BAB III

LANDASAN TEORI

Pada bab landasan teori ini akan menjelaskan tentang teori-teori yang mendukung dalam pengerjaan tugas ini, seperti teknologi VPN, konsep dasar jaringan, n*etwok device*, dan mikrotik.

3.1 VPN (Virtual Private Network)

(Sofana.Iwan., 2010)

VPN atau *Virtual Private Network* adalah teknologi jaringan komputer yang memanfaatkan media komunikasi publik (*open connection* atau *virtual circuits*), seperti *Internet*, untuk menghubungkan beberapa jaringan lokal. Informasi yang berasal dari node-node VPN akan "dibungkus" (*tunneled*) dan kemudian mengalir melalui jaringan publik. Sehingga informasi menjadi aman dan tidak mudah dibaca oleh orang lain.

Umumnya VPN diimplementasikan oleh lembaga/perusahaan besar. Biasanya perusahaan semacam ini memiliki kantor cabang yang cukup jauh dari kantor pusat. Sehingga diperlukan solusi yang tepat untuk mengatasi keterbatasan LAN. VPN dapat menjadi pilihan yang cukup tepat. Tentu saja VPN bisa diimplementasikan oleh pengguna rumah atau oleh siapa pun yang membutuhkannya.

1. Jenis VPN

VPN telah dikembangkan menjadi beberapa jenis. Para ahli berbeda pendapat tentang pembagian jenis VPN tersebut. Ada yang membagi VPN

berdasarkan cakupan area, yaitu *intranet*, *extranet* dan *internet*. Ada yang membagi VPN berdasarkan jenis protocol yang digunakan, yaitu jenis proteksi data, dan sebagainya. Secara umum VPN dapat dikelompokkan menjadi:

1. *Remote access* VPN

Remote access VPN disebut juga *Virtual Private Dial-up Network* (VPDN). VPDN adalah jenis use-to-LAN connection. Artinya, user dapat melakukan koneksi ke *private network* dari manapun, apabila diperlukan biasanya VPDN dimanfaatkan oleh karyawan komputer laptop yang sudah dilengkapi perangkat tertentu untuk melakukan koneksi dengan jaringan LAN di kantor.

Sebelum koneksi terjadi akan dilakukan proses *dial-up* ke *network access* (NAS). Biasanya NAS disediakan oleh provider yang memberikan komputer dan aplikasi untuk men*dial-up* NAS. Secara umum VPDN hampir mirip dengan *dial-up internet connection*. Namun, secara teknis tentu saja VPN lebih canggih dan lebih *secure* dibandingkan *dial-up internet*. Koneksi biasanya hanya dilakukan sewaktu-waktu.

2. Site-site VPN

Site-site VPN diimplementasikan dengan memanfaatkan perangkat *dedicated* yang dihubungkan via internet. Site-to-site VPN digunakan untuk menghubungkan berbagai area yang sudah *fixed* atau tetap, misal kantor cabang dengan kantor pusat. Koneksi antara lokasi-lokasi tersebut secara terus-menerus (24 jam) sehari.

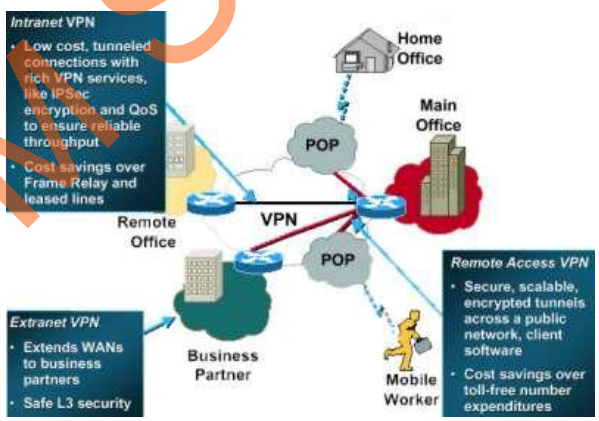
Jika ditinjau dari segi kendali atau *administrative control*. Secara umum site-to-site VPN dapat dibagi menjadi:

1. Intranet

Manakala VPN hanya digunakan untuk menghubungkan beberapa lokasi yang masih satu instansi atau satu perusahaan, seperti kantor pusat dihubungkan dengan kantor cabang. Dengan kata lain, *administrative control* berada sepenuhnya bahwa satu kendali.

2. Extranet

Manakala VPN digunakan untuk menghubungkan bebrapa instansi atau perushaan yang berbeda namun di antara mereka memiliki hubungan "dekat". Seperti perusahaan tekstil dengan perushaan angkutan barang yang digunakan oelh perushaan teksstil tersebut. Dengan kata lain, *administrative control* berada di bawah kendali beberapa instansi terkait.



Gambar 3.1 Ilustrasi Berbagai Jenis VPN

2. Security VPN

Untuk mengamankan informasi yang berasal dari berbagai jaringan internal, VPN menggunakan beberapa metode *security*, seperti:

1. Firewall

Firewall menyediakan "penghalang" antara jaringan lokal dengan internet. Pada *firewall* dapat ditentukan port-port mana saja yang boleh dibuka, paket apa saja yang boleh melalui *firewall* dan protokol apa saja yang dibolehkan. Beberapa perangkat VPN, seperti cisco 1700 router, menyediakan fasilias untuk *upgrade firewall*.

Gambar 3.2 Cisco 17500 Router

2. Enkripsi

Enkripsi merupakan metode yang umum untuk mengamankan data. Informasi akan "diacak" sedemikian rupa sehingga sukar dibaca orang lain. Secara umum ada dua buah metode *enkripsi*, yaitu:

1. *Symmetric-key encryption*

   Pada metode ini, masing-masing komputer pengirim dan penerima harus memiliki "*key*" yang sama. Informasi yang sudah di-*enkripsi* hanya dapat di-*dekripsi* menggunakan *key* tersebut.

2. *Public-key encryption*

   Pada metode ini, komputer pengirim menggunakan *public key* milik komputer penerima untuk melakukan *enkripsi*. Setelah

informasi dikirim maka proses dekripsi dapat dilakukan menggunakan *private key* komputer penerima.

Public key dapat disebarkan kepada siapa pun, namun *private key* hanya untuk pemilik sah saja.

3. IPSec

Internet Protocol Security Protocol (IPSec) menyediakan fitur *security* yang lebih baik. Seperti algoritma *enkripsi* yang lebih bagus dan *comprehensive authentication*. IPSec menggunakan dua buah mode *enkripsi*, yaitu:

1. Tunnel

   Tunnel melakukan *enkripsi* pada header dan *payload* masing-masing paket.

2. Transport

   Transport hanya melakukan *enkripsi* pada *payload* masing-masing paket.

Untuk dapat memanfaatkan IPSec, kita harus menggunakan perangkat yang mendukung. Setiap perangkat haruslah menggunakan *key* yang sama dan *firewall* setiap network harus mendukung *security policies* yang sama juga. IPSec dapat melakukan *enkripsi* data yang melalui berbagai *device* seperti:

1. Router ke router
2. *Firewall* ke router
3. PC ke router
4. PC ke server

Secara umum ada dua buah asumsi yang digunakan untuk menentukan *security* pada VPN. Yang pertama yaitu dengan mempercayai bahwa network yang digunakan aman atau dapat dipercaya. Ini yang disebut sebagai *trusted* model. Kedua adalah sebaliknya, diasumsikan network tidak aman sehingga diperlukan mekanisme *security* tertentu. Ini yang disebut *secure* model. Kedua-duanya tetap perlu menerapkan *otentikasi* user untuk mendapatkan akses jaringan VPN.

