# BAB II

# DASAR TEORI

Dalam simulasi dan Analisa *QOS* pada jaringan *VPN* berbasis ***IPSec*** terlebih dahulu perlu dipahami teori-teori dasar mengenai *Virtual Private Network(VPN), IPSec tunnel*, dan *routing OSPF, EIGRP* dan *RIP* .

## 2.1 Referensi jurnal terkait dalam penelitian

Adapun beberapa referensi jurnal terkait dalam penelitian adalah:

### 2.1.1 Analisis Dan Simulasi Perbandingan *QoS* Di *Routing Protokol* MPLS *OSPF* dan MPLS IS-IS Di Jaringan Ipv6 Menggunakan Gns3 Untuk Layanan Video Streaming Arisman, Rendy & Doan (2018)

Dalam Jurnal ini telah dilakukan penelitian *QoS* pada *routing* pada VPN dengan *protocol* MPLS dengan *routing OSPF* dan IS-IS untuk layanan video *streaming*. Hasil simulasi dan analisis yang didapat pada penelitian tersebut bahwa *routing protocol* IS-IS yang tidak diterapkan MPLS ataupun dengan MPLS xconnect mendapatkan hasil *QoS* yang lebih baik dari pada *OSPF* di jaringan IPv6. dilihat dari perbedaan *throughput* hingga 61 Kbps, delay 6 ms, *packet loss* 3% dan jitter sebesar 3ms. Hal ini disebabkan *routing* protocol *OSPF* memiliki kompleksitas yang lebih tinggi karena pengenalan *neighbour* OSPF yang lebih rumit di bandingkan IS-IS

### 2.1.2 *IPSec VPN Tunnel* Sebagai Alternatif Keamanan Konektivitas Antar Network, Fajri, Doan & Leanna (2018)

Berdasarkan hasil simulasi pada penelitian tersebut menunjukkan bahwa *IPSec vpn tunnel* bekerja dengan baik. Hasil dari simulasinya dapat dilihat dengan menggunakan *software wireshark*. Sedangkan untuk hasil uji performansi jaringan, jaringan dengan menggunakan tambahan security memiliki hasil yang lebih baik dibandingkan dengan jaringan yang tidak menggunakannya saat terjadi serangan (*throughput* sebesar 1253.16 kbps, delay 394.17ms, packet loss 9.22%). Hasil *QoS* yang diberikan serangan blackhole tanpa tambahan security mengalami penurunan. Untuk uji skenario menggunakan serangan rushing dan tanpa tambahan security terhadap perubahan jumlah node menghasilkan rata-rata nilai throughput sebesar 740.76 kbps, packet loss sebesar 2.2%, dan delay sebesar 233.53ms.Sedangkan skenario dengan tambahan security mengalami kenaikkan nilai *QoS*.

**2.1.3 *Design and Analysis QoS VOIP using BGP*, Eko Ramadhan, Ahmad Firdausi, Setiyo Budiyanto (2017)**

Dalam penelitian ini dilakukan design dan Analisa *QoS* dengan menggunakan routing *BGP* pada layanan voice dengan SIP protocol dan codec G.711. Pada penelitian ini pengukuran dilakukan pada tiga *bandwidth* yang berbeda yaitu 64Kbps, 128Kbps dan 256 Kbps. Hasil dari rata-rata pengukuran tiga kali percobaan dengan *bandwidth* 64Kbps adalah paket terkirim 2.143,33 dengan rata-rata delay 0,020003 s. *jitter* 10,24 ms, paket loss 0 dan *throughput* 25,167 bytes/s. pada percobaan dengan *bandwidth* 128Kbps adalah paket terkirim 1.910,33, delay 0,020029, Jitter 10,46 paket loss 0 dan throughput 35.839 bytes/s. pada pengukuran dengan bandwidth 256 Kbps didapatkan hasil paket terkirim 1.814,33 delay 0.019995 jitter 9.84 paket loss 0 throughput 36.748 bytes/s

**2.1.4 Perbandingan Kinerja *Routing IGP* Pada Jaringan VPN Berbasis MPLS Dan Direct-Link Backup penilitian dilakukan oleh Dimas Widya Putra Pratama , Ida Nurhaida (2018).**

Pada penelitian ini metode yang dilakukan adalah membandingkan waktu *konvergensi* dan *QoS* di antara tiga protokol *IGP routing*, yaitu *RIP* (versi 2), *OSPF* (single area dan sham-link), dan *EIGRP* (dengan dua nomor sistem otonom) dengan

desain topologi Ring antara Pusat Data dan DRC. Hasilnya menunjukkan bahwa QoS dalam tiga protokol routing memiliki tingkat kualitas yang baik sesuai dengan standar TIPHON dengan jumlah Indekses hingga 3.25 (Baik) dan waktu konvergensi tercepat ketika ada gangguan pada link utama (VPN) yaitu *EIGRP* dengan waktu konvergensi selama sekitar 15 detik.

