BAB 2
TINJAUAN PUSTAKA

2.1. Profil Instansi

2.1.1. Sejarah Instansi

Pusat Pengembangan Dan Pemberdayaan Pendidikan Dan Tenaga Kependidikan Ilmu Pengetahuaan Alam (PPPPTK IPA) Bandung pada awalnya bernamakan PPPG Teknologi Bandung. Pada hari Kamis 22 Agustus 2002.telah diadakan pertemuan di PPPG Teknologi Bandung untuk membahas tentang penentuan hari iadi PPPG Teknologi Bandung. Dari penelusuran sejarah berdirinya PPPG Teknologi Bandung, ditemukan fakta sejarah sebagai berikut:

1. Tanggal 1 April 1972. telah resmi ada satu satuan program peningkatan mutu guru teknik. melalui proyek yang disebut Proyek Peningkatan MutuPengajar Teknik (Proyek PMPT). yang berlangsung di Bandung dengan memakai sumber daya yang dimiliki STM Instruktor Bandung (ex SGPT).Di Jalan Dr. Rum No. 9 Bandung.
2. Pada tahun 1975.dihasilkan satu naskah yang berisikan konsep Technical Teacher Upgrading Centre (TTUC). disusun bekeria sama dengan tenagaahli Australia (Mr. Ian Scott dan Mr. Ken Sharp).
3. Tanggal 23 Juni 1978.dengan SK Menteri Pendidikan dan Kebudayaan.No.0205/O/1978. diterbitkan keputusan kelembagaan 7 Pusat Pengembangan Penataran Guru (PPPG). Termasuk PPPG Teknologi Bandung.
4. Pada tanggal 1 April 1980. PPPG Teknologi Bandung resmi beroperasi sebagai suatu lembaga (UPT = Unit Pelaksana Teknis). terhitung padatanggal diangkatnya Kepala Pusat PPPG Teknologi Bandung yang pertama.
5. Pada bulan Juni 1986. PPPG Teknologi Bandung, pindah kampus dari Jalan Dr. Rum No. 9. Bandung ke Jalan Pasantren, Cimahi Utara.
6. Pada tanggal 28 Juli 1988.peresmian pemakaian kampus baru di Jalan Pasantren. Cimahi Utara. oleh Bapak Prof. Dr. Fuad Hassan. Menteri

7. Pendidikan nan Kebudayaan dan The Hon. Bill Morisson. Duta Besar Australia untuk Indonesia.
8. Pada tanggal 14 Agustus 1990.terbit SK Menteri Pendidikan danKebudayaan No. 0529/O/1990. tentang:

Perampingan Organisasi PPPG Teknologi Bandung Pengakuan tugas.Selain tugas penataran juga melakukan tugas pengembangan teknis pendidikan. Setelah mempelajari dan menelaah makna sejarah perkembangan tersebut diatas.maka peserta rapat dalam pertemuan ini. sepakat menetapkan tanggal 1 April 1972 sebagai hari jadi PPPG Teknologi Bandung, dengan dasar pemikiran:

Pentingnya hari jadi sebagai momentum untuk flash back masa lalu. Dan memikirkan langkah strategik menuju masa depan bangsa.

Ide pentingnya peningkatan mutu guru teknik telah berkembang jauhsebelumnya, terutama atas dorongan keperluan pembangunan proyek-proyekSTM Pembangunan. BLPT (TTC). dan 80 STM. dan secara formal diakomodasimelalui Proyek Peningkatan Mutu Pengajar Teknik (Proyek PMPTI tahun1972/1973.

Sekalipun diselenggarakan dalam bentuk Proyek. tetapi telah cukup menjadi alasan kuat. karena untuk pertama kali melembaga. sebagai program nasionaldan ditandatangani oleh Menteri Pendidikan dan Kebudayaan.

2.1.2. Visi dan Misi

1. Visi

Berdasarkan pencermatan terhadap lingkungan internal dan eksternal serta adanya keinginan untuk memenuhi tuntutan masyarakat global, PPPPTK IPA menetapkan visi yaitu :

“Terwujudnya Pendidikan dan Tenaga Kependidikan IPA yang Profesional, Bermartabat, dan Berwawasan Global”.

2. Misi

Untuk menjembatani dan mencapai visi PPPPTK IPA, disusunlah misi lembaga sebagai berikut :

a. Mengembangkan model-model diklat berbasis penelitian dan kepakaran bagi PTK IPA.
b. Mengembangkan bahan dan media diklat berbasis riset dan kepakaran bagi PTK IPA.
c. Menyelengarakan layanan diklat secara prima bagi PTK IPA.
d. Mensosialisasi produk-produk inovasi pendidikan IPA pada forum nasionaldan internasional.
e. Mengembangkan jaringan kerja dalam upaya peningkatan profesionalitasPTK IPA secara nasional dan internasional.
f. Mengembangkan kualitas dan kuantitas SDM PPPPTK IPA.
g. Meningkatkan sarana dan prasarana PPPPTK IPA.
h. Melaksanakan ketatausahaan dan rumah tangga lembaga.

2.1.3. Logo Instansi

Pusat Pengembangan dan Pemberdayaan Pendidik dan Tenaga Kependidikan Ilmu Pengetahuan Alam (Science Education Development Centre) PPPPTK IPA Bandung memiliki logo sebagai berikut :



Gambar 2-1. Logo Instansi

Deskripsi :

Lingkaran merah yang ada di tengah merupakan matahari di mana matahari adalah sumber daya alam yang paling berguna di muka bumi ini, dapat terlihat pada logo instansi yang memposisikan lingkaran merah sebagai pusat dari logo. Diharapkan PPPPTK IPA dapat membantu dalam mengembangkan sains di Indonesia dengan berbagai sumber daya dan aktivitas didalamnya.

2.1.4. Badan Hukum Instansi

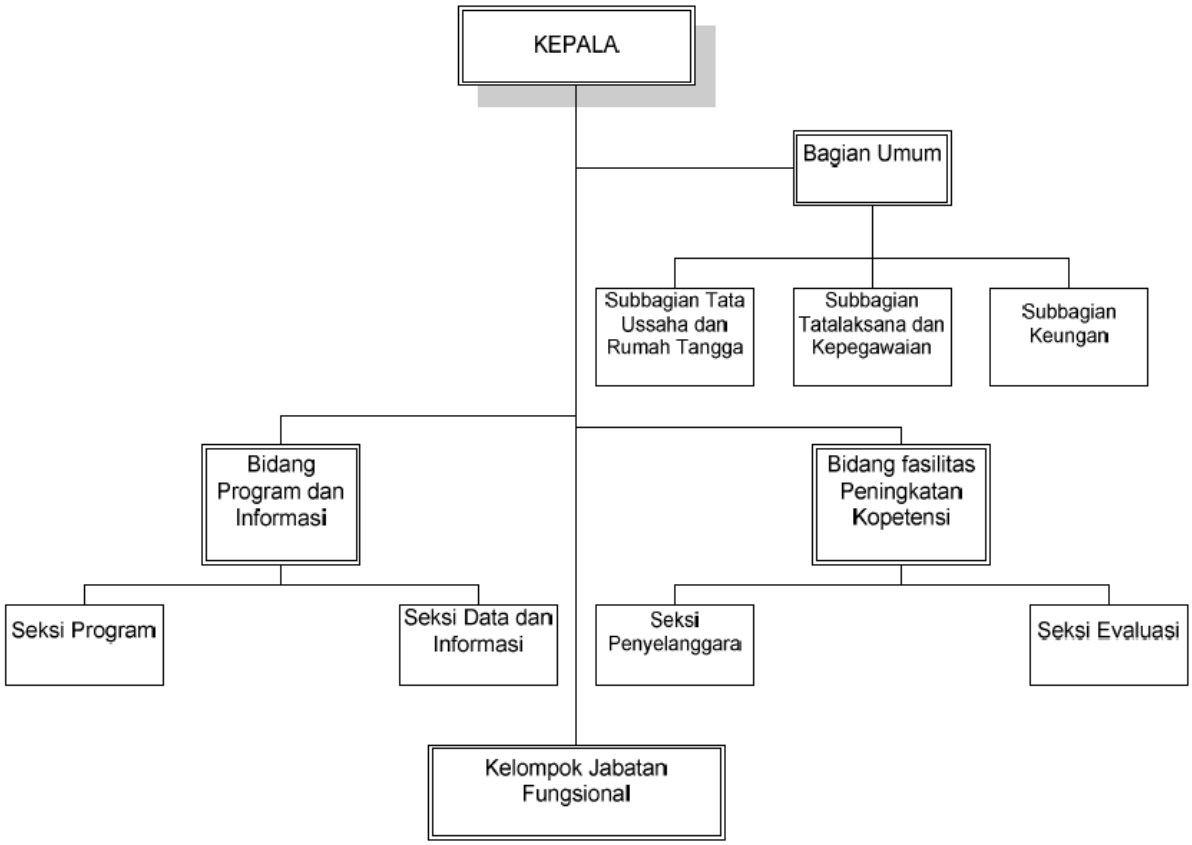
Dengan telah disetujuinya revitalisasi PPPG menjadi PPPPTK oleh Kepmenpan dengan No. B/243/M.Pan/1/2007, Tanggal 31 Januari 2007 maka struktur organisasi PPPPTK yang tertuang dalam SK Mendikbud No.0529/O/1990 akan mengalamiperubahan dan tugas pokok fungsi PPPPTK juga akan mengalami penyesuaian.Kedudukan dan struktur organisasi PPPPTK diusulkan sebagai berikut :

1. Pusat pengembangan dan pemberdayaan pendidik dan tenaga kependidikan yang selanjutnya dalam peraturan ini disebut PPPPTK adalah unit pelaksana teknis dilingkungan Departemen PendidikanNasional di bidang pengembangan dan pemberdayaan pendidik dan tenaga kependidikan.
2. PPPPTK dipimpin oleh seorang kepala yang berada di bawah dan bertanggungjawab kepada direktur jendral peningkatan mutu pendidik dan tenaga kependidikan

2.1.5. Struktur Organisasi

Struktur organisasi perusahaan menunjukan pola hubungan jalur komunikasi diantara fungsi-fungsi, bagian-bagian atau orang-orang yang ada dalam suatu organisasi dapat diketahui bagaimana wewenang dan tanggung jawab mengalir diantara bagian tersebut.

Dibawah ini gambar struktur organisasi Pusat Pengembangan Dan Pemberdayaan Pendidikan Dan Tenaga Kependidikan Ilmu Pengetahuaan Alam (PPPPTK IPA) berdasarkan Surat Keputusan Permendiknas Nomor 8 Tahun 2007, tentang Struktur Organisasi dan Tata Kerja PPPTK:



Gambar 2-2. Struktur Organisasi

Job Description merupakan penjelasan keseluruhan mengenai tugas didalam struktur organisasi untuk mencapai suatu tujuan. Adapun penjelasan mengenai tugas – tugas didalam struktur organisasi di PPPPTK IPA adalah :

1. Kepala

   Kepala adalah orang yang bertanggung jawab didalam mengatur dan mengawasi system kerja yang ada di perusahaan.

2. Bagian Umum

   Bagian umum adalah orang yang bertanggung jawab terhadap bagian umum dan terhadap sistem kerja yang ada di perusahaan

3. Sub bagian tata usaha dan rumah tangga

Sub bagian tata usaha dan rumah tangga adalah orang yang bertanggung jawab terhadap tata usaha, rumah tangga dan pemiliharan lingkungan yang ada di perusahaan

4. Sub bagian tata laksana dan kepegawaian

   Sub bagian tata laksana dan kepegawaian adalah orang yang bertanggung jawab terhadap tata laksana dan kepegawaian yang ada di perusahaan

5. Sub bagian keuangan

   Sub bagian keuangan adalah orang yang bertanggung jawab dalam bidang keputusan - keputusan strategis tentang keuangan.

6. Bidang Program dan Informasi

   Bidang Program dan Informasi adalah orang yang bertanggung jawab terhadap penyusunan program dan informasi yang ada di perusahaan

7. Seksi program

   Seksi program adalah orang yang bertanggung jawab terhadap seksi program

8. Seksi data dan Inforamasi

   Seksi data dan Inforamasi adalah orang yang bertanggung jawab mengenai data daninformasi yang ada di perusahan.

9. Bidang Fasilitas Peningkatan Kopentensi

   Mempersiapkan penyusunan program penataran, mengurus tatalaksana penataran,melaksanakan publikasi, perpustakaan dan pelaporan.

10. Seksi penyelanggara

    Seksi penyelenggara adalah orang yang bertanggung jawab mengenai penyelenggaraanyang ada di perusahan.

11. Seksi Evaluasi

    Seksi evaluasi adalah orang yang bertanggung jawab mengenai evaluasi yang ada diperusahan.

2.2. Landasan Teori

2.2.1. Jaringan Komputer

Jaringan komputer adalah sekumpulan komputer serta perangkat-perangkat lain pendukung komputer yang saling terhubung dalam suatu kesatuan. Media jaringan komputer dapat melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling melakukan pertukaran informasi, seperti dokumen dan data, dapat juga melakukan pencetakan pada printer yang sama dan bersama-sama memakai perangkat keras dan perangkat lunak yang terhubung dengan jaringan. Setiap komputer, ataupun perangkat-perangkat yang terhubung dalam suatu jaringan disebut dengan node. Dalam sebuah jaringan komputer dapat mempunyai dua, puluhan, ribuan atau bahkan jutaan node.

