BUKU JARINGAN KOMPUTER II

Penulis: 3D4 Telkom 2004
Editor: Sritrusta Sukaridhoto, ST. PhD. (dhoto@pens.ac.id)

Politeknik Elektronika Negeri Surabaya (PENS) – 2014

Daftar Isi

BAB 1. IPv6

Ria Puspita Sari [1)], Bagus Arianandhika [1)], Tiyas Agustina [1)]

[1)]Politeknik Elektronika Negeri Surabaya

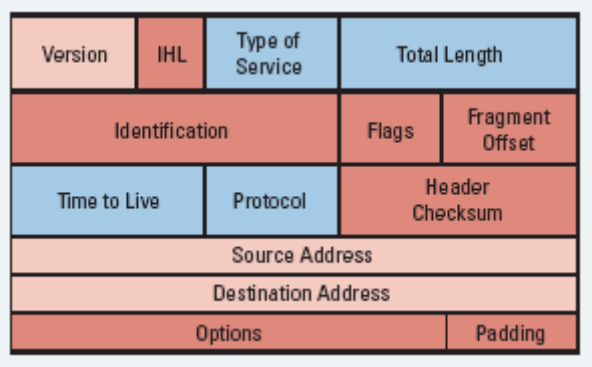
ABSTRAK

Perkembangan teknologi jaringan komputer dewasa ini semakin pesat seiring dengan kebutuhan masyarakat akan layanan yang memanfaatkan jaringan komputer. Pada sistem jaringan komputer, protokol merupakan suatu bagian yang paling penting. Protokol jaringan yang umum digunakan adalah IPv4, yang masih terdapat beberapa kekurangan dalam menangani jumlah komputer dalam suatu jaringan yang semakin kompleks. Telah dikembangkan protokol jaringan baru, yaitu IPv6 yang merupakan solusi dari masalah diatas. Protokol baru ini belum banyak diimplementasikan pada jaringan-jaringan di dunia.

IP versi 6 (IPv6) adalah protokol Internet versi baru yang didesain sebagai pengganti dari Internet protocol versi 4 (IPv4) yang didefinisikan dalam RFC 791. IPv6 yang memiliki kapasitas address raksasa (128 bit), mendukung penyusunan address secara terstruktur, yang memungkinkan Internet terus berkembang dan menyediakan kemampuan routing baru yang tidak terdapat pada IPv4. IPv6 memiliki tipe address anycast yang dapat digunakanuntuk pemilihan route secara efisien. Selain itu IPv6 juga dilengkapi oleh mekanisme penggunaan address secara local yang memungkinkan terwujudnya instalasi secara Plug&Play, serta menyediakan platform bagi cara baru pemakaian Internet, seperti dukungan terhadap aliran datasecara real-time, pemilihan provider, mobilitas host, end-to-end security, ataupun konfigurasi otomatis.

1.1 Latar Belakang dan Permasalahan IPv4

IPv4 yang merupakan pondasi dari Internet telah hampir mendekati batas akhir dari kemampuannya, dan IPv6 yang merupakan protokol baru telah dirancang untuk dapat menggantikan fungsi IPv4. Motivasi utama untuk mengganti IPv4 adalah karena keterbatasan dari panjang addressnya yang hanya 32 bit saja serta tidak mampu mendukung kebutuhan akan komunikasi yang aman, routing yang fleksibel maupun pengaturan lalu lintas data.



Gambar 1-1 struktur header dasar pada ipv4

IP versi 6 (IPv6) adalah protokol Internet versi baru yang didesain sebagai pengganti dari Internet protocol versi 4 (IPv4) yang didefinisikan dalam RFC 791. IPv6 yang memiliki kapasitas

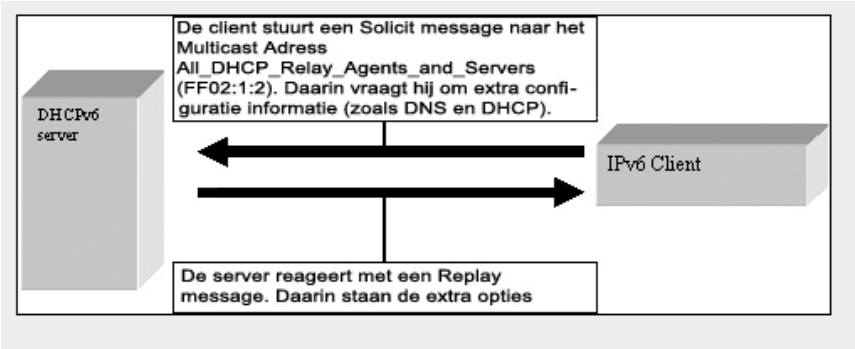
address raksasa (128 bit), mendukung penyusunan address secara terstruktur, yang memungkinkan Internet terus berkembang dan menyediakan kemampuan routing baru yang tidak terdapat pada IPv4. IPv6 memiliki tipe address anycast yang dapat digunakanuntuk pemilihan route secara efisien. Selain itu IPv6 juga dilengkapi oleh mekanisme penggunaan address secara local yang memungkinkan terwujudnya instalasi secara Plug&Play, serta menyediakan platform bagi cara baru pemakaian Internet, seperti dukungan terhadap aliran datasecara real-time, pemilihan provider, mobilitas host, end-to-end security, ataupun konfigurasi otomatis.

1.2 Keunggulan IPv6

Otomatisasi berbagai setting / Stateless-less auto-configuration (plug&play) Address pada IPv4 pada dasarnya statis terhadap host. Biasanya diberikan secara berurut pada host. Memang saat ini hal di atas bisa dilakukan secara otomatis dengan menggunakan DHCP (Dynamic Host Configuration Protocol), tetapi hal tersebut pada IPv4 merupakan fungsi tambahan saja, sebaliknya pada IPv6 fungsi untuk mensetting secara otomatis disediakan secara standar dan merupakan defaultnya. Pada setting otomatis ini terdapat 2 cara tergantung dari penggunaan address, yaitu ***setting otomatis stateless dan statefull***.

1.2.1 Setting otomatis statefull

Cara pengelolaan secara ketat dalam hal range IP address yang diberikan pada host dengan menyediakan server untuk pengelolaan keadaan IP address, dimana cara ini hampir mirip dengan cara DHCP pada IPv4. Pada saat melakukan setting secara otomatis, informasi yang dibutuhkan antara router, server dan host adalah ICMP (Internet Control Message Protocol) yang telah diperluas. Pada ICMP dalam IPv6 ini, termasuk pula IGMP (Internet Group management Protocol) yang dipakai pada multicast pada IPv4.

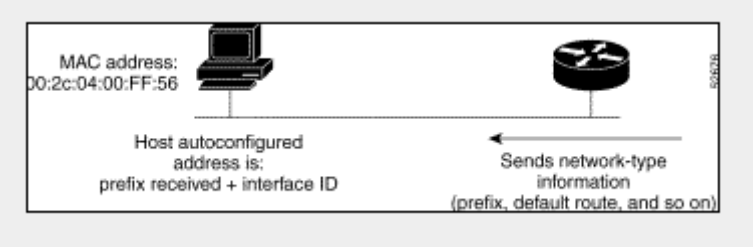


Gambar 1-2 Setting otomatis statefull

1.2.2 Setting otomatis stateless

Pada cara ini tidak perlu menyediakan server untuk pengelolaan dan pembagian IP address, hanya mensetting router saja dimana host yang telah tersambung di jaringan dari router yang ada pada jaringan tersebut memperoleh prefix dari address dari jaringan tersebut. Kemudian host menambah pattern bit yang diperoleh dari informasi yang unik terhadap host, lalu membuat IP address sepanjang 128 bit dan menjadikannya sebagai IP address dari host tersebut. Pada informasi unik bagi host ini, digunakan antara lain address MAC dari jaringan

interface. Pada setting otomatis stateless ini dibalik kemudahan pengelolaan, pada Ethernet atau FDDI karena perlu memberikan paling sedikit 48 bit (sebesar address MAC) terhadap satu jaringan, memiliki kelemahan yaitu efisiensi penggunaan address yang buruk.



Gambar 1-3 Setting otomatis stateless

1.3 Perubahan dari IPv4 ke IPv6

Perubahan dari IPv4 ke IPv6 pada dasarnya terjadi karena beberapa hal yang dikelompokkan dalam kategori berikut :

1.3.1 Kapasitas Perluasan Alamat

IPv6 meningkatkan ukuran dan jumlah alamat yang mampu didukung oleh IPv4 dari 32 bit menjadi 128bit. Peningkatan kapasitas alamat ini digunakan untuk mendukung peningkatan hirarki atau kelompok pengalamatan, peningkatan jumlah atau kapasitas alamat yang dapat dialokasikan dan diberikan pada *node* dan mempermudah konfigurasi alamat pada *node* sehingga dapat dilakukan secara otomatis. Peningkatan skalabilitas juga dilakukan pada *routing multicast* dengan meningkatkan cakupan dan jumlah pada alamat *multicast*. IPv6 ini selain meningkatkan jumlah kapasitas alamat yang dapat dialokasikan pada *node* juga mengenalkan jenis atau tipe alamat baru, yaitu alamat *anycast*. Tipe alamat *anycast* ini didefinisikan dan digunakan untuk mengirimkan paket ke salah satu dari kumpulan *node*.

1.3.2 Penyederhanaan Format Header

Beberapa kolom pada *header* IPv4 telah dihilangkan atau dapat dibuat sebagai *header* pilihan. Hal ini digunakan untuk mengurangi biaya pemrosesan hal-hal yang umum pada penanganan paket IPv6 dan membatasi biaya *bandwidth* pada *header* IPv6. Dengan demikian, pemerosesan *header* pada paket IPv6 dapat dilakukan secara efisien.

1.3.3 Peningkatan dukungan untuk header pilihan dan header tambahan (Options and extention header)

Perubahan yang terjadi pada *header-header* IP yaitu dengan adanya pengkodean *header Options* (pilihan) pada IP dimasukkan agar lebih efisien dalam penerusan paket (*packet forwarding*), agar tidak terlalu ketat dalam pembatasan panjang *header* pilihan yang terdapat dalam paket IPv6 dan sangat fleksibel/dimungkinkan untuk mengenalkan *header* pilihan baru pada masa akan dating.

1.3.4 Kemampuan pelabelan aliran paket

Kemampuan atau fitur baru ditambahkan pada IPv6 ini adalah memungkinkan pelabelan paket atau pengklasifikasikan paket yang meminta penanganan khusus, seperti kualitas mutu layanan tertentu (*QoS*) atau *real-time.*

1.3.5 Autentifikasi dan kemampuan privasi

Kemampuan tambahan untuk mendukung autentifikasi, integritas data dan data penting juga dispesifikasikan dalam alamat IPv6.

Perubahan terbesar pada IPv6 adalah perluasan IP address dari 32 bit pada IPv4 menjadi 128 bit.128 bit ini adalah ruang address yang kontinyu dengan menghilangkan konsep kelas. Selain itu juga dilakukan perubahan pada cara penulisan IP address. Jika pada IPv4 32 bit dibagi menjadi masing-masing 8 bit yang dipisah kan dengan "." dan di tuliskan dengan angka desimal, maka pada IPv6, 128 bit tersebut dipisahkan menjadi masing-masing 16 bit yang tiap bagian dipisahkan dengan ":"dan dituliskan dengan hexadesimal. Selain itu diperkenalkan pula struktur bertingkat agar pengelolaan routing menjadi mudah. Pada CIDR (Classless Interdomain Routing) table routing diperkecil dengan menggabungkan jadi satu informasi routing dari sebuah organisasi.

Tabel 1-1 Pembagian ruang address pada IPv6

Allocation	Prefix (binary)	Fraction of Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider based Unicast Address	010	1/8
Unassigned	011	1/8
Reserved for Neutral-Interconnect-Based Unicast Addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 1101	1/128
Unassigned	1111 1110	1/512
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

Untuk memahami tentang struktur bertingkat address pada IPv6 ini, dengan melihat contoh pada address untuk provider. Pertama-tama address sepanjang 128 bit dibagi menjadi beberapa field yang dapat berubah panjang. Jika 3 bit pertama dari address adalah "010", maka ini adalah ruang bagi provider. Sedangkan n bit berikutnya adalah registry ID yaitu field yang menunjukkan tempat/lembaga

yang memberikan IP address. Misalnya IP address yang diberikan oleh InterNIC maka field tersebut menjadi "11000". Selanjutnya m bit berikutnya adalah provider ID, sedangkan o bit berikutnya adalah Subscriber ID untuk membedakan organisasi yang terdaftar pada provider tersebut.

Kemudian p bit berikutnya adalah Subnet ID, yang menandai kumpulan host yang tersambung secara topologi dalam jaringan dari organisasi tersebut. Dan yang q=125-(n+m+o+p) bit terakhir adalah Interface ID, yaitu IP address yang menandai host yang terdapat dalam grup-grup yang telah ditandai oleh Subnet ID.

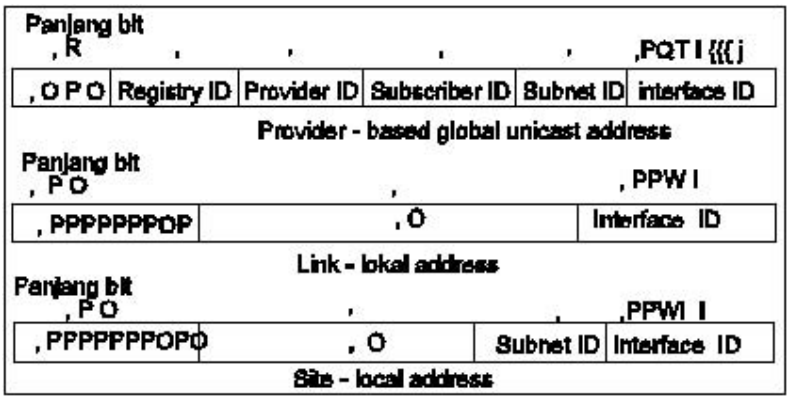
Subnet ID dan Interface ID ini bebas diberikan oleh organisasi tersebut. Organisasi bebas menggunakan sisa p+q bit dari IP address dalam memberikan IP address di dalam organisasinya setelah mendapat 128-(p+q) bit awal dari IP address. Pada saat itu, administrator dari organisasi tersebut dapat membagi menjadi bagian sub-jaringan dan host dalam panjang bit yang sesuai, jika diperlukan dapat pula dibuat lebih terstruktur lagi. Karena panjang bit pada provider ID dan subscriber ID bisa berubah, maka address yang diberikan pada provider dan jumlah IP address yang dapat diberikan oleh provider kepada pengguna dapat diberikan secara bebas sesuai dengan kebutuhan. Pada IPv6 bagian kontrol routing pada address field disebut prefix, yang dapat dianggap setara dengan jaringan address pada IPv4.

1.4 Alamat IPv6

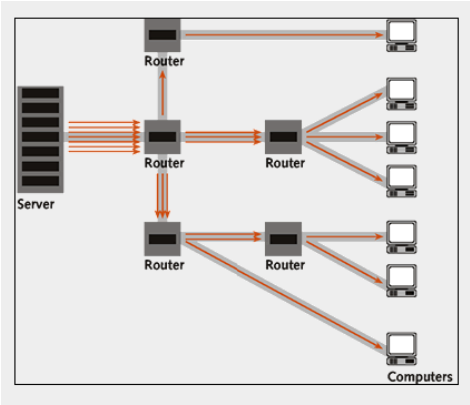
1.4.1 Unicast Address (one-to-one)

Digunakan untuk komunikasi satu lawan satu, dengan menunjuk satu host. Pada Unicast address ini terdiri dari :

1. Global, address yang digunakan misalnya untuk address provider atau address geografis.
2. Link Local Address adalah address yang dipakai di dalam satu link saja. Yang dimaksud link di sini adalah jaringan lokal yang saling tersambung pada satu level. Address ini dibuat secara otomatis oleh host yang belum mendapat address global, terdiri dari 10+n bit prefix yang dimulai dengan "FE80" dan field sepanjang 118-n bit yang menunjukkan nomor host. Link Local Address digunakan pada pemberian IP address secara otomatis.
3. Site-local, address yang setara dengan private address, yang dipakai terbatas di dalam site saja. Address ini dapat diberikan bebas, asal unik di dalam site tersebut, namun tidak bisa mengirimkan packet dengan tujuan alamat ini di luar dari site tersebut.
4. Compatible



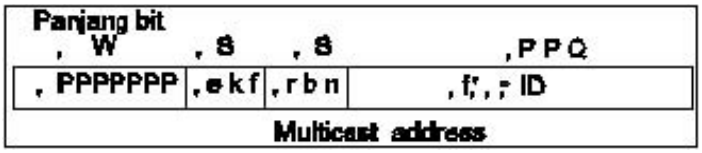
Gambar 1-4 Struktur unicast address



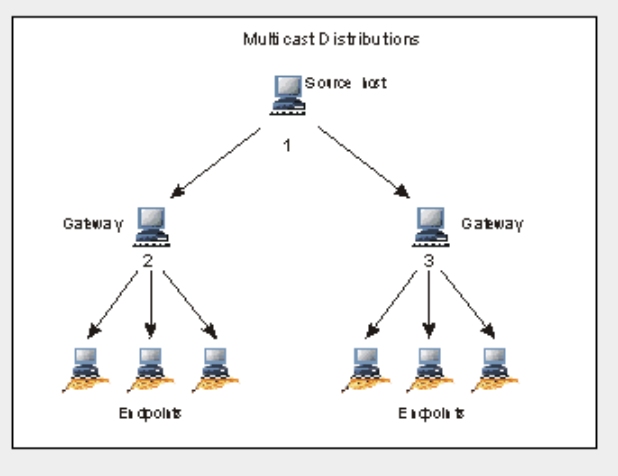
Gambar 1-5 Pengiriman paket pada unicast address

1.4.2 Multicast (one-to-many)

Yang digunakan untuk komunikasi 1 lawan banyak dengan menunjuk host dari group. Multicast Address ini pada IPv4 didefinisikan sebagai kelas D, sedangkan pada IPv6 ruang yang 8 bit pertamanya di mulai dengan "FF" disediakan untuk multicast Address. Ruang ini kemudian dibagi-bagi lagi untuk menentukan range berlakunya. Kemudian Blockcast address pada IPv4 yang address bagian hostnya didefinisikan sebagai "1", pada IPv6 sudah termasuk di dalam multicast Address ini. Blockcast address untuk komunikasi dalam segmen yang sama yang dipisahkan oleh gateway, sama halnya dengan multicast address dipilah berdasarkan range tujuan.



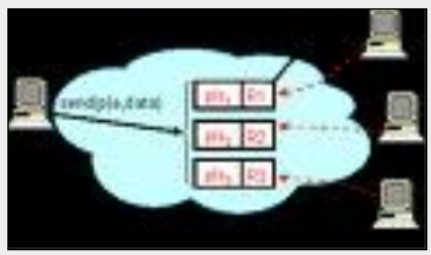
Gambar 1-6 Struktur multicast address



Gambar 1-7 Pengiriman paket pada multicast address

1.4.3 Anycast Address

Yang menunjuk host dari group, tetapi packet yang dikirim hanya pada satu host saja.Pada address jenis ini, sebuah address diberikan pada beberapa host, untuk mendifinisikan kumpulan node. Jika ada packet yang dikirim ke address ini, maka router akan mengirim packet tersebut ke host terdekat yang memiliki Anycast address sama. Dengan kata lain pemilik packet menyerahkan pada router tujuan yang paling "cocok" bagi pengiriman packet tersebut. Pemakaian Anycast Address ini misalnya terhadap beberapa server yang memberikan layanan seperti DNS (Domain Name Server). Dengan memberikan Anycast Address yang sama pada server-server tersebut, jika ada packet yang dikirim oleh client ke address ini, maka router akan memilih server yang terdekat dan mengirimkan packet tersebut ke server tersebut. Sehingga, beban terhadap server dapat terdistribusi secara merata.Bagi Anycast Address ini tidak disediakan ruang khusus. Jika terhadap beberapa host diberikan sebuah address yang sama, maka address tersebut dianggap sebagai Anycast Address.

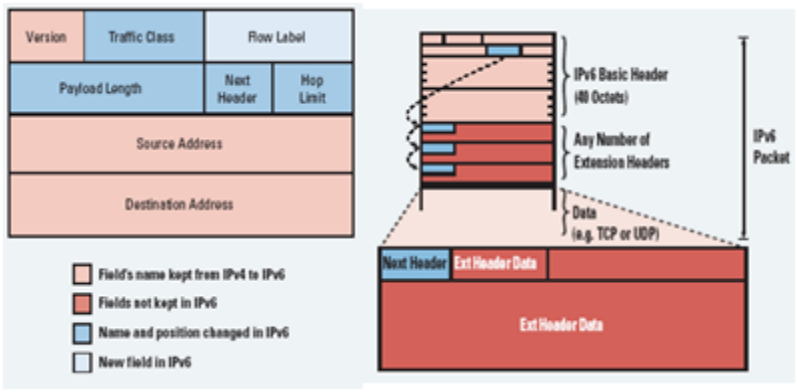


Gambar 1-8 Pengiriman paket pada anycast address

1.5 Struktur Paket data IPv6

Dalam pendesignan header packet ini, diupayakan agar cost/nilai pemrosesan header menjadi kecil untuk mendukung komunikasi data yang lebih real time. Misalnya, address awal dan akhir menjadi dibutuhkan pada setiap packet. Sedangkan pada header IPv4 ketika packet dipecah-pecah, ada field untuk menyimpan urutan antar packet. Namun field tersebut tidak terpakai ketika packet tidak dipecah-pecah. Header pada Ipv6 terdiri dari dua jenis, yang pertama, yaitu field yang dibutuhkan oleh setiap packet disebut header dasar, sedangkan yang kedua yaitu field yang tidak selalu diperlukan pada

packet disebut header ekstensi, dan header ini didifinisikan terpisah dari header dasar. Header dasar selalu ada pada setiap packet, sedangkan header tambahan hanya jika diperlukan diselipkan antara header dasar dengan data. Header tambahan, saat ini didefinisikan selain bagi penggunaan ketika packet dipecah, juga didefinisikan bagi fungsi sekuriti dan lain-lain. Header tambahan ini, diletakkan setelah header dasar, jika dibutuhkan beberapa header maka header ini akan disambungkan berantai dimulai dari header dasar dan berakhir pada data. Router hanya perlu memproses header yang terkecil yang diperlukan saja, sehingga waktu pemrosesan menjadi lebih cepat. Hasil dari perbaikan ini, meskipun ukuran header dasar membesar dari 20 bytes menjadi 40 bytes namun jumlah field berkurang dari 12 menjadi 8 buah saja.



Gambar 1-9 Struktur header dasar pada IPv6

1.6 Flow-Label dan REAL TIME PROCESS

Header dari packet pada IPv6 memiliki field label alir (flow-label) yang digunakan untuk meminta agar packet tersebut diberi perlakuan tertentu oleh router saat dalam pengiriman (pemberian ‘flag’). Misalnya pada aplikasi multimedia sedapat mungkin ditransfer secepatnya walaupun kualitasnya sedikit berkurang, sedangkan e-mail ataupun WWW lebih memerlukan sampai dengan akurat dari pada sifat real time.

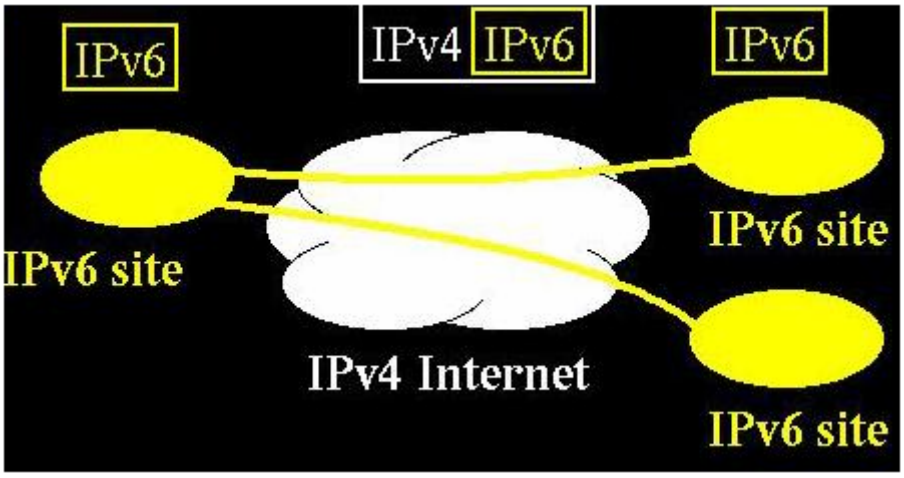
Tabel 1-2 Tabel label alir pada IPv6

Label	Kategori
0	Uncharacterized Traffic
1	"Filler" traffic (e.g., netnews)
2	Unattended data transfer (e.g., e-mail)
3	Reserved
4	Attended bulk transfer (e.g., FTP, HTTP, NFS)
5	Reserved
6	Interactive traffic (e.g., Telnet, X)
7	Internet control traffic (e.g., routing protocols, SNMP)
8-15	Realtime communications traffic, non-congestion-controlled traffic

Router mengelola skala prioritas maupun resource seperti kapasitas komunikasi atau kemampuan memproses, dengan berdasar pada label alir ini. Jika pada IPv4 seluruh packet diperlakukan sama, maka p ada IPv6 ini dengan perlakuan yang berbeda terhadap tiap packet, tergantung dari isi packet tersebut, dapat diwujudkan komunikasi yang aplikatif.

1.7 IPv6 TRANSITION (IPv4 – IPv6)

Untuk mengatasi kendala perbedaan antara IPv4 dan IPv6 serta menjamin terselenggaranya komunikasi antara pengguna IPv4 dan pengguna IPv6, maka dibuat suatu metode Hosts – dual stack serta Networks – Tunneling pada hardware jaringan, misalnya router dan server



Gambar 1-10 Network - tunneling (IPv6 transition)

Jadi setiap router menerima suatu packet, maka router akan memilah packet tersebut untuk menentukan protokol yang digunakan, kemudian router tersebut akan meneruskan ke layer diatasnya.

1.8 Representasi Alamat pada IPv6

Model x:x:x:x:x:x:x:x dimana ‘x‘ berupa nilai hexadesimal dari 16 bit porsi alamat, karena ada 8 buah ‘x‘ maka jumlah totalnya ada 16 * 8 = 128 bit. Contohnya adalah :

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Jika format pengalamatan IPv6 mengandung kumpulan group 16 bit alamat, yaitu **‘x‘**, yang bernilai 0 maka dapat direpresentasikan sebagai ‘**::**’. Contohnya adalah :

FEDC:0:0:0:0:0:7654:3210

dapat direpresentasikan sebagai

FEDC::7654:3210 **0:0:0:0:0:0:0:1**

dapat direpresentasikan sebagai

::1

Model x:x:x:x:x:x:d.d.d.d dimana ‘d.d.d.d’ adalah alamat IPv4 semacam 167.205.25.6 yang digunakan untuk automatic tunnelling. Contohnya adalah :

0:0:0:0:0:0:167.205.25.6 atau **::167.205.25.6**

0:0:0:0:0:ffff:167.205.25.7 atau **:ffff:167.205.25.7**

Jadi jika sekarang anda mengakses alamat di internet misalnya **167.205.25.6** pada saatnya nanti format tersebut akan digantikan menjadi semacam ***::ba67:080:18***. Sebagaimana IPv4, IPv6 menggunakan bit mask untuk keperluan subnetting yang direpresentasikan sama seperti representasi *prefix-length* pada teknik CIDR yang digunakan pada IPv4, misalnya :

3ffe:10:0:0:0:fe56:0:0/60

menunjukkan bahwa 60 bit awal merupakan bagian *network* bit.

Jika pada IPv4 anda mengenal pembagian kelas IP menjadi kelas A, B, dan C maka pada IPv6 pun dilakukan pembagian kelas berdasarkan ***fomat prefix*** (FP) yaitu format bit awal alamat. Misalnya :

```
3ffe:10:0:0:0:fe56:0:0/60
```

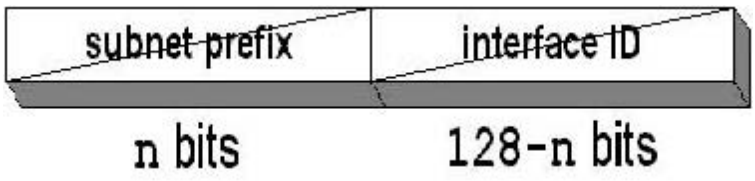
maka jika diperhatikan 4 bit awal yaitu hexa **'3'** didapatkan format prefixnya untuk 4 bit awal adalah **0011** (yaitu nilai '3' hexa dalam biner).

1.9 Kelas IPv6

Ada beberapa kelas IPv6 yang penting yaitu :

1. *Aggregatable Global Unicast Addresses* : termasuk di dalamnya adalah alamat IPv6 dengan bit awal **001**.
2. *Link-Local Unicast Addresses* : termasuk di dalamnya adalah alamat IPv6 dengan bit awal **1111 1110 10**.
3. *Site-Local Unicast Addresses* : termasuk di dalamnya adalah alamat IPv6 dengan bit awal **1111 1110 11**.
4. *Multicast Addresses :* termasuk di dalamnya adalah alamat IPv6 dengan bit awal **1111 1111**.

Pada protokol IPv4 dikenal alamat-alamat khusus semacam **127.0.0.1** yang mengacu ke *localhost*, alamat ini direpresentasikan sebagai **0:0:0:0:0:0:0:1** atau **::1** dalam protokol IPv6. Selain itu pada IPv6 dikenal alamat khusus lain yaitu **0:0:0:0:0:0:0:0** yang dikenal sebagai *unspecified address* yang tidak boleh diberikan sebagai pengenal pada suatu *interface.* Secara garis besar format *unicast address* adalah sebagai berikut :



Gambar 1-11 Format unicast address

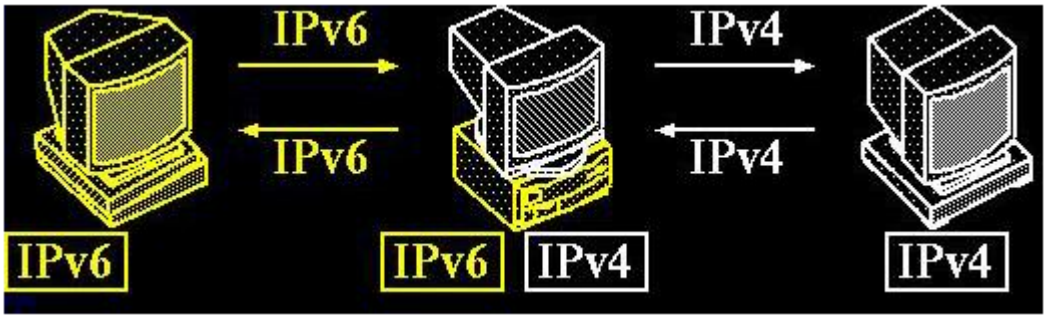
Interface ID digunakan sebagai pengenal unik masing-masing host dalam satu subnet. Dalam penggunaannya umumnya interface ID berjumlah 64 bits dengan format IEEE EUI-64. Jika digunakan media ethernet yang memiliki 48 bit MAC address maka pembentukan interface ID dalam format IEEE EUI-64 adalah sebagai berikut :

Misalkan MAC address-nya adalah 00:40:F4:C0:97:57

- Tambahkan 2 byte yaitu **0xFFFE** di bagian tengah alamat tersebut sehingga menjadi **00:40:F4:FF:FE:C0:97:57**
- Komplemenkan (ganti bit 1 ke 0 dan sebaliknya) bit kedua dari belakang pada byte awal alamat yang terbentuk, sehingga yang dikomplemenkan adalah **'00'** (dalam hexadesimal) atau **'00000000'** (dalam biner) menjadi **'00000010'** atau **'02'** dalam hexadesimal.
- Didapatkan interface ID dalam format IEEE EUI-64 adalah **0240:F4FF:FEC0:9757**

Tabel 1-3 Perbandingan IPv4 dan IPv6

Ipv4	Ipv6
Panjang alamat 32 bit (4 bytes)	Panjang alamat 128 bit (16 bytes)
Dikonfigurasi secara manual atau DHCP IPv4	Tidak harus dikonfigurasi secara manual, bisa menggunakan *address autoconfiguration.*
Dukungan terhadap IPSec opsional	Dukungan terhadap IPSec dibutuhkan
Fragmentasi dilakukan oleh pengirim dan pada router, menurunkan kinerja router.	Fragmentasi dilakukan hanya oleh pengirim
Tidak mensyaratkan ukuran paket pada link-layer dan harus bisa menyusun kembali paket berukuran 576 byte.	Paket link-layer harus mendukung ukuran paket 1280 byte dan harus bisa menyusun kembali paket berukuran 1500 byte
Checksum termasuk pada *header.*	Cheksum tidak masuk dalam *header*
Header mengandung *option*.	Data opsional dimasukkan seluruhnya ke dalam *extensions* *header*.
Menggunakan ARP Request secara broadcast untuk menterjemahkan alamat IPv4 ke alamat link-layer.	ARP Request telah digantikan oleh Neighbor Solitcitation secara multicast.
Untuk mengelola keanggotaan grup pada subnet lokal digunakan Internet Group Management Protocol (IGMP).	IGMP telah digantikan fungsinya oleh Multicast Listener Discovery (MLD).



Gambar 1-12 Network - tunneling (IPv6 transition)

1.10 Protokol Routing pada IPv6

Protokol *routing* yang digunakan pad a IPv6 adalah BGP4+ untuk external *routing* dan OSPFv6, RIPng untuk internal *routing*.

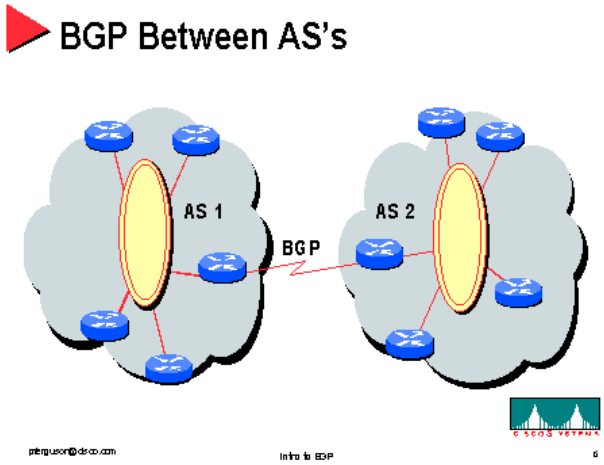
1.10.1 BGP4+

Border Gateway Protokol adalah *routing* protokol yang memakai system autonomous. Fungsi utama dari BGP adalah untuk saling tukar-menukar informasi konektivitas jaringan

antar BGP sistem. Informasi konektifitas ini antara lain adalah daftar dari Autonomous System (ASs). Informasi ini digunakan untuk membuat daftar *routing* sehingga terjadi suatu koneksi.

BGP4 mampu melakukan suatu advertaisement dan IP-prefix serta menghilangkan keterbatasan tentang network class. BGP memakai pola *Hop-by-Hop* yang artinya hanya meggunakan jalur yang berikutnya yang terdaftar dalam Autonomous System.

BGP menggunakan TCP sebagai media transport. BGP menggunakan port 179 untuk koneksi BGP. BGP mendukung CIDR.



Gambar 1-13 Model BGP

BGP mampu mempelajari jalur internet malalui internal atau eksternal BGP dan dapat memilih jalur terbaik dan memasukkannya dalam ip forwarding. BGP dapat digunakan pada dual maupun multi-homed, dengan syarat memiliki nilai AS. BGP tidak dapat digunakan pada single-homed.

Tabel 1-4 Format BGP Header

0 15		31
Marker		
Length	*Type*	Data

Type dari BGP:

1. OPEN, tipe pesan yang diterima sewaktu koneksi antar BGP tersambungkan.
2. UPDATE, tipe pesan yang dikirimkan untuk mengirimkan informasi *routing* antar BGP.
3. KEEPALIVE, tipe pesan yang dikirimkan untuk mengetahui apakah pasangan BGP masih hidup
4. NOTIFICATION, tipe pesan yang dikirimkan apabila terjadi error.

1.10.1.1 Atribut yang dimiliki oleh BGP:

AS_*path*, adalah jalur yang dilalui dan dicatat dalam data BGP route, dan dapat mendeteksi loop. *Next*_Hop, adalah jalur berikutnya yang akan dilalui dalam *routing* BGP, biasanya adalah local network dalam eBGP. Selain itu bisa didapat dari iBGP. Local Preference, penanda untuk AS BGP local Multi-Exit Discriminator (MED), bersifat non-transitif digunakan apabila memiliki eBGP yang lebih dari 1. Community, adalah sekumpulan

BGP yang berada dalam satu AS. Perbandingan BGP-4 antara yang digunakan untuk IPv4 dan IPv6 adalah kemampuan dari BGP yang dapat mengenali *scope* dari IPv6, yaitu *global, site-local, link-local*. Apabila IPv6 masih menggunakan IPv4 sebagai transport maka alamat *peer* pada BGP yang lainnya harus diikutkan pada konfigurasi.

1.10.2 RIPng

Routing Information Protocol *Next* Generation adalah protokol *routing* yang berdasarkan protokol *routing* RIP di IPv4 yang sudah mendukung IPv6. RIPng ini digunakan untuk internal *routing* protokol dan menggunakan protokol UDP sebagai transport. RIPng ini menggunakan port 521 sebagai komunikasi antar RIPng.

Metode yang dipakai RIPng adalah distance vector (vektor jarak), yaitu:

1. Jarak local network dihitung 0
2. Kemudian mencari neighbour sekitar dan dihitung jaraknya dan cost.
3. Dibandingkan jarak dan cost antar neighbour.
4. Dilakukan perhitungan secara kontinue.
5. Menggunakan algoritma Ballman-Ford.

Tabel 1-5 Format RIP header

Mac *header*	IPv6 *Header*	RIPng *Header*	Data

RIPng *Header*

0	15	31
Command	Version	0
Route entry		

Route entry

0	15	31
IPv6 prefix		
Route Tag	Prefix Length	Metric

Command pada RIPng *Header* berisi:

1. Request, meminta daftar tabel *routing* pada RIPng yang lain
2. Response, membalas request dari RIPng yang lain dan memberikan daftar *routing*.

Protokol RIPng ini memiliki beberapa kelemahan

1. Hanya bisa sampai 15 HOP
2. Lambat dalam memproses *routing*, dikarena melakukan pengecekan terus menerus
3. Bersifat Classful

Perbedaan yang terjadi antara RIP pada IPv4 (RIPv2) dan IPv6 (RIPng) adalah port UDP dimana pada IPv4 menggunakan port 520 sedangkan IPv6 menggunakan port 521 sebagai media transpor. RIPng hanya memiliki 2 perintah yaitu *response* dan *request*, berbeda dengan RIPv2 yang memiliki banyak perintah dan banyak yang tidak terpakai dan ada yang dibuang pada RIPng seperti authentifikasi. Perubahan yang terjadi dari RIPv2 ke RIPng antara lain, ukuran *routing* yang tidak lagi dibatasi, *subnet* IPv4 digantikan dengan *prefix* IPv6, next-

hop dihilangkan tetapi kegunaannya tidak dihilangkan, authentifikasi dihilangkan, namun kemampuan yang hanya sampai 15 hop masih sama.

1.10.3 OSPFv3

Open Shortest *Path* First adalah *routing* protokol yang digunakan pada IPv6. OSPF ini berdasarkan atas *Link*-state dan bukan berdasarkan atas jarak. Setiap *node* dari OSPF mengumpulkan data state dan mengumpulkan pada *Link* State Packet.

LSP dibroadcast pada setiap *node* untuk mencapai keseluruhan network. Setelah seluruh network memiliki "map" hasil dari informasi LSP dan dijadikan dasar *link*-state dari OSPF. Kemudian setiap OSPF akan melakukan pencarian dengan metode SPF (Shortest *Path* First) untuk menemukan jarak yang lebih efisien.

Routing table yang dihasilkan berdasarkan atas informasi LSP yang didapat sehingga OSPF memberikan informasi LSP secara flood, karena OSPF sudah memiliki kemampuan untuk memilih informasi LSP yang sama maka flood ini tidak mengakibat exhousted.

OSPF ini menggunakan protokol TCP bukan UDP, mendukung VLSM (Variable Length Subnet Mask).

OSPF menggunakan algoritma Shortest *Path* First (SPF) oleh Dijkstra, yaitu:

- Diasumsikan sudah ada data table sebelumnya. Data yang diperlukan antara lain *PATH* (ID, *path* cost, arah forwarding) TENTATIVE (ID, *path* cost, arah forwarding), Forwarding database.
- Taruh local sebagai root dari tree dengna ID,0,0 pada *PATH*
- Temukan *link* N dan taruh di *PATH*. Hitung jarak Root-N dan N-M, apabila M belum terdapat di *PATH* atau TENTATIVE, apabila nilainya lebih baik taruh di TENTATIVE.
- Apabila TENTATIVE bernilai kosong , batalkan. Lainnya, masukkan nilai TENTATIVE ke *PATH*.

Tabel 1-6 Format OSPF Header

Mac Addr	IP *header*	OSPF *Header*	Data
OSPF			
0	15		31
Version	*Type*	Length	
Router ID			
Area ID			
Checksum		Au*Type*	
Authentication			
Data			
OSPFv3			
0	15		31

Version	*Type*	Length	
Router ID			
Area ID			
Checksum		Instance ID	*Reserved*
Data			

Keterangan OSPF:

Version, 8 bit, diisi dengan dengan versi dari OSPF

Type, 8 bit, diisi dengan *Type* code dari OSPF yaitu:

1. Hello, untuk mengetahui adanya pasangan OSPF
2. Database Description, mengirimkan deskripsi dari OSPF
3. *Link* State Request, meminta data dari pasangan OSPF
4. *Link* State Update, mengupdate data table pada OSPF
5. *Link* State Aknowledgment, mengirimkan pesan error

Length, 16 bit, panjang header dan data dari OSPF

Router ID, 32 bit, Router ID dari source paket

Area ID, 32 bit, Area dari paket ini.

Checksum, 16 bit

AuType, 16 bit, model autentifikasi dari OSPF

Authentication, 64 bit, misal tanpa autenticasi, simple password, cryptographic password.

Keterangan untuk OSPFv3:

Version, 8 bit, diset 3

Checksum, 16 bit, CRC

Instance ID, 8 bit

Reserves, 8 bit diset 0

1.10.3.1 Perbandingan antara link-state daripada distance vector:

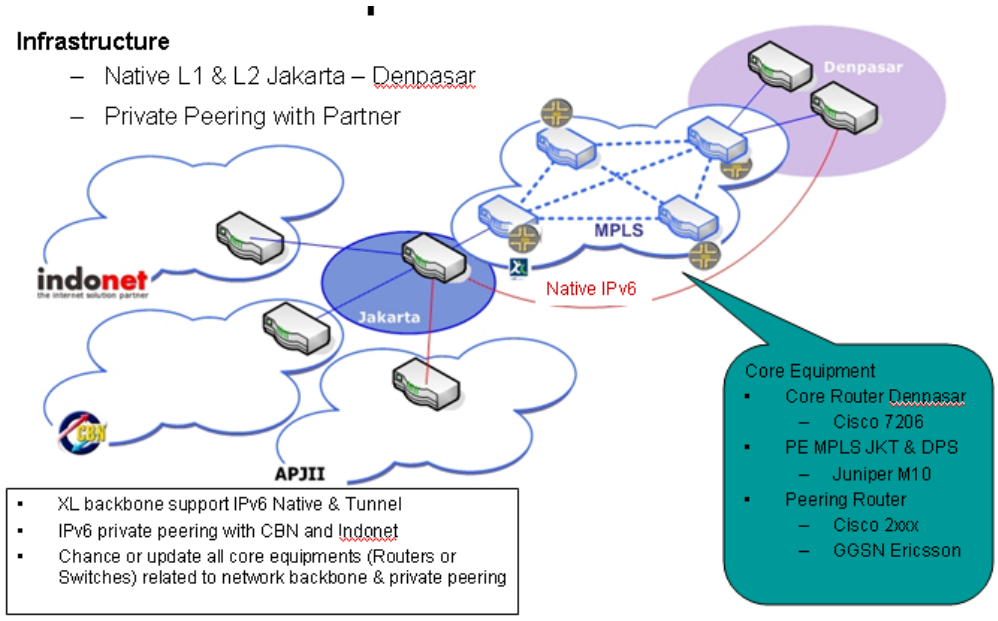
1. Konversi lebih cepat dari pada distance vector
2. Mudah dalam bentuk Topologi jaringan
3. Mudah dalam hal *Routing*
4. Bisa memiliki *routing* table yang komplek

1.10.3.2 Perbedaan yang terjadi antara OSPF IPv4 dengan OSPF IPv6 adalah:

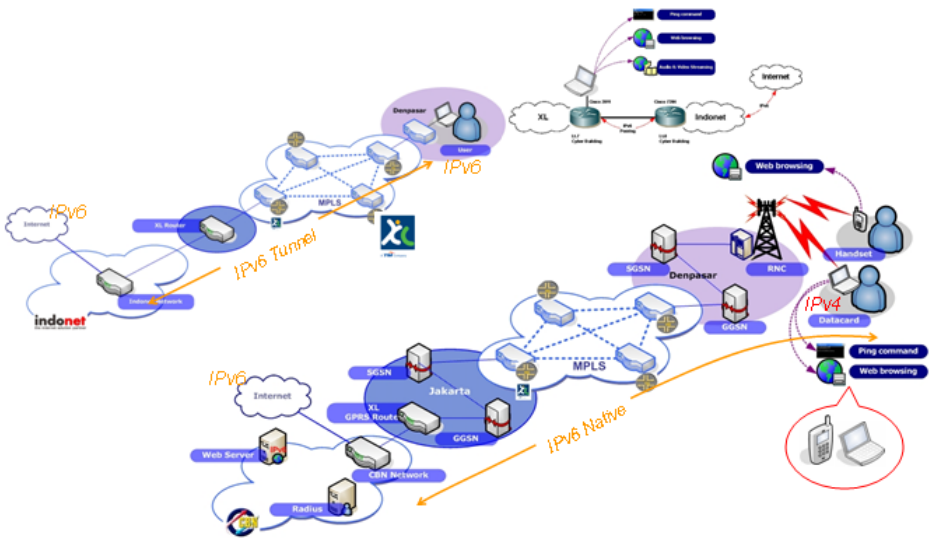
1. Komunikasi menggunakan *link-state* tidak menggunakan subnet.
2. Menghilangkan alamat semantic.
3. Menggunakan scope IPv6 yaitu: *link-local scope, area-scope, AS scope.*
4. Mendukung multi OSPF pada *link* yang sama.
5. Menggunakan alamat *link-local.*

6. Menghilangkan authentifikasi.
7. Perubahan format paket.

1.11 Contoh Infrastruktur IPv6



Gambar 1-14 Infrastruktur IPv6



Gambar 1-15 Infrastruktur IPv6

1.12 SOAL dan JAWABAN

1.12.1 Soal

1. Jelaskan secara singkat pengertian firewall beserta konfigurasi sederhananya!
2. Sebutkan dan jelaskan tentang tipe-tipe dari firewall!
3. Bagaimana langkah-langkah membangun firewall secara sederhana?
4. Apakah yang melatarbelakangi penggunaan NAT? Dan apa keuntungan menggunakan NAT?
5. Sebutkan komponen-komponen yang dimiliki oleh sebuah NAT!

1.12.2 Jawaban

1. Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya.

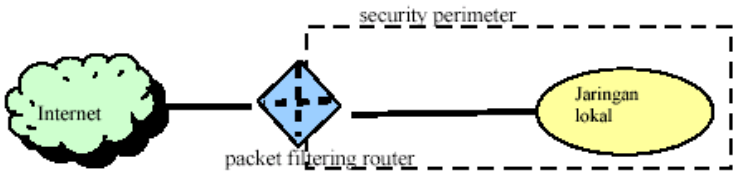
   Konfigurasi sederhananya:

   pc (jaringan local) == ***firewall*** == **internet** (jaringan lain)

2. a. Packet Filtering Router

   Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut.Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal(IP) dan alamat tujuan (IP), protokol transport yang digunakan(UDP,TCP), serta nomor port yang digunakan.

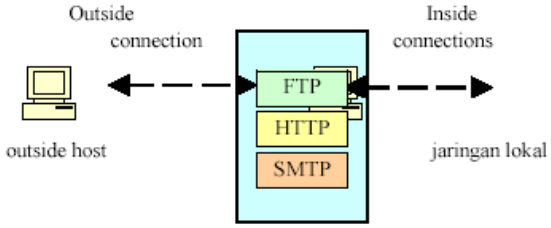
   Cara kerja Packet Filtering Router:



   b. Application-Level Gateway

   Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll.

   Cara kerja Packet Filtering Router:

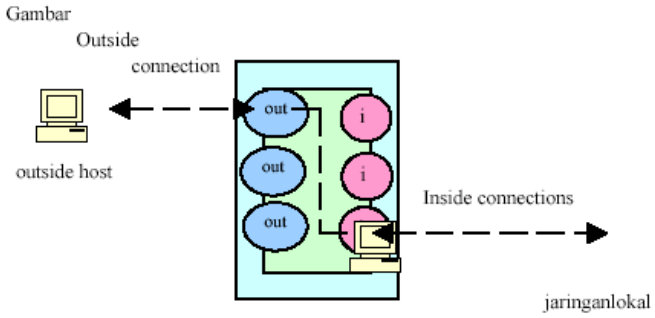


c. Circuit-level Gateway

Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung)

Cara kerja Packet Filtering Router:

Gambar



3. a. Mengidentifikasi bentuk jaringan yang dimiliki

   Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang di gunakan serta protocol jaringan.

   b. Menentukan Policy atau kebijakan

   Beberapa hal yang perlu diperhatikan:

   1. Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat
   2. Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut
   3. Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan
   4. Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
   5. Menerapkankan semua policy atau kebijakan tersebut

   c. Menyiapkan Software atau Hardware yang akan digunakan

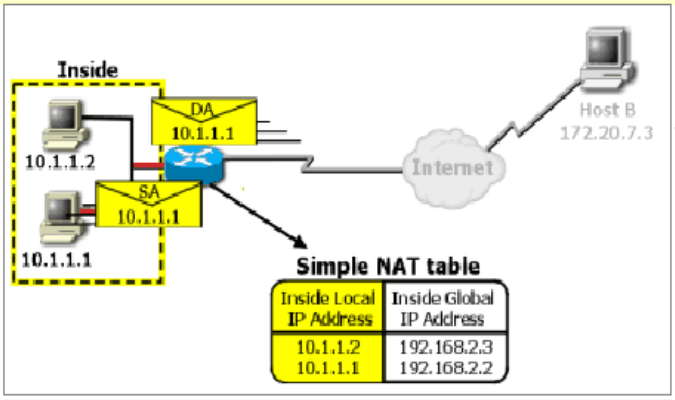
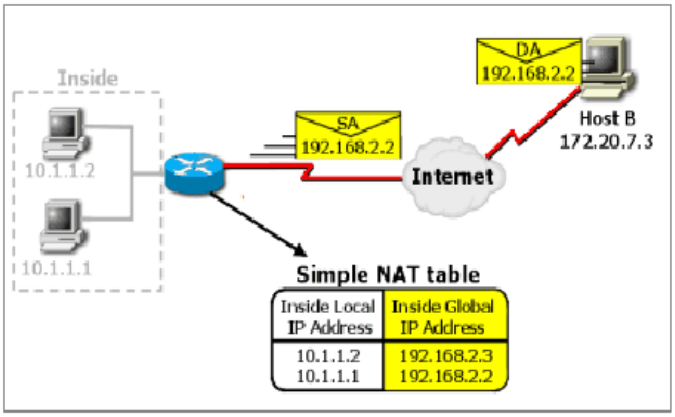
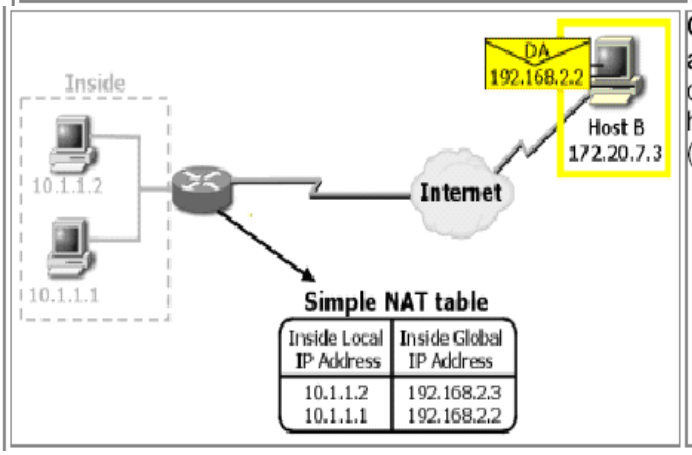
   d. Melakukan test konfigurasi

4 . I P *address* sebagai sarana pengalamatan di Internet semakin menjadi barang mewah dan ekslusif. Tidak sembarang orang sekarang ini bisa mendapatkan IP *address* yang valid dengan mudah. Oleh karena itulah dibutuhkan suatu mekanisme yang dapat menghemat IP *address*. Logika sederhana untuk penghematan IP *address* ialah dengan meng-*share* suatu nomor IP *address* valid ke beberapa *client* IP lainnya. Atau dengan kata lain beberapa komputer bisa mengakses Internet walau kita hanya memiliki satu IP *address* yang valid.

Keuntungannya, jika anda harus merubah IP internal anda dikarenakan anda berganti ISP atau dua intranet digabungkan (misalnya penggabungan dua perusahaan), NAT dapat digunakan untuk mentranslasikan alamat IP yang sesuai. NAT memungkinkan anda menambah alamat IP,

tanpa merubah alamat IP pada host atau komputer anda. Dengan demikian akan menghilangkan duplicate IP tanpa pengalamatan kembali host atau komputer anda.

5. Komponen NAT:

Gambar	Keterangan
	**Inside local IP address** – Alamat IP yang di set untuk sebuah host pada jaringan lokal (inside network). Pengalokasian alamat IP harus unik dan dalam satu subnet yang sama.
	**Inside global IP address** – Sebuah alamat IP legal (ditetapkan oleh NIC atau service provider) yang mewakili satu atau lebih alamat IP inside lokal ke dunia luar. Alamat IP ini dialokasikan dari kapasitas alamat global yang unik. Biasanya disediakan oleh Internet Service Provider (ISP).
	**Outside global IP address** – Alamat IP yang ditetapkan untuk sebuah host pada jaringan luar (outside network).

1.13 REFERENSI

[1] Uswatun Hasanah, Ria Puspitasari, “Laporan Kerja Praktek Shorewall”, 2007

[2] Sugiharta Tito, “Network Address Translation (NAT): Cara lain menghemat IP Address”, Laboratorium Sistem Informasi & Keputusan (LSIK) ,Teknik Industri ITB, Tito@TI.ITB.ac.id

[3] Triswikuharso Teguh, “Firewall dan NAT”, 1999

[4] Eueung Mulyana & Onno W. Purbo, “Firewall—Security Internet”, 2001 klik kanan

[5] **Tom Eastep, “** One-to-one NAT”, Copyright ©2001- 2004 Thomas M.Eastep

[6] www.ilmukomputer.com

[7] http://id.wikipedia.org/wiki/Network_address_translation

BAB 2. MULTI PROTOCOL LABEL SWITCHING (MPLS)

Ajeng Dwi Ayu Listari [1)], Atik Nur Faridah [1)], Pras Septiono [1)]

[1)] Politeknik Elektronika Negeri Surabaya

ABSTRAK

Seiring dengan kemajuan teknologi informasi dan telekomunikasi, maka kebutuhan terhadap suatu jaringan akan semakin meningkat, terutama untuk menghubungkan jaringan yang satu dengan jaringan yang lain, dimana kedua tempat jaringan tersebut letaknya saling berjauhan, maka untuk menghubungkan keduanya agar terjadi suatu koneksi yang lebih cepat dan lebih baik maka diperlukan suatu jalur yang dinamakan Multi Protocol Label Switching (MPLS).

Seperti kita ketahui bersama bahwa MPLS adalah suatu teknologi penyampaian paket pada jaringan backbone (jaringan utama) berkecepatan tinggi yang menggabungkan beberapa kelebihan dari sistem komunikasi circuit-switched dan packet switched yang melahirkan teknologi yang lebih baik dari keduanya. MPLS bekerja pada packets dengan MPLS header, yang berisi satu atau lebih label. Header MPLS terdiri atas 32 bit data, termasuk 20 bit label, 2 bit eksperimen, dan 1 bit identifikasi stack, serta 8 bit TTL. Label pada MPLS digunakan untuk proses forwarding, termasuk proses traffic engineering.

Diharapkan dengan adanya jalur MPLS tersebut maka suatu jaringan dapat terhubung dan terkoneksi dengan mudah dan diharapakan proses pengaksesannya bisa lebih cepat dan lebih baik.

2.1 Pengertian MPLS

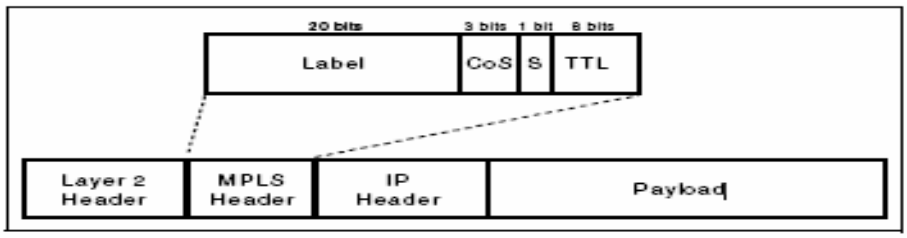
Multiprotocol Label Switching (MPLS) [1] adalah teknologi penyampaian paket pada jaringan backbone (jaringan utama) berkecepatan tinggi yang menggabungkan beberapa kelebihan dari sistem komunikasi circuit-switched dan packet-switched yang melahirkan teknologi yang lebih baik dari keduanya.

Multiprotocol Label Switching (MPLS) [2] adalah arsitektur network yang didefinisikan oleh IETF untuk memadukan mekanisme label swapping di layer 2 dengan routing di layer 3 untuk mempercepat pengiriman paket.

Paket-paket pada MPLS diteruskan dengan protokol routing seperti OSPF, BGP atau EGP. Protokol routing berada pada layer 3 sistem OSI, sedangkan MPLS berada di antara layer 2 dan 3. OSPF (Open Shortest Path First) adalah routing protocol berbasis link state (dilihat dari total jarak) setelah antar router bertukar informasi maka akan terbentuk database pada masing – masing router. BGP (Border Gateway Protocol) adalah router untuk jaringan external yang digunakan untuk menghindari routing loop pada jaringan internet.

2.2 Header MPLS

MPLS bekerja pada packets dengan MPLS header, yang berisi satu atau lebih labels. Ini disebut dengan label stack. Header MPLS dapat dilihat pada Error: Reference source not found dibawah ini:



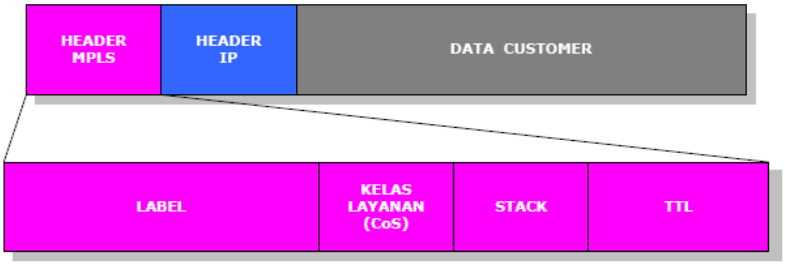
Gambar 2-16. Header MPLS

MPLS Header meliputi :

1. 20-bit label value : Suatu bidang label yang berisi nilai yang nyata dari MPLS label.
2. 3-bit field CoS : Suatu bidang CoS yang dapat digunakan untuk mempengaruhi antrian packet data dan algoritma packet data yang tidak diperlukan.
3. 1-bit *bottom of stack* flag : Jika 1 bit di-set, maka ini menandakan label yang sekarang adalah label yang terakhir. Suatu bidang yang mendukung hirarki label stack.
4. 8-bit TTL (time to live) field. Untuk 8 bit data yang bekerja.

2.3 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*. Untuk mengetahui enkapsulasi paket pada MPLS dapat dilihat pada Error: Reference source not found dibawah ini:



Gambar 2-17 Enkapsulasi Paket MPLS

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.

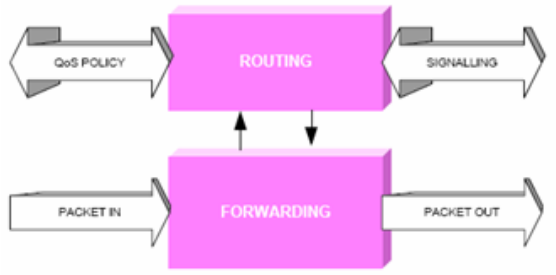
Selain paket IP, paket MPLS juga bisa dienkapsulasikan kembali dalam paket MPLS. Maka sebuah paket bisa memiliki beberapa header. Dan bit stack pada header menunjukkan apakah suatu header sudah terletak di 'dasar' tumpukan header MPLS itu.

2.4 Arsitektur MPLS

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 dapat dilihat pada Error: Reference source not found.

Network MPLS terdiri atas sirkit yang disebut *label-switched path* (LSP), yang menghubungkan titik-titik yang disebut *label-switched router* (LSR).

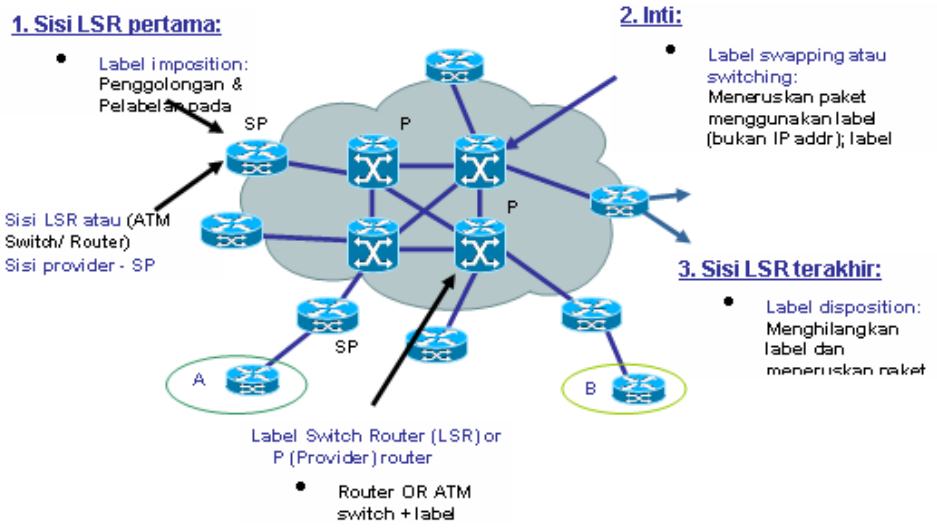
Setiap LSP dikaitkan dengan sebuah *forwarding equivalence class* (FEC), yang merupakan kumpulan paket yang menerima perlakukan *forwarding* yang sama di sebuah LSR. FEC diidentifikasikan dengan pemasangan label.



Gambar 2-18 Arsitektur MPLS

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

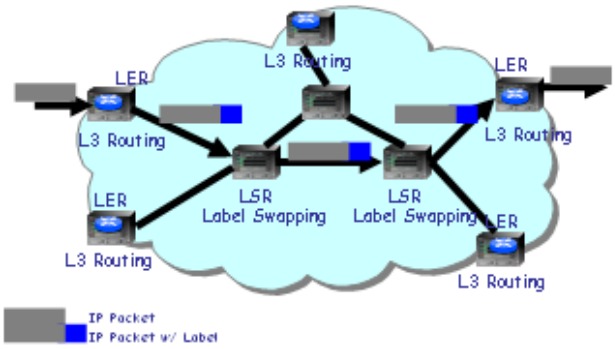
2.5 MPLS Network Arsitektur



Gambar 2-19. MPLS Network Arsitektur

1. Penggolongan dan pemberian label pada packet. Setelah itu packets akan menuju provider (P). Dari provider, packet akan diteruskan ke inti.
2. Pada inti, packet diteruskan berdasarkan label bukan berdasarkan pada IP address. Label ini menunjukkan penggolongan class (A, B, C, D) dan tujuannya.
3. Menghilangkan label dan meneruskan packet pada sisi penerima.

2.6 MPLS Cloud



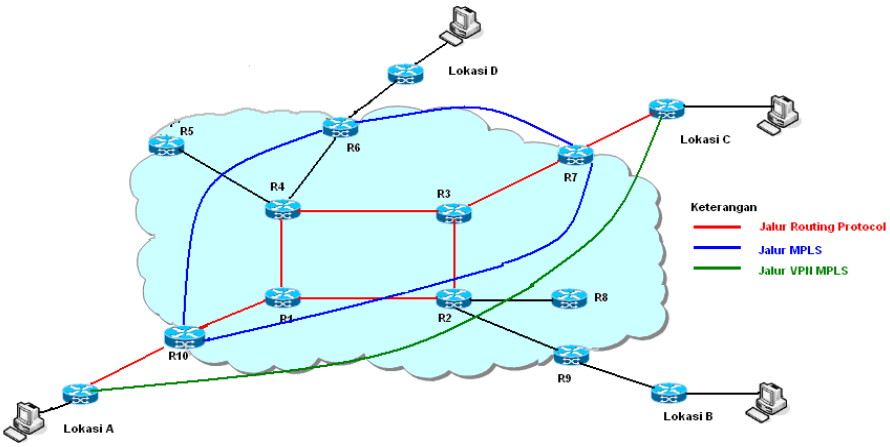
Gambar 2-20 MPLS Cloud

Keterangan :

1. LER : Label Edge Router (label pada sisi router)
2. LSR : Label Switch Router (label pada switch router)
3. FEC : Forward Equivalence Class, meneruskan packets pada class yang sama.
4. Label : menghubungkan suatu packet dalam FEC.
5. Label Stack : berbagai label yang berisi informasi tentang bagaimana packets akan diteruskan.
6. Label Switch Path : jejak packets untuk mengarahkan ke FEC tertentu.
7. LDP : Label Distribution Protocol, digunakan untuk mendistribusikan informasi label diantara MPLS dengan perangkat jaringan.
8. Label Swapping : berfungsi memanipulasi label untuk meneruskan packets sampai ke tujuan.

2.7 Contoh Penggunaan MPLS Pada Jaringan

MPLS biasa digunakan pada jaringan. Berikut ini merupakan contoh penggunaan MPLS pada jaringan yang dapat dilihat pada Gambar 2 -21.



Gambar 2-21. Topologi jalur MPLS

Keterangan :

Misalnya kita akan menghubungkan antara jaringan di Lokasi A dengan jaringan di Lokasi C maka kita dapat melakukannya dengan beberapa cara misalnya melalui jalur routing protocol ataupun melalui jalur MPLS.

2.7.1 Dengan Jalur Routing Protocol :

Jalur dari Lokasi A akan menuju ke R10 (Router 10) lalu menuju ke R1 (Router 1) selanjutnya ke R2 (Router 2) atau ke R4 (Router 4) kemudian jalurnya menuju ke R3 (Router 3) setelah itu ke R7 (Router 7) dan akhirnya langsung ke Lokasi C. Routing Protocol yang bisa digunakan antara lain yaitu OSPF, BGP dan RIP. Jalur internet yang menghubungkan antara Lokasi A dengan Lokasi C apabila menggunakan routing protocol akan memerlukan waktu yang lebih lama dibandingkan dengan jalur MPLS karena dengan routing protocol jalur yang dilewati lebih banyak.

2.7.2 Dengan Jalur MPLS :

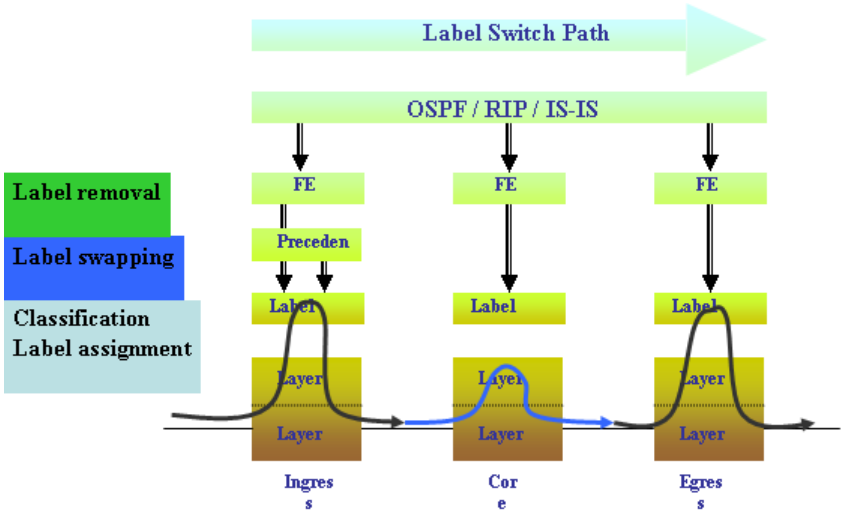
Jalur internet dari Lokasi A yang terhubung ke Lokasi C akan dihubungkan dengan jalur MPLS, dimana MPLS (Multi Protocol Label Switching) ini menggunakan teknologi seperti yang digunakan oleh ATM (Asynchronous Transfer Mode) yaitu Virtual Tunnel. Jalur yang terhubung dari Lokasi A akan menuju ke R10 (Router 10), dimana pada router ini akan terjadi proses penggolongan dan pemberian packet, setelah itu packet akan diteruskan langsung menuju ke R7 (Router 7), pada router ini terjadi proses penghilangan label dan packet akan diteruskan ke jaringan pada Lokasi C.

2.7.3 Dengan VPN MPLS:

VPN sama halnya dengan jalur MPLS, bedanya hanya data yang dikirim di enkripsi untuk menjaga keprivasian datanya. Selain itu dengan VPN MPLS dapat lebih singkat jalurnya hanya dengan menghubungkan Router di Lokasi A dengan Lokasi C.

2.8 Proses Pada MPLS

Untuk mengetahui proses switching yang terjadi pada MPLS dapat diketahui dengan Gambar 2 -22 [4] dibawah ini:



Gambar 2-22. Proses Switching pada jaringan MPLS

1. Prinsip kerja MPLS ialah menggabungkan kecepatan switching pada layer 2 dengan kemampuan routing dan skalabilitas pada layer 3.
2. Cara kerjanya adalah dengan menyelipkan label di antara header layer 2 dan 3 pada paket yang diteruskan.
3. Label dihasilkan oleh Label-Switching Router dimana bertindak sebagai penghubung jaringan MPLS dengan jaringan luar.
4. Label berisi informasi tujuan node selanjutnya kemana paket harus dikirim, kemudian paket diteruskan ke node berikutnya, di node ini label paket akan dilepas dan diberi label yang baru yang berisi tujuan berikutnya.
5. Paket-paket diteruskan dalam path yang disebut LSP (Label Switching Path).

