BAB II
TINJAUAN PUSTAKA

2.1 CCTV (*Closed Circuit Television*)

2.1.1 Pengertian CCTV

CCTV (*Closed Circuit Television*) merupakan suatu perangkat kamera video digital yang digunakan untuk merekam dan mengirimkan sinyal hasil tangkapannya ke layar monitor di suatu ruangan atau tempat tertentu dengan bantuan dari DVR (*Digital Video Recorder)*. Pemakaian CCTV memiliki tujuan untuk memantau keadaan suatu ruangan atau daerah tertentu agar dapat mencegah terjadinya suatu tindakan atau kegiatan yang menyimpang yang dilakukan oleh pihak-pihak tertentu atau hasil tangkapan dari CCTV dapat pula dijadikan sebagai barang bukti dari tindakan atau kegiatan menyimpang yang telah terjadi.

Pada umumnya, CCTV seringkali digunakan pada area umum seperti : Hotel, Bandar Udara, Kantor dan Pabrik. Namun seiring perkembangan zaman, CCTV juga telah mulai digunakan di perumahan – perumahan. Sistem kamera digital saat ini dapat dikontrol melalui Personal Computer ataupun telephone genggam dimanapun dan kapanpun selama ada komunikasi melalui internet maupun akses GPRS.

2.1.2 Sejarah CCTV

Salah satu kegunaan CCTV besar pertama di tahun 1940-an oleh Militer AS untuk menguji misil V2, kamera sirkuit tertutup digunakan untuk memonitori tes keselamatan. Teknologi ini menguntungkan karena seperti pengertian CCTV yang memungkinkan petugas untuk memantau dan melihat secara langsung kemungkinan yang terjadi saat misil diluncurkan, dan dapat dengan segara mencari jalan keluar apabila terjadi suatu kesalahan. Tanpa CCTV, misil yang diluncurkan tidak dapat diketahui kemana arah yang akan dituju.

Di Inggris pada 1960-an CCTV dipasang di beberapa tempat umum untuk mengamati kerumunan selama pawai dan rapat umum. Dengan ilmu pengetahuan dan teknologi yang semakin berkembang, telah menjadikan teknologi CCTV lebih banyak digunakan di tempat-tempat umum untuk memantau dan memonitori berbagai aktivitas. Selanjutnya CCTV banyak digunakan untuk untuk mencegah berbagai tindakan dan kegiatan yang menyimpang.

2.2 Dome CCD Camera

Gambar 2.1 Dome CCD Camera

(Sumber : Komponen yang digunakan dalam pembuatan Laporan Akhir)

Dome CCD Camera biasanya digunakan untuk di dalam ruangan dengan sudut tangkap yang lebar. Dome CCD Camera sangat efektif untuk memantau ruangan yang cukup luas, selain itu terdapat beberapa led inframerah yang berfungsi untuk menangkap titik fokus yang cukup jelas pada kondisi ruangan yang gelap.

Type ini menggunakan 1/3″ Sony CCD Sensor sehingga menghasilkan gambar yang bagus. Dilengkapi dengan Led Inframerah untuk perekaman cahaya minim (walaupun gelap total, switch to B/W), sehingga kamera ini masih bisa memantau ruangan dalam kondisi gelap.

Kamera CCTV tipe ini dapat ditambah dengan komponen lainnya seperti Audio, sehingga CCTV yang awalnya hanya dapat menangkap/merekam suatu aktivitas, dapat juga merekam suara yang ditimbulkan dari aktifitas tersebut. Hasil tangkapan audio inipun nantinya akan disimpan pada DVR dan dapat diputar ulang.

2.3 DVR (*Digital Video Recorder*)

Gambar 2.2 Standalone DVR

(Sumber : Komponen yang digunakan dalam pembuatan Laporan Akhir)

DVR *(Digital Video Recorder)* ini adalah alat untuk memonitori dan merekam obyek gambar yang nampak oleh kamera CCTV, dapat menampilkan dan merekam 4-8-9-16 kamera sekaligus secara bersamaan maupun bergantian (moving).

Alat ini meggunakan harddisk sebagai media penyimpanan data dari hasil rekaman. Hasil rekamannya akan disimpan ke dalam harddisk tersebut, dengan kompresi file rekaman yang kecil namun berkualitas tinggi. Metode perekaman juga dapat diatur berdasarkan waktu atau berdasarkan sensor gerak. Tapi dapat

juga di atur untuk merekam sampai dengan satu bulan, tapi hasil rekamannya kurang baik. Jadi bila Anda ingin merekam satu bulan secara real time dalam waktu satu bulan, Anda harus menggunakan kapasitas harddisk minimal 1 Terabyte.

Alat ini juga berfungsi sebagai *quad processor*, yang dapat menampilkan hasil real-time dari 4-8-9-16 kamera CCTV sekaligus dalam 1 layar. Alat ini dapat disambungkan langsung ke televisi untuk melihat tampilan gambarnya melalui AV 1 atau AV 2 yang tersedia pada layar televisi. Hasil rekaman juga dapat langsung diputar menggunakan alat ini. Terdapat slot RJ-45 untuk disambungkan ke *router / hub / switch* agar bisa melakukan remote viewing melalui komputer yang terhubung ke jaringan internet dan juga bisa dilakukan untuk *Local Area Network* (LAN) ke beberapa komputer di dalam area kantor arau area lainnya.

2.4 UPS (*Uninterruptible Power Supply)*

Gambar 2.3 UPS

(Sumber : Komponen yang digunakan dalam pembuatan Laporan Akhir)

UPS adalah singkatan dari *Uninterruptible Power Supply* yang merupakan peralatan listrik yang fungsi utamanya adalah untuk menyediakan listrik tambahan atau baterai back up pada bagain tertentu dari komputer atau alat elektronik lain yang perlu untuk mendapatkan asupan listrik secara terus-menerus. UPS dijual dalam berbagai ukuran, namun yang paling umum dijumpai di pasaran adalah berbentuk kotak seperti stavolt. Semua *Uninterruptible Power Supply* berat karena adanya baterai yang terletak dalam alat tersebut.

UPS bekerja di tengah-tengah peralatan, yaitu diantara terminal listrik di dinding dengan alat-alat elekronik lainnya. Dengan kata lain, alat-alat elektronik terhubung ke UPS dan UPS mendapatkan listrik dari terminal listrik. Satu atau lebih baterai yang terletak dalam UPS menyediakan listrik kepada alat-alat elektronik yang terhubung padanya, sehingga ketika listrik padam, peralatan tersebut masih teraliri listrik. Baterai pada UPS dapat di *charge* kembali (*rechargable*) dan seringkali juga dapat diganti dengan yang baru.

Selain menyediakan listrik tambahan saat listrik padam, UPS juga berperan sebagai alat untuk menstabilkan teganggan listrik yang mengalir ke alat-alat elektronik sehingga bebas dari tegangan naik atau turun yang dapat merusak alat-alat elektronik.

Dalam perkembangannya, UPS memiliki dua tipe, yaitu :

1. SPS atau *Stanby Power System* berfungsi memonitor tenaga listrik yang masuk melalui kabel dan akan mengalirkan listrik ke mode baterai segera setelah masalah terdeteksi.
2. On-line UPS tidak mengalirkan listrik ke mode baterai saat masalah terjadi, melainkan terus mensuplai listrik dari UPS walaupun listrik tidak padam.

Fungsi dari UPS adalah :

1. Dapat memberikan energi listrik sementara ketika terjadi kegagalan daya pada listrik utama (PLN).
2. Memberikan kesempatan waktu yang cukup kepada kita untuk segera menghidupkan Genset sebagai pengganti PLN.

3. Memberikan kesempatan waktu yang cukup kepada kita untuk segera melakukan back up data.
4. UPS secara otomatis dapat melakukan stabilisasi tegangan ketika terjadi perubahan tegangan pada input sehingga tegangan output yang digunakan oleh alat – alat elektronik berupa tegangan yg stabil.
5. UPS dapat melakukan diagnosa dan management terhadap dirinya sendiri sehingga memudahkan pengguna untuk mengantisipasi jika akan terjadi gangguan terhadap sistem.
6. User friendly dan mudah dalam installasi.
7. User dapat melakukan kontrol UPS melalui Jaringan LAN dengan menambahkan beberapa accessories yang diperlukan.
8. Dapat diintegrasikan dengan jaringan Internet.
9. Notifikasi jika terjadi kegagalan dengan melakukan setting software UPS management.

