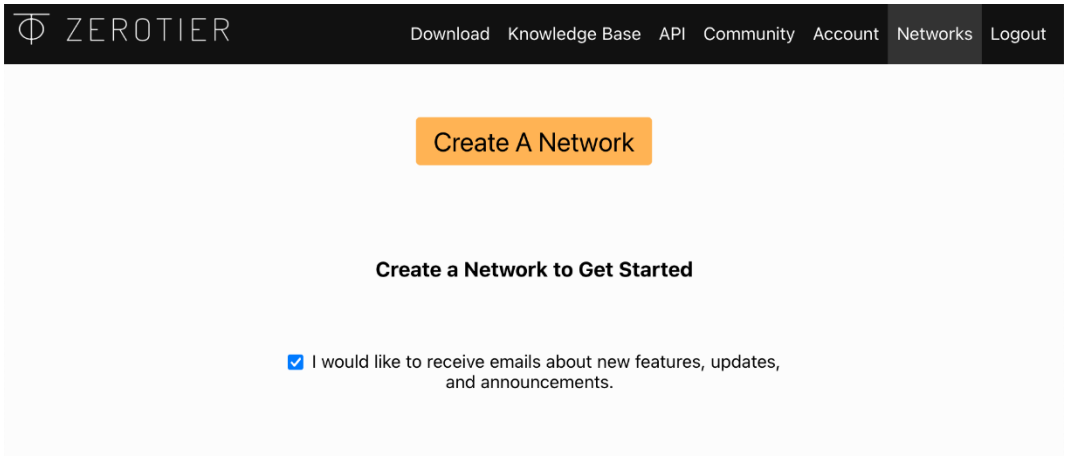
BAB II

DASAR TEORI DAN TINJAUAN PUSTAKA

2.1. DASAR TEORI

Dasar Teori berisi tentang teori dari apa yang digunakan oleh sistem yang mendukung penyelesaian

2.1.1. *Zerotier*



Gambar 2.1 *Platfom Zerotier*

ZeroTier adalah sebuah *platform* jaringan definisi perangkat lunak (SDN) yang menyediakan solusi VPN (*Virtual Private Network*) yang sederhana, aman, dan hemat biaya. *ZeroTier* menggunakan model *peer-to-peer*, yang memungkinkan perangkat untuk terhubung secara langsung melalui infrastruktur terdistribusi.

Dengan menggunakan *ZeroTier*, pengguna dapat menghubungkan perangkat mereka ke jaringan lokal dengan cara yang mirip dengan penggunaan VPN tradisional. Namun, *ZeroTier* menawarkan kemudahan penggunaan dengan antarmuka yang sederhana. Selain itu, *ZeroTier* juga menekankan pada keamanan dengan menyediakan *enkripsi end-to-end* dan autentikasi pengguna untuk melindungi lalu lintas data yang dikirim melalui jaringan.

Perlu di ketahui untuk dasar teori pada *zerotier* terdapat bebrapa istilah-istilah jaringan pada *zerotier*.

1. ***Node*:** Ini adalah setiap perangkat yang terhubung ke jaringan *ZeroTier*. *Node* dapat berperan sebagai *PLANE*T (*node* pusat), *LEAF* (*node* biasa), atau *RELAY* (node yang bertindak sebagai *relay* untuk perangkat lain).
2. ***PLANET*:** Ini adalah *node* pusat dalam jaringan *ZeroTier*. Ini bertanggung jawab untuk mengelola koneksi dan informasi tentang *node* lain dalam jaringan. Biasanya, ada beberapa PLANET dalam jaringan besar.
3. ***LEAF*:** Ini adalah node biasa dalam jaringan *ZeroTier*. *Node LEAF* terhubung ke PLANET untuk mendapatkan informasi tentang jaringan dan perangkat lainnya.
4. ***RELAY*:** Ini adalah *node* yang bertindak sebagai *relay*. Jika dua perangkat tidak dapat berkomunikasi secara langsung (misalnya, karena alamat IP *internal* atau *firewall)*, data dapat diarahkan melalui *node RELAY*.
5. ***Address (ZT Address):*** Setiap perangkat dalam jaringan *ZeroTier* memiliki alamat unik yang disebut "*ZT Address*." Alamat ini digunakan untuk mengidentifikasi perangkat dalam jaringan.
6. ***Network*:** Ini adalah jaringan virtual yang dibuat menggunakan *ZeroTier.* Semua perangkat yang terhubung dengan jaringan yang sama dapat berkomunikasi layaknya berada dalam jaringan lokal yang sama.

