BAB 2
LANDASAN TEORI

2.1 Landasan Teori

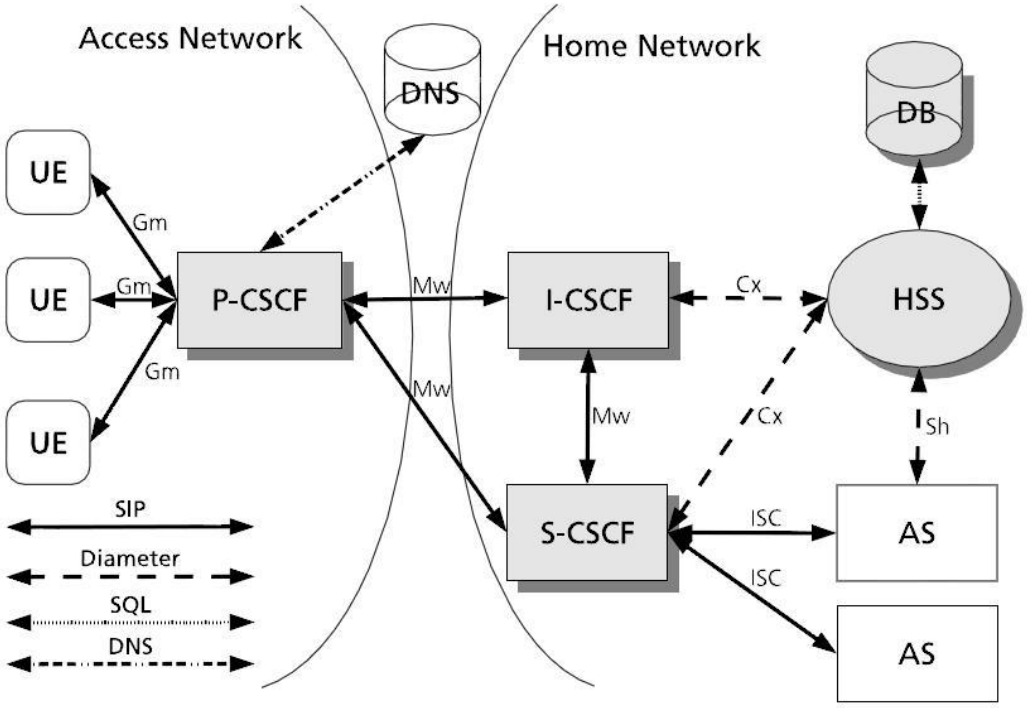
Landasan teori menjelaskan dasar-dasar teori yang digunakan dalam penelitian yang dulakukan pada tugas akhir ini. Teori-teori yang digunakan meliputi IMS, *Internet Protocol*, *Routing Protocol*, MPLS, MPLS-TE, QoS, Protokol persinyalan, Implementasi QoS pada MPLS, *Diffserv*, IPTV, Protokol Dasar IPTV.

2.1.1 IP Multimedia Subsystem (IMS)

IMS merupakan komponen utama untuk mendukung konvergensi layanan di mana teknologi ini didesain untuk mengisi *gap* antara telekomunikasi tradisional dan teknologi internet. IMS dirancang untuk memberikan sejumlah fungsi yang dibutuhkan untuk mendukung layanan berbasis IP melalui jaringan bergerak dan nirkabel. IMS secara spesifik dirancang untuk mendukung layanan multimedia yang bersifat *real-time* seperti *video telephony*, *video conference*, dan *push services*. Dalam dunia kovergensi, IMS memainkan peran penting dimana dengan bantuan SIP, IMS dapat memberikan layanan berbasis IP seperti VoIP, *video conference*, IPTV, dan layanan multimedia lainnya. SIP merupakan salah satu *signaling protocol* pada IMS dimana SIP menfasilitasi interkoneksi antara jaringan fixed dan jaringan bergerak[1].

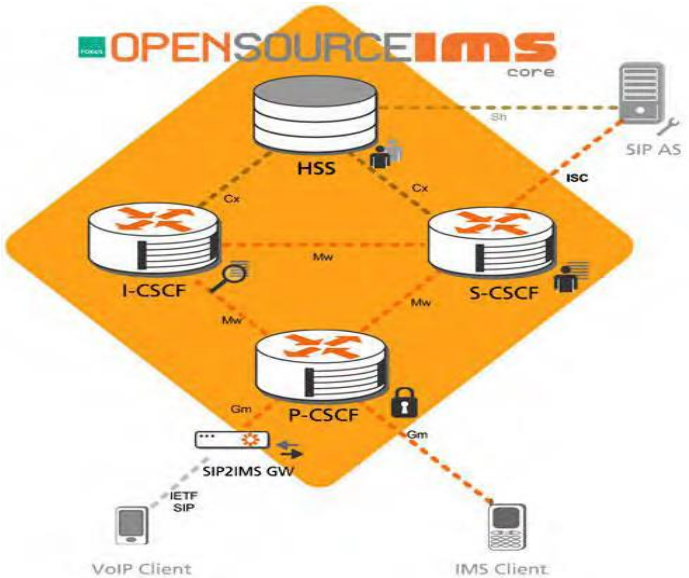
Latar belakang dikembangkan teknologi IMS ini adalah kemudahan dalam pembuatan layanan (*service*) baru pada jaringan telekomunikasi khususnya layaanan multimedia. Selain itu, IMS juga memberikan kemudahan dalam integrasi dengan internet dan meningkatkan kecepatan dalam mengakses data. Teknologi IMS menggunakan *Session Initiation Protocol* (SIP) sebagai protokol pengontrol sesi (*session control*) yang dilakukan oleh pengguna yang satu dengan yang lainnya ataupun dengan suatu aplikasi. Untuk menunjang fungsinya sebagai *session control*, maka IMS menyediakan beberapa fungsi seperti mekanisme

charging, *subscriber profile management* dan pengalokasian *Quality of Service* (QoS) pada media transmisinya[1].



Gambar 2.1 Open IMS Core Pada Jaringan IMS

Bagian terpenting dari jaringan IMS terletak pada IMS Core-nya yang terdiri dari beberapa komponen yaitu: *Home Subscriber Server* (HSS), *Proxy* CSCF (P-CSCF), *Interrogating* CSCF (I-CSCF), dan *Serving* CSCF (S-CSCF)[1].



Gambar 2.2 Elemen OpenIMSCore

2.1.1.1 *Home Subscriber Server* (HSS)

Pada implementasinya nanti, setiap pelanggan IMS akan memiliki satu atau lebih identitas pribadi (*Private User Identity*). Identitas ini berisi tentang informasi akan layanan-layanan apa saja yang bisa di akses oleh pengguna, berlaku secara global dan identitas ini akan disimpan di dalam *Home Subscriber Server* (HSS) ketika kita melakukan registrasi. HSS ini dapat dipandang sebagai evolusi dari *Home Location Register* (HLR) yang berfungsi sebagai database informasi tentang para pengguna. HSS menyimpan profil pengguna, informasi tentang pengguna mana saja yang sedang teregister serta status lokasi dari semua pengguna. Informasi-informasi ini diperlukan pada saat *Authentication, Authorization,* dan *Accounting* (AAA) dimana S-CSCF akan mengakses ke HSS yang keduanya terhubung dengan Cx *reference point.*

2.1.1.2 *Proxy Call Session Control Function* (P-CSCF)

Ketika kita melakukan akses layanan IMS maka titik masuk pertama menuju IMS adalah P-CSCF. P-CSCF berperan dalam meneruskan SIP messages antara *user equipment* dengan node yang benar pada IMS. Bila pengakses layanan berada di luar *server* asalnya maka *user equipment* akan melakukan akses ke P-CSCF jaringan tempat pengakses layanan berada dan kemudian diteruskan ke IMS server asalnya.

