BAB III

TEORI PENUNJANG

Pada bab tiga penulis menjelaskan tentang teori penunjang yang berisikan pengertian dan cara kerja router mikrotik serta pengertian dari DynDNS.

3.1 Router

Router adalah perangkat yang akan melewatkan paket IP dari suatu jaringan ke jaringan yang lain, menggunakan metode addressing dan protocol tertentu untuk melewatkan paket data tersebut. (http://wikipedia.org ; diakses : maret 2011)

Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router-router yang saling terhubung dalam jaringan internet turut serta dalam sebuah algoritma routing terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP dari system ke system lain. Proses routing dilakukan secara hop by hop. IP tidak mengetahui jalur keseluruhan menuju tujuan setiap paket. IP routing hanya menyediakan IP address dari router berikutnya yang menurutnya lebih dekat ke host tujuan. Fungsi : (http://iahhaku.blogspot.com ; diakses : maret 2011)

- Membaca alamat logika / ip address source & destination untuk menentukan outing dari suatu LAN ke LAN lainnya.
- Menyimpan routing table untuk menentukan rute terbaik antara LAN ke WAN.
- Perangkat di layer 3 OSI Layer.
- Bisa berupa “box” atau sebuah OS yang menjalankan sebuah daemon routing.
- Interfaces Ethernet, Serial, ISDN BRI.

Gambar 3.1 Router dan Fungsinya (Sumber : www.wikipedia.org)

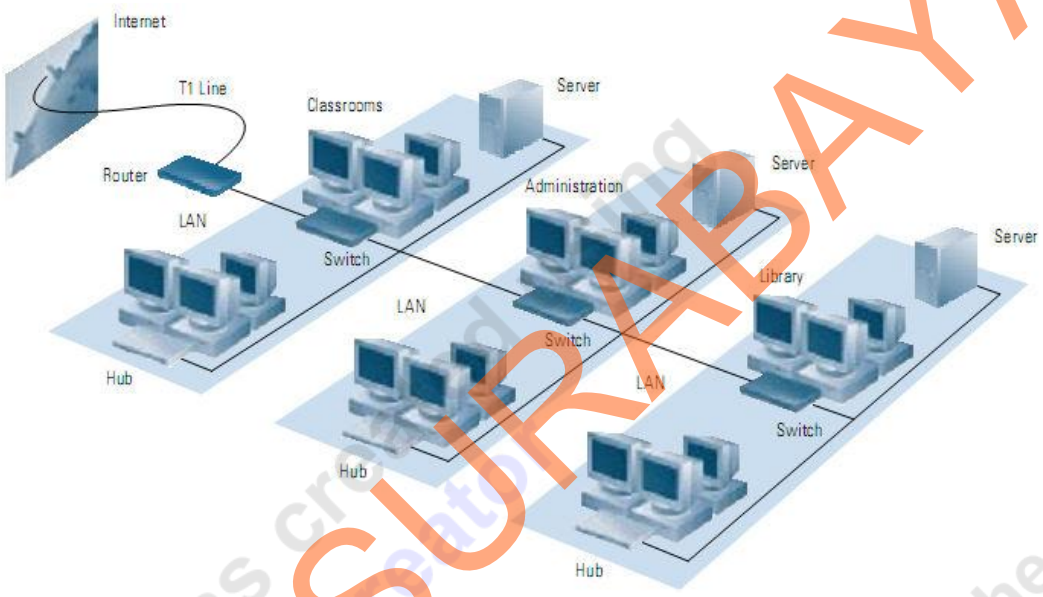
3.2 Jaringan Komputer

Jaringan komputer merupakan sekelompok komputer otonom yang saling dihubungkan satu sama lainnya, menggunakan suatu media dan protocol komunikasi tertentu, sehingga dapat saling berbagi data dan informasi. (http://iahhaku.blogspot.com ; diakses : maret 2011)

Jaringan komputer memungkinkan terjadinya komunikasi yang lebih efisien antar pemakai (mail dan teleconference). Jaringan komputer adalah sekelompok komputer otonom yang saling menggunakan protocol komunikasi melalui media komunikasi sehingga dapat berbagi data, informasi, program aplikasi dan perangkat keras seperti printer, scanner, CD-Drive maupun harddisk serta memungkinkan komunikasi secara elektronik. Sedangkan pada Aplikasi home user, memungkinkan komunikasi antar pengguna lebih efisien (chat), interaktif entertainment lebih multimedia (games, video,dan lain-lain).

