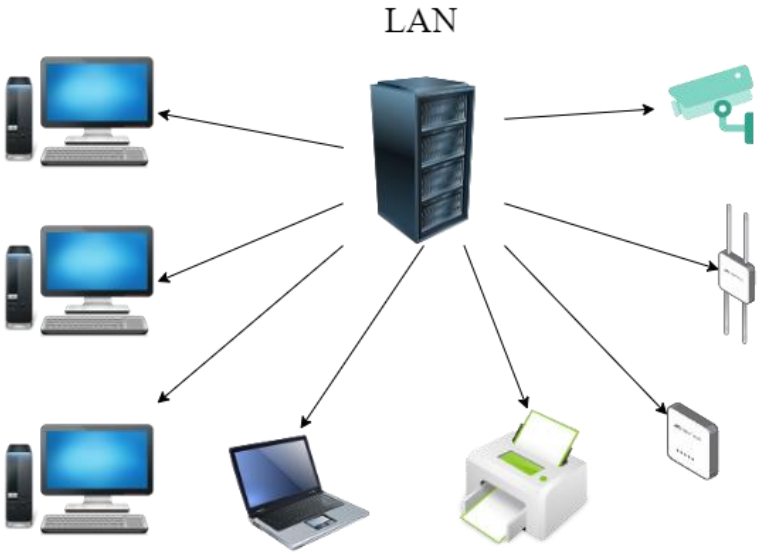
BAB II
TINJAUAN PUSTAKA

2.1 Pengertian Jaringan Komputer

Jaringan komputer merupakan kumpulan dari beberapa perangkat komputasi, printer serta perangkat keras lainnya dengan media konektivitas yang terhubung dan berinteraksi satu sama lain. konektivitas adalah media penghubung yang berupa kabel (*wire)* atau nirkabel (*wireless*) (Sumardi and Zaen, 2018).

2.1.1 *Local Area Network* (LAN)

Menurut (Wongkar, Sinsuw and Najoan, 2015) LAN adalah singkatan dari *Local Area Network.* Jaringan ini merupakan jaringan komputer yang hanya mencakup area kecil jaringan, yaitu seperti gedung, kantor, rumah dan sekolah yang membutuhkan hubungan atau koneksi antara dua komputer atau lebih dalam suatu ruangan seperti pada Gambar 2.1.

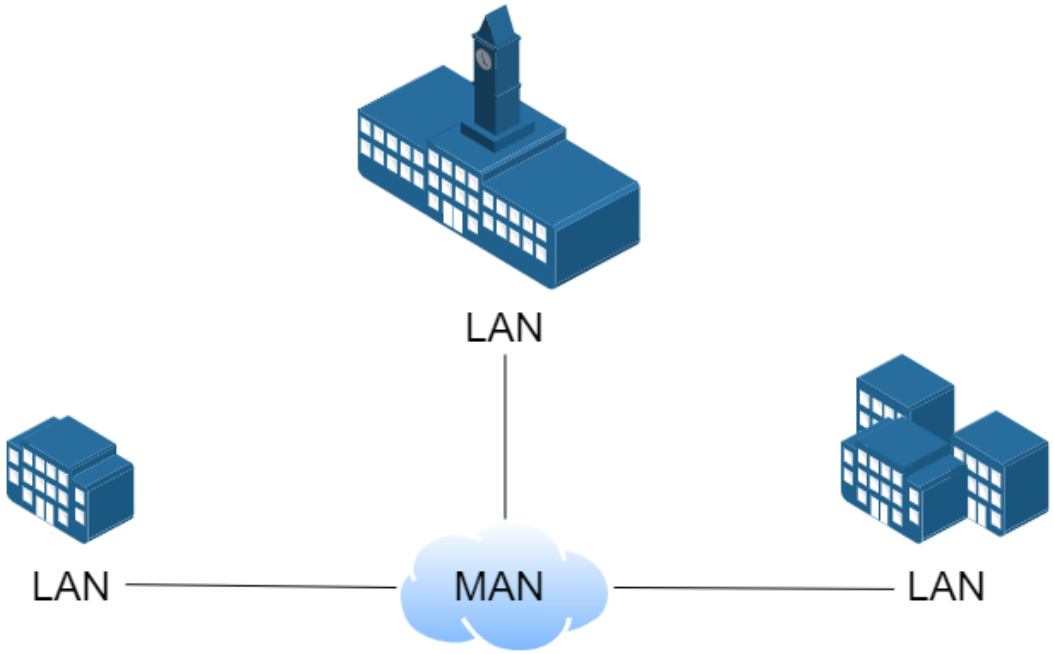


Gambar 2.1 LAN (*Local Area Network*)

2.1.2 *Metropolitan Area Network* (MAN)

Menurut (Wongkar, Sinsuw and Najoan, 2015) MAN singkatan dari *Metropolitan Area Network*. Jenis jaringan komputer MAN ini adalah suatu jaringan komputer dalam suatu kota dengan transfer data berkecepatan tinggi yang menghubungkan suatu lokasi antar gedung seperti sekolah, kampus, perkantoran

dan pemerintahan. Jaringan MAN juga merupakan gabungan dari beberapa jaringan LAN. Cakupan dari jaringan MAN ini bisa mencapai 10 – 50 km dapat dilihat pada Gambar2.2.

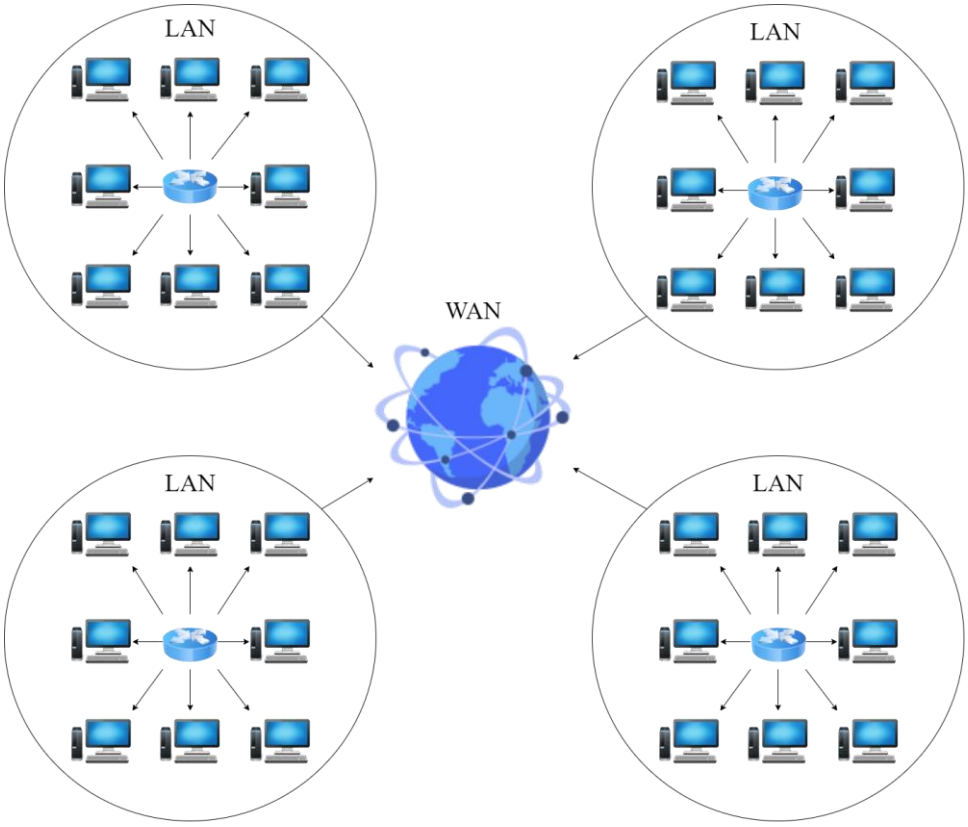


Gambar 2.2 MAN (*Metropolitan Area Network*)

2.1.3 *Wide Area Network* (WAN)

Wide Area Network (WAN) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota, atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik, seperti yang terlihat pada gambar 2.3 (Haqqi *and* Badrul, 2016).

WAN meliputi area geografi yang lebih luas lagi, yang meliput suatu negara atau dunia. WAN digunakan untuk menghubungkan banyak LAN yang secara gografis terpisah. WAN dibuat dengan cara menghubungkan LAN menggunakan layannan seperti *Leased Line*, *dial-up*, satelit atau layanan paket *carrier*. Umumnya jaringan ditempatkan pada banyak lokasi yang berbeda . Dengan WAN, Universitas yang ada di Jayapura dapat berkomunikasi dengan Universitas yang ada di Australia dalam beberapa menit saja tanpa mengeluarkan biaya yang banyak.