2.1.1.3 *Interrogating Call Session Control Function* (I-CSCF)

I-CSCF merupakan titik kontak untuk pengguna di jaringan asalnya dimana I-CSCF ini berfungsi dalam menentukan S-CSCF yang tepat untuk pengguna dengan berdasarkan informasi-informasi seperti: lokasi, kapabilitas dan availabilitas S-CSCF yang ada. Setelah memilih S-CSCF yang sesuai maka ICSCF akan menginformasikan S-CSCF yang harus dipilih oleh pengguna berdasarkan data di HSS.

2.1.1.4 *Serving Call Session Control Function* (S-CSCF)

S-CSCF berfungsi dalam menyediakan proses registrasi, *back-2-back agent* untuk control panggilan, dan layanan bagi pengguna sehingga pengguna

dapat mengakses aplikasi-aplikasi yang disediakan. Selain itu, S-CSCF juga berfungsi dalam mentranslasi format dari perangkat telekomunikasi seperti telepon rumah dan telepon seluler menjadi SIP URI dengan mekanisme translasi ENUM DNS.

2.1.2 *Internet Protocol* (IP)

Internet Protocol adalah adalah protokol lapisan jaringan atau protokol lapisan *internetwork* yang digunakan oleh protokol TCP/IP untuk melakukan pengalamatan dan *routing* paket data antar *host-host* di jaringan komputer berbasis TCP/IP. Didesain untuk interkoneksi sistem komunukasi komputer pada jaringan *packet switched*. Pada jaringan TCP/IP, sebuah komputer diidentifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda satu sama lainnya. Hal ini dilakukan agar mencegah kesalahan pada transfer data. Terkahir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protocol ini bertugas untuk menangani pendeteksian kesalahan pada transferdata.

Salah satu hal yang penting dalam IP, dalam pengiriman informasi adalah metode pengalamatan pengirim dan penerima. Saat ini terdapat standar pengalamatan yang sudah digunakan yaitu IPv4 dengan alamat terdiri dari 32 bit.

2.1.2.1 Pengalamatan IP

Pengalamatan bertujuan bagaimana supaya data yang dikirim sampai pada mesin yang sesuai dan bagaimana hal tersebut dapat dilakukan oleh operator dengan mudah. Untuk itu maka data dari suatu *host* harus dilewatkan ke jaringan menuju *host* tujuan, dan dalam komputer tersebut data akan disampaikan ke user atau proses yang sesuai.

Di jaringan IPv4, alamat IP mengunakan nomor sebanyak 32 bit, biasanya ditulis sebagai nomor empat 8-bit di ungkapkan dalam bentuk desimal dan terpisah oleh titik. Contoh alamat IP adalah 10.0.17.1, 192.168.1.1 atau 172.16.5.23. Jika anda memerinci setiap alamat IP mungkin, alamat IP akan mencakup dari 0.0.0.0 sampai 255.255.255.255. Ini menghasilkan jumlah total sebanyak lebih dari empat milyar alamat IP yang mungkin (255 x 255 x 255 x 255

= 4.228.250.625), walaupun banyak dari alamat tersebut di reserved untuk maksud khusus dan tidak digunakan pada mesin / komputer. Masing-masing alamat IP dapat digunakan sebagai penunjuk yang unik untuk membedakan satu mesin dengan mesin lain di jaringan. Pengalamatan Ipv4 terbagi dalam lima kelas yaitu :

1. Kelas A

   Alamat-alamat kelas A diberikan untuk jaringan skala besar. Nomor urut bit tertinggi di dalam alamat IP kelas A selalu diset dengan nilai 0 (nol). Tujuh bit berikutnya untuk melengkapi oktet pertama akan membuat sebuah *network identifier*. 24 bit sisanya (atau tiga octet terakhir) merepresentasikan *host identifier*. Ini mengizinkan kelas A memiliki hingga 126 jaringan, dan 16,777,214 host tiap jaringannya. Alamat IP pada kelas A dimulai dari 1.0.0.0 sampai dengan 126.255.255.255. Alamat dengan oktet awal 127 tidak diizinkan, karena digunakan untuk mekanisme *Interprocess Communication* (IPC) di dalam mesin yang bersangkutan.

2. Kelas B

   Alamat-alamat kelas B dikhususkan untuk jaringan skala menengah hingga skala besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B selalu diset ke bilangan biner 10. 14 bit berikutnya (untuk melengkapi dua oktet pertama), akan membuat sebuah *network identifier*. 16 bit sisanya (dua oktet terakhir) merepresentasikan *host identifier*. Kelas B dapat memiliki 16,384 network, dan 65,534 host untuk setiap network-nya. Alamat IP pada kelas A dimulai dari 128.0.0.0 sampai dengan 192.167.255.255.

3. Kelas C

   Alamat IP kelas C digunakan untuk jaringan berskala kecil. Tiga bit pertama di dalam oktet pertama alamat kelas C selalu diset ke nilai biner 110. 21 bit selanjutnya (untuk melengkapi tiga oktet

pertama) akan membentuk sebuah *network identifier*. 8 bit sisanya (sebagai oktet terakhir)akan merepresentasikan *host identifier*. Ini memungkinkan pembuatan total 2,097,152 buah network, dan 254 host untuk setiap network-nya. Alamat IP pada kelas A dimulai dari 192.168.0.0 sampai dengan 223.255.255.255.

4. Kelas D

   Alamat IP kelas D disediakan hanya untuk alamat-alamat IP multicast, sehingga berbeda dengan tiga kelas di atas. Empat bit pertama di dalam IP kelas D selalu diset ke bilangan biner 1110. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali host.

5. Kelas E

   Alamat IP kelas E disediakan sebagai alamat yang bersifat "eksperimental" atau percobaan dan dicadangkan untuk digunakan pada masa depan. Empat bit pertama selalu diset kepada bilangan biner 1111. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali host.

2.1.3 *Routing Protocol*

Routing Protocol adalah proses yang digunakan *router* untuk menyampaikan paket ke jaringan tujuan. *Routing Protocol* adalah metode yang digunakan router untuk saling menukar informasi *routing* dan menyediakan koneksi dengan internet. Aturan ini dapat di berikan secara *dynamic* ke sebuah *router* dari *router* yang lain, atau dapat juga diberikan secara *static* ke *router* oleh seorang *administrator*. *Routing* berbeda dengan *bridging*. Perbedaan utama antara keduanya yaitu *bridging* berlangsung pada *layer* 2 (*Data Link Layer*) dari model OSI, sedangkan *routing* berlangsung di layer 3 (*Network Layer*).

Sebuah *router* membuat keputusan untuk menruskan paket berdasarkan IP *address* tujuan dari paket tersebut. Untuk membuat keputusan yang tepat, *router* harus mempelajari bagaimana caranya untuk mencapai jaringan yang lokasinya jauh. Ketika sebuah *router* menggunakan *router dynamic*, informasi ini dipelajari

dari *router* yang lain. Ketika *routing static* digunakan, *administrato*r jaringan harus mengkonfigurasi informasi mengenai jaringan secara manual.

