BAB II

LANDASAN TEORI

2.1 Jaringan VOIP

Menurut Wahyuddin (2010 : 50) implementasi VOIP berbasis *freeware* menggunakan SIP diartikan sebagai teknologi yang mengirimkan data suara berbentuk paket secara *realtime* memakai jaringan internet protokol (IP).

Dari definisi di atas, dan terkait dengan penelitian yang dilakukan, penulis menyimpulkan bahwa VOIP adalah teknologi yang dapat melakukan komunikasi dengan menggunakan internet protokol pada suatu jaringan (*networking*). Sehingga teknologi ini dapat melakukan komunikasi untuk dijalankan diatas jaringan *packet network*. Teknologi ini bekerja dengan cara merubah suara analog menjadi suara digital tertentu yang dikirimkan melewati jaringan IP.

2.2 Komponen VOIP

Anton (2006) Komponen dalam VoIP yang perlu diketahui adalah : VoIP mempunyai empat komponen utama, yaitu User Agent, Proxy, Protokol, dan Codec. Berikut penjelasan mengenai masing-masing komponen dalam membangun jaringan VoIP.

2.2.1 *User Agent*

User agent adalah komponen yang digunakan oleh *user* untuk melakukan panggilan. Dalam VoIP, *user agent* merupakan komponen yang

melakukan dial VoIP atau menerimanya. *User agent* berupa software atau biasa disebut dengan softphone. Softphone adalah user agent yang paling populer, karena banyak softphone diperoleh secara gratis. Contoh user agent berbentuk softphone adalah X-Lite, ZoIPer, dan ABTO. Pada dasarnya fungsi softphone sama, yaitu dapat melakukan panggilan dan menerima panggilan berserta memutuskan panggilan, seperti melakukan panggilan dengan telepon biasa pada umumnya. *Softphone* harus terinstal dikomputer dan membutuhkan sebuah *microphone* dan *speaker* sebagai alat tambahan untuk melakukan komunikasi. Gambar di bawah merupakan tampilan X-Lite yang digunakan sebagai user agent.

Gambar 2.1 X-lite

2.2.2 Proxy

Proxy didalam VoIP, berbeda dengan proxy server internet yang ada dalam sebuah jaringan komputer. Proxy yang ada dalam teknologi VoIP adalah merupakan aplikasi server yang mengatur jaringan VoIP. Proxy

adalah komponen yang menerima registrasi user agent dan bertugas mengatur penomoran dan call routing. Proxy juga bias disebut juga sebagai IP PBX (*Private Branch Exchange*) Server. Proxy yang digunakan sekarang mempunyai 2 jenis, yaitu berupa hardware mesin IP PBX dan berupa software sebagai softswitch seperti Asterisk dan SER (SIP Express Router). Beberapa softswitch yang biasa digunakan sebagai Proxy atau IP PBX server adalah Asterisk, Trixbox, Briker, MiniSIP Server, dan Axon.

2.2.3 Asterisk

Asterisk merupakan perangkat lunak berfungsi menjadikan komputer menjadi server untuk voip. Asterisk bersifat open source, sehingga bebas untuk digunakan dan dikembangkan. Sampai sekarang, Asterisk mendukung beberapa protokol untuk membangun IPPBX (Internet Protocol Private Branch Exchange).

2.2.4 AsteriskNow

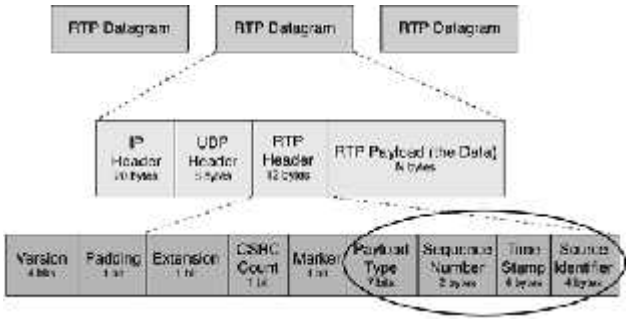
Adalah *software* untuk membangun sistem telepon (PBX) dengan menggbungkan Linux (CentOS) sebagai basis dan paket *software* appliance Asterisk menjadi sebuah distribusi Linux untuk memudahkan pengembang dalam membangun dan menjalankan sebuah sistem PBX.