2.9 Standarisasi Protokol MPLS

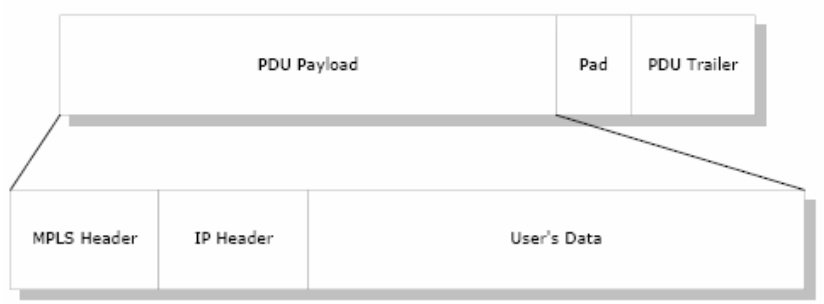
Ada dua standardisasi protokol untuk memanage alur MPLS yaitu:

1. CR-LDP (Constraint-based Routing Label Distribution Protocol)
2. RSVP-TE, suatu perluasan protocol RSVP untuk traffic rancang-bangun.
   a. Suatu header MPLS tidak mengidentifikasi jenis data yang dibawa pada alur MPLS.
   b. Jika header membawa 2 tipe jalur yang berbeda diantara 2 router yang sama, dengan treatment yang berbeda dari masing – masing jenis core router, maka header MPLS harus menetapkan jalurnya untuk masing – masing jenis traffic.

2.9.1 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 oleh customer. Gambar 2 -23 merupakan gambaran pada MPLS Over ATM.



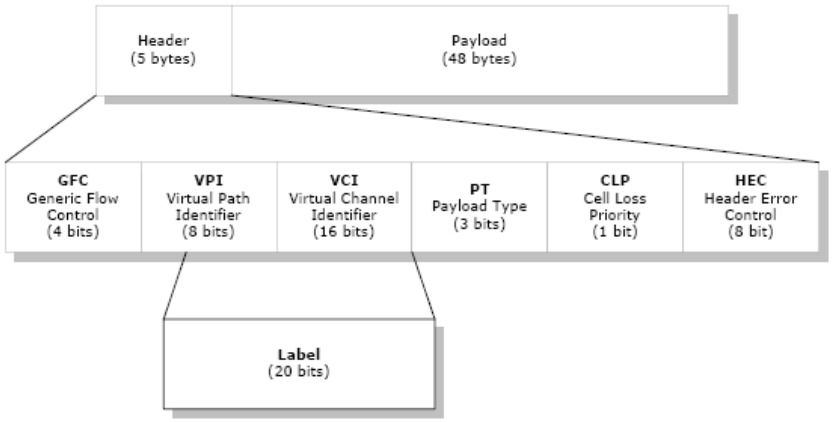
Gambar 2-23. MPLS Over ATM

- Seperti paket IP, paket MPLS akan dienkapsulasikan ke dalam AAL 5, kemudian dikonversikan menjadi sel – sel ATM.
- Kelemahan sistem MPLS over ATM ini adalah bahwa keuntungan MPLS akan berkurang, karena banyak kelebihannya yang akan *overlap* dengan keuntungan ATM. Alternatif ini sangat tidak cost-effective.

2.9.2 HIBRIDA MPLS-ATM

Hibrida MPLS-ATM adalah sebuah network yang sepenuhnya memadukan jaringan MPLS di atas core network ATM. MPLS dalam hal ini berfungsi untuk 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 pada Error: Reference source not found berikut ini.



Gambar 2-24 Hibrida MPLS-ATM

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.

2.9.3 LABEL DAN LABELED PACKET

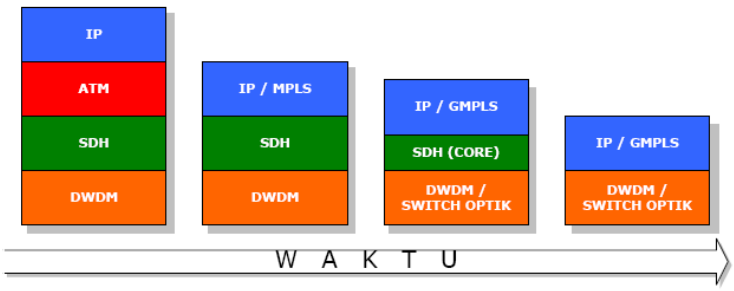
1. Peralatan MPLS memforward ke semua packet yang diberi label dengan cara yang sama.
2. Suatu label berada di tempat yang significant diantara sepasang peralatan MPLS.
3. MPLS label dapat diletakkan pada posisi yang berbeda di dalam data frame, tergantung pada teknologi layer-2 yang digunakan untuk transport. Jika teknologi layer 2 mendukung suatu label, MPLS label adalah encapsulated bidang label yang asli.

Jika teknologi layer 2 tidak secara asli mendukung suatu label, maka MPLS label terletak pada suatu encapsulasi header.

2.9.4 GMPLS

GMPLS (*Generalized MPLS*) [5] 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 digunakan 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. Proses enkapsulasi pada GMPLS dapat dilihat pada Error: Reference source not found berikut ini.



Gambar 2-25 Proses Enkapsulasi GMPLS

2.10 Implementasi MPLS

MPLS bersifat alami bagi dunia IP. Traffic engineering pada MPLS memperhitungkan sepenuhnya karakter traffic 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 memperlukan hal-hal itu .

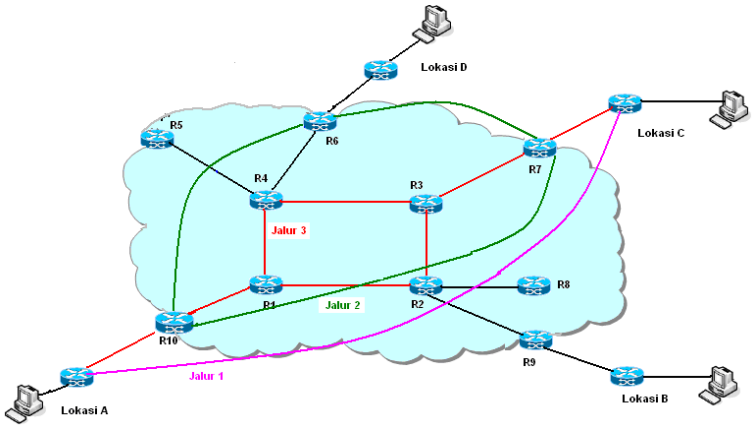
Persoalan besar dengan MPLS adalah bahwa hingga saat ini belum terbentuk dukungan untuk traffic non IP. Skema-skema L2 over MPLS (termasuk Ethernet over MPLS, ATM over MPLS, dan FR over MPLS) sedang dalam riset yang progressif, tetapi belum masuk ke tahap pengembangan secara komersial. Yang cukup menjadikan harapan adalah banyaknya alternatif konversi berbagai jenis traffic ke dalam IP, sehingga traffic jenis itu dapat pula diangkut melalui jaringan MPLS.

2.11 SOAL-SOAL

1. Bagaimana jaringan MPLS dapat menyampaikan paket atau data sampai ke Border Gateway Protocol (BGP) tujuan?

   MPLS memungkinkan untuk meneruskan paket ke BGP tujuan dengan mencocokkan labelnya dan mengirimkannya pada BGP berikutnya. BGP berikutnya harus dapat dicapai melalui IGP yang telah digabung dengan label MPLS. Hal ini memungkinkan router ISP hanya berjalan pada IGP. Router ISP PE menjadi salah satu yang diperlukan untuk menjalankan BGP.

2. Dari gambar suatu jaringan dibawah ini, manakah yang merupakan jalur untuk MLPS?

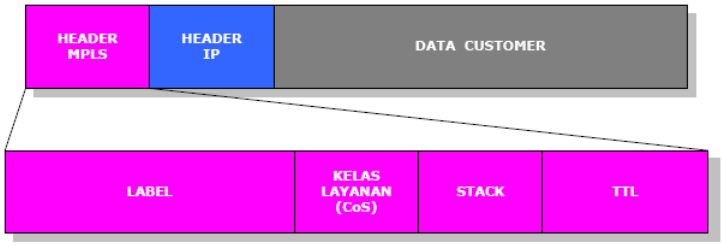


   Yang merupakan jalur untuk MPLS adalah jalur 2. Karena pada jalur 2, jalur untuk internet dari Lokasi A yang terhubung ke Lokasi C akan dihubungkan dengan jalur MPLS, dimana MPLS (Multi Protocol Label Switching) ini menggunakan teknologi seperti yang digunakan oleh ATM (Asynchronous Transfer Mode) yaitu Virtual Tunnel. Jalur yang terhubung dari Lokasi A akan menuju ke R10 (Router 10), dimana pada router ini akan terjadi proses penggolongan dan pemberian packet, setelah itu packet akan diteruskan langsung menuju ke R7 (Router 7), pada router ini terjadi proses penghilangan label dan packet akan diteruskan ke jaringan pada Lokasi C.

3. Bagaimana proses terjadinya enkapsulasi paket pada MPLS dan coba gambarkan enkapsulasi paket pada MPLS ?

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

Berikut ini adalah gambaran enkapsulasi paket pada MPLS.



4. Apa keuntungan kita menggunakan MPLS dalam membangun suatu jaringan ?

   Keuntungan pertama adalah MPLS tidak menggunakan kerumitan teknis, seperti enkapsulasi ke dalam AAL dan pembentukan sel-sel ATM yang masing-masing menambah delay, menambah header, dan memperbesar kebutuhan bandwidth. Keuntungan kedua adalah traffic engineering pada MPLS memperhitungkan sepenuhnya karakter traffic IP yang melewatinya.

5. Mengapa MPLS Over ATM digunakan pada jaringan?

   Karena MPLS over ATM merupakan salah satu 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 oleh customer.

2.12 REFERENSI

[1] Wikipedia, “MPLS”, http://www.wikipedia.org/wiki/MPLS

[2] KuncoroWastuwibowo, “PengantarMPLS”, Copyright©2003 lmuKomputer.com

[3] Michael Behringer and Monique Morrow, “04_MPLS_Security_MCWG_v02.ppt”, 2006, http://www.google.co.id

[4] Pramoda Nallur, “mpls_2.ppt”, 2000, http://www.google.co.id

[5] GMPLS. http://www.google.co.id

BAB 3. MOBILE IP

Bagus Lumaksono [1)], Rizal Aulia Firmansyah[1)]

[1)]Politeknik Elektronika Negeri Surabaya

ABSTRAK

Semakin pesat perkembangan teknologi komunikasi dan informasi terutama dalam bidang komunikasi wireless sehingga semakin hari kebutuhan akan mobile semakin tinggi. Sedangkan untuk setiap perpindahan jaringan terjadi perubahan nomor IP(internet protocol). Dengan demikian diperlukan sebuah teknologi yang bisa melakukan fungsi untuk tidak merubah alamat IP meskipun berpindah dari suatu jaringan dengan jaringan lainnya. Teknologi yang bisa melakukan fungsi itu adalah Mobile IP. Dimana dalam teknologi ini ketika sebuah host berpindah dari jaringan satu ke lainnya maka tidak mengalami perubahan IP. Dengan kata lain sebuah host akan mempunyai alamat yang tetap meskipun selalu berpindah jaringan. Semakin bertambahnya host yang berada pada suatu jaringan computer mengakibatkan kebutuhan akan IP semakin meningkat sehingga untuk memenuhi kebutuhan itu diperlukan adanya alokasi IP yang lebih banyak. Untuk itu dalam teknologi Mobile IP ini terdapat ada dua model, yaitu untuk mobile IP versi 4 dan mobile IP versi 6. Mobile IP versi 6 ini mendukung adanya koneksi yang lebih cepat karena didukung dengan adanya teknologi tunneling. Yaitu bidirectional tunnel dan route optimation. Dengan adanya Mobile IP ini diharapkan akan lebih memudahkan dalam pengaturan IP.

3.1 Mobilitas Pada Internet Protocol

Dalam jaringan internet yang menggunakan kabel, ditetapkan bahwa alamat IP mengidentifikasikan secara unik titik node yang terhubung pada internet. Karena itu sebuah sebuah note harus ditempatkan pada jaringan yang diidentifikasikan oleh alamat IP nya dalam rangka untuk menerima datagram yang ditujukan kepadanya jika tidak, datagram yang ditujukan kepada node tidak akan terkirim. Untuk sebuah node yang merubah point of attachmentnya tanpa kehilangan kemampuan untuk berkomunikasi, maka salah satu dari dua mekanisme berikut harus dilakukan:

- Node harus merubah alamat IP nya ketika node merubah titik hubungnya ke internet.
- Rute tertentu host harus disebarkan ke seluruh perusahaan penyedia internet.

Kedua alternatif ini sering tidak dapat diterima. Alternative pertama membuat ini menjadi tidak mungkin bagi sebuah node untuk menjaga sambungan layer transport dan layer yang lebih tinggi ketika node merubah lokasinya. Alternartif kedua secara jelas akan menjadi masalah. Karena ini diperlukan sebuah mekanisme baru untuk mengakomodasi mobilitas node dalam internet yang memungkinkan node merubah attachmentnya dengan internet tanpa merubah alamat IP nya.

Fitur dari mobile IP ini diantaranya yaitu :

1. Support Host yang berpindah-pindah.
2. Tidak ada batasan geografis
3. Tidak ada modifikasi terhadap nomor IP
4. Keamanan jaringan terjamin

3.2 Mobile IPv4 (MIPv4)

Mobile IP dimaksuidkan untuk memugkinkan node-node untuk berpindah dari satu subnet IP ke subnet IP lainnya. Ini semua cocoknya baik untuk mobilitas dalam media homogen maupun dalam media yang heterogen. Mobile IP memfasilitasi perpindahan node dari satu segmen ethernet ke ethernet lainnya sama baiknya dengan mengakomodasi perpindahan node dari satu segment ethernet ke wireless LAN, selama alamat IP tetap sama setelah perpindahan.

Mobile IP diibaratkan sama dengan logika pada post office yang terjadi dalam kehidupan sehari-hari. Disini terdapat beberapa entiti yang berbeda yaitu own post-office atau post office yang lama dalam mobile IP dikenal dengan istilah Home Network dimana untuk mendukung kerja dari home network maka didalamnya juga terdapat sebuah router yang dikenal dengan Home Agent. Post-office selanjutnya disebut dengan sebutan new post-office atau post-office baru yang akan dituju, dalam mobile IP ini dengan Foreign Network dan sama seperti pada home network, dalam foreign network juga terdapat sebuah router yang dikenal dengan Foreign Agent.

Dimana host yang selalu berpindah-pindah jaringan dikenal dengan Mobile Host. Diman host ini akan melakukan registrasi dengan home agent ketika berada pada lokasi baru atau Foreign Network. Sedangkan Home Agent dalam home network juga akan mengontrol paket untuk mobile host, dan meneruskannya ke foreign agent, yang kemudian dikirimkan ke mobile host. Untuk lebih jelasnya akan dijelaskan pada arsitektur dan cara kerja dari Mobile IP pada subbab selajutnya.

3.2.1 Arsitektur Mobile IPv4

Mobile IP memperkenalkan beberapa entities fungsional yang baru, yaitu:

1. Mobile Host

   Sebuah host atau router yang merubah point dari attachmentnya dari sebuah network atau subnetwork ke lainnya. Sebuah mobile node dapat merubah alamat IP nya. Ini dapat melanjutkan komunikasi dengan node internet lainya pada beberapa lokasi menggunakan alamat IP yang konstan, diandaikan konektifitas link layer ke point dari attachment yang tersedia.
2. Corresponding Host

   Adalah host lawan dari mobile host ketika ia berada pada jaringan selanjutnya, yaitu foreign network yang didalamnya terdapat Home Agent.
3. Care of Address

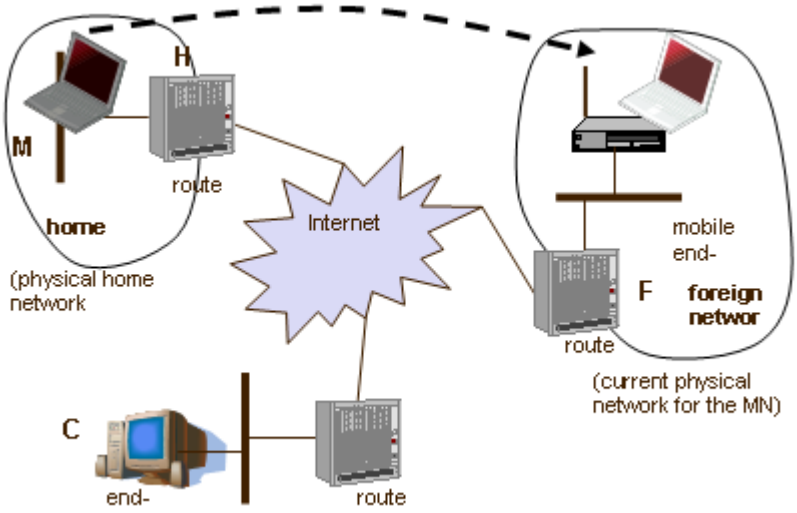
   Address yang dimiliki Mobile Host ketika dia berada pada jaringan tujuannya, yaitu foreign network yang didalamnya terdapat Foreign Agent.
4. Home Agent

   Sebuah router pada jaringan mobile node home yang membuka jalur datagram untuk pengiriman ke mobile node ketika ia jauh dari home dan menjaga informasi lokasi yang sekarang ke mobile node.
5. Foreign Agent

   Sebuah router pada jaringan mobile node yang dikunjungi menyediakan layanan routing mobile node sementara ia diregistrasi. Foreign agent menutup jalur dan mengirimkan datagram ke mobile node yang telah dibuka jalurnya oleh mobile node home agent. Untuk datagram yang dikirim oleh

mobile node, foreign agent dapat melayani seperti default router untuk mobile node yang telah diregitrasi.

Sebuah mobile node diberikan alamat IP yang panjang pada sebuah home home network. Home address ini diadministrasikan dengan cara yang sama seperti alamat IP yang tetap yang disediakan oleh host yang tetap. Ketika jauh dari home network, sebuah care-of address dihubungkan dengan mobile node dan mencerminkan mobile node point of attachment yang sekarang.



Gambar 3-26 Terminologi mobile IPv4

Keterangan :

M : Mobile host

C : Corespondent Host

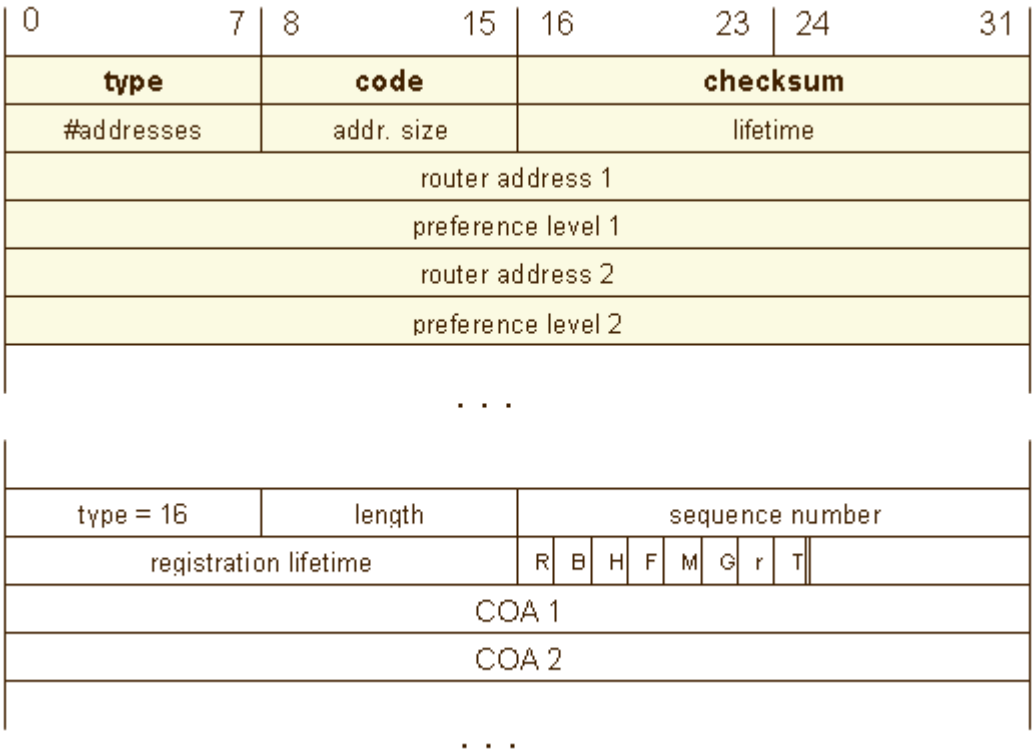
H : Home Agent

F : Foreign Agent

3.3 Operasi Pada MIPv4

Secara umum langkah-langkah operasi pada MIPv4 adalah sebagai berikut:

1. Agent Mobilitas (home agent dan foreign agent) memberitahukan kehadirannya melalui pesan-pesan Agent Advertisment. Sebuah mobile node dapat secara opsional meminta sebuah pesan. Agent Advertisement dari agen mobilitas yang berada di area local melalui pesan Agent Solicitation.



Gambar 3-27 Agent Advertisement

Keterangan :

Type = 16

Length = 6+4 *COAs

R : registration required

B : busy, no more registrations

H : home agent

F : foreign agent

M : minimal encapsulations

G :GRE encapsulations

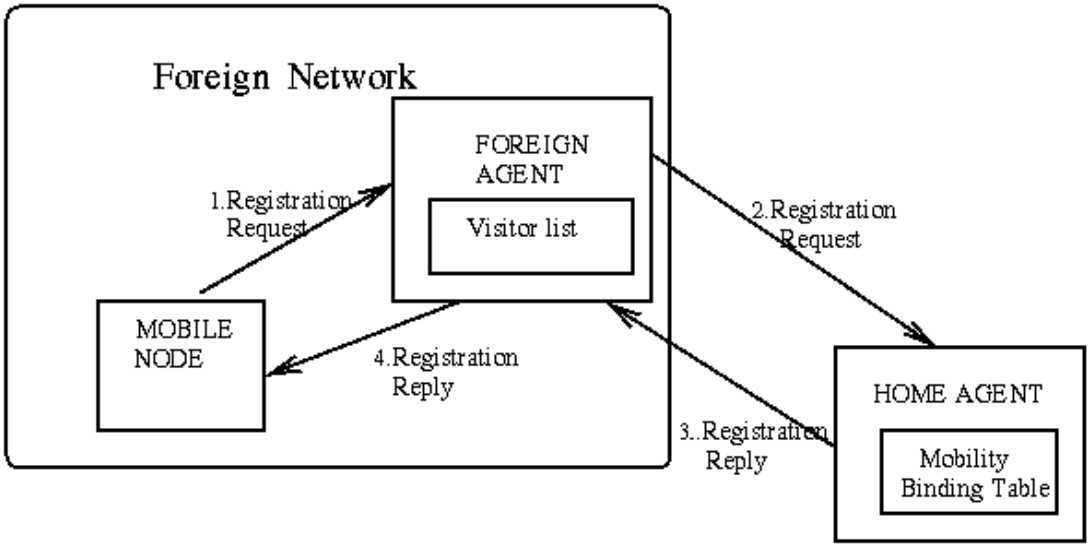
R = 0, ignored (former Van Jacobson compression)

T : FA support reverse tunneling

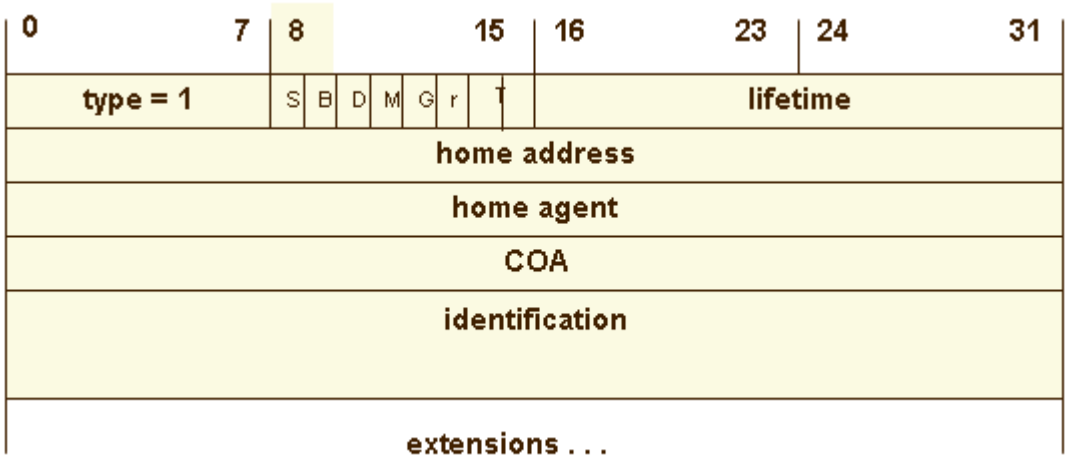
Reserved : = 0, ignored

2. Mobile node menerima Agent Advertisement ini dan menentukan apakah ini berada pada home network atau berada di foreign network.
3. Ketika mobile node mendeteksi bahwa ini berada pada networknya, ini beroperasi tanpa layanan mobilitas. Jika mobile node baru kembali ke home networknya dan telah diregistrasi di tempat lain, mobile node akan diregistrasi kembali oleh home agentnya melalui pertukaran pesan Registration Request dan Request Reply dengannya.

Analogi registrasi pada gambar di bawah ini :



Gambar 3-28 Proses Registrasi



Gambar 3-29 Registration request

Keterangan :

S : simultaneous bindings

B : broadcast datagram

D : decapsulations oleh MN

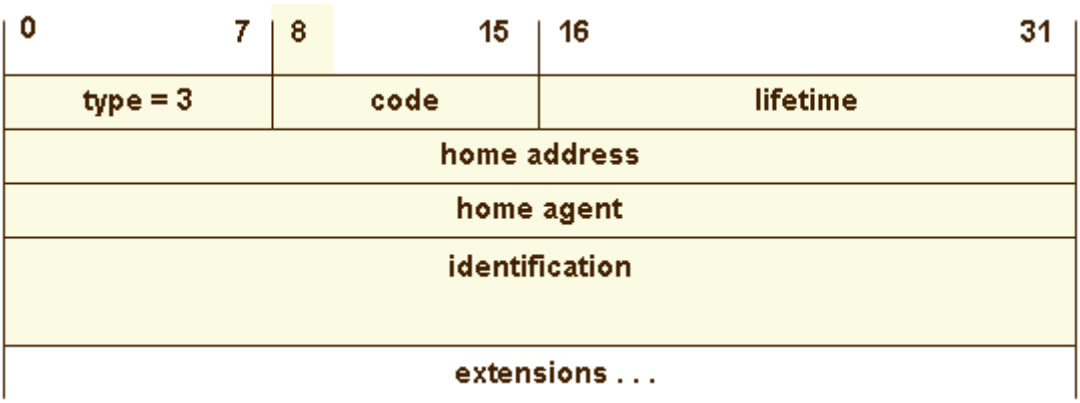
M : minimal encapsulations

G : GRE encapsulations

r : =0, ignored

T : reverse tunneling requested

x : =0, ignored



Gambar 3-30 Registration replay

Keterangan :

Example codes :

Registration succesful

0 registration accepted

1 registration accepted, but simultaneous mobility bindings unsuported

Registration denied by FA

65 administravely prohibited

66 insufficient resources

67 mobile node failed authentication

68 home agent failed authentication

69 requested Lifetime too long

Registration denies by HA

129 administratively prohibited

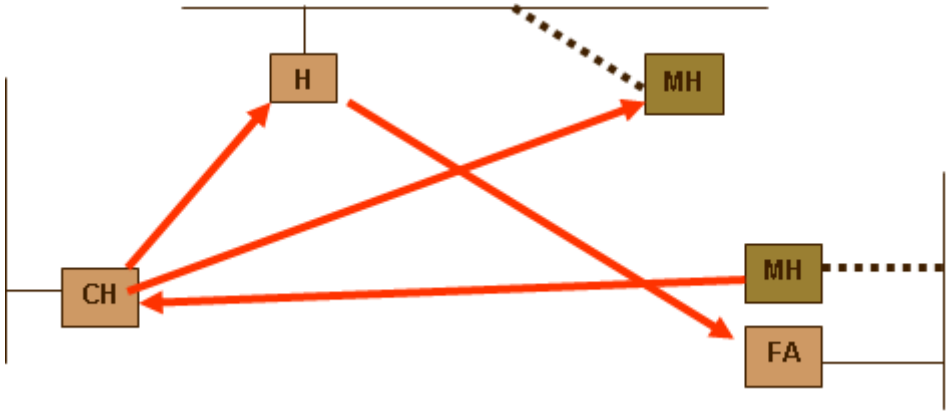
131 mobile node failes authentication

133 registration Identification mismatch

135 too many simultaneous mobility binding

4. Ketika sebuah mobile node mendeteksi bahwa ia telah pindah ke foreign network, ia akan mendapat care-of address pada foreign network. Care-of address dapat ditentukan baik dari foreign agents advertisement (sebuah foreign agent care-of address) atau dengan mekanisme penugasan eksternal seperti DHCP (sebuah co-located care-of address).
5. Mobile node yang beroperasi pada tempat yang jauh dari home agent akan diregistrasi care-of addressnya yang baru dengan home agentnya melalui pertukaran sebuah pesan Registration Request dan Registration Reply denganya memungkinkan melalui sebuah foreign agent.
6. Datagram yang dikirim ke mobile node home address akan ditahan oleh home agent, dibuatkan jalur oleh home agent ke mobile node care of address, diterima pada ujung akhir saluran (baik pada foreign agent atau mobile node itu sendiri) dan akhirnya dikirimkan ke mobile node.
7. Dalam arah yang berlawanan, datagram yang dikirim oleh mobile node secara umum akan dikirimkan ke destinationya menggunakan mekanisme routing IP standar, tidak perlu melalui home agent.

Ketika jauh dari home, Mobile IP menggunakan pembuatan jalur protocol untuk menyembunyikan mobile node home address dari campur tangan router antara home network dengan lokasinya sekarang. Jalur pengiriman diakhiri pada mobile node's care of address. Sebuah care-of address harus berupa sebuah alamat dimana datagram dapat dikirimkan melalui routing IP konvensional. Pada care of address, datagram asli dipindah dari jalur pengiriman dan dikirimkan ke mobile IPv4 ini biasa disebut Triangular Routing.



Gambar 3-31 Triangular routing

Keterangan :

- Corresp. Node C melakukan inisialisasi dengan Mobile Node dan mengirimkan paket kepada home address MN
- Home Agent menerima paket dan meneruskannya ke mobile node.
- Mobile node membalas langsung ke Corresp. Node C

3.4 Mobile IPv6 (MIPv6)

Desain dari mobile IPv6 mengambil keuntungan baik dari segi pengalaman dalam pengembangan dari mobile IPv6 dan dari kesempatan yang disediakan oleh IPv6. Karena itu mobile IPv6 berbagi beberapa ciri dengan mobile IPv4, tetapi terintegrasi pada IPv6 dan menawarkan beberapa peningkatan.

3.4.1 Protokol Mobile IPv6

Mobile IPv6 mendefinisikan sebuah protokol IPv6 baru berupa set pesan-pesan dan proses-proses yang digunakan untuk menetapkan hubungan antara node-node yang berdekatan. Protocol tersebut adalah Neighbor Discovery. Neighbor discovery merupakan pengganti dari ARP, ICMP Router Discovery dan ICMP redirect yang digunakan dalam IPv4 dengan beberapa fungsionalitas yang baru.

Proses-proses yang dilakukan oleh Neighbor Discovery adalah sebagai berikut:

1. Router Discovery

   Proses dimana sebuah host menelusuri router-router pada sebuah link.
2. Prefix Discovery

   Proses dimana host-host menelusuri prefix-prefix network untuk link-link lokal tujuan.
3. Parameter Discovery

Proses dimana host-host menelusuri parameter-parameter operasi tambahan, termasuk MTU dan hop limit default untuk outgoing packets.

4. Address autoconfiguration

   Proses pengkonfigurasian IP address untuk interface-interface secara otomatis.

5. Neighbor Unreachability detection

   Proses dimana sebuah node memastikan bahwa layer IPv6 suatu nde tetangga tidak lagi menerima paket-paket.

6. Duplicate Address Detection

   Proses dimana sebuah node memastikan bahwa sebuah address yang akan digunakan belum pernah dipakai oleh tetangga.

3.4.2 Operasi Dasar Mobile IPv6

Mobile node selalu diharapkan untuk dialamatkan pada home addressnya, meskipun ia berada pada home linknya atau jauh dari home. Home address adalah alamat IP diberikan pada mobile node dengan home subnet prefiknya pada home link. Sementara mobile node berada pada home, paket dialamatkan pada home link. Sementara mobile node berada pada home, paket dialamatkan pada home addresnya kemudian dirutekan ke sambungan mobile node link menggunakan mekanisme routing.

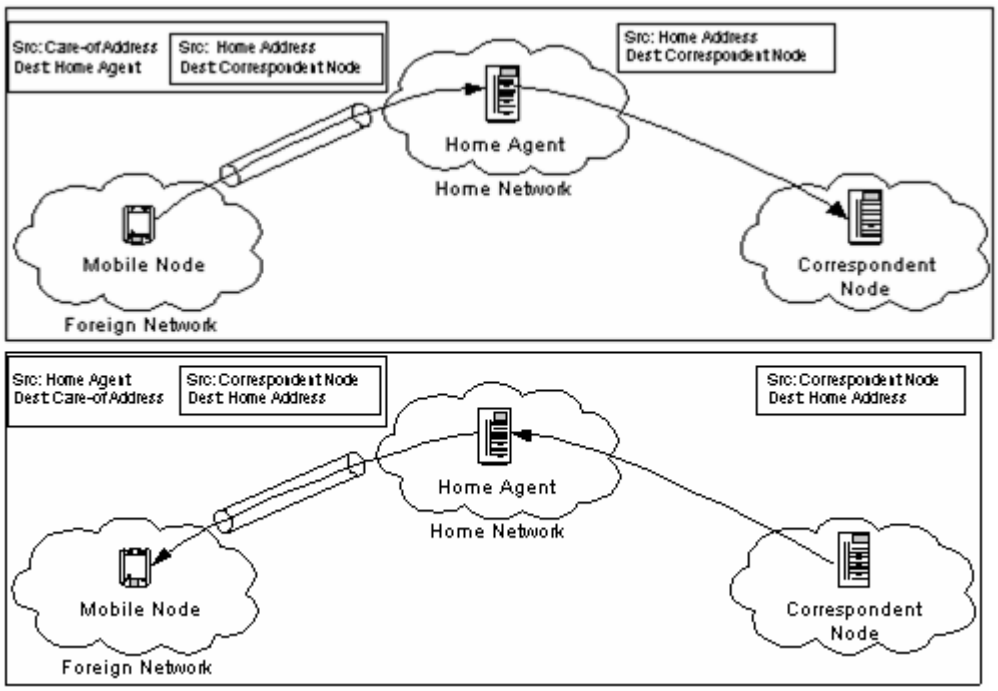
Sementara mobile node menempel pada beberapa foreign link yang jauh dari home, ia juga dapat dialamatkan pada satu atau lebih care-of address merupakan sebuah alamat IP yang dihubungkan dengan mobile node yang mempunyai subnet prefix dari sebuah foreign link tertentu. Mobile node dapat memperoleh care-of addressnya melalui mekanisme IPv6 konvensional seperti stateless atau statefull autoconfiguration. Selama mobile node tinggal pada lokasi ini, paket dialamatkan pada care-of address ini untuk kemudian dirutekan ke mobile node. Mobile node dapat juga menerima paket-paket dari beberapa care-of address, seperti ketika ia sedang bergerak tetapi masih dapat dicapai pada link sebelumnya.

Hubungan antara mobile node home address dan care-of address dikenal sebagai ”Correspondent node” untuk mobile node. Sementara ketika jauh dari home, sebuah mobile node meregistrasi care-of address secara utama dengan router pada home linknya, permintaan kepada router ini untuk beerfungsi sebagai ”home agent”untuk mobile node. Mobile node ini membuat registrasi binding dengan mengirimkan pesan ”Binding Update” ke home agent. Home agent membalas ke mobile node dengan mengembalikan pesan ”Binding Acknowledgement”.

Ada dua mode komunikasi yang mungkin antara mobile node dan correspondent node yaitu :

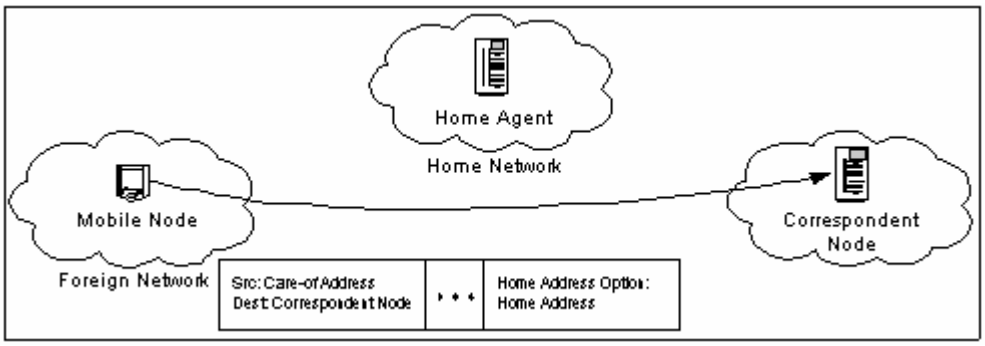
1. Mode yang pertama adalah bidirectional tunneling. Pada mode ini tidak memerlukan dukungan dari correspondent mode dan bahkan tersedia jika mobile node tidak meregistrasi bindingnya yang terbaru dengan correspondent node. Paket-paket dari correspondent node dirutekan ke home agent dan kemudian disalurkan ke mobile node. Paket paket ke correspondent node disalurkan dari mobile node ke home agent (”reverse tunneled”) dan kemudian secara normal dari home network ke correspondent node. Pada mode ini, home agent menggunakan proxy Neighbor Discovery untuk menahan beberapa paket IPv6 yang dialamatkan ke mobile node home address pada home link.

Setiap paket yang ditahan disalurkan ke mobile node's primary care –of address. Penyaluran ini menggunakan enkapsulasi IPv6.

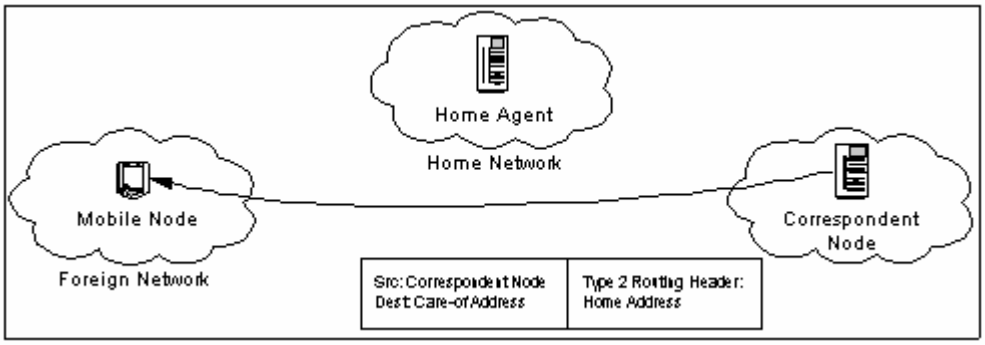


Gambar 3-32 Dari coresponden node ke mobile node

2. Mode kedua adalah route optimazation. Mode ini memerlukan dukungan mobile node untuk meregistrasi bindingnya pada correspondent node. Paket-paket dari correspndent node dapat dirutekan secara langsung ke care-of address dari mobile node. Ketika mengirimkan sebuah paket ke beberapa tujuan correspondent node mengecek binding yang tertahan untuk masukan untuk paket destinition address. Jika binding yang tertahan untuk alamat tujuan ditemukan, node menggunakan sebuah dari tipe dari IPv6 routing header yang baru untuk meroutekan paket mobile ke mobile node dengan cara care-of address menandai pada binding ini. Peroutingan paket secara langsung ke mobile node care of address membolehkan penggunaan jalur komunikasi terpendek. Ini juga menghilangkan congestion pada mobile node home agent dan home link. Sebagai tambahan, dampak dari kemungkinan kegagalan dari home agent atau network pada jalur dapat dikurangi. Ketika peroutingan paket secara langsung ke mobile node, correspondent node menyesuaikan destinition address pada IPv6 header ke node care-of address dari mobile node. Sebuah tipe IPv6 routing header yang baru juga ditambahkan ke paket untuk dibawa ke home address yang ditentukan. Sama miripnya, mobile node menyesuaikan source address dalam IPv6 paket header ke care-of address nya yang baru. Mobile node menambahkan pilihan tujuan IPv6 "home address" yang baru untuk membawanya ke home address. Pencantuman home addresss pada paket-paket ini membuat penggunaan care of address transparan diatas network layer.



Gambar 3-33 Dari mobile node ke coresponden node



Gambar 3-34 Dari coresponden node ke mobile node

3.5 Perbandingan Mobile IPv4 dengan Mobile IPv6

Mskipun Mobile IPv6 berbagi beberapa ciri dengan Mobile IPv4, namun ada beberapa perbedaan utama antara keduanya.

Perbedaan itu antara lain sebagai berikut :

1. Pada mobile IPv6 tidak ada keharusan untuk memperkejakan router khusus sebagai ”foreign agent” seperti di mobile IPv4. Mobile IPv6 beroperasi dibeberapa lokasi tanpa kebutuhan khusus dari router lokal.
2. Mobile IPv6 mendukung untuk optimasi rute yang menjadi bagian dasar protokol, daripada perluasan yang standar.
3. Optimasi rute mobile IPv6 dapat beroperasi secara aman bahkan tanpa pre-anggered security association. Ini diharapkan bahwa optimasi rute tersebut dapat dilakukan pada skala global antara seluruh mobile node dan correspondent node.
4. Kebanyakan paket dikirimkan ke mobile node sementara jauh dari home dalam mobile IPv6 dikirim menggunakan IPv6 routing header daripada enkapsulasi IP, mengurangi apa yang dikerjakan dalam mobile IPv4
5. Mobile IPv6 dipisahkan dari beberapa bagian link layer, sebagaimana digunakan pada Neighbor Discovery.Ini juga meningkatkan kekuatan dari protokol.
6. Penggunaan enkapsulasi IPv6 memindahkan kebutuhan dalam Mobile IPv6 memindahkan kebutuhan dalam Mobile IPv6 untuk mengatur ”tunnel sofr state”.

7. Mekanisme penemuan home agent address dinamis dalam Mobile IPv6 mengembalikan balasan tunggal ke mobile node. Pendekatan directed broadcast digunakan dalam IPv4 untuk mengembalikan balasan yang terpisah ke setiap home.

3.6 SOAL dan JAWABAN

3.6.1 Soal

1. Apa yang menyebabkan adanya teknologi Mobile IP?
2. Sebut dan jelaskan Komponen – komponen yang ada dalam mobile ip!
3. Bagaimana proses terjadinya mobile IP?
4. Perbedaan antara Mobile IPv4 dan Mobile IPv6?
5. Gambarkan analogi dari proses terjadinya proses Biderectional tunnel dan route optimation?

3.6.2 Jawaban

1. Mobile IP muncul karena perkembangan teknologi wireless yang semakin canggih dan kebutuhan akan teknologi mobile yang semakin tinggi dan proses pengolahan IP yang semakin rumit maka diperlukan sebuah teknologi mobile dengan asumsi dimana kita bisa melakukan koneksi kejaringan dengan teknologi wireless dalam keadaan mobile dan dengan menggunakan IP yang tetap meskipun kita berpindah-pindah dari suatu jaringan satu ke jaringan yang lainnya. Sebab itu lah muncul sebuah teknologi mobile yang baru dan dikenal dengan istilah Mobile IP.
2. Komponen-komponen yang ada dalam Mobile IP :

- Mobile Host

  Sebuah host atau router yang merubah point dari attachmentnya dari sebuah network atau subnetwork ke lainnya. Sebuah mobile node dapat merubah alamat IP nya. Ini dapat melanjutkan komunikasi dengan node internet lainya pada beberapa lokasi menggunakan alamat IP yang konstan, diandaikan konektifitas link layer ke point dari attachment yang tersedia.

- Corresponding Host

  Adalah host lawan dari mobile host ketika ia berada pada jaringan selanjutnya, yaitu foreign network yang didalamnya terdapat Home Agent.

- Care Of Address

  Address yang dimiliki Mobile Host ketika dia berada pada jaringan tujuannya, yaitu foreign network yang didalamnya terdapat Foreign Agent.

- Home Agent

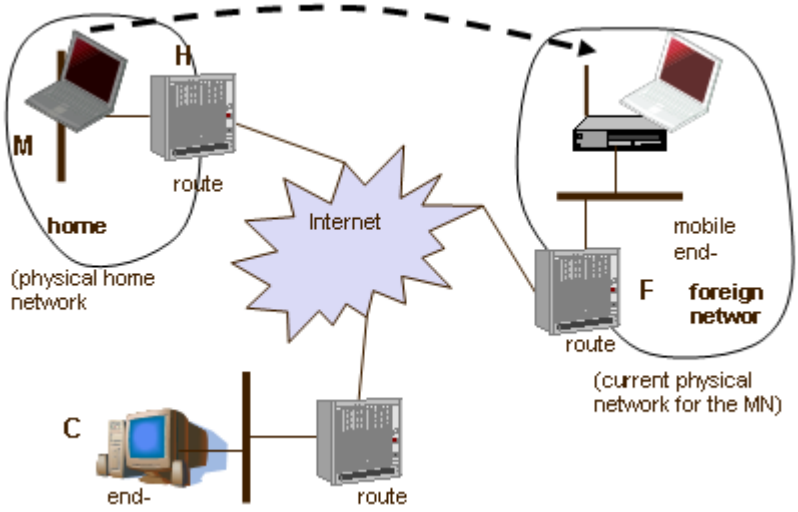
  Sebuah router pada jaringan mobile node home yang membuka jalur datagram untuk pengiriman ke mobile node ketika ia jauh dari home dan menjaga informasi lokasi yang sekarang ke mobile node.

- Foreign Agent

  Sebuah router pada jaringan mobile node yang dikunjungi menyediakan layanan routing mobile node sementara ia diregistrasi. Foreign agent menutup jalur dan mengirimkan datagram ke mobile node yang telah dibuka jalurnya oleh mobile node home agent. Untuk datagram yang

dikirim oleh mobile node, foreign agent dapat melayani seperti default router untuk mobile node yang telah diregitrasi.

3. Proses terjadinya Mobile IP



Proses terjadinya Mobile IP dapat diasumsikan seperti pada gambar diatas. Dimana sebuah Mobile host (disini menggunakan labtop) berpindah pada posisi awal yaitu dalam (home network) menuju ke posisinya yang baru yaitu (foreign network). Dengan perpindahan jaringan itu otomatis dalam kondisi yang biasa, mobile host akan mengalami perubahan alamat IP, tapi dalam teknologi mobile IP ini alamat IP dari mobile host akan tetap seperti dalam posisinya yang semula yaitu dalam home address.

4. Perbedaan antara Mobile IPv4 dan Mobile IPv6

Pada mobile IPv6 tidak ada keharusan untuk memperkejakan router khusus sebagai ”foreign agent” seperti di mobile IPv4. Mobile IPv6 beroperasi dibeberapa lokasi tanpa kebutuhan khusus dari router lokal. Mobile IPv6 mendukung untuk optimasi rute yang menjadi bagian dasar protokol, daripada perluasan yang standar.

Optimasi rute mobile IPv6 dapat beroperasi secara aman bahkan tanpa pre-anggered security association. Ini diharapkan bahwa optimasi rute tersebut dapat dilakukan pada skala global antara seluruh mobile node dan correspondent node.

Kebanyakan paket dikirimkan ke mobile node sementara jauh dari home dalam mobile IPv6 dikirim menggunakan IPv6 routing header daripada enkapsulasi IP, mengurangi apa yang dikerjakan dalam mobile IPv4

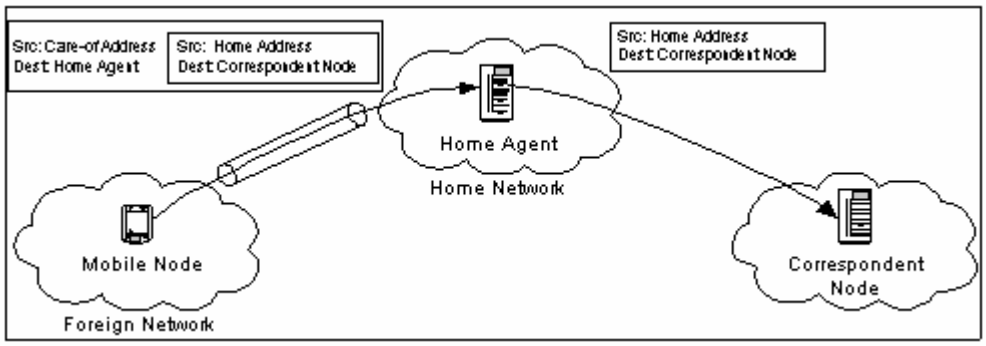
Mobile IPv6 dipisahkan dari beberapa bagian link layer, sebagaimana digunakan pada Neighbor Discovery.Ini juga meningkatkan kekuatan dari protokol.

Penggunaan enkapsulasi IPv6 memindahkan kebutuhan dalam Mobile IPv6 memindahkan kebutuhan dalam Mobile IPv6 untuk mengatur ”tunnel sofr state”.

Mekanisme penemuan home agent address dinamis dalam Mobile IPv6 mengembalikan balasan tunggal ke mobile node. Pendekatan directed broadcast digunakan dalam IPv4 untuk mengembalikan balasan yang terpisah ke setiap home.

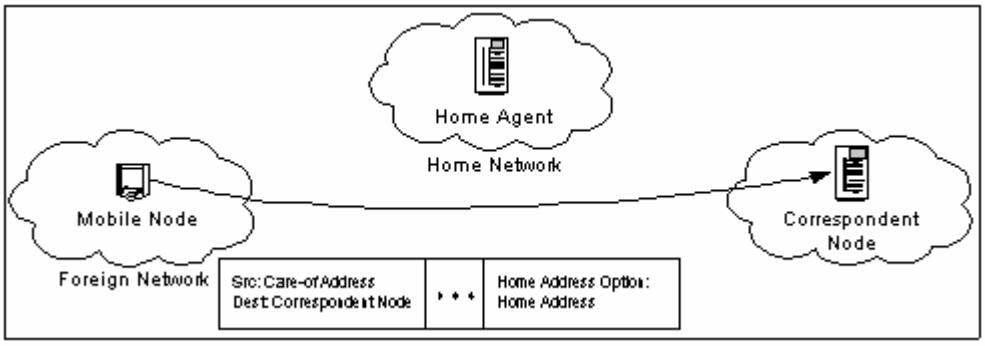
5. Analogi teknologi bidirectional tunnel dan route optimation

Analogi bidirectional tunnel



Dimana untuk melakukan koneksi menuju ke correspondent node dari mobile node langsung di tunnel menuju ke home agent baru ke correspondent. Disini akan mempercepat jalur pada saat menuju ke home agent. Hal yang sama juga pada saat correspondent node menghubungi mobile node.

Analogi route optimazation



Dalam teknonogi ini fungsi dari home agent dihilangkan sehingga dari mobile node untuk menghubungi correspondent node langsung menggunakan tunnel. Sehingga kecepatannya juga semakin tinggi. Hal yang sama jika correspondent node menghubungi mobile node.

3.7 REFERENSI

[1] http://www.wikipedia.org//

[2] http://www.google.co.id//

[3] http://www.ilmukomputer.com//

BAB 4. MULTIMEDIA PROTOKOL

Ajeng Dwi Pramesti[1)], Eko Adi Setiawan [1)], Titik Mariyanti [1)]
Politeknik Elektronika Negeri Surabaya

ABSTRAK

Peningkatan daya proses yang tersedia dalam komputer telah berkembang pada aplikasi multimedia dalam cakupan yang luas. Aplikasi- aplikasi tersebut mempengaruhi infrastrukrur jaringan yang ada untuk mengirimkam aplikasi video-based dan audio-based ke penerima. Jaringan tersebut digunakan tidaklah lama, semata-mata untuk mendukung transmisi data. Aplikasi tersebut menyediakan kemampuan yang lebih untuk dua jalur videoconferencing, audio broadcasting, whiteboard collaboration, interactive training dan IP telephony (VoIP). Dengan aplikasi ini, video dan audio streaming dikirimkan melalui jaringan antara peers atau antara client dan server. Pada bab ini menjelaskan penggambaran dari dua peer protokol yang digunakan untuk fasilitas aplikasi tersebut. Real-Time Transport Protocol (RTP) dan Real-Time Control Protocol (RTCP) digunakan untuk sinkronisasi dan mengontrol arus traffic pada aplikasi multimedia. Pada bab ini menyimpulkan dengan menganalisa standard IP telephony (VoIP). Aplikasi-aplikasi yang menggunakan standard tersebut mempercayakan pada RTP dan RTCP untuk service pengiriman.

4.1 Definisi Protokol Multimedia

Multimedia adalah penggunaan beberapa media yang berbeda untuk menggabungkan dan menyampaikan informasi dalam bentuk text, audio, grafik, animasi, video dan interaktif. Pada system multimedia terdistribusi, dibutuhkan protocol jaringan yang mengaturnya. Protocol adalah persetujuan tentang bagaimana komunikasi diproses antara 2 node. Tipe jaringan computer, yaitu :

1. Local Area Network (LAN)
   Jaringan kecepatan tinggi pada suatu lingkungan local tertentu.
2. Metropolitan Area Network (MAN)
   Kecepatan tinggi untuk node yang terdistribusi dalam jarak jauh (biasanya untuk satu kota atau suatu daerah besar).
3. Wide Area Network (WAN)
   Komunikasi untuk jarak yang sangat jauh. Contoh : internet.
4. Wireless Network
   Peralatan end-user untuk mengakses jaringan dengan menggunakan transmisi radio pendek atau sedang.
   1. Wireless WAN : GSM (sampai 20 Kbps).
   2. Wireless LAN/MAN : WaveLAN (2-11 Mbps, sampai 150 m).
   3. Wireless PAN (Personal Area Network) : Bluetooth (sampai 2Mbps, jarak <10 m).

Dengan meningkatnya daya proses yang tersedia dalam computer desktop mengakibatkan perkembangan suatu cakupan yang luas pada aplikasi multimedia. Aplikasi ini mempengaruhi infrastruktur jaringan yang ada untuk mengirimkan aplikasi video-based dan audio-based ke end user.

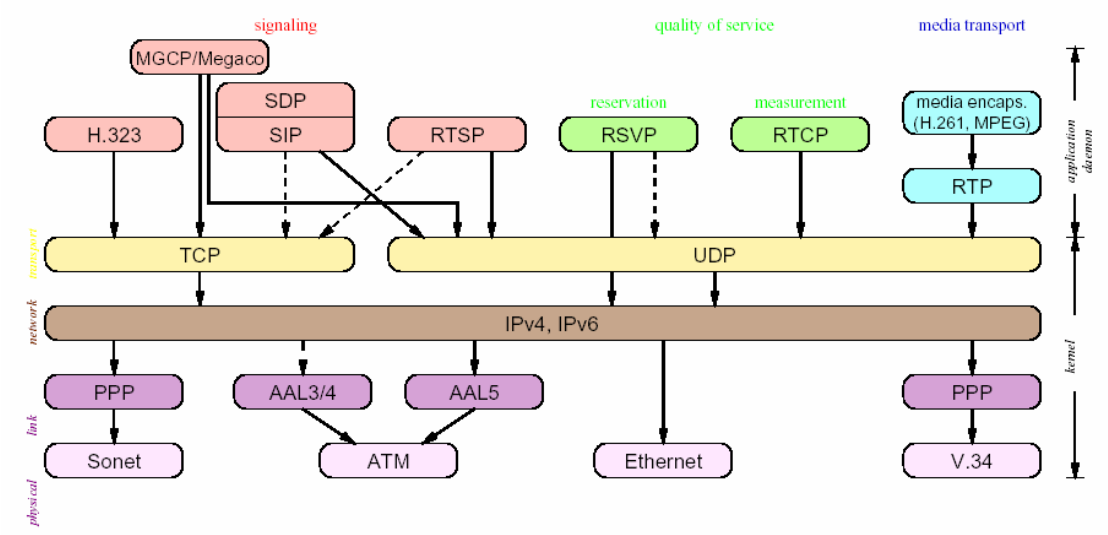
Jaringan tidak digunakan dalam waktu yang lama semata-mata untuk mendukung transmisi data traditional.

Aplikasi ini menyediakan peningkatan kemampuan untuk 2 jalur videoconverencing, audio broadcasting, whiteboard collaboration, interaktive training dan IP telephony. Dengan aplikasi ini, video dan audio stream ditransfer lewat jaringan antarapeer atau antara client dan server.

4.2 Karakteristik Data Multimedia

1. Terutama difokuskan pada Continous media (video dan audio).
2. Memliki karakteristik :
   a. Voluminous
      - Membutuhkan data rate tinggi dan berukuran besar
   b. Real-time and Interactive
      - Membutuhkan low delay
      - Membutuhkan sinkronisasi dan interaktif

   Protokol multimedia terdiri atas :
   a. Real Time Protocol (RTP)
   b. Real Time Control Protocol (RTCP)
   c. Resource Reservation Protocol (RSVP)
   d. Real Time Streaming Protocol (RTSP)



Gambar 4-35 Stack Internet Multimedia Protokol

4.3 Real Time Protocol (RTP)

4.3.1 Yang dilakukan RTP

a. RTP adalah suatu standard untuk mengirimkan data multimedia secara real-time seperti audio dan video.

b. Menyediakan layanan penyampaian end to end untuk data yang mempuyai karakteristik yang real-time, seperti audio dan video interactive.

c. RTP terdiri dari suatu data dan control part yang disebut RTCP.

d. Merupakan protokol pada layer application.

e. Berjalan di atas UDP tapi bisa juga di atas protokol lain (untuk mengotimalkan penggunaan mutiplexing dan layanan checksum yang ada di dalam protokol UDP).

f. Menyediakan servis pengiriman data end-to-end real-time.

g. Servis ini meliputi payload type identification, sequence numbering, time stamping dan delivery monitoring.

h. Mendukung pemindahan data ke beberapa tujuan menggunakan distribusi multicast, jika ternyata memang disediakan oleh jaringan tersebut.

i. RTP telah dikembangkan dengan kemampuan fleksibilitas dan scalability dan malah digunakan sebagai inti protokol real-time pada jaringan IP dan sistem hybrid MPOA (Multiprotocol Over ATM).

h. RTP adalah suatu standard untuk mengirimkan data multimedia secara real-time seperti audio dan video.

i. Menyediakan layanan penyampaian end to end untuk data yang mempuyai karakteristik yang real-time, seperti audio dan video interactive.

j. RTP terdiri dari suatu data dan control part yang disebut RTCP.

k. Merupakan protokol pada layer application.

l. Berjalan di atas UDP tapi bisa juga di atas protokol lain (untuk mengotimalkan penggunaan mutiplexing dan layanan checksum yang ada di dalam protokol UDP).

m. Menyediakan servis pengiriman data end-to-end real-time.

n. Servis ini meliputi payload type identification, sequence numbering, time stamping dan delivery monitoring.

j. Mendukung pemindahan data ke beberapa tujuan menggunakan distribusi multicast, jika ternyata memang disediakan oleh jaringan tersebut.

k. RTP telah dikembangkan dengan kemampuan fleksibilitas dan scalability dan malah digunakan sebagai inti protokol real-time pada jaringan IP dan sistem hybrid MPOA (Multiprotocol Over ATM).

4.3.2 Yang tidak dilakukan RTP :

a. Tidak menyediakan mekanisme apapun untuk memastikan pengiriman yang tepet waktu atau menyediakan jaminan kualitas layanan (reliable data delivery), tapi mendelegaasikan tugas tersebut ke lapisan yang lebih rendah yaitu RSVP yang berbasis QoS.

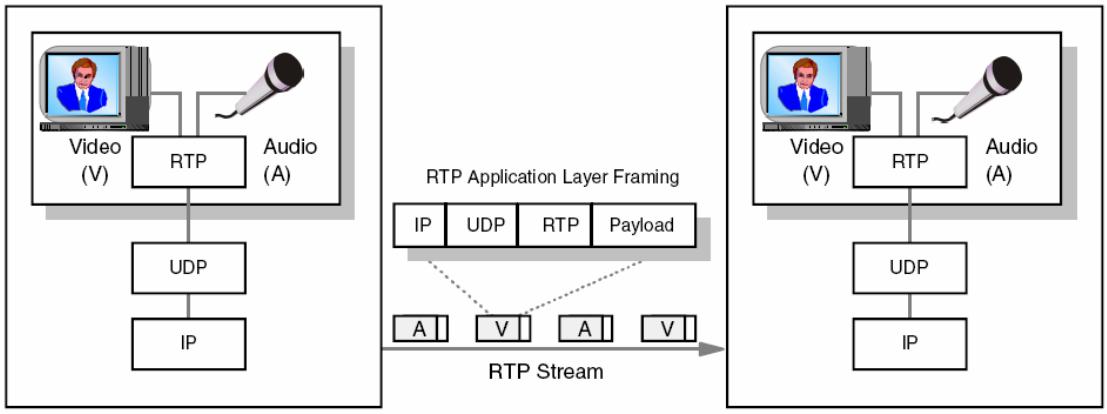
b. Tidak menjamin layanan Quality of Service (QoS) untuk aplikasi yang real-time.

c. Tidak menyediakan mekanisme pengalamatan pemesananan sumber (resource reservation addressing).

d. Tidak didesain untuk memenuhi kebutuhan banyak peserta dalam suatu konverensi multimedia (delivery of encryption key to participant), melainkan juga sebagai

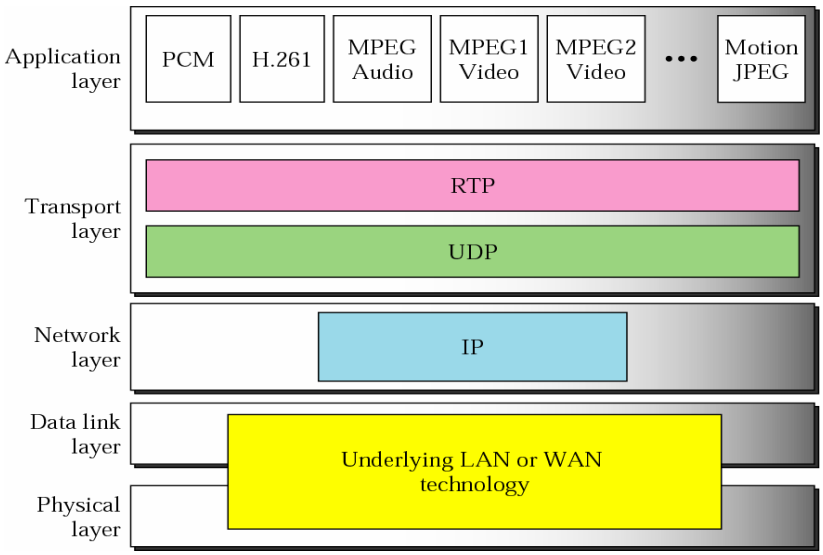
penyimpanan data yang kontinyu, simulasi interactive yang terdistribusi, dan aplikasi pengukuran dan pengendalian.

RTP mengimplementasikan transport fitur yang dibutuhkan untuk menyediakan sinkronisasi multimedia data stream. Dengan mempertimbangkan penggunaan aplikasi antara komponen video dan audio. RTP bias digunakan untuk menandai paket-paket yang duhubungkan dengan video individual dan audio stream. Ini melewatkan aliran untuk disinkronkan pada host penerima. Pada gambar 2 di bawah ini menampilkan operasi dari RTP pada transmisi multimedia. Data audio dan video diencapsulasi pada paket RTP lebih dahulu dari pengirim untuk penerima.



Gambar 4-36 Operasi RTP Pada Suatu Multimedia

Jika aplikasi multimedia tidak menggunakan RTP, penerima mungkin tidak bisa menghubungkan percakapan paket audio dan video. Mutimedia aplikasi ini dapat menghubungkan bermacam-macam level dari tampilan jaringan yang disediakan selama sesi multimedia. Kemacetan atau kondisi sementara yang lain dengan lingkungannya dapat menyebabkan paket-peket hilang atau pemesanan kembali selama trasnsit. Hal itu dapat menunda pengiriman paket oleh jumlah dari bermacam-macam waktu. Tingkah laku ini dapat kualitas masalah dengan berbagai tipe aplikasi-aplikasi multimedia.

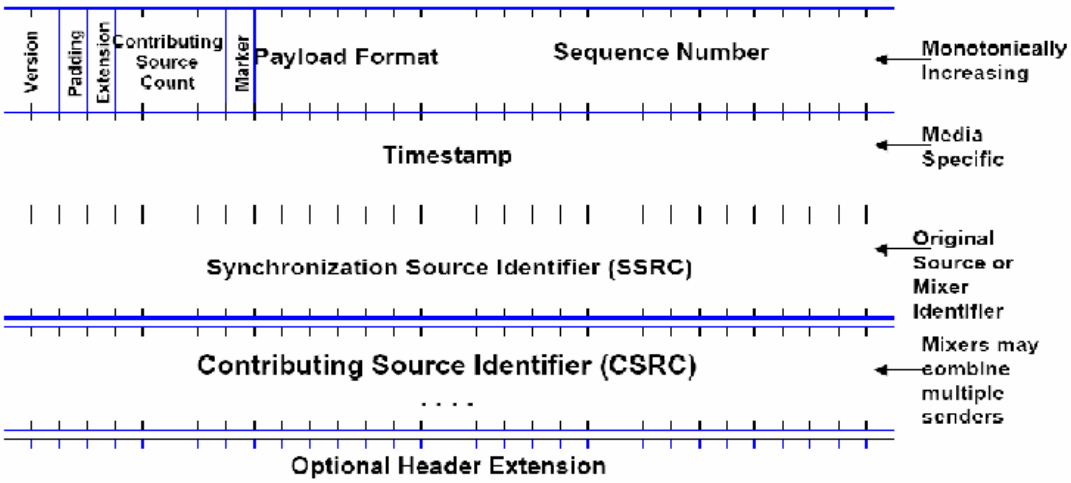


Gambar 4-37 Layer Aplikasi RTP

Keterangan :

1. UDP tidak mengindikasikan cara untuk mendeteksi packet loss dan memperbaiki packet sequence.
2. RTP menutupi masalah tersebut (menggunakan sequence number, time stamping).
3. RTP menyediakan mekanisme yang tepat dengan menggunakan QoS protocols.

4.3.3 Format header RTP



Gambar 4-38 Format Header RTP

Bagian-bagian yang terdapat di dalam format header RTP tersebut antara lain :

a. Version (V) : bidang yang panjangnya 2 bit menandakan aliran RTP. Aliran RTP yaitu 2.0 (untuk mengenali versi RTP).
b. Padding (P) : bidang ini panjangnya 1 bit. Jika P adalah di-set, paket berisi satu atau lebih komposisi 8 lapisan tambahan pada bagian akhir, yang mana bukanlah bagian dari payload. Lapisan ini diperlukan oleh beberapa algoritma encryption, yang mana menghendaki ukuran blok atau untuk membawa beberapa paket RTP di (dalam) suatu lower-layer PDU. Ketika dibuat, sebuah paket terdiri dari satu atau lebih padding (lapisan octet tambahan di bagian akhirnya yang tidak termasuk bagian dari payload (muatan)).
c. Extension (X) : bidang ini panjangnya 1 bit. Jika X adalah di-set, yang diikuti oleh tepatnyaa salah satu header extension. Header yang fixed biasanya diikuti oleh tepat satu extension (perluasan) header, dengan format yang sudah ditentukan.
d. CSRC count (CC) : Bidang ini panjangnya 4 bit. Bidang menandai adanya nomor dari identitas CSRC yang diikuti header. Bagian ini trdiri dari sejulah pengenal CSRC yang mengikuti fixed header.
e. Marker bit (M) : Bidang ini panjangnya 1 bit. Marker dapat diartikan sebagai profil. Marker dimaksudkan untuk menyediakan kejadian yang signifikan seperti frame boundaries yang ditandai dalam aliran paket.
f. Payload type (PT) : Bidang ini panjangnya 7 bit. Bagian ini dibuat agar format payload RTP dapat dikenali dan ditemukan oleh aplikasi yang menggunakannya. Sebuah profil

menentukan pemetaan statis standar dari tipe kode payload ke format payload. Tipe payload tambahan mungkin didefinisikan secara dinamik melalui artian non-RTP.

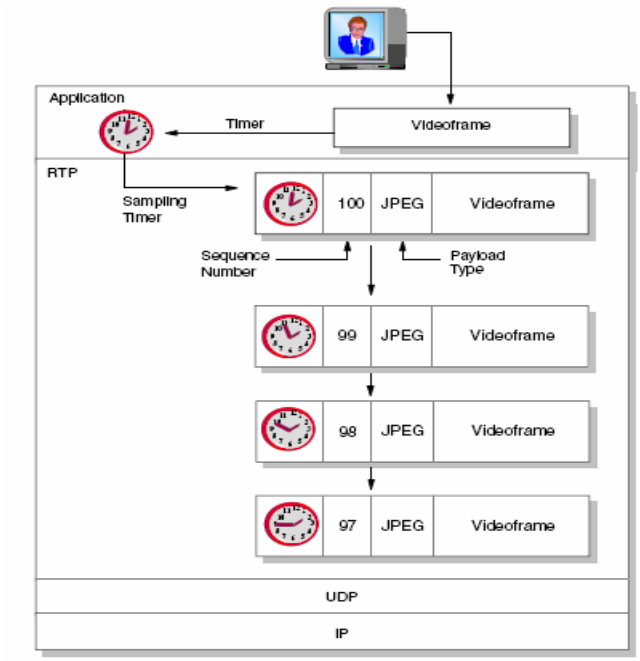
g. Sequence number : Bidang ini panjangnya 16 bit. Sequence number ditambahkan satu untuk tiap paket data RTP yang dikirimkan, dan mungkin digunakan oleh penerima untuk mendeteksi paket yang hilang (packet loss) dan mengembalikan urutan paket.

h. Time stamp : Bidang ini panjangnya 32 bit. Bagian ini mencerminkan pencuplikan yang instan dari octet pertama dalam paket data RTP. Pencuplikan ini harus diturunkan dari waktu yang bertambah secara monoton dan linear agar dapat terjadi sinkronisasi dan kalkulasi terhadap jitter. Resolusi dari waktu harus cukup untuk tingkat keakuratan sinkronisasi yang diinginkan dan untuk pengukuran paket jitter.

i. SSRC : Bidang ini panjangnya 32 bit. Merupakan bagian pengenal dari sumber sinkronisasi (synchronization source). Pengenal ini dipilih acak dengan maksud agar tidak ada 2 sumber sinkronisasi yang memilki pengenal SSRC yang sama pada satu sesi RTP.

