BAB II
DASAR TEORI

2.1 KAJIAN PUSTAKA

Penelitian yang dilakukan oleh Christian [6] pada tahun 2019 membahas mengenai perancangan terhadap hak akses *user* pada *port* menggunakan mikrotik *router* dan akan dilakukan uji coba keamanan dengan menggunakan metoda *port knocking* dan *firewall action tarpit.* Tujuan dari penelitian ini untuk mengetahui bagaimana model implementasi sebuah sitem keamanan suatu jaringan komputer agar dapat mendeteksi terhadap serangan *attacker* yang akan memasuki *port* dan secara otomatis akan memblokir sebuah *port* yang akan dimasukinya. Dari penelitian ini mendapatkan hasil dimana kinerja *port knocking* dapat bekerja dengan baik, hal tersebut dilihat dari peyerangan yang menggunakan *brute force attack* dimana *attacker* tidak berhasil menemukan *user* dan *password* dari layanan *port* tersebut.

Penelitian Puji dan Kusuma [7] pada tahun 2019 membahas mengenai cara untuk pengimplementasian terhadap akses yang akan diizinkan dan di-*bloking* menggunakan metoda *simple port knocking* pada *routerOS* mikrotik. Tujuan dari penelitian ini adalah untuk mengimplementasikan *simple port knocking* dengan simulasi *cloud* yang akan menggunakan *dyanamic routing* OSPF, bertujuan untuk memberikan sebuah sistem keamanan terhadap pengguna dalam mengakses jaringan komputer agar tidak terjadi pencurian data atau sebuah informasi sehingga data tersebut tetap aman. Pada hasil dari penelitian ini menunjukan untuk autentifikasi pada *port* membuat *server* aman, hal ini dikarenakan penutupan *port* dalam mencegah terjadinya sebuah serangan dari *attacker* yang tidak diberikan untuk mengakses *server*.

Penelitian Albar dan Putra [8] pada tahun 2022 membahas mengenai rancangan sebuah metode keamanan pada *firewall* dengan metode keamanan *port knocking* di mikrotik *router OS* V6.48.3. Tujuan dari penelitian ini adalah untuk meningkatkan keamanan jaringan untuk mencegah dari pihak yang tidak bertanggung jawab dalam melakukan

pencurian data. Untuk *rules port knocking* yang diterapkan pada *firewall* dalam penelitian ini diantaranya akan memanfaatkan *port* 23 *(telnet), port* 80 *(webfig), port* 21(FTP) dan *port* 8291 *(Winbox),* untuk waktu akses yang diterapkan pada masing-masing port yaitu 5 detik. Berdasarkan hasil pengujian yang sudah dilakukan menunjukan hasil bahwa metoda *port knocking* dapat berjalan dengan baik dan mampu meningkatkan sistem keamanan jaringan yang diimplementasikan pada *router OS* mikrotik V6.48.3 dibandingkan dengan sistem keamanan jaringan yang tidak menerapkan metoda *port knocking*.

Penelitian yang dilakukan oleh Saputro, dkk. [9] pada tahun 2020 membahas mengenai penggabungan metoda *DeMilitarized Zone* dan *Port Knocking* dalam mengamankan sistem keamanan jaringan komputer. Tujuan dari penelitian ini untuk menangkal dan meminimalisir dari serangan yang akan memasuki dan merusak sistem jaringan. *DeMilitarized Zone* dan *Port Knocking* diimplementasikan pada jaringan lokal maupun interlokal dimana jika suatu penyerang ingin meng*exploit* atau menyerang *server* utama maka yang pertama diserang adalah *server firewall* (*router*). Dari hasil penelitian tersebut diberikan informasi yaitu penggunaan fungsi *DMZ* dan *Port Knocking* dapat memberikan keamanan kepada *server* utama (*DMZ*) dan *server router* (*Port Knocking*) dari serangan *Distributed Denial of Services (DDoS)* dan *Port Scanning* yang akan membahayakan *server*. Akan tetapi keamanan tersebut hanya berlaku pada area *outside* (luar), sedangkan area *inside* (dalam) memiliki keamanan yang berbeda dari *outside*, sehingga perlu penambahan keamanan dari sisi yang lain misal seperti keamanan pada ruang penyimpanan dan sistem enkripsi *password* pada *server*.

2.2 DASAR TEORI

2.2.1 Jaringan Komputer

Menurut Badrul dan Akmaludin menyimpulkan bahwa: Jaringan komputer adalah kumpulan dari beberapa komputer (dan perangkat lain seperti *router, switch* dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Menurut Lestari dan Permana (2019), jaringan komputer

merupakan sebuah sistem yang terdiri dari sekelompok komputer otonom yang saling terkoneksi satu dengan yang lainnya menggunakan protokol komunikasi melalui media komunikasi untuk dapat saling berbagi informasi, programprogram atau pun penggunaan perangkat. Lestari dan Permana (2019) juga menjelaskan bahwa suatu jaringan komputer terdiri dari komputer, *software* dan perangkat jaringan yang bekerja sama dalam suatu ruang lingkup untuk mencapai suatu tujuan. Untuk mencapai tujuan tersebut, setiap bagian dari jaringan komputer meminta dan memberikan layanan. Pihak yang meminta atau menerima layanan disebut dengan *client* dan yang memberikan atau mengirim disebut *server*. Arsitektur jaringan ini disebut dengan sistem *client-server* yang mana telah digunakan pada hampir seluruh aplikasi jaringan komputer di dunia[10].

Menurut dari para ahli dalam memahami jaringan komputer sudah dibagi menjadi beberapa klasifikasi, diantaranya:

1. Berdasarkan *area* atau skala;
2. Berdasarkan *media* penghantar;
3. Berdasarkan fungsi;
4. Berdasarkan topologinya.

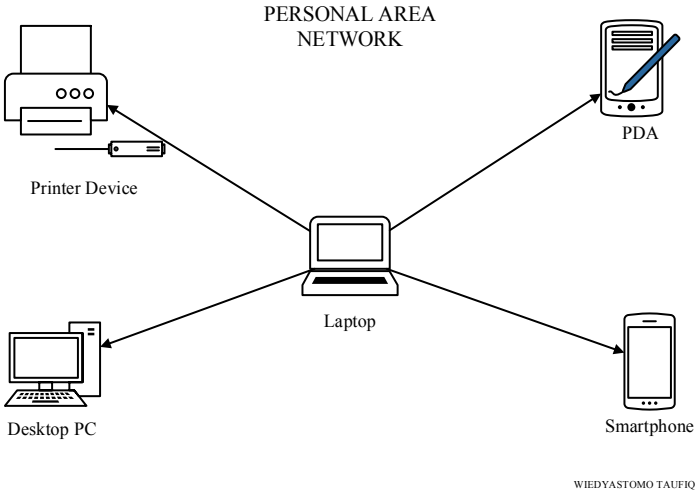
A. Berdasarkan *area* atau skala

Yang pertama adalah klasifikasi berdasarkan *area* atau geografisnya yang dibagi menjadi beberapa diantaranya:

1. *Personal Area Network* (PAN)