2.3 Protokol VOIP

2.3.1 RTP (Real-time Transport Protocol)

RTP adalah merupakan protocol yang digunakan untuk transportasi data *real time* seperti pada VOIP. Protokol ini digunakan oleh protocol SIP dab H.323. Protokol ini menyediakan informasi waktu kepada

penerima sehingga dapat melihat *delay*. RTP juga berfungsi mendeteksi paket yang hilang. *Header* RTP berisikan informasi yang membantu penerima agar dapat merekonstruksi ulang paket dan juga informasi mengenai bagaimana bit – bit dibagi menjadi paket oleh *codec*. RTP menyediakan informasi yang cukup kepada penerima sehingga dapat dipulihkan kembali apabila terjadi *packet loss* atau *jitter*.



Gambar 2.2 RTP diagram

2.3.2 RTCP (*Real-time Control Protocol*)

RTCP adalah merupakan protokol yang bekerja berkaitan dengan RTP. Dalam sesi tertentu RTP secara periodic mengirimkan paket RTCP untuk menyebarkan informasi yang bermanfaat mengenai QoS (*Quality of Service*). Fungsi dari RTCP adalah menyediakan timbal balik dari QoS, identifikasi user dan singkronisasi media.

2.3.3 SIP (*Session Initiation Protocol*)

Taufiq (2005 :16) SIP adalah merupakan protokol pada layer perangkat lunak yang memproses awal dan akhir sesi komunikasi yang melibatkan satu atau beberapa pengguna. Sesi komunikasi ini termasuk hubungan multimedia dan aplikasi lainya.

SIP adalah merupakan *layer* aplikasi yang dipergunakan untuk memanajemen suatu panggilan dan pengakhiran panggilan.

SIP terdiri dari dua buah komponen

1. User Agent

   User agent terdiri dari dua bagian yaitu:

   - UAS (*User Agent Server*) adalah *user agent* yang berfungsi untuk mendengarkan dan merespon terhadap *request* SIP
   - UAC (*User Agent Client*) adalah *user agent* yang berada disisi pemakai yang dipergunakan untuk melakukan inisiasi *request* dari server SIP ke UAS

2.3.4 Codec

Purbo dan anton (2011 : 280) *Codec* merupakan singkatan dari *Coding Decoding*. *Codec* adalah merupakan teknologi yang berfungsi megatur dan mengubah data suara kedalam format lain sehingga menjadi lebih mudah untuk dikirimkan. *Codec* berfungsi untuk mengurangi penggunaan *bandwith* didalam pengiriman sinyal setiap panggilan. Oleh karena itu VOIP mengjadi irit untung menggunakan *bandwith*. Banyak jenis protokol *codec* yang ada untuk implementasi VOIP.

2.4 QoS (*Quality of Service*)

VOIP merupakan jenis layanan *real time* yang menuntut QoS yang baik. Dengan demikian, ada beberapa factor yang mempengaruhi kualitas QoS dari VOIP yaitu :

2.4.1 Delay

Panderambo (2007) *Delay* adalah merupakan faktor penting untuk menentukan kualitas suara pada VOIP. Apabila nilai *delay* besar maka akan jelek kualitas suara pada VOIP yang dihasilkan. *Delay* adalah merupakan interfal waktu saat data dikirimkan oleh pemanggil ke penerima panggilan yang disebabkan oleh pengubahan suara berbentuk analog menjadi suara berbentuk digital.

Delay dapat dihitung dengan persamaan berikut:

Rata-rata delay= Total delay/ total paket yang diterima

2.4.2 Packet Loss

Setiap paket yangn di kirim dari pemanggil ke penerima tidak semuanya sampai, karena jalur jaringan internet yang bersifat *best effort*, yaitu jaringan hanya berusaha menjaga supaya paket sampai ke penerima. Apabila paket sebelumnya looping dijaringan, oleh *router* paket data itu akan di buang. Kelemahan protocol ini, tidak adanya pengiriman ulang apabila paket yang dikirim rusak.

