BAB 2
TINJAUAN PUSTAKA

2.1 Tempat Penelitian Tugas Akhir

Pada bab ini akan dijelaskan tentang teori-teori umum dan khusus yang berhubungan langsung dengan tempat penelitian tugas akhir diantaranya pengembangan sistem yang digunakan oleh penulis, teori-teori tentang jaringan komputer, macam-macam protokol *redudancy*, tentang bagaimana kinerja dari *Virtual Router Redudancy Protocol* (VVRP) dan teori pengukuran reliabilitas.

2.1.1 Profil PT. Infomedia Nusantara

PT. Infomedia Nusantara merupakan sebuah perusahaan yang berada di lingkungan Telkom Group yang mengkhususkan diri dibidang media penerbitan dan iklan sebagai jembatan komunikasi antar pelaku bisnis dan juga menjadi penyalur informasi bagi pelanggan telepon PT. Telkom Indonesia. Saat ini 51% sahamnya dimiliki langsung oleh Telkom dan 49% dimiliki oleh anak perusahaan Telkom lainnya.

2.1.2 Sejarah PT. Infomedia Nusantara

Pada tahun 1975 merupakan awal mula perjalanan usaha PT. Infomedia Nusantara menjadi perusahaan pertama penyedia layanan informasi telepon di Indonesia. Dibawah subdevisi Elnusa GTDI dari anak perusahaan PT. Pertamina, Infomedia telah menerbitkan buku petunjuk telepon Telkom yaitu *Yellow Pages*. Perkembangan yang tercatat selanjutnya adalah berdirinya PT. Elnusa Yellow Pages pada tahun 1984 yang berubah nama pada tahun 1995 menjadi PT. Infomedia Nusantara dan pada saat itu PT. Telkom mulai menanamkan investasi. Saat ini PT. Infomedia Nusantara telah berkembang menjadi 3 (tiga) pilar bisnis untuk memenuhi besarnya tuntutan masyarakat akan jasa informasi. Layanan direktori merupakan pilar pertama yang akan menjadi bukti kematangan usaha PT. Infomedia Nusantara dalam menjalani bisnis jasa penyedia informasi melalui penerbitan Buku Petunjuk Telepon (BPT), baik dalam bentuk media cetak maupun media elektronik.

Layanan *contact center* menyediakan jasa *outsourcing* untuk aktivitas pemasaran maunpun peningkatan kualitas layanan hubungan antara mitra PT. Infomedia Nusantara dengan pelanggannya. Layanan konten yang terfokus pada penyedia data sesuai dengan kebutuhan mitra dan pelanggan. Dalam perkembangan berikutnya, PT. Infomedia Nusantara juga mengembangkan bisnisnya sebagai sebuah perusahaan yang bergerak dibidang *contact center* yang saat ini telah mengelola lebih dari 170 klien dari berbagai segmen industri diseluruh wilayah Indonesia. Beberapa klien besar yang menjadi mitra PT. Infomedia Nusantara di bidang *contact center* diantaranya Telkomsel, Garuda Indonesia dan BPJS Kesehatan.

2.2 Visi dan Misi PT. Infomedia Nusantara

2.2.1 Visi

Menjadi penyedia jasa layanan informasi yang utama di kawasan regional.

2.2.2 Misi

Menjadi panutan dalam menciptakan nilai bagi *stakeholder*, dengan menyediakan layanan berikut ini: *Business Process Outsourcing, Knowledge Process Outsourcing* dan *Integrated Marketing.*

Gambar 2.1 Logo PT. Infomedia Nusantara

2.3 Teknologi Jaringan Komputer

Definisi jaringan komputer adalah terhubungnya dua komputer atau lebih dengan kabel penghubung (pada beberapa kasus, tanpa kabel atau *wireless* sebagai

penghubung), sehingga antar komputer dapat saling tukar informasi (data) [1]. Tujuan dari jaringan komputer adalah:

1. Membagi sumber daya seperti berbagi pemakaian printer, CPU, memori, harddisk dan lain-lain.
2. Komunikasi seperti e-mail, *instant messaging* dan *chatting*.
3. Akses informasi seperti *web browsing*, file *server* dan lain- lain.

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan. Pihak yang meminta layanan disebut klien (*client*) dan yang memberikan layanan disebut pelayan (*server*). Arsitektur ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer [1].

2.4 Jenis-Jenis Jaringan Komputer

Jenis-jenis jaringan terbagi dalam empat lingkup, lingkup pertama berdasarkan topologi, berdasarkan geografis, berdasarkan service dan berdasarkan pengembangan arsitektur jaringan komputer [1].

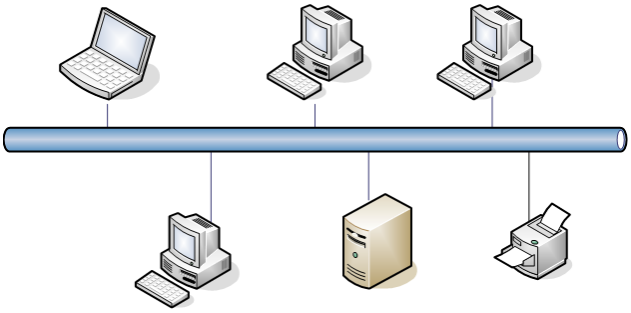
2.4.1 Berdasarkan Topologi Jaringan Komputer

Topologi jaringan merupakan suatu teknik untuk menghubungkan komputer yang satu dengan komputer lainnya yang merangkai menjadi sebuah jaringan, dimana penggunaan topologi jaringan didasarkan pada biaya, kecepatan akses data, ukuran maupun tingkat konektivitas yang akan mempengaruhi kualitas maupun efiensi suatu jaringan. Ada bermacam macam topologi jaringan komputer yang banyak di gunakan saat ini antara lain adalah Topologi Bus, Topologi Star, Topologi Tree, Topologi Ring dan Topologi Mesh serta masing-masing jenis topologi mempunyai kelebihan dan kekurangannnya sendiri.

1. **Topologi Bus**

   Topologi bus sering juga disebut *daisy chain* atau *ethernet bus topologies*. Sebutan terakhir diberikan karena pada topologi bus digunakan perangakt jaringan atau *network interface card* (NIC) bernama *ethernet*. Jaringan yang menggunakan topologi bus dapat dikenali dari penggunaan sebuah kabel *backbone* (kabel utama) yang menghubungkan semua peralatan jaringan.

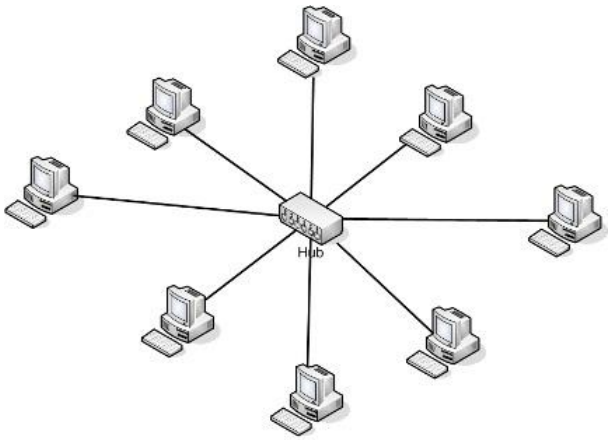
Kabel *backbone* menjadi satu-satunya jalan bagi lalu lintas data, maka apabila kabel *backbone* rusak atau terputus akan menyebabkan jaringan mati total.



Gambar 2.2 Topologi Bus

2. Topologi Star

Topologi star dikenal dengan keberadaan sebuah sentral berupa *Hub* yang menghubungkan semua *node.* Setiap *node* menggunakan sebuah kabel UTP atau STP yang dihubungkan dengan *ethernet card* ke *hub*. Cara kerja dari topologi star mirip dengan topologi bus, yang membedakan hanya keberadaan *hub* atau *switch* sebagai sentral karena setiap *node* yang terhubung dengan *hub* jika ada kabel atau segmen yang putus, tidak akan menyebabkan jaringan menjadi lumpuh.

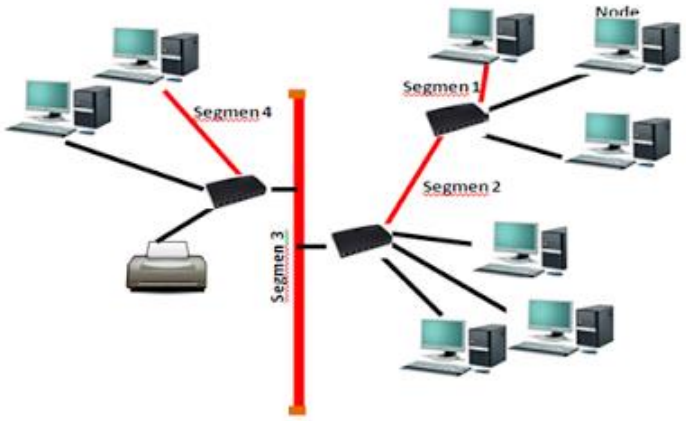


Gambar 2.3 Topologi Star

3. Topologi Tree

Topologi tree disebut juga topologi star-bus atau *hybrid.* Topologi tree merupakan gabungan beberapa topologi star yang dihubungkan dengan

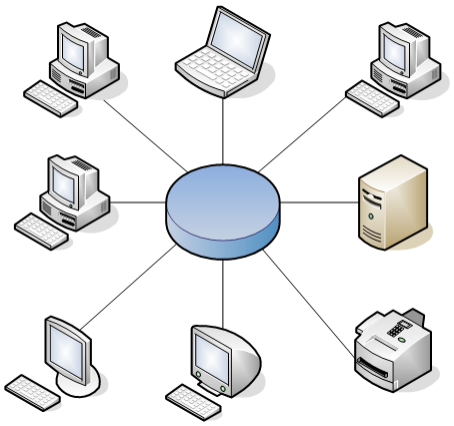
topologi bus. Topologi tree digunakan untuk menghubungkan beberapa jaringan LAN dengan jaringan LAN lain. Hubungan antar jaringan LAN dilakukan via *hub*, masing-masing *hub* dapat dianggap sebagai *root* (akar) dari masing-masing *tree* (pohon). Topologi tree dapat mengatasi kekurangan topologi bus yang disebabkan oleh *broadcast traffic* dan kekurangan topologi star yang disebabkan oleh kapasitas port *hub*.



Gambar 2.4 Topologi Tree

4. Topologi Ring

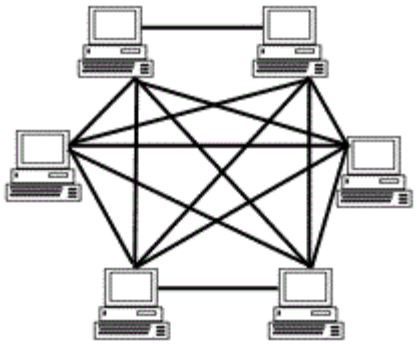
Topologi ring berbeda dengan bus, karena sesuai dengan namanya jaringan ini dapat dikenali dari kabel *backbone* yang membentuk cincin. Setiap komputer terhubung dengan kabel *backbone*, setelah sampai pada komputer terakhir maka ujung kabel akan kembali dihubungkan dengan komputer pertama. Hal yang menarik dari topologi ring adalah bagaimana data mengalir pada media transmisi data. Data mengalir dari satu arah atau *node* komputer ke *node* lainnya sehingga sampai tujuan ke *node* asal. Karena data mengalir ke satu arah artinya tidak akan pernah terjadi tabrakan data dan kecepatan transfer data relatif stabil.



