UNIVERSITAS INDONESIA

IMPLEMENTASI DAN ANALISIS PPTP DAN L2TP *REMOTE ACCESS VIRTUAL PRIVATE NETWORK* PADA JARINGAN *IMS* BERBASIS *OPEN IMS CORE*

SKRIPSI

HARI WIBAWA
0806459791

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK KOMPUTER
DEPOK
JULI 2012

UNIVERSITAS INDONESIA

IMPLEMENTASI DAN ANALISIS PPTP DAN L2TP *REMOTE ACCESS VIRTUAL PRIVATE NETWORK* PADA JARINGAN *IMS* BERBASIS *OPEN IMS CORE*

SKRIPSI

Diajukan sebagai salah satu syarat memperoleh gelar sarjana

HARI WIBAWA
0806459791

FAKULTAS TEKNIK UNIVERSITAS INDONESIA
DEPARTEMEN TEKNIK ELEKTRO
TEKNIK KOMPUTER
DEPOK

JULI 2012

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar

Nama : Hari Wibawa

NPM : 0806459791

Tanda Tangan : .....

Tanggal: 6 Juli 2012

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh	:
Nama	: Hari wibawa
NPM	: 0806459791
Program studi	: Teknik komputer
Judul Skripsi	: IMPLEMENTASI DAN ANALISIS PPTP DAN L2TP *REMOTE ACCESS VIRTUAL PRIVATE NETWORK* PADA JARINGAN *IMS* BERBASIS *OPEN IMS CORE*

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer, Fakultas Teknik, Universitas Indonesia

DEWAN PENGUJI

Pembimbing	: Muhammad Salman S.T., MIT	( )
Penguji	: Yan Maraden ST. MSc.	( )
Penguji	: I Gde Dharma Nugraha ST. MT.	( )

Ditetapkan di : Depok

Tanggal : 6 Juli 2012

KATA PENGANTAR

Puji syukur saya panjatkan kehadirat Allah SWT atas segala rahmat dan karunia-Nya saya dapat menyelesaikan skripsi ini. Saya menyadari bahwa skripsi ini tidak akan terselesaikan tanpa bantuan dari berbagai pihak. Mulai dari proses pembelajaran, analisis yang telah dijalani dan proses penyusunan dari skripsi ini, saya ingin mengucapkan terima kasih kepada:

1. Muhammad Salman S.T., MIT, selaku pembimbing skripsi yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini.
2. Orang tua dan keluarga saya yang telah memberikan bantuan dan dukungan materil, moral serta doa.
3. Zul Ramadhan, selaku pembimbing skripsi yang telah membantu dan memberikan ilmunya selama di R&D Center Telkom, Bandung, sehingga skripsi ini dapat selesai.
4. Sahabat dan teman-teman yang telah banyak memberikan dukungan dan bantuan kepada saya dalam menyelesaikan skripsi ini.

Akhir kata, semoga Allah SWT berkenan membalas kebaikan semua pihak yang telah membantu dan mendukung saya. Semoga skripsi ini bermanfaat bagi perkembangan ilmu pengetahuan ke depannya.

Depok, 2 Juli 2012

Hari Wibawa

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: Hari Wibawa
NPM	: 0806459791
Program Studi	: Teknik Komputer
Departemen	: Teknik Elektro
Fakultas	: Teknik
Jenis karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

IMPLEMENTASI DAN ANALISIS PPTP DAN L2TP *REMOTE ACCESS VIRTUAL PRIVATE NETWORK* PADA JARINGAN *IMS* BERBASIS *OPEN IMS CORE*

Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempumblikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok,
Pada tanggal : 6 Juli 2012,

Yang menyatakan,

(Hari Wibawa)

ABSTRAK

Nama : Hari Wibawa

Program Studi : Teknik Komputer

Judul : IMPLEMENTASI DAN ANALISIS PPTP DAN L2TP *REMOTE ACCESS VIRTUAL PRIVATE NETWORK* PADA JARINGAN *IMS* BERBASIS *OPEN IMS CORE*

Next Generation Network (NGN) merupakan sebuah sistem yang dirancang untuk mengintegrasikan berbagai macam layanan jaringan. Salah satu model yang dapat menyokong konvergensi pada NGN adalah IP Multimedia Subsystem (IMS). Perkembangan IMS saat ini menjadi salah satu celah bagi pihak-pihak yang tak bertanggung jawab untuk melakukan penyerangan pada keamanan IMS. Maka dari itu, muncullah sebuah pemikiran untuk menciptakan sebuah sistem keamanan pada jaringan IMS dengan menerapkan Protokol PPTP dan L2TP *remote access* Virtual Private Network.

Kedua protokol tentunya memiliki kelemahan dan kelebihannya masing-masing. Untuk itu, akan dibandingkan QoS dari kedua protokol tersebut pada jaringan IMS yang melakukan layanan VoIP. Dan akan dilakukan tiga skenario pengujian untuk mengukur QoS tersebut, yaitu pertama tanpa menerapkan VPN, kedua dengan menerapkan VPN PPTP, dan ketiga dengan menerapkan VPN L2TP. Nilai delay pada VPN PPTP lebih baik 4.08% daripada VPN L2TP. Nilai jitter pada VPN PPTP lebih baik 2.06% daripada VPN L2TP. Dan nilai throughput pada VPN PPTP lebih baik 4.07% daripada VPN L2TP.

Kata kunci:

IP Multimedia Subsystem, Virtual Private Network, Protokol PPTP dan L2TP, Vyatta OS.

ABSTRACT

Name : Hari Wibawa

Study Prorgam : Teknik Komputer

Title : IMPLEMENTATION AND ANALYSIS PPTP AND L2TP REMOTE ACCESS VIRTUAL PRIVATE NETWORK ON IMS NETWORK BASED ON OPEN IMS CORE

Next Generation Network (NGN) is a system designed to integrate wide range of network services. One of model that can support convergence in NGN is the IP Multimedia Subsystem (IMS). Nowadays, The development of IMS, is being one of the gaps for an unauthorized person to attack on security of IMS. Then it emerges an idea to build a security system on IMS network by implementing PPTP and L2TP Protocol remote access Virtual Network.

Both protocols certainly have weaknesses and strengths of each. Hence, It will compared the QoS of both protocols on the IMS network to VoIP services. And it will be carried out three test scenarios to measure the QoS, the first without implementing a VPN, the second by applying a PPTP VPN, and the third by applying the L2TP VPN. The result of this impelementation is delay value in VPN PPTP 4.08% better than the VPN L2TP. Jitter value in VPN PPTP 2.06% better than the VPN L2TP. And the throughput on the PPTP VPN 4.07% better than the VPN L2TP.

Keywords:

IP Multimedia Subsystem, Virtual Private Network, PPTP and L2TP Protocol, Vyatta OS.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi saat ini sangatlah pesat, terutama di bidang telekomunikasi. Persaingan para operator dan vendor telekomunikasi yang ada di Indonesia memicu perkembangan teknologi telekomunikasi semakin cepat. Mulai dari First Generation sampai menuju teknologi masa depan, yaitu Next Generation Network (NGN). Mulai dari teknologi jaringan *circuit switching* yang hanya menyajikan satu layanan saja seperti suara, hingga ke jaringan *packet switching* yang identik dengan layanan Internet yang variatif, seperti *Instant Messaging*, *IPTV*, dan lain sebagainya. Walaupun jaringan *circuit switching* hanya dapat menyajikan satu layanan, yaitu layanan suara, namun jaringan *circuit switching* masih banyak digunakan hingga saat ini, yang dikenal dengan jaringan telepon seluler. Kedua teknologi ini, *circuit switching* dan *packet switching*, mempunyai peranan berbeda tetapi mempunyai fungsi yang sama, yaitu menyediakan suatu layanan telekomunikasi demi kemudahan dalam komunikasi jarak jauh.

Sebuah model yang saat ini sedang dikembangkan oleh operator-operator telekomunikasi untuk membangun kedua teknologi tersebut adalah IMS (IP Multimedia Subsystem). IMS merupakan salah satu arsitektur yang dapat menyokong konvergensi pada NGN. IMS dikembangkan pertama kalinya oleh 3GPP (3rd Generation Partnership Project), yaitu operator telekomunikasi penyokong konvergensi pada NGN. Perkembangan IMS saat ini menjadi salah satu celah pihak-pihak yang tak bertanggung jawab untuk melakukan penyerangan pada keamanan IMS.