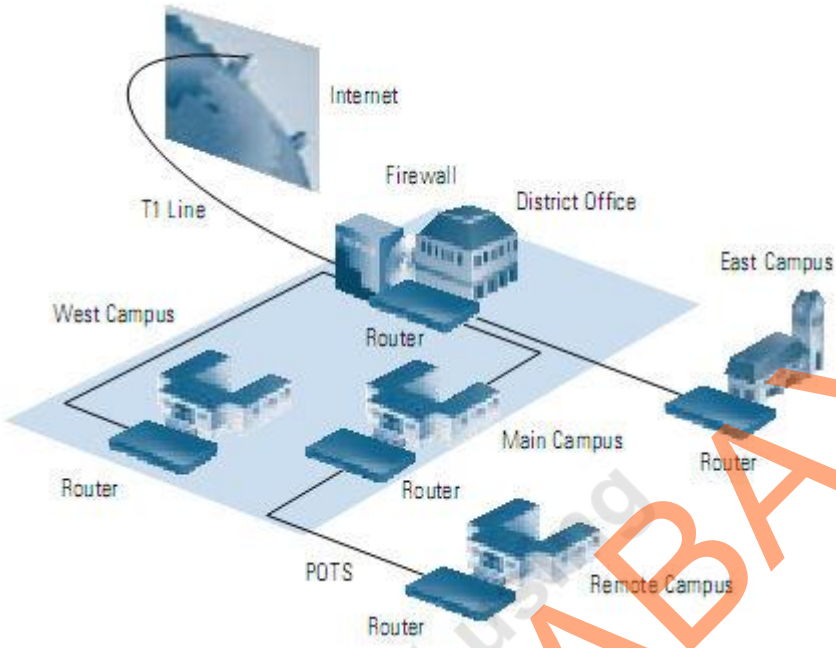
Klasifikasi Jaringan Komputer :

- LAN (Local Area Network) : Jaringan komputer yang saling terhubung ke suatu komputer server dengan menggunakan topologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 km.



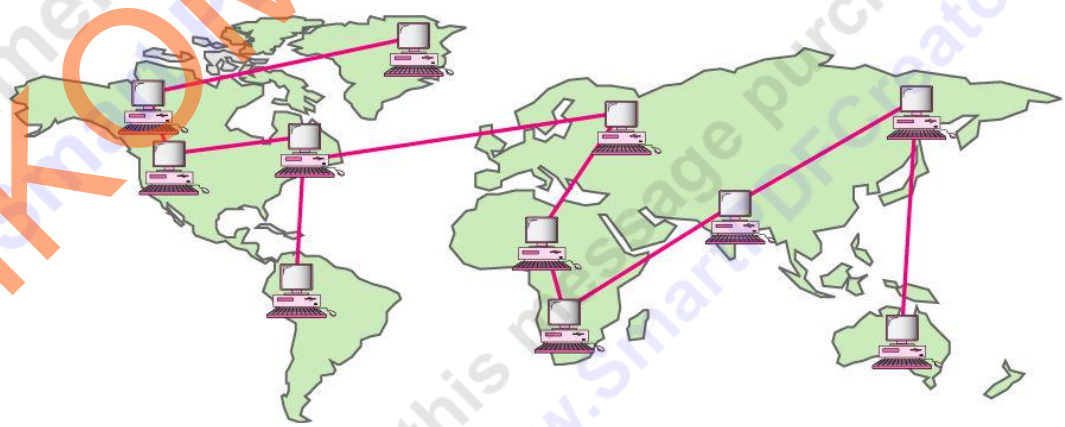
Gmabar 3.2 Local Area Network (Sumber : www.cisco.com)

- MAN (Metropolitan Area Network) : Jaringan komputer yang saling terkoneksi dalam satu kawasan kota yang jaraknya bisa lebih dari 1 km. Pilihan untuk membangun jaringan komputer antar kantor dalam suatu kota, kampus dalam satu kota.