2.1.3.1 *Static Routing*

Administrator sendiri yang menentukan secara manual jalur terbaik untuk mencapai jaringan tujuan dari jaringan asal. *Static Routing* merupakan metode *routing* yang paling sederhana. Karena *static route* di konfigurasi secara manual, *administrator* jaringan harus menambah dan menghapus *route* jika terjadi perubahan pada topologi jaringan. Pada jaringan yang besar, proses *maintenance* terhadap *routing table* akan memerlukan banyak waktu. *Static routing* jarang digunakan pada jaringan yang besar karena kesulitan *maintenance* terhadap *routing table* ini. Akan tetapi ada beberapa kasus dimana *static routing* digunakan bersama-sama dengan *dynamic routing*, misalnya *jika policy* jaringan mangharuskan *traffic* melalui *route* tertentu.

2.1.3.2 *Dynamic Routing*

Karena *static routing* dikonfigurasi secara manual, administrator jaringan harus menambahkan dan menghapus *static route* jika ada perubahan topologi. Oleh karena itu digunakanlah *dynamic routing*. Beberapa contoh dari *dynamic routing protocol* antara lain :

1. *Routing Information Protocol* (RIP)

   Routing protocol yang menggunakan algoritma *distance vector*, yaitu algortima Bellman-Ford. Pertama kali dikenalkan pada tahun 1969 dan merupakan algoritma *routing* yang pertama pada ARPANET. RIP yang merupakan routing protokol dengan algoritma *distance vector*, yang menghitungjumlah *hop (count hop)* sebagai *routing metric*. Jumlah maksimum dari *hop* yang diperbolehkan adalah 15 *ho*p. Tiap RIP *router* saling tukar informasi *routing* tiap 30 detik,melalui UDP *port* 520. Untuk menghindari *loop routing*, digunakan teknik *split horizon withpoison reverse*. RIP merupakan *routing protocol* yang paling

mudah untuk di konfigurasi.RIP memiliki 3 versi yaitu RIPv1, RIPv2, RIPng.

2. *Interior Gateway Routing Protocol* (IGRP)

   Interior Gateway Routing Protocol (IGRP) adalah *routing* milik Cisco. IGRP merupakan protokol *routing distance vector*. Seleksi jalurnya menggunakan metrik campuran berupa *bandwidth, load, delay dan realibility*. IGRP menukung 255 *hop count*. *Routing update*, secara *default*, akan dikirim secara *broadcast* setiap 90 detik. *Routing update* berisi semua tabel *routing* pengirim. Dibutuhkan nomor AS unik ketika mengimplementasikan IGRP pada sebuah jaringan.

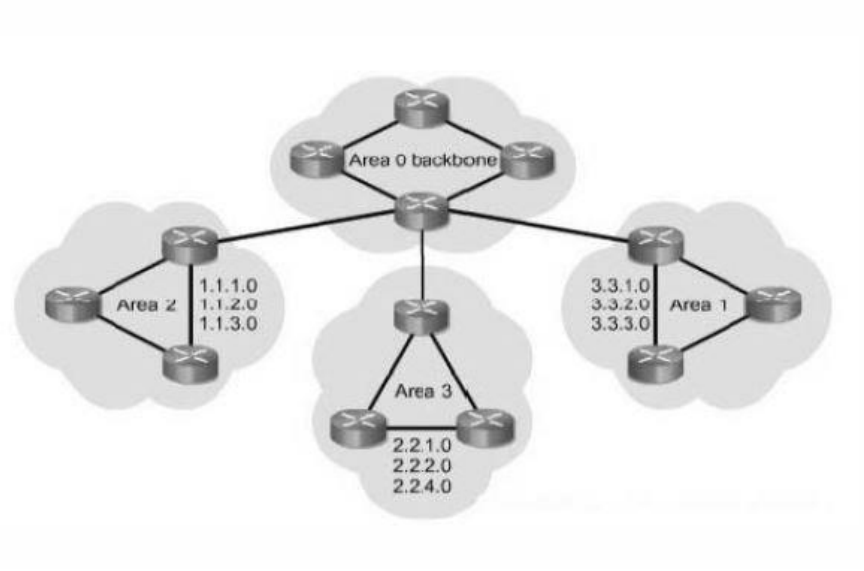
3. *Enhanced Interior Gateway Routing Protocol* (EIGRP)

   EIGRP merupakan routing protocol yang dibuat CISCO. EIGRP termasuk routing protocol dengan algoritma hybrid. Perangkat EIGRP bertukar informasi *hello packet* untuk memastikan daerah sekitar. Pada *bandwidth* yang besar *router* saling bertukar informasi setiap 5 detik, dan 60 detik pada *bandwidth* yang lebih rendah.

4. *Open Shortest-Path First* (OSPF)

   OSPF merupakan *routing protocol* berbasis *link state*, termasuk dalam *interior Gateway Protocol* (IGP). Menggunakan *algoritma Dijkstra* untuk menghitung *Shortest Path First* (SPF). Menggunakan *cost* sebagai *routing metric*. Setelah antar *router* bertukar informasi maka akan terbentuk *database link state* pada masing-masing *router*. Menggunakan metode MD5 untuk autentikasi antar *router* sebelum menerima *Link-state Advertisement* (LSA). *Router* dalam *broadcast* domain yang sama akan melakukan *adjacencies* untuk mendeteksi satu sama lainnya. Pendeteksian dilakukan dengan mendengarkan *"Hello Packet"*. Hal inidisebut 2 *way state*. *Router* OSPF mengirimkan *"Hello Packet"* dengan cara *unicast* dan *multicast*. Alamat *multicast*

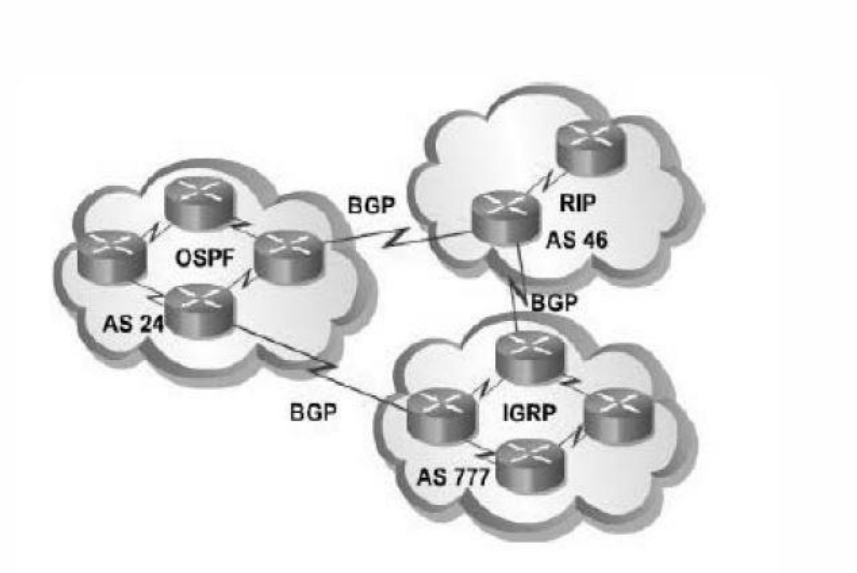
224.0.0.5 dan 224.0.0.6 digunakan OSPF, sehingga OSPF tidak menggunakan TCP atau UDP melainkan *IP protocol* 89.