Integritas data pelanggan merupakan hal yang paling penting dalam keamanan IMS. Pada kenyataannya, IMS akan menangani banyaknya jenis panggilan dari berbagai pelanggan. Tentunya seiring dengan berjalannya proses penanganan panggilan tersebut, terdapat data-data penting pelanggan. Jika data-data tersebut jatuh

ke pihak yang tidak bertanggung jawab maka akan dapat disalahgunakan oleh pihak tersebut. Oleh karena itu, pada skripsi ini akan dirancang suatu sistem IMS dengan menerapkan Protokol PPTP (Point-to-Point Tunneling Protocol) dan L2TP (Layer 2 Tunneling Protocol) *remote access* Virtual Private Network untuk mengenkripsi data-data pelanggan yang melakukan layanan multimedia.

1.2 TUJUAN PENELITIAN

Tujuan utama yang ingin dicapai dari penulisan skripsi ini, diantaranya adalah :

1. Mengimplementasikan suatu sistem keamanan pada jaringan IMS yang menerapkan Protokol PPTP dan Protokol L2TP Virtual Private Network dengan menggunakan Vyatta OSdi dalam Virtualbox berbasis Open IMS Core.
2. Menganalisis perbandingan QoS pada jaringan IMS yang telah menerapkan sistem keamanan VPN PPTP dan VPN L2TP, diukur dari

1.3 METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam penyusunan skripsi ini meliputi:

1. Pendekatan dari tinjauan pustaka, yaitu dengan melakukan studi literature dari website dan modul instalasi dari perangkat lunak.
2. Pendekatan dari narasumber, yaitu melalui diskusi dan tanya jawab dengan orang-orang yang ahli pada bidang-bidang yang berhubungan.
3. Perancangan perangkat lunak.
4. Pengujicobaan dan pengambilan data.
5. Analisis data.

Penelitian dilakukan melalui prosedur sebagai berikut:

1. Penginstalan dan konfigurasi server :
    a) Instalasi dan konfigurasi Open IMS Core.
    b) Konfigurasi DNS Forwarding antar domain yang berbeda.
    c) Konfigurasi ENUM Server.
2. Penginstalan MONSTER Client sebagai IMS Client.
3. Penginstalan dan Konfigurasi Vyatta OS.
4. Analisis performansi sistem keamanan pada IMS.

1.4 BATASAN MASALAH

Seperti yang telah dijelaskan sebelumnya bahwa penulisan skripsi ini hanya akan membahas keamanan pada jaringan IMS dengan menerapkan Virtual Private Network PPTP dan l2TP dan membandingkan penerapan kedua protokol tersebut di dalam Virtualbox berbasis Open IMS Core, dengan menggunakan komponen sebagai berikut:

1. Open IMS Core
2. MONSTER Client (Multimedia Open InerNtet Services and Telecommunication EnviRonment)
3. Vyatta OS versi 5
4. Sistem Operasi : Ubuntu versi 10.10
5. Virtualbox OSE versi 4

1.5 SISTEMATIKA PENULISAN

Penulisan skripsi ini dibagi menjadi beberapa bagian:

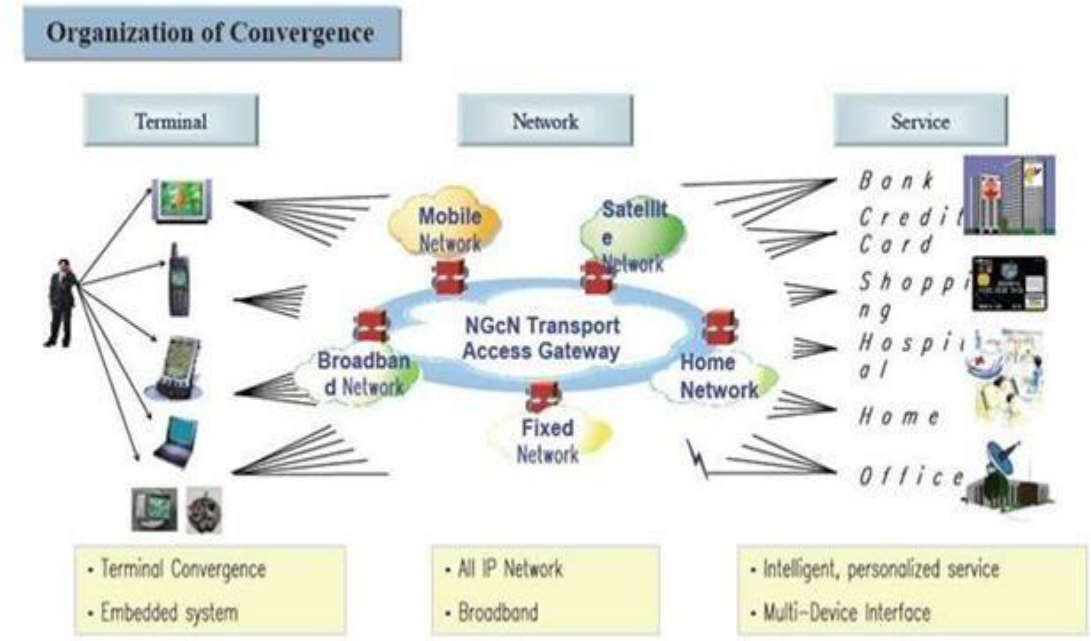
- BAB 1 Pendahuluan, berisikan latar belakang, perumusan masalah, tujuan penelitian, batasan masalah, metode penelitian, dan sistematika penulisan.
- BAB 2 Landasan Teori, berisikan teori-teori yang mendasari penelitian skripsi ini, yaitu mengenai konsep dasar IMS Core, VPN, Protokol SIP, dan parameter-parameter yang digunakan pada penelitian ini.
- BAB 3 Perancangan Sistem, membahas mengenai skenario perancangan topologi sistem yang akan digunakan serta cara instalasi dan konfigurasi Server Open IMS Core, ENUM Server, dan konfigurasi Vyatta OS.
- BAB 4 Implementasi dan Analisis Sistem, berisi mengenai analisis penerapan keamanan protokol PPTP dan L2TP pada jaringan IMS dengan menggunakan Vyatta OS.
- BAB 5 KESIMPULAN, berisi kesimpulan dari hasil analisis yang didapat dari penelitian ini.

BAB 2
LANDASAN TEORI

2.1 IP Multimedia Subsystem (IMS)

Perkembangan teknologi saat ini berkembang sangat pesat, terutama di Bidang telekomunikasi. Perkembangan ini mendorong perusahaan-perusahaan yang bekerja di Bidang tersebut ke arah NGN (Next Generation Network). NGN atau Next Generation Network merupakan suatu sistem yang mencoba mengintegrasikan berbagai macam jaringan yang ada, entah menjadi satu platform besar ataupun tetap memakai banyak jaringan hanya pada level aplikasinya disatukan[1]. Beberapa faktor yang mempengaruhi perubahan-perubahan tersebut, yaitu regulasi pasar, permintaan layanan baru yang inovatif oleh para pengguna layanan telekomunikasi dan peningkatan penggunaan internet. Konsep NGN meliputi aspek ekonomis dan aspek teknis. Secara ekonomis, NGN memungkinkan meningkatkan produktivitas dengan cara menyediakan suatu layanan yang sesuai dengan permintaan pengguna yang berhubungan dengan layanan suara dan data (VoIP, Streaming, IPTV, dan lain sebagainya). NGN juga memungkinkan penurunan biaya pemeliharaan infrastruktur jaringan, karena pada NGN hanya dikenal satu jaringan *transport,* yaitu jaringan yang berbasis *Internet Protocol*. Sedangkan secara teknis, NGN membuat arsitektur jaringan menjadi fleksibel untuk menyediakan layanan-layanan baru dengan mudah. Untuk mewujudkan NGN suatu teknologi yang menerapkan konvergen dan layanan berbasis IP. Teknologi tersebut dikenal dengan nama *IP Multimedia Subsytem* (IMS).
IMS (IP multimedia subsystem) adalah teknologi komunikasi yang bisa menyatukan alat wireless dan wired dalam suatu jaringan yang real time, ekstensibel, dan mampu member layanan multimedia secara interaktif. IMS merupakan masa depan teknologi komunikasi karena IMS didesain mampu menyediakan layanan aplikasi streaming voice, video, gambar yang lebih kompetitif, mobilitas yang lebih

besar, dan isi serta layanan yang lebih baik. IMS didesain untuk mampu bekerja tanpa dibatasi area maupun domain yang ada dan bisa menggunakan Ipv4 dan Ipv6[2].IMS memungkinkan terwujudnya suatu arsitektur layanan multimedia yang baru. Tidak seperti saat ini, dimana layanan multimedia yang menggunakan jaringan internet lebih cenderung bersifat *best effort*, dan tidak menjamin *Quality of Service* (QoS) di Internet. Oleh karena itu, diharapkan dengan diterapkannya IMS, pengguna layanan telekomunikasi dapat menikmati layanan-layanan multimedia dalam satu jaringan yang konvergen dan menjamin QoS di Internet.

