BAB II
LANDASAN TEORI

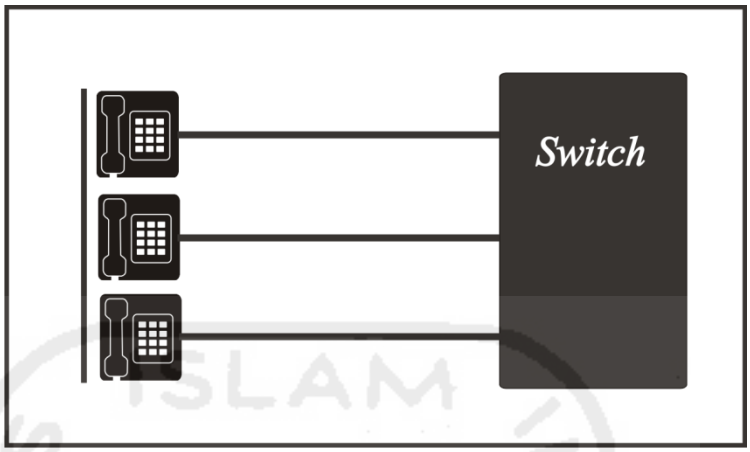
2.1. IP PBX

2.1.1 Pengertian IP PBX

IP PBX adalah *Private Branch Exchange* (PBX) yang memanfaatkan *Internet Protocol*, dalam membentuk komunikasi telepon. IP PBX dibangun sebagai konsep jaringan komunikasi generasi masa depan, sebab ia mampu memadukan antar jaringan, seperti jaringan PSTN (jaringan telepon tetap dengan memanfaatkan kabel), jaringan telepon bergerak (GSM/CDMA), jaringan telepon satelit, jaringan *Cordless* (DECT), dan jaringan telepon berbasis paket *Internet Protocol*/ATM (Raharja, 2010). Dengan konsep tersebut, IP PBX dapat mengendalikan hubungan telepon secara penuh. Pengendalian dilakukan, melalui perangkat-perangkat IP *Telephony*, yakni VoIP *Gateway*, *Access Gateway*, dan *Trunk Gateway*. Karena keunggulan yang dimilikinya, perangkat ini menjadi induk dari kinerja dasar VoIP, dalam melakukan transmisi suara dan data.

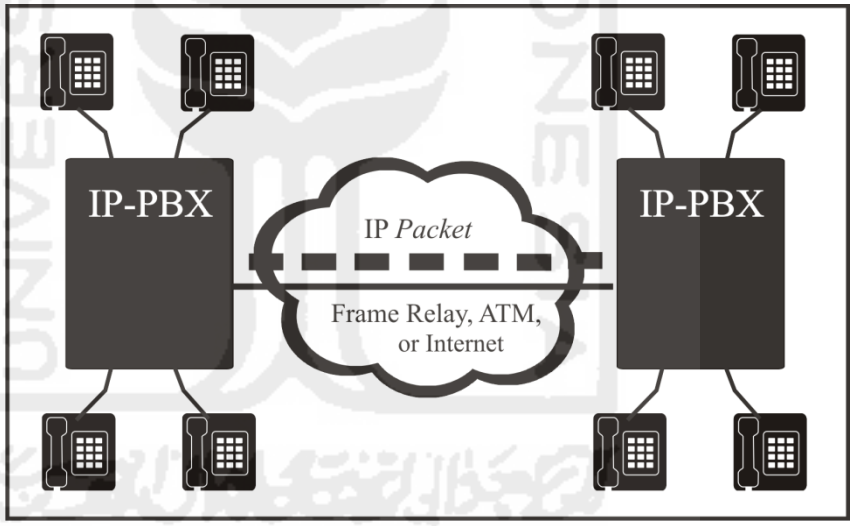
Kehadiran IP PBX telah memberikan kontribusi yang baik pada dunia telekomunikasi. Dengan menggunakan perangkat ini, komunikasi dapat dijalankan dengan lebih efektif dan efisien. Hal ini karena, jumlah *line* yang digunakan IP PBX, tidak menyesuaikan dengan jumlah telepon yang terpasang, seperti yang diterapkan dalam jaringan PSTN. Oleh karena itu, pemasangan IP PBX dapat menghemat biaya pengeluaran, pembangunan, serta perawatan jaringan (Edvian, 2010). Berikut topologi, untuk menggambarkan perbedaan terkait konsep jaringan PSTN dan IP PBX tersebut.

a) Topologi PSTN (Jumlah Telepon = Jumlah *Line*)



Gambar 2.1 Topologi PSTN

b) Topologi IP PBX (Jumlah Telepon > Jumlah *Line*)