2.5 *Wireless Media* (Media Tanpa Kabel)

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. Macam – macam jaringan wireless atau jaringan nirkabel yaitu :

a. Wireless Personal Area Network (WPAN)

Wireless Personal Area Network merupakan jaringan komputer yang digunakan untuk melakukan komunikasi antara perangkat komputer (termasuk telepon dan *Personal Digital Assistants* (PDA)) ke satu orang. Jangkauan untuk *Personal Area Network* hanya beberapa meter saja. Teknologi yang menggunakan WPAN misalnya adalah *bluetooth* dan *infared*.

b. *Wireless Local Area Network (WLAN)*

Wireless Local Area Network menggunakan radio untuk melakukan pengiriman data antar komputer pada jaringan LAN. Jenis – jenis WLAN adalah :

- *Wi-Fi*, biasanya menggunakan jaringan wireless dalam sistem komputer yang dapat menghubungkan internet atau mesin lainnya yang memiliki fungsi *Wi-Fi*.
- *Fixed Wireless Data*, merupakan tipe jaringan nirkabel data yang dapat digunakan untuk menghubungkan dua atau lebih gedug secara bersamaan untuk memperluas atau membagi *bandwitdh* jaringan tanpa menggunakan kabel (secara fisik) pada gedung.

c. *Wireless Metropolitan Area Network (WMAN)*

Koneksi ini dapat mencakup jangkauan yang sangat luas seperti pada sebuah kota atau negara, melalui beberapa antena atau sistem satelit yang digunakan oleh penyelenggara jasa telekomunikasi. Teknologi WMAN ini dikenal dengan sistem 2G (*Second Generation*). Inti dari sistem 2G ini termasuk di dalamnya Global System for *Mobile Communication* (GSM), *Celluler Digital Packet Data* (CDPD) dan *Code Divition Multiple Access* (CDMA)

2.6 *Wireless Router*

Wireless Router 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 *transmitter* 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.*

Wireless Router selain sebagai penghubung (*access point*) untuk jaringan *Local* bisa berfungsi mem-*forward* IP di luar dalam jaringan *Local.* Sebagai contoh kita mempunyai IP 192.168.0.1 untuk jaringan *Local* kita sedangkan kita ingin jaringan 192.168.0.1 kita tidak tersentuh oleh orang luar dari jaringan local itu. Dari *Wireless Router* itu kita bisa setting sebagai contoh menjadi IP 10.50.10.xxx. Otomatis *client* yang mendapat IP dari 10.50.10.1 itu tidak bisa masuk ke jaringan 192.168.0.1.

Inilah fungsi maksimal dari *router* yaitu untuk memprotect jarigan lokal kita sehingga resiko data diambil oleh orang luar lebih sedikit. Jadi kesimpulannya *Wireless Router* adalah sebuah *access point* yang berfungsi meneruskan IP *Local* kita sedangkan *Router* berfungsi meneruskan IP *Local* kita menjadi IP yang kita inginkan.

Wireless Router ini berfungsi menerima paket data internet yang diberikan oleh modem USB sesuai dengan provider yang digunakan, jaringan internet yang diterima kemudian dipancarkan kembali sehingga bisa diterima pada jarak kurang lebih 50 meter.

Gambar 2.4 Wireless Router

(Sumber : http://tutorialspoint.com, diakses 9 Mei 2014)

2.7 Modem (Modulator Demodulator)

Modem adalah singkatan dari modulator dan demodulator. Modulator berfungsi untuk melakukan proses menumpangkan data pada sinyal informasi ke sinyal pembawa agar dapat dikirim ke pengguna melalui media tertentu, proses ini biasa disebut dengan proses modulasi. Pada proses ini data dari komputer yang berbentuk sinyal digital akan diubah menjadi sinyal analog. Sedangkan Demodulator berfungsi sebagai proses mendapatkan kembali data yang dikirim oleh pengirim. Pada proses ini data akan dipisahkan dari frekuensi tinggi dan data yang berupa sinyal analog akan diubah kembali menjadi sinyal digital agar bisa dibaca oleh komputer.

Jadi kesimpulannya fungsi modem adalah sebuah perangkat keras yang berfungsi untuk komunikasi dua arah yang merubah sinyal digital menjadi sinyal analog atau sebaliknya untuk mengirimkan pesan/data ke alamat yang dituju. Bisa juga diartikan sebagai perantara untuk menghubungkan komputer kita ke jaringan internet.

Banyak jenis – jenis modem yang ada pada saat ini, jenis modem dapat dibedakan berdasarkan pemasangannya dan jaringannya. Jika berdasarkan pemasangannya modem bisa dibedakan menjadi modem internal dan modem eksternal :

1. Modem Internal merupakan sebuah kartu yang dipasangkan pada slot motherboard. Keuntungan modem ini adalah cara pemasangannya mudah dan harganya relatif lebih murah.
2. Modem eksternal adalah modem yang dipasang diluar komputer, biasanya ditancapkan pada slot USB.

Sedangkan berdasarkan jaringannya modem bisa dibedakan menjadi modem dengan media kabel dan modem dengan media tanpa kabel :

1. Modem yang menggunakan media kabel yaiitu sebuah modem yang menggunakan kaebl sebagai media perantaranya (contoh : TV kabel dan jaringan komputer)
2. Modem tanpa kabel, modem ini menggunakan media tanpa kabel untuk perantaranya (contoh : Modem GSM, Modem CDMA dan lain - lain).

2.7.1 Jenis Modem Berdasarkan Teknologi

Gambar 2.5 Jenis – jenis Modem
(Sumber : http://chotimtik.blogspot.com, diakses 9 Mei 2014)

Berdasarkan teknologi atau jenis koneksinya, modem dapat dibedakan menjadi beberapa jenis, yaitu sebagai berikut :

1. Modem Analog, yaitu mode yang dapat menerima data dalam bentuk sinyal anaog melalui sautu jaringan transmisi data dan mengubahnya menjadi data digital untuk dikirimkan ke komputer atau sebaliknya. Modem ini digunakan untk koneksi dial up lewat jaringan telepon, sehingga juga disebut modem dial up. Modem analog tersedia dalam berbagai kecepatan, misalnya 14,4 kbps, 28,8 kbps dan 56 kbps dengan berbagai merek.
2. Modem DSL (*Digital Subscriber Line*), yaitu modem untuk menerima dan mengirimkan data dengan teknologi DSL melalui suatu jaringan terdedikasi (*dedicated line* – jaringan khusus yang terus – menerus tersedia untuk keperluan internet, yang secara fisik dapat menggunakan kabel telepon). Dalam teknologi ini dara yang diterima/dkirim modem DSL berupa data digital, sehingga akses internet lebih cepat dibandingkan dengan modem analog. Ada dua jenis DSL, yaitu ADSL (*Asymetric Digital Subscriber Line*, kecepatan unduh atau donwnstream lebih cepat

daripada unggah atau upstream) dan SSL (*Symmetric Digital Subscriber Line*, kecepatan downstream sama dengan kecepatan upstream).

3. Modem kabel, yaitu modem yang menerima dan mengirim data internet yang melalui jaringan TV Kabel. Data yang diterima dan dikirim juga berupa data digital dengan kecepatan setara modem DSL.
4. Modem CDMA, yaitu modem dial up wiireless yang bekerja dengan teknologi CDMA (*Code Division Multiple Access*), misalnya modem CDMA USB atau dapat pula menggunakan telepon genggam CDMA.
5. Modem GSM, yaitu modem *wireless mobile* yang bekerja pada jalur komunikasi telepon genggam GSM. Modem ini mendukung layanan GPRS/EDGE atau layanan 3G. Contohnya berupa modem GSM USB atau dapat menggunakan telepon genggam GSM yang mendukung teknologi GPRS/EDGE atau 3G.