Sehubungan dengan kedua model *security* tersebut, maka telah diimplementasikan beberapa jenis protokol yang sesuai. Implementasi *trusted* model diantaranya:

1. Multi_Protocol Label Switching (MPLS)

   MPLS menggunakan *quality-of-service control* untuk mengantarkan informasi melalui *network* yang dianggap terpercaya.

2. Layer 2 Tunneling Protocol (L2TP)

   Gabungan dua buah protocol, yaitu *Cisco Layer 2 Forwarding* (L2F) dan *Microsoft Point-toPoint Tunneling Protocol* (PPTP).

Kedua jenis VPN tersebut tidak menerapkan mekanisme *cryptographic tunneling protocols*. Karena diasumsikan *network* sudah cukup aman. Sedangkan implementasi *secure* models antara lain:

1. IPSec (Internet Protocol Security)

   Sebuah standar *security* yang semula diperuntukkan bagi IPv6 (*Internet Protocol versi 6*) namun sudah dapat diimplementasikan pada IPv4 (*Internet Protocol versi 4*)

2. Transport Layer Security (SSL/TLS)

SSL/TLS banyak digunakan untuk *tunneling network traffic* berbagai aplikasi internet. VPN juga dapat memanfaatkan SSL untuk keperluan *tunneling*. SSL VPN telah diimplementasikan pada aplikasi bernama *OpenVPN*.

3. DTLS

Digunakan oleh Cisco untuk produk (*next generation VPN*) bernama *Cisco AnyConnect VPN*. DTLS dapat mengatasi masalah *tunneling* TCP yang dijumpai pada SSL/TLS.

4. Secure Socket Tunneling Protocol (SSTP)

SSTP dikembangkan oleh Microsoft dan mulai diperkenalkan di Windows Server 2008 dan Windows Vista Service Park 1. SSTP dapat melakukan *tunneling Point-to-Point Protocol* (PPP) atau *L2TP traffic* melalui SSL 3.0.

5. L2TPv3 (Layer 2 Tunneling Protocol version 3)

Merupakan versi pengembangan dari L2TP.

6. MPVPN (Multi Path Virtual Private Network)

MPVPN dikembangan oleh *Ragula System Development Company*.

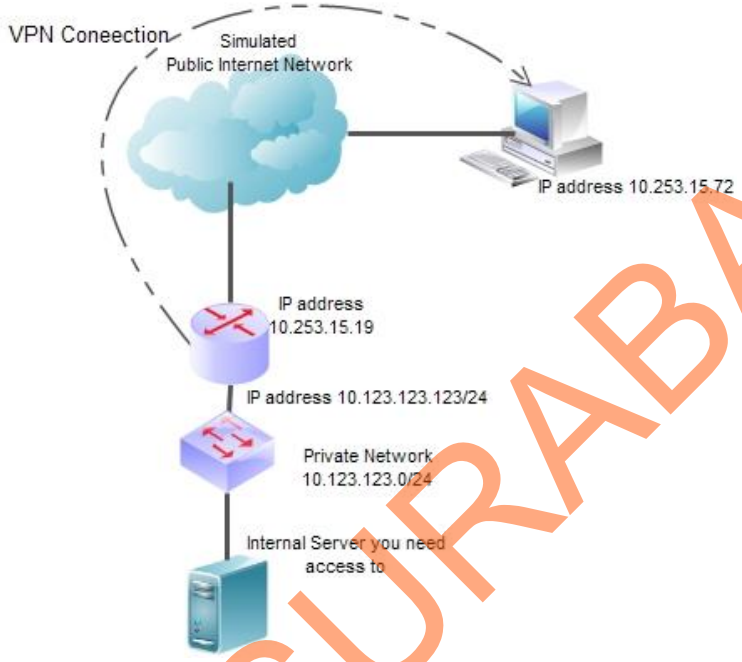
7. Cisco VPN

Jenis VPN yang digunakan oleh berbagai perangkat Cisco.

8. SSH VPN

Implementasi VPN menggunakan OpenSSH. SSH sudah sering digunakan untuk proses koneksi *remote shell secara secure*.

Server VPN menggunakan *cryptographic tunneling protocols* untuk mencegah *packet sniffing*, *identity spoffing* dan *message alteration*. Dengan cara ini, diharapkan dapat diperoleh tingkat keamanan yang cukup tinggi.



Gambar 3.3 Ilustrasi Topologi VPN

3.1.1 Cara Kerja VPN

1. VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC, server VPN ini bisa berupa komputer dengan aplikasi VPN Server atau sebuah Router, misalnya Mikrotik RB 450G.
2. Untuk memulai sebuah koneksi, komputer dengan aplikasi VPN Client mengontak Server VPN. VPN Server kemudian memverifikasi *username* dan *password* dan apabila berhasil maka VPN Server memberikan IP Address baru pada komputer *client* dan selanjutnya sebuah koneksi / *tunnel* akan terbentuk.

3. Untuk selanjutnya komputer *client* bisa digunakan untuk mengakses berbagai *resource* (komputer atau LAN) yang berada di belakang *gateway* yang diberikan dari VPN Server, melakukan *remote desktop* dan lain sebagainya.

3.1.2 Keuntungan atau manfaat VPN

Beberapa keuntungan dari teknologi VPN diantaranya adalah:

1. *Remote Access*, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet.
2. Keamanan, dengan koneksi VPN kita bisa berselancar dengan aman ketika menggunakan akses internet publik seperti *hotspot* atau *internet cafe*.
3. Menghemat biaya setup jaringan. VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil. Karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada tanpa perlu membangun jaringan pribadi.

3.1.3 Kekurangan atau kelemahan VPN

Setiap ada kelebihan pasti ada kekurangannya, beberapa kekurangan dari VPN diantaranya adalah:

1. Koneksi internet (jaringan publik) yang tidak bisa kita prediksi. Hal ini dapat kita maklumi karena pada dasarnya kita hanya *"nebeng"* koneksi pada jaringan pihak lain sehingga otomatis kita tidak mempunyai *control* terhadap jaringan tersebut.

2. Perhatian lebih terhadap keamanan. Lagi-lagi karena faktor penggunaan jaringan publik, maka diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan VPN.

3.2 Konsep Fisik Jaringan

(W.Purbo.onno,Ir.,1988)

a. Repeater : Untuk menerima sinyal suatu kabel dan memancarkan kembali.

b. Bridge : Untuk meneruskan paket dari satu segmen LAN ke segmen LAN lain.

c. Router : Untuk meneruskan paket dari satu sistem ke sistem lain yang mungkin memiliki banyak jalur diantara keduanya.

d. Switch : Untuk menghubungkan segmen LAN dengan kapasitas besar.

3.2.1 Pengertian Jaringan

Jaringan komputer adalah sejumlah *host* – bisa berupa komputer, printer ataupun *resource* lain yang dapat dibagi – pakai – yang terhubung satu sama lain dan dapat berkomunikasi.

