

## BAB II

### LANDASAN TEORI

#### 2.1 Tinjauan Pustaka

Pada tinjauan pustaka ini peneliti mengumpulkan informasi terkait apa saja yang diperlukan dalam pembuatan laporan yang berjudul Pembangunan Interkoneksi Antar SMK TKJ Se-Depok Dengan VPN L2TP IPsec Untuk Keperluan Pembelajaran Dan *video conference* Melalui Perangkat Lunak Jitsi. Hal ini bertujuan untuk mendapatkan landasan teori dan ruang lingkup pembahasan mengenai masalah yang akan diteliti.

##### 2.1.1 Jaringan Komputer

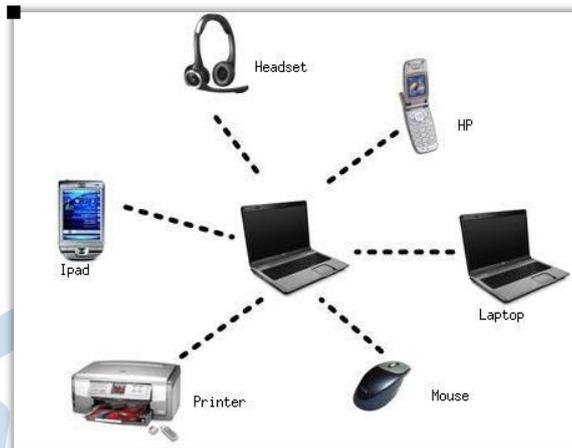
Jaringan komputer merupakan penggabungan teknologi komputer dan komunikasi yang merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya (Saputra, 2016). Sederhananya jaringan komputer digunakan untuk menghubungkan berbagai alat dalam jaringan sehingga dapat digunakan untuk beberapa kegunaan, seperti:

- Untuk berkomunikasi
- Untuk berbagi sumber daya
- Untuk akses informasi

Jaringan komputer memiliki beberapa jenis yang terbagi berdasarkan letak jarak geografis, diantaranya adalah:

a. PAN (*Personal Area Network*)

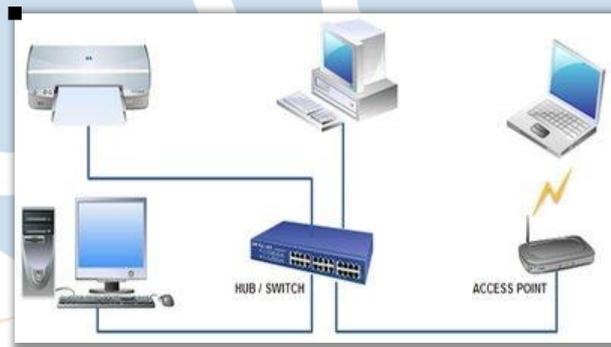
Merupakan jenis jaringan yang mencakup jaringan personal, atau jaringan yang lebih kecil seperti koneksi antar laptop dengan *handphone* menggunakan *wireless*. Berikut adalah contoh gambar dari jenis jaringan PAN:



Gambar 2.1 Jaringan PAN

b. LAN (*Local Area Network*)

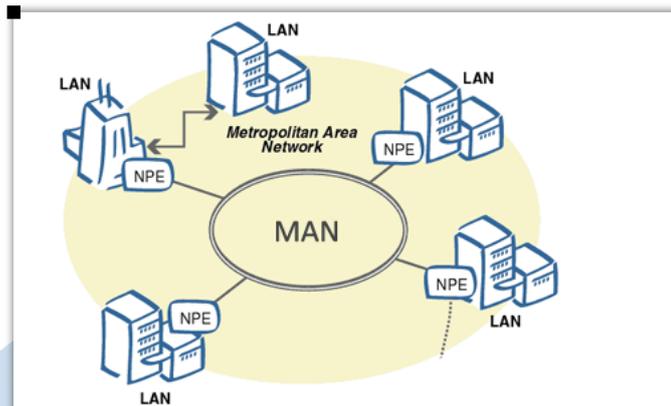
Merupakan jaringan komputer yang *mencover* area lokal, seperti rumah, kantor atau grup dari bangunan (Sukaridhoto ST. Ph.D, 2016). Jarak yang biasanya digunakan pada jenis jaringan ini adalah sampai 1 kilometer. Berikut adalah contoh gambar dari jenis jaringan LAN:



Gambar 2.2 Jaringan LAN

c. MAN (*Metropolitan Area Network*)