Gambar 2.3 Area pada OSPF

5. *Border Gateway Protocol* (BGP)

   Border Gateway Protocol (BGP) adalah inti dari protokol *routing* internet. Protocol ini yang menjadi *backbone* dari jaringan internet dunia. BGP dijelaskan dalam RFC 4271. RFC 4276 menjelaskan implementasi *report* pada BGP-4. RFC 4277 menjelaskan hasil ujicoba penggunaan BGP-4. Ia bekerja dengan cara memetakan sebuah tabel IP *network* yang menunjuk ke jaringan yg dapat dicapai antar *Autonomous System* (AS). Hal ini digambarkan sebagai sebuah protokol *path vector*. BGP tidak menggunakan metrik IGP tradisional, tapi membuat *routing decision* berdasarkan *path, network policies*, dan *ruleset*. BGP versi 4 masih digunakan hingga saat ini . BGP mendukung *Class Inter-Domain Routing* dan menggunakan *route aggregation* untuk mengurangi ukuran tabel *routing*.



Gambar 2.4 BGP

2.1.4 *Multiprotocol Label Switching* (MPLS)

Multiprotocol Label Switching (MPLS) adalah teknologi penyampaian paket pada jaringan *backbone* berkecepatan tinggi. Asas kerjanya menggabungkan beberapa kelebihan dari sistem komunikasi *circuitswitched* dan *packet-switched* yang melahirkan teknologi yang lebih baik dari keduanya. Sebelumnya, paket-paket diteruskan dengan protokol *routing* seperti OSPF, IS-IS, BGP, atau EGP. Protokol *routing* berada pada lapisan *network* (ketiga) dalam sistem OSI.

MPLS, *Multiprotocol Label Switching*, adalah arsitektur network yang didefinisikan oleh *Internet Engineering Task Foce* (IETF) untuk memadukan mekanisme label swapping di layer 2 dengan routing di layer 3 untuk mempercepat pengiriman paket. Arsitektur MPLS dipaparkan dalam RFC-3031 [7].

Network MPLS terdiri atas sirkit yang disebut *label-switched path* (LSP), yang menghubungkan titik-titik yang disebut *label-switched router* (LSR). LSR pertama dan terakhir disebut *ingress* dan *egress*. Setiap LSP dikaitkan dengan sebuah *forwarding equivalence class* (FEC), yang merupakan kumpulan paket

yang menerima perlakukan forwarding yang sama di sebuah LSR. FEC diidentifikasikan dengan pemasangan label.

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.*

2.1.5 MPLS-TE (*Traffic Engineering*)

Rekayasa trafik (*Traffic Engineering*, TE) adalah proses pemilihan saluran data traffic untuk menyeimbangkan beban trafik pada berbagai jalur dan titik dalam jaringan. Tujuan akhirnya adalah memungkinkan *operasional network* yang andal dan efisien, sekaligus mengoptimalkan penggunaan sumberdaya dan performansi trafik. Panduan TE untuk MPLS (disebut MPLS-TE) adalah RFC-2702. RFC-2702 menyebutkan tiga masalah dasar berkaitan dengan MPLS-TE, yaitu [4]:

1. Pemetaan paket ke dalam FEC
2. Pemetaan FEC ke dalam *trunk traffic*
3. Pemetaan untuk *trunk traffic* ke topologi jaringan fisik melalui LSP

Namun RFC hanya membahas soal ketiga. Soal lain dikaji sebagai soal-soal QoS. Menyusun sebuah model MPLS-TE, yang terdiri atas komponen-komponen : manajemen path, penempatan trafik, penyebaran keadaan network, dan manajemen network [3].

a. Manajemen Path

Manajemen path meliputi proses-proses pemilihan route eksplisit berdasar kriteria tertentu, serta pembentukan dan pemeliharaan tunnel LSP dengan aturan-aturan tertentu. Proses pemilihan route dapat dilakukan secara administratif, atau secara otomatis dengan proses routing yang bersifat constraint-based. Proses constraint-based dilakukan dengan kalkulasi berbagai alternatif routing untuk memenuhi spesifikasi yang ditetapkan dalam

kebijakan administratif. Tujuannya adalah untuk mengurangi pekerjaan manual dalam TE.

Setelah pemilihan, dilakukan penempatan path dengan menggunakan protokol persinyalan, yang juga merupakan protokol distribusi label. Ada dua protokol jenis ini yang sering dianjurkan untuk dipakai, yaitu RSVP-TE dan CR-LDP. Manajemen path juga mengelola pemeliharaan path, yaitu menjaga path selama masa transmisi, dan mematikannya setelah transmisi selesai. Terdapat sekelompok atribut yang melekat pada LSP dan digunakan dalam operasi manajemen path. Atribut-atribut itu antara lain:

1. Atribut parameter trafik, adalah karakteristrik trafik yang akan ditransferkan, termasuk nilai puncak, nilai rerata, ukuran burst yang dapat terjadi, dll. Ini diperlukan untuk menghitung resource yang diperlukan dalam trunk trafik.
2. Atribut pemilihan dan pemeliharaan path generik, adalah aturan yang dipakai untuk memilih route yang diambil oleh trunk trafik, dan aturan untuk menjaganya tetap hidup.
3. Atribut prioritas, menunjukkan prioritas pentingnya trunk trafik, yang dipakai baik dalam pemilihan path, maupun untuk menghadapi keadaan kegagalan network.
4. Atribut pre-emption, untuk menjamin bahwa trunk trafik berprioritas tinggi dapat disalurkan melalui path yang lebih baik dalam lingkungan *DiffServ*. Atribut ini juga dipakai dalam kegiatan restorasi network setelah kegagalan.
5. Atribut perbaikan, menentukan perilaku trunk trafik dalam kedaan kegagalan. Ini meliputi deteksi kegagalan, pemberitahuan kegagalan, dan perbaikan.
6. Atribut policy, menentukan tindakan yang diambil untuk trafik yang melanggar, misalnya trafik yang lebih besar dari batas yang diberikan. Trafik seperti ini dapat dibatasi, ditandai, atau diteruskan begitu saja.

Atribut-atribut ini memiliki banyak kesamaan dengan network yang sudah ada sebelumnya. Maka diharapkan tidak terlalu sulit untuk memetakan atribut trafik trunk ini ke dalam arsitektur switching dan routing network yang sudah ada.

b. Penempatan Trafik

Setelah LSP dibentuk, trafik harus dikirimkan melalui LSP. Manajemen trafik berfungsi mengalokasikan trafik ke dalam LSP yang telah dibentuk. Ini meliputi fungsi pemisahan, yang membagi trafik atas kelas-kelas tertentu, dan fungsi pengiriman, yang memetakan trafik itu ke dalam LSP. Hal yang harus diperhatikan dalam proses ini adalah distribusi beban melewati deretan LSP. Umumnya ini dilakukan dengan menyusun semacam pembobotan baik pada LSP-LSP maupun pada trafik-trafik. Ini dapat dilakukan secara implisit maupun eksplisit.

c. Penyebaran Keadaan Network

Penyebaran ini bertujuan membagi informasi topologi network ke seluruh LSR di dalam network. Ini dilakukan dengan protokol gateway seperti IGP yang telah diperluas. Perluasan informasi meliputi *bandwidth* link maksimal, alokasi trafik maksimal, pengukuran TE default, *bandwidth* yang dicadangkan untuk setiap kelas prioritas, dan atribut-atribut kelas resource. Informasi-informasi ini akan diperlukan oleh protokol persinyalan untuk memilih routing yang paling tepat dalam pembentukan LSP.

d. Manajemen Network

Performansi MPLS-TE tergantung pada kemudahan mengukur dan mengendalikan network. Manajemen network meliputi konfigurasi network, pengukuran network, dan penanganan kegagalan network. Pengukuran terhadap LSP dapat dilakukan seperti pada paket data lainnya. Traffic flow dapat diukur dengan melakukan monitoring dan menampilkan statistika hasilnya. Path loss dapat diukur dengan melakukan monitoring pada ujung-ujung LSP, dan mencatat trafik yang hilang. Path delay dapat diukur dengan mengirimkan paket probe menyeberangi LSP, dan mengukur waktunya.

