Pengantar MPLS

Kuncoro Wastuwibowo
http://kun.co.ro

Abstrak:

Riset dan inovasi dalam teknologi telekomunikasi dikembangkan atas dorongan kebutuhan mewujudkan jaringan informasi yang (1) menyediakan layanan yang beraneka ragam (2) memiliki kapasitas tinggi sesuai kebutuhan yang berkembang (3) mudah diakses dari mana dan kapan saja serta (4) terjangkau harganya. Network yang memenuhi kebutuhan itu adalah *broadband network* yang menghantarkan data paket dengan secara efisien, *scalable*, memungkinkan diferensiasi dalam satu sistem, serta mampu diakses secara *mobile*.

Teknologi semacam ATM memiliki mekanisme pemeliharaan QoS, dan memungkinkan diferensiasi, namun menghadapi masalah pada skalabilitas yang mengakibatkan perlunya investasi tinggi untuk implementasinya. Di lain pihak, Internet yang dengan protokol IP berkembang lebih cepat. IP sangat baik dari segi skalabilitas, yang membuat teknologi Internet menjadi cukup murah. Namun IP memiliki kelemahan serius pada implementasi QoS. Namun kemudian dikembangkan beberapa metode untuk memperbaiki kinerja jaringan IP, antara lain dengan MPLS.

MPLS merupakan salah satu bentuk konvergensi vertikal dalam topologi jaringan. MPLS menjanjikan banyak harapan untuk peningkatan performansi jaringan paket tanpa harus menjadi rumit seperti ATM. Pada perkembangannya, metode MPLS juga membangkitkan gagasan mengubah paradigma routing di layer-layer jaringan yang ada selama ini, dan mengkonvergensikannya ke dalam sebuah metode, yang dinamai GMPLS.

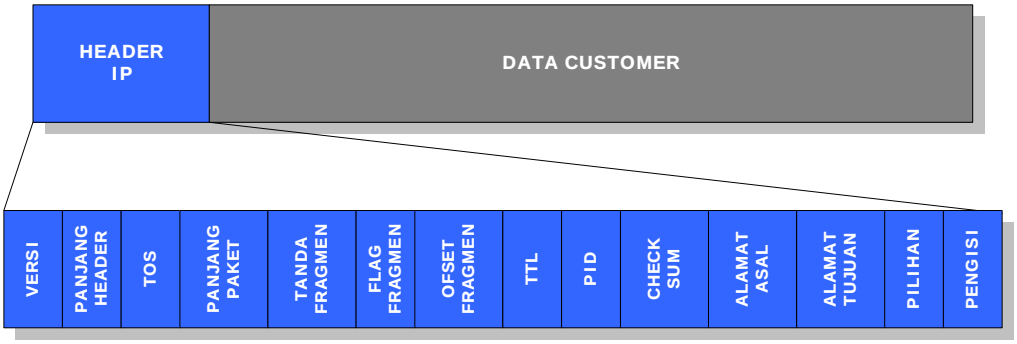
Keywords: mpls, ip, broadband network, qos, traffic engineering, gmpls

1. IP Network

1.1. Paket IP

IP adalah standar *de facto* dalam komunikasi komputer bersistem unix, yang kemudian menjadi standar komunikasi global. Buku [Hall 2000] banyak mendalami network IP dan protokol-protokol utama di dalamnya. Protokol-protokol dalam *suite* IP didefinisikan dalam RFC-RFC yang diterbitkan oleh IETF. IP sendiri dijelaskan dalam RFC-791. RFC-791 menyatakan bahwa IP dirancang sebagai sistem interkoneksi jaringan paket.

Paket adalah blok data yang dilengkapi dengan informasi alamat yang diperlukan untuk penghantaran data itu. Setiap paket dihantarkan secara terpisah tanpa saling berhubungan. Datagram adalah format paket data yang didefinisikan dalam IP, terdiri atas header dan data. Header mengandung informasi alamat dan fungsi kontrol lainnya.



1.2. *Routing* IP

IP menghantarkan paket dengan memeriksa alamat tujuan di header. Jika alamat tujuan masih merupakan bagian dalam sebuah network, paket dihantarkan langsung ke *host* tujuan. Jika alamat tujuan bukan merupakan bagian internal network, paket dikirimkan ke network lain dengan mekanisme yang disebut *routing*. Perangkat untuk memilih, mengirim, dan menerima paket IP antar network disebut *router*.

IP melakukan pemilihan routing untuk setiap paket. Tidak ada pertukaran informasi kontrol (handshake) untuk membentuk hubungan dari ujung ke ujung sebelum transmisi data. Karenanya, IP disebut protokol tanpa koneksi (connectionless). IP mengandalkan protokol di layer lain untuk keperluan itu, dan juga keperluan seperti pemeriksaan dan perbaikan kesalahan.

Dalam proses routing IP, tidak terdapat mekanisme pemeliharaan QoS. Protokol yang sering digunakan di atas IP, yaitu TCP, memiliki feature yang memungkinkan jaminan validitas data. Namun TCP tidak bersifat universal, karena memiliki banyak kelemahan untuk diaplikasikan pada paket suara atau multimedia. Dengan mulai digunakannya IP sebagai infrastruktur informasi global, mulai digagas berbagai cara untuk mewujudkan jaringan IP dengan QoS

1.3. Protokol di Atas IP

Saat sebuah datagram diterima di sebuah *host*, data dialihkan ke protokol di atas IP. Pemilihan protokol ini berdasar field identifikasi paket (PIDD) di header paket. Setiap protokol memiliki angka

yang unik dan baku. Misalnya PIDD 6 menunjukkan TCP, 17 untuk UDP, dan 1 untuk ICMP.

ICMP (*Internet Control Message Protocol*, RFC-792) adalah protokol yang bertugas menyampaikan pesan-pesan pengendalian penghantaran paket, seperti kontrol dan pelaporan kesalahan. Pesan-pesan ICMP meliputi juga deteksi alamat yang tak dapat dijangkau, pengubahan arah *routing*, dan pemeriksaan *host* jarak jauh.

TCP (*Transmission Control Protocol*, RFC-793) menghantarkan paket dari *host* ke *host* dengan jaminan validitas data. Jika terjadi kesalahan, TCP memiliki mekanisme meminta pengiriman ulang. TCP juga memungkinkan host mengelola banyak sambungan sekaligus. TCP sangat populer dalam transformasi data yang membentuk dunia Internet, sehingga diistilahkan bahwa Internet dibangun dengan *suite TCP/IP*.

