BAB II
DASAR TEORI

2.1 MPLS (*MultiLabel Protocol Label Switching*)

2.1.1 Pengertian MPLS

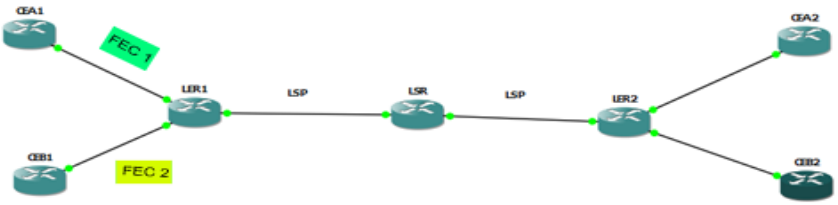
MPLS merupakan sebuah solusi masalah trafik pada sebuah jaringan dimana pada teknologi ini memiliki kemampuan pengiriman dengan kecepatan tinggi pada IP *routing* dimana dalam pengirimanya menggunakan label *header* yang diletakan di IP. MPLS menyediakan *control protocol* dan *connection oriented* yang berbasis IP dimana berarti pengiriman data dapat dipertanggung jawabkan karena traffic atau jalur yang digunakan merupakan jalur khusus dengan tingkat keamanan lebih handal., selain itu terdapat beberapa keunggulan dari teknologi jaringan MPLS tersebut diantaranya[1] :

1. MPLS dapat mengurangi banyaknya proses pengolahan trafik yang terjadi pada *router*, dikarenakan MPLS merupakan suatu metode *forwarding* yang merupakan peningkatan teknik *forwarding* pada koneksi tradisional dalam perpindahan data paket yang besar, tingkat keefisienan pada MPLS lebih baik dan lebih tinggi.
2. MPLS menjaga *Quality of Service* (QoS) pada jaringan.
3. Digunakan untuk memetakan IP secara sederhana.

MPLS memang didesain untuk mengatasi solusi jaringan untuk menunjang kecepatan pada IP *routing* dan MPLS tersebut juga merupakan teknologi untuk mengembangkan teknologi VPN (*Virtual Private Network*) dimana teknologi tersebut dapat mengirimkan sautu data pada jalur khusus yang ditumpangkan pada jalur umum seperti internet. Dewasa ini teknologi MPLS banyak digunakan oleh penyedia layanan jaringan karena dapat mewujudkan pengoptimalan performansi pengiriman data dengan harga operational yang lebih murah dari teknologi sebelumnya seperti ATM dan proses pengiriman data bisa lebih handal lagi.[1]

2.1.2 Komponen – Komponen MPLS[1]

Pada jaringan MPLS terdapat komponen-komponen penting yang perlu diketahui. Berikut gambaran komponen MPLS :



Gambar 2.1 Komponen - Komponen MPLS[1]

Pada gambar 2.1 dapat dilihat komponen yang terdapat pada teknologi jaringan MPLS. Diataranya adalah sebagai berikut[1] :

1. LSP (*Label Switched Path*)

   LSP merupakan singkatan dari *Label Switched Path* yang memiliki fungsi sebagai jalur suatu packet yang disediakan untuk perjalanan FEC yang ditetapkan pada sebuah pengaturan transmisi data , atau bisa juga merupakan sebuah jalur traffic pada rangkaian LSR yang mana paket diteruskan oleh label swapping dari satu MPLS node ke MPLS node yang lain.

2. LER (*Label Edge Route*)

   LER bekerja sebagai penentu keputusan QoS pada jaringan MPLS. Dengan menggunakan nomor port pada lapisan-4 dari paket, kebijakan QoS dapat dibangun dan dikelola.

3. LSR (*Label Switched Routers*)

   LSR adalah sebuah router yang memiliki kemampuan untuk memahami MPLS label dan bertanggung jawab untuk menerima dan mengirimkan paket label pada data link di jaringan MPLS MPLS ditampilkan pada gambar 2.1. Tiga operasi yang berhubungan dengan LSR adalah pop, push dan swap

4. *Forward Equivalence Class* (FEC)

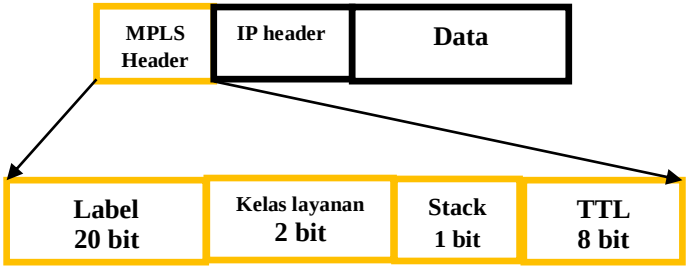
   Sekelompok paket yang memiliki jalur transmisi yang sama dan forwarding mekanisme dikenal sebagai FEC. Paket milik FEC yang sama memiliki label yang sama. Tapi beberapa paket tidak termasuk mekanisme FEC dan *forwarding* yang sama karena berbeda Nilai EXP.

2.1.3 Cara Kerja Jaringan MPLS

MPLS mempunyai kemampuan untuk men-*switch* dan men-*route* label yang dipasang pada setiap paket karena MPLS mempunyai rangkaian *node-node*. Domain MPLS terdiri dari serangkaian *node* MPLS yang saling terhubung satu sama lain. *Node* ini merupakan LSR. label yang dimaksutkan adalah *header* tambahan pada *address* yang nantinya difungsikan untuk mengarahkan aliran paket antara 2 titik *endpoint*. Pada pentrnasmisian data yang disalurkan melalui jaringan LSR tersebut menggunakan jalur khusus pada setiap aliranya dan jalur khusus tersebut disebut FEC. MPLS merupakan teknologi jaringan yang *connection-oriented*. Sebuah persyaratan QOS untuk setiap aliranya ditentukan oleh setiap FEC yang memiliki karakteristik pada lalu lintasnya. Pengiriman data pada teknologi MPLS menggunakan label pada setiap alamatnya dengan menambahkan *header* label, dengan begitu proses pentransmisian datapun akan lebih sederhana dari pada menggunakan *router* IP.[1]

1.2 Arsitektur MPLS

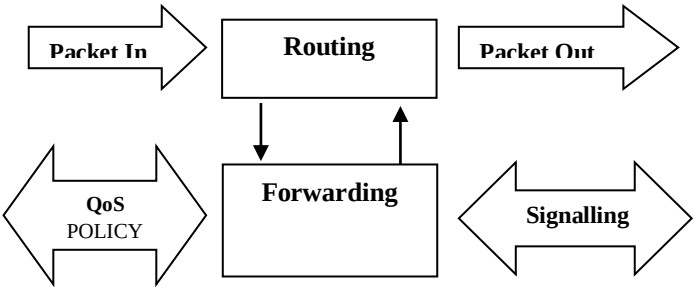
Pada jaringan MPLS pengiriman data dilakukan dengan menambahkan label pada alamat IP nya, *node-node* yang disebut *label switched router* dihubungkan melalui *Label Circuit Path* yang sebelumnya dikonfigurasi dalam pembangunan jaringan MPLS. *Forwarding Equivalence Class* (FEC) terhubung pada Seluruh *Label Switched Path* . *Header* MPLS terdiri dari 32 *bit* data, termasuk 20 *bit label*, 2 *bit* experimen dan 1 *bit* identifikasi *stack* serta 8 bit TTL [2]. Berikut gambar ilustrasi *enkapsulasi* pada MPLS :



Gambar 2.2 *Header* MPLS [3]

Gambar 2.2 merupakan tampilan enkapsulasi *header* MPLS. enkapsulasi pada MPLS menambahkan label *header* untuk digunakan sebagai identitas pada jaringan MPLS.