   Pada Gambar 2.1 merupakan *Personal Area Network* (PAN), sebuah jaringan yang digunakan untuk berkomunikasi dengan jarak dekat antarperangkat pribadi. Jaringan PAN menggunakan beberapa perangkat elektronik pribadi agar dapat berkomunikasi contohnya seperti PC, *smartphone* dan lain sebagainya. Sebuah jaringan PAN berupa jaringan nirkabel maupun kabel, untuk jaringan nirkabel dibutuhkan metoda seperti penggunaan *wifi, Bluetooth*, dan lain sebagainya, sementara untuk jaringan kabel menggunakan USB. Jaringan PAN mempunyai fungsi diantaranya sebagai titik awal dari berbagai perangkat agar dapat saling terhubung dan melakukan

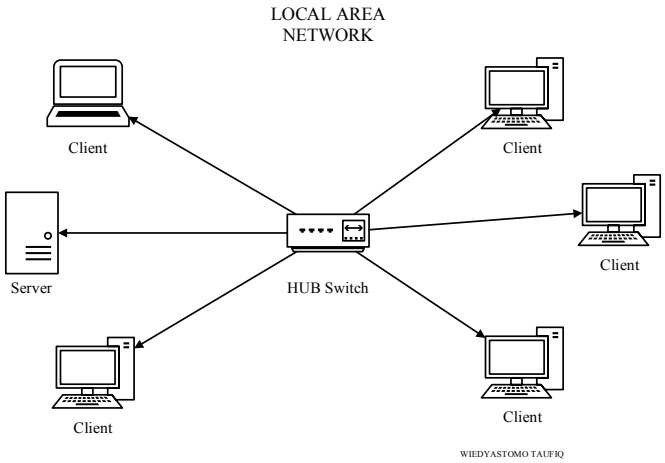
komunikasi maupun transmisi data dengan jarak yang dekat.



Gambar 2.1 *Personal Area Network (PAN)* [11]

2. *Local Area Network* (LAN)

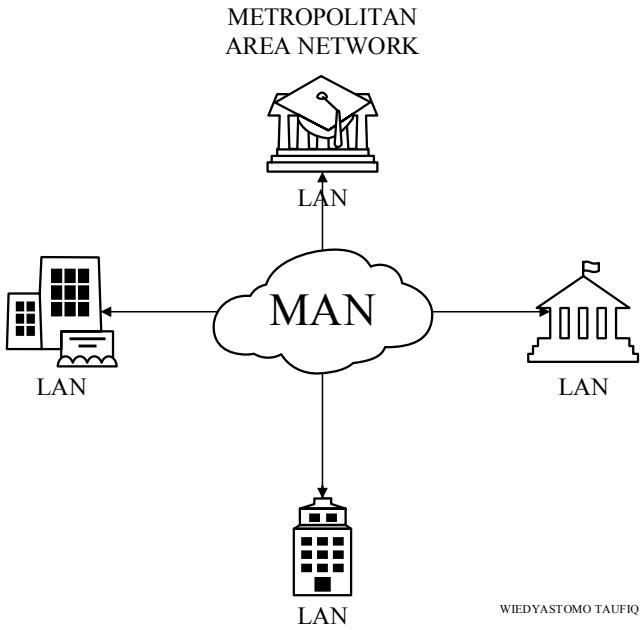
   Local Area Network (LAN) yang ditunjukan pada Gambar 2.2 merupakan sebuah jaringan komputer yang mencakup wilayah lokal saja, LAN akan menghubungkan perangkat ke sebuah jaringan internet melalui perangkat jaringan sederhana. Seringkali jaringan LAN ini disebut dengan jaringan personal atau jaringan *private*. Jaringan LAN biasanya digunakan untuk kebutuhan jaringan kecil dengan menggunakan *resource* yang bersamaan, contohnya penggunaan printer secara bersamaan dan lain-lain.



Gambar 2.2 *Local Area Network (LAN)* [11]

3. *Metropolitan Area Network* (MAN)

Metropolitan Area Network (MAN) merupakan jaringan komputer yang mencakup area yang luas dan menggunakan teknologi lebih canggih dari jaringan LAN, hal ini dapat dilihat pada Gambar 2.3. *Metropolitan Area Network* (MAN) merupakan jaringan yang menggabungkan beberapa jaringan LAN dimana jangkauan areanya mencapai 10 km sampai dengan 50 km. Jaringan MAN sangat cocok untuk diaplikasikan dalam membangun jaringan antar perkantoran atau instasi yang lingkup jangkauannya masih dalam satu kota, oleh karena itu jaringan MAN ini biasanya dipakai untuk menghubungkan lokasi seperti perkantoran, kampus, dan lain sebagainya. Jaringan MAN mempunyai kecepatan yang tinggi dalam mentransfer data, selain itu juga untuk proses instalasinya juga tidak terlalu rumit. Dalam jaringan MAN diperlukan seorang operator telekomunikasi yang mempunyai tanggung jawab untuk menghubungkan antar jaringan komputer.

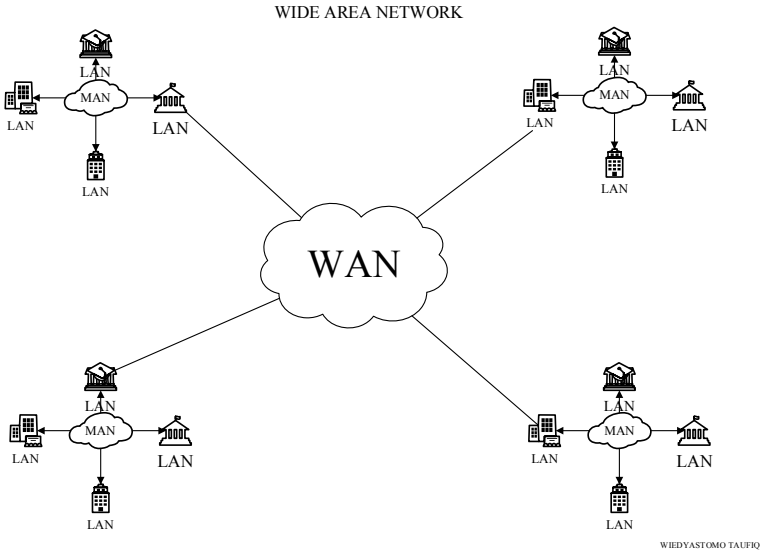


Gambar 2.3 *Metropolitan Area Network (MAN)* [11]

4. *Wide Area Network* (WAN)

Untuk *Wide Area Network* (WAN) yang tertera pada Gambar 2.4 merupakan sebuah jaringan komputer yang luas areanya mencapai

satu kawasan, satu pulau, satu negara atau bahkan benua. WAN memiliki kecepatan transmisi mulai dari 2 Mbps, 34 Mbps, 45 Mbps, 155 Mbps, 625 Mbps, atau bahkan lebih. *Wide Area Network* (WAN) merupakan jaringan yang menggabungkan jaringan LAN dan MAN dimana untuk wilayahnya dipisahkan secara geografis. Dalam membangun sebuah jaringan WAN diperlukan sebuah kabel dengan serat optik (*fiber optic*), kabel telepon, *microwave* atau juga menggunakan satelit. Dikarenakan jangkauan wilayahnya yang sangat luas dalam membangun sebuah jaringan WAN diperlukan juga biaya yang sangat besar. Jaringan WAN bekerja pada layer fisik dan layer data link dari layer OSI[11].