Jika koreksi validitas data tidak diperlukan, protokol UDP dapat dipakai. UDP (*User Datagram Protocol*, RFC-768) lebih sederhana dan lebih cepat dari TCP, tetapi nyaris tidak memberikan pengendalian data dalam bentuk apa pun. UDP umumnya dipakai untuk transfer data yang memerlukan kecepatan tetapi kurang peka pada kesalahan, seperti transfer suara dan video.

2. QoS pada IP Network

2.1. Konsep QoS

QoS adalah hasil kolektif dari berbagai kriteria performansi yang menentukan tingkat kepuasan penggunaan suatu layanan. Umumnya QoS dikaji dalam kerangka pengoptimalan kapasitas network untuk berbagai jenis layanan, tanpa terus menerus menambah dimensi network.

Berbagai aplikasi memiliki jenis kebutuhan yang berbeda. Misalnya transaksi data bersifat sensitif terhadap distorsi tetapi kurang sensitif terhadap delay. Sebaliknya, komunikasi suara bersifat sensitif terhadap tundaan dan kurang sensitif terhadap kesalahan. Tabel berikut [Dutta-Roy 2000] memaparkan tingkat kepekaan performansi yang berbeda untuk jenis layanan network yang berlainan.

LAYANAN	KEPEKAAN PERFORMANSI			
	BAND WIDTH	LOSS	DELAY	JITTER
Voice	Rendah	Medium	Tinggi	Tinggi
Transaksi Data	Rendah	Tinggi	Tinggi	Rendah
Email	Rendah	Tinggi	Rendah	Rendah
Browsing Biasa	Rendah	Medium	Medium	Rendah
Browsing Serius	Medium	Tinggi	Tinggi	Rendah
Transfer File	Tinggi	Medium	Rendah	Rendah
Video Conference	Rendah	Medium	Tinggi	Tinggi
Multicasting	Tinggi	Tinggi	Tinggi	Tinggi

IP tidak memiliki mekanisme pemeliharaan QoS. Protokol seperti TCP memang memungkinkan jaminan validitas data, sehingga suite TCP/IP selama ini dianggap cukup ideal bagi transfer data. Tetapi verifikasi data mengakibatkan tundaan hantaran paket. Lagipula mekanisme ini tidak dapat digunakan untuk paket dengan protocol UDP, seperti suara dan video.

Beberapa skema telah diajukan untuk mengelola QoS dalam network IP. Dua skema utama adalah *Integrated Services* (IntServ) dan *Differentiated Services* (DiffServ). IntServ bertujuan menyediakan sumberdaya seperti bandwidth untuk trafik dari ujung ke ujung. Sementara DiffServ bertujuan membagi trafik atas kelas-kelas yang kemudian diberi perlakuan yang berbeda.

2.2. Integrated Service (IntServ)

IntServ (RFC-1633) terutama ditujukan untuk aplikasi yang peka terhadap tundaan dan keterbatasan bandwidth, seperti videoconference dan VoIP. Arsitekturnya berdasar sistem pencadangan sumberdaya per aliran trafik. Setiap aplikasi harus mengajukan permintaan bandwidth, baru kemudian melakukan transmisi data. Dua model layanan IntServ adalah:

- *Guaranteed-service* (RFC-2212), layanan dengan batas bandwidth dan delay yang jelas
- *Controlled-load service* (RFC-2211), yaitu layanan dengan persentase delay statistik yang terjaga

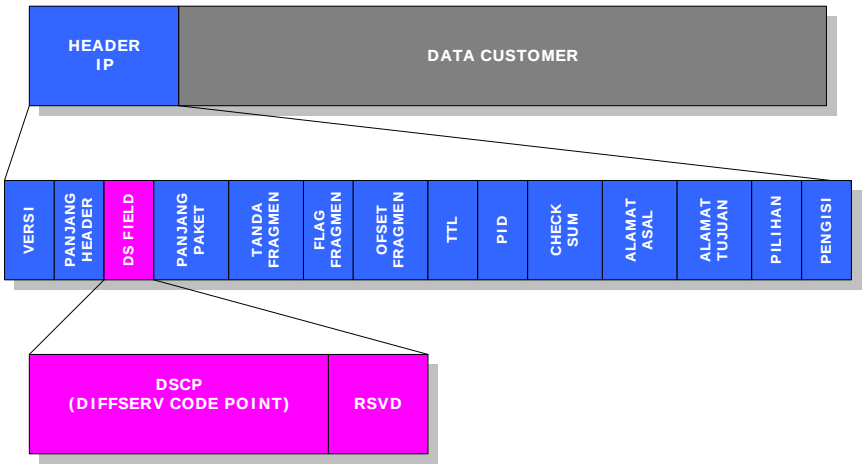
Layanan ketiga, yang paling jelek, adalah layanan *best-effort*, yang hanya memberikan routing terbaik, tetapi tanpa jaminan sama sekali.

Sistem pemesanan sumberdaya memerlukan protokol tersendiri. Salah satu protokol yang sering digunakan adalah RSVP (RFC-2205). Penggunaan RSVP untuk IntServ dijelaskan dalam RFC-2210.

Masalah dalam IntServ adalah skalabilitas (RFC-2998). Setiap node di network harus mengenali dan mengakui mekanisme ini. Juga protokol RSVP berlipat untuk setiap aliran trafik. Maka IntServ menjadi baik hanya untuk voice dan video, tetapi sangat tidak tepat untuk aplikasi semacam web yang aliran trafiknya banyak tapi datanya kecil.

2.3. Differentiated Service (DiffServ)

DiffServ (RFC-2475) menyediakan diferensiasi layanan, dengan membagi trafik atas kelas-kelas, dan memperlakukan setiap kelas secara berbeda. Identifikasi kelas dilakukan dengan memasang semacam kode DiffServ, disebut DiffServ code point (DSCP), ke dalam paket IP. Ini dilakukan tidak dengan header baru, tetapi dengan menggantikan field TOS (*type of service*) di header IP dengan DS field, seperti yang dispesifikasikan di RFC-2474. Dengan cara ini, klasifikasi paket melekat pada paket, dan bisa diakses tanpa perlu protokol persinyalan tambahan.



