuk kelas C.

Subnetting pada IP address 110.5.96.0 dengan *subnet mask* 255.255.255.192.

a. *Subnet mask* diubah menjadi bilangan biner. 255.255.255.192 = 11111111.11111111.11111111.11000000
b. Untuk menghitung banyaknya *subnet* dihitung dengan 2^x dimana x adalah banyaknya bilangan 1 pada octet terakhir. $2^2 = 4$, berarti ada 4 subnet.
c. Untuk menghitung banyaknya masing-masing *host* pada tiap subnet dihitung dengan 2^y-2 dimana y adalah banyaknya bilangan 0. 2^6-2 = 62.
d. Untuk lebih mempermudah, kita bias membuat tabel seperti berikut.

Tabel 2.4 Subnetting Kelas C

Subnet	*Network*	*Host Min*	*Host Max*	*Broadcast*
1	110.5.96.0	110.5.96.1	110.5.96.62	110.5.96.63
2	110.5.96.64	110.5.96.65	110.5.96.126	110.5.96.127
3	110.5.96.128	110.5.96.129	110.5.96.190	110.5.96.191
4	110.5.96.192	110.5.96.193	110.5.96.254	110.5.96.255

2.5 *Autonomous System Number* (ASN)

APNIC (*the Asia Pacific Network Information Centre*) adalah *Regional Internet Registry* untuk kawasan Asia Pasifik, yang bertanggung jawab mendistribusikan *address space* internet *public* dan sumber daya yang berkaitan, termasuk *Autonomous System Number* (ASN). *Autonomous System* (AS) adalah kelompok yang terdiri dari satu atau lebih IP *prefix* yang terkoneksi yang dijalankan oleh satu atau lebih operator jaringan dibawah satu kebijakan *routing* yang didefinisikan dengan jelas. *Autonomous System Number* (ASN) adalah nomor *two-byte* unik yang diasosiasikan dengan AS. ASN digunakan sebagai pengidentifikasi yang memungkinkan AS untuk saling menukar informasi

routing dinamik dengan AS yang lain. Protokol *routing* eksterior seperti *Border Gateway Protocol* (BGP) membutuhkan ASN untuk saling bertukar informasi antara jaringan.Seperti hal nya IP *address,* ASN juga dibagi menjadi 2 jenis yaitu, ASN *public* dan ASN *private*. ASN *public* memiliki *range* dari 1 – 64511 sedangkan ASN *private* memiliki *range* dari 64512 – 65535.

Menurut Rendra Towidjojo (2012, p135) dalam *Autonomous System,* protokol routing dapat dibagi menjadi dua, yaitu :

2.5.1 *Interior Gateway Protocol* (IGP)

Interior Gateway Protocol adalah protokol routing yang digunakan pada router-router yang berada dalam satu *Autonomous System.* Atau dengan kata lain IGP digunakan untuk menghubungkan jaringan-jaringan dalam sebuah *Autonomous System.* Contohnya bila ingin menerapkan routing pada sebuah jaringan internal kampus atau internal sebuah perusahaan, maka harus menggunakan protokol routing kategori IGP. Protokol routing yang termasuk IGP adalah RIP, IGRP, EIGRP, OSPF, BGP (iBGP) ,dan IS-IS.

2.5.2 *Exterior Gateway Protocol* (EGP)

Exterior Gateway Protocol adalah protokol routing yang digunakan pada router-router yang berasal dari *Autonomous System* yang berbeda. Atau dapat dikatakan EGP digunakan untuk menghubungkan jaringan-jaringan yang berasal dari *Autonomous System* yang berbeda. Contoh penggunaan EGP dapat dilihat jika ingin dilakukan routing antar kampus atau antar ISP. Satu-satunya protokol routing yang digunakan untuk keperluan ini adalah BGP (eBGP).

2.6 *Routing*

Routing menurut Rendra Towidjojo (2012, p47) adalah proses penentuan jalur terbaik (*best path*) untuk mencapai suatu network tujuan. Routing juga dapat berarti proses memindahkan paket data dari host pengirim ke host tujuan dimana host pengirim dan host tujuan tidak berada dalam satu *network.*

Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router-

router yang saling terhubung dalam jaringan internet turut serta dalam dalam sebuah algoritma *routing* terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP dari sistem ke sistem lain. Proses *routing* dilakukan secara *hop by hop*. IP tidak mengetahui jalur keseluruhan menuju tujuan setiap paket. IP *routing* hanya menyediakan IP Address dari router berikutnya yang menurutnya lebih dekat ke *host* tujuan.