Gambar 2.4 *Wide Area Network (WAN)* [11]

B. Berdasarkan *Media* Penghantar

Klasifikasi berdasarkan media penghantar jaringan komputer dibagi menjadi dua, yaitu:

1. *Wire Network*

   Wire Network adalah jaringan komputer yang menggunakan kabel sebagai media penghantar, jadi data mengalir pada kabel.

2. *Wireless Network*

   Wireless Network adalah jaringan tanpa kabel yang menggunakan media penghantar gelombang radio atau cahaya infrared, misalnya

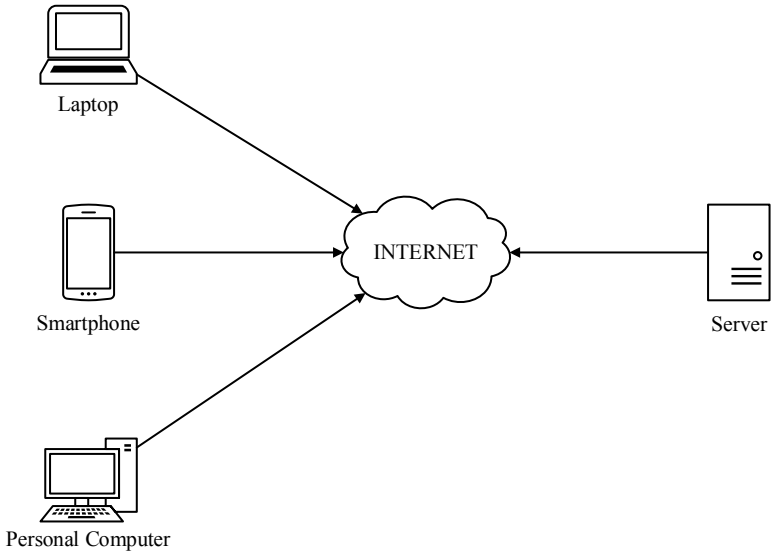
outlet atau tempat makan yang menyediakan layanan *wireless network*[12].

C. Berdasarkan Fungsi

Klasifikasi berdasarkan fungsinya dibagi menjadi dua, antara lain:

1. *Client-Server*

   Pada Gambar 2.5 yang merupakan jaringan klien *server (client-server)*, jaringan yang menggunakan satu komputer sebagai *server* (pelayan) yang melayani komputer lainnya yang dinamakan *client,* dengan menggunakan jaringan ini mengharuskan permintaan layanan sumber daya dari komputer klien harus melewati komputer *server.* Komputer *server* yang mengalami permintaan layanan yang banyak akan disiapkan lebih dari satu *computer* untuk membagi tugas, seperti *file-server, print-server, database,* dan seterusnya.

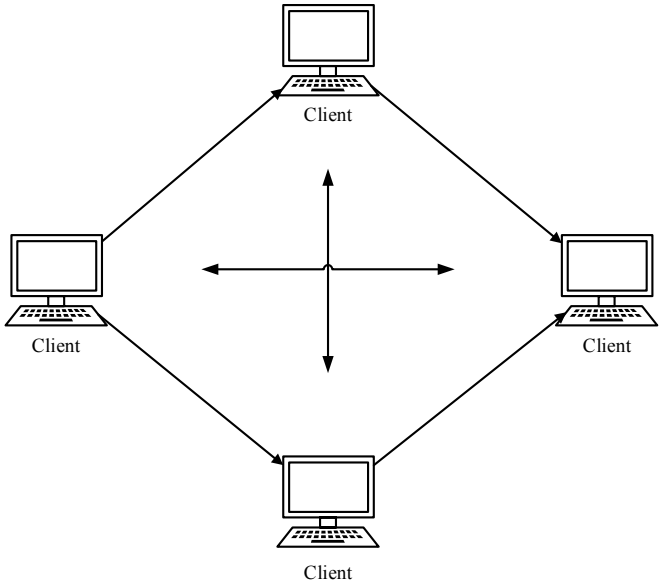


Gambar 2.5 *Client-Server* [13]

2. *Peer-to-peer*

   Jaringan *peer-to-peer* yang ditunjukan pada Gambar 2.6 merupakan komputer yang terhubung memiliki kedudukan dan hak istimewa yang sama. Tidak ada *server* pusat untuk melakukan koordinasi. Masing-masing perangkat dalam jaringan komputer bertindak baik sebagai klien maupun *server.* Masing-masing *peer* berbagi beberapa

sumber dayanya, seperti memori dan tenaga pemrosesan *(processing power),* dengan seluruh jaringan komputer[13].



Gambar 2.6 *Peer-to-Peer* [13]

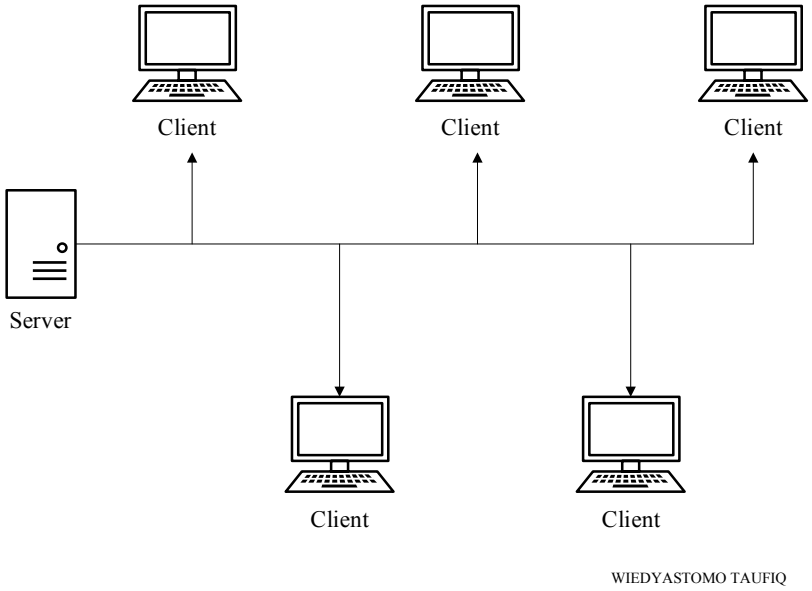
D. Jenis-Jenis Topologi Jaringan

Topologi jaringan memiliki beberapa jenis, dalam menentukan topologi mana yang ingin digunakan pemilihan sebuah topologi jaringan diliat dari kebutuhan *user,* mulai dari perangkta yang akan di instalasi, jarak cakupan suatu WiFi, serta berapa banyak ruangan yang nantinya akan dimasukan dalam proses instalasi dan lain sebagainya. Berikut beberapa jenis topologi jaringan komputer:

1. Topologi *Bus*

   Topologi jaringan *bus* adalah topologi jaringan komputer yang pertama kali dipergunakan dalam menghubungkan perangkat komputer, untuk topologi *bus* itu sendiri dapat dilihat pada Gambar 2.7. Media transmisi yang digunakan dalam proses instalasi berupa sebuah kabel panjang dengan beberapa terminal yang nantinya akan terhubung ke masing-masing komputer. Untuk topologi *bus* ini sudah sangat jarang digunakan oleh suatu perusahaan, hal ini dikarenakan resiko yang akan ditimbulkan sangat besar, salah satu resiko yang dapat merugikan sebuah perusahaan jika memakai

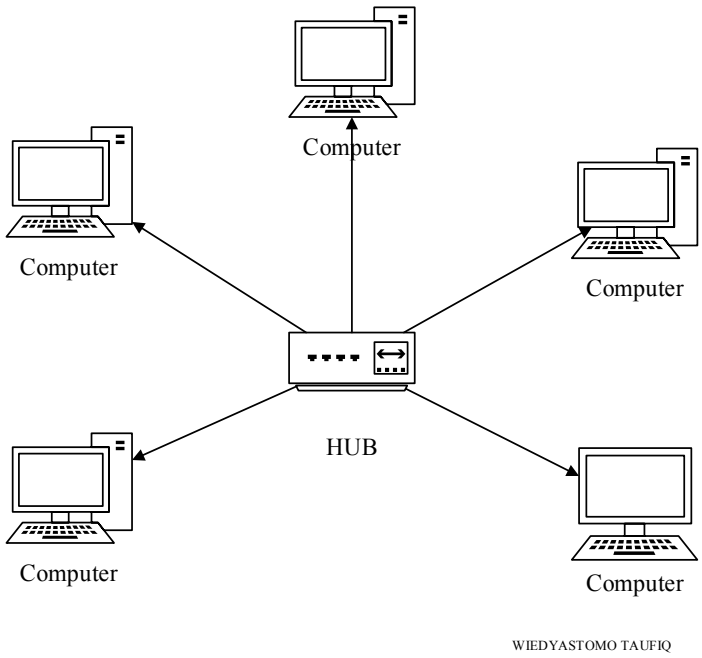
topologi *bus* ini terjadinya tabrakan suatu data dan jika ada perangkat komputer yang mengalami kerusakan, maka jaringan tersebut akan langsung tidak berfungsi dengan baik sebelum diperbaiki.



Gambar 2.7 Topologi *Bus* [14]

2. Topologi *Star*

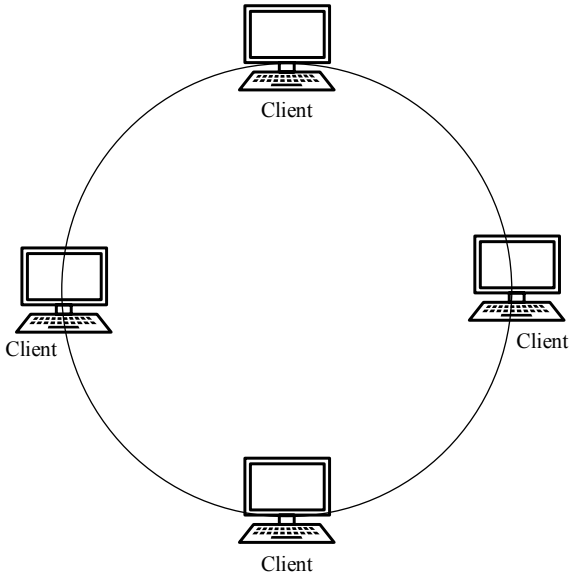
   Pada Gambar 2.8 merupakan topologi *star* atau yang biasa disebut dengan topologi bintang, topologi jaringan yang menghubungkan dua perangkat atau lebih dalam suatu jaringan yang berbentuk bintang. Topologi bintang ini adalah konvergensi dari node tengah ke setiap *node* atau *client*, yang dimaksudkan konvergensi disini merupakan penggabungan aliran daya yang saling terhubung dalam satu titik pada node ditengah, sementara untuk node tengah itu sendiri adalah berupa *hub* atau *switch* yang terhubung satu sama lain dari *user* ke *server* ataupun sebaliknya. Prinsip kerja dari topologi bintang ini yaitu semua link akan diarahkan menuju pusat terlebih dahulu, dimana link tersebut nantinya akan diarahkan ke semua node yang tentunya sudah dikehendaki oleh *server* pusat.



Gambar 2.8 Topologi *Star* [14]

3. Topologi *Ring*

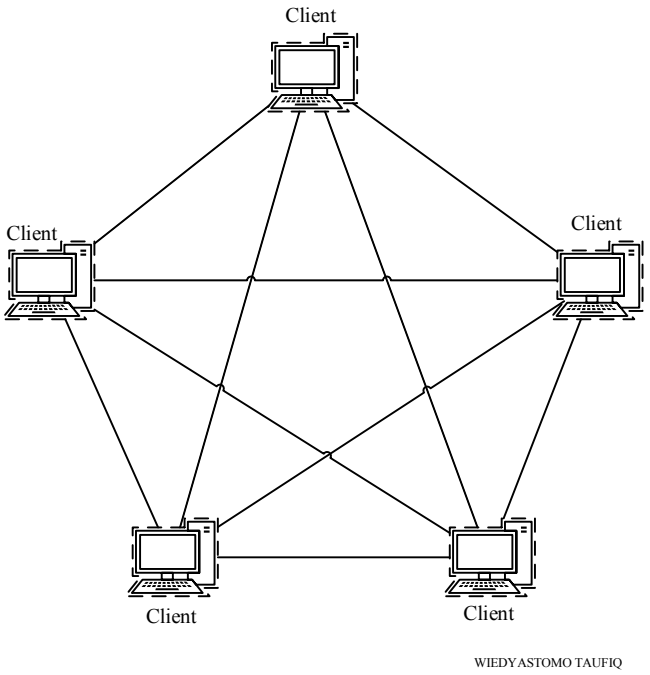
   Untuk topologi *ring* atau yang biasa dikenal dengan topologi cincin yang tertera pada Gambar 2.9, merupakan sebuah konsep atau sebuah tata cara yang dipergunakan sebagai penghubung satu komputer pada komputer lainnya dengan rangkaian yang membentuk titik-titik dimana titik-titik itu saling terhubung dengan dua titik lainnya pada satu jaringan. Topologi *ring* juga dapat diartikan untuk menghubungkan dua perangkat atau lebih dalam sebuah rangkaian yang membentuk cicin. Fungsi dari titik itu sendiri sebagai *repeater* untuk memperkuat sinyal sirkulasi, yang dimaksudkan dengan *repeater* merupakan sebuah perangkat yang berfungsi untuk menerima atau memperluas jangkauan sinyal. Dalam proses penerimaan sinyal akan dibantu dengan adanya token, dimana untuk token ini mempunyai informasi dari perangkat komputer sebelumnya yang kemudian data tersebut akan diteruskan ke bagian *node* berikutnya.