Jumlah kelas tergantung pada provider, dan bukan merupakan standar. Pada trafik lintas batas provider, diperlukan kontrak trafik yang menyebutkan pembagian kelas dan perlakuan yang diterima untuk setiap kelas. Jika suatu provider tidak mampu menangani DiffServ, maka paket ditransferkan apa adanya sebagai paket IP biasa, namun di provider berikutnya, DS field kembali diakui oleh provider. Jadi secara keseluruhan, paket-paket DiffServ tetap akan menerima perlakuan lebih baik.

DiffServ tidak memiliki masalah skalabilitas. Informasi DiffServ hanya sebatas jumlah kelas, tidak tergantung besarnya trafik (dibandingkan IntServ). Skema ini juga dapat diterapkan bertahap, tidak perlu sekaligus ke seluruh network.

2.4. Perbandingan IntServ dan DiffServ

Perbandingan IntServ dan DiffServ dipaparkan dalam tabel berikut [Dovrolis & Ramanathan 1999].

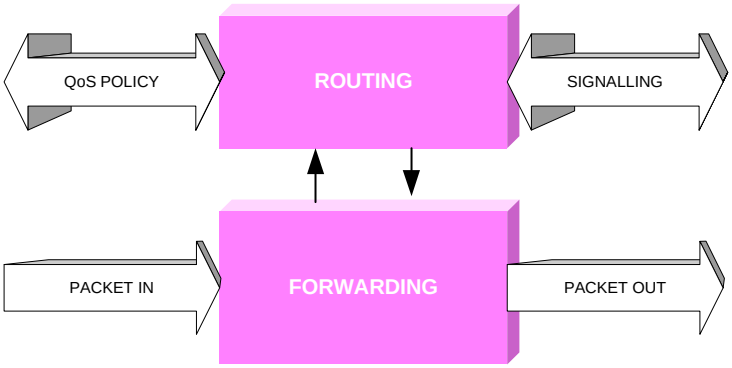
	INTSERV	DIFFSERV
Granularity of service differentiation	Individual flow	Aggregate of flows
Traffic classification basis	Deterministic or statistical guarantees	Absolute or relative assurances
Admission control	Required	Required for absolute differentiation only
Signalling protocol	Required (RSVP)	Not required for relative schemes
Coordination for service differentiation	End-to-end	Local (per-hop)
Scalability	Limited by the number of flows	Limited by the number of classes of service
Network management	Similar to circuit-switched networks	Similar to existing IP networks
Interdomain deployment	Multilateral agreements	Bilateral agreements

3. MPLS

3.1. Arsitektur MPLS

Teknologi ATM dan frame relay bersifat *connection-oriented*: setiap *virtual circuit* harus disetup dengan protokol persinyalan sebelum transmisi. IP bersifat *connectionless*: protokol *routing* menentukan arah pengiriman paket dengan bertukar info routing. MPLS mewakili konvergensi kedua pendekatan ini.

MPLS, *multi-protocol label switching*, adalah arsitektur network yang didefinisikan oleh IETF untuk memadukan mekanisme label swapping di layer 2 dengan routing di layer 3 untuk mempercepat pengiriman paket. Arsitektur MPLS dipaparkan dalam RFC-3031 [Rosen 2001].

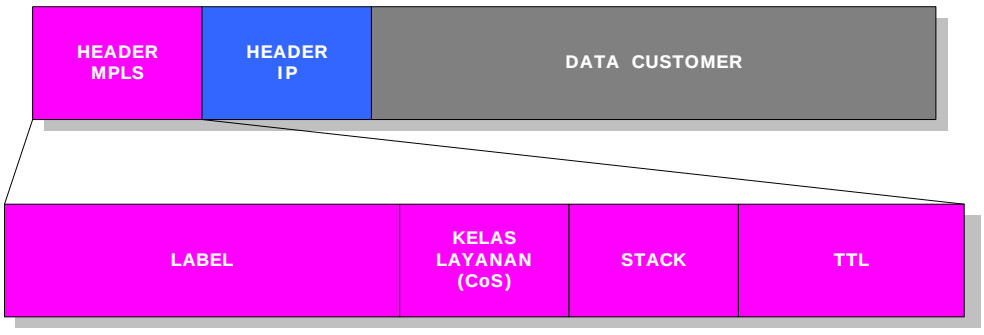


Network MPLS terdiri atas sirkit yang disebut *label-switched path* (LSP), yang menghubungkan titik-titik yang disebut *label-switched router* (LSR). LSR pertama dan terakhir disebut *ingress* dan *egress*. Setiap LSP dikaitkan dengan sebuah *forwarding equivalence class* (FEC), yang merupakan kumpulan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

3.2. Enkapsulasi Paket

Tidak seperti ATM yang memecah paket-paket IP, MPLS hanya melakukan enkapsulasi paket IP, dengan memasang header MPLS. Header MPLS terdiri atas 32 bit data, termasuk 20 bit label, 2 bit eksperimen, dan 1 bit identifikasi stack, serta 8 bit TTL. Label adalah bagian dari header, memiliki panjang yang bersifat tetap, dan merupakan satu-satunya tanda identifikasi paket. Label digunakan untuk proses forwarding, termasuk proses *traffic engineering*.



Setiap LSR memiliki tabel yang disebut *label-swiching table*. Tabel itu berisi pemetaan label masuk, label keluar, dan link ke LSR berikutnya. Saat LSR menerima paket, label paket akan dibaca, kemudian diganti dengan label keluar, lalu paket dikirimkan ke LSR berikutnya.

Selain paket IP, paket MPLS juga bisa dienkapsulasikan kembali dalam paket MPLS. Maka sebuah paket bisa memiliki beberapa header. Dan bit stack pada header menunjukkan apakah suatu header sudah terletak di 'dasar' tumpukan header MPLS itu.

3.3. Distribusi Label

Untuk menyusun LSP, *label-switching table* di setiap LSR harus dilengkapi dengan pemetaan dari setiap label masukan ke setiap label keluaran. Proses melengkapi tabel ini dilakukan dengan protokol distribusi label. Ini mirip dengan protokol persinyalan di ATM, sehingga sering juga disebut protokol persinyalan MPLS. Salah satu protokol ini adalah LDP (*Label Distribution Protocol*).