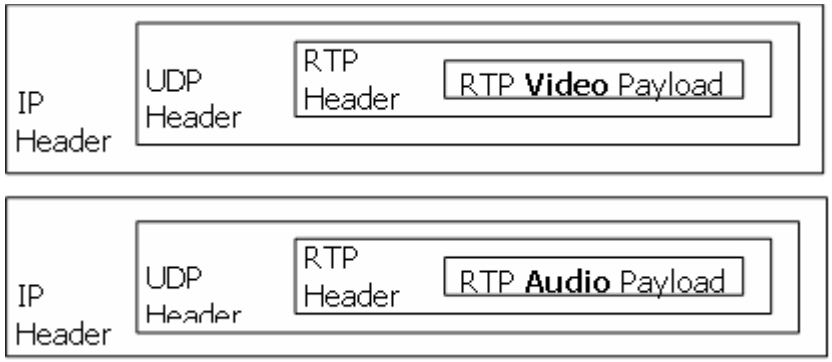
j. CSRC list : Mengkontribusi daftar pengenal sumber. CSRC dimaksudkan untuk mengenali sumber yang berkontribusi untuk payload yang diisi dalam paket.

Pada gambar di bawah dijelaskan bahwa Film / video merupakan sekumpulan dari beberapa gambar (TV/video). Tiap video frame ditambahkan timer (1 dtk s/d 25 frame) dan dimasukkan dalam protokol RTP. Dengan sequence number 100. Type payload diwakili dengan JPEG. Video dipecah-pecah dengan format gambar JPEG. Jam ke-n diberikan timer, termasuk dalam urutan ke berapa (sequence number) dengan type payload JPEG. Payload dan video frame harus sinkron dan dikirim ke UDP kemudian ke IP.



Gambar 4-39 Paket Generasi RTP Pada Aplikasi Video

4.4 Cara Kerja RTP



Gambar 4-40 cara kerja RTP

Keterangan :

1. Video dan audio payload dikirim secara terpisah.
2. Menggunakan sequence number untuk sinkronisasi audio dan video dalam sekali penerimaan.

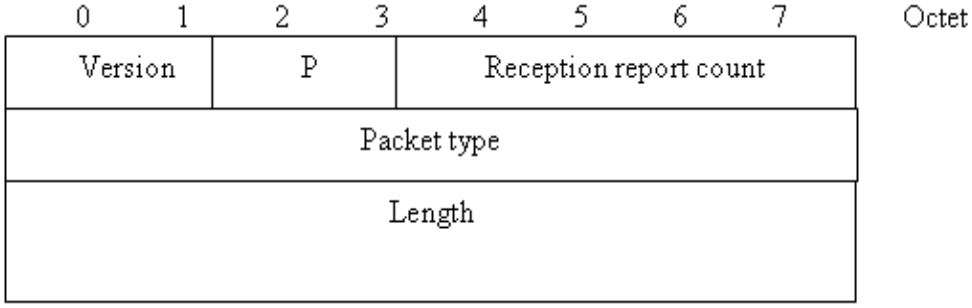
4.5 Real-time Control Protocol (RTCP)

a. Bekerja pada perangkai dengan RTP.
b. Setiap partisipan di sesi RTP secara periodic mengirim RTCP paket control untuk partisipan yang lain.
c. Pengaruh arus balik digunakan untuk mengontrol penampilan.
d. Pengirim dapat dimodifikasi pada transmisi berdasarkan pengaruh arus balik.
e. Setiap paket RTCP berisi laporan pengirim dan penerima.
f. Statistic termasuk jumlah paket yang terkirim, jumlah yang hilang, interarival jitter, dan lain-lain.

4.5.1 RTCP mempunyai 4 fungsi utama, yaitu :

1. Menyediakan umpan balik terhadap kualitas informasi yang ditransmisikan, sehingga modifikasi terhadap informasi tersebut diharapkan menghasilkan kinerja yang lebih baik.
2. Membawa pengenal level transport secara terus-menerus untuk sebuah sumber RTP yang lebih dikenal dengan sebutan canonical name (CNAME).
3. Untuk mengendalikan paket RTP yang dikirimkan oleh peserta konferensi sehingga dapat menampung penambahan peserta lainnya dalam sesi real-time tersebut.
4. Untuk menyampaikan informasi kendali pada sebuah sesi.

4.5.2 Format header RTCP



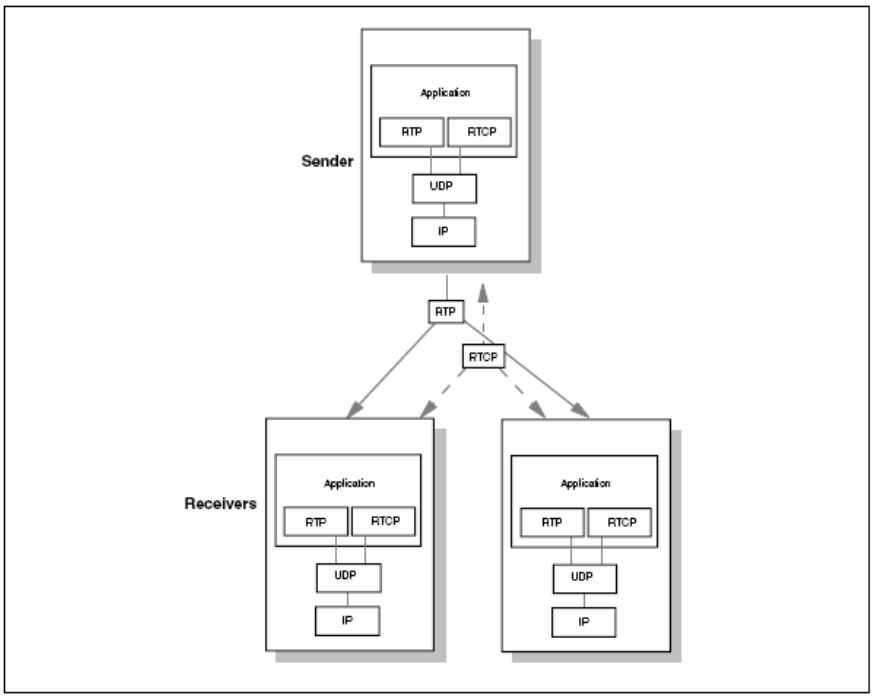
Gambar 4-41 Header RTCP

4.5.3 Bagian –bagian RTCP

Bagian-bagian yang terdapat di dalam format header RTCP tersebut antara lain :

1. Version : berfungsi sebagai pengenal versi RTP yang sama dengan paket RTCP dan paket data RTP. Version yang ditentukan untuk keperluan ini ada 2 jenis.
2. P, ketika dibuat, paket RTCP terdiri atas beberapa octet padding tambahan pada bagian akhir yang tidak termasuk dari informasi kendali.
3. Reception report count : jumlah blok reception report terdapat dalam paket ini. Walaupun nilainya nol tetap dianggap valid.
4. Packet type : terdiri atas nilai konstan 200 untuk mengenali bahwa sebuah paket memang benar paket RTCP SR.
5. Length : panjang dari paket RTCP adalah 32 bit dikurangi 1, termasuk header dan padding

4.5.4 Hubungan antara RTP dan RTCP



Gambar 4-42 Format Header antara RTP dan RTCP

4.6 Resource Reservation Protocol (RSVP)

RSVP adalah protocol pensinyalan unicast dan multicast yang dirancang untuk memasang dan mengatur informasi pemesanan pada tiap router sepanjang jalur data. Protokol ini digunakan terminal untuk memperoleh QoS tertentu dari jaringannya agar dapat digunakan oleh aplikasi VoIP. Dalam layer TCP/IP, RSVP berada pada layer transport. Tapi protokol ini tidak digunakan untuk mengirimkan data melainkan hanya sebagai sebuah internet control protokol saja.

Quality of Service diimplementasikan oleh suatu mekanisme kolektif yang disebut pengendalian trafik (traffic control). Mekanisme ini terdiri dari beberapa bagian, yaitu :

1. Packet classifier, menentukan kelas-kelas paket data.
2. Packet scheduler, merupakan mekanisme link, layer dependent.
3. Admission control, menentukan apakah router mempunyai QoS seperti yang diminta oleh terminal VoIP.

Policy control, menentukan apakah user yang menggunakan VoIP mempunyai kemampuan untuk untuk melakukan pemesanan.

4.7 Real-Time Streaming Protocol (RTSP)

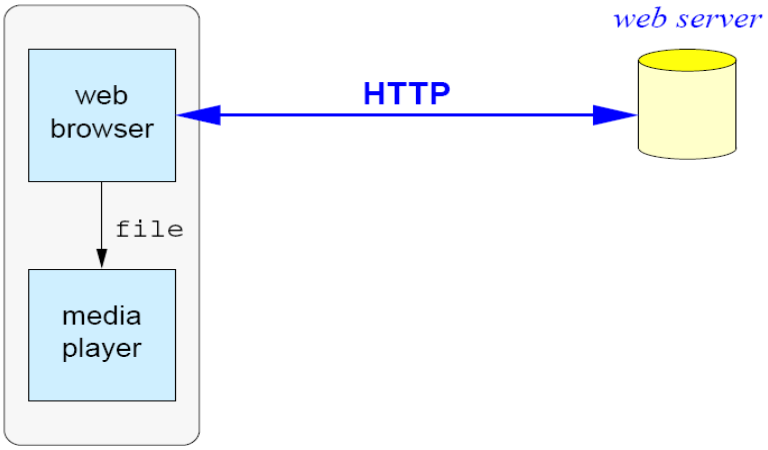
α. Digunakan oleh program streaming multimedia untuk mengatur data secara real-time, tidak bergantung pada protocol transport.

β. Metode yang ada: PLAY, SETUP, RECORD, PAUSE dan TEARDOWN.

χ. Digunakan pada Video on Demand.

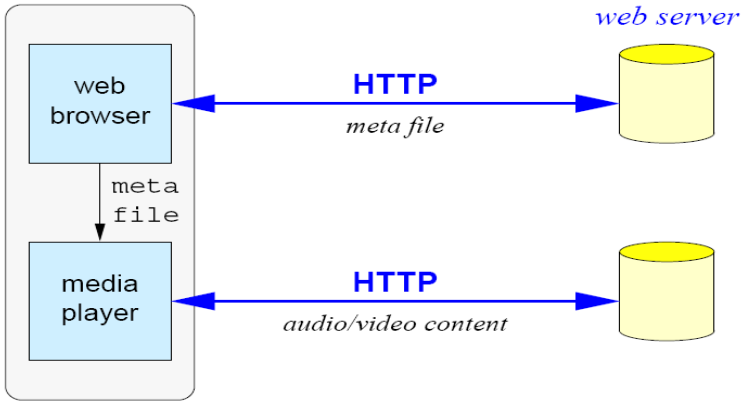
4.7.1 Arsitektur RTSP

a. Media file mendownload



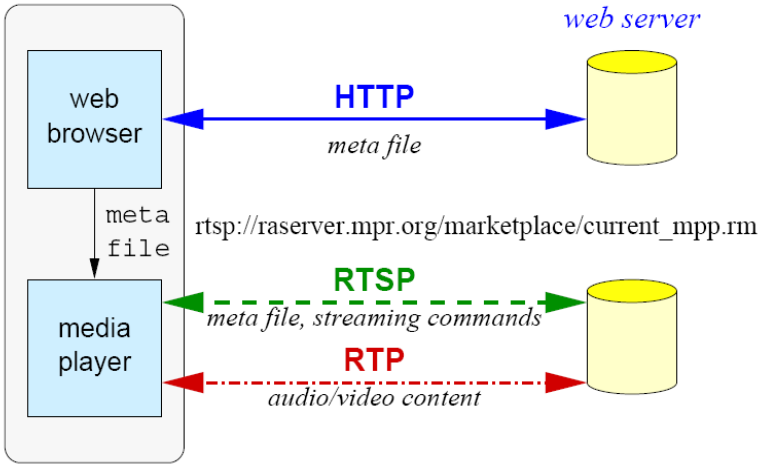
Gambar 4-43 Media file download

b. Meta files



Gambar 4-44 meta files

c. RTSP

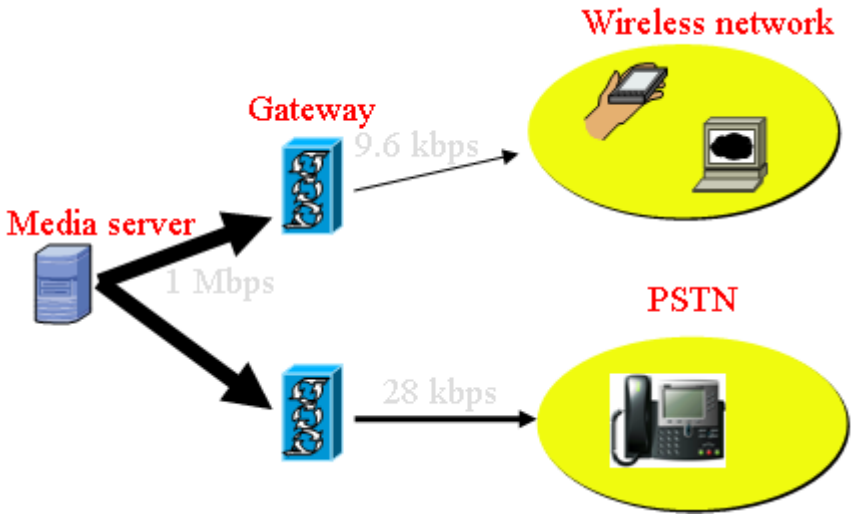


Gambar 4-45 Arsitektur RTSP

4.7.2 Aplikasi Multimedia

1. Audio
   a. Speech (CELP – type codecs)
   b. Music (MP3, WAV, WMA, Real)
2. Video (MPEG –1, 2, 4)
3. Video conference
4. QuickTime

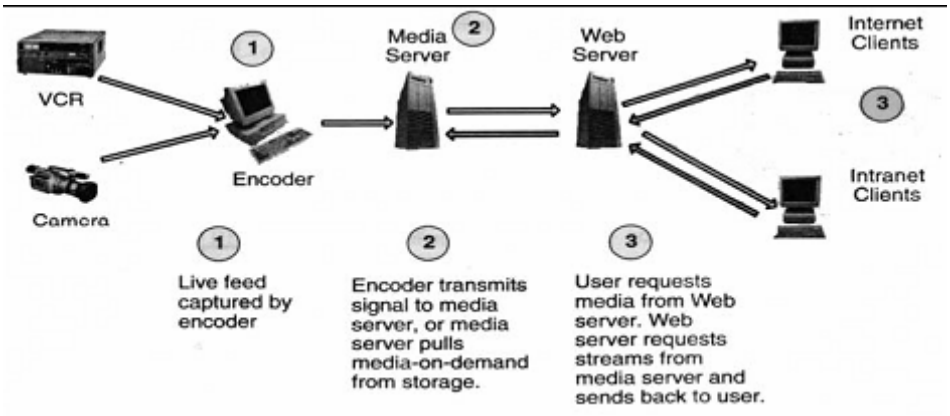
Streaming done using HTTP/TCP (MP3), or RTP/UDP (Video).



Gambar 4-46 Jringan Multimedia

4.7.3 Multimedia Streaming

1. Streaming media adalah suatu teknologi yang mampu mengirimkan file audio dan video digital secara real time pada jaringan komputer.



Gambar 4-47 Multimedia Streaming

2. Streaming vs Download

a. Download

- (+) download dan simpan file dalam HD sehingga dapat dinikmati pada saat offline.
- (+) dapat dilihat berkali-kali.
- (+) standard file (bisa dibaca oleh semua jenis mesin).
- (+) kualitas bagus
- (-) waktu download lama

a. Streaming

- (+) dapat dilakukan pada bandwith dengan kecepatan rendah
- (+) Web master tidak perlu risau dengan bandwith
- (+) Web master tidak dibatasi oleh besar file
- (-) Hanya dapat dilihat pada saat online

- (-) Kualitas gambar jelek

4.7.4 Hubungan antara RTP, RTCP dan RTSP

a. RTP merupakan protokol transport untuk penyampaian data rel-time, seperti streaming audio dan video
b. RTCP adalah bagian dari RTP dan membantu dengan menejemen QoS
c. RTSP merupakan control protocol untuk inisialisasi dan menyampaikan secara langsung multimedia streaming dari media server, "Internet VCR remote control protocol"
d. RTSP tidak menyampaikan data ,koneksi RSTP dapat digunakan untuk jalur tunnel RTP untuk kenyamanan dengan menggunakan firewall dan peralatan jaringan lainnya.
e. RTP dan RSTP akan digunakan bersama pada banyak sistem.

4.8 QuickTime

QuickTime adalah suatu multimedia framework yang dikembangkan oleh Apple Inc. yang mampu menangani berbagai format video digital, media clips, sound, teks, animasi, musik, dan beberapa tipe dari interactive panoramic images. Dimana tersedia untuk system operasi Mac OS X dan Microsoft Windows, dan berbagai macam variasi paket software seperti iTunes.

Teknologi QuickTime terdiri dari :

1. Aplikasi QuickTime Player diciptakan oleh Apple, yang mana merupakan suatu media player.
2. QuickTime framework, yang mana menyediakan suatu paket umum APIs untuk encoding dan decoding audio dan video.
3. QuickTime Movie (mov) file format, suatu media countainer dokumen terbuka.

QuickTime adalah gabungan Mac OS X, karena dengan versi awal Mac OS. Semua sistem Apple dikirim dengan QuickTime yang telah terinstall, hal itu menghadirkan 4D (disambiguation diperlukan) lapisan media untuk Mac OS X. QuickTime adalah pilihan untuk Sistem Windows, walaupun banyak aplikasi perangkat lunak memerlukan itu. Apple bundles itu dengan masing-masing iTunes untuk Windows Download. Software development kits (SDKs) untuk QuickTime tersedia kepada publik dengan suatu Apple Developer Connection (ADC) langganan.

4.8.1 QuickTime players

QuickTime dibagi-bagikan gratis, dan meliputi aplikasi QuickTime. Banyak aplikasi dapat ditulis untuk mengakses fitur yang disajikan oleh QuickTime framework, tetapi yang termasuk QuickTime Player terbatas hanya pada hal-hal yang paling mendasar operasi playback kecuali jika pengguna membeli suatu kunci lisensi QuickTime Pro, yang mana Apple menjual sebesar $ 29.95. Ahli kunci dikhususkan untuk versi QuickTime di mana mereka dibeli. Ahli kunci membuka fitur tambahan dari aplikasi QuickTime Player pada Mac OS X atau Windows, walaupun kebanyakan dapat mudah diakses dengan menggunakan player atau video editor dari sumber lainnya. Yang terdiri dari :

1. Full-Screen playback.

2. Movie baru yang merekam dari suatu FireWire DV atau kamera iSight.
3. Klip editing melalui fungsi cut, copy dan paste, salinan garis audio dan video track, dengan bebas menjiplak video track pada suaru kanvas virtual dengan pilihan cropping dan rotation.
4. Penghematan dan mengekspor (encoding) kepada banyak codecs yang didukung oleh QuickTime. QuickTime 7 meliputi menetapkan untuk pengeksporan video ke suatu iPod video-capable.

Gambar 4-48 QuickTime 7 Player Under Mac OS X

Beberapa aplikasi player gratis yang lain bersandar pada QuickTime framework menyediakan fitur yang tidak tersedia dalam dasar QuickTime Player. Sebagai contoh :

a. iTunes dapat bermain file QuickTime Movie dalam full-screen.
b. iTunes dapat mengekspor audio dalam WAV, AIFF, MP3, AAC, dan Apple Lossless.
c. RealPlayer dan Media Player Classic mendukung semua fitur playback yang meliputi pada QuickTime, mencakup full-screen playback.
d. Dalam Mac OS X, suatu AppleScript sederhana dapat digunakan untuk bermain suatu movie dalam full-screen mode.

Open source VLC media player dapat bermain QuickTime video saat mengabaikan pembatasan menempatkan pada versi non-Pro.

4.8.2 QuickTime framework

QuickTime framework menyediakan :

1. Encoding dan transcoding audio dan video dari format satu ke yang lainnya.
2. Decoding audio dan video, kemudian mengirimkan aliran yang dikodekan kepada subsistem audio atau grafik untuk playback. Dalam Mac OS X, QuickTime mengirimkan video playback kepada Quartz Extreme (OpenGL) Compositor.
3. Suatu arsitektur penyambungan untuk mendukung tambahan codecs (seperti DivX).

Framework mendukung jenis file berikut dan codecs dengan rapi :

Audio

1. Apple Lossless
2. Audio Interchange (AIFF)
3. Digital Audio: Audio CD - 16-bit (CDDA), 24-bit, 32-bit integer & floating point, dan 64-bit floating point
4. MIDI
5. MPEG-1 Layer 3 Audio (.mp3)
6. MPEG-4 AAC Audio (.m4a, .m4b, .m4p)
7. QDesign Music
8. Qualcomm PureVoice (QCELP)
9. Sun AU Audio
10. ULAW and ALAW Audio
11. Waveform Audio (WAV)

Video

1. 3GPP & 3GPP2 file formats
2. AVI file format
3. Bitmap (BMP) codec dan file format
4. DV file (DV NTSC/PAL and DVC Pro NTSC/PAL codecs)
5. Flash & FlashPix files
6. GIF dan Animated GIF files
7. H.261, H.263, dan H.264 codecs
8. JPEG, Photo JPEG, dan JPEG-2000 codecs dan file formats
9. MPEG-1, MPEG-2, dan MPEG-4 Video file formats dan associated codecs (seperti AVC)
10. Quartz Composer Composition (hanya.qtz, Mac OS X)
11. QuickTime Movie (.mov) dan QTVR movies
12. Sorenson Video 2 dan 3 codecs
13. Video codecs lainnya : Apple Video, Cinepak, Component Video, Graphics, dan Planar RGB
14. Masih image formats lainnya : PNG, TIFF, dan TGA
15. Cached information from streams: QTCH

4.8.3 File format QuickTime

QuickTime (.mov) memfile format yang berfungsi sebagai multimedia container file yang berisi satu atau lebih track, masing-masing yang mana menyimpan tipe data tertentu : audio, video, efek, atau teks (sebagai judul, sebagai contoh). Masing-Masing tiap track berisi suatu media stream digitally-encoded (penggunaan suatu codec spesifik) atau suatu acuan data kepada media stream terletak dalam file yang lain. Pemeliharaan track dalam suatu hierarchal struktur data terdiri dari object yang memanggil atom. Suatu atom dapat menjadi

suatu induk ke atom lainnya atau dapat berisi media atau edit data, tetapi tidak dapat dilakukan keduannya.

Kemampuan yang berisi acuan data abstrak untuk data media, dan salinan data media dari media offset dan daftar edit track berarti bahwa QuickTime terutama sekali cocok untuk editing, karena itu mampu mengedit dan mengimport pada tempatnya (tanpa mengcopy data). Format lain meliputi AIFF, DV, MP3, MPEG-1, dan Indeo video. Format container media Later-Developed lain seperti Microsoft's Advanced Systems Format atau open source Ogg dan Matroska container kekurangan abstrak ini, dan memerlukan semua data media untuk ditulis ulang setelah editing

4.8.4 QuickTime dan MPEG-4

Pada Pebruari 11, 1998 ISO menyetujui QuickTime file format berbasis MPEG-4 Part 14 (.mp4) standard container. Dengan 2000, MPEG-4 Part 14 menjadi suatu industri standart muncul pertama dengan dukungan pada QuickTime 6 pada 2002. Maka, MPEG-4 container dirancang untuk menangkap, mengedit, arsip, dan mendistribusikan media, tidak sama dengan file-as-stream pendekatan dari MPEG-1 yang sederhana dan MPEG-2.

4.8.5 Profile Support

QuickTme 6 tambahan dukungan terbatas untuk MPEG-4; khususnya encoding dan decoding menggunakan Simple Profile (SP). Fitur Advanced Simple Profile (ASP), seperti B-Frames, tanpa pendukung (pada kontras dengan, sebagai contoh, encoders seperti XviD). QuickTime 7 support H.264 encoder dan decoder.

4.8.6 Keuntungan container

Sebab kedua-duanya MOV dan MP4 container dapat menggunakan codecs MPEG-4 yang sama, mereka kebanyakan dapat bertukar tempat hanya dalam suatu lingkungan QuickTime. Bagaimanapun, MP4, menjadi standard internasional, mempunyai lebih dukungan. Ini terutama benar pada alat perangkat keras, seperti SONY PSP dan berbagai DVD player; pada sisi perangkat lunak, kebanyakan DirectShow / Video untuk Windows Codec packs yang meliputi suatu MP4 parser, tetapi bukan satupun untuk MOV.

Pada QuickTime Pro’s MPEG-4 mengekspor dialog, suatu pilihan disebut "Passthrough" mengijinkan suatu ekspor bersih ke MP4 tanpa mempengaruhi audio dan video streams. Satu pertentangan terbaru yang diumumkan oleh QuickTime 7 adalah bahwa MOV memfile format sekarang mendukung multichannel audio (yang digunakan, sebagai contoh, dalam high-definition trailler pada Apple site, saat dukungan QuickTime's untuk audio pada MP4 container yang terbatas pada stereo. Oleh karena itu multichannel audio harus re-encoded selama Mp4 export.

Apple melepaskan versi QuickTime yang pertama pada Desember 2, 1991 sebagai multimedia menambahkan untuk System Software 6 dan kemudian. Pengembang QuickTime, Bruce Leak, berlari publik demonstrasi yang pertama pada Mei 1991 Worldwide Developers Conference, di mana ia bermain Apple’s yang terkenal 1984 TV commercial pada Mac, ketika

waktu sangat mengejutkan pada pemecahan teknologi. Persaingan teknologi Microsoft's — Video untuk Windows— tidak nampak sampai November 1992.

4.9 Video conference

Video conferencing adalah penggunaan peralatan audio dan video untuk menyelenggarakan konferensi dengan orang-orang yang berada pada lokasi berbeda. Sistem pelayanan ini sekarang masih digunakan hanya untuk tingkat yang masih terbatas. Para pengguna saat ini adalah sektor-sektor bisnis dan industri seperti institusi finansial. Sistem satelit multimedia merupakan infrastruktur yang sangat cocok untuk video conferencing dibanding dengan jaringan lain karena tingkat fleksibilitasnya dan kemudahannya untuk dipasang di manapun.

Telekomunikasi Video conferencing menggunakan video dan audio untuk membawa orang pada lokasi berbeda secara bersamaan untuk suatu pertemuan. Ini bisa sesederhana seperti suatu percakapan antara dua orang pada private offices (point-to-point) atau melibatkan beberapa lokasi (multi-point) dengan lebih dari satu orang di dalam ruangan yang besar pada lokasi berbeda. Di samping audio dan visual transmission, video conferencing dapat digunakan untuk share dokumen, informasi computer-displayed, dan whiteboards.

Videoconferences Analog sederhana dibentuk sejak penemuan televisi. Sistem videoconference seperti itu terdiri dari dua sistem closed-circuit television menghubungkan via kabel. Saat penerbangan angkasa luar pertama kali, NASA menggunakan dua jalur radiofrequency (UHF atau VHF), satu pada seluruh direction. TV channel menggunakan videoconferencing jenis ini, contohnya reporting dari lokasi yang jauh. Kemudian komunikasi bergerak ke satelit menggunakan truk khusus menjadi sangat diperlukan.

Gambar 4-49 Video Conferencing Pertama Tahun 1968

Teknik ini sangat mahal, meskipun demikian, dan tidak bisa digunakan untuk aplikasi yang lebih keduniaan, seperti telemedicine, pendidikan jarak, pertemuan-pertemuan bisnis, dan seterusnya, terutama sekali di dalam aplikasi interlokal. Mencobalah pada penggunaan jaringan yang bersifat teleponi normal untuk memancarkan slow-scan video, seperti sistem yang pertama yang dikembangkan oleh AT&T, kegagalan kebanyakan dalam kaitan dengan mutu gambar yang jelek dan ketiadaan teknik tekanan video efisien. Semakin besar 1 MHZ luas bidang dan 6 Mbit/S bit rate Picturephone di tahun 1970 juga tidak menyebabkan layanan yang baik.

Teknologi inti digunakan di dalam suatu videoteleconference (VTC) sistem adalah tekanan arus video dan audio yang digital di waktu riil. Perangkat keras atau perangkat lunak yang melaksanakan tekanan disebut suatu codec (coder/decoder). Tekanan tingkat sampai 1:500 dapat dicapai.

Menghasilkan arus yang digital dari 0's dan 1's dibagi lagi ke dalam paket berlabel, yang mana kemudian adalah memancarkan melalui suatu jaringan yang digital (pada umumnya ISDN atau IP). Penggunaan audio modems dalam jalur transmisi mempertimbangkan penggunaan POT, atau Sistem Old Telephone yang sederhana, dalam beberapa kecepatan rendah aplikasi, seperti videotelephony, sebab mereka mengkonversi yang digital ke/dari gelombang analog di dalam cakupan spektrum audio.

Gambar 4-50 Sistem Video Conferencing Modern Dual Plasma

Komponen yang lain diperlukan untuk suatu VTC sistem meliputi :

1. Video input : kamera video atau webcam
2. Video output : monitor komputer, proyektor atau televisi
3. Audio input : mikropon
4. Audio output : pada umumnya pengeras suara dihubungkan dengan telepon atau display yang lain
5. Perpindahan data : jaringan telepon digital atau analog, LAN atau Internet

Pengaruh dalam videoteleconference antara lain :

1. Pada masyarakat umum

   Kecepatan tinggi Internet connectivitas telah menjadi lebih secara luas tersedia pada suatu biaya layak dan ongkos video menangkap dan teknologi pajangan telah berkurang. video sebagai konsekwensi Pribadi teleconference sistem berdasar pada suatu webcam, komputer pribadi sistem, perangkat lunak tekanan dan jalur lebar Internet connectivas sudah menjadi yang bisa mampu untuk kalayak ramai itu. Juga, perangkat keras menggunakan untuk teknologi ini telah tetap meningkatkan di dalam mutu, dan harga sudah jatuh secara dramatis. Ketersediaan freeware sering sebagai bagian dari bercakap-cakap program telah menjadikan perangkat lunak yang didasarkan videoconferencing dapat diakses bagi banyak orang.

2. Pada pendidikan

   Videoconferencing menyediakan para siswa dengan kesempatan untuk belajar dengan mengambil bagian di dalam suatu 2-way komunikasi platform. Lagipula, para guru dan pemberi ceramah/dosen dari seluruh penjuru dunia dapat dibawa ke kelas di dalam remote atau jika tidak mengasingkan tempat. Para siswa dari masyarakat berbeda dan latar belakang dapat datang bersama-sama untuk belajar sekitar satu sama lain. Para siswa bisa menyelidiki, komunikasi, meneliti dan berbagi gagasan dan informasi dengan [satu/ orang]

yang lain. Melalui/Sampai video yang conferencing para siswa dapat mengunjungi yang lain bagian dari dunia untuk berbicara dengan orang yang lain, mengunjungi suatu kebun binatang, suatu musium dan seterusnya, untuk belajar. Di sini adalah beberapa contoh bagaimana conferencing video dapat bermanfaat bagi orang di sekitar kampus, anggota fakultas/pancaindera terus berhubungan dengan kelas selagi/sedang diserbu suatu minggu pada suatu konferensi pemberi ceramah/ dosen tamu membawa ke dalam suatu kelas dari institusi yang lain peneliti bekerja sama dengan para rekan kerja pada institusi lain secara reguler tanpa kehilangan waktu dalam kaitan dengan perjalanan.

3. Pada obat-obatan dan kesehatan

Videoconferencing adalah suatu teknologi yang sangat bermanfaat untuk telemedicine dan aplikasi telenursing, seperti hasil diagnosa, berkonsultasi, transmisi dari gambaran medis, dll., di dalam waktu riil. Menggunakanlah VTC, pasien boleh menghubungi dokter dan perawat di dalam situasi rutin atau keadaan darurat, dokter dan para profesional paramedic lain dapat mendiskusikan kasus ke seberang jarak jauh.

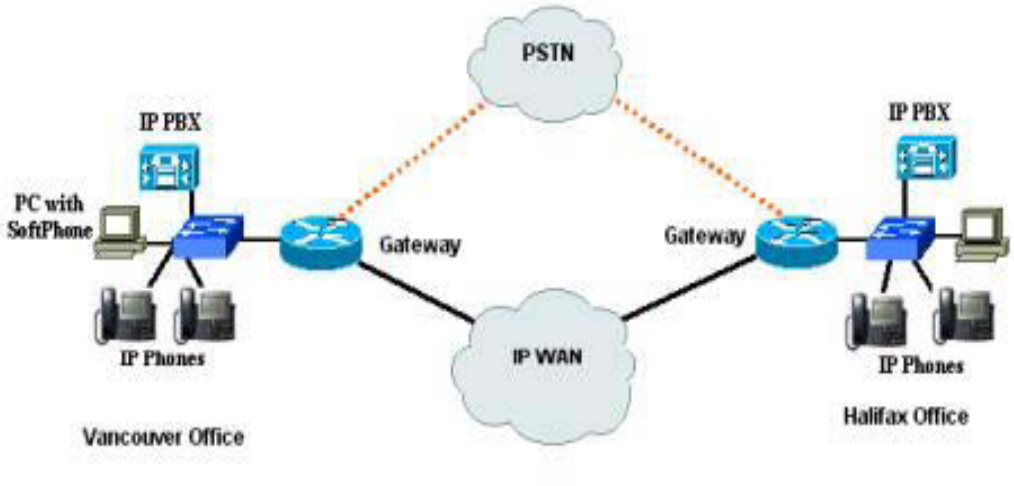
Sekeliling khusus seperti mikroskop dicoba dengan kamera digital, videoendoscopes, ultrasound medis yang imaging alat, alat pemeriksa telinga, dll., dapat digunakan bersama dengan VTC peralatan untuk memancarkan data tentang suatu pasien.

4. Pada bisnis

Videoconferencing dapat memungkinkan individu di tempat yang jauh untuk mempunyai pertemuan-pertemuan pada pemberitahuan singkat. uang dan Waktu yang digunakan untuk dibelanjakan di dalam keliling dapat digunakan untuk mempunyai pertemuan-pertemuan pendek/singkat. Teknologi seperti VOIP dapat digunakan bersama dengan desktop videoconferencing untuk memungkinkan face-to-face bisnis pertemuan-pertemuan tanpa meninggalkan desktop, terutama untuk bisnis dengan wide-spread kantor. Teknologi adalah juga digunakan untuk telecommuting, di mana karyawan bekerja dari rumah. Videoconferencing kini sedang diperkenalkan ke networking online websites, dalam rangka membantu bisnis membentuk hubungan menguntungkan dengan cepat dan secara efisien tanpa meninggalkan tempat pekerjaan mereka

4.10 Voice Over Internet Protokol (VoIP)

Voice over Internet Protocol (VoIP) adalah teknologi yang mampu melewatkan trafik suara, video dan data yang berbentuk paket melalui jaringan IP. Jaringan IP sendiri adalah merupakan jaringan komunikasi data yang berbasis packet-switch, jadi dalam bertelepon menggunakan jaringan IP atau Internet. Dengan bertelepon menggunakan VoIP, banyak keuntungan yang dapat diambil diantaranya adalah dari segi biaya jelas lebih murah dari tarif telepon tradisional, karena jaringan IP bersifat global. Sehingga untuk hubungan Internasional dapat ditekan hingga 70%. Selain itu, biaya maintenance dapat di tekan karena voice dan data network terpisah, sehingga IP Phone dapat di tambah, dipindah dan di ubah. Hal ini karena VoIP dapat dipasang di sembarang ethernet dan IP address, tidak seperti telepon tradisional yang harus mempunyai port tersendiri di Sentral atau PBX.



Gambar 4-51 VoIP

Perkembangan teknologi internet yang sangat pesat mendorong ke arah konvergensi dengan teknologi komunikasi lainnya. Standarisasi protokol komunikasi pada teknologi VoIP seperti H.323 telah memungkinkan komunikasi terintegrasi dengan jaringan komunikasi lainnya seperti PSTN.

4.10.1 Delay

Dalam perancangan jaringn VoIP, delay merupakan suatu permasalahan yang harus diperhitungkan karena kualitas suara bagus tidaknya tergantung dari waktu delay. Besarnya delay maksimum yang direkomendasikan oleh ITU untuk aplikasi suara adalah 150 ms, sedangkan delay maksimum dengan kualitas suara yang masih dapat diterima pengguna adalah 250 ms. Delay end to end adalah jumlah delay konversi suara analog – digital, delay waktu paketisasi atau bisa disebut juga delay panjang paket dan delay jaringan pada saat t (waktu). Beberapa delay yang dapat mengganggu kualitas suara dalam perancangan jaringan VoIP dapat dikelompokkan menjadi :

a. Propagation delay (delay yang terjadi akibat transmisi melalui jarak antar pengirim dan penerima).
b. Serialization delay (delay pada saat proses peletakan bit ke dalam circuit).
c. Processing delay (delay yang terjadi saat proses coding, compression, decompressior dan decoding).
d. Packetization delay (delay yang terjadi saat proses paketisasi digital voice sample.
e. Queuing delay (delay akibat waktu tunggu paket sampai dilayani).
f. Jitter buffer (delay akibat adanya buffer untuk mengatasi jitter).

Selain itu parameter – parameter lain yang mempengaruhi adalah Quality of Service (QoS), agar didapatkan hasil suara sama dengan menggunakan telepon tradisional (PSTN). Beberapa parameter yang mempengaruhi QoS antara lain :

a. Pemenuhan kebutuhan bandwidth
b. Keterlambatan data(latency)
c. Packet loss dan desequencing

d. Jenis kompresi data
e. Interopabilitas peralatan(vendor yang berbeda)
f. Jenis standar multimedia yang digunakan(H.323/SIP/MGCP)

Untuk berkomunikasi dengan menggunakan teknologi VoIP yang harus real time adalah jitter, echo dan loss packet. Jitter merupakan variasi delay yang terjadi akibat adanya selisih waktu atau interval antar kedatangan paket di penerima. Untuk mengatasi jitter maka paket data yang datang dikumpulkan dulu dalam jitter buffer selama waktu yang telah ditentukan sampai paket dapat diterima pada sisi penerima dengan urutan yang benar. Echo disebabkan perbedaan impedansi dari jaringan yang menggunakan four-wire dengan two-wire. Efek echo adalah suatu efek yang dialami mendengar suara sendiri ketika sedang melakukan percakapan.

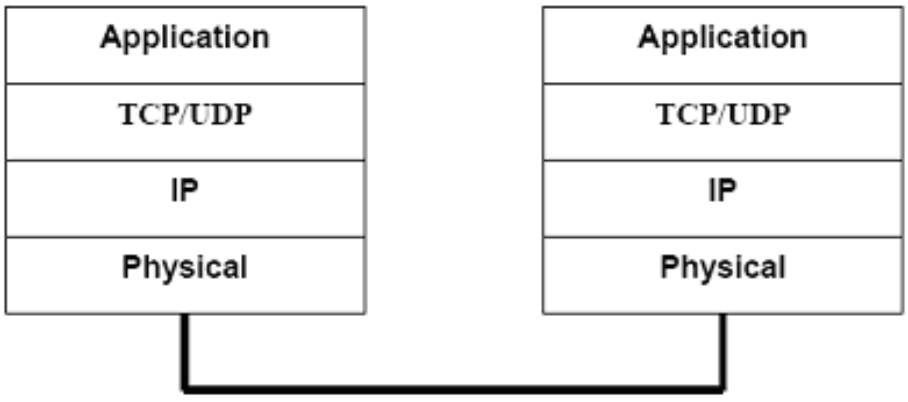
4.10.2 Bandwidth

Telah di jelaskan diatas bahwa bandwidth adalah kecepatan maksimum yang dapat digunakan untuk melakukan transmisi data antar komputer pada jaringan IP atau internet. Dalam perancangan VoIP, bandwidth merupakan suatu yang harus diperhitungkan agar dapat memenuhi kebutuhan pelanggan yang dapat digunakan menjadi parameter untuk menghitung jumlah peralatan yang di butuhkan dalam suatu jaringan. Perhitungan ini juga sangat diperlukan dalam efisiensi jaringan dan biaya serta sebagai acuan pemenuhan kebutuhan untuk pengembangan di masa mendatang. Packet loss (kehilangan paket data pada proses transmisi) dan desequencing merupakan masalah yang berhubugnan dengan kebutuhan bandwidth, namun lebih dipengaruhi oleh stabilitas rute yang dilewati data pada jaringan, metode antrian yang efisien, pengaturan pada router, dan penggunaan kontrol terhadap kongesti (kelebihan beban data) pada jaringan. Packet loss terjadi ketika terdapat penumpukan data pada jalur yang dilewati dan menyebabkan terjadinya overflow buffer pada router.

Protokol-Protokol Penunjang Jaringan VoIP

a. Protocol TCP/IP

TCP/IP (Transfer Control Protocol/Internet Protocol) merupakan sebuah protokol yang digunakan pada jaringan Internet. Protokol ini terdiri dari dua bagian besar, yaitu TCP dan IP. Ilustrasi pemrosesan data untuk dikirimkan dengan menggunakan protokol TCP/IP diberikan pada gambar dibawah ini



Gambar 4-52 Mekanisme Protokol TCP/IP

b. Application layer

Fungsi utama lapisan ini adalah pemindahan file. Perpindahan file dari sebuah sistem ke system lainnya yang berbeda memerlukan suatu sistem pengendalian untuk menangatasi adanya ketidak kompatibelan sistem file yang berbeda – beda. Protokol ini berhubungan dengan aplikasi. Salah satu contoh aplikasi yang telah dikenal misalnya HTTP (Hypertext Transfer Protocol) untuk web, FTP (File Transfer Protocol) untuk perpindahan file, dan TELNET untuk terminal maya jarak jauh.

c. Transmission Control Protocol (TCP)

Dalam mentransmisikan data pada layer Transpor ada dua protokol yang berperan yaitu TCP dan UDP. TCP merupakan protokol yang connection-oriented yang artinya menjaga reliabilitas hubungan komunikadasi end-to-end. Konsep dasar cara kerja TCP adalah mengirm dan menerima segment – segment informasi dengan panjang data bervariasi pada suatu datagram internet. TCP menjamin realibilitas hubungan komunikasi karena melakukan perbaikan terhadap data yang rusak, hilang atau kesalahan kirim. Hal ini dilakukan dengan memberikan nomor urut pada setiap oktet yang dikirimkan dan membutuhkan sinyal jawaban positif dari penerima berupa sinyal ACK (acknoledgment). Jika sinyal ACK ini tidak diterima pada interval pada waktu tertentu, maka data akan dikirikmkan kembali. Pada sisi penerima, nomor urut tadi berguna untuk mencegah kesalahan urutan data dan duplikasi data. TCP juga memiliki mekanisme flow control dengan cara mencantumkan informasi dalam sinyal ACK mengenai batas jumlah oktet data yang masih boleh ditransmisikan pada setiap segment yang diterima dengan sukses.

Dalam hubungan VoIP, TCP digunakan pada saat signaling, TCP digunakan untuk menjamin setup suatu call pada sesi signaling. TCP tidak digunakan dalam pengiriman data suara pada VoIP karena pada suatu komunikasi data VoIP penanganan data yang mengalami keterlambatan lebih penting daripada penanganan paket yang hilang.

d. User Datagram Protocol (UDP)

UDP yang merupakan salah satu protocol utama diatas IP merupakan transport protocol yang lebih sederhana dibandingkan dengan TCP. UDP digunakan untuk situasi yang tidak mementingkan mekanisme reliabilitas. Header UDP hanya berisi empat field yaitu source port, destination port, length dan UDP checksum dimana fungsinya hampir sama dengan TCP, namun fasilitas checksum pada UDP bersifat opsional. UDP pada VoIP digunakan untuk mengirimkan audio stream yang dikrimkan secara terus menerus. UDP digunakan pada VoIP karena pada pengiriman audio streaming yang berlangsung terus menerus lebih mementingkan kecepatan pengiriman data agar tiba di tujuan tanpa memperhatikan adanya paket yang hilang walaupun mencapai 50% dari jumlah paket yang dikirimkan.(VoIP) fundamental, Davidson Peters, Cisco System,163) karena UDP mampu mengirimkan data streaming dengan cepat, maka dalam teknologi VoIP UDP merupakan salah satu protokol penting yang digunakan sebagai header pada pengiriman data selain RTP dan IP. Untuk mengurangi jumlah paket yang hilang saat pengiriman data (karena tidak terdapat mekanisme pengiriman ulang) maka pada teknolgi VoIP pengiriman data banyak dilakukan pada private network.

e. Internet Protocol (IP)

Internet Protocol didesain untuk interkoneksi sistem komunikasi komputer pada jaringan *paketswitched*. Pada jaringan TCP/IP, sebuah komputer diidentifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda satu sama lainnya. Hal ini dilakukan untuk mencegah kesalahan pada transfer data. Terakhir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protokol ini bertugas untuk menangani pendeteksian kesalahan pada saat transfer data. Untuk komunikasi datanya, Internet Protokol mengimplementasikan dua fungsi dasar yaitu addressing dan fragmentasi. Salah satu hal penting dalam IP dalam pengiriman informasi adalah metode pengalamatan pengirim dan penerima. Saat ini terdapat standar pengalamatan yang sudah digunakan yaitu IPv4 dengan alamat terdiri dari 32 bit. Jumlah alamat yang diciptakan dengan IPv4 diperkirakan tidak dapat mencukupi kebutuhan pengalamatan IP sehingga dalam beberapa tahun mendatang akan diimplementasikan sistim pengalamatan yang baru yaitu IPv6 yang menggunakan sistim pengalamatan 128 bit.

4.10.3 Aplikasi VoIP

Salah satu aplikasi VoIP yang tersedia adalah Skype. Skype adalah software aplikasi komunikasi suara berbasis IP melalui internet antara sesama pengguna Skype. Pada saat menggunakan Skype maka pengguna Skype yang sedang online akan mencari pengguna Skype lainnya lalu mulai membangun jaringan untuk menemukan pengguna-pengguna lainnya. Skype memiliki berbagai macam feature yang dapat memudahkan penggunanya. Skype juga dilengkapi dengan SkypeOut dan SkypeIn yang memungkinkan pengguna Skype untuk berhubungan dengan pengguna telepon konvensional dan telepon genggam.

Skype menggunakan protokol HTTP untuk berkomunikasi dengan Skype server untuk otentikasi username/password dan registrasi dengan Skype directory server. Versi modifikasi dari protokol HTTP digunakan untuk berkomunikasi dengan sesama Skype client. Keuntungan yang dimiliki aplikasi ini adalah tersedianya layanan keamanan dalam pentransmisian data yang berupa suara.

4.10.4 Keuntungan VoIP

1. Biaya lebih rendah untuk sambungan langsung jarak jauh. Penekanan utama dari VoIP adalah biaya. Dengan dua lokasi yang terhubung dengan internet maka biaya percakapan menjadi sangat rendah.
2. Memanfaatkan infrastruktur jaringan data yang sudah ada untuk suara. Berguna jika perusahaan sudah mempunyai jaringan. Jika memungkinkan jaringan yang ada bisa dibangun jaringan VoIP dengan mudah. Tidak diperlukan tambahan biaya bulanan untuk penambahan komunikasi suara.
3. Penggunaan bandwidth yang lebih kecil daripada telepon biasa. Dengan majunya technologi penggunaan bandwidth untuk voice sekarang ini menjadi sangat kecil.

Tehnik pemampatan data memungkinkan suara hanya membutuhkan sekitar 8 kbps bandwidth.

4. Memungkinkan digabung dengan jaringan telepon lokal yang sudah ada. Dengan adanya gateway bentuk jaringan VoIP bisa disambungkan dengan PABX yang ada dikantor. Komunikasi antar kantor bisa menggunakan pesawat telepon biasa.
5. Berbagai bentuk jaringan VoIP bisa digabungkan menjadi jaringan yang besar. Contoh di Indonesia adalah VoIP Merdeka.
6. Variasi penggunaan peralatan yang ada, misal dari PC sambung ke telephone biasa, IP phone handset.

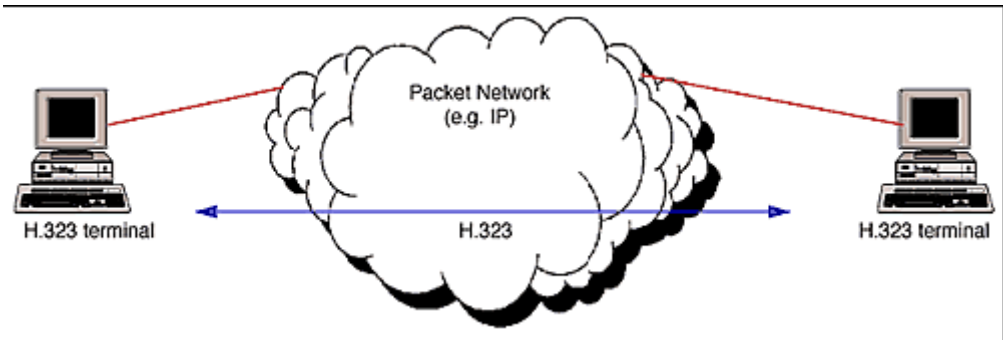
4.10.5 Kelemahan VoIP

1. Kualitas suara tidak sejernih Telkom. Merupakan efek dari kompresi suara dengan bandwidth kecil maka akan ada penurunan kualitas suara dibandingkan jaringan PSTN konvensional.
2. Ada jeda dalam berkomunikasi. Proses perubahan data menjadi suara, jeda jaringan, membuat adanya jeda dalam komunikasi dengan menggunakan VoIP. Kecuali jika menggunakan koneksi Broadband (lihat di poin atas).
3. Jika belum terhubung secara 24 jam ke internet perlu janji untuk saling berhubungan.
4. Jika memakai internet dan komputer dibelakang NAT (Network Address Translation), maka dibutuhkan konfigurasi khusus untuk membuat VoIP tersebut berjalan
5. Tidak pernah ada jaminan kualitas jika VoIP melewati internet.
6. Peralatan relatif mahal. Peralatan VoIP yang menghubungkan antara VoIP dengan PABX (IP telephony gateway) relatif berharga mahal. Diharapkan dengan makin populernya VoIP ini maka harga peralatan tersebut juga mulai turun harganya.
7. Berpotensi menyebabkan jaringan terhambat/Stuck. Jika pemakaian VoIP semakin banyak, maka ada potensi jaringan data yang ada menjadi penuh jika tidak diatur dengan baik. Pengaturan bandwidth adalah perlu agar jaringan di perusahaan tidak menjadi jenuh akibat pemakaian VoIP.
8. Penggabungan jaringan tanpa dikoordinasi dengan baik akan menimbulkan kekacauan dalam sistem penomoran.

4.10.6 H.323

VoIP dapat berkomunikasi dengan sistem lain yang beroperasi pada jaringan packet-switch. Untuk dapat berkomunikasi dibutuhkan suatu standar sistem komunikasi yang kompatibel satu sama lain. Salah satu standar komunikasi pada VoIP menurut rekomendasi International Telecommunications Union-Telecommunications (ITU-T) adalah H.323 (1995-1996). Standar H.323 terdiri dari komponen, protokol, dan prosedur yang menyediakan komunikasi multimedia melalui jaringan packet-based. Bentuk jaringan packet-based yang dapat dilalui antara lain jaringan internet, Internet Packet Exchange (IPX)-based, Local Area Network (LAN), dan Wide Area Network (WAN). H.323 dapat digunakan untuk layanan –

layanan multimedia seperti komunikasi suara (IP telephony), komunikasi video dengan suara (video telephony), dan gabungan suara, video dan data.



Gambar 4-53 Terminal Jaringan Paket

Tujuan desain dan pengembangan H.323 adalah untuk memungkinkan interoperabilitas dengan tipe terminal multimedia lainnya. Terminal dengan standar H.323 dapat berkomunikasi dengan terminal H.320 pada N-ISDN, terminal H.321 pada ATM, dan terminal H.324 pada Public Switched Telephone Network (PSTN). Terminal H.323 memungkinkan komunikasi real time dua arah berupa suara , video dan data.

4.10.6.1 Arsitektur H.323

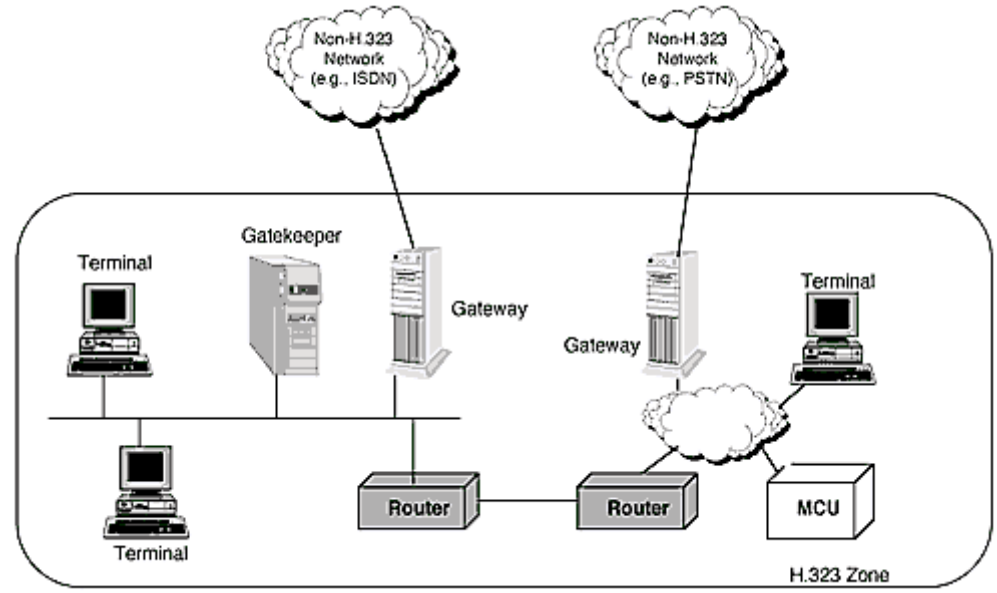
Standar H.323 terdiri dari 4 komponen fisik yg digunakan saat menghubungkan komunikasi multimedia point-to-point dan point-to-multipoint pada beberapa macam jaringan:

1. Terminal
2. Gateway
3. Gatekeeper
4. Multipoint Control Unit (MCU)

Keterangan :

1. Terminal, digunakan untuk komunikasi multimedia real time dua arah . Terminal H.323 dapat berupa personal computer (PC) atau alat lain yang berdiri sendiri yang dapat menjalankan aplikasi multimedia.
2. Gateway digunakan untuk menghubungkan dua jaringan yang berbeda yaitu antara jaringan H.323 dan jaringan non H.323, sebagai contoh gateway dapat menghubungkan dan menyediakan komunikasi antara terminal H.233 dengan jaringan telepon , misalnya: PSTN. Dalam menghubungkan dua bentuk jaringan yang berbeda dilakukan dengan menterjemankan protokol-protokol untuk call setup dan release serta mengirimkan informasi antara jaringan yang terhubung dengan gateway. Namun demikian gateway tidak dibutuhkan untuk komunikasi antara dua terminal H.323.
3. Gatekeeper dapat dianggap sebagai otak pada jaringan H.323 karena merupakan titik yang penting pada jaringan H.323.

4. MCU digunakan untuk layanan konferensi tiga terminal H.323 atau lebih. Semua terminal yang ingin berpartisipasi dalam konferensi dapat membangun hubungan dengan MCU yang mengatur bahan-bahan untuk konferensi, negosiasi antara terminal-terminal untuk memastikan audio atau video coder/decoder (CODEC). Menurut standar H.323 , sebuah MCU terdiri dari sebuah Multipoint Controller (MC) dan beberapa Multipoint Processor (MP). MC menangani negoisasi H.245 (menyangkut pensinyalan) antar terminal – terminal untuk menenetukan kemampuan pemrosesan audio dan video . MC juga mengontrol dan menentukan serangkaian audio dan video yang akan multicast. MC tidak menghadapi secara langsung rangkainan media tersebut. Tugas ini diberikan pada MP yang melakukan mix, switch, dan memproses audio, video, ataupun bit – bit data. Gatekeeper, gateway, dan MCU secara logik merupakan komponen yang terpisah pada standar H.323 tetapi dapat diimplementasikan sebagai satu alat secara fisik.



Gambar 4-54 Arsitektur H.323

4.10.6.2 Protocol H.323

Pada H.323 terdapat beberapa protocol dalam pengiriman data yang mendukung agar data terkirim real-time. Dibawah ini dijelaskan beberapa protocol pada layer network dan transport.

4.10.6.3 Keunggulan protocol H.323

a. Standard codec

H.323 membuat standard untuk kompresi dan dekompresi untuk aliran data video dan audio, untuk memastikan bahwa peralatan yang berbeda tetap mempunyai dukungan terhadap hal teknis yang sama.

b. Interoperabilitas

User yang ingin melaksanakan conference tidak harus khawati akan kompatibilitasan pada sisi penerima. Selain memastikan bahwa penerima dapat mendekompresi informasi yang dikirim, H.323 juga menembangkan metode untuk menerima client untuk berkomunikasi, yang sama kemampuannya dengan pengirim.

c. Network Independence

H.323 didesain agar dapat berjalan di lapisan atas dari arsitektur jaringan secara umum. Karena teknologi jaringan mengalami evolusi, dan teknik pengaturan bandwidth meningkat, maka solusi berbasis H.323 dirasakan akan dapat mengikuti perkambangan tersebut.

d. Platform dan Application Independence

H.323 tidak terikat pada salah satu jenis perangkat keras ataupun sistem operasi. Platform yang compliant dengan H.323 akan tersedia dalam berbagai ukuran dan bentuk, termasuk PC yang video-enabled, platform yang terdedikasi, peralatan telepon yang IP-enabled, maupun TV kabel.

e. Dukungan terhadap multipoint

Walaupun pada kenyataannya H.323 dapat mendukung conference sampai tiga atau lebih endpoint tanpa membutuhkan multipoint control unit yang soesial, sebenarnya MCU menyediakan arsitektur yang fleksibel dan powerful untuk conference multipoint. Kemampuan multipoint dapat disertakan dalam tiap komponen sistem H.323.

f. Bandwidth management

Trafik video dan audio adalah trafik yang membutuhkan bandwidth yang besar dan kebanyakan dapat membuat jaringan komunikasi data terhambat. H.323 berusaha menemukan solusi terhadap permasalahan ini dengan mempersiapkan pengaturan bandwidth (bandwidth management). Pengatur jaringan (network manager) dapat membatasi jumlah user yang tersambung ke jaringan H.323 secara bersamaan, sesuai dengan bandwidth yang tersedia untuk aplikasi H.323. batasan tersebut memastikan bahwa titik kritis dari trafik tidak akan mungkin dilewati.

g. Dukungan terhadap multicast

H.323 mendukung pengangkutan multicast dalam conference multipoint. Multicast mengirim paket tunggal ke subset tujuan dalam jaringan tanpa replikasi. Sedangkan unicast mengirim multiple transmisi point-to-point, dan broadcast mengirimkan paket ke semua tujuan. Dalam unicast atau broadcast, jaringan digunakan tidak efisien karena banyaknya paket yang direplikasi sepanjang jaringan. Transmisi multicast menggunakan bandwidth lebih efisien karena semua terminal dalam grup multicast hanya membaca aliran data yang tunggal.

h. Fleksibel

Sebuah conference H.323 dapat menyertakan sejumlah endpoint dengan kemampuan yang berbeda. Sebagai contoh, sebuah terminal yang berkemampuan suara saja dapat berpartisipasi dalam conference dengan terminal yang mempunyai kemampuan video dan data. Lebih jauh lagi, terminal multimedia H.323 dapat membagi porsi data intuk

conference video dengan terminal yang berkemampuan T.120 (data) saja, sembari membagi suara, data dan video dengan terminal H.323 lainnya.

i. Inter-Network Conferencing

Banyak user yang menginginkan untuk melaksanakan conference dari sebuah LAN ke jarak yang jauh. Oleh karena itu, H.323 berusaha membangun sambungan antara sistem desktop berbasis LAN dengan sistem grup berbasis ISDN. H.323 menggunakan teknologi codec yang umum untuk tiap standard video conference yang berbeda untuk mengurangi delay transcoding dan untuk menyediakan kinerja yang optimal.

4.10.7 Session Initition Protokol (SIP)

SIP adalah suatu signalling protokol pada layer aplikasi yang berfungsi untuk membangun, memodifikasi, dan mengakhiri suatu sesi multimedia yang melibatkan satu atau beberapa pengguna. Sesi multimedia adalah pertukaran data antar pengguna yang meliputi suara, video, atau text. SIP tidak menyediakan layanan secara langsung, tetapi menyediakan fondasi yang dapat digunakan oleh protokol aplikasi lainnya untuk memberikan layanan yang lebih lengkap bagi pengguna, misalnya dengan RTP (Real Time Transport Protocol) untuk transfer data secara real-time, dengan SDP (Session Description Protocol) untuk mendeskripsikan sesi multimedia, dengan MEGACO (Media Gateway Control Protocol) untuk komunikasi dengan PSTN (Public Switch Telephone Network). Meskipun demikian, fungsi dan operasi dasar SIP tidak tergantung pada protokol tersebut. SIP juga tidak tergantung pada protokol layer transport yang digunakan.

Pembangunan suatu komunikasi multimedia dengan SIP dilakukan melalui beberapa tahap :

1. User location : menentukan lokasi pengguna yang akan berkomunikasi.
2. User availability : menentukan tingkat keinginan pihak yang dipanggil untuk terlibat dalam komunikasi.
3. User capability : menentukan media maupun parameter yang berhubungan dengan media yang akan digunakan untuk komunikasi.
4. Session setup : “ringing”, pembentukan hubungan antara pihak pemanggil dan pihak yang dipanggil.
5. Session management : meliputi transfer, modifikasi, dan pemutusan sesi.

4.10.7.1 Susunan Protocol SIP

Protocol SIP didukung oleh beberapa protocol, antara lain RSVP untuk melakukan pemesanan pada jaringan, RTP dan RTCP untuk mentransmisikan media dan mengetahui kualitas layanan, serta SDP (Session Description Protocol) untuk mendeskripsikan sesi media dalam suatu komunikasi. Secara default, SIP menggunakan protocol UDP tetapi pada beberapa kasus dapat juga menggunakan TCP sebagai protocol transport.

4.10.7.2 Komunikasi dengan SIP

Komunikasi pada SIP dilakukan dengan mengirimkan message yang berbasis HTTP. Setiap pengguna mempunyai alamat yang dinyatakan dengan SIP-URI (Uniform Resource Identification).

Contoh SIP URI : sip: martin@bandung.com

Selain itu, alamat juga dapat dituliskan dalam tel-URL yang kemudian dikonversikan menjadi SIP-URI dengan parameter 'user' diisi 'phone'.

Contoh : tel: +62-22-2534119 ekivalen dengan

sip: +62-22-2534119@bandung.com ; user=phone

Hubungan yang dibangun oleh SIP pada proses signalling bersifat clientserve. Dengan demikian ada 2 jenis message, yaitu request dan response.

Tabel 4-7 SIP Request Message

SIP Request Messages	***Descriptions***
INVITE	Indicates that the user or service is being invited to participate in a session.
ACK	Confirms that the client has received a final response to an INVITE request.
BYE	Indicate the user wishes to terminate the call.
CANCEL	Cancels a pending request but does not affect a completed request.
REGISTER	Register the address listed in the To header field with a SIP server.
OPTIONS	Queries the capability of the servers.
INFO	Allows for the carrying of the session related control information that is generated during a session.

Tabel 4-8 SIP Respond Message

SIP Response Message Types	***Description***
1xx	Information Responses For example: 180 Ringing
2xx	Successful Responses For example: 200 OK
3xx	Redirection Responses For example: 302 Moved Temporarily
4xx	Request Failures Responses For example: 403 Forbidden
5xx	Server Failure Responses For example: 504 Gateway Time-out
6xx	Global Failure Responses For example: 600 Busy Everywhere

4.10.7.3 Komponen SIP

Dalam hubungannya dengan IP Telephony, ada dua komponen yang ada dalam sistem SIP, yaitu :

1. User agent

   User agent merupakan sistem akhir (end system) yang digunakan untuk berkomunikasi. User agent terdiri atas 2 bagian, yaitu :

a. User Agent Client (UAC)

   UAC merupakan aplikasi pada client yang didesain untuk memulai SIP request.

b. User Agent Server (UAS)

   UAS merupakan aplikasi server yang memberitahukan user jika menerima request dan memberikan respon terhadap request tersebut. Respon dapat berupa menerima atau menolak request.

2. Network server

   Agar user pada jarinagan SIP dapat memulai suatu panggilan dan dapat pula dipanggil maka user terlebih dahulu melakukan registrasi agar lokasinya dapat diketahui. Registrasi dapat dilakukan dengan mengirimkan pesan REGISTRASI ke server SIP. Lokasi user dapat berbeda-beda sehingga untuk mendapatkan lokasi user yang aktual diperlukan location server. Pada jaringan SIP, ada 2 tipe network server, yaitu :

a. Proxy server

   Proxy server adalah server yang menerima request, mengolahnya, serta meneruskan request yang diterimanya ke next hop server setelah mengubah beberapa header pada pesan request. Next hop server dapat berupa server SIP atau server lainnya dimana proxy server tidak perlu tahu. Proxy server dapat berfungsi client dan server karena proxy server dapat memberikan request dan respon.

b. Redirect server

   Komponen ini merupakan server yang menerima pesan request serta memberikan respon terhadap request tersebut yang berisi alamat dari next hop server.

4.10.7.4 Aplikasi SIP

a. Voice over Internet Protocol (VoIP)
b. Konferensi multimedia
c. Text-messaging
d. Event-notification -> voicemail notification, callback notification
e. Unified Messaging -> voicemail2email

4.10.7.5 Kelebihan SIP

1. General-purpose

   SIP dapat diintegrasikan dengan protokol stadar IETF lainnya untuk membuat suatu aplikasi yang berbasis SIP.

2. Arsitektur yang terdistribusi dan scalable

   a. Proxy-server

      Menerima request dari user-agent-client, melakukan autentikasi, memprosesnya, dan mengirimkan request tersebut kepada hop selanjutnya atas nama client tersebut.

   b. Redirect-server

      Menerima request dari client, membandingkan alamat tujuan yang ingin dicapai, setelah ditemukan, alamat tersebut dikembalikan kepada client.

   c. Registrar-server

      Menerima REGISTER request dari client.

   d. Location-server

      Menyimpan data yang diperoleh dari registrar-server. Location-server digunakan oleh proxy/redirect server untuk mendapatkan informasi mengenai alamat tujuan ya ng ingin dicapai.

   Dengan adanya fungsi yang terdistribusi, proses pengembangan pada salah satu komponen tidak akan mengganggu komponen lainnya (scalable).

3. Sederhana

   Pengiriman message berbasis HTTP (text-based), bukan binary-based. Hal ini menyebabkan SIP mudah diimplementasikan.

4. Mobility

   a. Seorang pengguna dapat menerima message/call yang ditujukan kepadanya.meskipun berpindah dari satu lokasi ke lokasi lainnya. Proxyserver akan meneruskan call ke lokasi pengguna pada saat ini.

   b. Device yang digunakan dapat berupa PC, baik di rumah maupun di kantor, wireless phone, IP-phone, ataupun telepon biasa.

5. Layanan dapat dibuat dengan Call Processing Language (CPL) dan Common Gateway Interface (CGI), antara lain :

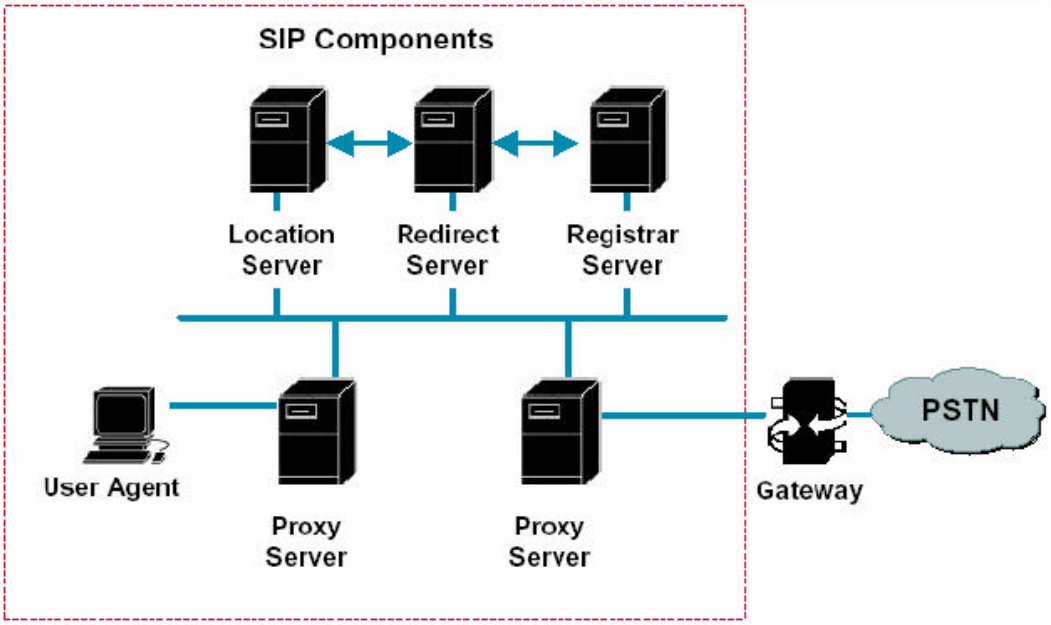
   ♋ Call waiting, call forwarding, call blocking (basic feature)

   ♌ Call-forking (melakukan call kepada beberapa endpoint)

   ♍ Instant-messaging

   ♎ Find-me / follow-me

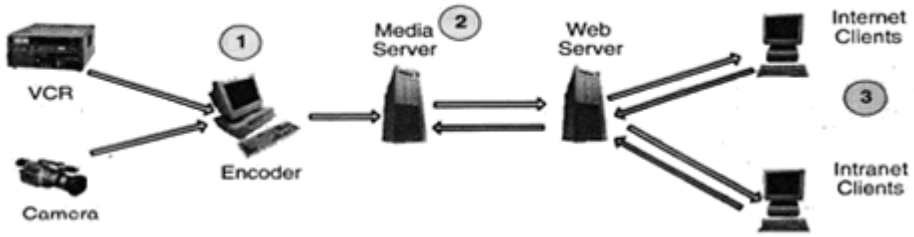
4.10.7.6 Arsitektur Sistem berbasis SIP



Gambar 4-55 Arsitektur SIP

4.11 SOAL dan JAWABAN

1. Sebutkan protokol apa saja yang terdapat pada multimedia!
2. Bagaimana cara mengatasi jitter ketika berkomunikasi menggunakan VoIP?
3. Sebutkan 3 keuntungan dan kelemahan dari VoIP?
4. Sebutkan beberapa aplikasi dari multimedia !
5. Jelaskan cara kerja dari jaringan multimedia streaming di bawah ini !