2.2.2. Tipe Jaringan Komputer

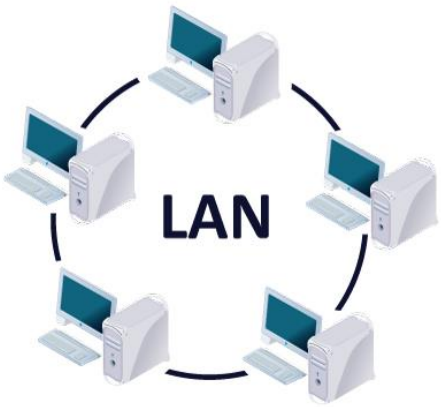
Jaringan komputer berdasarkan ruang lingkup dan jangkauan dibagi menjadi tiga kelompok:

1. Jaringan LAN (*Local Area Network*)

Jaringan LAN (Local Area Network) adalah jaringan yang menghubungkan beberapa komputer dalam satu lokal area saja (biasanya dalam satu gedung atau antargedung). Biasanya digunakan di dalam rumah, perkantoran, perindustrian, universitas atau akademik, rumah sakit dan daerah yang sejenis.

Pada jaringan LAN (Local Area Network), kecepatan transmisi data akan mencapai satu sampai 100 megabit per detik. Berbagai tipe LAN (Local Area Network) telah dibangun dan diinstalasi, namun beberapa tipe menjadi lebih dominan dari yang lain. Sistem LAN (Local Area Network) yang sering digunakan adalah sistem Ethernet yang dikembangkan oleh perusahaan Xerox. Penggunaan nodeintermediete (seperti repeater, bridge, dan switch) memungkinkan LAN (Local Area Network) terkoneksi membentuk jaringan yang lebih luas. LAN (Local Area Network) juga dapat terkoneksi ke LAN (Local Area Network), WAN (Wide Area Network), atau MAN (Metropolitan Area Network) lain menggunakan router. Secara garis besar, LAN (Local Area Network)adalah sebuah jaringan komunikasi yang memiliki ciri sebagai berikut :

a. Bersifat lokal (misal, satu gedung atau antargedung).
b. Dikontrol oleh satu kekuasaan administratif.
c. Pengguna dalam sebuah LAN dianggap dapat dipercaya.
d. Mempunyai kecepatan yang tinggi dan data dalam semua komputer selalu di-*sharing*



Gambar 2-3. Jaringan LAN (*Local Area Network*)

2. Jaringan MAN (*Metropolitan Area Network*)

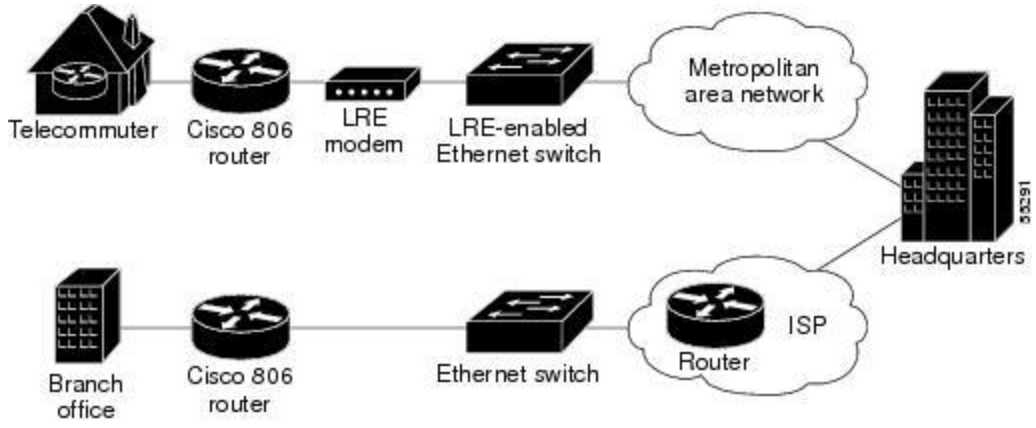
MAN (Metropolitan Area Network) merupakan jaringan yang menghubungkan beberapa jaringan komputer dalam wilayah yang lebih luas. MAN (Metropolitan Area Network) biasanya digunakan oleh sebuah korporasi jaringan komputer dalam satu kota, antarkampus, dalam suatu universitas, dan lain-lain. Tiga ciri khusus yang membedakan LAN (Local Area Network), MAN (Metropolitan Area Network) dan WAN (Wide Area Network), yaitu:

a. Luas jaringan MAN (*Metropolitan Area Network*) merupakan pertengahan antara luas jaringan LAN (*Local Area Network*) dengan jaringan WAN (*Wide Area Network*). MAN biasanya mempunyai luas jaringan antara 5 sampai 10 km dan mengkoneksikan komputer dalam suatu kota.
b. MAN (Metropolitan Area Network) seperti juga WAN (Wide Area Network) biasanya dimiliki oleh beberapa organisasi. Pada MAN (Metropolitan Area Network), jaringan komunikasi dan peralatan biasanya dimiliki oleh network provider yang menjual servis kepada pengguna. Servis yang ada tergantung

kepada operator MAN (Metropolitan Area Network) dan performance yang ada biasanya telah ditentukan.

c. MAN (Metropolitan Area Network) merupakan jaringan dengan kecepatan tinggi yang memungkinkan sharing data pada suatu area yang luas.

d. MAN (Metropolitan Area Network) dapat dikoneksikan ke jaringan lain untuk membentuk WAN (Wide Area Network).



Gambar 2-4. Jaringan MAN (*Metropolitan Area Network*)

Pada Internet, organisasi yang beroperasi memakai sistem jaringan ini adalah ISP (Internet Service Provider). ISP (Internet Service Provider) mengatur siklus komunikasi ke pengguna perorangan. Mereka juga memastikan dapat memonitor penggunaan pengguna dan pelayanan aksesnya. ISP (Internet Service Provider) mendapat keuntungan dari pelanggan-pelanggan jaringannya dan bertanggung jawab memenuhi kebutuhan konsumen yang telah membayarnya.

ISP (Internet Service Provider) sendiri membayar kepada penyedia WAN (Wide Area Network) atau NSP (Network Services Provider) untuk konektivitas yang diperlukan. Banyak ISP (Internet Service Provider) terkoneksi ke ISP (Internet Service Provider) lain atau dengan beberapa NSP (Network Services Provider) yang lain. Koneksi-koneksi tambahan ini terbukti jarang mengalami masalah.

3. Jaringan WAN (*Wide Area Network*)

Jaringan WAN (*Wide Area Network*) menghubungkan beberapa WAN (*Wide Area Network*) dari beberapa kota atau negara yang berbeda. WAN (*Wide Area Network*) biasanya terhubung via satelit. WAN (*Wide Area Network*) mempunyai daerah yang

sangat luas dan menggunakan siklus komunikasi yang menghubungkan *node-node intermediate*. Kecepatan transmisinya beragam dari 2 Mbps, 34 Mbps, 45 Mbps, 155 Mbps, sampai dengan 625 Mbps (atau kadang-kadang lebih). Faktor khusus yang mempengaruhi desain dan *performance*-nya terletak pada siklus komunikasi, seperti jaringan telepon, satelit atau komunikasi pembawa lain yang disewanya.

Ciri dari jaringan WAN (Wide Area Network) adanya penekanan pada fasilitas transmisi sehingga komunikasi dapat berjalan efisien. Sangatlah penting untuk mengontrol jumlah lalu lintas data dan mencegah delay yang berlebihan. Karena topologi WAN (Wide Area Network) lebih komplek dari MAN (Metropolitan Area Network) maka algoritma rute aliran data menjadi perhatian.

Banyak jaringan WAN (Wide Area Network) telah dibangun seperti jaringan publik, jaringan korporasi yang besar, jaringan militer, jaringan perbankan, jaringan perdagangan online dan jaringan pemesanan jasa angkutan. WAN (Wide Area Network) menjadi sangat luas, membentang keseluruh dunia.Organisasi yang mendukung WAN (Wide Area Network) adalah penggunaan protokol Internet yang dikenal sebagai NSP (Network Service Provider). NSP (Network Service Provider) merupakan bagian inti dari Internet.

WAN (Wide AreaNetwork) yang dikoneksikan melalui NSP (Network Service Provider) bersama-sama terkoneksi membentuk suatu jaringan Internet yang bersifat global .NSP (Network Service Provider) yang ada bervariasi dalam kecepatan transmisi data, transit delay, dan konektivitas yang diberikan. Keuntungan penggunaan WAN (Wide Area Network) adalah :

a. Luas jaringan WAN (Wide Area Network) dapat mencapai seluruh belahan dunia.
b. Transfer file pada tempat berjauhan dapat dikirim secara cepat melalui e-mail dan FTP (File Transfer Protocol).

2.2.3. Manfaat Jaringan Komputer

Sharing resources, bertujuan agar seluruh program, peralatan lainnya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pengaruh dari pemakai. Dengan kata lain, seorang computer

user yang letaknya jauh sekalipun dapat memanfaatkan data maupun informasi yang lainnya tanpa mengalami kesulitan.

Dengan jaringan komputer kita akan mendapatkan reliabilitas yang tinggi dengan memiliki sumber-sumber alternatif persediaan. Misal semua data data disimpan atau disalin ke dua, tiga atau lebih komputer yang terkoneksi ke suatu jaringan. Sehingga bila salah satu komputer rusak, maka data masih dapat digunakan dengan menggunakan komputer lainnya.

Jaringan komputer dapat menghemat uang. Kita dapat membeli suatu barang di Negara lain tanpa harus mengeluarkan uang yang banyak. Hanya dengan menggunakan jaringan komputer kita dapat membeli barang tersebut.

Sistem jaringan komputer memberikan perlindungan terhadap data.Jaminan keamanan tersebut diberikan melalui pengaturan hak akses para pemakai, serta teknik perlindungan terhadap harddisk (media penyimpanan data) sehingga data mendapatkan perlindungan yang efektif.

2.2.4. Topologi Jaringan

Topologi jaringan adalah metode yang digunakan untuk menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Dalam suatu jaringan komputer jenis topologi akan mempengaruhi kecepatan komunikasi. Untuk itu, sebelum membangun sebuah jaringan komputer, perlu diketahui karakteristik dari masing-masing topologi jaringan. Ada tiga tipe jaringan komputer berdasarkan topologinya, yaitu:

1. Topologi *Bus*
2. Topologi *star* (bintang)
3. Topologi *ring* (cincin)

Topologi jaringan yang sering digunakan dari ketiga topologi jaringan di atas adalah tipe star. Selain ketiga topologi jaringan tersebut, ada juga topologi jaringan hybrid.Seperti hybrid-star-bus, jaringan star-ring, dan jaringan mesh yang mengkoneksikan berbagai macam komputer dalam jaringan.

1. Topologi *Bus*

Pada topologi bus, kedua ujung jaringan harus diakhiri dengan sebuah terminator.Barel konektor dapat digunakan untuk memperluasnya.Jaringan hanya

terdiri dari satu saluran kabel menggunakan kabel BNC (Barel Network Cable). Komputer yang ingin terhubung ke jaringan dapat, mengaitkan dirinya dengan mentap Ethernet sepanjang kabel.

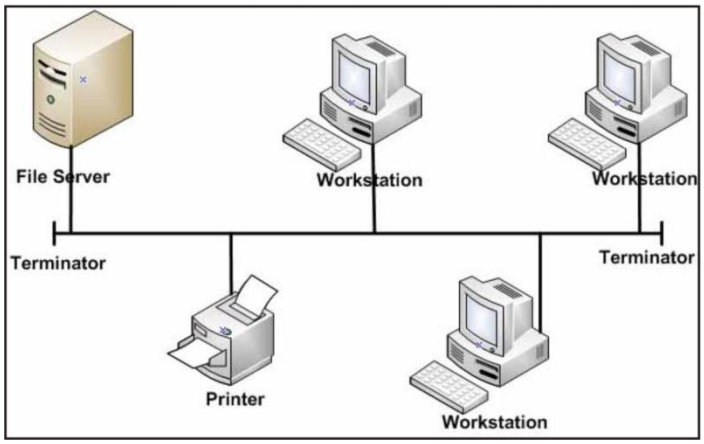
Instalasi jaringan Bus sangat sederhana, murah dan maksimal terdiri atas 5-7 komputer. Kesulitan yang sering dialami adalah kemungkinan terjadi tabrakan data karena mekanisme jaringan relatif sederhana dan jika salah satu *node* terputus maka akan mengganggu kinerja dan trafik seluruh jaringan.

Keuntungan topologi *bus*:

a. Hemat kabel
b. Layout kabel sederhana
c. Mudah dikembangkan

Sedangkan kerugian topologi *bus* adalah :

a. Deteksi dan isolasi kesalahan sangat kecil
b. Kepadatan lalu lintas
c. Bila salah satu *client* rusak, maka jaringan tidak bisa berfungsi
d. Diperlukan *repeater* untuk jarak jauh



Gambar 2-5. Topologi *Bus*

2. Topologi *star* (bintang)

Pada topologi star (bintang), semua komputer mengelilingi hub atau switch pusat yang mengontrol komunikasi jaringan dan dapat berkomunikasi dengan hub atau switch yang lain. Batas jarak komputer dengan hub sekitar 100 meter. Setiap node pada jaringan akan berkomunikasi melalui node pusat atau konsentrator

terlebih dahulu sebelum menuju server. Jaringan lebih fleksibel dan luas dibandingkan dua topologi yang lain.