Gambar 2.3 WAN (*Wide Area Network*)

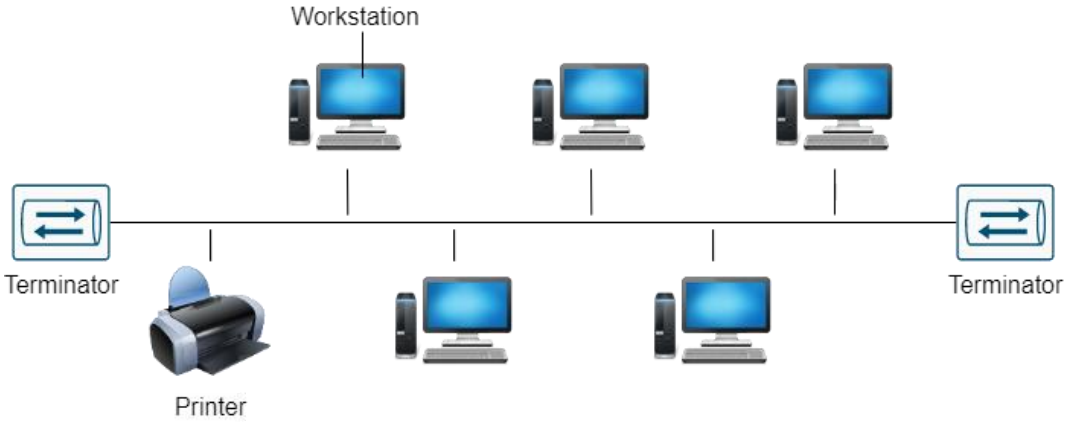
2.2 Topologi Jaringan

Menurut (Sari, Sulistiyono and Kemala, 2020) istilah topologi pada dasarnya berarti bentuk dan istilah topologi jaringan mengacu pada bentuk jaringan, yaitu cara semua titik jaringan yang saling berhubungan dengan menggunakan kabel atau nirkabel. Topologi jaringan memiliki beberapa jenis dan tingkat kinerja yang beragam. Berikut merupakan jenis dari topologi jaringan komputer.

2.2.1 Topologi *Bus*

Topologi *Bus* merupakan topologi di mana node terhubung bersama dalam satu garis. Untuk memahami bagaimana sebuah topologi bus yang berfungsi adalah menganggap seluruh jaringan sebagai satu kabel, dengan masing-masing node tersambung ke kabel sehingga dapat mengalirkan paket yang dikirim melalui kabel. Setiap node mengetahui setiap paket untuk menentukan apakah paket tersebut ditujukan untuknya. Jika demikian, node mengklaim paket tersebut. Jika tidak, node mengabaikan paket. Dengan cara ini, setiap komputer dapat menanggapi data yang dikirim dan mengabaikan data yang dikirim ke komputer

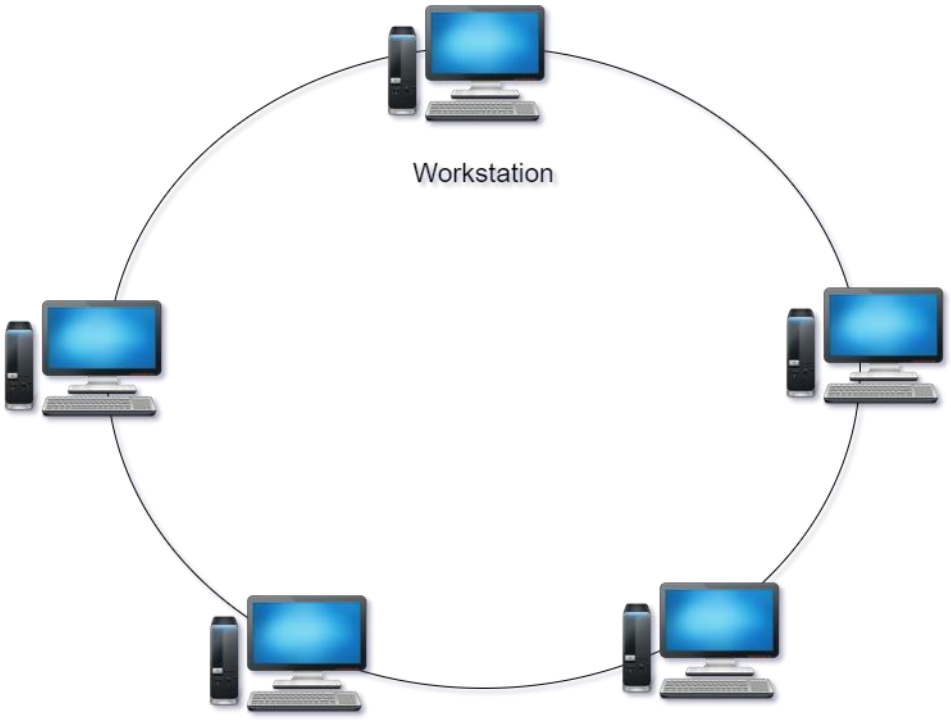
lain dalam jaringan. Selain nama *BUS*, topologi ini juga dikenal dengan nama topologi *backbone*, seperti yang terlihat pada gambar 2.4, yaitu berupa beberapa komputer yang dikoneksikan ke sebuah kabel coaxial yang menjulur panjang. Jika kabel dalam jaringan *BUS* putus, seluruh jaringan secara efektif dinonaktifkan (Ardhiansyah, Noris *and* Adrianto, 2020).



Gambar 2.4 Topologi *Bus*

2.2.2 Topologi *Ring*

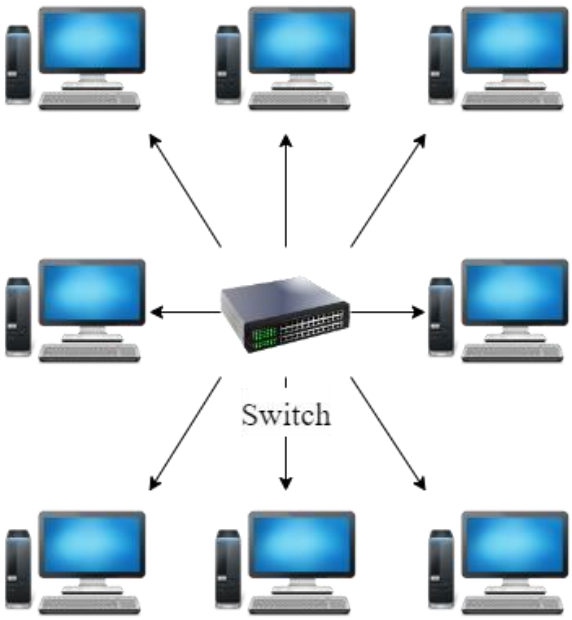
Topologi *Ring* dapat juga disebut dengan topologi cincin. Dalam topologi *ring*, paket dikirim mengelilingi lingkaran dari komputer ke komputer lain. Setiap komputer mengetahui setiap paket untuk memutuskan apakah paket itu ditujukan untuknya, Jika tidak, paket tersebut diteruskan ke komputer berikutnya dalam lingkaran *ring*. Topologi ring dikenal juga dengan nama topologi cincin dikarenakan konfigurasinya berbentuk menyerupai cincin, dapat dilihat pada gambar 2.5. Topologi *ring* adalah untaian media transmisi (berupa kabel) dari komputer yang satu ke komputer lain sampai membentuk sebuah lingkaran, dan jalur transmisinya hanya berupa satu arah (Ardhiansyah, Noris and Adrianto, 2020).



Gambar 2.5 Topologi *Ring*

2.2.3 Topologi *Star*

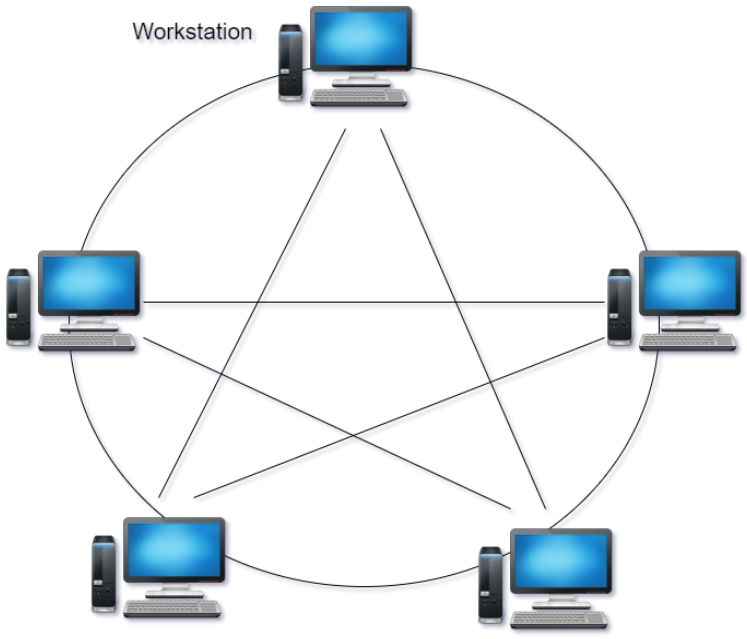
Topologi *star* adalah topologi jaringan yang mirip dengan simbol bintang karena setiap perangkat dihubungkan secara langsung menggunakan kabel UTP (*Unshielded Twisted Pair*) ke sebuah node pusat seperti *Hub/Switch* yang mengontrol lalu lintas data. mekanisme pada topologi ini akan mengirimkan sebuah data secara langsung dari node pusat ke perangkat yang diinginkan tanpa melalui perangkat lainnya. Kelebihan pada topologi ini yaitu mudah untuk mendeteksi masalah jaringan pada setiap perangkat yang terhubung dalam topologi star. Sedangkan kekuranganya yaitu membutuhkan banyak kabel dalam pemasangannya dan kestabilan jaringan bergantung pada node pusat, sehingga jika *Hub/Switch* mengalami gangguan maka seluruh jaringan akan terganggu (Hidayat and S, 2020).