**2.1.5 Analisis Performansi *Quality Of Service* I*nter As MPLS-VPN Backto-Back VRF* Pada Layanan IMS Sabrina Rendy Munadi,Danu Dwi Sanjoyo (2018)**

Pada penelitian ini telah dilakukan pengujian performansi kualitas layanan IMS yang dijalankan pada jaringan *backbone* berbasis *Inter* AS MPLS VPN *background traffic* 0, 1, 5, 10, 20 Mbps. Hasilnya menunjukan nilai throughput berbanding terbalik dengan besarnya nilai background traffic. Nilai *throughput* pada layanan *VoIP* menurur dari nilai sebesar s.d 0,08576 Mbps s.d. 0,06265 Mbps dan menurun sebesar 0,6802 Mbps s.d 0,5806 Mbps pada layanan video *call*. Pada kedua layanan didapatkan nilai *jitter* rata- rata << 1 ms dan *delay* < 150 ms. Dan didapatkan nilai *packet loss* dari kedua layanan pada kedua metode masuk kedalam kategori layak untuk background traffic 0 Mbps , 1 Mbps , dan 5 Mbps.

Klarifkasi kelima jurnal di atas akan diuraikan seperti pada table 2.1 berikut.

Tabel 2.1 Tinjauan Jurnal

| No | Nama Jurnal | Penulis | Tahun | Metode |
|---|---|---|---|---|
| 1 | Analisis Dan Simulasi Perbandingan *Qos Di Routing Protokol Mpls Ospf* Dan *Mpls* Is-Is Di | Arisman, Rendy & Doan | 2018 | Membandingkan *QoS* di *routing OSPF* dan IS-IS pada jaringan *MPLS*. |
| 2 | *Ipsec Vpn Tunnel* Sebagai Alternatif Keamanan Konektivitas Antar Network | Fajri & Leanna | 2018 | Membuat sebuah *VPN tunnel* kemudian dilakukan Analisa terhadap *QoS* |
| 3 | *Design and Analysis QoS VOIP using BGP* | Eko Ramadhan, Ahmad Firdausi, Setiyo Budiyanto (2017) | 2017 | Design dan Analisa *QoS* pada layanan *VoIP* dengan menggunakan routing *BGP* |
| 4 | Perbandingan Kinerja *Routing IGP* Pada Jaringan *VPN* Berbasis *MPLS* Dan *Direct-Link Backup* | Dimas Widya Putra Pratama , Ida Nurhaida | 2018 | Membandingkan waktu konvergensi dan *QoS* di antara tiga protokol *IGP routing*, yaitu *RIP (versi 2)*, *OSPF* dan *EIGRP* |
| 5 | Analisis Performansi *Quality Of Service Inter As MPLS-VPN* | Sabrina Rendy Munadi,Danu Dwi Sanjoyo | 2018 | pengujian performansi kualitas layanan IMS yang dijalankan pada jaringan *backbone* berbasis *Inter* AS *MPLS VPN* |

| No | Nama Jurnal | Penulis | Tahun | Metode |
|---|---|---|---|---|
| 6 | Simulasi dan Analisa *QoS* dalam Jaringan VPN *site to site* berbasis *IPSec* dengan *routing dynamic* | Hamam Wira W, Ahmad Firdausi | 2020 | Melakukan pengukuran *QoS* pada jaringan VPN dengan *IPSec* pada *layanan VoIP* |

## 2.2 *Virtual Private Network ( VPN )*

*Virtual Private Network (VPN)* adalah sebuah teknologi komunikasi yang memungkinkan pengguna untuk dapat terkoneksi ke jaringan publik (internet) dan menggunakan jaringan publik tersebut untuk dapat bergabung dengan jaringan lokal. Pembentukan VPN dapat dilakukan dengan menggunakan teknologi tunneling dan enkripsi. Komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan, hal tersebut dikarenakan koneksi VPN dapat terjadi pada semua layer pada protokol OSI. Oleh sebab itu banyak instansi, perusahaan atau organisai menggunakn VPN untuk berkomunikasi.( Fajri & Leanna, 2018)

### 2.2.1 Fungsi VPN

Teknologi VPN memiliki tiga fungsi utama, yaitu :

1. *Confidentially* Dengan digunakannya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan system kerja dengan cara mengenkripsi semua data yang lewat melaluinya.