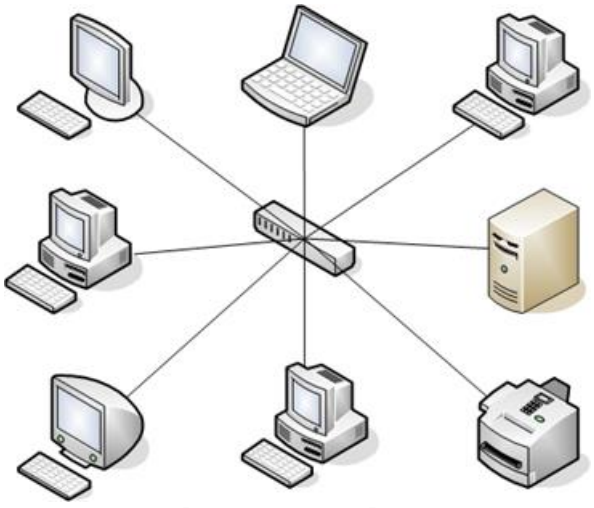
Keunggulan tipe star adalah jika salah satu node putus maka tidak akan mengganggu kinerja jaringan lainnya. Kabel yang biasa yang digunakan adalah kabel UTP (Unshielded Twisted Pair).

Adapun keuntungan dari topologi *star* adalah :

a. Paling fleksibel
b. Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jarigan lain
c. Kontrol terpusat
d. Kemudahan deteksi dan isolasi kesalahan/kerusakan
e. Kemudahan pengelolaan jaringan

Adapun kerugian dari topologi *star* adalah :

a. Boros kabel
b. Perlu penanganan khusus
c. Kontrol terpusat (HUB) jadi elemen yang sangat vital

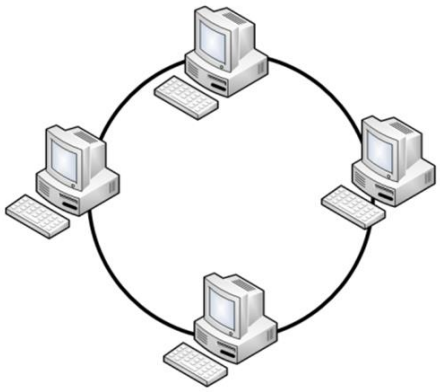


Gambar 2-6. Topologi *Star*

3. Topologi *ring* (cincin)

Pada topologi *ring* (cincin), jaringan membentuk lingkaran tertutup sehingga mengesankan cincin tanpa ujung. Komputer terkoneksi satu dengan yang lain seperti sebuah cincin. Sinyal akan mengalir satu arah sehingga dapat menghindari terjadinya

tabrakan paket. Namun, salah satu komputer yang putus akan tetap mempengaruhi keseluruhan jaringan.



Gambar 2-7. Topologi Ring

Keuntungan topoologi *ring* :

a. Hemat kabel

Kelemahan topologi *ring* :

a. Peka terhadap kesalahan
b. Pengembangan jaringan lebih kaku

2.2.5. IP Address

Alamat IP atau *Internet Protokol Address* adalah deretan angka biner antar 32 bit sampai 128 bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet. Panjang dari angka ini adalah 32 bit (untuk IPv4 atau IP versi 4), dan 12 bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan Internet berbasis TCP (Transport Control Protocol)/IP(Internet Protocol). Alamat IP adalah Kombinasi angka unik yang ditetapkan untuk mengindentifikasi / mengenali suatu host di suatu jaringan / Internet agar bisa berkomunikasi satu sama lain. Angka ini dibutuhkan oleh software-software Internet untuk mengakses informasi dari dan ke host tersebut. Setiap komputer yang ingin terhubung ke jaringan / Internet maka komputer tersebut harus memiliki alamat yang jelas agar bisa berkomunikasi satu sama lain. Pengguna Internet umumnya hanya mengenal nama domain dari alamat website yang akan dikunjungi, seperti: detik.com, ilmukomputer.com, e-dukasi.net, yahoo.com, gmail.com, dll. Tapi sebenarnya alamat-alamat tersebut merupakan

konversi dari alamat komputer/jaringan berbasiskan angka yang unik. Konsep dasarnya pengalamatan pada komputer menggunakan sekumpulan angka sebanyak 32 bit (IPv4) atau 128 bit (IPv6) yang dikenal sebagai *IP Address*.

Adanya *IP Address* merupakan konsekuensi dari penerapan Internet Protokol untuk mengintegrasikan jaringan komputer Internet di dunia. Seluruh *host* (komputer) yang terhubung ke Internet dan ingin berkomunikasi memakai TCP/IP harus memiliki *IP Address* sebagai alat pengenal host pada network. Secara logika, Internet merupakan suatu network besar yang terdiri dari berbagai sub-network yang terintegrasi.Oleh karena itu, suatu *IP Address* harus bersifat unik. Tidak boleh ada satu *IP Address* yang sama dipakai oleh dua host yang berbeda. Contoh *IP Address* : 66.249.89.99 (www.google.com) , 203.130.198.131 (www.e-dukasi.net) , 192.168.0.1.

Untuk itu, penggunaan IP *Address* di seluruh dunia dikoordinasi oleh lembaga sentral Internet yang di kenal dengan IANA (Internet Assigned Numbers Authority). Badan-badan yang mengawal IP di bawah IANA adalah:

1. APNIC (*Asia Pacific Network Information Centre*) kawasan Asia Pasifik.
2. ARIN (*American Registry for Internet Numbers*) kawasan Amerika Utara dan Afrika.
3. LACNIC (*Regional Latin-American and Caribbean IP Address Registry*) kawasan Amerika Latin dan beberapa Kepulauan karibia.
4. RIPE NCC (*Rseaux IP Europeans*) kawasan Eropa, Asia tengah dan Afrika utara.

Sistem pengalamatan IP ini terbagi menjadi dua, yakni :

1. IP versi 4 (Ipv4)
2. IP versi 6 (Ipv6)

2.2.6. IP versi 4

Alamat IP versi 4 (sering disebut dengan Alamat IPv4) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP (*Transport Control Protocol*)/IP (*Internet Protocol*) yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit, dan secara teoritis dapat mengalamati hingga 4

miliar host komputer atau lebih tepatnya 4.294.967.296 host di seluruh dunia, jumlah host tersebut didapatkan dari 256 (didapatkan dari 8 bit) dipangkat 4 (karena terdapat 4 oktet) sehingga nilai maksimal dari alamat IP versi 4 tersebut adalah 255.255.255.255 dimana nilai dihitung dari nol sehingga nilai *host* yang dapat ditampung adalah 256x256x256x256=4.294.967.296 host. Sehingga bila *host* yang ada diseluruh dunia melebihi kuota tersebut maka dibuatlah IP versi 6 atau IPv6.

2.2.7. Representasi Alamat IPv4

Alamat IP versi 4 umumnya diekspresikan dalam notasi desimal bertitik *(dotted decimal notation*), yang dibagi ke dalam empat buah oktet berukuran 8 bit. Dalam beberapa buku referensi, format bentuknya adalah w.x.y.z. Karena setiap oktet berukuran 8 bit, maka nilainya berkisar antara 0 hingga 255 meskipun begitu, terdapat beberapa pengecualian nilai.

Alamat IP yang dimiliki oleh sebuah host dapat dibagi dengan menggunakan subnet mask jaringan ke dalam dua buah bagian, yakni:

1. *Network IDentifier* (NetID) atau *Network Address* (alamat jaringan) yang digunakan khusus untuk mengidentifikasikan alamat jaringan dimana host berada. Dalam banyak kasus, sebuah alamat *network identifier* adalah sama dengan segmen jaringan fisik dengan batasan yang dibuat dan didefinisikan oleh routerIP. Meskipun demikian, ada beberapa kasus dimana beberapa jaringan logis terdapat di dalam sebuah segmen jaringan fisik yang sama dengan menggunakan sebuah praktek yang disebut sebagai *multinetting*. Semua sistem di dalam sebuah jaringan fisik yang sama harus memiliki alamat *network identifier* yang sama. *Network identifier* juga harus bersifat unik dalam sebuah *Internetwork*. Jika semua node di dalam jaringan logis yang sama tidak dikonfigurasikan dengan menggunakan *network identifier* yang sama, maka terjadilah masalah yang disebut dengan *routing error*. Alamat *network identifier* tidak boleh bernilai 0 atau 255.
2. *Host Identifier/HostID* atau *Host Address* (alamat host) yang digunakan khusus untuk mengidentifikasikan alamat *host* (dapat berupa *workstation*, server atau sistem lainnya yang berbasis teknologi TCP *(Transport Control*

Protocol)/IP(*Internet Protocol*) di dalam jaringan. Nilai *host identifier* tidak boleh bernilai 0 atau 255 dan harus bersifat unik di dalam *network identifier* atau segmen jaringan dimana ia berada.

2.2.8. Jenis – Jenis Alamat IPv4

Alamat IPv4 terbagi menjadi beberapa jenis, yakni sebagai berikut :

1. Alamat *Unicast*, merupakan alamat IPv4 yang ditentukan untuk sebuah antarmuka jaringan yang dihubungkan ke sebuah Internetwork. Alamat *unicast* digunakan dalam komunikasi *point-to-point* atau *one-to-one.*
2. 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.*
3. 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.*

2.2.9. Kelas – kelas Alamat IPv4

Dalam RFC 791, alamat IP versi 4 dibagi ke dalam beberapa kelas, dilihat dari oktet pertamanya, seperti terlihat pada tabel. Sebenarnya yang menjadi pembeda kelas IP versi 4 adalah pola biner yang terdapat dalam oktet pertama (utamanya adalah bit-bit *awal/high-order bit*), tapi untuk lebih mudah mengingatnya, akan lebih cepat diingat dengan menggunakan representasi desimal.

Tabel 2-1. *Kelas IP Address*

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	10xx xxxx	Alamat *unicast* untuk jaringan skala mengenah hingga skala besar.
Kelas C	192-223	110x xxxx	Alamat *unicast* untuk jaringan skala kecil
Kelas D	224-239	1110 0000	Alamat *multicast* (bukan alamat *unicast*)
Kelas E	240-255	1111 xxxx	Direservasikan; umunya digunakan sebagai alamat percobaan (eksperimen)

1. Kelas A

   Kelas A hanya menggunakan *octet* pertama untuk menunjukkan ID jaringan dan menggunakan tiga *octet* yang lain untuk menunjukkan ID *host*. *Bit high order* (bit pertama dari octet pertama) pada kelas ini selalu diset menjadi 0 (nol). Karena, *bit high-order* selalu diset menjadi 0 (nol), maka tujuh bit selanjutnya menunjukkan ID jaringan. Tujuh bit ini memungkinkan adanya 127 alamat jaringan. ID jaringan 127 disediakan khusus untuk fungsi umpan balik adapter jaringan sehingga kelas A mempunyai 126 alamat yang tersedia.24 bit sisanya disediakan untuk penggunaan ID host dari alamat. Tersedia 16.777.214 atau (224) host per jaringan. Karena kelas address ini menyediakan banyak ID host perjaringan, maka penggunaan kelas A diperuntukkan bagi perusahaan yang membutuhkan penyediaan akses host dalam jumlah sangat besar. Nomor pada kelas A sudah tinggal sedikit karena telah digunakan untuk jaringan universitas-universitas dan militer beberapa tahun lalu.

2. Kelas B

   Kelas B menggunakan *octet* pertama dan kedua untuk menentukan ID jaringan serta dua *octet* berikutnya untuk ID *host*. Bit *high order*(dua bit pertama dari *octet* pertama) dari alamat kelas ini selalu diset menjadi 10 (satu-nol). Karena bit hig-order diset menjadi 1 0, maka 14 bit sisanya menunjukkan ID jaringan. 14 bit

sisanya menyediakan 16.384 alamat jaringan. 16 bit sisanya digunakan untuk menyediakan ID *host*. Kelas B

3. Kelas C

   Kelas C menggunakan tiga *octet* pertama untuk menentukan ID jaringan, sedangkan satu *octet* sisanya untuk ID *host*.*Bit high-order* (3 bit pertama dari oktet pertama) dari alamat kelas ini selalu diset menjadi 110 (satu-satu-nol). Karena *bit high-order* diset menjadi 1 1 0, maka 21 bit sisanya menunjukkan ID jaringan. 21 bit menyediakan 2.097.152 alamat jaringan. 8 bit sisanya disediakan untuk penggunaan ID *host* dari alamat. Tersedia 254 (28) – 2 host perjaringan. Kelas address diperuntukkan bagi jaringan kecil yang hanya memerlukan nomor host dalam jumlah terbatas.

4. Kelas D

   Kelas D digunakan untuk *multicasting. Multicasting* digunakan untuk mengirim informasi ke nomor *host register*. Host-host dikelompokkan dengan meregistrasi dirinya kepada *router local* menggunakan alamat multicast dari range alamat kelas D. Bit hig-order untuk alamat kelas D di-set menjadi 1 1 1 0 (satu- satu- satu-nol). Bit sisanya digunakan untuk grup host di jaringan.

5. Kelas E

   Kelas E adalah kelas eksperiment yang dipersiapkan untuk penggunaan dimasa yang akan datang. Alamat-alamat di kelas ini di identifikasikan dengan *bit high-order* nya yang diset menjadi 1 1 1 1 (satu- satu- satu- satu).

2.2.10. IP versi 6 (IPv6)

Alamat IP versi 6 (sering disebut sebagai alamat IPv6) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 6. Panjang totalnya adalah 128-bit, dan secara teoritis dapat mengalamati hingga 2128=3,4 x 1038 host komputer di seluruh dunia. Contoh alamat IP versi 6 adalah :

1DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A.