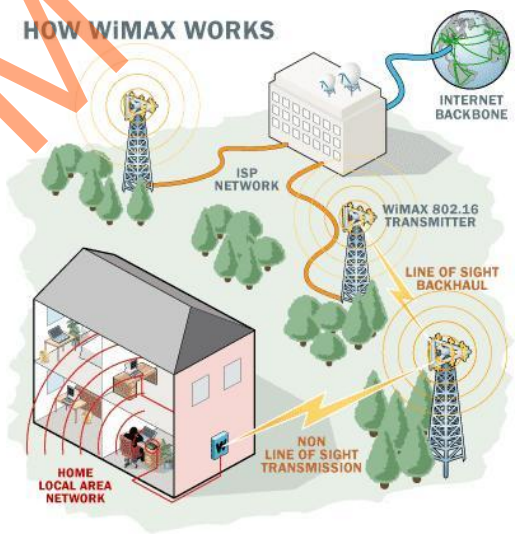
3.2.2 Metropolitan Area Network

Teknologi yang digunakan MAN mirip dengan LAN. Hanya saja areanya lebih besar dan komputer yang dihubungkan pada jaringan MAN jauh lebih banyak dibandingkan LAN. MAN merupakan jaringan komputer yang meliputi

area seukuran kota atau gabungan beberapa LAN yang dihubungkan menjadi sebuah jaringan besar.

MAN bisa saja berupa gabungan jaringan komputer beberapa sekolah atau kampus. MAN dapat diimplementasikan pada *wire* maupun *wireless network*. MAN dapat memanfaatkan jaringan TV kabel yang umumnya menggunakan kabel jenis *coaxial* atau serat optik. Pelanggan TV kabel dapat menikmasti akses internet berkecepatan tinggi. Di negara-negara maju, jaringan TV kabel telah memanfaatkan teknologi serat optik. Sehingga dapat mengangkut data berukuran gigabit dalam waktu singkat.

Dewasa ini, infrastruktur MAN mulai dipadukan dengan teknologi *wireless*. Wireless network semakin popular. Karena tidak memerlukan instalasi kabel yang cukup rumit dan mahal. Selain itu, *wireless network* dapat menjangkau area yang sulit dijangkau oleh kabel. Salah satu implementasi *wireless network* adalah WiMAX.



Gambar 3.4 Diagram MAN Menggunakan WiMAX

3.2.3 Topologi Jaringan

Topologi adalah istilah yang digunakan untuk menguraikan cara bagaimana komputer terhubung dalam suatu jaringan. Teknologi menguraikan *layout actual* dari perangkat keras jaringan sedangkan. Topologi Logika menguraikan perilaku komputer pada jaringan dari sudut pandang operator, dalam hal ini yaitu Topologi Fisik.

Istilah dari Topologi Jaringan mengacu pada organisasi spesial perangkat jaringan, pengkabelan fisik jaringan *(Physical Routing)* dan aliran paket data/informasi *(message)* dari satu titik koneksi ke titik koneksi yang lain. Titik koneksi jaringan dapat berupa perangkat seperti sistem komputer, printer atau router yang dihubungkan ke jaringan yang dapat mengirim dan menerima paket data. Secara garis besar, teknologi transmisi dengan hubungan *share*.

Jaringan komputer yang menggunakan hubungan secara *point-to-point* terdiri dari sejumlah pasangan komputer yang ada pada jaringan komputer yang apabila paket data yang dikirimkan dari sumber ke tujuan akan melewati komputer yang menjadi perantara yang berakibat rute dan jaraknya menjadi berbeda-beda dan membutuhkan beberapa jalur transmisi jika jumlah titik koneksi dalam jumlah besar. Untuk menghubungkan empat titik koneksi, enam jalur transmisi dibutuhkan tiga hubungan per titik. Dalam meningkatkan jumlah titik koneksi *point-to-point* dari jalur transmisi dapat digambarkan formula berikut:

$(n-1)! = 1 + 2 + 3 + .. + (n-1)$

Sedangkan Jaringan *broadcast* memiliki saluran komunikasi tunggal yang dipakai bersama-sama oleh semua mesin yang ada pada jaringan. Paket data-paket data berukuran kecil disebut paket data, yang dikirimkan oleh suatu mesin

akan diterima oleh mesin-mesin lainnya. *Field* alamat pada sebuah paket berisi keterangan tentang kepada siapa paket tersebut ditujukan. Saat menerima paket, mesin akan mencek *field* alamat. Bila paket tersebut ditujukan untuk dirinya, maka mesin akan memproses paket itu, bila paket ditujukan untuk mesin lainnya, mesin tersebut akan mengabaikannya.

Pada umumnya jaringan yang lebih kecil dan terlokalisasi secara geografis cenderung memakai *broadcasting*, sedangkan jaringan yang lebih besar menggunakan *point-to-point*. Jaringan komputer dalam implementasinya memiliki banyak bentuk. Namun, kesemuanya dapat digolongkan menjadi beberapa topologi, yaitu:

1. Peer-to-peer
2. Bus
3. Ring
4. Star
5. Hybrid

3.2.4 Peer-to-Peer

Topologi ini merupakan bentuk yang paling sederhana. Dalam topologi ini hanya terdapat dua *host*. Kedua *host* tersebut terhubung langsung satu dengan lainnya. Masing-masing dapat berfungsi sebagai server maupun *client*.

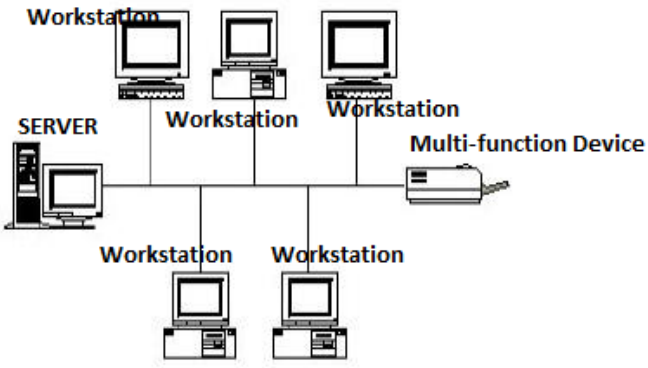
Gambar 3.5 Topologi Peer-to-Peer

3.2.5 Bus

Layout ini termasuk layout umum. Satu kabel utama menghubungkan tiap titik koneksi ke saluran tunggal komputer yang mengaksesnya ujung dengan ujung atau kedua ujungnya harus diakhiri dengan sebuah terminator. Masing-masing titik koneksi dihubungkan ke dua titik koneksi lainnya, kecuali komputer di salah satu ujung kabel, yang masing-masing hanya terhubung ke satu titik koneksi lainnya.

Topologi ini seringkali dijumpai pada sistem *client*/server, dimana salah satu komputer pada jaringan tersebut difungsikan sebagai file server, yang berarti bahwa komputer tersebut dkhususkan hanya untuk perindustrian data dan biasanya tidak digunakan untuk pemrosesan informasi. Dengan kata lain pada topologi jenis ini semua terminal terhubung ke jalur komunikasi.

Informasi yang akan dikirim akan melewati semua terminal pada jalur tersebut. Jika alamat yang tercantum dalam data atau informasi yang dikirim sesuai dengan alamat terminal yang dilewati, maka data atau informasi yang dikirim sesuai dengan alamat terminal yang dilewati, maka data atau informasi tersebut akan diterima dan diproses. Jika alamat tersebut tidak sesuai, maka informasi tersebut akan diabaikan oleh terminal yang dilewati.



Gambar 3.6 Jaringan Komputer dengan Topologi Bus

Barrel Connector dapat digunakan untuk memperluasnya dan jaringan ini hanya terdiri dari satu saluran kabel yang menggambarkan kabel BNC. Komputer yang ingin terhubung dengan ke jaringan dapat mengaitkan dirinya dengan men-tap Ethernetnya sepanjang kabel. Instalasi jaringa Bus sangat sederhana, murah dan maksimal terdiri atas 5-7 komputer. Kesulitan yang sering dialami adalah kemungkinan terjadi tabrakan data karena mekanisme jaringan relative sederhana dan jika salah satu titik koneksi putus makan akan mengganggu kinerja dan trafik seluruh jaringan.