Packet loss dapat dihitung dengan persamaan berikut:

Packet Loss = ((data yang dikirim – paket data yang diterima)/ paket yang dikirim)x 100%

2.4.3 Throughput

Througput adalah merupakan kecepatan rata-rata yang diterima oleh suatu node dalam selang waktu pengamatan tertentu. Throughput merupakan bandwidth aktual saat itu juga dimana kita sedang melakukan koneksi, satuan yang dimiliki sama dengan satuan bandwidth yaitu bps

Throughput dapat di hitung dengan persamaan berikut:

Throughput = Jumlah data yang dikirim / Waktu pengiriman data

2.5 Kelemahan pada VOIP

VOIP mempunyai data yang harus di amankan. Pembicaraan pada VOIP, rekaman telepon, dan nomer telepon VOIP adalah beberapa contoh yang harus dapat di rahasiakan.

Dalam sistem VOIP, paket data suara di kirim menggunakan protocol RTP(*Real-time Transport Protocol*). Paket RTP memiliki standar format, paket RTP dapat di *encoding* dengan hanya melihat isi dari RTP, pake RTP dapat ditangkap kemudian di mainkan ulang.

Area dari keamanan VOIP dan internet kurang di perhatikan, kenyataanya adalah para peretas melakukan berbagai cara untuk merusak sistsystem yang kita miliki dengan berbagai cara diantaranya adalah:

2.5.1 Call Hijacking

Call Hijacking yaitu peretas yang memanipulasi sistem yang memungkinkan pelaku untuk menggubah data server. Dalam jaringan VOIP Call Hijacking dapat berdampak besar dan beresiko server hack.

2.5.2 Distributed Denial of Service(DDOS)

DDOS adalah jenis serangan yang biasa dilakukan peretas untuk menyerang server yang berada jaringan internet dengan cara menyerang server dengan banyak user sampai server *over load*, dengan demikian pengguna lain tidak bisa mengakses layanan dari server.

2.6 Menggunakan VPN Sebagai Keamanan VOIP

VPN (*Virtual Private Network*) adalah merupakan pengamanan jaringan dengan membuat *tunnel* atau terowongan pada jaringan internet sehingga jaringan bersifat private dan aman. VPN bersifat private karena ketika memasuki jaringan VPN diperlukan autentikasi untuk memastikan user yang sesuai yang diberi kewenangan untuk mengankses. Setelah terbentuknya koneksi VPN maka data yang dikirim akan di enkripsi untuk menjaga kerahasiaan paket. Autentikasi dan enkripsi didalam VPN membuat keamanan lebih baik.

2.6.1 Tunneling

Tunneling adalah merupakan peran utama dari VPN. Tunneling adalah merupakan suatu teknik untung melakukan enkripsi terhadap seluruh data pada suatu paket yang menggunakan suatu format protokol tertentu. Dengan kata lain, header dari suatu protokol *tunneling* ditambahkan pada header paket yang asli. Kemudian barulah paket tersebut dikirimkan ke dalam jaringan paket data.

Ketika paket yang telah "*ditunnel*" dirutekan ke terminal tujuan. Maka paket–paket tersebut akan melewati suatu jalur logika yang dikenal dengan

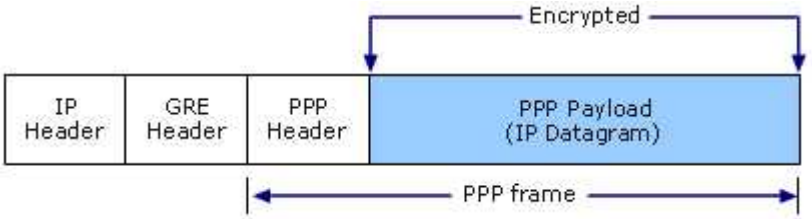
nama kanal. Ketika penerima menerima paket tersebut, maka akan dibuka dan dikembalikan lagi ke dalam format aslinya.