Gambar 2.2 Topologi IP PBX

2.1.2 Konsep Kerja IP PBX

Perangkat IP PBX bergerak, dengan menggunakan metode *packet switching*, yakni metode yang digunakan dalam memindahkan data di *internet*, seperti yang telah disinggung pada bab satu. Paket data yang dikirim dengan menggunakan jaringan ini, akan diubah dalam bentuk digital dan dilakukan enkripsi. Selanjutnya, paket dikembalikan dalam bentuk analog (suara), sebelum paket sampai ke tujuan**.** Pengubahan data dari digital ke analog maupun sebaliknya, dilakukan dengan menggunakan pesawat telepon khusus. Penyebutan pesawat telepon tersebut, untuk masing-masing vendor berbeda, misalnya Vendor Panasonic, mereka menyebutnya *key telephone*, atau *digital phone*, sedangkan *Network Interface Card* (NEC), menyebut perangkat ini *multi line terminal*, dll (Telemedia, 2014).

Dalam implementasinya, perangkat IP PBX membutuhkan sekumpulan nomor ekstensi yang diletakkan pada masing-masing perangkat telepon, baik *softphone* maupun *hardphone*. Tujuannya, sebagai identitas untuk melakukan hubungan komunikasi. Identitas harus dalam kondisi terdaftar, agar klien dapat melakukan panggilan ke nomor ekstensi yang lain, melalui *server* IP PBX (Simatupang, 2015). Pendaftaran tersebut dilakukan dengan memanfaatkan protokol *signaling*, yakni protokol yang berfungsi menghubungkan dan menjaga lalu lintas data dan suara, agar sampai ke tujuan (Farizqi, 2012).

2.2. VoIP

2.2.1. Pengertian VoIP

VoIP merupakan singkatan dari *Voice over Internet Protocol***.** Seperti yang dijelaskan pada sub bab sebelumnya, VoIP adalah salah satu bagian dari perangkat IP PBX, yang digunakan sebagai jalur komunikasi. Ada banyak vendor yang mendukung keberadaan VoIP ini, yaitu Asterisk, Avaya, Cisco, Linksys, Microsoft Office, Nortel, Siemens, dll (Edvian, 2010).

Dalam pengerjaan tugas akhir ini, penulis menggunakan salah satu vendor, yaitu Asterisk Digium. Vendor tersebut yang akan penulis gunakan sebagai *server* VoIP dalam uji coba nantinya. Penulis memilih perangkat tersebut, karena sifatnya yang *open source*, sehingga teknik pembangunannya dapat diketahui dari berbagai sumber.

2.2.2. Manfaat VoIP

Dalam bukunya yang berjudul "Membangun Telepon berbasis VoIP", Winarno Sugeng (2008), peneliti Jaringan Komputer dan Sistem Operasi Linux, menyebutkan, ada beberapa manfaat yang dapat diperoleh dari penggunaan VoIP, yaitu:

a) Alokasi *bandwidth* menjadi lebih efisien
b) Adanya kemampuan untuk menggunakan metode kompresi suara
c) Mampu menggunakan *single interface*
d) Meningkatkan keandalan jaringan komputer
e) Dapat menekan biaya operasional hingga mendekati gratis (Rp 0,-), misalnya untuk SLI atau SLJJ.

Manfaat yang terakhir itulah, yang ditunggu-tunggu kehadirannya oleh masyarakat. Hanya saja untuk di Indonesia, komunikasi telepon melalui jaringan *internet*, masih belum 100% gratis. Hal ini dikarenakan, pemakaian *internet* di Indonesia masih dibebani biaya pulsa. Berbeda dengan kondisi di negara maju, dimana pemakaian *internet* telah gratis, sehingga pemakaian VoIP pun juga gratis.

2.2.3. Unsur Pembentuk VoIP

Berdasarkan buku yang ditulisnya tersebut, Winarno Sugeng menjelaskan empat unsur pembentuk VoIP, yakni

2.2.3.1. *User Agent*

User agent berfungsi layaknya telepon yang kita kenal, yakni melakukan panggilan maupun menerima panggilan dari telepon lain. *User agent* merupakan perangkat pendukung yang melengkapi penggunaan VoIP. Ada yang berupa *software* dan juga *hardware*.

Dengan *user agent*, kita dapat melakukan panggilan antar komputer, komputer dengan *IP Phone*, maupun komputer dengan PSTN. Untuk sambungan dengan PSTN, dibutuhkan tambahan alat berupa ATA (*Analog Telephone Adaptor*), untuk mengubah sinyal telepon dari analog ke digital.