Jawab :

1. Protokol yang terdapat pada multimedia yaitu :
   a. Real Time Protocol (RTP)
   b. Real Time Control Protocol (RTCP)
   c. Resource Reservation Protocol (RSVP)
   d. Real Time Streaming Protocol (RTSP)

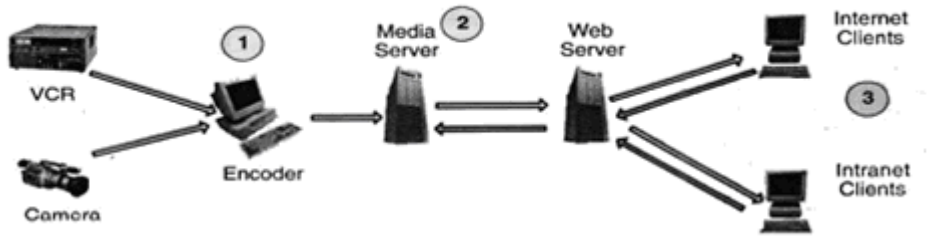
2. Untuk mengatasi jitter maka paket data yang datang dikumpulkan dulu dalam jitter buffer selama waktu yang telah ditentukan sampai paket dapat diterima pada sisi penerima dengan urutan yang benar.

3. Keuntungannya :
   α. Biaya lebih rendah untuk sambungan langsung jarak jauh.
   β. Memanfaatkan infrastruktur jaringan data yang sudah ada untuk suara.
   χ. Penggunaan bandwidth yang lebih kecil daripada telepon biasa.

   Kelemahannya :
   α. Kualitas suara tidak sejernih Telkom.
   β. Ada jeda dalam berkomunikasi.
   χ. Peralatan relatif mahal.

4. Aplikasi Multimedia :
   1. Audio
      a. Speech (CELP – type codecs)
      b. Music (MP3, WAV, WMA, Real)
   2. Video (MPEG –1, 2, 4)
   3. Video conference
   4. QuickTime
   5. Streaming done using HTTP/TCP (MP3), or RTP/UDP (Video).

5. Streaming media adalah suatu teknologi yang mampu mengirimkan file audio dan video digital secara real time pada jaringan komputer.



   1. Data yang berasal dari VCR dan Camera diambil/dicapture oleh Encoder (computer).
   2. Encoder mengirimkan sinyal ke media server atau media server pulls media-on-demand dari storage/tempat penyimpanan.

User meminta media dari web server, web server meminta streams dari media server dan mengirimkan kembali ke user.

4.12 REFERENSI

[1] http://www.wikipedia.org//
[2] http://www.google.co.id//

BAB 5. FIREWALL DAN NAT

Elly Kurniawati H [1)], Nur Indah Fatmawati [1)], Ayutya Agastya [1)]
Politeknik Elektronika Negeri Surabaya

ABSTRAK

Misi awal Internet adalah sebagai jaringan komunikasi non-profit. Pada awalnya, Internet didesain tanpa memperhatikan dunia bisnis. Kemudian hal ini menjadi masalah sekarang dan di masa depan. Dengan semakin banyaknya penghuni Internet, baik pencari informasi maupun penyedia informasi, ada beberapa permasalahan yang timbul, diantaranya adalah masalah kemanan dan masalah kebutuhan akan pengalamatan di internet yang makin membengkak. Adalah tugas dari operator jaringan yang bersangkutan, untuk menekan resiko tersebut seminimal mungkin. Pemilihan strategi dan kecakapan administrator jaringan ini, akan sangat membedakan apakah suatu jaringan mudah ditembus atau tidak. Untuk masalah keamanan, Firewall merupakan salah satu alat yang dapat digunakan untuk mengimplementasikan kebijakan security (security policy). Sedangkan kebijakan security, dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan implikasi security-nya. Semakin ketat kebijakan security, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan semakin banyak fasilitas yang tersedia atau sedemikian sederhananya konfigurasi yang diterapkan, maka semakin mudah orang orang 'usil' dari luar masuk kedalam sistem (akibat langsung dari lemahnya kebijakan security). Sedangkan untuk permasalahan keterbatasan pengalamatan untuk internet, dapat diatasi dengan menggunakan NAT. Logika sederhana untuk penghematan IP *address* ialah dengan meng-*share* suatu nomor IP *address* valid ke beberapa *client* IP lainnya. Atau dengan kata lain beberapa komputer bisa mengakses Internet walau kita hanya memiliki satu IP *address* yang valid. Salah satu Mekanisme tersebut disediakan oleh *Network Address Translation* (NAT).

5.1 Pendahuluan tentang Firewall

Ibarat sebuah rumah yang memiliki pagar sebagai pelindungnya, baik dari kayu, tembok beton, kawat berduri ataupun kombinasi beberapa jenis pagar, maka tak pula mengherankan apabila sebuah computer yang merupakan sebuah tempat vital dalam komunikasi data yang menyimpan semua harta dan benda yang kita miliki juga patut kita lindungi. Tetapi, apa pula jenis pagar yang akan kita pakai untuk membentengi komputer/jaringan pribadi kita terhadap semua ancaman khususnya dari luar terhadap semua property pribadi kita yang terdapat didalamnya? Pernah dengar istilah *Tembok Api?* sedikit terdengar lucu apabila diartikan per suku kata dari kata "*firewall*". Tetapi apa dan bagaimanakah firewall itulah yang akan kita coba kupas dalam tulisan ini.

5.2 FIREWALL

5.2.1 Pengertian Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) anda.

Konfigurasi sederhananya:

pc (jaringan local) == ***firewall*** == **internet** (jaringan lain)

Firewall untuk komputer, pertama kali dilakukan dengan menggunakan prinsip "non-routing" pada sebuah Unix host yang menggunakan 2 buah network interface card, network interface card yang pertama di hubungkan ke internet (jaringan lain) sedangkan yang lainnya dihubungkan ke pc (jaringan lokal)(dengan catatan tidak terjadi "route" antara kedua network interface card di pc ini). Untuk dapat terkoneksi dengan Internet(jaringan lain) maka harus memasuki server firewall (bisa secara remote, atau langsung), kemudian apabila perlu untuk menyimpan file/data maka dapat menaruhnya sementara di pc firewall anda, kemudian mengkopikannya ke pc(jaringan lokal). Sehingga internet(jaringan luar) tidak dapat berhubungan langsung dengan pc(jaringan lokal). Dikarenakan masih terlalu banyak kekurangan dari metoda ini, sehingga dikembangkan berbagai bentuk, konfigurasi dan jenis firewall dengan berbagai policy(aturan) didalamnya.

Firewall secara umum di peruntukkan untuk melayani :

Mesin/Komputer

Setiap mesin/komputer yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.

Jaringan

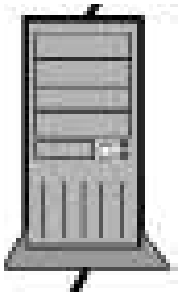
Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

5.2.2 Bentuk fisik firewall dapat berupa:

a. Router, seperti ditunjukkan pada gambar berikut:

Gambar 5-56 Router

b. PC Router, seperti ditunjukkan pada gambar berikut:



Gambar 5-57 PC Router

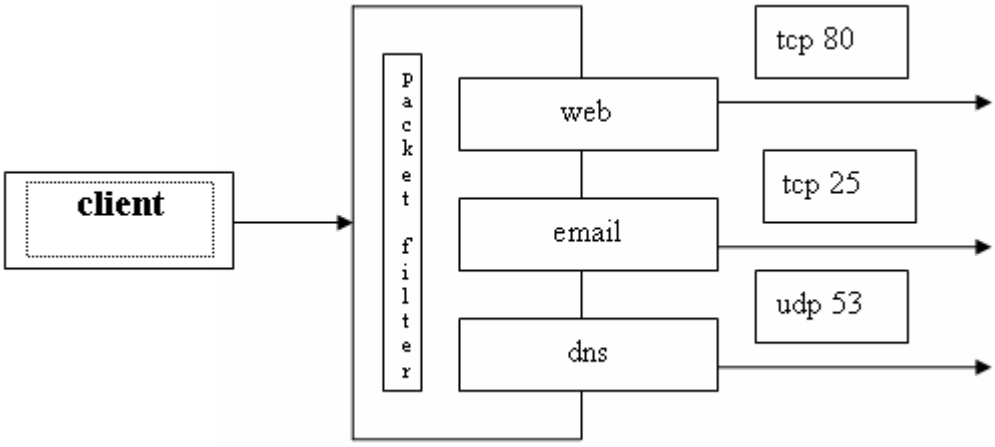
5.2.3 Karakteristik sebuah firewall

- Seluruh hubungan/kegiatan dari dalam ke luar , harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
- Hanya Kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.
- Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan system yang relatif aman

5.2.4 Teknik yang digunakan oleh sebuah firewall

1. Service control (kendali terhadap layanan)

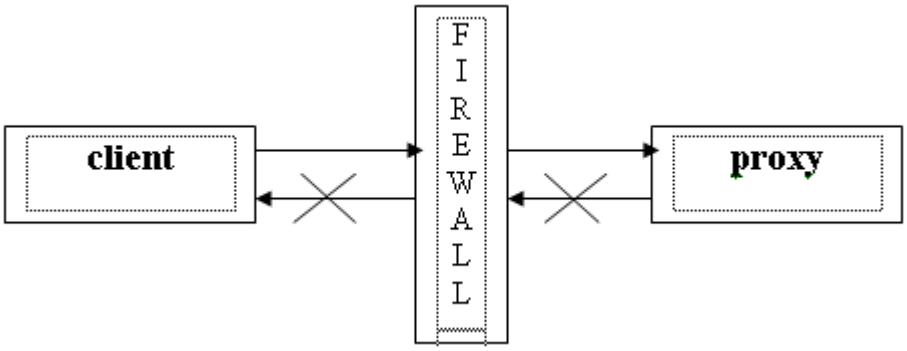
Berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall. Biasanya firewall akan mencek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi software pada server itu sendiri , seperti layanan untuk web ataupun untuk mail. Diagram untuk teknik service control ditunjukkan pada gambar berikut:



Gambar 5-58 Diagram teknik service control

2. Direction Conrol (kendali terhadap arah)

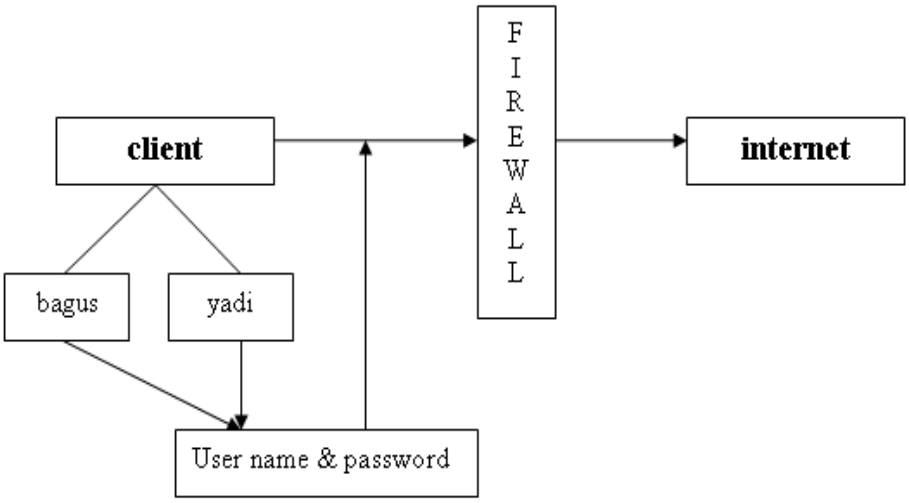
Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall. Diagram untuk teknik service control ditunjukkan pada gambar berikut:



Gambar 5-59 Diagram teknik direction control

3. User control (kendali terhadap pengguna)

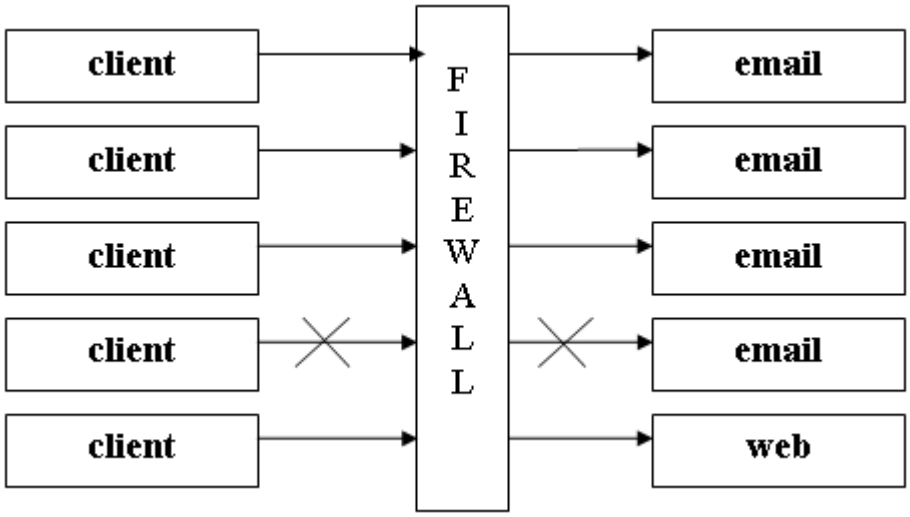
Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di ijinkan untuk melewati firewall. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar. Diagram untuk teknik service control ditunjukkan pada gambar berikut:



Gambar 5-60 Diagram teknik user control

4. Behavior Control (kendali terhadap perlakuan)

Berdasarkan seberapa banyak layanan itu telah digunakan. Misal, firewall dapat memfilter email untuk menanggulangi/mencegah spam. Diagram untuk teknik service control ditunjukkan pada gb.6 berikut:



Gambar 5-61 Diagram teknik direction control

5.2.5 Tipe-Tipe Firewall

Packet Filtering Router

Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan atau di tolak. Penyaringan packet ini di konfigurasikan untuk menyaring packet yang akan ditransfer secara dua arah (baik dari dan ke jaringan lokal). Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal(IP) dan alamat tujuan (IP), protokol transport yang digunakan(UDP,TCP), serta nomor port yang digunakan.

Kelebihan dari tipe ini adalah mudah untuk diimplementasikan, transparan untuk pemakai, relatif lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi.

Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah:

a) IP address spoofing :

   Intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan ip address jaringan lokal yang telah diijinkan untuk melalui firewall.

b) Source routing attacks :

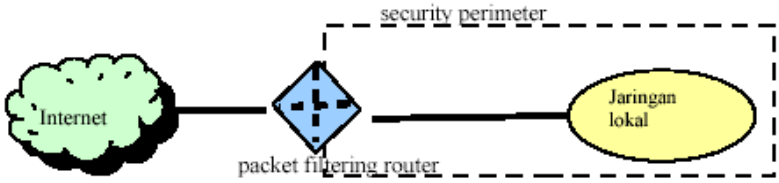
   Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk membypass firewall.

c) Tiny Fragment attacks :

   Intruder membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi

dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP).

Cara kerja Packet Filtering Router ditunjukkan pada gambar berikut:



Gambar 5-62 Packet filtering router

- Application-Level Gateway

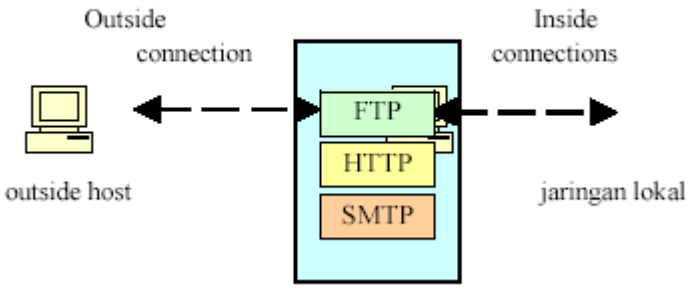
Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll.

Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal FTP untuk mengakses secara remote, maka gateway akan meminta user memasukkan alamat remote host yang akan di akses.Saat pengguna mengirimkan useer ID serta informasi lainnya yang sesuai maka gateway akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada remote host, dan menyalurkan data diantara kedua titik. apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini Firewall dapat di konfigurasikan untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati firewall.

Kelebihannya adalah relatif lebih aman daripada tipe packet filtering router lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi.

Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan. yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

Cara kerja Packet Filtering Router ditunjukkan pada gambar berikut:



Gambar 5-63 Application level gateway/proxy

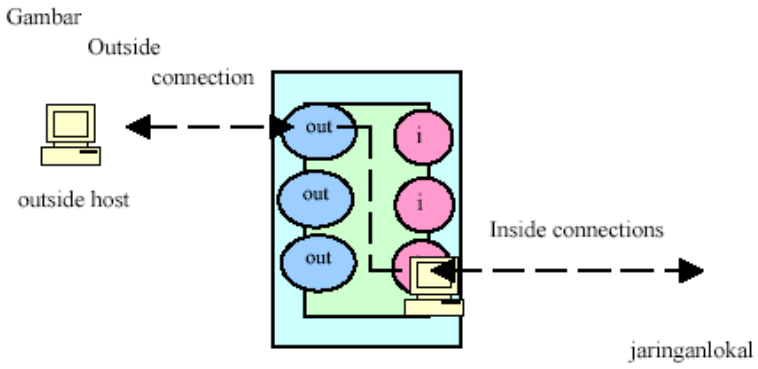
- Circuit-level Gateway

Tipe ketiga ini dapat merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung)

Cara kerjanya : Gateway akan mengatur kedua hubungan tcp tersebut, 1 antara dirinya (gw) dengan TCPpada pengguna lokal (inner host) serta 1 lagi antara dirinya (gw) dengan TCP pengguna luar (outside host). Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang di ijinkan.

Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna internal (internal users).

Cara kerja Packet Filtering Router ditunjukkan pada gb.9 berikut:



Gambar 5-64 Circuit-level Gateway

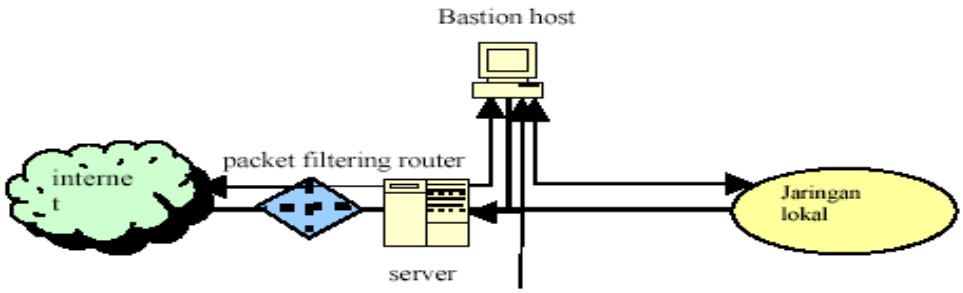
5.2.6 Konfigurasi Firewall

1. Screened Host Firewall system (single-homed bastion)

Pada konfigurasi ini, fungsi firewall akan dilakukan oleh packet filtering router dan bastion host*.Router ini dikonfigurasikan sedemikian sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju bastion host yang di ijinkan. Sedangkan untuk arus data (traffic) dari jaringan internal, hanyapaket IP dari bastion host yang di ijinkan untuk keluar. Konfigurasi ini mendukung fleksibilitasdalam Akses internet secara langsung, sebagai contoh apabila terdapat web server pada jaringan ini maka dapat di konfigurasikan agar web server dapat diakses langsung dari internet.

Bastion Host melakukan fungsi Authentikasi dan fungsi sebagai proxy. Konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada packet-filtering router atau application-level gateway secara terpisah.

Untuk lebih jelas, Screened Host FIrewall system (single-homed bastion) ditunjukkan pada gambar berikut:

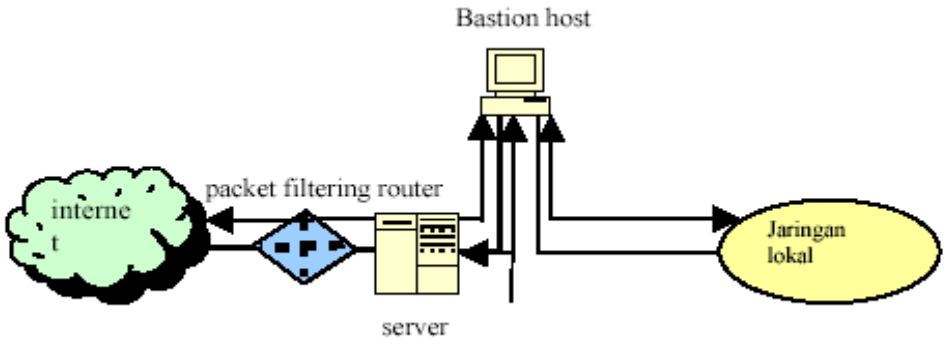


Gambar 5-65 Sceerned Host Firewall System (Single-homed Bastion)

2. Screened Host Firewall system (Dual-homed bastion)

Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya adalah dengan adanya dua jalur yang meisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama,adapun untuk server-server yang memerlukan direct akses (akses langsung) maka dapat di letakkan ditempat/segmenrt yang langsung berhubungan dengan internet. Hal ini dapat dilakukan dengan cara menggunakan 2 buah NIC (network interface Card) pada bastion Host.

Untuk lebih jelas, Screened Host FIrewall system (dual-homed bastion) ditunjukkan pada gambar berikut:



Gambar 5-66 Screened Host Firewall (Dual-homed Bastion)

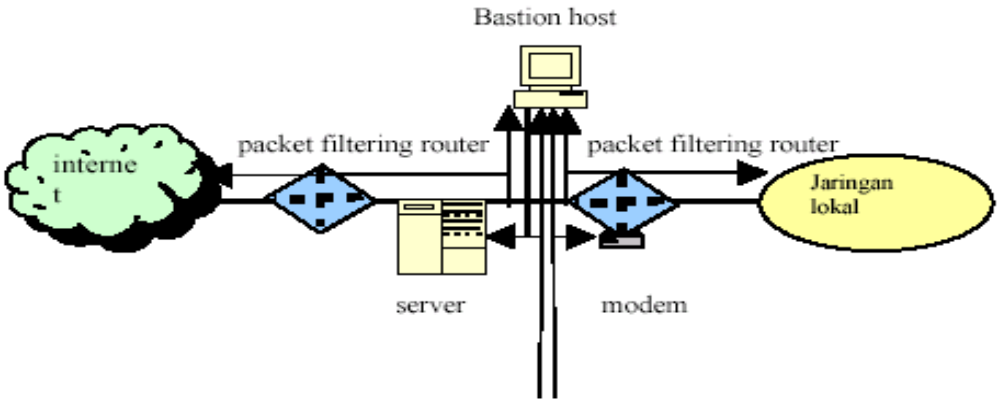
3. Screened subnet firewall

Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. kenapa? karena pada konfigurasi ini di gunakan 2 buah packet filtering router, 1 diantara internet dan bastion host, sedangkan 1 lagi diantara bastian host dan jaringan local konfigurasi ini membentuk subnet yang terisolasi.

Adapun kelebihannya adalah :

a. Terdapat 3 lapisan/tingkat pertahanan terhadap penyususp/intruder .
b. Router luar hanya melayani hubungan antara internet dan bastion host sehingga jaringan lokal menjadi tak terlihat (invisible).
c. Jaringan lokal tidak dapat mengkonstuksi routing langsung ke internet, atau dengan kata lain , Internet menjadi Invinsible (bukan berarti tidak bisa melakukan koneksi internet).

Untuk lebih jelas, Screened Subnet FIrewall system ditunjukkan pada gambar berikut:



Gambar 5-67 Screened subnet Firewall

5.2.7 Langkah-Langkah Membangun firewall

1. Mengidentifikasi bentuk jaringan yang dimiliki

Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang di gunakan serta protocol jaringan, akan memudahkan dalam mendesain sebuah firewall

2. Menentukan Policy atau kebijakan

Penentuan Kebijakan atau Policy merupakan hal yang harus di lakukan, baik atau buruknya sebuah firewall yang di bangun sangat di tentukan oleh policy/kebijakan yang di terapkan. Diantaranya:

a. Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat
b. Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut
c. Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan
d. Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
e. Menerapkankan semua policy atau kebijakan tersebut

3. Menyiapkan Software atau Hardware yang akan digunakan

Baik itu operating system yang mendukung atau software-software khusus pendukung firewall seperti ipchains, atau iptables pada linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.

4. Melakukan test konfigurasi

Pengujian terhadap firewall yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool tool yang biasa dilakukan untuk mengaudit seperti nmap.

** Bastion Host adalah sistem/bagian yang dianggap tempat terkuat dalam system keamanan jaringan oleh administrator.atau dapat di sebuta bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan*

komponen firewall atau bagian terluar sistem publik. Umumnya Bastion host akan menggunakan Sistem operasi yang dapat menangani semua kebutuhan (misal , Unix, linux, NT).

5.3 SHOREWALL [1]

5.3.1 Definisi Shorewal

Shoreline Firewall, yang lebih dikenal dengan "Shorewall", adalah sebuah tool tingkat tinggi untuk mengkonfigurasi Netfilter. Kita dapat mendeskripsikan kebutuhan firewall/gateway menggunakan masukan satu set file konfigurasi. Shorewall membaca file konfigurasi tersebut dengan bantuan iptables. Shorewall mengkonfigurasi Netfilter untuk menyesuaikan kebutuhan kita. Shorewall dapat digunakan pada suatu sistem deticated, gateway/router/server multifungsi atau pada standalone linux.

Shorewall tidak menggunakan mode kompatibel ipchain Netfilter dan dapat mengambil keuntungan pada kemampuan tracking connection state Netfilter.

Shorewall bukanlah sebuah daemon. Tugas dari shorewall sudah lengkap bila sudah mengkonfigurasi Netfilter. Setelah itu, tidak ada kode shorewall yang dijalankan meskipun program /sbin/shorewall dapat digunakan setiap waktu untuk memonitor firewall Netfilter. Shorewall bukanlah tools konfigurasi iptables yang termudah untuk digunakan, tapi shorewall adalah yang paling fleksibel dan powerful.

Sebelum kita membahas tentang shorewall, ada beberapa istilah yang harus kita ketahui diantaranya:

1. Netfilter - Fasilitas packet filter yang digunakan pada kernel linux 2.4 dan sesudahnya
2. ipchains - Fasilitas packet filter yang digunakann pada kernel linux 2.2. Juga merupakan program yang digunakan untuk mengkonfigurasi dan mengatur fasilitas tersebut. Netfilter dapat digunakan pada mode kompatible
3. ipchainsiptables - program yang digunakan untuk mengkonfigurasi dan mengontrol Netfilter. Istilah 'iptables' sering digunakan pada kombinasi dari iptables+Netfilter

5.3.2 NETFILTER dan IPTABLES

Netfilter merupakan salah satu perangkat di dalam linux kernel yang menyediakan modul inti untuk register fungsi callback dengan network stack. Register fungsi callback adalah pemanggilan kembali setiap paket data yang ditransfer tanpa network stack.

Iptables adalah struktur tabel secara umum untuk rulesets. Pada setiap tabel IP harus ada penggolongan nomor (iptables matches) dan satu koneksi (iptables target). Netfilter, ip_tables, connection tracking (ip_conntrack, nf_conntrack) dan subsystem NAT merupakan bagian utama pada framework.

Fungsi dari netfilter dan iptables yaitu:

a. Membangun firewall internet pada paket filtering stateless dan stateful.
b. Dapat menggunakan NAT dan masquerading untuk pembagian acces internet jika kita tidak mempunyai alamat IP public.
c. Dapat menggunakan NAT untuk implementasi proxy.

d. Membantu tc dan sistem iproute2 dalam membuat QoS yang canggih dan aturan router.

e. Memanipulasi paket selanjutnya (mangling) seperti mengubah TOS/DSCP/ECN bit pada IP utama.

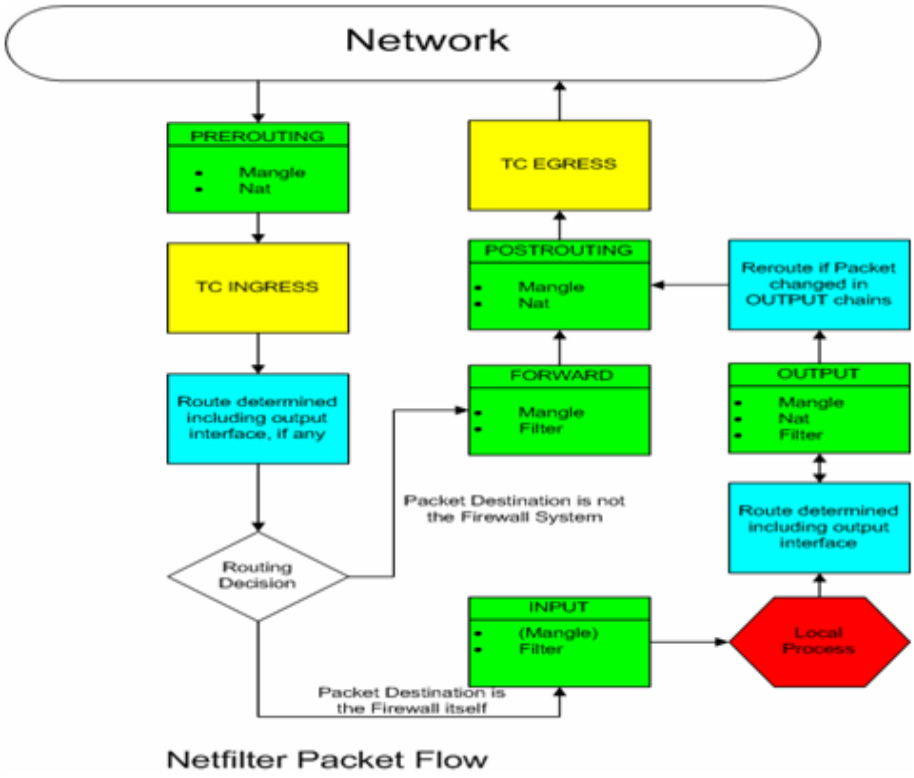
Netfilter terdiri dari tiga tabel yaitu: **Filter**, **Nat** dan **Mangle,** dimana setiap tabel tersebut mempunyai urutan: **PREROUTING**, **INPUT**, **FORWARD**, **OUTPUT** dan **POSTROUTING**.

Filter *yaitu* paket filtering yang digunakan untuk menolak, mengeluarkan dan menerima paket-paket data.

Nat *yaitu* Network Address Translation yang terdiri dari DNAT, SNAT dan Masquerading

Mangle *yaitu* modifikasi paket umum seperti menyeting nilai TOS atau kode paket untuk aturan routing dan pembentukan traffic.

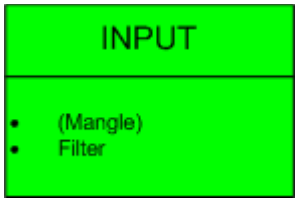
Di bawah ini merupakan diagram bagaimana paket data dikirim dengan rangkaian pembangun tanpa Netfilter (gb.13)



Gambar 5-68 Diagram paket data dikirim dengan Rangkaian pembangun tanpa Netfilter

Catatan : Tidak semua dari isi tabel digunakan,tergantung isi penggunaanya

"Local Process" berarti proses yang dijalankan di sistem shorewall itu sendiri.



Pada box diatas diberi nama blok pembangun (**INPUT**) yang berhubungan dengan nama tabel (**Mangle** and **Filter**). Dimana blok yang ada dan perintah dari blok tersebut ditransfer. Pada contoh diatas menunjukkan bahwa paket pertama seluruhnya menuju blok **INPUT** pada tabel **Mangle** selanjutnya menuju blok **INPUT** pada tabel **Filter** . Pada saat blok ditutup, Shorewall tidak menggunakan blok (**INPUT**) pada tabel (**Mangle**).

NOTE

*Rangkaian di tabel **Nat** hanya ditransfer untuk permintaan koneksi baru (terkait dengan koneksi tetap) sedangkan rangkaian pada tabel lain ditransfer setiap paketnya.*

Menurut peraturan menunjukkan bahwa semua tujuan traffic untuk firewall berasal dari firewall di eth0 disebut "eth0_in" . Seperti contoh di bawah ini.

Contoh dari status shorewall pada server dengan interface (eth0):

[root@lists html]# shorewall status

Shorewall-1.4.7 Status at lists.shorewall.net - Mon Oct 13 12:51:13 PDT 2003

Counters reset Sat Oct 11 08:12:57 PDT 2003

5.3.2.1 Tabel Filter :

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 679K  182M ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
 785K   93M accounting  all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       !icmp --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
```

Menurut peraturan menunjukkan bahwa semua tujuan traffic untuk firewall berasal dari firewall di eth0 disebut "eth0_in". Rangkaian akan ditunjukkan lebih jauh lagi.

```
 785K   93M eth0_in    all  --  eth0   *       0.0.0.0/0            0.0.0.0/0
    0     0 common     all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 6 prefix
`Shorewall:INPUT:REJECT:'
    0     0 reject     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 accounting  all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       !icmp --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
    0     0 eth0_fwd    all  --  eth0   *       0.0.0.0/0            0.0.0.0/0
    0     0 common     all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 6 prefix
`Shorewall:FORWARD:REJECT:'
    0     0 reject     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 1 packets, 60 bytes)
 pkts bytes target     prot opt in     out     source               destination
 679K  182M ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
 922K  618M accounting  all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       !icmp --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
 922K  618M fw2net     all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
```

```
    0     0 common     all  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 LOG        all  --  *      *       0.0.0.0/0           0.0.0.0/0           LOG flags 0 level 6 prefix
`Shorewall:OUTPUT:REJECT:'
    0     0 reject     all  --  *      *       0.0.0.0/0           0.0.0.0/0
```

Dibawah ini rangkaian dari eth0_in :

```
Chain eth0_in (1 references)
 pkts bytes target     prot opt in     out     source               destination
 785K   93M dynamic    all  --  *      *       0.0.0.0/0            0.0.0.0/0
 785K   93M net2fw     all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

5.3.2.2 Tabel Nat:

```
Nat table
Chain PREROUTING (policy ACCEPT 182K packets, 12M bytes)
 pkts bytes target     prot opt in     out     source               destination
20005 1314K net_dnat   all  --  eth0   *       0.0.0.0/0            0.0.0.0/0

Chain POSTROUTING (policy ACCEPT 678K packets, 44M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 678K packets, 44M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain net_dnat (1 references)
 pkts bytes target     prot opt in     out     source               destination
  638 32968 REDIRECT   tcp  --  *      *       0.0.0.0/0           !206.124.146.177     tcp dpt:80
redir ports 3128
```

5.3.2.3 Tabel Mangle:

```
Mangle Table

Chain PREROUTING (policy ACCEPT 14M packets, 2403M bytes)
 pkts bytes target     prot opt in     out     source               destination
1464K  275M pretos     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain INPUT (policy ACCEPT 14M packets, 2403M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 15M packets, 7188M bytes)
 pkts bytes target     prot opt in     out     source               destination
1601K  800M outtos     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain POSTROUTING (policy ACCEPT 15M packets, 7188M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain outtos (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 TOS        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 TOS set 0x10
```

```
 315K  311M TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp spt:22 TOS set
0x10
    0     0 TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp dpt:21 TOS set 0x10
  683 59143 TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp spt:21 TOS set
0x10
 3667 5357K TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp spt:20 TOS set
0x08
    0     0 TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp dpt:20 TOS set 0x08

Chain pretos (1 references)
 pkts bytes target     prot opt in     out     source               destination
 271K   15M TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp dpt:22 TOS set
0x10
    0     0 TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp spt:22 TOS set 0x10
  730 41538 TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp dpt:21 TOS set
0x10
    0     0 TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp spt:21 TOS set 0x10
    0     0 TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp spt:20 TOS set 0x08
 2065  111K TOS       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0
```

5.3.3 Konsep Shorewall

File konfigurasi untuk Shorewall diletakkan di direktori `/etc/shorewall`. Shorewall seperti jaringan yang bekerja dengan satu set zones. Zones ditempatkan pada file `/etc/shorewall/zones`. File ini untuk mendefinisikan zona asal trafik pada jaringan

Isi file `/etc/shorewall/zone` :

```
#ZONE        DISPLAY       COMMENTS
net               Net           Internet
loc               Local         Local networks
dmz           Dmz           Demilitarized zone
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT
REMOVE
```

Server tempat shorewall diinstall dikenal sebagai zona yang disebut *`fw`*

Aturan tentang traffic yang diterima dan traffic yang ditolak berkaitan dengan zones.

α. Kita menyampaikan default policy untuk koneksi dari zone satu ke zone yang lain pada file `/etc/shorewall/policy`. Beberapa pilihan dalam kebijakan tersebut adalah:

   α. **ACCEPT** – Menerima koneksi tersebut

   β. **DROP** – Mengabaikan permintaan koneksi

   χ. **REJECT** – Mengembalikan kesalahan sesuai permintaan koneksi

β. Kita menjelaskan aturan secara umum pada file `/etc/shorewall/rules`

χ. Kita hanya memerlukan permintaan koneksi. Kita tidak harus menggambarkan tentang peraturan bagaimana traffic menjadi bagian dalam pembentukan koneksi, dan pada beberapa kasus kita tidak perlu mencemaskan bagaimana koneksi yang terkait

ditangani (paket error pada ICMP dan permintaan koneksi TCP seperti yang digunakan pada FTP).

Untuk semua traffic yang lewat pada firewall diatur pada `/etc/shorewall/rules`, jika tidak terdefinisikan pada file tersebut maka akan dicek pada `/etc/shorewall/policy` jika tidak terdefinisikan akan dicek pada `/etc/shorewall/action` `/usr/share/shorewall/actions.std`)

Contoh aturan pada file `/etc/shorewall/policy` yang memiliki tiga-interfaces:

```
#SOURCE    DEST        POLICY      LOG LEVEL    LIMIT:BURST
loc        net         ACCEPT
net        all         DROP        info
all        all         REJECT      info
```

Jika kita menginginkan system firewall dapat mengakses internet secara penuh, kita mengganti command seperti di bawah :

```
#SOURCE    DEST        POLICY      LOG LEVEL    LIMIT:BURST
fw         net         ACCEPT
```

Kebijakan di atas akan:

- ♋ Mengizinkan semua permintaan koneksi dari local network kita ke internet.
- ♌ Mengabaikan semua permintaan koneksi dari internet ke local network atau firewall; jika pada koneksi drop, log level diisi info
- ♍ Menerima semua koneksi dari firewall ke internet (jika pada kondisi policy tidak ada komentar)
- ♎ Mereject semua koneksi; jika saat koneksi reject pada log level diisi info

`/etc/shorewall/interface`

File ini untuk menentukan interface yang akan terhubung dengan suatu zona

```
#ZONE      INTERFACE     BROADCAST     OPTIONS
net        eth0          detect        dhcp,routefilter,norfc1918
loc        eth1          detect
dmz        eth2          detect
```

File diatas berarti eth0 terhubung dengan jaringan internet, eth1 terhubung dengan jaringan local, dan eth2 terhubung dengan zona demilitarized.

Untuk menggambarkan bagaimana kebijakan tersebut memberi pengecualian, contohnya jika kita memiliki kebijakan tersebut tapi kita tidak dapat menghubungkan firewall dari internet yang menggunakan Secure Shell (SSH), meskipun SSH terhubung ke TCP port 22

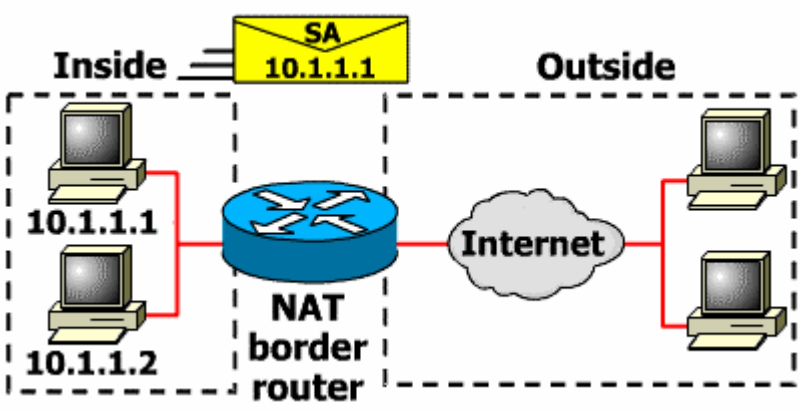
```
#ACTION    SOURCE        DEST       PROTO       DEST
#                                                PORT(S)
ACCEPT     net           fw         tcp         22
```

Jadi meskipun kita mempunyai kebijakan untuk mengabaikan semua koneksi ke internet, kita harus tetap menghubungkan ke SSH server pada firewall kita.

5.4 NAT (NETWORK ADDRESS TRANSLATION)

5.4.1 Pengertian NAT

I P *address* sebagai sarana pengalamatan di Internet semakin menjadi barang mewah dan ekslusif. Tidak sembarang orang sekarang ini bisa mendapatkan IP *address* yang valid dengan mudah. Oleh karena itulah dibutuhkan suatu mekanisme yang dapat menghemat IP *address*. Logika sederhana untuk penghematan IP *address* ialah dengan meng-*share* suatu nomor IP *address* valid ke beberapa *client* IP lainnya. Atau dengan kata lain beberapa komputer bisa mengakses Internet walau kita hanya memiliki satu IP *address* yang valid. Salah satu Mekanisme itu disediakan oleh *Network Address Translation* (NAT). Mekanisme tersebutsecara sederhana ditunjukkan pada gb.14:



Gambar 5-69 Mekanisme sederhana NAT

5.4.2 Pengguunaan NAT

Jika anda membutuhkan koneksi ke Internet dan hosts/komputer-komputer anda tidak mempunyai alamat IP global.

Jika anda berganti ke ISP baru dan anda diharuskan menggunakan alamat IP dari ISP baru tersebut untuk jaringan anda.

NAT digunakan untuk masalah pengalamatan IP

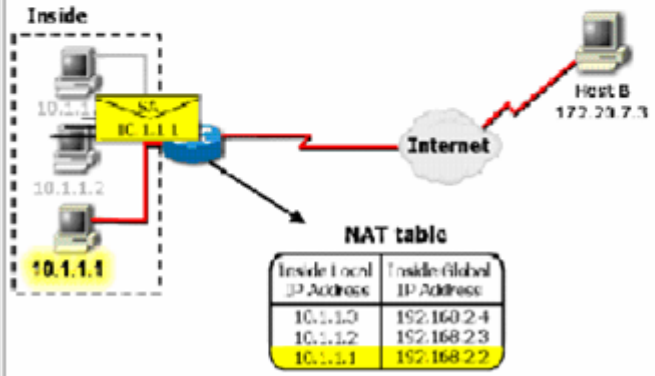
Teknologi NAT memungkinkan alamat IP local/ private terhubung ke jaringan public seperti internet. Sebagai router, NAT ditempatkan antara jaringan lokal (inside network) dan jaringan publik (outside network), dan mentranslasikan alamat lokal/ internal menjadi alamat IP global yang unik sebelum mengirimkan paket ke jaringan luar seperti internet. *Dengan NAT, jaringan lokal/ internal, tidak akan terlihat oleh dunia luar/ internet. IP lokal yang cukup banyak dapat dilewatkan ke internet hanya dengan melalui translasi ke satu IP publik/ global.*

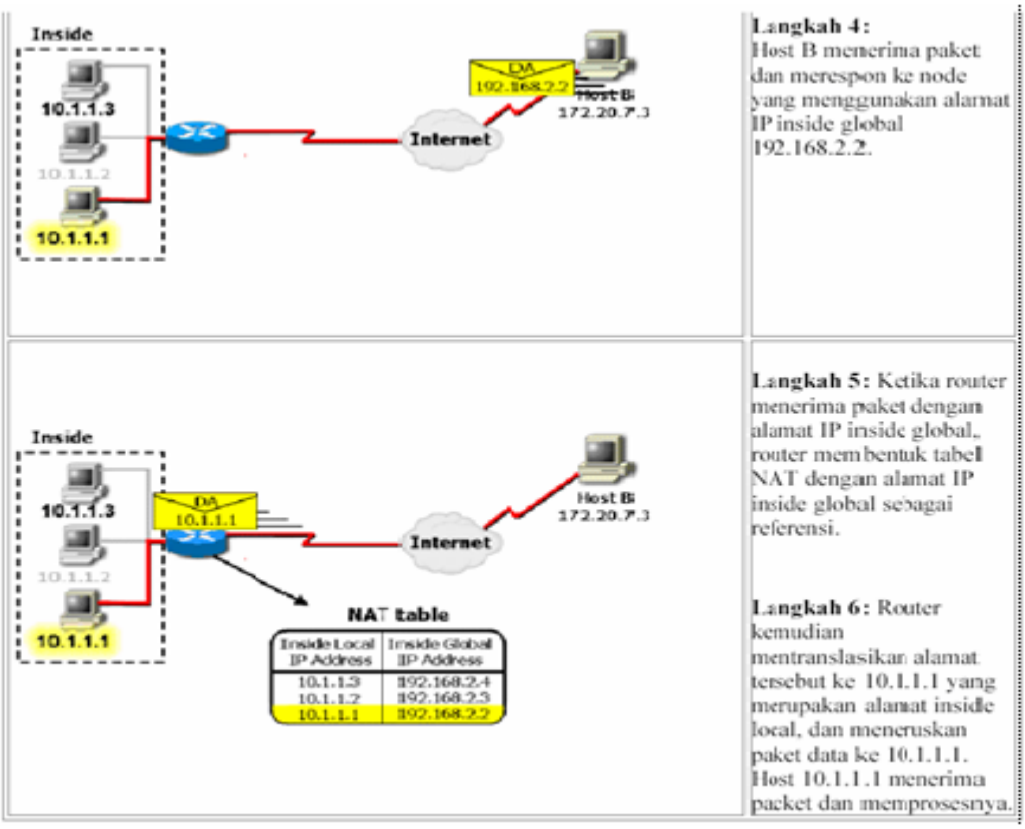
5.4.3 Keuntungan menggunakan NAT

Jika anda harus merubah IP internal anda dikarenakan anda berganti ISP atau dua intranet digabungkan (misalnya penggabungan dua perusahaan), NAT dapat digunakan untuk mentranslasikan alamat IP yang sesuai. NAT memungkinkan anda menambah alamat IP, tanpa merubah alamat IP pada host atau komputer anda. Dengan demikian akan menghilangkan duplicate IP tanpa pengalamatan kembali host atau komputer anda.

5.4.4 Bagaimana Alamat IP Inside Local ditranslasikan?

Berikut adalah ilustrasi NAT yang digunakan untuk mentranslasikan alamat dari dalam/ inside jaringan ke tujuan/outside.

Gambar	Keterangan
	**Langkah 1:** Pengguna pada host 10.1.1.1 membuat koneksi ke outside host B.
	**Langkah 2:** Paket pertama yang diterima oleh router dari host 10.1.1.1 dicocokkan dengan tabel NAT. Jika translasi ada, (karena sudah diset statik), maka router melanjutkan ke Langkah 3. Jika translasi tidak ditemukan, Router mengalokasikan sebuah alamat baru dan menset sebuah translasi dari inside local 10.1.1.1 ke sebuah alamat legal inside global dari kelompok (pool) alamat dinamik.



Gambar 5-70 Proses dari Sebuah alamat IP Inside Local yan ditranslasikan

5.4.5 Dua Tipe NAT

Dua tipe NAT adalah Static dan Dinamik yang keduanya dapat digunakan secara terpisah maupun bersamaan.

1. Statik

Translasi Static terjadi ketika sebuah alamat lokal (inside) di petakan ke sebuah alamat global/internet (outside).

Alamat lokal dan global dipetakan satu lawan satu secara Statik.

2. Dinamik

a. NAT dengan Pool (kelompok)

Translasi Dinamik terjadi ketika router NAT diset untuk memahami alamat lokal yang harus ditranslasikan, dan kelompok (pool) alamat global yang akan digunakan untuk terhubung ke internet. Proses NAT Dinamik ini dapat memetakan bebarapa kelompok alamat lokal ke beberapa kelompok alamat global.

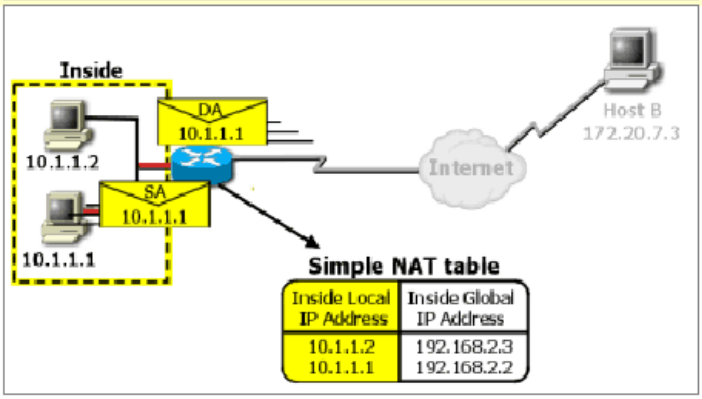
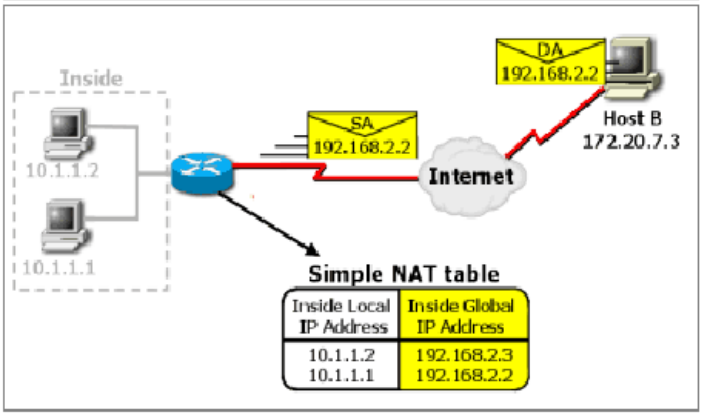
b. NAT Overload

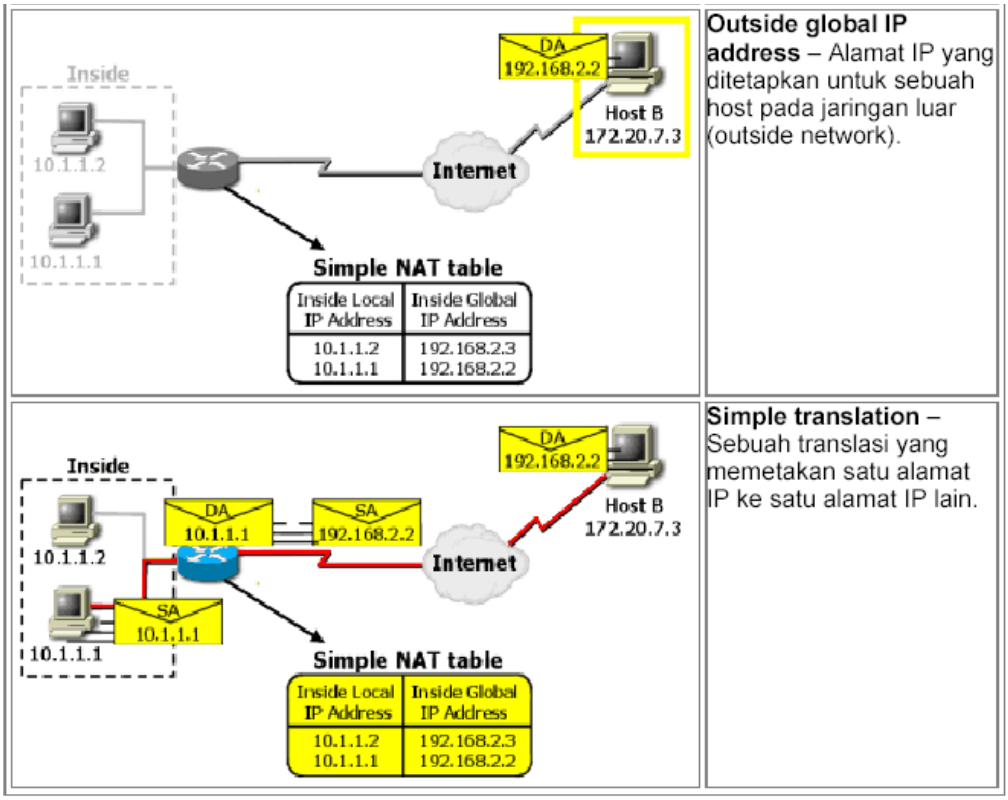
Sejumlah IP lokal/internal dapat ditranslasikan ke satu alamat IP global/outside. Hal ini sangat menghemat penggunakan alokasi IP dari ISP. Sharing/pemakaian bersama satu alamat IP ini menggunakan metoda port multiplexing, atau perubahan port ke packet outbound.

Komponen-komponen NAT

NAT dapat melewatkan alamat jaringan lokal (‘private’) menuju jaringan ‘public’ seperti Internet. Alamat ‘private’ yang berada pada jaringan lokal /"inside", mengirim paket melalui router NAT, yang kemudian dirubah oleh router NAT menjadi alamat IP ISP sehingga paket tersebut dapat diteruskan melewati jaringan publik atau internet. Awalnya Fitur ini hanya tersedia pada gateway pass-through firewall saja. Tapi sekarang sudah tersedia di semua router Cisco.

Komponen-komponen NAT dapat dilihat pada gambar berikut:

Gambar	Keterangan
	**Inside local IP address** – Alamat IP yang di set untuk sebuah host pada jaringan lokal (inside network). Pengalokasian alamat IP harus unik dan dalam satu subnet yang sama.
	**Inside global IP address** – Sebuah alamat IP legal (ditetapkan oleh NIC atau service provider) yang mewakili satu atau lebih alamat IP inside lokal ke dunia luar. Alamat IP ini dialokasikan dari kapasitas alamat global yang unik. Biasanya disediakan oleh Internet Service Provider (ISP).



Gambar 5-71 Komponen-komponen NAT

5.4.6 Mekanisme NAT [2]

Sebuah paket TCP terdiri dari *header* dan data. *Header* memiliki sejumlah *field* di dalamnya, salah satu *field* yang penting di sini adalah MAC (*Media Access Control*) *address* asal dan tujuan, IP *address* asal dan tujuan, dan nomor *port* asal dan tujuan.

Saat mesin A menghubungi mesin B, *header* paket berisi IP A sebagai IP *address* asal dan IP B sebagai IP *address* tujuan. *Header* ini juga berisi nomor *port* asal (biasanya dipilih oleh mesin pengirim dari sekumpulan nomor *port*) dan nomor *port* tujuan yang spesifik, misalnya *port* 80 (untuk *web*).

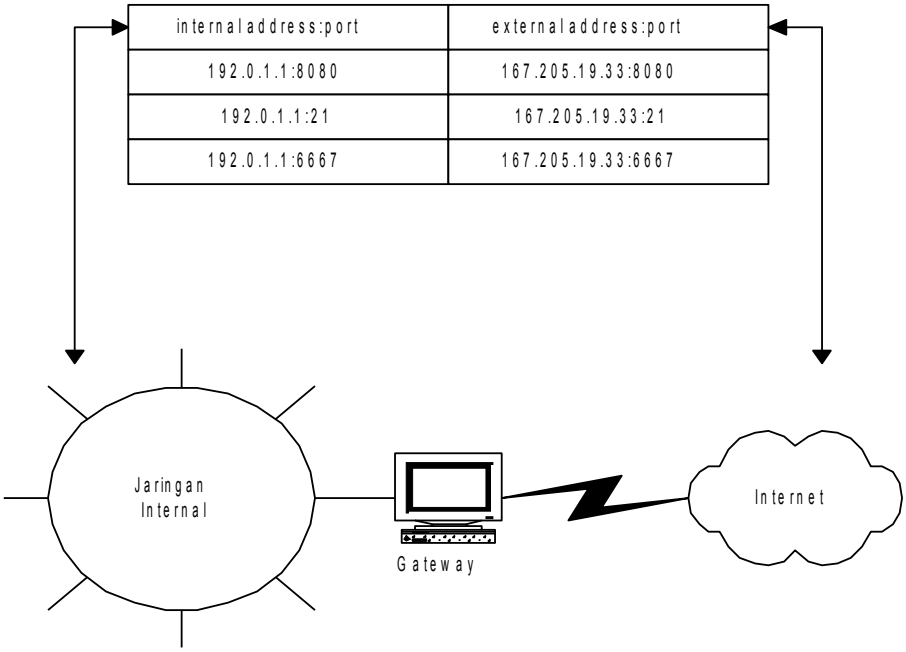
Kemudian B menerima paket pada *port* 80 dan memilih nomor *port* balasan untuk digunakan sebagai nomor *port* asal menggantikan *port* 80 tadi. Mesin B lalu membalik IP *address* asal & tujuan dan nomor *port* asal & tujuan dalam *header* paket. Sehingga keadaan sekarang IP B adalah IP *address* asal dan IP A adalah IP *address* tujuan. Kemudian B mengirim paket itu kembali ke A. Selama *session* terbuka, paket data hilir mudik menggunakan nomor *port* yang dipilih.

Router (yang biasa – tanpa Natd) memodifikasi *field* MAC *address* asal & tujuan dalam *header* ketika me-*route* paket yang melewatinya. IP *address*, nomor *port*, dan nomor *sequence* asal & tujuan tidak disentuh sama sekali.

NAT juga bekerja atas dasar ini. Dimulai dengan membuat tabel translasi internal untuk semua IP *address* jaringan internal yang mengirim paket melewatinya. Lalu men-*set* tabel nomor *port* yang akan digunakan oleh IP *address* yang valid. Ketika paket dari jaringan internal dikirim ke Natd untuk disampaikan keluar, Natd melakukan hal-hal sebagai berikut:

a. Mencatat IP *address* dan *port* asal dalam tabel translasi
b. Menggantikan nomor IP asal paket dengan nomor IP dirinya yang valid
c. Menetapkan nomor *port* khusus untuk paket yang dikirim keluar, memasukkannya dalam tabel translasi dan menggantikan nomor *port* asal tersebut dengan nomor *port* khusus ini.

Ketika paket balasan datang kembali, Natd mengecek nomor *port* tujuannya. Jika ini cocok dengan nomor *port* yang khusus telah ditetapkan sebelumnya, maka dia akan melihat tabel translasi dan mencari mesin mana di jaringan internal yang sesuai. Setelah ditemukan, ia akan menulis kembali nomor *port* dan IP *address* tujuan dengan IP *address* dan nomor *port* asal yang asli yang digunakan dulu untuk memulai koneksi. Lalu mengirim paket ini ke mesin di jaringan internal yang dituju. Natd memelihara isi tabel translasi selama koneksi masih terbuka. Contoh Mekanisme Natd dapat dilihat pada gambar berikut:



Gambar 5-72 Contoh Mekanisme NAT

5.4.7 Perbedaan NAT dengan sistem Proxy

Hampir mirip dengan NAT, suatu jaringan kecil dengan *proxy* bisa menempatkan beberapa mesin untuk mengakses *web* dibelakang sebuah mesin yang memiliki IP *address* valid. Ini juga merupakan langkah penghematan biaya dibanding harus menyewa beberapa account dari ISP dan memasang modem & sambungan telepon pada tiap mesin.

Namun demikian, *proxy* server ini tidak sesuai untuk jaringan yang lebih besar. Bagaimanapun, menambah *hard disk* dan RAM pada server *proxy* supaya *proxy* berjalan efisien tidak selalu dapat dilakukan (karena *constraint* biaya). Lagi pula, persentase *web page* yang bisa dilayani oleh *cache proxy* akan makin menurun sejalan dengan semakin menipisnya ruang kosong di *hard disk*, sehingga penggunaan *cache proxy* menjadi tidak lebih baik dari pada sambungan langsung. Tambahan lagi, tiap koneksi bersamaan akan meng-*generate* proses tambahan dalam *proxy*. Tiap proses ini harus menggunakan *disk I/O channel* yang sama, dan saat *disk I/O channel* jenuh, maka terjadilah *bottle neck*.

NAT menawarkan solusi yang lebih fleksibel dan *scalable*. NAT menghilangkan keharusan mengkonfigurasi *proxy*/*sock* dalam tiap *client*. NAT lebih cepat dan mampu menangani trafik *network* untuk beribu-ribu *user* secara simultan.

Selain itu, translasi alamat yang diterapkan dalam NAT, membuat para *cracker* di Internet tidak mungkin menyerang langsung sistem-sistem di dalam jaringan internal. *Intruder* harus menyerang dan memperoleh akses ke mesin NAT dulu sebelum menyiapkan serangan ke mesin-mesin di jaringan internal. Penting di ketahui bahwa, sementara dengan NAT jaringan internal terproteksi, namun untuk masalah *security*, tetap saja diperlukan paket *filtering* dan metoda pengamanan lainnya dalam mesin NAT.

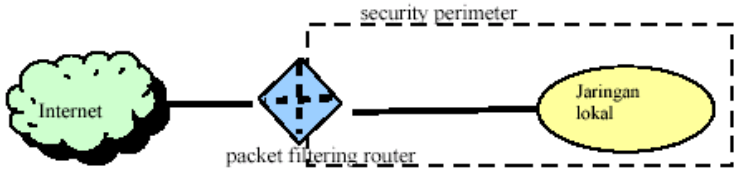
5.5 SOAL dan JAWABAN

1. Jelaskan secara singkat pengertian firewall beserta konfigurasi sederhananya!
2. Sebutkan dan jelaskan tentang tipe-tipe dari firewall!
3. Bagaimana langkah-langkah membangun firewall secara sederhana?
4. Apakah yang melatarbelakangi penggunaan NAT? Dan apa keuntungan menggunakan NAT?
5. Sebutkan komponen-komponen yang dimiliki oleh sebuah NAT!

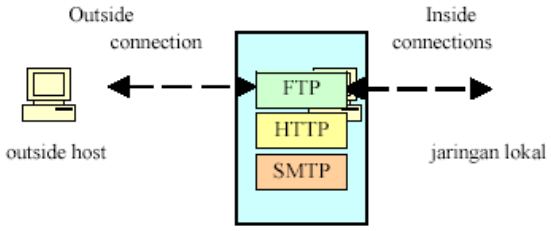
Jawaban

1. Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Konfigurasi sederhananya:
   pc (jaringan local) == ***firewall*** == **internet** (jaringan lain)

2. Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut.Aturan penyaringan didasarkan pada header IP dan transport header, termasuk juga alamat awal(IP) dan alamat tujuan (IP), protokol transport yang digunakan(UDP,TCP), serta nomor port yang digunakan.
   Cara kerja Packet Filtering Router:

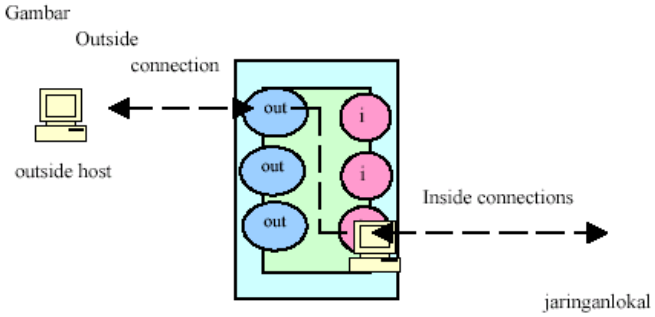


   Application-level Gateway yang biasa juga di kenal sebagai proxy server yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan layer aplikasi ,baik itu FTP, HTTP, GOPHER dll.
   Cara kerja Packet Filtering Router:



Circuit-level Gateway merupakan sistem yang berdiri sendiri , atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe application-level gateway.tipe ini tidak mengijinkan koneksi TCP end to end (langsung)

Cara kerja Packet Filtering Router:



3. Langkah-langkah membangun firewall secara sederhana
   a. Mengidentifikasi bentuk jaringan yang dimiliki
   b. Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang di gunakan serta protocol jaringan.
   c. Menentukan Policy atau kebijakan

      Beberapa hal yang perlu diperhatikan:

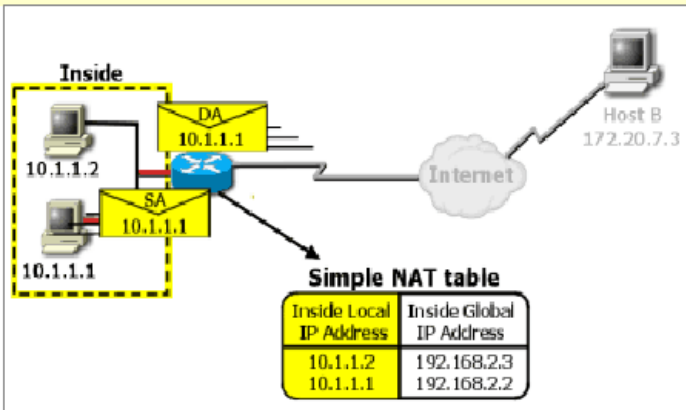
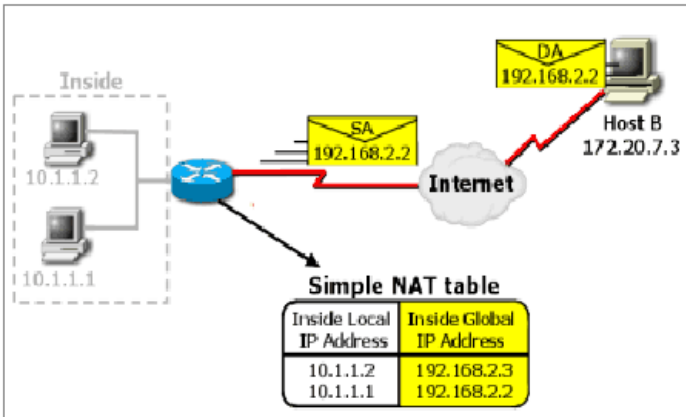
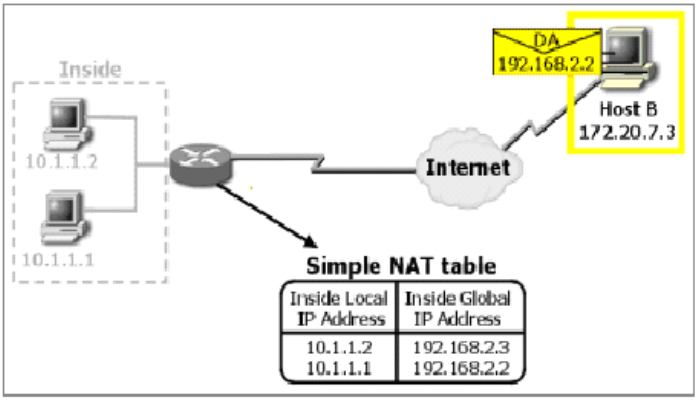
      - Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat
      - Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut
      - Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan
      - Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
      - Menerapkankan semua policy atau kebijakan tersebut

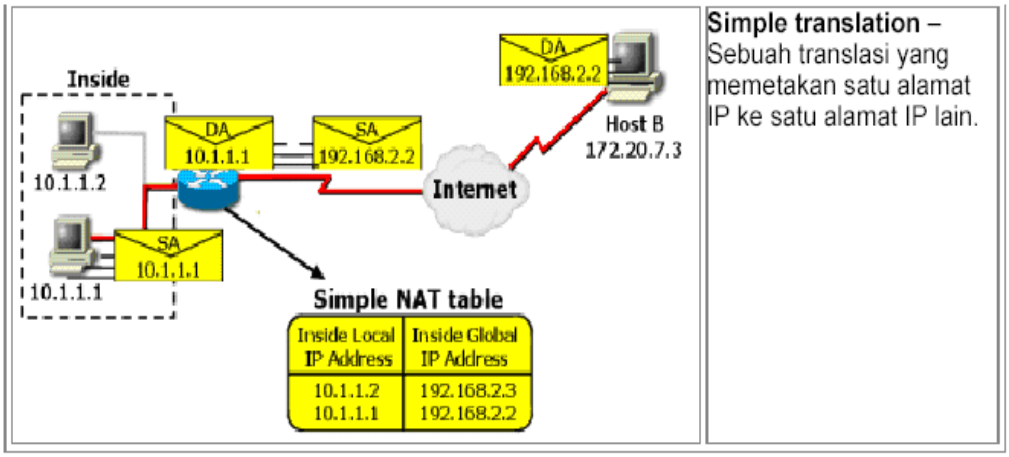
   d. Menyiapkan Software atau Hardware yang akan digunakan
   e. Melakukan test konfigurasi
4. IP *address* sebagai sarana pengalamatan di Internet semakin menjadi barang mewah dan ekslusif. Tidak sembarang orang sekarang ini bisa mendapatkan IP *address* yang valid

dengan mudah. Oleh karena itulah dibutuhkan suatu mekanisme yang dapat menghemat IP *address*. Logika sederhana untuk penghematan IP *address* ialah dengan meng-*share* suatu nomor IP *address* valid ke beberapa *client* IP lainnya. Atau dengan kata lain beberapa komputer bisa mengakses Internet walau kita hanya memiliki satu IP *address* yang valid.

Keuntungannya, jika anda harus merubah IP internal anda dikarenakan anda berganti ISP atau dua intranet digabungkan (misalnya penggabungan dua perusahaan), NAT dapat digunakan untuk mentranslasikan alamat IP yang sesuai. NAT memungkinkan anda menambah alamat IP, tanpa merubah alamat IP pada host atau komputer anda. Dengan demikian akan menghilangkan duplicate IP tanpa pengalamatan kembali host atau komputer anda.

5. Komponen NAT:

Gambar	Keterangan
	**Inside local IP address** – Alamat IP yang di set untuk sebuah host pada jaringan lokal (inside network). Pengalokasian alamat IP harus unik dan dalam satu subnet yang sama.
	**Inside global IP address** – Sebuah alamat IP legal (ditetapkan oleh NIC atau service provider) yang mewakili satu atau lebih alamat IP inside lokal ke dunia luar. Alamat IP ini dialokasikan dari kapasitas alamat global yang unik. Biasanya disediakan oleh Internet Service Provider (ISP).
	**Outside global IP address** – Alamat IP yang ditetapkan untuk sebuah host pada jaringan luar (outside network).



Simple translation – Sebuah translasi yang memetakan satu alamat IP ke satu alamat IP lain.

