BAB 2

LANDASAN TEORI

2.1 Video Streaming

Video telah menjadi media yang sangat penting untuk komunikasi dan hiburan selama puluhan tahun. Pertama kali video diolah dan ditransmisikan dalam bentuk analog. Munculnya digital *IC* (*Integrated Circuit*) dan berkembang-nya komputer telah membantu terbentuknya video digital. Salah satu penerapan video digital yang digunakan dalam transmisi pada jaringan komputer adalah *video streaming*.

Video streaming adalah urutan dari "gambar yang bergerak" yang dikirimkan dalam bentuk yang telah dikompresi melalui jaringan internet dan ditampilkan oleh *player* ketika video tersebut telah diterima oleh user yang membutuhkan. Pengguna atau user memerlukan *player*, yaitu aplikasi khusus yang melakukan dekompresi dan mengirimkan data berupa video ke tampilan layar monitor dan data berupa suara ke speaker. Sebuah *player* dapat berupa bagian dari *browser* atau sebuah perangkat lunak.

Ada beberapa tipe video *streaming*, antara lain *webcast*, di mana tayangan yang ditampilkan merupakan siaran langsung (*live*), dan VOD (*video on demand*), di mana program yang ditampilkan sudah terlebih dahulu direkam atau disimpan dalam server.

Faktor-faktor yang berpengaruh dalam distribusi *video streaming* melalui jaringan antara lain besar *bandwidth* tersedia yang bervariasi (terhadap waktu), *delay* (waktu tunda), dan *lost packets*, dan juga teknik mendistribusikan video tersebut ke beberapa tujuan secara merata dan efisien. (Apostolopoulos, 2002, p1)

Dua cara yang umum digunakan untuk menerima *stream* data (video, audio, dan animasi) dari internet atau jaringan, yaitu dengan cara *download* dan *streaming*. Adapun cara lain yang juga digunakan untuk menerima stream data adalah dengan cara *progressive downloading*.

1. *Download*

   Pada penerimaan stream data dengan cara *download*, akses video dilakukan dengan cara melakukan *download* terlebih dahulu suatu *file* multimedia dari server. Penggunaan cara ini mengharuskan keseluruhan suatu *file* multimedia harus diterima secara lengkap di sisi client. *File* multimedia yang sudah diterima kemudian disimpan pada perangkat penyimpanan komputer, di mana penyimpanan ini dapat berupa penyimpanan sementara. Setelah *file* multimedia tersebut berhasil diterima secara lengkap pada sisi client, user baru dapat mengakses video tersebut. Adapun salah satu keuntungan dari penggunaan cara ini adalah akses yang lebih cepat ke salah satu bagian dari *file* tersebut. Namun, kekurangan dari penggunaan cara ini adalah seorang user yang ingin mengakses secara langsung video yang diterima harus terlebih dahulu menunggu hingga keseluruhan suatu *file* multimedia selesai diterima secara lengkap.

2. *Streaming*

   Pada penerimaan video dengan cara streaming, seorang pengguna akhir dapat mulai melihat suatu *file* mutlimedia hampir bersamaan ketika *file* tersebut mulai diterima. Penggunaan cara ini mengharuskan pengiriman suatu *file* multimedia ke user dilakukan secara konstan. Hal ini bertujuan agar seorang user dapat menyaksikan video yang diterima secara langsung tanpa ada bagian yang hilang. Keuntungan utama dari penggunaan cara ini adalah seorang user tidak perlu menunggu hingga suatu *file* multimedia diterima secara lengkap. Dengan demikian, penggunaan cara ini memungkinkan sebuah server untuk melakukan pengiriman siaran langsung (*live events*) kepada user.

3. *Progressive Downloading*

   Progressive downloading adalah metode *hybrid* yang merupakan hasil penggabungan antara metode *download* dengan metode *streaming*, di mana video yang sedang diakses diterima dengan cara *download*, dan *player* pada sisi user sudah dapat mulai menampilkan video tersebut sejak sebagian dari *file* tersebut diterima walaupun *file* tersebut belum diterima secara sepenuhnya.

2.2 Streaming

Secara umum, terdapat empat buah komponen dari *streaming*, yaitu sebagai berikut:

1. Sumber / *Input*

   Sumber dari video yang akan di-*stream*, dapat berupa file video, DVD, *MPEG Card*, Satelit, ataupun TV.

2. *Encoder*

   Bagian dari aplikasi server yang bertugas untuk mengubah video sumber menjadi sebuah format yang sesuai untuk transmisi streaming, di mana format ini umumnya memiliki tingkat kompresi tinggi supaya dapat ditransmisikan dengan baik pada media jaringan.

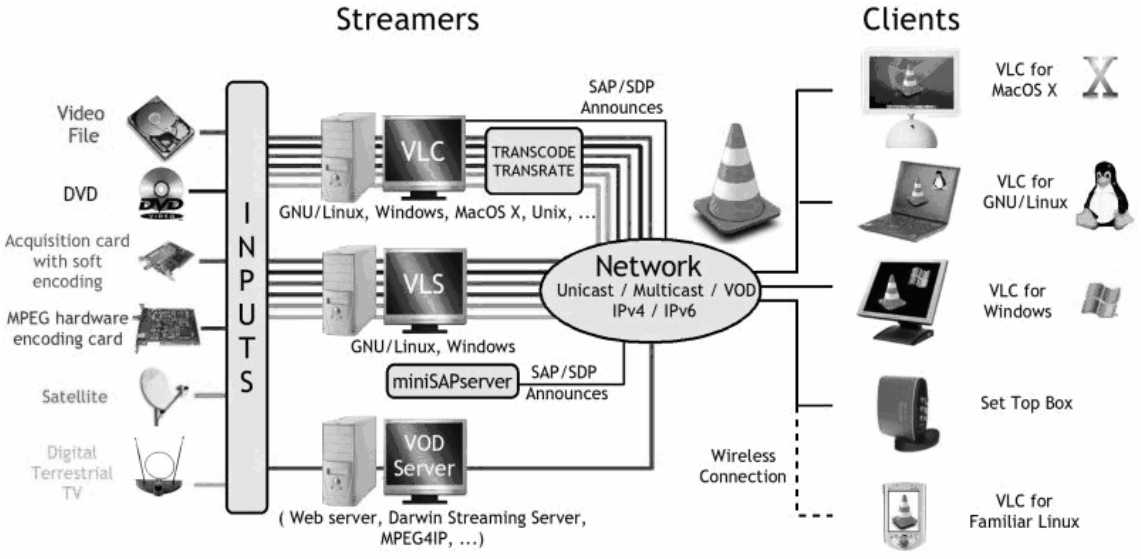
3. *Server*

   File hasil *encoding* kemudian didistribusikan oleh server kepada client. Pada aplikasi yang digunakan, *encoder* dan *server* berada pada satu aplikasi yang sama yang terintegrasi satu sama lain.

4. *Player* / Output

   Player berfungsi untuk melakukan *decoding* terhadap file hasil streaming dan menampilkan pada sisi client.

Gambar 2.1 berikut ini menunjukkan empat buah komponen streaming pada suatu sistem.



Sumber: http://www.videolan.org/vlc/streaming.html

Gambar 2.1 Diagram Komponen Dari Metode Streaming

2.3 Parameter Unjuk Kerja dalam Video Streaming

Penerapan teknologi *video streaming* mengharuskan dilakukannya perancangan sistem dan jaringan secara matang untuk memungkinkan pengiriman *video streaming* yang berkualitas tinggi. Adapun faktor-faktor yang sangat mempengaruhi unjuk kerja video streaming pada jaringan adalah *bandwidth*, *delay jitter*, dan *lost rate*. Ketiga faktor ini harus menjadi perhatian utama dalam melakukan suatu perancangan sistem dan jaringan. Ketiga faktor ini antara lain sebagai berikut:

- *Bandwidth*

  Bandwidth dapat didefinisikan sebagai jumlah bit-bit informasi yang dapat mengalir melewati sebuah koneksi jaringan dalam periode waktu tertentu. *Bandwidth* menjadi sangat penting karena hal-hal berikut:

- *Bandwidth* itu terbatas karena dibatasi oleh hukum fisika dan dukungan teknologi,
- *Bandwidth* itu tidak gratis,
- Cepatnya pertambahan tingkat kebutuhan akan *bandwidth* dalam jaringan, dan
- *Bandwidth* sangat mempengaruhi unjuk kerja jaringan.

Bandwidth yang tersedia antara dua *node* di internet pada umumnya tidak dapat diketahui secara pasti dan sangat bervariasi terhadap waktu. Besarnya *bandwidth* yang tersedia pada jaringan sangat mempengaruhi unjuk kerja suatu video streaming. Jika server melakukan pengiriman sebuah video dengan *bit rate* tinggi yang melebihi kapasitas *bandwidth* yang tersedia, maka *congestion* akan muncul dan paket-paket akan di-*drop*, sehingga akan terjadi penurunan kualitas video yang diterima. Jika server melakukan pengiriman dengan *bit rate* yang lebih rendah, hal ini akan menyebabkan penurunan kualitas video itu sendiri. Oleh karena itu, seorang perancang jaringan harus mampu memperkirakan besar kapasitas *bandwidth* yang tersedia dan menyesuaikan-nya dengan *bit rate* video yang dikirimkan.

