BAB II

MPLS VPN, *IPSEC* DAN *ROUTING PROTOKOL* BGP

2.1 *Multi Protocol Label Switching* (MPLS)

MPLS, *Multi Protocol Label Switching* adalah metode yang ditingkatkan untuk meneruskan paket melalui jaringan menggunakan informasi yang terkandung dalam label yang dilampirkan pada paket IP. Label disisipkan di antara header layer 3 (*network*) dan header layer 2 (*data-link*) dalam kasus teknologi layer 2 berbasis *frame*, dan label tersebut terkandung dalam bidang *Virtual Path Identifier* (VPI) dan *Virtual Channel Identifier* (VCI) dalam kasus teknologi berbasis sel seperti *Asynchronous Transfer Mode* [1]. Jaringan ini terdiri atas sirkit yang disebut *Label Switched Path* (LSP), yang menghubungkan titik-titik *Label Switching Router* (LSR) dan bukan merupakan jaringan IP ataupun jaringan ATM, tetapi merupakan jaringan baru. Jaringan baru ini mengurangi banyaknya proses pengolahan yang terjadi di IP *routers*, serta memperbaiki unjuk-kerja pengiriman suatu paket data, juga bisa menyediakan kualitas layanan QoS dalam jaringan *backbone*.

Untuk membentuk LSP, diperlukan suatu protokol persinyalan. Protokol ini menentukan *forwarding* berdasarkan label pada paket. Label yang pendek dan berukuran tetap mempercepat proses *forwarding* dan mempertinggi fleksibilitas pemilihan path. Hasilnya adalah network datagram yang bersifat lebih *connection-oriented* [15].

2.1.1 Komponen Jaringan MPLS

Dalam menjalankan fungsinya, MPLS memiliki sejumlah komponen dasar sebagai penyusun jaringannya, yaitu:

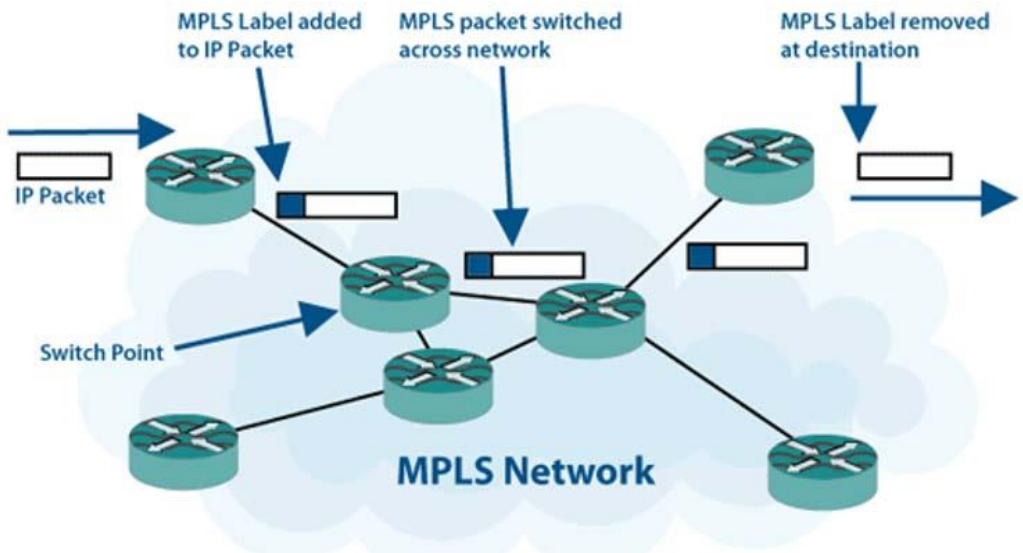
- *Label Switched Path* (LSP): LSP adalah jalur yang ditetapkan pada serangkaian link antar LSR, yang mengizinkan paket untuk diteruskan dari LSR satu menuju LSR lain melalui jaringan MPLS. Di dalam MPLS ada 2 cara untuk menetapkan LSP, yaitu: *Hop-by-hop routing* dan *Explisit routing*. Cara yang pertama membebaskan masing-masing LSR menentukan hop selanjutnya untuk mengirimkan paket. Cara ini mirip seperti OSPF dan RIP dalam IP routing. Cara yang lainnya, LSP ditetapkan oleh LSR pertama yang dilalui aliran paket.

- *Label Switching Router* (LSR) dan *Label Edge Router* (LER): LSR adalah sebuah router dalam jaringan MPLS yang berperan dalam menetapkan LSP dengan menggunakan teknik *label swapping* dengan kecepatan yang telah ditetapkan. Dalam fungsi pengaturan trafik, LSR dapat dibagi dua, yaitu: *Ingress* LSR dan *Egress* LSR. *Ingress* LSR berfungsi mengatur trafik saat paket memasuki jaringan MPLS sedangkan *Egress* LSR berfungsi untuk mengatur trafik saat paket meninggalkan jaringan MPLS menuju ke LER. Sedangkan, LER adalah suatu router yang menghubungkan jaringan MPLS dengan jaringan lainnya seperti Frame Relay, ATM dan Ethernet.
- *Forward Equivalence Class* (FEC): FEC adalah representasi dari beberapa paket data yang diklasifikasikan berdasarkan kebutuhan *resource* yang sama di dalam proses pertukaran data.
- *MPLS label*: Label adalah deretan bit informasi yang ditambahkan pada header suatu paket data. Label MPLS atau yang disebut juga MPLS header ini terletak diantara header layer 2 dan header layer 3.
- *Label Distribution Protocol (LDP)*: LDP adalah protokol baru yang berfungsi untuk mendistribusikan informasi yang ada pada label ke setiap LSR. Protokol ini digunakan untuk memetakan FEC ke dalam label, untuk selanjutnya akan dipakai untuk menentukan LSP. LDP message dapat dikelompokkan menjadi :
  - *Discovery Messages*, yaitu pesan yang memberitahukan dan memelihara hubungan dengan LSR yang baru tersambung ke jaringan MPLS.
  - *Session Messages*, yaitu pesan untuk membangun, memelihara dan mengakhiri sesi antara titik LDP.
  - *Advertisement Messages*, yaitu pesan untuk membuat, mengubah dan menghapus pemetaan label pada jaringan MPLS.
  - *Notification Messages*, yaitu pesan yang menyediakan informasi bantuan dan sinyal informasi jika terjadi error.