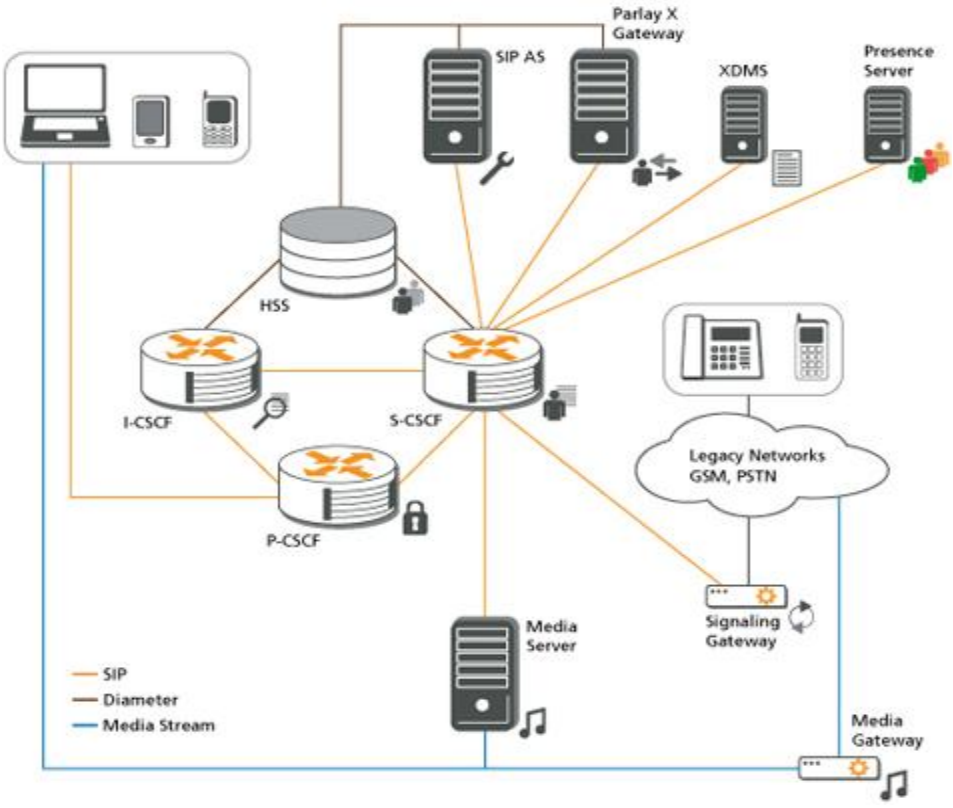


Gambar 2.1 Konvergensi perangkat, network & layanan [3]

2.1.1 Komponen-komponen Arsitektur IMS

Arsitektur IMS terdiri dari 4 komponen, yaitu IMS Core, IMS *Application Platform*, IMS *Client*, dan *Gateway*. IMS Core merupakan inti dari arsitektur IMS. IMS Core ini menjalankan fungsi-fungsi penting dari seluruh arsitektur, salah satunya adalah proses pembentukan sesi dan kontrol sesi (*signalling*) antara pelanggan dan

application server dengan menggunakan protokol SIP (*Session Initiation Protocol*). IMS *Application Platform* merupakan kumpulan aplikasi-aplikasi yang ada di server beserta antar-muka *application server* (AS) dengan komponen S-CSCF (Serving-Call Session Control Function) pada IMS Core untuk mengendalikan sesi SIP. IMS *Client* atau disebut juga dengan *User Equipment* merupakan *endpoint* atau divais-divais yang ada di sisi pengguna, seperti *smartphone*, komputer tablet, komputer laptop maupun *notebook,* dan lain sebagainya. Dan yang terakhir adalah *Gateway*, yaitu berfungsi sebagai antar-muka antara jaringan-jaringan telekomunikasi lawas, seperti GSM dan PSTN dengan IMS Core. Tujuan adanya *Gateway* adalah agar supaya divais-divais yang tidak menggunakan protokol pensinyalan SIP juga dapat berkomunikasi dengan IMS Core.



Gambar 2.2 Arsitektur IMS [4]

Seperti yang telah disebutkan sebelumnya bahwa penulisan skripsi ini secara khusus hanya akan membahas mengenai salah satu dari arsitektur IMS, yaitu IMS Core. Maka selanjutnya akan dibahas mengenai empat komponen yang menyusun IMS Core, yaitu HSS (Home Subscriber Server), P-CSCF (Proxy Call Session Control Function), I-CSCF (Interrogating Call Session Control Function), dan S-CSCF (Serving Call Session Control Function).

2.1.2 Home Subscriber Server (HSS)

Home Subscriber Server atau HSS merupakan sebuah master database yang menyimpan profile dari setiap pengguna IMS, termasuk informasi status pengguna dan profile layanan aplikasi[5]. Dalam penerapannya, IMS menyediakan layanan-layanan multimedia kepada pengguna sesuai dengan profilnya masing-masing. Untuk itu, IMS harus menyimpan seluruh identitas dan informasi dari pengguna, termasuk layanan-layanan apa saja yang dapat digunakan oleh pengguna dan server atau network apa saja yang diizinkan untuk pengguna akses (*individual filtering information*). HSS serupa dengan HLR (Home Location Register) pada sistem 2G, tetapi dikembangkan dengan diterapkannya *reference point* berbasis DIAMETER.

2.1.3 Proxy Call Session Control Function (P-CSCF)

P-CSCF merupakan komponen pertama yang menghubungkan pengguna dengan IMS Core. Interface antara P-CSCF dengan IMS Client dinamakan *Gm Interface*, sedangkan interface antara P-CSCF dengan I-CSCF dan S-CSCF dinamakan *Mw Interface*. Semua jenis trafik *signalling* SIP dari atau ke IMS Client akan melalui P-CSCF. Seperti layaknya sebuah proxy, P-CSCF berfungsi menerima dan meneruskan respon atau permintaan ke komponen lainnya. P-CSCF juga berfungsi untuk melakukan otorisasi terhadap pembawa sumber daya untuk level QoS tertentu, *monitoring*, panggilan darurat, kompresi dan dekompresi header, serta identifikasi I-CSCF[5].

2.1.4 Interrogating Call Session Control Function (I-CSCF)

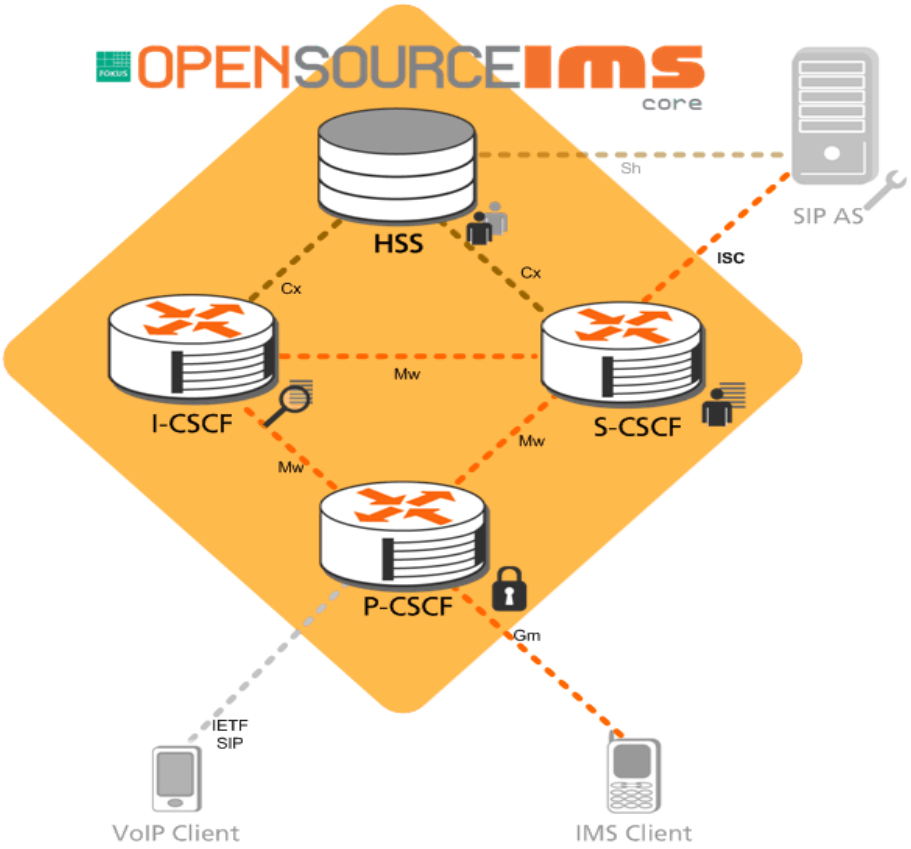
I-CSCF merupakan titik kontak dalam sebuah jaringan operator. Interface antara I-CSCF dengan HSS dinamakan *Cx Interface*, sedangkan interface antara I-CSCF denagn S-CSCF dinamakan *Mw Interface*. Proses registrasi pelanggan dilayani oleh I-CSCF. I-CSCF akan melalukan hubungan ke HSS untuk mendapatkan alamat yang diperlukan dari S-CSCF. I-CSCF berfungsi menugaskan S-CSCF ke pengguna untuk melakukan registrasi SIP, *charging* dan pemanfaatan sumber daya, seperti generasi CDRs (Charging Data Records), dan bertindak sebagai Topology Hiding Inter-working Gateway (THIG)[5].