Gambar 2.6 Topologi *Star*

2.2.4 Topologi *Mesh*

Topologi *mesh* mempunyai banyak koneksi antara masing-masing node di jaringan. Keuntungan topologi ini yaitu ketika ada kabel yang terputus, jaringan bisa memakai rute lain sebagai alternatif untuk mengirimkan paket datanya.



Gambar 2.7 Topologi Mesh

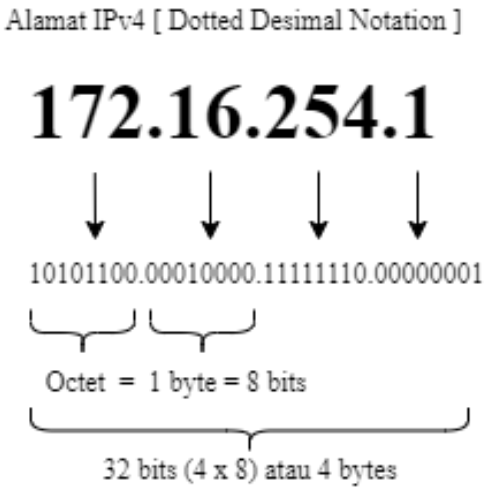
Jaringan *mesh* merupakan salah satu topologi jaringan yang cukup rumit dalam pengaturan LAN. Sebagai contoh, untuk jaringan lima komputer dalam topologi *mesh*, masing-masing komputer harus mempunyai lima *network interface card* atau kartu antarmuka jaringan. Selain itu, diperlukan jumlah kabel yang lebih banyak untuk menghubungkan setiap komputer ke 5 komputer lain dalam jaringan, seperti yang terlihat pada gambar 2.7 diatas. Jelas, skema ini tidak terlalu skalabel.

Secara umum topologi ini sengaja dibuat pada jaringan dengan skala yang tidak terlalu besar. Jaringan ini memakai router untuk merutekan paket dari jaringan yang satu ke jaringan yang lainnya. Untuk alasan kemampuan dan kinerja, router biasanya dikonfigurasi sedemikian rupa sehingga menyediakan banyak jalur antara dua simpul pada jaringan dalam pengaturan yang menyerupai mesh. Karena begitu banyak yang bisa salah bahkan dengan jaringan yang sederhana menunjuk satu orang sebagai administrator jaringan itu penting. Dengan cara ini, seseorang bertanggung jawab untuk memastikan bahwa jaringan tidak berantakan atau lepas kendali (Ardhiansyah, Noris and Adrianto, 2020).

2.3 IP *Address*

IP *Address* merupakan pengenal yang digunakan untuk memberi alamat pada tiap-tiap komputer dalam jaringan (Fadhilah, Supendar and Sw, 2021). IP *address* bisa dianalogikan seperti sebuah alamat rumah. Ketika sebuah datagram dikirim, informasi alamat inilah yang menjadi acuan datagram agar bisa sampai ke perangkat yang dituju.

IP *Address* terbagi dalam 2 versi, IPv4 dan IPv6. Sebuah IP *address* versi 4 atau IPv4 terbentuk dari 32 *binary bits*. Dari 32 *binary bits* tersebut terbagi lagi menjadi 4 *octet* (1 *octet* = 8 *bits*). Nilai tiap oktet diatara 0 sampai 255 dalam format desimal, atau 00000000 - 11111111 dalam format *binary*. Setiap octet dikonversi menjadi desimal dan dipisahkan oleh tanda titik (*dot*). Sehingga format akhir IP *address* biasanya berupa angka desimal yang dipisahkan dengan tanda titik (Sari, Sulistiyono and Kemala, 2020).



Gambar 2.8 IP *Address*

2.3.1 IP *Public*

Menurut (Sari, Sulistiyono and Kemala, 2020) IP *Adresss Public* merupakan alamat-alamat IP yang disediakan untuk digunakan pada jaringan internet. Karena kelas IP *address* ini digunakan di dalam jaringan internet maka IP ini bisa diakses melalui jaringan internet secara langsung. Perangkat yang menggunakan IP *public*, seperti *web server*, *mailserve*r, *DNS server*, *game server* ataupun perangkat lain dapat diakses dari jaringan manapun di dunia ini yang terkoneksi ke internet. Untuk dapat menggunakan IP *public*, suatu organisasi biasanya dapat mendaftarkan diri ke salah satu ISP (*Internet Service Provider*).

2.3.2 IP *Private*

IP *Private* merupakan alamat-alamat IP *Address* yang disediakan untuk digunakan pada jaringan lokal (LAN). IP *private* dapat terhubung ke internet jika router yang digunakan mempunyai kemampuan untuk melakukan NAT (*Network Address Translation*) agar semua *device* dengan IP *private* dapat terkoneksi ke internet dengan menggunakan IP *public* yang terkoneksi langsung ke internet. Meskipun sudah terkoneksi ke internet, IP *private* tetap tidak bisa diakses langsung dari jaringan internet.

2.4 OSI *Layer*

Lapisan OSI merupakan referensi model yang digunakan untuk memahami jaringan komputer secara umum. Lapisan OSI telah dijadikan sebagai acuan saat

mempelajari jaringan yang dibangun (Ariyadi, 2018). *Open Systems Interconnection Model* (OSI) dimasukkan dalam standar ISO 7489 dan dirilis pada tahun 1984. ISO adalah singkatan dari *International Organization for Standardization*. Model referensi OSI juga disebut model tujuh lapis. Ketujuh lapisan dari bawah ke atas adalah sebagai berikut:

- Lapisan fisik: mentransmisikan aliran bit antar perangkat dan mendefinisikan spesifikasi fisik seperti *level* listrik, kecepatan, dan pin kabel.
- Lapisan tautan data: merangkum bit menjadi oktet dan oktet ke dalam bingkai, menggunakan alamat MAC untuk mengakses media, dan mengimplementasikan pemeriksaan kesalahan.
- Lapisan jaringan: mendefinisikan alamat logis untuk router untuk menentukan jalur dan mengirimkan data dari jaringan sumber ke jaringan tujuan.
- Lapisan transportasi: mengimplementasikan transmisi data berorientasi koneksi dan non-koneksi, serta pengecekan kesalahan sebelum transmisi ulang.
- Lapisan sesi: menetapkan, mengelola, dan mengakhiri sesi antara entitas di lapisan presentasi. Komunikasi pada lapisan ini diimplementasikan melalui permintaan layanan dan tanggapan yang dikirimkan antar aplikasi pada perangkat yang berbeda.
- Lapisan presentasi: menyediakan pengkodean dan konversi data sehingga data yang dikirim oleh lapisan aplikasi dari satu sistem dapat diidentifikasi oleh lapisan aplikasi dari sistem lain.
- Lapisan aplikasi: menyediakan layanan jaringan untuk aplikasi dan lapisan OSI yang paling dekat dengan pengguna akhir.

2.5 TCP/IP

TCP/IP atau biasa disebut dengan *Tranmission Control Protocol/Internet Protocol* merupakan dua protokol jaringan komputer yang terpisah dan memiliki fungsi yang berbeda, namun kedua protokol ini saling berkaitan dan mempunyai tujuan yang sama yaitu memungkinkan hubungan *virtual* antar komputer, dimana

dua komputer atau lebih akan dapat saling berhubungan untuk pertukaran data serta layanan aplikasi jaringan lainnya (Yunus and M. As'Ad, 2012).

IP mendefinisikan alamat tujuan pengiriman data dan TCP bertanggung jawab untuk pengiriman data setelah alamat IP ditemukan (Fariza, 2021).