Gambar 2.5 Topologi Ring

5. **Topologi Mesh**

   Topologi mesh merupakan hubungan *point to point* atau satu persatu ke setiap perangkat jaringan. Topologi mesh sangat jarang diimplementasikan, selain rumit juga membutuhkan banyak kabel jaringan. Apabila jumlah perangkat yang terhubung semakin banyak, maka instalasi kabel jaringan akan semakin rumit.



Gambar 2.6 Topologi Mesh

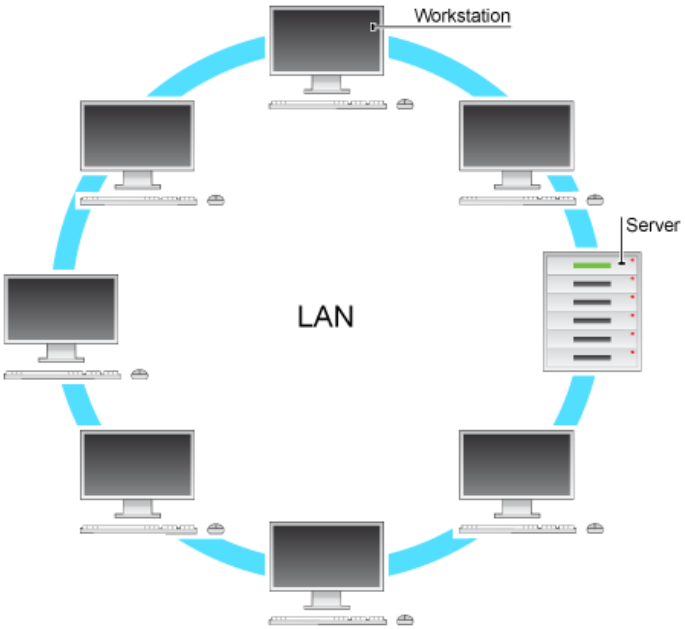
2.4.2 Berdasarkan Ruang Lingkup Geografis Jaringan komputer

Berdasarkan ruang lingkup geografis jaringan terdapat tiga jenis jaringan komputer [1].

1. **Local Area Network (LAN)**

   Local Area Network (LAN) adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung atau sebuah sekolah dan biasanya tidak jauh

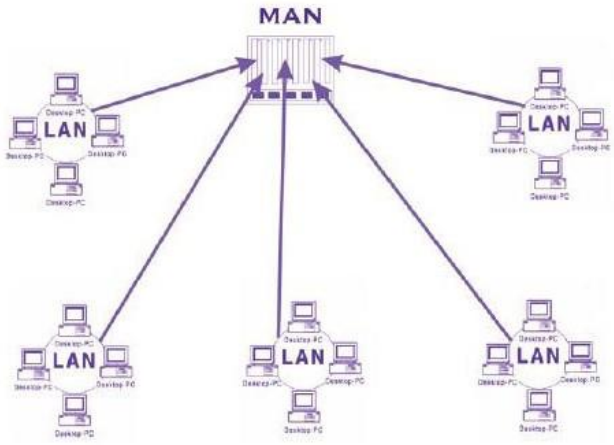
dari sekitar 1 km persegi. Beberapa model konfigurasi LAN, satu komputer biasanya dijadikan sebuah file server yang digunakan untuk menyimpan perangkat lunak (software) yang mengatur aktifitas jaringan, ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung ke dalam network. Komputer-komputer yang terhubung ke dalam jaringan (network) itu biasanya disebut dengan workstation. Biasanya kemampuan workstation lebih di bawah dari file server dan mempunyai aplikasi lain di dalam harddisknya selain aplikasi untuk jaringan. Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya [1].



Gambar 2.7 Skema Jaringan LAN

2. Metropolitan Area Network (MAN)

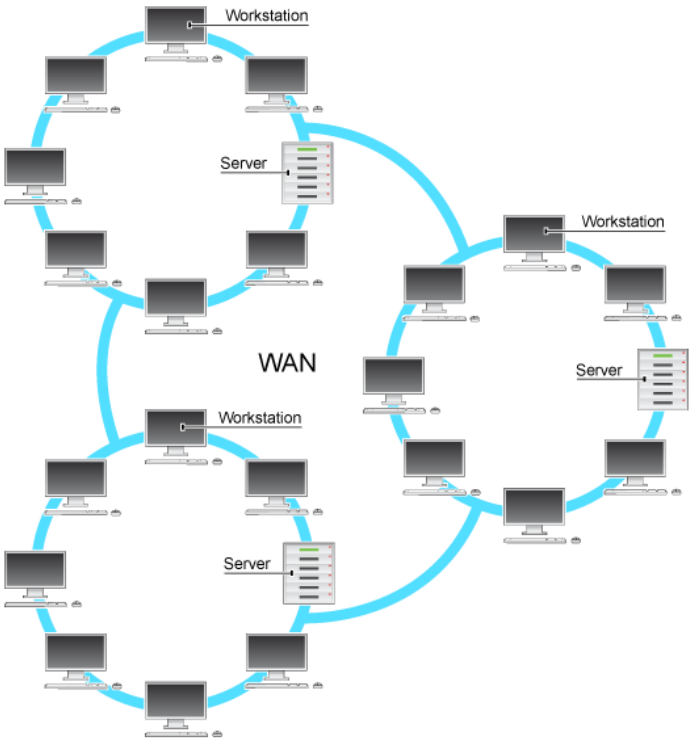
Metropolitan Area Network (MAN) biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu: jaringan Kantor pusat pada suatu bank dimana beberapa kantor cabang sebuah bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya. Misalnya bank tersebut yang ada di seluruh wilayah Bandung [1].



Gambar 2.8 Skema Jaringan MAN

3. Wide Area Network (WAN)

Wide Area Network (WAN) adalah kumpulan dari Local Area Network (LAN) atau Workgroup yang dihubungkan dengan menggunakan alat komunikasi, umumnya menggunakan modem untuk membentuk hubungan dari/ke kantor pusat dan kantor cabang, maupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan cepat serta dengan biaya relatif murah [1].



Gambar 2.9 Skema Jaringan WAN

2.4.3 Berdasarkan Service Jaringan Komputer

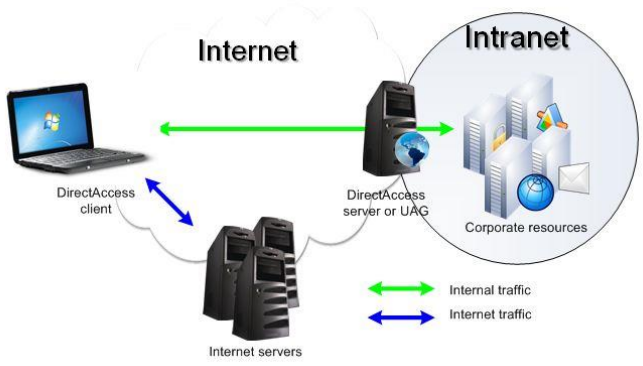
Berdasarkan service jenis jaringan komputer terdapat dua jenis jaringan komputer [2].

1. **Internet**

   Internet adalah jaringan global yang memungkinkan dua komputer atau lebih berkoneksi dengannya untuk mentransfer file dan tukar-menukar email dan pesan-pesan real-time. Internet merupakan landasan untuk world wide web. Internet juga merupakan kumpulan jaringan komputer yang berbeda-beda dan saling berhubungan di seluruh dunia. Semua komputer itu dihubungkan Internet agar dapat berkomunikasi satu sama lain dengan menggunakan TCP/IP [**2**].

2. **Intranet**

   Intranet adalah jaringan swasta yang berdasarkan standar teknologi internet (IP) yang sejenis world wide web internal dalam suatu organisasi. Intranet adalah penggunaan teknologi internet dalam pada jaringan internal suatu perusahaan berdasarkan teknologi web. Intranet hanya berada di dalam organisasi, sedangkan internet adalah jaringan global yang terbuka bagi semua orang. Intranet berhubungan erat dengan internet. Internet dan intranet berbagi perangkat lunak dan peralatan jaringan yang sama dan berbicara dengan bahasa yang sama pula. Intranet dijalankan pada internal perusahaan dan pada antar kantor cabang perusahaan mereka, serta tertutup bagi internet dari luar dengan menggunakan firewall yang memungkinkan para karyawan browsing ke luar, tetapi mencegah orang luar browsing ke dalam [2].



Gambar 2.10 Jaringan Internet dan Intranet

2.4.4 Berdasarkan Pengembangan Arsitektur Jaringan Komputer

Jenis jaringan berdasarkan arsitektur pengembangan jaringan komputer digolongkan menjadi tiga macam, diantaranya:

1. **Client Server**

   Merupakan jaringan yang memisahkan antara komputer server (yang memberi layanan) dengan komputer client (yang meminta layanan). Sehingga masing-masing client yang terhubung dengan server dapat meminta layanan berupa data maupun informasi, dengan mekanisme layanan yang diberikan dapat diakses oleh banyak komputer client maupun satu komputer server dapat melayani banyak permintaan dari komputer client.

2. **Peer to Peer**

   Merupakan jaringan yang dibangun untuk menghubungkan dua buah komputer agar dapat berkomunikasi antara satu dengan yang lainnya, tanpa ada komputer yang difungsikan sebagai server.

3. **VPN**

   Merupakan singkatan dari *Virtual Private Network* yaitu sebuah koneksi private melalui jaringan publik. *Virtual Network* berarti jaringan yang terjadi hanya bersifat virtual dimana tidak ada koneksi jaringan secara nyata antara 2 titik yang akan berhubungan. *Private* yang artinya jaringan terbentuk bersifat pribadi dimana tidak semua *user* dapat mengaksesnya. Data yang dikirimkan terenkripsi sehingga tetap terjaga rahasianya meskipun melalui jaringan publik. Dengan VPN ini kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut tunnel (terowongan). Tunneling adalah suatu cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada yaitu: PPTP, L2TP dan standar terbaru, Internet Protocol Security (biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi tunneling dan enkripsi.

2.5 Pengenalan Sistem Operasi

Istilah sistem operasi sering ditujukan kepada semua *software* yang masuk dalam satu paket dengan sistem komputer sebelum aplikasi-aplikasi *software* terinstal. Dalam Ilmu komputer, sistem operasi atau dalam bahasa Inggris: *operating system* (OS) adalah perangkat lunak sistem yang bertugas untuk melakukan kontrol dan manajemen perangkat keras serta operasi-operasi dasar sistem, termasuk menjalankan software aplikasi seperti program-program pengolah kata dan *browser web*. Secara umum, sistem operasi adalah *software* pada lapisan pertama yang disimpan pada memori komputer pada saat komputer dinyalakan. Sedangkan *software-software* lainnya dijalankan setelah sistem operasi berjalan dan sistem operasi akan melakukan layanan utama untuk *software-software* itu. Layanan utama tersebut seperti akses ke disk, manajemen memori, *scheduling task* dan antarmuka user. Sehingga masing-masing *software* tidak perlu lagi melakukan tugas-tugas utama tersebut, karena dapat dilayani dan dilakukan oleh sistem operasi [7].

2.5.1 Sejarah Linux

Linux pada awalnya dibuat oleh seorang mahasiswa Finlandia yang bernama Linus Benedict Torvalds. Dulunya Linux merupakan proyek hobi yang diinspirasikan dari Minix, yaitu sistem UNIX kecil yang dikembangkan oleh Andrew Tanenbaum. Linux versi 0.01 dikerjakan sekitar bulan Agustus 1991. Kemudian pada tanggal 5 Oktober 1991, Linus mengumumkan versi resmi Linux, yaitu versi 0.02 yang hanya dapat menjalankan shell bash(GNU Bourne Again Shell) dan gcc (GNU C Compiler) [7].