2.1.5 Serving Call Session Control Function (S-CSCF)

S-CSCF berfungsi mengendalikan sesi layanan (*session control service*) untuk *endpoint* dan menjaga *session state* yang dibutuhkan operator jaringan untuk mendukung layanan-layanan[5]. S-CSCF memutuskan kapan sebuah AS (Aplikasi Server) diperlukan untuk menerima informasi terkait dengan permintaaan sesi SIP yang masuk untuk memastikan penanganan layanan sesuai dengan permintaan pengguna. Interface antara S-CSCF dengan HSS dinamakan *Cx Interface*.

2.2 Open IMS Core

Open IMS Core merupakan implementasi dari Home Subscriber Server (HSS) dan Call Session Control Function (CSCF) yang bersifat bebas (*open source*). Open IMS Core ditetapkan oleh 3GPP, 3GPP2, ETSI TISPAN, dan PacketCable Iniative. Keempat komponen tersebut berbasis perangkat lunak yang bebas (*open source*), contohnya SIP Express Router (SER) dan MySQL).



Gambar 2.3 Arsitektur Open IMS Core [6]

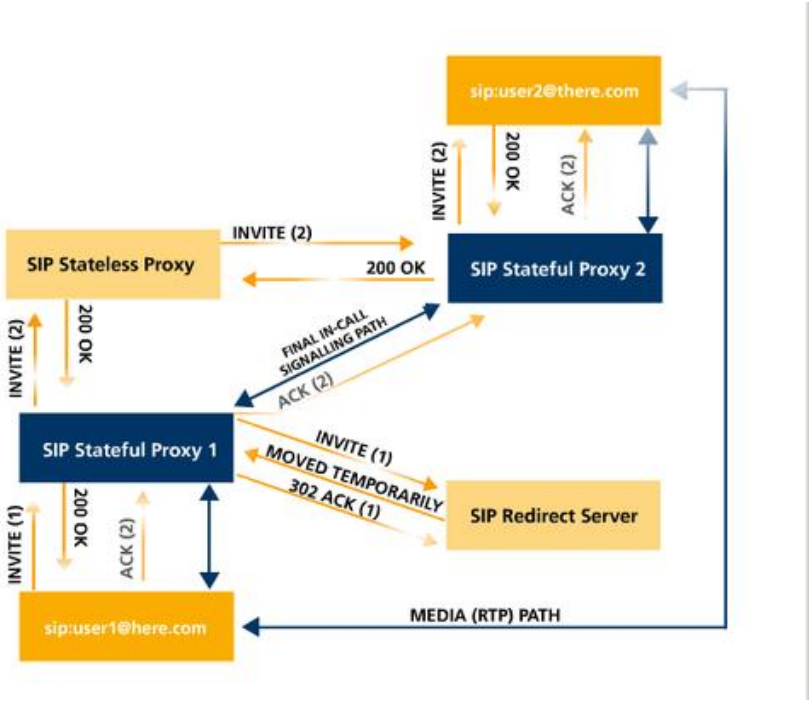
Open IMS Core yang dikembangkan oleh Institusi Fraunhofer bertujuan untuk mengisi kekosongan pada keberadaan IMS saat ini yang berbasis perangkat lunak yang bebas (*open source*) dengan solusi yang fleksibel dan dapat diperpanjang. Open IMS Core ini dibuat bukan untuk kepentingan komersial, melainkan untuk menciptakan komunitas pengembang Next Generation Network (NGN).

2.3 Protokol SIP

Session Initiation Protokol adalah sebuah protokol yang dikembangkan oleh IETF (Internet Engineering Task Force) yang digunakan untuk mengendalikan sesi komunikasi, seperti panggilan suara dan video melalui Internet Protokol (IP). Protokol tersebut digunakan untuk membuat, memodifikasi, dan mengakhiri sesi *unicast* maupun *multicast*[7].

Proses untuk membuat, memodifikasi, dan mengakhiri sesi multimedia dengan SIP melibatkan komponen SIP *User Agent* (SIP-UA) dan dengan menggunakan komponen tambahan, yaitu Proxy Server. Proses tersebut melibatkan dua atau lebih komponen SIP-UA (yang dipnaggil dan yang memanggil) dan hanya dapat terjadi jika pengguna mengetahui alamat IP dari setiap SIP-UA yang ingin dihubungi. Sementara itu, alamat IP yang akan dihubungi bersifat tidak statis dari waktu ke waktu, artinya alamat IP dari SIP-UA yang ingin kita hubungi dapat berubah-ubah sewaktu-waktu. Oleh karena itu, untuk memudahkan proses *signaling* dan menyederhanakan alamat IP, digunakanlah SIP Server. SIP Server terdiri dari Proxy Server dan Registrar Server.

Proxy server merupakan sebuah entitas *intermediary* (perantara) antara server dan *client.* Proxy server berperan seperti sebuah routing, yaitu bertugas meneruskan permintaan ke entitas lainnya yang lebih dekat sesuai tujuan pengguna jika domain yang dituju pengguna tidak berada di domain Proxy Server tersebut. Proxy server juga berfungsi untuk mengatur sebuah peraturan mengenai diperbolehkannya atau tidak pengguna dalam melakukan suatu panggilan. Sedangkan Registrar server berfungsi untuk menyimpan data dan informasi identitas pengguna dari domain tertentu, seperti alamat IP, *Publik Identity,* dan identitas lainnya. Registrar server disebut juga dengan *Redirect Server*. Berikut contoh aliran SIP dengan menggunakan proxy server ketika dilakukan panggilan.



Gambar 2.4 Aliran pesan SIP dengan menggunakan Proxy Server [7]

Pada gambar diatas, dapat dilihat aliran pesan SIP yang dikirim oleh sip:user1@here.com (User 1) ke sip:user2@there.com (User 2). User 1, sip:user1@here.com mengirimkan pesan INVITE ke proxy server 1 (SIP Stateful Proxy), namun user yang dituju (User 2) tidak berada pada domain proxy server tersebut sehingga proxy server meneruskan pesan ke proxy server terdekatnya, yaitu SIP Stateless Proxy. SIP Stateless Proxy meneruskan pesan tersebut ke domain yang dituju, yaitu SIP Stateful Proxy 2, dan pesan INVITE sampai ke sip:user2@there.com. User 2 memberikan tanggapan dan menerima panggilan dari User 1. User 2 mengirimkan pesan 200 OK ke User 1 yang berarti panggilan telah disetujui. Kemudian User 1 memberikan respon final ke User 2 dengan mengirimkan pesan ACK dan terhubunglah panggilan antara User 1 dengan User 2. Pada gambar juga terdapat SIP Redirect Server yang berfungsi sebagai penyimpan profile user.

Dalam sebuah jaringan SIP, alamat IP dari SIP-UA dikenal dengan URI (Uniform Resource Identifier). Format SIP URI adalah sip:username:password@host:port.

Contoh dari sebuah SIP URI sebagai berikut : sip:bob@open-ims.test. Dengan menerapkan skema alamat SIP URI, maka diperlukan proses penyelesaian alamat dengan menggunakan DNS Server pada sistem SIP Server. DNS server berguna untuk menentukan alamat IP dari divais yang dituju berdasarkan alamat SIP URI.

Pada skema aliran pesan SIP, terdapat beberapa jenis *SIP Message* yang digunakan, seperti INVITE, ACK, 200 OK, dan lain sebagainya. *SIP Message* ini dibagi menjadi dua bagian, yaitu SIP Request Message dan SIP Response Message.