Gambar 3.3 Metropolitan Area Network (Sumber : www.cisco.com)

- WAN (Wide Area Network) : Jaringan komputer yang menghubungkan banyak LAN ke dalam suatu jaringan terpadu, antara satu jaringan dengan jaringan lain dapat berjarak ribuan kilometer atau terpisahkan letak geografi dengan menggunakan metode komunikasi tertentu.



Gambar 3.4 Wide Area Network (Sumber : www.cisco.com)

Secara garis besar ada beberapa tahapan dalam membangun jaringan LAN, diantaranya ; (http://iahhaku.blogspot.com ; diakses : maret 2011)

- Menentukan teknologi tipe jaringannya (Ethernet, Fast Ethernet, Token Ring, FDDI)
- Memilih model perkabelan (Fiber, UTP, Coaxial)
- Menentukan bentuk topologi jaringan (Bus, Ring, dan Star)
- Menentukan teknologi Client/Server atau Peer to Peer
- Memilih Sistem Operasi Server (Windows NT, 2000, XP, atau Linux)

3.2.1 Gateway

Pintu gerbang sebagai keluar-masuknya paket data dari local network menuju outer network. Tujuannya agar client pada local network dapat berkomunikasi dengan internet. Router dapat disetting menjadi Gateway dimana ia menjadi penghubung antara jaringan local dengan jaringan luar. (http://iahhaku.blogspot.com ; diakses : maret 2011)

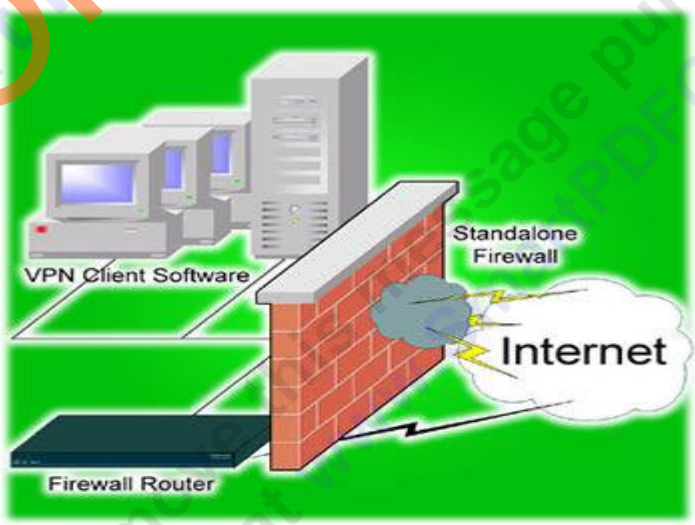
3.2.2 Proxy Server

Sebuah fasilitas untuk menghubungkan diri ke internet secara bersama-sama. Memenuhi permintaan user untuk layanan Internet (http, FTP,Telnet) dan mengirimkannya sesuai dengan kebijakan. Bertindak sebagai gateway menuju layanan. Mewakili paket data dari dalam dan dari luar. Menangani semua komunikasi internet – ekternal. Bertindak sebagai gateway antara mesin internal dan eksternal. Proxy server mengevaluasi dan mengontrol permintaan dari client, jika sesuai policy dilewatkan jika tidak di deny/drop. (http://iahhaku.blogspot.com ; diakses : maret 2011)

3.2.3 Firewall

Sistem keamanan yang menggunakan device atau sistem yang diletakkan di dua jaringan dengan fungsi utama melakukan filtering terhadap akses yang akan masuk. Berupa seperangkat hardware atau software, bisa juga berupa seperangkat aturan dan prosedur yang ditetapkan oleh organisasi.

Firewal juga dapat disebut sebagai sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggapnya aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan local dan jaringan lainnya. Firewall juga umumnya digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari hak luar. Saat ini, istilah firewall menjadi istilah generic yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. (http://cisco.com ; diakses : maret 2011)



Gambar 3.5 Mekasnisme Firewall (Sumber : www.cisco.com)

3.3 Mikrotik Router OS

MikroTik RouterOS™, merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). (http://mikrotik.com ; diakses : maret 2011)

Selain itu instalasi dapat dilakukan pada Standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

3.3.1 Sejarah MikroTik OS

MikroTik adalah sebuah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia. (http://mikrotik.com ; diakses : maret 2011) Pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John rully adalah seorang berkewarganegaraan Amerika yang berimigrasi ke Latvia. Di Latvia ia bejumpa dengan Arnis, Seorang darjana Fisika dan Mekanik sekitar tahun 1995. John dan Arnis mulai me-routing dunia pada tahun 1996 (misi MikroTik adalah merouting seluruh dunia). Mulai dengan sistem Linux dan MS-DOS yang dikombinasikan dengan teknologi Wireless-LAN (WLAN) Aeronet berkecepatan 2 Mbps di Moldova, negara tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia.