2.1.2 Cara Kerja MPLS

Prinsip kerja MPLS ialah menggabungkan kecepatan switching pada layer 2 dengan kemampuan routing dan skalabilitas pada layer 3. Dengan memperhatikan gambar 1, cara kerjanya adalah dengan menyelipkan label di antara header layer 2 dan layer 3 pada paket yang diteruskan. Label dihasilkan oleh *Label Switching*

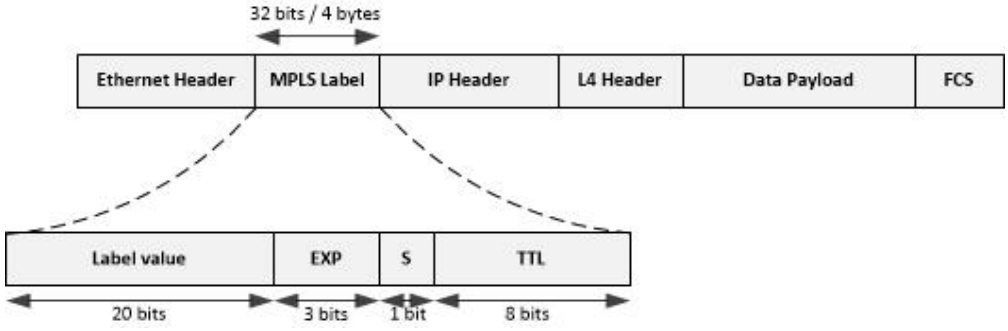
Router dimana bertindak sebagai penghubung jaringan MPLS dengan jaringan luar. Label berisi informasi tujuan node selanjutnya kemana paket harus dikirim. Kemudian paket diteruskan ke node berikutnya, di node ini label paket akan dilepas dan diberi label yang baru yang berisi tujuan berikutnya. Paketpaket diteruskan dalam path yang disebut LSP (*Label Switching Path*).



Gambar 2.1. Konsep MPLS
Sumber: (https://www.mushroomnetworks.com/what-is-mpls/)

Dengan *label switching*, paket dianalisa secara menyeluruh dari header lapisan 3 dan dilakukan hanya sekali, yakni pada label switch router (LSR) di *edge*, yang dialokasikan bagi setiap edge dari jaringan.

MPLS hanya melakukan enkapsulasi paket IP dengan memasang header MPLS, perhatikan gambar 2 berikut ini. Label adalah bagian dari header, memiliki panjang yang bersifat tetap, dan merupakan satu-satunya tanda identifikasi paket. Label digunakan untuk proses *forwarding*, termasuk proses *traffic engineering*.



Gambar 2.2. Header MPLS
Sumber: (http://thebitbucket.co.uk/ccie/topic-notes/vpns/mpls-vpn-topic-notes/)

Pada gambar 2.2 terlihat MPLS header memiliki panjang 32 bit yang terdiri dari:

- *Label*, 20 bit yang merupakan nilai aktual untuk label. Label ini menentukan jalur pengiriman paket ke LSR berikutnya dan operasi yang akan dilakukan pada MPLS header sebelum dikirimkan.
- *EXP* (*Experimental*), 3 bit yang dicadangkan untuk kegiatan eksperimen. Bagian ini juga berfungsi untuk mengidentifikasi *Class of Service* (*CoS*).
- *S* sepanjang 1 bit yang merupakan dasar MPLS header. Bit ini akan diset ”satu” apabila paket yang dikirimkan merupakan paket terakhir pada MPLS header dan ”nol” untuk paket yang lainnya.
- *Time to Live* (*TTL*) sepanjang 8 bit digunakan untuk mengkodekan suatu nilai TTL.

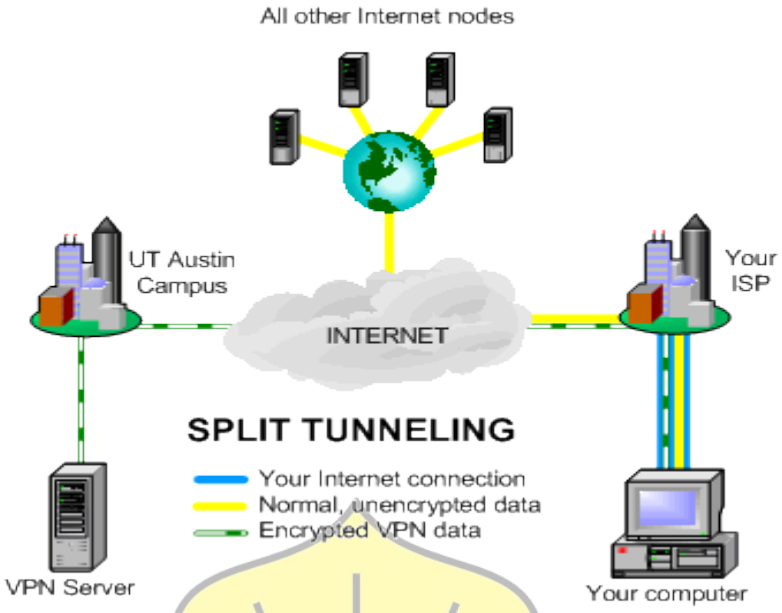
Dalam proses pembuatan label ada beberapa metode yang dapat digunakan, yaitu:

- Metode berdasarkan topologi jaringan, yaitu dengan menggunakan protocol IP- routing seperti OSPF dan BGP.
- Metode berdasarkan kebutuhan resource suatu paket data, yaitu dengan menggunakan protocol yang dapat mengontrol trafik suatu jaringan seperti RSVP (*Resource Reservation Protocol).*
- Metode berdasarkan besar trafik pada suatu jaringan, yaitu dengan menggunakan metode penerimaan paket dalam menentukan tugas dan distribusi sebuah label.

2.2 *Virtual Private Network* (VPN)

Virtual Private Network (VPN) merupakan sebuah jaringan *private* yang menghubungkan satu *node* jaringan ke *node* jaringan lainnya dengan menggunakan jaringan public (internet). Data yang dilewatkan dibungkus (*encapsulation*) dan dienkripsi agar terjamin kerahasiaannya.

Jaringan VPN dikoneksikan oleh penyedia jasa komunikasi (*service provider*) melalui routernya ke router-router lain dengan menggunakan jalur internet yang telah dienkripsi di antara dua titik, seperti yang ditunjukkan pada Gambar 2.3.



Gambar 2.3. skema *tunneling* pada VPN
Sumber: (https://ut.service-now.com/sp?id=kb_article&number=KB0012334)

Sistem keamanan di VPN menggunakan beberapa lapisan, yaitu:

a) Metode *tunneling* (terowongan)

Membuat terowongan virtual di atas jaringan public menggunakan protocol seperti *Point-to-Point Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), *Generic Routing Encapsulation* (GRE) atau *IPSec*. *PPTP dan L2TP* adalah protocol tunneling di layer 2, keduanya melakukan pembungkusan *payload* pada *frame PPTP* untuk dilewatkan pada jaringan. Sedangkan *IPSec* berada di layer 3, menggunakan paket, dan melakukan pembungkusan *IP Header* sebelum dikirim ke jaringan.

b) Metode Enkripsi

Untuk membungkus paket data yang lewat di dalam *tunneling*, data yang dilewatkan pada pembungkusan tersebut akan diubah dengan algoritma kriptografi tertentu seperti *DES, 3DES* dan *4AES*.