Didalam jaringan MPLS terdapat sirkuit yang disebut *label-switched path* (LSP), yang berfungsi sebagai penghubung titik-titik yang disebut *labe-switching router* (LSR). LSR pertama dan terakhir disebut *ingress* dan *egress*. Diperlukan suatu *protocol* pensinyalan, untuk membentuk sebuah LSP. Pada *protocol* ini *forwarding* ditentukan berdasarkan label pada paket label yang pendek dan berukuran tetap sehingga proses *forwarding* semakin cepat dan fleksibilitas pemilihan *path* semakin tinggi. Berikut gambar Arsitektur jaringan MPLS seperti yang ditampilkan pada gambar 2.3:

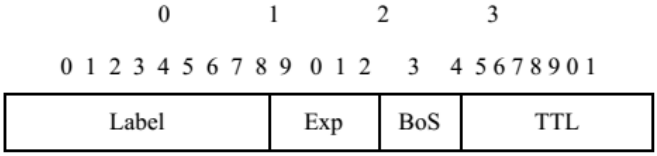


Gambar 2.3 Arsitektur MPLS [3]

Pada gambar 2.3 mendapat gambaran bahwa packet data yang masuk akan di forwarding sehinga data sebelum di kirimkan akan dikenai label sebelum packet tersebut keluar, pada MPLS juga menggunakan teknologi layer 3 maka pada pengirimanya juga melawati proses routing.

1.2.1 Label Struktur MPLS

Label struktur MPLS memiliki struktur tertentu 32-*bits* seperti yang ditunjukkan pada gambar 2.4



Gambar 2.4 Label MPLS[1]

- pada gambar 2.4 dapat dilihat table *enkapsulasi* pada jaringan MPLS, berikut adalah penjelasan tiap bagian pada table tersebut[1] :

1. *Label*: 20 *bit* pertama pada label MPLS merupakan Label Nilai dan nilai 16 pertama yang dibebaskan untuk penggunaan

normal dikarenakan untuk penggunaan khusus. Sistem mempelajari hop berikutnya dan operasi yang akan dilakukan, setelah menerima paket berlabel dan nilai label di bagian atas.

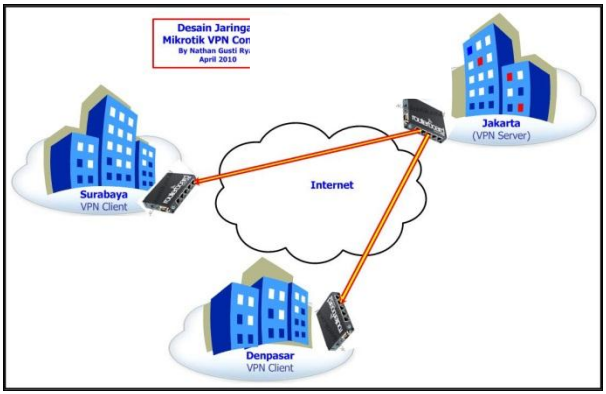
2. *EXP*: *bit* ini dimulai dari 20-22 yang dicadangkan untuk penggunaan eksperimental, dan digunakan hanya untuk QoS
3. *BOS*: *Bit* 23 dikenal sebagai *Bottom of Stack bit*, set pertama untuk entri terakhir pada label *stack*. *stack* adalah kumpulan label dan dapat terdiri dari satu label atau beberapa label.
4. *TTL*: *bit ke* - 8 (24-31) memiliki fungsi yang sama seperti pada *header* IP. Pada umumnya digunakan untuk pengkodean nilai TTL. nilai *time-to-live* mengalami penurunan sebesar 1 pada setiap hop yang menghindari paket dari yang tertangkap pada lingkaran *routing*.

2.3 *Virtual Private Network* (VPN)

2.3.1 Pengertian VPN

Virtual Private Network merupakan sebuah jaringan yang bersifat *private* dimana jaringan tersebut dibangun menggunakan jaringan publik. Secara fundamental penerapan VPN yaitu untuk membentuk sebuah jaringan yang bersifat *private* dengan jaringan yang bersifat publik untuk menghubungkan situs atau *user remote.* Dalam performansinya VPN menggunakan koneksi *virtual* yang dirutekan melintasi *internet* pada jaringan *private* [4].

VPN merupakan salah sutu cara untuk membuat sebuah jaringan yang bersifat *private* dan memiliki tingkat keamanan tinggi dengan menggunakan jaringan publik misalnya *internet* seperti ditampilkan pada gambar 2.6. VPN mampu mengirim data antara dua *client* yang melewati jaringan publik namun seolah-olah terhubung secara *point to point (private).* Berikut adalah ilustrasi jaringan VPN :



Gambar 2.5 jaringan VPN [4]

Pada gambar 2.5 dapat dilihat jaringan VPN pada setiap *client* dapat terhubung secara *private* pada jaringan *public* seolah-olah terhubung pada jaringan *point–to-point.*

2.3.2 Keuntungan VPN

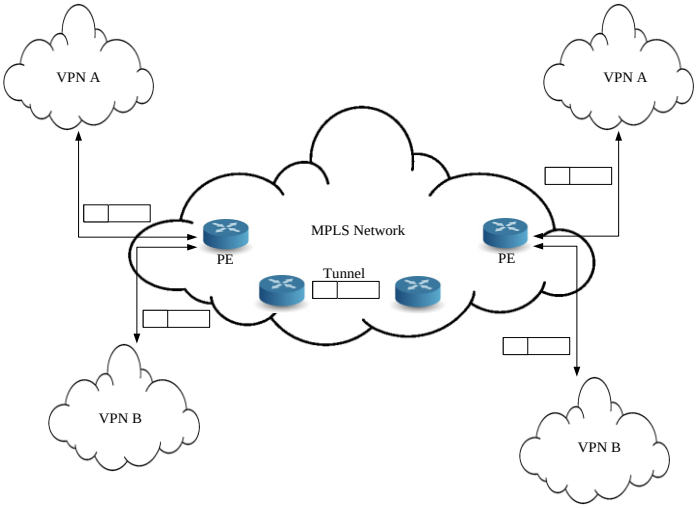
VPN memberikan beberapa keuntungan diantaranya menigkatkan keamanan jaringan, lalu memberikan konektivitas yang luas, dan karena menggunakan jaringan publik maka arsitektur jaringan lebih murah, topologi jaringan yang dipergunakan juga semakin sederhana dan tidak hanya itu ,jaringan VPN memberikan ROI (*return on invesment*) yang lebih cepat dibandingkan jaringan WAN yang lainya.[3]