Gambar 2.9 Topologi *Ring* [14]

4. Topologi *Mesh*

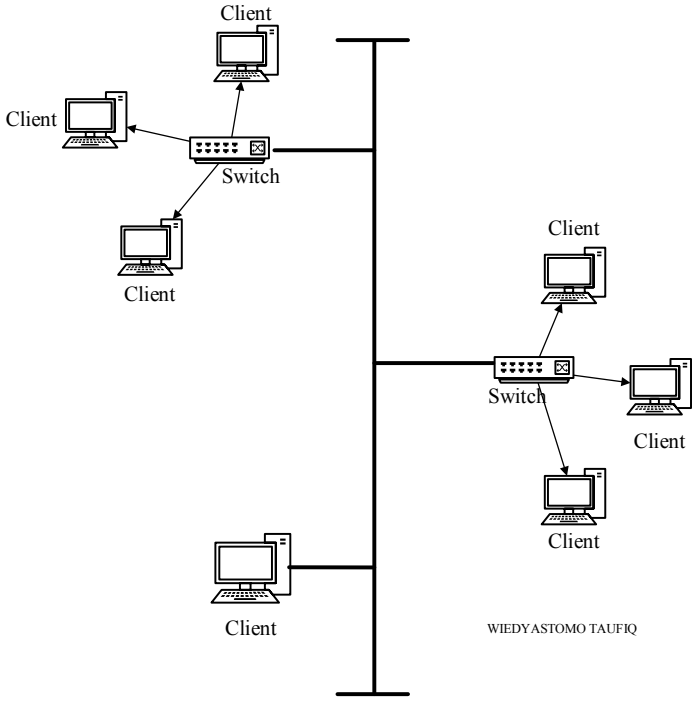
   Topologi *Mesh* atau yang seringkali disebut dengan topologi jala merupakan sebuah topologi jaringan komputer yang mana bentuk koneksi antara perangkat komputer akan saling berhubungan secara langsung hanya pada satu jaringan saja tanpa perlu melewati perangkat lainnya, untuk topologi *mesh* dapat dilihat pada Gambar 2.10. Topologi ini dibuat untuk skala jaringan yang tidak terlalu besar, akan tetapi membutuhkan komunikasi yang cepat walaupun untuk topologi *mesh* ini jarang dipergunakan, karena sulitnya dalam mengelola seta menggunakanya, hal ini dikarenakan terlalu banyak kabel yang dipergunakan, terlebih lagi jika terdapat sebuah kerusakan pada salah satu komputer tidak akan mempengaruhi perangkat komputer lainnya. Untuk topologi *mesh* mempunyai kelebihan dimana dapat melakukan pendeteksian terhadap sebuah gangguan yang terdapat pada jaringan dengan waltu yang cepat dan tepat. Selain kelebihan yang dimiliki topologi ini tentunya mempunyai kekurangan salah satunya adalah proses instalasi yang rumit dimana untuk proses instalasi itu sendiri harus dilakukan oleh orang yang sudah ahli dibidang komputer jaringan.



Gambar 2.10 Topologi *Mesh* [14]

5. Topologi *Tree*

   Untuk topologi jaringan pada Gambar 2.11 merupakan topologi *Tree* atau topologi pohon, topologi ini gabungan dari topologi *star* yang dihubungkan dengan topologi *bus* yang berfungsi sebagai tulang punggung atau (*backbone*). Pada topologi ini memiliki beberapa susunan yang mana susunan tersebut berbentuk seperti pohon, untuk dahan pohon adalah jaringan yang lebih besar dibandingkan ranting, hal ini membuat topologi pohon disebut dengan topologi bertingkat dikarenakan mempunyai *heirarki* jaringan, *heirarki* yang memiliki tingkat lebih tinggi akan sangat mempengaruhi dan dapat mengontrol jaringan yang lebih rendah, oleh karena itu topologi *tree* sering dipergunakan pada satu kelompok agar *client* dapat berkomunikasi dengan *client* kelompok lainnya, selain itu juga topologi ini dipergunakan untuk interkoneksi antar sentral dan juga *heirarki* yang berbeda. Akan tetapi dalam mengirimkan suatu data, harus melewati simpul pusat terlebih dahulu sebelum sampai pada tujuan[14].



Gambar 2.11 Topologi *Tree* [14]

2.2.2 *IP Address*

IP Address merupakan alamat yang diberikan pada jaringan komputer menggunakan *protocol Transmission Control Protocol/Internet Protocol* (TCP/IP), untuk TCP/IP itu sendiri adalah sekelompok *protocol* yang mengatur komputer dan komunikasi pada jaringan internet, bahwasannya setiap komputer yang terhubung di jaringan internet harus memiliki alamat *IP* dimana untuk alamat *IP* itu sendiri harus mempunyai alamat *IP* yang unik, hal ini dikarenakan perangkat atau *computer server* tidak boleh menggunakan alamat *IP* yang sama di dalam suatu jaringan internet, selain itu *IP address* mempunyai fungsi sebagai alamat pengiriman data ke perangkat yang akan digunakan. Ketika *user* mengakses sebuah situs, sebenarnya ada proses pengunduhan (*download* data) yang dikirim dari situs tersebut. Untuk cara kerja dari *IP Address* itu sendiri komputer yang terhubung ke *router* jaringan biasanya tersedia oleh penyedia layanan internet (ISP), selanjutnya *router* akan berkomunikasi dengan *server* tempat *website* disimpan untuk mengakses *file* yang perlu dikirim kembali ke komputer. Untuk saat ini terdapat dua versi alamat *IP*, yaitu alamat *IP* versi

4 *(IPv4)* dan *IP* versi 6 *(IPv6)*[15]. Perbedaan terkait *IP address* berdasarkan IPv4 dan IPv6 yang terdapat pada Tabel 2.1.

Tabel 2.1 Perbedaan IPv4 dengan IPv6

IPv4	Perbedaan	IPv6
32-*bit*	Ukuran Alamat	128-bit
12	Jumlah Bidang *Header*	8
20 *byte*	Panjang Bidang *Header*	40 *byte*
IPv4 hanya alamat *numerik*	*Metode Addressing*	IPv6 berupa alamat *afanumerik*
Broadcast, multicast, dan unicast.	Jenis Alamat	*Anycast, multicast, dan unicast.*
Lima kelas yang berbeda, dari A sampai E.	Jumlah Kelas	Jumlah IP address tidak terbatas.
Pengguna harus mengonfigurasi sistem baru agar IPv4 dapat berkomunikasi dengan sistem lain.	Konfigurasi	Konfigurasi opsional, bergantung pada fungsi yang diperlukan.
Jaringan dikonfigurasi secara manual atau melalui DHCP.	Konfigurasi Jaringan	IPv6 memiliki kemampuan konfigurasi otomatis.