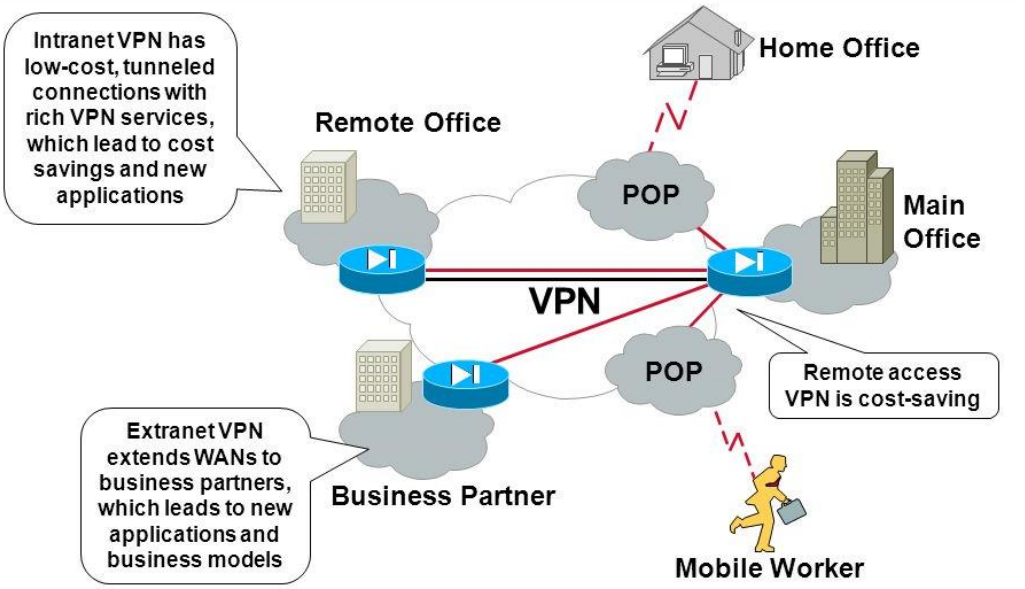
c) Metode Autentikasi User

Karena banyak user yang mengakses biasanya digunakan beberapa metode autentikasi user seperti *Remote Access Dial In User Services (RADIUS)* dan *Digital Certificates*.

d) Integritas Data

Paket data yang dilewatkan pada jaringan publik perlu jaminan keutuhan data, apakah terjadi perubahan atau tidak. Metode VPN menggunakan *HMA C-MD5* atau *HMA C-SHA1* agar paket data tidak berubah pada saat pengiriman.

Jenis implementasi jaringan VPN ditunjukkan oleh Gambar 2.4 berikut di bawah ini



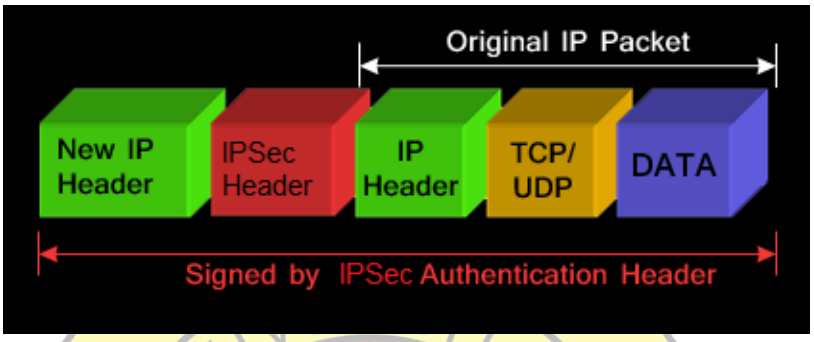
Gambar 2.4. *Intranet VPN*, *Extranet VPN*, dan *Remote Access VPN*
Sumber: (http://www.powernetix.com/main/network/vpn.html)

Tiga jenis implementasi jaringan VPN seperti yang ditunjukkan Gambar 2.4, antara lain:

- *Intranet VPN* – Menghubungkan antara kantor pusat suatu perusahaan dengan kantor cabang atau kantor pembantu melalui *shared network* menggunakan koneksi yang permanen (*dedicated*).
- *Extranet VPN* – Menghubungkan konsumen, *suppliers*, mitra bisnis, dan beberapa komunitas dengan kepentingan yang sama ke jaringan internal perusahaan melalui infrastruktur yang terbagi menggunakan koneksi *dedicated*.
- *Remote Access VPN* – Menyediakan *remote access* ke jaringan intranet atau extranet perusahaan yang memiliki kebijakan yang sama sebagai jaringan privat. VPN jenis ini memungkinkan *user* uantuk dapat mengakses data perusahaan kapanpun dan dimanapun mereka inginkan.

2.3 *IP Security (IPSec)*

IPSec adalah sebuah protocol yang digunakan untuk mengamankan transmisi dalam sebuah jaringan berbasis TCP/IP. IPSec masih cukup popular digunakan untuk mengamankan komunikasi VPN sampai saat ini. Protocol ini menggunakan skema security *end-to-end*, hal ini berarti data yang mengalir dalam tunnel IPSec akan dilakukan enkripsi pada satu router dan dekripsi pada router yang lain. Berikut gambaran struktur paket tanpa dan menggunakan IPSec.

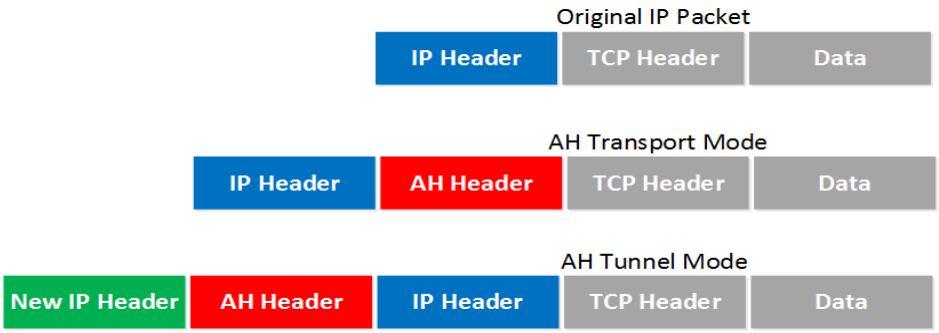


Gambar 2.5. Struktur IPSec pada paket data
Sumber: (https://www.firewall.cx/networking-topics/protocols/)

IPSec *tunnel* memperbolehkan *peer* untuk mengirimkan informasi secara aman melalui jaringan *IP public* atau jaringan yang tidak dipercayai. Dengan menggunakan IPSec *tunnel*, kita dapat melakukan enkripsi dan/atau membuat media *tunnel* terautentifikasi tergantung pada kondisi protocol yang diinginkan oleh dua *peer* tersebut. Dalam komunikasi IPSec, ia terdiri dari beberapa komponen, yang akan dijelaskan dalam sub-poin berikutnya.