- *Delay Jitter*

  Waktu tunda (*delay*) *end-to-end* yang terjadi dalam pengiriman paket-paket data sangat bervariasi. Dalam transmisi data pada jaringan, waktu tunda yang terjadi antara pengiriman paket satu dengan pengiriman paket lainnya mengalami fluktuasi (perubahan turun-naik). Variasi dalam waktu tunda ini

disebut dengan *delay jitter*. Adanya variasi waktu tunda dalam transmisi *video streaming* menimbulkan masalah tersendiri, yaitu paket-paket yang datang terlambat akibat dari *delay jitter* ini dapat mengganggu video yang hendak direkonstruksi ulang. Masalah ini biasanya dapat diatasi dengan adanya *buffer* pada sisi penerima, namun hal ini juga dapat ikut menyebabkan terjadinya *delay* tambahan.

- *Lost rate*

  Loss (kehilangan) dapat terjadi dengan jenis beragam, misalnya pada jaringan kabel, *lost packet* yang dimaksud adalah paket yang terhapus. Namun pada jaringan nirkabel, hal ini bisa saja diwakili oleh *bit errors* atau *burst errors*. *Losses* dapat menimbulkan degradasi kualitas unjuk kerja pada video streaming. Hal ini biasanya dapat diatasi dengan menggunakan *error control*. Empat pendekatan dalam *error control* ini antara lain, *forward error correction* (FEC), *retransmission*, *error concealment*, *error-resilient video coding*.

2.4 VOD (Video On Demand)

Sistem VOD memungkinkan pengguna untuk memilih dan menyaksikan video yang hendak diakses dalam jaringan sebagai bagian dari sistem interaktif. VOD dapat memanfaatkan proses *streaming, progressive downloading,* ataupun *download*. Sistem VOD juga memungkinkan pengguna untuk melakukan kendali pada protokol RTSP , seperti *pause, fast forward, fast rewind*, *slow forward*, dan

lain-lain. Namun pada sistem yang menggunakan metode *streaming*, hal ini akan membebani server dan memerlukan pemakaian *bandwidth* yang lebih besar.

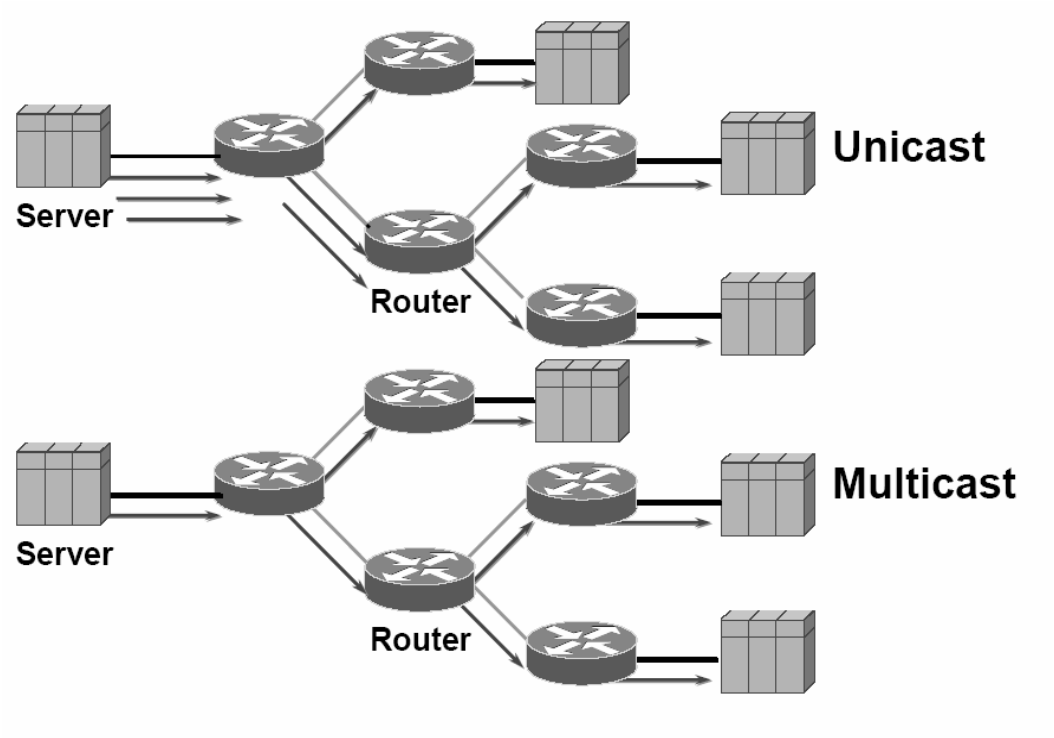
2.5 Metode Transmisi Data

Melakukan transmisi secara *broadcast*, merupakan cara transmisi yang cukup banyak dikenal. Contoh transmisi dengan metode ini adalah penyiaran televisi yang digunakan untuk mengirimkan siaran-siaran penting seperti berita dan siaran langsung. *Broadcast* mengirimkan transmisi *file* ke seluruh penerima pada waktu yang bersamaan, walaupun karakteristik media yang tersedia untuk penerima biasanya bervariasi. Seluruh user harus memproses setiap *file* yang diterimanya, walaupun mungkin terdapat beberapa user yang tidak meminta untuk dikirimkan; dan walaupun pada akhirnya *file* yang diterima tersebut tidak diteruskan untuk diproses lebih lanjut. Masalah ini akan menjadi besar bila *file* yang dikirimkan mempunyai ukuran yang cukup besar, maka jalur yang seharus-nya dipakai untuk lalu-lintas data lain menjadi terpakai untuk sesuatu yang mungkin tidak diinginkan oleh user tersebut.

Pada metode *unicast*, sebuah server mengirimkan *file* multimedia ke satu atau beberapa client penerima. Permasalahan pada metode *unicast* terjadi ketika beberapa client mengakses suatu *file* multimedia tersebut secara bersamaan. Ketika hal ini terjadi, maka *copy* dari *file* tersebut akan direplikasi sebanyak client yang mengakses. Oleh sebab itu, semakin banyak client yang mengakses pada saat yang bersamaan, maka jalur jaringan akan menjadi padat oleh lalu lintas data *file* multimedia yang diminta oleh client-client tersebut, khususnya untuk *file* video multimedia yang umumnya berukuran cukup besar. Hal ini menyebabkan

permasalahan keterbatasan skalabilitas pada penerapan metode *unicast*. Dua faktor yang akan mempengaruhi utilisasi bandwidth bila melakukan transmisi menggunakan metode ini adalah jumlah koneksi client, dan jumlah replikasi file yang ditransmisikan untuk setiap client.

Cara yang paling efisien untuk melakukan transmisi streaming *file* video multimedia adalah *multicast*. Metode ini bekerja dengan mengirimkankan satu buah *copy* untuk setiap grup yang terdiri dari client-client yang membutuhkan. Setiap grup ditandai dengan sebuah alamat IP. Pada lingkungan yang menerapkan metode *multicast*, server akan mengirimkan satu buah *file* ke sebuah grup *multicast*, sehingga pengiriman ini tidak dipengaruhi oleh jumlah client yang hendak menerima *file* tersebut. Metode ini memungkinkan client untuk bergabung dan keluar dari suatu grup secara dinamis, dan seorang client bisa saja bergabung dengan lebih dari satu grup pada saat yang bersamaan. Hal ini meningkatkan faktor skalabilitas transmisi dibandingkan dengan transmisi secara *unicast*. Berikut ini adalah gambar yang menunjukkan perbedaan metode transmisi data pada penerapan *unicast* dan *multicast*.



Sumber: http://www.cisco.com

Gambar 2.2 Perbedaan Transmisi Unicast dengan Multicast

Konsep penerapan metode multicast didasarkan pada konsep grup di mana setiap client yang hendak menerima suatu data harus bergabung terlebih dahulu ke dalam grup yang menggunakan alamat IP *multicast*. Grup ini tidak mengenal batasan fisik, di mana client bisa memiliki lokasi di mana saja di internet. IGMP digunakan dalam proses bergabungnya sebuah client ke dalam sebuah grup.

2.6 Real-time Encoding dan Pre-encoded Video

Real-time encoding adalah proses di mana video di*capture* kemudian di*encode* untuk berkomunikasi secara *real-time*, sedangkan *pre-encoded video* adalah proses di mana video di*encode* terlebih dahulu, lalu disimpan untuk dilihat

kemudian. Contoh aplikasi *real-time encoding* adalah siaran langsung, *video-conference*, dan permainan interaktif. Dalam banyak aplikasi, cara *pre-encoded video* lebih banyak digunakan, di mana video disimpan secara lokal ataupun *remote*. Contoh penyimpanan secara lokal, yaitu menggunakan DVD atau CD. Sedangkan contoh penerapan yang menggunakan penyimpanan secara *remote* adalah VOD (*video on demand*) dan *video streaming* melalui internet.

2.7 Bit Rate

Bit rate adalah jumlah bit yang diproses per satu satuan waktu. *Bit rate* dapat disamakan dengan *transfer speed*, kecepatan koneksi, *bandwidth*, *throughput* maksimum. *Bit rate* juga bisa diartikan sebagai jumlah bit yang diproses dalam satu satuan waktu untuk mewakili media yang kontinu seperti video dan audio setelah dilakukannya kompresi. Satuannya adalah *bits per second* atau bps.

2.8 Kompresi Video

Kompresi video adalah metode mengurangi jumlah data yang digunakan untuk menampilkan video tanpa mengurangi kualitas gambar secara signifikan dan mengurangi jumlah bit yang digunakan untuk menyimpan dan/atau mengirimkan gambar digital.