2. *Data Integrity* Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai data dikirim hingga data sampai di tempat tujuan.

3. *Origin Authentication* Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. (Farooq, Zain, Uzair, 2016)

### 2.2.2 Teknologi VPN

VPN memadukan dua teknologi dari teknologi tunneling dan teknologi enkripsi.

1. Tunneling Tunneling merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi point-to-point dari sumber ke tujuannya. Pada tunnel terdapat sebuah sistem enkripsi yang berfungsi untuk menjaga data yang melewati tunnel tersebut, sehingga data yang melewati tunnel tetap aman. Proses enkripsi inilah yang menjadikan teknologi VPN aman dan bersifat pribadi

2. Enkripsi Teknologi enkripsi menjamin data yang berlalu-lalang di dalam tunnel tidak dapat di baca dengan mudal oleh orang lain yang bukan merupakan komputer tujuan. Informasi yang berada pada tunnel akan dirubah menggunakan teknologi enkripsi menjadi sebuah chipertext atau teks yang dikacaukan dan tidak ada artinya sama sekali apabila dibaca secara langsung. Jika ingin membacanya atau menjadikannya memiliki arti kembali maka harus dilakukan proses dekripsi. Proses dekripsi ini terjadi di ujung-ujung VPN sehingga penerima akan mendapatkan informasi yang sudah bisa di baca. (Farooq, Zain, Uzair, 2016)



### 2.2.3 Implementasi VPN

Jenis Implementasi VPN Pada kenyataannya VPN banyak diimplementasikan oleh perusahan - perusahaan yang memiliki banyak kantor cabang perusahaan dan juga memiliki banyak pegawai untuk melakukan komunikasi jarak jauh antar perusahan. VPN diimplementasikan menjadi dua jenis yaitu:

1. *Remote Access VPN* atau dikenal juga dengan virtual private dial-up network (VPDN), merupakan implementasi VPN yang menghubungkan antara pengguna yang mobile dengan local area network (LAN). Pengimplementasian remote access VPN ini biasanya digunakan oleh karyawan perusahan untuk mengakses data yang ada di

perusahaannya, metode remote acces VPN ini sangat efisien dan juga bisa di akses oleh banyak user tergantung dari pengaturan jumlah user yang diperbolehkan untuk mengakses VPN tersebut.

2. *Site-to-site VPN* menghubungkan antara dua tempat yang letaknya berjauhan seperti halnya kantor pusat dengan kantor cabang atau suatu perusahaan dengan mitra kerjanya. Dibandingkan dengan remote access VPN, site-to-site VPN bersifat lebih kaku karena pengaksesan VPN haya bisa dilakukan melalui satu site ke site lain. Dengan kata lain siteto-site VPN tidak bisa di akses dari mana saja atau bersifat statis, sehingga mobilitas pengguna site-to-site VPN sangat terbatas. (Farooq, Zain, Uzair, 2016)

## 2.3 Jaringan Komputer

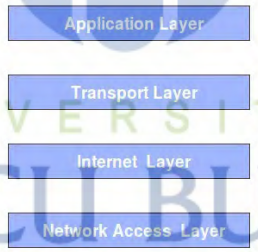
Jaringan komputer adalah sekumpulan komputer yang dapat saling berhubungan antara satu dengan lainnya dengan menggunakan media komunikasi, sehingga dapat saling berbagi data, informasi, program, dan perangkat keras. Komputer – komputer tersebut bisa saja memiliki tipe yang berbeda-beda, menggunakan sistem operasi yang berbeda, dan menggunakan program atau aplikasi yang berbeda pula. Tetapi komputer-komputer yang terhubung dalam jaringan komputer harus memakai aturan komunikasi (protokol) yang sama. Hal ini dimaksudkan agar masing-masing komputer dapat berkomunikasi yang baik dengan komputer lainnya. Protokol yang menjadi Standar Internasional adalah TCP/IP (Transmission Control Protocol / Internet Protocol).