2.3.1 *Authentication Header (AH)*

AH mendukung proses autentikasi untuk melindungi data dari serangan sabotase. Dalam prosesnya AH Header disisipkan setelah IP Header.

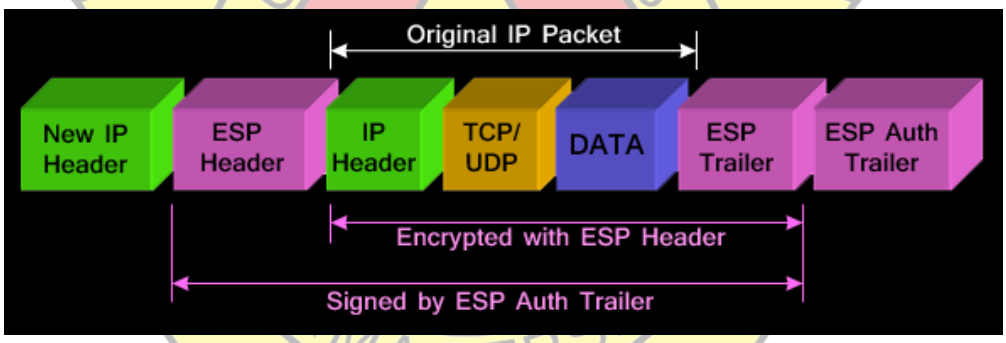


Gambar 2.6. Header Autentikasi yang disisipkan pada paket data.
Sumber: (https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security)

Walaupun AH melakukan perlindungan dengan menerapkan autentikasi paket, namun AH tidak melakukan enkripsi pada isi data (*content/payload*), sehingga bila autentikasi berhasil dijebol oleh pihak ketiga, maka isi data dapat dibaca.

2.3.2 *Encapsulation Security Payload (ESP)*

ESP adalah bagian dari komponen IPSec yang mendukung proses autentikasi sama seperti AH namun yang terpenting adalah ESP mendukung proses enkripsi. Dengan melakukan enkripsi akan mentranslasikan data menjadi format tertentu sehingga data bersifat acak dan tidak dapat dibaca secara langsung. Kemudian paket dapat dibaca kembali atau dilepas enkripsinya oleh *end-device* (router) di ujung *tunnel*, proses ini dinamakan dekripsi. Sehingga yang dapat membaca data yang dikirim adalah pengirim dan penerima yang telah diberi hak (*authorized*). Proses Autentikasi di ESP hanya berlaku untuk data (payload) saja, tidak berlaku untuk IP Header.



Gambar 2.7. Header-header ESP yang mengenkapsulasi paket data
Sumber: (https://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html)

2.3.3 *Security Associations (SA)*

IPSec mengenal konsep SA (*security association*), yaitu bentuk koneksi yang terjalin antara dua perangkat yang melakukan transfer data menggunakan tunnel IPSec. SA digunakan untuk mengumpulkan informasi yang dibutuhkan oleh dua perangkat yang berkomunikasi dengan menentukan beberapa parameter sebagai berikut:

- Protokol Security, apakah menggunakan AH atau ESP
- IP Address tujuan
- Kunci Autentikasi, apakah menggunakan *shared key*, atau *public key*.

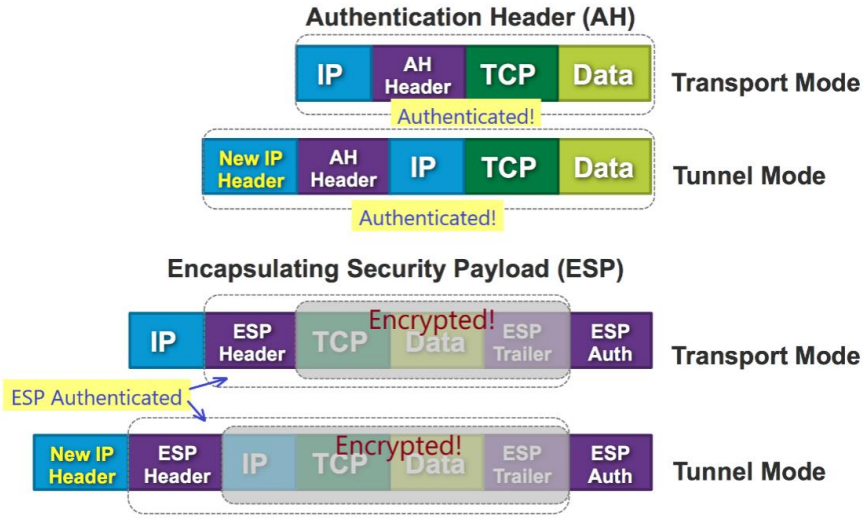
Ada 2 mode bagaimana SA dapat terbentuk. Mode ini adalah metode bagaimana penerapan IPSec dalam sebuah paket. IPSec dapat terbentuk menggunakan mode Transport atau mode Tunnel. Biasanya IPSec mode Transport digunakan untuk komunikasi *host-to-host* (PC-to-PC), sedangkan mode Tunnel lebih sering digunakan untuk komunikasi *gateway-to-gateway* (router ke router).

- ***Transport Mode***

Pada mode ini, SA diimplementasikan pada trafik antara 2 *host*. Contoh komunikasi antara server dengan *client*, atau bisa juga antara *gateway* (router) dengan *workstation* (*host*). Mode Transport mendukung proteksi data protocol AH maupun ESP. Dalam kasus protocol security ESP, maka IPSec akan mengenkapsulasi data (payload) yang terdiri TCP/UDP + Data. ESP Header dan ESP Trailer akan disisipi masing-masing di kedua ujung Payload tersebut.Untuk IP Header tidak termasuk dalam enkapsulasi. Dalam kasus menggunakan protocol AH, maka AH header akan disisipkan sebelum Payload, untuk IP Header sama seperti menggunakan ESP yaitu utuh tanpa dienkapsulasi, tetapi AH memberikan perlindungan autentikasi pada IP Header atau header tambahan lainnya.

