BAB 2
TINJAUAN PUSTAKA

2.1 Profil Instansi

BBKPM Bandung didirikan pada Bulan November Tahun 1952, dengan nama BP5 (Balai Penyelidikan dan Pemberantasan Penyakit Paru-Paru) dengan tujuan sebagai pusat pemberantasan penyakit tuberculosis (TB). BP5 Bandung menempati gedung di Jl. Ir. H. Juanda 45 kemudian pindah ke Jl. Pasir Kaliki 121. Gedung BBKPM yang saat ini menjadi lokasi BBKPM Bandung mulai ditempati pada bulan Juli tahun 1955.

Pada tahun 1974, BP5 berubah menjadi BP4 (Balai Pengobatan Penyakit Paru-Paru) dan mengacu pada Keputusan Menteri Kesehatan RI No.144/Menkes/SK/IV/1978 tentang Susunan Organisasi dan Tata Kerja Balai Pengobatan Penyakit Paru-Paru yang di dalamnya mengatur tugas, fungsi, klasifikasi dan Susunan Organisasi BP4, maka tugas pokok dan fungsi BP4 tidak hanya mengobati tuberkulosis tetapi juga penyakit paru lainnya.

Lokasi BBKPM Bandung di Jalan Cibadak No 214 Bandung menempati bangunan seluas 3.641 m^2 yang berdiri diatas tanah seluas 3.330 m^2, BKPM Garut Jl. Rumah Sakit Umum Dokter Slamet No. 13 Garut menempati bangunan seluas 246 m^2 yang berdiri diatas tanah seluas 1.704 m^2, dan BKPM Cianjur Jalan Jl. Siliwangi No. 15 Cianjur adalah bangunan seluas 662 m^2 yang berdiri diatas tanah seluas 2.450 m^2.

Dalam menjalankan tugas pokok BBKPM Bandung jelas memilikikarakteristik berbeda dengan rumah sakit ataupun layanan kesehatan lain, selain secara spesialistik menangani penyakit paru sebagai layanan dan rujukan juga memiliki program pemberdayaan kesehatan paru masyarakat, dengan layanan unggulan:

1. Pusat pelayanan dan rujukan kesehatan paru masyarakat, artinya BBKPM melakukan pelayanan yang menyeluruh terhadap kesehatan paru masyarakat dengan dilengkapi fasilitas sumber daya yang memadai, kompeten

berkualitas dan bersifat spesialistik untuk mendukung peningkatan derajat kesehatan paru masyarakat.

2. Pusat pemberdayaan masyarakat dan promosi kesehatan paru masyarakat, artinya BBKPM membuat pengkajian dan penerapan model-model pemberdayaan masyarakat disertai pengembangan media dan kegiatan promosi kesehatan yang terpadu untuk memandirikan masyarakat dalam menjaga kesehatan parunya dan untuk mendukung peningkatan derajat kesehatan paru masyarakat.

3. Pusat jejaring kerjasama/kemitraan kesehatan paru masyarakat, artinya BBKPM melakukan koordinasi dan menggerakkan institusi lain dalam mengatasi kesehatan paru masyarakat untuk mendukung peningkatan derajat kesehatan paru masyarakat.

4. Pusat pendidikan dan pelatihan kesehatan paru masyarakat, artinya BBKPM menjadi tempat pendidikan dan pelatihan kesehatan paru masyarakat bagi tenaga kesehatan dan non kesehatan untuk mendukung peningkatan derajat kesehatan paru masyarakat.

5. Pusat penelitian dan pengembangan khatan paru masyarakat, artinya BBKPM menjadi tempat penelitian dan pengembangan kesehatan paru masyarakat bagi tenaga kesehatan dan non kesehatan untuk mendukung peningkatan derajat kesehatan paru masyarakat.

2.1.1 Logo BBKPM Bandung

Dibawah ini adalah logo BBKPM (Balai Besar Kesehatan Paru Masyarakat)

Gambar 2.1 Logo BBKPM Bandung

2.1.2 Badan Hukum

Merujuk pada Kep.Men.PAN No.62/KEP/M.PAN/7/2003 tentang Pedoman Organisasi Unit Pelaksana Teknis di Lingkungan Departemen dan Lembaga Pemerintah Non Departemen, yang ditindaklanjuti dengan Peraturan Menteri Kesehatan RI Nomor: 1352/MENKES/PER/IX/2005 tentang Organisasi dan Tata Kerja Unit Pelaksana Teknis di Bidang Kesehatan Paru Masyarakat, menetapkan BP4 Bandung sebagai Balai Kesehatan Paru Masyarakat (BKPM) eselon 3b.