Router dapat digunakan untuk menghubungkan sejumlah LAN sehingga trafik yang dibangkitkan oleh suatu LAN terisolasikan dengan baik dari trafik yang dibangkitkan oleh LAN yang lain. Jika dua atau lebih LAN terhubung dengan router, setiap LAN dianggap sebagai *subnetwork* yang berbeda.

Router terletak pada Layer 3 dalam OSI, router hanya perlu mengetahui Net-Id (Nomor Jaringan) dari data yang diterimanya untuk diteruskan ke jaringan yang dituju. Cara kerjanya setiap paket data yang datang, paket data tersebut dibuka lalu dibaca *header* paket datanya kemudian mencocokkan atau membandingkan ke dalam tabel yang ada pada *routing* jaringan dan diteruskan ke jaringan yang dituju melalui suatu *interface*.

2.6.1 *Routing* Statik

Routing Statik (*Static Routing*) menurut Rendra Towidjojo (2012, p74) adalah teknik routing yang dilakukan dengan memasukan *entry route* ke network tujuan (*remote network*) ke dalam table routing secara manual oleh Administrator jaringan. Bila sebuah router memiliki satu network tujuan, maka Administrator jaringan juga harus memasukkan satu *entry route* ke network tersebut. Jika terdapat dua *remote network* , maka Administrator akan memasukkan *entry route* sebanyak dua kali untuk masing – masing *remote network* tersebut. Dalam memasukkan *entry route* tersebut Administrator harus dapat mengetahui dengan pasti *gateway* yang akan digunakan untuk mencapai *remote network.* Untuk jaringan yang terdiri dari beberapa router, maka penentuan *gateway* maupun jalur (*path)* harus dilakukan dengan lebih cermat.

2.6.2 *Routing* Dinamik

Menurut Rendra Towidjojo (2012, p76) , routing dinamik tidak seperti pada routing static dimana *entry route* pada tabel routing diisi

manual oleh Administrator jaringan, routing dinamik merupakan teknik routing dimana router akan memasukkan sendiri *entry-entry route* ke dalam tabel routingnya. Untuk melakukan itu, router akan saling bertukar informasi routing dengan router yang lain tentang jaringan yang mereka ketahui masing-masing. Setelah mempelajari keberadaan jaringan lain beserta cara mencapai jaringan tersebut, router akan membuat *entry route* dan pada akhirnya memasukkannya ke dalam tabel routing.

2.6.3 Protokol *Routing*

Protokol *routing* adalah komunikasi antara router-router. Protokol *routing* mengijinkan router-router untuk *sharing* informasi tentang jaringan dan koneksi antar router. Router menggunakan informasi ini untuk membangun dan memperbaiki *table routingnya*. Berikut contoh dari protokol *routing*:

2.6.3.1 *Open Shortest Path First* (OSPF)

Menurut Rendra Towidjojo (2012, p231) *Open Shortest Path First* (OSPF) merupakan protokol routing *link state* dan digunakan untuk menghubungkan router-router yang berada dalam satu *Autonomous System* (AS), sehingga protokol routing ini termasuk juga kategori *Interior Gateway Protocol* (IGP). OSPF dikembangkan untuk menutupi kekurangan-kekurangan yang dimiliki oleh RIP, terutama pengimplementasian di jaringan berskala besar.

Link state merupakan routing protokol yang digunakan pada OSPF, *link state* routing protokol mampu mengenali topologi dari jaringan. Router-router yang menjalankan protokol routing *link state* bahkan mampu mengetahui status (*state*) dari setiap jalur (*link*) antar router yang ada dalam jaringan. Routing protokol *link state* melakukan serangkaian proses yang kompleks untuk menyusun tabel-tabel routingnya. Router yang menjalankan protokol routing *link state* akan menggunakan *hello packet* untuk mengetahui keberadaan dan status dari router tetangga, menyusun *link state advertisement* (LSA), saling mengirimkan LSA keseluruh

router dalam jaringan, membangun *link state database* dan barulah kemudian menyusun tabel routingnya.