LDP hanya memiliki feature dasar dalam melakukan forwarding. Untuk meningkatkan kemampuan mengelola QoS dan rekayasa trafik, beberapa protokol distribusi label lain telah dirancang dan dikembangkan juga. Yang paling banyak disarankan adalah CR-LDP (*constraint-based routing LDP*) dan RSVP-TE (RSVP dengan ekstensi *Traffic Engineering*).

4. Rekayasa Trafik dengan MPLS

Rekayasa trafik (*traffic engineering*, TE) adalah proses pemilihan saluran data traffic untuk menyeimbangkan beban trafik pada berbagai jalur dan titik dalam network. 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 [Awduche 1999a]. RFC-2702 menyebutkan tiga masalah dasar berkaitan dengan MPLS-TE, yaitu:

- Pemetaan paket ke dalam FEC
- Pemetaan FEC ke dalam trunk trafik
- Pemetaan trunk trafik ke topologi network fisik melalui LSP

Namun RFC hanya membahas soal ketiga. Soal lain dikaji sebagai soal-soal QoS. Awduche [1999b] menyusun sebuah model MPLS-TE, yang terdiri atas komponen-komponen: manajemen path, penempatan trafik, penyebaran keadaan network, dan manajemen network.

4.1. 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:

- 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.

- Atribut pemilihan dan pemeliharaan path generik, adalah aturan yang dipakai untuk memilih route yang diambil oleh trunk trafik, dan aturan untuk menjaganya tetap hidup.
- Atribut prioritas, menunjukkan prioritas pentingnya trunk trafik, yang dipakai baik dalam pemilihan path, maupun untuk menghadapi keadaan kegagalan network.
- 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.
- Atribut perbaikan, menentukan perilaku trunk trafik dalam kedaan kegagalan. Ini meliputi deteksi kegagalan, pemberitahuan kegagalan, dan perbaikan.
- 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.

4.2. 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.

4.3. Penyebaran Informasi 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.

4.4. 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.

4.5. 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 tebal berikut [Wang 2001]

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. Lebih jauh, RSVP-TE dikaji dalam RFC-3209.

5. 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.

5.1. MPLS dengan IntServ

Baik RSVP-TE maupun CR-LDP mendukung IntServ [Gray 2001]. RSVP-TE lebih alami untuk soal ini, karena RSVP sendiri dirancang untuk model IntServ. Namun CR-LDP tidak memiliki kelemahan untuk mendukung IntServ.

Permintaan reservasi dilakukan dengan pesan PATH di RSVP-TE atau *Label Request* di CR-LDP. Di ujung penerima, *egress* akan membalas dengan pesan RESV untuk RSVP-TE atau *Label Mapping* untuk CR-LDP, dan kemudian resource LSR langsung tersedia bagi aliran trafik dari *ingress*. Tidak ada beda yang menyolok antara kedua cara ini dalam mendukung model IntServ.

5.2. MPLS dengan DiffServ

Dukungan untuk DiffServ dilakukan dengan membentuk LSP khusus, dinamai L-LSP, yang secara administratif akan dikaitkan dengan perlakukan khusus pada tiap kelompok PHB. Alternatif lain adalah dengan mengirim satu LSP bernama E-LSP untuk setiap kelompok PHB.

Beda L-LSP dan E-LSP adalah bahwa E-LSP menggunakan bit-bit EXT dalam header MPLS untuk menunjukkan kelas layanan yang diinginkan; sementara L-LSP membedakan setiap kelas layanan dalam label itu sendiri.

Baik RSVP-TE dan LDP dapat digunakan untuk mendukung LSP khusus untuk model DiffServ ini.

6. Perbandingan Penggelaran Jaringan

6.1. ATM

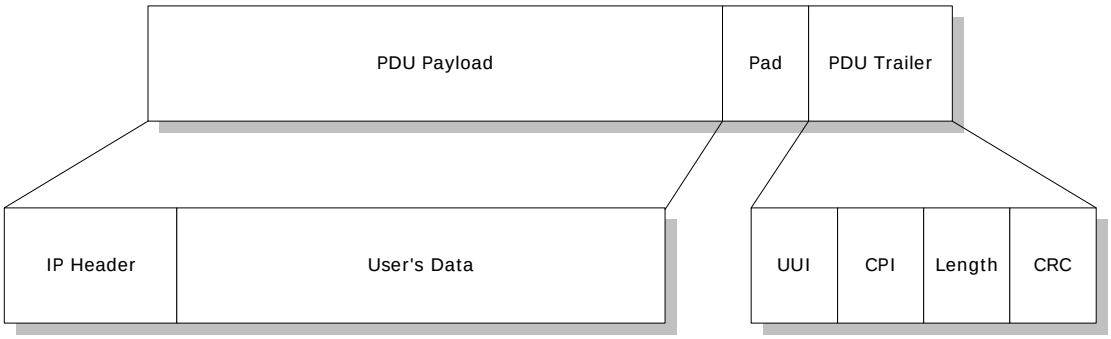
Sesuai spesifikasi ITU, ATM telah memiliki implementasi QoS yang sangat baik. Kontrak trafik dengan user selalu meliputi jenis trafik dan QoS yang dibutuhkan. Diferensiasi layanan disediakan dengan berbagai jenis AAL. Trafik IP misalnya, akan diangkut dengan AAL 5. AAL 1 hingga 4 digunakan untuk trafik suara, video, dan trafik data non IP.

Kelemahan implementasi langsung ATM adalah bahwa customer harus menyediakan terminal ATM pada instalasi mereka. Ini bukan soal mudah, karena sebagian besar customer diperkirakan hanya akan menggunakan perangkat IP. Keharusan mengadakan perangkat baru akan mengurangi minat menggunakan layanan ini.

6.2. IP over ATM

Untuk mempermudah customer, provider dapat membangun skema IP over ATM; yaitu dengan membangun core network berbasis ATM dan interface ke customer menggunakan IP. Customer dapat langsung berkomunikasi dengan IP dari instalasi mereka tanpa perangkat tambahan. Customer yang memiliki kebutuhan network bukan IP dapat langsung berinterface dengan struktur ATM yang juga tersedia. Kontrak trafik akan menyebutkan apakah pelanggan akan terhubung ke router IP atau switch ATM.

IP akan terenkapsulasi dalam AAL 5, yaitu AAL yang digunakan untuk trafik non-real-time, variable-bit-rate, yang bersifat baik *connectionless* or *connection oriented*. Enkapsulasi ini digambarkan dalam diagram berikut.