2.4 MPLS VPN

2.4.1 Penerapan MPLS VPN

Penerapan MPLS dapat diimplementasikan pada VPN yang terdapat pada layer 2 dan layer 3 dari OSI layer. Pada layer 2 terdapat teknologi *Frame Relay* dan ATM. Sedangkan pada layer 3 terdapat IP *Tunneling* berbasis GRE atau *IPSec* yang dilewatkan pada jaringan IP. MPLS VPN merupakan teknologi yang cukup populer dan tersebar luas penggunaannya. Sejak ditemukanya teknologi MPLS ini, teknologi MPLS menjadi salah satu teknologi jaringan yang cukup diminati dan cepat populer. MPLS *tunnels* didukung oleh jaringan MPLS guna menetapkan VPN yang berada pada layer 2 seperti *frame relay,* ATM ,dan sebagainya. Fungsi *tunnels* ini yaitu mampu membentuk *virtual wire* yang dihubungkan dari sumber ke tujuan pada jaringan VPN[6]. Pendeknya beberapa mekanisme *tunneling* yang

digunakan sebagai transmisi paket melalui jaringan IP diberikan oleh MPLS pada proses pengenkapsulasian paket. Mekanisme tunneling ini bermanfaat ketika VPN menggunakan MPLS. Berikut ilustrasi penerapan jaringan MPLS VPN :



Gambar 2.6 jaringan MPLS VPN [6]

Pada gambar 2.6 dapat dilihat bahwa jaringan MPLS VPN merupakan memanfaatkan tunneling pada jaringan yang dibuat di jaringan publik (Internet) sebagai jalur agar data bisa dikirim secara *private* dan lebih cepat dari segi performansi. Dengan memanfaatkan tekologi MPLS VPN dapat membuat koneksi user tidak perlu dihubungkan *end-to-end* dengan jalur *private*, sehingga meminimalisir pembentukan link baru. Beberapa keutungan menggunakan MPLS VPN yaitu *Overlapping* IP, proses *fast switching*, dan faktor keamanan data. Arsitektur MPLS VPN memiliki kelebihan untuk menangani infrastruktur jaringan pribadi yang mengirimkan layanannya pada infrastruktur jaringan publik[6]. Dari segi penerapanya ,jaringan MPLS VPN tidak membutuhkan konfigurasi pada titik-titik jaringan yang dilewati VPN ,sehingga penerapanya cenderung lebih mudah [3] . MPLS *Tunnel* terhubung dengan beberapa VPN ditampilkan pada gambar 2.6.

2.4.2 Komponen MPLS VPN

Sebelumnya sudah sedikit dijelaskan komponen pada jaringan MPLS , berikut adalah ilustrasi dari komponen pada jaringan MPLS VPN :

Gambar 2.7 Komponen MPLS VPN [7]

Pada gambar 2.7 dapat dilihat beberapa komponen MPLS VPN, berikut adalah penjelasan dari masing-masing komponen [7]:

1. CE : *Customer Edge*, merupakan perangkat pelanggan yang secara langsung terhubung dengan *service provider*.
2. PE : *Provider Edge*, merupakan perangkat yang berada di dalam jaringan *provider* yang terhubung dengan CE dan bertanggung jawab untuk memberikan akses layanan VPN
3. P : *Provider*, merupakan perangkat yang berada di dalam jaringan *provider* yang tidak terhubung langsung dengan CE dan bertanggung jawab untuk fungsi *routing* dan *forwarding*

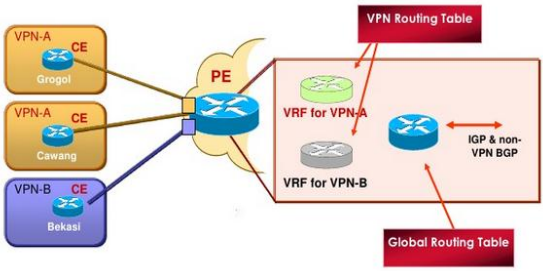
2.4.3 Parameter MPLS VPN

Pada Jaringan VPN Terdapat parameter-parameter yang perlu diperhatikan pada *router* PE (*provider edge*) yang berfungsi dalam pembentuk *layer*-3 di VPN diantaranya [7]:

1. VPN *Routing* dan *Forwarding Instance* (VRF)

   VRF yaitu sebuah *virtual router*, setiap VPN membutuhkan setiap *router* PE yang memiliki VRF yang terpisah, VRF digabungkan dengan *interface/sub-interface* yang terhubung dengan CE. Site atau titik jaringan lain yang biasanya terkoneksi dengan PE lain akan mendistribusikan suatu VPN

yang memiliki sama *route* di VRF. Berikut ilustrasi dari penerapan VRF :

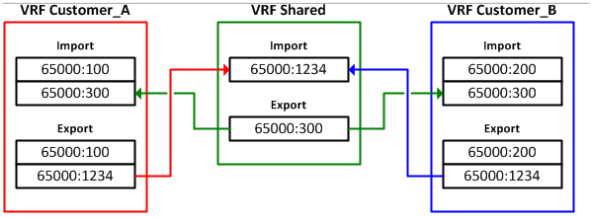


Gambar 2.8 VPN *Routing* dan *Forwarding Instance*[7].

Pada gambar 2.8 memperlihatkan bahwa pada jaringan VPN terdapat VRF yang nantinya digunakan sebagai penanda agar CE yang memiliki VRF berbeda tidak dapat berkomunikasi untuk perihal keamanan.

2. *Route Distinguisher* (RD)

Untuk merubah bentuk *non-unique* 32-*bit address* IPv4 *user* menuju 96-*bit* unik VPNv4 *address* perlu adanya penggunaan *Route Distinguisher*. Seperti yang ditampilkan pada gambar 2.9



Gambar 2.9 *Route Distinguisher*[7]

Pada gambar 2.9 fungsi VRF dapat dioperasikan maka memerlu menggunakan RD(*Route Distinguisher*. VRF yang tidak sama, akan mempunyai RD yang berbeda, *Route Distinguisher* untuk setiap VRF dikonfigurasi oleh *Router* PE .