2.5.1.1 Distribusi Linux

Terdapat banyak distribusi Linux (lebih dikenali sebagai distro) yang dibuat oleh individu, grup, atau lembaga lain. Masing-masing disertakan dengan program sistem dan program aplikasi tambahan, di samping menyertakan suatu program yang memasang keseluruhan sistem di komputer (installer program). Inti di setiap distribusi Linux adalah kernel, koleksi program dari proyek GNU (atau proyek lain), cangkang (*shell*), dan aturan cara utilitas seperti pustaka (*libraries*),

kompilator dan penyunting (*editor*). Kebanyakan sistem juga menyertakan aturan cara dan utilitas yang bukan GNU. Bagaimanapun, utilitas tersebut dapat dipisahkan dan sistem ala UNIX masih tersedia. Beberapa contoh adalah aturan cara dan utiliti dari BSD dan sistem grafik-X (X-*Window System*). X menyediakan antarmuka grafis (GUI) yang umum untuk Linux. Contoh-contoh distribusi Linux : Ubuntu, SuSE, Fedora, Mandriva, Slackware, Debian, PCLinuxOS, Knoppix, Xandros [7].

2.5.2 Sejarah Windows

Microsoft Windows atau lebih dikenal dengan sebutan Windows adalah keluarga sistem operasi komputer pribadi yang dikembangkan oleh Microsoft yang menggunakan antarmuka dengan pengguna berbasis grafik (*graphical user interface*) [7].

Dimulai dari DosShell for DOS 6 buatan Microsoft dan inginnya Microsoft bersaing terhadap larisnya penjualan Apple Macintosh yang menggunakan GUI, Microsoft menciptakan Windows 1.0. Nama ini berasal dari kelatahan karyawan Microsoft yang menyebut nama aplikasi tersebut sebagai program windows (Jendela Program). Windows versi 2 adalah versi Windows pertama yang bisa diinstal program. Satu-satunya program yang bisa ditambahkan adalah Microsoft Word versi 1. Windows versi 3 menjanjikan aplikasi tambahan yang lebih banyak, kelengkapan penggunaan, kecantikan user interface atau antarmuka dan mudahnya konfigurasi [7].

Windows versi 3.1 adalah versi Windows yang bisa mengoptimalisasi penggunaannya pada prosesor 32-bit Intel 80386 ke atas. Windows versi 3.11 adalah versi Windows terakhir sebelum era Start Menu. Windows 3.11 pun adalah versi Windows pertama yang mendukung networking/jaringan. Versi Hibrida dapat dijalankan tanpa MS-DOS. Versi Hibrida tersebut menginstalasi dirinya sendiri dengan DOS 7. Tidak seperti Windows versi 16-bit yang merupakan shell yang harus diinstalasi melalui DOS terlebih dahulu. Aplikasinya pun berbeda. Meskipun Windows 9X dapat menjalankan aplikasi Windows16-bit, namun Windows 9X memiliki grade aplikasi sendiri -X86-32, Windows 9X sangat terkenal dengan BSOD (Blue Screen of Death) [7].

2.5.2.1 Versi Versi Windows

Versi dari Windows sudah banyak yang telah diliris dari tahun 1985 sampai dengan tahun 2012,[7].

16-bit, berjalan di atas MS-DOS

1. 1985 November - Windows 1.0
2. 1987 9 Desember - Windows 2.0
3. 1990 22 Mei - Windows 3.0
4. 1992 Agustus - Windows 3.1
5. 1992 Oktober - Windows for Workgroups 3.1
6. 1993 November - Windows for Workgroups 3.11

Hibrida (16-bit/32-bit), berjalan tanpa MS-DOS (meski tidak sepenuhnya)

1. 1995 24 Agustus - Windows 95 (Versi: 4.00.950)
2. 1998 25 Juni - Windows 98 (Versi: 4.1.1998)
3. 1999 5 Mei - Windows 98 Second Edition (Versi: 4.1.2222)
4. 2000 19 Juni - Windows Millennium Edition (Me) (Versi: 4.9.3000)

Berbasis kernel Windows NT

1. 1993 Agustus - Windows NT 3.1
2. 1994 September - Windows NT 3.5
3. 1995 Juni - Windows NT 3.51
4. 1996 29 Juli - Windows NT 4.0
5. 2000 17 Februari - Windows 2000 (Versi: NT 5.0.2195)
6. 2001 - Windows XP (Versi: NT 5.1.2600)
7. 2003 - Windows Server 2003 (Versi: NT 5.2.3790)
8. 2006 - Windows Vista (Versi 6.0 Build 6000)
9. 2007 - Windows Home Server (Versi 6.0.1800.24)
10. 2008 - Windows Server 2008 (Versi 6.1)
11. 2009 - Windows 7 (Versi 6.1 Build 7600)
12. 2009 - Windows Server 2008 R2 (Versi 6.1)
13. 2011 - 2012 - Windows 8.1

2.6 OSI Layer (Open System Interconnect)

Sebuah arsitektur model komunikasi data (disebut *Open System Interconnect* atau *OSI Refference Model*) telah dibuat oleh International Standards Organization (ISO) yang ditujukan untuk menemukan strukturdan fungsi protokol komunikasi data pada berbagai tingkat komunikasi di dalam jaringan komputer [1].

Model OSI berisi tujuh lapis (layer) yang menentukan fungsi protokol komunikasi data. Setiap lapis yang ada dalam model OSI memiliki fungsi dalam komunikasi data didalam jaringan computer [1].

1. **Physical Layer**

   Physical layer yaitu lapisan fisik yang berkaitan dengan elektronik dari komputer ke Local Area Network melalui Ethernet Card atau perangkat wireless atau perangkat modem satelit atau perangkat modem leased line. Perangkat elektronik yang digunakan ini memberikan karakteristik fisik media jaringan komputer [1].

2. **Data Link Layer**

   Data link layer yaitu lapisan data berisi ketentuan yang mendukung sambungan fisik seperti penentuan biner 0 dan 1, penentuan kecepatan penentuan biner terebut dan lainnya agar sambungan jaringan komputer bisa berjalan baik. Dengan kata lain Data link layer menterjemahkan sambungan fisik menjadi sambungan data.

3. **Network Layer**

   Network layer yaitu memungkinkan perangkat yang tersambung menyebutkan perbedaan yang ada antara satu komputer dengan komputer lainnya. Aliran pengalamatan dan komunikasi dasar ini ditangani oleh network layer. Lapisan ini juga menentukan kaidah jumlah informasi yang dapat di kirim di dalam sebuah paket data dan koreksi erornya [1].

4. **Transport Layer**

   Paket data yang mengalir dari host ke host bisa datang atau tidak datang ketika paket itu dikirimkan. Dengan berbagai alasan seperti karena adanya kesalahan rute (error routing) dan kesalahan network (error network), paket data yang dikirimkan dari sebuah host ke host lain bisa saja tidak sampai ke tujuan. Lapisan transport ini menyusun ulang perintah pengiriman paket

data ke dalam urutan yang benar dan biasanya memakai mekanisme pengecekan untuk menemukan apakah paket telah tiba di tujuan atau belum. Transport layer dapat bertanya kepada host tujuan untuk memastikan apakah paket data telah diterima atau belum. Bila belum diterima, maka akan dikirim paket data kembali. Pada layer ini protokol yang bekerja adalah TCP (*Transmission Control Protocol),* UDP (*User Datagram Protocol*) dan SPX (*Sequenced Packet Exchange*) [1].

5. **Session Layer**

   Session layer adalah tempat berikutnya yang akan dilalui oleh paket data yang telah diterima. Lapisan ini memakai paket data untuk menghasilkan multi sambungan [1].

6. **Presentation Layer**

   Presentation layer yaitu lapisan presentasi yang berperan menyusun kembali paket data yang dikirim. Paket data yang dikirim selalu berupa pecahan paket data. Ada kira kira 10 buah pecahan paket data yang dibuat dari sebuah data. Pecahan ini setelah diterima dengan baik, oleh lapisan presentasi akan disusun ulang sesuai dengan data aslinya. Aplikasi yang bekerja pada layer presentasi yaitu PICT, TIFF, JPEG, merupakan format data untuk aplikasi bergambar, lalu aplikasi MIDI dan MPEG untuk aplikasi sound dan movie serta pada aplikasi web seperti HTTP [1].

7. **Application Layer**

   Application layer adalah tempat dimana program dapat memesan, meminta servis yang terdapat di dalam sebuah jaringan komputer seperti file transfer, otentikasi pengguna atau melacak database. Dalam hal Internet, protokol seperti ini adalah FTP, Telnet, Gopher dan World Wide Web [1].

Tabel 2.1 Standarisasi ISO Pada OSI Layer

OSI Layer		
Layer	**Fungsi**	**Protokol**
Layer 7 Application	Menyediakan jasa untuk aplikasi pengguna. Layer ini bertanggungjawab atas pertukaran informasi antara program komputer, seperti program e-mail, dan service lain yang berjalan di jaringan, seperti server printer atau aplikasi komputer lainnya	FTP, TFTP, DNS, SMTP, SFTP, SNMP,Rlogin, BootP, MIME
Layer 6 Presentation	Bertanggung jawab bagaimana data dikonversi dan diformat untuk transfer data. Contoh konversi format text ASCII untuk dokumen, gif dan JPG untuk gambar. Layer ini membentuk kode konversi, translasi data, enkripsi dan konversi.	JPEG, HTTP, MPEG, TIFF
Layer 5 Session	Menentukan bagaimana dua terminal menjaga, memelihara dan mengatur koneksi serta bagaimana mereka saling berhubungan satu sama lain.	SQL, X-Window, ASP, NFS
Layer 4 Transport	Bertanggung jawab membagi data menjadi segmen, menjaga koneksi logika end-to-end antar terminal dan menyediakan penanganan error (error handling).	TCP, UDP, SPX
Layer 3 Network	Bertanggung jawab untuk menentukan alamat jaringan, menentukan rute yang harus diambil selama perjalanan dan menjaga antrian trafik di jaringan. Data pada layer ini berbentuk paket.	IP, OSPF, ICMP, RIP, ARP, RARP
Layer 2 Data Link	Menyediakan link untuk data lalu dipaketkan menjadi frame yang berhubungan dengan hardware kemudian dibawa melalui media komunikasinya dengan kartu jaringan serta mengatur komunikasi layer physical antara sistem koneksi dan penanganan error.	SLIP, PPP, MTU

Layer 1 Physical	Bertanggung jawab atas proses data menjadi bit dan mentransfernya melalui media, seperti kabel dan menjaga koneksi fisik antar sistem.	IEEE 802, EIA RS-232

2.7 Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) telah dirancang untuk memberikan alokasi alamat yang dapat stasis dan dinamis. DHCP didasarkan pada gagasan dari sebuah *server* khusus yang memberikan alamat IP untuk *host*.

Untuk menemukan alamat IP-nya, mesin yang baru di-*boot* menyebarkan paket DHCP DISCOVER. DHCP *relay agen* menyadap semua siaran DHCP di LAN. Ketika menemukan sebuah paket DHCP DISCOVER, akan mengirimkan paket sebagai paket *unicast* ke *server* DHCP, pada jaringan dengan jarak tertentu. Satu-satunya informasi yang dibutuhkan agen *relay* adalah alamat IP dari *server* DHCP. "DHCP tidak memerlukan MAC *address* pada tiap *device*. DHCP hanya listen terhadap request IP *address* yang dibuat oleh DHCP *client*. DHCP menetapkan sebuah *address* kepada *client* dari standar *pool* [4].

