**BAB II**

**TINJAUAN PUSTAKA**

* 1. **Landasan Teori**

**2.1.1 Pengertian Mikrotik**

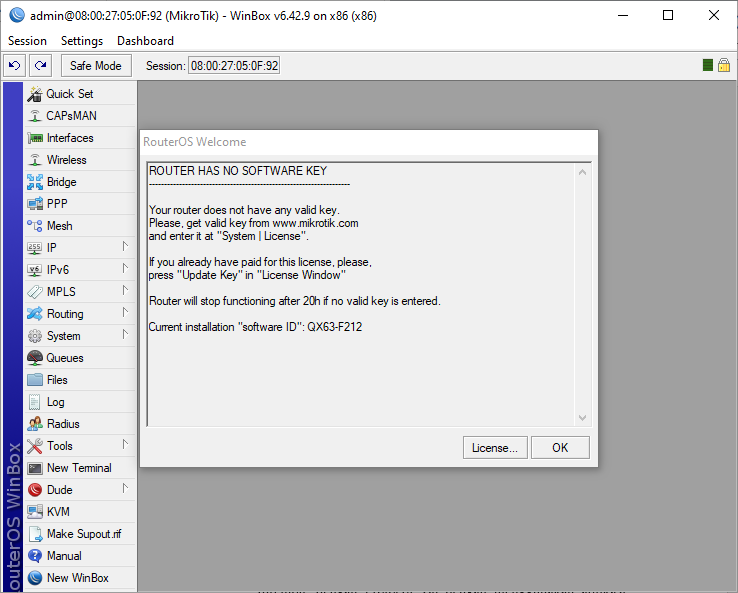
Mikrotik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot (mikrotik.co.id). Jenis Mikrotik sebagai berikut:

1. Mikrotik RouterOS™ adalah versi MikroTik dalam bentuk perangkat lunak yang dapat diinstal pada komputer rumahan (PC) melalui CD. Anda dapat mengunduh file image MikroTik RouterOS dari website resmi MikroTik, [www.mikrotik.com](http://www.mikrotik.com). Namun, file image ini merupakan versi trial MikroTik yang hanya dapat dalam waktu 24 jam saja. Untuk dapat menggunakannya secara full time, anda harus membeli lisensi key dengan catatan satu lisensi hanya untuk satu harddisk.
2. BUILT IN Hardware adalah Mikrotik dalam bentukperangkat keras yang khusus dikemas dalam board router yang didalamnya sudah terinstal Mikrotik Router Operating System.

Terdapat beberapa cara untuk me-remote MikroTik, antara lain, melalui winbox, Browser, telnet dan ssh.

1. **Remot menggunakan winbox**

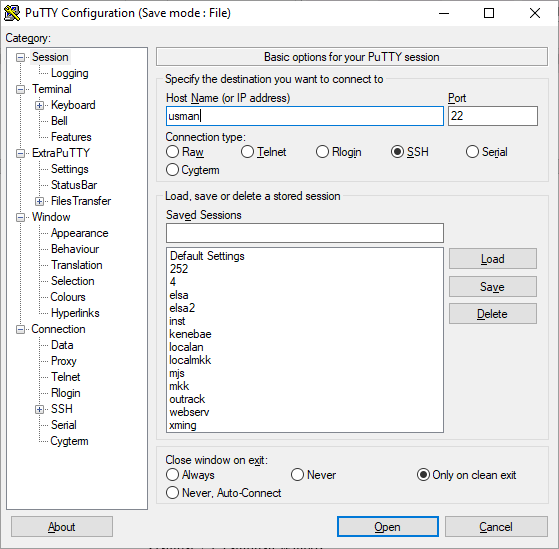
Mikrotik bisa diakses atau diremote menggunakan tool winbox. Winbox adalah sebuah utility untuk melakukan remote ke server mikrotik dalam mode GUI. Winbox bisa mendeteksi mikrotik dengan mendeteksi Mac address dari ethernet yang terpasang di Mikrotik RouterOS. Gambar winbox dapat dilihat pada gambar 2.1 :



Gambar 2.1 Tampilan Winbox

1. **Remote menggunakan SSH**

Bagi pengguna system operasi windows, MikroTik dapat diremote dengan Protocol ssh dengan menggunakan aplikasi putty. Bagi pengguna linux ssh secara default telah terinstal sehingga tidak memerlukan lagi aplikasi semacam putty. Gambar putty dapat dilihat pada gambar 2.4 :