Notifikasi dan alarm dapat dibangkitkan jika parameter-parameter yang ditentukan itu telah melebihi ambang batas.

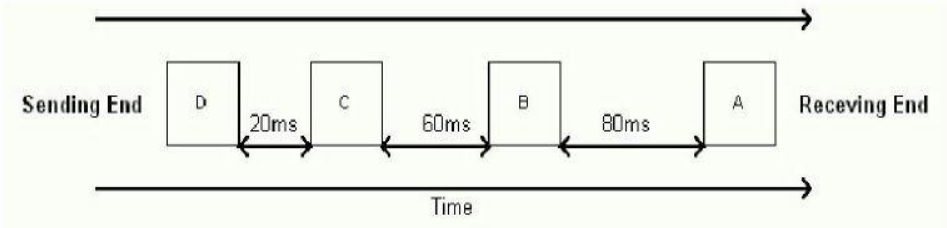
2.1.6 Quality of Service (QoS)

Ketika pertama kali mendengar kata QoS atau Quality of Service, kita pasti mendefinisikannya sebagai kualitas dari suatu layanan. Sebenarnya, QoS sangat terkenal dan menyimpan istilah yang beraneka ragam yang meiliki perspektif yang berbeda dari berbagai macam segi bidang terutama dalam segi jaringan.

Jika dilihat dari segi jaringan, QoS mengacu kepda kemampuan memberikan layanan berbeda kepada lalu lintas jaringan dengan kelas – kelas berbeda. Tujuan akhir dari QoS adalah memberikan network service yang baik dan terencana dengan melalui parameter – parameter QoS yang diatur di dalam QoS tersebut. Adapun berikut ini merupakan parameter – parameter yang digunakan dalam pengukuran QoS yaitu sebagai berikut [6]:

1. *Throughput*, yaitu kecepatan (*rate*) transfer data efektif, yang diukur dalam bps (*bit/second*). *Throughput* merupakan jumlah total kedatangan paket yang sukses diamati pada destination selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. *Throughput* maksimal dari sutau titik atau jaringan komuniksai menunjukan kapasitasnya.
2. *Packet Loss*, merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena collision dan congestion pada jaringan dan hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia untuk aplikasiaplikasi tersebut. Umumnya perangkat jaringan memiliki buffer untuk menampung data yang diterima. Jika terjadi kongesti yang cukup lama, *buffer* akan penuh, dan data baru tidak akan diterima.
3. *Delay* (*latency*), adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Delay dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama.

4. *Jitter*, didefiniskan juga sebagai variasi *delay* yang diakibatkan oleh panjang *queue* dalam suatu waktu pengolahan data, *reassemble* paket-paket data di akhir pengiriman akibat kegagalan sebelumnya dan proses pengiriman paket dalam media. *Jitter* dapat juga dikatakan sebagai variasi delay jaringan.



Gambar 2.5 Ilustrasi *Jitter* suatu paket data

Jitter dapat diilustrasikan seperti pada gambar 2.2, suatu *source* mengirimkan paket data A-B-C-D, setiap paket dikirimkan ke *destination* dengan variasi *delay* (*jitter*) yang berbeda-beda, antara paket A dan B terdapat variasi *delay* sebesar 80 ms, antara paket B dan C sebesar 60 ms, dan antara paket C dan D sebesar 20 ms. Jitter bernilai < 50ms (ITU-T Y.1541), dan bernilai < 30ms (Cisco).

2.1.7 Protokol Persinyalan

Pemilihan path, sebagai bagian dari MPLS-TE, dapat dilakukan dengan dua cara: secara manual oleh administrator, atau secara otomatis oleh suatu protokol persinyalan. Dua protokol persinyalan yang umum digunakan untuk MPLS-TE adalah CR-LDP dan RSVP-TE. RSVP-TE memperluas protokol RSVP yang sebelumnya telah digunakan untuk IP, untuk mendukung distribusi label dan routing eksplisit. Sementara itu CR-LDP memperluas LDP yang sengaja dibuat untuk distribusi label, agar dapat mendukung persinyalan berdasar QoS dan routing eksplisit.

Ada banyak kesamaan antara CR-LDP dan RSVP-TE dalam kalkulasi routing yang bersifat *constraint-based*. Keduanya menggunakan informasi QoS yang sama untuk menyusun routing eksplisit yang sama dengan alokasi *resource* yang sama. Perbedaan utamanya adalah dalam meletakkan layer tempat protokol

persinyalan bekerja. CR-LDP adalah protokol yang bekerja di atas TCP atau UDP, sedangkan RSVP-TE bekerja langsung di atas IP. Perbandingan kedua protokol ini dipaparkan dalam tabel 2.1 [2].

Tabel 2.1 Tabel Perbandingan CR-LDR dan RSVP-TE [2]

Feature	CR-LDP	RSVP-TE
Transport	TCP and UDP	Raw IP
Security	IP-Sec	RSVP Authentication
Multipoint-to-point	Yes	Yes
LSP merging	Yes	Yes
LSP state	Hard	Soft
LSP refresh	Not needed	Periodic
Redundancy	Hard	Easy
Rerouting	Yes	Yes
Explicit routing	Strict and loose	Strict and loose
Route pinning	Yes	By recording path
LSP pre-emption	Priority based	Priority based
LSP protection	Yes	Yes
Shared reservations	No	Yes
Traffic control	Forward path	Reverse path
Policy control	Implicit	Explicit
Layer 3 protocol ID	No	Yes

Untuk standardisasi, sejak tahun 2003 sebagian besar implementor telah memilih untuk menggunakan RSVP-TE dan meninggalkan CR-LDP. Hal ini diinformasikan dalam RFC-3468[2]. Lebih jauh, RSVP-TE dikaji dalam RFC-3209.

2.1.8 Implementasi QoS pada MPLS

Untuk membangun jaringan lengkap dengan implementasi QoS dari ujung ke ujung, diperlukan penggabungan dua teknologi, yaitu implementasi QoS di *access network* dan QoS di *core network*. Seperti telah dipaparkan, QoS di *core network* akan tercapai secara optimal dengan menggunakan teknologi MPLS. Ada beberapa alternatif untuk implementasi QoS di *access network*, yang sangat tergantung pada jenis aplikasi yang digunakan *customer*.

2.1.9 *Differentiated Service Model* (DiffServ)

Model QoS ini merupakan model yang sudah lama ada dalam standarisasi QoS dari organisasi IETF. Model QoS ini bekerja dengan cara melakukan klasifikasi terlebih dahulu terhadap semua paket yang masuk kedalam sebuah jaringan. Pengklasifikasian ini dilakukan dengan cara menyisipkan sebuah

informasi tambahan yang khusus untuk keperluan pengaturan QoS dalam header IP pada setiap paket.