Jaringan VPN (*Virtual Private Network*):

1. ***Server VPN*:** Ini adalah *server* yang melayani koneksi dari perangkat yang ingin bergabung dengan jaringan VPN. *Server* ini mengelola koneksi dan menyediakan alamat IP kepada perangkat klien.
2. **Klien VPN:** Ini adalah perangkat yang ingin terhubung ke jaringan VPN. Perangkat ini membuat koneksi ke server VPN dan menerima alamat IP dari *server.*

3. ***Tunneling*:** Ini adalah proses mengemas data dalam paket yang aman dan mengirimkannya melalui koneksi internet. Data yang dikirim melalui VPN *dienkripsi* sehingga tidak dapat diakses oleh pihak ketiga yang tidak berwenang.

4. ***Enkripsi:*** Proses mengubah data menjadi format yang tidak dapat dibaca (*ciphertext*) tanpa kunci enkripsi yang sesuai. Data yang dikirimkan melalui VPN *dienkripsi* sehingga hanya penerima yang memiliki kunci *dekripsi* yang dapat membaca data tersebut.

5. ***Protokol VPN:*** Ini adalah aturan yang mengatur bagaimana data dikemas, dienkripsi, dan dikirim melalui jaringan. Contoh *protokol VPN* termasuk *OpenVPN, IPSec, L2TP, dan PPTP*.

6. ***<ztaddr>:*** Ini adalah alamat unik yang diberikan kepada setiap *peer* dalam *jaringan ZeroTier*. Setiap perangkat memiliki alamat ini untuk diidentifikasi dalam jaringan.

7. ***<ver>:*** Versi perangkat lunak *ZeroTier* yang digunakan oleh *peer*. Versi ini mencerminkan versi perangkat lunak yang *diinstal* pada perangkat tersebut.

8. ***<role>:*** Peran perangkat dalam jaringan. Peran dapat berupa PLANET (node pusat dalam jaringan), *LEAF* (*node* biasa dalam jaringan), atau *RELAY* (*node* yang bertindak sebagai *relay* untuk perangkat lain dalam jaringan).

9. ***<lat>:*** *Latensi* (waktu tunda) dalam *milidetik* antara perangkat saat ini dengan *node* PLANET terdekat.

10. ***<link>:*** Tipe koneksi yang digunakan oleh perangkat, seperti *DIRECT* (koneksi langsung) atau *RELAY* (melalui *relay*).

11. ***<lastTX>:*** Jumlah paket yang dikirimkan oleh perangkat terakhir kali data dikirimkan.

12. **<*lastRX*>:** Jumlah paket yang diterima oleh perangkat terakhir kali data diterima.

13. **<*path*>:** Alamat IP dan *port* yang digunakan untuk menghubungi *peer*. Jika tipe koneksi adalah *DIRECT*, maka alamat ini adalah alamat IP langsung peer. Jika tipe koneksi adalah *RELAY*, maka alamat ini adalah alamat relay yang digunakan.

2.1.2. *PuTTY*

PuTTY adalah sebuah aplikasi terminal *emulator* yang digunakan untuk mengakses dan mengendalikan perangkat jaringan secara *remote* melalui *protokol SSH*, *Telnet*, dan *rlogin*. Aplikasi ini sangat populer di kalangan *administrator* jaringan dan pengguna yang sering berinteraksi dengan perangkat jarak jauh.

Gambar 2.2 *Aplikasi Putty*

PuTTY menyediakan antarmuka yang sederhana dan intuitif, dengan berbagai fitur yang berguna. Beberapa fitur utama dari *PuTTY* meliputi:

1. Koneksi *SSH*: *PuTTY* memungkinkan pengguna untuk mengakses perangkat jaringan melalui koneksi *SSH* yang aman dan terenkripsi.
2. *Telnet* dan *rlogin*: Selain *SSH*, *PuTTY* juga mendukung *protokol Telnet* dan *rlogin* untuk mengakses perangkat yang tidak menggunakan koneksi yang terenkripsi.
3. *Konfigurasi* yang *fleksibel*: Pengguna dapat mengatur berbagai pengaturan seperti nama *host*, nomor *port*, jenis koneksi, dan pengaturan *enkripsi* sesuai kebutuhan.
4. Keamanan: *PuTTY* menyediakan opsi *enkripsi* yang kuat untuk menjaga kerahasiaan dan *integritas* data yang dikirim melalui koneksi.
5. Penyimpanan sesi: *PuTTY* memungkinkan pengguna untuk menyimpan pengaturan dan detail koneksi dalam bentuk sesi, sehingga memudahkan akses kembali ke perangkat yang sama di masa depan.