2.2.3 Sistem Keamanan Jaringan

A. Pengertian Sistem Keamanan Jaringan

Sistem keamanan jaringan merupakan sebuah sistem dimana untuk mencegah dan mengidentifikasi segala bentuk ancaman fisik maupun logic baik langsung maupun tidak langsung dari orang yang tidak bertanggung jawab yang berusaha masuk dan mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer[16]. Sistem keamanan jaringan itu sendiri sebagai hasil beberapa faktor yang bervariasi tergantung pada bahan dasarnya, akan tetapi secara normal sekiranya mempunyai beberapa hal yang diikutsertakan yaitu:

1. *Confidentiality* (kerahasiaan)

   merupakan segala pencegahan dari berbagai serangan yang dilakukan oleh orang yang tidak bertanggung jawab untuk mencapai sebuah informasi. Secara umum dapat disimpulkan bahwasannya *confidentiality* mempunyai makna dimana informasi hanya dapat diakses oleh mereka yang mempunyai hak akses, dianalogikan dengan *e-mail* maupun data-data perdagangan dari sebuah perusahaan.

2. *Integrity* (integritas)

   merupakan sebuah aspek yang menekankan bahwa sebuah informasi tidak dapat diubah tanpa seijin pemilik dari informasi tersebut.

3. *Authentication*

   merupakan langkah untuk menentukan atau memberikan informasi bahwa seseorang tersebut asli atau atentik. Dalam melakukan autentikasi terhadap sebuah objek biasanya dilakukan dengan mengkonfirmasi terhadap kebenaran pada objek tersebut, sementara untuk autentikasi pada seseorang biasanya dilakukan dengan cara memverifikasi identitas orang tersebut.

4. *Non-repudiation*

   Merupakan sebuah aspek yang bertujuan untuk menjaga agar seseorang tidak dapat menyangkal bahwasannya telah melakukan sebuah transaksi. Contohnya seseorang yang telah mengirimkan sebuah *e-mail* untuk memesan barang tidak dapat menyangkal bahwa dia sudah melakukan *pengiriman e-mail* tersebut. Aspek ini sangat penting dalam hal *e-commerce,* dimana dalam penggunaan *digital signature* dan teknologi kriptografi secara umum dapat menjaga aspek ini, tetapi untuk menjaga aspek ini harus didukung oleh status hukum dari *digital signature* yang legal.

5. *Access Control*

   Merupakan sebuah aspek yang berhubungan dengan metode atau cara pengaturan akses terhadap sebuah informasi. *Access control*

ini biasanya berhubungan dengan masalah *privacy* dan *authentication,* sebagai contoh yang biasa dilakukan yaitu dengan mengkombinasikan *user id* dan password atau dengan menggunakan mekanisme yang lain.

6. *Accountability*

   Merupakan kegiatan yang mana *user* didalam jaringan akan direkam, *user* yang berada dalam jaringan tersebut tidak akan bisa melanggar kebijakan keamanan dikarenakan identitas dan segala kegiatannya akan dikenali, jika mereka melakukan sebuah pelanggaran maka mereka dapat dituntut secara hukum[17].

B. Tipe Sistem Keamanan Jaringan

Orang yang tidak bertanggung jawab akan melakukan serangan demi mendapatkan sebuah data atau informasi yang terdapat disuatu perusahaan. Oleh karena itu, dalam mendapatkan sebuah pertahanan yang lebih maksimal diperlukan sistem keamanan jaringan, berikut untuk tipe sistem keamanan jaringan yaitu:

1. *Antimalware software*

   Merupakan sebuah perangkat lunak antivirus dan *antimalwalware* yang mampu melindungi sebuah data atau informasi pada suatu perusahaan dari berbagai *malicious software*, misalnya *virus, ransomware, worm*, dan *trojan*. Dalam penggunaan *antimalware* dapat meminimalisir dan melacak *file* berbahaya yang terdapat dalam suatu jaringan.

2. *Application Security*

   Sebuah aplikasi yang tidak mempunyai sistem keamanan yang maksimal seringkali digunakan *attacker* untuk mengakses jaringan. Dengan menerapkan sebuah sistem keamanan aplikasi hal tersebut dapat melindungi aplikasi apa saja yang berkaitan dengan jaringan.

3. *Behavioral Analytics*

   Dalam mengetahui seperti apa perilaku jaringan normal, agar lebih mudah untuk mendeteksi *anomaly* didalam jaringan dibutuhkan

network anomaly detection engines (ADE) yang memungkinkan untuk menganalisis jaringan sehingga jika terjadi sebuah pelanggaran maka pengguna akan memperoleh notifikasi.

4. *Data Loss Prevention*

   User dapat menjadi rantai terdepan dalam sistem keamanan jaringan. Oleh karena itu, *user* dapat memanfaatkan *tools data loss prevention* agar data *sensitive* tidak hilang dan disalahgunakan atau diakses oleh *user* yang tidak mempunyai kewenangan.

5. *Email Security*

   Email security juga perlu digunakan untuk mencegah dari serangan *email phising*. Dengan adanya *email security* membantu dalam mengidentifikasi terhadap *email* berbahaya serta juga memblokir serangan.

6. *Intrusion Prevention Systems*

   Intrusion Prevention Systems akan menganalisis dan memindai lalu lintas jaringan sehingga dapat mengidentifikasi berbagai jenis serangan secara mudah.

7. *Virtual Private Network* (VPN)

   Merupakan perangkat yang dapat melakukan autentikasi komunikasi antara perangkat dan jaringan. *Virtual private network* ini akan menciptakan sebuah "terowongan" yang sudah terenkripsi sehingga aman untuk menghubungkan perangkat dengan jaringan internet.

8. *Web Security*

   Merupakan sebuah skema keamanan yang diperlukan untuk memastikan penggunaan *website* yang aman saat terhubung ke dalam jaringan *internal*. *Web security* ini membantu untuk mencegah dari serangan berbasis *website* yang menggunakan *browser* sebagai titik akses untuk masuk ke dalam jaringan.

9. *Security Information and Event Management* (SIEM)

   SIEM akan memberikan sebuah informasi kepada *IT Security* untuk mengetahui *record* yang terjadi di dalam *IT environment*

perusahaan. Dengan adanya SIEM akan membantu sebuah perusahaan dalam mengidentifikasi dan menanggapi berbagai macam serangan.

10. *Endpoint Security*

    Biasanya perangkat pribadi menjadi target serangan ketika pengguna menggunakan untuk mengakses jaringan. *Endpoint security* disini berfungsi sebagai perlindungan ketika terhubung dengan *remote device*.

11. *Network Segmentation*

    Network segmentation dapat meningkatkan sistem keamanan jaringan, dimana mampu membangun jaringan komputer menjadi beberapa bagian, hal ini memudahkan untuk mengontol bagaimana *traffic* yang mengalir di dalam jaringan[18].

C. Bentuk-bentuk Serangan Pada Jaringan

Ancaman yang membahayakan jaringan komputer tidak hanya terdapat dari satu ataupun dua akan tetapi banyak sekali bentuk serangan siber yang akan mengancam keamanan jaringan sekaligus dapat membahayakan keselamatan penggunanya di dunia nyata. Berikut bentuk-bentuk serangan pada jaringan antara lain:

1. *Probe*

   Probe merupakan sebuah usaha untuk mengakses sistem. Contoh *probing* yaitu percobaan *login* ke akun yang tidak digunakan. *Probing* dianalogikan menguji kenop-kenop pintu guna mencari pintu mana yang tidak dikunci sehingga dapat diakses dengan mudah.