5.6 REFERENSI

[1] Uswatun Hasanah, Ria Puspitasari, “Laporan Kerja Praktek Shorewall”, 2007

[2] Sugiharta Tito, “Network Address Translation (NAT): Cara lain menghemat IP Address”, Laboratorium Sistem Informasi & Keputusan (LSIK) ,Teknik Industri ITB, Tito@TI.ITB.ac.id

[3] Triswikuharso Teguh, “Firewall dan NAT”, 1999

[4] Eueung Mulyana & Onno W. Purbo, “Firewall—Security Internet”, 2001 klik kanan

[5] Tom Eastep, **“** One-to-one NAT”, Copyright ©2001- 2004 Thomas M.Eastep

[6] www.ilmukomputer.com

[7] http://id.wikipedia.org/wiki/Network_address_translation

BAB 6. VPN (VIRTUAL PRIVATE NETWORK)

Basuaji Sundoro [1] , Nurcahyadi [1], Novita Rahma Eka S [1]

[1]Politeknik Elektronika Negeri Surabaya

ABSTRAK

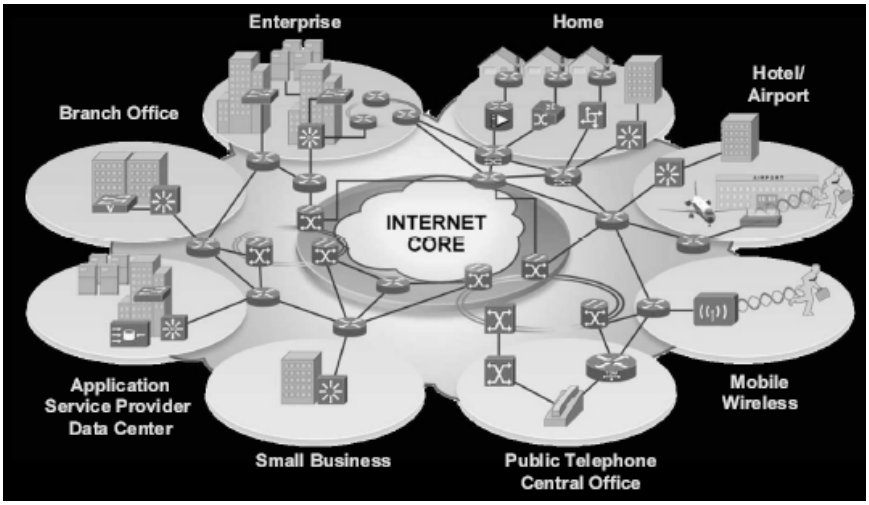
Kebutuhan bisnis dimasa sekarang didukung dengan variasi jaringan komunikasi yang luas. Para karyawan di perusahaan mengakses sumberdaya perusahaan untuk mendukung pekerjaan mereka melalaui jaringan komunikasi yang perusahaan mereka miliki. Belum lagi rekanan bisnis perusahaan yang turut mengakses sumberdaya perusahaan dengan jaringan yang lain dalam rangka kerja sama membagi informasi bisnis, perencanaan bisnis bersama, dan lain sebagainya.

Pada umumnya perusahaan menggunaakan berbasis *leased lines* atau sirkit *frame relay* untuk menghubungkan kantor pusat dengan kantor cabang yang ada, hal tersebut tidak fleksibel mengingat saat ini sebuah perusahaan biasanya ingin cepat mempunyai jaringan komunikasi dengan rekanan bisnis yang lain atau untuk mendukung karyawan yang sedang bekerja mengerjakan proyek yang bersifat lapangan dan menuntut mobilitas.

VPN menggunakan jaringan internet yang sudah tersedia untuk menjawab persoalan jaringan perusahaan seperti yang dideskripsikan seperti diatas. Dibandingkan jaringan *leased lines* atau *frame relay*, VPN menggunakan infrastruktur yang sudah ada di internet untuk melakukan pertukaran data antara kantor pusat sebuah perusahaan dan kantor cabangnya.

6.1 MEMBANGUN KONEKSI VPN

Sedikit mengulas apa yang kita ketahui tentang VPN akan menjadi solusi di waktu koneksi Wide Area Network (WAN) sangat rumit diimplementasikan.



Gambar 6-73 Wide Area Network (WAN)

Kebingungan kita semakin bertambah jika sistem yang dikehendaki meliputi beberapa aspek kepentingan. Sentralisasi data, VOIP, remote sistem, dan masih banyak lagi keinginan keinginan sebagai dampak pemenuhan kebutuhan perusahaan. Sebenarnya sadar nggak sadar kita akan digantungkan oleh suatu infrastruktur yang ada. Dengan keterbatasan infrastruktur yang ada sebenarnya kita bisa membangun sistem yang tidak tergantung pada infrastruktur tersebut. Dari gambar diatas kita sangat mendambakan koneksi tiada batas. Akses kabel (frame relay, ISDN, leased line, PSTN, DSL, Fiber Optic) dan wireless (GSM, CDMA, VSAT) sebenarnya sudah tidak menjadi kendala dalam era ”high tech” sekarang ini. Cuman masalahnya adalah kita hdup di negara Indonesia yang sangat mahal dalam urusan teknologi. Kami tidak usah memaparkan betapa mahalnya infrastruktur yang kita bayar setiap bulannya., belum lagi dibelenggunya masalah legalitas.

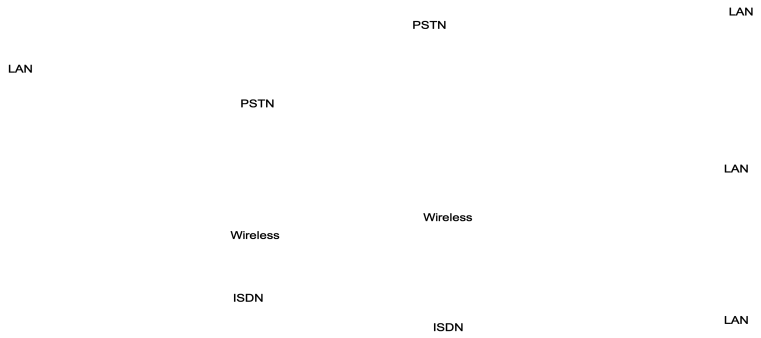
Untuk membangun konsep tiada batas dan ”menghemat uang”, kita hendaknya berpikir kreatif dan mengerti apa saja yang menjadi kebutuhan kita. Sebagai contoh : jika kita tidak menggunakan sistem secara real time dan night runing, saran kami nggak usah menggunakan jaringan sewa dedicated. List juga provider provider yang mempunyai commitment tinggi dalam pelayanan dan harga. Selain itu support teknologi yang ditawarkan provider tersebut. Apabila support yang ditawarkan sangatlah minim, maka anda dituntut lebih kreatif dalam meramu koneksi jaringan anda. Untuk menggabungkan (sentralisasi) data seperti gambar dibawah ini sangatlah mungkin untuk diterapkan di Indonesia dengan biaya murah dan stabil. Dan sistem yang digunakan ”Tidak harus WEB”. Sering kali kita terbentur dengan pemilihan platform aplikasi yang kita pilih. Kecendrungan aplikasi yang ada di Indonesa adalah aplikasi untuk LAN untuk keperluan SOHO (Small Office Home Office). Tatkala kebutuhan akan ”sentralisasi data” diwujudkan maka berbondong bondong kita melakukan *porting* (migrate) ke WEB based. Padahal hal tersebut sangat tidak perlu dilakukan.

Gambar 6-74 Penerapan Wide Area Network (WAN)

Dengan VPN ”dial on demand ” kita bisa menerapkan sistem tersebut. Beberapa faktor yang mempengaruhi sulitnya WAN untuk diimplementasikan pada jaringan yang komplek diantaranya :

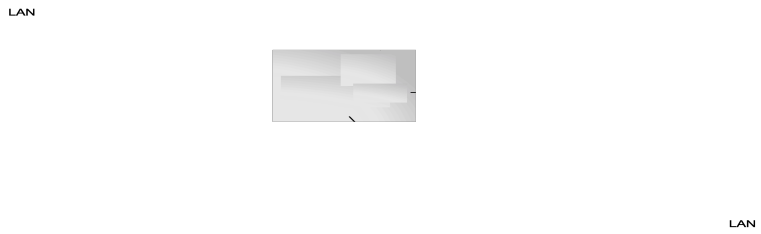
1. Alasan finansial

Wide Area Network atau sering disingkat WAN adalah konsep jaringan yang sangat mahal untuk diaplikasikan pada sistem jaringan komplek. Bayangkan saja berapa nilai investasi anda untuk semuanya tersebut. Apalagi jika sistem tersebut diimplementasikan pada perusahaan anda yang notabene mempunyai cabang (branch office) tersebar ke seluruh propinsi. Belum lagi ditambah dengan penambahan perangkat keras (baca uang) untuk setiap lokasinya. Selain itu kita harus memikirkan kendala geografi yang dihadapi seperti gedung yang selalu menjadi momok bagi pemain wireless.



Gambar 6-75 WAN untuk koneksi point to point

Pada gambar diatas jelas terlihat WAN untuk koneksi Point to Point dari cabang (branch office) ke kantor pusat (corporate). Setiap penambahan koneksi selalu menyediakan hardware dan jaringan pada kedua belah pihak (branch office dan corporate).



Gambar 6-76 Skema VPN

VPN menawarkan penghematan hardware pada sisi corporate dengan system IP base (IPSec dan PPTP)

2. Penggunaan infrastruktur berlebihan

”Boros” merupakan ungkapan yang pas untuk design WAN yang digunakan pada siang hari. Bagaimana dengan malam hari? Sebagian masih sadar dengan memanfaatkan proses di malam hari (night runing) untuk sinkronosasi data (replikasi) dari cabang ke corporate. Dengan

VPN anda bisa *custome* sistem anda sendiri. Saran kami tempatkan 1 IP public di corporate anda. Sedangkan untuk branch office deikembalikan pada *policy* perusahaan anda sendiri. Pilih ISP yang paling murah. Kalau memang untuk transaksi di siang hari saja dan hanya diperlukan beberapa modul untuk proses sinkronisasi ada baiknya pada client (branch office) menggunakan ”dial up connection”.

3. Keamanan jaringan

Seperti kata sponsor ”Apapun koneksi anda, pastikan VPN securitynya”. VPN menawarkan beberapa konsep yang berhubungan dengan keamanan jaringan anda diantaranya :

1. Firewall

Firewall pada internet mempunyai fungsi sama dengan firewall pada gedung dan mobil yang memproteksi beberapa bagian agar terhindar dari kebakaran. Dengan menerapkan authentikasi dan enkripsi, VPN sudah cukup *secure* sebagai firewall internet. Sekarang ini sudah banyak beberapa vendor yang menerapkan VPN diantaranya : Cisco Private Interne Exchange (PIX), 3 COM US Robotics Total Control, Juniper Netscreen series dan ALCATEL.

2. Authentikasi

Teknik authentikasi sangatlah penting untuk VPN. Dengan authentikasi kita bisa memastikan hanya dengan user dan password yang benarlah hak akses diberikan. Banyak cara melakukan teknik authentikasi mulai dari shared key, algoritma hash, Chalange Handshake Authentication Protocol (CHAP) atau bahkan menggunakan algoritma yang umum digunakan, RSA.

3. Mekanisme Authentisasi

Subyek autentisasi adalah pembuktian. Yang dibuktikan meliputi tiga kategori, yaitu: sesuatu pada diri kita (*something you are* SYA), sesuatu yang kita ketahui (*something you know* SYK), dan sesuatu yang kita punyai (*something you have* SYH). SYA berkaitan erat dengan bidang biometrik, seperti pemeriksaan sidik-jari, pemeriksaan retina mata, analisis suara dll. SYK identik dengan password. Sedangkan bagi SYH umumnya digunakan kartu identitas seperti *smartcard*.

Barangkali, yang sekarang masih banyak digunakan adalah sistem ber-password. Untuk menghindari pencurian password dan pemakaian sistem secara ilegal, akan bijaksana bila jaringan kita dilengkapi sistem password sekali pakai. Bagaimana caranya penerapan metoda ini?

Pertama, menggunakan sistem perangko-waktu ter-enkripsi. Dengan cara ini, password baru dikirimkan setelah terlebih dulu dimodifikasi berdasarkan waktu saat itu. Kedua, menggunakan sistem *challenge-response* (CR), dimana password yang kita berikan tergantung *challenge* dari server. Kasarnya kita menyiapkan suatu daftar jawaban (*response*) berbeda bagi ‘pertanyaan’ (*challenge*) yang berbeda oleh server. Karena tentu sulit sekali untuk menghafal

sekian puluh atau sekian ratus password, akan lebih mudah jika yang dihafal adalah aturan untuk mengubah challenge yang diberikan menjadi response (jadi tidak random). Misalnya aturan kita adalah: “kapitalkan huruf kelima dan hapus huruf keempat”, maka password yang kita berikan adalah **MxyPtlk1W2** untuk challenge sistem **Mxyzptlk1W2**.

Kalau pada sistem CR, harus diketahui ‘*aturan*‘-nya, maka pada sistem perangko-waktu, kita mesti mengingat password bagi pemberian perangko-waktu ini. Apakah cara seperti ini tidak mempersulit? Beruntung sekali mekanisme tersebut umumnya ditangani oleh suatu perangkat, baik perangkat lunak ataupun dengan perangkat keras. Kerberos, perangkat lunak autentisasi yang dibuat di MIT dan mengadopsi sistem perangko-waktu, mewajibkan modifikasi client bagi sinkronisasi waktu dengan server serta pemberian password perangko-waktu. Modifikasi program client mengingatkan kita pada proxy dan memang, kurang lebih seperti itu. Sistem CR biasanya diterapkan sekaligus dengan dukungan perangkat keras. Contoh sistem CR operasional adalah perangkat *SNK-004 card* (*Digital Pathways*) yang dapat diterapkan bersama-sama dengan paket TIS-FWTK (*Trusted Information System - internet FireWall ToolKit*).

TIS-FWTK menawarkan solusi password sekali pakai (sistem CR) yang ‘menyenangkan’**:** S/Key. S/Key menerapkan prosedur algoritma *hash* iteratif terhadap suatu *seed*, sedemikian sistem dapat memvalidasi response-client instant tapi tidak mempunyai kemampuan untuk memprediksi response-client berikutnya. Sehingga bila terjadi penyusupan pada sistem, tidak ada ‘sesuatu’ yang bisa dicuri (biasanya daftar password). Algoritma hash mempunyai dua sifat utama. Pertama, masukan tidak bisa diregenerasikan dari keluaran (non-reversibel). Kedua, terdapat dua kemungkinan masukan bagi sebuah keluaran yang sama.

4. Enkripsi

Enkripsi merupakan proses mengkodekan data sehingga maknanya menjadi tidak jelas/sulit dibaca. Enkripsi juga dapat diartikan mengubah sebuah kata atau kalimat menjadi sandi/kode-kode tertentu dengan menggunakan algoritma tertentu pula. Tujuan dari enkripsi adalah meningkatkan dan menjaga keamanan data baik yang disimpan maupun yang dikirim.

Pengertian

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu. Encryption berasal dari bahasa yunani *kryptos* yang artinya tersembunyi atau rahasia.

Metode yang digunakan.

Umumnya proses enkripsi dilakukan dengan sebuah rumus dan kunci untuk mendekripsi data.

Contoh :

Misalnya pesan M (plaintext) dienkodekan dengan fungsi E dan kunci K untuk menjadi chipertext.

$$E(K,M) = \{M\}K$$

Pesan dapat didekripsi dengan menggunakan fungsi D dan kunci L

D (K,E(K,M)) = M

Cara enkripsi yang paling sederhana adalah dengan mengganti suatu alpabet dengan karakter lain.

Misalnya:

Plaintext : universitas duta wacana

Kunci : a = b, b = c, c = d, dst

Chipertext : vojwfstjubt evub xbdbob.

Manfaat dan kerugian

Beberapa manfaat yang bisa didapatkan dari enkripsi ini adalah :

a. Kerahasiaan suatu informasi terjamin

b. Menyediakan authentication dan perlindungan integritas pada algoritma checksum/hash

c. Menanggulangi penyadapan telepon dan email

d. Untuk digital signature. Digital signature adalah menambahkan suatu baris statemen pada suatu elektronik copy dan mengenkripsi statemen tersebut dengan kunci yang kita miliki dan hanya pihak yang memiliki kunci dekripsinya saja yang bisa membukanya.

e. Untuk digital cash

Penyalahgunaan dan kerugian dari enkripsi adalah:

a. Penyandian rencana teroris

b. Penyembunyian record criminal oleh seorang penjahat

c. Pesan tidak bisa dibaca bila penerima pesan lupa atau kehilangan kunci (decryptor).

Koneksi yang terenkripsi adalah syarat wajib dari VPN. Teknik enkripsi secara garis besar terbagi menjadi dua bagian: secret (or private) key encryption dan public key encryption. Secret key biasanya menggunakan Data Encryption Standard (DES) yang di share hanya untuk anggota yang ditentukan saja. Sistem ini sengaja di design untuk sistem yang tidak untuk dipublikasikan secara umum. Sedangkan Public key encryption menggunakan sertifikat (key) yang sudah tersedia dan bebas dipakai untuk kepentingan public seperti Pretty Good Privacy (PGP).

5. Enkripsi dan Cryptography

Cryptography telah berkembang sejak lama, ketika orang menginginkan informasi yang ia kirimkan tidak dapat ‘dibaca’ oleh pihak tak berkepentingan. Secara tradisional cryptography dikenal dengan dua mekanisme, kunci privat atau kunci publik. DES (*data encryption standard*) yang digunakan oleh Kerberos menggunakan sistem kunci-privat. RSA (*Rivest Shamir Addleman*) mengimplementasikan sistem kunci-publik. Salah satu dari kontributor RSA, Ron Rivest kemudian membuat MD4 (*message digest function # 4*) yang digunakan oleh S/Key-nya TIS-FWTK. Optimasi dan blasteran antara kedua metoda tradisional ini melahirkan PGP (*Pretty*

Good Privacy). Pembahasan dari DES, RSA, atau PGP merupakan buku tersendiri dan tidak pada tempatnya diungkapkan disini. Tapi yang jelas, sistem kunci-privat dicirikan dengan proses *encrypt-decrypt* melalui kunci identik, sedangkan pada sistem kunci-publik, proses ini dilakukan dengan dua buah kunci: kunci publik untuk *encrypt* dan kunci rahasia untuk *decrypt* dimana kedua kunci ini digenerasikan dan mempunyai relasi dekat melalui sebuah algoritma matematis. Karena diperlukan proses matematis terlebih dulu, kecepatan sistem kunci-publik bisa ribuan kali lebih lambat dari algoritma kunci-privat ekivalen walaupun disisi lain menawarkan proteksi lebih baik. Eksploitasi terhadap kelebihan dan kekurangan sistem kunci privat dan publik dilakukan PGP, dimana untuk transmisi data dilakukan secara sistem kunci-privat dengan *session-key* sehingga berjalan cepat, sedangkan transmisi *session-key*- nya sendiri menggunakan kunci-publik.

Dengan enkripsi, informasi yang kita kirimkan ke suatu jaringan melalui jaringan lain yang keamanannya meragukan (internet), relatif lebih terjamin. Enkripsi antar jaringan menyebabkan seorang 'pencuri' harus berusaha sedikit lebih keras untuk mendapatkan informasi ilegal yang ia harapkan. Ada beberapa kesempatan bagi implementasi enkripsi, yaitu: pada level aplikasi, level *data-link*, dan level jaringan.

Enkripsi pada level aplikasi mensyaratkan penggunaan perangkat lunak client-server khusus. Sesuai dengan model referensi OSI, enkripsi data-link hanya berlaku untuk hubungan titik ke titik, seperti sistem enkripsi pada modem telepon. Sedangkan enkripsi level jaringan (*network layer*) diterapkan pada router atau peralatan lain yang bersebelahan dengan jaringan dikedua sisi. Optimasi kepentingan dan kebijakan security dilakukan dengan mengatur jenis/bagian paket IP yang akan dienkrip, penyesuaian terhadap arsitektur firewall dan konsekuensinya, efektifitas distribusi kunci-enkripsi dll. Di masa depan, dimana teknologi VLAN (*Virtual LAN*) diperkirakan menjadi pilihan utama untuk Intranet (*enterprisewide*), penggunaan enkripsi level jaringan ini menjadi begitu penting. Barangkali sama pentingnya dengan keadaan sebuah perusahaan yang sementara ini 'terpaksa' menggunakan internet sebagai jalur bagi pengiriman informasi sensitif antara kantor pusat dengan cabangnya dibelahan bumi yang lain.

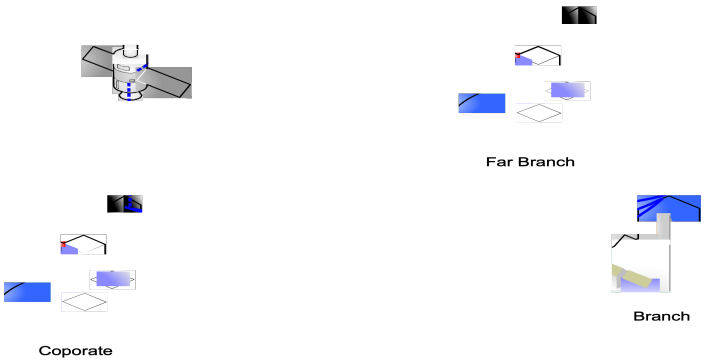
6. Tunneling

VPN juga menggunakan "tunneling" untuk menciptakan koneksi antar host, termasuk yang akan dibahas pada buku ini, Point to Point Tunneling Protocol (PPTP) dan Internet Protocol Security (IPSec).

7. Alasan jarak

Jarak merupakan kendala tersendiri bagi "pemain korporasi". Kita tidak akan mempermasalahkan jarak jika aktifasi yang dilakukan hanya satu kota saja. Apalagi pemain wireless sudah banyak. Selain itu regulasi untuk 2,4 Ghz sudah sangat melegakan bagi dunia IT Indonesia (Thx berat bagi pejuang IT). Pengalaman kami waktu bekerja pada perusahaan retail di Surabaya, yang notabene lokasi hanya sekitar Surabaya. Admin nggak perlu pusing pusing

membuat koneksi VPN, dikarenakan money tersedia, bandwidth nggak begitu penting, dan jumlah cabang sedikit. Tetapi ketika pertumbuhan perusahaan meningkat maka kebutuhan akan teknologi tak terhindarkan. ”Duar....biaya investasi semakin meninggi”. Investasi dengan membuka cabang barupun jadi mikir 1000 kali. Apalagi cabang dengan letak goegrafis lintas benua....hueuheuhue.



Gambar 6-77 Jaringan VPN pengaruh jarak

Masalah tidak akan muncul jika branch (cabang) yang kita punya masih satu kawasan geografi. Tetapi akan muncul jika kawasan geografi yang kita punya sangat berjauhan sehingga menggunakan infrastruktur yang sangat sangat mahal untuk disewa.....weks ngeri.

8. Keterbatasan infrastruktur

Faktor ini juga sangat menarik untuk dibahas. Alasannya simple yaitu ”Indonesia”. Kreatif dan penuh inovatif merupakan syarat mutlak seorang network admin di Indonesia. Kita nggak bisa mengandalkan satu provider saja dalam menangani kebutuhan kita. Tatkala ada problem di sisi provider yang kita sewa maka problem itu mau nggak mau berimbas pada kinerja perusahaan. Kita tidak bisa mengatakan ADSL itu bagus jika dibangun diatas jaringan ”old wire”. Kita juga tidak bisa mengatakan wireless 2,4 GHz murah dan bagus jika banyak interferensi disana sini dan saling menaikkan *ampli*. Dan kita nggak bisa mengatakan 5,8 GHz dan jaringan sewa lainnya bagus jika downtime yang lama. Pada dasarnya system backup sangatlah mutlak diperlukan untuk system yang stabil. Dan nggak semua system backup bagus (cost efficiency). Tetapi dengan mempunyai system backup yang ”cukup pintar”, kita bisa tidur dengan tenang dibuatnya. Buku ini juga membahas pemilihan provider yang tepat untuk VPN yang akan kita bangun.

9. Keterbatasan software pendukung

Mungkin dibenak pemain aplikasi internet bertanya *”Kok nggak di porting aja boss ??? Dari database dan programing yang sudah jamak digunakan misal: PHP dan mysql atau PHP dan postgreSQL”*. Weleh.... porting adalah mimpi buruk bagi seorang DBA dan programer. Bagaimana nggak dulunya ada **ALTER TABLE** sekarang nggak ada. Dulunya ada **TRIGER** sekarang tidak tersedia, bener bener pening dibuatnya. Atau bahkan ada yang usul direplikasi ke database engine yang berbeda via DTS. Hiks.....nggak segampang gitu brur....bisa sih bisa cuman butuh analisa yang cermat. Sedangkan kebutuhan akan online system semakin

meningkat. Selain itu nggak semua SDM yang ada experience pada multi database. Dengan alasan itulah VPN sebagai solusi untuk meringkan beban DBA dan programer.

10. Minimnya bandwidth yang ada

”Save your cost, with save your bandwidth”. Dengan meminimalkan paket yang lewat hanya yang diinginkan saja berarti kita sudah memaksimalkan kinerja **network traffic** yang kita punyai. VPN sangat *consern* dengan hal itu. Pada bab selanjutnya akan kita bahas beberapa tipe VPN kelebihan dan kekurangannya jika kita lihat dari traffic yang lewat.

Mahalnya infrastruktur di Indonesia merupakan tantangan tersendiri bagi seorang network administrator untuk membuat sistem jaringan yang hemat tapi secure. Ide dasar dalam penerapan sistem VPN *ala* Indonesia adalah ”VPN dial on demand”. Maksudnya, buku ini akan membahas perencanaan dan pembuatan VPN yang diterapkan untuk infrastruktur Indonesia. Jika saja kita hidup di Amerika atau negara maju di bidang IPTEK lainnya yang biaya sewa jaringan sangatlah murah, maka kita tidak perlu membahas secara detail koneksi VPN dial on demand. Just ”Plug and Play” gitu loh.....

Buku ini juga menyebutkan beberapa provider, baik provider GSM, CDMA dan Internet secara langsung dikarenakan memang hanya provider tersebutlah yang sangat mungkin untuk dikembangkan menggunakan konsep dial on demand. Kami sudah berusaha untuk bernegoisasi dengan beberapa provider tetapi belum *”dikabulkan”*.

6.2 Model VPN

VPN menggunakan teknologi IPSec. Dimana IPSec adalah sekumpulan ekstensi dari keluarga protokol IP. IPSec menyediakan layanan kriptografi untuk keamanan transmisi data. Layanan ini termasuk *authenticity*, *integrity*, *access control*, *confidentiality*, dab *anti replay*. Layanan IPSec mirip dengan SSL namun, IPSec melayani lapisan *network*, dan dilakukan secara transparan. Layanan tersebut dideskripsikan sebagai berikut:

- ***Confidentiality***, untuk meyakinkan bahwa sulit untuk orang lain tetapi dapat dimengerti oleh penerima yang sah bahwa data telah dikirimkan. Contoh: Kita tidak ingin tahu seseorang dapat melihat password ketika login ke *remote* server.
- ***Integrity***, untuk menjamin bahwa data tidak berubah dalam perjalan menuju tujuan.
- ***Authenticity***, untuk menandai bahwa data yang dikirimkan memang berasal dari pengirim yang benar.
- ***Anti Replay***, untuk meyakinkan bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan untuk mengulang.

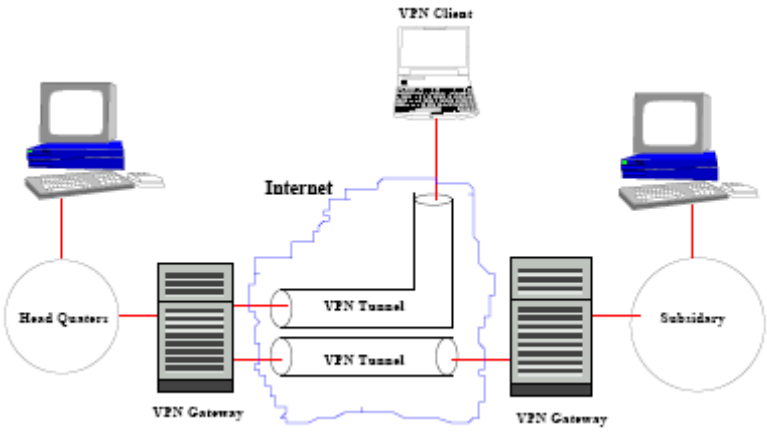
IPSec bekerja dengan tiga jalan, yaitu:

1. *Network-to-network*
2. *Host-to-network*
3. *host-to-host*

Contoh koneksi *network-to-network*, misalnya sebuah perusahaan yang mempunyai banyak kantor cabang dan ingin berbagi data dengan aman, maka tiap cabang cukup menyediakan sebuah

gateway dan kemudian data dikirimkan melalui infrastuktur jaringan internet yang telah ada. Semua lalu lintas data antara *gateway* disebut *virtual tunnel*. Kedua *tunnel* tersebut memverifikasi otentifikasi pengirim dan penerima dan mengenkripsi semua lalu lintas. Namun lalu lintas didalam sisi *gateway* tidak diamankan karena diasumsikan bahwa LAN merupakan segment jaringan yang dapat dipercaya.

Koneksi *host-to-network*, biasanya digunakan oleh seseorang yang menginkan akses aman terhadap sumberdaya suatu perusahaani. Prinsipnya sama dengan koneksi *network-to-network* hanya saja salah satu sisi *gateway* digantikan oleh *client*.



Gambar 6-78 Network to Network dan Host to Network

Protokol yang berjalan dibelakang IPSec adalah:

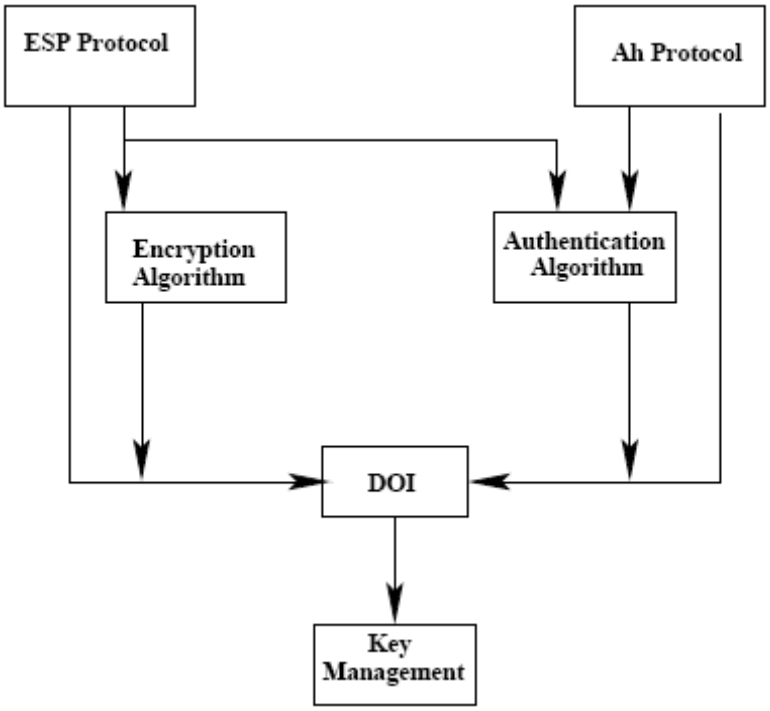
- AH (*Authentication header*), AH menyediakan layanan *authentication*, *integrity*, dan *replay protection*, namun tidak dengan *confidentiality*. AH juga melakukan pengamanan terhadap header IP.
- ESP (*Encasulapted security payload*), ESP menyediakan layanan *authentication*, *integrity*, *replay protection*, dan *confidentiality* terhadap data (ESP melakukan pengamanan terhadap segala sesuatu dalam paket data setelah header).

Pengamanan hubungan dalam IPSec didefinisikan dalam istilah *security associations* (SA). Tiap SA mendefinisikan satu hubungan data secara unidirectional. Ada tiga *fields* dalam SA yaitu *destination IP address*, *security parameter index*, dan *security protocol*.

6.2.1 IPSec Modes

Berdasarkan fungsi, IPSec diaplikasikan berdasarkan titik akhir dimana IPSec melakukan enkasulapsi. Pembagian berdasarkan fungsi tersebut adalah:

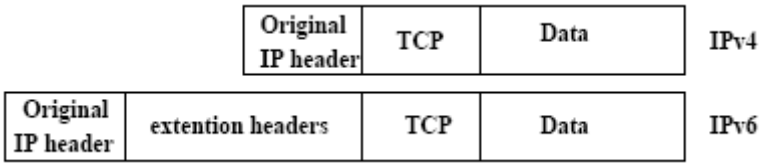
- *Transport mode*. *Transport mode* digunakan untuk mengenkripsi dan mengotentifikasi (*optional* data IP (*transport layer*).



Gambar 6-79 Arsitektur IPsec

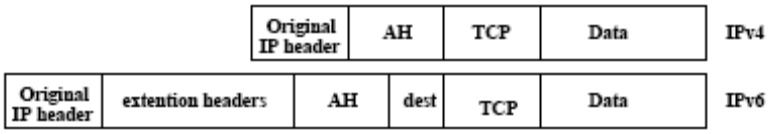
Tunnel mode. *Tunnel mode* mengenkripsi seluruh paket IP.

Transport mode biasanya digunakan untuk komunikasi *peer-to-peer* antara *nodes* dan *tunnel mode* biasanya digunakan untuk mengamankan komunikasi *gateway* dengan yang lainnya. Untuk VPN digunakan *tunnel mode*. Implementasi AH pada IPv4 dan IPv6 diperlihatkan pada gambar:

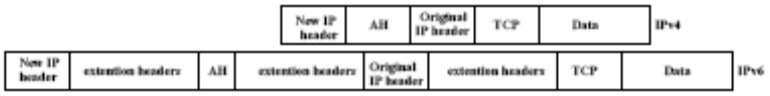


Gambar 6-80 Paket IP sebelum memasukkan AH

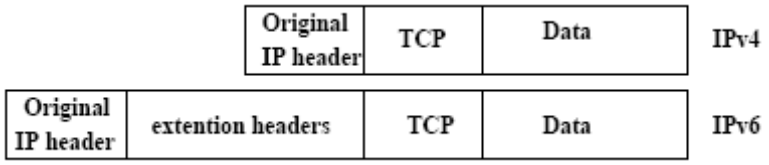
Implementasi ESP pada IPv4 dan IPv6 diperlihatkan pada gambar:



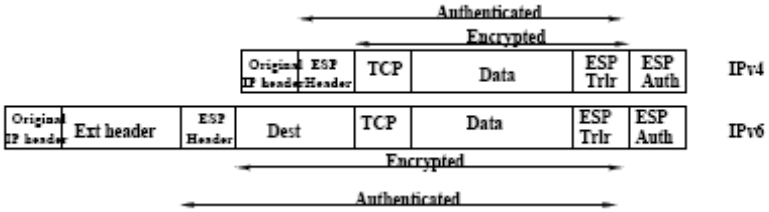
Gambar 6-81 Transport Mode dan AH



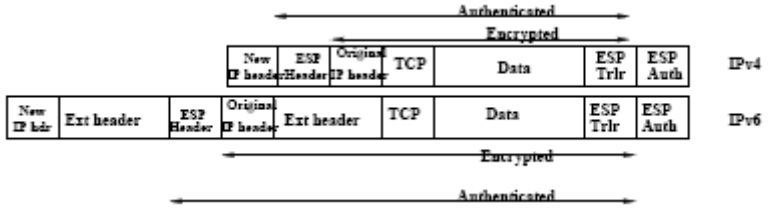
Gambar 6-82 Tunnel Mode dan AH



Gambar 6-83 Paket IP Sebelum Memasukkan ESP



Gambar 6-84 Transport Mode dan EPS



Gambar 6-85 Tunnel Mode dan EPS

Secara umum IPSec mempunyai kompleksitas yang cukup besar. IPSec terlalu banyak memiliki *options* dan terlalu banyak memiliki fleksibilitas [4]. Ada cukup banyak cara untuk melakukan hal yang sama dalam IPSec, sebagai akibat dari para *developer* IPSec yang mencoba mendukung berbagai macam situasi dengan *options* yang berbeda-beda. Akibat kompleksitas tersebut muncul potensi kelemahan dan menyulitkan analisis keamanan terhadap IPSec.

Hal kedua yang perlu mendapat perhatian adalah dokumentasi. Dokumentasi IPSec sangat sulit dimengerti. Tidak ada pendahuluan, pembaca harus sedikit demi sedikit secara perlahan memahami dokumentasi IPSec. Salah satu contoh dokumentasi IPSec yang sulit dimengerti adalah spesifikasi ISAKMP.

Dokumentasi IPSec tidak menyebutkan tujuan secara eksplisit. Tanpa tujuan yang eksplisit tidak ada standar analisis yang tepat untuk keamanan data melalui IPSec. Kekurangan spesifikasi IPSec juga menyulitkan pengguna untuk menggunakan IPSec, ada banyak *prerequisites* yang tidak disebutkan secara eksplisit dalam dokumentasi IPSec. Seorang desainer jaringan yang mencoba menggunakan IPSec tanpa mengetahui dengan jelas dokumentasi serta *prerequisites* yang tidak utuh akan menghasilkan fungsi IPSec yang tidak optimal atau dengan

kata lain tidak mencapai tujuan keamanan yang diharapkan. Perlu diingat bahwa **"Hampir aman sama dengan tidak aman"**.

6.2.1.1 Penanganan Data

Inti dari IPSec terdiri atas fungsi-fungsi yang menyediakan layanan otentifikasi dan *confidentiality* untuk paket IP. Ini yang digunakan contohnya untuk membangun VPN diatas jaringan internet yang tidak dapat dipercaya untuk mengamankan transmisi paket data.

IPSec mempunyai dua macam operasi yaitu *transport* dan *tunnel*. Ada dua protokol yang digunakan yaitu AH dan ESP. AH menyediakan layanan otentifikasi dan ESP menyediakan layanan otentifikasi, enkripsi, dan keduanya. Hal ini membuat masalah kompleksitas. Misalkan dua mesin yang yang ingin melakukan otentifikasi sebuat paket ada mempunyai empat cara berbeda yaitu: transport dengan AH, tunnel dengan AH, transport dengan ESP, dan transport dengan ESP.

Beberapa saran yang diajukan oleh Ferguson dan Schneier [4] adalah menghapus *transport mode* karena dapat mengurangi kebutuhan untuk memisahkan mesin dalam satu jaringan kedalam dua kategori yaitu *hosts* dan *gateway*, dan secara umum *hosts* dalam satu jaringan masih dapat dianggap sebagai *trusted machines* sehingga *transport mode* jarang digunakan. Dalam kenyataan sehari-hari sebuah perusahaan dalam berkomunikasi dengan kantor cabang atau rekan bisnis mereka lebih banyak menggunakan VPN, artinya *tunnel mode* lebih sering digunakan dalam kehidupan sehari-hari.

Ferguson dan Scheneier [4] juga mengusulkan agar protokol AH tidak perlu digunakan, karena protokol ESP selalu dapat menyediakan layanan otentifikasi dan enkripsi. Dalam semua kasus, enkripsi tanpa otentifikasi adalah hal yang sia-sia, karena itu Ferguson dan Scheneier [4] juga mengusulkan agar memodifikasi protokol ESP agar selalu menyediakan layanan otentifikasi, namun layanan enkripsi menjadi *optional*.

6.2.1.2 Layer 2 Tunneling Protocol (L2TP)

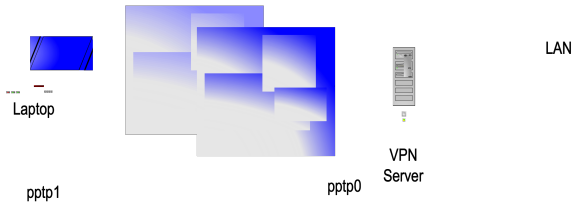
L2TP adalah protokol tunnel yang digunakan pada model VPN IPSec yang berjalan di layer 2 pada OSI layer. Protokol ini tidak memberikan fasilitas enkripsi ataupun kerahasiaan dengan sendirinya, melainkan mengandalkan dari protokol enkripsi yang berjalan pada tunnel yang dibangun.

Protokol ini dibangun pada tahun 1999 berdasarkan RFC 2661, pada awalnya merupakan protokol point-to-point komunikasi dari Cisco Layer 2 Forwarding Protocol (L2F) dan USRobotics Point-to-Point Tunneling Protocol (PPTP). Versi terbaru dari protokol ini adalah L2TPv3, dimana terdapat pada RFC 3931 terbit pada tahun 2005.

Keseluruhan paket L2TP, termasuk juga payload dan header dikirim dalam bentuk UDP datagram. Didalamnya membawa juga informasi sesi PPP dalam tunnel L2TP. Dikarenakan protokol ini tidak menjamin kerahasian data, implementasi protokol ini digunakan bersama dengan protokol IPSec. Sehingga implementasi dari protokol ini menjadi L2TP/IPSec, dan distandardkan dalam RFC 3193. Kedua endpoint dari tunnel L2TP disebut juga sebagai LAC

(L2TP Access Concentrator) dan LNS (L2TP Network Server). LAC adalah bagian client yang mencoba untuk membangun koneksi VPN, sedangkan LNS adalah bagian Server yang menunggu koneksi permintaan tunnel baru.

6.2.2 PPTP

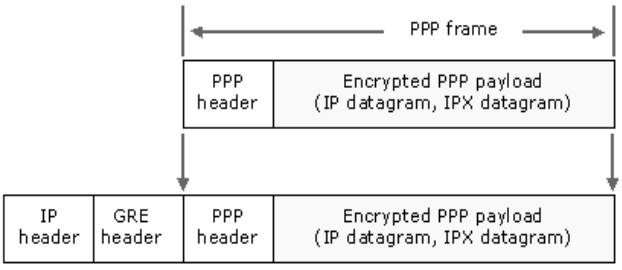


Gambar 6-86 Point to Point Tunnelling Protokol (PPTP)

Point to Point Tunnelling Protocol (PPTP) merupakan perluasan dari PPP (Point to Point Protocol). Service tunneling disediakan oleh PPTP dan diharapkan untuk bekerja pada bagian atas layer IP. PPP dimodifikasi sedemikian hingga agar dapat memenuhi kebutuhan untuk koneksi VPN yaitu point to point tunnel. Dengan tunnel PPTP lebih secure dibandingkan koneksi LAN to LAN. PPTP sudah memenuhi syarat menjadi salah satu komponen penting VPN yaitu enkapsulasi dan enkripsi.

6.2.2.1 Enkapsulasi

Frame PPP (terdiri IP datagram atau IPX datagram) dibungkus oleh Generic Routing Encapsulation (GRE) header dan IP header. Didalam header IP source dan destination address terhubung langsung dengan VPN client dan VPN server. Gambar dibawah ini menunjukkan format frame PPTP.



Gambar 6-87 Format Frame PPTP

6.2.2.2 Enkripsi

Pada keluarga windows, PPTP di support oleh Microsoft Point-to-Point Encryption (MPPE) dengan menggunakan kunci generator dari MS-CHAP atau EAP-TLS. Virtual private clients harus menggunakan salah satu diantaranya, MS-CHAP atau EAP-TLS yang berfungsi sebagai authentication protocol.

6.2.2.3 Support Microsoft untuk PPTP

Bagi keluarga Microsoft, tidak semua windows mensupport protocol dan algoritma untuk proses authentikasi, dan bahkan ada yang harus di patch terlebih dahulu DUN (Dial Up Networking) nya. Tabel dibawah ini menunjukkan supporting PPTP terhadap operating system windows.

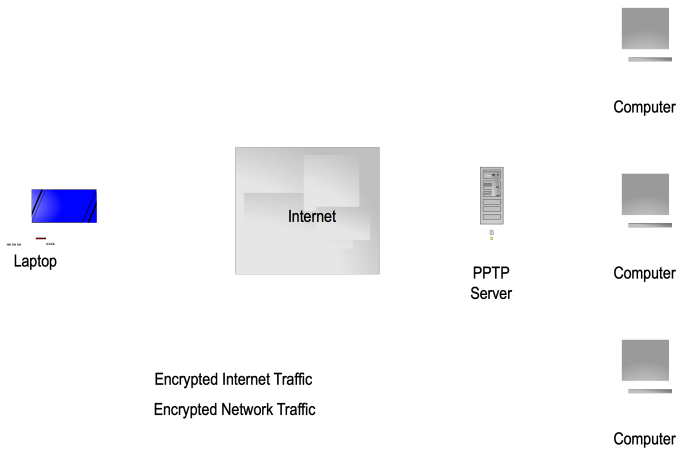
Table 6-1 Tabel supporting PPTP terhadap OS Windows

Virtual private networking client	Supported tunneling protocols	Unsupported tunneling protocols
Windows 2000	Point-to-Point Tunneling Protocol (PPTP)and Layer Two Tunneling Protocol (L2TP)	
Windows NT version 4.0	PPTP	L2TP
Windows 98	PPTP	L2TP
Windows 95	PPTP with the Windows Dial-Up Networking 1.3 Performance & Security Upgrade for Windows 95	L2TP

Untuk windows 95 diperlukan upgrade DUN (Dial UP Networking) terlebih dahulu untuk support PPTP. Menurut pengalaman kami performance PPTP pada wndows 95 sangat jelek untuk time koneksinya. Jadi anda harus sabar menunggu untuk terkoneksi ke VPN server .

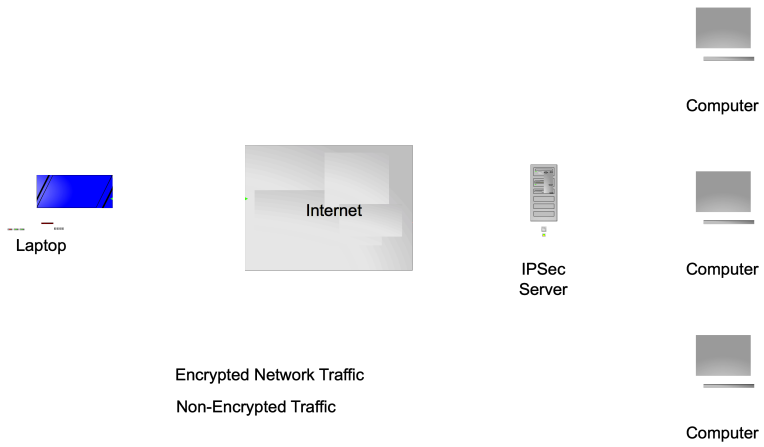
6.2.3 IPSec vs PPTP

Jika kita telaah lebih lanjut, ada kelebihan dari IPSec dibandingkan PPTP jika dilihat dari sisi konsumsi bandwidth. Pada gambar dibawah ini menunjukkan perbedaan konsumsi bandwidth diantara keduanya.



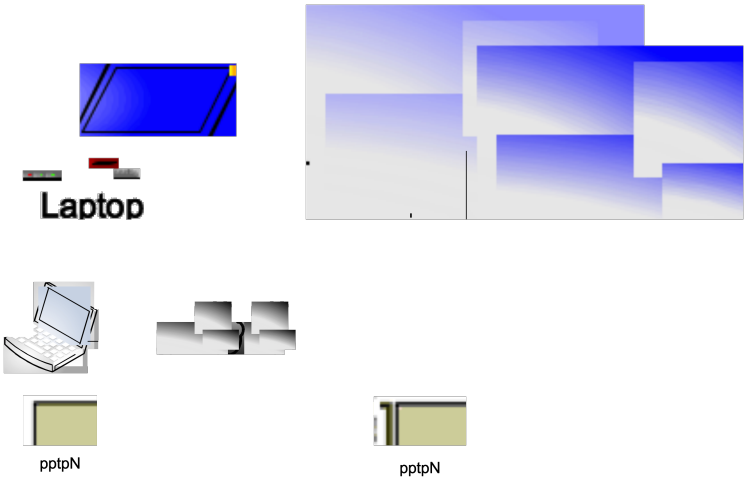
Gambar 6-88Jaringan PPTP

Pada PPTP baik paket yang diinginkan maupun yang tidak diinginkan di enkripsi dan dikirim ke tujuan. Sehingga menyebabkan traffic dari user menjadi sangat tinggi.



Gambar 6-89 jaringan IPSec

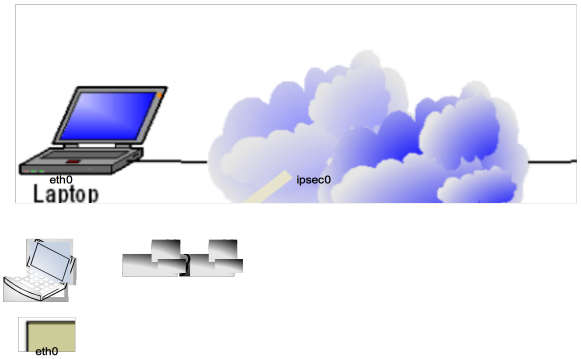
Sedangkan pada IPSec traffic bisa dikontrol dengan membatasi port port mana saja atau aplikasi aplikasi mana saja yang akan ditumpangi dengan IPSec. Pada bab selanjutnya juga dibahas teknik ”custome’ tersebut. Selain itu kelebihan IPSec yang lain jika dibandingkan dengan PPTP adalah management user yang simple.



Gambar 6-90 Perbandingan IPSec dan PPTP

Konfigurasi PPTP selalu menentukan terlebih dahulu user, password dan jumlah pool setiap networknya. Artinya setiap koneksi PPTP harus menyediakan virtual interface pada sisi server sejumlah user yang akan melakukan koneksi ke server. PPTP bekerja pada layer 2 (Data link layer). Sehingga kinerja dari PPTP belum sepintar IPSec yang bekerja pada layer3 (Network layer). Fungsi-fungsi pada layer 3 seperti routing belum bekerja pada PPTP. Lebih

detail dari keterangan gambar diatas, IP Pool yang disiapkan oleh VPN PPTP harus satu network dengan IP tujuan. Maksudnya jika yang dituju adalah host dibelakang PPTP server dengan nomer IP 192.168.200.2, maka IP Pool yang disediakan harus bernilai 192.168.200.0/24. Jika tidak, admin harus menyediakan router tersendiri agar network dibelakang server bisa terkoneksi dengan client PPTP. Sedangkan jumlah network untuk IP pool boleh lebih dari satu dan sesuai dengan kebutuhan. Misalnya IP pool disiapkan untuk keperluan koneksi multi network pada jaringan corporate. Pada bab selanjutnya akan dijelaskan IP pool pada sistem operasi windows dan system operasi linux.



Gambar 6-91 Penerapan IPSec dengan VPN Server

Sedangkan IPSec cukup menyediakan satu interface dalam melayani beberapa koneksi yang ada. Client 1 dan client 2 pada gambar diatas menggunakan masing masing interface terluarnya (eth0) untuk melakukan koneksi dengan VPN server yang menggunakan ipsec0 sebagai interface terluarnya. Maksud dari interface terluar adalah interface yang mendapat akses langsung ke internet. Sebagai contoh diatas adalah eth0. Dalam praktek sehari hari interface bisa berupa virtual interface seperti ppp0. Sedangkan ipsec0 adalah virtual interface yang dihasilkan oleh IPSec tools dalam hal ini FreeSWAN sebagai pengganti physical interface. Dengan memberikan certificate kepada client, maka kita dapat membatasi hak akses client tersebut. Hak akses dalam IPSec bisa berupa pengelompokan certificate, jumlah network yang akan diakses dan jenis port yang diteruskan. Untuk pembatasan user berdasarkan certificate dengan FreeSWAN kita bisa menggunakan opsi **uniqueids=yes**, maksudnya certificate tersebut bersifat unik dan hanya aktif dan digunakan oleh satu user saja. Jika ada user lain yang menggunakan maka salah satunya akan berstatus “Negotiating IP Security”.(keluar dari system).

```
    config setup
interfaces=%defaultroute
klipsdebug=none
plutodebug=none
plutoload=%search
plutostart=%search
uniqueids=yes
```

IPSec juga bisa membatasi hanya network network tertentu saja yang dapat diakses oleh clientnya.

conn Hamburg

left=%any

mac=00-01-02-97-C2-E3

right=193.96.216.190

rightsubnet=193.22.11.192/26

rightca="C=DE, S=Germany, L=Essen, O=e.bootis AG, OU=Root CA, CN=e.bootis VPN Root CA (c) 2001"

network=lan

authmode=sha

rekey=1800S/30000K

auto=start

pfs=yes

Lihat opsi right subnet diatas, yang hanya membolehkan usernya untuk akses network dibelakang server **193.22.11.192/26** saja dan bukan keseluruhan network (**193.22.11.192/24**). Dengan beroperasinya IPSec di layer 3 sebenarnya kita diuntungkan nggak usah repot repot pasang routing disana sini. Tinggal kasih akses yang jelas jadi deh. But….. dibalik itu semua kewaspadaan harus tetap ditingkatkan dengan hanya membolehkan paket paket tertentu saja (yang sesuai dengan ketentuan firewall yang dipakai) boleh melewati rule yang telah ditetapkan.

6.3 Pengertian PGP

PGP adalah suatu metode penyandian informasi yang bersifat rahasia sehingga jangan sampai diketahui oleh orang yang tidak berhak. Informasi ini bisa berupa e-mail yang sifatnya rahasia, nomor kode kartu kredit, atau pengiriman dokumen rahasia perusahaan melalui internet. PGP menggunakan metode kriptografi yang disebut “public key encryption”; yaitu suatu metode kriptografi yang sangat sophisticate.

Beberapa istilah yang sering digunakan

- **cryptography/encryption**

ilmu pengetahuan yang mempelajari pengacakan text sehingga tidak seorang pun yang dapat mengetahuinya kecuali bila ia tahu kode yang digunakan untuk men-dechipernya.

- **conventional cryptography**

suatu metode encryption/enkripsi di mana suatu kunci digunakan untuk melakukan enksripsi dan dekripsi suatu plaintext.

- **encrypt/encipher**

pengacakan/scramble dari suatu informasi.

- **decrypt/decipher**

mengembalikan informasi yang telah diacak menjadi bentuk informasi yang semula.

- **ciphertext/cipher**

text setelah dilakukan proses enkripsi

- **plaintext**

text yang akan dienkripsi

- **key/kunci**

kode yang digunakan untuk melakukan enchiper dan atau dechiper suatu text. Dalam kriptografi konvensional, kunci yang digunakan untuk enkripsi dan dekripsi adalah sama. Dalam public-key cryptography,kunci untuk enkripsi dan dekripsi berbeda.

- **public-key crypto**

suatu sistem yang menggunakan dua kunci; yaitu **public key** dan the **secret key** yang lebih baik dan lebih praktis dibandingkan dengan conventional crypto. Tujuan utamanya adalah kemudahan dalam manajemen kunci.

- **algorithm/algoritma**

algorithm adalah program crypto apa yang digunakan untuk melakukan enkripsi. Ia bukanlah suatu kunci, tetapi menghasilkan kunci. Suatu algoritma yang kuat/bagus akan manghasilkan crypto yang kuat.bagus juga. PGP menggunakan IDEA untuk bagian crypto yang konvensional, dan RSA untuk bagian public-key . keduanya adalah algoritma yang bagus, namun RSA lebih bagus daripada IDEA.

- **passphrase**

adalah suatu word atau phrase, atau bahkan hanya karakter acak, yang digunakan PGP untuk mengidentifikasi seseorang sebagai person yang diinginkan oleh orang tersebut. Suatu passphrase sebaiknya lebih dari satu word, dan jangan pernah membuat yang orang lain dapat menebaknya, seperti nama, nama tengah, binatang kesayangan, nama anak, hari ultah, nama pacar, alamat, band favorit dsb. suatu passphrase yang ideal, adalah setengah dari baris text. Sebaiknya lebih dari tiga word dan mengandung hal-hal berikut: proper name, suatu slang atau vulgar word, dan irregular capitalization, sebagai contoh: tHe, βenny, dll. JUGA, Sifat lainnya adalah ia harus mudah diketik secara cepat, tanpa error, dan tanpa perlu melihatnya pada layar.

- **public key**

adalah suatu kunci yang memiliki sifat sebagai berikut : mempunyai suatu koneksi, sangat berbeda dari yang lainnya, didistribusikan dalam jumlah yang besar , melaluui banyak channel, secure atau insecure.

- **secret key**

adalah suatu kunci yang dimiliki oleh kita dan hanya kita seorang, dan tidak pernah diperlihatkan kepada publik.

- **ASCII armor/radix-64**

adalah suatu format yang digunakan PGP untuk mengkonversi default binary ciphertext, yang tidak dapat ditransfer melalui jaringan, menjadi suatu bentuk ASCII yang dapat dikirmkan melalui email atau usenet.

6.3.1 Prinsip Kerja PGP

1. PGP, seperti yang telah dijelaskan sebelumnya, menggunakan teknik yang disebut public-key encryption dengan dua kode. Kode-kode ini berhubungan secara intrinsik, namun tidak mungkin untuk memecahkan satu dan yang lainnya.
2. Bila suatu ketika kita membuat suatu kunci, maka secara otomatis akan dihasilkan sepasang kunci yaitu public key and secret key. Kita dapat memberikan public key ke manapun tujuan yang kita inginkan, melalui telephone, internet, keyserver, dsb. Secret key yang disimpan pada mesin kita dan menggunakan messager decipher akan dikirimkan ke kita. Jadi orang yang akan menggunakan public key kita (yang hanya dapat didekripsi oleh oleh secret key kita), mengirimkan messages kepada kita , dan kita akan menggunakan secret key untuk membacanya.
3. Kenapa menggunakan dua kunci ?.

   Karena dengan conventional crypto, di saat terjadi transfer informasi kunci, suatu secure channel diperlukan. Dan jika kita memiliki suatu secure channel, mengapa kita menggunakan crypto? Namun dengan public-key system, tidak akan menjadi masalah siapa yang melihat kunci milik kita, karena kunci yang dilihat orang lain adalah yang digunakan hanya untuk enkripsi dan hanya kita sebagai pemilik yang mengetahui secret key; yaitu key yang berhubungan secara fisik dengan komputer kita yang dapat melakukan proses dekripsi dengan public key yang ada dan kemudian kita masukan lagi passphrase. Jadi seseorang mungkin dapat mencuri passphrase yang kita ketikkan, namun ia dapat membaca hanya jika ia dapat mengakses komputer kita

6.3.2 Ilustrasi Pemakaian PGP

- Public-key sangat lambat bila dibandingkan dengan konvensional, jadi PGP akan mengkombinasikan dua algoritma, yaitu RSA and IDEA, untuk melakukan enkripsi plaintext kita.
- Sebagai contoh, Badrun (pemilik PGP) ingin mengenkripsi suatu file yang diberi nama plain.txt sedemikian sehingga hanya si Matangin yang dapat mendekripsi-nya. Maka Badrun mengirimkan PGP perintah (command line) untuk melakukan enkripsi :

  pgp -e plain.txt Matangin

  Pada command line ini, pgp adalah file executable, -e berarti memberitahukan PGP untuk meng-**e**ncrypt file, plain.txt adalah nama plaintext, dan `dul` merepresentasikan public key suatu tujuan (Matangin) yang diinginkan Badrun untuk mengenkripsi message-nya. PGP menggunakan suatu *random number generator,* dalam file randseed.bin untuk

menghasilkan suatu kunci (session key) temporary IDEA. Session key itu sendiri di-enkripsi dengan kunci RSA public yang direpresentasikan oleh Matangin yang disematkan pada plaintext.

- Kemudian, PGP menggunakan session key untuk mengenkripsi message, ASCII-armors dan menyimpan seluruhnya sebagai cipher.asc. Bila Matangin ingin membaca pesannya, ia mengetikkan command:

pgp cipher.asc

- PGP menggunakan *secret key* milik Matangin, yang merupakan kunci RSA, untuk men-dekripsi sessi kunci yang mana, yang jika dipanggil oleh Badrun akan dienkripsi oleh public key. kemudian, conventional crypto digunakan dalam bentuk session key untuk mendekripsi sisa dari message. Alasan prinsip ini adalah sebagai pengganti/kompensasi dari RSA karena "RSA is too slow, it's not stronger, and it may even be weaker." (-PGP Documentation, pgpdoc2.txt).

6.3.3 Enkripsi untuk File-File Biner

Untuk mereka yang terbiasa bekerja dengan file-file biner, pada usenet mengetahui istilah uuencode. Uuenconde adalah suatu program, yang terutama untuk UNIX, namun sekarang berkembang sehingga dapat mengubah file-file biner seperti .GIF or .AU menjadi ASCII text yang sesuai dengan format pengiriman usenet. Feature ini juga dimiliki oleh PGP. File config.txt (mungkin disebut pgp.ini atau .pgprc ; tergantung protokol local) memiliki suatu option untuk berapa banyak baris file ASCII yang dapat dimuat. Jika jumlah ini tercapai, PGP akan memecah-mecah file armored .asc menjadi .as1, .as2, .as3, ... dan semuanya harus digabungkan satu sama lain secara bersama-sama dan menjalankan PGP dalam suatu file yang besar. Untuk mengenkripsi suatu file biner, gunakan command berikut:

pgp -a picture.gif

atau option TextMode diset ke ON:

pgp -a picture.gif +textmode=off

6.3.4 Compile dan patch kernel

Secara default, kebanyakan kernel yang ada belum melayani aplikasi enkripsi. Hal ini dikarenakan tidak semua pengguna, akan mengimplementasikan enkripsi dalam aplikasi yang dipakai. Disise lain jelas alasan performasi yang semakin menurun pada level level tertentu misalnya : bandwidth, delay dan jitter. Hal ini dikarenakan seiring bertambahnya jumlah paket header yang ada pada aplikasi VPN tersebut. Untuk proses compile kernel dilakukan step by step seperti berikut :

1. Upgrade kernel

   Distro yang digunakan pada tugas akhir kali ini adalah debian woody relase 0, yang notabene mempunyai default kernel 2.4.18. Untuk itu kernel perlu diupgrade menjadi 2.4.27. Buka compress kernel terlebih dahulu dengan perintah :

   ```
   # bunzip2 -xzvf  kernel-source-2.4.27.tar.bz
   ```

```
# tar -xvf kernel-source-2.4.27.tar
```

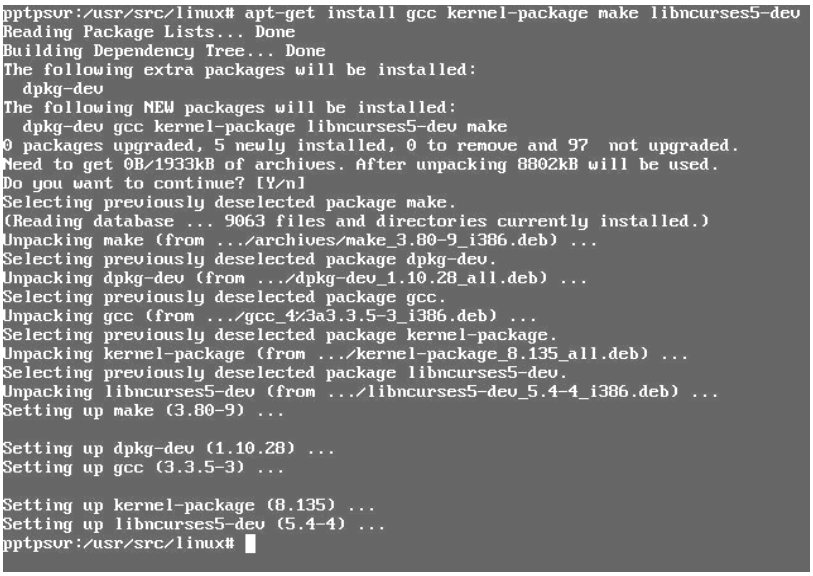
Setelah kompresi terbuka maka buat link dengan nama linux :

```
# ln -s  /usr/src/kernel-source-2.4.27 usr/src/linux
```

2. Install paket pendukung proses compile

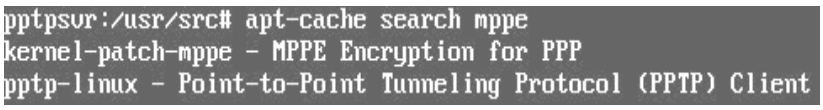
Untuk proses kompilasi kernel dibutuhkan beberapa software pendukung diantaranya gcc dan make. Untuk distro debian kita tinggal memanfaatkan utility apt-get untuk proses instalasinya.

```
# apt-get install make-kpkg gcc libncurses5-dev make kernel-package
```



Patch kernel

Setelah semua paket untuk proses compile kernel telah tersedia, maka kernel siap di lakukan proses compile untuk diupgrade. Tetapi sebelum proses upgrade dilakukan, kernel di patch MPPE terlebih dahulu. Pastikan anda telah mempunyai paket kernel-patch terlebih dahulu di dalam apt cache.



Dari keterangan diatas dapat diketahui kernel-patch sudah tersedia tinggal melakukan proses instalasi. Jika belum ada coba update cache apt dengan debian mirror yang ada di Indonesia.

Install kernel patch untuk MPPE dengan perintah :

```
# apt-get install kernel-patch-mppe
```

```
pptpsvr: # apt-get install kernel-patch-mppe
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  grep-dctrl libc6 libdb1-compat patch
The following NEW packages will be installed:
  grep-dctrl kernel-patch-mppe libdb1-compat patch
1 packages upgraded, 4 newly installed, 0 to remove and 93  not upgraded.
Need to get 5112kB of archives. After unpacking 3240kB will be used.
Do you want to continue? [Y/n]
Get:1 http://kambing.ui.ac.id stable/main libdb1-compat 2.1.3-7 [30.8kB]
Get:2 http://kambing.ui.ac.id stable/main libc6 2.3.2.ds1-22sarge3 [4914kB]
1% [2 libc6 41748/4914kB 0%]                                  9664B/s 8m41s
```

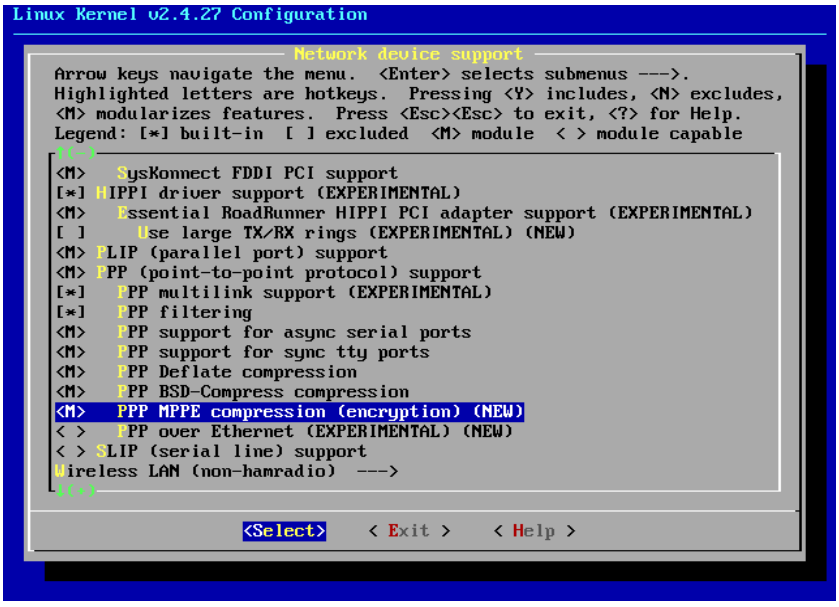
Setelah paket untuk patch kernel telah terdownload semua maka proses patch kernel siap dilakukan.

```
# cd /usr/src/linux
/usr/src/linux# /usr/src/kernel-patch/all/apply/mppe
```

```
pptpsvr:/usr/src/linux# /usr/src/kernel-patches/all/apply/mppe
START applying mppe patch (MPPE encryption support for PPP)
Testing whether "MPPE encryption support for PPP" patch for 2.4.27 applies (dry
run):
"MPPE encryption support for PPP" patch for 2.4.27 succeeded
Removing empty files:
Done.
END applying mppe patch
```

```
# make menuconfig
```

Pilih bagian Network device dan pilih PPP (Point To Point Protocol) dan pastikan MPPE Compression (encryption) ada didalamnya.



Simpan file konfigurasi dan install module yang ada dengan perintah :

```
# make dep && make modules && make modules_install
```

3. Instalasi PPTP Server

Untuk aplikasi PPTP server pada projek kali ini menggunakan PoPToP. Cek menggunakan perintah :

```
# apt-cache search pptpd
```

```
pptpsvr:/usr/src/linux# apt-cache search pptpd
kernel-patch-mppe - MPPE Encryption for PPP
pptpd - PoPToP Point to Point Tunneling Server
```

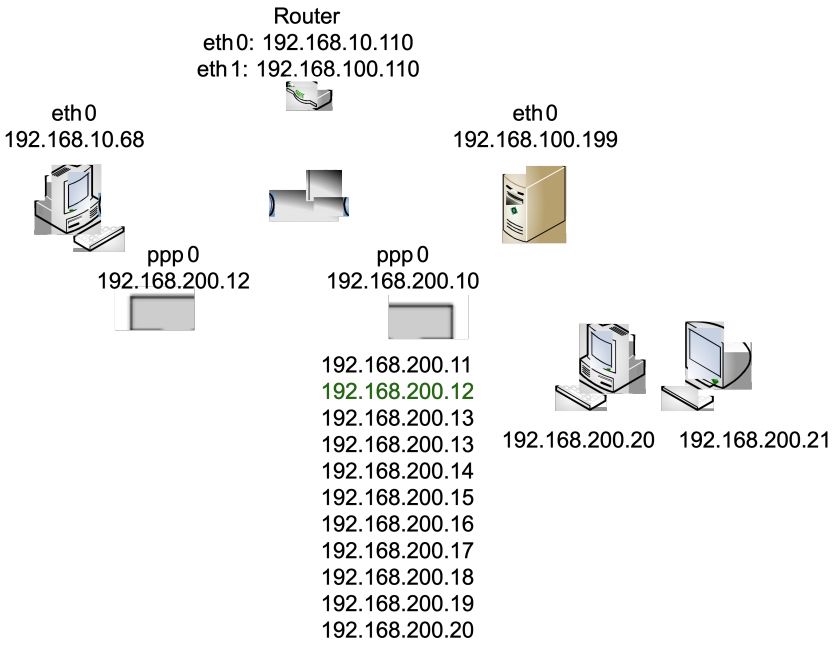
Setelah paket tersedia tinggal menginstall paket tersebut dengan perintah :

```
# apt-get install pptpd
```

```
pptpsvr:~# apt-get install pptpd
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  libpam-runtime libpam0g libpcap0.7 ppp zlib1g
The following NEW packages will be installed:
  libpcap0.7 pptpd zlib1g
3 packages upgraded, 3 newly installed, 0 to remove and 94  not upgraded.
Need to get 651kB of archives. After unpacking 1013kB will be used.
Do you want to continue? [Y/n] 
```

4. Perancangan network

Topologi jaringan untuk projek kali ini dapat dilihat seperti gambar dibawah ini. VPN Server dan client terhubung dengan internet cloud. Pada internet cloud dipasang router yang berfungsi meroutingkan network client dan server. Selain itu pada router akan dipasang tools (tcpdump) untuk mengcapture setiap paket yang lewat.