Pada tahun 2007 melalui Surat Keputusan Menteri Kesehatan Republik Indonesia Nomor: 532/MENKES/PER/IV/2007 BKPM Bandung selanjutnya ditetapkan menjadi Balai Besar Kesehatan Paru Masyarakat (BBKPM) eselon 2b, dengan Tugas Pokok dan Fungsi melaksanakan pelayanan kesehatan rujukan paru spesialistik dan atau subspesialistik yang berorientasi kesehatan masyarakat; pemberdayaan masyarakat dalam bidang kesehatan paru; kemitraan dan pengembangan sumber daya di bidang kesehatan paru masyarakat; pendidikan dan pelatihan teknis di bidang kesehatan paru; serta penelitian dan pengembangan kesehatan paru. Di dalam surat keputusan tersebut juga dinyatakan bahwa wilayah kerja BBKPM Bandung meliputi 13 Provinsi yaitu seluruh Provinsi di Pulau Sumatera, Provinsi Jawa Barat, Provinsi Banten dan Provinsi DKI Jakarta. Selain berlokasi di Kota Bandung, BBKPM Bandung memiliki dua buah unit fungsional yang berada di Cianjur dan Garut, yang melayani kesehatan paru masyarakat di kedua wilayah tersebut, namun tetap berada dalam satu satuan kerja BBKPM Bandung.

2.2 Landasan Teori

2.2.1 Jaringan Komputer

Jaringan komputer adalah sekumpulan komputer otonom yang terinterkoneksi oleh teknologi yang sama dan dapat saling bertukar informasi [4]. Koneksi dapat menggunakan media kawat tembaga, serat optik, gelombang mikro, sinar inframerah ataupun menggunakan komunikasi satelit [4].

Untuk membuat jaringan komputer, switch dan router menggunakan berbagai protokol dan algoritma untuk bertukar informasi dan untuk membawa data ke titik akhir yang diinginkan. Setiap titik akhir (kadang disebut host) dalam jaringan memiliki pengenal unik, sering kali alamat IP atau alamat Media Access Control yang digunakan untuk menunjukkan sumber atau tujuan transmisi [4]. Endpoint dapat mencakup *server*, komputer pribadi, telepon, dan berbagai jenis hardware jaringan.

Jaringan komputer juga mungkin dibuat dengan menggunakan gabungan teknologi kabel dan wireless. Perangkat jaringan berkomunikasi melalui medium transmisi kabel atau wireless. Untuk jaringan yang menggunakan kabel, Anda mungkin membutuhkan optical fiber, coaxial cable, atau kabel tembaga [4]. Sementara itu, jalur jaringan wireless termasuk jaringan komputer yang menggunakan koneksi data wireless untuk menghubungkan titik akhir. Titik akhir ini termasuk radio siaran, radio seluler, microwave, dan satelit.

Jaringan bisa menjadi private atau publik. Jaringan private biasanya memerlukan user untuk memasukkan kredensial untuk mengakses jaringan [4]. Biasanya, ini diberikan secara manual oleh administrator jaringan atau diperoleh langsung oleh pengguna melalui kata sandi atau dengan kredensial lainnya. Jaringan publik seperti internet tidak membatasi akses.

2.2.2 TCP/IP

TCP dan IP merupakan salah satu standar protokol yang dirancang untuk melakukan fungsi-fungsi komunikasi data dalam jaringan internet. TCP/IP terdiri atas sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dalam komunikasi data [4]. Dengan prinsip ini maka tugas masing-masing protokol menjadi jelas dan sederhana, sehingga mudah untuk diimplementasikan di seluruh perangkat dan perangkat lunak jaringan dan juga mudah dalam melakukan proses troubleshooting.

Dari beberapa macam protokol yang ada dalam TCP & IP, protokol IP merupakan inti dari protokol TCP & IP. Seluruh data yang berasal dari lapisan diatas IP harus dilewatkan, diolah oleh protokol IP dan kemudian

dikirimkan sebagai paket IP ke tujuan. Dalam melakukan pengiriman paket, protokol IP bersifat *unreliable*, *connectionless* dan *datagramdelivery service*. Saat ini terdapat dua versi dari protokol IPv4 (32 bit) dan IPv6 (128 bit). *Unreliable* berarti protokol IP tidak menjamin datagram yang dikirim pasti sampai di tujuan [4]. Protokol IP hanya berusaha sebaik mungkin untuk membawa *datagram* sampai ke tujuan. *Connectionles*s berarti dalam mengirim paket ke tujuan tidak ada perjanjian terlebih dahulu (*handshake*). *Datagramdelivery service* berarti paket data yang dikirim independent terhadap paket data yang lain [4].

2.2.3 IP Address

(Internet Protocol Address atau sering disingkat IP) adalah deretan angka biner antara 32 bit sampai 128 bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet. Pengiriman data dalam jaringan TCP/IP berdasarkan IP address komputer pengirim dan komputer penerima. IP address memiliki dua bagian, yaitu alamat jaringan (network address) dan alamat komputer lokal (host address) dalam sebuah jaringan.