2. *Trojan Horse*

   Trojan Horse merupakan program berbahaya yang berkamuflase sehingga terlihat normal dan dapat bekerja sesuai dengan keinginan si *attacker.*

3. *Packet Sniffer*

   Packet Sniffer merupakan program yang dapat menangkap data dari paket yang lewat di jaringan. Data yang dicuri berupa

username, password serta informasi penting lainnya yang terdapat di jaringan dalam bentuk *text.*

4. *Denial of Service* (DOS)

   Merupakan serangan untuk menghabiskan sumber daya dari perangkat jaringan komputer dimana berakibat layanan jaringan komputer menjadi terganggung[19].

5. *Eavesdropping*

   Serangan ini dilakukan oleh *attacker* agar mereka mampu memantau alur komunikasi atau transmisi data yang terdapat pada jaringan komputer. Contohnya penanaman penyadap suara pada jaringan komputer.

6. *Logic Bomb*

   Logic Bomb di program oleh orang dalam yang sudah paham akan seluk-beluk jaringan komputer yang terdapat di perusahaan. *Logic Bomb* akan bekerja secara normal akan tetapi mengandung unsur yang mencurigakan.

7. *Spoofing*

   Sebuah metode serangan yang bekerja untuk memalsukan pengguna agar dapat dipercaya dalam mengakses sebuah jaringan. Metode *spoofing* ini membutuhkan beberapa *tools* diantaranya URL *spoofing* yang akan bekerja dengan menampilkan URL palsu dan menyalahgunakan DNS *cache*.

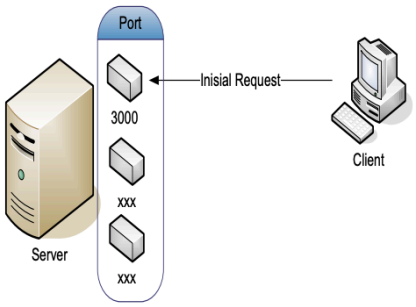
8. *Phishing*

   Metode *Phishing* bekerja dengan cara memancing korban supaya memberikan sebuah informasi atau data pribadinya. *Attacker* akan menyamar sebagai pihak yang tepercaya agar dapat menggunakan dan menyalahgunakan akun pengguna[20].

2.2.4 *Port Knocking*

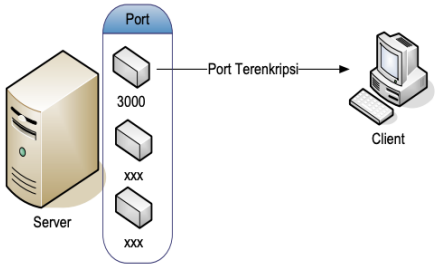
Port Knocking merupakan metode keamanan jaringan yang mempunyai maksud dan tujuan untuk membuka atau menutup akses *block* ke *port* dengan menggunakan *firewall* pada perangkat jaringan dengan mengirimkan paket atau koneksi tertentu[21]. Koneksi bisa berupa *protocol*

Transmission Control Protocol (TCP), *User Datagram Protocol* (UDP) maupun *Internet Control Message Protocol* (ICMP). Jika koneksi yang dikirimkan oleh *host* tersebut sudah sesuai dengan *rule port knocking* yang diterapkan, maka secara dinamis *firewall* akan memberikan akses ke *port* yang sudah di*block*. *Port knocking* bekerja seperti halnya brankas dengan kombinasi angka putar. *Port knocking* menggunakan sistem kombinasi lapisan kunci agar dapat mengamankan *port* komunikasi. Kunci disini merupakan *port-port* komunikasi itu sendiri. Untuk membuka kunci tersebut menggunakan cara dengan mengakses beberapa *port* yang memang sudah ditutup sebelumnya. Ketika *port* komunikasi tersebut diakses dengan kombinasi tertentu, maka akan terbuka sebuah *port* komunikasi baru yang bebas untuk diakses. Dengan cara ini, perangkat jaringan seperti *router* akan lebih aman, sebab admin jaringan bisa melakukan *blocking* terhadap *port-port* yang rentan terhadap serangan seperti *winbox* (8291), SSH (22), *Telnet* (23), atau *webfig* (80) [22]. Secara garis besar berikut untuk cara kerja dari metode *port knocking*:



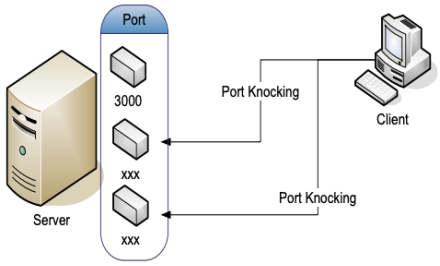
Gambar 2.12 Insial *Request*[23]

Pada Gambar 2.12 *Client* mengirimkan *request* komunikasi kepada *server* melalui *port* awal yang selalu terbuka untuk menerima *request* awal. *Port* yang digunakan merupakan *port* bebas seperti *port* 3000.



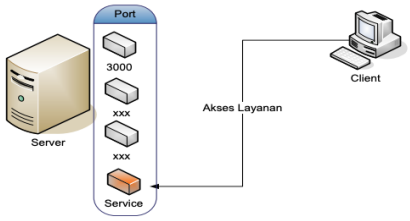
Gambar 2.13 *Server* mengirimkan urutan *port*[23]

Pada Gambar 2.13 *server* memeriksa hasil dekripsi dan jika *valid* maka *server* akan membangkitkan urutan *port* secara acak dan mengirimkannya kembali kepada *clie*nt dalam keadaan terenkripsi.



Gambar 2.14 *Client* melakukan komunikasi terhadap urutan *port* yang ditentukan[23]

Pada Gambar 2.14 *client* menerima urutan *port* terenkripsi yang kemudian mendekripsi urutan *port t*ersebut untuk memulai proses *port knocking* dengan melakukan komunikasi terhadap *port* yang ditentukan.



Gambar 2.15 *Client* terautentikasi dan dapat mengakses layanan *server*[23]

Pada Gambar 2.15 *server* secara aktif memantau komunikasi yang dilakukan oleh *client* dimana jika urutan komunikasi yang dilakukan oleh *client* telah *valid* maka *server* akan memberikan akses kepada *client* untuk melakukan komunikasi terhadap *port* layanan yang diminta oleh *client* [23].

2.2.5 *Firewall*

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas *firewall* adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. *Firewall* bertanggung jawab untuk memastikan bahwa *access control policy* yang diikuti oleh semua pengguna didalam jaringan tersebut, *firewall* sama seperti alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun tidak seperti alat-alat jaringan lain, sebuah *firewall* harus mengontrol lalu lintas *network* dengan memasukkan faktor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah apa yang seperti terlihat. *Firewall* digunakan untuk mengontrol akses antara *network internal* sebuah organisasi Internet, sekarang ini *firewall* semakin menjadi fungsi standar yang ditambahkan untuk semua *host* yang berhubungan dengan *network*[24].

2.2.6 *Port Scanning*

Port Scanning adalah tahapan awal untuk mendeteksi port-port yang terbuka dan mendapatkan informasi dari port yang terbuka pada target, servis apa yang sedang dijalankan, versi dari server dan lain sebagainya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan *firewall* atau tidak) dan seterusnya[25].