## 2.4 TCP/IP

*Transmission Control Protocol* atau internet protokol dikembangkan pada awal 1970 oleh DARPA (*Defense Advanced Research Projects Agency*) bertujuan untuk mengembangkan sebuah protokol yang dapat melakukan interkoneksi antar jaringan komputer yang terpisah dan memiliki jaringan-jaringan berbeda-beda untuk membentuk sebuah jaringan yang lebih luas (*Wide Area Network*). Protokol ini

awalnya dibangun untuk universitas dan militer serta para peniliti untuk membagi data dan penemuan. Pengalamatan yang digunakan oleh internet prokol disebut alamat IP (IP *address*) yang mengizinkan berjuta-juta komputer dapat terhubung satu sama lain dalam internet. Karna sifatnya *routable* internet protokol dapat menghubungkan sistem-sistem berbeda contohnya, *microsoft windows* dan keluarga UNIX.

Dengan seiringnya waktu, perkembangan akan kebutuhan jaringan komputer dan internet meningkat beberapa badan organisasi melakukan riset dan pengembangan tentang TCP/IP yaitu, *Internet Architecture Board* (IAB) dan *Internet Engineering Task Force*. *Request For Comments* (RFC) yang mendifinisikan segala macam protokol yang berjalan di atas TCP/IP dari segi skema pengalamatan dan konsep TCP/IP yang dikeluarkan oleh IETF. Macam-macam protokol tersebut dapat dijelaskan dalam TCP/IP *suite* yang merupakan sekelompok mengatur komunikasi data untuk dari satu komputer ke komputer yang lain dalam jaringan internet untuk memastikan pengiriman paket sampai ke alamat yang dituju.




Gambar 2.2 Contoh Model TCP/IP

TCP/IP protokol *suite* terdiri dari 4 *layers*, yaitu layer *Application*, *Transport*, *Internet Layer*, dan *Network Interface Layer*, yaitu :

- *Application Layer*

  Menyediakan akses kepada aplikasi layanan jaringan TCP/IP seperti, HTTP, FTP, *email* dan *web browser*.
- *Transport Layer*

*Transport layer* yang mengatur untuk komunikasi antara aplikasi. Menggunakan sesi koneksi yang bersifat *connection-oriented* dan *connectionless*.

- *Internet Layer*

  Bertanggung jawab untuk pemetaan (*routing*) dan enkapsulasi paket-paket data jaringan menjadi paket-paket IP. Protokol yang bekerja pada lapisan ini adalah *internet protocol* (IP), ICMP, dan IGMP

- *Network Interface Layer*

  Merupakan level yang paling bawah dari TCP/IP. *Layer* ini dapat bekerja dengan banyak teknologi *transport*, menggunakan jaringan sebuah kabel, *ethernet, frame relay, token ring,* ISDN, dll.

### *2.5 IPSec*

*Internet Protocol Security* atau sering disebut *IPsec* adalah *end-to-end security* skema operasi di Internet Layer dari Internet Protocol Suite. Hal ini dapat digunakan dalam melindungi arus data antara sepasang *host (host-to-host),* antara sepasang *gateway* keamanan (jaringan-jaringan), atau antara gateway keamanan dan host (jaringan-to-host) .



*Internet Protocol Security (IPsec)* adalah protokol untuk mengamankan Internet Protocol (IP) komunikasi dengan otentikasi dan mengenkripsi setiap paket IP dari suatu sesi komunikasi. IPsec juga mencakup protokol untuk mendirikan otentikasi bersama antara agen pada awal sesi dan negosiasi kunci kriptografi yang akan digunakan selama sesi. Beberapa sistem keamanan Internet lainnya digunakan secara luas, *seperti Secure Socket Layer (SSL), Transport Layer Security (TLS)* dan *Secure Shell (SSH),* beroperasi di lapisan atas dari model TCP / IP. Di masa lalu, penggunaan TLS / SSL harus dirancang ke dalam aplikasi untuk melindungi protokol aplikasi. Sebaliknya, sejak hari pertama, aplikasi tidak perlu dirancang khusus untuk menggunakan IPsec. Oleh karena itu, IPsec melindungi lalu lintas aplikasi di jaringan IP.( Fajri, Doan & Leanna 2018)

### 2.6 *Routing Dynamic*

*Dynamic routing* merupakan mekanisme *routing* dimana *table routing* berubah secara dinamik mengikuti kondisi suatu jaringan. Berbeda dengan *static routing* yang biasa digunakan untuk jaringan dengan skala yang kecil *dynamic routing* digunakan pada jaringan yang berskala besar. Pada *dynamic routing* terbagi menjadi 2 *routing protocol* yaitu *distance vector*, dan *link state*.