Alamat jaringan digunakan oleh router untuk mencari jaringan tempat sebuah komputer lokal berada, sementara alamat komputer lokal digunakan untuk mengenali sebuah komputer pada jaringan lokal. Panjang dari angka ini adalah 32 bit (untuk IPv4 atau IP versi 4), dan 128 bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan Internet berbasis TCP/IP. Sistem pengalamatan IP ini terbagi menjadi dua, yakni:

1. **Ipv4**

Model pengalamatan dalam IPv4 menggunakan 32 bit bilangan biner. Namun untuk mempermudah penulisannya maka setiap delapan bit biner diwakili oleh satu segmen bilangan oktet, sehingga setiap alamat akan memiliki empat buah segmen dari 0.0.0.0 sampai dengan 255.255.255.255 misalnya 202.152.254.254 sehingga total alamat sebesar 232. Alamat IPv4 terbagi menjadi beberapa jenis, yakni sebagai berikut:

a) Alamat Unicast, merupakan alamat IPv4 yang ditentukan untuk sebuah antarmuka jaringan yang dihubungkan ke sebuah Internetwork IP. Alamat Unicast digunakan dalam komunikasi point-to-point atau one-to-one.

b) Alamat Broadcast, merupakan alamat IPv4 yang didesain agar diproses oleh setiap node IP dalam segmen jaringan yang sama. Alamat broadcast digunakan dalam komunikasi one-to-everyone.

c) Alamat Multicast, merupakan alamat IPv4 yang didesain agar diproses oleh satu atau beberapa node dalam segmen jaringan yang sama atau berbeda. Alamat multicast digunakan dalam komunikasi *one-to-many*.

Kelas Alamat IP	Oktet pertama (desimal)	Oktet pertama (biner)	Digunakan oleh
Kelas A	1–126	0xxx xxxx	Alamat unicast untuk jaringan skala besar
Kelas B	128–191	1xxx xxxx	Alamat unicast untuk jaringan skala menengah hingga skala besar
Kelas C	192–223	110x xxxx	Alamat unicast untuk jaringan skala kecil
Kelas D	224–239	1110 xxxx	Alamat multicast (bukan alamat unicast)
Kelas E	240–255	1111 xxxx	Direservasikan;umumnya digunakan sebagai alamat percobaan (eksperimen); (bukan alamat unicast)

Gambar 2.2. Alamat *Unicast* IP versi 4.

Alamat IPv4 dibagi menjadi dua bagian yaitu alamat jaringan (network address) dan alamat komputer (host address). Network address digunakan untuk menunjukkan di jaringan mana komputer berada, sedangakan “host address” menunjukkan komputer tersebut dalam jaringannya tersebut.

2. Ipv6

IPv6 atau IPng (Internet Protocol Next Generation) dirancang sebagai perbaikan dari internet protocol yang digunakan sekarang yaitu IPv4. IPv6 dapat diinstall seperti mengupgrade software biasa dan dapat dioperasikan bersama-sama dengan IPv4. IPv6 dirancang untuk bekerja dengan baik pada jaringan dengan perfomansi tinggi dan juga efisien untuk jaringan dengan bandwidth yang kecil seperti wireless. IPv6 juga menyediakan platform untuk fungsi-fungsi baru pada internet yang akan dibutuhkan di masa depan [14]. IPv6 dirancang sebagai perbaikan dari IPv4, dan bukan merupakan perubahan yang ekstrem dari IPv4. Sama seperti halnya IPv4, IPv6 juga mengizinkan adanya DHCP *Server* sebagai pengatur alamat otomatis. Jika dalam IPv4 terdapat dynamic address dan static address, maka dalam IPv6,

konfigurasi alamat dengan menggunakan DHCP *Server* dinamakan dengan stateful address configuration, sementara jika konfigurasi alamat IPv6 tanpa DHCP *Server* dinamakan dengan stateless address configuration.

Seperti halnya IPv4 yang menggunakan bit bit pada tingkat tinggi (high-order bit) sebagai alamat jaringan sementara bit bit pada tingkat rendah (low-order bit) sebagai alamat host, dalam IPv6 juga terjadi hal serupa. Dalam IPv6, bit bit pada tingkat tinggi akan digunakan sebagai tanda pengenal jenis alamat IPv6, yang disebut dengan Format Prefix (FP). Dalam IPv6, tidak ada subnet mask, yang ada hanyalah Format Prefix.

Dalam IPv6, alamat 128 bit akan dibagi ke dalam 8 blok berukuran 16 bit, yang dapat dikonversikan ke dalam bilangan heksadesimal berukuran 4-digit. Setiap blok bilangan heksadesimal tersebut akan dipisahkan dengan tanda titik dua (:). Karenanya, format notasi yang digunakan oleh IPv6 juga sering disebut dengan colon-hexadecimal format, berbeda dengan IPv4 yang menggunakan dotted-decimal format.

Berikut ini adalah contoh alamat IPv6 dalam bentuk bilangan biner:

```
00100001110110100000000011010011000000000000000000010111100111011000000101010101000000000111111111111111100001010001001110001011010
```

Untuk menerjemahkannya ke dalam bentuk notasi *colon-hexadecimal format*, angka-angka biner di atas harus dibagi ke dalam 8 buah blok berukuran 16 bit:

```
0010000111011010 0000000011010011 0000000000000000 0010111100111011 0000001010101010 0000000011111111 1111111000101000 1001110001011010
```

Lalu, setiap blok berukuran 16 bit tersebut harus dikonversikan ke dalam bilangan heksadesimal dan setiap bilangan heksadesimal tersebut dipisahkan dengan menggunakan tanda titik dua. Hasil konversinya adalah sebagai berikut:

```
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
```

Konvensi pengalamatan IPv6 juga mengizinkan penyederhanaan alamat lebih jauh lagi, yakni dengan membuang banyak karakter 0, pada sebuah

alamat yang banyak angka 0-nya. Jika sebuah alamat IPv6 yang direpresentasikan dalam notasi colon-hexadecimal format mengandung beberapa blok 16 bit dengan angka 0, maka alamat tersebut dapat disederhanakan dengan menggunakan tanda dua buah titik dua (::). Untuk menghindari kebingungan, penyederhanaan alamat IPv6 dengan cara ini sebaiknya hanya digunakan sekali saja di dalam satu alamat, karena kemungkinan nantinya pengguna tidak dapat menentukan berapa banyak bit 0 yang direpresentasikan oleh setiap tanda dua titik dua (::) yang terdapat dalam alamat tersebut. Tabel berikut mengilustrasikan cara penggunaan hal ini.