Pada dasarnya, video terdiri dari susunan titik warna secara tiga dimensi. Dua dimensi digunakan untuk menentukan arah horisontal dan vertikal pada gambar bergerak, dan satu dimensi digunakan untuk menentukan posisi waktu.

Frame adalah kumpulan titik yang menampilkan satu posisi pada suatu waktu. Pada dasarnya, sebuah *frame* adalah gambar diam.

Data video terdiri dari spasial dan temporal. Spasial adalah perbedaan gambar yang terjadi di dalam frame. Temporal adalah perbadaan gambar yang terjadi antar frame. *Spatial encoding* dilakukan dengan memanfaatkan keuntungan bahwa mata manusia tidak mampu mengenali perbedaan kecil pada warna sehingga daerah pada gambar yang memiliki warna yang sama akan dilakukan proses penyederhaan. *Temporal encoding* dilakukan dengan menghitung bagian frame yang memiliki gambar yang sama dan disederhanakan menjadi jumlah bit yang lebih sedikit.

2.9 Standar Kompresi Video

Berikut ini dua standar kompresi video yang dikeluarkan oleh ITU-T dan ISO. (Apostolopoulos, 2002, p7)

- H.261

  Standar ini dirancang untuk *videoconferencing* yang beroperasi di atas jaringan ISDN dengan kecepatan = p x 64 kbps, di mana p adalah angka dari 1 sampai dengan 30.

- H.263

  Standar ini dikembangkan untuk *videotelephony* yang beroperasi di atas jaringan PSTN dengan kecepatan 33,6 kbps.

Berikut ini adalah beberapa contoh standar kompresi video yang digunakan saat ini.

- MPEG-1

  Moving Pictures Expert Group (MPEG) dikembangkan oleh ISO tahun 1988 sebagai standar kompresi dari gambar yang bergerak (video) dan audio dalam media penyimpanan digital (CD-ROM). Tahun 1991 MPEG-1 dihasilkan dan mencapai kualitas video dan audio VHS yaitu sekitar 1,5 Mbps.

- MPEG-2

  Pengembangan dari MPEG-1, ditujukan untuk aplikasi televisi digital (DTV dan HDTV) dan *bit rate* yang lebih tinggi sekitar 2 sampai 20 Mbps.

- MPEG-4

  Standar ini dirancang untuk menyediakan efisiensi fitur kompresi dan deteksi kesalahan, tambahan kegunaan seperti *object-based processing*, penyatuan dari konten alami, *synthetic*, dan sebagainya.

- H.264

  Standar ini merupakan pengembangan fitur kompresi yang paling maju di antara standar lainnya, dan diadaptasi oleh ITU-T dan ISO, mempunyai nama lain MPEG-4 Part 10. Standar ini memiliki *bit rate* sekitar 10 sampai 100 kbps.

Tabel 2.1 di bawah ini menunjukkan perbandingan beberapa standar kompresi video.

Tabel 2.1 Perbandingan Standar Kompresi Video

Standar Coding Video	Aplikasi	Bit Rate
H.261	Video Telephony dan teleconference melalui ISDN	p x 64 kb/s
MPEG-1	Video pada media penyimpanan digital (CD-ROM)	1.5 Mb/s
MPEG-2	Televisi Digital	2 - 20 Mb/s
H.263	Video Telephony melalui PSTN	33.6 kb/s
MPEG-4	Object-based coding, konten static, interaktif, dan video streaming	Bervariasi
H.264 / MPEG-4 Part 10 (AVC)	Kompresi Video Terbaru	10 – 100 kb/s

2.10 MPEG-TS (Transport Stream)

MPEG-TS adalah bagian pertama dari format yang ditentukan oleh standar MPEG-2. MPEG-TS berperan sebagai standar untuk melakukan *multiplexing* terhadap audio dan video digital, dan untuk melakukan sinkronisasi terhadap output. TS menawarkan fitur koreksi kesalahan untuk pengiriman pada media yang tidak dapat diandalkan.

2.11 RTSP (Real Time Streaming Protocol)

RTSP dikembangkan oleh IETF dan dipublikasikan pada tahun 1998. RTSP adalah protokol yang digunakan dalam sistem *streaming*, yang memungkinkan sebuah *client* untuk mengendalikan sebuah *streaming media server* secara *remote* (dari jauh). Perintah kendali tersebut menyerupai perintah pada *VCR* seperti “play”, “pause”. Beberapa *server* RTSP menggunakan RTP

sebagai *transport protocol* bagi data berupa video/audio. Beberapa yang lain menggunakan protokol dari RealNetworks yaitu RDT sebagai *transport protocol*.

2.12 RTP (Real-Time Transport Protocol)

RTP mendefinisikan sebuah format paket standar untuk mengirimkan audio dan video melalui Internet. Protokol ini dikembangkan oleh IETF Audio-Video Transport Working Group dan sekarang ini menggunakan RFC 3550. RTP tidak memiliki standar port TCP atau UDP untuk digunakan dalam berkomunikasi. Standar yang digunakan adalah komunikasi menggunakan UDP dengan nomor port yang genap dan nomor port ganjil berikutnya yang memiliki nilai lebih tinggi digunakan untuk komunikasi RTP *Control Protocol* (RTCP). Walaupun tidak terdapat standar yang tetap, namun yang biasa digunakan adalah port antara 16384 sampai dengan 32767. RTP dapat membawa data apapun dengan karakteristik *real-time*, seperti audio dan video interaktif.

Pada awalnya RTP dikembangkan untuk protokol *multicast*, namun banyak digunakan juga untuk aplikasi *unicast*. RTP dibangun berdasarkan protokol UDP. Aplikasi yang menggunakan RTP kurang peka terhadap hilangnya paket (*packet loss*), namun sangat peka terhadap *delay*, sehingga hal ini menjadikan UDP sebagai pilihan yang lebih baik daripada TCP untuk aplikasi semacam itu.

Protokol RTP tidak menyediakan mekanisme untuk menjamin pengiriman akan sampai tepat waktu. Protokol ini juga tidak memberikan jaminan *Quality of Service*(QoS) apapun, sehingga harus mengandalkan mekanisme lain untuk menjamin hal semacam ini. Bahkan pengiriman paket data yang rusak mungkin

terjadi, serta *flow and congestion control* tidak didukung secara langsung. Namun, RTP mengirimkan data-data yang diperlukan agar aplikasi dapat menyusun paket data yang diterima dalam urutan yang benar. Selain itu juga RTP menyediakan informasi mengenai kualitas penerimaan yang dapat digunakan oleh aplikasi untuk dibuat penyesuaian. Sebagai contoh, bila ada kemungkinan terbentuknya *congestion*, maka aplikasi dapat memutuskan untuk menurunkan *data rate*.

2.13 OSI Layer

Pada akhir tahun 1970, *International Organization for Standarization* (ISO) merancang model referensi *Open System Interconnection* (OSI) untuk membantu para *vendor* agar bisa membuat alat-alat dan perangkat lunak yang dapat saling bekerja sama, dalam bentuk protokol-protokol sehingga jaringan dengan *vendor* yang berbeda bisa saling bekerja sama. OSI layer terdiri dari 7 lapisan sebagai berikut:

1. Physical

   Layer ini menggambarkan hubungan data dalam bit-bit antar perangkat yang meliputi tegangan, kabel, dan susunan pin dalam kabel.

2. Data Link

   Layer ini bertugas menggabungkan paket menjadi *byte* kemudian *byte* menjadi frame, dan menyediakan akses ke media menggunakan alamat MAC, serta melakukan deteksi kesalahan.

3. Network

   Layer ini menyediakan pengalamatan secara logika, yang digunakan oleh router untuk menentukan rute. Contohnya adalah pengalamatan IP.

4. Transport

   Layer ini menyediakan metode pengiriman baik yang dapat diandalkan maupun tidak, dan melakukan perbaikan kesalahan sebelum pengiriman paket. Contoh protokol pada layer ini adalah protokol TCP dan UDP.

5. Session

   Layer ini bertugas menjaga agar *session* dari masing-masing aplikasi tetap terpisah. Contoh: *Network File System* (NFS), RPC, dan SQL.

6. Presentation

   Layer ini bertugas untuk menyajikan data dan menangani pemrosesan seperti enkripsi. Contoh: JPEG, MPEG, dan MIDI.

7. Application

   Layer ini secara garis besar menyediakan tatap muka ke pengguna. Contoh: FTP, TFTP, HTTP, SMTP, DNS, TELNET, dan SNMP.

2.14 TCP / IP

Transmission Control Protocol/Internet Protocol dibuat oleh Department of Defense (DoD) untuk memastikan dan menjaga integritas data sama seperti halnya menjaga komunikasi dalam situasi kekacauan perang. Dengan perancangan dan implementasi yang benar, jaringan TCP/IP dapat menjadi protokol yang sangat handal dan fleksibel. Pada dasarnya, TCP/IP adalah versi pemadatan dari OSI layer, yang terdiri atas 4 layer sebagai berikut:

- Process / Application Layer

  Layer ini mengintegrasikan berbagai macam aktivitas dan tugas-tugas yang melibatkan fokus dari layer OSI yaitu *Application, Presentation* dan *Session*.

Layer ini juga mendefinisikan protokol untuk komunikasi aplikasi node-to-node dan juga mengendalikan spesifikasi tatap muka pengguna.