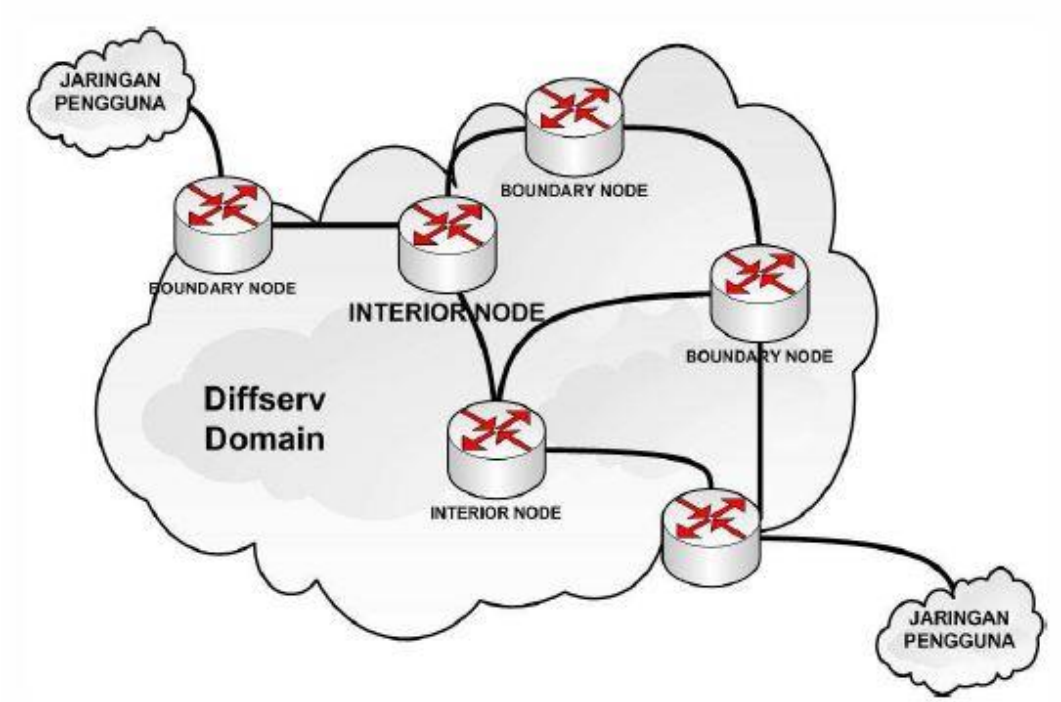
Setelah paket diklasifikasikan pada perangkat-perangkat jaringan terdekatnya, jaringan akan menggunakan klasifikasi ini untuk menentukan bagaimana traffic data ini diperlakukan, seperti misalnya perlakuan queuing, shaping dan policing nya. Setelah melalui semua proses tersebut, maka akan didapat sebuah aliran data yang sesuai dengan apa yang dikomitmenkan kepada penggunanya.

Informasi untuk proses klasifikasi pada field IP header atau dengan kata lain proses klasifikasi pada layer 3 standar OSI ada dua jenis, yaitu IP Precedence dan *Differential Service Code Point* (DSCP). Informasi klasifikasi ini ditentukan dalam tiga atau enam bit pertama dari field *Type of Service* (ToS) pada header paket IP.

Klasifikasi ini juga dapat dibawa dalam frame layer 2 dalam *field Class of Service* (CoS) yang dibawa dalam frame ISL maupun 802.1Q. Tidak seperti *IntServ,* model QoS *DiffServ* ini tidak membutuhkan kemampuan QoS pada sisi pengguna dan aplikasi-aplikasi yang bekerja di dalamnya[10].

Arsitektur *Diffserv* adalah sebuah arsitektur jaringan komputer yang mampu memperikan perlakuan seperti klasifikasi trafik, manajemen trafik dalam jaringan, dan penyediaan jaminan kualitas layanan, pada proses lalu lintas trafik dalam suatu jaringan IP. *Diffserv* bekerja dengan cara mengelompokkan aliran trafik tertentu dalam sejumlah kelas-kelas trafik untuk selanjutnya mampu memberikan perlakuan yang berbeda terhadap kelas-kelas tersebut.

Gambar 2.6 merupakan arsitektur umum pada jaringan *Diffserv*. Terdapat dua komponen utama dalam jaringan di bawah ini, yaitu *Boundary Node* dan *Interior Node.*



Gambar 2.6 Arsitektur *Diffserv*

a. *Boundary Node* adalah simpul dalam domain *Diffserv* yang mempunyai tugas untuk melakukan klasifikasi dan juga pengkondisian paket ketika paket pertama kali masuk domain tersebut.
b. *Interior node* berfungsi sebagai penghubung antar simpul pada domain *Diffserv*. Interior nodes dapat melakukan proses pengkondisian trafik yang terbatas, seperti pengkodean ulang nilai *Diffserv Code Point* (DSCP) pada suatu paket.

2.1.9.1 *Diffserv Code Point* (DSCP)

Pada jaringan *diffserv*, node-node di pinggir (*ingress*) sebuah domain memproses dan member tanda *Type of Service* (TOS) *byte* di dalam IP *header* dari sebuah paket oleh sebuah kode yang dinamakan *Diffserv Code Points* (DSCP) atau DS *byte* yang berdasarkan negosiasi kontrak dan router-router yang lainnya dalam domain tersebut. *Diffserv* menggunakan 6-bit *Diffserv Code Point* (DSCP) pada 8-bit *Differentiated services Field* (DS *field*) didalam IP *header* untuk tujuan klasifikasi paket. DS field dan ECN *field* menggantikan IPv4 TOS *field* yang sudah usang. Dalam hal ini yang menerima paket hanya melihat nilai DSCP yang memberi perlakuan istimewa pada paket tersebut. Perlakuan istimewa ini

dinamakan *Per-Hop Behavior* (PHB)[10]. Saat ini *Internet Engineering Task Force* (IETF) mempunyai standar klasifikasi PHB, yaitu *Expedited Forwarding* (EF), *Assured Forwarding*(AF), *Best Effort* (BE). Masing-masing PHB ini dikarakteristikkan dari *resources* yang mereka miliki (seperti ukuran *buffer* dan *bandwidth*), prioritas relatif terhadap *Per Hop Behavior* (PHB) lainnya atau karakteristik pengamatan yang mereka miliki (seperti *delay* dan *loss*).

Klasifikasi trafik multimedia digolongkan dalam kelas diffserv meliputi voip dan video yang digolongkan kelas EF, data UDP sebagai kelas AF dan data TCP (FTP) sebagai kelas BE. Dari keterangan di atas dapat dijelaskan beberapa hal yang menjadi karakteristik DiffServ, yaitu:

1. *Header* pada IP termasuk DSCP menunjukkan tingakat layanan yang diinginkan.
2. DSCP memetakan paket ke PHB tertentu untuk diproses oleh *router* yang kompatibel.
3. PHB menyediakan tingkat layanan tertentu (seperti *bandwidth*, *queueing*, dan *dropping decisions*) yang sesuai dengan *network policy*. Misal untuk paket-paket yang sangat *sensitive* terhadap timbulnya *error*, seperti pada aplikasi keuangan, paket-paket tersebut dikodekan dengan sebuah DSCP yang mengindikasikan layanan dengan *bandwidth* tinggi dan lintasan *routing* yang bebas *error* (0-*frame-loss*).