2.3.1 SIP Request Message

SIP Request Message adalah sebuah pesan yang digunakan oleh SIP untuk membentuk komunikasi[8]. Berikut macam-macam dan fungsi dari SIP Request Message[11]:

Tabel 2.1 SIP Request Messages

Nama Pesan	Keterangan
REGISTER	Digunakan oleh UA (*User Agent*) untuk menunjukkan URL dan alamat IP yang akan menerima panggilan.
INVITE	Digunakan untuk membentuk sesi media (*media session*) antar SIP-UA.
ACK	Digunakan sebagai *acknowledgement* (pemberitahuan) atas respon final untuk permintaan INVITE.
Cancel	Digunakan untuk mengakhiri permintaan yang tertunda.
BYE	Digunakan untuk mengakhiri sesi media antar kedua UA dalam satu percakapan.
OPTIONS	Digunakan untuk mengetahui informasi kemampuan UA dan ketersediaan dari sebuah UA maupun Server.
PRACK	*Provisional Response Acknowledgement* digunakan untuk pemberitahuan atas pesan *response* sementara dengan format 1xx.
SUBSCRIBE	Digunakan untuk membentuk suatu layanan *subscription* dengan tujuan menerima pemberitahuan menggunakan metode NOTIFY mengenai *event* tertentu.

Tabel 2.1 SIP Request Messages

Nama Pesan	Keterangan
NOTIFY	Digunakan untuk menyampaikan notifikasi ke UA mengenai *event* tertentu yang mempunyai sesi *subscription*.
PUBLISH	Digunakan untuk mempublikasikan suatu *event* tertentu ke Server.
INFO	Digunakan untuk mengirim informasi *call signalling* ke UA lainnya yang memiliki sesi media.
REFER	Digunakan untuk meminta akses ke URI atau URL UA lainnya.
MESSAGE	Digunakan untuk menyampaikan pesan instan (Instant Message) menggunakan SIP.
UPDATE	Digunakan untuk memodifikasi keadaan sebuah sesi tanpa harus merubah keadaan dialog.

2.3.2 SIP Response Message

SIP Reponse Message adalah sebuah pesan yang digunakan oleh SIP untuk menanggapi SIP Request Message. Berikut macam-macam dan fungsi dari SIP Response Message[9]:

Tabel 2.2 SIP Response Messages

No Pesan	Nama Pesan	Keterangan
100	Trying	Digunakan untuk memberitahukan UA yang melakukan permintaan bahwa proses sedang dilakukan.
180	Ringing	Digunakan untuk memberitahukan bahwa pesan INVITE sudah diterima dan proses berdering sedang terjadi.
181	Call Is Being Forwarded	Digunakan untuk memberitahukan UA bahwa panggilan akan diteruskan ke UA lainnya.
182	Queued	Digunakan untuk memberitahukan UA bahwa pesan INVITE telah diterima namun sedang dalam antrian untuk diproses.
183	Session Progress	Digunakan untuk mengetahui status panggilan.

Tabel 2.2 SIP Response Messages

No Pesan	Nama Pesan	Keterangan
200	OK	Digunakan untuk menyetujui panggilan sesi dan permintaan sesi lainnya.
201	Accepted	Digunakan untuk memberitahukan kepada UA bahwa permintaan telah sudah diminta dan dimengerti.
300	Multiple Choices	Mengindikasikan *respon direction* yang terdiri dari beberapa lokasi yang mungkin untuk sebuah SIP URI.
301	Moved Permanently	Memberitahukan URI pemanen baru dari sebuah kontak.
302	Moved Temporarily	Memberitahukan URI sementara dari sebuah kontak.
305	Use Proxy	Memberitahukan alamat proxy server yang harus dihubungi untuk berkomunikasi dengan suatu UA.
380	Alternative Service	Memberitahukan bahwa layanan sedang dialihkan ke alternatif lain, misalnya ke layanan Voice Mail.
400	Bad Request	Mengindikasikan bahwa permintaan tidak dimengerti oleh server.
401	Unauthorized	Mengindikasikan bahwa UA harus melakukan autentikasi terlebih dahulu.
402	Payment Required	Digunakan untuk mendefinisikan biaya panggilan.
403	Forbidden	Digunakan untuk menolak permintaan yan dilakukan oleh UA karena server akan melayani permintaan tersebut.
404	Not Found	Memberitahukan bahawa SIP URI tidak dapat ditemukan oleh server.
405	Method Not Allowed	Mengindikasikan bahwa server telah menerima dan mengerti pesan yang dilakukan oleh UA, tetapi server tidak menolak untuk memenuhi permintaan tersebut.

Tabel 2.2 SIP Response Messages

No Pesan	Nama Pesan	Keterangan
406	Not Acceptable	Mengindikasikan bahwa permintaan tersebut tidak dapat diproses karena ada syarat tertentu yang harus dipenuhi untuk melakuka permintaan.
407	Proxy Authentication Required	Mengindikasikan bahwa UA yang ingin melakukan suatu panggilan harus terautentikasi dengan proxy server terlebih dahulu.
408	Request Timeout	Mengindikasikan bahwa lama waktu pesan INVITE telah habis.
409	Conflict	Mengindikasikan bahwa permintaan tidak dapat diproses karena adanya konflik pada permintaan.
410	Gone	Sama halnya dengan pesan 404, hanya saja pada pesan ini diberitahukan bahwa pengguna tidak dapat dihubungi lagi oleh URI tersebut.
411	Length Required	Mengindikasikan proxy menolak permintaan karena mencantumkan *field* "Content-length" pada *header* pesan.
413	Request Entity to Large	Mengindikasikan proxy menolak permintaan karena *message body* berukuran terlalu besar.
414	Request-URI Too Long	Mengindikasikan pesan URI terlalu panjang sehingga tidak dapat diproses.
415	Unsupported Media Type	Digunakan oleh UA untuk mengindikasikan bahwa tipe media yang didefinisikan di pesan INVITE tidak bisa dilayani.

Tabel 2.2 SIP Response Message

No Pesan	Nama Pesan	Keterangan
416	Unsupported Media Scheme	Memberitahukan bahwa server tidak mengerti skema URI.
420	Bad Extension	Mengindikasikan bahwa server atau UA tidak melayani ekstensi yang didefinisikan di *field require* pada pesan permintaan.
421	Extension Required	Memberitahukan bahwa server meminta ekstensi tertentu karena pada *field supported* tidak didefinisikan di pesan permintaan.
422	Session Timer Interval to Small	Digunakan untuk menolak pesan permintaan yang berisi *field* Session-Expires dengan nilai waktu yang terlalu kecil.
423	Interval Too Brief	Digunakan oleh registrar untuk menolak permintaan registern karena *expiration time* pada pesan permintaan terlalu singkat.
428	Use Authentication Token	Digunakan oleh server untuk meminta *Authentication Information Body*.
429	Provide Referror Identity	Digunakan untuk meminta header "Referred-by" dikirimkan ulang dengan token keamanan "Referred-by" yang benar.
480	Temporary Unavailable	Memberitahukan bahwa permintaan telah diterima ke tujuan yang benar, tetapi pengguna yang ditujukan tidak tersedia untuk sementara waktu.
481	Dialog/Transaction Does Not Exist	Mengindikasikan respon yang mereferensikan panggilan atau transaksi yang sudah terbangun dan telah diterima server tidak mempunyai informasi keadaan.

Tabel 2.2 SIP Response Message

No Pesan	Nama Pesan	Keterangan
482	Loop Detected	Mengindikasikan bahwa terjadi *looping* (pelemparan) pesan permintaan dan dikembalikan ke proxy yang meneruskan pesan tersebut.
483	Too Many Hops	Mengindikasikan bahwa pesan permintaan telah diteruskan dengan jumlah waktu maksimal yang telah ditetapkan pada header "Max-Forwards".
484	Address Incomplete	Memberitahukan bahwa alamat permintaan URI tidak lengkap.
485	Ambigious	Mengindikasikan bahwa alamat URI ambigu dan harus diklarifikasikan ulang agar dapat diproses.
486	Busy Here	Mengindikasikan bahwa UA tidak dapat menerima panggilan pada lokasi ini.
487	Request Terminated	Digunakan sebagai respon yang dilakukan oleh UA ketika menerima pesan CANCEL pada saat melakukan permintaan pesan INVITE yang tertunda.
488	Not Acceptable Here	Memberitahukan bahwa beberapa aspek dari sesi tidak dapat diterima dan mungkin mengandung "Warning" header.
489	Bad Event	Digunakan untuk menolak permintaan *subscription* atau notifikasi yang mengandung paket "Event" yang tidak diketahui atau tidak dapat dilayani oleh server.
491	Request Pending	Digunakan untuk menyelesaikan pesan re-INVITE yang simultan secara tidak langsung pada suatu dialog.
493	Request Undecipherable	Digunakan ketika pesan "S/MIME" tidak dapat dideskripsi karena *publik key* tidak tersedia.
500	Server Internal Error	Memberitahukan bahwa server sedang mengalami error tertentu sehingga tidak dapat melayani proses.