6. Penggunaan kunci publik dan pribadi: *PuTTY* mendukung penggunaan kunci publik dan pribadi untuk autentikasi yang lebih kuat dan menghindari penggunaan *password.*

PuTTY merupakan aplikasi *open-source* Dengan antarmuka yang *user-friendly* dan fungsionalitas yang lengkap untuk mengakses dan mengendalikan perangkat jaringan secara *remote.*

2.1.3. *JuiceSSH*

JuiceSSH adalah sebuah *aplikasi terminal emulator* yang dirancang khusus untuk perangkat *Android*. Aplikasi ini memungkinkan pengguna untuk mengakses dan mengendalikan perangkat jaringan secara *remote* melalui *protokol* SSH *(Secure Shell*).

Gambar 2.2 *Aplikasi JuiceSSH For Android*

JuiceSSH menyediakan antarmuka yang *intuitif* dan mudah digunakan, dengan fitur-fitur yang berguna bagi pengguna yang sering *berinteraksi* dengan perangkat jaringan. Beberapa fitur utama dari *JuiceSSH* meliputi:

1. Koneksi SSH: Aplikasi ini mendukung koneksi SSH yang aman dan terenkripsi, sehingga memastikan kerahasiaan dan integritas data yang dikirim melalui jaringan.
2. Pengelolaan Kunci SSH: *JuiceSSH* memungkinkan pengguna untuk mengelola kunci SSH mereka, termasuk mengimpor kunci yang ada atau menghasilkan kunci baru.

3. Konfigurasi Profil: Pengguna dapat menyimpan dan mengatur berbagai profil koneksi dengan pengaturan yang berbeda, seperti nama *host*, nomor *port*, dan pengaturan *otentikasi*.
4. *Integrasi* dengan *Aplikasi Eksternal*: *JuiceSSH* dapat *terintegrasi* dengan aplikasi lain di *perangkat Android,* sehingga pengguna dapat dengan mudah membuka file *teks* atau mengirim perintah dengan aplikasi pihak ketiga.
5. *Kustomisasi* Antarmuka: Pengguna dapat mengkustomisasi tampilan dan tema antarmuka *JuiceSSH* sesuai *preferensi* mereka.
6. Keamanan: *JuiceSSH* mendukung otentikasi menggunakan kata sandi atau kunci publik dan pribadi untuk memastikan akses yang aman ke perangkat jaringan.

JuiceSSH menjadi pilihan yang populer bagi pengguna *Android* yang ingin mengakses dan mengendalikan perangkat jaringan secara *remote*.

2.1.4. *Winbox*

Winbox adalah sebuah aplikasi manajemen jaringan yang dikembangkan oleh *MikroTik*. Aplikasi ini dirancang khusus untuk mengkonfigurasi, mengelola, dan mengontrol perangkat *MikroTik RouterOS* melalui antarmuka grafis yang *intuitif*.

Gambar 2.3 *Aplikasi Winbox.*

Dengan menggunakan *Winbox*, pengguna dapat melakukan berbagai tugas *administratif* pada perangkat *MikroTik*, seperti mengatur pengaturan jaringan,

mengkonfigurasi *firewall*, mengelola antarmuka, memantau kinerja jaringan, dan melakukan *troubleshooting*.

2.1.5 Kabel UTP Cat 5E

Kabel UTP (*Unshielded Twisted Pair*) Cat 5 adalah jenis kabel jaringan yang sering digunakan untuk menghubungkan perangkat jaringan seperti komputer, *switch, router,* dan perangkat lainnya. Cat 5 merupakan singkatan dari "*Category 5*

.