Berbeda dengan IPv4 yang hanya memiliki panjang 32-bit (jumlah total alamat yang dapat dicapainya mencapai 4,294,967,296 alamat), alamat IPv6 memiliki panjang 128-bit. IPv4, meskipun total alamatnya mencapai 4 miliar, pada kenyataannya tidak

sampai 4 miliar alamat, karena ada beberapa limitasi, sehingga implementasinya saat ini hanya mencapai beberapa ratus juta saja. IPv6, yang memiliki panjang 128-bit, memiliki total alamat yang mungkin hingga 2128=3,4 x 1038 alamat. Total alamat yang sangat besar ini bertujuan untuk menyediakan ruang alamat yang tidak akan habis (hingga beberapa masa ke depan), dan membentuk infrastruktur *routing* yang disusun secara hierarkis, sehingga mengurangi kompleksitas proses *routing* dan tabel *routing*. 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*. Pengalamatan IPv6 didefinisikan dalam RFC 2373.

2.2.11. Format Alamat IPv6

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:

```
00100001110110100000000011010011000000000000000000
01011110011101100000010101010100000000
11111111111111100010100010011100010110 10
```

Gambar 2-8. Alamat IPv6 (*biner*)

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
```

Gambar 2-9. Alamat IPv6 (8 blok)

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

Alamat di atas juga dapat disederhanakan lagi dengan membuang angka 0 pada awal setiap blok yang berukuran 16-bit di atas, dengan menyisakan satu digit terakhir. Dengan membuang angka 0, alamat di atas disederhanakan menjadi:

21DA:D3:0:2F3B:2AA:FF: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 penggunaannya :

Tabel 2-2. Alamat Ipv6

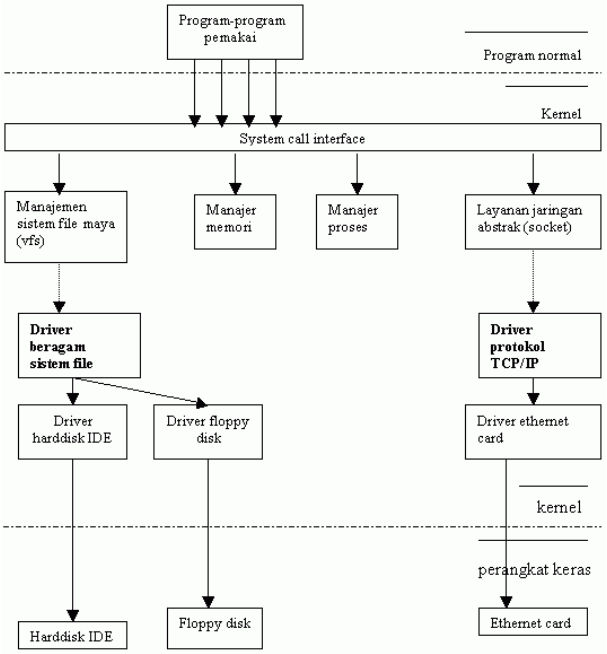
Alamat Asli	Alamat Asli yang Disederhanakan	Alamat yang Telah Dikompress
FE80:0000:0000:0000:02AA:00FF:FE9A:4CA2	E80:0:0:0:2AA:FF:FE9A:4CA2	FE80::2AA:FF:FE9A:4CA2
FF02:0000:0000:0000:0000:0000:0000:0002	FF02:0:0:0:0:0:0:2	FF02::2

Untuk menentukan berapa banyak bit bernilai 0 yang dibuang (dan digantikan dengan tanda dua titik dua) dalam sebuah alamat IPv6, dapat dilakukan dengan menghitung berapa banyak blok yang tersedia dalam alamat tersebut, yang kemudian dikurangkan dengan angka 8, dan angka tersebut dikalikan dengan 16. Sebagai contoh, alamat FF02::2 hanya mengandung dua blok alamat (blok FF02 dan blok 2). Maka, jumlah bit yang dibuang adalah (8-2) x 16 = 96 buah bit.

2.2.12. Linux

GNU/Linux adalah sistem operasi yang dibuat oleh Linus BenedictTorvalds dan disebarkan secara bebas di internet dimana orang lain bisa mengembangkan dan menggunakan untuk keperluannya sendiri. Namun, perlu dijelaskan bahwa GNU/Linux disini bisa bermakna ganda.Pertama, GNU/Linux berarti kernel linux. Pengertian kedua berarti sebuah sistem yang didalamnya sudah terdapat kernel, shell dan program pendukung lain yang siap di distribusikan dan dipakai. GNU/Linux dalam penelitian ini mengacu pada pengertian yang kedua.GNU/Linux adalah sistem operasi yang bebas dipakai, didistribusikan dan dikembangkan kembali. Oleh karena itu, GNU/Linux mempunyai banyak varian yang lebih dikenal dengan istilah distro.

Sistem operasi GNU/Linux terdiri atas kernel linux (inti), program sistem, dan beberapa program aplikasi. Kernel linux merupakan inti dari sistem operasi. Program sistem dan semua program-program lainnya yang berjalan di atas kernel disebut *user mode*. Perbedaan antara program sistem dan program aplikasi adalah program sistem dibutuhkan agar suatu sistem operasi dapat berjalan sedangkan program aplikasi adalah program yang dibutuhkan untuk menjalankan suatu aplikasi tertentu.



Gambar 2-10. Arsitektur SO Linux

2.2.13. Distro Linux

Distro adalah bundel dari kernel linux, beserta sistem dasar linux, program instalasi, *tools basic*, dan program-program lain yang bermanfaat sesuai dengan tujuan pembuatan distro. Menurut fungsi dan target penggunanya, distro dibagi menjadi dua, yaitu :

1. Distro Umum

   Distro umum adalah distro yang dipakai untuk keperluan umum.Distro jenis ini umumnya disebarkan dalam beberapa keping CD/DVD dengan paket *software* yang sangat lengkap. Distro ini bias dipakai untuk keperluan desktop, server ataupun untuk keperluan pengembangan *software*.

2. Distro Khusus

   Distro khusus adalah distro yang ditujukan untuk keperluan khusus seperti untuk keamanan jaringan, pemrograman atau untuk keperluan spesifik lainnya. Umumnya distro-distro ini berukuran kecil dan bias diinstall dimedia floppy disk, USB flashdrive atau didistribusikan dalam mode Live CD/DVD. Contoh distro jenis ini adalah damnsmall Linux, puppy Linux dan openSuSE.

2.2.14. Debian GNU/Linux

Debian adalah Sistem Operasi komputer yang tersusun dari paket – paket perangkat lunak yang dirilis sebagai *free software* dan *open source* dengan mayoritas lisensi GNU *General Public*. Debian GNU/Linux memuat *tools* sistem operasi GNU dan kernel Linux yang didistribusikan dengan akses ke repositori dengan ribuan paket *software* yang siap untuk instalasi dan digunakan. Debian dapat digunakan pada beragam *device* seperti laptop, *desktop*, telepon genggam, hingga komputer server. Hal ini dikarenakan Debian berfokus pada kestabilan dan keamanan sistem operasi, sehingga Debian banyak digunakan sebagai basis dari banyak distribusi GNU/Linux lainnya.

Debian pertama kali diperkenalkan oleh Ian Murdock, seorang mahasiswa dari Universitas Purdue, Amerika Serikat, pada tanggal 16 Agustus 1993. Nama Debian berasal dari kombinasi nama Ian dengan mantan kekasihnya Debra Lynn, yaitu Deb dan Ian.

Pada awalnya Ian memulainya dengan memodifikasi distribusi SLS (*Softlanding Linux System*). Namun ia tidak puas dengan SLS yang telah dimodifikasi olehnyasehingga ia berpendapat bahwa lebih baik membangun sistem (*Linux Distribution*) dari nol. Proyek ini tumbuh dengan sangat lambat karena pada awal rilis bersi 0.9x pada tahun 1994 dan 1995. Pengalihan arsitektur ke selain i386 dimulai pada tahun 1995. Versi 1.x dimulai di tahun 1996.

Tahun 1996, Bruce Perens menggantikan Ian Murdoch sebagai Pemimpin Proyek. Dalam tahun yang sama pengembang Debian Ean Schuessler berinisiatif untuk membentuk Debian Social Contract dan Debian Free Software Guidelines, memberikan standar dasar komitmen untuk pengembangan distribusi Debian. Dia juga membentuk organisasi “Software in Public Interest” untuk menaungi debian secara legal dan berdasarkan hukum.

Di akhir tahun 2000, proyek Debian melakukan perubahan dalam *archive* dan *release management*. Serta pada tahun yang sama para *developer* memulai konferensi dan workshop tahunan yang disebut “debconf”.

Tanggal 8 April 2007 Debian GNU/Linux 4.0 dirilis dengan nama kode “Etch”. Rilis bersi terbaru Debian 2009 diberi nama kode “Lenny”. Dan akhirnya

pada Februari 2011 dirilis *stable release* versi 6.0 dengan kode nama *squeeze*. Untuk versi ini, Tim Keamanan Debian memutakhirkan sistem keamanan.

Sistem operasi Debian merupakan gabungan dari perangkat lunak yang dikembangkan dengan lisensi GNU, dan utamanya menggunakan kernel Linux, sehingga populer dengan nama Debian GNU/Linux. Sistem operasi Debian yang menggunakan kernel Linux merupakan salah satudistro Linux yang populer kestabilannya.

Banyak distribusi Linux lainnya berbasiskan Debian, antara lain Ubuntu, Mepis, Dreamlinux, Damn Small Linux, Xandros, Knoppix, BackTrack, Linspire, dan edisi Debian dari Linux Mint.

Debian dikenal karena pilihannya yang beragam. *Stable Realease* saat ini memuat lebih dari 29000 paket perangkat lunak untuk 9 arsitektur komputer. Debian menggunakan kernel Linux dan juga menggunakan 2 kernel FreeBSD (kfreebsd-i386 and kfreebsd-amd64). Arsitektur komputer ini mulai dari Intel/AMD 32-bit/X86-64bit yang umumnya ditemukan pada komputer pribadi hingga arsitektur ARM yang umumnya ditemukan di sistem *embedded* dan server *mainframe* IBM zSeries.

Fitur yang menonjol dari Debian adalah APT sistem pengaturan paket, repositori dengan jumlah paket yang banyak, kebijakan paket yang ketat, dan kualitas rilis yang terjaga. Praktik ini memungkinkan pemutakhiran yang sederhana di setiap rilis.

Standar instalasi Debian menggunakan GNOME *desktop environment*. Termasuk didalamnya aplikasi OpenOffice.org, Iceweasel, Evolution, program penulisan CD/DVD, *music player and video*, editor, PDF *viewer*.

2.2.15. Multi Router Traphic Grapher (MRTG)

Multi Router Traffic Grapher (MRTG) merupakan suatu *tool* yang digunakan untuk monitoring *traffic load* didalam suatu jaringan. Pengguna dapat melihat laporan dalam bentuk grafik. MRTG ditulis dalam bentuk Perl dan dapat berjalan di UNIX/Linux, dapat juga berjalan di sistem operasi Windows.

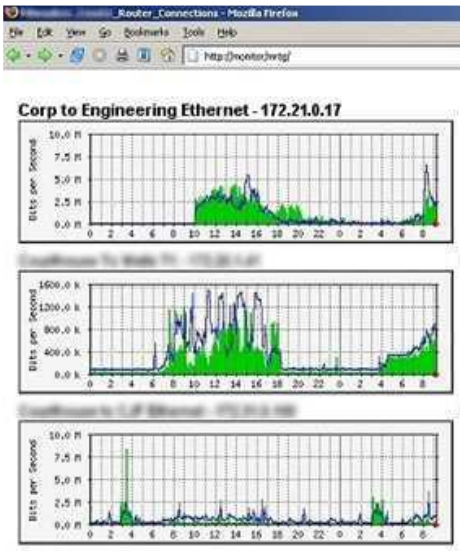
MRTG pertama kali dikembangkan oleh Tobias Oetiker dan Dave Rand. Pertama kali digunakan untuk memonitoring router, namun sekarang sudah dikembangkan untuk memonitoring berbagai macam media transmisi.

MRTG berkembang mendaji RRDTool, yaitu *Round-Robin Database Tool*. Penggunaan RRDTool dapat dikembangkan menjadi berbagai macam aplikasi contohnya cacti, JFFNms dan masih banyak lainnya.

Penggunaan MRTG akan menghasilkan halaman HTML yang berisi gambar yang menyediakan visualisasi secara langsung mengenai keadaan trafik pada suatu jaringan sehingga membantu Administrator jaringan dalam memantau keadaan jaringannya berdasarkan suatu periodik waktu yang telah ditentukan. Hal ini dimungkinkan karena MRTG menyimpan log semua data trafik yang telah dikumpulkan sebelumnya.

CARA KERJA MRTG

Data hasil logging oleh MRTG disimpan dalam file ASCII, file ini akan ditulis ulang selama lima menit sekali sesuai dengan update yang dilakukan oleh MRTG dan secara instant digabungkan dan dianalisis sehingga file logging tersebut membesarnya terkendali. File logging tersebut hanya digunakan untuk menyimpan data yang dibutuhkan untuk menggambarkan grafik pada halaman web. Grafik ini dikonversi ke format GIF dari format PNM. Dibawah ini merupakan contoh grafik dari MRTG :



Gambar 2-11. Tampilan Sistem MRTG

Sebagai aplikasi *monitoring*, MRTG memiliki beberapa fitur yang dapat dimanfaatkan yaitu :

a. Dapat mengukur dua buah nilai (1 untuk *input*, 0 untuk *output*).
b. Mengambil data dengan menggunakan sebuah SNMP agen, atau melalui output yang dihasilkan dari *command line*.
c. Dapat menghasilkan laporan data setiap 5 menit sekali.
d. Menghasilkan sebuah halaman HTML per target, yang menghasilkan tampilan gambar dalam bentuk 4 grafik.
e. Menghasilkan laporan berdasarkan periode waktu tertentu (hari, minggu, bulan, tahun)
f. Secara otomatis dapat menghasilkan skala Y axis dari grafik, untuk menampilkan grafik secara detail.

2.2.16. Squid Proxy Server

Squid adalah sebuah daemon yang digunakan sebagai *porxy server* dan *webcache*. Squid memiliki banyak jenis penggunaan, mulai dari mempercepat server web dengan melakukan *caching* pencarian komputer di dalam jaringan untuk sekelompok komputer yang menggunakan sumber daya jaringan yang sama, hingga membantu keamanan dengan melakukan penyaringan (*filter*) lalu lintas. Meskipun seringnya digunakan untuk protokol HTTP dan FTP, Squid juga menawarkan dukungan terbatas untuk beberapa protokol lainnya termasuk *Transport Layer Security* (TLS), *Secure Socket Layer* (SSL), Internet Grapher, dan HTTPS Versi Squid 3.1 mencakup dukungan protokol Ipv5 dan *Internet Content Adaptation Protocol* (ICAP)