Tabel 2.2 SIP Response Messages

No Pesan	Nama Pesan	Keterangan
501	Not Implemented	Memberitahukan bahwa server tidak dapat melayani pesan permintaan karena tidak didukung.
502	Bad Gateway	Dikirimkan oleh proxy yang bertindak sebagai gateway ke jaringan lain dan mengindikasikan beberapa masalah pada jaringan lain yang mencegah proses permintaan.
503	Service Unavailable	Mengindikasikan bahwa layanan yang diminta tidak tersedia sementara waktu.
504	Gateway Timeout	Mengindikasikan bahwa proses permintaan gagal karena *timeout* yang terjadi pada jaringan lain yang disambungkan oleh gateway.
505	Version Not Supported	Memberitahukan bahwa permintaan telah ditolak oleh server karena nomor versi dari permintaan.
513	Message Too Large	Digunakan oleh server untuk mengindikasikan bahwa pesan permintaan terlalu besar untuk diproses.
600	Busy Everywhere	Merupakan pesan respon *client error*, seperti “486 Busy Here”, tetapi pesan 600 merupkan pesan versi definitif.
603	Decline	sama halnya dengan “600 Busy Everywhere”, tetapi tidak memberikan informasi apapun tentang keadaan panggilan (Call State) server.
604	Does Not Exist Anywhere	sama halnya dengan “404 Not Found”, tetapi pesan 604 mengindikasikan bahwa pengguna pada Request-URI tidak dapat ditemukan dimana-mana.
606	Not Acceptable	Digunakan untuk menerapkan beberapa kemampuan negoisasi sesi di SIP.

2.4 Vyatta OS Networking

Vyatta OS merupakan sistem operasi yang berfungsi sebagai router untuk mengatur jaringan di dalam sebuah gedung atau perusahaan yang berhubungan dengan adanya aktivitas Server dan Client dalam melakukan pengiriman dan penerimaan data secara digital. Vyatta mengubah dunia networking dengan mendistribusikan router, firewall,

dan VPN sebagai sebuah komiditi, sama halnya dengan Komoditi Linux memasarkan Sistem Operasinya.

Vyatta OS memiliki beberapa fitur untuk membantu jaringan perusahaan agar:

1. Mampu mengimplementasikan BGP dalam skala besar.
2. Menjaga jaringan perusahaan tetap aman dengan *stateful-inspection firewall*.
3. Koneksi ke *remote office* dengan aman melalui VPN.
4. Menghindari biaya dalam *upgrade* jaringan.
5. Bisa menjalankan lingkungan jaringan secara virtual, seperti di XEN ataupun di Vmware.

2.5 Virtual Private Network

VPN merupakan sebuah jaringan pribadi yang menggunakan medium nonpribadi (internet) untuk menghubungkan antar remote-site secara aman. Konsep kerja VPN pada dasarnya memb utuhkan sebuah server untuk menghubungkan antar PC. Jika digambarkan maka akan seperti ini:

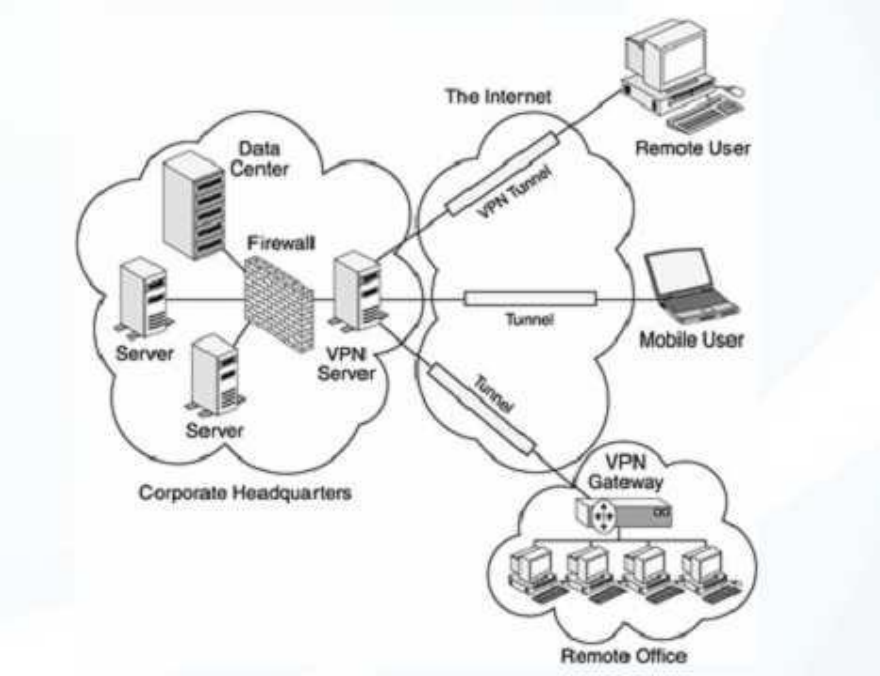
Internet ←→ VPN Server ← → VPN Gateway ←→ VPN Client ←→ Client

Setiap data yang dikirimkan akan melalui sebuah terowongan atau biasa disebut dengan *tunnel*. Tunneling merupakan inti dari teknologi VPN.Tunneling merupakan suatu teknik untung melakukan enkapsulasi 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.

2.5.1 Macam-macam Jaringan VPN

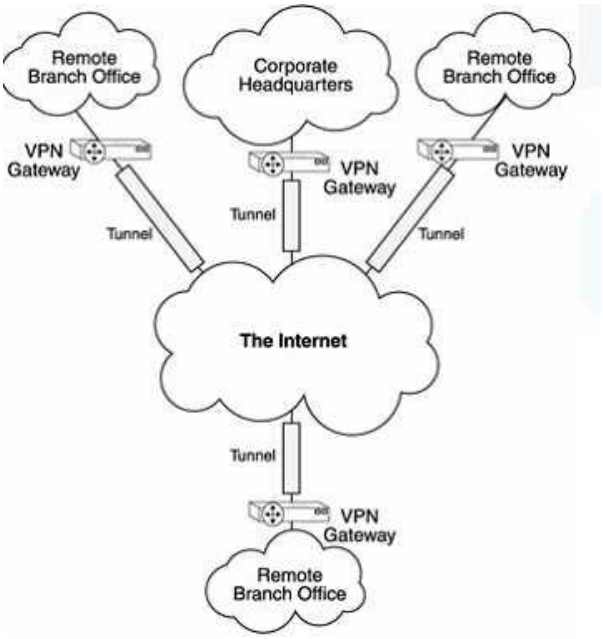
Ada tiga jenis jaringan VPN, yaitu :

1. Access VPN, yaitu menyediakan remote access ke jaringan intranet atau extranet perusahaan atau instansi yang memiliki kebijakan yang sama sebagai jaringan private. Access VPN memungkin user dapat mengakses data perusahaan atau instansi dimanapun, kapanpun, dan bagaimanapun user mau.



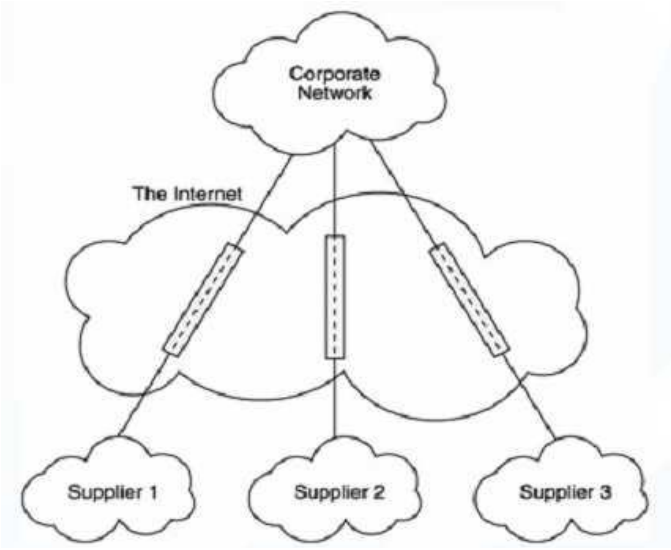
Gambar 2.5 Access VPN [10]

2. Intranet VPN, yaitu mengubungkan antara kantor pusat perusahaan dengan kantor cabang, kantor pembantu melalui *shared network* menggunakan koneksi permanen (dedicated).



Gambar 2.6 Intranet VPN [10]

3. Extranet VPN, yaitu menghubungkn konsumen, *suppliers*, mitra bisnis atau beberapa komunitas dengan kepentingan yang sama ke jaringan intranet perusahaannatau instansi melalui infrastruktur yang terbagi menggunakan koneksi permanent(dedicated).