****

Gambar 2.2 Tampilan Remote browser

**2.1.2 Router**

**Router adalah perangkat yang menghubungkan beberapa jaringan data dalam level protokol yang sama, beroperasi di layer network OSI dan juga berfungsi sebagai pemisah antara Broadcast Domain yang satu dengan yang lain. Router mempunyai fungsi utama memilih route dalam melewatkan informasi dari satu pengguna ke pengguna lainnya dengan memilih kombinasi lintasan yang optimal.**

1. **Konsep Router**

**Konsep router yaitu suatu media pengiriman data yang mampu mengatur kegiatan komunikasi data berbasis Connectionless Oriented yang mengirimkan data dengan konsep datagram untuk mencegah efek-efek negatif seperti data yang datang tidak berurutan maupun data yang tidak sampai ditujuan.**

1. **Fungsi Router**

**Sebuah router menampung traffik dari sumber-sumber traffik kemudian menyalurkan dengan cara memilihkan jalan yang terdekat ke tujuannya. Jadi pada dasarnya fungsi sebuah router adalah sebagai pengatur jalannya data/informasi. Sebuah router menampung traffik dari sumber-sumber traffik kemudian menyalurkan dengan cara memilihkan jalan yang terdekat ke tujuannya. Jadi pada dasarnya fungsi sebuah router adalah sebagai pengatur jalannya data/informasi. Secara mudah dapat dikatakan, router menghubungkan dua buah jaringan yang berbeda, tepatnya mengarahkan rute yang terbaik untuk mencapai network yang diharapkan.**

**2.1.3 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. Agar dapat mencapai mesin di Internet, alamat IP private (alamat IP RFC1918) harus diubah menjadi alamat IP publik yang dapat di routing di Internet global. Hal ini dapat dicapai menggunakan teknik yang dikenal sebagai Network Address Translation, atau NAT.

**2.1.4 Wireless Network**

**Wi-Fi (Wireless Fidelity) merupakan istilah yang diberikan untuk sistem wireless LAN yang menggunakan standar IEEE 802.11. Istilah Wi-Fi diciptakan oleh sebuah organisasi bernama Wi-Fi Alliance yang bekerja menguji dan memberikan sertifikasi untuk perangkat-perangkat WLAN. Perangkat wireless diuji berdasarkan interoperabilitasnya dengan perangkat-perangkat wireless lain yang menggunakan standar yang sama. Setelah diuji dan lulus, sebuah perangkat akan diberi sertifikasi Wi-Fi Certified. Artinya perangkat ini bisa bekerja dengan baik dengan perangkat-perangkat wireless lain yang juga bersertifikasi ini. Semua produk yang telah di test dan disetujui dengan label Wi-Fi Certified (registered trademark) oleh Wi-Fi Alliance berarti memiliki interoperabilitas satu sama lain sekalipun berbeda jenis, merk dan vendor. Secara umum setiap produk Wi-Fi bekerja pada frekuensi yang sama 2,4 Ghz dan 5.x Ghz dan dapat saling bekerja satau sama lain meskipun tidak tersertifikasi oleh Wi-Fi Alliance. Istilah Wi-Fi umumnya digunakan untuk teknologi berbasis standar IEEE 802.11, sebagaimana istilah Ethernet digunakan untuk standar IEEE 802.3. Pada awalnya, sertifikasi Wi-Fi hanya diberikan pada perangkat wireless yang bekerja pada standar IEEE 802.11b. Namun, saat ini standar ini juga diberikan pada semua perangkat yang menggunakan standar IEEE 802.11. Sertifikasi Wi-Fi sudah dianggap sebagai sertifikasi standar untuk perangkat wireless yang ada saat ini. Wi-Fi telah banyak digunakan di berbagai sektor seperti bisnis, akademis, perumahan, dan banyak lagi. Singkatan Wireless Fidelity, istilah untuk teknologi Wireless berbasis standar IEEE 802.11. IEEE 802.11 adalah spesifikasi standar yang dibangun oleh IEEE untuk mendefinisikan teknologi Wireless LAN dan disetujui pada 1997.**

**Keuntungan dari sistem Wi-Fi, pemakai tidak dibatasi ruang gerak dan hanya dibatasi pada jarak jangkauan dari satu titik pemancar Wi-Fi. Untuk jarak pada sistem Wi-Fi mampu menjangkau area 100feet atau 30M radius. Selain itu dapat diperkuat dengan perangkat khusus seperti booster yang berfungsi sebagai relay yang mampu menjangkau ratusan bahkan beberapa kilometer ke satu arah (directional). Bahkan hardware terbaru, terdapat perangkat dimana satu perangkat Access Point dapat saling merelay (disebut bridge) kembali ke beberapa bagian atau titik sehingga memperjauh jarak jangkauan dan dapat disebar dibeberapa titik dalam suatu ruangan untuk menyatukan sebuah network LAN.**