- Transport Layer (Host-to-Host Layer)

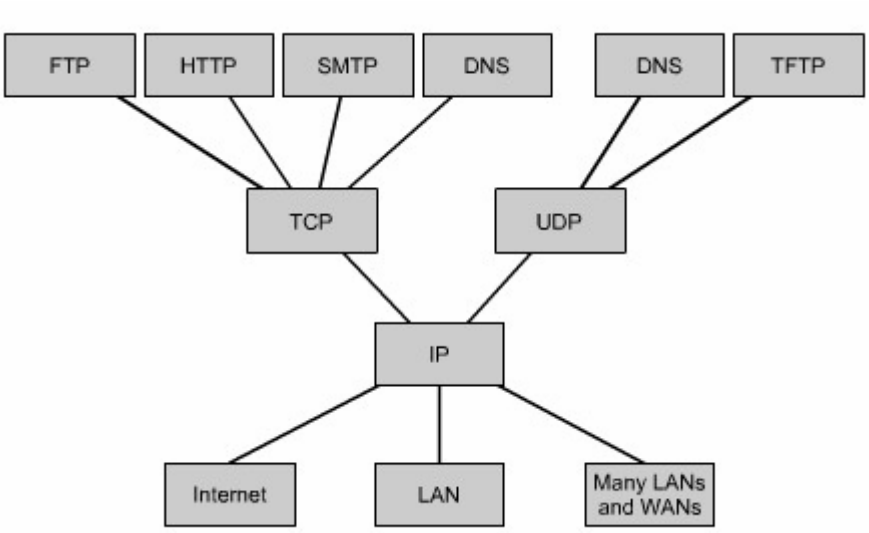
  Layer ini sejalan dengan layer *Transport* di model OSI. Layer ini mendefinisikan protokol untuk mengatur tingkat layanan transmisi untuk aplikasi. Layer ini juga menangani masalah seperti menciptakan komunikasi *end-to-end* yang handal dan memastikan data bebas dari kesalahan saat pengiriman, serta menangani mengenai urutan paket dan menjaga integritas data.

- Internet Layer

  Layer ini setara dengan layer *Network* dalam OSI, yaitu mengalokasikan protokol yang berhubungan dengan transmisi logika sebuah paket ke seluruh network. Layer ini menjaga pengalamatan host dengan memberikan alamat IP dan menangani routing dari paket yang melalui beberapa jaringan.

- Network Access Layer

  Layer ini merupakan gabungan dari layer *Physical* dan *Data Link* di OSI. Layer ini memantau pertukaran data antara *host* dan jaringan, dan bertugas mengawasi pengalamatan secara *hardware* dan mendefinisikan protokol untuk transmisi fisik data.



Sumber: Cisco Networking Academy Program Course Materials CCNA 1 - Modul 1

Gambar 2.3 Struktur Protokol pada TCP/IP

Gambar 2.3 di atas adalah gambar susunan struktur protokol pada TCP/IP yang disajikan secara berurutan, dimulai dari Application Layer, yang terdiri dari FTP, HTTP, SMTP, DNS, dan TFTP; kemudian dilanjutkan dengan Transport Layer yang terdiri dari TCP dan UDP; dan Internet Layer yang terdiri dari IP.

2.15 TCP (Transport Control Protocol)

Protokol ini menggunakan blok informasi yang besar dari aplikasi dan memecahnya ke dalam segmen. TCP memberi nomor dan mengurutkan setiap segmen supaya pada lokasi tujuan, setiap segmen dapat diurutkan kembali. Setelah segmen ini dikirim, TCP menunggu tanda *acknowledgement* dari penerima yang berada pada ujung satunya lagi, melakukan transfer ulang untuk pengiriman segmen yang tidak mendapatkan *ack* balasan. Sebelum host pengirim mengirim segmen, protokol TCP pada pengirim menghubungi protokol TCP pada

penerima dan membuat sebuah koneksi. Koneksi yang dibuat ini dikenal dengan *Virtual Circuit*. Jenis komunikasi ini disebut *connection-oriented.* Pada saat terjadi proses inisialisasi, kedua protokol TCP membuat persetujuan tentang jumlah informasi yang akan dikirim sebelum TCP pada penerima mengirim tanda *acknowledgement*. Dengan semua kesepakatan yang sudah disiapkan sebelumnya, jalur komunikasi akan terjamin. TCP memiliki sifat yang sangat kompleks dan hal ini menambah beban jaringan karena ukuran *network overhead*nya.

(Apostolopoulos, 2002, p12), TCP bukanlah protokol *Host-to-Host* yang baik ketika digunakan untuk melakukan *streaming*. Ada pun faktor penyebabnya adalah karena keuntungan TCP berupa penjaminan bahwa paket-paket data yang ditransmisikan akan sampai di penerima dengan cara transmisi ulang jika ada paket data yang hilang atau rusak sehingga menimbulkan waktu tunggu yang lama. Selain itu, karakteristik file multimedia berupa video atau audio ketika dilakukan proses *streaming* adalah cenderung untuk tetap melanjutkan walaupun ada frame yang rusak atau hilang (tampilan yang kurang baik); hal ini yang menyebabkan TCP tidak dipilih untuk implementasi streaming karena pada TCP terdapat transmisi ulang ketika terdapat frame yang rusak/hilang.

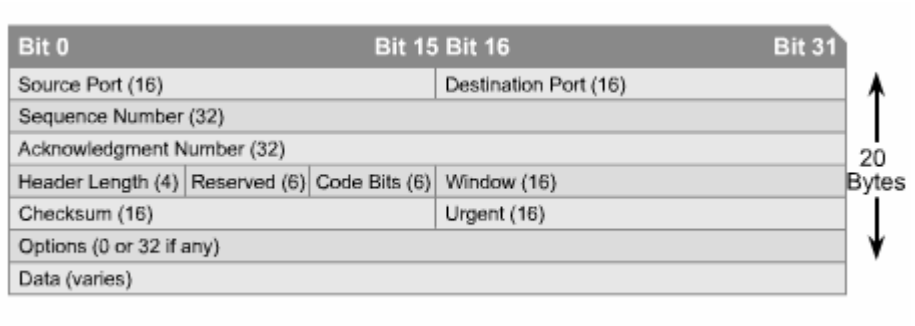
2.16 UDP (User Datagram Protocol)

Sebagian besar aplikasi multicast menggunakan protokol UDP dibandingkan dengan protokol TCP, di mana protokol TCP umum digunakan pada transmisi unicast. UDP menawarkan "*best effort delivery*" dan tidak menawarkan fungsi-fungsi yang dimiliki TCP, seperti kehandalan (*reliability*), *flow control*, dan fungsi *error recovery*.

UDP melakukan pengiriman informasi yang tidak membutuhkan kehandalan. Walaupun pengiriman dengan UDP kurang handal dibandingkan dengan protokol TCP, pengiriman data dengan UDP mengurangi *overhead* jaringan. Hal ini disebabkan karena ukuran header paket UDP yang jauh lebih kecil dibandingkan dengan header TCP. Hal ini dapat terlihat dari perbandingan ukuran header UDP dengan TCP, di mana header UDP memiliki ukuran 8 bytes, sedangkan header TCP memiliki ukuran 20 bytes.

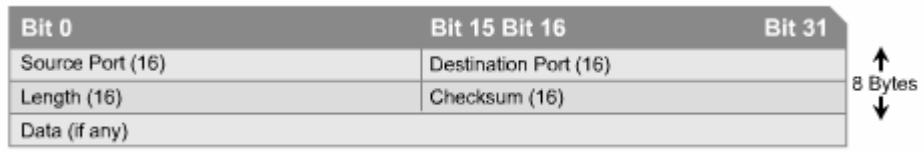
Pada protokol UDP, masalah kehandalan diserahkan pada protokol di layer *Application*. Protokol ini sangat bergantung pada protokol layer yang lebih tinggi untuk menangani *error* dan melakukan pengiriman ulang data.

UDP tidak menggunakan windows atau ACK. UDP tidak mengurutkan segmen dan dirancang untuk aplikasi yang tidak memerlukan urutan segmen. Protokol ini juga tidak menjamin bahwa segmen akan sampai di sisi penerima dengan baik sehingga protokol ini disebut sebagai protokol yang tidak handal. UDP tidak membuat *virtual circuit*, dan juga tidak menghubungi tujuan sebelum mengirimkan informasi, sehingga disebut dengan *connectionless*. Protokol UDP beranggapan bahwa aplikasi akan menggunakan metode kehandalannya sendiri, sehingga pada UDP tidak terdapat fungsi kehandalan. Hal ini memberikan pilihan kepada pengembang aplikasi apakah akan menggunakan TCP untuk kehandalan atau UDP untuk kecepatan transfer. Gambar 2.4 dan gambar 2.5 berikut ini menunjukkan perbandingan format segmen TCP dan UDP.



Sumber: Cisco Networking Academy Program Course Materials CCNA 1 - Modul 11

Gambar 2.4 Format Segmen TCP



Sumber: Cisco Networking Academy Program Course Materials CCNA 1 - Modul 11

Gambar 2.5 Format Segmen UDP

2.17 Routing Protocol

Routing adalah proses yang digunakan router untuk meneruskan paket ke jaringan tujuan. Router melihat alamat IP tujuan dalam proses ini. *Routing protocol* dibagi menjadi dua, yaitu sebagai berikut:

- *Static Routing*

  Pada *static routing*, administrator menentukan jalur/rute yang dituju secara manual. Kekurangan dari *static routing* adalah apabila terjadi perubahan pada jaringan, maka administrator harus menambah atau menghapus *route* secara manual. *Static routing* dapat menyebabkan permasalahan besar ketika terjadi perubahan pada sebuah jaringan yang

sangat besar. Sebaliknya dalam jaringan yang kecil, *static routing* ini mempunyai kelebihan dalam kemudahan konfigurasi dan *maintenance*.