Gambar 2.7 Extranet VPN [10]

2.5.2 Protokol pada VPN

2.5.2.1 Point to Point Tunneling VPN

Point-to-Point Tunneling Protocol (PPTP) adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari remote client kepada server perusahaan swasta dengan membuat suatu virtual private network (VPN) melalui jaringan data berbasis TCP/IP.Teknologi jaringan PPTP merupakan perluasan dari remote access Point-to-Point protocol yang telah dijelaskan dalam RFC 1171 yang berjudul "The Point-to- Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-to-Point Links" . PPTP adalah suatu protokol jaringan yang membungkus paket PPP ke dalam IP datagram untuk transmisi yang dilakukan melalui internet atau jaringan publik berbasis TCP/IP.PPTP dapat juga digunakan pada jaringan LAN-to-LAN.

Protokol PPTP termasuk dalam sistem operasi server Windows NT versi 4.0 dan Windows NT Workstastion versi 4.0.Komputer menjalankan sistem operasi ini dapat dengan menggunakan protokol PPTP untuk koneksi ke jaringan private sebagai *remote access client* secara aman melalui jaringan publik data seperti internet. Dengan kata lain, PPTP digunakan sesuai dengan permintaan, misalnya dapat digunakan dengan VPN melalui internet atau jaringan publik data berbasis TCP/IP lainnya. PPTP juga dapat digunakan pada LAN untuk membuat VPN dalam LAN.

Fitur penting dalam penggunaan PPTP adalah PPTP mendukung VPN dengan menggunakan Publik-Switched Telephone Networks (PSTNs). PPTP menyederhanakan dan mengurangi biaya dalam penggunaan pada perusahaan besar dan sebagai solusi untuk remote atau mobile users karena PPTP memberikan komunikasi yang aman dan terenkripsi melalui line publik telephone dan internet.

Secara umum, terdapat tiga komponen di dalam komputer yang menggunakan PPTP, yaitu :

1. PPTP client
2. Network access server
3. PPTP server

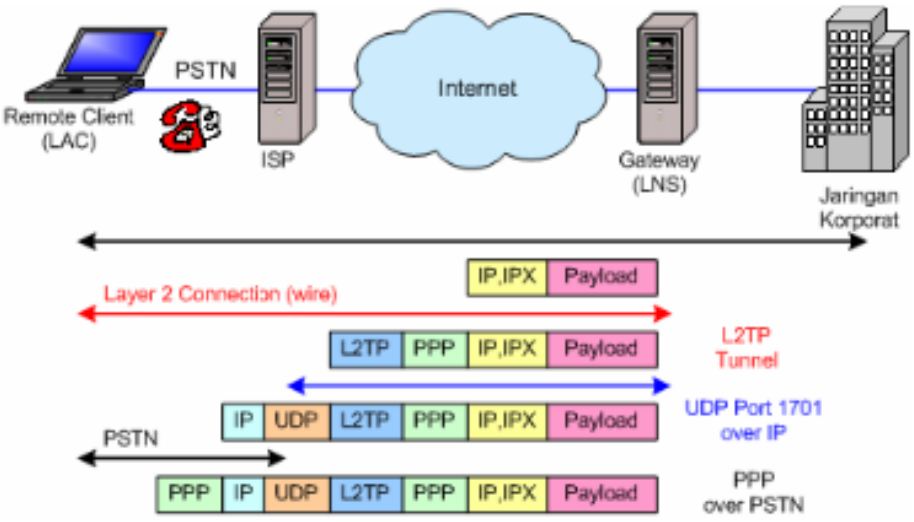
Dimana PPTP juga adalah sebuah protokol yang mengizinkan hubungan Point-to Point Protocol (PPP) melewati jaringan IP, dengan membuat Virtual Private Network (VPN). Berikut adalah karakteristik dari PPTP VPN :

- algorima enkripsi (40bit - 128bit)
- cara kerja :
    1. Membuat enkapsulasi frame pada ip, ipx atau netbeui dalam sebuah Generic Routing Encapsulation (GRE).
    2. GRE dibungkus dalam sebuah paket IP untuk membuat tunnel data asli dienkripsi dengan MPPE (Microsoft Point to Point Encryption).
- Kelemahan :

  session key (kunci akses yang digenerate server) diambil dari password user sehingga mudah dibobol.
- Keamanan melalui paket-2 enkripsi PPTP ini kurang aman dibanding dengan jenis protocol L2TP/IPSec.
- Tidak memberikan integritas data (yaitu semacam suatu bukti bahwa data tidak dimodifikasi selama dalam transit pengiriman)
- Tidak memberikan data authentikasi asli/asal (semacam bukti bahwa data dikirim oleh user yang *authorized*)
- Berdasarkan pada ektensi protokol Point-to-point (PPP)
- Mendukung enkripsi melalui enkripsi Microsoft Point-to-Point Encryption (MPPE)
- Menggunakan username dan password untuk authentication
- Pilihan yang bagus untuk kemampuan dasar VPN
- Protocol PPTP ini sudah ada beserta didalam semua client OS Windows modern
- Tidak memerlukan suatu publik-key infrastructure (PKI)

2.5.2.2 L2TP/IP Security (IPSec)

L2TP atau Layer 2 Tunneling Protocol merupakan gabungan dari L2F (Layer 2 Forwading) milik cisco dengan PPTP milik Microsoft. L2TP dapat membawa seluruh jenis protokol komunikasi. Umumnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP encapsulated PPP frame sebagai data yang di tunnel. Ada dua tipe model tunnel L2TP, yaitu *compulsory* dan *voluntary*. Perbedaan yang utama dari keduanya adalah terletak pada *endpoint* tunnel-nya. Model compulsory ujung tunnel-nya berada pada ISP sedangkan model voluntary ujung tunnel-nya berada pada klien remote. Yang perlu diketahui dari L2TP adalah bahwa L2TP ini murni hanya membentuk jaringan tunnel, oleh karena itu L2TP sering dikombinasikan dengan IPSec sebagai metode enkripsi.



Gambar 2.8 Voluntary Model L2TP [17]

1. *Remote client* mempunyai koneksi *pre-established* ke ISP. Remote Client berfungsi juga sebagai LAC (L2TP Access Concentrator). Dalam hal ini,

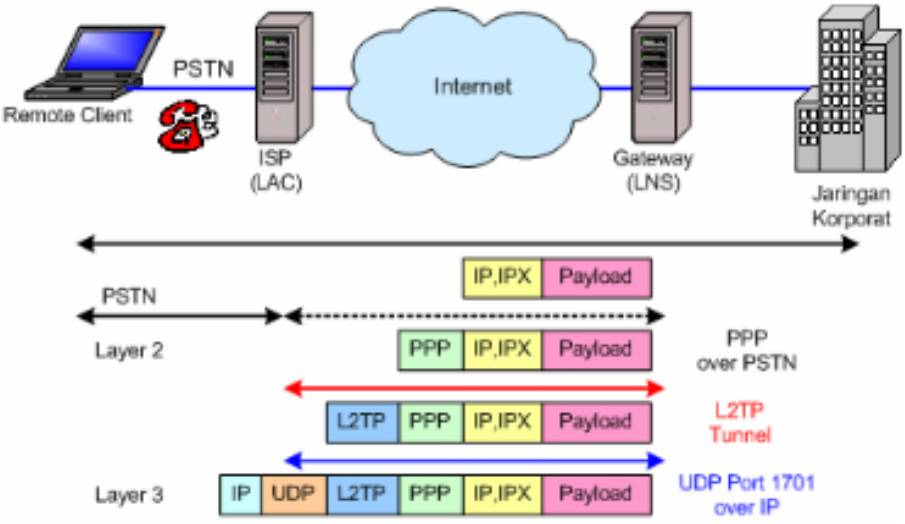
host berisi *software client* LAC mempunyai suatu koneksi ke jaringan publik (internet) melalui ISP.

2. *Client* L2TP (LAC) menginisiasi *tunnel* ke L2TP ke LNS (L2TP Network Server).

3. Jika LNS menerima koneksi, LAC kemudian meng-enkapsulasi PPP dengan L2TP, dan meneruskannya melalui *tunnel*.

4. LNS menerima *frame-frame* tersebut, kemudian melepaskan L2TP, dan memprosesnya sebagai *frame incoming* PPP biasa.

5. LNS kemudian menggunakan pengesahan PPP untuk memvalidasi *user* dan kemudian menetapkan alamat IP.



Gambar 2.9 Compulsory Model L2TP[17]

1. *Remote Client* memulai koneksi PPP ke LAC. Pada gambar diatas LAC berada di ISP.