2.6 UDP

UDP atau biasa dikenal dengan *User Datagram Protocol* adalah protokol yang mentransmisikan paket data terlepas dari kontrol kemacetan dan koreksi kesalahan data dalam jaringan. Namun, karena kecepatan transfer data tidak dapat dikontrol, protokol UDP akan menghabiskan bandwidth jaringan. Sehingga, UDP dapat lebih unggul dalam hal kecepatan transfer dibandingkan dengan TCP.

Berbeda dengan TCP, protokol UDP adalah protokol yang bersifat *connectionless* dalam mentransmisi data dan tidak mengenal dalam pengecekan terhadap error pengiriman data (Mardiana and Sahputra, 2017).

2.7 *Subnetting*

Subnetting adalah proses memecah atau membagi jaringan menjadi banyak jaringan yang lebih kecil, atau *subnetting* adalah teknik yang memungkinkan administrator jaringan untuk menggunakan alamat IP 32-bit yang tersedia secara lebih efisien. Tujuan subnetting ialah sebagai berikut.

1. Untuk mengefisienkan jumlah host dalam jaringan kecil dimana jumlah hostnya tidak sampai 254 buah.
2. Untuk mengurangi kepadatan lalu lintas jalur data pada jaringan.
3. Untuk membuat lebih efisien alokasi IP *Address* dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP *Address*.
4. Untuk mengatasi masalah perbedaan antara hardware dengan topologi fisik jaringan.

2.8 VPN (*Virtual Private Network*)

2.8.1 Pengertian VPN

VPN (*Virtual Private Network*) adalah suatu teknologi komunikasi yang digunakan untuk menghubungkan koneksi antara sebuah jaringan dengan jaringan yang lain secara pribadi melalui internet atau suatu jaringan pribadi yang dibuat dengan menggunakan jaringan publik (Zarkasyi *et al.*, 2018b). Dengan

menggunakan jaringan publik seseorang dapat bergabung kedalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti ketika berada di dalam jaringan lokal tersebut.

VPN dapat terjadi antara dua buah PC atau bisa juga antara dua atau lebih jaringan yang berbeda. VPN dibentuk dengan membangun sebuah terowongan dan enkripsi. Secara umum proses pengiriman data akan dienkapsulasi dengan mengguanakan header yang berisi informasi *routing* untuk mendapatkan koneksi secara *point to point*, data dapat melewati jaringan publik dan mencapai pada tujuan akhir. Sedangkan saat menggunakan VPN, proses pengiriman data akan dienkripsi terlebih dahulu agar isi paket yang tertangkap saat melewati jarinangan publik tidak dapat terbaca karena isi paket yang dikirimkan harus melewati proses dekripsi. VPN memiliki tiga fungsi utama dalam penggunaannya yakni:

1. *Confidentialy* (Kerahasiaan)

   VPN memiliki salah satu sistem kerja untuk mengenkripsi semua data yang ditransmisikan melaluinya. Dengan adanya enkripsi data, maka kerahasiaan data menjadi lebih terjaga sehingga biarpun ada pihak yang ingin menyadap data yang terlintas saat proses transmisi data berlangsung, belum tentu pihak tersebut bisa membaca isi dari data yang ditransmisikan dengan mudah, karena data tersebut sudah diacak.

2. *Data Integrity* (Integritas Data)

   Pada proses transmisi data, data yang dikirimkan akan melewati beberapa rute perjalanan hingga mencapai pada akhir tujuan yang ditentukan. Di tengah perjalanannya, apapun bisa terjadi pada isinya. Baik itu hilang, rusak bahkan dimanipulasi oleh pihak yang tidak diinginkan. VPN memiliki teknologi yang dapat menjaga keutuhan data yang ditransmisikan ke tujuannya tanpa cacat, hilang atau dimanipulasi oleh pihak yang tidak diinginkan.

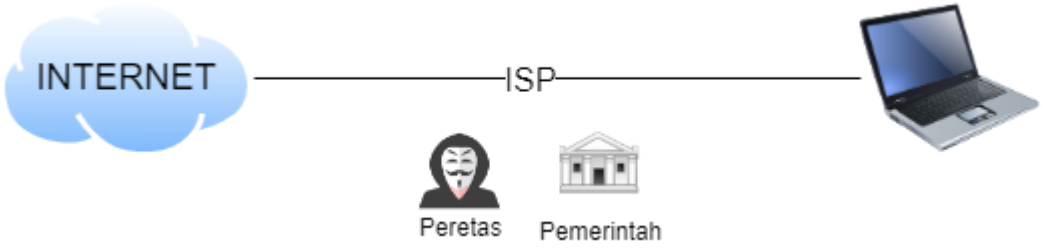
3. *Origin Authentication* (Autentikasi Sumber)

   Teknologi VPN memiliki autentikasi terhadap sumber pengirim. VPN akan melakukan pemeriksaan secara mendetail mengenai data yang masuk dan mengambil informasi dari mana datanya berasal. Kemudian akan diterima jika proses autentikasinya berhasil. Dengan demikian, VPN akan memastikan

bahwa data dikirim dari sumber yang jelas dan tidak ada data yang dirusak atau dimanipulasi oleh pihak yang tidak bertanggung jawab.

2.8.2 Cara Kerja VPN

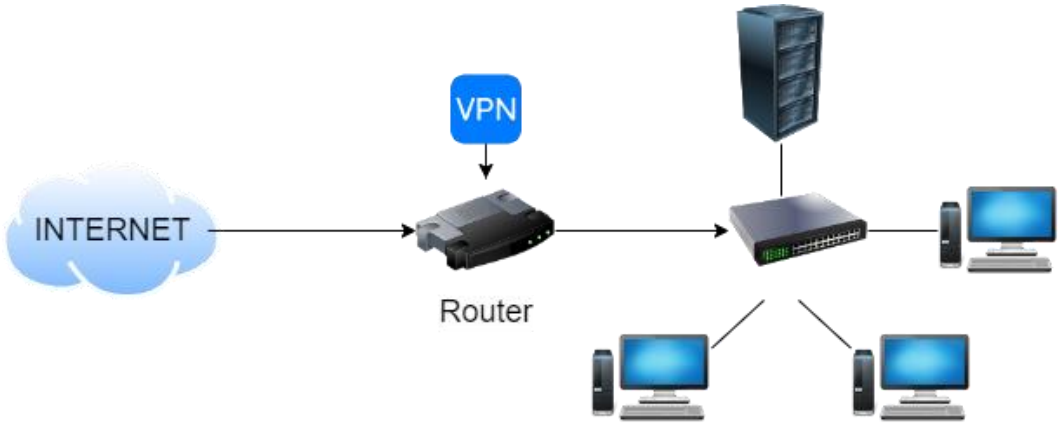
Cara kerja VPN sederhananya adalah melakukan enkripsi pertukaran data. VPN memberikan lapisan privasi dan anonimitas ekstra sehingga dapat menyembunyikan aktivitas komunikasi data agar tidak terbuka/terlacak. Berikut merupakan beberapa gambaran dari cara kerja sebuah teknologi VPN.



Gambar 2.9 Koneksi Internet Tanpa VPN

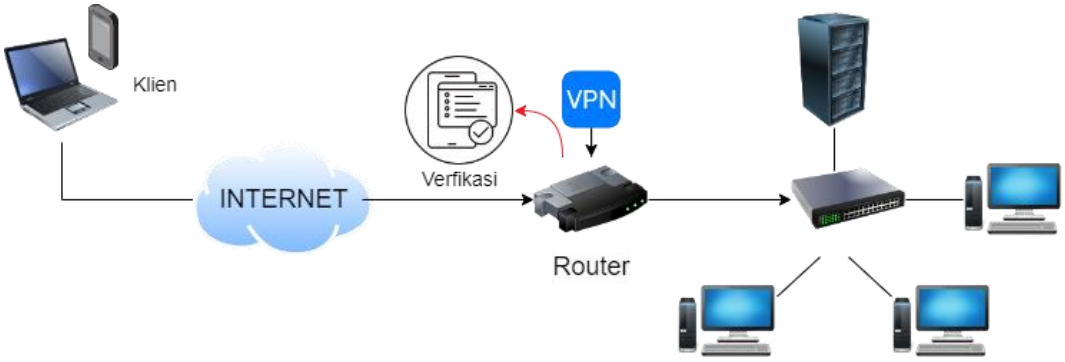
Pada Gambar 2.9 merupakan kondisi standar jika mengakses sebuah internet. Belum adanya enkrispsi dan aktivitas internet dapat terekam/dilihat oleh pihak ISP, pemerintah, peretas dan pihak ketiga lainnya. Kondisi ini sangat beresiko jika aktivitas internet yang menyangkut dengan sebuah data pribadi/ perusahaan yang bersifat sensitif atau penting.