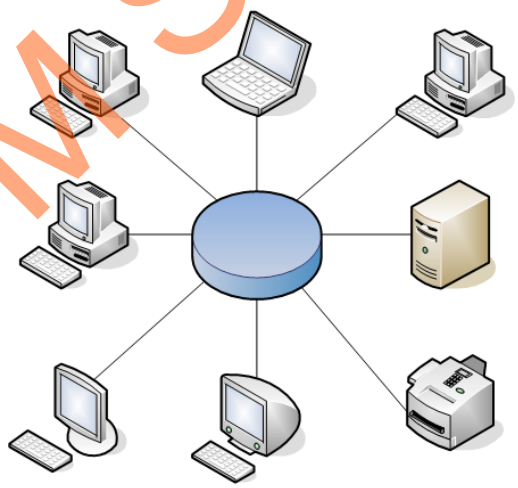
Keuntungan dan kerugian dari jaringan komputer dengan topologi Bus adalah:

1. Keuntungan, hemat kabel, layout kabel sederhana, mudah dikembangkan, tidak butuh kendali pusat dan penambahan maupun pengurangan terminal dapat dilakukan tanpa menganggu operasi yang berjalan.
2. Kerugian, deteksi dan isolasi kesalahn sangat kecil, kepadatan lalu lintas tinggi, keaman data kurang terjamin, kecepatan akan menurun bila jumlah pemakai bertambah dan diperlukan Repeater untuk jarak jauh. Topologi ini memiliki jalur khusus yang berfungsi sebagai *backbone*. Salah satu ciri fisik yang khas dari topologi bus adalah adanya terminator pada komputer paling

ujung dari jalur tersebut. Terminator berfungsi sebagai *ground* untuk menghancurkan data yang sudah tidak diperlukan lagi.

3.2.6 Ring

Topologi ring ini adalah pengembangan dari topologi bus, dimana tiap ujung bus dihubungkan sehingga membentuk sebuah siklus atau lingkaran. Topologi ini mirip dengan topologi Bus, tetapi kedua terminal yang berada di ujung saling dihubungkan, sehingga menyerupai seperti lingkaran. Setiap paket yang diperoleh diperiksa alamatnya oleh terminal yang dilewatinya. Jika bukan untuknya, paket data dilewatkan sampai menemukan alamat yang dilewatinya. Setiap terminal dalam jaringan saling tergantung, sehingga jika terjadi kerusakan pada satu terminal maka seluruh jaringan akan terganggu. Namun paket data mengalir satu arah sehingga dapat menghindari terjadinya tabrakan.



Gambar 3.7 Topologi Ring

Keuntungan dan kerugian jaringan komputer dengan topologi Ring:

1. Keuntungan, hemat kabel dan dapat melayani lalu lintas data yang padat.

2. Kerugian, peka kesalahan, pengembangan jaringan lebih kaku, kerusakan pada media pengirim/terminal dapat melumpuhkan kerja seluruh jaringan dan lambat karena pengiriman menunggu giliran *token*.

3.2.7 Star

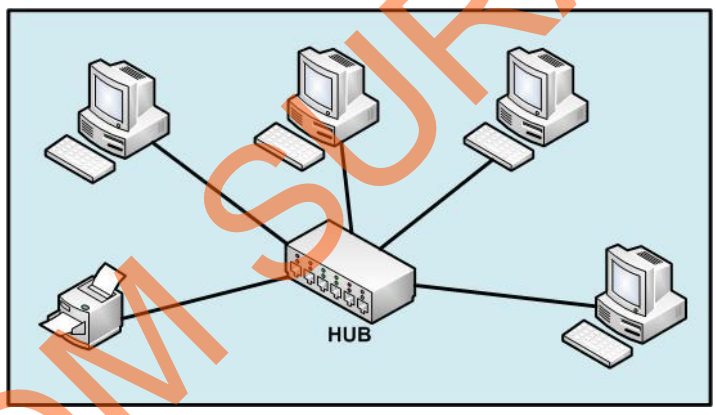
Dalam Topologi Star, sebuah terminal pusat bertindak sebagai pengatur dan pengendali semua komunikasi data yang terjadi, maksudnya semua komputer mengelilingi Hub pusat yang mengontrol komunikasi jaringan dan dapat berkomunikasi dengan Hub lain. Batas jarak komputer dengan Hub sekitar 100 meter. Setiap titik koneksi pada jaringan akan berkomunikasi melalui titik koneksi pusat atau konsentrator terlebih dahulu sebelum menuju server. Jaringan lebih fleksibel dan luas dibandingkan dengan dua topologi lainnya. Keunggulan topologi Star adalah jika salah satu titik koneksi putus maka tidak menganggu kinerka jaringan lainnya. Kabel yang biasa digunakan adlah kabel UTP *(Unshielded Twisted Pair)*.

Keuntungan dan kerugian dari jaringan komputer dengan topologi Star adalah:

1. Keuntungan, paling fleksibel karena pemasangan kabel mudah, penambahan atau pengurangan stasiun sangat mudah dan tidak mengganggu sebagian jaringan yang lain dan kontrol yang terpusat karena memudahkan dalam deteksi dan *isplasi* kesalahan/kerusakan sehingga memudahkan pengelolaan jaringan.
2. Kerugian, boros kabel, perlu penangan khusus bundel kabel dan kontrol terpusat (HUB) jadi elemen kritis.

Pada saat pemilihan topologi jaringan, faktor-faktor yang perlu menjadi pertimbangan adalah:

1. Biaya, sistem apa yang paling efisien yang dibutuhkan organisasi.
2. Kecepatan, sampai sejauh mana kecepatan yang dibutuhkan dalam sistem.
3. Lingkungan, adalah faktor-faktor lingkungan (missal: listrik) yang berpengaruh pada jenis perangkat keras yang digunakan.
4. Ukuran, sampai seberapa besar ukuran jaringan. Apakah jaringan memrlukan file server atau sejumlah server khusus.
5. Konektivitas, apakah pemakai yang lain (misalkan petugas lapangan yang menggunakan komputer perlu mengakeses jaringan dari berbagai lokasi).



Gambar 3.8 Topologi Star

3.2.8 Hybrid

Topologi ini adalah gabungan dari beberapa topologi yang disebutkan di atas.

3.6 Netwok Device

3.6.1. Switch

Switch tidak digunakan untuk membuat internetwork tapi digunakan untuk memaksimalkan jaringan LAN. Tugas utama dari switch adalah membuat LAN bekerja dengan lebih baik dengan mengoptimalkan unjuk kerja *(performance)*, menyediakan lebih banyak bandwidth untuk penggunaan LAN. Switch tidak seperti router, switch tidak meneruskan paket ke jaringan lain. Switch hanya menghubung-hubungkan frame dari satu port ke port yang lainnya di jaringan mana dia berada.

Secara default, switch memisahkan *collision* domain. Istilah collision domain adalah istilah di dalam Ethernet yang menggambarkan sebuah kondisi network dimana sebuah alat mengirimkan paket pada sebuah segment network, kemudian memaksa semua alat yang lain di segment tersebut untuk memperhatikan paketnya. Pada saat yang bersamaan, alat yang berbeda mencoba mengirimkan paket yang lain, yang mengakibatkan terjadinya *collision*. Paket yang dikirim menjadi rusak akibatnya semua alat harus melakukan pengiriman ulang paket, sehingga seperti ini menjadi tidak efisien.