2.5 KONSEP *ROUTING PROTOCOL*

Routing protocol adalah proses mengkomunikasikan antara *router-router*, *routing protocol* juga mengijinkan *router* untuk sharing informasi

tentang jaringan dan koneksi antar *router*. *Router* menggunakan informasi ini untuk membangun dan memperbaiki tabel *routing*nya[8].

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing*. *Router* sering digunakan untuk menghubungkan beberapa jaringan. Baik jaringan yang sama maupun berbeda. *Router* juga digunakan untuk membagi jaringan besar menjadi beberapa buah *subnetwork* (*network-network* kecil). Informasi yang dibutuhkan *router* dalam melakukan *routing* yaitu[8]:

1. Alamat tujuan/ *destination address*
2. Mengenal sumber informasi
3. Menemukan *route*
4. Pemilihan *route*
5. Menjaga informasi *routing*

Routing melibatkan dua aktifitas dasar, yaitu menentukan *path routing* yang paling optimal dan membawa paket informasi melalui suatu jaringan. Alur yang paling optimal diperoleh dari hasil penelusuran algoritma *routing*. Untuk membantu proses penentuan alur, algoritma *routing* menginisialisasi dan memelihara tabel *routing*, yang berisi informasi *routing*. Informasi *routing* bervariasi tergantung pada algoritma *routing* yang digunakan. Informasi *routing* tersbebut merupakan hasil pengukuran standar tertentu yang disebut *metric*.

2.6 *OPEN SHORTEST PATH FIRST* (OSPF)

OSPF bekerja berdasarkan algoritma *Shortest Path First*.. *Interior Gateway protocol* atau *Interior Routing Protocol* dikembangkan untuk menghubungkan *router-router* dibawah kendali administrator jaringan OSPF mendistribusikan informasi *routing*-nya di dalam *router-router* yang tergabung ke dalam suatu AS. AS adalah jaringan yang dikelola oleh administrator setempat. OSPF menggunakan *routing protocol link-state*, didesain untuk bekerja dengan sangat efisien dalam proses pengiriman update informasi *route*. OSPF merupakan *protocol* alternatif untuk menutupi kelemahan RIP. OSPF juga merupakan *routing protocol* yang menggunakan prinsip *multipath (multi path protocol*) dapat mempelajari berbagai *route* dan memilih lebih dari satu *route* ke *host* tujuan.

OSPF juga merupakan *routing protocol* yang berstandar terbuka. Maksudnya adalah *routing protocol* ini bukan ciptaan dari vendor manapun. Dengan demikian, siapapun dapat menggunakannya, perangkat manapun

dapat kompatibel dengannya, dan di manapun *routing protocol* ini dapat diimplementasikan. OSPF merupakan *routing protocol* yang menggunakan konsep hirarki *routing*, artinya OSPF membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan *area*. Dengan menggunakan konsep hirarki *routing* ini sistem penyebaran informasinya menjadi lebih teratur dan tersegmentasi, tidak menyebar ke sana ke mari dengan sembarangan. Efek dari keteraturan distribusi *routing* ini adalah jaringan yang penggunaan *bandwidth*-nya lebih efisien, lebih cepat mencapai konvergensi, dan lebih presisi dalam menentukan *route-route* terbaik menuju ke sebuah lokasi. OSPF merupakan salah satu *routing protocol* yang selalu berusaha untuk bekerja demikian. Teknologi yang digunakan oleh *routing protocol* ini adalah teknologi *link State* yang memang didesain untuk bekerja dengan sangat efisien dalam proses pengiriman update informasi *route*. Hal ini membuat *routing protocol* OSPF menjadi sangat cocok untuk terus dikembangkan menjadi *network* berskala besar. Pengguna OSPF biasanya adalah para administrator jaringan berskala sedang sampai besar. Jaringan dengan jumlah *router* lebih dari sepuluh buah, dengan banyak lokasi-lokasi remote yang perlu juga dijangkau dari pusat, dengan jumlah pengguna jaringan lebih dari lima ratus perangkat komputer, mungkin sudah layak menggunakan *routing protocol* ini. [9]

OSPF digunakan bersamaan dengan IP, maksudnya paket OSPF dikirim bersamaan dengan *header* paket data IP. Setiap *router* OSPF mempunyai *database* yang identik yang menggambarkan topologi suatu *Autonomous System* yang disebut dengan l*ink state database* (*Topological database*). Dari database ini, perhitungan *Shortest Path First* dilakukan untuk membentuk *Routing Table*. Perhitungan ulang terhadap *Shortest Path First* dilakukan apabila terjadi perubahan pada topologi jaringan. OSPF memungkinkan beberapa jaringan untuk dikelompokkan bersama. Pengelompokkan seperti ini dinamakan dengan *area* dan topologinya tersembunyi dari seluruh AS. Informasi yang tersembunyi ini memungkinkan penurunan *traffic routing*. Dengan menggunakan konsep *area* sistem penyebaran informasinya menjadi lebih teratur dan tersegmentasi. Dengan adanya distribusi *routing* yang teratur, maka penggunaan *bandwidth* akan lebih efisien, lebih cepat mencapai konvergensi, dan lebih presisi dalam menentukan *route* terbaik dalam mengirim paket. [9]

Secara garis besar, routing *protocol* OSPF bekerja berdasarkan tahapan sebagai berikut:

a. Selama proses inisialisasi (permulaan), maupun dikarenakan adanya perubahan informasi *routing* berupa perubahan pada topologi jaringan, *router* akan menghasilkan sebuah *Link State Advertisement* (LSA). LSA ini berisikan informasi mengenai semua *link (interface*) pada *router* tersebut.

b. Pada proses selanjutnya, semua *router* akan melakukan pertukaran *link state* dengan mengirimkan paket *Link State Update* (LSU) yang berisikan LSA masing-masing *router*. Proses ini dikenal dengan proses *flooding* pada jaringan. Melalui proses ini, setiap *router* yang menerima LSU dari *router* lain akan menyimpan informasi tersebut ke dalam *Link state (topological*) *database*-nya, kemudian mengumumkan *update* tersebut ke *router* lain.

c. Setelah informasi l*ink state* database pada setiap *router* terbentuk, *router* akan melakukan perhitungan *Shortest Path* ke semua *router* lain pada jaringan dengan menggunakan *Dijkstra algorithm*. Alamat tujuan *cost* dan *hop* selanjutnya untuk mencapai alamat tujuan inilah yang kemudian membentuk tabel *routing* pada *router.*

d. Apabila tidak ada perubahan pada informasi *routing* misalnya: perubahan terhadap *cost* dan *link* pada suatu *router* ataupun terjadi penambahan maupun pengurangan *router* dalam jaringan, *router* akan sangat tenang (tidak terjadi pengiriman informasi *routing*).