Alamat asli	Alamat asli yang disederhanakan	Alamat setelah dikompres
FE80:0000:0000:0000:02AA:00FF:FE9A:4CA2	FE80:0:0:0:2AA:FF:FE9A:4CA2	FE80::2AA:FF:FE9A:4CA2
FF02:0000:0000:0000:0000:0000:0000:0002	FF02:0:0:0:0:0:0:2	FF02::2

Gambar 2.3 Penyederhanaan Bentuk Alamat IP versi 6.

2.2.4 Mekanisme Transisi IPv4 ke IPv6

2.2.4.1 Pengertian Mekanisme Transisi IP

Mekanisme transisi secara umum didefinisikan sebagai sekumpulan teknik yang dapat diimplementasikan oleh node IPv6 untuk dapat kompatibel dengan node IPv4 yang sudah eksis sebelumnya. Berikut adalah beberapa mekanisme yang dikembangkan untuk transisi dari IPv4 ke IPv6 :

1. Tunneling.
2. Dual Stack.

2.2.4.2 Transisi Metode Tunneling

IPv4 dan IPv6 merupakan dua protokol yang berbeda. Oleh karena itu, host dengan alamat IPv4 tidak dapat berkomunikasi langsung dengan host IPv6. Metode tunneling merupakan suatu metode yang dapat digunakan dalam mengatasi permasalahan tersebut. Tunneling merupakan mekanisme enkapsulasi suatu network protocol ke dalam delivery protocol yang berbeda, sehingga pada penerapannya, paket-paket IPv6 dapat dilewatkan pada jaringan IPv4, begitu juga sebaliknya [3]. Mekanisme ini umumnya dicapai melalui Manual atau alat parameter berbasis entri, layanan yang ada

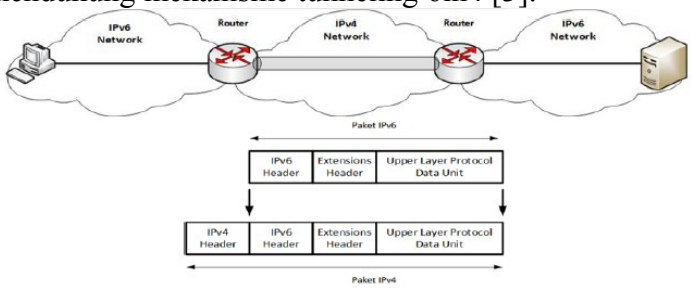
seperti DNS atau DHCP, atau dengan memperhatikan penggunaan informasi embedment ke alamat IP atau menerapkan alamat anycast IPv6.

Tunneling disebut juga sebagai enkapsulasi, yaitu mekanisme yang menggunakan tunnel traffic antara dua titik melalui proses enkapsulasi dan melewatkannya di atas jaringan IPv4 [19]. Mekanisme ini digunakan ketika dua node yang menggunakan protokol yang sama ingin berkomunikasi menggunakan jalur yang dimiliki protokol lain. Ada dua jenis tunneling, yaitu secara otomatis (automatic tunneling) dan secara terkonfigurasi (configured tunneling).

Perangkat jaringan dapat mencapai dua proses enkapsulasi dan dekapsulasi di endpoint tunnel. Secara umum, mekanisme tunneling adalah penyebaran sederhana dengan konfigurasi point-to-point [19]. Namun demikian, tunneling juga dapat diimplementasikan secara hierarkis dan berurutan. Hingga saat ini, terdapat metode tunneling yang berbeda seperti 6to4, ISATAP, Teredo, DSTM, dan 6over4. Tunneling dapat dikonfigurasi secara manual atau secara otomatis..Terdapat beberapa turunan metode dari Configured Tunneling diantaranya adalah :

1. 6 in 4 Tunneling

Tunneling 6in4 berarti enkapsulasi header IPv6 dalam header IPv4. Sedangkan sehingga paket-paket IPv6 dapat dikirim pada jaringan IPv4. Mekanisme ini telah distandarkan dalam IETF 2473. Configured tunneling 6in4 mengkoneksikan dua jaringan IPv6 secara point-to-point dengan penggunaan protocol 41. Tunneling 6in4 merupakan mekanisme yang paling umum digunakan saat ini, karena hampir seluruh perangkat jaringan maupun sistem operasi mendukung mekanisme tunneling 6in4 [3].