- ***Tunnel Mode***

Mode Tunnel digunakan apabila komunikasi dilakukan di antara dua router IPSec tunnel (gateway-to-gateway). Pada mode ini, terdapat IP Header tambahan di luar yang menspesifikasikan tujuan pemrosesan IPSec. Sedangkan IP Header *existing* yang ada di dalam menunjukkan alamat tujuan paket yang sebenarnya. Header protocol keamanan akan tampak pada bagian setelah IP Header tambahan di luar, dan sebelum IP Header *existing* di dalam. Pada kasus ESP, proteksi hanya diberikan pada paket yang di-*tunnel* saja. Sedangkan dalam kasus AH, bagian IP Header tambahan di luar termasuk dalam perlindungan seperti paket IP yang di-*tunnel*. Contoh skema AH dan ESP pada dua mode SA ditunjukkan oleh Gambar 2.8 dibawah ini,



Gambar 2.8. AH dan ESP masing-masing dalam mode Transport dan mode Tunnel. *Sumber: (https://networkmasters.wordpress.com/2017/02/28/ccna-sec-lec7-all-about-ipsec/)*

2.3.4 *Internet Key Exchange (IKE)*

IPSec menggunakan IKE untuk mendukung pembentukan SA, yaitu melakukan pertukaran *key* di antara dua perangkat. Dengan menggunakan *key* tersebut maka hanya pengirim dan penerima yang berhak saja yang dapat melakukan komunikasi dan mengakses data didalamnya. Selain itu, IKE menggunakan algoritma *Diffie-Hellman* untuk menciptakan *key* yang simetris antar *peer* dalam membentuk tunnel. *Key* ini hanya akan berlaku sepanjang nilai *Time To Live* (TTL), setelah itu *key* baru akan dipertukarkan kembali.

2.3.5 *Internet Security Association Key Management Protocol (ISAKMP)*

ISAKMP adalah bagian dari IKE, yaitu merupakan protocol yang digunakan untuk melakukan *sharing* kebijakan *security* dan autentikasi yang dinamakan key. Dalam ISAKMP akan ditentukan apakah *key* menggunakan *pre-shared* atau RSA, kemudian apakah *key* akan dienkripsi menggunakan algoritma AES, DES, atau 3DES.

Dalam melakukan komunikasi IPSec di antara kedua perangkat dilakukan melalui 2 tahap, yaitu bisa kita sebut *IKE Phase 1* dan *IKE Phase 2.*

IKE Phase 1

Yang dilakukan pada IKE Phase 1 adalah membentuk *peer* antara dua perangkat yang menjalankan IPSec yaitu melakukan negosiasi dan mencocokkan autentikasi.

IKE Phase 1 memiliki fungsi sebagai berikut:

- Melakukan autentikasi diantara kedua *peer (device)*.
- Negosiasi mencocokkan parameter SA (*security association*) IKE
- Membentuk *tunnel* untuk melakukan negosiasi IKE Phase 2.

IKE Phase 2

Setelah terbentuk IKE Phase 2 selanjutnya dilakukan negosiasi kembali, adapun fungsi pada IKE Phase 2 adalah:

- Negosiasi IPSec SA, menentukan apakah menggunakan AH atau ESP.
- *Establish* IPSec SA.
- Secara periodic melakukan negosiasi ulang untuk meyakinkan keamanan.

2.4 *Routing*

Routing 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 jaringan yang sama. Pada saat melakukan routing, router akan menyimpan berbagai informasi routing sehingga dapat menentukan kemana sebuah paket atau trafik akan dikirimkan. Informasi routing ini berisi jalur terbaik (*best* path) yang sebaiknya ditempuh oleh sebuah paket.

2.4.1 *Routing Protocol*

Pada routing statik, jaringan harus secara manual ditentukan sendiri *entry route*-nya oleh seorang Administrator jaringan untuk mencapai *network* tujuan. Sedangkan pada routing dinamik proses menentukan entry route tersebut dilakukan oleh router sendiri. Pada jaringan yang menerapkan routing dinamik, router membangun sendiri table routingnya. Untuk menerapkan routing dinamik, wajib menggunakan Routing Protocol agar dapat saling bertukar informasi routing. Pertukaran informasi ini dilakukan secara dinamis sehingga jika terjadi perubahan dalam jaringan, protokol routing akan memberitahukan perubahan tersebut kepada router-router lain yang ada dalam jaringan. Routing pada jaringan TCP/IP terbagi dua macam:

- Interior Gateway Protocol (IGP)

  IGP adalah protokol routing yang digunakan pada router-router yang berada dalam satu *Autonomous System* (AS), atau dengan kata lain IGP digunakan untuk menghubungkan jaringan-jaringan dalam sebuah *Autonomous System*. Contoh bila ingin menerapkan routing pada jaringan internal sebuah organisasi/perusahaan, maka yang dipakai adalah protokol routing kategori IGP. Kategori IGP diantaranya adalah RIP, IGRP, EIGRP, OSPF dan IS-IS.

- Exterior Gateway Protocol (EGP)

  EGP adalah protokol routing yang digunakan pada router-router yang berasal dari *Autonomous System* yang berbeda sehingga dapat menghubungkan jaringan-jaringan yang berasal dari berbagai AS yang berbeda. Contoh penerapannya bila ingin dilakukan routing antar ISP atau routing antar Enterprise Network dengan ISP. Saat ini satu-satunya protokol routing yang digunakan untuk keperluan internet adalah BGP.

2.4.2 *Internet Routing*

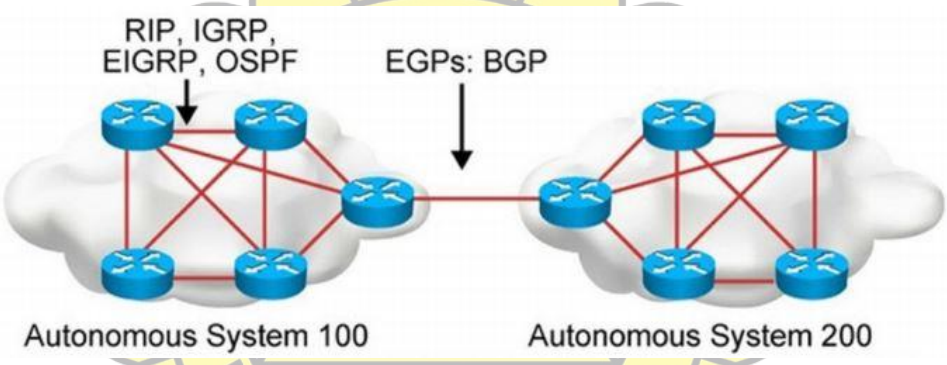
Internet merupakan kumpulan jaringan yang terhubung satu sama lain, sering disebut dengan *network of network* atau jaringannya jaringan. Jaringan-jaringan tersebut terdiri dari sekumpulan router, sekumpulan server, maupun sekumpulan computer dari user. Jaringan-jaringan yang ada di Internet adalah jaringan milik ISP maupun jaringan enterprise. Sehingga internet akan lebih terlihat sebagai jaringan yang terdiri dari ISP yang saling terhubung maupun enterprise network yang terhubung ke ISP.