e. Apabila terjadi perubahan pada informasi *routing* yang menyebabkan dikirimnya paket LSU maka *router* akan melakukan perhitungan ulang terhadap *Shortest Path* menggunakan *Dijkstra algorithm*. [11]

2.6.1 Prinsip Kerja OSPF

Pada prinsip kerja *routing protocol* OSPF ini yang perlu diperhatikan adalah setiap router membuat LSP (*link state packet*) karena penggunaan OSPF dipergunakan lebih kepada jaringan link state, Kemudian LSP didistribusikan ke semua *neighbour* menggunakan *Link State Advertisement* (LSA) *type* 1 dan menentukan DR dan BDR dalam 1 *Area* . Masing-masing *router* menghitung jalur terpendek *(Shortest Path*) ke semua *neighbour* berdasarkan *cost routing*. Jika ada perbedaan atau perubahan tabel *routing*, *router* akan mengirimkan LSP ke DR dan BDR melalui alamat *multicast* 224.0.0.6 . dan terakhir LSP akan didistribusikan oleh DR ke *router neighbour* lain dalam 1 *area* sehingga semua *router neighbour* akan melakukan perhitungan ulang jalur terpendek.[10]

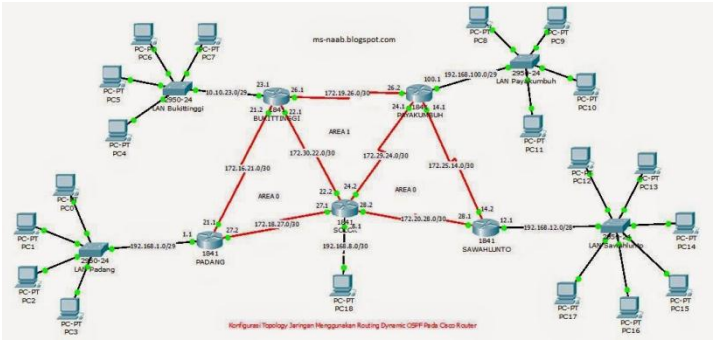
2.6.2 Konfigurasi OSPF - *Backbone Area*

OPSF merupakan *routing protocol* yang menggunakan konsep hirarki *routing*, dengan kata lain OSPF mampu membagi-bagi jaringan menjadi beberapa tingkatan. Tingakatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan yaitu *area*. OSPF memiliki beberapa tipe *area* diantaranya[10]:

- ***Bakcbone* - *Area* 0 (*Area* ID 0.0.0.0)** -> Bertanggung jawab mendistribusikan informasi *routing* antara *non-backbone area*. Semua sub-*Area* harus terhubung dengan *backbone* secara logikal.
- ***Standart/Default Area*** : Merupakan sub-*Area* dari *Area* 0. *Area* ini menerima LSA intra-*area* dan *inter-area* dar ABR yang terhubung dengan *area* 0 (*Backbone area*).
- ***Stub Area*** : *Area* yang paling "ujung". *Area* ini tidak menerima *advertise external route* (digantikan *default area*).
- ***Not So Stubby Area*** : Stub *Area* yang tidak menerima *external route* (digantikan *default route*) dari *area* lain tetapi masih bisa mendapatkan *external route* dari *router* yang masih dalam 1 *area*.

2.6.3 *IMPLEMENTASI ROUTING PROTOCOL OSPF*

Implementasi *routing protocol* OSPF dilakukan dengan menggunakan jaringan komputer dengan konfigurasi jaringan seperti pada gambar berikut :



Gambar 2.10 Topologi OSPF [10]

Pada gambar 2.10 tersebut dapat dilihat penggunaan *routing protocol* ospf sangat cocok digunakan pada jaringan berskala besar dan luas maka dari itu ospf merupakan salah satu dynamic routing yang termasuk dalam *routing protocol* jaringan *link state.*

Untuk memulai semua aktivitas OSPF dalam menjalankan pertukaran informasi *routing*, hal pertama yang harus dilakukannya adalah membentuk sebuah komunikasi dengan para *router* lain. *Router* lain yang berhubungan langsung atau yang berada di dalam satu jaringan dengan *router* OSPF tersebut disebut dengan *Neighbour Router* atau *Router Neighbors*. Langkah pertama yang harus dilakukan sebuah *router* OSPF adalah harus membentuk hubungan dengan *Neighbor Router*. *Router* OSPF mempunyai sebuah mekanisme untuk dapat menemukan *router neighbors*-nya dan dapat membuka hubungan. Mekanisme tersebut disebut dengan istilah *Hello protocol*. Dalam membentuk hubungan dengan *neighbors*nya, *router* OSPF akan mengirimkan sebuah paket berukuran kecil secara periodik ke dalam jaringan atau ke sebuah perangkat yang terhubung langsung dengannya. Paket kecil tersebut dinamai dengan istilah *Hello packet*. Pada kondisi standar, *Hello packet* dikirimkan berkala setiap 10 detik sekali dalam media *broadcast multiaccess* dan 30 detik sekali dalam media *Point-to-point*. *Hello packet* berisikan informasi seputar pernak-pernik yang ada pada *router* pengirim. *Hello packet* pada umumnya dikirim dengan menggunakan *multicast address* untuk menuju ke semua *router* yang menjalankan OSPF (IP *multicast* 224.0.0.5). Semua *router* yang menjalankan OSPF pasti akan mendengarkan *protocol* hello ini dan juga akan mengirimkan *hello packet*-nya secara berkala. Cara kerja dari hello *protocol* dan pembentukan neighbour *router* terdiri dari beberapa jenis, tergantung dari jenis media di mana *router* OSPF berjalan[14] . OSPF memiliki 3 tabel di dalam *router* :

1. *Routing table* biasa juga disebut sebagai *Forwarding database*. *Database* ini berisi the *lowest cost* untuk mencapai *router-router*/*network-network* lainnya. Setiap *router* mempunyai *Routing table* yang berbeda-beda.
2. *Adjecency database*, *Database* ini berisi semua *router neighbors*nya. Setiap *router* mempunyai *Adjecency database* yang berbeda-beda.
3. *Topological database*, *Database* ini berisi seluruh informasi tentang *router* yang berada dalam satu jaringannya/*area*nya.

Kelebihan dari routing *protocol* OSPF ini diantaranya tidak menghasilkan *routing loop*. Selain itu juga mendukung penggunaan beberapa metric

sekaligus. Lalu dapat menghasilkan banyak jalur ke sebuah tujuan ,membagi jaringan yang besar meja di beberapa area, dan terakhir waktu yang diperlukan untuk konvergensi lebih cepat.