Prinsip dasar mereka bukan membuat Wireless ISP (W-ISP), tetapi membuat program router yang handal dan dapat dijalankan diseluruh dunia. Latvia hanya merupakan tempat eksperimen John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang

melayani sekitar 400 pengguna. Linux yang pertama kali digunakan adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5-15 orang staff Research and Development (R&D) MikroTik yang sekarang menguasai dunia routing di negara-negara berkembang. Menurut Arnis, selain staf di lingkungan MikroTik, mereka juga merekrut tenega-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan MikroTik secara marathon.

3.3.2 Jenis-jenis MikroTik

Terdapat beberapa jenis mikrotik yaitu : (http://mikrotik.com ; diakses : maret 2011)

1. MikroTik RouterOS yang berbentuk software yang dapat di-download di www.mikrotik.com. Dapat diinstal pada kompuetr rumahan (PC).
2. BUILT-IN Hardware MikroTik dalam bentuk perangkat keras yang khusus dikemas dalam board router yang didalamnya sudah terinstal MikroTik RouterOS.

3.3.3 Fitur-Fitur MikroTik

Terdapat beberapa fitur MikroTik yaitu : (http://mikrotik.com ; diakses : maret 2011)

1. Address List : Pengelompokan IP Address berdasarkan nama
2. Asynchronous : Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
3. Bonding : Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.

4. Bridge : Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging firewalling.
5. Data Rate Management : QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer
6. DHCP : Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.
7. Firewall dan NAT : Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8. Hotspot : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
9. IPSec : Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkirpsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5
10. ISDN : mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.
11. M3P : MikroTik Protokol Paket Packer untuk wireless links dan ethernet.
12. MNDP : MikroTik Discovery Neighbour Protokol, juga mendukung Cisco Discovery Protokol (CDP).

13. Monitoring / Accounting : Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
14. NTP : Network Time Protokol untuk server dan clients; sinkronisasi menggunakan system GPS.
15. Poin to Point Tunneling Protocol : PPTP, PPPoE dan L2TP Access Consentrator; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPoE; limit data rate.
16. Proxy : Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
17. Routing : Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
18. SDSL : Mendukung Single Line DSL; mode pemutusan jalur koneksi dan jaringan.
19. Simple Tunnel : Tunnel IPIP dan EoIP (Ethernet over IP).
20. SNMP : Simple Network Monitoring Protocol mode akses read-only.
21. Synchronous : V.35, V.24, E1/T1, X21, DS3 (T3) media ttypes; sync-PPP, Cisco HDLC; Frame Relay line protokol; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); Frame Relay jenis LMI.
22. Tool : Ping, Traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.
23. UPnP : Mendukung antarmuka Universal Plug and Play.

24. VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan ethernet dan wireless; multiple VLAN; VLAN bridging.
25. VoIP : Mendukung aplikasi voice over IP.
26. VRRP : Mendukung Virtual Router Redudant Protocol.
27. WinBox : Aplikasi mode GUI untuk meremote dan mengkonfigurasi MikroTik RouterOS.

3.4 DynDNS

3.4.1 DNS Server

Domain Name System (DNS) adalah distribute database system yang digunakan untuk pencarian nama komputer (name resolution) di jaringan yang mengunakan TCP/IP (Transmission Control Protocol/Internet Protocol). (http://cisco.com ; diakses : maret 2011)

Fungsi dari DNS adalah menerjemahkan nama komputer ke IP address (memetakan). Client DNS disebut dengan resolvers dan DNS server disebut dengan name servers. Resolvers atau client mengirimkan permintaan ke name server berupa queries. Name server akan memproses dengan cara mengecek ke local database DNS, menghubungi name server lainnya atau akan mengirimkan message failure jika ternyata permintaan dari client tidak ditemukan.