Untuk menghubungkan ISP-ISP tersebut tentu perlu dilakukan routing. Dan untuk melakukan routing dengan kondisi tersebut haruslah menggunakan routing protocol IGP seperti RIP, OSPF, EIGRP tidak cocok jika akan digunakan untuk melakukan routing antar ISP maupun antar enterprise network. Masalah utama yang ada pada IGP adalah masalah *metric* dan tidak adanya fitur *policy route* yang lengkap. Sehingga untuk memenuhi semua aspek routing antar ISP, maka dibutuhkan routing protocol lain. Routing protocol tersebut haruslah masuk kategori *Exterior Gateway Protocol* (EGP). EGP yang digunakan saat ini untuk melakukan *Inter-ISP Routing* adalah *Border Gateway Protocol* (BGP). Routing protocol inilah yang saat ini mejadi satu-satunya pilihan routing di internet.

2.4.3 *Autonomous System*

Autonomous System merupakan sekumpulan jaringan atau sekumpulan router yang menjalankan satu kesatuan *policy routing* dan berada di bawah satu kendali administrator serta menunjukkan identitas suatu jaringan. Autonomous System dinyatakan dalam bentuk nomor sehingga lebih sering dikenal sebagai Autonomous System Number (ASN). ASN dinyatakan dalam bilangan 16 bit (2 Byte) dan dikelola oleh Internet Registries.

AS Number juga terdiri dari AS Number privat maupun AS Number public, layaknya IP address. Karena dinyatakan dengan bilangan 16 bit, maka AS Number akan bernilai dari 0 – 65535. AS Number privat bernilai 64512 sampai dengan 65535 (RFC-1930), selain nilai tersebut maka termasuk kategori AS Number publik.



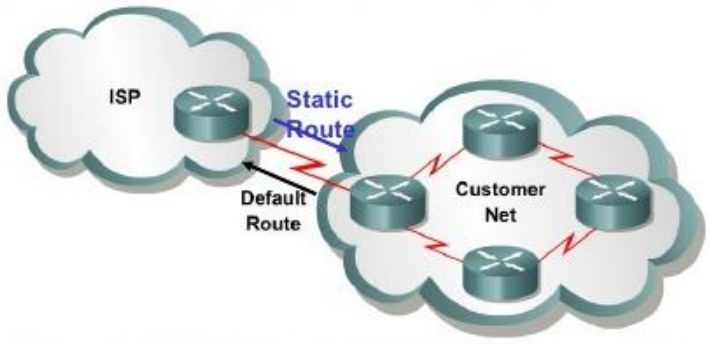
Gambar 2.9. Autonomous System dan Routing Protocol.
Sumber: (https://academy.hsoub.com/certificates/cisco/ccna/)

Untuk menghubungkan router-router yang berada dalam satu AS Number digunakan Interior Gateway Protocol (IGP) seperti RIP, OSPF, IS-IS, maupun EIGRP milik Cisco. Sedangkan untuk menghubungkan router-router yang berasal dari AS Number yang berbeda digunakanlah Exterior Gateway Protocol (EGP), dan BGP adalah satu-satunya pilihan yang ada.

Untuk membangun, membuat dan memilih bentuk Autonomous System, maka dibuatlah beberapa pedoman. Ada 3 (tiga) jenis Autonomous System yang dapat menjadi pilihan, yaitu:

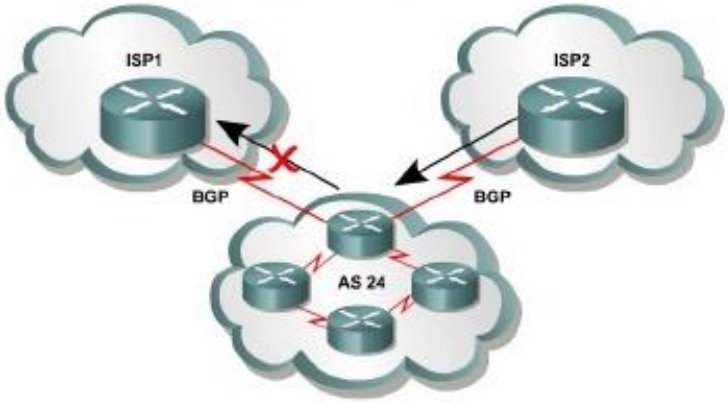
1. Stub atau Single-homed
2. Multi-homed Non-Transit
3. Multi-homed Transit

Stub AS adalah jaringan yang terhubung ke internet melalui 1 (satu) Internet Service Provider. Untuk terhubung ke 1 (satu) ISP, routing dengan BGP sebenarnya tidak diperlukan, umumnya hubungan ini cukup dilakukan dengan *static routing (default route)*. Namun meskipun terhubung ke 1 ISP, terkadang BGP diperlukan jika ternyata Stub AS memiliki alokasi IP Address publik sendiri.



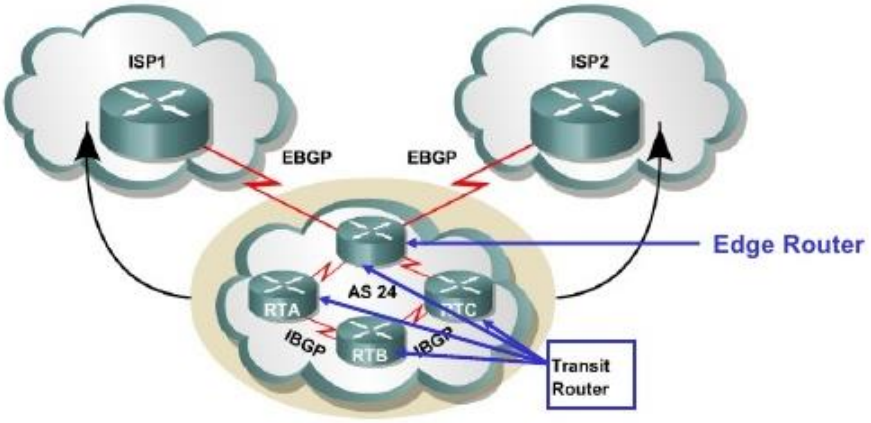
Gambar 2.10a. Stub AS
Sumber: (https://www.slideshare.net/cisconetworker/part1-1135729)

Adapun Multi-homed Non-Transit adalah AS yang terhubung ke beberapa AS yang berbeda. Network yang ingin menggunakan AS jenis ini harus memiliki AS Number sendiri (public) dan seharusnya memiliki alokasi IP Address sendiri. Multi-homed Non-Transit tidak akan melewatkan route atau traffic dari suatu AS ke AS lain.



Gambar 2.10b. *Multi-homed Non-Transit*
Sumber: (https://www.slideshare.net/cisconetworker/part1-1135729

Multi-homed Transit AS adalah Autonomous System yang melakukan pertukaran informasi routing BGP dengan beberapa AS dan meneruskan informasi routing dari satu AS ke AS yang lain. Gambar berikut memperlihatkan bahwa AS 24 sudah menjadi Transit AS.