Konfigurasi IP over ATM umumnya membutuhkan pembentukan PVC antara router di tepian network ATM. Routing IP dan switching ATM merupajan proses yang sama sekali terpisah dan tidak saling mempengaruhi. Artinya pembentukan routing IP sama sekali tidak mempertimbangkan topologi network ATM di bawahnya. Ada potensi masalah di sini. Bagi network ATM, proses ini dapat menurunkan efisiensi total, karena PVC dilihat oleh IP sebagai sebuah link tunggal yang cost dan prioritasnya sama dengan link lainnya. Bagi IP, jika sebuah link ATM putus, beberapa link antar router dapat terputus, mengakibatkan masalah pada *update* data routing sekaligus dalam jumlah besar.

6.3. MPLS

Karena sebagian besar kelebihan ATM telah terlingkupi dalam teknologi ATM, sebenarnya jaringan IP over ATM dapat digantikan oleh sebuah jaringan MPLS. MPLS bersifat alami bagi dunia IP. Traffic engineering pada MPLS memperhitungkan sepenuhnya karakter trafik IP yang melewatinya.

Keuntungan lain adalah tidak diperlukannya kerumitan teknis seperti enkapsulasi ke dalam AAL dan pembentukan sel-sel ATM, yang masing-masing menambah delay, menambah header, dan memperbesar kebutuhan bandwidth. MPLS tidak memerlukan hal-hal itu.

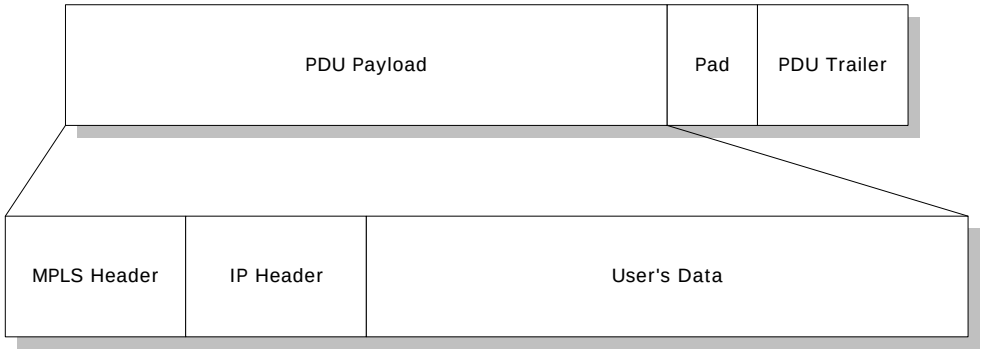
Persoalan besar dengan MPLS adalah bahwa hingga saat ini belum terbentuk dukungan untuk trafik non IP. Skema-skema L2 over MPLS (termasuk *Ethernet over MPLS*, *ATM over MPLS*, dan *FR over MPLS*) sedang dalam riset yang progresif, tetapi belum masuk ke tahap pengembangan secara komersial.

Yang cukup menjadikan harapan adalah banyaknya alternatif konversi berbagai jenis trafik ke dalam IP, sehingga trafik jenis itu dapat pula diangkut melalui jaringan MPLS. Juga proposal-proposal teknologi GMPLS sedang memasuki tahap standarisasi, sehingga ada harapan bahwa berbagai jenis teknologi dari layer 3 hingga layer 0 dapat dikonvergensikan dalam skema GMPLS.

6.4. MPLS over ATM

MPLS over ATM adalah alternatif untuk menyediakan interface IP/MPLS dan ATM dalam suatu jaringan. Alternatif ini lebih baik daripada IP over ATM, karena menciptakan semacam IP over ATM yang tidak lagi saling acuh. Alternatif ini juga lebih baik daripada MPLS tunggal, karena mampu untuk mendukung trafik non IP jika dibutuhkan customer.

Seperti paket IP, paket MPLS akan dienkapsulasikan ke dalam AAL 5, kemudian dikonversikan menjadi sel-sel ATM.

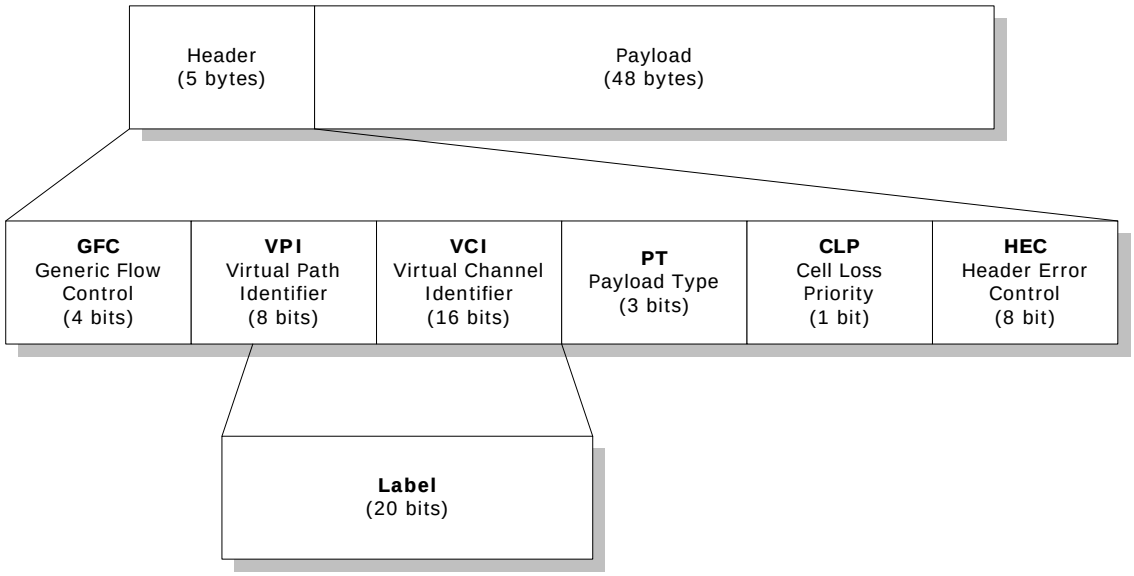


Kelemahan sistem ini adalah bahwa keuntungan MPLS akan berkurang, karena banyak kelebihannya yang akan *overlap* dengan keuntungan ATM. Alternatif ini sangat tidak cost-effective.