Umumnya pada Gambar 2.10 VPN membutuhkan sebuah *server* serperti router dalam suatu jaringan lokal yang berfungsi sebagai media penghubung antar perangkat komputasi.



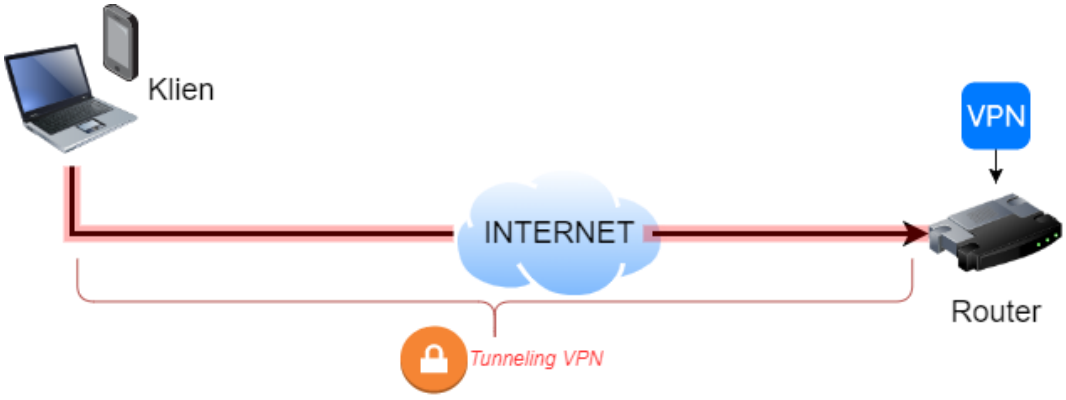
Gambar 2.10 *Server* VPN

Saat memulai koneksi dengan menggunakan VPN, perangkat komputer seperti laptop atau *smartphone* yang berperan sebagai klien akan mengontak dan melakukan autentikasi pada server VPN yang dituju melalui internet. Kemudian *server* VPN akan memverifikasi akun dari klien agar dapat terhubung kedalam *server* VPN. Gambar 2.11 menjelaskan proses koneksi dari klien ke *server* VPN.



Gambar 2.11 Proses Koneksi dari Klien ke *Server* VPN

Jika berhasil, maka klien akan menerima sebuah IP *Private* baru dari *server* VPN untuk menyembunyikan identitas asli dari perangkat klien. selanjutnya, akan terbentuk sebuah koneksi/*Tunneling* VPN yang akan mengenkripsikan seluruh aktivitas komunikasi data. Dapat dilihat pada Gambar 2.12.



Gambar 2.12 *Tunneling* VPN terhubung

2.8.3 Keuntungan menggunakan VPN

Ada beberapa keuntungan yang dapat diperoleh dengan menggunakan VPN yakni:

1. Jangkauan jaringan lokal yang dimiliki suatu perusahaan atau instansi akan menjadi lebih luas sehingga waktu yang dibutuhkan untuk

menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena pada saat proses instalasi infrastruktur jaringan yang dilakukan dari perusahaan atau instansi yang baru atau cabangnya yang baru dengan ISP terdekat di daerahnya.

2. Penggunaan VPN dapat mereduksi biaya operasional bila dibandingkan dengan penggunaan *leased line* jika ingin menghubungkan dua jaringan lokal yang berbeda dan jauh tempatnya. VPN dapat mengurangi biaya instalasi jaringan karna tidak membutuhkan kabel (*leased line)* yang panjang dan permanen. VPN menggunakan internet sebagai media komunikasinya, karena internet telah tersebar ke seluruh dunia dan internet digunakan sebagai media komunikasi publik yang terbuka.
3. VPN memberikan kemudahan terhadap pengguna untuk mengakses jaringan lokal suatu perusahaan atau instansi dimana saja, karena VPN terhubung ke internet. Selama pengguna memiliki akses internet ke ISP terdekatnya, pengguna dapat melakukan koneksi dengan jaringan khusus dari suatu perusahaan atau instansi.

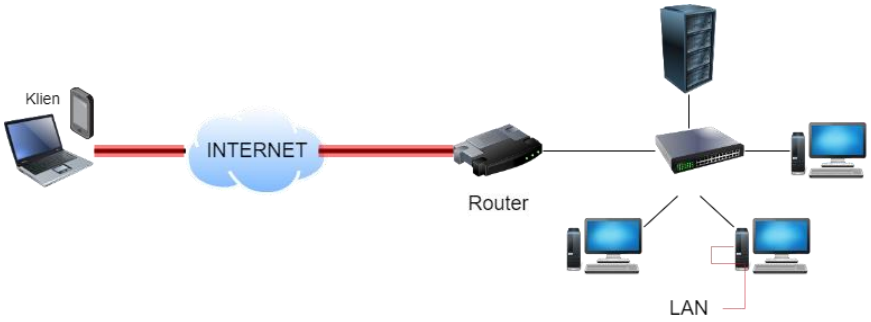
2.8.4 Kerugian menggunakan VPN

1. Ketersediaan dan peforma jaringan *private* pada suatu perusahaan atau instansi melalui internet sangat tergantung pada faktor-faktor yang berada diluar kendali pihak perusahaan atau instansi. Kecepatan dan keandalan transmisi data melalui internet yang digunakan sebagai media komunikasi jaringan VPN, tidak dapat diatur oleh pihak pengguna jaringan VPN.
2. Perangkat pembangun jaringan VPN dari beberapa vendor yang berbeda ada kemungkinan tidak dapat digunakan bersama-sama karna standar yang ada untuk VPN belum memadai. Oleh karena itu pemilihan perangkat yang sesuai dengan kebutuhan perusahaan atau instansi harus diperhatikan.

2.8.5 Jenis Implementasi VPN

1. *Remote Access* VPN

   Remote Access VPN atau biasa disebut juga dengan *Virtual Private Dial-up Network* (VPDN) adalah jenis VPN yang memungkinkan penggunanya untuk terhubung ke dalam jaringan lokal melalui internet. Jenis ini biasanya digunakan oleh karyawan untuk terhubung dengan aman ke jaringan kantor agar dapat mengakses file dan data perusahaan.

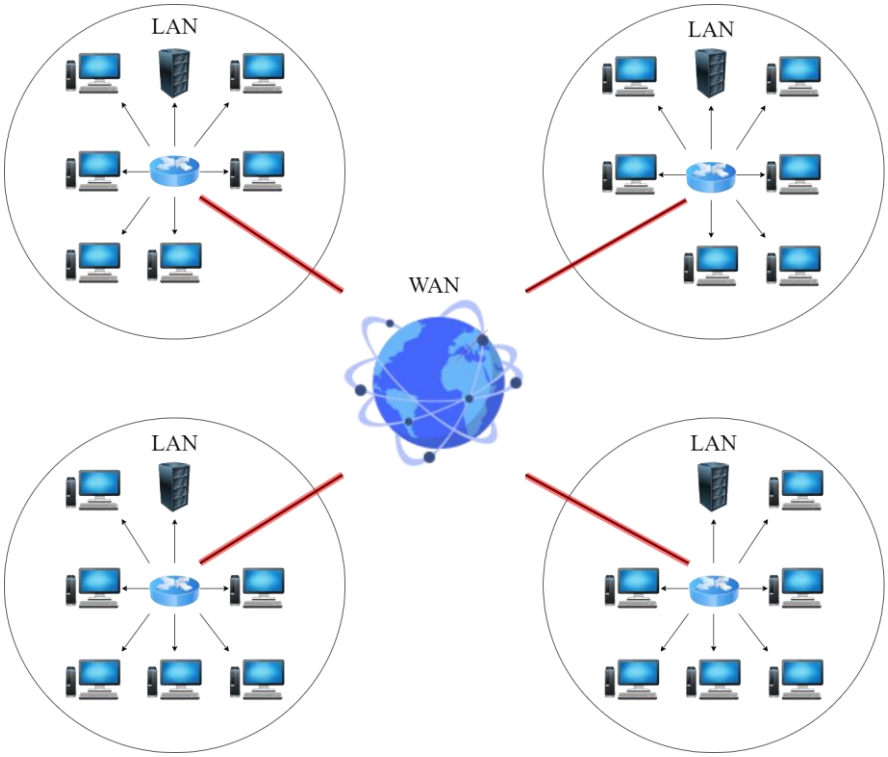


Gambar 2.13 *Remote access* VPN

   Jenis VPN ini sangat cocok untuk karyawan yang sedang WFH (*Work From Home*). pengguna dapat mengakses file kerja seolah-olah mereka berada di kantor. Enkripsi juga penting untuk melindungi data sensitif perusahaan atau instansi saat menggunakan hotspot Wi-Fi publik.