- *Dynamic Routing*

  Pada *dynamic routing*, informasi mengenai rute ke jaringan lain atau jaringan yang dituju diperoleh dari router lainnya. Contoh protokol dynamic routing adalah RIP, IGRP, EIGRP, OSPF.

2.18 Alamat IP

Pengalamatan *Internet Protocol* (IP) adalah pengidentifikasian dengan angka yang diberikan ke setiap antarmuka perangkat di dalam jaringan IP. Pengalamatan IP digunakan untuk menunjukkan lokasi spesifik dari perangkat dalam jaringan. Alamat IP terdiri dari 32 bit informasi, terbagi menjadi 4 bagian, yang dikenal sebagai *octet* atau *byte*, di mana masing-masing terdiri atas 1 *byte* (8 bit) dan dapat dikonversi menjadi bilangan desimal. Alamat *network* memberikan identifikasi unik untuk setiap jaringan. Setiap perangkat pada jaringan yang sama menggunakan atau berbagi alamat *network* yang sama sebagai bagian dari pengalamatan IP. Alamat *node* memberikan identifikasi secara unik pada setiap perangkat di dalam jaringan. Bagian dari alamat ini haruslah unik karena alamat *node* mengidentifikasikan sebuah perangkat tertentu.

Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

Sumber: Cisco Networking Academy Program Course Materials CCNA 1 - Modul 9

Gambar 2.6 Perbandingan Jumlah Host dan Network berdasarkan Kelas IP

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

Sumber: Cisco Networking Academy Program Course Materials CCNA 1 - Modul 9

Gambar 2.7: Perbandingan Aturan Bit berdasarkan Kelas IP

Gambar 2.6 dan gambar 2.7 di atas menunjukkan kelas-kelas alamat IP yang dibedakan menurut ukuran jaringan. Berikut ini adalah penjabaran kelas-kelas alamat IP di atas.

- Kelas A

  Octet pertama pada pengalamatan kelas A digunakan untuk *network*; *octet* kedua, ketiga dan terakhir adalah untuk alamat *host*. Jangkauan alamat kelas A adalah 0-127 ditandai dengan bit pertama dari *octet* pertama yang harus bernilai 0 sedangkan yang lainnya adalah bebas (0xxxxxxx). Kelas A digunakan pada jaringan dengan network yang sedikit dengan jumlah *host* yang sangat banyak.

- Kelas B

  Pada pengalamatan kelas B, *octet* pertama dan kedua digunakan untuk *network*, sedangkan *octet* ketiga dan keempat adalah untuk *host*. Jangkauan alamat kelas B adalah 128-191, ditandai dengan bit pertama dan bit kedua dari *octet* pertama yang harus bernilai 1 dan 0, sedangkan sisanya bernilai bebas (10xxxxxx).

- Kelas C

  Pada pengalamatan kelas ini, *octet* pertama, kedua, dan ketiga digunakan untuk *network*, sedangkan *octet* terakhir untuk *host*. Jangkauan alamat kelas C adalah 192-223, ditandai dengan bit pertama, kedua, dan ketiga dari *octet* pertama yang harus bernilai 1, 1, dan 0 (110xxxxx). Kelas C digunakan untuk jumlah network yang banyak dan jumlah *host* yang sedikit.

- Kelas D

  Pengalamatan kelas D adalah pengalamatan yang tidak memiliki alokasi khusus untuk *network* maupun *host*. Pengalamatan ini mempunyai jangkauan alamat dari 224 hingga 239, ditandai dengan nilai bit pertama sampai dengan bit keempat dari *octet* pertama yang bernilai 1110, sedangkan bit-bit lainnya dapat bernilai bebas (1110xxxx). Pengalamatan kelas D memiliki perbedaan dengan pengalamatan kelas A, B, dan C. Hal ini disebabkan karena 28 bit terakhir dari pengalamatan kelas D tidak terstruktur. Pengalamatan kelas D ini diperuntukkan untuk pengalamatan IP *multicast*.

- Kelas E

  Pengalamatan kelas E digunakan untuk penelitian dan mempunyai jangkauan alamat dari 240 sampai dengan 255. Pengalamatan kelas ini ditandai dengan nilai bit pertama sampai dengan bit keempat dari *octet* pertama yang memiliki nilai 1 (1111xxxx).

2.19 Alamat Ethernet

Ethernet menggunakan alamat *Media Access Control* (MAC) yang telah ditanamkan ke dalam setiap kartu adapter jaringan (NIC) pada saat proses pembuatan. Alamat MAC, atau alamat perangkat keras adalah sebuah alamat 48 bit yang ditulis dalam format heksadesimal, di mana 24 bit pertama disebut alamat OUI (*Organizationally Unique Identifier*) yang ditetapkan oleh IEEE (*Institute of Electrical and Eectronics Engineers*) untuk menandakan sebuah organisasi (dalam hal ini yaitu organisasi atau *vendor* yang membuat kartu jaringan), sedangkan sisanya adalah nomor seri dari kartu jaringan yang dibuat.

2.20 *Mapping* (Pemetaan) Alamat IP dan MAC

Pada komunikasi menggunakan pengalamatan IP *multicast*, terdapat 23 bit dari alamat IP yang diambil untuk dipetakan menjadi alamat MAC. Sedangkan dari 9 bit sisanya, 4 bit sudah digunakan untuk menunjukkan alamat kelas D yaitu 1110 sehingga terdapat sisa 5 bit lagi yang tidak digunakan untuk pemetaan. Berapapun nilai dari kelima bit ini, alamat *ethernet* untuk *multicast* adalah sama, sehingga ada kemungkinan 32 alamat IP (hasil dari 2^5) memiliki alamat *ethernet* yang sama.

2.21 Pengalamatan IP Multicast

Dalam penerapan multicast, terdapat beberapa protokol yang juga menggunakan jangkauan alamat IP kelas D ini seperti yang sudah ditentukan oleh IANA (*Internet Assigned Numbers Authority*) dan disebut *well-known address*. Berikut ini adalah tabel yang berisi daftar alamat IP multicast yang memiliki fungsi khusus.

Tabel 2.2 Daftar IP Multicast dengan Fungsi Khusus

Alamat IP	Identifikasi
224.0.0.1	Semua Host dalam Subnet
224.0.0.2	Semua Route dalam Subnet
224.0.0.4	DVMRP Router
224.0.0.5	OSPF Router
224.0.0.6	OSPF designated Router
224.0.0.9	RIPv2 Router
224.0.0.10	IGRP Router
224.0.0.13	PIM Router

Alamat 224.0.0.1 adalah alamat *multicast* untuk grup yang terdiri dari semua *host*. Ketika metode *multicast* diaktifkan pertama kali, setiap *host* yang berada dalam jaringan tersebut harus bergabung dalam alamat ini. Semua *host* yang mendukung *multicast* akan membalas *ping* yang ditujukan untuk alamat ini. Sedangkan alamat 224.0.0.2 adalah alamat *multicast* untuk semua *router multicast* di dalam jaringan.

Alamat IP *multicast* dengan jangkauan mulai dari 224.0.0.0 sampai dengan 224.0.0.255 digunakan untuk administrasi dan *maintenance*. Semua router yang mendukung dan mengaktifkan *multicast* tidak akan meneruskan paket yang ditujukan untuk jangkauan alamat ini.

Alamat IP yang dimulai dari 239.0.0.0 sampai dengan 239.255.255.255 digunakan untuk *administrative scoping*; yang mengizinkan pengaturan dari sebuah batasan dengan menentukan jangkauan alamat *multicast* yang tidak akan dikirimkan baik yang masuk maupun yang keluar. Alamat ini bersifat lokal sehingga tidak harus unik dalam jaringan.

2.22 IP Multicast Protocol

Untuk mendukung implementasi IP *multicast routing*, Cisco IOS mendukung protokol-protokol berikut:

- *Internet Group Management Protocol* (IGMP)

  Protokol ini digunakan oleh *host-host* dalam sebuah LAN dan router yang berada dalam LAN tersebut untuk mengidentifikasi grup *multicast* yang digunakan oleh pengguna.

- *Protocol Independent Multicast* (PIM)

  Protokol PIM digunakan antar router agar mereka dapat menentukan paket *multicast* yang harus dikirimkan ke setiap router-router tersebut dan ke LAN yang terhubung langsung dengan mereka.

- *Distance Vector Multicast Routing Protocol* (DVMRP)

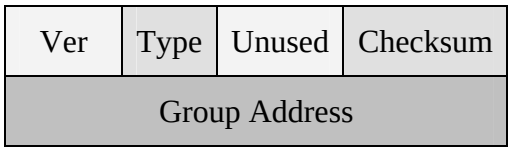
  Protokol ini biasanya digunakan pada jaringan MBONE (*multicast backbone*) di internet.

- *Cisco Group Management Protocol* (CGMP)

  Protokol CGMP digunakan pada router yang terhubung dengan switch *Catalyst* untuk melakukan tugas yang mirip dengan IGMP.

2.22.1 IGMP v.1

IGMP digunakan pada *host-host* untuk memberitahukan router yang terhubung langsung grup *multicast* mana yang mereka pilih. Gambar berikut ini adalah format pesan IGMP.