Gambar 2.10c. *Multi-homed Transit AS*
Sumber: (https://www.slideshare.net/cisconetworker/part1-1135729

2.4.4 *Border Gateway Protocol (BGP)*

Sebagai satu-satunya protokol kategori Exterior Gateway Protocol, maka cara kerja dan proses pemilihan jalur terbaik (*best path*) dari BGP sangat berbeda jauh dengan routing-routing protocol kategori IGP seperti RIP, OSPF, IS-IS maupun EIGRP. BGP juga sudah mendukung *Classless Interdomain Routing* sehingga dapat digunakan untuk jaringan-jaringan yang sudah mengalami *subnetting*, VLSM, ataupun *summarization*.

Berikut beberapa karakteristik utama dari BGP:

1. BGP adalah *Path Vector* routing protocol, dalam proses menentukan jalur terbaiknya selalu mengacu kepada *path* terpilih yang didapatnya dari router BGP yang lain.
2. Tabel routing akan dikirim full router di awal sesi BGP, update selanjutnya hanya bersifat menambah atau mengurangi routing yang sudah ada saja.
3. Router BGP membangun dan menjaga koneksi antar-peer menggunakan port TCP 179.
4. Koneksi antar-*peer* dijaga dengan menggunakan sinyal *keepalive* secara periodic.
5. Apabila gagal menemukan sinyal *keepalive*, *routing update*, atau sinyal-sinyal notifikasi lainnya pada sebuah router BGP dapat memicu perubahan status BGP peer dengan router lain, sehingga mungkin saja akan memengaruhi update ke router lain.
6. *Metric* yang digunakan BGP untuk menentukan rute terbaik sangat kompleks

dan dapat dimodifikasi dengan sangat fleksibel, ini merupakan sumber kekuatan BGP yang sebenarnya. *Metrik-metrik* ini sering disebut sebagai *Attribute*.

7. Penggunaan sistem pengalamatan hirarki dan kemampuannya untuk melakukan manipulasi aliran trafik membuat routing protocol BGP sangat *scalable* untuk perkembangan jaringan di masa mendatang.
8. BGP memungkinkan kita memanipulasi trafik menggunakan *attribute*-nya yang cukup banyak. *Attribute* ini memiliki tingkat prioritas untuk dijadikan sebagai acuan.

2.5 Teknologi *Video Streaming*

2.5.1 Pengertian *Video Streaming*

Dalam dunia internet, *streaming* merupakan sebuah teknologi yang mampu mengkompresi atau menyusutkan ukuran file *audio* dan *video* agar mudah ditransfer melalui jaringan internet [11]. Transfer file *audio* dan *video* tersebut dilakukan secara terus menerus. Dari sudut pandang prosesnya, *streaming* berarti sebuah teknologi pengiriman file dari server ke *client* melalui jaringan *packet-based*. *Streaming* merupakan sebuah metode untuk membuat *audio*, *video* dan multimedia lain yang tersedia secara *real-time* pada tipe jaringan yang berbeda. Data pada file *streaming* di bagi-bagi ke dalam beberapa paket kecil yang dikirim ke sebuah aliran secara terus menerus ke perangkat *end-user* atau *mobile phone*.

Aplikasi dalam layanan *streaming* dibagi menjadi dua, yaitu "*on-demand*" dan "*live*". Layanan *streaming on-demand* contohnya adalah musik dan video. Sedangkan layanan *streaming* yang *live* contohnya adalah acara radio atau acara televisi yang disiarkan secara langsung pada saat itu juga. Menurut (Jaromil, 2002), ide dasar dari video *streaming* adalah untuk membagi-bagi video asli menjadi beberapa paket yang kemudian dikirim secara berurutan, dan memungkinkan *receiver* melakukan *decoding* dan *playback* video berdasarkan paket tersebut tanpa harus menunggu seluruh video terkirim. Menurut (Austerbery, 2013), ada beberapa masalah dasar dalam video *streaming* [6], yaitu:

a) Bandwidth

Jika pengirim mengirimkan data lebih cepat dibandingkan dengan ketersediaan *bandwith* yang ada, maka akan terjadi *congestion* (kemacetan)

pada jaringan, *packet loss*, dan kualitas video yang jelek. Tapi apabila pengirim mengirimkan paket data lebih lambat dari *bandwidth* yang tersedia, maka kualitas video yang sampai ke penerima akan kurang optimal.

b) Jitter

Jitter merupakan masalah yang menyebabkan penerima harus menerima/ decode/menampilkan frame dengan rate yang konstan, dan setiap frame yang terlambat datang akan menyulitkan rekonstruksi video yang diterima.

c) Loss rate

Pada jaringan *wireless*, *loss rate* dapat disebabkan oleh bit error dan *burst error*. *Loss rate* ini dapat menimbulkan kerusakan pada kualitas video hasil rekonstruksi. Untuk mengatasi *loss rate* ini, sistem video streming dapat didesain dengan fasilitas *error rate control*.

2.5.2 *Real Time Encoding dan Pre-encoded (Stored Video)*

Video dapat di*capture* dan di*encode* untuk kebutuhan komunikasi *real time* atau dapat juga di*pre-encoded* dan disimpan dalam format DVD atau Video-CD untuk dijalankan pada saat dibutuhkan. Contoh aplikasi yang membutuhkan *real time encoding* adalah *videophone*, *video conferencing* dan *interactive games*. Sedangkan aplikasi *video pre-encoded* antara lain DVD, Video-CD, dan yang dikenal dengan penyimpanan secara lokal atau *Video On Demand* (VOD). Penyimpanannya dilakukan secara remote di server.

2.5.3 Transfer Video via File Download dan Transfer Video via *Streaming*

Sebuah file video dapat ditampilkan di user dengan menggunakan dua metode transfer file. Pertama, dengan mendownload keseluruhan file video dan yang kedua, dengan melakukan proses *streaming*. Kedua metode ini memiliki kekurangan dan kelebihannya masing-masing. File video yang diambil dari server dengan cara download, tidak dapat ditampilkan sebelum seluruh file video tersebut selesai tersalin ke *buffer*. Untuk itu, diperlukan media penyimpanan yang cukup besar dan waktu yang diperlukan untuk proses *download* cukup lama karena file video biasanya berukuran besar. Ide dasar dari *video streaming* ini adalah membagi beberapa paket video menjadi beberapa bagian, mentransmisikan paket data tersebut, kemudian penerima (*receiver*) dapat men-*decode* dan memainkan

potongan video tanpa harus menunggu seluruh file terkirim ke mesin penerima.

2.5.4 *Streaming Protocol*

Teknik *streaming* tingkat aplikasi untuk mendapatkan hasil terbaik dari layanan best effort:

a) *Buffer* disisi client
b) Menggunakan UDP, bukan TCP
c) Menggunakan teknik pengkodean multimedia.