Gambar 2.4 Kabel UTP

Ciri khas kabel UTP Cat 5 adalah adanya pasangan kabel yang dijalin (*twisted pair*) yang tidak dilapisi pelindung adalah jenis kabel yang umum digunakan dalam jaringan komputer untuk menghubungkan perangkat-perangkat seperti komputer, *switch, router*, dan perangkat jaringan lainnya. Berikut adalah definisi singkat tentang kabel UTP Cat 5:

1. Jenis Kabel: Kabel UTP Cat 5 adalah kabel jaringan yang terdiri dari beberapa pasang kabel tembaga yang dijalin (*twisted pair*). Kabel ini tidak memiliki pelindung *eksternal* (*unshielded*), yang berarti rentan terhadap gangguan *elektromagnetik.*
2. Kecepatan dan *Frekuensi*: Kabel UTP Cat 5 mendukung kecepatan *transfer* data hingga 100 Mbps (*Megabit per detik*) dan *frekuensi* hingga 100 MHz. Ini memadai untuk kebanyakan jaringan komputer dalam lingkungan rumah atau kecil.

3. Jumlah Pasang Kabel: Kabel UTP Cat 5 terdiri dari empat pasang kabel yang dijalin. Setiap pasang kabel terdiri dari dua *konduktor* tembaga yang ditarik bersama dan dijalin untuk mengurangi *interferensi elektromagnetik*.

4. Penggunaan RJ-45: Kabel UTP Cat 5 menggunakan konektor *RJ-45* (*Registered Jack* 45) pada ujungnya. Konektor *RJ-45* digunakan untuk menghubungkan kabel ke perangkat jaringan seperti komputer atau *switch.*

5. Jarak Maksimum: Jarak maksimum yang dapat ditempuh oleh kabel UTP Cat 5 adalah sekitar 100 meter. Melebihi jarak ini dapat mengurangi kualitas sinyal dan mempengaruhi kecepatan *transfer* data.

Kabel UTP Cat 5e umumnya digunakan dalam instalasi jaringan lokal (LAN) di lingkungan kantor, sekolah, rumah, dan sebagainya. Kabel ini memungkinkan transfer data yang cepat dan dapat diandalkan dalam jaringan komputer yang biasa digunakan sehari-hari.

2.1.6 Hub

Hub adalah perangkat jaringan yang digunakan untuk menghubungkan beberapa perangkat dalam jaringan lokal (LAN) dengan menggunakan teknologi Ethernet. Fungsinya adalah meneruskan data yang diterima dari satu perangkat ke semua perangkat yang terhubung dalam jaringan.

Gambar 2.4 Hub 100mbps

Berikut adalah beberapa Spesifikasi dan fungsi utama dari hub:

1. Hubungan Perangkat: Hub memiliki beberapa *port* yang digunakan untuk menghubungkan perangkat-perangkat dalam jaringan, seperti komputer, printer, *server*, dan perangkat jaringan lainnya.

2. Penerusan Data: Ketika sebuah paket data diterima di salah satu port hub, hub akan mengirimkan paket tersebut ke semua *port* yang lain.
3. *Broadcast*: Hub melakukan penerusan data dalam bentuk *broadcast*, yang berarti semua perangkat dalam jaringan menerima paket data yang sama.
4. Kecepatan transmisi: Hub mendukung kecepatan transmisi hingga 100mbps

Hub umumnya di gunakan pada skala rumah maupun kantor kecil dengan alasan karena keterbatasan *port ethernet* pada *router* atau *modem*.

2.1.7 *Router Mikrotik*

Router MikroTik adalah perangkat jaringan yang diproduksi oleh perusahaan *MikroTik*. Router ini didesain untuk mengatur lalu lintas data antara jaringan yang berbeda dan menyediakan konektivitas yang andal di dalam jaringan tersebut. Berikut adalah definisi singkat tentang router *MikroTik*:

Gambar 2.6 *Router Mikrotik.*

Router MikroTik berfungsi sebagai pengatur lalu lintas data di dalam jaringan. Ia mampu mengarahkan paket data antara jaringan lokal (LAN), jaringan luas (WAN), dan jaringan lainnya seperti jaringan virtual pribadi (VPN) atau jaringan publik.