Sedangkan untuk kekurangan *routing protocol* OSPF diantaranya yaitu membutuhkan basis data yang besar dan lebih rumit

2.7 *INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM* (ISIS)

ISIS menggunakan metode *link state* sebagai metode pengumpulan *route*nya dan menggunakan algoritma *Shortest Path First* (algoritma *Djikstra*) dalam melakukan perhitungannya. *Protocol* ini dirancang untuk beroperasi di OSI C*onnectionless Network Service* (CLNS). ISIS mempunyai prinsip kerja yang mirip dengan *protocol* OSPF, tetapi berbeda dalam sistem pengalamatan dan struktur hirarki. Sistem pengalamatan yang digunakan ISIS dalam sistem pengalamatan ciptaan ISO sendiri, yaitu sistem pengalamatan ISO (ISO *Addressing*). Jadi semua perangkat yang ingin digunakan untuk menjalankan ISIS harus dapat dikonfigurasi dengan alamat ISO. Tetapi karena sistem pengalamatan IP lah yang banyak digunakan, maka sistem pengalamatan ISO juga dibuat kompatibel dengan IP. ISIS menggunakan *ConnectionLess Network Protocol* (CLNP) *address*, dan ketika CLNP *address* digunakan di *router* maka disebut *Network Service Access Point* (NSAP) dan NSAP ini yang digunakan dalam sistem pengalamatan di ISIS. [12]

ISIS *protocol* dikembangkan oleh *Digital Equipment Corporation* sebagai bagian dari Tahap DECnet V standar oleh ISO pada tahun 1992 sebagai ISO 10589 untuk komunikasi antara perangkat jaringan yang disebut Sistem *Intermediate* oleh ISO. Tujuan dari ISIS adalah untuk memungkinkan *routing* datagram menggunakan ISO-OSI dikembangkan tumpukan *protocol* yang disebut CLNS. ISIS dikembangkan di sekitar waktu yang sama bahwa Internet Engineering Task Force IETF mengembangkan *protocol* yang sama disebut OSPF. ISIS kemudian diperluas untuk mendukung *routing* datagram dalam Internet *Protocol* (IP), *Network Layer protocol* Internet global. Ini versi ISIS *routing protocol* kemudian disebut Terpadu ISIS (RFC 1195). [13]

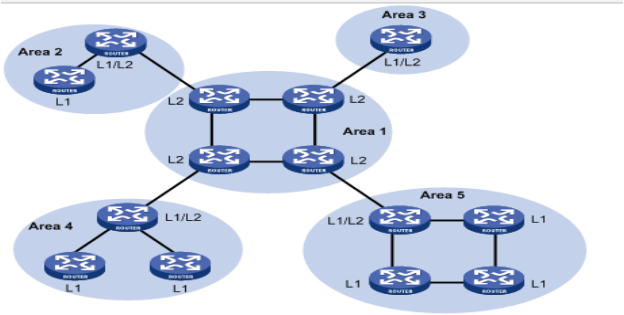
ISIS merupakan salah satu *routing protocol* IGP *(internal Gateway Protocol*) yang digunakan oleh *network device* dalam hal ini *router* untuk menentukan *best route* (*route* terbaik) untuk meneruskan *traffic* data ke suatu tujuan. ISIS didevelop oleh DECnet sekitar tahun 1992 dimana pada waktu itu IETF juga sedang mengembangkan *protocol* OSPF. sebagai IGP *routing protocol* ISIS ber-operasi didalam *Administrative Domain* yang sama. seperti OSPF, *protocol* ISIS juga merupakan *link-state protocol* dan

sama-sama menggunakan *Djikstra Algorithm* untuk melakukan perhitungan dalam memilih *best path.* Bila dalam *protocol* OSPF terdapat konsep *Area*, di ISIS terdapat Level, Level disini merupakan batasan dari pengkelompokan *router-router*. terdapat Level 2, Level 1 dan L1/L2 level. **Level 2** merupakan *backbone area* dimana Level 2 ISIS *router* akan saling berbagi informasi bila *router-router* tersebut sama-sama dikonfigurasi sebagai level 2 *area*. *router* yang dikonfigurasi sebagai **Level 1** makan akan berbagi informasi *routing* bila sama-sama dikonfigurasi Level 1 dan nilai ISIS *Area* nya sama. sebelum ISIS *router* dapat saling bertukar informasi, maka *router-router* tersebut harus membentuk adjacency terlebih dahulu. berikut merupakan proses pengkomunikasian antara router terdekat pada ISIS sebagai berikut *:*

1. ***New*** : Proses ISIS *adjacency* baru dimulai
2. ***One-Way*** : Pada saat ISIS *router* mengirim ISIS Hello PDU *state router* akan berubah Menjadi *One-Way*, dalam *state* ini lokal *router* belum menerima *hello message* dimana tercantum *address* nya sebagai *neighbor*
3. ***Initializin*** : Lokal *router* menerima *hello message* yang mencantum alamat lokal *router*, pada *state* ini komunikasi 2 arah sudah terbentuk
4. ***Up*** : *Adjacency* terbentuk dan pertukaran *database* sudah dapat dilakukan
5. ***Down*** : *Adjacency* tidak berhasil dibentuk kemungkinan dikarenakan konfigurasi *area* yang tidak cocok, atau dikarenakan kesalahan konfigurasi parameter *hold time* atau parameter *authentikasi*
6. ***Reject*** : Apabila terjadi kesalahan authentikasi maka *state* akan bergulir ke status *Reject*

Apabila dalam OSPF terdapat LSA yang dipertukarkan untuk membentuk OSPF databse, dalam ISIS *network* informasi yang dipertukarkan berbentuk LSP (*Link-state PDU*), pada MPLS juga terdapat term LSP (*Label Switching Path*) keduanya adalah hal yang berbeda. *Link-state* PDU berisis informasi tentang *router-router* yang tergabung didalam ISIS *network* dan informasi mengenasi *interface* yang terkoneksi serta metrik nya. *Link-state* PDU ini dibungkus dalam format TLV (*Type Length Value*), dengan format TLV memungkinkan

protocol untuk memperluas kemampuan dan fungsinya dengan mudah. Berikut gambaran topologi menggunakan *routing protocol* ISIS :



Gambar 2. 11 topologi ISIS

Pada gambar 2.11 merupakan bentuk sederhana topologi ISIS .Standarisasi ISIS adalah ISO 10589 yang menetapkan OSI *routing protocol* ISIS untuk lalu lintas CLNS (*ConnectionLess Network*), ISIS juga merupakan Sebuah *protocol Link State* dengan hirarki 2 tingkat arsitektur. Pada *routing protocol* ISIS terdapat RFC 1195 menambahkan dukungan IP , sehingga dapat menguhungkan jaringan ISIS yang notabenya berjalan di layer 2 yaitu *Data link* maka dapat berjalan di layer 3.

Routing protocol OSPF dan ISIS memiiliki beberapa kesamaan diantarayna Keduanya menggunakan *Interior Gateway Protocol* (IGP), selain itu kedua *routing protocol* tersebut mendistribusikan informasi *routing* antara *router* milik *Autonomus System*. Lalu kedua *routing protocol* tersebut mendukung untuk melakukan CIDR *(Classless Inter-Domain Routing)* untuk mengklasifikasikan *class* alamat IP , mendukung membuat VLSM , *Multi-path, link* IP bernomor.