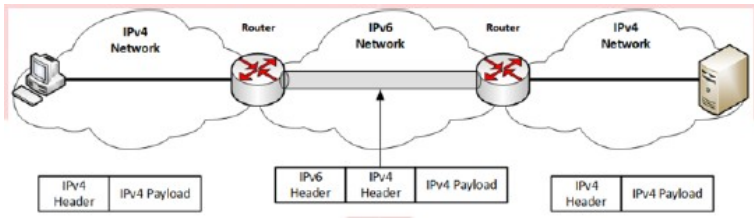


Gambar 2.4 Mekanisme 6 in 4 *Tunneling*.

2. 4 in 6 Tunneling

Merupakan kebalikan dari 6in4, tunneling 4in6 berarti enkapsulasi header IPv4 dalam header IPv6, sehingga paket-paket IPv4 dapat dikirim pada jaringan IPv6 secara point-to-point. Mekanisme ini telah distandarkan

pada IETF RFC 2473 [3]. Sama seperti tunneling 6in4, perbedaannya host tersebut menggunakan IPv4 akan berkomunikasi dengan *server* yang juga terletak di jaringan IPv4, namun pada jaringan backbone menggunakan IPv6.



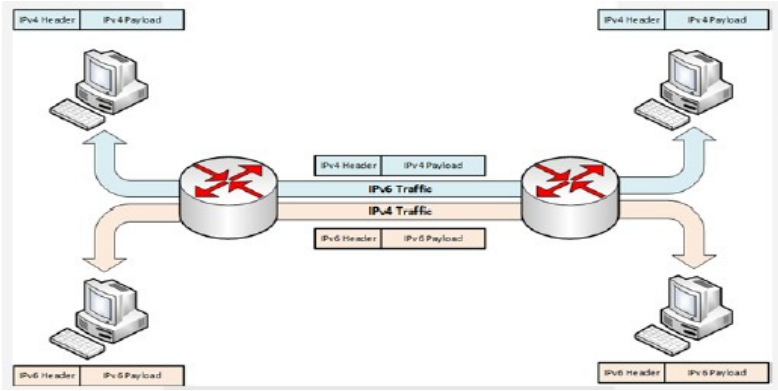
Gambar 2.5 Mekanisme 4 *in* 6 *Tunneling*.

2.2.4.3 Transisi Metode Dual Stack

Dual stack adalah sebuah metode transisi dari IPv4 menuju IPv6, yang di dalamnya telah disediakan dukungan terhadap IPv4 dan IPv6, jadi dalam metode ini akan mengirimkan dan menerima paket data dalam format IPv4 dan IPv6, dan dapat berjalan bersamaan dalam sebuah perangkat di semua protokol layer tanpa saling menggangu dan terpengaruh satu sama lainnya [3]. Metode dual stack diimplementasikan pada lapisan jaringan (network layer) untuk IPv4 dan IPv6. Sebelum mentransfer paket ke lapisan berikutnya, lapisan jaringan akan memilih mana yang akan digunakan berdasarkan informasi dari lapisan data link [5]. Jaringan perusahaan besar yang memutuskan untuk transit IPv6 dapat menerapkan metode dual-stack sebagai strategi dasar, yang melibatkan konfigurasi perangkat untuk dapat memanfaatkan IPv4 dan IPv6 pada saat yang sama pada router inti, perimeter router, firewall, *server*-farm, dan router akses desktop. Tergantung pada menanggapi permintaan DNS, aplikasi dapat memilih untuk menggunakan protokol dan pilihan ini dapat dibuat dalam harmoni dengan jenis lalu lintas IP. Selanjutnya, komputer host dapat mencapai kedua konten IPv4 yang tersedia dan konten IPv6. Dengan demikian, mekanisme dual stack menyajikan strategi transisi yang fleksibel.

Namun, seperti peraturan pada umumnya, penerimaan teknologi baru terletak pada cara mengintegrasikan ke dalam infrastruktur saat ini tanpa gangguan serius dari layanan. Sebuah jaringan perusahaan besar termasuk

banyak jaringan IPv4 dan ribuan node IPv4. Oleh karena itu, transisi dari IPv4 ke IPv6 tidak memerlukan upgrade pada semua node pada saat yang sama yaitu IPv4 dan IPv6 akan koneksi berdampingan untuk beberapa waktu. Akibatnya, perusahaan dapat menerapkan metode dual-stack untuk transit IPv6. Metode dual-stack secara harfiah menggunakan dua IPv4 dan IPv6 tumpukan untuk operasi secara bersamaan, yang memungkinkan perangkat untuk berjalan di kedua protokol, menurut layanan yang tersedia, ketersediaan jaringan, dan kebijakan administratif. Akibatnya, IPv4 memungkinkan program menggunakan IPv4 dan ini berlaku sama untuk IPv6. Header IP akan memainkan peran penting dalam menerima dan mengirimkan paket. Dengan kata lain, jenis transisi IPv6 adalah enkapsulasi IPv6 dalam IPv4. Transisi lengkap dapat dikelola oleh DNS (Domain Name *Server*), misalnya, dalam situasi yang perangkat ganda stacked query nama tujuan dan DNS memberikan alamat IPv4 (DNS "A" Record), ia akan mengirimkan paket IPv4, atau dalam kasus DNS merespon dengan alamat IPv6 (DNS "AAAA" Record), ia akan mengirimkan paket IPv6. Mekanisme ini saat ini pilihan terbaik untuk transisi karena banyak sistem operasi telah menerapkan IP ganda tumpukan protokol [18].