Gambar 2.8 Format Pesan IGMP v.1

Spesifikasi mengenai IGMP versi 1 ini didefinisikan oleh RFC 1112. IGMP dienkapsulasi di dalam datagram IP dan diberi nilai *protocol identifier* 2. Berikut ini adalah penjabaran format pesan IGMP yang terdapat pada gambar 2.8 di atas.

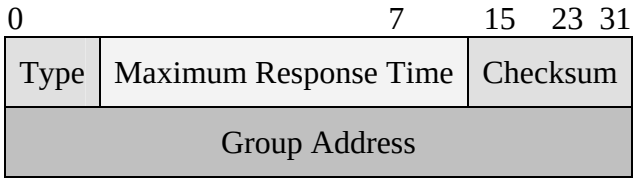
- *Ver field* menunjukkan versi dari IGMP yang digunakan. *Field* ini dapat berisi versi IGMP 1, 2, atau 3.

- *Type field* bernilai 1 jika tipe dari pesan IGMP yang dikirim ini adalah *Host Membership Query* dan 2 jika pesan IGMP yang dikirim ini adalah *Host Membership Report*.
- *Unused field* bernilai nol ketika dikirimkan, dan ketika diterima akan diabaikan.
- *Checksum* adalah 16 bit *1's complement* dari *1's complement sum* dari 8 *octet* pesan IGMP. Untuk proses penghitungan checksum, *field* ini akan diberi nilai nol.
- *Group Address*; jika pesan IGMP merupakan *Host Membership Query*, maka nilai dari *Group Address* ini adalah nol dan diabaikan ketika diterima. Ketika pesan IGMP merupakan *Host Membership Report*, maka berisi alamat IP *multicast* dari grup yang dilaporkan.

Host mengirimkan IGMP *Membership Report* berisi alamat IP *multicast* dari grup ketika mereka ingin menjadi anggota dari grup tersebut. Secara periodik router akan mengirimkan IGMP *Membership Query* ke alamat grup semua *host* (224.0.0.1) untuk memastikan paling tidak ada satu *host* yang masih menerima paket data yang dikirimkan ke alamat grup IP *multicast* tersebut. Jika tidak ada *reply* terhadap IGMP *Membership Query* selama pengiriman tiga kali berturut-turut maka router akan menghentikan pengiriman paket ke alamat tersebut.

2.22.2 IGMP v.2

Perincian mengenai IGMP versi 2 terdapat dalam RFC 2236. Adapun format dari IGMP versi 2 dapat dilihat pada gambar di bawah ini.



Gambar 2.9 Format Pesan IGMP v.2

Berikut ini adalah penjabaran format pesan IGMP v.2 yang terdapat pada gambar 2.9 di atas.

- Type field berisi jenis pesan IGMP versi 2. Adapun jenis pesan ini terdiri dari 4 jenis pesan, yaitu sebagai berikut:
  - *IGMP Membership Query*

    IGMP Membership Query ditandai dengan nilai 0x11.
  - *IGMP Version 2 Membership Report*

    Jenis pesan ini ditandai dengan nilai 0x16.
  - *Leave Group Report*

    Jenis pesan ini ditandai dengan nilai 0x17
  - *IGMP Version 1 Membership Report*

    Jenis pesan ini ditandai dengan nilai 0x12. Tujuan dari jenis pesan ini adalah untuk memberikan kompatibilitas dengan IGMP versi 1. Dengan demikian, IGMP versi 1 dan IGMP versi 2 dapat saling *compatible*.
- *Maximum Response Time Field*

  Pada IGMP versi 2 terdapat *field* tambahan yang berisi *Maximum Response Time*. *Field* ini berguna untuk menentukan waktu yang diberikan untuk *query* sebelum mengirimkan *membership report*. Nilai *default* pada *field* ini untuk

jenis pesan *membership query* adalah 10 detik, dan *field* ini bernilai nol untuk jenis pesan lain.

- *Checksum* digunakan untuk fungsi deteksi dan perbaikan kesalahan. Sebelum proses perhitungan dilakukan, *field checksum* diberi nilai inisial nol. Jika nilai *checksum* tidak benar, maka pesan *error* dikirim dan data diabaikan.

IGMP versi 2 bekerja hampir sama dengan IGMP versi 1. Perbedaan utama adalah adanya jenis pesan IGMP *leave group report* yang dikirimkan ke semua router dalam subnet (alamat 224.0.0.2). IGMP versi 1 tidak menyediakan mekanisme bagi *host* untuk memberitahukan kepada router terdekatnya bahwa *host* tersebut akan meninggalkan suatu grup (tidak lagi menjadi anggota dari suatu grup). Dengan IGMP versi 2, *host* dapat secara aktif memberitahukan kepada router terdekat mereka yang mengaktifkan *multicast* bahwa mereka akan meninggalkan atau tidak lagi menjadi anggota dari suatu grup multicast. Router tersebut kemudian akan mengirimkan *Group-Spesific Query* yang digunakan untuk menentukan apakah sebuah alamat grup *multicast* masih mempunyai anggota yang aktif. Jika tidak ada balasan (*reply*), maka router akan menganggap grup tersebut telah habis waktunya (*time out*) dan berhenti mengirimkan paket ke alamat tersebut. Hal ini bertujuan untuk mengurangi *latency* yang ditimbulkan pada mekanisme IGMP versi 1 untuk menentukan apakah suatu grup *multicast* masih memiliki anggota yang aktif atau tidak.

Perbedaan lain antara IGMP v.2 dengan IGMP v.1 adalah terdapatnya mekanisme pemilihan router yang akan menjadi *Querier Router* pada IGMP versi 2. Kondisi yang memerlukan mekanisme ini adalah bila ada lebih dari satu router pada suatu jaringan LAN. Router yang akan terpilih sebagai *Querier Router* yang

mengirimkan *Membership Query* adalah router yang mempunyai alamat IP yang paling rendah.

2.22.3 CGMP dan IGMP *Snooping*

Karakteristik dari sebuah switch adalah meneruskan paket *multicast* ke setiap port yang menjadi milik dari LAN tujuan. Hal ini berbeda dengan peran switch sesungguhnya yaitu membatasi lalu-lintas jaringan hanya ke port yang memerlukan data (Internetworking Technologies Handbook, chapter 43, p6). Dua buah metode yang dikembangkan untuk menangani masalah ini pada lingkungan *layer* 2 adalah sebagai berikut:

- ***Cisco Group Management Protocol* (CGMP)**

  CGMP adalah protokol yang dikembangkan oleh Cisco yang memungkinkan switch Cisco Catalyst dapat menggunakan informasi IGMP pada router untuk membuat keputusan *forwarding* layer 2. Untuk mengaktifkan CGMP, protokol ini harus diaktifkan baik pada router maupun pada switch. Hasilnya adalah paket *multicast* hanya akan dikirimkan ke port-port milik client yang tergabung dalam grup *multicast*. Cara kerja secara singkat adalah ketika sebuah client hendak menjadi anggota dari sebuah grup atau meninggalkan grup, maka client tersebut akan mengirimkan IGMP *membership report* kepada router. Kemudian router akan membuat sebuah pesan CGMP berisi informasi mengenai client-client yang tergabung atau meninggalkan sebuah grup kepada switch. Informasi tersebut akan dicatat oleh switch untuk digunakan pada keputusan *forwarding*nya.

- **IGMP *Snooping***

  IGMP *Snooping* bekerja dengan cara melakukan pemeriksaan terhadap paket-paket data IGMP yang dikirimkan client kepada router sebelum paket sampai di router. Dengan menggunakan informasi tersebut, switch dapat menentukan client mana yang terletak pada suatu port yang hendak menjadi anggota (*member*) ataupun hendak meninggalkan grup tersebut. Karena paket-paket data IGMP dikirimkan sebagai paket *multicast*, maka switch harus memeriksa seluruh paket multicast tersebut, sehingga untuk *low-end* switch dengan kemampuan CPU yang rendah, tidak disarankan untuk menggunakan IGMP *Snooping*.

2.22.4 PIM (Protocol Independent Multicast)

Protokol IP *multicast routing* yang didukung oleh Cisco IOS adalah PIM (Protocol Independent Multicast). Protokol IP *multicast routing* bertugas menemukan grup multicast dan membangun jalur untuk setiap grup tersebut menggunakan *distribution tree*. Jadi lingkup dari protokol IP *multicast routing* adalah distribusi lalu-lintas (*traffic*) antarrouter yang mendukung *multicast*.

Ciri utama dari PIM adalah *protocol-independent*, artinya protokol PIM dapat menggunakan protokol *unicast routing* apapun, termasuk EIGRP, OSPF, BGP; atau bahkan *static route* untuk melakukan fungsi *multicast forwarding*. PIM tidak mengirim dan menerima *multicast routing update* dari router lain seperti yang umumnya dilakukan oleh protokol-protokol *routing* lainnya.

Berikut ini adalah dua jenis pendekatan dasar dalam protokol IP *multicast routing* yang didasarkan pada penyebaran anggota *multicast* di dalam jaringan (Cisco IOS IP Configuration Guide, p402).

- *Dense Mode*

  Pendekatan ini dilakukan berdasarkan asumsi bahwa hampir semua router di dalam jaringan akan meneruskan paket multicast untuk setiap grup multicast. Jika sebuah router menerima paket multicast, dan tidak memiliki anggota grup multicast yang terhubung secara langsung atau tidak memiliki "router tetangga" yang menjalankan protokol PIM, maka pesan *prune* akan dikirimkan ke pengirim. Pengiriman pesan *prune* ini berarti tidak ada paket *multicast* yang akan dikirimkan ke "cabang" tersebut.