2.8 Macam – Macam Jaringan Internet

Teknologi senantiasa berkembang sejalan dengan perubahan zaman, termasuk dalam bidang telekomunikasi dan informasi. Kebutuhan akan akses data nirkabelpun juga terus meningkat, baik dari segi kuantitas maupun kualitasnya. Beberapa perusahaan telekomunikasi terus berlomba menyediakan jaringan terbaik dalam menunjang kebutuhan akses data bagi pelanggannya.

2.8.1 GPRS (*Global Package Radio Service*)

Suatu teknologi yang memungkinkan pengiriman dan penerimaan data dalam bentuk paket data yang berkaitan dengan e-mail, data gambar dan penelusuran internet. GPRS yang juga disebut teknologi 2.5G merupakan evolusi ari teknologi 1G dan 2G sebelumnya. Di Indonesia, GPRS diperkenalkan pada tahun 2001 saat penyedia jaringan seperti IM3 mempromosikannya. Idealya jaringan GPRS memiliki kecepatan mulai dari 56 kbps sampai 115 kbps, namun kenyataanya, hal tersebut tergantung dari faktor – faktor seperti konfigurasi dan alokasi tiime slot pada level BTS, software yang digunakan dan dukungan fitur serta aplikasi ponsel yang digunakan.

2.8.2 EDGE (*Enchance Data Rates for Global Evolution*)

Merupakan kelanjutan evolusi dari GSM dan IS-136 dengan tujuan pengembangan teknologi untuk meningkatkan kecepatan transmisi data, efisiensi spektrum dan memungkinkannya penggunaan aplikasi – aplikasi baru serta meningkatkan kapasitas. Jaringan EDGE juga disebut sebagai teknologi 2.7G diperkenalkan pertama kali oleh Cingular (sekarang AT&T) di Amerika Serikat pada tahun 2003. Jaringan EDGE pada idealnya memiliki kecepatan mencapai 236 kbps.

2.8.3 Teknologi 3G (*Third-Generation Technology*)

Merupakan teknologi evolusi dari generasi sebelumnya yang memiliki kapasitas pengiriman dan penerimaan dari lebih besar dan lebih cepat. Oleh karena itulah, teknologi ini dapat digunakan untuk melakukan video call. Teknologi 3G sering juga disebut dengan mobile boarband karena keunggulannya sebagai modem untuk internet yang bersifat portable. Perkembangan 3G secara komersial dimulai pada tahun 2001 di Jepang oleh NTTDoCoMo yang kemudian disusl oleh Korea Selatan pada tahun 2002.

Idealnya teknologi ini memiliki kecepatan transfer data pada level minimum 2Mbps pada penguna yang berada pada posisi diam ataupun berjalan kaki, dan 384kbps pada pengguna yang berada di dalam kendaraan yang sedang berjalan. Frekuensi yang digunakan oleh teknologi 3G, yaitu :

1. Frekuensi penerimaan (downlink) 1920-1980 MHz.
2. Frekuensi pengiriman (uplink) 2110-2170 MHz.

2.8.3.1 Tujuan Teknologi 3G

Pada awal diperkenalnya teknologi 3G, teknologi 3G mempunyai tujuan sebagai berikut :

1. Menambah efisiensi dan kapasitas jaringan.
2. Menambah kemampuan jelajah (roaming).
3. Untuk mencapai kecepatan transfer data yang lebih tinggi.

4. Peningkatan kualitas layanan (*Quality of Service – QOS*).
5. Mendukung kebutuhan internet bergerak (*mobile internet*).

2.8.3.2 Kelebihan Teknologi 3G

Teknologi 3G merupakan perkembangan dari teknologi – teknologi sebelumnya, kelebihan teknologi 3G dari generasi sebelumnya yaitu :

1. Kualitas suara yang lebih bagus.
2. Keamanan yang terjamin.
3. Kecepatan data mencapai 2 Mbps untuk lokal/Indoor/slow-moving access dan 384 kbps untuk *wide area access*.
4. Support beberapa koneksi secara simultan, sebagai contoh, pengguna dapat browse internet bersamaan dengan melakukan call (telepon) ke tujuan yang berbeda.
5. Infrastruktur bersama dapat mensupport banyak operator dilokasi yang sama. Interkoneksi ke other mobile dan *fixed users*.
6. Roaming nasional dan internasional.
7. Bisa menangani *packet-and circuit-switched service* termasuk internet (IP) dan *Video conferencing*. Juga *high data rate communication services* dan *asymmetric data transmission*.
8. Efisiensi spektrum yang bagus, sehingga dapat menggunakan secara maksimum bandwidth yang terbatas.
9. Support untuk *multiple cell layer*.
10. *Co-existance* and interconnection dengan *satellite-based* services.
11. Mekanisme billing yang baru tergantung dari volume data, kualitas service dan waktu.

2.8.4 HSDPA (*High-Speed Downlink Packet Access*)

Merupakan teknologi yang disempurnakan dari teknologi sebelumnya yang juga dapat disebut 3.5G, 3G+ atau Turbo 3G yang memungkinkan jaringan berbasis *Universal Mobile Telecommunication System* (UMTS) memiliki kecepatan dan kapasitas transfer data yang lebih tinggi. Penggunaan HSDPA saat

ini menyokong kecepatan penelusurandari 1.8, 3.6, 7.2 hingga 14 Mbps.Oleh karena itulah jaringan HSDPA ini sangat memungkinkan untuk digunakan sebagai modem internet pada komputer ataupun notebook.

Pemasaran HSDPA dalam bentuk modem yang digunakan sebagai koneksi mobile broadband baru diperkenalkan pada tahun 2007. Pada Agustus tahun 2009, 250 jaringan HSDPA secara komersial telah meluncurkan layanan mobile broadband di 109 negara.

2.8.5 HSUPA (*High-Speed Uplink Packet Access*)

HSUPA merupakan salah satu protokol ponsel yang memperbaiki proses uplink atau penaikkan data dari perangkat ke server (unggah) yang mencapai 5,76 Mbps. Dengan kecepatan ini, pengguna dapat lebih mudah mengunggah tulisan, gambar, maupun video ke blog pribadi ataupun situs seperti YouTube hanya dalam waktu beberapa detik saja. HSUPA juga dapat mempermudah melakukan video streaming dengan kualitas DVD, konferensi video, game *real-time*, e-mail dan MMS.

Saat terjadi kegagalan dalam pengiriman data, HSUPA dapat melakukan pengiriman ulang. Tingkat kecepatan pengiriman juga dapat disesuaikan dengan keadaan ketika terjadi gangguan jaringan transmisi. HSUPA diluncurkan secara komersial pertama kali pada awal tahun 2007.

2.8.6 HSPA (*High-Speed Packet Access*)

Merupakan koleksi protokol telepon genggam dalam ranah 3.5G yang memperluas dan memperbaiki kinerja protokol *Universal Mobile Telecommunication System* (UMTS). *High-Speed Downlink Packet Access* (HSDPA), *High-Speed Uplink Packet Access* (HSUPA) dan *High Speed Packet Access+* (HSPA+) adalah bagian dari keluarga *High-Speed Packet Access* (HSPA).

HSPA merupakan hasil pengembangan teknologi 3G gelombang pertama, *Release 99* (R99). Sehingga HSPA mampu bekerja jauh lebih cepat bila dibandingkan dengan koneksi R99. Terkait jaringan CDMA, HSPA dapat

disejajarkan dengan Evolution Data Optimied (EV-DO) yang merupakan perkembangan dari CDMA2000.

Jaringan HSPA sebagian besar tersebar pada spektrum 1900 MHz dan 2100 MHz namun beberapa berjalan pada 850 MHz. Spektrum yang lebih besar digunakan karena operator dapat menjangkau area yang lebih luas serta kemampuannya untuk refarming dan realokasi spektrum UHF.

HSPA menyediakan kecepatan transmisi data yang berbeda dalam arus data turun (*downlink*) an dalam arus naik (*uplink*), terkait standar pengembangan yang dilakukan *Third Generation Partnership* (3GPP). Perkembangan lanjutan HSPA dapat semakin memudahkan akses ke dunia maya karena sarat fitur rapi dan canggih sehingga dapat mengurangi biaya transfer data per megabit.