Aplikasi layanan streaming saat ini banyak menggunakan RTSP (*Real Time Streaming Protocol*). Adapun cara kerjanya adalah sebagai berikut:

a) *Metafile* berkomunikasi melalui *web browser*
b) *Browser* menjalankan *player*
c) *Player* membuat kondisi kendali RTSP dan koneksi data ke server streaming

Real Time Protokol (RTP) merupakan struktur paket standar untuk membawa data *audio* dan *video*. RTP berfungsi untuk transmisi real time data seperti audio, video, multimedia secara end-to-end. RTP mendukung transmisi *unicast*, *broadcast* dan *multicast*. RTP hanyalah sebagai protokol transport dan hal ini tidak menjamin quality of service untuk layanannya. Streaming server memotong media data untuk masing-masing *track* menjadi paket RTP yang kemudian ditransmisikan melalui UDP. Masing-masing paket RTP ditransmisikan dengan beberapa informasi yaitu:

a) RTP *header*
b) RTP *payload header*
c) RTP *payload data*

Pada RTP *header* memuat informasi tentang versi RTP, *sequence number*, *timestamp*, *Synchronization Source Identifier (SSRC)*. *Sequence number* digunakan untuk inisialisasi paket yang dikirimkan dan bisa dipakai untuk penghitungan packet loss. *Timestamp* menunjukkan waktu paket yang dipakai untuk sinkronisasi dan penghitungan *jitter*. SSRC mengindikasikan keunikan dan keaslian paket dalam suatu *session*. Kunci keunggulan RTP adalah kemampuan interoperabilitas: jika dua aplikasi Internet Phone menggunakan RTP, maka tidak akan terjadi masalah.

2.6 Parameter Kinerja Jaringan

Dalam lingkup jaringan, dikenal istilah QoS yang merupakan metode pengukuran untuk mengetahui seberapa baik jaringan dan mengetahui bagaimana karakteristik serta sifat dari satu layanan. Qos mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Salah satu lembaga yang mengeluarkan standarisasi tentang kinerja jaringan adalah *Telecommunication and Internet Protocol Harmonization Over Network* (TIPHON). TIPHON mendefinisikan QoS sebagai pengaruh kolektif atas kinerja layanan yang menentukan tingkat kepuasan pemakai layanan. Tabel 2.0 menampilkan peringkat dan kriteria QoS.

Tabel 2.0. Peringkat dan kriteria QoS (TIPHON, 1999)

Nilai	Persentase (%)	Indeks
3,8 – 4 | 95	100	Sangat Memuaskan
3 – 3,79 | 75	94,75	Memuaskan
2 – 2,99 | 50	74,75	Kurang Memuaskan
1 – 1,99 | 25	49,75	Buruk

Parameter-parameter QoS terdiri dari (TIPHON, 1999):

1. ***Throughput*** yaitu kecepatan (rate) transfer data efektif, yang diukur dalam bps. *Header-header* dalam paket-paket data mengurangi nilai throughput. Maka penggunaan sebuah saluran secara bersama-sama juga akan mengurangi nilai ini. Persamaan (2.1) menunjukkan cara mendapatkan nilai *throughput* sebuah jaringan [10].

$$Throughput = \frac{\text{Jumlah Data yang dikirimkan}}{\text{waktu pengiriman data}} \quad \text{..... (2.1)}$$

Nilai *Throughput* pada suatu jaringan dapat dikategorikan dalam standarisasi TIPHON pada Table 2.1.

Tabel 2.1 Peringkat dan kinerja *Throughput* (TIPHON, 1999)

Nilai	Persentase (%)	Indeks
4	100	Sangat Bagus
3	75	Bagus
2	50	Kurang Bagus
1	<25	Buruk

2. ***Packet Loss***, adalah kegagalan transmisi paket data mencapai tujuannya. Umumnya perangkat *network* memiliki *buffer* untuk menampung data yang diterima. Jika terjadi kongesti yang cukup lama, buffer akan penuh, dan data baru tidak diterima. Satuan yang digunakan pada perhitungan *packet loss* adalah persen. Persamaan (2.2) menunjukkan cara memperoleh nilai *packet loss* [10].

$$Packet\ Loss = \frac{\text{Packet data dikirim} - \text{Packet data diterima}}{\text{Packet Data dikirim}} \times 100\% \quad \text{..... (2.2)}$$

Kategori *Packet Loss* ditampilkan pada table 2.2.

Tabel 2.2 Peringkat dan kriteria *Packet Loss* (TIPHON, 1999)

Nilai	Persentase (%)	Indeks
4	0	Sangat Bagus
3	3	Bagus
2	15	Kurang Bagus
1	25	Buruk

3. ***Latency (Delay)***, adalah waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. Waktu tunda ini bisa dipengaruhi oleh jarak (misalnya akibat pemakaian satelit), atau kongesti (yang memperpanjang antrian), atau bisa juga akibat waktu olah yang lama (misalnya untuk *digitizing* dan kompresi data). Persamaan (2.3) menunjukkan cara memperoleh nilai *delay* dalam suatu jaringan. Dalam perhitungan *delay* digunakan satuan ms (*mili second*) [10].

$$Delay = \frac{\text{Waktu dari awal pengiriman sampai akhir penerimaan packet}}{\text{Total packet}} \quad \text{..... (2.3)}$$

Peringkat *Delay* pada suatu jaringan dapat dikategorikan berdasarkan standarisasi TIPHON pada Table 2.3.

Tabel 2.3 Standarisasi *Delay* oleh TIPHON

Nilai	Besar Delay	Indeks
4	<150 ms	Sangat Bagus
3	150 s/d 300 ms	Bagus
2	300 s/d 450 ms	Kurang Bagus
1	>450 ms	Buruk

4. ***Jitter***, diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu *pengolahan* data, dan juga dalam waktu penghimpunan ulang paket-paket di

akhir perjalanan *jitter*. *Jitter* dapat juga dikatakan sebagai variasi delay jaringan dan dapat dirumuskan sebagai berikut:

$$Jitter = \frac{\text{Total variasi Delay}}{\text{Total paket yang diterima} - 1} \quad \text{..... (2.4)}$$

$$Total\ variasi\ Delay = Delay - (rata - rata\ Delay) \text{..... (2.5)}$$

Peringkat *Jitter* pada suatu jaringan dapat dikategorikan berdasarkan standarisasi TIPHON pada Table 2.4.

Tabel 2.4. Standarisasi *Jitter* oleh TIPHON

Nilai	Besar Jitter (ms)	Indeks
4	0	Sangat Bagus
3	0 – 75 ms	Bagus
2	75 – 125	Kurang Bagus
1	125 - 225	Buruk