2.2.7 Mikrotik RouterOS

Mikrotik RouterOS yang tertera pada Gambar 2.16 merupakan sistem operasi berbasis Linux yang digunakan untuk menjadikan PC berbasis Intel atau AMD (*personal computer*) mampu melakukan beberapa fungsi di dalamnya yaitu *router, bridge, firewall, pengaturan bandwidth, wireless Access Point* atau *Client* dan fungsi *networking* serta beberapa fungsi *server,* sehingga cocok untuk routing jaringan atau internet di perkantoran bahkan juga digunakan oleh ISP dan provider *hospot.* Administrasinya biasanya dilakukan melalui *Windows Application*

(Winbox), selain itu untuk instalasi dapat dilakukan pada standar komputer PC, PC yang akan dijadikan *router* Mikrotik tidak memerlukan *resource* yang tinggi untuk penggunaan standar, misalnya hanya sebagai *gateway*[26]. Sejarah mikrotik awalnya dimulai saat dua orang ahli jaringan, yaitu John Trully dan Arnis Riekstins berhasil membuat *routing* ke jaringan yang lebih luas, sehingga hal ini menjadi visi dari mikrotik sampai saat ini yaitu *"Routing The World"*. John Trully berkebangsaan Amerika, tetapi bermigrasi ke Latvia, sebuah negara yang menjadi tetangga Rusia, bersama dengan Arnis Riekstins asli Latvia, mereka bekerja sama untuk membuat sebuah perangkat yang benar-benar dapat diandalkan untuk pekerjaan *routing* jaringan. Dimulai dengan membuat mikrotik yang bebasis kernel linux, mereka berdua membangun sebuah ISP dengan kecepatan 2 *Mbps* yang bernama Aeronet, di Maldova, sebuah negara tetangga dengan Latvia, dan setelah itu mereka mampu melayani 5 pelanggannya di Latvia. Dari sinilah sistem operasi mikrotik dikembangkan, di mana pada awal visi mereka untuk membuat sebuah *router* yang handal dan dapat di-*install* dengna mudah pada komputer biasa dan memiliki fitur serta fasilitas yang cukup lengkap. Fitur-fitur yang disediakan pada mikrotik diantaranya adalah sebagai berikut:

1. *Firewall* dan NAT;
2. *Routing-Static;*
3. *Hospot;*
4. *Point-to-Point tunneling protocols;*
5. *Simple tunnels;*
6. *IPSec;*
7. *Web Proxy;*
8. *Caching DNS Client;*
9. DHCP;
10. VRRP;
11. *Monitoring/Accounting* dan *Tools* jaringan lainnya[27].

Gambar 2.16 *Router OS Mikrotik* [28]

2.2.8 Quality of Service (QoS)

Quality of Service (QoS) adalah metode pengukuran yang digunakan untuk menentukan kapabilitas jaringan, seperti aplikasi jaringan, host, atau router untuk menyediakan layanan jaringan yang lebih baik dan lebih terencana yang memenuhi kebutuhan layanan.

A. *Throughput*

Throughput adalah kecepatan data yang terukur dalam ukuran waktu saat mentransmisikan berkas. *Throughput* bersifat dinamis bergantung pada trafik yang sedang terjadi. Untuk persamaan *throughtput* dapat dilihat pada 2.1 dan dalam menentukan performasi kualitas jaringan nilai *throughput* berdasarkan standarisasi TIPHON dapat diliat dalam Tabel 2.2.

$$Throughput = \frac{Jumlah\ data\ yang\ dikirim}{Waktu\ pengiriman\ data} \quad \text{.....(2.1)}$$

Tabel 2.2 Performasi Jaringan Berdasarkan *Throughput* [29]

Kategori *Throughput*	*Throughput*	Indeks
Bad	0 – 338 Kbps	0
Poor	338 – 700 Kbps	1
Fair	700 – 1200 Kbps	2
Good	1200 Kbps – 2,1 Mbps	3
Excelent	>2,1 Mbps	4

B. *Delay*

Delay merupakan waktu yang dibutuhkan data untuk menempuh jarak hingga terkirimnya paket. *Delay* dalam jaringan terdiri dari *delay processing, delay jitter buffer*, dan *delay network.* Untuk persamaan

delay dapat dilihat pada 2.2 dan dalam menentukan performasi kualitas jaringan nilai *delay* berdasarkan standarisasi TIPHON dapat diliat dalam Tabel 2.3.

$$Rata - rata\ Delay/Paket = \frac{total\ delay}{total\ paket\ diterima} \text{.....(2.2)}$$

Tabel 2.3 Performasi Jaringan Berdasarkan *Delay* [29]

Kategori *Delay*	*Delay* (ms)	Indeks
Poor	<450 ms	1
Medium	300 – 450 ms	2
Good	150 – 300 ms	3
Perfect	>150 ms	4

C. *Packet Loss*

Packet loss merupakan parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena *collision* dan *congestion* pada jaringan. Beberapa penyebab terjadinya *packet loss* yaitu *overload* trafik jaringan, tabrakan *(congestion)* pada jaringan, *error* pada media fisik, kegagalan disisi penerima yang disebabkan karena *overflow* pada *buffer*. Untuk persamaan *packet loss* dapat dilihat pada 2.3 dan dalam menentukan performasi kualitas jaringan nilai *packet loss* berdasarkan standarisasi TIPHON dapat diliat dalam Tabel 2.4.

$$Packet\ Loss = \frac{Paket\ dikirim - Packet\ diterima}{Paket\ dikirim}\ x\ 100\% \text{.....(2.3)}$$

Tabel 2.4 Performasi Jaringan Berdasarkan *Packet Loss*[29]

Kategori *Packet Loss*	*Packet Loss* (%)	Indeks
Poor	>25 %	1
Medium	15 – 24 %	2
Good	3 – 14 %	3
Perfect	0 – 2 %	4

D. *Jitter*

Jitter merupakan perubahan variasi *delay* pada suatu periode, *jitter* juga disebut gangguan komunikasi digital atau analog yang disebabkan oleh perubahan sinyal karena referensi posisi waktu. Beberapa penyebab *jitter,* yaitu panjangnya antrian dalam waktu pengolahan data, meningkatnya trafik secara tiba-tiba yang berakibat penyempitan *bandwith*, kecepatan kirim dan terima paket dari setiap titik [29]. Untuk persamaan *jitter* dapat dilihat pada 2.4 dan dalam menentukan performasi kualitas jaringan nilai *jitter* berdasarkan standarisasi TIPHON dapat diliat dalam Tabel 2.5.

$$Rata - rata\ Jitter/Paket = \frac{Total\ Jitter}{Total\ Paket\ Diterima} \quad \text{.....(2.4)}$$

Tabel 2.5 Performasi Jaringan Berdasarkan *Jitter* [29]

Kategori Jitter	***Jitter* (ms)**	**Kualitas**
Poor	125 - 225 ms	1
Medium	75 ms – 125 ms	2
Good	0 ms – 75 ms	3
Perfect	0 ms	4