Proses tersebut disebut dengan Forward Lookup Query, yaitu permintaan dari client dengan cara memetakan nama komputer (host) ke IP address.

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 intranet dimana DNS memiliki keunggulan seperti: (http://cisco.com ; diakses : maret 2011)

1. Mudah, DNS sangat mudah karena user tidak lagi direpotkan untuk mengingat IP address sebuah komputer cukup host name (nama Komputer).
2. Konsisten, IP address sebuah komputer bisa berubah tapi host name tidak berubah.
3. Simple, user hanya menggunakan satu nama domain untuk mencari baik di Internet maupun di Intranet.

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 anda minta tersebut berapa IP address-nya. IP address ini yang digunakan untuk mengkoneksikan komputer anda dengan komputer lainnya.

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

1. Root-Level Domains

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 (“.”).

2. Top-Level Domains

Pada bagian dibawah ini adalah contoh dari top-level domains:

- com : Organisasi Komersial
- edu : Institusi pendidikan atau universitas
- org : Organisasi non-profit
- net : Networks (backbone Internet)
- gov : Organisasi pemerintah non militer
- mil : Organisasi pemerintah militer
- num : No telpon
- arpa : Reverse DNS

Top-level domains dapat berisi second-level domains dan hosts.

3. Second-Level Domains

Second-level domains dapat berisi host dan domain lain, yang disebut dengan subdomain. Untuk contoh: Domain Bujangan, bujangan.com, bujanganalways.com terdapat komputer (host) seperti server1.bujangan.com dan subdomain training.bujangan.com.

Subdomain training.bujangan.com juga terdapat computer atau sering disebut sebagai host seperti client1.training.bujangan.com.

4. Host Names

Domain name yang digunakan dengan host name akan menciptakan fully qualified domain name (FQDN) untuk setiap komputer. Sebagai contoh, jika terdapat fileserver1.detik.com, dimana fileserver1 adalah host name dan detik.com adalah domain name.

3.4.2 *Dynamic* DNS

Dynamic DNS merupakan suatu metode / protokol / jaringan pelayanan yang menyediakan kemampuan untuk perangkat jaringan, seperti router atau sistem komputer menggunakan *Internet Protocol Suite*, untuk memberitahu sebuah nama Domain Name System (DNS) server yang berubah secara real time dan konfigurasi DNS yang meliputi nama host, alamat, dan informasi lainnya. (http://wikipedia.org ; diakses : maret 2011)

Dynamic DNS adalah lapisan yang ditambahkan di atas sistem DNS standar yang memungkinkan nama domain untuk mengikuti alamat IP secara otomatis dengan memiliki catatan DNS yang akan berubah ketika ada perubahan alamat IP. Jika perubahan IP dan catatan DNS tidak diperbaharui maka setiap orang yang mencoba untuk menemukan komputer tersebut tidak akan berhasil. Pembaharuan otomatis catatan DNS bisa dilakukan dengan menggunakan software / klien hardware atau URL *bookmarked* atau dengan mengirim informasi ke server ketika ada perubahan IP. Alamat IP yang baru akan ditulis ke dalam catatan DNS dan alamat IP tersebut akan dipublikasikan secara global.

Provider *Dynamic DNS* menawarkan program perangkat lunak klien yang mengotomatisasi penemuan dan pendaftaran alamat IP publik klien. Program client dijalankan pada komputer atau perangkat dalam jaringan pribadi. Terhubung ke sistem penyedia layanan dan sistem itu akan menghubungkan alamat umum dan alamat IP dari jaringan asal dengan hostname dalam sistem nama domain. Tergantung pada penyedia, nama host adalah terdaftar dalam domain yang dimiliki oleh operator atau nama domain sendiri pelanggan. Layanan ini memunginakan adanya sejumlah mekanisme. Seringkali ada permintaan untuk layanan HTTP karena lingkungan yang terbatas.