6.5. Hibrida MPLS-ATM

Hibrida MPLS-ATM adalah sebuah network yang sepenuhnya memadukan jaringan MPLS di atas core network ATM. MPLS dalam hal ini berfungsi mengintegrasikan fungsionalitas IP dan ATM, bukan memisahkannya. Tujuannya adalah menyediakan network yang dapat menangani trafik IP dan non-IP sama baiknya, dengan efisiensi tinggi.

Network terdiri atas LSR- ATM. Trafik ATM diolah sebagai trafik ATM. Trafik IP diolah sebagai trafik ATM-MPLS, yang akan menggunakan VPI and VCI sebagai label. Format sel ATM-MPLS digambarkan sebagai berikut.



Integrasi switch ATM dan LSR diharapkan mampu menggabungkan kecepatan switch ATM dengan kemampuan multi layanan dati MPLS. Biaya bagi pembangunan dan pemeliharaan network masih cukup optimal, mendekati biaya bagi network ATM atau network MPLS.

6.6. Rekomendasi

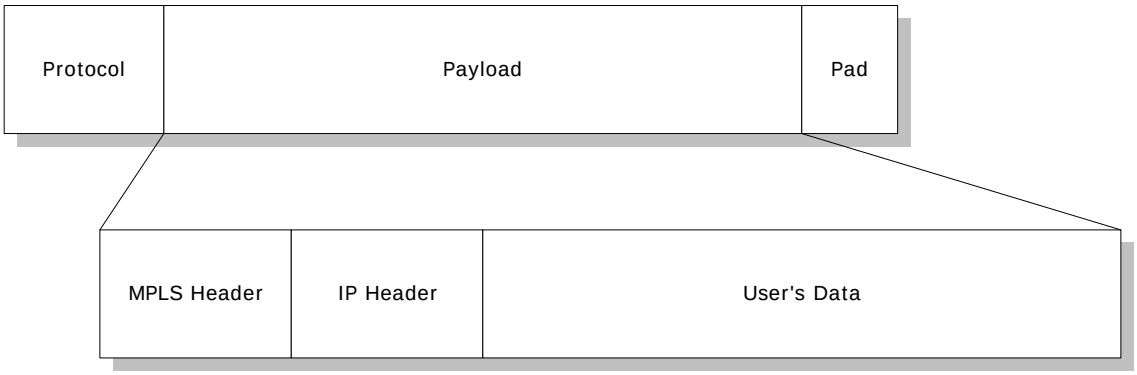
Secara singkat: jika permintaan untuk transportasi trafik non IP cukup besar relatif terhadap trafik IP, maka direkomendasikan pembangunan network hibrida MPLS-ATM. Namun jika trafik non IP tidak cukup besar, maka pembangunan network MPLS tanpa ATM akan lebih menghemat biaya. Diperlukan value management yang teliti untuk memutuskan platform network yang akan dibangun.

7. Interface ke Layer Bawah

Di network yang tidak memiliki ATM, paket MPLS dapat langsung dilewatkan pada struktur SDH. Salah satu metode yang disarankan adalah dengan POS (*packet over SDH*), seperti yang dikaji dalam RFC-1619. POS adalah interface yang dirancang untuk mentransferkan paket point-to-point ke dalam frame-frame SONET atau SDH.

7.1. Point-to-Point Protocol (PPP)

Protokol yang dirancang sebagai metode komunikasi dalam link point-to-point adalah PPP (RFC-1661). PPP memiliki fungsi enkapsulasi multi protokol, *error control*, dan kontrol inisialisasi link. *Overhead* PPP juga relatif kecil, sehingga tepat digunakan untuk link yang hemat bandwidth. Enkapsulasi MPLS dengan PPP digambarkan sebagai berikut::



7.2. Pemetaan ke SDH

Seperti yang dipersyaratkan dalam RFC-1662, paket yang telah dienkapsulasi dengan PPP harus diframekan dengan *high-level data-link control* (HDLC).

Untuk dikirim melalui SDH, frame HDLC ini kemudian dipetakan secara sinkron ke SPE (*synchronous payload envelope*). Rate dasar untuk PPP over SDH adalah STM-1, yaitu 155.52 Mb/s, yang mengandung rate informasi sebesar 149.76 Mb/s, yaitu sebesar STM-1 dikurangi *overhead*.

Informasi dengan rate lebih kecil bisa dipetakan ke VT (virtual tributary) dari SDH, yang setara dengan sinyal E1, hingga E3.

8. VPN dengan MPLS

Salah satu feature MPLS adalah kemampuan membentuk tunnel atau virtual circuit yang melintasi networknya. Kemampuan ini membuat MPLS berfungsi sebagai platform alami untuk membangun *virtual private network* (VPN).

VPN yang dibangun dengan MPLS sangat berbeda dengan VPN yang hanya dibangun berdasarkan teknologi IP, yang hanya memanfaatkan enkripsi data. VPN dpada MPLS lebih mirip dengan virtual circuit dari FR atau ATM, yang dibangun dengan membentuk isolasi trafik. Trafik benar-benar dipisah dan tidak dapat dibocorkan ke luar lingkup VPN yang didefinisikan.

Lapisan pengamanan tambahan seperti IPSec dapat diaplikasikan untuk data security, jika diperlukan. Namun tanpa metode semacam IPSec pun, VPN dengan MPLS dapat digunakan dengan baik.

8.1. Feature bagi Customer

Di dalam VPN, customer dapat membentuk hubungan antar lokasi. Konektivitas dapat terbentuk dari titik mana pun ke titik mana pun (banyak arah sekaligus), tanpa harus melewati semacam titik pusat, dan tanpa harus menyusun serangkaian link dua arah. Ini dapat digunakan sebagai platform intranet yang secara efisien melandasi jaringan IP sebuah perusahaan. Ini juga dapat digunakan sebagai extranet yang menghubungkan perusahaan-perusahaan yang terikat perjanjian.

Mekanisme pembentukan VPN telah tercakup dalam konfigurasi MPLS, sehingga tidak diperlukan perangkat tambahan di site customer. Bahkan, jika diinginkan, konfigurasi VPN sendiri dapat dilakukan dari site provider.

8.2. Mekanisme VPN

Ada beberapa rancangan yang telah diajukan untuk membentuk VPN berbasis IP dengan MPLS. Belum ada satu pun yang dijadikan bakuan. Namun ada dua rancangan yang secara umum lebih sering diacu, yaitu MPLS-VPN dengan BGP, dan explicitly routed VPN. MPLS-VPN dengan BGP saat ini lebih didukung karena alternatif lain umumnya bersifat propriertary dan belum menemukan bentuk final.