Ada banyak *user agent* yang dapat diperoleh secara gratis di *internet*. Tentu saja, ini hanya berlaku untuk *user agent* berbasis *software*, meskipun ada pula yang berbayar, seperti Eyebeam misalnya. Sedangkan penulis sendiri, akan menggunakan *user agent* Zoiper, karena gratis dan dapat diletakkan pada *platform* manapun.

2.2.3.2. *Proxy*

Proxy digunakan sebagai penghubung antara jaringan *server* dengan jaringan klien. *Proxy* inilah yang bertugas mengendalikan, maupun memonitor lalu lintas data yang melewatinya (Adhitya, 2014). *Proxy* dapat berupa *web proxy*, FTP klien, dll. *Proxy* yang bersifat *open source*, ada bermacam-macam, yakni Asterisk, OpenSER, SER, Yate, dll. Penulis sendiri akan menggunakan *proxy* dari *Mikrotik RouterOS*, yang dikonfigurasi melalui Winbox, untuk pengerjaan tugas akhir ini.

2.2.3.3. Protokol

Dalam menjalankan tugasnya, VoIP membutuhkan kerja sama dari dua protokol, yaitu protokol *signaling* dan protokol *transport*. Meski berbeda fungsi, protokol tersebut saling terhubung satu sama lain. Pendapat ini dikutip dari tugas akhir, milik salah satu mahasiswi UII, Yanuarika Insanul R. F. (2012). Berikut penjabaran kedua protokol.

a. Protokol *Signaling*

Protokol *signaling* berfungsi menjaga dan menjamin paket data dan suara yang terkirim, benar-benar sampai ke tujuan. Protokol ini juga, yang mengatur seluruh operasi di dalam jaringan VoIP, sehingga dengan adanya protokol ini, pengguna VoIP dapat saling berkomunikasi satu sama lain.

Dalam perkembangannya, protokol ini telah mengalami beberapa kali perbaikan, sehingga menghasilkan tiga jenis protokol *signaling*, yaitu H.323, SIP, dan IAX2. Berikut penjabaran mengenai ketiga protokol.

a) H.323

Protokol H.323 adalah protokol *signaling* pertama diterbitkan oleh ITU-T (*International Telecommunications Union-Telecommunication*). Protokol ini diciptakan sebagai standar protokol *signaling* dalam mengatur percakapan suara. Penggunaannya tergolong rumit. Lebih rumit daripada penggunaan SIP, sehingga jarang digunakan untuk saat ini.

b) *Session Initial Protocol* (SIP)

Meskipun tidak menyediakan layanan secara langsung, protokol ini justru menyediakan fondasi yang dapat digunakan oleh protokol aplikasi lainnya. Fondasi tersebut disediakan, untuk memberikan layanan yang lebih lengkap bagi pengguna, seperti protokol *transport* RTP yang memanfaatkan fondasi tersebut, untuk melakukan dekripsi sesi multimedia. Karena kelebihannya itulah, yang membuat protokol ini lebih sering direkomendasikan, daripada protokol sebelumnya, H.323.

c) *Inter Asterisk Exchange* (IAX)

IAX/IAX2 merupakan protokol pengembangan dari Asterisk. Protokol ini dibuat oleh seorang praktisi teknologi informasi, Mark Spencer. Diciptakan guna menyempurnakan SIP yang telah menjadi standar IETF (*Internet Engineering Task Force*). Pernyataan ini sesuai dengan penelitian yang telah dilakukan Yanuarika. Dalam tugas akhirnya terkait studi komparasi SIP dan IAX2, ia membuktikan bahwa kinerja IAX2 memang lebih baik daripada SIP, karena jumlah *port* yang digunakan IAX2, lebih sedikit daripada SIP, yakni satu *port* (4569) untuk IAX2, dan dua *port* (5060 dan 5061) untuk SIP.

b. Protokol *Transport*

Protokol yang bertugas mengantar pesan, berupa suara dan data ke alamat tujuan. Contoh protokol ini adalah RTP (*Real time Transport Protocol*), yang digunakan protokol SIP untuk melakukan transmisi data dan suara, sedangkan IAX2, protokol *transport* yang digunakan, adalah dirinya sendiri dengan memanfaatkan *port* 4569. Dengan menggunakan *port* tersebut, IAX2 dapat melakukan pengiriman pesan, langsung setelah proses *signaling* dijalankan (Kautsar dkk, 2012). Dalam protokol inilah, data dikirim dalam bentuk potongan kecil. Kemudian potongan tersebut, dirangkai oleh UDP (*User Datagram Protocol*), hingga membentuk paket data, dan selanjutnya dikirim ke pengguna lain, melalui jaringan IP.