Squid pada awalnya dikembangkan oleh Duane Wessels sebagai "Harvest Object Cache" yang merupakan bagian dari proyek Harvest yang dikembangkan di University Of Collorado at Boulder. Pekerjaan selanjutnya dilakukan hingga selesai di University of California, San diego dan didanai melalui National Science Foundation. Squid kini hampir secara eksklusif dikembangkan dengan cara usaha sukarela.

Squid pada umunya didesain untuk berjalan diatas sistem operasi mirip UNIX, meski squid juga bisa berjalan di atas sistem operasi Windows, karena dirilis di bawah lisensi GNU General Public License, maka Squid merupakan perangkat lunak bebas.

Proxy server adalah sebuah komputer server atau program komputer yang dapat bertindak sebagai komputer lainya untuk melakukan request terhadap content dari internet dan intranet (http://squid.org/)

Proxy server bertindak sebagai gateway terhadap dunia internet untuk setiap komputer client. Dalam menjalankan tugasnya proxy server tidak terlihat oleh komputer client sebagai contoh saat seorang pengguna yang berinteraksi dengan Internet melalui sebuah proxy server tidak akan mengetahui bahwa sebuah proxy server sedang menangani request yang dilakukannya. Web server yang menerima request dari Proxy server akan menginterpresentasikan request-request tersebut seolah-olah datang secara langsung dari komputer client, bukan dari proxy server.

Proxy server dalam suatu jaringan memiliki tiga fungsi utama yaitu sebagai Connection sharing, filtering, dan caching.

a. Connection Sharing

Dalam suatu jaringan lokal yang terhubung ke jaringan lain atau internet, pengguna tidak langsung berhubungan dengan jaringan luar atau internet, tetapi harus melewati suatu gateway, yang bertindak sebagai batas antara jaringan lokal (privat) dan jaringan luar (publik). Gateway ini sangat penting, karena jaringan lokal harus dapat dilindungi dengan baik dari bahaya yang mungkin berasal dari internet, dan hal tersebut akan sulit dilakukan bila tidak ada garis batas yang jelas antara jaringan lokal dan internet. Gateway juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung kepadanya, dan suatu koneksi ke jaringan luar juga terhubung kepadanya. Dengan demikian, koneksi dari jaringan lokal ke internet akan menggunakan sambungan yang dimiliki oleh gateway secara bersama-sama (connection sharing).

b. Filtering

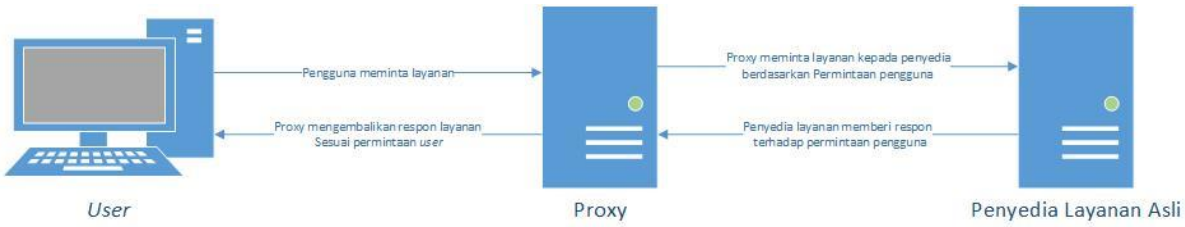
merupakan sebuah usaha pengamanan atau pembatasan sehingga dengan adanya filtering sebuah proxy server dapat mengamankan dan membatasi hak akses client pada jaringan privat. Jadi meskipun mula-mula dibuat sebagai cache nonsekuriti, tujuan utama proxy server sekarang menjadi firewalling. Proxy server memperbarui request layanan pada jaringan eksternal atas nama client mereka pada jaringan private. Ini secara otomatis menyembunyikan identitas dan jumlah client pada jaringan internal dari jaringan eksternal. Karena posisi mereka di antara client internal dan server publik, proxy juga dapat menyimpan content yang sering diakses dari jaringan publik untuk mengurangi akses ke jaringan publik tersebut. Kebanyakan implementasi nyata proxy sekuriti meliputi pemfilteran paket dan Network Address Translation untuk membangun firewall yang utuh. Teknologi tersebut dapat digabungkan dengan proxy untuk menghilangkan serangan yang terhadapnya proxy rentan.

c. Caching (Internet Object caching)

Caching adalah suatu cara untuk menyimpan hasil permintaan internet-object. (seperti: data yang ada dari HTTP, FTP, dan ghoper protokol) untuk membuat sistem dekat dengan permintaan daripada ke sumber aslinya. Web browser dapat menggunakan lokal squid cache sebagai proxy HTTP server, ini akan mengurangi waktu akses seperti halnya penghematan bandwidth. Dengan kata lain sebuah client tidak harus melakukan kontak dengan server untuk meminta layanan akan tetapi client dapat mendapatkan layanan *(data)* yang sudah tersimpan pada proxy server, dengan hal ini maka akses akan semakin cepat.

Squid Proxy Server sendiri adalah software publik domain berbasis UNIX. fungsi dari squid adalah meng-‘cache’ atau menyimpan data yang diminta oleh pengguna (komputer client) biasanya berupa web pages dan FTP. Platform UNIX yang di support oleh Squid adalah FreeBSD, BSDI, Digital Unix, Irix, Linux, Solaris dan SunOs. Tidak semua data bisa di cache oleh Squid, data-data yang bersifat dinamik seperti CGI-BIN tidak di cache oleh Squid, jadi tiap kali ada permintaan CGI-BIN, maka Squid akan menghubungi langsung server tujuan. Saat ini protokol yang bisa dilayani oleh Squid adalah HTTP, FTP, Gopher, dan Wais.

Dari sisi pengguna, proxy sama seperti penyedia layanan asli. Pengguna hanya perlu mengirimkan permintaan layanan, dan proxy akan melayani permintaan tersebut. Namun dalam proses eksekusi layanan tersebut, proxy melakukan permintaan layanan ke penyedia layanan asli. Setelah penyedia layanan asli memberikan respon, lalu proxy akan mengembalikan hasil eksekusi permintaan layanan ke pengguna. Sehingga dari sisi penyedia layanan asli, proxy sama seperti pengguna layanan. Adapun ilustrasinya adalah sebagai berikut :



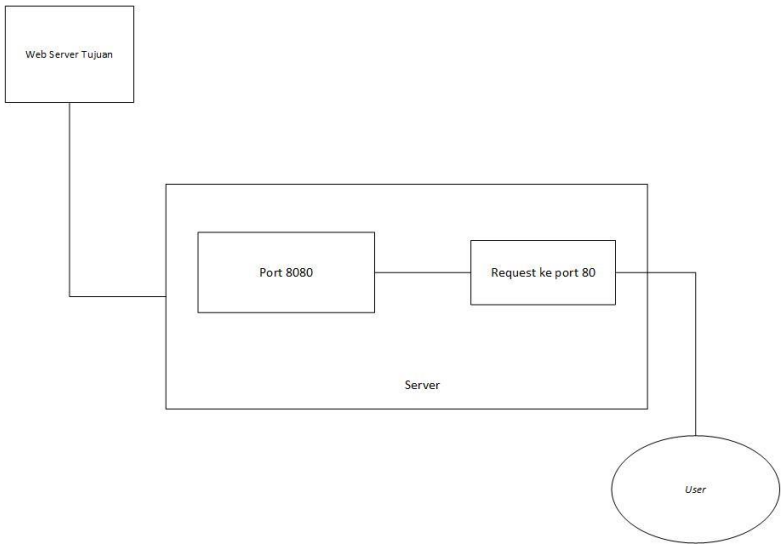
Gambar 2-12. Cara Kerja Proxy

Salah satu komplesitas dari proxy pada level aplikasi adalah bahwa pada sisi pengguna, pengguna diharuskan melakukan konfigurasi yang spesifik untuk suatu proxy tertentu agar bisa menggunakan layanan dari suatu proxy server. Agar pengguna tidak harus melakukan konfigurasi khusus, Admin dapat mengkonfigurasi proxy/cache server agar berjalan secara benar – benar transparan terhadap pengguna (*transparent proxy*).

Dengan adanya *transparent proxy*, pengguna tidak perlu melakukan konfigurasi lebih lanjut karena pengguna benar – benar tidak mengetahui tentang keberadaan proxy ini namun dengan sendirinya pengguna akan menggunakan proxy/cache ini. Cara membuat *transparent proxy* dalah dengan membelokkan arah (*redirecting*) dari paket – paket untuk suatu aplikasi tertentu dengan menggunakan satu atau lebih aturan pada firewall/router. Prinsipnya setiap aplikasi berbasis TCP akan menggunakan salah satu port yang tersedia, dan firewall membelokkan paket yang menuju ke port layanan tertentu, ke arah port dari proxy yang bersesuaian.

Sebagai contoh : saat seorang pegawai Dinas PPPPTK IPA Bandung membuka hubungan HTPP (port 80) dengan suatu web server, firewall pada router yang menerima segera mengenali bahwa ada paket data yang berasal dari klien

dengan nomor port 80. Di sisi lain, admin jaringan Dinas memiliki satu HTTP proxy server yang berjalan di port 8080. Pada firewall router Admin membuat satu aturan yang menyatakan bahwa setiap paket yang datang dari jaringan lokal menuju ke port 80 harus dibelokkan ke arah alamat HTTP proxy server port 8080. Maka semua permintaan web dari pengguna akan masuk dan diwakili oleh HTTP proxy server diatas.



Gambar 2-13. Ilustrasi *Transparent Proxy*

2.2.17. Queue Tree

Dengan metode *Queue Tree*, setiap paket yang akan dialokasikan *bandwidth* nya tidak perlu diurutkan terlebih dahulu. Paket tidak perlu melewati setiap *queue* yang ada. Pada *Queue Tree* semua paket melewati trafik secara bersamaan tanpa harus diurutkan dahulu, oleh karena itu metode ini tidak menghasilkan *delay* yang lebih lama dibanding dengan *Simple Queue*. Adapun perbedaan yang terdapat antara metode *Queue Simple* dan *Queue Tree* adalah :

Queue Simple :

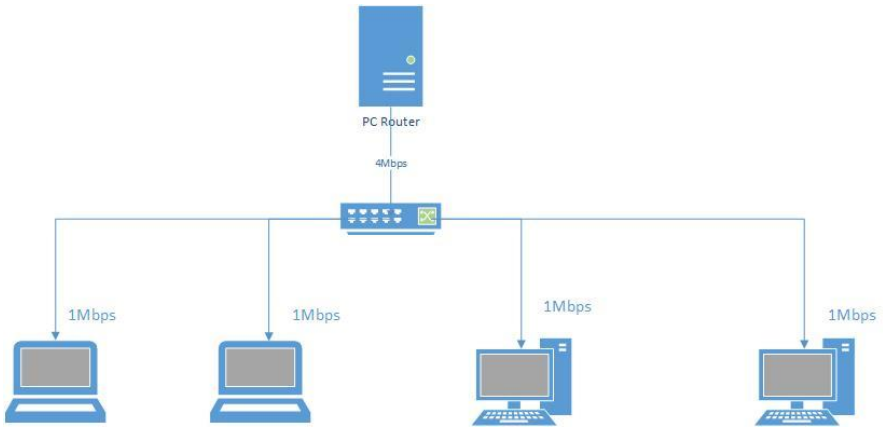
1. Memiliki aturan urutan yang ketat, antrian akan diproses mulai dari yang paling atas hingga paling bawah.
2. Mengatur aliran paket secara *bidirectional* (dua arah)
3. Mampu membatasi trafik berdasarkan IP

4. Satu antrian dapat membatasi trafik 2 arah sekaligus (*upload/download*)

Queue Tree :

1. Tidak memiliki urutan, setiap antrian akan diproses secara bersama-sama
2. Mengatur aliran paket secara *directional* (satu arah)
3. Lebih fleksibel dalam membagi *bandwidth* sehingga dapat dilakukan konfigurasi sesuai dengan kondisi jaringan.
4. Mendukung pengguanaan PCQ (*Per Connection Queue*) sehingga mampu membagi *bandwidth* secara adil dan merata.
5. Mampu membagi *bandwidth* secara *fixed*

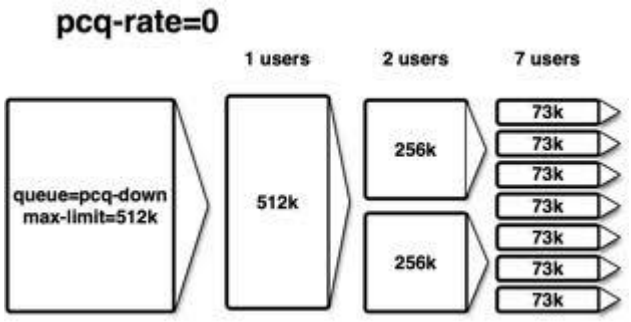
Didalam metode *queue tree* semua layanan alokasi *bandwidth* dilakukan dalam waktu yang bersamaan tanpa melihat urutan antrian sehingga dalam kasus ini semua *host* meski melakukan *request* atau permintaan layanan alokasi *bandwidth* secara bersamaan akan tetap dilayani dalam waktu yang bersamaan. Adapun ilustrasi terhadap prinsip tersebut adlah sebagai berikut :



Gambar 2-14. Ilustrasi *Queue Tree*

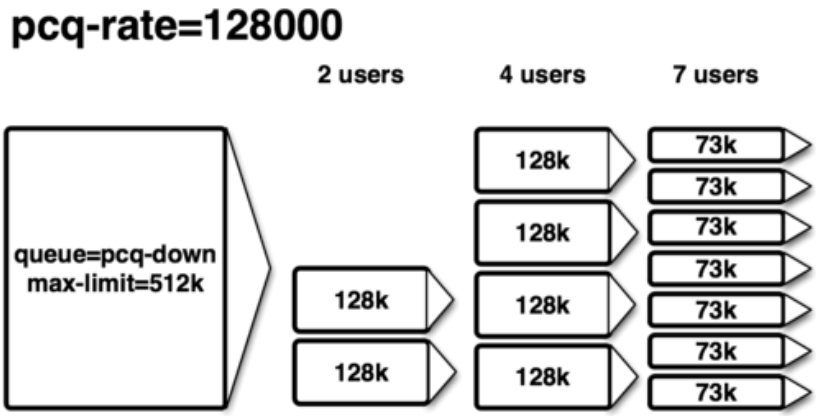
Berdasarkan *point – point* tersebut, pada Metode *Queue Tree* dapat dilihat istilah PCQ (*Per Connection Queue*). PCQ merupakan suatu metode yang

menggunakan konsep antrian/*Queue* untuk menyeimbangkan *bandwidth* yang dipakai pada *multiple client*. Sebagai contoh akan dilakukan alokasi *bandwidth* kepada sejumlah *user* dengan besar total *bandwidth* sebesar 512Kbps, dengan menggunakan prinsip PCQ maka ilustrasinya adalah sebagai berikut :



Gambar 2-15. PCQ rate-0

Berdasarkan ilustrasi tersebut dapat dilihat *bandwidth* tersebut dibagi secara adil kepada setiap *user* yang ada didalam jaringan. PCQ tersebut tidak menggunakan limit atau rate = 0. Apabila PCQ tersebut menggunakan *rate* (pembatasan) maka ilustrasinya sebagai berikut :



Gambar 2-16. PCQ-rate=128000

Ilustrasi tersebut menggambarkan PCQ dengan rate (pembatasan) sebesar 128000. Dapat dilihat pada penggunaan untuk 2 user, pada PCQ dengan rate=0 kedua user menggunakan bandwidth sepenuhnya untuk 2 device, namun dengan

rate = 128000 total bandwidth tersebut diberikan limit sehingga kedua user hanya mendapatkan sebesar 128Kbps.

2.2.18. Protokol SNMP

Simple Network Management Protocol (SNMP) adalah *Internet Protocol Suite* yang dibuat oleh *Internet Engineering Task Force* (IETF) pada sekitar tahun 1988. Tujuan awal diciptakannya protokol SNMP ini adalah untuk memgatur berbagai *device* yang semakin banyak seiring dengan berkembangnya jaringan internet. SNMP dikembangkan untuk menyediakan peralatam manajemen jaringan yang mendasar dan mudah diimplementasikan untuk rangkaian protokol jenis *Transpor Control Protocol/ Internet Protocol* (TCP/IP). SNMP merupakan protokol dari lapis aplikasi yang digunakan untuk *network management system* untuk memonitor perangkat jaringan sehingga dapat memberikan informasi yang dibutuhkan bagi pengelolanya. SNMP mencakup protokol yang aktual, definisi informasi yang ditangani (*managed information*) dan komponen – komponen terkait lainnya.