**2.1.5 *Access Point***

*Access Point* adalah sebuah alat yang berfungsi untuk menyambungkan alatalat *wireless* ke sebuah jaringan berkabel (*wired network*) menggunakan *wifi*,*bluetooth* dan sejenisnya. *Wireless Access Point* digunakan untuk membuat jaringan WLAN (*Wireless Local Area Network*) ataupun untuk memperbesar cakupan jaringan *wifi* yang sudah ada menggunakan *mode bridge*. *Access Point* berfungsi sebagai *Hub* atau *Switch* yang bertindak untuk menghubungkan jaringan lokal dengan jaringan *wireless*, di *access point* ini koneksi data *internet* dipancarkan atau dikirim melalui gelombang radio, ukuran kekuatan sinyal juga mempengaruhi area *coverage* yang akan dijangkau, semakin besar kekuatan sinyal ukurannya dalam satuan dBm atau mW semakin luas jangkauannya.

**2.1.6** ***QoS (Quality of Service)***

QoS (*Quality of Service*) merupakan suatu pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan. Parameter-parameter performansi dari sebuah jaringan antara lain :

* 1. *Delay*, didefinisikan sebagai total waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya.
  2. *Packet loss*, adalah perbandingan seluruh paket IP yang hilang dengan seluruh paket IP yang dikirimkan antara pada source dan *destination*.
  3. *Throughput*, adalah jumlah total kedatangan paket IP sukses yang diamati di tempat pengukuran pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.
  4. *Bandwidth* adalah jumlah data yang dapat ditransfer melalui jaringan dalam jangka waktu tertentu.

**2.1.7 *Queue Tree***

*Queue tree* adalah konfigurasi yang bersifat *one way* (satu arah), yang berarti sebuah konfigurasi *queue* hanya akan mampu melakukan *queue* terhadap satu arah jenis *traffic*.Jika sebuah konfigurasi *queue* pada *queue* *tree* ditujukan untuk melakukan *queue* terhadap *bandwidth* *download*,maka konfigurasi tersebut tidak akan melakukan *queue* untuk *bandwidth* *upload*, demikian pula sebaliknya. sehingga untuk melakukan *queue* *tree* terhadap *traffic* *upload* dan *download* dari sebuah komputer pengguna, harus membuat 2 (dua) konfigurasi *queue* yaitu, *download* dan *upload*. Prinsip *top to bottom* dalam mengeksekusi konfigurasi *queue* *tree* juga tidak berlaku lagi di *queue* *tree*. Jika memiliki beberapa konfigurasi *queue* pada *queue* *tree*, maka konfigurasi *queue* tersebut akan dieksekusi secara simultan atau bersamaan. Dengan diprosesnya packet secara simultan, maka penggunaan *queue* *tree* jelas akan lebih mempercepat processing packet.Penandaan paket (*Mark Packet*) berfungsi mengidentifikasi sebuah aliran paket data dalam sebuah *queue* *tree*. Apabila saat penandaan paket pada *firewall mangle* tidak tepat, maka pekerjaan penandaan paket akan gagal. Jika penandaan paket

dipastikan manajemen menggunakan *queue* treepun akan gagal .

**2.1.8 *Firewall***

*Firewell* adalah sistem keamanan yangmenggunakan sistem yang diletakkan di dua jaringan dengan fungsi utama melakukan filtering terhadap akses yang akan masuk. *Firewall* Berupa seperangkat *hardware* atau *software*, bisa juga berupa seperangkat aturan dan prosedur yang ditetapkan oleh organisasi. *Firewall* 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 bentuk sebuah mesin terdedikasi, yang berjalan pada pintu gerbang *(gateway)* antara jaringan lokal dan jaringan lainnya. *Firewall* atau “tembok penghalang” merupakan sebuah perangkat yang ditujukan untuk melindungi network dari “kejahatan dunia luar”. Biasanya firewall digunakan untuk melindungi LAN (*Local Area* *Network*) dari berbagai serangan atau intrusions.Serangan dapat ditujukan kepada host tertentu yang dapat menyebabkan data *corrupt* atau *service* menjadi tidak berfungsi

**2.1.9 Analisis Sistem**

Tujuan analisis sistem adalah untuk mengetahui pasti hal-hal yang menjadi kebutuhan dan harapan pengguna sehingga sistem yang dibuat nantinya merupakan sistem yang efektif dan efisien. Kegiatan – kegiatan yang dilakukan pada analisis sistem ini adalah analisis pengguna, analisis kebutuhan fungsional dan analisis non fungsional.. Kebutuhan fungsional merupakan kebutuhan akan fasilitas yang dibutuhkan serta aktivitas apa saja yang dilakukan oleh sistem secara umum.