Dengan menggunakan protokol UDP, proses pengiriman data menjadi lebih cepat dilakukan. Ketika paket yang dikirim dari RTP/*port* 4569 mengalami *drop*, proses pengiriman tetap dilanjutkan dengan mengabaikan perbaikan data. Hal ini sesuai dengan standar protokol UDP, yang lebih mementingkan kecepatan pengiriman data, agar segera sampai ke tujuan, sehingga pengguna tidak perlu menunggu lama (*delay*).

2.2.3.4. *Codec*

Codec berfungsi mengubah kode suara dari analog ke dalam kode digital. *Codec* sendiri merupakan singkatan dari *compressor-decompressor*. Dikembangkan untuk memampatkan suara, agar dapat menghemat penggunaan *bandwidth*, tanpa mengorbankan kualitas suara.

Ada berbagai jenis *codec*, yang telah dibangun saat ini, yaitu GIPS, GSM, iLBC, ITU G.711, ITU G.722, ITU G.723.1, ITU G.726, ITU G.728, ITU G.729, Speex, LPC10, dan DoD CELP. Di Indonesia sendiri, *codec* yang umum digunakan adalah GSM dan iLBC. Hal ini karena, kualitasnya yang cukup baik, *open source*, dan tidak menuntut adanya lisensi.

2.2.4. Kendala Implementasi VoIP

Kendala implementasi VoIP, tidak terlepas dari pengamanan serta reliabilitas penggunaan jaringan *internet*. Hal ini dikarenakan, jaringan tersebut merupakan komponen penting VoIP, agar pengguna dapat saling berkomunikasi. Oleh karena itu, jika jaringan ini mengalami masalah, maka kinerja VoIP pun juga akan bermasalah, sedangkan kondisi yang ada saat ini, belum ada satu pun pihak, yang mampu menjamin keamanan serta reliabilitas jaringan *internet*, dari serangan *hacker* (Margono, 2015).

Untuk menanggulangi masalah di atas, maka Adi Kurniawan Y. (2009), seorang profesional IT, menawarkan beberapa solusi untuk mengamankan jaringan VoIP, yakni dengan membangun jaringan VPN, melakukan *setting Firewall*, atau dengan menggunakan segmentasi VLAN. Untuk memperoleh hasil yang maksimal, maka penulis akan mencoba menggabungkan metode-metode tersebut, untuk dilakukan uji coba dan analisis. Penggabungan tersebut, diharapkan dapat memberikan hasil dan informasi yang lebih baik, terkait metode pengamanan VoIP.

2.3. MPLS-VPN

MPLS-VPN adalah metode gabungan dari metode pengamanan itu sendiri (VPN) dengan teknologi penunjangnya (MPLS). VPN merupakan singkatan dari *Virtual Private Network*, yang dapat mengamankan jaringan VoIP, dengan melakukan *route* lalu lintas data dan suara ke dalam jaringan privat. Metode ini memanfaatkan *Multi Protocol Label Switching* (MPLS), sebagai teknologi penunjang *Quality of Service* (QoS). Dengan bantuan teknologi ini, jaringan IP menjadi *reliable* untuk mengirim data bersifat *real time*.

Dalam implementasinya, metode MPLS-VPN dapat menghemat biaya pengelolaan. Pasalnya, metode dijalankan secara *virtual*, sehingga dapat meminimalkan penambahan jalur fisik pada *private network* (Saputra, 2010). Dengan menggunakan pengaturan *virtual* itulah, yang membuat lalu lintas jaringan *internet*, menjadi aman, yakni mampu memenuhi kebutuhan perusahaan dalam menjaga kerahasiaan, kendali akses, autentikasi, integritas, dan *non-repudiation*.

Meskipun metode ini terkenal tangguh, namun kenyataannya, kemungkinan penyadapan masih dapat terjadi, dengan memasang *radio shack* misalnya. Dengan perangkat tersebut, *attacker* dengan mudah dapat menyadap *VoIP Call*, dan melakukan *decode* terhadap jaringan yang telah dilakukan enkripsi dengan metode tersebut (Yusro, 2009).

2.4. Segmentasi VLAN

Segmentasi VLAN (*Virtual Local Area Network*) adalah metode pengamanan jaringan, yang digunakan untuk melindungi akses jaringan, dari kendali pihak luar. Metode ini membiarkan komunikasi antar *port* terhubung, asalkan *port* berada dalam satu segmen yang sama. Kemudian untuk *port* yang berada di luar segmen, mereka akan ditangani oleh VLAN yang berbeda.