Server Manajemen SNMP dapat melakukan tes untuk memeriksa status antara perangkat jaringan yang merupakan fungsi pada lapis fisik. Pada lapis *Data Link, Server* manajemen SNMP dapat digunakan untuk mengkonfigurasi, mengaktifkan, dan mematikan jaringan. *Server* manajemen dapat menerima *frame* keluar dan masuk, dan perhitungan *error* pada setiap perangkat. *Server* manajemen SNMP bekerja pada lapis *Network* dengan memeriksa IP *address assignments, address translation tables, and routing tables*. Dengan demikian, *server* manajemen SNMP dapat menghitung trafik IP dan *error*. Di lapis *transport*, *server* manajemen SNMP dapat durasi koneksi TCP pada sistem sehingga dapat menghitung trafik TCP dan UDP serta *error* yang terjadi.

Dengan demikian SNMP dapat digunakan untuk pengawasan, pengkoleksian statistik, pemeriksa unjuk kerja dan keamanan dari suatu jaringan. Untuk melakukan fungsi – fungsi tersebut SNMP dibagi menjadi tiga bagian yang bekerja sama satu sama lain yaitu *managed device*, agen dan *Network Management System* (NMS). Berikut ini deskripsi mengenai fungsi dari ketiga elemen tersebut:

a. *Managed device*

Managed device adalah node jaringan yang memiliki SNMP agen dan berada dalam jaringan yang dimanajemen. *Managed device* akan mengumpulkan informasi yang nantinya bisa diakses oleh NMS dengan menggunakan SNMP. *Managed device* bisa berupa router, switch, hub, ethernet/NIC, ataupun elemen *network* lainnya.

b. Agen

Agen merupakan *software* untuk manajemen *network* yang berada di *managed device.* Agen berperan untuk menerjemahkan informasi kedalam "bahasa" yang kompatibel dengan SNMP.

c. *Network Management Stations*

Network Management Server adalah bagian dalam jaringan yang akan melakukan pengawasan ataupun mengatur *managed device*. Istilah lain dari *Network Management Station* adalah *Network Management Server*.

2.2.19. Managed Object

Berikut ini merupakan tiga atribut yang merepresentasikan sebuah *managed object* atau yang sering juga disebut dengan *managed device,* yaitu :

a. Nama

Nama atau *object identifier* (OID) dengan jelas mendefinisikan sebuah *managed object.* Nama – nama ini umumnya dipakai dalam dua bentuk yaitu *numeric* dan "*human readable"*.

b. Tipe dan Sintaks

Tipe data dari sebuah *managed object* merupakan subset dari *Abstract Syntax Notation One* (ASN.1) merupakan cara untuk menspesifikasikan bagaimana data direpresentasikan dan dikirimkan antara manajer dan agen. Tipe dan sintaks dari ASN.1 bersifat independent sehingga komputer dengan sistem operasi yang berbeda dapat saling berkomunikasi.

c. *Encoding*

Sebuah *managed object* di-*encoded* ke sebuah *string* menggunakan Basic Encoding Rules (BER). BER mendefinisikan bagaimana objek di-*encoded* dan

di-*decoded* maka *object* tersebut ditransmisikan melalui media transport seperti *Ethernet*.

2.2.20. Manajer SNMP

Manajer SNMP merupakan *platform* sistem manajemen atau pelaksana dari manajemen jaringan, pada kenyataannya manajer ini merupakan komputer biasa yang ada pada jaringan yang mengoperasikan perangkat lunak untuk manajemen jaringan. Manajer ini terdiri atas satu proses atau lebih yang berkomunikasi dengan agen – agennya dan berfungsi untuk mengumpulkan informasi dari agen dalam jaringan. Manajer akan mengumpulkan informasi dari jaringan yang diminta oleh Administrator saja dan bukan semua informasi yang dimiliki oleh agen. Bila seorang administrator melakukan peran pemantauan terhadap suatu jaringan, maka manajer SNMP akan meminta kepada agen untuk menjalankan peran sebagai pemantau, dan bukan sebagai pengontrol, jadi operasi pelaporan agen kepada manajer hanya berupa "*read only running system*" dan bukan "*system setting*". Banyak manajer saat ini memiliki antarmuka pengguna teks dan grafis dengan sistem pelaporan sederhana yang memungkinkan manajer jaringan memeriksa status jaringan dan mengambil tindakan tertentu bila diperlukan.

Manajer SNMP bertanggungjawab untuk melakukan pengaksesan, modifikasi atau menerima informasi dari agen – agen yang dikelola. Sama juga halnya dengan agen, manajer SNMP dapat melakukan dua peran. Pada peran pemantauan, manajer SNMP hanya meminta dan menerima laporan berupa informasi dari agen – agen yang dikelola. Sedangkan pada peran pengontrolan, manajer SNMP dapat melakukan berbagai modifikasi terhadap agen – agen yang dikelola. Manajer dan agen mungkin bisa tinggal satu atap serta dapat bekerja dalam entitas atau kesatuan manajemen yang sama. Manajer bertanggung jawab secara khusus untuk mengatur atau menjalankan serangkaian atau sebidang tugas agen. *Platform* pemantauan manaher SNMP yang baik harus menyediakan beberapa komponen dasar berikut, yaitu :

a. *Polling*

Polling adalah kemampuan untuk mengatur *thresholds* pada objek MIB SNMP dan memberikan respon dengan beberapa tipe notifikasi ketika *thresholds* tersebut dilewati. Tujuan dari fungsi ini adalah kemampuan untuk menentukan perangkat mana yang memberikan respon (misalnya: perangkat mana yang sedang online) dan perangkat mana yang tidak memberikan respon, misalnya sedang rusak.

b. *Monitoring*

Monitoring adalah kemampuan untuk secara terus menerus mengawasi nilai SNMP sepanjang waktu, mengumpulkan contoh nilai pada interval periodik untuk melihat trend jaringan. Fungsin ini digunakan untuk menentukan keluaran dari jaringan sepanjang waktu (dengan mengawasi *bandwith*).

c. *Tool Set*

Tool Set adalah *tool* manajemen tradisional dari SNMP adalah MIB *browser*, yang mengijinkan administrator melihat objek MIB pada kelompok perangkat tertentu. Hal ini prinsip dasar antarmuka utnuk mengatur nilai pada SNMP agen dan secara aktual perubahan pada jaringan melalui SNMP.

d. *MIB Compiler*

MIB *Compiler* (*Management Information Base Compiler*) adalah kemampuan menambahkan objek MIB baru yang disediakan oleh perangkat jaringan tertentu. Dalam hal ini MIB *compiler* ekstensi khusus agar perangkat jaringan dari *vendor* tersebut dapat diamati.

SNMP memiliki kemampuan untuk melakukan *polling* (menannyakan kondisi) pada perangkat dan mengambil informasi – informasi manajemen dari perangkat tersebut. SNMP dapat melakukan *internal polling* atau *external polling*. *Internal Polling* digunakan pada aplikasi yang berjalan sebagai sebuah *daemon* yang secara periodik dijalankan pada aplikasi lokal. *External polling* dikerjakan oleh NMS. *OpenView* NMS menyediakan implementasi luar biasa pada *external*

polling karena dapat menggambarkan dan menyimpan data untuk mengingatkan administrator jaringan jika terjadi sesuatu yang salah pada jaringan.

Proses *Polling* membutuhkan alokasi *bandwith* yang tidak sedikit terlebih jika pada suatu jaringan terdapat ratusan atau ribuan perangkat yang akan di-*polling* . karena itu diperlukan *internal polling* untuk menangani perangkat lokal. *Internal polling* berjalan dengan agen internal atau *built-in* pada perangkat yang dimanajemen. Selama *polling* tersebut merupakan bagian dalam internal perangkat, maka tidak dibutuhkan trafik antara agen dan NMS. Namun untuk hak teknikal dan keamanan pada jaringan tidak mungkin dapat dilakukan *polling* sebuah perangkat secara internal. Untuk itu diperlukan *external polling* untuk mengkoleksi informasi dari setiap perangkat lokal, *external polling* dapat melibatkan satu atau lebih NMS atau banyak mesin.

2.2.21. Management Information Base (MIB)

MIB adalah sekumpulan informasi yang teratur tentang keberadaan seluruh peralatan jaringan. Semua informasi yang diakses atau dimodifikasi melalui agen sama dengan MIB. Informasi – informasi tersebut akan diambil oleh agen dan diberikan kepada manajer SNMP berdasarkan permintaan. Tidak semua informasi yang ada pada MIB diberikan oleh agen, akan tetapi berdasarkan tindakan yang dilakukan oleh manajer SNMP. MIB terdiri dari informasi sekumpulan objek – objek yang diatur (*managed object*) dan memiliki pengidentifikasian yang unik yang disebut dengan MIB *Object identify*.

Untuk setiap objek MIB akan muncul definisi MIB yang menentukan objek secara terstruktur. Struktur MIB bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi atau variabel setiap objek dapat dikelola dengan mudah. Untuk memudahkan proses pengelolaan informasi, objek – objek ini dikelompokkan menjadi sepuluh kelompok. Kesepuluh kelompok tersebut dimaksudkan untuk menyediakan basis tentang apa yang harus dimengerti oleh stasiun manajemen (manajer atau *platform* antarmuka aplikasi manajemen).

Kelompok baru dan objek baru akan secara pasti ditambah di masa depan. Dan *vendor* mempunyai kebebasan untuk menentukan objek – objek tambahan bagi

produknya. Pada awalnya MIB hanya berisikan objek – objek dari sekelompok sistem. Pada kelompok sistem, agen akan menginformasikan kepada manajer SNMP dengan *platform* antar muka tertentu, utnuk mengizinkan administrator untuk mengetaui alamat IP *address*, nama peralatan baik *hardware* maupun *software* yang dikandung, nama penanggungjawab, lokasi dan tugas – tugas yang perlu dikerjakan, dan memeriksa kesalahan sehingga dapat diperbaiki secepat mungkin dengan waktu yang relatif singkat.

2.2.22. Manajer dan Agen

Dalam SNMP, Manajer dan agen merupakan perangkat yang mengelola informasi yang diberikan oleh *managed device*. Manajer merupakan sebuah *server* yang berjalan dengan berbagai jenis *software* yang dapat melakukan tugas – tugas manajemen pada suatu jaringan. Manajer sering disebut sebagai *Network Management Station* (NMS). Sebuah NMS bertanggung jawab untuk polling dan menerima *traps* dari agen pada jaringan. Sebuah polling, dalam konteks manajemen jaringan adalah tindakan menanyakan keadaan (*querying*) pada agen untuk beberapa informasi dari *managed device* seperti *router, switch, Unix server,* dan lainnya. Informasi ini dapat berguna untuk menentukan apakah terjadi permasalahan pada jaringan. *Trap* merupakan cara agen memberitahukan NMS jika sesuatu terjadi. *Trap* dikirimkan secara asinkron, dan bukan merupakan tanggapan *query* yang dikirimkan oleh NMS. NMS akan bertanggung jawab untuk melakukan tindakan berdasarkan informasi yang diterima dari agen. Sebagai contoj ketika kinerja perangkat TI ke internet berkurang, maka router dapat mengirim *trap* ke NMS. Kemudian NMS melakukan tindakan untuk memberitahukan apa yang terjadi kepada administrator jaringan.

Agen merupakan *software* yang dapat berjalan pada perangkat jaringan yang dimanajemen. Agar menyediakan informasi untuk NMS dengan mengawasi beragam aspek operasional perangkat. Sebagai contoh, agen pada router mampu mengawasi keadaan dari setiap *interface* (perangkat antar muka), yang mana yang aktif dan yang mana yang tidak aktif. NMS dapat menanyakan status dari setiap *interface* dan melakukan sesuatu ketika ada dari perangkat – perangkat tersebut

yang padam. Ketika agen memutuskan telah terjadi sesuatu yang buruk, agen mengirimkan *trap* kepada NMS. Beberapa perangkat akan mengirimkan *trap* yang berbunyi "*all clear"* sebagai respon ketika telah terjadi perubahan dari *bad state* ke *good state*. Hal ini sangat berguna dalam menentukan apakah permasalahan telah teratasi.

2.2.23. Bandwith