Suatu masalah yang timbul adalah seberapa lama suatu alamat IP harus dialokasikan secara otomatis dari *pool* DHCP. Jika *host* meninggalkan jaringan dan tidak mengembalikan alamat IP ke *server* DHCP, alamat IP tersebut akan hilang secara permanen. Untuk mencegah hal itu terjadi, penetepan alamat IP mungkin terjadi dalam jangka waktu tertentu dengan teknik yang disebut *leasing*. Sebelum *leasing* berakhir, host harus meminta DHCP untuk pembaharuan. Jika gagal untuk membuat permintaan atau permintaan tersebut ditolak, *host* sudah tidak memungkinkan lagi menggunakan alamat IP yang diberikan sebelumnya.

2.8 Hierarkial Network

Ketika membangun sebuah jaringan LAN ataupun *client-server* yang memenuhi kebutuhan sebuah bisnis kecil atau menengah, perencanaan akan lebih mungkin berhasil jika model jaringan yang digunakan secara hierarki. Dibandingkan dengan jaringan yang lain, jaringan hierarki lebih mudah untuk dikelola dan dikembangkan dan juga dapat mengatasi masalah lebih cepat.

Desain jaringan hierarkial melibatkan pembagian jaringan ke dalam *layer* berlainan. Setiap *layer* menyediakan fungsi yang spesifik bahwa *layer* didefinisikan peranannya di dalam keseluruhan jaringan. Dengan memisahkan berbagai fungsi yang ada dalam jaringan, desain jaringan menjadi modular, dengan kemampuan dalam hal scalability dan performa. Tipe dari desain hierarki adalah memecah jaringan menjadi tiga *laye*r, yaitu *access, distribution* dan *core* [5].

2.8.1 Core Layer

Core layer adalah hierarkial *network* yang memiliki *high-speed backbone* pada *internetwork*. Karena *core layer* sangat penting untuk inter-koneksi, maka *core layer* harus dirancang dengan *redundant components*. *Core layer* haruslah handal dan dapat beradaptasi dengan perubahan cepat.

Ketika mengkonfigurasi *router* pada *core layer*, diharuskan untuk menggunakan fitur *routing* yang dapat mengoptimalkan *packet throughtput*. Saat mengkonfigurasi *router* harus menghindari penggunaan filter paket atau fitur lain yang memperlambat manipulasi paket dan *core* harus dioptimasi untuk *low latency* dan pengelolaan yang baik.

Core layer memiliki diameter yang terbatas. *Distribution layer routers* (atau *switch*) dan klien LAN dapat ditambahkan ke model tanpa meningkatkan diameter *core layer*. Dengan membatasi diameter *core* inti, kinerja jaringan dapat diprediksi dan saat terjadi masalah akan lebih mudah untuk diatasi.

Untuk jaringan yang perlu terhubung ke jaringan kantor lain melalui intranet atau internet, topologi *core layer* harus satu atau lebih *link* ke jaringan eksternal. *Corporate network administrator* harus mencegah regional dan administrator kantor cabang lain untuk perancangan intranet atau internet mereka sendiri. Pemusatan fungsi-fungsi pada *core layer* dapat mengurangi kompleksitas dan potensi terjadinya masalah pada routing dan juga dapat meminimalkan masalah keamanan.

2.8.2 Distribution Layer

Distribution layer adalah pembatas antara *core layer* dan *access layer*. *Distribution layer* memiliki banyak peran, diantaranya dapat mengontrol akses ke

sumber daya untuk alasan keamanan dan pengendalian jaringan yang melintasi *core layer* untuk alasan kinerja. *Distribution layer* adalah lapisan yang membatasi wilayah *broadcast domain*. Dalam mendesain jaringan *virtual* LAN, *distribution layer* dapat dikonfigurasikan untuk rute pada jaringan VLAN.

Distribution layer memungkinkan *core layer* untuk terhubung dengan situs yang berjalan pada *protocol* yang berbeda dengan tetap mempertahankan kinerja yang baik. Untuk mempertahankan kinerja yang baik pada *core layer*, *distribution layer* dapat mendistribusikan antara *bandwidth-intensive access layer* routing *protocol* dan optimasi *core routing protocol*.

Untuk meningkatkan kinerja *routing protocol*, *distribution layer* dapat meringkas rute dari *access layer*. Untuk beberapa jaringan, *distribution layer* menawarkan rute *default* untuk *router access layer* dan hanya berjalan pada *dynamic routing protocol* ketika komunikasi dengan *core routers*.

Untuk memaksimalkan hierarki, modularitas dan kinerja, *distribution layer* memperkecil rute dengan hanya satu rute *default* jika memungkinkan. *Distribution layer* dapat memberikan *access layer* dengan rute terdekat yang memiliki akses ke *core layer*.

2.8.3 Access Layer

Access layer menyediakan pengguna pada segmen lokal dengan akses ke *internetwork*. *Access layer* dapat termasuk *router, switch, bridges, share-media hub* dan *wireless access point*. *Switch* sering diimplementasikan pada *access layer* di jaringan kampus untuk membagi *bandwith domain* untuk memenuhi tuntutan aplikasi yang membutuhkan banyak *bandwith*. *Access layer* memiliki tujuan utama yaitu dengan menyediakan sarana yang menghubungkan *device* ke jaringan dan mengendalikannya untuk berkomunikasi melalui jaringan tersebut [5].

Untuk *interworks* yang meliputi kantor cabang kecil dan *telecommuter home office, access layer* dapat memberikan akses ke dalam *corporate internetwork* menggunakan teknologi *wide-area* seperti ISDN dan *frame relay*. Dapat juga menerapkan fitur *routing*, seperti *dial-on-demand routing* (DDR) dan *static routing* untuk mengontrol *bandwidth* dan meminimalisasi biaya *remote access layer* (DDR membuat *link* tidak aktif kecuali ketika lalu lintas tertentu harus dikirim).

2.9 Media Transmisi

Media transmisi adalah suatu jalur antara pemancar dan penerima dalam sistem transmisi data. Media transmisi dapat diklasifikasikan menjadi *guided* dan *unguided* (dengan perantara dan tanpa perantara). Media transmisi akan dilewati oleh gelombang elektromagnetik, jadi signal yang ada baik itu analog maupun digital harus diubah ke dalam gelombang elektromagnetik. Jenis media transmisi *guided* seperti *copper twisted pair* (sepasang kabel tembaga), *copper coaxial cable* (kebel tembaga coaxial) dan *fiber optic*. Sedangkan media transmisi *unguided* mengantarkan gelombang atau signal elektromagnetik tanpa melalui suatu perantara yang solid, yaitu melalui udara, baik di dalam atmosfir maupun di ruang angkasa. Bentuk transmisi ini biasa disebut juga dengan transmisi tanpa kabel (*wireless transmission*) [9].

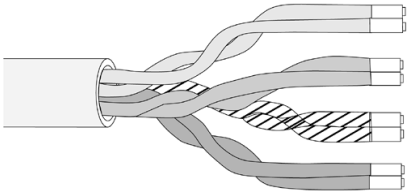
2.9.1 Media Transmisi Kabel

Dalam jaringan komputer terjadi proses transmisi data, media transmisi adalah media atau alat yang digunakan untuk menghubungkan antara pengirim dan penerima informasi ketika mengirimkan suatu data. Data terlebih dahulu diubah menjadi sinyal analog yang bisa dibaca oleh media transmisi atau kode enkripsi yang akan dimanipulasi dengan berbagai macam cara untuk diubah kembali menjadi data. Media kabel ini lebih baik dari pada media nirkabel, karena media kabel mampu membawa data dalam jumlah yang cukup besar tanpa diganggu oleh cuaca, sehingga menghasilkan komunikasi data yang cepat. Salah satu media transmisi yang sering digunakan yaitu media terlindung dan yang termasuk media terlindung adalah media transmisi data tersebut terbungkus dalam fisik tertentu.

1. **Twisted Pair (Kabel Berpasangan)**

   Twisted pair merupakan medium yang paling murah dan banyak digunakan dalam transmisi *guided*. *Twisted pair* terdiri dari dua kabel tembaga yang terisolasi yang disusun dalam jalinan bentuk spiral. Sepasang kabel tersebut berfungsi sebagai satu aliran komunikasi. Sejumlah pasangan kabel ini disatukan menjadi satu bundel kabel dengan membungkus bundelan kabel-kabel tersebut dalam suatu sarung (pelapis pengaman) yang lentur. Untuk jarak yang jauh, kabel tersebut dapat berisi ratusan pasangan

kabel tembaga dan kabel jenis ini dapat menimbulkan terjadinya *crosstalk* antar dua pasang kabel yang berdekatan [9].

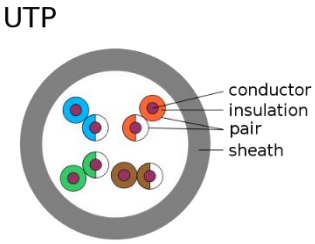


Gambar 2.11 Kabel Berpasangan (Twisted Pair)

Jenis kabel berpasangan menurut pelindungnya dibagi menjadi:

a. *Unshielded Twisted Pair* (UTP)

Kabel UTP (*Unshielded Twisted Pair*) merupakan salah satu media transmisi yang paling banyak digunakan untuk membuat sebuah jaringan yang berbasis lokal atau biasa disebut LAN (*Local Area Network*). Sesuai namanya yaitu *Unshielded Twisted Pair* berarti kabel pasangan yang berpilin atau terbelit tanpa pelindung. Fungsi dari lilitan ini adalah sebagai eleminasi terhadap induksi dan kebocoran. Kabel jenis banyak digunakan untuk membuat sebuah jaringan selain harganya yang tidah terlalu mahal, kabel ini juga mudah untuk memotongnya karena hanya mempunyai satu kulit penyelubung, oleh karena itu banyak orang yang menggunakan kabel jenis ini untuk membuat sebuah jaringan.

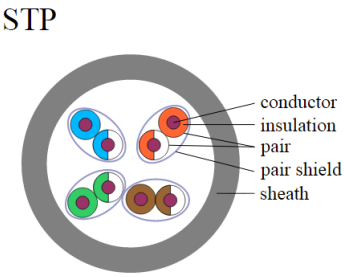


Gambar 2.12 Kabel Unshielded Twisted Pair (UTP)

b. *Shielded Twisted Pair* (STP)

Kabel STP (*Shielded Twisted Pair*) merupakan salah satu media transmisi yang digunakan untuk membuat sebuah jaringan yang berbasis lokal atau biasa disebut LAN (Local Area Network). Sesuai namanya *Shielded Twisted Pair* berarti kabel pasangan berpilin atau

terbelit dengan pelindung. Hampir sama dengan kabel UTP tapi kabel STP mempunyai selubung lagi yang menyelubungi ke 4 lilitan kabel di dalamnya. Fungsi lilitan dan kulit penyelubung ini adalah sebagai eleminasi terhadap induksi dan kebocoran.