Protokol routing *link state* menggunakan algoritma routing yang disusun oleh Edsger Dijkstra. Oleh sebab itu protokol routing ini sering disebut juga protokol routing yang menggunakan algoritma Dijkstra atau *Shortest Path First* (SPF). Disebut *shortest path first* karena protokol routing ini selalu mencari jalur (*path*) yang terpendek untuk mencapai suatu *remote network*. Dalam mencari *path* terpendek, algoritma OSPF tidak menggunakan jumlah lompatan (*hop count*). Algoritma OSPF menggunakan *cost* kumulatif dari setiap *link* antar router untuk mencapai suatu *remote network*. Algoritma OSPF akan memilih *path* dengan *cost* terendah sebagai *best path*, walaupun *path* tersebut akan memiliki *hop count* yang lebih banyak dibanding dengan *path* lain dan juga OSPF memiliki beberapa keunggulan yaitu informasi akan diupdate jika ada perubahan topologi jaringan, lebih cepat untuk konvergen, tidak rentan terhadap routing loop dan lebih sedikit menghabiskan bandwidth dibanding distance vector.

OSPF pertama kali dikembangkan pada tahun 1987 oleh Internet Engineering Task Force (IETF) dan yang pertama kali dipublikasikan adalah OSPFv1. OSPFv1 ini tidak pernah diimplementasikan dan selalu disempurnakan. Pada tahun 1991, OSPFv2 dipublikasikan oleh John Moy dan juga selalu mengalami penyempurnaan. OSPFv2 ditujukan untuk jaringan IPv4. Saat ini juga telah ada OSPFv3 yang ditunjukan untuk implementasi jaringan yang menggunakan IP Address versi 6 (IPv6).

Untuk dapat menangani jaringan yang berskala besar, maka OSPF menerapkan konsep area dalam implementasinya. Sehingga pengimplementasian OSPF dikenal dengan dua cara, yaitu *Single Area* OSPF dan *Multi Area* OSPF. Untuk jaringan yang masih berskala kecil, dapat diterapkan *Single Area* OSPF, namun untuk jaringan yang berskala besar maka harus diterapkan *Multi Area* OSPF.

OSPF memiliki karakteristik sebagai berikut :

- Merupakan link state routing protocol, sehingga setiap router memiliki gambaran topologi jaringan.
- Menggunakan *Hello Packet* untuk mengetahui keberadaan *neighbor router.*
- *Routing update* hanya dikirimkan bila terjadi perubahan dalam jaringan dan dikirimkan secara *multicast.*
- Dapat bekerja dengan konsep hirarki karena dapat dibagi berdasarkan konsep *area.*
- Menggunakan *cost* sebagai *metric*, dengan *cost* terendah yang akan menjadi *metric* terbaik.
- Tidak memiliki keterbatasan *hop count*, tidak seperti RIP yang hanya menjangkau 15 *hop count.*
- Merupakan *classless routing protocol.*
- Secara default nilai *Administrative Distance 110.*
- Memiliki fitur *authentication* pada saat pengiriman *routimg update.*

OSPF merupakan protokol *routing* yang menggunakan konsep hirarki *routing*, artinya OSPF membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan area. Dalam penerapan OSPF, area dapat dibagi menjadi dua, yaitu :

- *Backbone Area, area* ini memiliki *Area-ID* 0.0.0.0 dan merupakan *area* yang diharapkan dapat melakukan forward paket data secepat-cepatnya. *Area* ini wajib ada jika ternyata hanya akan ada satu *area* dalam suatu jaringan. Jika ternyata dalam jaringan tersebut akan dibuat beberapa *area*, maka Backbone wajib ada karena berfungsi menghubungkan *area-area* yang lain.
- *Regular Area, area* ini adalah *area* selain backbone dan berfungsi menghubungkan *end user*. Jika dalam satu jaringan ada dua regular *area*, maka kedua

area tersebut harus melewati backbone *area* untuk berkomunikasi.

Dengan menggunakan konsep hirarki *routing* ini sistem penyebaran informasinya menjadi lebih teratur dan tersegmentasi. Efek dari keteraturan distribusi *routing* ini adalah jaringan yang penggunaan *bandwidth*-nya lebih efisien, lebih cepat mencapai konvergensi, dan lebih presisi dalam menentukan rute-rute terbaik menuju ke sebuah lokasi. OSPF merupakan salah satu protokol *routing* yang selalu berusaha untuk bekerja demikian. Teknologi yang digunakan oleh protokol *routing* ini adalah teknologi *link state* yang memang didesain untuk bekerja dengan sangat efisien dalam proses pengiriman *update* informasi rute.