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 *user* yang dapat digunakan menjadi parameter untuk menghitung jumlah peralatan yang dibutuhkan 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 berhubungan 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*.

Terdapat dua jenis *bandwidth* yaitu :

a. *Digital Bandwidth,* adalah jumlah atau volume data yang dapat dikirimkan melalui sebuah saluran komunikasi dalam satuan bits persecond tanpa distorsi.
b. *Analog Bandwidth,* adalah perbedaan antara frekuensi terendah dengan frekuensi tertinggi dalam sebuah rentang frekuensi yang diukur dalam satuan Hertz (Hz) atau siklus per detik, yang menentukan berapa banyak informasi yang bisa ditransimisikan dalam satu saat.

2.2.24. Management Bandwidth

Manajemen bandwidth adalah suatu alat yang dapat digunakan untuk management dan mengoptimalkan berbagai jenis jaringan dengan menerapkan layanan Quality Of Service (QoS) untuk menetapkan tipetipe lalu lintas jaringan.

Maksud dari manajemen bandwidth adalah bagaimana menerapkan pengalokasian atau pengaturan bandwidth dengan menggunakan sebuah PC Router. Manajemen bandwidth memberikan kemampuan untuk mengatur bandwidth jaringan dan memberikan level layanan sesuai dengan kebutuhan dan prioritas sesuai dengan permintaan pelanggan.

2.2.25. Quality of Service (QOS)

Quality of Service (QoS) adalah kemampuan untuk menggambarkan suatu tingkatan pencapaian didalam suatu sistem komunikasi data. QoS biasanya digunakan untuk mengukur sekumpulan attribut performansi yang telah di spesifikasikan dan biasanya diasosiasikan dengan suatu servis. Pada jaringan berbasis IP, IP QoS mengacu pada performansi dari paket-paket IP yang lewat melalui satu atau lebih jaringan.

QoS didesain untuk membantu pemakai menjadi lebih produktif dengan memastikan bahwa dia mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan.

QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. QoS merupakan suatu tantangan yang cukup besar dalam jaringan berbasis IP dan internet secara keseluruhan. Tujuan dari QoS adalah untuk memuaskan kebutuhan - kebutuhan layanan yang berbeda, yang menggunakan infrastruktur yang sama. QoS menawarkan kemampuan untuk mendefinisikan atribut-atribut layanan jaringan yang disediakan, baik secara kualitatif maupun kuantitatif

2.2.26. Terminologi QOS

Terminologi Qos diklasifikasikan ke dalam 3 area, antara lain layanan (service), jaringan (network), dan manjemen (management).

1. QoS yang berhubungan dengan kualitas layanan (service) terdiri dari kecepatan pemrosesan (speed), tingkat ketepatan (accuracy), tingkat kepastian atau jaminan (dependability), ketersediaan (availability), keandalan (reliability), kemudahan (simplicity) dan sebagainya.
2. QoS yang berhubungan dengan jaringan (network) terdiri dari network accessibility, connection accessibility, connection error probability, connection failure probability, misrouting probability bit error ratio, transmission performance dan sebagainya.
3. QoS yang berhubungan dengan manajemen (management) terdiri dari resource management, class of service, customer relationship management, benchmark, service level agreement, time between interruptions, interruption duration, mean time between interruption, mean time to restoration, fault coverage, repair coverage, maintenance, disaster recovery, complaint, directory service dan sebagainya.

2.2.27. PC Desktop

PC *desktop* adalah komputer personal yang digunakan untuk menjalankan aplikasi *desktop* grafis dalam keperluan sehari-hari. Aplikasi yang dijalankan umumnya merupakan aplikasi yang membutuhkan kualitas grafis yang cukup tinggi. PC *desktop* memiliki perangkat keras yang lebih lengkap bila dibandingkan dengan laptop ataupun tablet PC. PC *desktop* memiliki ruangan yang jauh lebih luas untuk dilengkapi dengan drive-drive seperti CD-rom CD-*rewriter*. Namun, PC dekstop memiliki kekurangan, yaitu tidak bersifat portabel sehingga kurang praktis untuk dibawa bepergian.

PC *desktop* membutuhkan system operasi grafis karena aplikasi yang dijalankan umumnya menuntut antarmuka grafis. Aplikasi Internet saat ini pun umumnya membutuhkan antarmuka grafis yang cukup tinggi. Selain itu, PC *desktop* saat ini juga dituntut untuk mampu menjalankan aplikasi multimedia sehingga memberikan kenyamanan yang optimal dalam penggunaannya.

PC *desktop* umumnya dilengkapi dengan harddisk tersendiri dimana sistem operasi dan data tersimpan. Namun, ada juga PC *desktop* yang tidak membutuhkan

hardisk atau sering disebut dengan jaringan *diskless workstation*. *Diskless workstation* membutukan jaringan dengan sistem operasi Unix atau Windows NT.

2.2.28. Network Interface Card (NIC)

Network Inteface Card (NIC) atau LAN *Card* adalah sebuah kartu yang terpasang pada sebuah komputer sehingga komputer tersebut mampu terkoneksi pada jaringan. NIC menyediakan antarmuka ke media. NIC bisa menggunakan *transceiver eksternal* atau melalui *transceiver internal* terintegrasi yang dipasang pada *Network Interface Card* PCB. NIC biasanya juga dilengkapi protokol *control firmware* dan *Ethernet Controller* yang dibutuhkan untuk mendukung protokol *data-link Medium Access Control* (MAC) yang digunakan Ethernet. Setiap NIC mendapatkan *Ethernet source address* dari perusahaan pembuat NIC (biasanya disimpan di ROM pada NIC*). Address* tersebut bersifat unik secara global. Ada sekitar 16 blok (atau 8 juta) *address* yang disediakan oleh perusahaan pembuat NIC berdasarkan struktur *addressing flat.* Hal ini untuk memastikan bahwa tidak ada dua *Ethernet Network Interface* (NIC) yang akan mempunyai *source Address* yang sama.

Pada komputer personal dan *workstation* dalam suatu *Local Area Network* (LAN) biasanya terpasang *Network Interface Card* yang di desain khusus untuk transmisi data pada LAN. Teknologi pada LAN card yang umumnya digunakan adalah *Ethernet* atau *Token Ring*. Kebanyakan LAN card yang ada dipasaran menggunakan teknologi *Ethernet* sehingga banyak orang yang menyebut *Network Inteface Card* (NIC) sebagai Ethernet Card. Teknologi *Ethernet* dikembangkan oleh ternama Xerox.

Standard IEEE 802.3 menentukan Ethernet berdasarkan fisik dan lapisan data link pada model OSI. Sebagian besar *system Ethernet* menggunakan :

a. *Carrier-sense multiple-access with collision detection* (CSMA/CD) untuk mengontrol akses ke media jaringan.
b. *Broadcast base band*
c. Metode pemaketan data menjadi paket data yang disebut frame.
d. Kecepatan transmisinya 10Mbps, 100Mbps dan 1Gbps.

Tipe – tipe *Ethernet* :

a. 10Base5, tipe kartu *Ethernet* menggunakan kabel koaksial dengan diameter 0,5 inci dan berwarna kuning. Topologi yang digunakan menggunakan Topologi *Bus*. Jangkauan jarak maksimum 500 meter. Apabila ditambahkan *repeater* (penguat) akan dapat mencapai jarak ±2,5 km. Kecepatan transmisi data 10 Mbps.
b. 10Base2, tipe kartu *Ethernet* menggunakan kabel koaksial dengan diameter 5 mm. Topologi yang digunakan berbentuk *bus*. Jangkauan jarak maksimum 185 m dan kecepatan transmisi data 10 Mbps.
c. 10BaseT, tipe kartu *Ethernet* menggunakan kabel *twisted pair*. Topologi yang digunakan adalah *Star*. Jangkauan jarak maksimum 100 m dan kecepatan transmisi data 100 Mbps.
d. 10BaseF, tipe *Ethernet* yang menggunakan kabel serat optik *(fiber optic*). Topologi yang digunakan adalah *star*. Jangkauan jarak sampai dengan 2000 m. Untuk transmisi *output* dan *input* menggunakan kabel yang berbeda. Kecepatan transmisi data mencapai 100 Mbps.
e. 100BaseT series, tipe *Ethernet* menggunakan kabel *twisted pair*. Tipe ini memiliki beragam metode akses. Kecepatan transmisi data mencapai 20-200 Mbps.

2.2.29. Hub

Hub adalah alat yang berfungsi sebagai tempat untuk menerima data dan meneruskannya menuju tempat yang lain. Hub terdiri dari port-port RJ-45 *female* sehingga kabel-kabel *twisted pair* yang sudah terpasang konektor RJ-45 pada ujung-ujungnya dapat dengan mudah ditancapkan pada *hub*. *Hub* digunakan pada topologi *star* dan dapat diparalel hingga maksimum tiga buah *hub*. *Hub* dipasaran beredar dengan jumlah 5 *port, 10 port*, 12 *port*, 16 *port*, 24 *port*, 32 *port* dan yang terbesar 64 *port*. Untuk jaringan yang menggunakan *hub* yang diparallel lebih dari tiga buah, diperlukan sebuah *router* untuk menghubungkan *hub* yang keempat.

2.2.30. Switch

Switch atau *switch hub* pada dasarnya adalah *hub* juga. *Switch* memiliki kemampuan untuk mentransfer data hanya pada *port* yang dituju saja, berbeda dengan *hub* yang mem-*broadcast* data yang datang ke semua *port* yang dimiliki termasuk *port* tempat data tersebut berasal. Perbedaan ini membuat *switch* lebih cepat dalam mentransferkan data walaupun memiliki kecepatan yang sama dengan *hub*. Dengan sistem teknologi *Etherne*t dalam sebuah LAN, *switch* akan membedakan alamat komputer tempat data tersebut berasal dan alamat komputer (MAC *Addres*s atau *Media Access Control Address*) tempat data tersebut dituju.

Pada jaringan yang luas atau Internet, *switch* akan membedakan IP asal dan IP tujuan ke data tersebut.

Pada suatu LAN yang menggunakan model OSI, *switch* melakukan fungsi komunikasi layer 2 atau data-link layer. Namun, pada jaringan luas atau Internet, *switch* membutuhkan sebuah *router* untuk dapat meneruskan paket datanya. Beberapa s*witch* model terbaru mampu melakukan komunikasi layer 3 atau melakukan fungsi *routing* sehingga disebut IP *switch*. Kehadiran *switch* menggeser keberadaan hub sehingga di pasaran saat ini lebih banyak ditemui *switch* karena dengan selisih harga yang sedikit, menawarkan kinerja yang lebih baik dibandingkan *hub*.

2.2.31. Router

Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing.* Proses *routing* terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protokol) dari stack protokol tujuh-lapis OSI. *Router* berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. *Router* berbeda dengan switch. Switch merupakan penghubung beberapa alat untuk membentuk suatu Local Area Network (LAN).

Sebagai ilustrasi perbedaan fungsi dari *router* dan *switch* adalah *switch* merupakan suatu jalanan, dan *router* merupakan penghubung antar jalan. Masing-

masing rumah berada pada jalan yang memiliki alamat dalam suatu urutan tertentu. Dengan cara yang sama, *switch* menghubungkan berbagai macam alat, dimana masing-masing alat memiliki alamat IP sendiri pada sebuah LAN.

Router sangat banyak digunakan dalam jaringan berbasis teknologi protokol TCP/IP, dan *router* jenis itu disebut juga dengan IP *Router*. Selain IP *Router*, ada lagi AppleTalk *Router*, dan masih ada beberapa jenis *router* lainnya. Internet merupakan contoh utama dari sebuah jaringan yang memiliki banyak *router* IP. *Router* dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan *Internet-work*, atau untuk membagi sebuah jaringan besar ke dalam beberapa sub-*network* untuk meningkatkan kinerja dan juga mempermudah manajemennya. *Router* juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan media yang berbeda atau berbeda arsitektur jaringan, seperti halnya dari *Ethernet* ke Token Ring.