Kebanyakan *Router System networking* sudah memiliki fitur ini dan sudah dibangun ke dalam firmware router tersebut. Salah satu router awal yang mendukung Dynamic DNS adalah UMAX UGate-3000 pada tahun 1999, yang mendukung layanan TZO.COM dinamis DNS. Contohnya adalah pengguna perumahan yang ingin mengakses komputer pribadi mereka di rumah saat bepergian. Jika komputer rumah memiliki alamat IP tetap statis, pengguna dapat terhubung langsung menggunakan alamat ini, namun banyak penyedia jaringan sering memaksa perubahan alamat IP dikonfigurasi dalam peralatan pelanggan mereka. Dengan DNS dinamis, komputer rumah dapat secara otomatis mengasosiasikan alamat IP dengan nama domain. Akibatnya pengguna remote dapat menyelesaikan nama host yang digunakan untuk masuk layanan DNS dinamis ke alamat saat ini komputer rumah dengan query DNS. Jika sebuah program remote control seperti VNC server dapat disimpan berjalan pada host di jaringan pribadi,

pengguna dapat terhubung ke jaringan rumah dengan sebuah program klien VNC.

Dalam jaringan Microsoft Windows, DNS dinamis adalah bagian integral dari Active Directory. Dalam upaya untuk mengamankan komunikasi Internet saat ini pasti melibatkan hal-hal yang dinamis melalui Internet. Karena itu dynamic DNS sering disalahgunakan untuk merancang pelanggaran keamanan. metode berbasis standar dalam protokol DNSSEC, seperti TSIG, metode untuk mengamankan update DNS sudah dikembangkan, namun tidak banyak digunakan.

3.5 IP Private

Setiap node IP membutuhkan sebuah alamat IP yang secara global unik terhadap *Internetwork* IP. Pada kasus Internet, setiap *node* di dalam sebuah jaringan yang terhubung ke Internet akan membutuhkan sebuah alamat yang unik secara global terhadap Internet. Karena perkembangan Internet yang sangat amat pesat, organisasi-organisasi yang menghubungkan *intranet* miliknya ke Internet membutuhkan sebuah alamat publik untuk setiap *node* di dalam *intranet* miliknya tersebut. Tentu saja, hal ini akan membutuhkan sebuah alamat publik yang unik secara global.

Ketika menganalisis kebutuhan pengalamatan yang dibutuhkan oleh sebuah organisasi, para desainer Internet memiliki pemikiran yaitu bagi kebanyakan organisasi, kebanyakan host di dalam intranet organisasi tersebut tidak harus terhubung secara langsung ke Internet. Host-host yang membutuhkan sekumpulan layanan Internet, seperti halnya akses terhadap web atau e-mail, biasanya mengakses layanan Internet tersebut melalui

gateway yang berjalan di atas lapisan aplikasi seperti proxy server atau e-mail server. Hasilnya, kebanyakan organisasi hanya membutuhkan alamat publik dalam jumlah sedikit saja yang nantinya digunakan oleh node-node tersebut (hanya untuk proxy, router, firewall, atau translator alamat jaringan) yang terhubung secara langsung ke Internet.

Untuk *host-host* di dalam sebuah organisasi yang tidak membutuhkan akses langsung ke Internet, alamat-alamat IP yang bukan duplikat dari alamat publik yang telah ditetapkan mutlak dibutuhkan. Untuk mengatasi masalah pengalamatan ini, para desainer Internet mereservasikan sebagian ruangan alamat IP dan menyebut bagian tersebut sebagai ruangan alamat pribadi. Sebuah alamat IP yang berada di dalam ruangan alamat pribadi tidak akan digunakan sebagai sebuah alamat publik. Alamat IP yang berada di dalam ruangan alamat pribadi dikenal juga dengan **alamat pribadi** atau *Private Address*. Karena di antara ruangan alamat publik dan ruangan alamat pribadi tidak saling melakukan *overlapping*, maka alamat pribadi tidak akan menduplikasi alamat publik, dan tidak pula sebaliknya.

Ruangan alamat pribadi yang ditentukan di dalam RFC 1918 didefinisikan di dalam tiga blok alamat berikut:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

3.6 NAT *(Network Address Translation)*

Network Address Translation atau yang lebih biasa disebut dengan NAT 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 administrasi jaringan.