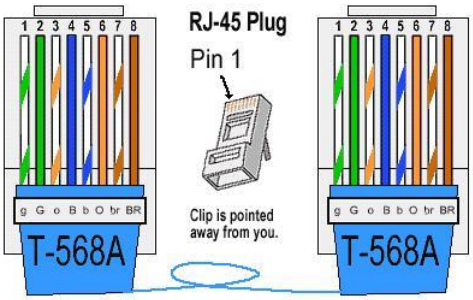


Gambar 2.13 Kabel Shielded Twisted Pair (STP)

Kabel UTP dapat didesain menjadi tiga jenis yaitu:

a. *Straight Through Cable*

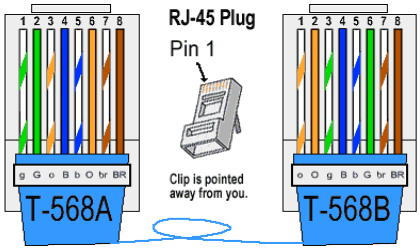
Kabel ini memiliki urutan warna yang sama pada kedua ujungnya, kabel ini digunakan untuk menghubungkan *network device* yang berbeda.



Gambar 2.14 Straight Through Cable

b. *Crossover Cable*

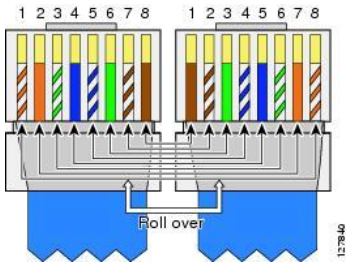
Kabel ini mempunyai urutan warna pada kabel ini yaitu warna pada pin 1 ditukar dengan pin 3 dan pin 2 ditukar dengan pin 6. Hal tersebut terjadi karena pin pengirim dan penerima berada pada lokasi yang berbeda. Kabel ini digunakan untuk menghubungkan *network device* yang sejenis (sama).



Gambar 2.15 Crossover Cable

c. *Rollover Cable*

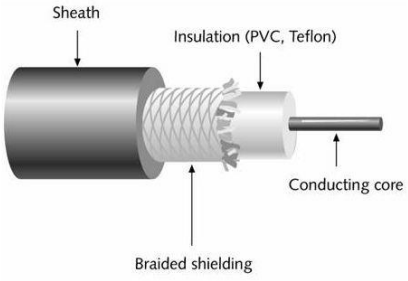
Pada kabel ini, kombinasi warna pin dibalik pada ujung yang satunya. Kabel ini digunakan untuk menghubungkan PC ke port *console* pada *network device*.



Gambar 2.16 Rollover Cable

2. Kabel Coaxial

Seperti *Twisted pair* kabel *coaxial* terdiri dari dua konduktor, tetapi dapat digunakan untuk frekuensi yang lebih tinggi. Kabel ini terdiri dari konduktor berbentuk silinder untuk lapisan luar, yang mengelilingi konduktor bagian dalam. Konduktor bagian dalam dilapisi oleh bahan isolator, sedangkan konduktor bagian luar dilapisi oleh jaket pelindung. Diameter berkisar antara 0,4 - 1,0 inci. Karena konstruksi dan pelapis kabel yang baik, maka kabel *coaxial* lebih sedikit mengalami interfensi dan *crosstalk* bila dibandingkan dengan *twisted pair*. Kabel *coaxial* dapat digunakan untuk jarak yang lebih jauh dan dalam jaringan komunikasi yang lebih luas dengan stasiun dan jalur komunikasi yang lebih banyak [9].

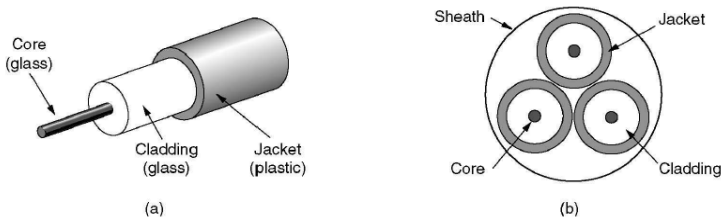


Gambar 2.17 Kabel Coaxial

Konduktor luar berbentuk anyaman, sedangkan konduktor dalam berupa tembaga yang padat. Antara dua konduktor akan dipisahkan dengan isolator.

3. Fiber Optic

Fiber optic menggunakan cahaya sebagai pengganti arus listrik untuk mengirimkan sinyal. Data digital direpresentasikan dengan ada atau tidaknya cahaya. Bit 1 menunjukkan adanya cahaya dan bit 0 menunjukkan tidak ada cahaya. *Fiber optic* biasanya digunakan untuk menyediakan koneksi yang berkecepatan tinggi dengan jarak tempuh sinyal yang lebih jauh dibandingkan dengan kabel *coaxial*. Karena menggunakan cahaya sebagai sinyal, *fiber optic* tidak terpengaruh interfensi elektromagnetik dan tidak mengalami *crosstalk*. Namun *fiber optic* lebih mahal dan lebih sulit dipasang dan ditangani dibandingkan media kabel *coaxial*.



Gambar 2.18 Fiber Optic

Berdasarkan jumlah sumber cahaya yang masuk pada core *fiber optic*, kabel *fiber optic* dibagi menjadi 2 yaitu:

a. *Multimode*, jumlah sumber lebih dari 1. Menggunakan diameter *core* dengan ukuran 50 *micron* – 100 *micron*.

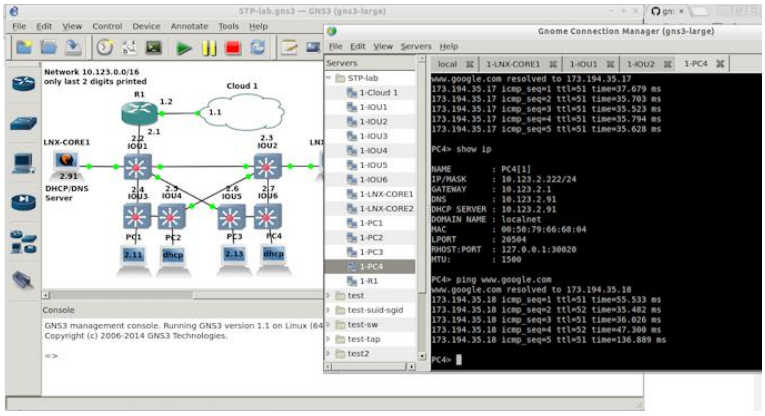
b. *Singlemode*, jumlah sumber 1. Menggunakan diameter *core* dengan ukuran 2 – 8 *micron*.

2.9.2 Media Transmisi Tanpa Kabel

Untuk terhubung ke jaringan *wireless*, suatu host harus mempunyai *wireless network adapter*. Untuk meningkatkan kompatibilitas, biasanya sebuah *access point* (AP) dipasang pada jaringan yang berfungsi sebagai hub bagi infrastruktur WLAN. *Access point* mempunyai antena untuk menyediakan konektivitas *wireless* untuk jangkauan daerah tertentu, biasanya disebut sebagai *cell*. Untuk melingkupi area yang lebih luas, *access point* dapat dipasang secara *overlap* hingga *host* dapat melakukan roaming diantara *cell* [9].

2.10 Graphic Network Simulator (GNS3)

GNS3 adalah software simulasi jaringan komputer berbasis GUI yang mirip dengan *Cisco Packet Tracer*. Namun pada GNS3 memungkinkan simulasi jaringan yang kompleks, karena menggunakan operating system asli dari perangkat jaringan seperti mikrotik, cisco dan juniper. Sehingga kita berada kondisi lebih nyata dalam mengkonfigurasi router langsung daripada di *Cisco Packet Tracer*. Dynamips adalah program inti dari GNS3 yang memungkinkan sebuah emulasi IOS Cisco berjalan. Dynamips dioperasikan diatas aplikasi GNS3 sehingga membuat suatu *environtment* yang lebih *user friendly* dengan menggunakan grafik dalam pengoperasian aplikasi tersebut. GNS3 adalah alat pelengkap yang sangat baik untuk laboratorium nyata bagi *network engineer*, karena GNS3 mensupport beberapa jenis aplikasi virtual lainnya seperti Pemu, Qemu, Virtual Box dan dapat mensupport *virtual* yang lainnya. *Router virtual* yang terdapat di GNS3 juga dapat dikoneksikan ke *hardware* yang sebenarnya. Prinsip kerja dari GNS3 adalah mengemulasi *device virtual* pada komputer, sehingga PC dapat berfungsi layaknya sebuah atau beberapa *router* bahkan *switch*, dengan cara mengaktifkan fungsi dari *Ethernet Switch Card*.



Gambar 2.19 Graphic Network Simulator (GNS3)

2.11 Protokol Redudansi

Pada jaringan komputer bagian penting lain dari perancangan suatu *network* adalah reliabilitas. Dalam rangka untuk menjaga reliabilitas yang tinggi, maka dibutuhkan protokol redudansi untuk membantu menghilangkan titik tunggal kegagalan. Berikut terdapat beberapa kelas protokol redundansi yang biasa digunakan.

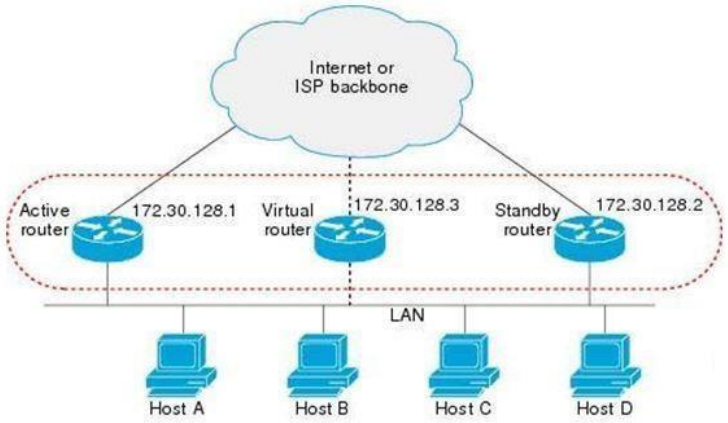
2.11.1 Hot Standby Routing Protocol (HSRP)

Hampir semua *host* komputer memiliki satu buah *ip router sebagai default gateway*. Saat HSRP digunakan, HSRP *virtual ip address* di digunakan sebagai *default gateway* dari *host*. HSRP digunakan oleh *host* yang tidak mendukung *router discovery* protokol (ICMP *Router Discovery Protocol* [IRDP]) dan tidak dapat mencari jalur lain saat *router* utama mengalami masalah. HSRP memberikan solusi untuk masalah ini dengan secara dinamis memilih jalur lain untuk meneruskan *traffic* jaringan.

Pada saat HSRP diaktifkan dalam suatu segmen jaringan, langsung memberikan layanan berupa *virtual mac address* dan *virtual ip address* yang disebarkan kepada setiap *router* yang menjalankan HSRP. Alamat dari grup HSRP ini tergantung pada *virtual ip* nya. Salah satu *router* terpilih sebagai *router* aktif yang tugasnya menerima dan meneruskan paket dari setiap MAC *address* dari group tersebut. Saat router aktif mengalami kegagalan dalam tugasnya, maka pada saat itu standby router mengambil alih semua pekerjaannya dan pada saat itu sebuah standby *router* yang baru dipilih. HSRP menggunakan prioritas *router* untuk

menentukan *router* mana yang dipilih untuk menjadi *active router* dan *standby router*. Untuk menetapkan suatu *router* menjadi *router* aktif secara manual dapat merubah prioritasnya menjadi lebih besar dari *router* HSRP lainya.

Secara *default*, *router* memiliki prioritas 100. Perangkat yang menjalankan HSRP mengirimkan dan menerima *multicast User Datagram Protocol* (UDP) *hello messages* untuk mendeteksi kegagalan router yang gunanya untuk menentukan *active* dan *standby router*. Saat *router* aktif tidak mengirimkan *hello message* dengan waktu yang telah di tentukan, maka *router* tersebut dinyatakan tidak aktif dan digantikan tugasnya oleh *standby router* yang akan berubah statusnya menjadi router aktif. Gambar dibawah ini menjelaskan sebuah network yang menggunakan HSRP. Dengan *virtual* MAC dan *IP address sharing*, dua atau lebih *router* dapat bertindak sebagai sebuah *virtual router*. *Virtual router* tidak ada secara fisik tetapi sebagai *default gateway* untuk *router* yang diatur sebagai *backup* pada setiap *router*. *Default gateway* pada setiap host diatur dengan virtual ip address yang dimiliki *router*.