2.7.1 Jenis PDU *Packet* di ISIS *Routing*

OSI *layer* mendefinisikan unit data sebagai *protocol* data unit (PDU). Sebuah frame karena itu dianggap oleh OSI sebagai *PDU data-link*, dan paket dianggap sebagai PDU jaringan. Ada empat jenis paket PDU, dan masing-masing jenis dapat Level 1 atau Level 2:

- LSP : suatu LSP adalah PDU yang dikirimkan antara dua *neighbors* ISIS. LSP berisi informasi tentang *neighbors* dan biaya jalur, termasuk *adjacencies neighbors*, prefiks IP terhubung, *Open System Interconnection* (OSI) sistem akhir, dan alamat daerah. LSP digunakan oleh *router* penerima untuk mempertahankan tabel *routing* mereka.

- IIH : suatu ISIS *Hello* PDU digunakan untuk membangun dan mempertahankan *adjacencies.*
- PSNP : sebuah parsial nomor urut PDU (PSNP) berisi ringkasan dari hanya sebagian dari LSP dikenal. Sebuah PSNP digunakan untuk mengakui dan meminta *link-state* informasi dengan meminta versi yang lebih baru dari lengkap LSP, atau mengakui penerimaan dari LSP masing-masing.
- CSNP -sebuah nomor urut lengkap PDU (CSNP) berisi ringkasan dari semua LSP yang diketahui oleh *router*.

2.7.2 Overload

Pada ISIS juga di kenal fitur *Overload* yang amat bermanfaat bila terjadi gangguan link ataupun mau dilakukan *maintenance* terhadap *router* tersebut. *router* yang di *set overload* maka ISIS akan membuat *traffic* tidak akan melalui *router* yang diset *overload* (*router* yang diset *overload* akan dihapus dari *Topology*), seting *overload* dapat bersifat *permanent*, maupun *temporary* (diset berapa lama *router* tersebut akan dianggap *overload*).

2.7.3 SISTEM PENGALAMATAN ISIS

ISIS merupakan *routing protocol* yang diciptkana oleh *Interational Standarization Organization* (ISO). Tujuan diciptakan ISIS oleh ISO adalah agar *routing protocol* ini menjadi sebuah standar terbuka yang dapat digunakan oleh semua perangkat jaringan. Namun kenyataan yang lebih banyak digunakan adalah semua *protocol* dan sistem pengalamatan yang diciptakan berdasarkan organisasi standar *Open System interconnection* (OSI). Sistem pengalamatan IP yang selama ini dikenal di seluruh dunia dan *routing protocol* seperti OSPF diciptakan berdasarkan standarisasi dari OSI ini. Dengan demikian ISIS tidak menggunakan sistem pengalamaan berdasarkan nomor IP. Sistem pengalamatan yang digunakan adalah sistem pengalamatan ciptaan ISO sendiri (ISO *Addressing*). Perangkat yang digunakan untuk menjalankan ISIS harus dikonfigurasi dengan alamat ISO. Sistem pengalamatan ISO juga dibuat kompatibel dengan IP. Dalam penerapan pada sebuah *router* yang menjalankan ISIS digunakan untuk membawa informasi *route* dalam *format* IP maka dari itu sebuah *router* yang tergabung dalam jaringan ini harus diberi alamat ISO untuk dapat mengirim dan menerima informasi ini. [14]

2.7.4 STRUKTUR HIRARKI PENGALAMATAN ISIS

Routing protocol jenis *link state* menggunakan konsep *area* dalam sistem pengalamatannya sehingga jaringannya membentuk sebuah hirarki yang teratur. Sistem *area* dalam ISIS diberikan untuk keseluruhan perangkat *router*, artinya sebuah *router* hanya akan tergabung dengan sebuah *area* saja, tidak bisa tergabung kedalam banyak *area*. Hal ini dikarenakan peraturan nomor-nomor pada *area* ISIS hanya diberikan pada alamat ISO nya saja, dimana alamat tersebut biasanya hanya diberikan satu buah pada setiap *router*. *Router* yang berada dalam *area* sama baik OSPF maupun ISIS dapat langsung saling berkomunikasi. ISIS merupakan salah satu *routing protocol Link-State*, Tidak seperti OSPF , yang dikembangkan dan distandarisasi oleh *Internet Engineering Task Force* (IETF) , IS - IS adalah *protocol* ANSI ISO dan pada awalnya didasarkan pada Teknologi *Digital Equipment* Perusahaan DECNET Tahap V *Network*.

Pada IS- IS semua *router* menempatkan informasi dalam PDU *link*-lain yang diterima ke dalam *database link-state* mereka , dan semua *router* memiliki *routing table* yang sama dari topologi jaringan . IS - IS menjalankan algoritma SPF pada informasi dalam database *link-state* untuk menentukan jalur terpendek ke setiap tujuan pada jaringan, menempatkan pasangan tujuan / *next- hop* yang dihasilkan dari perhitungan SPF ke *database* IS- IS *routing* . Tidak seperti *protocol* lain yang biasanya berjalan pada TCP , UDP , atau IP, yaitu *OSI Layer* 3 atau Layer 4 *protocol* , IS - IS berjalan secara langsung pada data *link* layer (Layer 2) . [14]

2.7.5 BAGIAN ALAMAT ISIS

Pada pengalamatan *routing protocol* IS- IS sendiri terdiri dari tiga bagian ,berikut contoh tampilan peroutingan menggunakan *routing protocol* ISIS

NSAP Address
49.0002.0000.0c12.3456.00

IDI		DSP	
AFI	Area ID	System ID	NSEL
49	0002	0000.0c12.3456	00
3 bytes		6 bytes	1 byte

Gambar 2.12 *NSAP addressing*[15]

Pada gambar 2.12 dapat dilihat struktur pengalamatan pada *routing protocol* ISIS terdiri atas beberapa bagian yaitu AFI.Area, ID.System ID.NSEL. berikut penjelasan masing-masing bagian :

1. *AFI* : tiga *byte* pertama adalah ID daerah . *Byte* pertama dari contoh ini - 49 - adalah *Authority and Format Identifier* (AFI). Berikut adalah gambar macam *AFI Value* pada ISIS :

AFI Value	Address Domain
39	ISO Data Country Code (DCC)
45	E.164
47	ISO 6523 International Code Designator (ICD)
49	Locally administered (private)

Gambar 2.13 *AFI value of addressing domain* [15]