Gambar 2.6 Mekanisme *Dual Stack*.

Namun, meskipun fleksibilitas terbesar, masih ada beberapa masalah yang bersangkutan dengan metode ini seperti setiap perangkat dual -stack masih membutuhkan alamat IPv4; dua tabel routing harus dipertahankan di setiap router yaitu sebagai dual-stack (routing) harus dijalankan pada saat yang sama, memori tambahan dan power CPU akan diperlukan. Selain itu,

setiap jaringan membutuhkan protokol routing sendiri yaitu konsep keamanan tambahan dan aturan harus diatur dalam firewall akan cocok untuk setiap DNS dengan kemampuan untuk menyelesaikan IPv4 dan IPv6 [5]. akhirnya, semua program harus dapat memilih komunikasi lebih baik IPv4 atau IPv6, dan diperlukan perintah manajemen jaringan secara terpisah.

2.2.5 *Quality of Service*s

Quality of Service (*QoS*) merupakan deskripsi atau pengukuran kinerja keseluruhan suatu layanan, seperti jaringan telepon atau komputer atau layanan komputasi Cloud, terutama kinerja oleh pengguna jaringan [17]. Untuk mengukur kualitas layanan secara kuantitatif beberapa aspek terkait dari layanan jaringan sering dipertimbangkan, seperti tingkat kesalahan, kecepatan bit, *throughput*, *delay* transmisi, ketersediaan, jitter, dll.

Kinerja jaringan komputer dapat bervariasi akibat beberapa masalah, seperti halnya masalah bandwidth, latency dan jitter, yang dapat membuat efek yang cukup besar bagi banyak aplikasi [17]. Sebagai contoh, komunikasi suara (seperti VoIP atau IP Telephony) serta video streaming dapat membuat pengguna frustrasi ketika paket data aplikasi tersebut dialirkan di atas jaringan dengan bandwidth yang tidak cukup, dengan latency yang tidak dapat diprediksi, atau jitter yang berlebih. Fitur *Quality of Service* (*QoS*) ini dapat menjadikan bandwidth, latency, dan jitter dapat diprediksi dan dicocokkan dengan kebutuhan aplikasi yang digunakan di dalam jaringan tersebut yang ada.

Pengukuran performansi merupakan salah satu upaya dalam peningkatan efisiensi dan efektifitas kerja suatu jaringan guna meningkatkan produktifitas kerja pada jaringan [17]. Letak pengukuran performansi dalam suatu jaringan merupakan suatu performansi. Walaupun ada suatu nilai performansi, nilai tersebut hanyalah menggambarkan tingkat utilitas dari suatu performansi jaringan. Terdapat dua arsitektur utama dalam pengelolaan *QoS* dalam jairngan IP, yaitu :

2.2.5.1 Integrated Services (IntServ)

Bertujuan menyediakan sumberdaya seperti bandwidth untuk trafik dari end to end [15]. Ditujukan untuk aplikasi yang peka terhadap *delay* dan keterbatasan bandwidth seperti *video conference* dan VoIP. Arsitekturnya didasarkan pada system pemesanan sumber daya per aliran trafik. Sistem pemesanan sumber daya memerlukan protokol tersendiri. Salah satu protokol yang sering digunakan adalah RSVP. IntServ sesuai untuk VoIP 309 dan video tetapi sangat tidak tepat untuk aplikasi semacam web yang aliran trafiknya banyak tetapi datanya kecil [15].

Integrated Services menyediakan aplikasi dengan tingkat jaminan layanan melalui negosiasi parameter-parameter jaringan secara end-to-end. Aplikasi-aplikasi akan meminta tingkat layanan yang dibutuhkan untuk dapat beroperasi dan bergantung pada mekanisme *QoS* untuk menyediakan sumber daya jaringan yang dimulai sejak permulaan transmisi dari aplikasi-aplikasi tersebut. Aplikasi tidak akan mengirimkan trafik, sebelum menerima tanda bahwa jaringan mampu menerima beban yang akan dikirimkan aplikasi dan juga mampu menyediakan *QoS* yang diminta secara end-to-end [15]. Untuk itulah suatu jaringan akan melakukan suatu proses yang disebut admission control. Admission control adalah suatu mekanisme yang mencegah jaringan mengalami over-loaded. Jika *QoS* yang diminta tidak dapat disediakan, maka jaringan tidak akan mengirimkan tanda ke aplikasi agar dapat memulai untuk mengirimkan data. Jika aplikasi telah memulai pengiriman data, maka sumber daya pada jaringan yang sudah dipesan aplikasi tersebut akan terus dikelola secara end-to-end sampai aplikasi tersebut selesai [16].

2.2.5.2 Differentiated Services (DiffServ)

Differentiated Services bertujuan untuk membagi trafik atas kelas-kelas yang kemudian diberi perlakuan yang berbeda [15]. DiffServ menyediakan diferensiasi layanan dengan membagi trafik atas kelas-kelas dan memperlakukan setiap kelas secara berbeda.