Gambar 2.20 Contoh Topologi Protokol HSRP

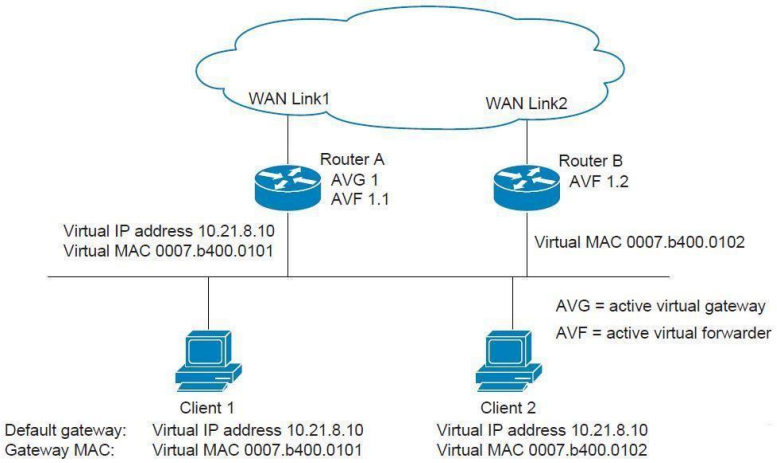
2.11.2 Gateway Load Balancing Protocol (GLBP)

Gateway Load Balancing Protocol (GLBP) menjaga *traffic* data dari kegagalan *router* atau *circuit*. Seperti *Hot Standby Router Protocol* (HSRP) dan *Virtual Router Redudancy Protocol* (VRRP), GLBP akan meneruskan pembagian beban paket diantara satu grup redudant *router*. Sebelum melakukan konfigurasi GLBP, pastikan *router* mendukung *multiple* MAC *address* pada *interface* fisik.

Setiap GLBP *forwarder* menggunakan MAC *address* tambahan untuk konfigurasinya. MAC *Address* tambahan tersebut disebut *virtual* MAC *Address*.

Secara *default*, *router* lain yang tersambung secara langsung pada LAN mengkombinasikan IP *virtual router* saat melakukan pembagian beban paket. *Router* lainnya berperan sebagai *router* GLBP *redudant* yang akan aktif bila *router* yang bekerja sebagai *forwarding* gagal. GLBP memiliki fungsi yang mirip seperti HSRP dan VRRP. HSRP dan VRRP mengijinkan *multiple router* untuk berperan dalam *virtual Router group* yang di-setting dengan *virtual IP address*. Salah satu *router* dipilih sebagai *router* aktif untuk meneruskan pengiriman paket melalui alamat *IP virtual*.

Sedangkan *router* lain dalam grup tersebut berperan sebagai *redudant router* hingga *router* aktif mengalami kegagalan dalam mengirim paket. *Standby Router* tersebut memiliki *bandwidth* yang tidak terpakai. Walaupun sekelompok *multiple virtual router* dapat dikonfigurasi untuk set *router* yang sama, namun hostnya harus dikonfigurasi untuk default *gateway* yang berbeda, yang menghasilkan administrasi beban yang lebih. Keuntungan GLBP adalah menyediakan pembagian beban melalui *multiple router* (*gateway*) menggunakan satu *virtual IP address* dan banyak *virtual MAC address*. Pengiriman beban dibagi diantara semua router yang ada dalam kelompok GLBP *router*, berbeda dengan HSRP dan VRRP yang menggunakan satu router aktif saja dalam pengiriman paket dan router lainnya hanya *standby*. Setiap *router* dalam satu kelompok GLBP melakukan komunikasi satu sama lain melalui *hello message* yang dikirimkan setiap 3 detik ke alamat 224.0.0.102 secara *multicast* menggunakan *User Datagram Protocol* (UDP) dengan *port* 3222 (pengirim dan penerima).

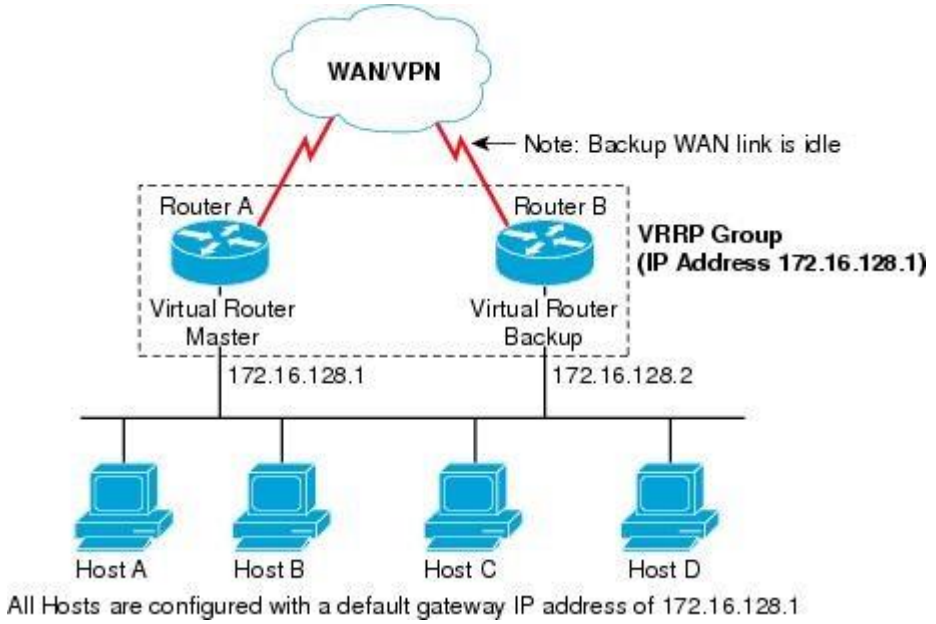


Gambar 2.21 Contoh Topologi Protokol GLBP

2.11.3 Virtual Router Redudancy Protocol (VRRP)

VRRP adalah protokol yang secara dinamis menunjuk satu atau lebih *virtual router* untuk menjadi VRRP *router* di dalam LAN, yang memungkinkan beberapa *router* di *multiaccess link* untuk menggunakan *virtual ip address* yang sama.

Sebuah VRRP *router* dikonfigurasikan untuk menjalankan VRRP protokol di dalam menghubungkan satu atau lebih *router* lainnya yang berada pada satu group di LAN yang sama. Dalam mengkonfigurasikan VRRP, satu *router* dipilih menjadi *virtual router master* dan *router* lain akan menjadi *backup* bila terjadi kegagalan di *virtual router master*. VRRP dirancang untuk digunakan di *multiaccess*, *multicast* maupun *broadcast* dengan menggunakan *ethernet* LAN. VRRP tidak dimaksudkan sebagai pengganti dari protokol dinamis yang ada. VRRP mendukung *Ethernet*, *Fastethernet, Bridge Group Virtual Interface* (BVI), *Gigabit Ethernet interfaces* dan pada *Multiprotocol Label Switching* (MPLS) *Virtual Private Networks* (VPNs).



Gambar 2.22 Contoh Topologi Protokol VRRP

2.11.3.1 Keuntungan VRRP

1. **Redudancy**

   VRRP memungkinkan untuk mengkonfigurasi beberapa *router* sebagai default *gateway router*, yang mengurangi kemungkinan satu titik kegagalan dalam sebuah jaringan.

2. **Load Sharing**

   VRRP dapat dikonfigurasi sedemikian rupa sehingga lalu lintas ke dan dari klien LAN dapat digunakan bersama oleh beberapa *router*, sehingga dapat membagi beban lalu lintas yang tersedia secara lebih merata di antara router.

3. **Multiple Virtual Router**

   VRRP mendukung hingga 255 *virtual router* (VRRP group) pada sebuah *router physical interface*. Beberapa dukungan *router virtual* memungkinkan untuk melaksanakan *redudancy* dan *load sharing* dalam topologi LAN.

4. **Multiple IP Addresses**

   Virtual Router dapat mengelola beberapa IP *address*, termasuk *secondary* ip *address*. Oleh karena itu, jika memiliki beberapa subnet yang dikonfigurasi pada *Ethernet interface*, VRRP dapat dikonfigurasikan pada setiap *subnet*.

5. **Preemption**

   Skema redundansi dari VRRP memungkinkan untuk membuat terlebih dahulu *virtual router* cadangan yang telah mengambil alih *virtual router master* yang gagal dengan prioritas yang lebih tinggi dari *virtual router* cadangan yang tersedia.

6. **Authentication**

   Pesan VRRP *digest* 5 (MD5) algoritma otentikasi melindungi VRRP-*spoofing* terhadap perangkat lunak dan menggunakan standar industri algoritma MD5 untuk meningkatkan kehandalan dan keamanan.

7. **Advertisement Protocol**

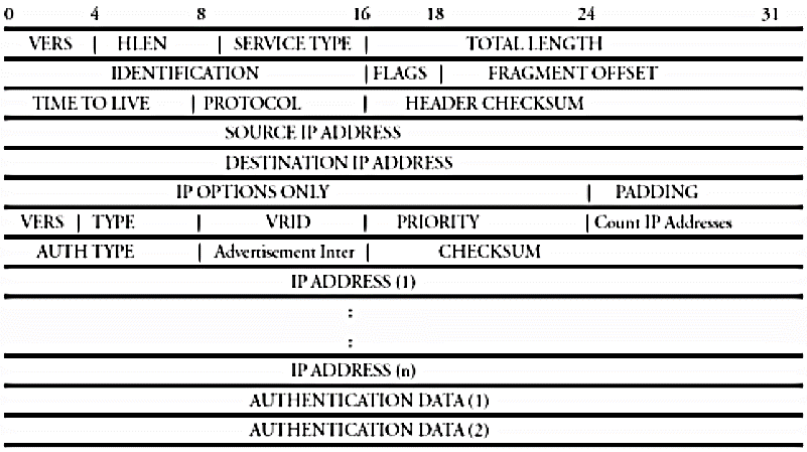
   VRRP menggunakan *Internet Assigned Numbers Authority* (IANA) dengan *standard multicast address*-nya (224.0.0.18). Skema pengalamatan ini meminimalkan jumlah *router* yang harus melayani *multicasts* dan memungkinkan peralatan tes untuk mengidentifikasi secara akurat paket VRRP pada segmen.

8. **VRRP Object Tracking**

   VRRP *Object Tracking* menyediakan cara untuk memastikan *router virtual master* terbaik dari *router* VRRP untuk VRRP *group* dengan mengubah prioritas ke status *Object Tracking* seperti *interface* atau IP *route states*.