Pada tahun 2008 terddapat lebih dari 32 juta koneksi HSPA di dunia. Hal ini bertolak belakang dengan akhir kuartal pertama 2007 yang hanya berjumlah 3 juta. Pada tahun yang sama, sekitar 80 negara telah memiliki layanan HSPA dengan lebih dari 467.000 jenis perangkat HSPA yang tersedia di seluruh dunia, seperti perangkat bergerak, notebook, data card, wireless router, USB modem.

2.8.7 HSPA+ (*High Speed Packet Access*)

HSPA+ atau disebut juga Evolusi HSPA adalah teknologu standar pita lebar nirkabel yang akan hadir dengan kemampuan pengiriman data mencapai 42 Mbps untuk downlink dengan menggunakan modulasi 64QAM dan 11 Mbps untuk uplink dengan modulasi 16QAM.

Pengembangan lainnya pada HSPA+ adalah tambahan penggunaan antena *Multiple Input Multiple Ouput* (MIMO) untuk membantu peningkatan kecepatan data. HSPA+ memberikan pilihan berupa arsitektur all-IP (*Internet Protokol*) yang dapat mempercepat jaringan serta lebih murah dalam penyebaran dan pengenaliannyya. Sampai Agustur 2009, terdapat 12 jaringan HSPA+ di dunia dengan kecepatan downlink mencapai 21 Mbps. Pelopornya adalah Telstra di Australia pada akhir 2008. Sedangkan jaringan untuk kecepatan 28 Mbps telah hadir untuk pertama kalinya di dunia dengan Italia sebagai negara perintisnya.

2.8.8 EV-DO (*Evolution Data Optimized*)

EVDO juga dikenal dengan EV-DO, 1xEvDO dan 1xEV-DO merupakan sebuah standar pada wireless broadband berkecepatan tinggi. EVDO adalah singkatan dari "*Evolution, Data Only*" atau "*Evolution, Data Optimized*". Istilah resminya dikeluarkan oleh Assosiasi Industri Telekomunikasi yaitu CDMA2000, merupakan interface data berkecepatan tinggi pada media udara. EVDO satu dari dua macam standar utama wireless Generasi ke-3 atau 3G. Adapun standar yang lainnya adalah W-CDMA.

Kelebihan EVDO dibandingkan CDMA biasa, tentu lebih mengirit spektrum frekuensi dari regulator dan amat mahal pastinya, menurunkan biaya pengembangan dan memanfaatkan jaringan baru. Di Amerika AVDO dipakai oleh Verizon dan Sprint, di Korea juga digunakan. Saat artikel ini dbuat AVDO tidak terlalu berpengaruh di pasar Eropa dan Sebagian besar Asia karena di Wilayah tersebut telah memilih 3G sebagai pilihan mereka. Namun demikian di Indonesia telah ada beberapa operator ang memakai teknologi EVDO.

2.9 *Internet Protokol* (IP)

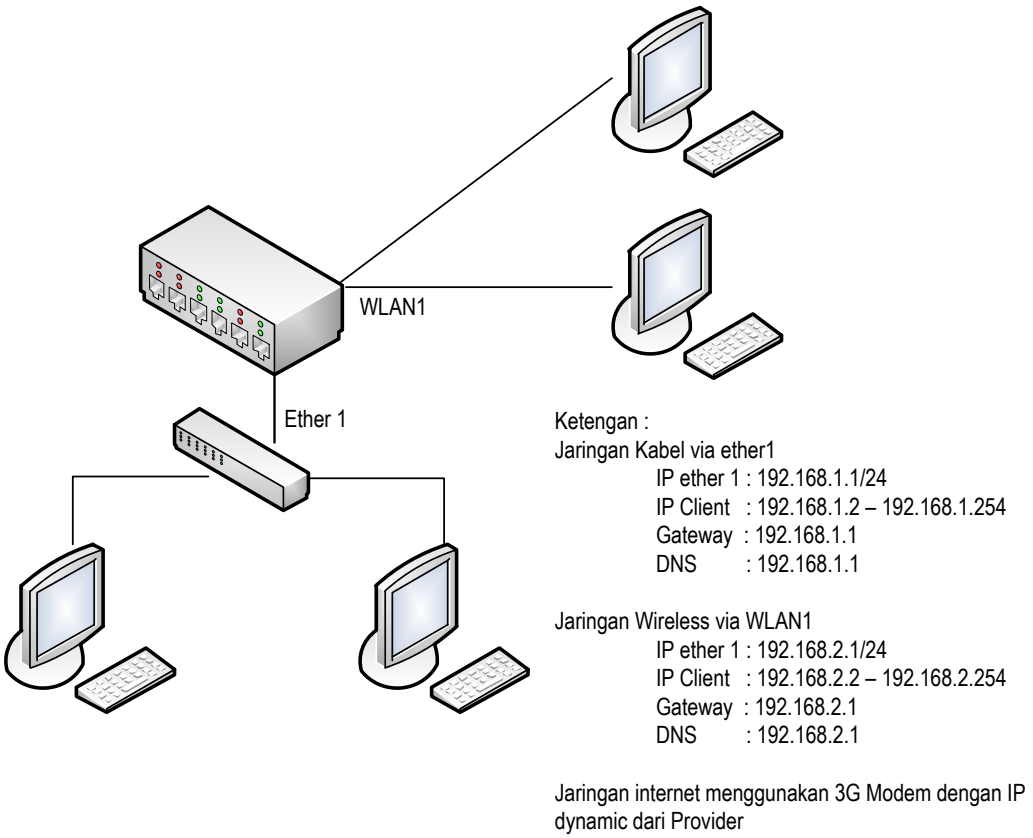
Secara sederhana IP merupakan standar komunikasi data yang digunakan oleh komunitas internet dalam prose tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet. Agar jaringan internet ini berlaku semestinya harus ada aturan standar yang mengaturnya karena itu diperlukan suatu protokol internet.

Namun secara lebih *complicated* defini *Intrenet Protocol* adalah protokol lapisan jaringan (*network layer* dalam OSI *Reference Model*) atau protokol lapisan internetwork (*internetwork layer* dalam DARPA *Reference Model*) yang digunakan oleh protokol TCP/IP untuk melakukan pengalamatan dan *routing* paket data antar *host-host* di jaringan komputer berbasis TCP/IP. Versi IP yang banyak digunakan adalah IP versi 4 (Ipv4) yang didefinisikan pada RFC 791 dan dipublikasikan pada tahun 1981, tetapi akan digantikan oleh IP versi 6.

Protokol IP merupakan salah satu protokol kunci di dalam kumpulan protokol TCP/IP. Sebuah paket IP akan membawa data aktual yang dikirimkan melalui jaringan dari satu titik ke titik lainnya. Metode yang digunakannya adalah connectionless yang berarti ia tidak perlu membuat dan memelihara sebuah sesi koneksi. Selain tu, protokol ini juga tidak menjamin penyampaian data, tapi hal ini diserahkan kepada protokol padda lapisan yang lebih tinggi (lapisan *transport* dalam OSI *Reference Model* atau lapisan antar *host* dalam DARPA *Reference Model*), yakni *Transmission Control Protocol* (TCP).

Internet Protocol dikembangkan pertama kali oleh *Defense Advanced Research Projects Agency* (DARPA) pada tahun 1970 sebagai awal dari usaha untuk mengembangkan protokol yang dapat melakukan interkoneksi berbagai jaringan komputer yang terpisah, yang masing-masing jaringan tersebut menggunakan teknologi yang berbeda. Protokol utama yang dihasilkan proyek ini adalah *Internet Protocol* (IP). Riset yang sama dikembangkan pula yaitu beberapa protokol level tinggi yang didesain dapat bekerja dengan IP.

Hal ini paling penting dari proyek tersebut adalah *Transmission Control Protocol* (TCP), dan semua *group protocol* diganti dengan TCP/IP *suite*. Pertama kali TCP/IP diterapkan di ARPANET dan mulai berkembang setelah Universitas California di Berkeley mulai menggunakan TCP/IP dengan sistem operasi UNIX. Selain *Defense Advanced Research Projects Agency* (DARPA) ini yang mengembangkan *Internet Protocol*, yang juga mengembangkan TCP/IP adalah *Department of Defense* (DOD).