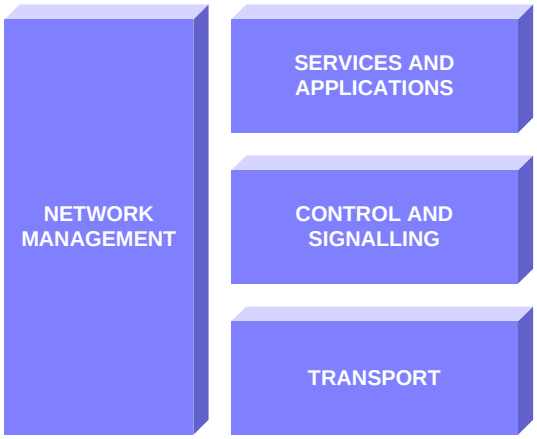
Panduan implementasi MPLS-VPN dengan BGP adalah RFC-2547. BGP mendistribusikan informasi tentang VPN hanya ke router dalam VPN yang sama, sehingga terjadi pemisahan trafik. E-LSR dari provider berfungsi sebagai *provider-edge router* (PE) yang terhubung ke *customer-edge router* (CE). PE mempelajari alamat IP dan membentuk sesi BGP untuk berbagi info ke PE lain yang terdefinisikan dalam VPN. BGP untuk MPLS berbeda dengan BGP untuk paket IP biasa, karena memiliki ekstensi multi-protokol seperti yang didefinisikan dalam RFC-2283.

9. Next Generation Network

9.1. Konsep NGN

NGN dirancang untuk memenuhi kebutuhan infrastruktur infokom abad ke 21. Jaringan tidak lagi diharapkan bersifat TDM, melainkan sudah dalam bentuk paket-paket yang efisien, namun dengan QoS terjaga. NGN harus mampu mengelola dan membawa berbagai macam trafik sesuai kebutuhan customer yang terus berkembang.

NGN disusun dalam blok-blok kerja yang terbuka, dan bersifat open system, seperti gambar di bawah. Setiap blok memiliki pengembangan yang terbuka lebar, namun harus selalu dapat dikomunikasikan dengan pengembangan blok-blok lainnya.



Pada blok “Services and Application”, saat ini tengah dikembangkan penggunaan standar JAIN dan OSA/Parlay. Untuk “Control and Signalling”, terdapat beberapa standar yang disepakati ITU dan IETF. Signalling untuk multimedia dapat menggunakan suite H.323 yang distandarkan ITU, atau SIP yang distandarkan IETF. Sedangkan untuk control, baik ITU dan IETF telah bersepakat menggunakan standar bersama yang disebut H.248 oleh ITU atau MEGACO oleh IETF.

Level “Transport” harus dioptimasi sesuai jenis trafik yang akan dilewatkan. Untuk jenis trafik yang beraneka ragam namun menuntut QoS yang terpelihara, teknologi MPLS adalah pilihan terbaik. Untuk network yang spesifik mengangkut jenis trafik tertentu, teknologi lain dapat disiapkan.

Konsep NGN yang lengkap meliputi juga teknologi yang tak mungkin diabaikan, yaitu teknologi wireless, baik untuk perangkat diam, bergerak lambat, maupun bergerak cepat, dengan berbagai rate data yang dibutuhkan.

9.2. Softswitch

Teknologi switching, yang masih berfokus pada data yang bersifat TDM, harus mulai mengikuti paradigma network yang bersifat broadband. Pada perkembangan teknologi sebelumnya, telah dilakukan pemisahan kanal data dengan signalling. Pemisahan ini, seperti pada CCS#7, bukan saja memberikan efisiensi network yang lebih baik, namun juga telah memungkinkan pembentukan IN dengan berbagai layanannya.

Trend ini dipertahankan dan dikembangkan dalam teknologi switching broadband. Data multimedia dipaketkan dalam paket RTP dalam suite IP, dan ditransferkan antar media gateway (MG). Signalling memiliki signalling gateway (SG) tersendiri. Signalling untuk multimedia dapat menggunakan suite H.323 yang distandarkan ITU, atau SIP yang distandarkan IETF.

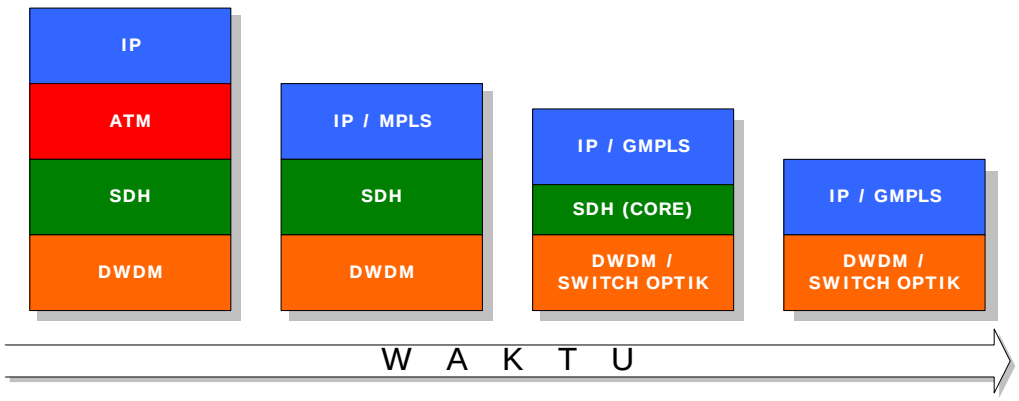
Sistem switching yang besar dapat digantikan oleh softswitch, yaitu sistem switching dalam ujud fisik kecil, namun dengan kekuatan software yang mengendalikan MG-MG berdasar informasi dari SG-SG. Pengendalian oleh softswitch telah distandarkan bersama dengan protocol MEGACO (atau H.248).

Implementasi softswitch diharapkan mengakhiri era VoIP transisi, dan membentuk sistem network infokom yang terpadu, lebih baik, dan efisien biaya.