3.6.2 Cara Kerja Switch

Switch dapat dikatakan sebagai *multi-port brigde* karena mempunyai *collision* domain dan *broadcast* domain tersendiri, dapat mengatur lalu lintas paket yang melalui switch jaringan. Cara menghubungkan komputer ke switch sangat mirip dengan cara menghubungkan komputer atau router ke hub. Switch

dapat digunakan langsung untuk menggantikan hub yang sudah terpasang pada jaringan.

3.6.3 Hub

Hub biasanya titik koneksi pertama antara sebuah titik koneksi jaringan dan sebuah LAN. Variasi hub sangat luas dalam fungsi dan kapabilitasnya. Hub yang paling sederhana tidak lebih dari koneksi pemasangan terpusat pada titik tunggal dan biasanya dinamakan *Wiring Concentrator*.

Jaringan hub sesuai dengan perkembangan teknik mutakhir lebih tidak dapat bekerja sama dengan fungsi routing, bridges dan switching. Hubs untuk token ring LAN lebih *sophisticated* dari hub untuk tipe LAN karena mereka harus *mengerate* sebuah *token* ketika jaringan dimulai atau jika *token* asli hilang dan sekitar jalur transmisi ulang terputus atau gagal terhubung. Jalur transmisi yang dihubungkan ke sebuah NIU atau jaringan hub dengan standar konektor. Konektor RJ-45 sperti konektor telepon RJ-11 kecuali lebih besar dan menghubungkan 8 kabel, ada beberapa standar untuk konektor *fiber optic* termasuk ST,SC,LT and MT-RJ. Standar MT-RJ telah mendukung peralatan *vendor* termasuk Cisco dan 3com.

3.6.4 Router

Router sering digunakan untuk menghubungkan beberapa *network*. Baik *network* yang sama maupun 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*.

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 yang satu *network* ataukah berbeda *network*. Jika paket-paket ditujukan untuk *host* pada *network* lain maka *router* akan menghalangi paket-paket keluar, sehingga paket-paket tersebut tidak "membanjiri" network yang lain.

Pada diagram atau bagan jaringan, sebuah *router* seringkali dinyatakan dengan symbol khusus. Berikut disajikan symbol yang digunakan untuk menggambarkan *router*.

Gambar 3.9 Gambar Router

3.6.5 Server

Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Server didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan atau *network operating system*. Server jug amnejalankan perangkat lunak administratif yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat penectak (printer) dan memberikan akses kepada *workstation* anggota jaringan.

Umumnya, di atas sistem operasi server terdapat aplikasi-aplikasi yang menggunakan arsitektur *client*/server. Contoh dari aplikasi ini adalah DHCP Server, Mail Server, HTTP Server, FTP Server, DNS Server dan lain sebagainya. Setiap sistem operasi server umumnya membundle layanan-layanan tersebut atau layanan tersebut juga dapat diperoleh dari pihak ketiga. Setiap layanan-layanan tersebut akan merespon terhadap *request* dari klien. Sebagai contoh, *client* DHCP akan memberikan *request* kepada server yang menjalankan server DHCP, ketika sebuah *client* membutuhkan alamat IP, klien akan memberikan perintah/*request* kepada server, dengan bahasa yng dipahami oleh server DHCP, yaitu *protocol* DHCP itu sendiri.

Contoh sistem operasi server adalah Windows NT 3.51, dan dilanjutkan dengan Windows NT 4.0. Saat ini sistem yang cukup popular adalah Windows 200 Server dan Windows Server 2003, kemudian Sun Solaris, Unix dan GNU/Linux. Server biasanya terhubung dengan *client* dengan kabel UTP dan sebuah *Network Card*. Kartu jaringan ini biasanya berupa kartu PCI atau ISA. Fungsi server sangat banyak, misalnya untuk situs internet, ilmu pengetahuan atau sekedar penyimpanan data. Namun yang paling umum adalah untuk mengkoneksikan komputer *client* ke *Internet.*

3.6.6 Jaringan Ethernet

Ethernet adalah sebuah metode akses media jaringan dimana semua *host* di jaringan tersebut berbagi *bandwidth* yang sama dari sebuah *link*. Ethernet menjadi popular karena ia mudah sekali disesuaikan dengan kebutuhan *(scalable).* Artinya cukup mudah untuk mengintegrasikan teknologi baru seperti FastEthernet

dan GigabitEthernet, ke dalam infrastruktur network yang ada. Ethernet juga mudah untuk diimplementasikan dari awal dan cara pemecahan masalahnya juga mudah. Ethernet menggunakan spesifikasi layer *physical* dan dara link.

Jaringan Ethernet menggunakan apa yang dinamakan *carrier sense multiple access with coliision detection (CSMA/CD),* yaitu sebuah protokol yang membantu peralatan jaringan untuk berbagi bandwidth secara merata tanpa mengalami kejadian dimana dua peralatan mengirimkan data pada saat yang bersamaan. CSMA/CD diciptakan untuk mengatasi masalah *collision* yang terjadi ketika paket-paket dikirimkan secara serentak dari titik jaringan *(node)* yang berbeda.

3.6.7 IP Address

Alamat IP *(Internet Protocol Address atau sering disingkat IP)* adalah deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer *host* dalam jaringan *Internet*. Panjang dari angka ini adalah 32-bit (untuk IPv4 atau IP versi 4), dan 128-bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan *Internet* berbasis TCP/IP.

Sistem pengalamatan IP ini terbagi menjadi dua, yakni:

1. IP versi 4 (IPv4)
2. IP versi 6 (IPv6)

3.6.8 Perbandingan Alamat IPv6 dan IPv4

Tabel perbandingan menjelaskan karakteristik antara alamat IP versi 4 dan alamat IP versi 6.

Kriteria	Alamat IP versi 4	Alamat IP versi 6
Panjang alamat	32 bit	128 bit
Jumlah total host (teoritis)	2^{32}=±4 miliar host	2^{128}
Menggunakan kelas alamat	Ya, kelas A, B, C, D, dan E. Belakangan tidak digunakan lagi, mengingat telah tidak relevan dengan perkembangan jaringan Internet yang pesat.	Tidak
Alamat multicast	Kelas D, yaitu **224.0.0.0/4**	Alamat *multicast IPv6*, yaitu **FF00:/8**
Alamat *broadcast*	Ada	Tidak ada
Alamat yang belum ditentukan	**0.0.0.0**	**::**
Alamat *loopback*	**127.0.0.1**	**::1**
Alamat IP publik	Alamat IP publik IPv4, yang ditetapkan oleh otoritas Internet (IANA)	Alamat IPv6 *unicast global*
Alamat IP pribadi	Alamat IP pribadi IPv4, yang ditetapkan oleh otoritas Internet	Alamat IPv6 *unicast site-local* (FEC0::/48)
Konfigurasi alamat otomatis	Ya (APIPA)	Alamat IPv6 *unicast link-local* (FE80::/64)
Representasi tekstual	*Dotted decimal format notation*	*Colon hexadecimal format notation*
Fungsi Prefiks	*Subnet mask* atau panjang prefiks	Panjang prefiks
Resolusi alamat DNS	*A Resource Record (Single A)*	*AAAA Resource Record (Quad A)*

Tabel 3.2 Perbandingan Alamat IPv4 dan IPv6

3.6.9 IP Publik

IP address yang digunakan untuk lingkup internet, host yang menggunakan IP publik dapat diakses oleh seluruh user yang tergabung di internet baik secara langsung maupun tidak langsung (melalui proxy/NAT).