Gambar 2.6 Jaringan IP

(Sumber : http://mikrotikindo.blogspot.com, diakses 10 mei 2014)

Adapun layanan yang ditawarkan oleh IP adalah sebagai berikut :

a. IP menawarkan layanan sebagai protokol antar jaringan (*inter-network*)

IP juga sering disebut sebagai protokol yang bersifat *routable*. *Header* IP mengandung informasi yang dibutuhkan untuk menentukan rute paket, yang mencakup alamat IP sumber (*source IP Address*) dan alamat IP tujuan (*destination IP Address*). Anatomi alamat IP terbagi menjadi dua bagian, yakni alamat jaringan (*network address*) dan alamat node (*node address.host address*). Penyampaian paket antar jaringan (umumnya disebut sebagai proses routing), dimungkinkan karena adanya alamat jaringan tujuan dalam alamat IP. Selain itu, IP juga mengizinkan pembuatan sebuah jaringan yang cukup besar, yang disebut sebagai IP

internetwork, yang terdiri atas dua atu lebih jarngan yag dihubungkan dengan menggunakan rouuter berbasis IP.

b. IP mendukung banyak protokol client

IP merupakan "kurir" pembawa data yang dikirimkan oleh protokol – protokol lapisan yang lebih tinggi dibandingka dengannya. Protokol IP dapat membawa beberapa protokol lapisan tinggi yang berbeda-beda, tapi setiap paket IP hanya dapat mengandung data dari satu buah protokol dari banyak protokol tersebut dalam satu waktu. Karena setiap paket dapat membawa satu buah paket dari beberapa paket data, maka harus ada cara yang digunakan untuk mengidikasikan protokol lapisan tinggi dari paket data yang dikirimkan sehingga dapat diteruskan kepada protokol lapisan tinggi yang sesuai pada sisi penerima.

Mengingat klien dan server selalu menggunakan protokol yang sama untuk sebuah data yang saling dipertukarkan, maka setiap paket tidak harus mengidikasikan sumber dan tujuan yang terpisah. Contoh dari protokol-protokol lapisan yang lebih tinggi dibandingkan IP adalah *Internet Control Management Protocol* (ICMP), *Internet Group Management Protocol* (IGMP), *User Datagram Protocol* (UDDP) dan *Transmission Control Protocol* (TCP).

c. IP mengirimkan data dalam bentuk datagram

IP hanya menyediakan layanan pengiriman data secara connectionless serta tidak andal (*unreliable*) kepada protokol – protokol yang berada lebih tinggi dibandingkan dengan protokol IP. Pengiriman *connectionless*, berarti tidak perlu ada negosiasi koneksi (*handshaking*) sebelum mengirimkan data dan tidak ada koneksi yang harus dibuat atau dipelihara dalam lapisan ini. *Unreliable*, berarti IP akan mengirimkan paket tnapa proses pengurutan dan tanpa acknowledgent ketika pihak yang dituju telah dapat diraih. IP hanya akan melakukan pengiriman sekali kirim daja untuk menyampaikan paket – paket kepada hop selanjutnya atau tujuan akhir

(teknik seperti ini disebut sebagai "*best effort delivery*"). Keandalan data bukan merupakan tugas dari protokol IP, tetapi merupakan protokol yang berada pada lapisan yang lebih tinggi, seperti halnya protokol TCP.

d. Bersifat independen dari lapisan antarmuka jaringan (lapisan pertama dalam DARPA *Reference Model*)

IP didesain agar mendukung banyak komputer dan antarmuka jaringan. IP bersifat independen terhadap atribut lapisan fisik, seperti halnya pengabelan, pensinyalan dan bit rate. Selain itu, IP juga bersifat independen terhadap atribut lapisan data link seperti halnya mekanisme *Media Access Control* (MAC), pengalamatan MAC, serta ukuran frame terbesar. IP menggunakan skema pengalamatannya sendiri, yang disebut sebagai "*IP Address*", yang merupkan bilangan 32-bit dan independen terhadap skema pengalamatan yang digunakan dalam lapisan antarmuka jaringan.

e. Mendukung ukuran frame terbesar yang dimiliki oleh teknologi lapisan antarmuka jaringan yang berbeda – beda

IP dapat melakukan pemecahan terhadap paket data ke dalam beberapa fragmen sebelum diletakkan di atas sebuah saluran jaringan. Paket data tersebut akan dipecah ke dalam fragmen – fragmen yang memiliki ukuran *Maximum Transmission Unit* (MTU) yang lebih rendah dibandingkan dengan ukuran datagram IP.

Proses ini dinamakan dengan fragmentasi. *Router* atau *host* yang mengirimkan data akan memecah data yang hendak ditransmisikan dan proses fragmentasi dapat berlangsung beberapa kali. Selanjutnya host yang dituju akan menyatukan kembali fragmen – fragmen tersebut menjadi paket data utuh, seperti halnya sebelum dpecah. Dapat diperluas dengan menggunakan fitur *IP Options* dalam *header IP*. Fitur yang dapat ditambahkan contohnya adalah kemampuan untuk menentukan jalur yang harus diikuti oleh datagram IP melalui sebuah *internet network* IP.

2.9.1 Istilah – istilah di dalam *Internet Protocol*

Ada beberapa istilah yang sering ditemukan di dalam pembicaraan mengenai TCP/IP, yaitu diantaranya :

a. *Host* atau *End-System*

Seorang pelanggan pada layan jaringan komunikasi. *Host* biasanya berupa *individual workstation* atau personal computers (PC) dimana tugas dari Host ini biasanya adalah menjalankan aplikasi dan program software server yang berfungsi sebagai user dan pelaksana pelayanan jaringan komunikasi.

Internet, yaitu merupakan suatu kumpulan dari jaringan (*network of networks*) yang menyeluruh dan menggunakan protokol TCP/IP untuk berhubungan seperti *virtual networks*.

b. Node

Node adalah istilah yang diterapkan untuk *router* dan *host-protocol*, yaitu merupakan sebuah prosedur standar atau aturan untuk pendefinisian dan pengaturan transmisi data antara komputer – komputer.

c. Router

Router adalah suatu devais yang digunakan sebagai penghubung antara dua *network* atau lebih. *Router* berbeda dengan *host* karena *router* biasanya bukan berupa tujuan atau data *traffic*. *Routing* dari datagram IP biasanya telah dilakukan dengan *software*. Jadi fungsi *routing* dapat dilakukan oleh *host* yang mepunyai dua *networks connection* atau lebih.

2.9.2 Alamat IP (*Internet Protocol Address*)

Alamat IP adalah deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan internet. IP sangat berbeda dengan DNS. Panjang dari angka ini adalah 32-bit (untuk Ipv4 atau IP versi 4) dan 128bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan Internet berbasis TCP/IP. Sistem pengalamatan IP ini terbagi menjadi dua, yakni :

- IP versi 4 (Ipv4)
- IP versi 5 (Ipv6)

Contoh IP :

- 192.168.0.1
- 192.168.0.2
- 192.168.0.3
- 202.134.0.13

(Sumber : Konsep ddan Penerapan Microsoft TCP/IP.2001:105)

2.9.3 Pembagian Kelas IP *Address*

Pembagian kelas – kelas ini ditujukan untuk mempermudah alokasi IP *Address*, baik untuk host/jaringan tertentu atau untuk keperluan tertentu. IP *Address* dapat dipisahkan menjadi 2 bagian, yakni bagian *network* (net ID) dan bagian *host* (*host* ID). Net ID berperan dalam identifikasi suatu *network* dari *network* yang lain, sedangkan *host* ID berperan untuk identifikasi *host* dalam suatu *network.* Jadi, seluruh *host* yang tersambung dalam jaringan yang sama memiliki net ID yang sama. Sebagian dari bit – bit bagian awal dari IP Address merupakan *network bit/networknumber*, sedangkan sisanya untuk host. Garis pemisah antara bagian *network* dan *host* tidak tetap, bergantung kepada kelas *network*. IP *Address* dibagi ke dalam lima kelas, yaitu kelas A, kelas B, kelas C, kelas D dan kelas E.