2. *Site to site* VPN

   Jenis implementasi ini menggabungkan dua jaringan lokal di lokasi yang berbeda. Contoh nya seperti pada *event* Pekan Olahraga Nasionl (PON) yang diselenggarakan di Papua pada tahun 2021 yang dimana jaringan lokal yang ada pada tiap *Venue* Cabang Olahraga di lokasi yang berbeda terhubung dengan pusat kendali utama.



Gambar 2.14 *Site to site* VPN

Banyak perusahaan global yang menggunakan kombinasi *site-to-site* VPN dan *remote access* VPN. *Site-to-site* VPN menggabungkan semua jaringan pribadi perusahaan di seluruh dunia, sedangkan *remote access* VPN memungkinkan karyawan mengakses jaringan lokal yang ada pada perusahaannya dalam satu waktu (Faradilla A, 2022).

2.8.6 Jenis-jenis Protokol VPN

VPN adalah teknologi jaringan yang menggunakan jaringan publik (Internet/WAN) untuk membangun koneksi yang aman/terenkripsi antar node jaringan. Contoh implementasi mengelola jaringan yang terdiri dari beberapa kantor di lokasi yang berbeda atau melakukan remote access secara jarak jauh ke dalam *server* jaringan kantor. VPN memiliki beberapa jenis protokol, seperti:

1. *Point to Point Tunnel Protocol* (PPTP)

   PPTP adalah protokol yang dikembangkan oleh sebuah konsorsium dimana microsoft adalah salah satu anggotanya, protokol ini dibuat sebagai salah satu implementasi VPN (Zarkasyi et al., 2018b). Sebagian besar sistem operasi didukung sebagai klien PPTP, baik sistem operasi di PC maupun *gadget*

seperti Android. Komunikasi PPTP menggunakan protokol TCP *port* 1723, dan menggunakan IP *Protocol* 47/GRE untuk enkapsulasi paket datanya. Pada konfigurasi PPTP, protokol keamanan jaringan yang digunakan untuk proses autentikasi PPTP pada Mikrotik, seperti pap,chap,mschap dan mschap2. Kemudian setelah *tunnel* terbentuk, data yang ditransmisikan akan dienkripsi menggunakan *Microsoft Point-to-Point Encryption* (MPPE) (Mikrotik, 2020).

2. *Layer* 2 *Tunnel Protocol* (L2TP).

   L2TP adalah sebuah *tunneling* protokol yang memadukan dan mengombinasikan dua buah *tunneling* protokol, yaitu L2F (*layer 2 forwarding*) yang dikembangkan oleh cisco system dan PPTP (*Point-to-Point Tunneling Protocol*) (Sinurat, 2013). Protokol keamanan jaringan dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP *port* 1701. L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. Contohnya untuk *Operating system* Windows, secara *default* OS Windows menggunakan L2TP/IPSec. Akan tetapi, konsekuensinya tentu saja konfigurasi yang harus dilakukan tidak se-*simple* PPTP. Sisi *client* pun harus sudah *support* IPSec ketika menerapkan L2TP/IPSec (Mikrotik, 2020). Saat *tunnel* terbentuk data yang ditransmisikan akan dienkripsi menggunakan jenis enkripsi sha1 dan aes.

3. *Secure Socket Tunneling Protocol* (SSTP)

   Secure Socket Tunneling Protocol adalah salah satu protokol VPN yang tersedia di *platform* Microsoft. Protokol ini didasarkan pada kombinasi teknologi SSL dan TCP (Farly, Najoan *and* Lumenta, 2017). Protokol ini memerlukan sertifikat SSL di masing-masing perangkat, kecuali keduanya menggunakan RouterOS. Komunikasi SSTP menggunakan TCP *port* 443 (SSL), sama hal nya seperti website yang *secure* (HTTPS). Namun belum semua OS *support* dengan protokol SSTP (Mikrotik, 2020).

4. *Open*VPN

Secara *default*, *Open*VPN adalah protokol yang menggunakan UDP *port* 1194 dan memerlukan *certificate* pada masing-masing perangkat agar bisa saling terkoneksi dalam jaringan *private*. *Open*VPN dapat dibangun pada semua OS dengan bantuan aplikasi pihak ketiga dan *Open*VPN menggunakan algoritma enkripsi sha1 dan md5 untuk proses otentikasi dan menggunakan beberapa *chiper* yaitu, blowfish128, aes128, aes192 dan aes256.

2.9 Enkripsi VPN

Enkripsi adalah proses mengubah sebuah informasi atau data menjadi sebuah kode yang tidak beraturan. Tujuan enkripsi adalah untuk mencegah akses yang tidak sah dan melindungi informasi dan kerahasiaan data agar tidak sampai terhadap orang yang tidak diinginkan dalam sebuah jaringan atau internet (SJ, 2022). Enkripsi adalah komponen inti dari VPN. Saat melakukan *Tunneling,* VPN akan mengenkripsi seluruh data yang melewati perangkat pengguna VPN ke *server* penyedia VPN sehingga seluruh aktivitas komunikasi data tetap terjaga dari pandangan pihak ketiga (ISP, Pemerintah dan Peretas).

2.9.1 Metode Enkripsi VPN

Secara garis besar ada 2 metode pengenkripsian data yaitu *symmtric cryptography* dan *asymmetric cryptography.*

1. *Symmtric Cryptography*

   Teknik *Cryptography* ini merupakan teknik yang sangat sederhana dengan cara menggunakan sebuah *key* atau kunci untuk mendekripsi sebuah teks hasil sebuah enkripsi (*ciphertext).*

   Pada algorima *symmetric key,* pengirim dan penerima harus memiliki kunci yang digunakan bersama dan dijaga kerahasiaannya. Pengirim menggunakan kunci untuk enkripsi dan penerima menggunakan kunci yang sama untuk dekripsi.

2. *Asymmetric Cryptography*

   Teknik *cryptography asymmetric* merupakan teknik yang menggunakan 2 buah kunci untuk mendekripsi sebuah teks hasil sebuah enkripsi (*ciphertext)* yaitu *public key* dan *private key.*

   Dalam algoritma kunci asimetris, ada 2 kunci yang berbeda. *Public key* diterbitkan dan diizinkan bagi siapa saja pengirimnya untuk melakukan enkripsi. Sedangkan private key dirahasiakan oleh penerima dan digunakan untuk dekripsi (Putra, 2018).

2.9.2 Jenis Enkripsi VPN

Secara umum terdapat beberapa jenis enkripsi yang digunakan pada VPN. Berikut adalah daftar enkripsi yang digunakan pada VPN.

1. *Blowfish*

   Blowfish adalah tingkat perintis enkripsi VPN menggunakan teknik block cipher dengan kunci simetris. *Blowfish* memiliki ukuran blok 64 bit. Namun, tingkat enkripsi ini tidak mengamankan jumlah data pengguna yang lebih besar. Menariknya, OpenVPN menerapkan enkripsi *Blowfish* dengan enkripsi 256-bit AES tingkat militer.

2. 3DES (*Data Encryption Standard*)

   3DES (*Triple Data Encryption Standard*) adalah algoritma yang dapat digunakan untuk mengenkripsi data sehingga data asli hanya dapat dibaca oleh seseorang yang memiliki kunci enkripsi. Awalnya, algoritma DES dirancang menggunakan kunci 56-bit, dan ukuran ini dianggap cukup untuk menerapkan teknik enkripsi yang aman. Namun seiring berjalannya waktu, daya komputasi komputer semakin meningkat, sehingga semakin memungkinkan untuk membobol keamanan data. Algoritma ini memberikan solusi sederhana tanpa harus membuat algoritma baru, terdiri dari menjalankan algoritma DES sebanyak 3 kali untuk setiap blok data. Proses ini meningkatkan ukuran kunci dari 56 bit menjadi 168 bit dan membuat algoritma ini lebih aman daripada pendahulunya.

3. AES (*Advanced Encryption Standard*)

Enkripsi AES merupakan salah satu jenis enkripsi yang menggunakan metode kriptografi simteris. Enkripsi ini terdiri atas 3 blok *cipher*, yaitu AES-128, AES-192 dan AES-256. Namun, biasanya hanya AES-128 dan AES-256 yang digunakan pada Implementasi VPN. Enkripsi ini jauh lebih aman dan lebih cepat daripada enkripsi *Blowfish* dan 3DES. Protokol *Open*VPN juga menggunakan enkripsi AES-128 dan AES-256 bit untuk memberikan perlindungan dan anonimitas bagi penggunanya. Selain itu, fitur kompatibilitas membuat enkripsi yang dijelaskan di atas menjadi pilihan yang menarik bagi pengguna.