IP Publik memiliki pengertian sebagai berikut:

a. IP Publik bersifat *worldwide*, bisa digunakan untuk mengakses internet namun penggunaan atau konfigurasinya tidak bebas (ada yang mengatur).

b. IP Addressing juga dikelompokkan berdasarkan negara, Indonesia umumnya dimulai dengan kepala 202 & 203.

c. Alamat IP publik ditugaskan untuk komputer oleh *Internet Service Provider* secara langsung setelah komputer terhubung ke *gateway Internet.*

d. Sebuah alamat IP *public static* tidak dapat berubah dan digunakan terutama untuk *hosting* halaman Web atau layanan di *Internet*.

3.6.10 IP Privat

IP address yang digunakan untuk lingkup intranet, host yang menggunakan IP privat hanya bisa diakses di lingkup intranet saja.

IP Privat memiliki pengertian sebagai berikut:

a. IP Privat hanya bersifat lokal & tidak bisa digunakan untuk mengakses *Internet* & penggunaannya bebas.

b. Perangkat dengan alamat IP privat tidak dapat terhubung langsung ke *Internet*. Demikian juga, komputer di luar jaringan lokal tidak dapat terhubung langsung ke perangkat dengan IP pribadi. Hal ini dimungkinkan untuk menghubungkan dua jaringan pribadi dengan bantuan router atau perangkat serupa yang mendukung *Network Address Translation*.

Tabel IP Private

Kelas	IP Address	Total Addresses
A	10.0.0.0 – 10.255.255.255	16,777,216
B	172.16.0.0 – 172.31.255.255	1,048,576
C	192.168.0.0 – 192.168.255.255	65,536

Tabel 3.3 Tabel IP Privat

3.6.11 MAC Address

Jika penggunaan titik koneksi mencoba untuk mengirimkan melewati medium yang sama pada waktu yang sama, paket data-paket data yang dikirim akan bercampur, yang bisa menghasilkan *noise* atau intervensi, yang dinakaman juga sebuah *collision*. Metode-metode untuk menghadapi kegagalan *collision* di dalam dua katagorinya yang mengijinkan *collision* tetapi mendeteksi dan *merecover* dari mereka sendiri, seperti CSMA/CD, dan yang menghadiri *collision* secara bersamaan, seperti *token passing*. Titik koneksi mengikuti sebuah protokol *Media Access Control (MAC)* untuk menentukan kapan mereka dapat mengakses medium transmisi yang *dishare*.

CSMA/CD merupakan teknik *medium access control (MAC)* yang paling banyak digunakan pada topologi bus dan star. Dewasa ini, dimana CSMA/CD dan beberapa teknik pendahulunya dapat dikategorikan sebagai teknik *random access*. *Random access* disini dalam arti bahwa: tidak terdapat prediksi atau rencana *(schedule)* bahwa suatu station akan melakukan transmit data, dengan kata lain *transmisi* data dari suatu *station* dilakukan secara acak (tidak terduga).

Versi paling awal dari teknik, disebut sebagai ALOHA, dikembangkan untuk jaringan paket radio. Yang merupakan teknik yang dapat dipakai juga pada setiap media transmisi yang dipakai bersama. ALOHA, atau *pure* ALOHA, sebagaimana sering disebut, merupakan teknik yang benar-benar bebas *(a true free all).*

ALOHA dibuat semudah mungkin, sehingga banyak kelemahan yang ditimbulkan sebagai akibatnya. Karena jumlah tubrukan meningkat tajam seiring

meningkatnya *traffic*, maka utilisasi maksimum dari sebuah *channel* hanya sekitar 18 persen, sehingga untuk meningkatkan efisiensi, dikembangkanlah *slotted* ALOHA. Pada teknik ini, waktu di dalam *channel* di organisasikan dalam slot-slot yang seragam, dimana panjang slot sama dengan waktu *transmisi frame*. Beberapa *central clock* diperlukan untuk melakukan sinkronisasi semua station. Dengan cara ini, transmisi data diijinkan jika dilakukan pada batas-batas slot. Hal ini meningkatkan utilisasi channel menjadi sekitar 37 peersen, yang kemudian melalui observasi lebih lanjut adalah dengan dikembangkannya teknik *carrier sense multiple access (CSMA).* Dengan CSMA, sebuah station yang ingin melakukan transmisi data, memeriksa media transmisi untuk menentukan apakah sedang terjadi suatu transmisi data lain *(carrier sense).*

Versi orisinil *baseband* dari teknik ini pertama kali dirancang dan dipatenkan oleh Xerox sebagai bagian dari Ethernet LAN yang dikembangkannya. Sedangkan versi broadbandnya dirancang dan dipatenkan oleh MITRE sebagai bagian dari MITREnet LAN yang dikembangkannya. Semua pengembangan ini menjadi dasar bagi standar IEEE 802.3 untuk CSMA/CD. Sebelum melihat lebih detil mengenai CSMA/CD ada baiknya kita melihat terlebih dahulu beberapa teknik sebelumnya sebagai dasar pengembangan CSMA/CD, dimana strategi dasar adalah tidak untuk menghindari collision, tetapi untuk mendeteksi dan merecover dari mereka. Detil-detil dari ptotokol seperti berikut ini:

1. Sebuah titik koneksi yang akan mendengarkan transmisi *(Carrier Sense)* sampai tidak ada *traffic* yang dideteksi.
2. Titik koneksi lalu mentransmisikan paket data.

Titik koneksi mendengarkan selama dan secara langsung sesudah transmisi. Jika tinggi level signal tidak normal terdengar (sebuah *collision* terdeteksi), maka titik koneksi menghentikan transmisi.

4. Jika sebuah *collision* terdeteksi titik koneksi menunggu untuk interval waktu secara acak dan mentransmisikan ulang paket data.

Protocol Token Passing MAC biasanya digunakan di dalam topologi jaringan Ring. Sebuah control paket data dinamakan sebuah token yang dilewati dari titik koneksi ke titik koneksi dan hanya titik koneksi yang "mempunyai" token diperbolehkan untuk mentransmisikan paket-paket data. Token ini melewati dari satu titik koneksi ke titik koneksi di dalam jaringan. Sebuah titik koneksi harus mentransmisikan token ke lain titik koneksi setelah waktu interval atau sesegera setelah paket tidak ada data untuk ditransmisikan.

Keuntungan utama dari CSMA/CD adalah kesederhanaan. Tidak ada Token yang dilewati antara titik koneksi dan tidak ada pengurutan keturutan dari titik koneksi di dalam jaringan. Titik koneksi bisa ditambahkan atau dihapus tanpa mengupdate dari *token passing*. Hardware dan Software yang diimplementasikan protokol adalah lebih sederhana, cepat dan tidak mahal dari pada hardware dan software yang diimplementasikan protokol yang lebih komplek.

Kekurangan utama dari CSMA/CD adalah tidak potensi untuk digunakan pada kapasitas transfer data. Kapasitas transmisi jairngan terbuang setiap waktu pada saaat *collision* muncul. Seperti pada saat lalu lintas jaringan meningkat, *collision* menjadi lebih sering. Pada saat tingkat lalu lintas tinggi, keluaran dari network menurun karena *collision* melampaui dan paket data transmisi ulang.

Token Passing menghindari ketidakefisienan secara potensial dari CSMA/CD karena tidak ada kapasitas transmisi yang terbuang dalam *collision* dan transmisi ualng. Kecil tetapi berarti dari kapasitas network yang digunakan untuk mentransmisikan token diantara titik koneksi. Walaupun ini memungkinkan untuk sebuah token jaringan ring untuk mencapai kecepatan data transfer yang efektif sama dengan transfer data mentah.