- *Sparse Mode*

  Pendekatan ini dilakukan berdasarkan asumsi bahwa router-router tidak akan mengirimkan paket *multicast*, kecuali terdapat permintaan terhadap paket tersebut. Pendekatan ini juga berasumsi bahwa pengirim paket *multicast* dan penerima paket *multicast* tidak berada pada daerah yang berdekatan. Hal ini bukan berarti *sparse mode* tidak dapat diterapkan pada lingkungan LAN, melainkan *mode* ini akan bekerja secara lebih efisien dalam lingkungan WAN.

2.22.4.1 PIM-DM (Protocol Independent Multicast - Dense Mode)

PIM-DM menggunakan model *push* untuk mengirimkan paket *multicast* ke setiap "ujung" dari jaringan. Penerapan konfigurasi PIM-DM akan menjadi efisien jika dalam setiap subnet dalam jaringan tersebut terdapat anggota *multicast.*

Pada awalnya protokol PIM-DM akan mengirimkan paket *multicast* ke semua *interface* dalam jaringan, di mana proses ini disebut *flooding*. Router-router yang tidak memiliki anggota di *interface*nya akan mengirimkan pesan *prune*. Proses ini akan berulang setiap 3 menit. Mekanisme *flood and prune* ini akan digunakan oleh router untuk membangun tabel *multicast forwarding* mereka.

2.22.4.2 PIM-SM (Protocol Independent Multicast - Sparse Mode)

Pada penerapan PIM dengan *sparse mode*, digunakan model *join* di mana paket *multicast* hanya akan diteruskan ke suatu *interface* jika *host* yang hendak menerima telah bergabung dalam grup atau terdapat permintaan terhadap paket tersebut. Dalam lingkungan ini, terdapat titik pusat (*central point*) yang digunakan oleh seluruh sumber pengirim dalam mengirimkan paketnya. Setiap pengirim paket melakukan proses pengiriman dengan memilih jalur terbaik ke *central point*. Kemudian *central point* mendistribusikan paket tersebut ke seluruh penerima yang tergabung dalam grup tujuan menggunakan jalur terbaik. Titik pusat ini disebut *Rendezvous Point* (RP). Dalam sebuah jaringan, bisa terdapat lebih dari satu RP, namun hanya ada satu RP untuk satu grup *multicast* (William R. Parkhurst, 1999, p150).

Auto-RP adalah fitur yang melakukan pemetaan grup ke RP secara otomatis. Fitur ini memiliki beberapa keuntungan sebagai berikut:

- Kemudahan dalam penggunaan lebih dari satu RP untuk melayani lebih dari satu grup,

- Memudahkan pembagian beban (load) antar-RP dan penyusunan RP berdasarkan lokasi dari anggota grup, dan
- Menghindari konfigurasi RP secara manual yang dapat menyebabkan masalah konektivitas.

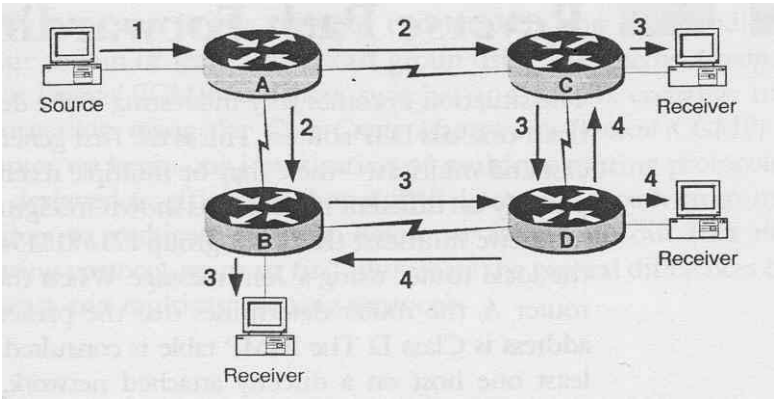
Untuk menjalankan Auto-RP, sebuah router harus menjadi RP-*mapping agent*, yang menerima pemberitahuan dari RP. Lalu *agent* ini akan mengirimkan hasil pemetaan grup-ke-RP yang konsisten ke router-router lain. Kemudian router akan secara otomatis menemukan RP mana yang digunakan untuk grup yang mereka tangani.

2.22.4.3 Sparse-Dense Mode

Cisco telah mengimplementasikan salah satu alternatif dari pemilihan penggunaan *sparse mode* atau *dense mode*. Pemilihan *mode* akan lebih efisien jika pemilihan mode tersebut dilakukan berdasarkan per-grup, bukan per-*interface*. Kemampuan ini difasilitasi dengan adanya konfigurasi *sparse-dense mode*. Penerapan konfigurasi ini memungkinkan sebuah grup dapat mengikuti *mode sparse* atau *dense* bergantung pada eksistensi *rendezvous point* dalam jaringan. Jika dalam suatu jaringan terdapat sebuah RP maka *mode* yang digunakan adalah *sparse mode*. Sebaliknya, jika dalam suatu jaringan tidak terdapat RP, maka *mode* yang digunakan adalah *dense mode.*

2.22.5 RPF (Reverse Path Forwarding)

Untuk menentukan jalur terbaik antara sumber pengirim dengan penerima dan menghindari terjadinya *multicast routing loop*, diperlukan sebuah mekanisme yang dapat menentukan *interface* yang akan digunakan untuk mengirimkan paket *multicast*. Mekanisme yang dimaksud adalah RPF (*Reverse Path Forward-ing*). Contoh keadaan yang memungkinkan terjadinya *routing loop* adalah bila dalam sebuah jaringan terdapat empat buah router (A, B, C, dan D), di mana masing-masing router memiliki jaringan LANnya sendiri. Dalam jaringan tersebut, router A terhubung dengan router B dan router C; router B terhubung dengan router D; dan router C juga terhubung dengan router D, sehingga topologi tersebut membentuk kondisi yang *loop*. Gambar jaringan ini dapat dilihat pada gambar 2.10 berikut.



Sumber: Parkhurst, William R., Ph.D., CCIE #2969, *Cisco Multicast Routing & Switching*.

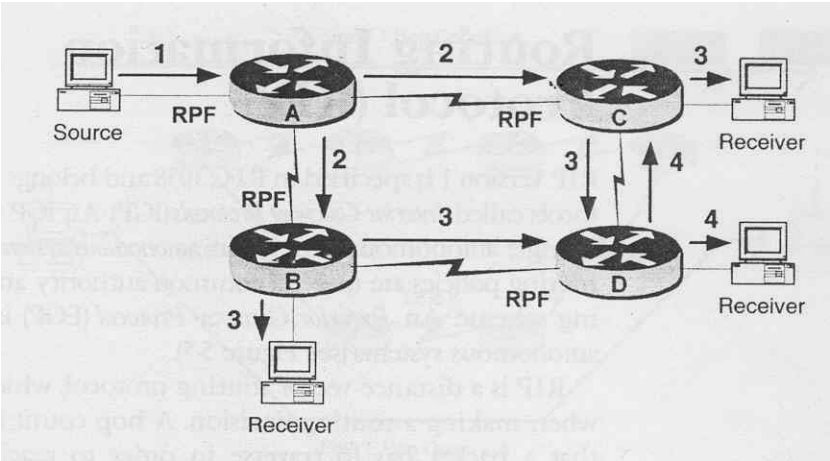
Gambar 2.10 Gambar Jaringan Tanpa RPF Diaktifkan

Cara kerja paket multicast dengan topologi di atas adalah bila ada sumber pada jaringan LAN A yang mengirimkan paket *multicast*, router A kemudian mengirimkan paket tersebut ke router B dan router C. Router B dan C kemudian

juga mengirimkan paket tersebut ke jaringan LANnya masing-masing dan ke router D. Router D juga mengirimkan paket tersebut ke jaringannya sendiri dan mengirimkannya kembali ke router B dan C. Kemudian hal yang sama terjadi berulang-ulang hingga paket tersebut mencapai masa habisnya dan di*drop*.

Penerapan RPF memungkinkan setiap router untuk menentukan *interface* mana yang memiliki jalur yang terbaik ke router-router sebelahnya maupun ke sumber. Pada penerapan ini, bila paket multicast tidak diterima dari RPF *interface*, maka paket tersebut akan di*drop*. Berikut ini adalah contoh penerapan RPF pada contoh sebelumnya (Gambar 2.10).

Sebuah client dalam jaringan LAN A mengirimkan paket multicast. Router A akan melakukan pemeriksaan apakah paket multicast tersebut diterima oleh RPF *interface*nya. Jika paket ini diterima oleh RPF *interface*nya, router A kemudian mengirimkan paket tersebut ke semua *interface* kecuali ke *interface* di mana paket multicast diterima. Kemudian router B dan router C menerima paket multicast tersebut di RPF *interface* mereka, sehingga kedua router tersebut meneruskan paket tersebut ke semua *interface* kecuali pada *interface* di mana paket diterima. Lalu router D menerima dua paket *multicast* dari router B dan router C. Namun hanya paket yang masuk melalui RPF *interface* router D saja yang diterima. Router D kemudian meneruskan paket tersebut ke jaringan LAN-nya dan ke router C. Router C yang menerima paket ini tidak meneruskan paket tersebut karena tidak diterima dari RPF *interface*nya. Gambar berikut menunjukkan proses yang terjadi pada contoh ini.