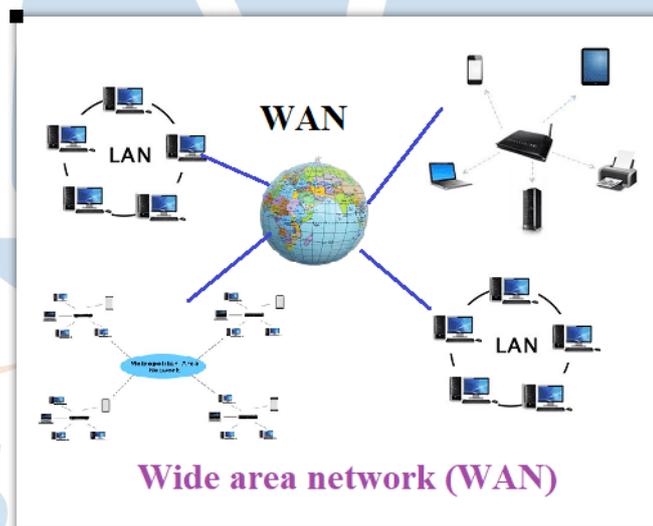
Merupakan jenis jaringan yang mencakup wilayah antar kota. Jaringan MAN ini merupakan kumpulan dari jaringan LAN yang memiliki jarak sampai 50 kilometer. Berikut adalah contoh gambar dari jenis jaringan MAN:



Gambar 2.3 Jaringan MAN

d. WAN (*Wide Area Network*)

Merupakan jaringan komputer dimana memiliki cakupan daerah yang lebih luas (Sukaridhoto ST. Ph.D, 2016). Contoh dari penerapan jenis jaringan ini adalah internet. Jaringan WAN ini lebih luas dari jaringan MAN. Berikut adalah contoh gambar dari jenis jaringan WAN:



Gambar 2.4 Jaringan WAN

Dalam jaringan komputer terdapat beberapa istilah untuk mengukur jaringan komputer, diantaranya adalah:

a. *Delay*

*Delay* adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ketujuan (Carol et al., 2017). Hitungan *delay* diperoleh dari

waktu paket data diterima dikurangi dengan waktu paket data dikirimkan.

$$Delay = \frac{\text{waktu paket diterima} - \text{waktu paket dikirim}}{\text{Total Paket Yang Diterima} - 1}$$

(Sumber: TIPHON)

Gambar 2.5 Rumus Menghitung *Delay*

b. *Jitter*

*Jitter* adalah kumpulan dari semua *delay* terjadi dalam jaringan pada saat waktu tertentu. Untuk menghitung *jitter* memerlukan total variasi *delay* dan juga total *packet* data.

$$Jitter = \frac{\text{Total Variasi Delay}}{\text{Total Paket Yang Diterima} - 1}$$

Gambar 2.6 Rumus Menghitung *Jitter*

c. *Packet Loss*

*Packet Loss* adalah parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena *collision* dan *congestion* pada jaringan dan hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah *bandwith* cukup tersedia untuk aplikasi-aplikasi tersebut (Zamalia et al., 2018). Cara mencari nilai *packet loss* dapat dilihat dari rumus gambar di bawah ini:

$$Packet\ loss = \frac{(\text{Packet transmitted} - \text{Packet received})}{\text{Packet transmitted}} \times 100\%$$

Gambar 2.7 Rumus Menghitung *Packet Loss*

### 2.1.2 Open System Interconnection Layer (OSI Layer)

OSI adalah referensi komunikasi dari *Open System Interconnection*. OSI model digunakan sebagai titik referensi untuk membahas spesifikasi dari protokol (Sukaridhoto ST. Ph.D, 2016).

OSI model terdiri dari 7 *layer*. Dimana bagian atas dari *layernya* (*layer* 7, 6, dan 5) di fokuskan untuk bentuk pelayanan dari suatu aplikasi. Sedangkan untuk *layer* bagian bawahnya (*layer* 4, 3, 2 dan 1) berorientasikan tentang aliran data dari ujung satu ke ujung yang lainnya.