Differentiated Services menyediakan suatu set perangkat klasifikasi dan mekanisme antrian terhadap protokol-protokol atau aplikasi-aplikasi dengan prioritas tertentu di atas jaringan yang berbeda. Differentiated

service bergantung pada kemampuan edge router untuk memberikan klasifikasi dari paket-paket yang berbeda tipenya yang melewati jaringan. Trafik jaringan dapat diklasifikasikan berdasarkan alamat jaringan, protocol dan port, ingress interface, atau klasifikasi lainnya selama masih didukung oleh standard access list atau extended access list [16].

2.2.5.3 Best-Effort Service

Penggunakan best-effort service tidak akan memberikan jaminan agar paket dapat sampai ke tujuan yang dikehendaki. Sebuah aplikasi dapat mengirimkan data dengan besar yang bebas kapan saja tanpa harus meminta ijin atau mengirimkan pemberitahuan ke jaringan. Beberapa aplikasi dapat menggunakan best- effort service, sebagai contohnya FTP dan HTTP yang dapat mendukung best-effort service tanpa mengalami permasalahan. Untuk aplikasi-aplikasi yang sensitif terhadap network *delay*, fluktuasi bandwidth, dan perubahan kondisi jaringan, penerapan best-effort service bukanlah suatu tindakan yang bijaksana. Sebagai contohnya aplikasi telephony pada jaringan yang membutuhkan besar bandwidth yang tetap, agar dapat berfungsi dengan baik, dalam hal ini penerapan best-effort akan mengakibatkan panggilan telephone gagal atau terputus [15].

2.2.6 Parameter Kinerja Pengujian *QoS*

2.2.6.1 Teori *Throughput*

Di dalam jaringan telekomukasi *throughput* adalah jumlah data persatuan waktu yang dikirim untuk suatu titik jaringan atau suatu titik ke titik jaringan yang lain [5]. Sistem *throughput* atau jumlah *throughput* adalah jumlah rata-rata data yang dikirimkan untuk semua terminal pada sebuah jaringan.

Throughput merupakan kecepatan (rate) transfer data efektif, yang di ukur dalam bps. *Throughput* menghitung jumlah total kedatangan paket yang sukses yang di amati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut [6]. Persamaan perhitungan *throughput*:

$$\textit{Throughput} = \frac{\text{Paket data diterima}}{\text{Lama pengamatan}}$$

Sumber : TIPHON (1999)

Tabel 2.1. Standarisasi *Throughput* versi TIPHON.

Kategori *Throughput*	***Throughput***	**Indeks**
Sangat Bagus	100 %	4
Bagus	75 %	3
Sedang	50 %	2
Jelek	< 25 %	1

2.2.6.2 Teori *Delay*

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, atau juga waktu proses yang lama [6]. *Delay* ini di dalam jaringan dapat di golongkan sebagai berikut:

a) *Delay* propagasi

Delay propagasi adalah waktu yang dibutuhkan oleh sinyal informasi untuk bergerak dalam media komunikasi seperti kabel,serat,optic,gelombang mikro dan satelit [5].

b) *Delay* transmisi

Delay transmisi adalah waktu yang dibutuhkan suatu system untuk melewatkan sejumlah paket data. *Delay* berbanding lurus dengan besarnya paket data dan berbanding terbalik dengan kecepatan *bandwith* jaringan tersebut [5].

c) *Delay* antrian

Delay antrian adalah lamanya waktu yang di butuhkan suatu paket data sebelum paket tersebut di teruskan ketujuannya. *Delay* ini juga termasuk *delay* yang terjadi pada perangkat jaringan .

Menurut versi TIPHON, persamaan dan besarnya *delay* dapat diklasifikasikan sebagai berikut :

Persamaan perhitungan *delay* :

$$Delay = \frac{\text{Total } delay}{\text{Total paket yang diterima}}$$

Sumber : TIPHON (1999)

Tabel 2.2. Standarisasi *Delay* versi TIPHON.

Kategori *Delay*	*Delay*	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 – 450 ms	2
Jelek	> 450 ms	1

2.2.6.3 Teori *Packet loss*

Packet loss merupakan jumlah paket yang hilang dalam proses pengiriman data dari satu titik ke titik yang lain. Perhitungannya dilakukan dengan mengurangi jumlah paket yang dikirmkan dengan jumlah paket yang diterima [5].

Packet loss merupakan sebagai kegagalan dalam melakukan transmisi paket data untuk mencapa sebuah tujuannya [6]. Kegagalan paket tersebut mencapai tujuan,dapat di sebabkan oleh beberapa kemungkinan, di antaranya yaitu:

a) Terjadinya overload trafik di dalam jaringan.
   Terjadinya *overload* trafik ini di sebabkan oleh beban yang terlalu berat dalam lalulintas jaringan tersebut.
b) Terjadinya tabrakan(*congestion*)
   Adanya tabrakan informasi atau data dalam sebuah jarigan tersebut
c) Error yang terjadi pada media fisik
   Kegagalan yang terjadi pada sisi penerima antara lain bisa di sebabkan karena *overflow* yang terjadi pada *buffer*

Packet loss adalah salah satu parameter yang sangat menentukan dalam proses *video conference*. Makin kecil besaran *packet loss* nya maka kualitas suatu Webinar akan semakin baik. Menurut versi TIPHON, besarnya *Packet loss* dapat diklasifikasikan sebagai berikut :

Tabel 2.3. Standarisasi *Packet loss* versi TIPHON.