Saat ini, protokol IP yang banyak digunakan adalah IP versi 4 (IPv4). Dengan panjang alamat 4 byte berarti terdapat 2 pangkat 32 = 4.294.967.296 alamat IP yang tersedia. Jumlah ini secara teoretis adalah jumlah komputer yang dapat langsung koneksi ke internet. Karena keterbatasan inilah sebagian besar ISP (Internet Service Provider) hanya akan mengalokasikan satu alamat untuk satu penggna dan alamat ini bersifat dinamik, dalam arti alamat IP yang diberikan akan berbeda setiap kali user melakukan koneksi ke internet. Hal ini akan menyulitkan untuk bisnis golongan menengah ke bawah. Di satu sisi mereka membutuhkan banyak komputer yang terkoneksi ke internet, akan tetapi di sisi lain hanya tersedia satu alamat IP yang berarti hanya ada satu komputer yang bisa terkoneksi ke internet. Hal ini bisa diatasi dengan metode NAT. Dengan NAT gateway yang dijalankan di salah satu komputer, satu alamat IP tersebut dapat dibagi ke beberapa komputer yang lain dan mereka bisa melakukan koneksi ke internet secara bersamaan.

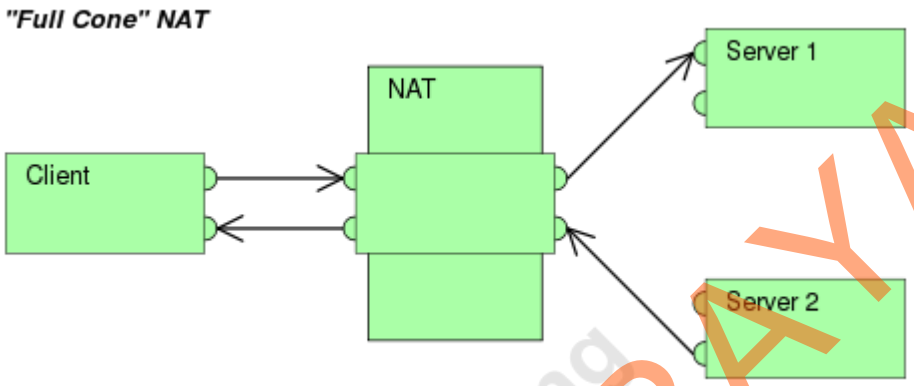
Ketika suatu komputer terkoneksi ke internet, komputer tersebut tidak saja dapat mengakses, misalnya ke server suatu situs tertentu, tetapi komputer tersebut juga sangat mungkin untuk diakses oleh komputer lain yang juga terkoneksi ke internet. Jika disalahgunakan, hal tersebut bisa sangat berbahaya. Data-data penting bisa saja dilihat atau bahkan dicuri oleh orang yang tak bertanggungjawab. 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, sehingga dapat menambahkan atau mengurangi jumlah komputer tanpa memengaruhi jaringan secara keseluruhan. Selain itu, pada gateway NAT modern terdapat server DHCP yang dapat mengkonfigurasi 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. Secara keseluruhan, dengan segala kelebihan gateway NAT tersebut, admin jaringan akan sangat terbantu dalam melakukan tugas-tugasnya.

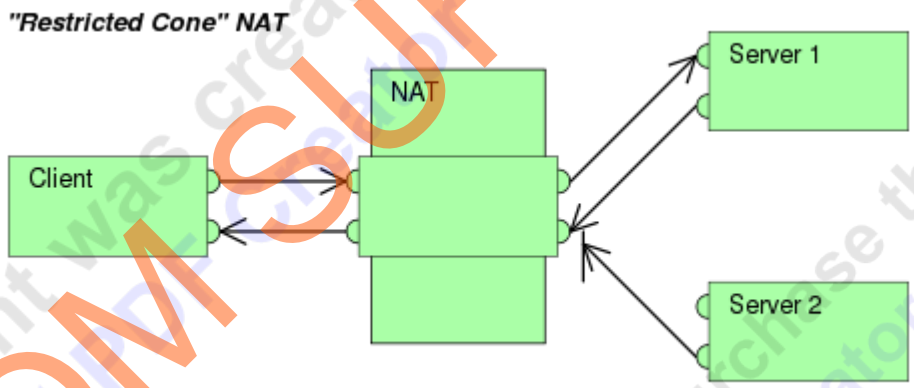
NAT dikelompokkan ke dalam beberapa jenis sebagai berikut : (http://wikipedia.org ; diakses : April 2011)