9.3. GMPLS

GMPLS (*Generalized MPLS*) adalah konsep konvergensi vertikal dalam teknologi transport, yang tetap berbasis pada penggunaan label seperti MPLS. Setelah MPLS dikembangkan untuk memperbaiki jaringan IP, konsep label digunakan untuk jaringan optik berbasis DWDM, dimana panjang gelombang (λ) digunakan sebagai label. Standar yang digunalan disebut MPλS. Namun, mempertimbangkan bahwa sebagian besar jaringan optik masih memakai SDH, bukan hanya DWDM, maka MPλS diperluas untuk meliputi juga TDM, ADM dari SDH, OXC. Konsep yang luas ini lah yang dinamai GMPLS.

GMPLS merupakan konvergensi vertikal, karena ia menggunakan metode *label switching* dalam layer 0 hingga 3 [Allen 2001]. Tujuannya adalah untuk menyediakan network yang secara keseluruhan mampu menangani bandwidth besar dengan QoS yang konsisten serta pengendalian penuh. Dan terintegrasi Diharapkan GMPLS akan menggantikan teknologi SDH dan ATM klasik, yang hingga saat ini masih menjadi layer yang paling mahal dalam pembangunan network.



10. Daftar Singkatan

AAL = ATM Adaptation Layer
ATM = Asynchronous Transfer Mode
BGP = Border Gateway Protocol
CE = Customer Edge
CR = Constraint-Based Routing
DiffServ = Differentiated Service
DSCP = DiffServ Code Point
DWDM = Dense Wavelength Division Multiplexing
FEC = Forwarding-Equivalence Class
FR = Frame Relay
GMPLS = Generalized Multi Protocol Label Switching
HDLC = High-Level Data-Link Control
IETF = Internet Engineering Task Force
IntServ = Integrated Service
IP = Internet Protocol

LDP = Label Distribution Protocol
LSP = Label-Switched Path
LSR = Label-Switched Router
MEGACO = Media Gateway Controller
MPLS = Multi Protocol Label Switching
MPλS = Multi Protocol Lambda (Wavelength) Switching
NGN = Next Generation Network
OXC = Optical Cross Connect
PE = Provider Edge
POS = Packet over SONET, Packet over SDH
PPP = Point to Point Protocol
PVC = Permanent VC
QoS = Quality of Service
RFC = Request for Comments
RSVP = Resource Reservation Protocol
RTP = Real-Time Transfer Protocol
SDH = Synchronous Digital Hierarchy
SIP = Session Initiation Protocol
SPE = Synchronous Payload Envelope
TCP = Transmission Control Protocol
TDM = Time Division Multiplexing
TE = Traffic Engineering
TTL = Time to Live
UDP = User Datagram Protocol
VC = Virtual Circuit (ATM), Virtual Container (SDH)
VPN = Virtual Private Network
VT = Virtual Tributary

11. Referensi

11.1. Buku, Paper, Standar

- Awduche E et.al. (1999a). Requirements for Traffic Engineering over MPLS. RFC-2702. Internet Society.
- Gray EW (2001). MPLS: Implementing The Technology. Boston, Addison-Wesley.
- Hall EA (2000). Internet Core Protocols: The Definitive Guide. Sebastopol, O'Reilly.
- Rosen E and Rekhter Y (1999). BGP/MPLS VPNs. RFC-2547. Internet Society.
- Rosen E et.al. (2001). Multiprotocol Label Switching Architecture. RFC-3031. Internet Society.
- Wang Z (2001). Internet QoS: Architectures and Mechanisms for Quality of Service. San Francisco, Morgan-Kaufmann.
- Xiao X (2000). Providing Quality of Service in the Internet. PhD Dissertation. Michigan, Michigan State University.

11.2. Artikel di Jurnal dan Majalah

- Allen D (2001) How Will Multiprotocol Lambda Switching Change Optical Networks? Network Magazine, May 2001, pp 70-74.
- Awduche D (1999b). MPLS and Traffic Engineering in IP Networks. IEEE Communications Magazine, December 1999, pp 42-47.
- Bernet Y (2000). The Complementary Roles of RSVP and Differentiated Services in the Full-Service QoS Network. IEEE Communications Magazine, February 2000, pp 154-162.

- Courtney R (2001). IP QoS: Tracking the Different Level. Telecommunications Magazine, January 2001, pp 58-60.
- Dovrolis C and Ramanathan P (1999). A Case for Relative Differentiated Services and the Proportional Differentiation Model. IEEE Network, September/October 1999, pp 26-34.
- Dutta-Roy A (2000). The Cost of Quality in Internet-style Networks. IEEE Spectrum, September 2000.
- Hay R (2000). Comparing POS and ATM Interfaces. IEEE Computer, August 2000, pp 102-106.
- Lawrence J (2001). Designing Multiprotocol Label Switching Networks. IEEE Communications Magazine, July 2001, pp 134-142.
- Manchester J et.al. (1998). IP over SONET. IEEE Communications Magazine, May 1998, pp 136-142.
- Mathy L et.al. (2000). The Internet: A Global Telecommunications Solution? IEEE Network, July/August 2000, pp 46-57
- Viswanathan A et.al. (1998). Evolution of Multiprotocol Label Switching. IEEE Communications Magazine, May 1998, pp 165-172.
- White P (1997). RSVP and Integrated Service in the Internet: A Tutorial. IEEE Communications Magazine, May 1997, pp 100-106.

12. Biografi Penulis

Kuncoro Wastuwibowo. Lahir di Bandung pada 19 Juni 1970. Lulus dari Universitas Brawijaya tahun 1993 (Ir, teknik elektro), dan dari Coventry University tahun 2001 (MSc, teknologi telekomunikasi, atas beasiswa Chevening Award). Anggota IEEE (Communications Society dan Computer Society), IECI, ISOC, dan ACCU. Saat ini bekerja di Telkom Divisi Regional III sebagai Analis Pengembangan Teknologi (sejak tahun 2003), setelah sebelumnya menjadi Spesialis Rekayasa Network (1996) dan Spesialis Internet (2002) serta sempat memberikan pelatihan2 di Divisi Pelatihan Telkom. Memperoleh penghargaan prestasi Telkom dari Menteri Perhubungan di tahun 1999. Merancang program dalam bahasa C dan kemudian C++ sebagai alat bantu bekerja. Menulis artikel-artikel pemrograman di Mikrodata dan Jawa Pos selama masih kuliah.

Informasi lebih lanjut dapat diperoleh melalui:
Web: http://kun.co.ro
Mail: mail@kun.co.ro

Versi 1.0