2.11.3.2 Paket VRRP

Paket VRRP dikemas dalam paket IP. Gambar 2.23 menunjukan tata letak paket IP *header* dan paket itu sendiri



Gambar 2.23 Paket Data VRRP

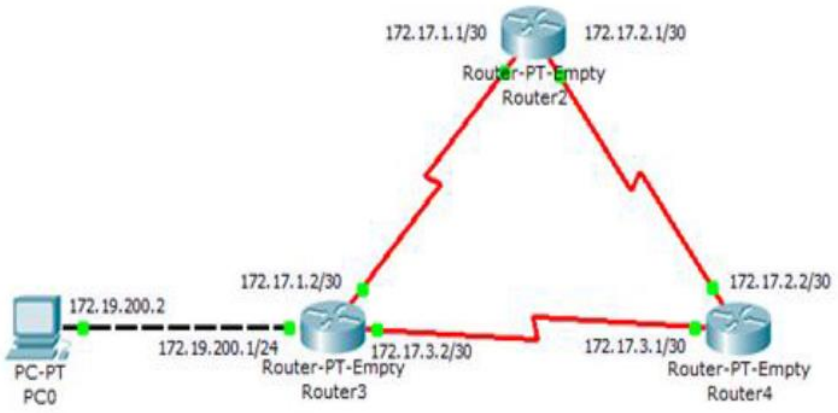
Pada bidang penting dalam header IP yang dijelaskan dibawah ini:

1. Sumber IP Address : ini adalah field 32-bit. Alamat sumber IP address interface utama dari paket yang sedang dikirim. Ini adalah IP address master interface router yang terhubung ke LAN.
2. Tujuan IP Address : ini adalah field 32-bit. Ini adalah IP address multicast yang diberikan oleh IANA untuk VRRP. Ini adalah IP Address multicast 224.0.0.18. Semua router yang menjalankan VRRP menerima multicast ini.
3. Time to Live (TTL) : ini adalah field 8-bit, nilai dalam field ini harus sama dengan 255. Setiap paket VRRP yang diterima tidak sama dengan 255 maka paket akan dibuang. Router tidak meneruskan datagram dengan alamat tujuan multicast VRRP, terlepas dari TTLnya.
4. Protokol : ini adalah field 8-bit yang menentukan protokol yang digunakan. IP protokol nomor yang di tetapkan oleh IANA untuk VRRP adalah 112.

2.12 OSPF

Routing Open Shortest Path First (OSPF) adalah sebuah *routing protocol open source* yang telah diimplementasikan oleh sejumlah besar vendor jaringan. Alasan untuk mengkonfigurasi OSPF dalam sebuah topologi adalah untuk mengurangi *overhead* (waktu pemrosesan) *routing*, mempercepat *convergance*, serta membatasi ketidakstabilan *network* disebuah area dalam suatu *network*. OSPF *Message Encapsulation* terjadi pada lapisan *data-link* dengan nomor protokol 89. *Data field* ini dapat berisi salah satu dari lima tipe paket OSPF.

Pada IP *packet header*, alamat tujuannya mempunyai dua alamat *multicast* yaitu 224.0.0.5 dan 224.0.0.6 namun yang diset cukup salah satu dari alamat tersebut. Bila paket OSPF dienkapsulasi di sebuah *frame Ethernet*, alamat tujuan dari *MAC address* juga merupakan sebuah alamat *multicast*, yaitu 01-00-5E-00-00-05 dan 01-00-5E-00-00-06. Semua paket OSPF mempunyai 24 *byte* yang berisikan informasi yang diperlukan. *Packet header* ini terdiri dari berbagai bidang seperti jenis-jenis paket OSPF, *router ID* serta alamat IP dari *router* yang mengirimkan paket.



Gambar 2.24 OSPF Routing

2.13 Reliabilitas

Reliabilitas adalah indeks yang menunjukkan sejauh mana suatu alat pengkur dapat dipercaya atau dapat diandalkan. Reliabilitas menunjukkan konsistensi hasil pengukuran. Suatu alat pengukur dikatakan konsisten, apabila dalam mengukur sesuatu berulang kali, alat pengukur itu menunjukkan hasil yang sama, dalam kondisi yang sama. Untuk dapat mendapatkan hasil dari reliabilitas, maka perlu dilakukan serangkaian pengujian.

Suatu perusahaan membutuhkan ketersediaan tinggi (*high availability*) jaringan yang tinggi, hal tersebut tidak lepas dari perangkat yang terhubung pada jaringan dapat berfungsi secara normal dan ketersediaan tinggi mendekati 100%. Dalam implementasinya diperlukan syarat sebagai berikut:

a. Memastikan ketersediaan akses aplikasi, tujuan dari perusahaan membuat jaringan adalah untuk memfasilitasi pengoperasian aplikasi yang menggunakan jaringan dan dapat berfungsi dengan baik.
b. Menambah kualitas karyawan dan memberikan loyalitas kepada pelanggan.
c. Mengurangi biaya belanja perangkat, solusi dalam hal ini yaitu dengan pemeliharaan (*maintenance*) perangkat secara berkala.
d. Mengurangi kerugian, sebuah jaringan atau perangkat yang mengalami kegagalan dapat mengurangi nilai penjualan dan pinalti terhadap kontrak kerja.

2.13.1 Teori Pengukuran Reliabilitas

Dalam membangun dan mengembangkan sistem, diperlukan suatu alat ukur yang dapat menentukan sejauh mana sistem dapat berjalan sesuai target dan spesifikasi pencapaian tertentu. Berikut teori-teori yang digunakan dalam mengukur tingkat reliabilitas.

2.13.1.1 Downtime

Downtime adalah jumlah waktu dimana suatu perangkat atau jalur yang menghubungkan antar perangkat tidak beroperasi yang disebabkan oleh bermacam faktor, namun biasanya disediakan perangkat atau jalur lain untuk mengambil alih. Jumlah downtime yang lama pada jaringan perusahaan sangat mempengaruhi kinerja maupun kerugian dari sisi *cost*.

$$Downtime = Finish\ Time - \ Start\ Time$$

2.13.1.2 Availability

Availability merupakan ukuran yang menunjukan sejauh mana sistem, subsistem atau peralatan dalam keadaan beroperasi dan dapat dijalankan yang dimana nilainya ditetapkan pada awal pekerjaan. Ada beberapa pengukuran yang digunakan dalam penelitian ini, yaitu [11]:

1. **MTTR**

   MTTR (*Mean Time To Repair*) adalah waktu rata-rata yang diperlukan untuk memperbaiki suatu kegagalan. Dalam prakteknya, kadang-kadang perhitungan MTTR tidak hanya mencakup waktu yang diperlukan untuk memperbaiki peralatan tetapi juga waktu yang diperlukan untuk persiapan, memanggil ahlinya, mendatangkan barang dan sebagainya.

   $$MTTR = \frac{Total\ Maintenance\ Time}{Number\ of\ Repairs}$$

2. **MTBF**

   MTBF (*Mean Time Between Failure*) adalah waktu rata-rata di antara dua kegagalan. Dalam banyak analisis, laju kegagalan biasanya dinyatakan tetap (tidak berubah terhadap waktu). Untuk peralatan elektronik, asumsi ini

biasanya cukup memadai dan bisa diterima. Jika laju kegagalan dianggap tetap maka peralatan elektronik biasanya mempunyai laju kegagalan yang relatif tetap. Peralatan mekanik, karena ada keausan, laju kegagalannya biasanya naik dengan berjalannya waktu.

$$MTBF = \frac{\Sigma(Operation\ Availability - Downtime)}{Number\ of\ Repairs}$$

Jadi, untuk perhitungan *Availability* terhadap penilaian sistem adalah sebagai berikut:

$$Availability = \frac{MTBF}{MTBF + MTTR} * 100$$

Setelah mendapat nilai dari *availability* sistem, diperlukan suatu ukuran atau standarisasi yang menentukan sejauh mana kualitas yang telah dicapai, berikut pada Tabel 2.2 merupakan standar dari perhitungan *availability* sistem [12].

Tabel 2.2 Standar Perhitungan Availability

Availability Target	Minutes Per Month Allowed	Score
99.99%	4.2	Excellent
99.98%		
99.90%	42	Average
99.50%	216	
99.00%	432	
98.60%	600	Poor
98.00%	840	

Ada beberapa pencapaian yang harus dipenuhi dalam meningkatkan reliabilitas adalah sebagai berikut:

1. Struktur sistem jika terjadi kegagalan dapat terselesaikan dengan cepat, sehingga menambah nilai MTBF.
2. Struktur sistem harus memungkinkan adanya bagian yang dibatasi dari sistem yang akan melakukan *restart*, hal ini untuk mengurangi nilai MTTR.
3. Tersedianya sistem monitoring yang dapat bereaksi dengan cepat memberikan pemberitahuan ketika terjadi kegagalan untuk mengurangi nilai MTTR.

4. Peremajaan dan pemeliharaan secara berkala komponen dari bagian perangkat sistem untuk mencegah kegagalan yang berkaitan dengan pengelolaan sumber daya dengan demikian dapat meningkatkan nilai MTBF.

Yang diharapkan dari pengembangan sistem dalam penelitian ini adalah, meningkatkan MTBF dan menurunkan MTTR.

2.14 Komponen-komponen Jaringan Komputer

Dalam merancang jaringan diperlukan komponen-komponen *hardware* untuk menghubungkan antar *user*. Komponen-komponen *hardware* ini dapat meningkatkan efisiensi dalam pengiriman paket dan *cost* yang dikeluarkan dalam merancang jaringan. Berikut Komponen-komponen *hardware*n yang menghubungkan jaringan secara garis besar terbagi menjadi dua, yaitu:

2.14.1 End-User Device

End-user device merupakan alat yang digunakan untuk menciptakan, menyimpan, mengambil dan berbagi informasi dari jaringan ke pemakai. *End-user device* biasanya disebut juga sebagai *host*. Contoh dari *end-user device* adalah : *notebook*, *pocket* PC, *printer*, *server*, *mainframe*, dan lain-lain. *End-user device* tidak mempunyai simbol yang standar, biasanya *end-user device* digambarkan menyerupai bentuk aslinya agar mudah dikenali.

Agar bisa dihubungkan ke jaringan, setiap *end-user device* mempunyai *Network Interface Card / Network Interface Controller* (NIC), yaitu sebuah papan sirkuit yang bertugas untuk menangani fungsi-fungsi yang berhubungan dengan jaringan. Setiap NIC bersifat unik karena mempunyai *media access control* (MAC) *address* yang berbeda pada setiap NIC. MAC *address* ini digunakan untuk mengatur komunikasi antar *host* pada jaringan.

2.14.2 Network Device

Network Device adalah alat yang digunakan untuk menghubungkan *end-user device* ke jaringan, memperluas jangkauan jaringan, melakukan konversi format data, dan banyak fungsi jaringan lainnya. Contoh *network device* adalah:

1. **Router**

   Router sering digunakan untuk menghubungkan beberapa *network*. Baik *network* yang sama maupun yang berbeda dari segi teknologinya. Seperti menghubungkan *network* yang menggunakan topologi *Bus*, *Star*, dan *Ring*. *Router* juga digunakan untuk membagi *network* besar menjadi beberapa buah *subnetwork* (network-network kecil). Setiap *subnetwork* seolah-olah "terisolir" dari *network* lain. Hal ini dapat membagi-bagi *traffic* yang akan berdampak positif pada performa *network* [13].

   Sebuah *router* memiliki kemampuan *routing*. Artinya *router* secara cerdas dapat mengetahui kemana rute perjalanan informasi (yang disebut packet) akan dilewatkan. Apakah ditujukan untuk *host* lain dalam satu *network* ataukah berbeda *network*. Jika paket-paket ditujukan untuk *host* pada *network* yang sama maka *router* akan menghalangi paket-paket keluar, sehingga paket-paket tersebut tidak "membanjiri" *network* yang lain [13].



Gambar 2.25 Router

2. **Hub**

   Hub menghubungkan semua komputer yang terhubung ke LAN. *Hub* adalah repeater dengan jumlah port banyak (*multiport repeater*). *Hub* tidak mampu menentukan tujuan, hanya mentransmisikan sinyal ke setiap *line* yang terkoneksi dengannya dengan menggunakan mode *half-duplex*.