1. Full Cone NAT



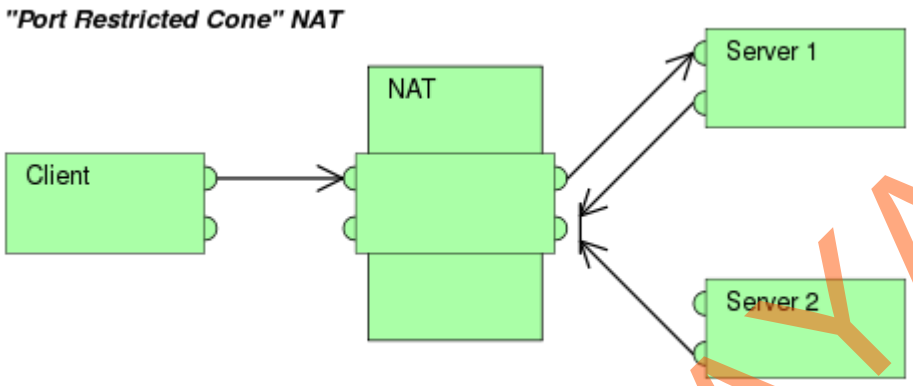
Gambar 3.6 Full Cone NAT

2. Restricted Cone NAT



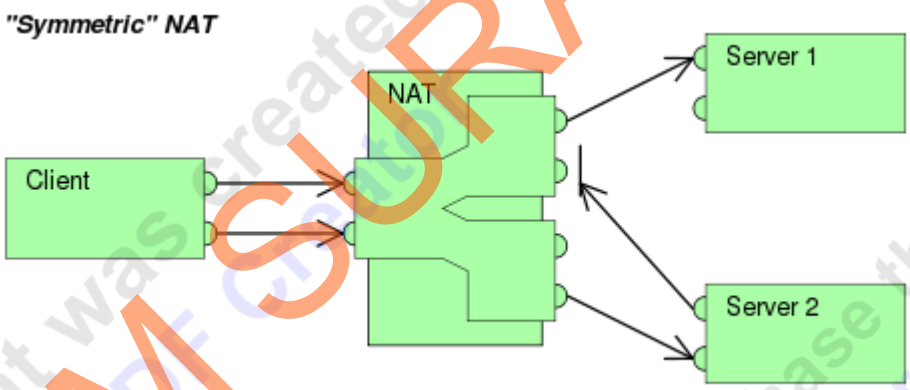
Gambar 3.7 Restricted Cone NAT

3. Port Restricted cone NAT



Gambar 3.8 Port Restricted Cone NAT

4. Symmetric NAT



Gambar 3.9 Symmetric Cone NAT

3.7 IP Camera F-Series

IP Camera F-series adalah kamera pengintai yang dapat diakses menggunakan jaringan TCP/IP *network*. Kamera ini memiliki slot untuk RJ-45 ethernet, dimana apabila terhubung ke jaringan akan mendapatkan *IP address* sendiri, yang mana kita dapat mengakses untuk melihat kamera tersebut dari komputer-komputer yang terhubung ke jaringan melalui Internet Explorer.(cukup ketikkan IP

address dari kamera tersebut pada Internet Explorer)

Selain melalui RJ-45, Kamera ini juga bisa difungsikan sebagai web camera dengan menggunakan kabel USB yang telah disediakan dalam paket. Kamera ini menggunakan sensor low-lux, yang memungkinkan kita melihat hasil kamera meskipun dalam kondisi cukup gelap. IP Camera ini memiliki built-in Microphone, yang memungkinkan kita untuk juga mendengarkan suara di sekitar kamera tersebut.

Software dari kamera tersebut memungkinkan kita untuk merekam hasil dari kamera tersebut secara real-time. Dan software-nya support sampai 16 kamera.

Gambar 3.10 Skema Penggunaan Grand IP Camera.

Spesifikasi dari *IP Camera F-series* adalah sebagai berikut :

- High Resolution Image Processor (640*480:15fps,320x240:30 fps).
- Ethernet RJ-45, 10/100 Base-T auto-sensed
- Remote view through the IE browser just typing IP address
- Low-lux Sensor provide image in the dark.
- USB 1.1 Interface: Compatible with Microsoft MSN and NetMeeting
- Support 4,9,16 Cameras (Movie Recording)