Model jaringan yang digunakan dalam segmentasi VLAN, merupakan perkembangan dari model jaringan LAN (*Local Area Network*). Perbedaannya, LAN sangat bergantung pada area fisik *workstation*, sedangkan VLAN, ia berjalan pada lapisan *logic*, sehingga masing-masing *user*/*workstation* dapat saling terhubung meskipun mereka terpisah secara fisik. Dengan menggunakan metode ini, manajemen VLAN dapat dilakukan secara terpusat, sehingga hal ini dapat memudahkan administrator dalam melakukan konfigurasi dan kontrol jaringan.

Metode VLAN tidak hanya digunakan untuk memisahkan lalu lintas data dan suara, akan tetapi juga digunakan untuk memisahkan *MAC address*, *IP address*, tipe protokol, dan aplikasi. Pemisahan lalu lintas data dan suara itulah, teknik yang akan penulis gunakan, dalam pengerjaan tugas akhir ini. Pemisahan dilakukan dengan membagi fungsi *port switch*, dengan tujuan untuk melindungi *data network* dari berbagai serangan lalu lintas jaringan.

Meskipun dari segi keamanan, VLAN lebih baik daripada LAN, hal ini belum menjamin keamanan jaringan secara keseluruhan. Dalam implementasinya, VLAN memerlukan berbagai tambahan teknik, untuk meningkatkan keamanan jaringan, seperti pengaturan *firewall*, pembatasan hak akses individu, *intrusion detection* (upaya untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan), enkripsi jaringan, dll (Deden, 2007).

2.5. Parameter Pengujian VoIP

Dalam melakukan pengujian terkait metode pengamanan VoIP, penulis menggunakan dua tahapan pengujian, yakni pengujian *Quality of Service* (QoS) dan pengujian keamananan jaringan, yakni

2.5.1 *Quality of Service* (QoS)

QoS adalah mekanisme jaringan, yang digunakan untuk mengukur kebutuhan aplikasi (VoIP) dalam jaringan yang dibangun (Dewandono, 2012). Berikut beberapa parameter yang digunakan untuk mengetahui nilai QoS.

a) *Throughput*

Throughput digunakan untuk menghitung waktu sebenarnya dari aktivitas *download* yang berjalan, berbeda dengan *bandwidth* yang digunakan untuk menghitung waktu yang dibutuhkan, agar memperoleh hasil *download* terbaik. Oleh karena itu, parameter ini dapat digunakan untuk mengukur kualitas suatu jaringan, sehingga semakin tinggi nilai *throughput*, maka nilai *delay* akan semakin rendah, sehingga kualitas jaringan menjadi lebih baik (Anggita dkk, 2012).

b) *Packet Loss*

Parameter yang digunakan untuk menghitung paket data yang hilang ketika proses transmisi terjadi. Parameter ini, memberikan pengaruh yang besar terhadap *IP Telephony*, dimana apabila terjadi *packet loss* dalam jumlah tertentu, akan menyebabkan interkoneksi TCP menjadi melambat.

c) *Delay*

Delay adalah parameter waktu yang dibutuhkan sebuah paket, dari saat paket tersebut dikirim sampai diterima. Parameter ini penting digunakan untuk menentukan kualitas VoIP. Semakin besar *delay*, berarti semakin rendah kualitas VoIP yang dihasilkan.

d) *Jitter*

Jitter adalah parameter yang digunakan, untuk menghitung perbedaan waktu kirim dan sampainya paket data ke tujuan. Parameter ini, merupakan hasil variasi dari *delay*. Perbedaannya, keterlambatan yang dimiliki *delay* cenderung konstan, sedangkan keterlambatan *jitter*, cenderung tidak menentu. Hal ini dikarenakan, kemampuan alat yang berbeda-beda dalam merespon suatu data tiap waktu, sehingga menyebabkan data ketika melintasi jaringan, jarak antar blok informasi, menjadi tidak seragam lagi (Firmansyah, 2008).

2.5.2 Keamanan Jaringan

Pengujian ini akan dilakukan dengan menggunakan lima teknik serangan, yakni ARP *poisoning* (*arpspoof*), VLAN *hopping* (*voiphopper*), IP *spoofing* (*inviteflood*), *ping flooding* (*hping3*), dan *eavesdropping* (*ucsniff*). Kelima teknik akan dijalankan pada Sistem Operasi *Backtrack*. Hasil analisis dari pengujian ini, akan memberikan informasi tentang seberapa kuat jaringan VoIP, dalam menahan serangan *cybercrime*.