2. *Area* ID : - 0001 atau 0002 - mewakili IS- IS *level* nomor 1 atau nomor 2, AFI dan *Area* ID disebut IDP (*Initial Domain Part*). Misalnya 47.0005 untuk *U.S Civilian Goverement*.
3. System ID : Mengidentifikasi node (*router*) pada jaringan . Identifier sistem setara dengan *host* atau bagian alamat pada alamat IP
4. NSEL (*NSAP Selector*) : *value* pada *router* harus 0(00), selain itu bukan termasuk IS (*Intermediate System/Router*). NSEL dengan *value* 0 disebut juga NET (*Network Entity title), system ID* dan NSEL disebut juga dengan DSP (*Domain Selector Part*)

.2.7.6 Perbandingan ISIS dan OSPF

Berikut ini adalah perbandingan konsep antara *routing* OSPF dengan ISIS. pada kedua *routing protocol* kali ini memiliki perbandingan dalam masalah istilah diantaranya adalah seperti berikut :

A. Perbandingan dari segi istilah

Table 2.1 tabel istilah *routing protocol OSPF dan ISIS*

OSPF	ISIS	Penjelasan
Host	*End System*	perangkat komputer jaringan
Router	*Intermediate System*	istilah untuk perangkat penghubung jaringan berbeda
Link	*Circuit*	acuan jalur
Packet	*Protocol Data Unit*	potongan data
Area	*Sub domain area*	menentukan area pada router
Non backbone area	*Level-1 area*	menentukan area bukan backbone pada router
Backbone area	*Level-2 sub domain*	menentukan area backbone router
Area border router	*L1 L2 router*	perbatasan area pada router pada router
Automonous system boundary router	*Any IS*	pengelompokan jaringan berbeda pada router

B . Perbandingan dari segi *enkapsulasi*

Selain dari segi istilah proses pengiriman packet data pada masing-masing routing protocol antara OSPF dan ISIS juga berbeda, berikut perbedaan konsep enkapsulasi pada OSPF dan ISIS:

- OSPF menggunakan IP *Protocol* sebagai transportasi

Data Link Header	*Ip Header*	*OSPF Header*	*OSPF Data*

Gambar 2.14 enkapsulasi ospf

Pada *enkapsulasi* routing protocol OSPF masih menggunakan peran ip *header* karena *routing protocol* OSPF menggunakan pengiriman packet layer 3.

- ISIS langsung dikemas dalam Layer 2

Data Link Header	*ISIS Header*	*ISIS Data*

Gambar 2.15 enkapsulasi isis

Pada *enkapsulasi* routing protocol ISIS tidak menggunakan peran IP dalam pengirimanya karena pengalamatan *routing protocol* ISIS menggunakan pengiriman packet layer 2

C. Perbandingan Dalam pemilihan IGP

IGP adalahdigunakan untuk routing intra sistem otonom – routing di dalam sistem otonom Perbedaan *routing protocol* dari segi pemilihan IGP adalah pada *routing protocol* OSPF adalah semua jaringan harus memiliki area 0 yang difungsikan sebagai *backbone*, sedangakan pada *routing protocol* ISIS jaringan *backbone* hanya memerlukan sambungan ke router level L2 , dalam segi fleksibilitas ISIS lebih fleksibel dari pada OSPF.

Pada penggunaannya pun terdapat beberapa dasar pertimbangan dalam penggunaan *routing* OSPF dan ISIS diantaranya :

1. Keamanan
   Dikarenakan *routing protocol* ISIS berjalan pada *layer link* maka sulit untuk menusupi IGP menggunakan IP seperti *routing protocol* OSPF karena tidak tergantung pada pengalamtan IP .
2. Keandalan
   Pengunaan ISIS dalam jaringan ISP sebagai mayoritas *routing protocol* yang digunakan , kepercayaan bahwa vendor peralatan lebih memperhatikan ISIS dalam kehandalan, skalabilitas, dan fitur..
3. Migrasi ke IPv6
   Pada proses migrasi ke IPV6 *routing protocol* OSPF versi 2 maupun 3 perlu ditambahkan kedalam jaringan sedangkan pada *routing protocol* ISIS hanya perlu menambahkan IPV6 pada *address family.*

2.7.7 Persamaan dan Perbedaan antara OSPF dengan ISIS

A. Persamaan OSPF dan ISIS :

Protocol ISIS dan OSPF memiliki beberapa persamaan diantaranya keduanya sama-sama menggunakan *Interior Gateway Protocols* , selain itu keduanya juga digunakan pada jaringan linkstate dan menggunakan algoritma djisktra.

B. Perbedaan OSPF dan ISIS :

Setelah mengetahui persamaan maka selanjutnya terdapat beberapa perbedaan pada *routing protocol* OSPF dan ISIS diantaranya adalah pada OSPF menggunakan metode TCI/IP milik IETF, sedangkan ISIS menggunakan metode OSI (ISO/IEC 10589:2002) , kemudian protocol ISIS menggunakan *service* OSI layer 2 yang bernama CLNS (*ConnectionLess Network Service*) untuk *adjency*-nya , lalu OSPF menggunakan *service*-nya IP dan UDP , IP *protocol* ISIS adalah CLNP (*ConnectionLess Network Protocol)* , IP *addresing* ISIS adalah NSAP (*Network Service Access point)* , OSPF terkenal dengan istilah *area sedangkan* ISIS terkenal dengan istilah *level* , pada penghubunganya protocol OSPF menghubungkan menggunakan ABR (*Area Boundary Router)* sedangkan ISIS menghubungkan *inter-level* perlu L2L1, tidak seperti OSPF yang semua *router* harus konek ke *area backbone* yang sama , Pada OSPF terdapat DR (*Designated Router*)/BDR (*Backup Designated Router*) sedangkan pada ISIS terdapat DIS (*Designated IS*) tapi tidak terdapat *backup* DIS , Pada OSPF tidak terdapat konfigurasi untuk mengganti DR/DBR secara otomatis tanpa harus di *shutdown* terlebih dahulu. , kemudian Pada ISIS terdapat mekanisme konfigurasi untuk mengganti DIS secara otomatis yang disebut *Preemptive*.[14]

2.8 Conection Oriented dan Conectionless

1. **Connection Oriented** adalah suatu hubungan membutuhkan pembangunan komunikasi dan perawatan (penjagaan) komunikasi selama berlangsung. Dimana pada conection-oriented penggunaan bandwidth digunakan untuk satu komunikasi jadi terasa kurang efektif.[18]
2. **ConnectionLess** adalah suatu hubungan yang tidak membutuhkan pembangunan komunikasi dalam komunikasinya. Pada connectionless tidak memperdulikan bandwith dikarenakan data dikirim begitu saja karena penggunaan bandwith lebih effective karena semua jalur yang tersedia dapat digunakan oleh pemakai lain. Lalu keunggulanya yang lain adalah connectionless memiliki sifat Highly Roubus yaitu jika ada node data paket hilang dapat diperoleh lewat node yang lain.[18]