4. SHA1 (*Secure Hashing Algorithm)*

   SHA1 atau *Secure Hash Algorithm* 1 merupakan salah satu algoritma hashing yang sering digunakan untuk enkripsi data. Hasil dari sha1 adalah data dengan lebar 20 byte atau 160 bit, biasa ditampilkan dalam bentuk bilangan heksadesimal 40 digit. Aplikasi umum SHA adalah melakukan enkripsi kata sandi dengan mengacak *hash* penggunaan pengiriman data tertentu dengan sandi yang sebenarnya. Jika terjadi peretasan, maka SHA akan melindungi dengan memberikan *hash* yang tidak dapat dibaca tanpa adanya dekripsi atau sandi asli.

5. IP-Sec (*Internet Protocol-Security*)

   IPSec merupakan keamanan jaringan berbasis kriptografi yang dikembangkan oleh *Internet Engineering Task Force* (IETF) untuk IPv4 dan IPv6. Jenis enkripsi ini juga digunakan pada Protokol *Tunneling Layer* 2 (L2TP). Saat melakukan transmisi data, IPsec menggunakan *Encapsulation Security Payload* (ESP) untuk mengenkapsulasi paket data. ESP adalah anggota dari kumpulan protokol *Internet Protocol Security* (IPsec) yang mengenkripsi dan mengotentikasi paket data antar komputer menggunakan VPN, kemudian De-enkapsulasi terjadi pada akhir tujuan. Hanya pihak yang berwenang yang memegang kunci untuk dapat mendekripsi kode ini.

6. MPPE.

MPPE disebut sebagai Enkripsi *Microsoft Point to Point* yang digunakan dalam koneksi *dial-up* dan PPTP. *Level* enkripsi tersebut menggunakan algoritma RSA dan membantu kunci sesi 40-bit dan 128-bit.

7. Bunga Kamelia

   Enkripsi *camellia* merupakan algoritma kriptografi simetris blok *cipher*. *Camellia* adalah gagasan dari sebuah perusahaan NTT(*Nippon Telegraph and Telephone*) dan Mitsubishi. Enkripsi ini melakukan sangat mirip seperti *Blowfish* dan kompatibel dengan kunci 128-bit, 192-bit dan 256-bit. Protokol *Open*VPN juga menggunakan enkripsi *Camellia*.

2.10 Perangkat Jaringan

2.10.1 Switch

Switch merupakan salah satu perangkat dari jaringan komputer yang bekerja pada bagian OSI *Layer* 2 (*data link*) dan sebagai peyambung data antara satu koneksi ke koneksi lainnya. Sesuai dengan fungsinya pada OSI *Layer* 2 (*data link*) switch berfungsi sebagai pengenal adanya MAC *Address* untuk memilah tujuan dari paket data yang akan ditransmisikan. Selain itu switch dapat digunakan sebagai *repeater*, dapat sebagai penghubung kabel UTP antara satu perangkat jaringan dengan perangkat jaringan lainnya, serta di dalam switch terdapat routing yang fungsinya sebagai batu loncatan jaringan LAN untuk terkoneksi dengan komputer (Fardani and Neforawati, 2020).

Gambar 2.15 Switch

2.10.2 *Router* Mikrotik

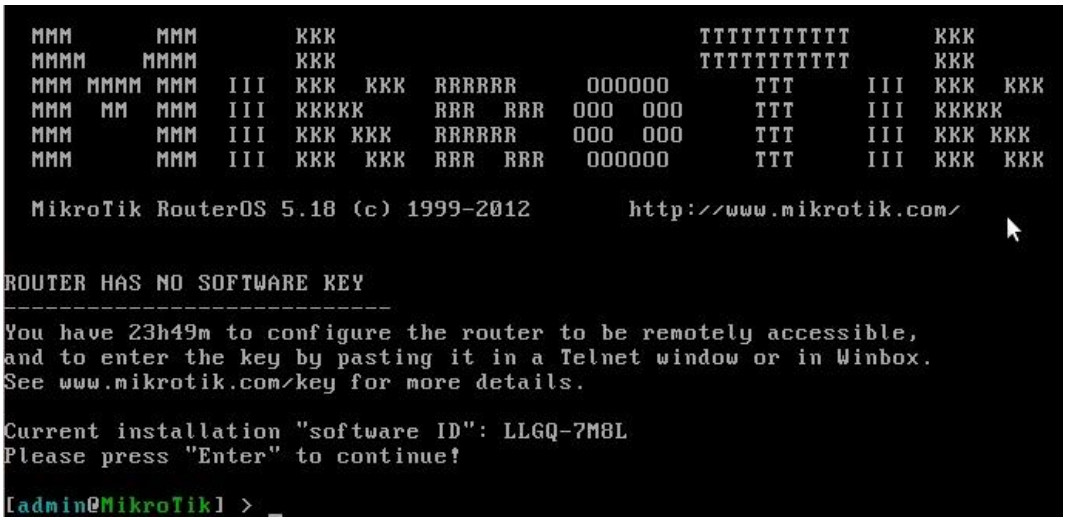
Router adalah perangkat jaringan komputer yang dapat berfungsi untuk menerima, menganalisis dan meneruskan paket data dari satu jaringan ke jaringan lainnya yang berbeda dalam sebuah jaringan komputer (Amarudin and Ulum, 2018). Berdasarkan mekanismenya *router* dapat dibagi menjadi dua jenis dan setiap jenisnya memiliki fungsi yang dapat dimanfaatkan sesuai dengan kebutuhan penggunanya. Berikut merupakan jenis-jenis dari mekanisme *router*:

- *Static Router* yaitu *router* yang memiliki rangkaian *routing* statis. Pengaturan pada *router* ini dilakukan secara manual oleh administrator jaringan.
- *Dynamic Router* yaitu *router* yang memiliki rangkaian *routing* dinamis. Cara kerja router ini yaitu dengan mendengarkan lalu lintas jaringan dan juga saling terkait dengan router lainnya.

Mikrotik adalah sebuah nama perusahaan yang berpusat di negara Latvia yang didirikan oleh John Trully serta Arnis Riekstins pada tahun 1996. MikroTik sekarang menyediakan perangkat keras dan perangkat lunak untuk konektivitas Internet di sebagian besar negara di dunia. Pada tahun 2002 MikroTik memutuskan untuk meproduksi perangkat keras-nya sendiri yaitu MikroTik *RouterBoard* (Mikrotik.com).

Gambar 2.16 *Router* Mikrotik (RB750Gr3)

MikroTik *Router* OS adalah sistem operasi berbasis Linux yang digunakan untuk menjadikan PC (*personal computer*) menjadi *router* khusus yang berfungsi sebagai *router, bridge, firewall, pengaturan bandwidth, wireless Access Point* atau *Client* dan fungsi *networking* serta beberapa fungsi server lainnya (Mikrotik.com).



Gambar 2.17 Tampilan Mikrotik *Router* OS

2.10.3 *Web Server*

Web server adalah sebuah jaringan komputer yang melayani khusus permintaan HTTP dan HTTPS. *Web server* menerima kode sedemikian rupa dari *browser*, lalu mengirimnya kembali dalam bentuk laman web. Laman *web* tersebut dikirim oleh *web server* dalam bentuk dokumen HTML dan CSS yang kemudian diproses oleh *browser* menjadi laman-laman *web* yang menarik dan mudah dibaca oleh pengguna. *web server* memiliki fungsi utama mengirim berkas yang diminta oleh pengguna sebelumnya melalui *browser* dengan protokol khusus. Sehingga pengguna dapat mengakses berupa teks, gambar, video, dan sebagainya melalui *browser*.

2.10.4 File *Server*

File server adalah jaringan komputer yang memberikan akses berupa *lokasi disk. Lokasi disk* tersebut berisikan *file* seperti gambar, video, musik, *database,* dokumen, dll. *Server* ini dirancang untuk pengguna memungkinkan dalam penyimpanan dan pengambilan data dengan perhitungan melalui *workstation.*

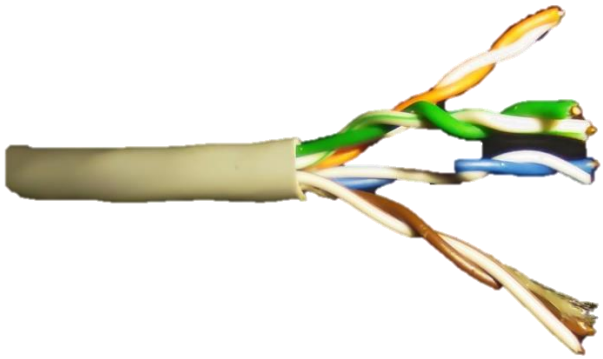
2.10.5 DHCP *Server*

Dynamic Host Configuration Protocol (DHCP) Server merupakan jaringan yang menjalankan layanan penyediaan IP address dan informasi TCP/IP kepada *client*. Secara garis besar fungsi server ini adalah memberikan layanan alamat IP secara otomatis kepada *client/*komput*er/host* pada jaringan TCP/IP yang meminta. Sehingga peran *administrator* tidak perlu disibukkan dengan membuat alamat IP secara manual untuk klien karena IP tersebut telah diberikan oleh *server.*

2.10.6 Kabel *Unshielded Twisted Pair*

Kabel *Unshielded Twisted Pair* merupakan salah satu kabel media transmisi yang digunakan dalam jaringan komputer untuk menghubungkan perangkat keras jaringan komputer antara satu dengan yang lainnya. Disebut demikian karena di dalam selubung luar kabel terdapat empat pasang kawat berisolasi kecil dan tidak memiliki pelindung. Pasangan ini diberi kode warna: biru, hijau, *orange*, dan cokelat. Untuk setiap pasangan, ada satu kawat warna

solid dan satu kawat bergaris, jadi, pasangan biru terdiri dari kawat biru solid dan kawat bergaris biru-putih.