Tabel 2 .1 OSI Layer

Nama layer	Fungsi	Contoh
Aplikasi (layer 7)	Aplikasi yang saling berkomunikasi antar komputer. Aplikasi layer mengacu pada pelayanan komunikasi pada suatu aplikasi.	Telnet, HTTP, FTP, WWW Browser, NFS, SMTP, SNMP
Presentasi (Layer 6)	Pada layer bertujuan untuk mendefinisikan format data, seperti ASCII text, binary dan JPEG.	JPEG, ASCII, TIFF, GIF, MPEG, MIDI
Sesi (Layer 5)	Sesi layer mendefinisikan bagaimana memulai, mengontrol dan mengakhiri suatu percakapan (biasa disebut session)	RPC, SQL, NFS, SCP
Transport (Layer 4)	Pada layer 4 ini bisa dipilih apakah menggunakan protokol yang mendukung error-recovery atau tidak. Melakukan multiplexing terhadap data yang datang, mengurutkan data yang datang apabila datangnya tidak berurutan.	TCP, UDP, SPX
Network (Layer 3)	Layer ini mendefinisikan pengiriman data dari ujung ke ujung. Untuk melakukan pengiriman pada layer ini juga melakukan pengalamatan. Mendefinisikan pengiriman jalur (routing).	IP, IPX, Appletalk DDP
Data Link (layer 2)	Layer ini mengatur pengiriman data dari interface yang berbeda. Semisal pengiriman data dari ethernet 802.3 menuju ke High-level Data Link Control (HDLC), pengiriman data WAN.	IEEE 802.2/802.3, HDLC, Frame relay, PPP, FDDI, ATM
Physical (Layer 1)	Layer ini mengatur tentang bentuk interface yang berbeda-beda dari sebuah media transmisi. Spesifikasi yang berbeda misal konektor, pin, penggunaan pin, arus listrik yang lewat, encoding, sumber cahaya dll	EIA/TIA-232, V35, EIA/TIA-449, V.24, RJ45, Ethernet, NRZI, NRZ, B8ZS

### 2.1.3 Protokol Jaringan

Protokol jaringan merupakan himpunan aturan-aturan yang memungkinkan komputer satu dapat berhubungan dengan komputer yang lain. Aturan-aturan ini meliputi tata cara bagaimana agar komputer bisa saling berkomunikasi, biasanya berupa bentuk (model) komunikasi, waktu saat berkomunikasi, barisan *traffic* saat berkomunikasi, pemeriksaan *error* saat transmisi data, dan lain-lain. Berbagai protokol yang terdapat dari lapisan teratas sampai terbawah yang ada dalam sederetan protokol. Dipandang dari

sudut komunikasi data, ada beberapa protokol yang banyak digunakan pada jaringan komputer, diantaranya:

1. TCP/IP ( *Transmission Control Protocol/Internet Protocol* )

TCP/IP merupakan protokol standar pada jaringan internet yang tidak tergantung pada jenis komputer yang digunakan. Dengan menggunakan TCP/IP akan memungkinkan berbagai komputer (seperti PC IBM, Machintosh, Sun, HP, dan lain-lain) berinteraksi satu dengan lain tanpa mengalami masalah yang berarti.

2. UDP ( *User Datagram Protocol* )

*User Datagram Protokol* (UDP) adalah sebuah protokol yang bekerja pada *Transport Layer*, mulai digunakan dan dikembangkan oleh US *Department of Defence* (DoD) untuk digunakan bersama protokol IP di *Network Layer*. protokol UDP memberikan alternatif *transport* untuk proses yang tidak membutuhkan pengiriman yang handal.

#### **2.1.4 Routing Protokol OSPF**

OSPF ( *Open Shortest Path First* ) adalah sebuah *routing protocol* yang dipergunakan untuk merutekan paket data yang akan di kirimkan dari sebuah komputer ke komputer lain di dalam jaringan. OSPF merupakan *Intra – Domain Internet Routing Protocol* yang paling sering dipergunakan. *Routing protocol* ini akan mengarahkan lalu lintas data di dalam jaringan dengan berdasarkan hubungan ukuran antar data yang telah ditentukan oleh seorang administrator jaringan. Masing-masing *router* yang terdapat di dalam AS ( *Autonomous Systems* ) akan menghitung jalur yang paling pendek dan membuat tabel tujuan yang dipergunakan untuk mengirimkan paket data kepada *router* berikutnya dalam rangka untuk mengirimkan paket data menuju tujuannya yang terakhir (Utomo & Purnama, 2012).