Perbedaan tiap kelas adalah pada ukuran dan jumlahnya. Contohnya IP kelas A dipakai oleh sedikit jaringan namun jumlah host yang dapat ditampung oleh tiap jaringan sangat besar. Kelas D dan E tidak digunakan secara umum, kelas D digunakan bagi jaringan *multicast* dan kelas E untuk keperluan eksperimental. Perangkat lunak *Internet Protocol* menentukan pembagian jenis kelas ini dengan menguji beberapa bit pertama dari IP *Address*.

a. IP Address kelas A

Penentuan kelas ini dilakukan dengan cara, Bit pertama IP *Address* kelas A adalah 0, dengan panjang net ID 8 bit dan panjang host ID 24 bit.

Jadi *byte* pertama IP *Address* kelas A mempunyai range dari 0-127. Jadi pada kelas A terdapat 127 *network* dengan tiap *network* dapat menampung sekitar 16juta *host* (225x225x225). IP Address kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar.

b. IP Address kelas B

Dua bit IP *Address* kelas B selalu diset 10 sehingga *byte* pertamanya selalu bernilai antara 128-191. *Network* ID adalah 16 bit pertama dan 16 bit sisanya adalah *host* ID sehingga kalau ada komputer mempunyai IP *Address* 167.205.26.161, network ID = 167.205 dan host ID = 26.161. Pada IP *Address* kelas B ini mempunyai range IP dari 128.0.xxx.xxx sampai 191.155.xxx.xxx, yakni berjumlah 65.255 *network* dengan jumlah host tiap *network* 255x255 *host* atau sekitar 65 ribu host.

c. IP Address kelas C

IP Address kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga bit pertama IP *Address* kelas C selalu diset 111. *Network* ID terdiri dari 24 bit dan *host* ID 8 bit sisanya sehingga dapat terbentuk sekitar 2 juta *network* dengan masing – masing *network* memiliki 256 host.

d. IP Address kelas D

IP *Address* kelas D digunakan untuk keperluan *multicasting*. 4 bit pertama IP *Address* kelas D selalu diset 1110 sehingga *byte* pertamanya berkisar antara 224-247, sedangkan bit – bit berikutnya diatus sesuai keperluan *multicast group* yang menggunakan IP *Address* ini. Dalam multicasting tidak dikenal istilah *network* ID dan *host* ID.

e. IP Address kelas E

IP kelas ini tidak diperuntukkan untuk keperluan umum. 4 bit pertama IP *Address* kelas ini diset 1111 sehingga *byte* pertamanya berkisar antara

248-255. Sebagai tambahan dikenal juga istilah *Network Prefix*, yang digunakan untuk IP *Address* yang menunjuk bagian jaringan. Penulisan *Network Prefix* adalah dengan tanda slash "/" yang diikuti angka yang menunjukkan panjang *Network Prefix* ini dalam bit. Misal untuk menunjukkan satu network kelas B 167.205.xxx.xxx digunakan penulisan 167.205/16. Angka 16 ini merupakan panjang bit untuk *Network Prefix* kelas B.

2.9.4 *Subnet Mask*

Subnet Mask adalah bilangan 32 bit. Angka digit 1 pada *subnet mask* menunjukkan bahwa bit tersebut pada alamat IP adalah bagain dari *netid*. Angka 0 pada *subnet mask* menandakan bahwa bit tersebut adalah bagian dari *hosted*.

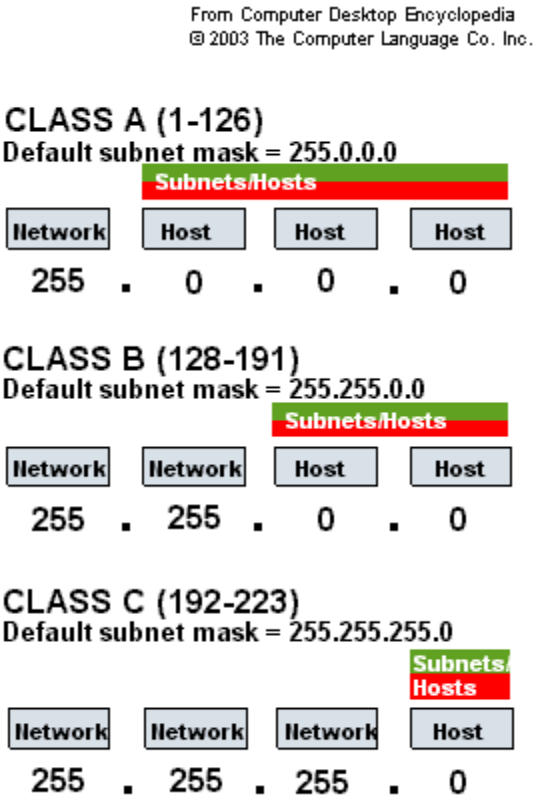
Subnet Mask hampir selalu terdiri dari bit – bit ordo tinggi yang berurutan. Sehingga, kita hanya perlu mengingat delapan bilangan desimal agar mampu mengenali sebagian besar *subnet mask*. Delapan subnet mask umum tersebut adalah :

Tabel 2.1 Subnet Mask Umum

Biner	Desimal
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

(Sumber : Konsep dan Penerapan Microsoft TCP/IP.2001 : 112)

Saat sebuah jaringan dikonfigurasikan untuk mendukung pengalamatan *subnet, subnet mask* harus diberikan, walaupun mungkin tidak ada *subnetting* yang dipergunakan. *Subnet mask* ditentukan dengan memberikan nilai 1 pada bit yang bersesuaian dengan *dield netid* pada alamat kelas tersebut.



Gambar 2.7 Subnet Mask

(Sumber : http://ik13.blogspot.com, diakses 9 Mei 2014)

2.10 DNS (*Domain Name System*)

2.10.1 Sejarah DNS (*Domain Name System*)

Sebelum dipergunakannya DNS, jaringan komputer menggunkan *Hosts Files* yang berisi informasi dari nama komputer dan IP *Address*. Di Internet, *file* ini dikelola secara terpusat dan di setiap lokasi harus di copy versi terbaru dari *Hosts Files*, dari sini bisa dibayangkan betapa repotnya jika ada penambahan 1 komputer di jaringan, maka kita harus copy versi terbaru file ini ke setiap lokasi. Dengan makin meluasnya jaringan internet, hal ini makin merepotkan, akhirnya

dibuatkan sebuah solusi dimana DNS di desian menggantikan fungsi *Hosts Files*, dengan kelebihan *Unlimited Database Size* dan *Performance* yang baik.

DNS adalah sebuah aplikasi *services* di Internet yang menerjemahkan sebuuah domain name ke IP *Address*. Sebagai contoh, "www" untuk penggunaan di Internet, lalu diketikkan nama domain, misalnya : yahoo.com" maka akan dipetakan ke sebuah IP mis 202.68.0.134. Jadi DNS dapat dianalogikan pada pemakaian buku telepon, dimana orang yang kita kenal berdasarkan nama untuk menghubunginya kita harus memutar nmor telepon di pesawat telepon. Sama persis, *host* komputer mengirimkan *queries* berupa nama komputer dan domain server ke DNS, lalu oleh DNS dipetakan ke IP *Address*.