Keuntungan lainnya dari token passing meliputi kegunaan untuk meningkatkan *performance* jaringan dan kegunaan yang lebih dari rata-rata untuk menunjang tipe tertentu dari aplikasi jaringan. Kemampuan jaringan lebih lama dari yang lain. Semakin lama token dapat menahan bisa memberikan titik koneksi yang dibutuhkan untuk mentransmisikan data kapasitas yang besar, seperti file dan webserver. Karena setiap titik koneksi mempunyai token dengan waktu menahan maksimum. Maksimum waktu yang sebuah titik koneksi harus menunggu antara kesempatan mentransmisikan paket data adalah total dari maksimum waktu dari semua titik koneksi bisa menahan *token*. Perkiraan waktu menunggu maksimum adalah penting dibanyak apliksi seperti video *conference* dan jaringan telepon.

Kekurangan dari *token passing* adalah kompleksitas. Ini lebih tidak terpengaruh menuju kegagalan dan membutuhkan prosedur khusus ketika jaringan pertama kali dimulai. Kepemilikan dari token orisinil. Lebih jauh, setiap titik koneksi harus tahu titik koneksi berikutnya di dalam urutan *token passing*. Kegagalan dari sebuah titik koneksi membutuhkan titik koneksi sebelumnya untuk melewatkan titik koneksi yang gagal.

Beberapa utilitas jaringan dapat menampilkan MAC Address, yakni sebagai berikut:

1. IPCONFIG (dalam Windows NT, Windows 2000, Windows XP dan Windows Server 2003)
2. WINIPCFG (dalam Windows 95, Windows 98, dan Windows Millenium Edition).
3. /sbin/ifconfig (dalam keluarga sistem operasi UNIX)

3.7 Mikrotik

3.7.1 Sejarah Mikrotik

Cisco tentunya bukan nama yang asing lagi dalam dunia router yaitu perangkat yang berfungsi untuk mengarahkan alamat di internet. Namun, selain Cisco, terdapat nama lain yang dikenal sebagai salah satu solusi murah untuk membangun sebuah router, yaitu MikroTik RouterOS^{TM}.

MikroTik RouterOS^{TM} adalah sistem operasi yang dirancang khusus untuk network router. Dengan sistem operasi ini, Anda daoat membuat router dari komputer rumahan (PC).

MikroTik adalah perusahaan kecil yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah seorang Amerika yang berimigrasi ke Latvia. Di Latvia ia berjumpa dengan Arnis, seorang sarjana Fisika dan Mekanik sekitar 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 Molcova, tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia.

Prinsip dasar mereka bukan membuat Wireless ISP (WISP, tetapi membuat program router yang andal 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 ratusa pelanggannya. Linux yang pertama kali mereka gunakan adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5-15 orang staf R&D MikroTik yang sekarang menguasai dunia routing di negara-negara berkembang. Menurut Arnis, selain staf di lingkungan MikroTik, mereka merekrut pula tenaga-tenaga lepas dan pihak ketiga yang dengan inisiatif mengembangkan MikroTik secara marathon.

Untuk negara berkembang solusi MikroTik sangat membantu ISP atau perusahaan-perusahaan kecil yang ingin bergabung dengan Internet. Walaupun sudah banyak tersedia perangkat router mini sejenis NAT, MikroTik merupakan solusi terbaik dalam beberapa kondisi penggunaan komputer dan perangkat lunak.

3.7.2 Jenis-jenis MikroTik

1. MikroTik RouterOS^{TM}

Adalah versi MikroTik dalam bentuk perangkat lunak yang dapat diinstal pada computer rumahan (PC) melalui CD. Anda dapat mengunduh file image MikroTik RouterOS dari website resmi MikroTik, *www.mikrotik.com* yang hanya dapat digunakan dalam waktu 24 jam saja. Untuk menggunakannya secara *full*

time, Anda harus membeli lisensi *key* dengan catatan satu lisensi key hanya untuk satu harddisk.

2. Built in hardware MikroTik

Merupaka MikroTik dalam bentuk perangkat keras yang khusus dikemas dalam board router yang didalamnya sudah terinstal MikroTik RouterOS. Untuk versi ini, lisensi sudah termasuk dalam harga router board MikroTik.

3.7.3 Fitur-fitur MikroTik

1. Address list

   Pengelompokan IP address berdasarkan nama.

2. Asynchronous

   Mendukung serial PPP dial-in/dial out, dengan otentiksi 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 yang cepat.

4. Bridge

   Mendukung fungsi bridge spanning tree, multiple bridge interface, bridge 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 da MSS.

8. Hotspot

   Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL, HTTPS.

9. IPSec

   Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellman groups 1,2,5; MD5 dan algoritma SHA1 hashing; algortima enkripsi 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, x75bui line protokol

11. M3P

    MikroTik Protocol Packet Packer untuk wireless links dan Ethernet.

12. MNDP

    MikroTik Discovery Neighbor Protocol, juga mendukung Cisco Discovery Protocol (CDP).

13. Monitoring/Accounting

    Laporan traffic IP, log, statistic graphs yang dapat diaskses melalui HTTP.

14. NTP

    Network Time Protocol untuk server dan *client*; sinkronisasi menggunakan system GPS.

15. Point to Point Tunneling Protocol

    PPTP, PPPoE dan L2TP Access Concentrator; 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 SOKCS; mendukung *parent proxy*; static DNS.

17. Routing

    Routing statik dan dinamik; RIPv1/v2, OSPFv2, BGPv4.

18.. SDSL

    Mendukung Single Line DSL; mode pemutusan jalur koneksi dan jaringan.

19. Simple Tunnels

    Tunnel IPIP dan EoIP (Ethernet over IP).

20. SNMP

    Mode akses read-only.

21. Synchronous

    V..335, V.24, E1/T1, X21, DS3 (T3) media types; sync-PPP, Cisco HDLC; Frame Relay line protocol; 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 aantarmuka universal Plug and Play.

24. VLAN

    Mendukung Virtual LAN IEEE802.1q untuk jaringan Ethernet dan wireless; multiple VLAN; VLAN bridging.

25. VOIP

    Mendukung aplikasi voice over IP.

26. VRRP

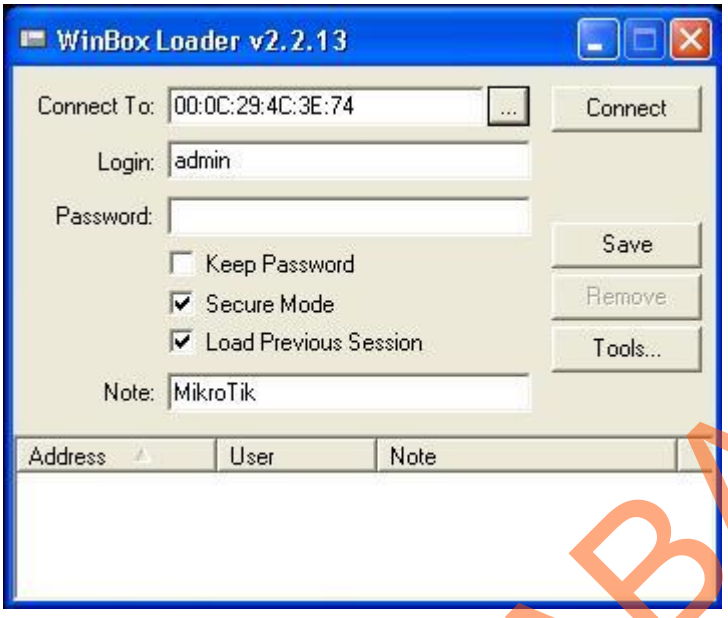
    Mendukung Virtual Router Redudant Protocol.