#### 2.6.1 *OSPF*

*Open Shortest Path First (OSPF)* adalah suatu protocol routing yang handal dengan fasilitas *least-cost routing*, *multipath routing* dan *load balancing*. Penentuan jalur tercepat dan terbaik pada jaringan dihitung dengan metode algoritma *Dijkstra*. Pertama router menggunakan paket "*hello*" untuk mengindentifikasi informasi interface sekitarnya dan membangun *adjacencies* (hubungan untuk pertukaran update routing) dengan yang lain. Selanjutnya router memulai dengan fase ExStart, dengan mempertukarkan database inisial. Selanjutnya fase pertukaran ini masuk dalam pengiriman informasi routing pada pembuatan jalur dan menerima acknowledgment (ack) yang diterima dari router baru. Selama fase loading, router baru mengkompilasi table routing. (Arisman, Rendy & Doan, 2018)

#### 2.6.2 *RIP*

*Routing Information Protokol (RIP)* adalah standard dasar dari protocol routing distance vector, Interior gateway. RIP menggunakan hop *count* untuk menentukan jalur terbaik diantara dua lokasi. Setiap paket melewati router maka dihitung 1 hop. *Maximum* yang dapat dijangkau oleh protokol routing RIP adalah 15 hop. RIP terdapat dua versi yaitu RIP versi 1 dengan RIP versi 2.( Dimas Widya Putra Pratama , Ida Nurhaida, 2018)

#### 2.6.3 *EIGRP*

EIGRP (Enhanced Interior Gateway Routing Protocol) adalah routing protocol yang hanya di adopsi oleh router cisco atau sering disebut sebagai proprietary protocol

pada cisco. Dimana *EIGRP* ini hanya bisa digunakan sesama router cisco saja. *EIGRP* akan mengirimkan hello packet utk mengetahui apakah router-router tetangganya masih hidup ataukah mati. Pengiriman hello packet tersebut bersifat simultant, dalam hello packet tersebut mempunyai hold time, bila dalam jangka waktu hold time router tetangga tidak membalas, maka router tersebut akan dianggap mati. Biasanya hold time itu 3x waktunya hello packet, hello packet defaultnya 15 second. Lalu DUAL akan meng-kalkulasi ulang untuk path-pathnya. Hello packet dikirim secara multicast ke IP Address 224.0.0.10.

### 2.7 *Static Routing*

*Static routing table* dibuat, dipertahankan, dan di-*update* oleh *network administrator* secara manual. *Static route* ke semua jaringan harus dikonfigurasi pada setiap *router* untuk mendapatkan konektifitas secara utuh. *Static routing* biasa digunakan pada jaringan skala kecil dan tidak disarankan untuk digunakan pada jaringan skala besar.

### 2.8 *Quality of Service*

*Quality of Service (QoS)* adalah metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefiniskan karateristik dan sifat dari suatu service. *QoS* digunakan untu mengatur sekumpulan datribut kinerja yang telah dispesifikasikan dengan suatu service.Berikut ini merupakan parameter yang digunakan dalam menghitung *QoS.* (Sabrina Rendy Munadi,Danu Dwi Sanjoyo, 2018).

#### 2.8.1 *Delay*

Waktu yang dibutuhkan untuk sebuah paket untuk mencapai tujuan, karena adanya antrian yang panjang atau mengambil rute yang lain untuk menghindari kemacetan. *Delay* dapat dicari dengan membagi antara panjang paket (L, *packet length* (bit/s)) di bagi dengan *link bandwidth (*R, *link bandwidth (bit/s)).*Nilai yang dikategorikan oleh ITU-T G114 untuk *delay* yang bagus (*good*) yaitu kurang dari 150 ms. [7]

*Tabel 2.2 Rekomendasi ITU-T G114 untuk delay.*

| Kategori *Delay* | Besar *Delay* |
|---|---|
| Baik sekali | < 150 ms |
| Bagus | 150 s/d 300 ms |
| Buruk | 300 s/d 450 ms |
| Tidak dapat diterima | >450 ms |