Router juga dapat digunakan untuk menghubungkan LAN (*Local Area Network*) ke sebuah layanan telekomunikasi seperti halnya telekomunikasi *leased line* atau DSL (*Digital Subscriber Line*). *Router* yang digunakan untuk menghubungkan LAN (*Local Area Network*) ke sebuah koneksi *leased line* seperti T1, atau T3, sering disebut sebagai *access server*. Sementara itu, *router* yang digunakan untuk menghubungkan jaringan lokal ke sebuah koneksi DSL (*Digital Subscriber Line*) disebut juga dengan DSL (*Digital Subscriber Line*) *router*. Router-router jenis tersebut umumnya memiliki fungsi *firewall* untuk melakukan penapisan paket berdasarkan alamat sumber dan alamat tujuan paket tersebut, meski beberapa *router* tidak memilikinya. *Router* yang memiliki fitur penapisan paket disebut juga dengan packet *filtering router*. *Router* umumnya memblokir lalu lintas data yang dipancarkan secara *broadcast* sehingga dapat mencegah adanya *broadcaststorm* yang mampu memperlambat kinerja jaringan.

2.2.32. Bridge

Pengertian dari sebuah *bridge* adalah bekerja pada *data link layer* pada OSI. *Bridge* adalah alat yang digunakan pada suatu jaringan yang berfungsi untuk memisahkan sebuah jaringan yang luas menjadi segment yang lebih kecil. Bridge

membaca alamat MAC (*media access control*) dari setiap paket data yang diterima yang kemudian akan mempelajari *bridging table* untuk memutuskan apa yang akan dikerjakan *bridge* selanjutnya pada paket data tersebut, apakah diteruskan atau diabaikan. jika *switch* menpunyai *domain collision* sendiri-sendiri di setiap portnya, begitu juga dengan *bridge* memiliki *domain collision* tetapi ia juga dapat membaginya dari sebuah *domain collision* yang besar menjadi yang lebih kecil, dan *bridge* hanya akan melewatkan paket data antar *segment - segment* jika hanya *segment* itu sangat diperlukan terdapat tiga jenis *bridge* jaringan yang umum dijumpai :

a. Bridge lokal : sebuah bridge yang dapat menghubungkan segmen – segmen jaringan lokal.
b. Bridge remote : dapat digunakan untuk membuat sebuah sumbangan (link) antara LAN (*Local Area Network*) untuk membuat sebuah *Wide Area Network*.
c. Bridge Nirkabel : sebuah bridge yang dapat menggabungkan jaringan LAN (*Local Area Network*) berkabel dan jaringan LAN nirkabel.

2.2.33. Repeater

Repeater adalah sebuah *device* yang meregenerasi/menghasilkan kembali sinyal yang ditransmisikan pada kabel. *Repeater* mengijinkan sinyal untuk mengalir diluar batas keterbatasan panjang kabel. Sebuah repeater tidak melakukan translasi atau filterisasi paket. *Repeater* mempunyai beberapa karakteristik antara lain :

a. Digunakan untuk meregenerasi sinyal *baseband* yang ada
b. Digunakan terutama pada topologi *bus koaksial* (linear) segmen yang dihubungkan oleh sebuah repeater.
c. Harus menggunakan metode *media access control* (MAC) yang sama (misalnya, sebuah repeater tidak bisa melewatkan *traffic* antara *Ethernet* dan *token ring*) *Repeater* bisa melewatkan *traffic* antara beberapa media yang berbeda (misalnya, c*oax* ke *fiber optic*).

d. Jika *Interface* yang sesuai tersedia repeater tidak melakukan akselerasi atau mengubah sinyal, ia hanya meregenerasinya saja.
e. Repeater tidak melalukan *filter packet* atau batasan kongesti/kemacetan.
f. Repeater akan melewatkan paket *broadcast.*
g. Repeater beroperasi di *physical* layer pada model OSI fungsi dasar dari repeater (regenerasi sinyal) bisa dilakukan oleh *device-device* penghubung (misalnya hub atau bridge).

Karena repeater tidak melakukan apa-apa terhadap filterisasi atau pembatasan *traffic*, ia seharusnya dilihat terutama sebagai penghubung workstasion yang jauh, tidak sebagai penambah workstasion tambahan. Dengan kata lain, *repeater* seharusnya digunakan untuk menambahkan jarak dari *network*, bukan kepadatannya.

2.2.34. Access Point

Digunakan untuk melakukan pengaturan lalu lintas jaringan dari *mobile radio* ke jaringan kabel atau dari *backbone* jaringan *wireless client/server*.Biasanya berbentuk kotak kecil dengan 1 atau 2 antena kecil. Peralatan ini merupakan *radio based*, berupa *receiver* dan *transmiter* yang akan terkoneksi dengan LAN (Local Area Network) kabel atau *broadband Ethernet*. Saat ini beredar di pasaran adalah *access point* yang telah dilengkapi dengan *router* di dalamnya yang biasa disebut *wireless rout*er.

2.2.35. Modem

Modem berasal dari singkatan *Modulator Demodulator*. *Modulator* merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (*carrier*) dan siap untuk dikirimkan, sedangkan *Demodulator* adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik. Modem merupakan penggabungan kedua-duanya, artinya modem adalah alat komunikasi dua arah. Setiap perangkat komunikasi jarak jauh dua-arah umumnya menggunakan bagian yang disebut "modem", seperti VSAT, *Microwave Radio*, dan lain sebagainya, namun umumnya istilah modem lebih dikenal sebagai Perangkat keras

yang sering digunakan untuk komunikasi pada komputer. Data dari komputer yang berbentuk sinyal digital diberikan kepada modem untuk diubah menjadi sinyal analog. Sinyal analog tersebut dapat dikirimkan melalui beberapa media telekomunikasi seperti telepon dan radio. Setibanya di modem tujuan, sinyal analog tersebut diubah menjadi sinyal digital kembali dan dikirimkan kepada komputer. Terdapat dua jenis modem secara fisiknya, yaitu modem eksternal dan modem internal. Terdapat beberapa jenis modem yaitu :

a. Modem analog yaitu modem yang mengubah sinyal analog menjadi sinyal digital.
b. Modem ADSL (*Asymetric Digital Subscribe Line*) yaitu modem yang memungkinkan berselancar Internet dan menggunakan telepon analog secara berbarengan. Caranya sangat mudah, untuk ADSL diberikan sebuah alat yang disebut sebagai *Splitter* atau pembagi *line*. Posisi *Splitter* ditempatkan di depan ketika *line* telepon masuk. Artinya anda tidak boleh mencabangkan *line* modem untuk ADSL dengan suara secara langsung. Alat *Splitter* berguna untuk menghilangkan gangguan ketika anda sedang menggunakan ADSL modem. Dengan *Splitter* keduanya dapat berjalan bersamaan, sehingga pengguna dapat menjawab dan menelpon seseorang dengan telepon biasa. Di sisi lain, pengguna tetap dapat terkoneksi dengan Internet melalui ADSL modem.
c. Modem kabel yaitu modem yang menerima data langsung dari penyedia layanan lewat TV Kabel.
d. Modem CDMA yaitu modem *dial up wireless* yang bekerja pada teknologi CDMA (*Code Division Multiple Access*)

2.2.36. Media Transmisi

Media transmisi adalah media yang dapat digunakan untuk mengirimkan informasi dari suatu tempat ke tempat lain. Dalam jaringan, semua media yang dapat menyalurkan gelombang listrik atau elektromagnetik atau cahaya dapat dipakal sebagai media pengirim, baik untuk pengiriman dan penerimaan

data.Pilihan media transmisi (pengirim) untuk keperluan komunikasi data tergantung pada beberapa faktor, seperti harga, Performance jaringan yang dikehendaki, ada atau ada tidaknya medium tersebut. Beberapa jenis media transmisi akan dibahas pada *point* selanjutnya.

2.2.37. Copper Media

Copper media merupakan semua media transmisi data yang terbuat dari bahan tembaga. Orang biasanya menyebut dengan nama kabel. Data yang dikirim melalui kabel, bentuknya adalah sinyal listrik (tegangan atau arus) digital.

Jenis – Jenis kabel yang dipakai sebagai transmisi data pada jaringan :

a. Koaksial
b. STP
c. UTP

2.2.38. Kabel Koaksial

Kabel ini sering digunakan sebagai kabel antena TV. Disebut juga sebagai kabel BNC (*Bayonet Naur Connector*). Kabel ini merupakan kabel yang paling banyak digunakan pada LAN (*Local Area Network*), karena memiliki perlindungan terhadap derau yang lebih tinggi, murah, dan mampu mengirimkan data dengan kecepatan standar . Ada 2 jenis yaitu RG-58 (10Base2) dan RG-8 (10Base5). Ada 3 jenis konektor pada kabel Coaxial, yaitu T konektor, I konektor (*socket*) dan BNC konektor.Keuntungan menggunakan kabel koaksial adalah lebih murah dari pada kabel fiber optic dan jarak jangkauannya cukup jauh dari kabel jenis UTP/STP yang menggunakan *repeater* sebagai penguatnya. Kekurangannya adalah sulit pada saat instalasi, baik installasi konektor maupun kabel. Untuk saat ini kabel koaksial sudah tidak direkomendasikan lagi intuk instalasi jaringan.

2.2.39. Twisted Pair

Twisted pair terdiri dari 2 jenis :

a. *Unshielded Twisted Pair* (UTP)
b. *Shielded Twisted Pair* (STP)

Kabel ini terdiri dari 4 pasang kabel yang dipilin (*twisted pair*), instalasinya mudah, harganya relatif murah dan cukup handal.

a. *Shielded Twisted Pair*

   Keuntungan menggunakan kabel STP adalah lebih tahan terhadap interferensi gelombang elektromagnetik baik dari dari dalam maupun dari luar. Kekurangannya adalah mahal, sulit pada saat instalasi (terutama masalah *grounding*), dan jarak jangkauannya hanya 100m.

b. *Unshielded Twisted Pair*

   Keuntungan menggunakan kabel UTP adalah murah dan mudah diinstalasi. Kekurangannya adalah rentan terhadap interferensi gelombang elektromagnetik, dan jarak jangkauannya hanya 100m. Ada beberapa kategori untuk kabel *Twisted Pair*, yaitu :

   - Kategori 1 (Cat-1), Umumnya menggunakan konduktor padat standar AWG sebanyak 22 atau 24 pin dengan range impedansi yang lebar. Digunakan pada koneksi telepon dan tidak direkomendasikan untuk transmisi data.
   - Kategori 2 (Cat-2), Range impedansi yang lebar, sering digunakan pada sistem PBX dan sistem alarm. Transmisi data ISDN menggunakan kabel kategori 2, dengan *bandwidth* maksimum 1 MBps.
   - Kategori 3 (Cat-3), Sering disebut kabel *voice grade*, menggunakan konduktor padat sebanyak 22 atau 24 pin dengan impedansi 100 Ω dan berfungsi hingga 16 MBps. Dapat digunakan untuk jaringan 10BaseT dan *Token Ring* dengan *bandwidth* 4 Mbps.
   - Kategori 4 (Cat-4), Seperti kategori 3 dengan *bandwidth* 20 MBps, diterapkan pada jaringan *Token Ring* dengan *bandwidth* 16 Mbps.
   - Kategori 5 (Cat-5), Merupakan kabel *Twisted Pair* terbaik (*data grade*) dengan *bandwidth* 100 Mbps dan jangkauan transmisi maksimum 100m.

2.2.39.1. Wireless Network

Saat ini sudah banyak digunakan jaringan tanpa kabel *(wireless network*), transmisi data menggunakan sinar infra merah atau gelombang mikro untuk menghantarkan data. Walaupun kedengarannya praktis, namun kendala yang dihadapi disini adalah masalah jarak, bandwidth, dan mahalnya biaya. Namun demikian untuk kebutuhan LAN *(Local Area Network*) di dalam gedung, saat ini sudah dikembangkan teknologi wireless untuk *Active Hub* (*Wireless Access Point*) dan *Wireless LAN Card*, sehingga bisa mengurangi kompleksitas kabel transmisi data pada jaringan komputer. *Wireless Access Point* juga bisa digabungkan (*up-link*) dengan *Active Hub* dari jaringan yang sudah ada.

Media transmisi *wireless* menggunakan gelombang radio frekuensi tinggi. Biasanya gelombang elektromagnetik dengan frekuensi 2.4 Ghz dan 5 Ghz. Data-data digital yang dikirim melalui *wireless* ini akan dimodulasikan ke dalam gelombang elektromagnetik ini.