DSCP didalam RFC-4594 adalah rentang angka antara 0..63 yang ditempatkan ke dalam sebuah paket IP untuk menandainya menurut kelas yang melewati jaringan. Setengah dari nilai-nilai ini dialokasikan untuk standar layanan, dan sebagian lainnya disediakan untuk definisi lokal. Tabel 2.2 berikut merupakan bentuk umum untuk nilai DSCP :

Tabel 2.2 Nilai *Diifserv Code Point* (DSCP)

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
101 110	46	High Priority Expedited Forwarding (EF)	N/A	101 - Critical
000 000	0	Best Effort	N/A	000 - Routine
001 010	10	AF11	Low	001 - Priority
001 100	12	AF12	Medium	001 - Priority
001 110	14	AF13	High	001 - Priority
010 010	18	AF21	Low	001 - Immediate
010 100	20	AF22	Medium	001 - Immediate
010 110	22	AF23	High	001 - Immediate
011 010	26	AF31	Low	011 - Flash
011 100	28	AF32	Medium	011 - Flash
011 110	30	AF33	High	011 - Flash
100 010	34	AF41	Low	100 - Flash Override
100 100	36	AF42	Medium	100 - Flash Override
100 110	38	AF43	High	100 - Flash Override
DSCP Value	**Decimal Value**	**Meaning**	**Drop Probability**	**Equivalent IP Precedence Value**
001 000	8	CS1		1
010 000	16	CS2		2
011 000	24	CS3		3
100 000	32	CS4		4
101 000	40	CS5		5
110 000	48	CS6		6
111 000	56	CS7		7
000 000	0	Default		
101 110	46	EF		

2.1.10 *Internet Protocol Television* (IPTV)

IPTV adalah layanan multimedia seperti TV, video, grafis, data yang disajikan melalui jaringan berbasis IP yang dikelola untuk memberikan tingkat kualitas dalam hal layanan, kualitas interaktivitas, dan kehandalan. IPTV juga merupakan konvergensi antara teknologi telekomunikasi dengan penyiaran (broadcast).

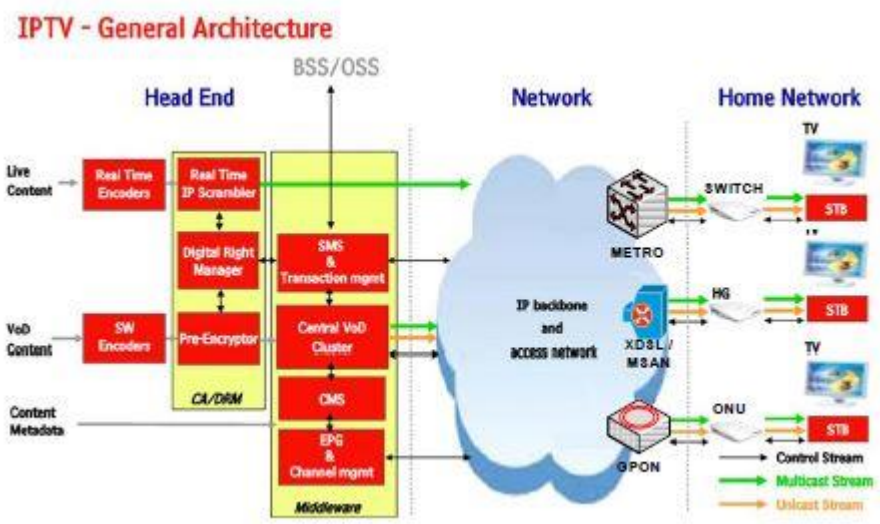
Fitur – fitur atau layanan – layanan yang terdapat pada IPTV minimal terdapat 4 layanan sebagai berikut :

1. Live TV adalah IPTV melayani pengiriman channel-channel atau siaran – siaran yang live menggunakan teknologi protocol internet yaitu IGMP v2.
2. *Video On Demand* (VoD) adalah IPTV melayani pengiriman channel – channel atau siaran – siaran yang tidak live, di mana siaran-siaran atau channel – channel disimpan di dalam server dan dapat disaksikan oleh konsumen melalui teknologi *Real Time Streaming Protocol* (RTSP).
3. *Personal Video Recording* (PVR) adalah fitur IPTV di mana siaran langsung dapat disimpan pada jaringan server yang kemudian dapat diakses oleh pelanggan sesuai waktu yang mereka tentukan tanpa biaya tambahan seperti memilki PVR pribadi yang terpasang di jaringan.
4. *Time Shifted TV* (TSTV) biasa disebut Rewind TV dimana pelanggan dimungkinkan untuk memutar/memainkan kembali tayangan program TV yang telah tersedia dengan basis program live TV. Layanan ini memungkinkan pengguna untuk menghentikan siaran dan melanjutkannya kemudian.

IP *video service quality metrics* dengan fokus utama pada kebutuhan yang berhubungan kepada persepsi pengguna dengan kinerja jaringan dan operasi yang telah dianalisis. QoE pada IPTV tidak hanya ditentukan oleh kualitas video, tetapi juga tergantung pada faktor – faktor lain seperti waktu perubahan channel, keakuratan *Electronic Program Guide* (EPG), ketanggapan untuk *pause, resume, fast forward, fast rewind, record*, dan menghentikan perintah yang dikeluarkan oleh pengguna[9].

2.1.10.1 Arsitektur dan Pengiriman *Content* Pada IPTV

IPTV Merupakan layanan yang menyediakan konten program televisi (*sport, news*, film, dll) dan konten entertainment interaktif lainnya (musik, game, *advertising*) melalui suatu jaringan broadband IP *network. End terminal* pada pelangggan dapat berupa PC desktop maupun monitor televisi yang terhubung dengan set top box.



Gambar 2.7 IPTV Arsitektur

Gambar 2.7 di atas merupakan contoh dari arsitektur IPTV secara umum. Teknologi yang terlibat dalam layanan IPTV dapat diklasifikasikan menjadi beberapa bagian utama sebagai berikut:

1. *Head-end*
   a. *Integrated Receiver Decoder* (IRD)

      Merupakan salah satu komponen di Head-End yang merupakan penerima kanal televisi melalui satelit.

   b. *Encoder*

      Encoder merupakan komponen yang merubah format *content* ke standard MPEG-4 untuk dilewatkan ke IP *Network*.

2. *Middleware*

   Middleware merupakan komponen pengendali utama layanan IPTV. *Middleware* terintegrasi dengan VoD Server, *Content provider* melalui *Content Management System* (CMS), NMS, *Set-top box*, CA/DRM system serta EMS IPTV. Dalam *Middleware* ada beberapa bagian utama lainnya berupa:

   a. *Video On Demand* (VoD)

      Sistem *Video On Demand* (VoD) merupakan sistem yang memberikan layanan VoD kepada pelanggan. VoD di *deliver* menggunakan topologi

terdistribusi yang merupakan salah satu mekanisme untuk menekan cost, terutama cost *network.*

b. EPG

Electronic Program Guide (EPG) merupakan interface layanan IPTV kepada pelanggan yang dapat di-customisasi berdasarkan profile pelanggan.

3. *Network*

Jaringan IPTV merupakan penghubung dari *Head-end* dan *Home Network*. Di dalam jaringan IPTV terjadi proses perutean yang biasa disebut routing.

4. *Home Gateway*

Home gateway merupakan merupakan perangkat antarmuka jaringan broadband yang ditempatkan di sisi pelanggan dan digunakan untuk mengakses Internet, telephony, IPTV, serta koneksi *wireless*.