2.6.2 Protokol Tunneling pada VPN

Untuk bisa saling berhubungan antar user pada VPN diperlukan protokol untuk menyatukan hubungan tersebut. Terdapat banyak protokol pada jaringan VPN, akantetapi yang akan di bahas adalah yang dipergunakan pada tugas akhir ini yaitu *Point to Point Protocol* (PPTP).

2.6.2.1 Point to Point Tunneling Protocol (PPTP)

Proses pengamanan pada PPTP terjadi dengan melapisi paket data yang dikirim untuk kemudian dikirimkan melewati jaringan pada internet. Pada tahap ini PPTP menggunakan koneksi TCP yang dikenal sebagai PPTP control connection untuk menciptakan, merawat dan mengakhiri tunnel serta *Generic Routing Encapsulation* (GRE).

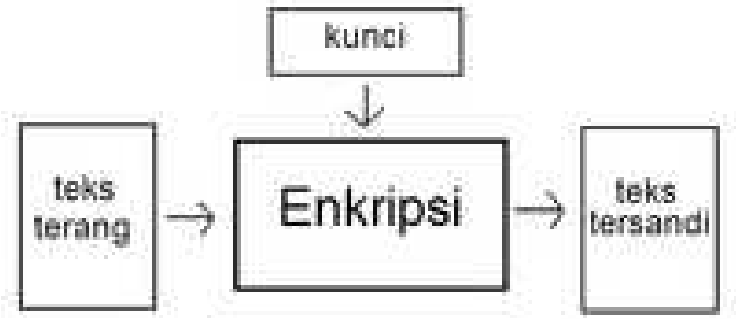


Gambar 2.3 Struktur Paket PPTP Mengandung IP Datagram

2.6.3 Enkripsi

Enkripsi adalah merupakan suatu proses keamanan suatu data dengan membuat data tersebut tidak dapat terbaca tanpa sandi khusus. Dikarenakan enkripsi sudah digunakan untuk keamanan data di berbagai sector.

Enkripsi dapat juga digunakan untuk tujuan keamanan, tetapi teknik diperlukan supaya data yang di kirimkan aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan komputer.



Gambar 2.4 proses enkripsi

2.7 *Software* Penunjang

2.7.1 Asterisknow

Asterisknow adalah merupakan perangkat lunak open sourse untuk membuat sistem telepon (PBX) dengan menyatukan Linux CentOS sebagai default linux yang dipakai sebagai basis dan software Asterisk

sebagai software SIP menjadi sebuah software baru yang memudahkan untuk membangun sistem telepon.

Gambar 2.5 Asterisknow

2.7.2 X-Lite

X-lite adalah merupakan perangkat lunak yang dikembangkan oleh CounterPath Solutions Inc., yang dipergunakan untuk menjalankan VoIP berbasis protokol SIP pada suatu komputer. Perangkat lunak ini diibaratkan dapat mengubah PC yang di dukung headset menjadi telepon. X-lite membuat PC dapat digunakan seperti pesawat telepon pada umumnya untuk melakukan panggilan dan menerima panggilan di sebuah PC, perangkat lunak ini dapat berjalan di sistem Windows, Linux dan mac os.

Gambar 2.6 X-lite

2.7.3 Wireshark

Wireshark adalah merupakan suatu alat atau aplikasi penganalisa jaringan. Menganalisa kinerja jaringan melingkupi berbagai hal, mulai dari proses penangkapan paket data yang melewati pada jaringan, aplikasi ini juga digunakan untuk *sniffing* (tindakan penyadapan yang dilakukan dalam jaringan dengan tujuan untuk dapat mencuri data-data pribadi ataupun account lain yang bersifat pribadi.). Wireshark merupakan *free tools* untuk *Network Analyzer* yang ada saat ini. Dan tampilan dari wireshark ini sendiri sangat mudah untuk di analisa karena sudah terdapat grafis dan data-data yang lengkap. Dan aplikasi ini juga mudah untuk di pergunakan untuk analisa pada jaringan.

Gambar 2.7 Gambar Aplikasi Wireshark