2.10.2 Pengertian DNS (*Domain Name System*)

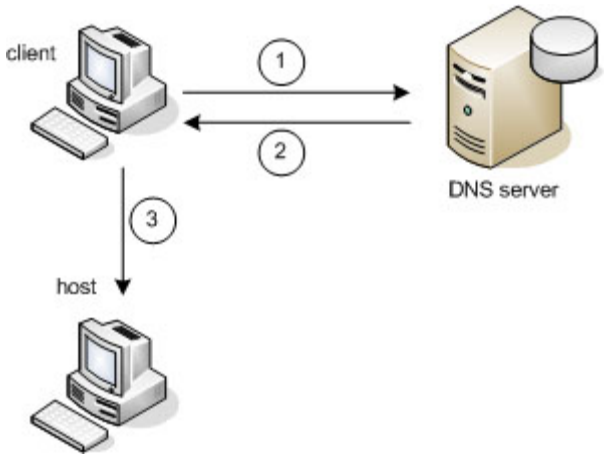
Domain Name System (DNS) adalah *distribute database system* yang digunakan untuk pencarian nama kompur (*name resolution*) di jaringan yang menggunakan TCP/IP (*Transmission Control Protocol/Internet Protocol*). DNS biasa digunakan pada aplikasi yang terhubung ke Internet seperti *web browser* atau e-mail, dimana DNS membantu memetakan *host name* sebuah komputer ke IP *Address*.

Selain digunakan di Internet, DNS juga dapat di implementasikan ke *private network* atau internet dimana DNS memiliki keunggulan karena DNS sangat mudah, sehingga pengguna tidak lagi direpotkan untuk mengingkat IP Address sebuah komputer cukup dengan *host name* (nama komputer). IP Address sebuah komputer bisa berubah tapi *host name* tidak berubah. Pengelola dari sistem DNS terdiri dari tiga komponen :

1. DNS *resolver*, sebuah program klien yang berjalan di komputer pengguna, yang membuat permintaan DNS dari program aplikasi.
2. *Recursive* DNS *server*, yang melakukan pencarian melalui DNS sebagai tanggapan permintaan dari *resolver* dan mengembalikan jawaban kepada para *resolver* tersebut.

3. *Authoritative* DNS *server*, yang memberikan jawaban terhadap permintaan dari *recursor* baik dalam bentuk sebuah jawaban. Maupun dalam bentuk delegasi (misalkan : mereferensikan ke *authoritative* DNS *server* lainnya).

DNS dapat disamakan fungsinya dengan buku telepon. Dimana setiap komputer di jaringan Internet memiliki *host name* (nama komputer) dan *Internet Protocol* (IP) *Address*. Secara umum, setiap *client* yang akan mengkoneksikan komputer yang satu ke komputer yang lain, akan menggunakan *host name*. Lalu komputer anda akan menghubungi DNS server untuk mencek *host name* yang diminta tersebut berapa IP *Address*-nya. IP *Address* ini yang digunakan untuk mengkoneksikan komputer anda dengan komputer lainnya.



Gambar 2.8 Hubungan Client dan DNS Server
(Sumber : http://amanubelajarmenguasaikomputer.blogspot.com, diakses 9 Mei 2014)

Penjelasan ilustrasi dari gambar di atas adalah :

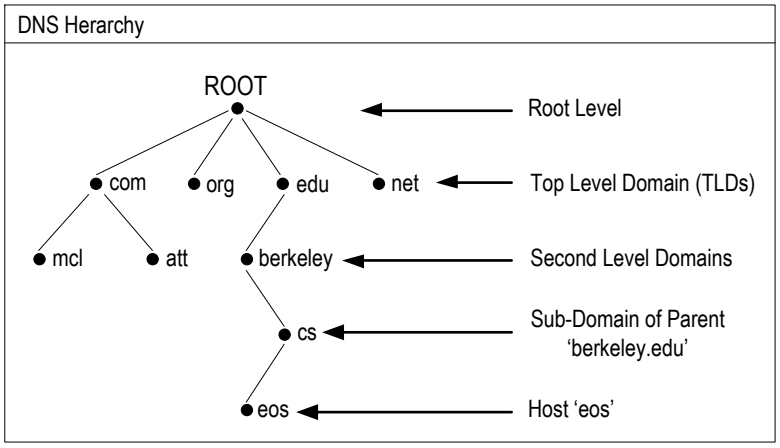
1. *Resolvers* meminta alamat IP dari “www.tamia.org” ke DNS *Server*.
2. DNS *Server* mengirim jika alamat IP nya ada maka dikirim ke *Resolvers* lagi, namun kalau tiidak ada pesan *message failure note* akan muncul.
3. Resolvers menghubungi host yang ituju dengan menggunakan IP *Address* yang diperoleh dari *Name Server*.

2.10.3 Strukur DNS

Domain Server Space merupakan sebuah hirarki pengelompokan domain berdasarkan nama, yang terbagi menjadi beberapa bagian diantaranya :

2.10.3.1 *Root Level Domain* (RLD)

Domain ditentukan berdasarkan tingkatan kemampuan yang ada di struktur hirarki yang disebut dengan level. Level paling atas di hirarki disebut dengan *root domain*. Root domain di ekspresikan berdasarkan periode dimana lambang untuk *root domain* adalah (".")



Gambar 2.9 Diagram *Root Level*

(Sumber : http://prstie.blogspot.com, diakses 10 Mei 2014)

2.10.3.2 *Top Level Domain* (TLD)

Top Level Domain adalah domain pada level teratas di bawah *root* (.). Ada tiga pengelompokkan *Top Level Domain* :

a. Domain Generik

Terdiri dari 7 domain, yaitu :

1. com : untuk organisasi komersial. Contoh : ibm.com, cun.com.
2. net : untuk organisasi/perusahaan penyedia layanan jaringan/internet. contoh : interniic.net, nsf.net.
3. gov : untuk lembaga/organisasi pemerintahan. contoh : whitehouse.gov, nasa.gov.
4. mil : untuk badan/organisasi militer. Contoh : army.mil.

5. org : untuk organsasi non-komersial.contoh : linux.org.
6. edu : untuk lembaga pendidikan. Contoh : mit.edu,berkeley.edu.
7. int : untuk oranisasi internasional. Contoh : nato.int

Selain 7 domain di atas, ada 7 domain baru dai ICANN (www.icann.org), yaitu :

1. aero : untuk industrii atau perusahaan udara.
2. biz : untuk perusahaan atau lembaga bisnis.
3. coop : untuk perusahaan atau lembaga kooperatif.
4. info : untuk penggunaan umum.
5. museum: untuk museum.
6. name : untuk registrasi bagi penggunaan individual/personal.
7. pro : untuk para profesional seperti : akuntan dan lain – lain.

b. Domain Negara

Merupakan standar pembagian geografis berdasarkan kode negara, contoh : id untuk Indonesia, au untuk Australia, uk untuk Inggris dan lain – lain. Domain negara ini dapat dan umumnya diturunkan lagi ke level – level di bawahnya yang diatur oleh NIC dari masing – masing negara, untuk Indonesia yaitu IDNIC. Contoh level di bawah dari id yaitu net.id, co.id, web.id.\

c. Domain Arpa

Merupakan domain untuk jaringan ARPAnet. Tiap domain yag tergabung ke internet berhak memiliki name-space .in-addr.arpa sesuai dengan alamat IP-nya.

2.11 DMZ (*Demilitarized Zone*)

Firewall DMZ (*Demilitarized Zone*) atau jaringan perimeter adalah jaringan security boundary yang terletak diantara suatu jaringan coorporate / private LAN dan jaringan public (Internet). Firewall DMZ ini harus dibuat jika membuat segmentasi jaringan untuk meletakkan server yang bisa diakses public

dengan aman tanpa harus bisa menggangu keamanan system jaringan LAN di jaringan private. Perimeter (DMZ) network didesain untuk melindungi server pada jaringan LAN coorporate dari serangan hackers dari internet.

Firewall DMZ dapat diimplementasikan tepat pada border coorporate LAN mempunyai tiga jaringan interface :

- Interface Internet : Interface ini berhubungan langsung dengan internet dan IP Addressnya juga IP public yang terregister.
- Interface Private atau Interface Intranet : Interface yang terhubung langsung dengan jaringan coorporate LAN dimana anda meletakkan server – server yang rentan terhadap serangan.
- Jaringan DMZ : Interface DMZ ini berada di dalam jaringan internet yang sama sehingga bisa diakses oleh user dari internet. Resources public yang umumnya berada pada firewall DMZ adalah web-server, proxy dan mail-server.