#### **2.1.5 MikroTik (RouterOS dan RouterBoard)**

MikroTik adalah *router embedded* produk dari MikroTik (Mila, 2018). Selain ini MikroTik *RouterOS* merupakan sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *router* yang handal, mencakup berbagai fitur yang dibuat untuk IP *network* dan jaringan

*wireless*. MikroTik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.

```
MMMM  MMMM   KKK          TTTTTTTTTT   KKK
MMM  MMMM  MMM  III  KKK  KKK  RRRRRR   000000   TTT   III  KKK  KKK
MMM  MM  MMM  III  KKKKK  RRR  RRR  000 000   TTT   III  KKKKK
MMM  MMM  III  KKK  KKK  RRRRRR   000 000   TTT   III  KKK  KKK
MMM  MM  III  KKK  KKK  RRR  RRR  000000   TTT   III  KKK  KKK

MikroTik RouterOS 6.46.5 (c) 1999-2020      http://www.mikrotik.com/

-----
ROUTER HAS NO SOFTWARE KEY
-----
You have 23h36m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.

Current installation "software ID": G09U-CQ7V
Please press "Enter" to continue!

[admin@MikroTik] > _
```

Gambar 2.8 MikroTik RouterOS

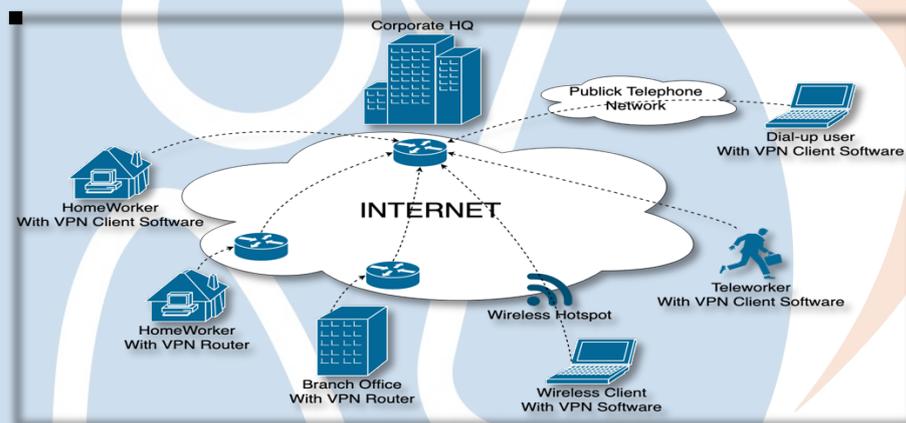
*RouterBoard* adalah *router embedded* produk dari MikroTik. *RouterBoard* seperti sebuah PC mini yang terintegrasi karena dalam satu *board* tertanam prosesor, RAM, ROM, dan memori *flash*. *RouterBoard* menggunakan sistem operasi *RouterOS* yang berfungsi sebagai *router* jaringan, *bandwidth management*, *proxy server*, dan sebagainya. *Server* dan bisa juga berfungsi sebagai *hotspot server*. Ketika membeli sebuah MikroTik *RouterBoard* biasanya sudah *terinstall RouterOS* didalamnya. Seri dari *RouterBoard* bisa dikenali dari huruf dan angka *kodenya*. Contohnya RB951, menandakan bahwa perangkat itu merupakan *RouterBoard* seri ke 9 dengan 5 *ethernet port* dan 1 *wireless*.



Gambar 2.9 MikroTik RouterBoard

## 2.1.6 VPN (L2TP dan IPSec)

*Virtual Private Network* (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal (RACHMAWAN, 2018). Dalam pengertian lain VPN adalah sebuah cara aman untuk mengakses jaringan lokal yang berada pada jangkauan tertentu, dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data paket secara pribadi (Sujadi & Burhanuddin, 2017).



Gambar 2.10 *Virtual Private Network*

Dalam VPN (*Virtual Private Network*) terdapat berbagai macam cara untuk melakukan koneksi, berikut adalah macam-macam cara koneksi VPN:

### 1. *Remote Access*

Merupakan cara koneksi ke VPN dengan menghubungkan komputer individu yang ada diperkantoran, kampus, dan lain-lain ke jaringan VPN. Biasa digunakan oleh perusahaan agar beberapa orang yang terhubung dari luar perusahaan dengan jarak yang jauh (Arafah & Gunawan, 2017).

### 2. *Site to Site*

Merupakan cara koneksi ke VPN dengan meghubungkan dua jaringan bersama.

### 3. *Hub and Spoke*

Merupakan cara koneksi ke VPN dengan menghubungkan banyak jaringan ke *VPN Concentrator*.