Gambar 2.26 Hub

3. Switch

Switch adalah sebuah alat jaringan yang melakukan *bridging* transparan (penghubung segementasi banyak jaringan dengan *forwarding* berdasarkan alamat MAC). *Switch* jaringan dapat digunakan sebagai penghubung komputer atau *router* pada satu area yang terbatas, *switch* juga bekerja pada lapisan *data link*, cara kerja *switch* hampir sama seperti *bridge*, tetapi *switch* memiliki sejumlah port sehingga sering dinamakan *multi-port bridge*. *Switch* menghubungkan semua komputer yang terhubung ke LAN, sama seperti hub. Perbedaannya adalah *switch* dapat beroperasi dengan *mode full-duplex* dan mampu mengalihkan jalur dan memfilter informasi ke dan dari tujuan yang spesifik. Pada operasi *full-duplex*, kedua *station* mungkin mentransmisi secara serentak. Pada sistem ini aliran dapat terjadi di kedua arah pada saat yang bersamaan. Sistem ini dapat terjadi hanya menggunakan sebuah saluran komunikasi data atau dengan menggunakan dua saluran komunikasi data.



Gambar 2.27 Switch

4. Modem

Modem (*modulator-demodulator*) digunakan untuk mengubah informasi digital menjadi sinyal analog. Modem mengubah tegangan bernilai biner menjadi sinyal analog dengan melakukan *encoding* data digital ke dalam frekuensi *carrier*. Modem yang umum digunakan dihubungkan ke jalur telepon. Oleh karena itu modem ini mampu memodulasi data digital ke dalam sinyal berspektrum suara, yang disebut sebagai proses modulasi. Modem juga dapat mengubah kembali sinyal analog yang termodulasi menjadi data digital, sehingga informasi yang terdapat di dalamnya dapat dimengerti oleh komputer, proses ini disebut demodulasi.



Gambar 2.28 Modem

5. **Wireless 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 kabel atau *broadband ethernet*. Saat ini beredar di pasaran adalah *access point* yang telah dilengkapi dengan *router* di dalamnya yang biasa disebut *wireless router*. Fungsi utama dari *wireless access point* adalah untuk mengembangkan jaringan lokal kabel kita secara *wireless*.



Gambar 2.29 Wireless Access Point

2.15 Mikrotik

Mikrotik adalah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia, pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully yang berkebangsaan Amerika Serikat berimigrasi ke Latvia dan berjumpa Arnis yang sarjana Fisika dan Mekanika di sekitar tahun 1995. Tahun 1996 John dan Arnis mulai me-routing dunia (visi Mikrotik adalah me-routing seluruh dunia). Mulai dengan sistem Linux dan MS DOS yang dikombinasikan dengan teknologi Wireless LAN (W-LAN) Aeronet berkecepatan 2Mbps di

Moldova, tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia, karena ambisi mereka adalah membuat satu peranti lunak *router* yang handal dan disebarkan ke seluruh dunia. Dengan informasi yang ada di *web* Mikrotik, bahwa mereka mempunyai 600 titik (pelanggan) *wireless* dan terbesar di dunia [8].

Prinsip dasar mereka bukan membuat *Wireless* ISP (WISP), tapi membuat program *router* yang handal dan dapat dijalankan di seluruh dunia. Latvia hanya merupakan "tempat eksperimen" John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar empat ratusan pelanggannya. Mikrotik mempunyai 2 produk antara lain Mikrotik OS dan Mikrotik *Routerboard*.

1. MikroTik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk ip *network* dan jaringan *wireless*, cocok digunakan oleh ISP dan provider *hotspot*. Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.
2. Mikrotik *RouterBoard* adalah *router embedded* produk dari mikrotik. *Routerboard* seperti sebuah pc mini yang terintegrasi karena dalam satu *board* tertanam prosesor, ram, rom, dan memori flash. *Routerboard* menggunakan os RouterOS yang berfungsi sebagai *router* jaringan, *bandwidth management*, *proxy server*, DHCP, DNS *server* dan bisa juga berfungsi sebagai *hotspot server*.



Gambar 2.30 Logo Mikrotik

2.15.1 Fungsi Mikrotik

Fungsi utama mikrotik adalah menjadikan sebuah komputer sebagai network *router* (*Routing*). Selain itu, mikrotik juga mempunyai fungsi untuk menjalankan aplikasi, meliputi [8]:

1. Aplikasi kapasitas akses *Bandwith Management*
2. Aplikasi *Firewall*
3. *Wireless Access Point* (Wi-Fi)
4. Aplikasi *Backhaul Link*
5. Sistem *Hotspot*
6. *Virtual Private Network* (VPN) *Server*

2.15.2 Fitur-fitur Mikrotik

Fungsi utama mikrotik adalah menjadikan sebuah komputer sebagai network *router* (Routing). Selain itu, mikrotik juga mempunyai fungsi untuk menjalankan aplikasi, meliputi [8]:

1. **Penanganan Protokol TCP/IP**
   a. **Firewall and NAT** - stateful packet filtering; Peer-to-Peer protocol filtering; source and destination NAT; classification by source MAC, IP addresses, ports, protocols, protocol options, interfaces, internal marks, content, matching frequency.
   b. **Routing** - Static routing; Equal cost multi-path routing; Policy based routing (classification by source and destination addresses and/or by firewall mark); RIP v1 / v2, OSPF v2, BGP v4.
   c. **Data Rate Management** - per IP / protocol / subnet / port / firewall mark; HTB, PCQ, RED, SFQ, byte limited queue, packet limited queue; hierarchical limitation, CIR, MIR, contention ratios, dynamic client rate equalizing (PCQ).
   d. **HotSpot** - HotSpot Gateway with RADIUS authentication/accounting; data rate limitation; traffic quota; real-time status information; walled-garden; customized HTML login pages; iPass support; SSL secure authentication.

e. **Point-to-Point tunneling protocols** - PPTP, PPPoE and L2TP Access Concentrators and clients; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; MPPE encryption; compression for PPPoE; data rate limitation; PPPoE dial on demand.
f. **Simple tunnels** - IPIP tunnels, EoIP (Ethernet over IP).
g. **IPsec** - IP security AH and ESP protocols; Diffie-Hellman groups 1,2,5; MD5 and SHA1 hashing algorithms; DES, 3DES, AES-128, AES-192, AES-256 encryption algorithms; Perfect Forwarding Secresy (PFS) groups 1,2,5.
h. **Web proxy** - FTP, HTTP and HTTPS caching proxy server; transparent HTTP caching proxy; SOCKS protocol support; support for caching on a separate drive; access control lists; caching lists; parent proxy support.
i. **Caching DNS client** - name resolving for local use; Dynamic DNS Client; local DNS cache with static entries.
j. **DHCP** - DHCP server per interface; DHCP relay; DHCP client; multiple DHCP networks; static and dynamic DHCP leases.
k. **Universal Client** - Transparent address translation not depending on the client's setup.
l. **VRRP** - VRRP protocol for high availability.
m. **UPnP** - Universal Plug-and-Play support.
n. **NTP** - Network Time Protocol server and client; synchronization with GPS system.
o. **Monitoring/Accounting** - IP traffic accounting, firewall actions logging.
p. **SNMP** - read-only access.
q. **M3P** - MikroTik Packet Packer Protocol for Wireless links and Ethernet.
r. **MNDP** - MikroTik Neighbor Discovery Protocol; also supports Cisco Discovery Protocol (CDP).
s. **Tools** - ping; traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer.

2. **Layer 2 Konektifitas**
    a. **Wireless** - IEEE802.11a/b/g wireless client and Access Point; Wireless Distribution System (WDS) support; virtual AP; 40 and 104 bit WEP; access control list; authentication on RADIUS server; roaming (for wireless client); Access Point bridging.
    b. **Bridge** - spanning tree protocol; multiple bridge interfaces; bridge firewalling.
    c. **VLAN** - IEEE802.1q Virtual LAN support on Ethernet and WLAN links; multiple VLANs; VLAN bridging.
    d. **Synchronous** - V.35, V.24, E1/T1, X.21, DS3 (T3) media types; sync-PPP, Cisco HDLC, Frame Relay line protocols; ANSI-617d (ANDI or annex D) and Q933a (CCITT or annex A) Frame Relay LMI types.
    e. **Asynchronous** - serial PPP dial-in / dial-out; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; onboard serial ports; modem pool with up to 128 ports; dial on demand.
    f. **ISDN** - ISDN dial-in / dial-out; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; 128K bundle support; Cisco HDLC, x75i, x75ui, x75bui line protocols; dial on demand.
    g. **SDSL** - Single-line DSL support; line termination and network termination modes.

2.15.3 Level Mikrotik dan Kemampuan

Mikrotik Router hadir dalam berbagai level. Tiap level memiliki kemampuannya yang berbeda-beda., diantaranya [8]:

a. **Level 0** (gratis). Tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
b. **Level 1** (demo). Dapat digunakan sebagai fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.

c. **Level 3**. Mencakup level 1 ditambah dengan kemampuan untuk menajemen router berinterface ethernet.
d. **Level 4**. Mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola wireless client atau serial interface, untuk aplikasi hotspot bisa digunakan untuk 200 pengguna.
e. **Level 5**. Mencakup level 1, 3 dan 4 ditambah dengan kemampuan wireless AP, untuk aplikasi hotspot bisa digunakan untuk 500 pengguna.
f. **Level 6**. Mencakup semua level dan tidak memiliki limitasi apapun, untuk aplikasi hotspot bisa digunakan untuk pengguna yang tidak terbatas.

Tabel 2.3 Level Mikrotik

Level Number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited

Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	unlimited
Number of KVM guests	none	1	unlimited	unlimited	unlimited	unlimited

2.15.4 Produk Mikrotik

Pada perkembangannya sampai saat ini produk-produk Mikrotik sudah lebih bermacam-macam. Berikut merupakan produk-produk dari Mikrotik [8]:

1. **DOM**

   Berbentuk media penyimpanan seperti hardisk dari beberapa vendor yang sudah ada di Indonesia yang berisikan Mikrotik OS sekaligus dengan lisensinya.



Gambar 2.31 DOM Mikrotik

2. **Routerboard**

   Routerboard adalah *router embedded* produk dari mikrotik. *routerboard* seperti sebuah pc mini yang terintegrasi karena dalam satu *board* tertanam *processesor*, ram, rom, dan memori *flash*. *Routerboard* menggunakan os RouterOS fungsinya sebagai *router* jaringan, *bandwidth management*, *proxy server*, DHCP, DNS *server* dan bisa juga berfungsi sebagai *hotspot server*. Ada beberapa seri *routerboard* yang juga bisa berfungsi sebagai wifi. sebagai wifi *access point*, *bridge*, wds ataupun sebagai wifi *client*. seperti seri RB411, RB433, RB600. dan sebagian besar isp *wireless*

menggunakan *routerboard* untuk menjalankan fungsi wirelessnya baik sebagai ap ataupun *client* [8].

Dengan *routerboard* kita bisa menjalankan fungsi sebuah *router* tanpa tergantung pada pc lagi, karena semua fungsi pada *router* sudah ada dalam *routerboard*. Dibandingkan dengan pc yang diinstal routerOS, *routerboard* ukurannya lebih kecil, lebih kompak dan hemat listrik karena hanya menggunakan *adaptor*. untuk digunakan di jaringan wifi bisa dipasang diatas tower dan menggunakan PoE (*Power On Ethernet*) sebagai sumber arusnya.



Gambar 2.32 Routerboard Mikrotik