Gambar 6-92 Perancangan jaringan VPN

5. Konfigurasi server

Dari gambar diatas jelas terlihat kita menginginkan pool IP untuk client dengan ketentuan 192.168.200.11-192.168.200.20. Sedangkan local server akan mendapatkan IP 192.168.200.10. File konfigurasi untuk pool IP dengan konfigurasi diatas dapat dilihat pada (/etc/pptpd.conf).

option /etc/ppp/pptpd-options

localip 192.168.200.10

remoteip 192.168.200.11-20

Sedangkan untuk konfigurasi yang mencakup enkripsi ada pada file /etc/ppp/pptpd-options.

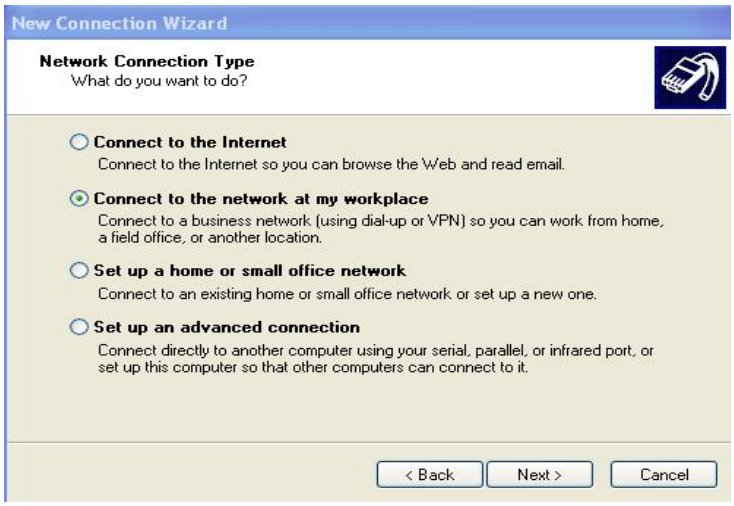
```
# cat /etc/ppp/pptpd-options
name *
lock
mtu1450
mru 1450
proxyarp
auth
ipcp-accept-local
ipcp-accept-remote
lcp-echo-failure 3
lcp-echo-interval 5
deflate 0
require-mschap-v2
require-mppe-128
```

File konfigurasi diatas menunjukkan bahwa authentikasi yang digunakan adalah mschap-v2 dan untuk enkripsi dipakai MPPE dengan 128 bit enkripsi. Selain file konfigurasi diatas kita juga membubuhkan user dan password pada setiap awal koneksi.

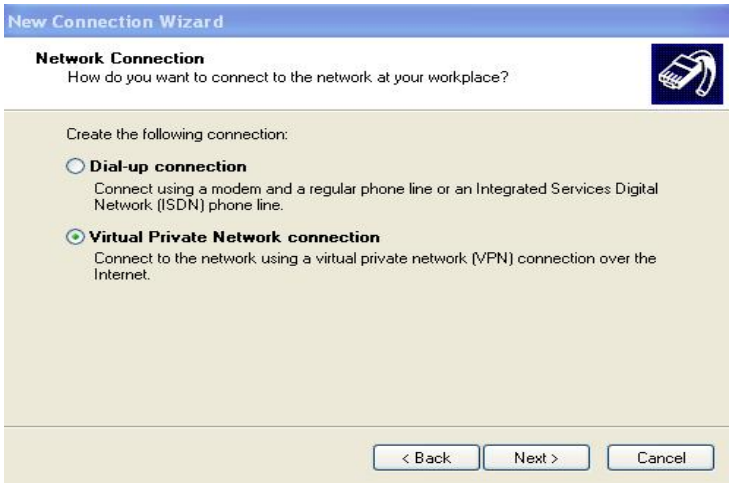
```
# cat /etc/ppp/chap-secrets
#Secrets for authentication using CHAP
# client     server    secret    IP addresses
test         *    testjuga  *
```

6. Instalasi Client

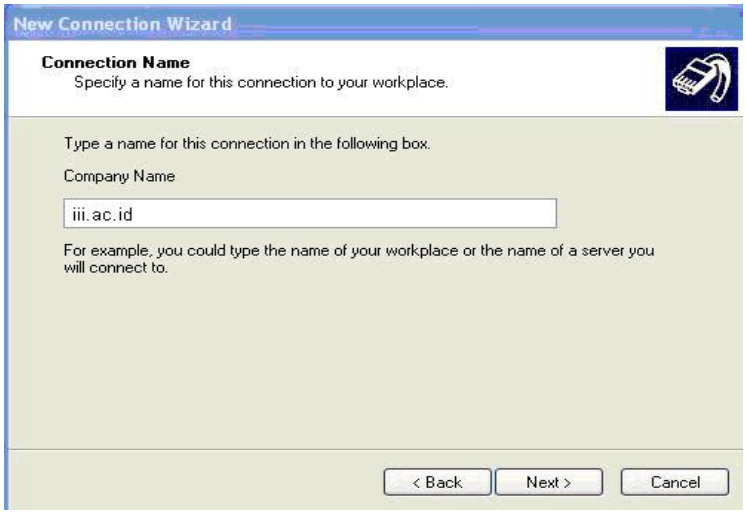
Untuk instalasi client digunakan windows XP. Klik Start → Control Panel → Network connection →Create a new connection → Connect to the network at my workplace klik Next



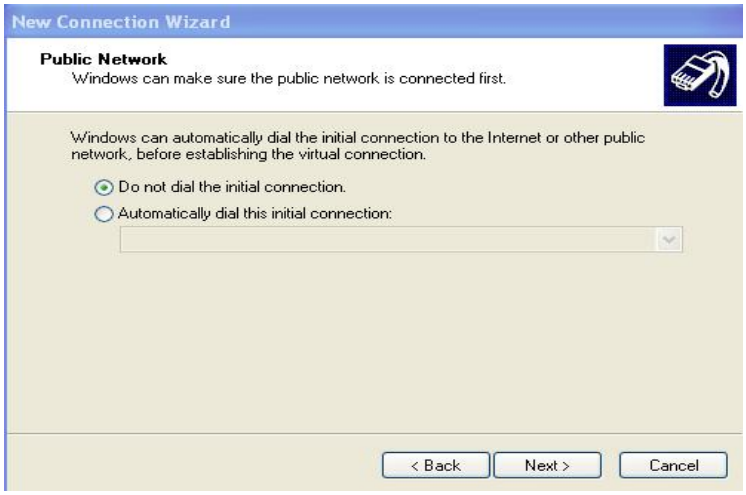
Pilih Virtual Private Network connection untuk membuat koneksi VPN yang diiginkan.



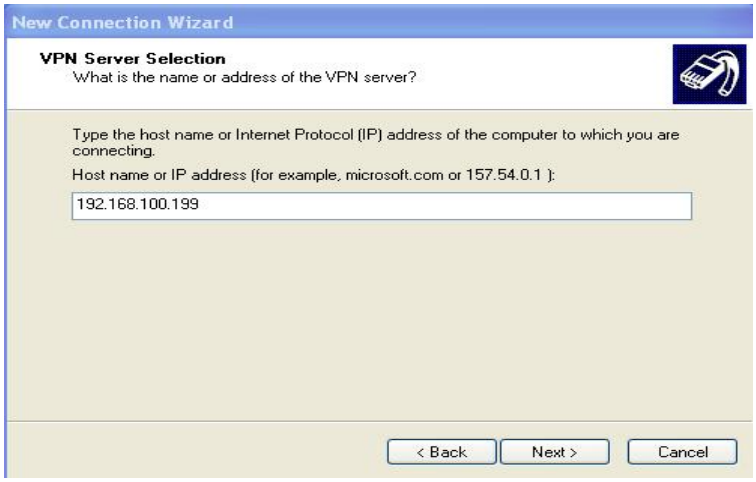
Inputkkan nama koneksi yang dibuat dengan nama iii.ac.id.



Untuk default koneksi gunakan “Do not dial the initial connection”

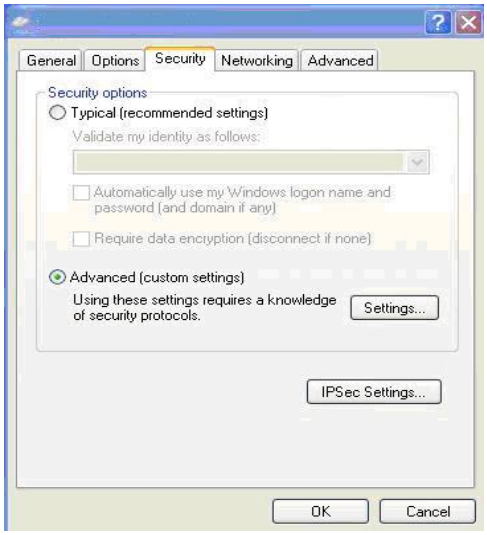


Inputkan IP address VPN server sebagai tujuan koneksi dari client ke server. Dalam hal ini IP address server adalah 192.168.100.199



Instalasi VPN client lewat wizard telah selesai dilakukan klik Finish untuk mengakhiri konfigurasi.

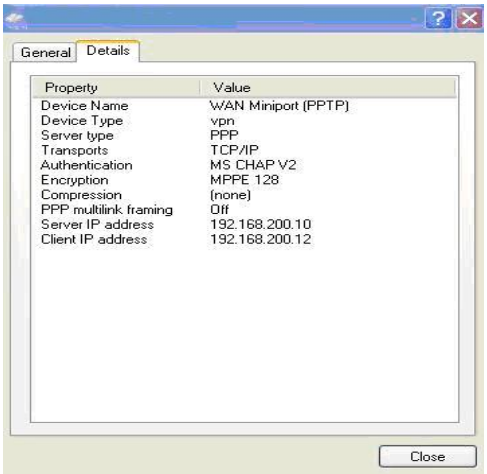
Untuk informasi security dapat dilihat pada Advanced (custom settings)



Konfigurasi client disesuaikan dengan konfigurasi server dengan memakai Microsoft CHAP Version 2 (MS-CHAP v2)

Proses koneksi siap dilakukan dengan memasukkan user dan password authentikasi dari client ke server.

Setelah koneksi telah terbentuk, lihat konfigurasi pada details koneksi



Lihat konfigurasi interface dengan perintah ipconfig pada client dengan perintah

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.10.68
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.10.110
```