#### 4. *Roadwarrior*

Merupakan cara koneksi jaringan VPN yang menghubungkan perangkat personal (PC/Laptop/*Smartphone*) dengan jaringan *private* melalui internet dengan menggunakan VPN. Istilah lain *roadwarrior* VPN adalah kesatria jalanan.

Kelebihan VPN :

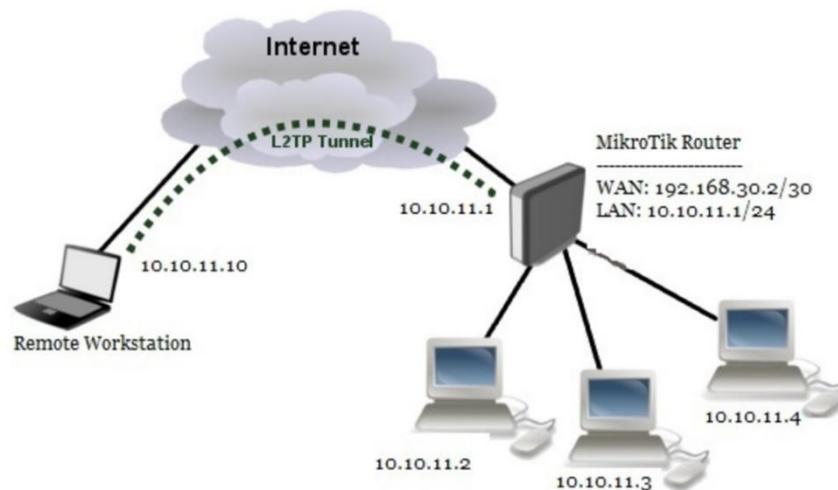
- Biaya lebih murah.
- Fleksibel.
- Keamanan data kuat.

Kelemahan VPN :

- Tidak ada kendali utama pengguna.
- Membutuhkan internet.

- **L2TP (*Layer 2 Tunneling Protokol*)**

L2TP adalah *tunneling* yang berkerja di *layer 2*, tetapi tidak memiliki pengamanan khusus sehingga biasanya ditambahkan sistem keamanan yang lebih baik, yaitu menggunakan IPSec (Ikhwan & Amalina, 2017). Sedangkan *tunneling* adalah dasar dari VPN untuk membuat suatu jaringan *private* melalui jaringan internet (RACHMAWAN, 2018). Teknologi VPN dan *tunneling* ini akan melakukan enkapsulasi data pada jaringan yang melewatinya.