Sumber: Parkhurst, William R., Ph.D., CCIE #2969, *Cisco Multicast Routing & Switching*.

Gambar 2.11 Gambar Jaringan dengan RPF Diaktifkan

2.22.6 DVMRP (Distance Vector Multicast Routing Protocol)

Beberapa versi dari DVMRP digunakan untuk router *multicast backbone* (MBONE). DVMRP bekerja berdasarkan *reverse path flooding*. Ketika router yang menjalankan DVMRP menerima sebuah paket, router tersebut akan meneruskannya ke semua jalur kecuali jalur yang mengarah kembali ke sumber. Hal ini menunjukkan sebuah paket dapat mencapai semua LAN di dalam jaringan. Tapi terdapat beberapa LAN yang tidak mempunyai anggota dari grup yang menjadi tujuan dari paket yang diteruskan oleh router tersebut. Bila tidak ada penerima, maka pesan *prune* dikirimkan ke sumber untuk mencegah pengiriman kembali ke *interface* tersebut. DVMRP menggunakan *unicast routing protocol* miliknya sendiri untuk menentukan jalur agar paket dapat kembali ke sumber pengirim. Protokol ini mirip dengan *Routing Information Protocol* (RIP), yang melakukan pemilihan jalur terbaik berdasarkan *hop count*.

Untuk menentukan apakah terdapat penerima yang hendak bergabung dengan sebuah grup *multicast*, maka router DVMRP secara periodik akan

mengirinkan pesan ke semua jaringan. Akibat dari pengiriman pesan ini adalah DVMRP tidak mampu beradaptasi dengan topologi jaringan yang sangat besar dengan lokasi penerima yang saling berjauhan. Hal ini disebabkan karena DVMRP mengandalkan *flooding* untuk menentukan keanggotaan dari sebuah grup mutlicast. Router Cisco tidak mendukung protokol DVMRP, namun dapat bekerja sama dengan router-router yang mengaktifkan DVMRP.

2.23 Perangkat Keras Pendukung Kemampuan Multicast

Dalam melakukan penerapan metode multicast pada suatu jaringan, seorang perancang jaringan harus terlebih dahulu memastikan seluruh perangkat dalam jaringan tersebut mendukung kemampuan multicast. Berikut ini adalah beberapa contoh sistem dan perangkat jaringan yang mendukung kemampuan multicast (*multicast-capable*).

- Cisco Systems

  Sistem IOS untuk router Cisco dengan versi 10.2 ke atas yang dikeluarkan Cisco dalam tahun-tahun terakhir ini sudah mendukung kemampuan multicast. Untuk menerapkan routing IP multicast, Cisco IOS mendukung beberapa protokol berikut.

  - IGMP
  - PIM
  - Dukungan PIM-to-DVMRP.

    Walaupun Cisco IOS tidak mendukung DVMRP, Cisco IOS memberikan dukungan interaksi dengan router-router lain yang menggunakan protokol DVMRP.

- CGMP

- Juniper Networks

  Seluruh produk E-series dari Juniper sudah mendukung kemampuan multicast. Berikut ini adalah beberapa dukungan multicast yang diberikan seluruh produk Juniper Networks E-series.

  - Dukungan penuh router untuk melakukan multicast berbasis IPv4 dan IPv6.
  - Dukungan terhadap protokol PIM dan MBGP.
  - Dukungan proxy untuk lalu-lintas IGMPv2 dan IGMPv3 (untuk IPv4); dan lalu-lintas MLDv1 dan MLDv2 (untuk IPv6).
  - Pengaturan QoS dinamis berdasarkan pemrosesan IGMP *join*/*leave*.
  - IGMP *accounting*.
  - Kendali *multicast call admission*.
  - Protokol Layer 2 Control (L2C).

- D-Link

  Berikut ini adalah beberapa contoh perangkat D-Link yang mendukung kemampuan multicast, yaitu:

  - D-Link DES-3350SR

    D-Link DES-3350SR adalah switch layer 3 10/100BASE-T yang memberikan dukungan terhadap pengiriman multicast *content*, seperti IP Video.

- D-Link DFE-550TX

  D-Link DFE-550TX adalah PCI NIC yang memberikan dukungan IP Multicast *Packet Filtering*. Perangkat ini memungkinkan dilakukannya pengiriman dan penerimaan data secara multicast.

2.24 Wireless LAN (WLAN)

Wireless LAN adalah metode menghubungan dua atau lebih komputer menjadi satu jaringan, tanpa menggunakan kabel. *WLAN* menggunakan teknologi *spread-spectrum* berdasarkan pada gelombang radio untuk melakukan komunikasi antar*devic*e pada ruang yang terbatas. *WLAN* mengizinkan pengguna melakukan aktivitas mobilitas dalam jangkauan area nirkabel. Tabel berikut ini menunjukkan standar-standar IEEE 802.11x yang digunakan *WLAN*.

Tabel 2.3 Perbandingan Standar IEEE 802.11x

Protocol	Release Date	Frequency	Data Rate (Typical)	Data Rate (Max)
Legacy	1997	2.4-2.5 GHz	1 Mbit/s	2 Mbit/s
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s
802.11n	2006(draft) 2007(Linksys)	2.4 GHz or 5 GHz bands	200 Mbit/s	540 Mbit/s

Berikut ini adalah beberapa faktor yang harus diperhatikan pada jaringan nirkabel supaya koneksi dapat terjaga dengan baik.

- ***Link Budget***

  Link Budget dipengaruhi oleh daya pancar yang cukup, sensitivitas penerima, *fade margin*, dan penguatan antena yang cukup.

- ***Line of Sight***

  Dua jenis LOS yang biasanya harus diperhatikan pada transmisi data antara *Access Point* dengan client pada jaringan nirkabel (Onno W. Purbo, 2006, p54):

  - ***Optical* LOS**

    Berhubungan dengan kemampuan masing-masing perangkat untuk melihat.

  - ***Radio* LOS**

    Berhubungan dengan kemampuan penerima radio untuk "melihat" sinyal dari pemancar radio.

- ***Fresnel Zone***

  Daerah yang cukup bebas tanpa halangan.

- **Instalasi**

  Dalam melakukan instalasi awal, antena harus dipasang dengan benar dan arahnya benar.

2.25 VLC Media Player

VLC Media Player adalah aplikasi yang digunakan sebagai *encoder*, *server*, dan juga sebagai aplikasi pada *client*. VLC bisa digunakan untuk

menjalankan berbagai macam *file* multimedia dan juga untuk melakukan *video streaming*.

2.26 Iperf

Iperf adalah aplikasi yang berfungsi untuk melakukan pengukuran terhadap kualitas jaringan, serta mengukur efektivitas dan efisiensi *bandwith* pada jaringan dengan menggunakan protokol TCP maupun UDP. Aplikasi ini dapat juga digunakan untuk mengukur efektivitas dan efisiensi metode transmisi, baik transmisi *unicast* maupun transmisi *multicast*.

2.27 IPTV

IPTV (*Internet Protocol Television*) adalah sebuah sistem di mana sebuah layanan televisi digital dikirimkan menggunakan *Internet Protocol* (IP) melewati sebuah infrastruktur jaringan, di mana bisa termasuk pengiriman oleh koneksi *broadband*. Untuk pengguna di daerah perumahan, IPTV sering disediakan bersama dengan *Video on Demand* dan bisa juga digabungkan dengan layanan internet, seperti akses web dan VoIP.

Salah satu keterbatasan IPTV disebabkan karena IPTV berbasis *Internet Protocol*, di mana hal ini menyebabkan pengiriman IPTV sangat dipengaruhi oleh *packet lost* dan *delay* jika koneksi IPTV tidak terlalu cepat. Oleh karena itu, dibutuhkan media yang dapat memberikan kecepatan pengiriman yang tinggi untuk menyediakan layanan IPTV yang berkualitas. Dengan kata lain, pengiriman IPTV sangat dipengaruhi oleh besar kapasitas bandwidth yang tersedia pada jaringan.

Salah satu penyedia perangkat jaringan yang saat ini juga menyediakan layanan IPTV adalah Cisco Systems. Cisco menggabungkan dua teknologi jaringan untuk memungkinkan layanan TV berbasis internet kepada jutaan client. Dua buah teknologi ini adalah IP Multicast dan IPTV.

Cisco IP/TV adalah aplikasi client-server yang dikeluarkan Cisco untuk mendukung layanan IPTV. Aplikasi ini menggunakan IP Multicast untuk mengirimkan program-program TV berkualitas melewati jaringan data ke PC client. Dengan Cisco IP/TV, pengguna yang terhubung ke dalam jaringan bisa menerima tayangan TV bisnis, program pelatihan, kelas kuliah, dan program-program lain di komputer mereka.

Dengan penerapan IP Multicast pada Cisco IP/TV memungkinkan pengiriman TV berkualitas dengan kecepatan tinggi secara bersamaan kepada jutaan pengguna. Hal ini disebabkan karena pengiriman secara multicast hanya melibatkan pengiriman sebuah *stream* ke seluruh client yang tergabung dalam suatu grup. Dari penerapan ini akan diperoleh *delay* pengiriman yang kecil, layanan IPTV yang berkualitas tinggi, dan penghematan penggunaan bandwidth jaringan walaupun diakses oleh jutaan pengguna secara bersamaan.