Kategori *Packet loss*	*Packet Loss*	Indeks
Sangat Bagus	0	4
Bagus	3 %	3
Sedang	15 %	2
Jelek	25 %	1

Persamaan perhitungan *Packet loss* :

Packet Loss= (Paket yang hilang / Paket yang dikirim) * 100%

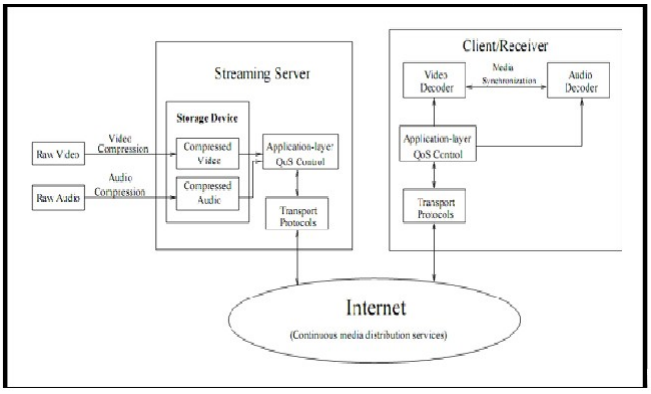
Sumber : TIPHON (1999)

2.2.7 Webinar atau *Video conference*

Pengertian secara harfiah dari *Video conference* atau Webinar adalah sebuah teknologi untuk memainkan *file* video secara langsung ataupun dengan pre-recorder dari sebuah mesin *server* (web *server*) [5]. Dengan kata lain, *file* video yang terletak dalam sebuah *server* dapat secara langsung dijalankan pada saat setelah ada permintaan dari user, sehingga proses running aplikasi yang di*download* berupa waktu yang lama dapat dihindari tanpa harus melakukan proses penyimpanan terlebih dahulu. Saat *file* video di stream, akan berbentuk sebuah *buffer* di komputer *client*, dan data video tersebut akan mulai di *download* ke dalam *buffer* yang telah terbentuk pada mesin *client*. Dalam waktu sepersekian detik, *buffer* telah terisi penuh dan secara otomatis *file* video dijalankan oleh sistem. Sistem akan membaca informasi dari *buffer* dan tetap melakukan proses *download file*, sehingga proses streaming tetap berlangsung [5].

Salah satu kendala yang dihadapi dalam pelaksanaan kegiatan Webinar adalah adanya jarak yang cukup jauh antara peserta yang menjadi target Webinar tersebut. Salah satu solusi untuk mengatasi kendala ini adalah dengan menyelenggarakan seminar tersebut dengan metode Webinar.

Ide da ket video menjadi beber kemudian



penerima (*receiver*) dapat men-decode dan memainkan potongan paket video tersebut tanpa harus menunggu keseluruhan *file* selesai terkirim ke mesin penerima [5]. Dalam *video conference* memiliki beberapa proses yang harus diperhatikan yaitu, proses kompresi, *Quality of Service* (*QoS*), *continous media distribution services, streaming server,* mekanisme sinkronisasi, dan protokol untuk media *streaming*.

Gambar 2.7. Sistematis *Video conference*.

Streaming server akan mengirimkan data yang telah dikompresi dan tersimpan dalam storage device ketika menerima request dari klien (melalui internet). Data akan dikirimkan oleh Streaming *server* dengan modul application layer *QoS*. *QoS* control lau menyesuaikan bit stream data ke dalam status jaringan dan persyaratan *QoS*. Selanjutnya paket data tersebut akan dikirimkan oleh transport protocol ke dalam jaringan setelah mengalami penyesuaian. Setiap paket yang sampai disisi penerima akan diproses terlebih dahulu oleh transport layer dan application layer protokol lalu didekodekan oleh decoder [5].

2.2.8 Wireshark

Wireshark merupakan salah satu *tools* atau aplikasi "*Network Analyzer*" atau Penganalisa Jaringan [15]. Penganalisaan Kinerja Jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap paket-paket data atau informasi yang berlalu-lalang dalam jaringan. Tampilan dari wireshark ini sendiri terbilang sangat bersahabat dengan user karena menggunakan tampilan grafis atau GUI (Graphical User Interface). Pada pembahasan kali ini, saya akan membahas fitur-fitur yang ada pada dalam aplikasi wireshark. Dengan menjelaskan fitur-fitur tersebut, maka akan mempermudah penggunaan dari aplikasi wireshark.

Sebagai salah satu network protocol analyzer, tentu saja Wireshark memiliki beberapa fitur. Berikut merupakan fitur utama Wireshark :

1. Multi platform bisa digunakan pada Unix dan Windows.

2. Open source dan gratis .
3. Dapat menampilkan dan menyimpan paket yang di-capture.
4. Mendukung beberapa macam protokol jaringan. Protokol – protokol tersebut antara lain TCP, IP, RTP, UDP, RTCP, RTSP, dan lain lain.