```
PPP adapter itats.ac.id:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.200.12
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 192.168.200.12
 Sedangkan log pada server dapat dilihat dengan menggunakan
perintah :
#tail –f /var/log/messages
Aug 9 18:45:01 aris-knx CRON[4831]: (pam_unix) session closed
for user root
Aug 9 18:42:47 aris-knx pppd[4639]: Sent 75 bytes, received 61
bytes.
Aug 9 18:42:47 aris-knx pppd[4639]: Exit.
Aug 9 18:43:04 aris-knx pppd[4675]: pppd 2.4.3 started by root,
uid 0
Aug 9 18:43:04 aris-knx pppd[4675]: Using interface ppp0
Aug 9 18:43:04 aris-knx pppd[4675]: Connect: ppp0 <-->
/dev/ttyp0
Aug 9 18:43:04 aris-knx pppd[4675]:MPPE 128-bit stateless
compression enabled
Aug 9 18:43:07 aris-knx pppd[4675]: local  IP address
192.168.200.10
Aug 9 18:43:07 aris-knx pppd[4675]: remote IP address
192.168.200.12
```

6.4 SOAL dan JAWABAN

Apa yang dimaksud dengan VPN (*Virtual Private Network*) ?

Jawab :

VPN merupakan suatu bentuk private internet yang melalui public network (internet), dengan menekankan pada keamanan data dan akses global melalui internet. Hubungan ini dibangun melalui suatu tunnel (terowongan) virtual antara 2 node.

Sebutkan komponen penting yang harus dimiliki VPN? Berikan penjelasan masing-masing syarat tersebut!

Jawab :

PPTP sudah memenuhi syarat menjadi salah satu komponen penting VPN yaitu enkapsulasi dan enkrips.

Enkripsi :

Enkripsi merupakan proses mengkodekan data sehingga maknanya menjadi tidak jelas/sulit dibaca. Enkripsi juga dapat diartikan mengubah sebuah kata atau kalimat menjadi sandi/kode-kode tertentu dengan menggunakan algoritma tertentu pula. Tujuan dari enkripsi adalah meningkatkan dan menjaga keamanan data baik yang disimpan maupun yang dikirim.

Autehentikasi :

Teknik authentikasi sangatlah penting untuk VPN. Dengan authentikasi kita bisa memastikan hanya dengan user dan password yang benarlah hak akses diberikan. Banyak cara melakukan teknik authentikasi mulai dari shared key, algoritma hash, Chalange Handshake Authentication Protocol (CHAP) atau bahkan menggunakan algoritma yang umum digunakan, RSA.

Sebutkan kelemahan-kelemahan dari VPN-Public?

Jawab :

Pada VPN-Public walaupun lebih murah, namun VPN dengan public network memiliki beberapa kelemahan-kelemahan yang perlu dipertimbangkan diantaranya adalah :

- Bandwidth yang lebih rendah dibandingkan dengan direct-dial-in ke server anda.
- Performance yang tidak konsisten karena sangat tergantung dari bandwidth yang tersedia oleh ISP.
- Tidak bisa melakukan akses tanpa koneksi ke internet.

Salah satu protokol yang biasa digunakan untuk mengimplementasikan VPN di internet adalah IPSec (IP-Security Protokol). Apa yang dimaksud dengan IPSec? Dan sebutkan protokol yang berjalan di IPSec?

Jawab :

IPSec adalah sekumpulan ekstensi dari keluarga protokol IP. IPSec menyediakan layanan kriptografi untuk keamanan transmisi data. Layanan ini termasuk *authenticity*, *integrity*, *access control*, *confidentiality*, dab *anti replay*.

Protokol yang berjalan dibelakang IPSec adalah:

1) AH (*Authentication header*), AH menyediakan layanan *authentication*, *integrity*, dan *replay protection*, namun tidak dengan *confidentiality*. AH juga melakukan pengamanan terhadap header IP.
2) ESP (*Encasulapted security payload*), ESP menyediakan layanan *authentication*, *integrity*, *replay protection*, d a n *confidentiality* terhadap data (ESP melakukan pengamanan terhadap segala sesuatu dalam paket data setelah header).

Sebutkan layanan-layanan yang ada pada IPSec? dan beri penjelasan dari masing-masing layanan!

Jawab :

Layanan-layanan yang disediakan pada IPSec dapat dideskripsikan sebagai berikut :

- ***Confidentiality***, untuk meyakinkan bahwa sulit untuk orang lain tetapi dapat dimengerti oleh penerima yang sah bahwa data telah dikirimkan. Contoh: Kita tidak ingin tahu seseorang dapat melihat password ketika login ke *remote* server.
- ***Integrity***, untuk menjamin bahwa data tidak berubah dalam perjalan menuju tujuan.
- ***Authenticity***, untuk menandai bahwa data yang dikirimkan memang berasal dari pengirim yang benar.
- ***Anti Replay***, untuk meyakinkan bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan

6.5 REFERENSI

[1] Budi Rahardjo, “Keamanan Sistem Informasi Berbasis Internet”, PT Insan Komunikasi/Indonesia- Bandung, 2001

[2] Kurniawan. Y,”Kriptografi Keamanan Internet dan Jaringan Komunikasi”, Informatika Bandung , April 2004

[3] Application Security Inc, “Encryption of Data At Rest –Database Encryption-“. White Paper dalam format PDF.

[4] Kornbrust, Alexander, “Circumvent Oracle’s Database Encryption and Reverse Engineering of Oracle Key Management Algorithms”. Red-Database Security. Dalam format PDF

[5] Fraase, Michael, “Crypthography”. Dari website Information Eclipse

[6] “Oracle Advanced Security" (dalam format PDF).
[7] “Transparent Data Encryption Technology”. Dari website SecurityHeaven Crypto Approach.
[8] Anonymous, Virtual Private Networks (VPNs) Tutorial, The International Engineering Consortium, http://www.iec.org
[9] Anonymous, Introduction to IPSec VPN’s, Cisco Systems, Inc., 1998
[10] Anonymous, Using IPSec : OpenBSD FAQ, http://www.openbsd.org/faq/faq13.html
[11] Ferguson, N., and Schneier, B., A Cryptographic Evaluation of IPSec, Counterpane Internet Security, 2000.
[12] Scandariato, R., and Risso, F., Advanced VPN Support on FreeBSD Systems, BSDCon Europe, Netherland, 2002.
[13] Stallings, W., Cryptography and Network Security, third edition, Prentice Hall, 2002.

BAB 7. QUALITY OF SERVICE

Aditya Pradana [1)] , Neneng Rahmawati [1)], Uswatun hasanah [1)]

[1)]Politeknik Elektronika Negeri Surabaya

ABSTRAK

Seiring dengan kemajuan teknologi informasi dan telekomunikasi, maka kebutuhan terhadap suatu jaringan akan semakin meningkat, terutama penggunaan IP pada jaringan khususnya Internet. Untuk mengukur kualitas koneksi jaringan TCP/IP internet atau intranet maka diperlukan QoS atau Quality Of service, dimana ada beberapa metode untuk mengukur kualitas koneksi seperti konsumsi bandwidth oleh user, ketersediaan koneksi, latency, losses dll.

Seperti kita ketahui bersama bahwa Qos sangat diperlukan untuk aplikasi real-time di dalam Internet. Suatu Qos dapat diuraikan sebagai satuan parameter yang menguraikan mutu (sebagai contoh, bandwith, pemakaian buffer, prioritas, pemakaian CPU, dan yang lainnya) pada suatu data. Dasar dari protokol IP adalah menyediakan upaya terbaik Qos atau *best-effort*.. Ada dua dasar utama Qos untuk Internet dan IP yang didasarkan pada jaringan, yaitu: Integrated Services dan Differentiated Services.

Diharapkan dengan adanya QoS maka suatu jaringan dapat terukur kualitas koneksi jaringan TCP/IP internet atau internet dengan proses pengaksesannya bisa lebih cepat dan lebih baik.

7.1 Definisi QoS

Quality of Service atau QoS digunakan untuk mengukur tingkat kualitas koneksi jaringan TCP/IP internet atau intranet. Ada beberapa metode untuk mengukur kualitas koneksi seperti konsumsi bandwidth oleh user, ketersediaan koneksi, latency, losses dll. Sekarang kita bahas istilah – istilah dalam Quality of Service :

Bandwidth

Bandwidth adalah kapasitas atau daya tampung kabel ethernet agar dapat dilewati trafik paket data dalam jumlah tertentu. Bandwidth juga bisa berarti jumlah konsumsi paket data per satuan waktu dinyatakan dengan satuan bit per second [bps]. Bandwidth internet di sediakan oleh provider internet dengan jumlah tertentu tergantung sewa pelanggan. Dengan QoS kita dapat mengatur agar user tidak menghabiskan bandwidth yang di sediakan oleh provider.

Latency

Jika kita mengirimkan data sebesar 3 Mbyte pada saat jaringan sepi waktunya 5 menit tetapi pada saat ramai 15 menit, hal ini di sebut latency. Latency pada saat jaringan sibuk berkisar 50 – 70 msec.

Losses

Losses adalah jumlah paket yang hilang saat pengiriman paket data ke tujuan, kualitas terbaik dari jaringan LAN / WAN memiliki jumlah losses paling kecil.

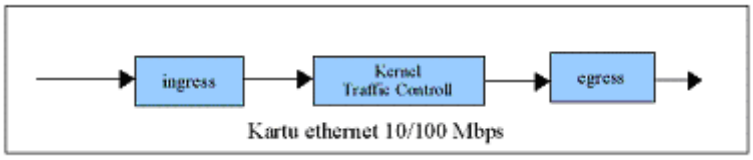
Availability

Availability berarti ketersediaan suatu layanan web, smtp, pop3 dan aplikasi pada saat jaringan LAN / WAN sibuk maupun tidak.

7.2 Traffic Control

7.2.1 Struktur kernel traffic control

Pada dasarnya kernel traffic controll memiliki 3 bagian, yang pertama perangkat ingress yaitu jika paket data diterima oleh kartu LAN maka paket tersebut akan diproses oleh ingress, biasanya ingress dipakai untuk mengendalikan traffic upload / uplink. Kemudian perangkat egress dipergunakan untuk mengendalikan paket data yang keluar dari kartu ethernet, sehingga trafik download oleh komputer klien dapat dibatasi sesuai konfigurasi.



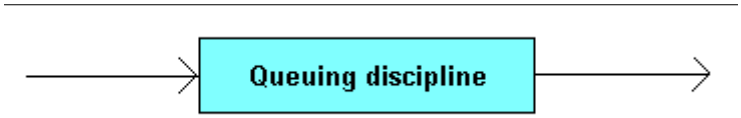
Gambar 7-93 Struktur kernel traffic control

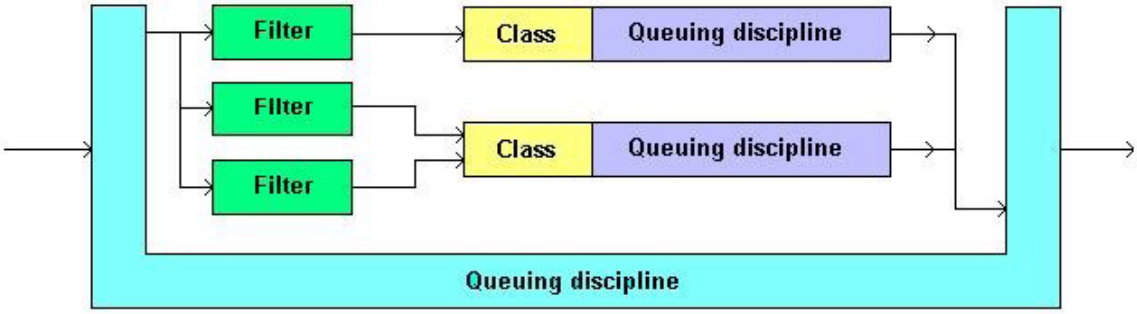
7.3 Cara pengontrolan Quality of service meliputi

7.3.1 Packet scheduler

Paket scheduler mengatur penyampaian arus paket yang berbeda didalam host dan router yang didasarkan atas kelas layanan, penggunaan antri manajemen dan berbagai penjadwalan algoritma. Paket scheduler harus memastikan bahwa penyerahan paket yang sesuai dengan parameter Qos untuk masing-masing arus. Suatu scheduler juga harus dapat menjaga ketertiban atau membentuk lalu lintas untuk dicocokkan dengan suatu tingkatan layanan tertentu. Paket scheduler harus dapat diimplementasikan dititik dimana paket dikirim.

Paket scheduler juga disebut dengan queing discipline. Queing disipline yaitu Antrian dalam setiap kartu ethernet yang dipergunakan untuk menyimpan antrian paket data, paket data masuk ataupun keluar melalui qdisc. Paket data yang memasuki qdisc akan dipisahkan oleh bagian filter untuk menentukan port / alamat ip yang akan di atur aliran trafiknya. Bagian class atau klasifikasi trafik akan dibahas pada bagian berikutnya, sedangkan qdisc yang berwarna ungu dipergunakan untuk mengeluarkan paket data ke kartu ethernet.



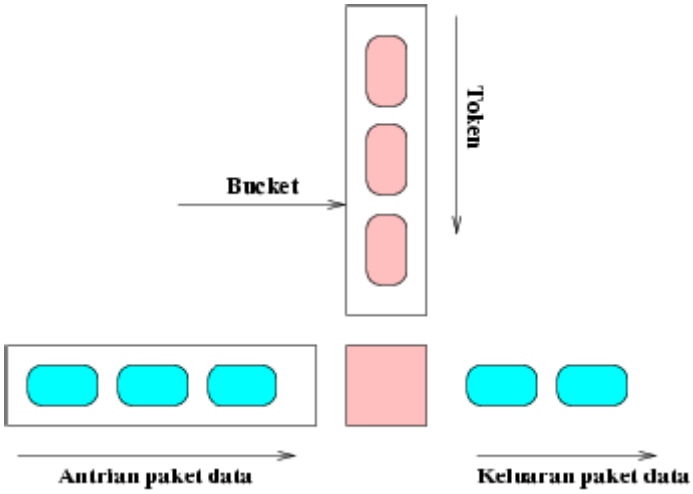


Gambar 7-94 Queuing Disipline

Setiap alat jaringan mempunyai suatu queuing discipline yang berhubungan dengan QoS. Fungsi utama pada queing disipline adalah mengendalikan bagaimana paket enqueued berada pada alat tertentu. Berbagai queuing disipline yang mendukung linux meliputi :

7.3.2 Token bucket Filter (TBF)

Token bucket filter (TBF) membatasi bandwidth dengan metode shape & drop, prinsip kerja menggunakan aliran token yang memasuki bucket dengan kecepatan (rate) konstan, jika token dalam bucket habis maka paket data akan di antri dan kelebihannya dibuang, setiap paket data yang dikeluarkan identik dengan token. Token dalam bucket akan lebih cepat habis jika aliran paket data melampaui kecepatan token memasukki bucket, jadi kita asumsikan bahwa trafik melebihi batas konfigurasi.



Gambar 7-95 Token bucket Filter

Parameter TBF

rate

batas bandwidth yang di set oleh administrator, jika aliran paket data melebihi nilai ini maka data akan di buang (drop) atau mengalami penundaan, bandwidth dipotong.

Limit / latency

limit merupakan jumlah byte yang dapat diantri sebelum token tersedia, sedangkan latency adalah lama waktu (dalam mili detik [msec]) paket dapat diantri.

Burst/buffer/maxburst

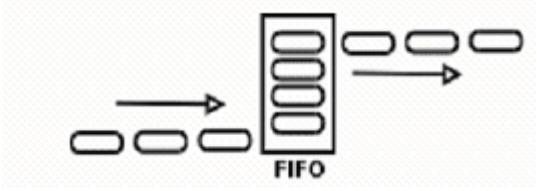
Kapasitas bucket dalam byte, paket data yang melebihi nilai ini akan dibuang atau mengalami penundaan.

Peakrate

Batas maksimum rate menangani lonjakan bandwitdh sesaat dengan syarat paket data tidak boleh melebihi kapasitas bucket dan mtu.

7.3.3 First In First Out (FIFO)

Teknik antrian FIFO mengacu pada FCFS (First Come First Server), paket data yang pertama datang diproses terlebih dahulu. Paket data yang keluar terlebih dahulu di masukan ke dalam antrian FIFO, kemudian dikeluarkan sesuai dengan urutan kedatangan. Teknik antrian FIFO sangat cocok untuk jaringan dengan bandwidth menengah 64kbps tetapi cukup menghabiskan sumber daya prosessor dan memori.



Gambar 7-96 Antrian FIFO

Gambar diatas menunjukkan kedatangan beberapa paket data yang berbeda waktu, paket pertama (1) dari flow 8 yang tiba lebih awal dikeluarkan ke port terlebih dahulu oleh antrian FIFO. Untuk men-set antrian kita memerlukan perintah “tc” dengan qdisc pfifo, parameter limit untuk menentukan batas maksimum antrian.

Pada metode FIFO jika trafik melebihi nilai set maka paket data akan dimasukkan ke antrian, paket data tidak mengalami pembuangan hanya tertunda beberapa saat. Metode FIFO cocok diterapkan pada koneksi internet dengan bandwidth menengah 64kbps, untuk menghindari bootle neck pada jaringan LAN. Paket data jika melebihi batas konfigurasi akan di masukkan ke dalam antrian dan pada saat jaringan LAN tidak sibuk maka paket data dalam antrian akan dikeluarkan.

7.3.4 RED (Random Early Detection)

Random Early Detection atau bisa disebut Random Early Drop biasanya dipergunakan untuk gateway / router backbone dengan tingkat trafik yang sangat tinggi. RED mengendalikan trafik jaringan sehingga terhindar dari kemacetan pada saat trafik tinggi berdasarkan pemantauan perubahan nilai antrian minimum dan maksimum. Jika isi antrian dibawah nilai minimum maka mode 'drop' tidak berlaku, saat antrian mulai terisi hingga melebihi nilai maksimum maka RED akan membuang (drop) paket data secara acak sehingga kemacetan pada jaringan dapat dihindari.

Parameter RED sebagai berikut:

min

Nilai rata – rata minimum antrian (queue)

max

Nilai rata – rata maksimum antrian, biasanya dua kali nilai minimum atau dengan rumus;

max = bandwidth [Bps] * latency [sec]

probability

Jumlah maksimum probabilitas penandaan paket data nilainya berkisar 0.0 sampai dengan 1.0.

limit

Batas paling atas antrian secara riil, jumlah paket data yang melewati nilai limit pasti dibuang. Nilai limit harus lebih besar daripada 'max' dan dinyatakan dengan persamaan.

limit = max + burst

burst

digunakan untuk menentukan kecepatan perhitungan nilai antrain mempengaruhi antrian riil (limit). Untuk praktek nilainya kita set dengan rumus;

burst = (min+min+max) / 3 * avpkt

avpkt

Nilai rata – rata paket data / trafik yang melintasi gateway RED, sebaiknya diisi 1000.

bandwidth

Lebar band (bandwidth) kartu ethernet.

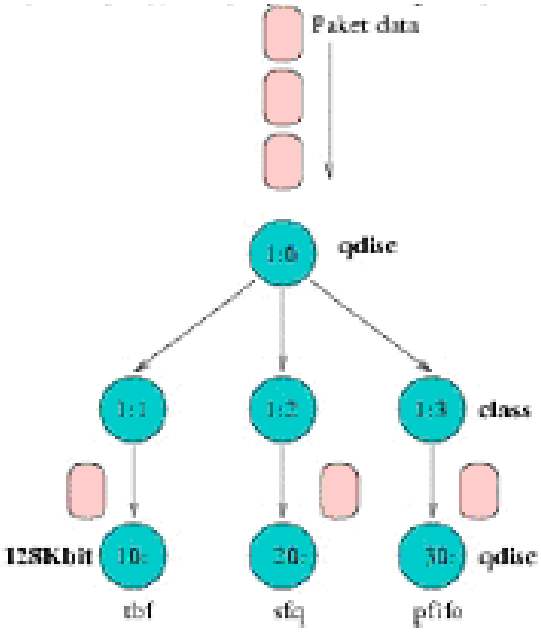
ecn

Explicit Congestion Notification memberikan fasilitas gateway RED untuk memberitahukan kepada klien jika terjadi kemacetan.

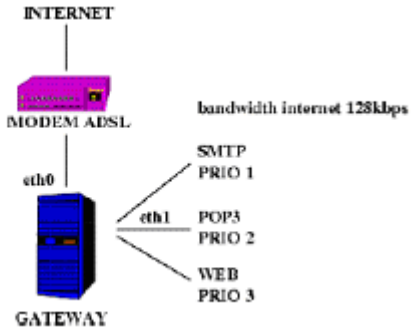
7.4 Paket Classifier

Paket classifier atau paket penggolongan mengidentifikasi paket dari suatu IP yang mengalir didalam host dan router yang akan menerima suatu tingkatan layanan tertentu. Untuk merealisasikan kontrol lalu lintas yang efektif, untuk paket-paket yang datang dipetakan oleh penggolongan ke dalam kelas spesifik. Semua paket yang digolongkan ke dalam kelas yang sama akan mendapatkan perlakuan yang sama dari paket scheduler. Pemilihan suatu kelas didasarkan atas alamat IP sumber dan nomor port didalam paket header atau suatu nomor tambahan untuk penggolongan yang harus ditambahkan untuk masing-masing paket. Sebagai contoh, semua video yang berasal dari video conference dengan beberapa sumber dapat digolongkan dalam satu kelas layanan. Tetapi ini juga mungkin hanya ada satu arus dalam suatu kelas layanan

Klasifikasi paket merupakan cara memberikan suatu kelas atau perbedaan pada setiap paket, hal ini dilakukan untuk mempermudah penanganan Puket oleh antrian. Klasifikasi berbeda dengan filtering yang berfungsi mengarahkan dan menyaring aliran paket data. Contoh pada gambar 5.1. dibawah ini menunjukkan paket data dibagi menjadi tiga kelas 1:1, 1:2 dan 1:3 dan tiap kelas tersebut ditangani oleh teknik antrian (qdisc) 10: (tbf), 20:(sfq) dan 30: (pfifo).



Gambar 7-97 Klasifikasi paket data



Gambar 7-98 klasifikasi prioritas

7.4.1 Class Based Queue (CBQ)

Teknik klasifikasi paket data yang paling terkenal adalah CBQ, mudah dikonfigurasi, memungkinkan sharing bandwidth antar kelas (class) dan memiliki fasilitas user interface. CBQ mengatur pemakaian bandwidth jaringan yang dialokasikan untuk tiap user, pemakaian bandwidth yang melebihi nilai set akan dipotong (shaping), cbq juga dapat diatur untuk sharing dan meminjam bandwidth antar class jika diperlukan.

parameter CBQ:

avpkt

Jumlah paket rata – rata saat pengiriman

bandwidth

lebar bandwidth kartu ethernet biasanya 10 – 100Mbit

rate

Kecepatan rata – rata paket data saat meninggalkan qdisc, ini parameter untuk men-set bandwidth.

cell

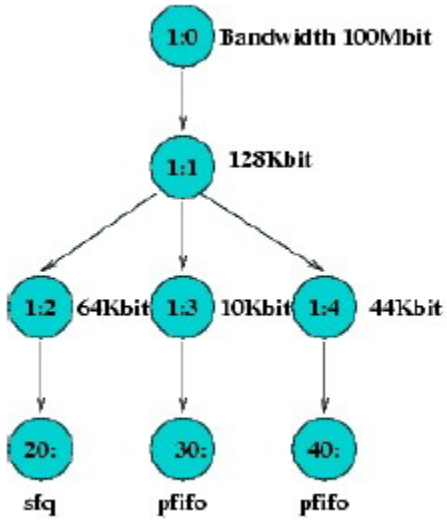
Peningkatan paket data yang dikeluarkan ke kartu ethernet berdasarkan jumlah byte, misalnya 800 ke 808 dengan nilai cell 8.

isolated / sharing

parameter isolated mengatur agar bandwidth tidak bisa dipinjam oleh klas (class) lain yang sama tingkat / sibling. Parameter sharing menunjukkan bandwidth kelas (class) bisa dipinjam oleh kelas lain.

bounded / borrow

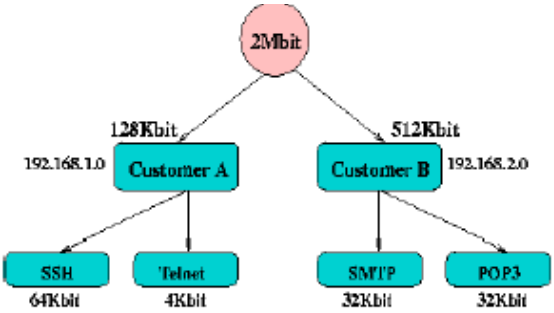
parameter borrow berarti kelas (class) dapat meminjam bandwidth dari klas lain, sedangkan bounded berarti sebaliknya.

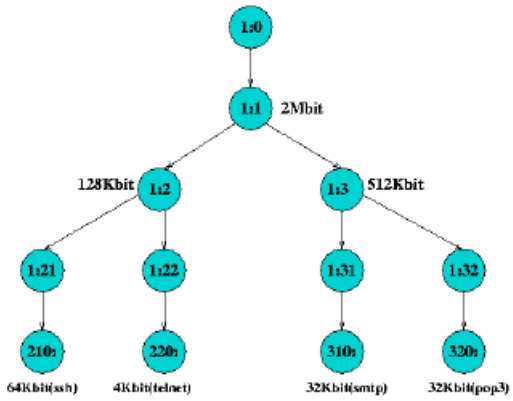


Gambar 7-99 Bounded / Borrow

7.4.2 Hierarchy Token Bucket (HTB)

Teknik antrian HTB mirip dengan CBQ hanya perbedaannya terletak pada opsi, HTB lebih sedikit opsi saat konfigurasi serta lebih presisi. Teknik antrian HTB memberikan kita fasilitas pembatasan trafik pada setiap level maupun klasifikasi, bandwidth yang tidak terpakai bisa digunakan oleh klasifikasi yang lebih rendah. Kita juga dapat melihat HTB seperti suatu struktur organisasi dimana pada setiap bagian memiliki wewenang dan mampu membantu bagian lain yang memerlukan, teknik antrian HTB sangat cocok diterapkan pada perusahaan dengan banyak struktur organisasi.





Gambar 7-100 antrian data pada HTB

7.4.3 Admission control

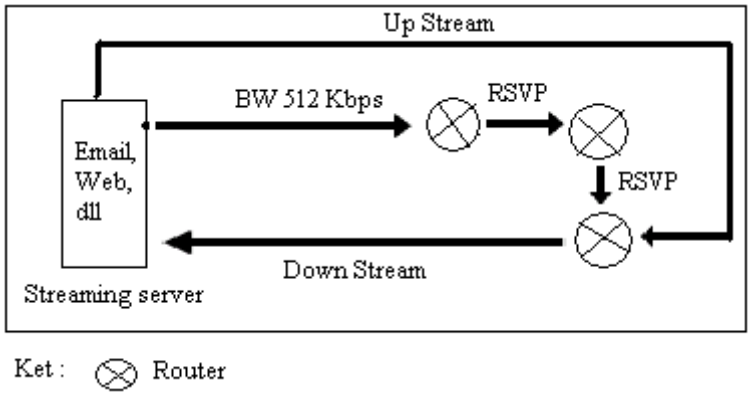
Admission control atau kontrol pintu masuk berisi algoritma keputusan bahwa suatu penggunaan router untuk menentukan jika ada routing yang cukup untuk menerima yang diminta Qos untuk arus yang baru. Jika tidak ada routing yang kosong, penerimaan arus yang baru akan berdampak pada jaminan yang lebih awal dan arus yang baru harus ditolak. Jika arus yang baru diterima, kejadian reservasi di dalam router akan menugaskan penggolong paket dan paket scheduler untuk memesan atau mencadangkan permintaan Qos untuk arus ini. Algoritma admission control harus konsisten dengan model layanan. Admission control kadang-kadang dikacaukan dengan kebijakan kendali, yang mana suatu packet-by-packet yang diproses oleh paket scheduler.

7.5 Sifat QoS

7.5.1 Integrated Service

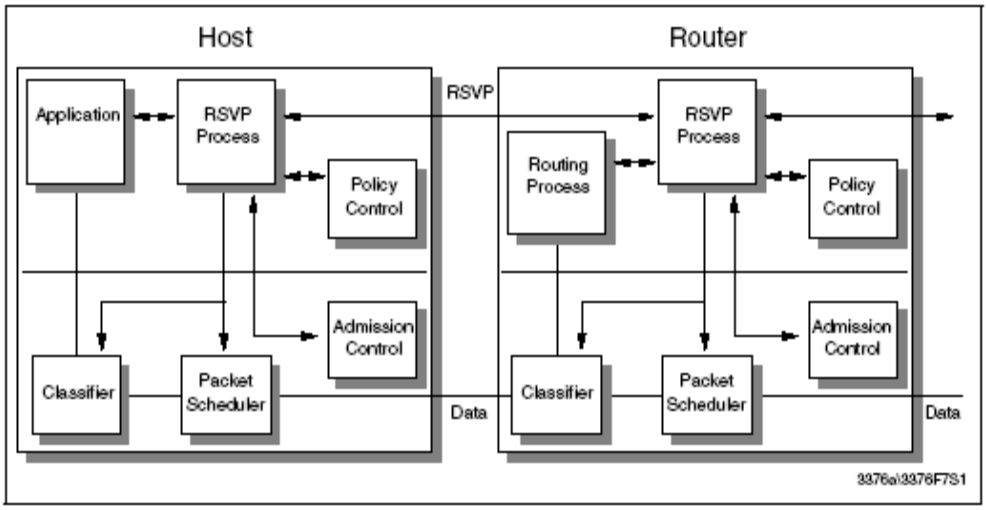
Model Integrated Services (IS) ditegaskan oleh kelompok kerja IEFT untuk menjadi dasar dari jaringan internet. Model arsitektur Internet ini meliputi upaya terbaik yang digunakan untuk melayani dan layanan real-time yang baru ini menyediakan fungsi untuk memesan/mencadangkan bandwith pada Internet dan jaringan. Integrated Services

dikembangkan untuk mengoptimalkan jaringan dan pemanfaatan sumber daya jaringan untuk yang baru aplikasi, seperti multimedia real-time, yang mana memerlukan jaminan Qos. Oleh karena, routing delay dan congestion losses, aplikasi real-time tidak bekerja baik pada Internet. Video conference, siaran video dan software audio conference membutuhkan jaminan bandwith untuk menyediakan audio dan video yang mutu dan kualitasnya bias diterima. Integrated Services membuatnya mungkin untuk membagi lalu lintas internet ke dalam standar upaya lalu lintas untuk aplikasi data dan penggunaan yang dijamin QoS.



Gambar 7-101 Pengontrolan pesanan data

Gambar dibawah ini menunjukkan operasi dari model Integtrated services yang berada didalam host dan router



Gambar 7-102 Model Integrated Services

Integrated Services menggunakan Resource Reservation Protocol (RSVP) untuk memberi sinyal menyangkut reservation atau pemesanan. Integrated Services berkomunikasi melalui RSVP untuk menciptakan dan memelihara jalannya data didalam endpoint host dan didalam router sepanjang alur dari suatu arus.

Seperti yang ditunjukkan pada gambar 1 diatas, aplikasi yang ingin mengirimkan paket data arus yang dipesan untuk berkomunikasi dengan reservasi RSVP. Protokol RSVP mencoba

untuk menyediakan suatu arus reservasi sesuai dengan yang diminta QoS, yang mana akan diterima jika aplikasi memenuhi pembatasan kebijakan dan router mampu menangani yang diminta QoS. RSVP memberitahu packet classifier atau paket penggolongan dan packet scheduler pada setiap titik node untuk memproses paket sesuai dengan arus yang ada. Jika aplikasi mengirim paket data kepada classifier (penggolong) ke dalam node yang pertama, yang mana telah memetakan arus ini ke dalam suatu kelas layanan yang spesifik sesuai dengan persetujuan yang diminta QoS, arus dikenali dengan alamat IP pengirim dan data akan ditransmisikan ke paket scheduler. Paket schedulerakan meneruskan paket, bergantung pada kelas layanan ke router yang berikutnya dan akhirnya paket data diterima oleh host penerima.

Karena RSVP merupakan suatu protokol yang simple, QoS reservation hanya dibuat untuk satu arah, dari titik pengirim sampai titik penerima yang ditentukan. Jika aplikasi di dalam contoh ingin membatalkan reservasi untuk mengalirkan data, aplikasi akan mengirimkan

pesan kepada reservasi sesuai dengan yang dipesan QoS didalam semua router di sepanjang alur. Spesifikasi dari integrated Service didefinisikan didalam RFC 1633.

7.5.2 Differentiated Services

Mekanisme jasa yang dibedakan tidak menggunakan pemberian isyarat per-flow, dan sebagai hasil, tidak mengkonsumsi status per-flow selama routing. Perbedaan level layanan dapat dialokasikan untuk layanan yang lainnya yang termasuk dalam satu group pada user, yang mana berarti bahwa semua lalu lintas dibagi bagikan ke dalam kelas atau kelompok dengan parameter QoS yang berbeda. Ini mengurangi biaya pemeliharaan bila dibandingkan dengan Integrated Services.

Konsep Differentiated Services(DS) sekarang ini dibawah pengembangan kelompok kerja IEFT. Spesifikasi DS digambarkan dalam beberapa draft internet dan belum tersedia dalam RFC. Bagian ini memberi suatu ikhtisar tentang gagasan dan dasar untuk menyediakan pembedaan layanan didalam Internet. Suatu komponen dari DS adalah Service Level Agreement (SLA). SLA adalah suatu kontrak jasa antara suatu pelanggan dan suatu penyedia layanan yang menetapkan detil dari penggolongan lalu lintas dan bersesuaian menyampaikan layanan yang diminta sesuai keinginan pelanggan.

7.5.3 Differentiated Services architecture

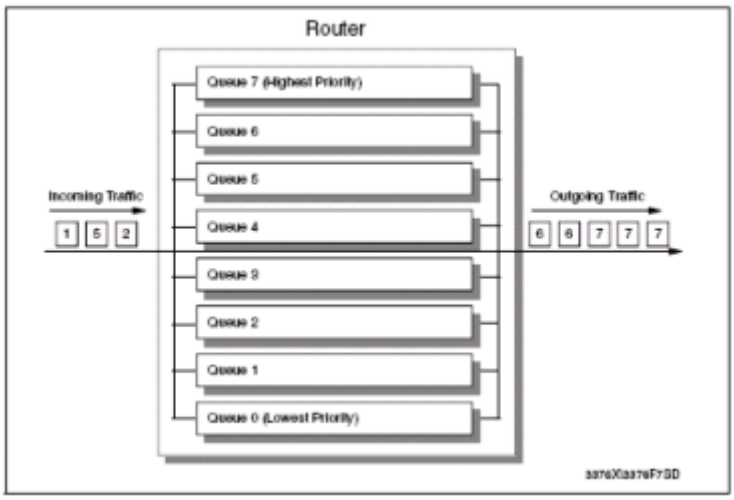
Differentiated Services architecture tidak seperti *Integrated Services*, jaminan QoS dibuat dengan *Differentiated Services* yang statis dan *stay long-term* di *router*. Hal ini bahwa aplikasi menggunakan DS tidak harus menyediakan reservasi QoS untuk paket data spesifik. Semua lalu lintas yang lewat jaringan *DS-capable* dapat menerima spesifik QoS. Paket data harus ditandai dengan *field* DS yang diinterpretasikan oleh *router* di jaringan.

1) Per-hop behavior (PHB)

Field DS menggunakan enam bit untuk menentukan *Differentiated Services Code Point* (DSCP). Kode titik ini akan digunakan oleh masing-masing node pada net untuk memilih

PHB. Dua bit *field currently unused* (CU) dipesan. Nilai dari bit CU diabaikan oleh *node differentiated services-compliant*, saat PHP digunakan untuk paket yang diterima.

Contoh ***DS routing***



Gambar 7-103 DS Routing

2) Organization of the DSCP
   - Ada beberapa pertimbangan IANA mengenai DSCP. *Codepoint space* untuk DSCP membedakan antara 64 nilai-nilai *codepoint*. Proposal akan membagi *space* ke dalam *tree pools*.
   - *Pool1* bisa digunakan untuk *standard actions*. *Pool* yang lain mungkin digunakan untuk pemakaian lokal bersifat eksperimental, dimana salah satu dari kedua *pool* dilengkapi untuk keperluan eksperimental lokal pada masa depan yang dekat.

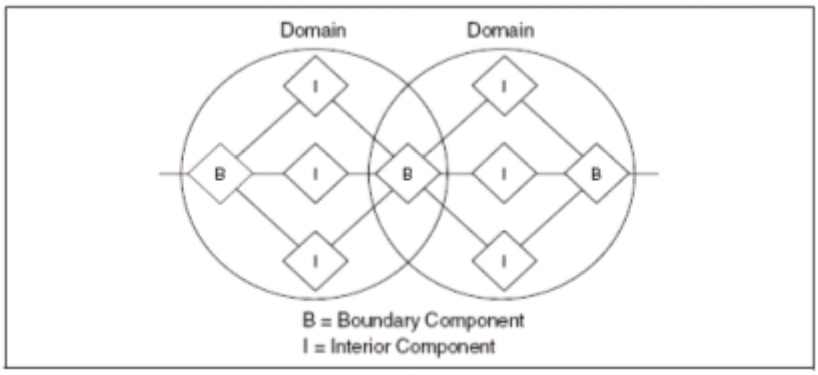
Table 7-2 DSCP pools

Pool	Codepoint space	Assignment
1	xxxxx0	standard action
2	xxxx11	experimental/local use
3	xxxx01	future exp./local use

3) Differentiated Services domains
   - Penyediaan jaminan QoS tidak diciptakan untuk spesifikasi koneksi *end-to-end,* tetapi untuk perumusan *Differentiated Services domains* yang baik.
   - Dapat merepresentasikan perbedaan daerah administratif atau *autonomus systems*, *different trust regions*, teknologi jaringan yang berbeda, seperti *cell* atau teknik *frame-based*, *host*, dan *router*.
   - Suatu daerah DS terdiri dari komponen batas yang digunakan untuk menghubungkan daerah DS yang berbeda satu sama lain dan komponen interior yang hanya digunakan didalam daerah tersebut.

     Suatu daerah DS secara normal terdiri dari satu atau lebih jaringan di bawah administrasi yang sama. Sebagai contoh, suatu perusahaan intranet atau suatu *Internet Service*

Provider (ISP). Administrasi dari DS daerah bertanggung jawab untuk memastikan bahwa sumber daya yang cukup dipesan dan menetapkan untuk mendukung SLAS yang ditawarkan oleh daerah tersebut. Administrator jaringan harus menggunakan teknik pengukuran untuk memonitor jika sumber daya jaringan didalam daerah DS adalah cukup untuk mencukupi semua hak permintaan QoS.



Gambar 7-104 Penggunaan komponen internal dan batas untuk dua daerah DS

4) DS boundary nodes

Semua paket data yang melewati satu daerah DS pada daerah yang lain harus lewat boundary nodes, yang mana bisa merupakan suatu *router*, suatu *host*, atau suatu *firewall*. Suatu DS *boundary nodes* menangani lalu lintas yang meninggalkan suatu daerah DS disebut suatu *boundary nodes* dan *boundary nodes* yang menangani lalu lintas yang memasuki suatu daerah DS disebut suatu *ingress boundary nodes*. Secara normal, DS *boundary nodes* bertindak baik sebagai *ingress node* dan *node*, tergantung pada arah trafik.

Komponen-komponen yang terdapat pada Lalu lintas penentu *(traffic conditioner)* :

- ***Classifier***

Classifier memilih paket berdasar pada *header* paketnya dan meneruskan paket yang memenuhi aturan classifier pengolahan lebih lanjut. DS model menetapkan dua jenis paket *classifier*:

1. *Multi-Field (MF) Classifier* dapat menggolongkan pada bidang DS seperti halnya pada IP lain, contoh, IP address and the port number, seperti RSVP.

2. Behavior Aggregate (BA) *Classifier*, hanya menggolongkan pada bit didalam bidang DS.

- ***Meter***

Traffic meters mengukur jika penyampaian paket itu terpilih oleh *classifier* yang sesuai dengan profil lalu lintas yang menguraikan QoS untuk SLA antara pelanggan dan penyedia jasa layanan. Suatu meter lewat status informasi ke fungsi pengkondisian yang lain untuk men-*trigger* tindakan tertentu untuk masing-masing paket, baik mengerjakan maupun tidak mematuhi yang diminta kebutuhan Qos

- ***Marker***

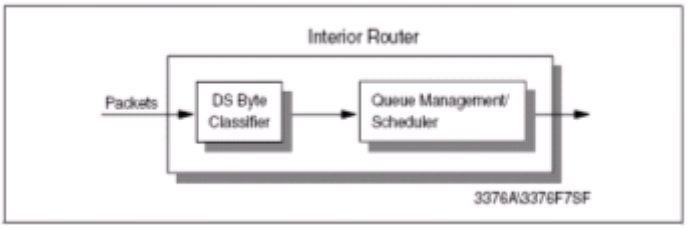
DS menetapkan DS *field* dari paket IP berikutnya untuk bit tertentu. PHB adalah yang ditetapkan dalam 6 bit yang pertama DS *field* sehingga paket-paket yang ditandai disampaikan di dalam daerah DS menurut SLA antara pelanggan dan *service provider*.

- ***Shaper/dropper***

  Paket *shapers* dan *droppers* menyebabkan konformasi pada beberapa properti lalu lintas yang dikonfigurasi, sebagai contoh, *token bucket filter*, seperti "*Service classes*" Mereka menggunakan metoda berbeda untuk membawa arus ke dalam pemenuhan dengan profil lalu lintas profil. *Shaper* menunda beberapa atau semua paket tersebut. *Dropper* pada umumnya mempunyai suatu *finite-size buffer*, dan paket tidak mungkin dibuang jika ada *space* bufffer cukup untuk memegang paket yang ditunda. Dropper membuang beberapa atau semua paket itu. Proses ini adalah mengetahui menjaga ketertiban arus itu. Suatu dropper dapat diterapkan sebagai kasus yang khusus dari *shaper* dengan pengaturan ukuran *shaper buffer* pada paket nol(*zero packets*).

5) DS interior components

   Komponen interior dalam daerah DS memilih cara penyampaian untuk paket berdasarkan DS *field*-nya.

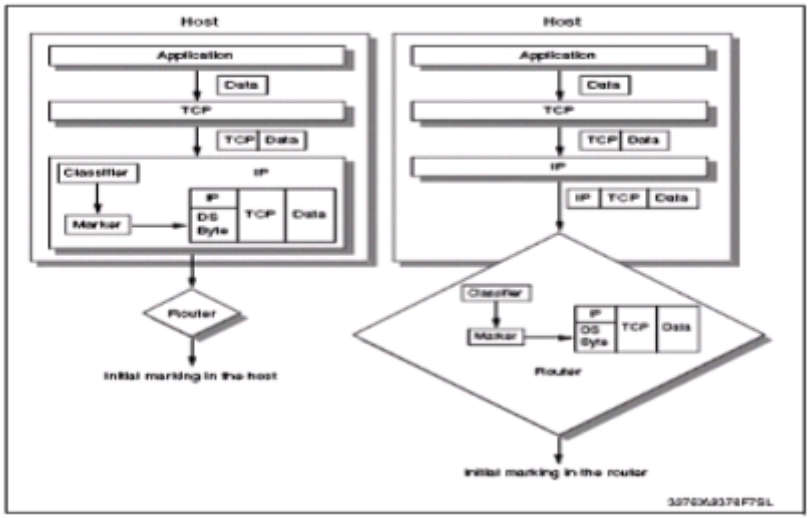


Gambar 7-105 DS interior

6) Source domains

   Sumber lalu lintas dan *node intermediate* di dalam suatu daerah sumber dapat menampikan klasifikasi lalu lintas dan fungsi pengkondisian. Lalu lintas yang dikirim dari suatu daerah sumber mungkin ditandai oleh sumber lalu lintas secara langsung atau oleh *node intermediate* sebelum meninggalkan daerah sumber.

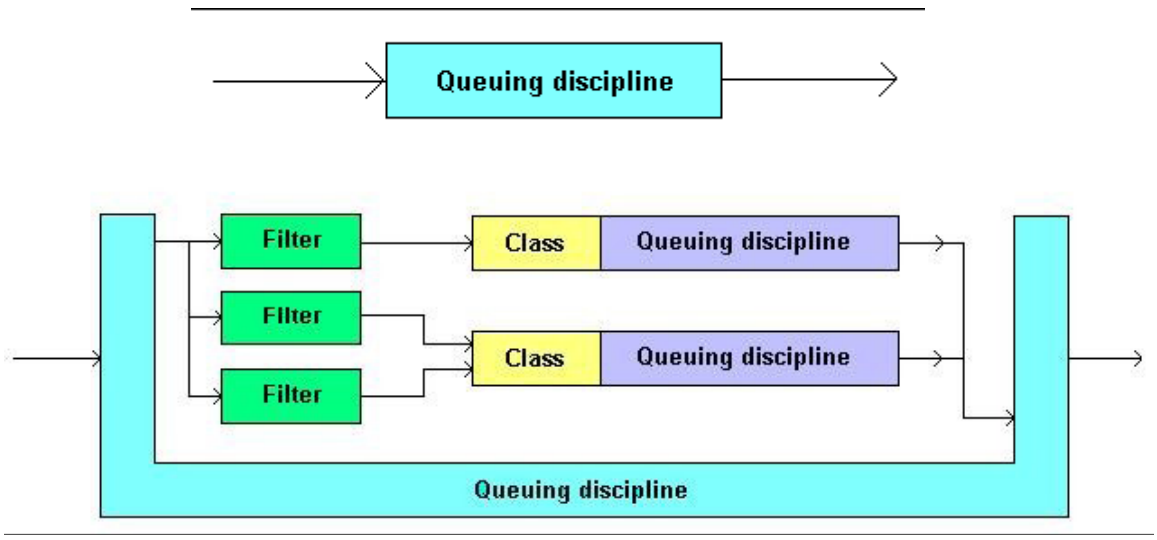
   PHB yang pertama yang menandai paket data tidak dilakukan oleh pengiriman aplikasi dirinya sendiri. Aplikasi tidak memesan ketersediaan dari Differentiated Services didalam suatu jaringan. Oleh karena itu, aplikasi menggunakan jaringan DS tidak ditulis ulang untuk mendukung DS. Ini adalah suatu perbedaan penting untuk *Integrated Services*, dimana kebanyakan aplikasi mendukung protokol RSVP secara langsung ketika beberapa perubahan kode diperlukan.



Gambar 7-106 Intial marking pada paket data

7.6 SOAL dan JAWABAN

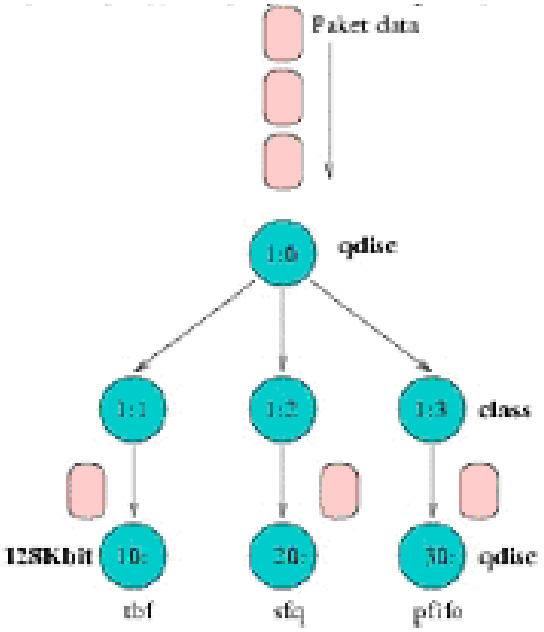
1. Mengapa QoS sangat diperlukan dalam jaringan internet ? Karena Qos dalam jaringan internet diperlukan untuk mengukur kualitas koneksi jaringan TCP/IP internet atau intranet.
2. Jelaskan dengan gambar bagaimana paket queing disipline dapat melewatkan antrian paket data ?



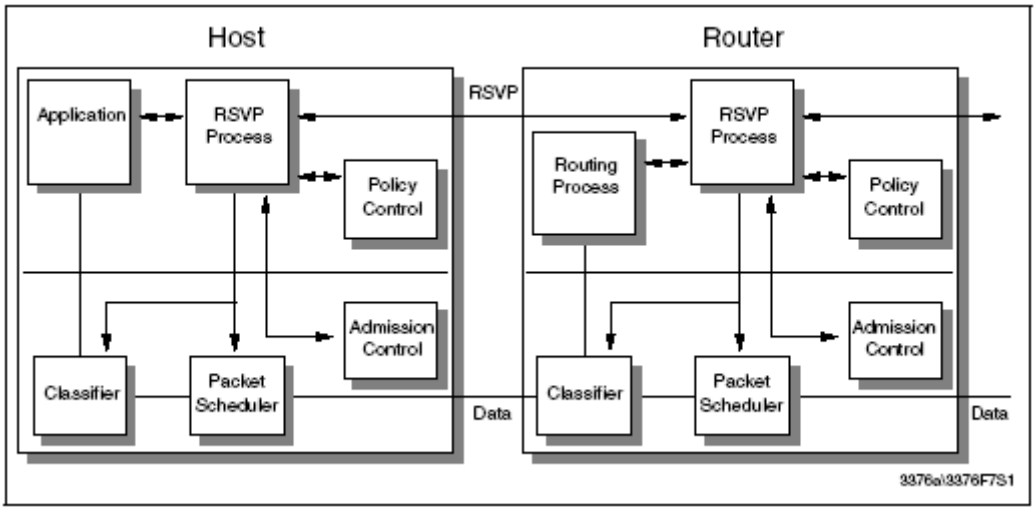
3. Jelaskan perbedaan dari sifat QoS differential servives dan integrated service?

   Pada integrated service model arsitektur Internet ini meliputi upaya terbaik yang digunakan untuk melayani dan layanan real-time baru yang menyediakan fungsi untuk memesan/mencadangkan bandwith pada Internet dan jaringan. Sedangkan untuk Diferential service yaitu level layanan dapat dialokasikan untuk layanan yang lainnya yang termasuk dalam satu group pada user, yang mana berarti bahwa semua lalu lintas dibagi bagikan ke dalam kelas atau kelompok dengan parameter QoS yang berbeda. Ini mengurangi biaya pemeliharaan bila dibandingkan dengan Integrated Services.

4. Jelaskan bagaimana paket classifier membagi penggolongan dari IP? Klasifikasi paket merupakan cara memberikan suatu kelas atau perbedaan pada setiap paket, hal ini dilakukan untuk mempermudah penanganan Puket oleh antrian. Klasifikasi berbeda dengan filtering yang berfungsi mengarahkan dan menyaring aliran paket data. Contoh pada gambar 5.1. dibawah ini menunjukkan paket data dibagi menjadi tiga kelas 1:1, 1:2 dan 1:3 dan tiap kelas tersebut ditangani oleh teknik antrian (qdisc) 10: (tbf), 20:(sfq) dan 30: (pfifo).



5. Mengapa integrated service menggunakan RSVP dalam pemesanan data? Integrated Services menggunakan Resource Reservation Protocol (RSVP) untuk memberi sinyal menyangkut reservation atau pemesanan. Integrated Services berkomunikasi melalui RSVP untuk menciptakan dan memelihara jalannya data didalam endpoint host dan didalam router sepanjang alur dari suatu arus.



7.7 REFERENSI

[1] Budi Santoso. ST, “Manajemen Bandwidth Intenet dan Intranet”, linux.multimedia@gmail.com

[2] Visolve Squid Team, “ QoS bandwidth Management”, Visolvo.com

[3] Adolfo Rodriguez, john gatrell, John Karas, Roland Peschke, “TCP/IP tutorial and Technical Overview, ibm.com/redbooks

BAB 8. LOAD BALANCING DAN SCALABILITY

Ginanjar Satriawan [1)] , Ninis Fahrina [1)], Gunawan Wicaksono [1)]

[1)]Politeknik Elektronika Negeri Surabaya

ABSTRAK

Perkembangan teknologi saat ini semakin maju dengan pesat. Dan seiring dengan perkembangan jaman maka manusia banyak membutuhkan informasi yang lebih,diantaranya manusia mencari informasi tersebut melalui internet(website).Dimana semakin banyaknya pengguna internet maka semakin banyak jalur yang terpakai yang menyebabkan para design merancang peralatan yang mampu menanpung begitu banyaknya para pengguna jasa internet.Dan dari rancangan tersebut didapatkan suatu hasil untuk mengatasi banyaknya pengguna jasa internet tersebut yaitu load balancing dan scalabilty. Load Balancing adalah proses distribusi beban terhadap sebuah servis yang ada pada sekumpulan server atau perangkat jaringan ketika ada permintaan dari pengguna.

8.1 Definisi

Load Balancing adalah proses distribusi beban terhadap sebuah servis yang ada pada sekumpulan server atau perangkat jaringan ketika ada permintaan dari pengguna. Maksudnya adalah ketika sebuah sever sedang diakses oleh para pengguna, maka server tersebut sebenarnya sedang dibebani kerena harus melakukan proses terhadap permintaan para penggunanya. Jika penggunanya banyak, maka proses yang dilakukan juga menjadi banyak.

Session-session komunikasi dibuka oleh server tersebut untuk memungkinkan para penggunanya menikmati servis dari server tersebut. Jika satu server saja yang dibebani, tentu server tersebut tidak akan dapat melayani banyak pengguna karena kemampuannya dalam melakukan *processing* ada batasnya. Batasan ini bisa berasal dari banyak hal, misalnya kemampuan *processing*-nya, *bandwidth* internetnya, dan banyak lagi.

Untuk itu, solusi yang paling ideal adalah dengan membagi-bagi beban yang datang tersebut ke beberapa server. Jadi, yang berugas melayani pengguna tidak hanya terpusat pada satu perangkat saja. Inilah yang disebut sistem load balancing.

Misalnya ketika Anda mengakses ke situs www.detik.com, maka *web server* yang berisi dokumen-dokumen berita, akan langsung melayani Anda. Server tersebut memberikan apa yang Anda minta dengan membuka komunikasi menggunakn servis HTTP port 80. Informasi halaman utama akan langsung dikirimkan ke PC melalui port 80 tersebut, sehingga Anda dapat melihatnya di halaman browser.

Ketika Anda meng-klik suatu *link* pada halaman web tersebut, permintaan Anda kemudian diproses kembali oleh server. Web server akan melayani permintaan Anda lagi dengan berbagai cara yang telah ditentukan oleh pengelolanya, apakah mengarahkan Anda kedalam folder tertentu, menjalankan *script-script* tertentu, mengirimkan gambar, memutar klip suara, dan banyak lagi. Pada saat ini, server detik.com sedang terbebani oleh permintaan Anda. Hingga

halaman atau layanan yang Anda minta terbuka, maka selesailah proses tersebut dan server kembali bebas dari beban.

Jika yang mengakses halaman web www.detik.com hanya Anda seorang, tentu sistem load balancing tidak diperlukan, karena sebuah server tentu masih sangat cukup untuk melayani permintaan Anda. Namun apa jadinya jika www.detik.com dibuka oleh hampir sebagian besar pengguna internet di Indonesia, setiap detik, dan setiap hari seperti keadaan saat ini. Mungkin sebuah server saja tidak akan sanggup melayani permintaan seberat itu. Permintaan akan terus datang dan proses juga akan terus-menerus dilakukan.

Umumnya para pengguna Internet tidak ingin kehilangan beberapa detik saja untuk dapat segera mengakses situs atau fasilitas Internet lain. Jika sudah terkoneksi ke Internet, setiap detik menjadi begitu berharga. Setiap detik waktu mereka menjadi penting karena mungkin saja dapat mengubah hidup mereka secara drastis.

Selain tingkat ketergantungan yang tinggi, mungkin biaya yang dikeluarkan untuk mendapatkan koneksi Internet juga salah satu faktor penyebabnya. Tentu mereka tidak ingin mengeluarkan biaya sia-sia hanya untuk menunggu menit demi menit sebuah halaman situs Internet banking terbuka misalnya. Intinya, para pengguna Internet sangat sensitif terhadap waktu tunggu dan kelancarannya jika sudah ber-Internet.

Kenyamanan dan kelancaran browsing situs-situs Internet memang didukung oleh banyak faktor. Bandwidth yang besar, server-server yang menggunakan teknologi processing terbaru dengan memory besar, media penyimpanan data yang cepat diakses, dan besar daya tampungnya, merupakan beberapa faktor yang mewakili itu. Melihat begitu krusialnya kelancaran ber-Internet, tentu para penyedia jasa Internet, penyedia web dan e-mail service, perusahaan e-commerce, dan penyedia fasilitas Internet lainnya, harus benar-benar memperhatikan kualitas koneksi dan reliabilitas server-server mereka.

8.2 Sistem Load balancing

Seperti telah dijelaskan di atas, sistem load balancing sebenarnya dapat dibuat dengan banyak cara. Pembuatannya tidak terikat oleh sebuah operating system saja, atau hanya dapat dibuat oleh sebuah perangkat saja. Namun secara garis besar cara pembuatan sistem load balancing terbagi menjadi tiga kategori besar yaitu :

1. DNS round robin
2. Integrated load balancing
3. Dedicated load balancing.

Ketiga jenis ini memiliki cara kerja yang unik dan berbeda satu sama lain, tetapi tetap menuju suatu hasil akhir yang sama, yaitu menciptakan sebuah sistem yang lebih menjamin kelangsungan hidup jaringan di belakangnya dan membuatnya lebih scalability.

Load adalah suatu hal yang sangat penting sekali pada sistem yang diharapkan dapat menangani beban simultan yang besar. Load balancing adalah suatu proses untuk memindahkan proses dari host yang memiliki beban kerja tinggi ke host yang memiliki beban kerja kecil. Ini bertujuan agar waktu rata-rata mengerjakan tugas akan rendah dan menaikkan utilitas prosesor.

8.2.1 DNS Round - robin

Metode yang paling sederhana untuk menciptakan sistem load balancing adalah dengan menggunakan metode DNS Round robin. Metode ini sebenarnya merupakan sebuah fitur dari aplikasi bernama BIND (Berkeley Internet Name Domain). Ini merupakan aplikasi open source khusus untuk membangun server DNS yang tampaknya sudah menjadi semacam standar yang digunakan di mana-mana. Sistem DNS round robin banyak mengandalkan teknik input penamaan yang teratur rapi dan dipadukan dengan sistem perputaran round robin.

Seperti Anda ketahui, DNS merupakan sebuah sistem penamaan terhadap perangkat-perangkat komputer. Penamaan ini dibuat berdasarkan alamat IP dari perangkat tersebut. Sebuah perangkat yang memiliki alamat IP dapat diberi nama dan dapat diakses menggunakan namanya saja jika Anda memiliki DNS server.

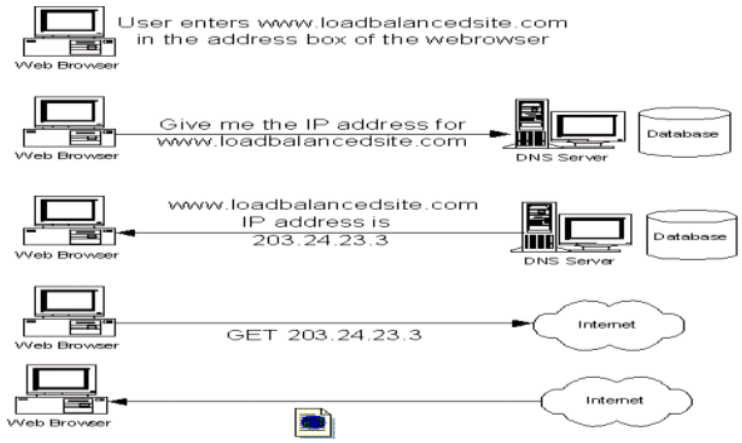
Sistem penamaan tersebut banyak sekali manfaatnya, misalnya hanya untuk sekadar lebih mudah diakses atau untuk diproses lebih lanjut. Anda tentu akan lebih mudah mengingat nama-nama yang spesifik daripada deretan-deretan angka alamat IP, bukan?

Dari sistem penamaan ini dapat dibuat sebuah sistem load balancing sederhana dan murah yang memanfaatkan sifat alami dari program BIND ini, yaitu sistem perputaran round robin.

Pada sebuah record DNS yang berisikan informasi penamaan, Anda dapat memasukkan beberapa nama lain (canonical) untuk diwakili oleh sebuah nama utama. Beberapa nama lain itu memiliki masing-masing record sendiri yang juga mewakili alamat-alamat IP dari perangkat jaringan. Jadi setelah proses input penamaan selesai, Anda akan mendapatkan sebuah nama utama yang mewakili beberapa nama-nama lain yang mewakili beberapa perangkat jaringan seperti server misalnya.

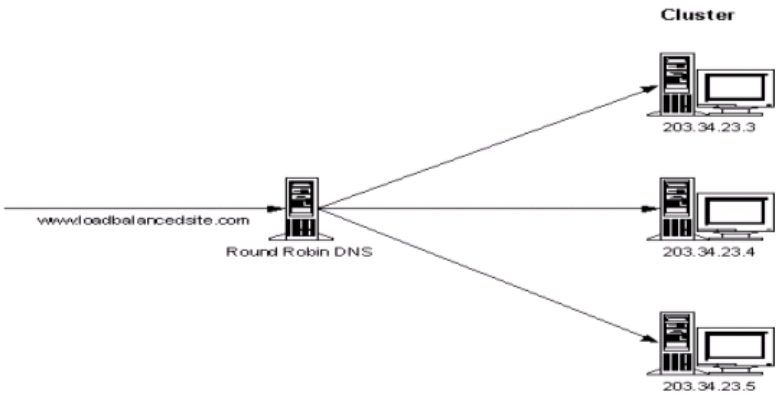
Di sinilah kuncinya, ketika ada yang mengakses nama utama tersebut, DNS server akan dihubungi oleh si pencari. Setelah menerima permintaan, DNS server akan mencari record dari nama utama tersebut. Ternyata di dalam record tersebut terdapat beberapa nama lain yang berhubungan dengan nama utama. Pada kondisi inilah, DNS server akan menjalankan sistem perputaran round robin untuk menggilir informasi nama-nama lain mana saja yang akan diberikan ke para pemintanya. Di sini, sistem load balancing sebenarnya sudah terjadi. Alamat IP dari server-server yang diwakili oleh nama lain tersebut akan diberikan kepada para peminta secara bergiliran sesuai dengan algoritma round robin. Ini menjadikan beban terbagi-bagi secara bergilir ke server-server lain dengan sendirinya.

Sebagai contoh, misalnya Anda memiliki empat buah server yang ingin digunakan untuk kepentingan situs perusahaan Anda. Nama domain utama Anda bernama myserver.mydomain .com. Empat buah server ini ingin Anda masukkan ke dalam sistem load balancing, sehingga pendistribusian bebannya tidak tersentralisasi. Dengan menggunakan sistem DNS round robin, yang perlu dilakukan adalah melakukan input penamaan keempat server Anda tersebut di DNS server secara teratur.



Gambar 8-107 DNS round robin

Dimisalkan masing-masing server diberi nama myserver0.mydomain.com sampai myserver3.mydomain.com. Input-lah semua alamat IP server-server Anda dan berikan nama record A (biasanya untuk mendeskripsikan sebuah host) pada saat pemberian nama ini. Setelah itu, buatlah nama utamanya dan input-lah semua nama server-server yang Anda dalam record CNAME.



Gambar 8-108 record CNAME

Konfigurasi ini akan menjadikan setiap kali pengguna mengakses nama utama yang dibuat, maka DNS server akan memberikan informasi IP ke pengguna secara bergilir dan berurut mulai dari IP myserver0. mydomain.com hingga myserver3. mydomain.com.

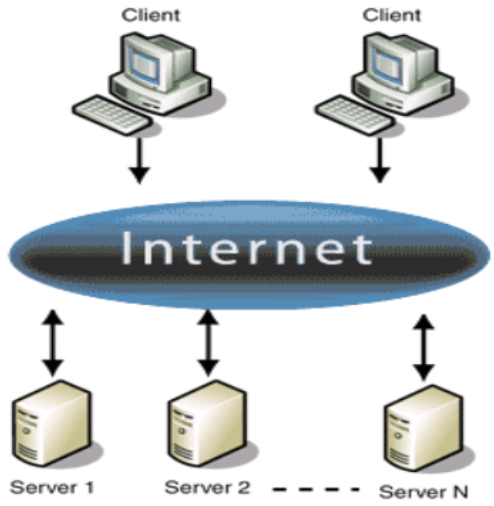
Sistem load balancing ini terbilang mudah dan sederhana untuk diimplementasikan, namun ada juga beberapa kelemahan yang cukup signifikan. Problem yang sering terjadi adalah ketika ada sebuah DNS server lain (misalkan DNS A) di Internet yang masih meng-cache hasil pencariannya yang pertama.

Jadi jika kali pertama server DNS A tersebut mendapatkan informasi IP dari myserver.mydomain.com adalah IP 1.1.1.2, maka DNS A tidak mengetahui alamat IP yang lain dari myserver. mydomain.com. Ini membuat para pengguna yang menggunakan server DNS ini

juga tidak dapat mengetahui sistem load balancing yang ada, sehingga load balancing tidak bekerja.

Kelemahan lainnya adalah ketika sebuah server di dalam sistem load balancing ini tidak dapat bekerja, maka sistem DNS tidak dapat mendeteksinya. Hal ini menyebabkan server yang tidak dapat bekerja tersebut malahan mendapatkan banyak request dari luar, meskipun tidak dapat bekerja. Kekacauan baru segera dimulai.

8.2.2 Integrated Load Balancing



Gambar 8-109 Integrated Load Balancing

Sesuai dengan namanya, Integrated load balancing biasanya merupakan solusi load balancing tambahan dari sebuah aplikasi atau operating system. Biasanya aplikasi atau operating system yang memiliki fitur ini adalah yang memiliki kemampuan beroperasi sebagai server.

Sistem load balancing-nya bukan merupakan fungsi utama. Oleh sebab itu, biasanya fitur, performa, dan kemampuannya cukup sederhana dan digunakan untuk sistem berskala kecil menengah. Fasilitasnya juga lebih banyak bersifat general saja, jarang yang spesifik. Meski demikian, fitur ini amat berguna jika digunakan pada jaringan yang tepat.

Salah satu Integrated load balancing ini dapat Anda temukan di Microsoft Windows 2000 Advance Server yang merupakan fitur tambahan. Pada operating system yang memiliki kemampuan jaringan yang hebat ini, Anda dapat mengonfigurasi sistem load balancing dengan cukup mudah. Selain itu, fitur-fitur yang diberikan untuk keperluan ini juga terbilang cukup lengkap. Fitur-fitur yang ada dalam teknologi load balancing pada Windows 2000 Advance Server dan juga Windows 2000 Datacenter Server adalah sebagai berikut:

- **Network Load Balancing (NLB)**

  Network load balancing merupakan fasilitas yang memungkinkan mesin Windows 2000 Advance Server melakukan load balancing terhadap aplikasi-aplikasi yang berjalan berdasarkan jaringan IP. Aplikasi yang berjalan diatas IP seperti HTTP/HTTPS, FTP, SMTP,dan banyak lagi dapat dengan mudah di-load balance dengan menggunakan fasilitas ini. Dengan menggunakan NLB, Anda dapat membuat satu grup cluster server

yang dilengkapi dengan sistem load balancing terhadap semua servis-servis TCP, UDP, dan GRE (Generic Routing Encapsulation). Untuk semua proses tersebut, dikenal sebuah istilah Virtual Server yang bertindak sebagai satu titik pusat pengaksesan server-server di bawahnya. Dengan adanya fasilitas ini, servis dan layanan yang dijalankan oleh server-server ini lebih terjamin kelancarannya. Sangat ideal digunakan untuk keperluan servis-servis front end, seperti web server agar masalah-masalah seperti bottleneck pada server dapat dikurangi.

- **Component Load Balancing (CLB)**

  Teknologi load balancing ini menyediakan sistem load balance terhadap komponen-komponen yang mendukung jalannya sebuah software atau aplikasi. Aplikasi atau software yang dapat di-load balance adalah yang komponen-komponennya menggunakan COM+.

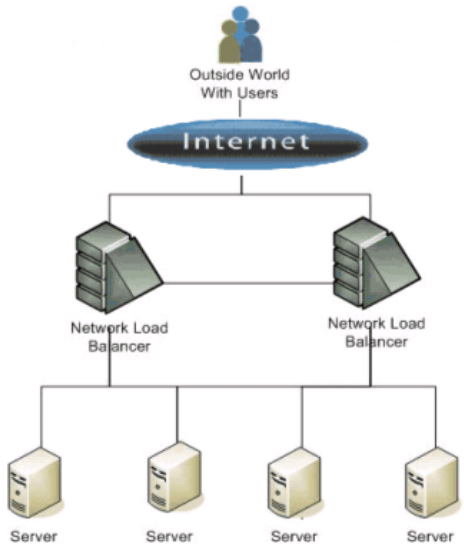
  Dengan melakukan load balancing terhadap komponen-komponen COM+ yang ada di beberapa server, maka jalannya sebuah aplikasi lebih terjamin dan lebih skalabel melayani para pengguna aplikasi.

- **Server Cluster.**

  Dengan menggunakan teknologi Server Cluster ini, Anda dapat membuat aplikasi dan data yang ada pada beberapa server terpisah dapat bergabung menjadi satu dalam sebuah konfigurasi cluster. Semua dapat saling terhubung untuk melayani penggunanya, sehingga integritas data tetap terjaga. Biasanya teknologi ini ideal untuk keperluan aplikasi-aplikasi back-end dan database. Sistem load balancing yang terintegrasi tidak hanya terdapat pada Windows 2000 saja. Jika Anda adalah pecinta open source yang menggunakan Apache sebagai web server Anda, module Backhand merupakan modul khusus untuk menambah kemampuan server Anda agar dapat di-cluster.

  Untuk membuat sistem load balancing yang lebih skalabel di Linux, Linux Virtual Server (LVS) merupakan salah satu aplikasi yang dapat Anda gunakan. LVS sudah merupakan semacam standar untuk membangun sistem load balancing di dunia open source. Metode dan teknologinya juga bervariasi dan tidak kalah hebatnya dengan apa yang dimiliki oleh Windows 2000. Di samping kehebatan dan kesederhanaannya, sistem load balancing terintegrasi ini memiliki beberapa kekurangan. Masing-masing fitur tambahan ini tidak dapat digunakan untuk melayani server-server atau perangkat yang berbeda platform dengannya. Misalnya, fitur load balancing dari Microsoft tidak bisa digunakan oleh Apache web server atau sebaliknya modul Apache tidak dapat digunakan oleh Microsoft IIS. Atau misalnya solusi dari IBM Websphere untuk membuat server farm, tidak dapat digunakan oleh sistem yang berbeda platform.

8.2.3 Dedicated Load balancing



Gambar 8-110 Dedicated Load balancing

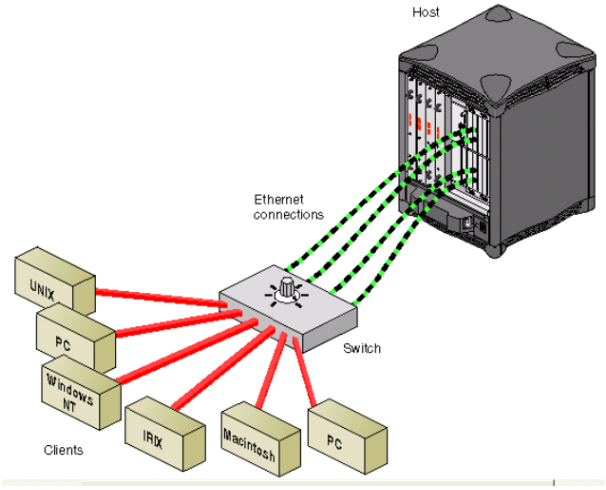
Metode load balancing yang satu ini diklaim sebagai sistem load balancing yang sesungguhnya karena kerja dan prosesnya secara total diperuntukan bagi proses load balancing terhadap server atau jaringan di bawahnya. Secara umum, metode ini masih dibagi lagi menjadi tiga jenis:

1. Load Balancing dengan hardware atau switch

   Sistem load balancing jenis ini diciptakan dengan menggunakan bantuan sebuah chip yang dikhususkan untuk itu. Biasanya chip khusus tersebut sering disebut dengan istilah ASICS, yang biasanya berwujud sebuah microprocessor khusus yang hanya memproses algoritma dan perhitungan spesifik. Dengan adanya ASICS ini, performa load balancing tidak perlu diragukan lagi kehebatannya karena memang hanya perhitungan dan logika load balancing saja yang dioptimisasi di dalamnya.

   Load balancing jenis ini umumnya berwujud sebuah switch. Dalam praktiknya, sering kali perangkat jenis ini membutuhkan keahlian khusus untuk digunakan karena interface-nya yang kurang user friendly. Selain itu, tingkat fleksibilitas perangkat ini juga rendah karena sebagian besar intelejensinya sudah tertanam di dalam hardware, sehingga penambahan fitur dan fasilitas-fasilitas lain menjadi lebih sulit dilakukan.

2. Load Balancing dengan software



Gambar 8-111 Load Balancing dengan software

Keuntungan yang paling menonjol dari solusi load balancing menggunakan software adalah tingkat kemudahan pengoperasiannya yang sudah lebih user friendly dibandingkan jika Anda mengonfigurasi switch load balancing. Keuntungan lainnya, jika ada fitur tambahan atau ada versi upgrade terbaru, Anda tidak perlu mengganti keseluruhan perangkat load balancing ini.

Namun karena proses logikanya berada di dalam sebuah software, maka tentu untuk menggunakannya dibutuhkan sebuah platform sebagai tempat bekerjanya. Perangkat komputer dengan spesifikasi tertentu pasti dibutuhkan untuk ini.

Performa dan kehebatannya melakukan proses load balancing juga akan dipengaruhi oleh perangkat komputer yang digunakan, tidak bisa hanya mengandalkan kemapuan software yang hebat saja. Kartu jaringan yang digunakan, besarnya RAM pada perangkat, media penyimpanan yang besar dan cepat, dan pernak-pernik lainnya tentu juga dapat mempengaruhi kinerja dari software ini. Karena dari isu inilah, maka performa dari keseluruhan sistem load balancing ini lebih sulit diperkirakan.

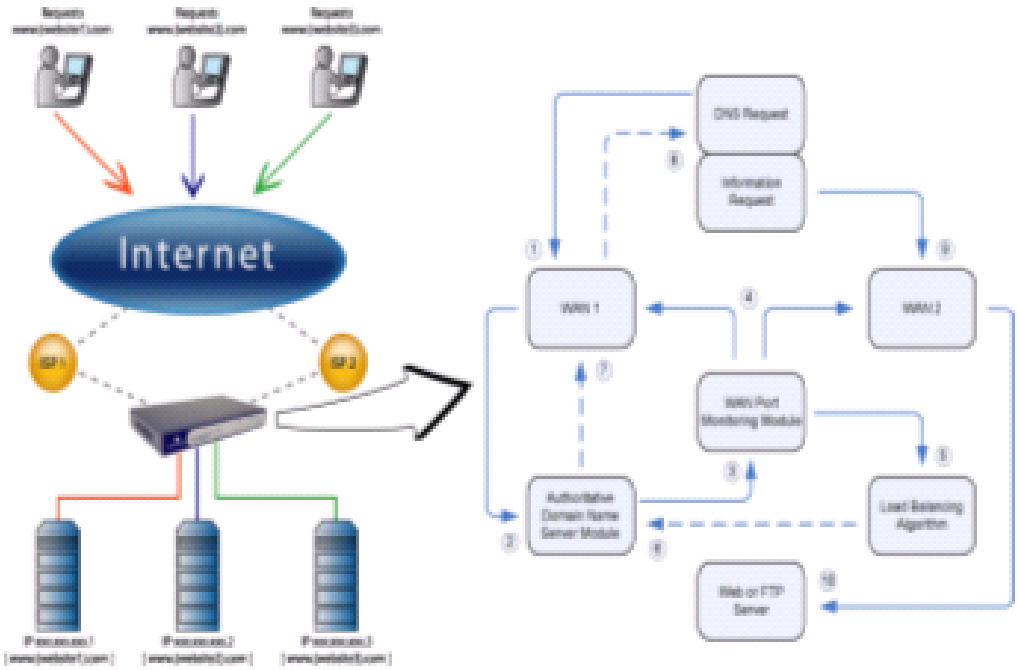
3. Load balancing dengan perangkat perpaduan hardware dan software

Solusi membuat sistem dedicated load balancing adalah dengan memadukan kedua jenis sistem load balancing di atas, yaitu memadukan software load balancing dengan perangkat yang dibuat khusus untuk melayaninya. Performa dari hardware yang khusus yang sengaja dioptimisasi untuk mendukung software load balancing yang user friendly dan fleksibel, menjadikan perangkat load balancing jenis ini lebih banyak disukai oleh pengguna saat ini. Perangkat jenis ini sering disebut dengan istilah load balancing black box.

Hardware yang dioptimisasi dan diisi dengan platform berbasis Linux atau BSD yang dioptimisasi adalah konfigurasi yang biasanya digunakan untuk menjalankan software utama load balancing. Dari konfigurasi ini, banyak sekali manfaat yang bisa didapatkan oleh pengguna maupun produsennya. Fleksibilitas yang luar biasa bisa didapatkan mulai dari menggunakan hardware yang selalu up-to-date sampai dengan operating system dengan patch terbaru.

Dengan demikian, waktu guna dari perangkat ini dapat lebih panjang daripada sebuah switch khusus yang tidak fleksibel. Solusi ini tentunya jauh lebih murah dibandingkan dengan solusi hardware khusus, atau bahkan dari solusi software saja.Bagian penting dari suatu strategi dalam load balancing adalah migration policy, yang menentukan kapan suatu migrasi terjadi dan proses mana yang dimigrasikan.

8.3 Cara Kerja LOAD BALANCING



Gambar 8-112 Rangkaian Pada Load Balancing

Langkah1

Sebuah domain name request yang dikirim dari remote web browser masuk ke gateway.

Request tersebut dicek oleh algoritma load balancing yang berdasar gateway current load statistic untuk menentukan port wan mana yang digunakan.

Langkah 2

Balasan dikirim ke remote web browser. Gatewaynya akan mengarahkan browser session ke WAN port yang memiliki traffic paling sedikit.

Langkah 3

Remote web browser ini kemudian menghubungkan ke IP address yang ditentukan memiliki WAN port yang telah tersedia.

8.3.1 Pada Load Balancer

1. web browser membuat sebuah request. Request ini dikirim oleh WAN 1.
2. domain name request ditransfer proses melalui DNS authotirative module.

3. DNS modul kemudian memerintahkan WAN port monitoring module untuk memberikan IP address dari request yang diminta.
4. WAN port monitoring modul akan mengecek traffic beban pada WAN 1 dan WAN 2.
5. Algoritma load balancing akan diterap pada request. Algoritma tsb. Akan menjaga gateway user preference dan menyeting load share dan type load balance.
6. algoritma load balancing menetukan bahwa
7. WAN 2 memiliki traffic yang paling sedikit.
8. Kemudian memerintah DNS module untuk mengunakan WAN 2.
9. Jawaban dari gateway kemudian dikirim balik melalui WAN 1 ke sumber DNS request.
10. Web browser menerima jawaban dari gateway dan diteruskan ke domain name yang merespon IP address tsb.
11. web browser menerima jawaban dari gateway dan diteruskan ke domain name yang merespon IP address, Web browser akan retrive infomasi yang direquest.
12. Informasi request kemudian diteruskan melalui wan 2.
13. request informasi dari web browser sekarang dapat diakses melalui web atau lokasi FTP server lokasi dibelakang gateway.

8.3.2 Proses migrasi

Terdapat dua bentuk proses migrasi pada load balancing:

- **Remote execution** (juga disebut non-preemptive migration). Pada strategi ini suatu proses baru (bisa secara otomatis) dieksekusi pada host remote.
- **Pre-emptive migration**, pada strategi ini proses akan dihentikan dipindahkan ke node lain dan diteruskan.

Load Balancing dapat dilakukan secara eksplisit oleh user ataupun secara implisit oleh sistem. Migrasi secara implisit dapat dilakukan dengan memanfaatkan informasi prioritas atau pun tidak. Sudah barang tentu, setiap pemindahan proses akan menimbulkan suatu overhead. Jadi bagaimana granularitas migrasi dari proses versus overhead dari proses migrasi harus juga dipertimbangkan.

Pada prinsipnya metoda load balancing yang digunakan haruslah memenuhi beberapa kriteria :

- **Overhead yang rendah** untuk pengukuran, sehingga pengukuran dapat dilakukan sesering mungkin untuk mengetahui kondisi sistem paling kini (up to date).
- **Memiliki kemampuan merepresentasikan beban** dan ketersediaan sumber daya komputasi dari sistem.
- **Pengukuran dan pengaturan yang tak saling bergantung**

  Dalam mengimplementasikan suatu strategi load baancing dapat dibedakan menjadi beberapa variasi, antara lain :
- **Lokal atau global**.

Pada pejadualan lokal, penjadwalan dilakukan oleh tiap node lokal, juga termasuk penentuan time slice pada prosesor tunggal. Sedangkan pada penjadwalan global, penjadwalan dan penentuan di manakah proses tersebut akan dijalankan, dilakukan oleh suatu titik koordinasi pusat.

- **Statis atau dinamis**.

  Pada model statis diasumsikan semua informasi yang digunakan untuk meletakkan proses telah tersedia ketika program hendak dijalankan. Pada model dinamis penentuan ini dapat berubah ketika sistem telah berjalan. Dikenal juga dengan istilah pengaturan yang adaptif dan dynamic assignment untuk model dinamis, dan non adaptif dan one time assingment untuk model statis.

- **Optimal atau suboptimal**.

  Pada model optimal penentuan strategi berdasarkan pertimbangan nilai optimal seluruh sistem.

- **Aproksimasi vs heuristik**.

  Pada model pertama menggunakan pendekatan model aproksimasi matematika seperti enumerative, teori graf, program matematika, teori antrean. Sedang model ke dua menggunakan pendekatan seperti nueral network, genetic algorithm. Di samping itu dalam menggunakan model matematika dapat dipilih model deterministik ataupun probabilistik.

- **Terdistribusi atau sentralisasi,**

  Artinya pihak mana yang bertanggung jawab terhadap pengambilan keputusan, apakah ada suatu sistem sentral yang melakukan keputusan migrasi, atau tersebar pada sistem yang terdistribusi.

- **Kooperatif atau non kooperatif**.

  Pada model non kooperatif setiap prosesor mengambil keputusan tanpa bergantung pada prosesor lainnya.

8.4 Algoritma LOAD BALANCING

Dalam sistem load balancing, proses pembagian bebannya memiliki teknik dan algoritma tersrndiri. Pada perangkat load balancing yang kompleks biasanya disediakan bermacam-macam algoritma pembagian beban ini. Tujuannya adalah untuk menyesuaikan pembagian beban dengan karakteristik dari server-server yang ada di belakangnya.

Secara umum, algoritma-algoritma pembagian beban yang banyak di gunakan saat ini adalah:

- ***Round Robin***

Algoritma Round Robin merupakan algoritma yang paling sederhana dan banyak digunakan oleh perangkat load balancing. Algoritma ini membagi beban secara bergiliran dan berurutan dari satu server ke server lain sehingga membentuk putaran.

- ***Ratio***

Ratio (rasio) sebenarnya merupakan sebuah parameter yang diberikan untuk masing-masing server yang akan di masukkan kedalam sistem load balancing. Dari parameter Ratio ini, akan dilakukan pembagian beban terhadap server-server yang diberi rasio. Server dengan rasio

terbesar diberi beban besar, begitu juga dengan server dengan rasio kecil akan lebih sedikit diberi beban.

- ***Fastest***

Algoritma yang satu ini melakukan pembagian beban dengan mengutamakan server-server yang memiliki respon yang paling cepat. Server di dalam jaringan yang memiliki respon paling cepat merupakan server yang kan mengambil beban pada saat permintaan masuk.

- ***Least Connection***

Algoritma Least connection akan melakukan pembagian beban berdasarkan banyaknya koneksi yang sedang dilayani oleh sebuah server. Server dengan pelayanan koneksi yang paling sedikit akan diberikan beban yang berikutnya akan masuk.

8.5 Keuntungan LOAD BALANCING

Ketika server atau jaringan Anda diakses oleh banyak pengguna, maka disinilah keuntungan load balancing yang paling dirasakan. Atau ketika sebuah aplikasi yang sangat penting yang ada di sebuah server, tiba-tiba tidak bisa diakses karena server-nya mengalami gangguan, maka dengan adanya load balancing bisa dialihkan ke server lain.

Secara garis besar, keuntungan dari penerapan load balancing adalah :

- ***Menjamin reliabilitas servis.***

Reliabilitas sistem artinya tingkat kepercayaan terhadap sebuah sistem untuk dapat terus melayani pengguna dengan sebaik-baiknya. Reliabilitas yang terjamin artinya tingkat kepercayaan yang selalu terjaga agar para penggunanya dapt menggunakan servis tersebut dan melakukan pekerjaannya dengan lancar. Hal ini amat penting bagi situs-situs komersial.

- ***Scalability dan avability.***

Satu buah server yang digunakan untuk melayani beribu-ribu pengguna, tentunya tidak mungkin dapat menghasilkan pelayanan yang baik. Meskipun telah menggunakan sebuah server dengan teknologi tercanggih sekalipun, tetap saja bisa kewalahan melayani penggunanya. Selain itu, satu buah server artinya satu buah titik masalah. Jika tiba-tiba server tersebut mati, masalah pasti akan terjadi terhadap situs atau servis di dalamnya. Namun dengan menggunakan sistem load balancing, server yang bekerja mendukung sebuah situs atau servis dapat lebih dari satu buah. Artinya jika ternyata satu buah server kawalahan melayani pengguna, Anda dapat menambah satu buah demi satu buah untuk mendukung kelancaran situs Anda. Tidak perlu server yang paling canggih untuk mengatasi masalah tersebut.

Selain itu juga titik masalah menjadi terpecah. Jika ada sebuah server bermasalah, maka masih ada dukungan dari yang lain. Situs atau servis yang Anda jalankan belum tentu bermasalah ketika sebuah server mengalami masalah.

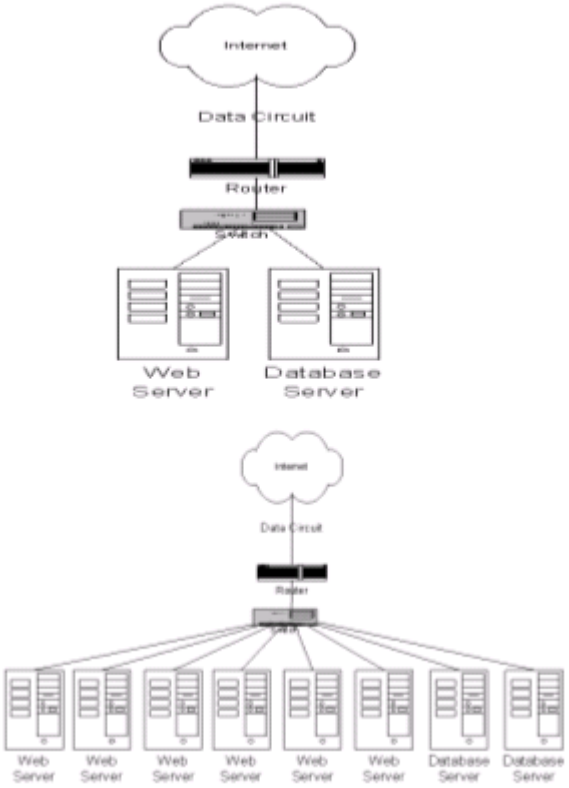
- **Improved scalabilitas (peningkatan skalabilitas).**

Level load-balanced Scalable memungkinkan sistem untuk memelihara performance yang bisa diterima tingkatkan avability.

- **Higher availability**.

Load-balanced memungkinkan kita untuk mengambil suatu maintenance server offline tanpa kehilangan aplikasi yang ada.

8.6 Scaling yang ada pada jaringan :



Gambar 8-113Scaling pada jaringan

8.7 Dua pendekatan Scaling Servers:

8.7.1 Multiple smaller servers

a. Penambahan server untuk skalabilitas
b. Paling umum dilakukan dengan web servers

8.7.2 Sedikit server lebih besar untuk penambahan internal resources

a. penambahan processors, memory, and disk space
b. Paling umum dilakukan dengan database servers

8.8 Dimana kita menggunakan Scalability ?

α. Pada jaringan
β. pada individual server
χ. Meyakinkan kapasitas suatu jaringan sebelum scaling dengan menambahkan server

8.9 Pendekatan pada Scalability :

8.9.1 Applikasi Service Providers (sites) dikembangkan oleh

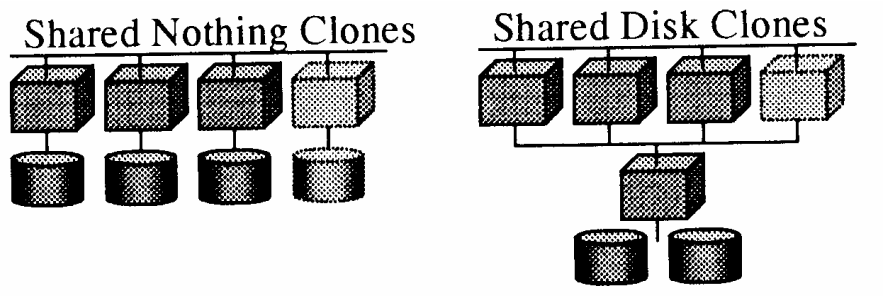
1. scale up: menggantikan server dengan server yang lebih besar
2. scale out: penambahan extra servers

8.9.2 Pendekatan

8.9.2.1 Farming

1. Farm – mengumpulkan semua server, aplikasi, dan data pada site khusus.
2. Farms mempunyai service khusus (misalnya : directory, security, http, mail, database dll)

8.9.2.2 Cloning



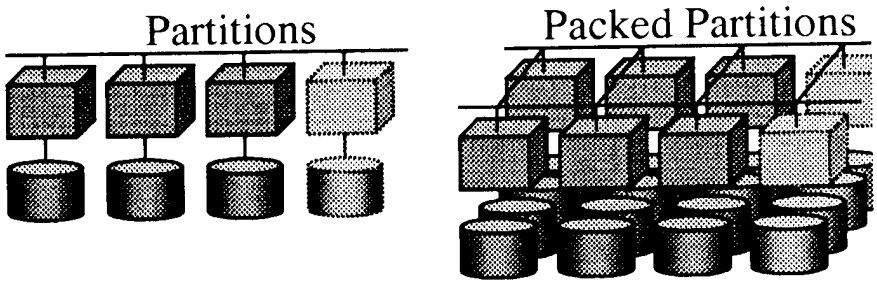
Gambar 8-114 Cloning

a. Suatu service yang dapat me-cloning pada beberapa replika nodes, dimana setiap node mempunyai software dan data yang sama.
b. Cloning menawarkan scalability and availability.
    1. Jika salah satu overloaded, sistem load-balancing dapat digunakan untuk mengalokasikan kerja diantara duplikat tsb.
    2. Jika salah satu gagal, yang lain akan meneruskan layanan.

8.9.2.3 RACS (Reliable Array of Cloned Services)

1. Mengumpulkan clones dari layanan khusus.
2. shared-tanpa RACS
    a. setiap clone diduplikat pada storage locally
    b. updates harus diaplikasikan pada semua clone storage
3. shared-disk RACS (cluster)
    α. semua clones di share pada storage manager
    β. storage server bisa mentoleransi error/kesalahan

8.9.2.4 Partition



Gambar 8-115 Partition

1. Perkembangan layanan melalui :
   a. Duplikasi hardware and software
   b. Membagi data diantara node (oleh obyek), misal : mail server oleh mail box
2. Bisa diapplikasikan untuk transparents
3. requests untuk layanan partisi diroutingkan untuk partisi data yang relevan
4. Tidak meningkatkan availability
5. Penyimpanan data hanya pada satu tempat
6. Partisi diimplementasikan untuk mengemas dua node atau lebih akses ke storage meningkat.

8.9.2.5 RAPS (Reliable Array of Partitioned Services)

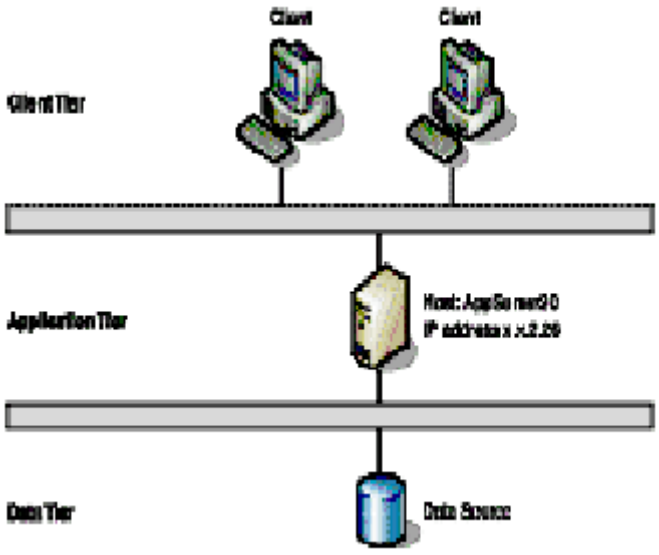
1. node yang mendukung layanan partisi packet
2. share-tanpa RAPS, shared-disk RAPS
3. Intensif update dan aplikasi database yang besar lebih baik disimpan pada routing request sebagai dedikasi server untuk melayani partisi data(RAPS).

8.10 Pencapaian Scalability

Untuk mencapai scalabilitas, diskusi yang berikut membandingkan suatu solusi non-load-balanced yang ada, yang berisi single system (single point dari kegagalan) pada level aplikasi, untuk solusi yang sangat scalable untuk mengatur pencapaian dan meningkatkan availability.

8.11 Level NON-LOAD-BALANCED

Pada awalnya, suatu organisasi mungkin memulai dengan suatu arsitektur solusi seperti yang digambarkan pada gambar 4, yang mungkin sesuai dengan pencapaian harapan awal. Seperti peningkatan beban, level aplikasi harus disesuaikan dengan peningkatan beban untuk pencapaian maintain yang diharapkan.

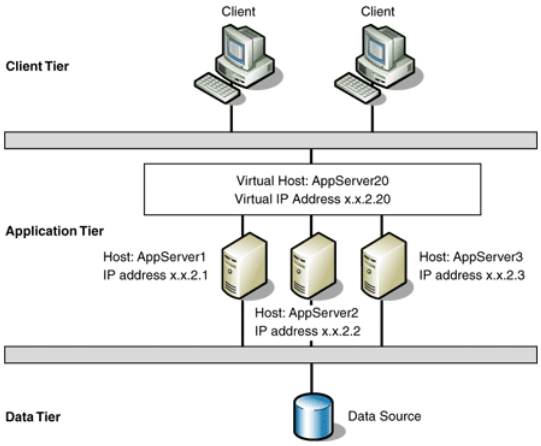


Gambar 8-116 Level Aplikasi Server

Pada gambar, level aplikasi berisi hanya satu aplikasi server (Appserver20), Yang melayani request dari client. Jika server menjadi overload, maka solusi yang akan diambil adalah mencapai level yang tersedia atau menjadi tidak tersedia.

8.12 Level Load-Balanced

Untuk meningkatkan scalabilitas dan untuk pencapaian maintain, suatu organisasi mungkin menggunakan suatu load balancer untuk meluaskan level suatu aplikasi. Contoh yang berikut, seperti yang ditunjukkan gambar, ditambahkan dua server pada level aplikasi untuk menciptakan load-balanced cluster, yang mengakses data dari level data dan menyediakan aplikasi access untuk client pada sisi client.



Gambar 8-117 Level Load Balancing

Hasilnya adalah desain standard load-balanced. Baik peralatan hardware maupun software yang running pada mesin yang ditugaskan pada virtual hostname (Appserver20) dan suatu IP address untuk Appserver1, Appserver2, dan Appserver3.

Load-balanced mengekspos virtual IP address dan host name pada jaringan dan menyeimbangkan beban dari request yang datang sekali melewati server yang stabil pada suatu group.

Jika Appserver1 gagal, request hanya diarahkan pada Appserver2 Atau Appserver3. Tergantung teknologi yang digunakan untuk menyediakan kemampuan ini, pada jumlah tertentu, server dapat ditambahkan load-balanced cluster untuk memaksimalkan scalabilitas dan tinggal menunggu peningkatan yang diinginkan.

8.13 Daftar Pustaka

1. 1.Retrieved from "http://en.wikipedia.org/wiki/Scalability"
2. http://www.freepatentsonline.com/20030158940.html
3. all right reserved, copying or reproducing any material on this website
   without prior consent from PC Media is Prohibited
4. Replication in MySQL:
   www.mysql.com/documentation/mysql/bychapter/manual_MySQL_Database_Administration.html#Replication
5. http://pop.umm.ac.id/~taufiq/Tutor/Tutor_umum/Perancangan%20Load%20Balancing%20Dan%20Clustering%20Pada%20Webserver%20Apache.doc.
6. from "http://en.wikipedia.org/wiki/Scalability"

BAB 9. DYNAMIC ROUTING

Muhammad Subakir [1)] , Fin Tho'at Bilton [1)], Ratnasari Putri Kusuma [1)]

[1)]Politeknik Elektronika Negeri Surabaya

ABSTRAK

Dengan semakin berkembangnya jaringan maka diperlukan suatu protocol yang mampu untuk membuat route untuk tabel routing. Routing merupakan fungsi yang bertanggung jawab membawa data melewati sekumpulan jaringan dengan cara memilih jalur terbaik untuk dilewati data. Dan hal tersebut tidak dapat dilakukan dengan baik apabila untuk mengupdate tabel routing menggunakan seorang admin. Supaya Router bisa meneruskan data, komputer yang ada pada jaringan tersebut harus menugaskan router untuk meneruskan data, penugasan dilakukan dengan cara setting komputer default gateway ke router, jika kita tidak setting *default gateway* maka bisa dipastikan *LAN* tersebut tidak bisa terkoneksi dengan jaringan lainnya. Permasalahan dalam membangun tabel routing tersebut dapat diatasi dengan menggunakan *dynamic routing*.

Dynamic Routing adalah salah satu tipe routing, dimana terjadi proses pembelajaran oleh router dan mengupdate table routing jika terjadi perubahan. Pembelajaran dilakukan dengan komunikasi antar router-router dengan protokol-protokol tertentu. Algoritma yang digunakan dalam dynamic routing antara lain *Distance vector routing protocols*, *Link state routing protocols, Hybrid.*

Makalah ini membahas mengenai Dynamic routing protokol yang digunakan dalam membuat tabel routing pada sebuah jaringan. Mulai dari algoritma yang digunakan dalam dynamic routing sampai konfigurasinya.

9.1 PENDAHULUAN

Fungsi utama dari layer network adalah pengalamatan dan routing, Routing merupakan fungsi yang bertanggung jawab membawa data melewati sekumpulan jaringan dengan cara memilih jalur terbaik untuk dilewati data.

Tugas Routing akan dilakukan device jaringan yang disebut sebagai Router. Router merupakan komputer jaringan yang bertugas atau difungsikan menghubungkan dua jaringan atau lebih. Type router antara lain dapat berupa: komputer yang kita fungsikan sebagai Router atau peralatan khusus yang dirancang sebagai Router. Tugas router memforward data (Fungsi IP Forward harus diaktifkan) menggunakan routing protokol (Algoritma Routing).Data diatur oleh Routed Protocol.

Router adalah komputer *general purpose* (untuk tujuan yang lebih luas) dengan dua atau lebih *interface* jaringan (*NIC Card*) di dalamnya yang berfungsi menghubungkan 2 jaringan atau lebih, sehingga dia bisa meneruskan paket dari satu jaringan ke jaringan yang lain. Untuk jaringan kecil, *interface*-nya adalah *NIC Card*, sehingga *router* mempunyai 2 *NIC* atau lebih yang bisa menghubungkan dengan jaringan lain. Untuk *LAN* kecil yang terhubung internet, salah satu *interface* adalah *NIC card*, dan *interface* yang lain adalah sembarang hardware jaringan misal modem untuk *leased line* atau *ISDN* atau koneksi internet *ADSL* yang digunakan.

Supaya Router bisa meneruskan data, komputer yang ada pada jaringan tersebut harus menugaskan router untuk meneruskan data, penugasan dilakukan dengan cara setting komputer default gateway ke router, jika kita tidak setting *default gateway* maka bisa dipastikan *LAN* tersebut tidak bisa terkoneksi dengan jaringan lainnya.

9.1.1 Cara Membangun Tabel Routing yaitu

1. Static Routing
   Dibangun berdasarkan definisi dari administrator, administrator harus cermat, satu saja tabel routing salah jaringan tidak terkoneksi
2. Default Routing
   Mengirim paket ke jaringan yang tidak ada di dalam tabel routing ke Router selanjutnya. Hal ini terjadi jika Router hanya mempunyai satu port keluar.
3. Dynamic Routing
   Secara otomatis router jalur routingnya, dengan cara bertukar informasi antar router menggunakan protokol tertentu.

9.2 Pengertian Dinamik ROUTING

Dynamic routing adalah salah satu tipe routing, dimana terjadi proses pembelajaran oleh router dan mengupdate table routing jika terjadi perubahan. Pembelajaran dilakukan dengan komunikasi antar router-router dengan protokol-protokol tertentu.

Konsep metode dynamic routing memiliki dua bagian:

1. **routing protocol** digunakan diantara Router tetangga untuk saling memberi informasi tentang jaringan mereka.
2. **algoritma routing** yang menentukan pilihan melalui jaringan itu

Protokol tergantung metode yang digunakan untuk membagi informasi external, dimana algoritma sebagai metode yang digunakan untuk memproses informasi internal.

Tabel routing di dynamic router diupdate secara otomatis berdasarkan perubahan informasi routing dengan router lain. Algoritma yang digunakan dalam dynamic routing antara lain:

1. Distance vector routing protocols
2. Link state routing protocsols
3. Hybrid

Untuk mengerti bagaimana protocol ini dapat bekerja, anda dapat memilih tipe dari dynamic routing yang terbaik yang dibutuhkan oleh jaringan. Algoritma diatas memiliki protokol yang berfungsi sebagai perangkat lunak yang mempertukarkan informasi routing untuk membentuk table routing, melakukan update table routing secara periodic, menentukan rute terbaik.

Kelebihan dari dynamic routing jika dibandingkan dengan yang lain adalah karena network bukan sebuah sistem yang statis, maksudnya disini adalah bahwa network bersifat dynamic yang artinya berubah – ubah hal ini sesuai dengan dynamic routing yang secara otomatis akan beradaptasi dengan perkembangan network, pekembangan network pada umumnya sangat pesat. Berbeda dengan static routing yang pergantian rutenya berlangsung lambat tapi pada dynamic routing ini berbeda hal

tersebut disebabkan karena adanya update kondisi network secara periodic serta adanya respon terhadap perubahan link yang terjadi.

9.3 Jenis-jenis Algoritma DINAMIK ROUTING

9.3.1 Distance Vector Routing Protocols

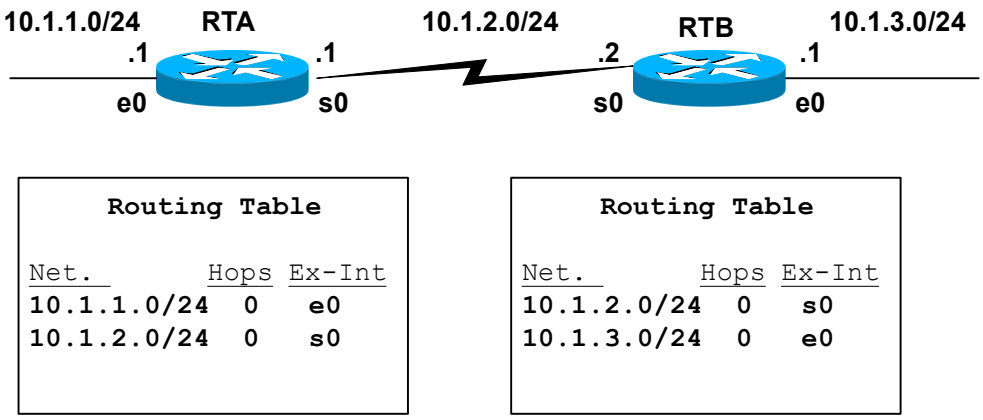
Sebuah distance vector protocol menginformasikan banyaknya hops ke jaringan tujuan (the distance) dan arahnya dimana sebuah paket dapt mencapai jaringan tujuan (the vector). Algoritma distance vector, juga dikenal sebagai *algoritma Bellman-Ford*, router mampu untuk melewatkan updates route ke tetanggganya pada interval rutin terjadwal. Setiap tetangga kemudian menerima nilai tujuannya sendiri dan menyalurkan informasi routing ke tetangga terdekat. Hasil dari proses ini sebuah table yang berisi kumpulan semua distance/tujuan ke semua jaringan tujuan.

Distance vector routing protocols, dynamic routing protocol awal, peningkatan atas static. Routing , tetapi memiliki beberapa keterbatasan , ketika topology internetwork berubah , distance vector routing protocol membutuhkan waktu beberapa menit untuk mendeteksi perubahan dan membuat koreksi penyesuaian.

Satu keuntungan dari distance vector routing protocols kesederhanaan, Distance vector routing protocols mudah untuk dikonfigurasi dan diurus, Sesuai untuk jaringan kecil dengan persyaratan-persyaratan kinerja yang rendah.

Sebagian besar menggunakan distance vector routing protocols menggunakan hitungan hop (loncatan) sebagai metric routing . Metric routing adalah nomor yang berhubungan dengan route dimana route digunakan untuk memilih beberapa route terbaik untuk tabel ip routing. Hitungan hop adalah jumlah router dimana sebuah paket harus dilewatikan umtuk mencapai tujuan.

Cara kerja dari dari distance vector



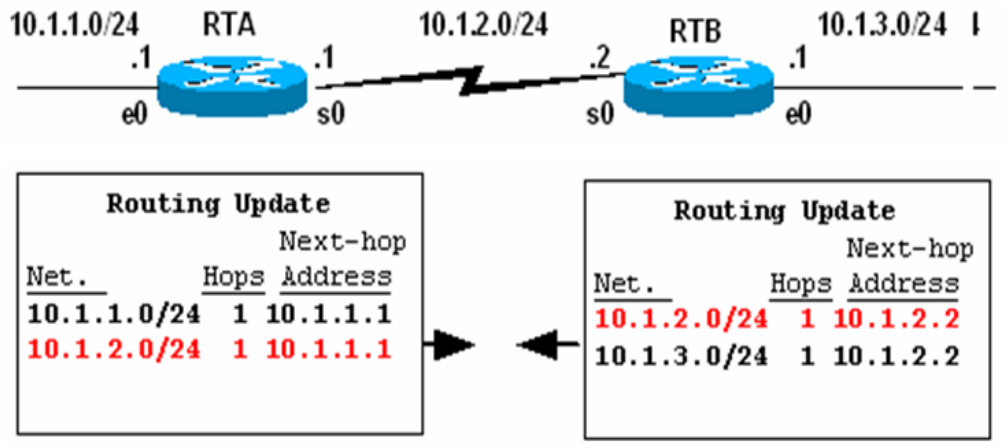
Gambar 9-118 cara kerja Distance Vector

a) Pada Error: Reference source not found asumsi router keadaan baru menyala
b) Awal router hanya punya informasi tentang jaringan yang terhubung secara langsung dengan dia

c) Pada Gambar 9 -119 Router saling mengirim Informasirouter akan saling mengirimkan informasi yang dia punya.

d) Router RTA mengirimkan data tentang jaringan yang terhubung dia secara langsung

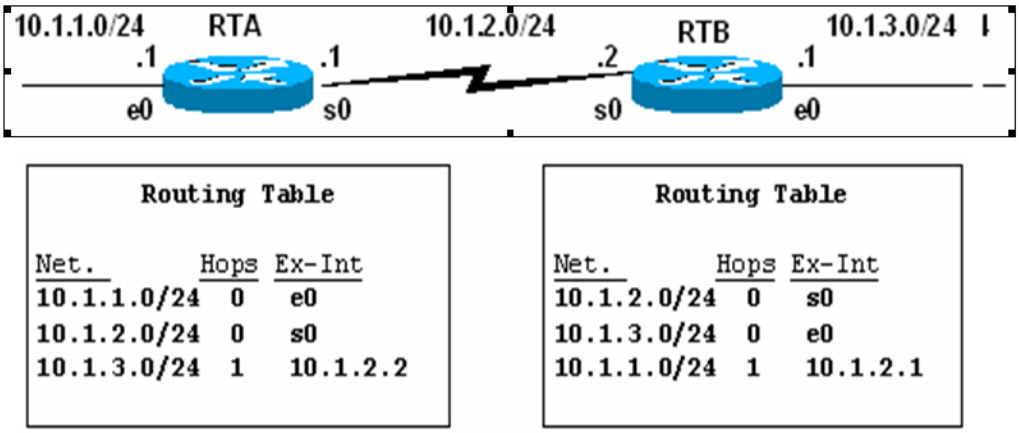
e) Router RTB juga mengirimkan data jaringan yang terhubung dia secara langsung



Gambar 9-119 Router saling mengirim Informasi

f) Setiap router melakukan pemeriksaan terhadap data yang didapat, dibandingkan dengan tabel routing masing-masing router

g) Bila belum ada dimasukkan, jika sudah dibandingkan jumlah hop



Gambar 9-120 Router melakukan perbandingan table routing

Type distance vector routing protocols :

1) RIP (Routing Information Protocol)

2) BGP (Border Gateway Protocol)

9.3.1.1 RIP (Routing Information Protocol)

Dikenal dengan Algoritma Bellman-Ford yang merupakan algoritma tertua yang terkenal lambat dan terjadi routing loop. Pertama kali dikenalkan pada tahun 1969 dan merupakan algoritma routing yang pertama pada ARPANET.

RIP yang merupakan routing protokol dengan algoritma distance vector, yang menghitung jumlah hop (count hop) sebagai routing metric. Jumlah maksimum dari hop yang diperbolehkan adalah 15 hop. Tiap RIP router saling tukar informasi routing tiap 30

detik, melalui UDP port 520. Untuk menghindari loop routing, digunakan teknik split horizon with poison reverse. RIP merupakan routing protocol yang paling mudah untuk di konfigurasi.

Routing Loop adalah suatu kondisi antar router saling mengira untuk mencapai tujuan yang sama melalui router tetangga tersebut. Misalnya pada router A mengira untuk mencapai jaringan xxx melalui router B, sedangkan router B sendiri mengira untuk mencapai jaringan xxx melalui routerA, hal tersebut bisa juga terjadi antar 3 router.

Untuk memperbaiki kinerjanya dikenal split horizon, dimana router tidak perlu mengirim data yang pernah dia terima dari jalur dimana dia mengirim data, misalnya router mengirim routing melalui eth0, maka router tidak akan pernah mengirim balik data yang pernah dia dapatkan dari interface eth0.

Sedangkan untuk mempercepat proses dikenal juga trigger update, sehingga jika terjadi perubahan info routing, router tidak perlu menunggu waktu selang normal untuk mengirimkan perubahan informasi routing tapi sesegera mungkin.

RIP memiliki 3 versi yaitu RIPv1, RIPv2, RIPng

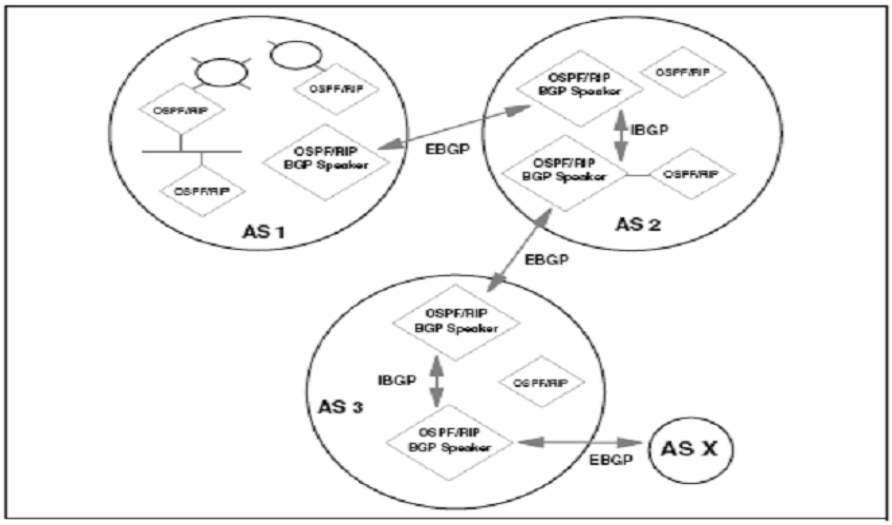
1. RIPv1 didefinisikan pada RFC 1058, dimana menggunakan classful routing, tidak menggunakan subnet. Tidak mendukung Variable Length Subnet Mask (VLSM).
2. RIPv2 hadir sekitar tahun 1994, dengan memperbaiki kemampuan akan Classless Inter-Domain Routing. Didefinisikan pada RFC 2453.
3. RIPng merupakan protokol RIP untuk IPv6. Didefinisikan pada RFC 2080.

Routing Information Protocol (RIP) yang terbaik dan paling luas menggunakan distance vector routing protocols. RIP version 1 (RIP v1), dimana sekarang sebagai model routing protocol pertama yang diterima sebagai standar untuk TCP/IP. RIP version 2 (RIP v2) menyediakan authentification support, multicast announcing, dan support yang lebih baik untuk pengkelasan jaringan.

9.3.1.2 BGP (Border Gateway Protocol)

BGP adalah router untuk jaringan external. BGP digunakan untuk menghidari routing loop pada jaringan internet. Standar BGP menggunakan RFC 1771 yang berisi tentang BGP versi 4.

Konsep dan terminologi BGP dapat dilihat pada gambar berikut :



Gambar 9-121 Komponen BGP

1) BGP Speaker : Router yang mendukung BGP
2) BGP Neighbor (pasangan) : Sepasang router BGP yang saling tukar informasi. Ada 2 jenis tipe tetangga (neighbor) :
   a. Internal (IBGP) neighbor : pasangan BGP yang menggunakan AS yang sama.
   b. External (EBGP) neighbor : pasangan BGP yang menggunakan AS yang berbeda.
3) BGP session : sesi dari 2 BGP yang sedang terkoneksi
4) Tipe traffik :
   a. Lokal : trafik lokal ke AS
   b. Transit : semua trafik yang bukan lokal
5) Tipe AS :
   a. Stub : bagian AS yang terkoneksi hanya 1 koneksi dengan AS.
   b. Multihomed : bagian ini terkoneksi dengan 2 atau lebih AS, tetapi tidak meneruskan trafik transit.
6) Transit : bagian ini terkoneksi dengan 2 atau lebih AS, dan meneruskan paket lokal dan transit
7) Nomer AS : 16 bit nomer yang unik
8) AS path : jalur yang dilalui oleh routing dengan nomer AS
9) Routing Policy : aturan yang harus dipatuhi tentang bagaimana meneruskan paket.
10) Network Layer Reachability Information (NLRI) : digunakan untuk advertise router.
11) Routes dan Path : entri tabel routing

BGP neighbor, peer, melakukan koneksi sesuai dengan konfigurasi manual pada perangkat router dan membuat jalur TCP dengan port 179. BGP speaker akan mengirimkan 19 byte pesan tetap ada untuk menjaga konektivitas (dilakukan tiap 60 detik). Pada waktu BGP berjalan pada dalam sistem AS, melakukan pengolahan informasi routing IBGP hingga mencapai administrative distance 200. Ketika BGP berjalan diantara sistem AS, maka akan melakukan pengolahan informasi routing EBGP hingga mencapai administrative distance 20. BGP router yang mengolah trafik IBGP

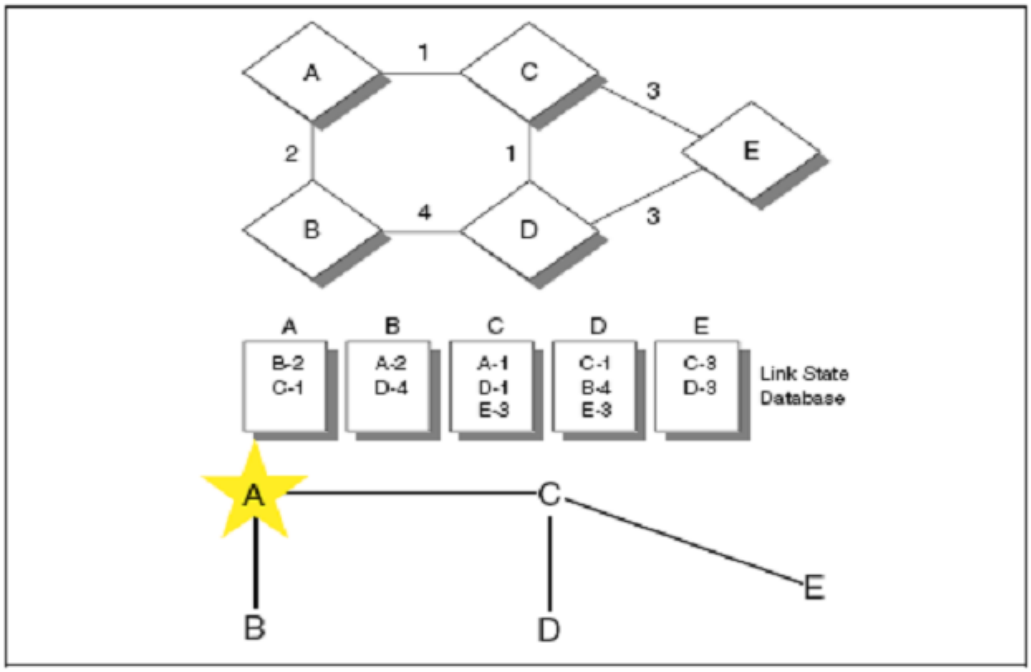
disebut transit router. Router yang berada pada sisi luar dari sistem AS dan menggunakan EBGP akan saling tukar informasi dengan router ISP.

Semakin bertambahnya jaringan akan mengakibatkan jumlah table routing yang semakin banyak pada router BGP. Untuk mengatasi hal tersebut dapat dilakukan route reflector (RFC 2796) dan Confederation (RFC 3065). Router reflector akan mengurangi jumlah koneksi yang dibutuhkan AS. Dengan sebuah router (atau dua router untuk redundansi) dapat dijadikan sebagai router reflector (duplikasi router), sehingga router yang lainnya dapat digunakan sebagai peer. Confederation digunakan untuk jaringan AS dengan skala besar, dan dapat membuat jalan potong sehingga internal routing pada AS akan mudah di manaj. Confederation dapat dijalankan bersamaan dengan router reflector.

9.3.2 Link state routing protocols

Routing ini menggunakan teknik link state, dimana artinya tiap router akan mencari informasi tentang interface, bandwidth, roundtrip dan sebagainya. Kemudian antar router akan saling menukar informasi, nilai yang paling efisien yang akan diambil sebagai jalur dan di entri ke dalam table routing. Informasi state yang ditukarkan disebut Link State Advertisement (LSA).

Dengan menggunakan algoritma pengambilan keputusan Shortest Path First (SPF), informasi LSA tersebut akan diatur sedemikian rupa hingga membentu suatu jalur routing. Ilustrasi SPF dapat dilihat pada Gambar 9 -122 Shortest Path First dibawah ini :

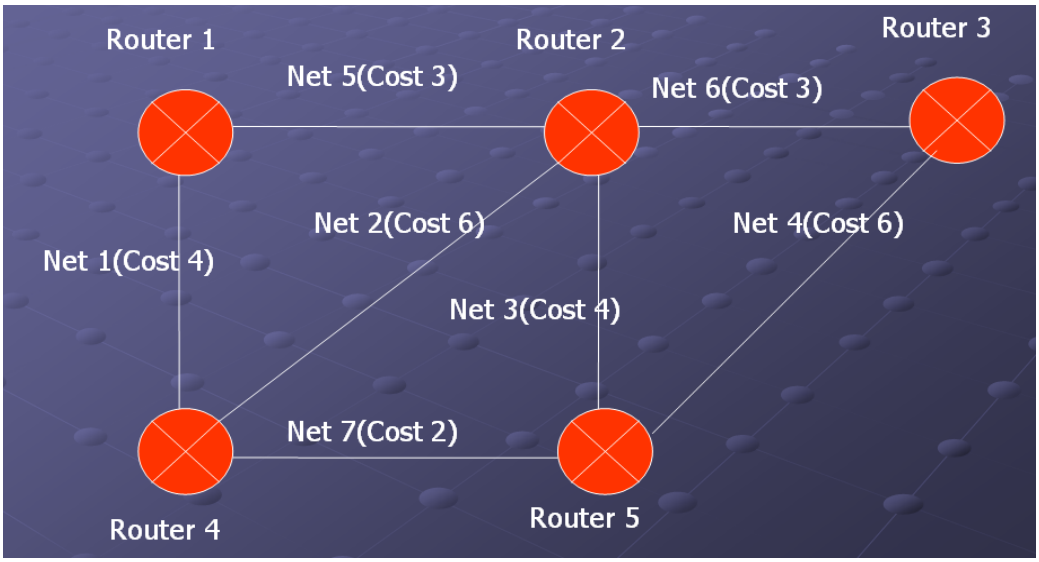


Gambar 9-122 Shortest Path First

Beberapa batasan alamat link state routing protocols dari distance vector routing protocols, sebagai contoh link state routing protocols menyediakan convergence yang lebih cepat dari pada distance vector routing protocols, Convergence adalah proses dimana router mengupdate table routing setelah perubahan topologi jaringan – perubahan itu adalah

menggantikan untuk semua router yang perlu untuk mengetahuinya. Meskipun link state routing protocols lebih lebih dipercaya (reliable) dan membutuhkan sedikit bandwith daripada distance vector routing protocols, mereka juga lebih komplek, memory lebih banyak-intensive, dan beban yang besar di CPU.

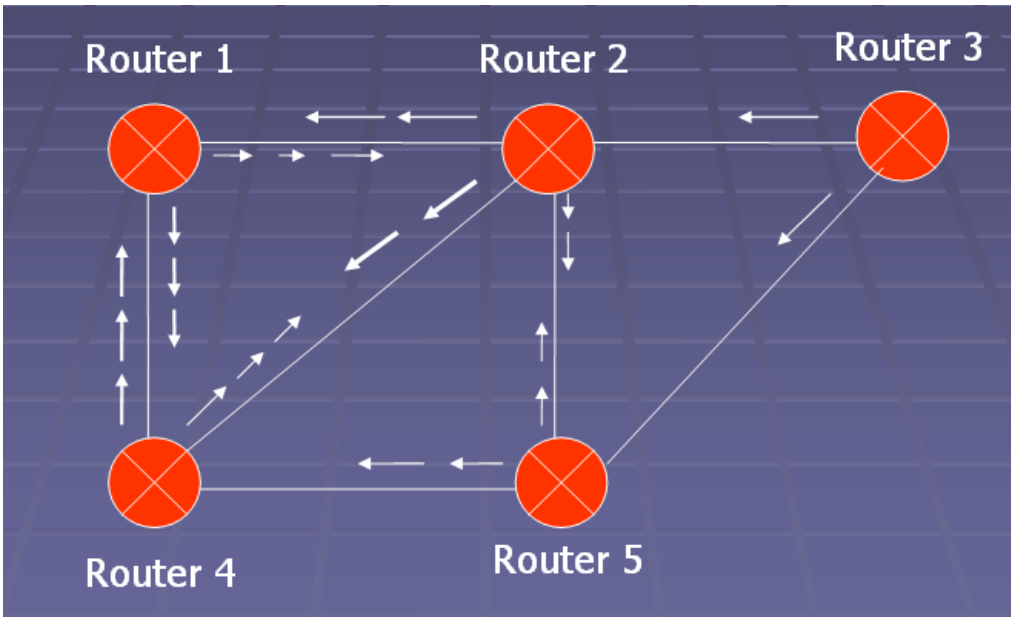
Setiap jalur ada metric, yang menunjukkan biaya, semakin kecil biaya semakin bagus. Setiap router akan membuat tree router tujuan berdasarkan biaya yang ada, tidak seperti distance vector routing protocols, dimana broadcast updates ke semua router pada jadwal interval rutin, link state routing protocols mengupdate hanya ketika kondisi link jaringan berubah. Jika hal itu terjadi ,sebuah pemberitahuan dalam bentuk pengumuman kondisi link yang dikirim melewati jaringan. Seperti pada Gambar 9 -123 Tahap Link State dibawah :



Gambar 9-123 Tahap Link State

Tahap tahap Link-State

a. Setiap router memperkenalkan diri, dengan mengirimkan paket hallo
b. Setiap router akan tahu tetangga berdasarkan paket hallo beserta biaya, dimasukkan database
c. Setiap router mengirimkan basis datanya ke tetangganya dalam paket LSA
d. Router yang menerima paket LSA harus meneruskan ke sel. tetangga sebelahnya
e. Paket LSA dimasukkan database jika infonya lebih baru
f. Awalnya terjadi flooding karena setiap router ketika ada update data akan mengirimkan sampai convergen, seperti Gambar 9 -124 Terjadinya Floading.
g. Selanjutnya setiap router menghitung jarak terpendek ke router yang lain dengan Shortest Path First, dan terbentuklah tree
h. Dimungkinkan untuk mencapai Router yang sama, antar router punya tree yang berbeda



Gambar 9-124 Terjadinya Floading

Routing protokol yang menggunakan algoritma antara lain OSPF.

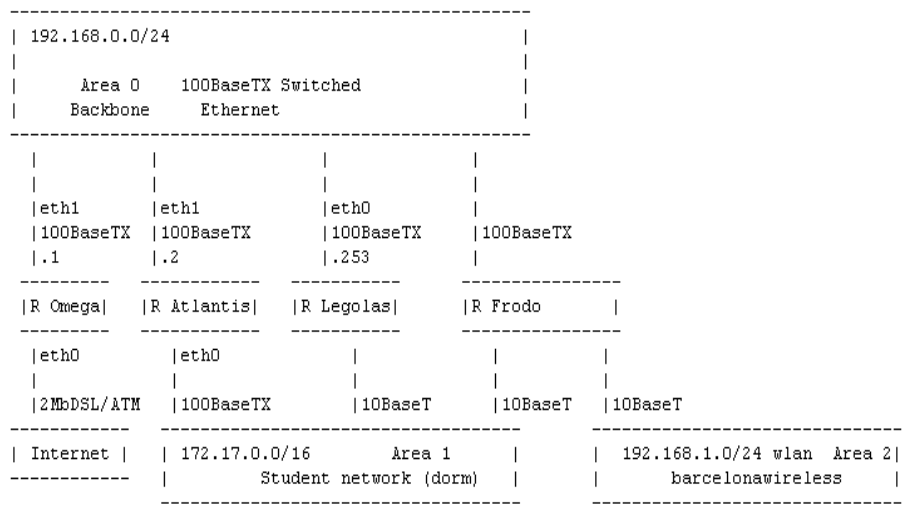
9.3.2.1 OSPF (Open Shortest Path First)

Protokol yang paling diketahui dan paling luas menggunakan link state routing protocol. OSPF adalah standar pengembangan terbuka oleh Internet Engineering Task Force (IETF) sebagai alternative dari RIP. OSPF mengcompile lengkap database topologi dari internetwork. Algoritma shortest path first (SPF), juga dikenal sebagai algoritma Djikstra, yang digunakan untuk mengolah biaya yang paling sedikit untuk mencapai tujuan. Dimana RIP menghitung biaya hanya berdasarkan hitungan hop, OSPF dapat menghitung berdasarkan metric sebagai kecepatan link dan realibility pada penambahan hitungan hop. Jika terjadi perubahan topologi terjadi Routing updates dengan sistem flooded.

Tidak seperti RIP, OSPF dapat mensuport sebuah jaringan dengan diameter 65,535(asumsi setiap link ditandai satu biaya). OSPF memancarkan multicast frames,mengurangi penggunaan CPU pada LAN. Secara herarki membagi jaringan OSPF menjadi area, meringankan memory router dan CPU.

Router dalam broadcast domain yang sama akan melakukan *adjacencies* untuk pendeteksi satu sama lainnya. Pendeteksian dilakukan dengan mendengarkan “Hello Packet”. Hal ini disebut 2 way state. Router OSPF mengirimkan “Hello Packet” dengan cara unicast dan multicast. Alamat multicast 224.0.0.5 dan 224.0.0.6 digunakan OSPF, sehingga OSPF tidak menggunakan TCP atau UDP melainkan IP protocol 89.

Contoh jaringan OSPF :



Contoh routing OSPF melalui Zebra :

```
User Access Verification

Password:
atlantis> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

K>* 0.0.0.0/0 via 192.168.0.1, eth1
C>* 127.0.0.0/8 is directly connected, lo
O   172.17.0.0/16 [110/10] is directly connected, eth0, 06:21:53
C>* 172.17.0.0/16 is directly connected, eth0
O   192.168.0.0/24 [110/10] is directly connected, eth1, 06:21:53
C>* 192.168.0.0/24 is directly connected, eth1
atlantis> show ip ospf border-routers
============ OSPF router routing table =============
R    192.168.0.253          [10] area: (0.0.0.0), ABR
                            via 192.168.0.253, eth1
                                  [10] area: (0.0.0.1), ABR
                            via 172.17.0.2, eth0
```

Contoh menggunakan IProute