Cara OSPF membentuk hubungan dengan router lain adalah dengan membentuk komunikasi dengan router lain. Kemudian membentuk hubungan dengan router *neighbor* router. Router OSPF memiliki sebuah mekanisme untuk dapat menemukan router yang lain dan dapat membentuk suatu hubungan. Mekanisme itu disebut dengan istilah *hello protocol*. Dalam membentuk hubungan dengan router lain OSPF akan mengirimkan sebuah paket yang memiliki ukuran yang kecil dengan mengirimkan secara berkala kedalam jaringan yang terhubung langsung dengan OSPF. *Hello packet* merupakan sebutan untuk paket kecil yang dikirim oleh OSPF dan didalam paket tersebut berisikan informasi seputar pernak-pernik yang ada pada router pengirim. Pada kondisi yang standart *hello packet* akan dikirim 10 detik sekali di dalam media *broadcast multi-access* dan 30 detik sekali dalam media *point to point*. *Hello packet* pada umumnya dikirim dengan menggunakan *multicast address* untuk menuju ke semua router yang menjalankan OSPF. Semua router yang menjalankan OSPF pasti akan mendengarkan *protocol hello* ini dan juga akan mengirimkan *hello packet*nya secara berkala.

2.6.3.2 *Border Gateway Protocol* (BGP)

Menurut Uyless Black (2000, p157) *Border Gateway Protocol* (BGP) adalah inti dari protokol *routing* internet yang sudah digunakan sejak 1989. Protokol ini yang menjadi *backbone* dari jaringan internet dunia yang digunakan untuk melakukan pertukaran informasi *routing* antar jaringan. Tujuan BGP adalah untuk memperkenalkan pada dunia luar alamat-alamat IP apa saja yang ada dalam jaringan tersebut. Setelah dikenal dari luar, *server-server*, perangkat jaringan, dan perangkat komputer lainnya yang ada dalam jaringan tersebut juga dapat dijangkau dari dunia luar.

Protokol *routing* BGP dibagi menjadi 2 jenis, yaitu:

a. iBGP (*Internal* BGP)

iBGP adalah sebuah sesi BGP yang terjalin antara dua router yang menjalankan BGP yang berada dalam ASN yang sama. iBGP biasanya digunakan pada jaringan internal ISP. Sebuah sesi iBGP antar dua buah router atau lebih tidak memerlukan koneksi secara langsung, atau dengan kata lain tidak memerlukan koneksi *Point-to-Point*. iBGP bisa dibangun meskipun router berada dalam jarak yang jauh, asalkan masih dengan ASN yang sama.

b. eBGP (*External* BGP)

eBGP adalah sesi BGP yang terjadi antar dua router atau lebih yang berbeda ASN. Ketika kita ingin berkomunikasi dengan ISP lain, maka kita harus melakukan eBGP. Hal ini disebabkan masing-masing ISP mempunyai ASN yang berbeda. Sesi eBGP biasanya dibuat dengan menggunakan bantuan media *Point-to-Point* seperti *line Point-to-Point serial*, *satelite Point-to-Point*, *wireless Point-to-Point*, dan sebagainya. Sesi eBGP biasanya terjadi pada router yang letaknya berada di perbatasan antara jaringan kita dengan jaringan lain, atau sering disebut juga dengan istilah border router. Tujuan utama dibuatnya eBGP adalah untuk memudahkan pendistribusian informasi *routing* dari pihak luar ke jaringan kita.

BGP bekerja dengan cara memetakan sebuah tabel IP *network* yang menunjuk ke jaringan yang dapat dicapai antar AS. Hal ini digambarkan sebagai sebuah *protocol path vector*. Protokol *routing* BGP baru dikatakan pada sebuah router jika sudah terbentuk sesi komunikasi dengan router tetangganya yang juga menjalankan BGP. Sesi komunikasi ini adalah berupa komunikasi dengan protokol TCP dengan nomor *port* 179. Setelah terjalin komunikasi ini, maka kedua buah router BGP dapat saling bertukar informasi rute.