27. Winbox

    Aplikasi mode GUI untuk meremote menkonfigurasi MikroTik RouterOS^{TM}.

3.7.4 Remote menggunakan Winbox

WinBox merupakan aplikasi yang mengubah ‘hitam putihnya’ MikroTik menjadi mode GUI yang *user friendly* dibanding dengan router lainnya yang masih menggunakan console mode.



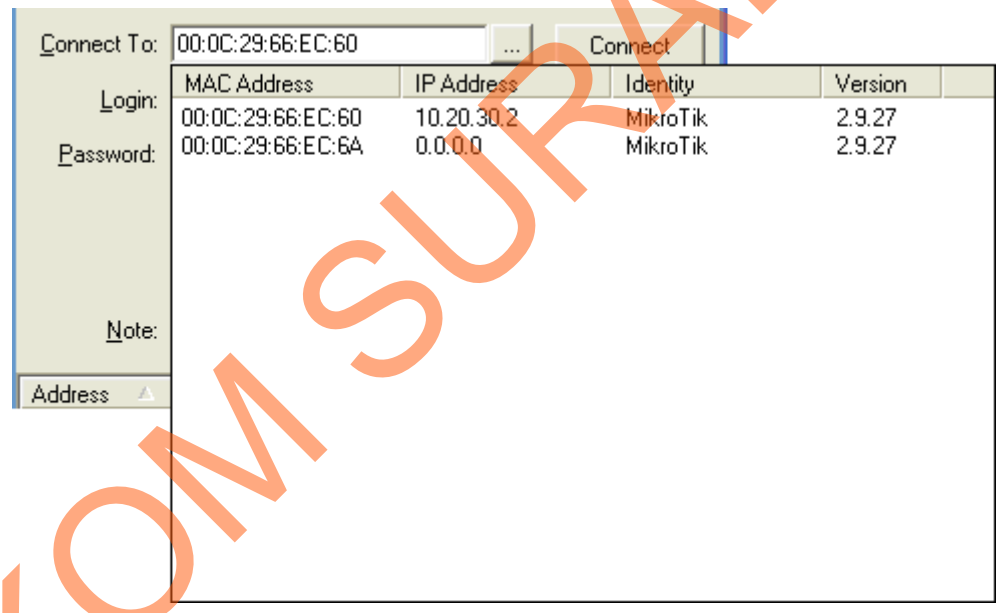
Gambar 3.10 Winbox Login

Keterangan:

1. Connect To : Alamat IP komputer yang akan di-remote.
2. Login : Nama user yang akan login MikroTik.
3. Password : Password user
4. Note : Keterangan tambahan, missal nama dari MikroTik yang di-remote.
5. Save : Untuk menyimpan alamat MikroTik beserta nama user dan password-nya. Dengan demikian Anda tidak perlu menulis kembali alamat komputer, user, dan password setiap kali akan login.
6. Tool :
    1) Remove All Addresses, digunakan untuk meghapus semua alamat, user dan keterangan yang terdapat pada daftar alamat.
    2) Clear Chace, berfungsi membersihkan cache yang tersimpan.
    3) Export Addresses digunakan untuk mengekspor semua data yang terdapat pada daftar alamat (backup data).

4) Import Addresses digunakan untuk mengimpor data dari file hasil backup data, yang nantinya akan ditempatkan pada daftar alamat.

Anda dapat pula me-remote MikroTik yang belum mempunyai IP address dengan cara menekan tombol 'tiga titik' [...] di sebelah kiri tombol [Connect]. Setelah tombol [...] ditekan, akan muncul menu *pop-up* yang menampilkan daftar alamat MAC dari Ethernet komputer yang akan di-remote. Cara ini dipakai untuk me-remote MikroTik via MAC address. Klik ganda pada alamat MAC tersebut lalu tekan tombol [Connect].

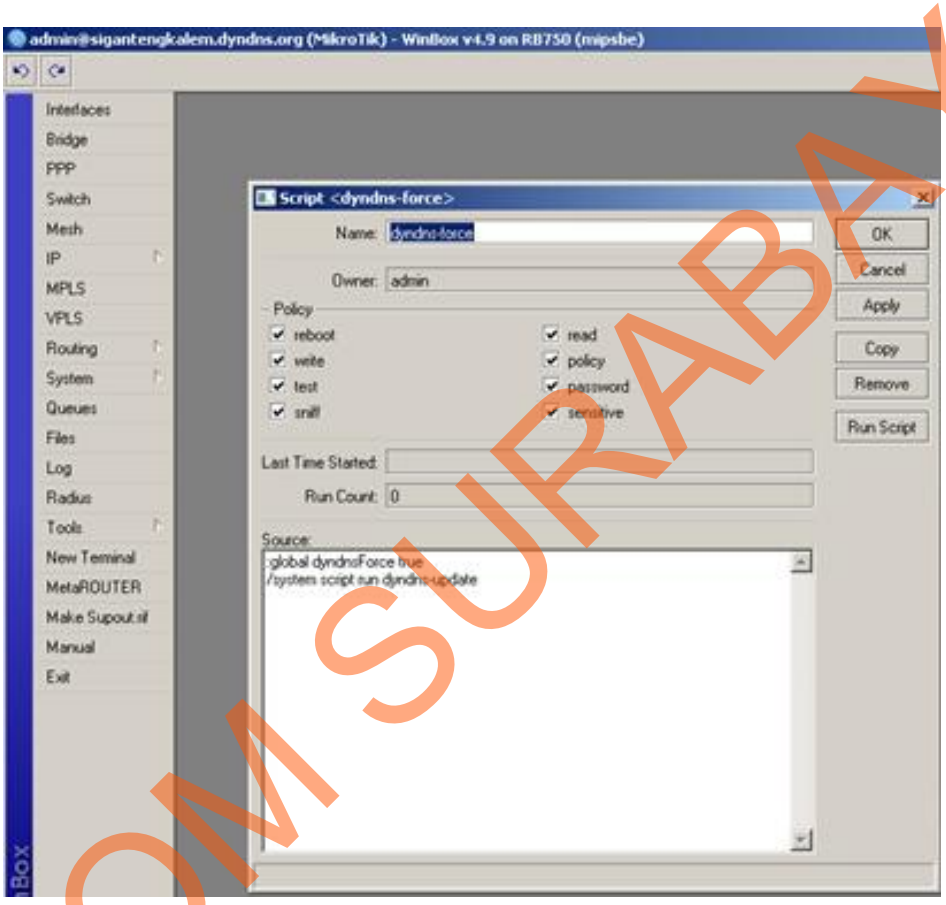


Gambar 3.11 Menu Pop-Up Daftar MAC address

Jadi, terdapat dua metode untuk me-remote MikroTik melalui winbox, yaitu dengan menginputkan langsung alamat IP atau melalui alamat MAC Ethernet router. Jika MikroTik belum memliki IP, gunakan alamat MAC. Jika MikroTik sudah memiliki, gunakannalamat IP dengan cara

mengetikkan nomor IP pada kolom Connect To diakhiri dengan menekan tombol Connect.

Berikut adalah tampilan gambar dari winbox yang berhasil me-remote MikroTik.



Gambar 3.12 Remote Via Winbox

Jika Anda ingin menkonfigurasi MikroTik melalui perintah (command), Anda tinggal menekan menu new terminal.