```
root@omega:~# ip route
212.170.21.128/26 dev eth0  proto kernel  scope link  src 212.170.21.172
192.168.0.0/24 dev eth1  proto kernel  scope link  src 192.168.0.1
172.17.0.0/16 via 192.168.0.2 dev eth1  proto zebra  metric 20
default via 212.170.21.129 dev eth0  proto zebra
root@omega:~#
```

9.4 Hybrid Routing

Routing merupakan gabungan dari Distance Vector dan Link State routing. Contoh penggunaan algoritma ini adalah EIGRP.

9.4.1 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP merupakan routing protocol yang dibuat CISCO. EIGRP termasuk routing protocol dengan algoritma hybrid. EIGRP menggunakan beberapa terminologi, yaitu :

1. Successor : istilah yang digunakan untuk jalur yang digunakan untuk meneruskan paket data.

2. Feasible Successor : istilah yang digunakan untuk jalur yang akan digunakan untuk meneruskan data apabila successor mengalami kerusakan.
3. Neighbor table : istilah yang digunakan untuk tabel yang berisi alamat dan interface untuk mengakses ke router sebelah
4. Topology table : istilah yang digunakan untuk tabel yang berisi semua tujuan dari router sekitarnya.
5. Reliable transport protocol : EIGRP dapat menjamin urutan pengiriman data.

Perangkat EIGRP bertukar informasi hello packet untuk memastikan daerah sekitar. Pada bandwidth yang besar router saling bertukar informasi setiap 5 detik, dan 60 detik pada bandwidth yang lebih rendah.

Perluasan dari distance vector routing protocol. kombinasi dari kemampuan distance vector and link-state. Untuk menghitung jarak terpendek digunakan Diffused Update Algorithm (DUAL). Tidak ada broadcast informasi tapi ditrigger ketika ada perubahan topologi sehingga lebih cepat.

Tabel 9-9 Perbandingan RIP, OSPF, BGP

RIP	OSPF	BGP
● Internal routing protocol ● Dikenal dengan Algoritma Bellman-Ford ● Algoritma tertua, terkenal lambat dan terjadi routing loop ● Untuk memperepat proses dikenal juga trigger update ● Hanya hop count yang dipakai untuk pengukuran ● Jika hop count lebih besar dari 15 , data akan didiscard ● Menggunakan Prinsip Distance Vector ● Beroperasi dengan UDP port 520 ● Destination adalah Network, bukan Router	● Internal routing protocol ● Menggunakan **link-state** routing protocol. ● **Open standard** routing protocol didiskripsikan pada RFC 2328. ● Menggunakan **SPF algorithm** untuk menghitung biaya terendah ke tujuan. ● Jika terjadi perubahan topologi terjadi **Routing updates dengan sistem flooded**	● external routing protocol ● Perbedaan Vector Distance Protocol: tidak merugikan dalan transmisi. ● jalur di monitor and ditukar, tetapi complete gambaran lengkap jalur ● Mempertimbangkan security dan peraturan lainnya (Routing Policies) ● Ber the neighbor routers the whole path which komunikasi antar seluruh Router tetangga untuk digunakan (deterministically) ● menggunakan TCP untuk pertukaran data ● Standar BGP menggunakan RFC 1771 yang berisi tentang BGP versi 4.

9.5 SOAL dan JAWABAN

9.5.1 SOAL

1. Apa yang kamu ketahui tentang dynamic routing dan konsepnya?
2. Jelaskan kelebihan dari dynamic routing!
3. Jelaskan dengan singkat yang dimaksud dengan distance vector routing protocol!
4. Sebutkan dan jelaskan terminology pada EIGRP!
5. Bandingkan dari protocol OSPF, BGP, RIP!

9.5.2 JAWABAN

1. Dynamic routing adalah salah satu tipe routing, dimana terjadi proses pembelajaran oleh router dan mengupdate table routing jika terjadi perubahan. Pembelajaran dilakukan dengan komunikasi antar router-router dengan protokol-protokol tertentu. Konsep metode dynamic routing memiliki dua bagian:
   - **routing protocol** digunakan diantara Router tetangga untuk saling memberi informasi tentang jaringan mereka.
   - **algoritma routing** yang menentukan pilihan melalui jaringan itu
2. Kelebihan dari dynamic routing jika dibandingkan dengan yang lain adalah karena network bukan sebuah sistem yang statis, maksudnya disini adalah bahwa network bersifat dynamic yang artinya berubah – ubah hal ini sesuai dengan dynamic routing yang secara otomatis akan beradaptasi dengan perkembangan network, pekembangan network pada umumnya sangat pesat. Berbeda dengan static routing yang pergantian rutenya berlangsung lambat tapi pada dynamic routing ini berbeda hal tersebut disebabkan karena adanya update kondisi network secara periodic serta adanya respon terhadap perubahan link yang terjadi.
3. Sebuah distance vector protocol menginformasikan banyaknya hops ke jaringan tujuan (the distance) dan arahnya dimana sebuah paket dapt mencapai jaringan tujuan (the vector). Algoritma distance vector, juga dikenal sebagai *algoritma Bellman-Ford*, router mampu untuk melewatkan updates route ke tetanggganya pada interval rutin terjadwal. Setiap tetangga kemudian menerima nilai tujuannya sendiri dan menyalurkan informasi routing ke tetangga terdekat. Hasil dari proses ini sebuah table yang berisi kumpulan semua distance/tujuan ke semua jaringan tujuan.
4. EIGRP menggunakan beberapa terminologi, yaitu :
   α. Successor : istilah yang digunakan untuk jalur yang digunakan untuk meneruskan paket data.
   β. Feasible Successor : istilah yang digunakan untuk jalur yang akan digunakan untuk meneruskan data apabila successor mengalami kerusakan.
   χ. Neighbor table : istilah yang digunakan untuk tabel yang berisi alamat dan interface untuk mengakses ke router sebelah
   δ. Topology table : istilah yang digunakan untuk tabel yang berisi semua tujuan dari router sekitarnya.
   ε. Reliable transport protocol : EIGRP dapat menjamin urutan pengiriman data.
5. Perbedaan dari protocol routing :

RIP	OSPF	BGP

• Internal routing protocol • Dikenal dengan Algoritma Bellman-Ford • Algoritma tertua, terkenal lambat dan terjadi routing loop • Untuk memperepat proses dikenal juga trigger update • Hanya hop count yang dipakai untuk pengukuran • Jika hop count lebih besar dari 15 , data akan didiscard • Menggunakan Prinsip Distance Vector • Beroperasi dengan UDP port 520 • Destination adalah Network, bukan Router	• Internal routing protocol • Menggunakan **link-state** routing protocol. • **Open standard** routing protocol didiskripsikan pada RFC 2328. • Menggunakan **SPF algorithm** untuk menghitung biaya terendah ke tujuan. • Jika terjadi perubahan topologi terjadi **Routing updates dengan sistem flooded**	• external routing protocol • Perbedaan Vector Distance Protocol: tidak merugikan dalan transmisi. • jalur di monitor and ditukar, tetapi complete gambaran lengkap jalur • Mempertimbangkan security dan peraturan lainnya (Routing Policies) • Ber the neighbor routers the whole path which komunikasi antar seluruh Router tetangga untuk digunakan (deterministically) • menggunakan TCP untuk pertukaran data • Standar BGP menggunakan RFC 1771 yang berisi tentang BGP versi 4.

9.6 REFERENSI

[1] http://www.wikipedia.org//

[2] http://www.google.co.id//

[3] http://www.ilmukomputer.com//

BAB 10. WI-MAX DAN WI-MESH

Rifka Arfina Ramadani [1)], Madalena Afandinatasari [1)], Rizqi Aulia Hafidha [1)]
Politeknik Elektronika Negeri Surabaya

ABSTRAK

Standar 802.16 dikembangkan oleh *Institute of Electrical and Electronics Engineers (IEEE),* yang disebut *WirelessMAN™*, memberikan perspektif baru dalam mengakses *internet* dengan kecepatan tinggi tanpa tergantung pada jaringan kabel atau *modem*. Tahun 2002 terbentuk forum *Worldwide Interoperability for Microwave Access (Wi-MAX)* yang mengacu pada standar 802.16 dan bertugas menginterkoneksikan berbagai standar teknis yang bersifat global menjadi satu kesatuan. Teknologi *Wi-MAX* lebih murah dibandingkan dengan teknologi *broadband* lain seperti *digital subscriber line (DSL)* atau kabel *modem*. Kecepatan koneksi atau kemajuan teknologi yang baru bukan hanya aspek yang penting yang harus dievaluasi, tetapi keduanya merupakan fakta transmisi *wireless* yang tidak aman untuk berkomunikasi. Aspek keamanan merupakan hal yang sangat penting untuk teknologi *broadband* dalam mengakses informasi dari *internet*.

Jaringan Mesh adalah suatu cara untuk mengarahkan data, suara dan instruksi antar nodes. Hal ini merupakan koneksi lanjutan dan juga "hopping" dari node-to-node sampai dengan tujuannya tercapai. Jarinagn Mesh, semua nodes dihubungkan satu sama lain dalam satu jaringan. Mesh berbeda dari jaringan lainnya, dalam arti bahwa seluruh bagian komponen dapat dihubungkan satu sama lain dengan berbagai hops, dan umumnya tidak mobile. Mesh dapat dilihat sebagai salah satu jenis ad-hoc. Mobile ad-hoc networking (MANet), dan yang kemudian saling berhubungan, tetapi jaringan mobile ad-hoc juga harus berhadapan dengan permasalaha mobilitas dari node.

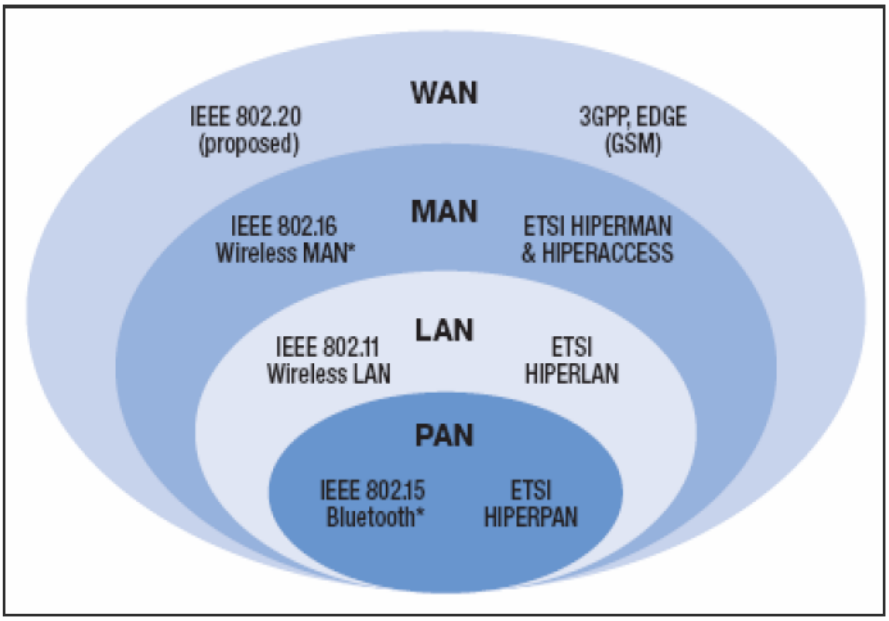
Dalam makalah ini dibahas tentang perkembangan *Wi-MAX*, perbedaannya dengan *WiFi*, fitur-fitur yang ada serta sistem keamanan yang terdapat pada teknologi *WirelessMAN™* berdasarkan pada spesifikasi standar 802.16. Dibahas pula tentang perkembangan *WiMESH*, serta prinsip kerja dari *WiMESH.*

10.1 WI-MAX

10.1.1 Pendahuluan

Wi-MAX *(Worldwide Interoperability for Microwave Access)* adalah standar *Broadband Wireless Access* dengan kemampuan menyediakan layanan data berkecepatan tinggi[1]. Teknologi Wi-MAX merupakan pengembangan dari teknologi WiFi (802.11x) yang didisain untuk memenuhi kondisi non *LOS (Line of Sight)*. Saat ini Wi-MAX digunakan untuk koneksi internet secara nirkabel dengan kecepatan hingga 70 Mbps. Tidak seperti WiFi yang cakupannya hanya sekitar rumah atau kantor, Wi-MAX mempunyai cakupan yang lebih luas hingga 50 km. Teknologi Wi-MAX dapat dimanfaatkan untuk berbagai aplikasi misalnya akses *broadband, backhaul* dan *personal broadband*[1]. Untuk akses *broadband*, Wi-MAX dapat dimanfaatkan sebagai teknologi *lastmile* untuk melayani kebutuhan layanan *broadband* bagi korporasi, SoHo

(Small Office Home Office) maupun pelanggan residensial. Untuk aplikasi *backhaul,* Wi-MAX dapat dimanfaatkan sebagai *backhaul* Wi-MAX itu sendiri, *backhaul hotspot* atau *backhaul* teknologi seluler.



Gambar 10-125 Standar-standar spesifikasi komunikasi

10.1.2 Sejarah Wi-MAX

Bagaimana asal usul teknologi Wi-MAX dan nama Wi-MAX itu sendiri? Menurut James A. Johnson (Vice President, Intel Communications Group/General Manager, Wireless Networking Group), istilah Wi-MAX berasal dari singkatan wireless (disingkat Wi) Microwave Access (disingkat MAX). Wi-MAX menyerupai Wi-Fi dalam hal penggunaan teknologi modulasi yang sama[2].

Teknologi ini disebut OFDM (*Orthogonal Frequency Division Multiplexing*). OFDM merupakan sebuah sistem modulasi digital di mana sebuah sinyal dibagi menjadi beberapa kanal dengan pita frekuensi yang sempit dan saling berdekatan, dengan setiap kanal menggunakan frekuensi yang berbeda. Teknologi tersebut dikembangkan dalam tahun 1960-an - 1970-an. Teknologi ini dikembangkan pada saat dilakukannya penelitian untuk mengurangi terjadinya interferensi frekuensi di antara berbagai kanal yang jaraknya saling berdekatan.

Pada frekuensi non-Wi-MAX, sebuah gelombang radio biasanya akan saling mengganggu gelombang radio lain, khususnya jika frekuensi tersebut memiliki siklus getaran yang berdekatan[2]. Hal yang paling terlihat adalah saat kita memainkan dua mobil *remote control* pada frekuensi radio yang berdekatan, misalnya mobil A (frekuensi 27,125MHz) dan mobil B (frekuensi 27,5MHz). Jika kedua mobil (berikut kontrol radionya) dihidupkan, kedua frekuensi tersebut akan bisa saling mengganggu. Akibatnya, jika kita akan menggerakkan mobil A, mobil B bisa ikut berjalan. Atau jika kita membelokkan mobil B, mobil A akan mundur beberapa meter[2].

Bayangkan apa yang akan terjadi jika hal ini dialami oleh frekuensi yang dipakai untuk membawa data (*carrier*) seperti pada komunikasi data nirkabel. Gangguan tersebut bisa menimbulkan aneka kerugian, seperti terjadinya kerusakan data yang dibawa frekuensi tersebut, terjadinya kegagalan pengiriman data, atau terjadinya kesalahan dalam pengalihan data.

Dengan teknologi yang ditawarkan Wi-MAX, semua kendala tersebut akan sirna dengan sendirinya. Teknologi Wi-MAX memungkinkan kita memancarkan berbagai sinyal dalam jarak yang sangat berdekatan, tanpa harus cemas bahwa aneka sinyal tersebut akan saling mengganggu/berinterferensi[2]. Dengan demikian, kita bisa menumpangkan lalu lintas data dengan kepadatan tinggi dalam berbagai kanal tersebut. Dengan banyaknya kanal yang bisa ditumpangi oleh data yang berlimpah dalam satu waktu, ISP atau penyedia layanan *broadband* bisa menghadirkan layanan berbasis kabel atau DSL untuk banyak pelanggan sebagai ganti media kabel tembaga.

Meskipun teknologi dasarnya sama, Wi-Fi dan Wi-MAX masih memiliki perbedaan. Menurut James, perbedaan antara keduanya terletak pada pembagian spektrum yang dipakai, dan pada penggunaan frekuensi berlisensi dalam Wi-MAX[2]. Meskpun Wi-MAX dan Wi-Fi menggunakan salah satu frekuensi tidak berlisensi (yakni frekuensi 5,8GHz), Wi-MAX juga diarahkan untuk bisa memanfaatkan dua frekuensi lain yang berlisensi, yakni 2,5GHz and 3,5GHz. Hal ini memungkinkan kita meningkatkan daya keluaran perangkat Wi-MAX sehingga bisa menjangkau jarak yang lebih jauh.

Dengan demikian, jika WiFi hanya beroperasi pada kisaran meter, Wi-MAX bisa beroperasi pada kisaran kilometer. Selain itu, Wi-MAX dirancang dalam tataran teknologi *carrier-grade*. Hal ini membuat Wi-MAX memiliki kehandalan dan kualitas pelayanan yang lebih baik dibandingkan Wi-Fi. Dengan jangkauan jarak yang lebih jauh, dan kemampuan untuk melewati aneka penghalang seperti gedung atau pohon, Wi-MAX sesuai untuk diterapkan di daerah perkotaan yang memiliki gedung perkantoran dan pemukiman.

10.1.3 Wi-MAX dan WiFi

Sebenarnya perfomansi Wi-MAX hampir sama dengan WiFi yaitu, keduanya menggunakan “hotspot” atau lingkungan sekitar antenna dimana kita dapat mengakses informasi dengan PDA, Laptop atau gadget lainnya. Perbedaannya adalah pada segi jangkauan radiusnya. Untuk WiFi bisa menjangkau 100 feet atau sekitar radius 30 meter, sedangkan Wi-MAX memiliki jangkauan 25-30 mile atau sekitar 40-50 Km (maksimal 50 Km)[3]. Hal ini berarti bahwa Wi-MAX dapat digunakan sebagai pengganti broadband tradisional yang masih menggunakan line telepon (seperti, ASDL, ISDN) dan kabel (Internet melalui TV Kabel atau jaringan PLN misalnya). Untuk permulaan, Wi-MAX ditujukan untuk penggunaan fixed wireless.

Saat ini Memang banyak pebisnis teknologi informasi yakin Wi-MAX akan segera mendunia. Padahal pengembangan Wi-Fi saja memerlukan waktu 10 tahun. Teknologi ini sebenarnya adalah pengembangan lebih lanjut dari konsep Wi-Fi. Teknologi ini sudah banyak memberikan kemudahan bagi manusia, namun mempunyai kendala terbatasnya kapasitas dan

jangkauannya. Sedangkan banyak perusahaan besar di dunia membutuhkan akses jaringan tanpa kabel yang memiliki kapasitas data besar, biaya murah dan bisa diakses dari semua tempat.

Teknologi Wi-Fi memiliki jangkauan yang terbatas, paling jauh sekira 100 meter saja. Bandingkan dengan Wi-MAX memiliki radius jangkauan sekira 7 sampai dengan 10 km. Tidak salah kalau Wi-MAX diproyeksikan sebagai teknologi jaringan tanpa kabel untuk daerah perkotaan.

Dengan Wi-MAX kemana pun kita pergi di dalam kota, akses internet dapat dilakukan tanpa biaya yang terlalu mahal. Untuk mencari informasi tidak perlu pergi ke kantor ataupun warung internet, cukup duduk di mobil sambil menunggu lalu lintas yang macet, kemudian membuka notebook. Sedangkan untuk Wi-Fi begitu keluar dari area hotspot, koneksi data langsung mati.

Wi-MAX memiliki kemampuan menghantarkan data sampai dengan kecepatan 75 megabit perdetik (Mbps), sedangkan Wi-Fi hanya 11 Mbps. Keunggulan lainnya adalah Wi-MAX bermain pada frekuensi yang cukup rendah dan lebar, yaitu 2 - 6 gigahertz (GHz). Sedangkan Wi-Fi yang diatur dalam protokol 802.11b di 2,4 GHz dan protokol 802.11a di 5 GHz.

Standar Wi-MAX ini menjanjikan penyediaan konektifitas broadband jarak jauh dengan kecepatan DSL. Komponen nirkabel ini diharapkan dapat menjadi suatu rancangan system-on-a-chip yang pertama bagi Customer Premise Equipment (CPE) dengan efektifitas biaya yang mendukung IEEE 802.16-2004 (dulu dikenal sebagai IEEE 802.16REVd). CPE sendiri digunakan untuk aplikasi pengiriman dan penerimaan suatu sinyal broadband nirkabel yang menyediakan konektifitas Internet.

WiFi (Wireless Fidelity) sebagai teknologi nirkabel lain yang cukup popular dengan ruang lingkup jaringan local. Tentu saja, dengan teknologi WiFi ini telah banyak diigunakan di restoran maupun kafe yang menyajikan layanan WiFi untuk pelanggannya dengan membeli kartu prabayar WiFi untuk dapat mengakses internet nirkabel dari notebook maupun PDA.

Yang membedakan WiFi dengan Wi-MAX adalah, WiFi dipasang terutama di satu spectrum yaitu 2.4 GHz yang umumnya tidak memerlukan lisensi. Sedangkan jika dibandingkan dengan Wi-MAX, berbasis frekuensi antara 2 – 11 GHz.

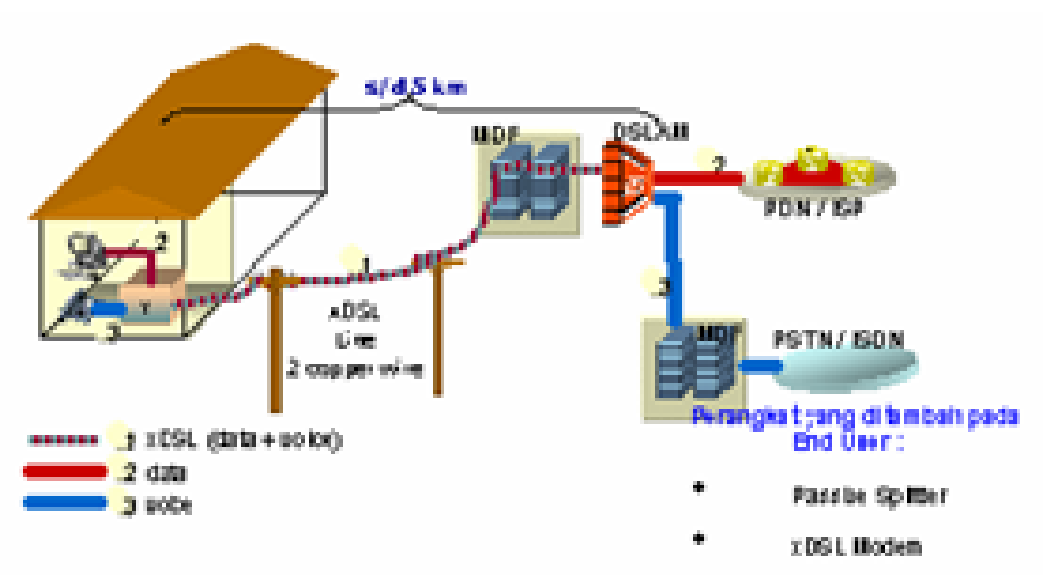
Gambar 10-126 Wi-MAX dan WiFi

10.1.4 Wi-MAX dan DSL

Banyak ragam yang digunakan oleh operator telekomunikasi untuk memberikan layanan broadband akses ke pelanggan. Dari sisi media yang digunakan dapat dibedakan menjadi dua yaitu teknologi wireline (kabel) dan teknologi wireless (tanpa kabel). Dari kategori teknologi wireline dapat digunakan teknologi DSL (Digital Subscriber Line), kabel modem, HFC ,maupun optik. Sedangkan dari kategori wireless dapat memanfaatkan teknologi wireless LAN, BWA (Broadband Wireless Access) maupun teknologi terbaru Wi-MAX (Worldwide Interoperability for Microwave Access).

Dengan berbagai solusi di atas, sebagian operator memanfaatkan teknologi DSL (kabel) dan BWA (untuk *wireless*). Bagi operator telekomunikasi yang *incumbent* di suatu negara, contoh TELKOM untuk Indonesia dimana telah menggelar kabel sekitar 6 juta line maka akan memanfaatkan teknologi DSL guna meng-*enhanced* jaringan fisiknya untuk menyalurkan data kecepatan tinggi ke pelanggan. Sedangkan bagi operator baru tentunya sangat sulit dan mahal bila menggelar jaringan broadband dengan DSL. Alternatifnya memanfaatkan teknologi *wireless* (BWA). Dengan lahirnya teknologi *wireless* terbaru (Wi-MAX) maka dapat dijadikan sebagai pengganti atau alternatif untuk menyalurkan layanan *broadband* ke pelanggan.

Bila dilihat dari segmen pasarnya, maka antara Wi-MAX dan DSL memiliki kesamaan yaitu sama-sama ditujukan untuk MAN (*Metro Area Network*) dimana jarak ke pelanggan sekitar 10 km.



Gambar 10-127 Konfigurasi DSL

DSL sendiri memang berkecepatan tinggi dengan akses broadband kabel hanya tersedia bagi sebagian pengguna computer. Sehingga dengan Wi-MAX akan memungkinkan terjadinya koneksi nirkabel berkecepatan tinggi dengan biaya relative lebih murah dan efektif bagi pengguna rumahan dan bisnis, baik di daerah perkotaan maupun daerah pedesaaan.

Permasalahan yang ada di sector broadband telah diselesaikan dengan adanya teknologi Wi-MAX. Hal yang sangat disayangkan bagi pengguna/konsumen yang ingin menikmati

layanan seperti telepon dan jaringan local yang mulai beranjak ke system nirkabel, akses broadband untuk bisnis atau perumahan masih cenderung mengandalkan kabel untuk penyaluran datanya. Akibatnya, merugikan operator sekaligus konsumen yang ada diluar jangkauan kabel tersebut.

Teknologi kabel seperti Digital Subscriber Line (DSL), moden kabel dan leasedline masih memiliki daya saing dalam hal biaya, kemudahan dan perangkat yang mudah ditemui. Dan solusinya jatuh pada Wi-MAX yang berupaya menyatukan industri nirkabel sekaligus menurunkan harga perangkat nirkabel tersebut.

10.1.5 Keuntungan dan Kekurangan Wi-MAX

Ada beberapa keuntungan dengan adanya *Wi-MAX*, jika dibandingkan dengan *WiFi* antara lain sebagai berikut.

1. Para produsen mikrolektronik akan mendapatkan lahan baru untuk dikerjakan, dengan membuat *chip-chip* yang lebih *general* yang dapat dipakai oleh banyak produsen perangkat *wireless* untuk membuat *BWA*-nya. Para produsen perangkat *wireless* tidak perlu mengembangkan solusi *end-to-end* bagi penggunanya, karena sudah tersedia standar yang jelas.
2. Operator telekomunikasi dapat menghemat investasi perangkat, karena kemampuan *WI-MAX* dapat melayani pelanggannya dengan area yang lebih luas dan dengan kompatibilitas yang lebih tinggi.
3. Pengguna akhir akan mendapatkan banyak pilihan dalam ber*internet*. *Wi-MAX* merupakan salah satu teknologi yang dapat memudahkan kita untuk koneksi dengan *internet* secara mudah dan berkualitas.
4. Memiliki banyak fitur yang selama ini belum ada pada teknologi *WiFi* dengan standar *IEEE* 802.11. Standar *IEEE* 802.16 digabungkan dengan *ETSI HiperMAN*, maka dapat melayani pangsa pasar yang lebih luas.
5. Dari segi *coverage*-nya saja yang mencapai 50 kilometer maksimal, *Wi-MAX* sudah memberikan kontribusi yang sangat besar bagi keberadaan *wirelass MAN*. Kemampuan untuk menghantarkan data dengan *transfer rate* yang tinggi dalam jarak jauh dan akan menutup semua celah *broadband* yang tidak dapat terjangkau oleh teknologi kabel dan *digital subscriber line (DSL)*.
6. Dapat melayani para *subscriber*, baik yang berada pada posisi *line of sight (LOS)* maupun yang memungkinkan untuk tidak *line of sight (NLOS)*.

Sedangkan kekurangan yang ada pada *Wi-MAX* adalah :

1. Karena menggunakan pita spektrum frekuensi tinggi, maka cakupan layanan Wi-MAX lebih kecil dibanding 3G sehingga jumlah base station yang dibutuhkan untuk mencakup luas yang sama dibutuhkan lebih banyak jumlah base station.

2. Alokasi spektrum frekuensi Wi-MAX memerlukan penyesuaian terhadap alokasi frekuensi eksisting di tiap negara. Ketidakseragaman alokasi frekuensi menyebabkan harga perangkat menjadi mahal.
3. Kemampuan Wi-MAX untuk mobilitas akan tidak sebagus sistem seluler dan konsumsi battery akan lebih boros.

10.1.6 Standarisasi Wi-MAX

Standar *IEEE* 802.16 merupakan keluaran dari organisasi *IEEE*, sama seperti *IEEE* 802.11 adalah standar yang dibuat khusus untuk mengatur komunikasi lewat media *wireless.* Yang membedakannya adalah *Wi-MAX* mempunyai tingkat kecepatan *transfer* data yang lebih tinggi dengan jarak yang lebih jauh, sehingga kualitas layanan dengan menggunakan komunikasi ini dapat digolongkan ke dalam kelas *broadband.* Standar ini sering disebut *air interface for fixed broadband wireless access system* atau *interface* udara untuk koneksi *broadband*.

Sebenarnya standarisasi *IEEE* 802.16 ini lebih banyak mengembangkan hal-hal yang bersifat teknis dari *layer physical* dan *layer datalink (MAC)* dari system komunikasi *BWA*. Versi awal dari standar 802.16 ini dikeluarkan oleh *IEEE* pada tahun 2002. Pada sesi awal ini, perangkat 802.16 beroperasi dalam lebar frekuensi 10- 66 GHz dengan jalur komunikasi antar perangkatnya secara *line of sight (LOS). Bandwidth* yang diberikan oleh teknologi ini sebesar 32-134 Mbps dalam *area coverage* maksimal 5 kilometer. Kapasitasnya dirancang mempu menampung ratusan pengguna setiap satu *BTS*. Dengan kemampuan semacam ini teknologi perangkat yang menggunakan standar 802.16 cocok digunakan sebagai penyedia koneksi *broadband* melalui *media wireless*. Perbedaan teknis antara *IEEE* 802.11 dengan *IEEE* 802.16 dapat dilihat pada tabel berikut ini.

Tabel 10-10 Perbedaan teknologi IEEE 802.11 dengan IEEE 802.16

	IEEE 802.11	IEEE 802.16	Perbedaan Teknis
Jarak	Dibawah 9 Km	Hingga 50 Km	Teknik 256 *FFT* sistem *signaling*nya menciptakan fitur ini.
Coverage	Optimal jika bekerja di dalam ruangan	Dirancang untuk penggunaan diluar ruangan dengan kondisi *NLOS*	IEEE 802.16 memiliki sistem gain yang lebih tinggi, meng-akibatkan sinyal lebih kebal terhadap halangan dalam jarak yang lebih jauh.
Skalabilitas	Skala pengguna-annya hanya dalam tingkat *LAN*. Ukuran frekuensi kanalnya dibuat *fix* (20 MHz)	Dibuat untuk men-dukung sampai 100 pengguna. Ukuran frekuensi kanal dapat bervariasi mulai dari 1,5 sam-pai dengan 20 MHz.	Sistim *TDMA* dan peng-aturan *slot* komunikasi, sehingga semua frekuensi yang termasuk dalam *range* IEEE 802.16 dapat dipakai serta jumlah pengguna dapat bertambah.
Bit Rate	2,7 bps/Hz hingga 54Mbps dalam kanal 20 MHz	5 bps/Hz hingga 100 Mbps dalam kanal 20 MHz.	Teknik modulasi yang lebih canggih disertai koreksi *error* yang lebih fleksibel, sehingga penggunaan freku-ensi kanal lebih *effisien*.
QoS	Tidak mendukung *QoS*	*QoS* dibuat dalam *layer MAC*	Adanya pengaturan secara otomatis terhadap slot-slot *TDMA*, sehingga dimanfa-atkan untuk peng-aturan *QoS*.

10.1.7 Teknologi Wi-MAX

Wi-MAX (*worldwide interoperability for microwave access*, IEEE.802.16) dikembangkan secara khusus dari teknologi OFDM (*orthogonal frequency division multiplexing*) untuk mencapai *coverage area* yang luas (beberapa mil atau sekitar 50-an km) dengan kecepatan tinggi (sekitar 72 Mbps *wireless*) dan tambahan *multiple access* (lihat IEEE.802.16e: *OFDMA access method*) yang mungkin bisa diaplikasikan untuk sistem komunikasi selluler masa depan. Tambahan *multiple access* ini dengan performansi yang baik bisa-bisa akan menjadi kompetitor baru bagi jaringan telepon seluler yang sudah ada.

Teknologi pendahulunya, yaitu WiFi (IEEE.802.11) yang sekarang masih kita pakai di laboratorium, kampus, airport, ruang konferensi sampai *coffee shop* dan supermarket, hanya mampu menjangkau 20-100 meter dengan kecepatan beberapa puluh Mbps. Karena itulah Wi-MAX lebih menjanjikan untuk memperluas jaringan murah di pedesaan dimana pembangunan infrastruktur seperti kabel DSL terasa sangat mahal. Mungkin inilah yang mendasari komentar para pakar, bahwa teknologi Wi-MAX adalah vital dan sangat cocok (baca: murah) untuk diaplikasikan di negara-negara berkembang seperti Indonesia, dimana biaya investasi *fixed communication* masih dirasa berat.

10.1.8 OFDM Wi-MAX

OFDM bukanlah barang baru karena sebenarnya sudah ramai diteliti sejak tahun 60-an meskipun baru *booming* setelah dipicu dengan penemuan FFT (*Fast Fourier Transform*) sekitar

tahun 70-an, ditambah dengan aplikasi akhir-akhir ini dalam DSL, cable modem, WiFi, Televisi Digital dan Wi-MAX. OFDM mampu mensupport data kecepatan tinggi karena efisiensinya yaitu dengan frekuensi tumpang tindih (*overlapping*) tapi dijamin tidak rusak karena orthogonal (kecuali ada masalah lain seperti frekuensi offset karena efek Doppler).

Dengan karakter dasar OFDM di atas, dalam Standard Wi-MAX, OFDM akan mampu mencapai 72Mbps (data bersih) atau sampai 100Mbps (data plus coding) dalam spektrum 20MHz. Artinya, OFDM dalam Wi-MAX mampu mengirimkan 3.6 bps per Hz. Misalnya kita punya alokasi bandwidth 100MHz, diimplementasikan pada frekuensi 5.8GHz (yaitu misal 5.725-5.825GHz), diperoleh 5 blok band (yaitu 5 x 20MHz = 100MHz), maka kita akan peroleh kapasitas 5x72Mbps = 360Mbps (dengan asumsi seluruh channel ditambahkan dan dengan 1x *frequency reuse*). Kemudian dengan sektorisasi, maka total kapasitas suatu base station akan mencapai lebih dari 1Gbps, sebuah kecepatan sangat tinggi untuk *wireless access*.

10.1.9 Komponen Wi-MAX

Komponen utama Wi-MAX system adalah Subscriber Station (SS) atau yang dikenal dengan nama CPE dan Base Station (BS). BS dan satu atau lebih SS dapat membentuk sebuah sel dengan struktur point-to-multipoint (P2MP). Di udara, BS mengontrol aktifitas bersama sel, termasuk akses ke medium oleh SS, alokasi untuk kualitas layanan (QoS) dan mengatur keamanan jaringan yang dibawahinya.

Sistem 802.16 menggunakan antenna di site SS. Antena ini meng-cover daerah cakupannya. Perlengkapan seperti Adaptive Antenna System (AAS) dan sub-kanal juga didukung oleh standar untuk perencanaan link budget untuk instalasi indoor. IEEE 802.16e bekerja khusus untuk standar mobilitas dan men-support kekuatan terminal SS.

BS umumnya menggunakan antenna sector directional atau omni-directional. Fixed SS umumnya menggunakan negara directional sedangkan mobile atau portable SS umumnya menggunakan negara directional.

Multiple BS dapat dikonfigurasi untuk membentuk jaringan selular wirelessw. Ketika Orthogonal Frequency Division Multiplexing (OFDM) digunakan, radius sel mencakup 30 mile. Paling tidak, praktisnya radius minimal sel mencakup kurang lebih 5 mile. Standar 802.16 juga dapat digunakan pada point-to-point (P2P) atau topologi Mesh, menggunakan sepasang negara directional. Hal ini dapat digunkan untuk meningkatkan range yang efektif dengan system yang relative untuk mendukung mode P2MP.

Wi-MAX merupakan standar IEEE 802.16 yang membawahi aneka standar turunannya. Standar ini mengatur penggunaan perangkat nirkabel untuk keperluan jaringan perkotaan (*Metropolitan Area Network*/MAN). Standar ini khususnya dirancang untuk memenuhi kebutuhan jaringan akan akses nirkabel berkecepatan tinggi atau BWA (*broadband wireless access*). Kehadiran teknologi ini diharapkan akan memungkinkan akses terhadap aneka aplikasi multimedia via koneksi nirkabel dengan jarak antarperangkat yang lebih jauh.

10.1.10 Karakteristik Wi-MAX

Standar 802.16 (dan turunanannya) beroperasi pada pita frekuensi radio antara 2GHz sampai 11GHz. Standar ini memiliki *transfer rate* 75Mbit per detik dengan tingkat *latency* yang rendah, dan efisiensi penggunaan ruang spektrum frekuensi.

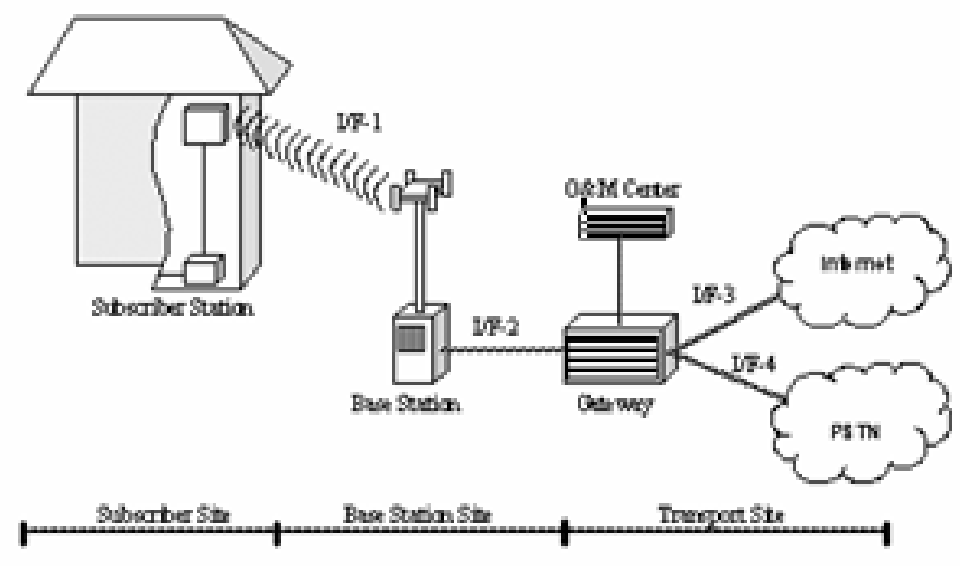
Untuk mengamankan koneksi yang terjadi, standar ini juga telah mendukung *feature* enkripsi data, dengan pengaturan kesalahan bertipe Forward Error Correction (FEC). Jarak yang bisa dijangkau oleh standar ini dapat diperluas sampai sekitar 30 mil, atau sekitar 48 kilometer dengan tingkat *throughput* yang masih memadai untuk mentransfer data.

Wi-MAX terbagi menjadi dua model pemanfaatan yang masing-masing diwakili oleh dua standar IEEE yang berbeda. Model pemanfaatan pertama adalah pemanfaatan *fixed-access*, atau sambungan tetap yang menggunakan standar IEEE 802.16-2004 (sebagai hasil revisi atas standar IEEE 802.16a). Standar ini termasuk dalam golongan layanan "fixed wireless" karena menggunakan antena yang dipasang di lokasi pelanggan. Antena ini dapat dipasang di atap atau tiang tinggi persis seperti cakram parabola untuk TV. Teknologi dari standar inilah yang menjadi subsitusi dari teknologi-teknologi seperti *modem* kabel, segala macam *digital subscriber* line (xDSL), sirkuit *transmit/exchange* (Tx/Ex), dan sirkuit *optical carrier* (Oc-x).

Sementara model pemanfaatan kedua, sering disebut pemanfaatan *portable* atau *mobile* yang menggunakan standar IEEE 802.16e. Standar ini khususnya diimplementasikan untuk komunikasi data pada aneka perangkat genggam, atau perangkat bergerak (*mobile*) seperti PDA atau notebook.

10.1.11 Konfigurasi Wi-MAX

Secara umum konfigurasi Wi-MAX dibagi menjadi 3 bagian yaitu *subscriber station*, *base station* dan *transport site*. Untuk *subscriber station* terletak di lingkungan pelanggan (bisa *fixed* atau *mobile/portable*). Sedangkan *base station* biasanya satu lokasi dengan jaringan operator (jaringan IP/internet atau jaringan TDM/PSTN). Untuk memperjelas dari konfigurasi dimaksud, maka gambar berikut (Gambar 2) merupakan konfigurasi generik dari Wi-MAX.



Gambar 10-128Konfigurasi Wi-MAX

- Open standar, salah satu kelebihan Wi-MAX adalah open standar. Sehingga baik vendor, pelanggan maupun operator tidak perlu dipusingkan lagi karena dapat memanfaatkan merk apa saja (tidak tergantung salah satu merk).
- Kecepatan instalasi, kelebihan lain Wi-MAX adalah kecepatan instalasi. Untuk instalasi pelanggan dengan antena *outdoor* memakan waktu tidak sampai satu jam. Bandingkan bila harus menggelar jaringan kabel dan modem DSL
- Masalah regulasi, nampaknya masyarakat harus bersabar untuk bisa memanfaatkan Wi-MAX. Hal tersebut dikarenakan belum adanya regulasi dari pemerintah khususnya menyangkut masalah frekuensi. Untuk frekuensi Wi-MAX 3,5 GHz saat ini masih berbenturran dengan frekuensi satelit sedangkan 2,5 GHz interferensi dengan *Microwave* dan TV kabel.
- *High speed*, Wi-MAX mampu untuk menyalurkan data hingga kecepatan 75 Mbps dengan lebar spasi yang digunakan sebesar 20 MHz
- Fleksibel, Wi-MAX tidak hanya diperuntukkan bagi pelanggan *fixed* seperti pelanggan DSL, namun dapat pula untuk melayani pelanggan *nomadic* dan *mobile.*
- Investasi, seiring dengan maturitas produk Wi-MAX maka banyak vendor yang menjanjikan akan turunnya harga investasi perangkat Wi-MAX. Bahkan tahap selanjutnya Wi-MAX nantinya akan diproduksi embeded (bersatu layaknya WiFi pada *notebook* centrino) dengan perangkat *notebook*, PDA bahkan *Handphone*.
- Tidak tergantung kabel, lain dengan DSL yang membutuhkan jaringan kabel, maka Wi-MAX tidak tergantung infrastruktur kabel tersedia. Dengan demikian Wi-MAX lebih fleksibel digunakan untuk memberikan layanan akses *broadband* hingga ke daerah rural atau lokasi yang belum atau sulit bila menggunakan jaringan kabel.

10.1.12 Prinsip Kerja Wi-MAX

Teknologi *Wi-MAX* dapat meng-*cover* area sekitar 50 kilometer, dimana ratusan pelanggan akan di-*share* sinyal dan kanal untuk mentransmisikan data dengan kecepatan sampai 155 Mbps. Aspek keamanan merupakan aspek yang sangat penting dan akan dievaluasi oleh

para pengguna *internet* dengan menggunakan fasilitas *ADSL* atau teknologi kabel *modem* maupun yang berlangganan dengan teknologi *Wi-MAX*.

Sistem pengamanan data dilakukan pada *layer physical (PHY)* dan *data link layer (MAC)* pada suatu arsitektur jaringan, tepatnya pada *base station (BS)* untuk didistribusikan ke wilayah sekelilingnya dan *subscriber station (SS)* untuk komunikasi *point to multipoint. Base station (BS)* dihubungkan secara langsung dengan jaringan umum *(public network)*.

Secara umum *WirelessMAN traffic* dibedakan menjadi tiga bagian, seperti berikut ini.

1. Pelanggan mengirimkan data dengan kecepatan 2 – 155 Mbps dari *subscriber station (SS)* ke *base station (BS)*.

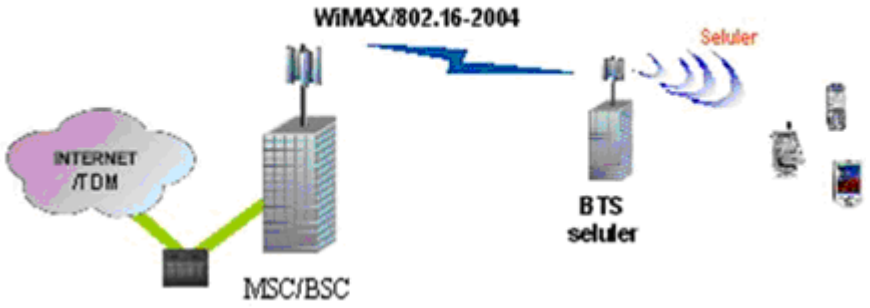
2. *Base station* akan menerima sinyal dari berbagai pelanggan dan mengirimkan pesan melalui *wireless* atau kabel ke *switching center* melalui protokol IEEE 802.16.

3. *Switching center* akan mengirimkan pesan ke *internet service provider (ISP)* atau

4. public switched telephone network (PSTN).

10.1.13 Aplikasi Wi-MAX

Wi-MAX dapat dimanfaatkan untuk backhaul Wi-MAX itu sendiri, backhaul Hotspot dan backhaul teknologi lain. Dalam konteks Wi-MAX sebagai backhaul dari Wi-MAX aplikasinya mirip dengan fungsi BTS sebagai repeater untuk memperluas jangkauan dari Wi-MAX. Sedangkan sebagai backhaul teknologi lain, Wi-MAX dapat digunakan untuk backhaul seluler. Juga Kalau biasanya hotspot banyak menggunakan saluran ADSL sebagai backhaulnya, namun karena keterbatasan jaringan kabel, maka Wi-MAX dapat dimanfaatkan sebagai backhaul hotspot.



Gambar 10-129 Wi-MAX Sebagai Backhaul Selular

Wi-MAX dapat digunakan sebagai ”Last Mile” teknologi untuk melayani kebutuhan broadband bagi pelanggan. Dari pelanggan perumahan maupun bisnis dapat dipenuhi oleh teknologi Wi-MAX ini.

Wi-MAX sebagai penyedia layanan personal broadband dapat dimanfaatkan untuk dua 2 pangsa pasar yaitu yang bersifat nomadic dan mobile. Untuk solusi nomadic, maka biasanya tingkat perpindahan dari user Wi-MAX tidak sering dan kalaupun pindah dalam kecepatan yang rendah. Perangkatnya pun biasanya tidak sesimpel untuk aplikasi mobile. Untuk aplikasi

mobile, pengguna layanan Wi-MAX melakukan mobilitas layaknya menggunakan terminal WiFi seperti notebook, PDA atau smartphone.

10.2 Wi-MESH

10.2.1 Pendahuluan

Jaringan Mesh adalah suatu cara untuk mengarahkan data, suara dan instruksi antar nodes. Hal ini merupakan koneksi lanjutan dan juga "hopping" dari node-to-node sampai dengan tujuannya tercapai. Jarinagn Mesh, semua nodes dihubungkan satu sama lain dalam satu jaringan. Mesh berbeda dari jaringan lainnya, dalam arti bahwa seluruh bagian komponen dapat dihubungkan satu sama lain dengan berbagai hops, dan umumnya tidak mobile. Mesh dapat dilihat sebagai salah satu jenis ad-hoc. Mobile ad-hoc networking (MANet), dan yang kemudian saling berhubungan, tetapi jaringan mobile ad-hoc juga harus berhadapan dengan permasalaha mobilitas dari node. Jarinagn mesh self-healing dimana suatu jaringan masih dapat beroperasi bahkan ketika suatu node break down atau tidak ada koneksi sama sekali.

Sebuah jaringan Wi-Mesh didesain untuk memperluas jangkauan jaringan Wi-Fi di dalam dan di luar ruangan secara jarak jauh. Caranya dengan membiarkan banyak *access point* saling menghantarkan lalu lintas data *acces point* yang berbeda-beda. Jika Wi-Fi *hotspot* memerlukan koneksi langsung ke internet, jaringan *mesh* melanjutkan permintaan data sampai koneksi jaringan ditemukan.

10.2.2 Prinsip Kerja Wi-Mesh

Dimana internet kebanyakan berbasis kabel, infrastruktur komunikasi elektronik kooperatif serupa dengan persetujuan yang berhubungan dengan pos internasional, pesan-pesan dikirimkan satu sama lain dan disiarkan di daerah-daerah terpisah secara gratis (yaitu. jika kamu menyiarkan ulang pesan-pesan yang terkirim di dalam daerah mu maka pesan tersebut akan disiarkan ulang di dalam daerahmu), Mesh adalah satu infrastruktur komunikasi kooperatif wireless antar satu jumlah besar dari individu transceiver wireless (yaitu. satu wireless mesh) itu sudah Eternet.

Infrastruktur jenis ini dapat didesentralisasi (dengan tidak ada server pusat) untuk aplikasi yang tidak berubah atau dikontrol secara terpusat untuk aplikasi yang tidak berubah (dengan satu server), keduanya adalah relatif murah, dan sangat dapat dipercaya dan resilent, selama masing-masing node hanya membutuhkan transmit sejauh node berikutnya. Node-node bertindak sebagai repeter untuk tarnsmit data dari node terdekat untuk peer yang terlalu jauh untuk jangkauan, menghasilkan satu jaringan yang dapat memutar jarak-jarak besar. Jaringan mesh juga sangat dapat dipercaya, ketika masing-masing node dihubungkan sampai beberapa node lain. Jika satu jaringan node putus, dalam kaitan dengan kegagalan perangkat keras atau alasan lain, maka neighbournya hanya temukan route lain. Kapasitas besar dapat diinstall oleh banyak node. Jaringan mesh boleh menggunakan peralatan fixed atau peralatan mobile. Solusi-solusi adalah sama ketika berkomunikasi di dalam situasi sulit seperti situasi-situasi keadaan

darurat, memesang tunnel dan oil ring sampai aplikasi video gerak kecepatan tinggi dan kecepatan aplikasi vidio mobile pada public transport.

Prinsipnya adalah sama dengan cara pengiriman paket-paket melalui kabel internet — data akan hop dari satu alat ke alat yang lain sampai ke satu tujuan yang diberi. Kemampuan pe-rute-an dinamik tercakup di masing-masing alat. Untuk menerapkan kemampuan pe-rute-an dinamik seperti itu, setiap peralatan memerlukan untuk menginformasikan rotingnya kesetiap perangkat yang terhubung dengannya. Masing-masing alat kemudian menentukan apa yang akan dilakukan dengan data yang diterima — melewatkan ke alat berkutnya atau menyimpannya. Routing algoritma yang digunakan selalu memastikan bahwa pengambilan data cepat sampai ke tujuan.

Pilihan dari teknologi radio untuk jaringan wireless mesh adalah rumit. Dalam suatu laptop-laptop dimana jaringan wireless secara sederhana dihubungkan untuk single access point, masing-masing laptop harus berbagi satu kolam yang ditetapkan dari bandwidth. Dengan teknologi mesh dan radio adaptip, peralatan dalam suatu jaringan mesh hanya dihubungkan dengan alat-alat lain yang ada dalam satu range. Keuntungannya adalah, seperti satu sistem penyeimbangan beban, semakin peralatan semakin banyak bandwidth yang tersedia, dengan ketentuan bahwa banyaknya hop di dalam rata-rata jalur komunikasi tetap rendah.

10.2.3 Membangun Wi-Mesh dari WLAN

Secara fisik menghubungkan access point wireless pada infrastruktur jaringan wired bisa jadi salah satu tugas yang paling menantang dan mahal yang berhubungan dengan suatu penyebaran wireless LAN. Dalam organisasi dengan system pengkabelan yang terstruktur fleksibel, itu hanyalah suatu pelengkap nuisance, tapi dalam suatu kampus yang terbagi-bagi, kompleks perumahan atau kotamadya, menarik kabel ke setiap acces point hampir mustahil.

Pada lingkungan terbagi-bagi, jaringan mesh bisa jadi pertimbangan. Sebagai pengganti backhaul lalu-lintas Wi-Fi melewati suatu kabel Ethernet yang dikoneksikan ke switch, kita dapat backhaul secara wireless. Jaringan mesh bukanlah konsep yang baru. Standard 802.11 termasuk ketentuan untuk WDS (wireless distribution system) yang saling menghubungkan AP melalui radio sebagai pengganti kabel. Tetapi WDS menawarkan kemampuan terbatas dibandingkan dengan modern mesh systems (didesain khusus hanya untuk mengkoneksiksn dua AP secara wireless), jadi kelompok kerja IEEE 802.11s mengembangkan standard mesh yang baru, bertujuan untuk penyelesaian pada tahun 2007.

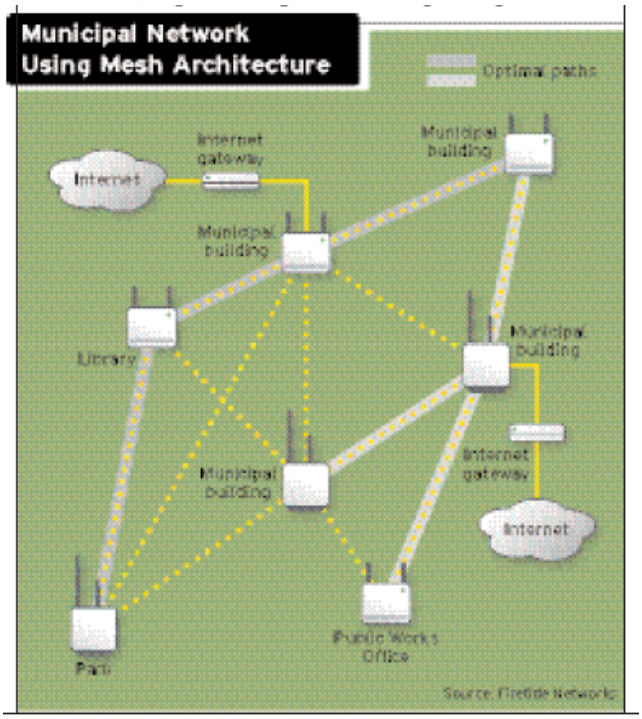
Pada wireless mesh, masing-masing wireless node jaringan bisa menjadi peserta aktif dalam sebuah mesh.. Mesh yang khusus secara teoritis menyediakan cakupan luas dengan biaya yang paling rendah. Tetapi, karena node bisa tampak dan menghilang pada waktu tertentu, jenis dari mesh ini tidak sesuai untuk banyak aplikasi. Suatu infrastruktur mesh, di mana mesh meneruskan pengiriman jasa wireless backhaul/backbone, biasanya lebih menyebar.

Pada jaringan wired dapat mengambil jalur alternative melewati mesh. Mesh node mengoptimisasi jalur-jalur tersebut. Arsitektur wimesh ini hampir sama dengan wired mesh yang digunakan pada internet, dimana router membuat keputusan forwarding menggunakan

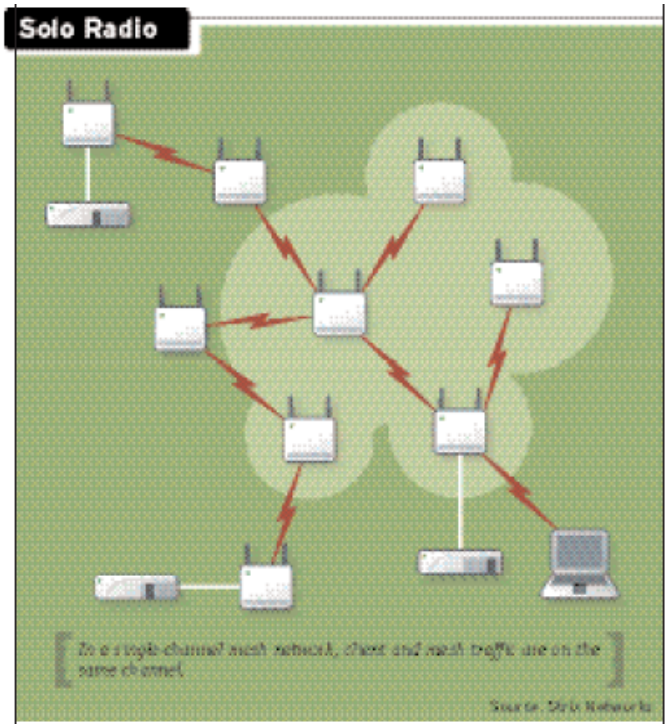
dynamic routing protocol. Dalam kedua kasus, jalur khusus dimana paket-paket melewati titik intermediate, adalah transparan di sisi client. Banyak faktor, termasuk level trafik, kapasitas link, efisiensi routing-protocol dan overhead, dapat berpengaruh terhadap seluruh performansi. Jaringan dengan diameter kecil (small hop counts) secara umum akan mempunyai throughput dan karakteristik latency lebih baik daripada jaringan dengan diameter besar, dimana pengalaman suatu performance hit untuk setiap intermediate hop. Untuk mengatasi ini, kemungkinan diinginkan suatu koneksi mesh backhaul yang cepat dan dedicated.

10.2.4 Pemilihan Desain Wi-Mesh

Meski beberapa system mesh membatasi diri untuk menyediakan layanan backbone wireless, sebagian besar menyediakan suatu kombinasi dari backbone/infrastruktur dan layanan client access. Oleh karena itu, suatu client Wi-Fi dapat berkoneksi ke sebuah node yang secara simultan berperan sebagai sebuah perangkat infrastruktur untuk backbone mesh. Dalam sistem ini, mesh node harus menghandle standard akses Wi-Fi (biasanya 802.11 b/g tapi terkadang 802.11 a dengan baik), ingress traffic dari titik mesh lainnya, egress traffic ke titik mesh lain dan, dalam beberapa kasus, sebuah koneksi Ethernet ke jaringan kabel/wired.



Desain wireless mesh yang paling sederhana menggunakan sebuah single-radio untuk akses, ingress dan egress. Karakteristik distinguish-nya sederhana dan biaya rendah, dalam sebuah desain single-radio, baik akses client maupun komunikasi antara titik-titik mesh mengambil tempat melebihi satu radio, yang secara dinamis bertukar fungsi dari AP-node ke mesh-node (lihat bagan “Solo radio” di bawah).



Sistem ini, secara tipikal menggunakan 2.4 GHz 802.11b/g, adalah sistem yang sedikit mahal untuk disebarkan, tetapi sistem menawarkan pembatasan performance dan kapasitas. Itulah sebabnya single-radio dalam setiap titik mesh harus time-slice antara akses client, ingress dan egress. Untuk mengatasi pembatasan ini, jaringan harus didesain untuk meminimalisasi penghitungan hop. Jadi sekitar sepertiga sampai setengah dari seluruh titik mesh juga harus mempunyai koneksi ke jaringan kabel, secara direct melalui Ethernet atau melalui suatu dedicated point-to-point, atau point-to-multipoint, sistem fixed wireless backhaul. Lebih besar lagi, jaringan mesh single-radio secara tipikal disebarkan dalam konjungsi dengan 5 GHz sistem multipoint wireless backhaul dari Alvarion atau Motorola. Itu dapat berarti biaya yang lebih tinggi sebaik komplikasi manajemen jaringan.

Jaringan wireless mesh yang lebih canggih menggunakan suatu desain multiradio, memisahkan akses, fungsi ingress dan egress. Dalam suatu desain two-radio, trafik akses client mengambil tempat pada satu kanal radio (biasanya 2.4 GHz 802.11b/g) sementara trafik mesh infress/egress menggunakan sebuah kanal berbeda (biasanya 5 GHz 802.11a). dengan memisahkan akses dan fungsi mesh, desain dual radio menawarkan beberapa performansi dan keuntungan desain.

Didapatkan suatu peningkatan dalam keseluruhan kapasitas sistem dan alokasi yang lebih fleksibel dari kanal RF. Perdagangan berhenti, meski begitu,sistem dual-radio cenderung untuk menghabiskan banyak biaya daripada sistem single-radio, karena hardware untuk setup dual-radio lebih mahal dan umumnya rely pada 5 GHz untuk komunikasi mesh.

Sinyal-sinyal ini teratenuasi berat oleh gedung-gedung dan dedaunan dari pohon, jadi dibutuhkan lebih banyak titik mesh untuk sistem seperti ini daripada sistem single-radio, desain

2.4 GHz. Dan penyebarannya membutuhkan rancang bangun radio-link yang lebih kompleks untuk memastikan LOS antara titik-titik mesh.

Yang terakhir dan desain jaringan mesh yang paling canggih dan yang bisa dibantah menggunakan tiga atau lebih radio per titiknya. Radio-radio tambahan ini dapat digunakan utnutk dua tujuan. Pertama, dapat membuat suatu system akses multisector dan/atau multikanal dengan antenna directional untuk menambah range dan menyediakan kapasitas akses client lebih besar. Kedua, dapat mengoptimalisasi trafik mesh dengan memisahkan trafik ingress dan egress pada kanal radio yang berbeda. Multiradio ini menawarkan performansi yang sangat baik, tapi butuh lebih banyak biaya dan kompleks penginstalannya.

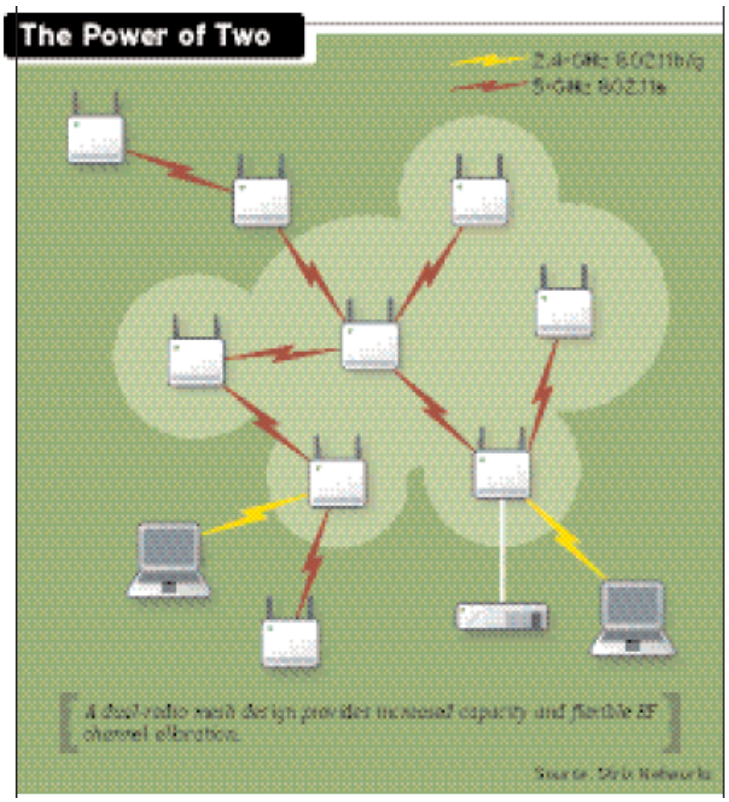
Agar diingat bahwa menambah banyak radio ke suatu titik mesh tidak selalu menjamin kinerja yang superior. Itu karena factor-faktor lain, termasuk efisiensi radio, routing protocol, dan diameter mesh, juga kontribusi ke performansi. Pada umumnya, bagaimanapun juga, semakin banyak radio menerjemahkan ke performansi dan kapasitas yang lebih baik sekalipun hanya pada biaya yang lebih tinggi.

10.2.5 MIX dan MASH

Karena belum ada standard wireless mesh, interoperability antar sistem dari berbagai vendor yang berbeda dibatasi. Secara teoritis memungkinkan untuk membangun jaringan mesh besar menggunakan gear dari banyak vendor, tetapi kebanyakan organisasi memilih untuk suatu vendor tunggal. Karena popularitas dari wireless mesh meningkat, kebutuhan akan interoperability akan meningkat dengan baik. Hal ini benar sekali untuk sistem yang dirancang untuk pasar konsumen, dimana kesenangan dalam instalasi adalah sebuah kunci yang dibutuhkan.

Kelompok kerja IEEE 802.11 memulai pertimbangan proposal dari suatu perluasan mesh ke standard 802.11 pada bulan Juli. Proposal terkemuka, yang diterima dari 83 persen oleh pemilih, dikenal dengan SEEMesh (Simple, Efficient, and Extensible Mesh). SEEMesh digawangi oleh suatu kelompok besar high-profile vendor termasuk Intel, Motorola, Nokia, NTT DoCoMo, dan Texas Instruments. Keterangan lebih rinci mengenai proposal ini tidak tersedia untuk sementara waktu, tetapi diorientasikan untuk membuat standarisasi kemampuan mesh yang tersedia untuk pasar konsumen yang mungkin luas.

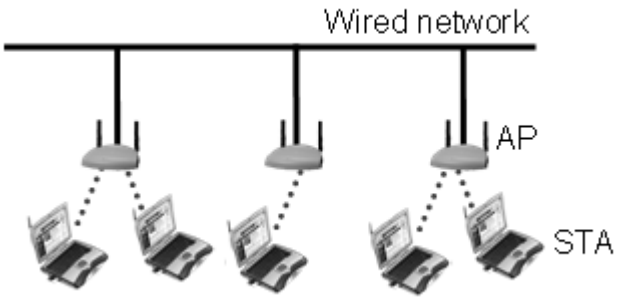
Dekat di belakang (dengan selisih 76 persen dari pemilih) adalah suatu proposal yang disubmit oleh Wi-Mesh Aliance, yang termasuk Accton, Nexthop, Nortel dan Philips. Proposal Wi-Mesh mengalamatkan suatu cakupan kebutuhan lebih luas, termasuk kedua desain elemen single dan multi-radio, kualitas servis (QoS) dan peningkatan keamanan. Keterangan lebih rinci dari proposal tersebut, tersedia di www.wi-mesh.org.



10.2.6 Pengembangan Wi-Mesh

Dalam pengembangan WLAN, terdapat perbedaan yang jelas diantara peralatan infrastruktur dan yang berada di clien untuk bisa bergabung dalam WLAN. Peralatan infrastruktur WLAN dikembangkan berdasarkan standar 802.11 AP yang menyediakan beberapa service, khususnya dukungan terdapat penghemtan daya peralatan, untuk menyimpan trafik, services autentifikasi dan menggunakan jaringan

AP biasanya langsung terhubung jaringan kabel, dan menyediakan layanan konektifitas wireless kepada peralatan client melebihi konektifitas peraltan wireless itu sendiri. Perlatan client, dengan kata lain, di implementasikan sebagai 802.11 yang harus digabungkan dengan AP dalam access gain ke jaringan. STA tergantung pada AP yang tehubung untuk berkomunikasi. Model pengembangan WLAN dan peralatannya diilustrasikan dalam gambar berikut :



Gambar 10-130 Model pengembangan 802.11 dan peralatannya

Tidak ada alasan, akan tetapi, banyak peralatan yang digunakan dalam WLAN tidak dapat mendukung conektivitas wireless secara fleksibel. Infrastruktur peralatan seperti AP harus bisa menetapkan peer-to-peer wireless dengan AP berdekatan untuk menetapkan satu infrastruktur mesh backhaul, tanpa memerlukan kabel jaringan yang dikoneksikan ke masing-masing AP. Biasanya, peralatan lama yang dikategorikan sebagai client perlu juga ditetapkan peer-to-peer wireless dengan clientnhya dan AP pada jaringan mesh. Dalam beberapa hal, perangkat client mesh-enable ini menyediakan layanan yang sama seperti AP untuk membantu menetapkan STA access gain pada jaringan.

Tujuan arsitektur disini peralatan wireless dibagi dalam dua kelas utama : nodes klas mesh adalah node-node yang mampu melayani mesh, sedangkan klas non-mesh meliputi client STA. Node-node klas mesh bisa secara optimal memdukung layanan AP dan bisa diatur atau tidak.

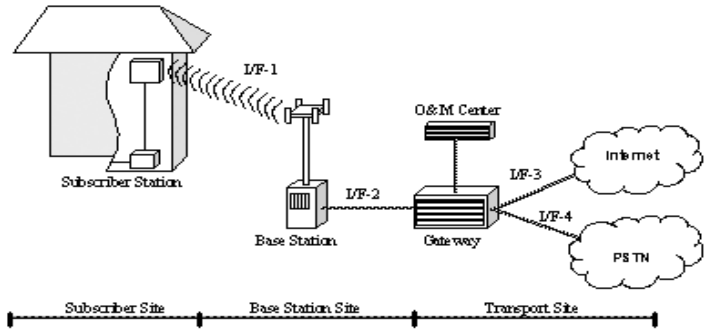
Layanan mesh bisa diimplementasikan sebagai interface MAC yang tidak tergantung pada 802.11 MAc. Prinsipnya, peralatan tunggal bisa dimainkan dari fungsi kedua point mesh dan AP atau fungsi dari kedua ponit mesh dengan STA. Singkatnya bagaimana cara merealisasikan peralatan multi-role.

10.3 SOAL dan JAWABAN

1. Jelaskan apa yang dimaksud dengan Wi MAX dan jelaskan prinsip kerjanya secara singkat.
2. Sebutkan standard yang dipakai pada Wi-MAX serta sebutkan perbedaannya dengan standard WLAN.
3. Jelaskan apa yang dimaksud dengan WiMESH dan jelaskan secara singkat prinsip kerjanya.
4. Gambarkan konfigurasi Wi-MAX dan beri penjelasan singkat.
5. Bagaimana cara membuat jaringan WiMESH dari WLAN?

JAWABAN

1. Wi-MAX *(Worldwide Interoperability for Microwave Access)* adalah standar *Broadband Wireless Access* dengan kemampuan menyediakan layanan data berkecepatan tinggi.
   Prinsip kerjanya : Teknologi *Wi-MAX* dapat meng-*cover* area sekitar 50 kilometer, dimana ratusan pelanggan akan di-*share* sinyal dan kanal untuk mentransmisikan data dengan kecepatan sampai 155 Mbps
2. Standard yang digunakan pada Wi-MAX adalah IEEE 802.16.
   Yang membedakan antara 802.16 dengan 802.11 adalah *Wi-MAX* mempunyai tingkat kecepatan *transfer* data yang lebih tinggi dengan jarak yang lebih jauh, sehingga kualitas layanan dengan menggunakan komunikasi ini dapat digolongkan ke dalam kelas *broadband.*
3. WiMESH adalah suatu cara untuk mengarahkan data, suara dan instruksi antar nodes.
   Prinsip kerjanya : dengan cara mengirimkan paket-paket melalui kabel internet dimana data akan dihop dari satu alat ke alat yang lain sampai ke satu tujuan yang diberi.

4. 

Subscriber station terletak di lingkungan pelanggan (bisa *fixed* atau *mobile/portable*). Sedangkan base station biasanya satu lokasi dengan jaringan operator (jaringan IP/internet atau jaringan TDM/PSTN).

5. Pada jaringan wired dapat mengambil jalur alternatif melewati MESH. Mesh node mengoptimisasi jalur tersebut.

10.4 REFERENSI

1. Siyamta, ***Sistem Keamanan pada Worldwide Interoperability for Microwave Access (Wi-MAX)***, Institut Teknologi Bandung, Bandung, 2004
2. _____, ***Wi-MAX Wordwide Interoperability for Microwave Access***, Inti edisi 2006.
3. _____, ***Wi-MAX dan DSL : Musuh atau Teman ?***, http://www_ristishop_com/image/article/DSL4_gif.htm
4. _____, ***Wi-MAX,*** *http://*wikipedia.com/ensiklopedia bebas berbahasa Indonesia.htm
5. _____, ***Capacity of Wireless Mesh Network***, BelAir Network 2006
6. J.Sharpe Smith Vol.3 , ***Enterprise Embraces Wi-Mesh***, EWM, 2007.
7. Dave Molta, ***Make A Mesh of Your WLAN***, http://www.nwc.com/Inetwork Computing, 2005.