Untuk membentuk dan mempertahankan sebuah sesi BGP dengan router tetangganya, BGP mempunyai mekanisme yang unik. Pembentukan sesi BGP ini mengkitalkan paket-paket pesan yang terdiri dari empat macam. Paket-paket tersebut adalah sebagai berikut:

a. *Open Message*

Paket pesan jenis ini merupakan paket pembuka sebuah sesi BGP. Paket inilah yang pertama dikirimkan ke router tetangga untuk membangun sebuah sesi komunikasi. Paket ini berisikan informasi mengenai BGP *version number*, AS *number*, *hold time*, dan router ID.

b. *Keepalive Message*

Paket *keepalive message* bertugas untuk menjaga hubungan yang telah terbentuk antar kedua router BGP. Paket jenis ini dikirimkan secara periodik oleh kedua buah router yang bertetangga. Paket ini berukuran 19 *byte* dan tidak berisikan data sama sekali.

c. *Notification Message*

Paket pesan ini adalah paket yang bertugas menginformasikan *error* yang terjadi terhadap sebuah sesi BGP. Paket ini berisikan *field-field* yang berisi jenis *error* apa yang telah terjadi, sehingga sangat memudahkan penggunanya untuk melakukan *troubleshooting*.

d. *Update Message*

Paket *update* merupakan paket pesan utama yang akan membawa informasi rute-rute yang ada. Paket ini berisikan semua informasi rute BGP yang ada dalam jaringan tersebut. Ada tiga komponen utama dalam paket pesan ini, yaitu *Network Layer Reachability Information* (NLRI), *path atribut*, dan *withdrawn routes*.

Salah satu ciri khas dan juga merupakan kekuatan dari protokol *routing* BGP ada pada atribut-atribut pendukungnya. Atribut-atribut ini yang nantinya digunakan sebagai parameter untuk menentukan jalur terbaik untuk menuju ke suatu situs. Atribut ini juga dapat mengatur keluar masuknya *routing update* dari router-router BGP tetangga. Dengan mengatur atribut ini, kita dapat dengan bebas mengatur bagaimana karakteristik dan sifat dari sesi BGP tersebut.

Berikut adalah macam-macam atribut BGP. Masing-masing memiliki ciri khas dan tugasnya tersendiri untuk memungkinkan kita memanajemen *routing update* dan *traffic* yang keluar masuk.

a. *Origin*

Jika sumbernya berasal dari router BGP dalam jarigan lokal atau menggunakan ASN yang sama dengan yang sudah ada maka indikator atribut ini adalah huruf “i” untuk *interior*. Apabila sumber rute berasal dari luar jaringan lokal maka indikatornya adalah huruf “e” untuk *exterior*. Sedangkan apabila rute didapat dari hasil *redistribusi* dari protokol *routing* lain maka indikatornya adalah “?” yang artinya *incomplete*.

b. *AS_Path*

Atribut ini harus ada pada setiap rute yang dipertukarkan menggunakan BGP. Atribut ini menunjukkan perjalanan paket dari awal hingga berakhir di tempat kita. Perjalanan paket ini ditunjukkan secara berurut dan ditunjukkan dengan menggunakan ASN. Dengan demikian akan tampak melalui mana saja sebuah paket data berjalan ke tempat kita.

c. *Next Hop*

Next hop merupakan atribut yang menjelaskan kemana selanjutnya sebuah paket data akan dilemparkan untuk menuju ke suatu lokasi.

d. *Multiple Exit Discriminator* (MED)

Atribut ini berfungsi untuk menginformasikan router yang berada di luar AS untuk mengambil jalan tertentu untuk mencapai si pengirimnya. Atribut ini dikenal sebagai metric eksternal dari sebuah rute.

e. *Local Preference*

Atribut ini bersifat *wellknown discreationary* dimana sering digunakan untuk memberitahukan router-router BGP lain dalam satu AS kemana jalan keluar yang di *prefer* jika ada dua atau lebih jalan keluar dalam router tersebut.

f. *Atomic Aggregate*

Atribut ini bertugas untuk memberitahukan bahwa sebuah rute telah di*aggregate* (disigkat menjadi pecahan yang lebih besar) dan ini meyebabkan sebagian informasi ada yang hilang.

g. *Weight*

Atribut ini merupakan atribut dengan *priority* tertinggi dan sering digunakan dalam proses *path selection*. Fungsi dari atribut ini adalah untuk memilih salah satu jalan yang diprioritaskan dalam sebuah router.