5. *Set Top Box* (*STB)*

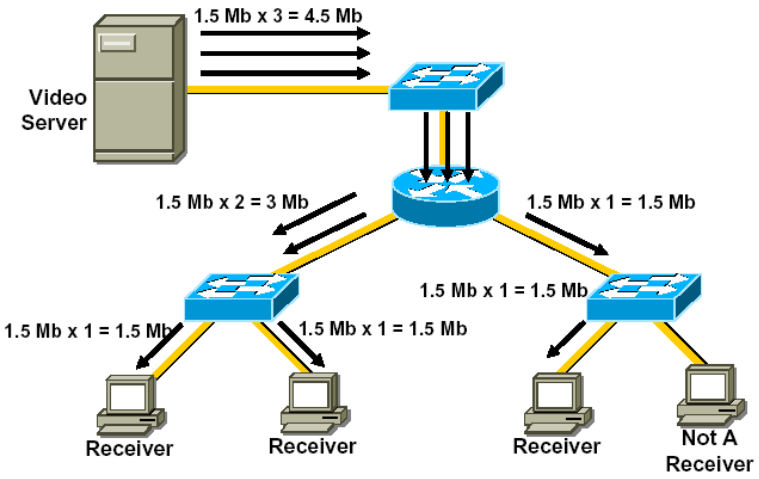
STB merupakan perangkat antarmuka dari *home gateway* ke terminal TV pelanggan. STB terintegrasi dengan perangkat *Middleware* untuk dapat memberikan layanan IPTV kepada pelanggan.

2.1.11 Protokol Dasar IPTV

Protocol dasar IPTV terdiri atas beberapa konsep, yaitu konsep *Unicast*, *Multicast*, *Broadcast*, dan IP *Multicast*.

1. *Unicast*

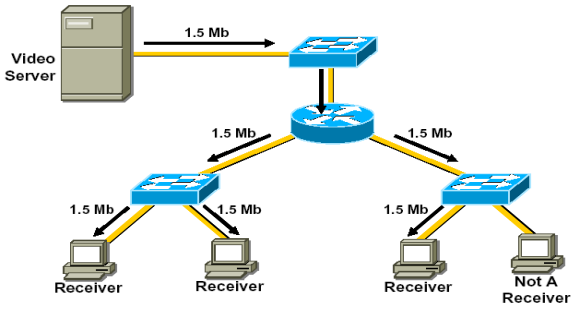
Pengiriman paket informasi hanya untuk satu tujuan saja. Unicast merupakan lawan dari broadcast, contoh *unicast* adalah *Video on Demand* (VoD). Pada saat pengiriman informasi, sumber harus menerima permintaan dari pengguna. Alamat dari pengguna akan digunakan sebagai tujuan dari pengiriman paket data.



Gambar 2.8*Unicast Traffic*

2. *Multicast*

Multicast atau *multiplexed broadcast* adalah pengiriman informasi ke suatu grup tujuan secara bersamaan dengan menggunakan suatu strategi ruting dan duplikasi, sehingga hanya tujuan yang membutuhkan saja yang mendapatkan pengiriman informasi. Pengiriman menggunakan grup alamat sebagai tujuan alamat IP di dalam paket datanya. Penerima menggunakan grup alamat untuk menginformasikan perangkat jaringan bahwa mereka butuh untuk menerima paket data yang dikirimkan untuk grup tersebut.



Gambar 2.9 *Multicast Traffic*

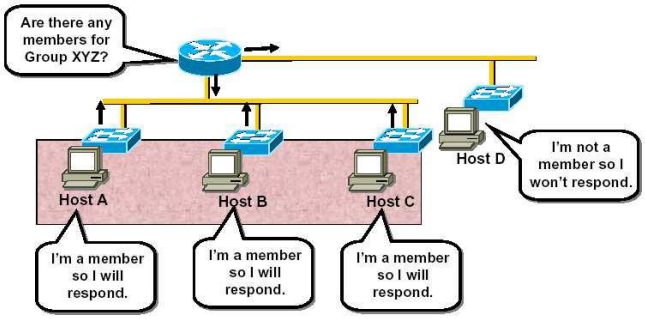
Sebuah *server multicast* mengrimkan suatu data *stream* tunggal ke banyak *client* yang menggunkan suatu alamat *broadcast* khusus. Prinsip kerja Multicast, yaitu :

a) Memfasilitasi Trafik Multimedia.

b) Mengkoordinasi operasi *Multicast* perangkat *network*.

c) Membangun lintasan antara *source* dan destinasi.

d) Meneruskan trafik *multicast* melalui *network*.

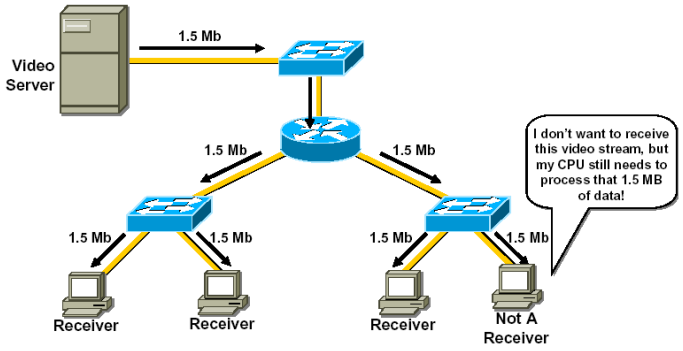


Gambar 2.10 Prinsip kerja *Multicast*

Multicast menggunakan pesan *query* dan *report* untuk membangun dan memelihara keanggotaan kelompok/group.

3. Broadcast

Broadcast adalah pengiriman paket data yang dapat diterima oleh setiap perangkat yang ada di dalam jaringan. Implementasi biasanya terbatas untuk LAN, spesifik untuk *ethernet* dan *token ring*, hal ini dimaksudkan untuk mengurangi implikasi adanya *burst* data. *Broadcast* domain adalah logik segmen jaringan dimana setiap komputer yang terhubung dapat mengirimkan data ke komputer lain di dalam domain tanpa melewati suatu perangkat ruting. Dalam implementasinya biasa dikenal dengan *VLAN*.

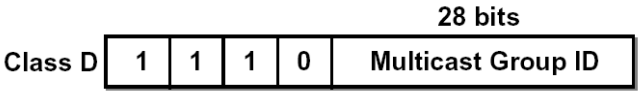


Gambar 2.11 *Broadcast Traffic*

Host-host yang tidak menggunakan aplikasi multimedia tetap harus memproses trafik *broadcast*.

4. IP *Multicast*

*S*truktur IP *address multicast*



Gambar 2.12 IP *Multicast*

Alamat kelas D yang terdiri dari 1110 sebagai *high order bit* pada oktet pertama diikuti dengan alamat 28-bit grup. Alamat kelas D mempunyai *range* dari 224.0.0.0 hingga 239.225.225.225. *High order bit* pada oktet pertama menandakan alamat berbasis 224.

Tabel 2.3 *Well-Known* IP *Multicast Address*

Start Address	Description
224.0.0.0	Reserved; not used
224.0.0.1	All devices on the subnet
224.0.0.2	All routers on the subnet
224.0.0.3	Reserved
224.0.0.4	All routers using DVMRP
224.0.0.5	All routers using OSPF
224.0.0.6	Designated routers using OSPF
224.0.0.9	Designated routers using RIP-2
224.0.0.11	Mobile agents (for mobile IP)
224.0.0.12	DHCP server / Relay Agent

Untuk setiap *channel multicast* (*live* TV atau PiP), dialokasikan satu IP *address multicast* :

a) IP *address* ganjil untuk *channel* utama.

b) IP *address* genap untuk *channel picrute in Picture* (PiP).