*Delay* memiliki jenis yang dapat digolongkan dalam jaringan yaitu :

- *Delay Propagasi* merupakan waktu proses perjalanan informasi selama dalam media transmisi.
- *Queuing Delay*, *delay* yang disebabkan oleh proses waktu yang diperlukan oleh *router* dalam menangani paket di sepanjang jaringan. Umumnya *delay* ini memiliki *delay* yang sangat kecil yaitu hanya 100 *micro second.*
- *Packetisasi Delay*, *delay* yang disebabkan oleh waktu yang diperlukan untuk proses pembentukan paket IP dari informasi *user*. *Delay* ini terjadi hanya sekali yaitu *source* informasi.
- *Component Delay*,*delay* yang disebabkan oleh banyaknya komponen yang digunakan dalam sistem transmisi.
- *Code* (*processing*) *delay, delay* ini disebabkan oleh standar *codec* yang digunakan.

### 2.8.2 *Packet Loss*

Packet loss merupakan banyaknya paket yang gagal dikirimkan ke tujuan pada saat pengiriman paket. Namun pada protokol TCP yang bersifat connection oriented ketika paket gagal maka paket tersebut akan dikirimkan kembali, oleh karena itu inilah TCP juga disebut juga dengan koneksi yang reliable atau dapat diandalkan. Akan tetapi tidak menutup kemungkinan adanya paket yang gagal terkirim.Tabel 2.2 Standar *Packet Loss* Berdasarkan ITU G.114 [7]

Tabel 2.3 Standar packet loss

| NO | *Packet Loss* (%) | Kualitas |
|---|---|---|
| 1. | 0 % | Baik |
| 2. | 1 – 5 % | Dapat diterima |
| 3. | > 10 % | Tidak dapat diterima |

### 2.8.3 *Throughput*

*Throughput* adalah kecepatan (*rate*) transfer data efektif, yang diukur dalam satuan bps (bits per second). *Throughput* merupakan jumlah total kedatangan paket yang berhasil diamati pada *destination* selama interval waktu tertentu dibagi durasi interval waktu tersebut. [7]

$$Throughput = \frac{\text{Jumlah data yang sukses diterima}}{\text{Jumlah total pengiriman paket}} \text{ (Satuan bps).}$$

Menurut ITU-T H.261 besarnya *bit error rate code* video untuk layanan audiovisual > 64 kbit/s atau > 8kB/s.

## *2.9 VoIP*

*Voice over Internet Protocol* adalah teknologi yang menjadikan media internet untuk bisa melakukan komunikasi suara jarak jauh secara langsung. Sinyal suara analog, seperti yang anda dengar ketika berkomunikasi di telepon diubah menjadi data digital dan dikirimkan melalui jaringan berupa paket-paket data secara real time. Dalam komunikasi *VoIP*, pemakai melakukan hubungan telepon melalui terminal yang

berupa PC atau telepon biasa. Dengan bertelepon menggunakan *VoIP*, banyak keuntungan yang dapat diambil diantaranya adalah dari segi biaya jelas lebih murah dari tarif telepon tradisional, karena jaringan IP bersifat global. Sehingga untuk hubungan Internasional dapat ditekan hingga 70%. Selain itu, biaya *maintenance* dapat di tekan karena *voice* dan data *network* terpisah, sehingga IP Phone dapat di tambah, dipindah dan di ubah. Hal ini karena VoIP dapat dipasang di sembarang ethernet dan IP address, tidak seperti telepon konvensional yang harus mempunyai port tersendiri di Sentral atau *PBX* (Rismada, Dodi, Erwid 2019)

## 2.10 *Asterisk*

*Asterisk* adalah *software IP PBX* untuk membuat sistem layanan komunikasi telepon melalui internet atau biasa disebut *VoIP (Voice over Internet Protocol). Asterisk* merupakan *software open source* yang berjalan pada sistem operasi berbasis Linux. Asterisk salah satu *software server VoIP* yang di distribusikan melalui GPL (General Public License). Asterisk disebut juga IP PBX, karena memiliki fungsi dan kemampuan layaknya PBX namun berbasis IP. Asterisk digunakan untuk membangun suatu sistem layanan komunikasi serta memberikan kemudahan kepada penggunanya untuk mengembangkan suatu sistem layanan komunikasi serta telepon sendiri dengan kustomisasi yang seluas-luasnya diberikan kepada pihak pengguna. (Rismada, Dodi, Erwid 2019)