Gambar 2.18 Kabel *Unshielded Twisted Pair*

Kabel ini dapat di kategorikan menjadi 8 kategori berdasarkan data *rate* maksimum :

- CAT 1 - Memiliki data rate maksimum sebesar 1 Mbps.
- CAT 2 - Memiliki data rate maksimum sebesar 4 Mbps.
- CAT 3 - Memiliki data rate maksimum sebesar 16 Mbps.
- CAT 4 - Memiliki data rate maksimum sebesar 20 Mbps.
- CAT 5 - Memiliki data rate maksimum sebesar 100 Mbps sampai dengan 1000 Mbps.
- CAT 5E - Memiliki data rate maksimum sebesar 1000 Mbps.
- CAT 6 - Kabel Cat-6 yang lebih baru dan agak mahal dapat membawa data hingga 10 GB/s tetapi dapat mempertahankan kecepatan hanya 55 meter.
- CAT 7 - Memiliki data rate maksimum mencapai 1.2 GHz.

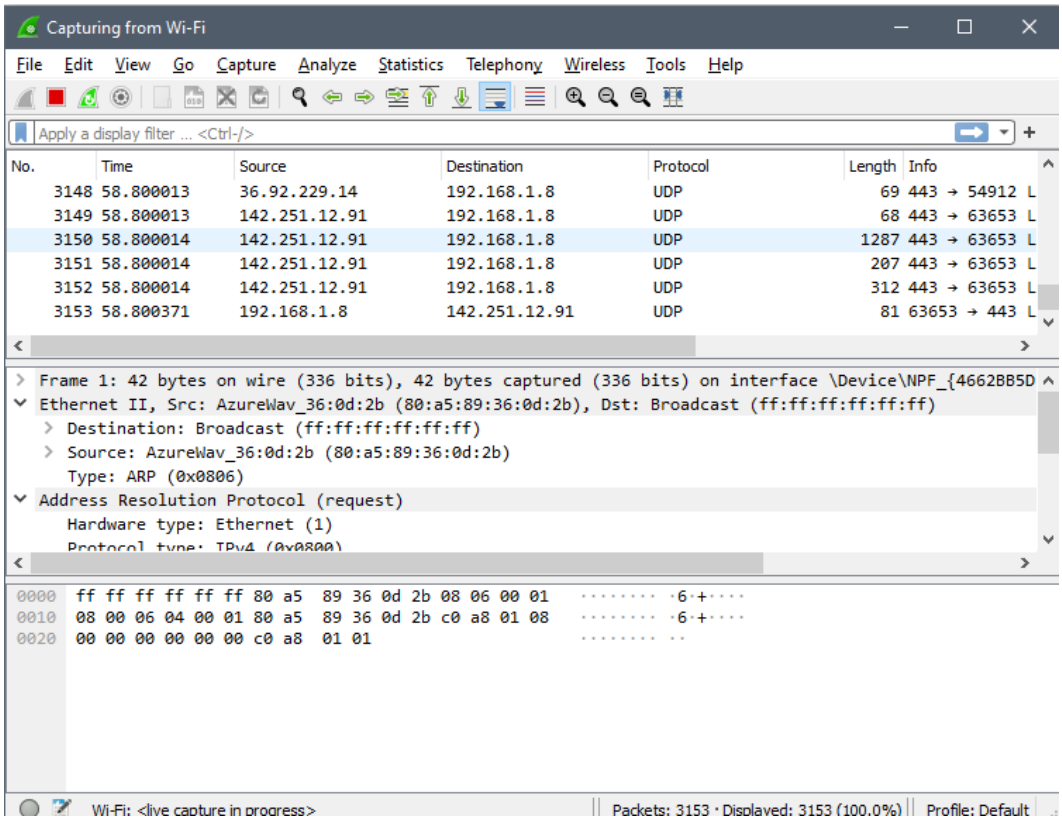
2.10.7 FTP *Server*

File Transfer Protocol (FTP) *server* adalah sebuah protokol internet yang memberikan akses data *server* pada satu jaringan. Klien dapat meminta akses tukar menukar file melalui *server*. Fungsi utama *server* ini adalah untuk memberikan pelayanan kepada klien dan pengunjung untuk melakukan akses transfer data tersimpan yang ada pada *server*.

2.11 WireShark

Wireshark adalah aplikasi yang digunakan untuk menganalisa paket data dalam sebuah kinerja jaringan. Wireshark dapat menangkap paket data atau informasi yang berada di dalam jaringan, sehingga data yang tertangkap dapat di analisa untuk berbagai keperluan seperti:

- Masalah dalam jaringan.
- Memeriksa keamanan jaringan.
- Data-data yang bersifat pribadi (Afrida and Rahmatia, 2018).



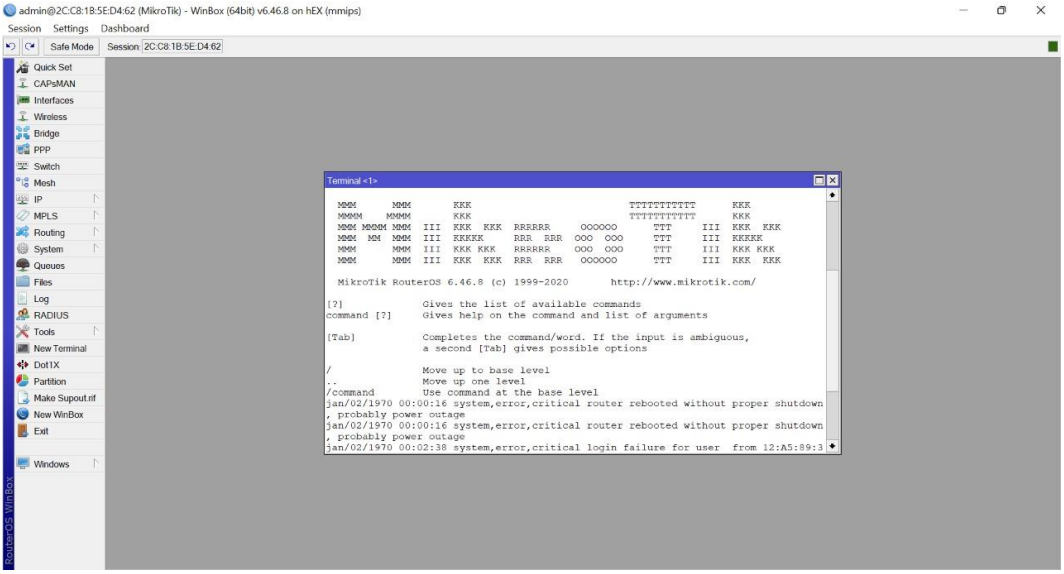
Gambar 2.19 Tampilan aplikasi *wireshark*

Wireshark memliki pengawasan paket data secara *real time*. Aplikasi wireshark dapat diakses secara gratis dan dapat dijalankan di beberapa *platform* seperti linux, mac dan windows.

2.12 *Winbox*

Winbox merupakan sebuah perangkat lunak *utility* yang dapat mengelolah MikroTik RouterOS menggunakan GUI (*Graphical User Interface*). Jika untuk mengonfigurasikan sebuah *router* biasanya *user* harus menggunakan sebuah

perintah yang terdapat dalam *console.* Namun dengan menggunakan winbox berbasis GUI *user* dapat lebih mudah mengonfigurasi sebuah router tanpa perlu menghafal berbagai perintah yang terdapat pada *console*. Fungsi utama Winbox yaitu untuk mempermudah user saat mengonfigurasi router mikrotik seperti melakukan manajemen jaringan sesuai dengan kebutuhan pengguna. Winbox dapat digunakan pada sistem operasi Linux, MacOS dan Windows (wiki.mikrotik.com).



Gambar 2.20 Tampilan Winbox