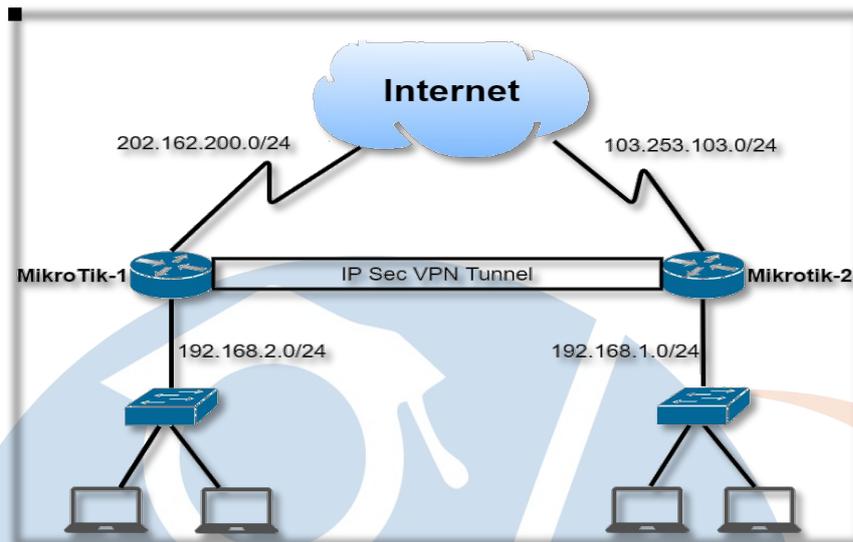


Gambar 2.11 L2TP Tunnel

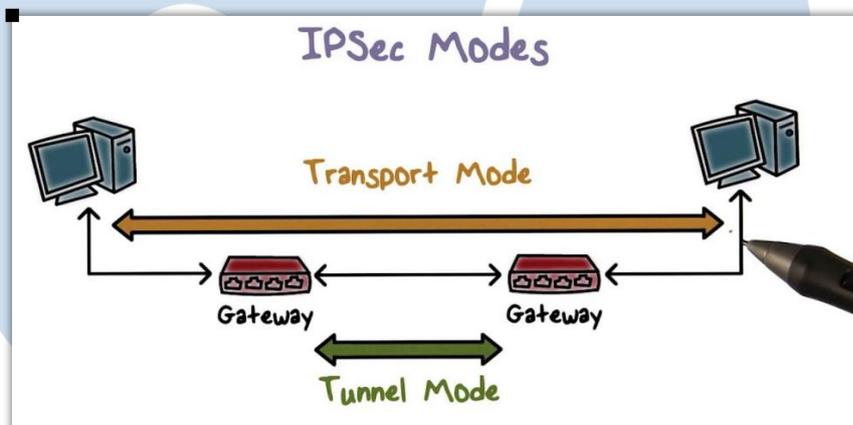
- **IPSec (IP Security)**

IPSec merupakan *tunneling protocol* yang berkerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih *protocol* keamanan yang diperlukan, algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta (Zamalia et al., 2018).

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalu lintas yaitu *Authentication Header* (AH) dan *Encapsulating Security Payload* (ESP). Implementasi IPSec harus mendukung ESP dan juga AH. Protokol AH menyediakan integritas hubungan, otentikasi data asal dan layanan anti jawaban sedangkan protokol ESP menyediakan kerahasiaan (enkripsi), dan pembatasan aliran lalu lintas kerahasiaan. ESP juga menyediakan layanan. Kedua protokol ini merupakan pembawa kontrol akses berbasis distribusi kunci kriptografi dan manajemen aliran lalu lintas relatif terhadap protokol keamanan.



Gambar 2.12 Jaringan IPsec



Gambar 2.13 IPsec Modes

### 2.1.7 Video Conference (Jitsi)

*Video conference* adalah teknologi yang digunakan untuk berkomunikasi jarak jauh dalam bentuk visualisasi video/audio dengan menggunakan komputer dan media internet. Dalam penjelasan lain *video conference* merupakan teknologi untuk telekomunikasi interaktif yang memungkinkan untuk berinteraksi secara dua arah dengan audio dan video.

Berikut ini adalah kelebihan dan kekurangan menggunakan teknologi *video conference*:

Kelebihan *video conference* :

- Memudahkan untuk pertemuan secara *online*
- Fleksibel
- Menghemat waktu

Kekurangan *video conference*:

- Memerlukan koneksi yang stabil
- Memerlukan alat untuk melakukan *video conference*

Jitsi adalah *communicator open source* yang memungkinkan panggilan konferensi video/audio dilakukan secara aman (Laksmiati, 2019). Sederhananya Jitsi merupakan salah satu alat yang bisa digunakan untuk melakukan *video conference*. Jitsi merupakan serangkaian proyek sumber terbuka. Pada aplikasi Jitsi pengguna tidak perlu membuat akun untuk melakukan *video conference*, cukup membuat ruangan untuk melakukan *conference* lalu ruangan tersebut diberikan akses ke pengguna agar bisa bergabung untuk telekomunikasi.

Fitur-fitur Jitsi:

- Tersedia fitur *chatting*
- Fitur *share screen*
- Memberikan keamanan *password*
- Latensi yang rendah
- *Scalable* dan murah

STT - NF

## 2.2 Penelitian Terkait

Tabel 2.2 Penelitian Terkait

No	Nama	Tahun	Judul	Hasil
1	Rahmat Hidayat	2018	Perancangan Dan Implementasi <i>Virtual Private Network</i> (VPN) Berbasis Layer 2 <i>Tunneling Protocol</i> (L2TP) Dan IPsec Dengan Menggunakan Router MikroTik	Interkoneksi Antar Kantor dengan aman melalui VPN L2TP dan IPsec.
2	Aditya Prasetya	2011	Perancangan Dan Penerapan Teknologi VPN ( <i>Virtual Private Network</i> ) Untuk Komunikasi Data	Jaringan Gardanet Cooperation bisa diakses dimana saja selama terhubung dengan internet dan memberikan keamanan data yang terjamin.
3	Dewi Laksmiati	2019	Implementasi <i>Cloud Based Video Conference System</i> Menggunakan Jitsi	Pengujian Kinerja Server untuk <i>Video Conference</i> Jitsi