1. Fungsi *Routing*: *Router MikroTik* menggunakan protokol routing seperti OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*), BGP (*Border Gateway Protocol*), atau *protokol routing statis* untuk menentukan jalur terbaik dan mengirimkan paket data ke tujuan yang tepat.

2. *Firewall: Router MikroTik* dilengkapi dengan fitur *firewall* yang memungkinkan *administrator* jaringan untuk mengatur kebijakan keamanan dan membatasi akses ke jaringan. Hal ini membantu melindungi jaringan dari serangan dan ancaman yang tidak diinginkan.
3. Manajemen Jaringan: *Router MikroTik* menyediakan berbagai fitur untuk manajemen jaringan, seperti manajemen *bandwidth* untuk mengontrol alokasi sumber daya jaringan, DHCP *server* untuk memberikan alamat IP secara otomatis, dan fitur *monitoring* untuk memantau kinerja jaringan.
4. Pengaturan *Wireless*: Beberapa model *Router MikroTik* mendukung konektivitas nirkabel dan menyediakan fungsi *akses point* (AP) atau *bridge* untuk menghubungkan perangkat nirkabel ke jaringan.

Router MikroTik sering digunakan dalam berbagai skenario jaringan, mulai dari jaringan kecil hingga jaringan besar. Dengan kemampuan routing yang kuat, fitur keamanan yang lengkap, dan fleksibilitas konfigurasi, *router MikroTik* menjadi pilihan yang populer bagi *administrator* jaringan untuk membangun dan mengelola jaringan yang andal dan aman.

2.1.8 Mini Pc

Mini PC sebagai *server* skala kecil untuk kebutuhan rumahan memiliki spesifikasi yang sesuai untuk memenuhi kebutuhan jaringan di lingkungan rumah.

Gambar 2.7 Mini PC

Berikut adalah penjelasan singkat mengenai spesifikasi mini PC sebagai *server* skala kecil untuk kebutuhan rumahan:

1. *Prosesor*: Mini PC yang cocok untuk kebutuhan rumahan biasanya dilengkapi dengan *prosesor* yang cukup untuk menjalankan tugas-tugas rumahan seperti berbagi file, streaming media, atau menjalankan *server* game. *Prosesor* dengan kecepatan sedang seperti *Intel Core i3* atau *prosesor* serupa dari AMD dapat menjadi pilihan yang baik.

2. RAM: RAM yang cukup adalah penting untuk menjalankan aplikasi rumahan dengan lancar. Mini PC sebagai *server* rumahan biasanya memiliki kapasitas RAM mulai dari 4GB hingga 8GB, yang cukup untuk menangani kebutuhan rumahan umum.

3. Penyimpanan: Mini PC sebagai server rumahan membutuhkan penyimpanan yang cukup untuk menyimpan file dan data rumah tangga. *Solid-state drive* (SSD) dengan kapasitas mulai dari 128GB hingga 1TB dapat menjadi pilihan yang baik untuk performa yang cepat dan responsif.

4. Konektivitas: Mini PC sebagai *server* rumahan harus dilengkapi dengan port konektivitas yang mencakup *port Ethernet* untuk koneksi jaringan, port USB untuk perangkat penyimpanan *eksternal* atau *printer*, dan port HDMI atau VGA untuk koneksi monitor atau TV.

5. Sistem Operasi: Mini PC sebagai *server* rumahan dapat menjalankan sistem operasi seperti *Windows* 10, *Linux* (seperti *Ubuntu* atau *Linux Debian*), atau sistem operasi lainnya yang sesuai dengan preferensi dan kebutuhan pengguna rumahan.

6. Keandalan dan Efisiensi Energi: Mini PC sebagai *server* rumahan harus memiliki desain yang handal dan efisiensi energi yang baik. Pastikan memilih mini PC dengan kualitas yang baik dari produsen terpercaya untuk memastikan keandalan dan stabilitas operasional dalam jangka waktu yang lama.

Mini PC sebagai *server* skala kecil untuk kebutuhan rumahan memberikan kemudahan dan effisien dalam konsumsi energi. Untuk spesifikasi yang di butuhkan dalam membangun jaringan vpn ini tidak memerlukan spesifikasi tinggi cukup dengan *prosesor i3* sudah mumpuni karena dalam proyek akhir ini mini pc di gunakan sebagai client VPN *Zerotier* yang terhubung dengan node 1 jaringan *Zerotier.*