2.11.1 DMZ Host

Beberapa rumah router merujuk pada DMZ host. Sebuah rumah router DMZ host adalah host di jaringan internal yang memiliki semua port terbuka, kecuali yang port diteruskan sebaliknya. Dengan definisi ini bukan benar DMZ (Zona Ddemiliterisasi), karena DMZ sendiri tiidak terpisah dari host jaringan internal. Artinya, DMZ host dapat terhubung ke host pada jaringan internal, sedangkan host dalam DMZ nyata dihalangi dari berhubungan dengan jarngam internal oleh firewall yang mengizinkan ini jika sebuah host pada jaringan internal permintaan pertama sambungan ke host dalam DMZ.

2.12 NAT (*Network Address Translator*)

NAT (*Network Address Translator*) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (security)

dan kemudahan serta *fleksibilitas* dalam admnistrasi jaringan. Saat ini, protokol IP yang banyak digunakan adalah IP versi 4 (IPv4).

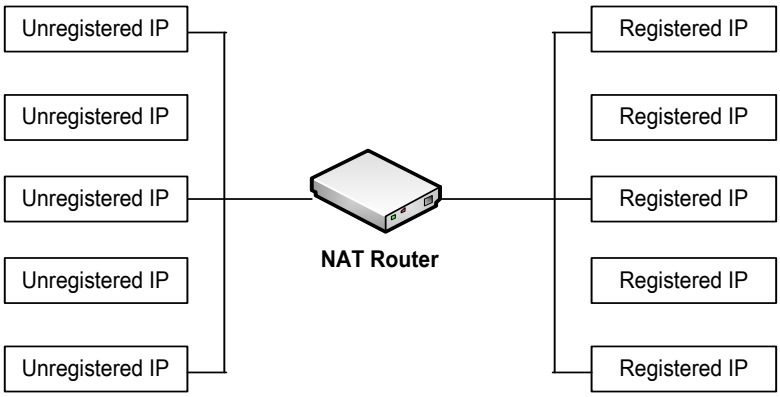
NAT secara otomatis akan memberikan proteksi seperti halnya firewall dengan hanya mengizinkan koneksi yang berasal dari dalam jaringan. Hal ini berarti tingkat keamanan suatu jaringan akan meningkat, karena kemungkinan koneksi dari luar ke dalam jaringan menjadi relatif sangat kecil. Dengan NAT, suatu jaringan yang besar dapat dipecah – pecah menjadi jaringan yang lebih kecil. Bagian – bagian kecil tersebut masing – masing memiliki satu alamat IP, sehngga dapat menambahkan atau mengurangi jumlah komputer tanpa mempengaruhi jaringan secara keseluruhan. Selain itu, pada *gateway* NAT modem terdapat server DHCP yang dapat mengkonfigurasikan komputer *client* secara otomatis.

Hal ini sangat menguntungkan bagi admin jaringan karena untuk mengubah konfigurasi jaringan, admin hanya perlu mengubah pada komputer server dan perubahan ini akan terjadi pada semua komputer *client*. Selain itu *gateway* NAT mampu membatasi akses ke internet, juga mampu mencatat semua traffic dari dan ke internet.

Proses dari *Network Address Translation* (NAT) atau dikenal dengan nama *network masquerading* atau IP-*masquerading* mengakibatkan penulisan alamat ulang sumber dan atau tujuan dari paket IP ketika melewati *router* atau *firewall*. *Network Address Translator* terdirii dari berbagai jenis yaitu *Static* NAT, *Dynamic* NAT, *Masquerading* NAT.

2.12.1 *Static* NAT

Network Address Translation (NAT) menerjemahkan sejumlah IP *Address* tidak terdaftar menjadi sejumlah IP Address yang terdaftar sehingga setiap *client* dipetakan kepada IP *Address* terdaftar yang dengan jumlah yang sama. Jenis NAT ini merupakan pemborosan IP *Address* terdaftar, karena setiap IP *Address* yang tdak terdaftar (*Un-Registered* IP) dipetakan kepada satu IP *Address* terdaftar.

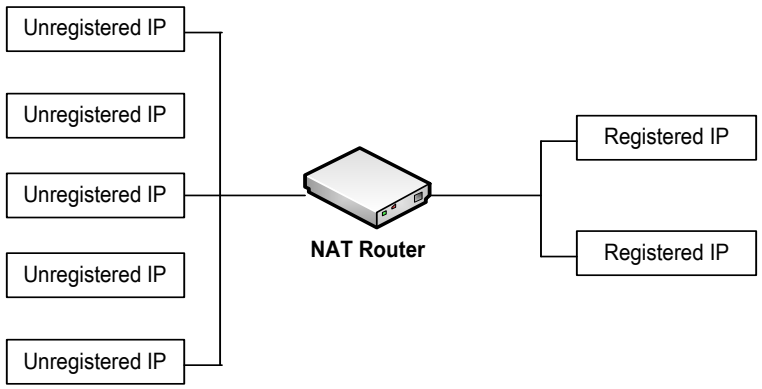


Gambar2.10 *Static* NAT

(Sumber : http://prstie.blogspot.com, diakses 10 Mei 2014)

2.12.2 *Dynamic* NAT

Dynamic Network Address Translation dimaksudkan untuk suatu keadaan dimana anda mempunyai IP Address terdaftar yang lebih sedikit dari jumlah IP *Address Un-Registered*. *Dynamic* NAT menerjemahkan setiap komputer dengan iP tak terdaftar kepada salah satu IP *Address* terdaftar untuk konek ke internet. Hal ini agak menyulitkan para penyusup untuk menembus komputer di dalam jaringan anda karena IP *Address* terdaftar yang diasosiasikan ke komputer selalu berubah secara dinamis, tidak seperti NAT statis yang dipetakan sama. Kekurangan utama dari *Dynamic NAT* ini adalah bahwa jika jumlah IP *Address* terdaftar sudah terpakai semuanya, maka untuk komputer yang berusaha konek ke internet tidak lagi bisa karena IP *Address* terdaftar sudah terpakai semuanya.

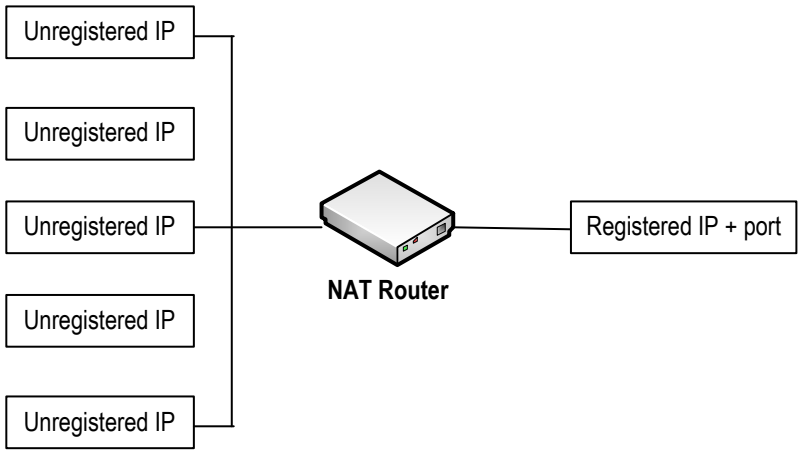


Gambar 2.11 *Dinamic* NAT

(Sumber : http://prstie.blogspot.com, diakses 10 Mei 2014)

2.12.3 *Masquerading* NAT

Masquerading NAT ini menerjemahkan semua IP *Address* tak terdaftar pada jaringan anda dipetakan kepada satu IP *Address* terdaftar. Agar banyak *client* bisa mengakses internet secara bersamaan, *router* NAT menggunakan nomor *port* untuk bisa membedakan antara paket – paket yang dihasilkan oleh atau ditujukan komputer – komputer yang berbeda. Solusi *Masquerading* ini memberikan keamanan paling bagus dari jenis – jenis NAT sebelumnya. Karena asosiasi antara *client* dengan IP tak terdaftar dengan kombinasi IP *Address* terdaftar dan nmor *port* di dalam *router* NAT hanya berlangsung sesaat terjadi satu kesempatan koneksi saja, setelah itu dilepas.



Gambar 2.12 *Masquerading* NAT

(Sumber : http://prstie.blogspot.com, diakses 10 Mei 2014)