Router perlu melakukan pemilihan rute terbaik ketika mendapatkan dua atau lebih rute untuk menuju ke suatu lokasi di luar. Ketika dihadapkan pada dua jalan dengan tujuan yang sama, maka tugas router BGP adalah harus memilih salah satu jalan untuk digunakan meneruskan informasi yang dibawanya. Dalam proses pemilihan jalur terbaik atau *path selection*, atribut sangat berperan penting. Semua atribut memiliki tingkat prioritasnya sendiri dalam proses penentuan jalur terbaik. Proses *path selection* ke sebuah lokasi yang terjadi dalam sebuah sesi BGP hingga menemukan sebuah jalur terbaik adalah sebagai berikut:

a. Jika hanya ada sebuah rute menuju ke lokasi A, maka rute tersebutlah yang pasti dijadikan rute terbaik dan akan langsung digunakan.

b. Jika ada dua buah rute menuju ke lokasi A, maka router BGP akan menggunakan atribut *weight* untuk memilih rute mana yang paling baik. Rute dengan nilai *weight* tertinggi akan dipilih sebagai jalur terbaik.

c. Jika nilai *weight* keduanya sama, maka router akan menggunakan atribut *local preference* sebagai bahan pembanding. Rute dengan nilai *local preference* tertinggi adalah rute yang terpilih sebagai rute terbaik.

d. Jika nilai *local preference* sama, maka sebagai bahan pembanding router BGP akan memeriksa rute mana yang berasal dari dirinya sendiri. Jika rute tersebut berasal dari dirinya sendiri maka rute tersebut yang akan dijadikan rute terbaik.

e. Jika rute menuju A bukan berasal dari dirinya, maka router akan menggunakan atribut AS_Path untuk mencari rute terbaik. Rute dengan atribut AS_Path terpendek akan dipilih sebagai rute terbaik. Apabila atribut AS_Path nya sama, maka atribut selanjutnya yang digunakan untuk memilih rute terbaik adalah Origin. Atribut origin terdiri dari parameter IGP, EGP, dan *Incomplete*. Parameter dengan nilai referensi terendah akan dipilih menjadi rute terbaik. IGP memiliki nilai *referensi* terendah, disusul EGP, dan yang terakhir *Incomplete.*

f. Jika atribut origin pada rute-rute tersebut sama, maka atribut selanjutnya yang digunakan adalah MED. Jenisnya kurang lebih sama seperti *local preference* namun bedanya atribut MED ini hanya disebarkan dalam satu AS yang sama saja. Rute dengan nilai MED yang paling rendah adalah yang dipilih sebagai jalur terbaik.

g. Jika nilai MED pada kedua rute tersebut sama, maka router BGP akan melakukan pemilihan berdasarkan jenis sesi BGP dari rute-rute tersebut. Jenis BGP ada dua yaitu

iBGP dan eBGP. Sebuah rute yang berasal dari sebuah sesi eBGP memiliki prioritas yang lebih tinggi daripada rute dari sesi iBGP.

h. Jika setelah melalui ketentuan di atas, kedua rute tersebut juga masih identik, maka proses *path selection* selanjutnya adalah menggunakan parameter jalur terdekat dalam jaringan internal untuk menuju ke *next hop*. Maksudnya adalah, router BGP akan membaca atribut *next hop* dari kedua jalur tersebut. Setelah diketahui, router tersebut akan memeriksa jalur mana yang memiliki *next hop* yang terdekat dari router tersebut. Jalur yang diperiksa ini merupakan jalur yang berasal dari protokol *routing* internal seperti OSPF, EIGRP, atau bahkan statik. Setelah didapatkan rute mana yang memiliki *next hop* yang paling dekat dan mudah diakses, maka rute tersebut langsung dipilih menjadi yang terbaik.

i. Jika prosedur ini masih tidak menghasilkan sebuah rute terbaik juga, maka jalan terakhir untuk menemukannya adalah dengan membandingkan BGP router ID dari masing-masing rute. Sebuah rute pasti akan membawa informasi BGP router ID dari router asalnya. Parameter inilah yang menjadi pembanding terakhir untuk proses *path selection*. Karena BGP router ID tidak mungkin sama, maka sebuah jalan terbaik pastilah dapat terpilih. BGP router ID biasanya adalah alamat IP tertinggi dari sebuah router atau dapat juga berupa IP *interface loopback*. Router BGP akan memilih rute dengan nilai BGP router ID terendah.

Kekuatan BGP yang lainnya adalah kita dapat memodifikasi dan mengubah atribut-atribut yang ada pada sebuah rute, sehingga proses pemilihan jalur terbaik ini juga dapat kita atur. Dengan mengatur proses ini, maka kita dapat mengatur lalu-lintas data yang keluar masuk jaringan kita.