2. ISP menerima koneksi tersebut dan *link* PPP ditetapkan.

3. ISP melakukan *partial authentication* (pengesahan parsial) untuk mempelajari *user name*. Database *map user* untuk layanan-layanan dan *endpoint tunnel* LNS, dipelihara oleh ISP.
4. LAC kemudian menginisiasi *tunnel* L2TP ke LNS.
5. Jika LNS menerima koneksi, kemudian mengenkapsulasi PPP dengan L2TP, dan meneruskannya melalui *tunnel* yang tepat.
6. LNS menerima *frame-frame* tersebut, LAC kemudian melepaskan L2TP, dan memrosesnya sebagai *frame incoming* PPP biasa.
7. LNS kemudian menggunakan pengesahan PPP untuk memvalidasi *user* dan kemudian menetapkan alamat IP.

Yang perlu diketahui dari L2TP adalah bahwa L2TP ini murni hanya membentuk jaringan tunnel, oleh karena itu L2TP sering dikombinasikan dengan IPSec sebagai metode enkripsi.

IPsec atau IP Security didesain untuk menyediakan interoperabilitas, kualitas yang baik, keamanan jaringan berbasis kriptografi untuk IPv4 dan IPv6. layanan yang disediakan meliputi kontrol akses, integritas hubungan, autentifikasi data asal, proteksi jawaban lawan, kerahasiaan (enkripsi), dan pembatasan aliran lalulintas kerahasiaan. Layanan-layanan ini tersedia dalam IP layer, memberi perlindungan pada IP dan lapisan protokol berikutnya[11]. Ada empat layanan yang disediakan oleh IPSec, yaitu[12]:

- *Confidentiality*: Untuk menjamin kerahasiaan agar supaya pihak-pihak yang tidak berwenang tidak dapat melihat data yang dikirimkan.
- *Integrity* : Untuk menjamin agar supaya data tidak berubah selama data dalam perjalanan menuju tujuan.

- *Authenticity* : Untuk menjamin agar supaya data yang dikirimkan berasal dari pengirim yang benar.
- *Anti Reply* : Untuk menjamin agar supaya transaksi data hanya dilakukan sekali, kecuali pihak yang berwenang mengizinkan untuk melakukan transaksi data secara berulang.

2.6 ENUM Server

Padaskripsi ini akan digunakan ENUM server sebagai pemappingan (pemetaan) nomor-nomor identitas pelanggan (misal nomor telepon rumah) ke dalam sistem DNS URI (*Uniform Resources Identifier*). Pada umumnya manusia cenderung lebih mudah untuk menggunakan sebuah nomor dalam menghubungi seseorang ketimbang mengingat DNS URI orang tersebut, sedangkan satu DNS URI dapat memiliki beberapa nomor yang berbeda-beda. Untuk itu digunakanlah ENUM untuk melakukan pemetaan nomor-nomor tersebut ke dalam DNS URI agar dapat dikenali oleh server.

Selain itu ENUM juga dapat berfungsi dalam memprioritaskan alamat-alamat URI yang digunakan. Jadi misalkan satu nomor telepon memiliki 3 URI, yaitu sip:alice@telkom.co.id, sip:alice@open-ims.test, dan satu lagi voice mailbox, jika salah satu URI diatas gagal untuk dihubungi maka nomor telepon tersebut akan ke urutan berikutnya sampai dengan prioritas terakhir yaitu masuk ke voice mailbox.

2.7. Parameter QoS

Terdapat beberapa parameter QoS yang biasanya digunakan dalam melakukan suatu penerapan sistem seperti *delay, jitter, packet loss, round trip time, throughput*, dan lain sebagainya. Namun ada penelitian ini hanya akan digunakan tiga parameter saja, yaitu *delay, jitter,* dan *throughput*.

2.7.1 Delay

Delay merupakan lama waktu dari awal paket dikirim sampai dengan paket sampai tujuan (terminal penerima). Delay merupakan parameter QoS yang sangat penting untuk menentukan kualitas dari jaringan IMS. Menurut standar ITU-T G.104, kualitas VoIP yang baik jika delay-nya lebih kecil daripada 150ms agar supaya tidak terjadi overlap komunikasi.

2.7.2 Jitter

Jitter merupakan parameter QoS yang mempengaruhi kualitas suara. Semakin kecil jitter yang dihasilkan maka akan semakin bagus suara yang didengar oleh si penerima. Begitu juga sebaliknya, semakin besar jitter yang dihasilkan maka akan semakin buruk suara yang didengar oleh si penerima (putus-putus). Menurut standar ITU-T G.104, jitter yang baik jika nilainya lebih kecil daripada 30ms.

2.7.3 Throughput

Throughput merupakan banyaknya paket yang dapat dikirim dapat satuan waktu. Throughput dapat diukur dari kecepatan transmisi paket. Semakin besar nilai throughput maka semakin banyak paket yang terkirim dan itu artinya semakin baik kualitas suara yang diterima.

2.8. Hipotesis

Berdasarkan dari beberapa referensi, diperlukan sebuah sistem keamanan untuk menjaga integritas data pada layanan multimedia, terutama untuk layanan yang tersambung pada jaringan publik yang ingin terhubung ke jaringan internal. Penerapan VPN ini akan dapat meningkatkan keamanan pada jaringan internal namun tentunya akan mempengaruhi nilai QoS yang ada pada sistem jaringan internal tersebut.

Pengaruh penerapan VPN terhadap QoS suatu sistem bergantung pada protokol yang digunakan. Menurut Ahmed A. Joha, dalam *paper*nya yang melakukan uji coba

pengiriman paket TCP perbandingan PPTP dan L2TP terhadap beberapa parameter QoS terlihat pada tabel berikut:

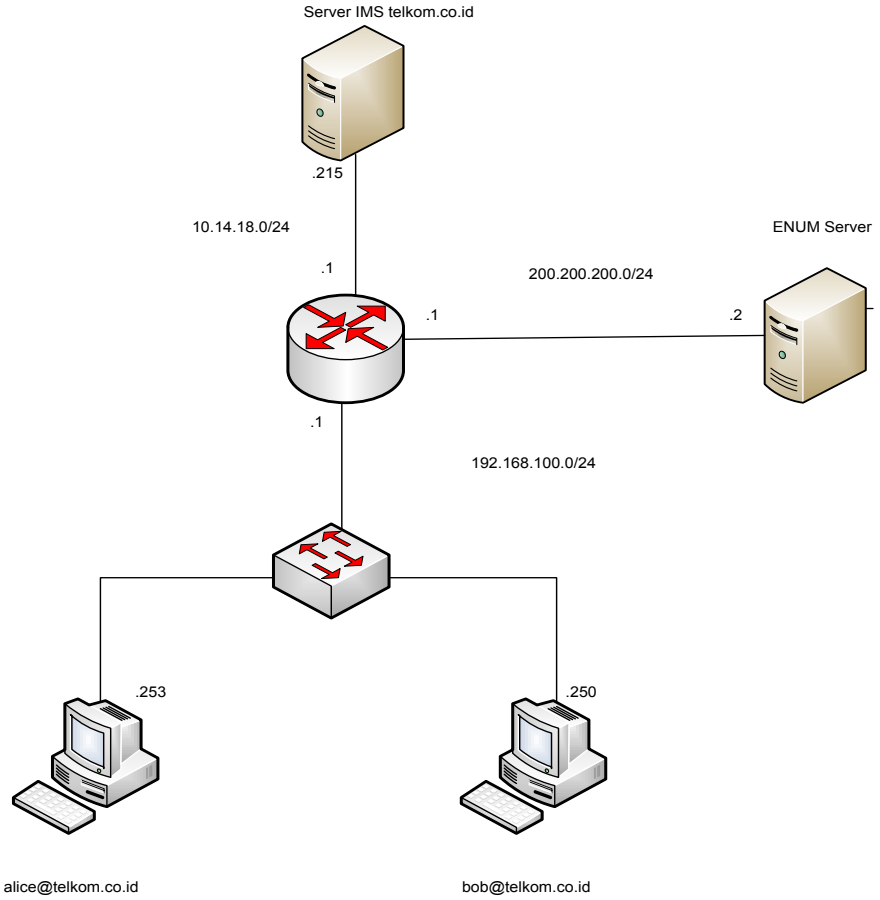
Tabel 2.3 Hipotesis QoS VPN PPTP dan VPN L2TP

No	Parameter	PPTP	L2TP
1	TCP Throughput	1st	2nd
2	Round Trip Time	1st	2nd
3	UDP Throughput	1st	2nd
4	Jitter	Low	High
5	Packet Loss	Low	High

Berdasarkan tabel diatas dapat dilihat bahwa nilai *throughput* dan *jitter* pada VPN PPTP lebih baik dibandingkan pada VPN L2TP. Kemudian yang jadi pertanyaan apakah VPN PPTP dan VPN L2TP juga memberikan hasil pengaruh yang sama ketika dilakukan layanan VoIP pada jaringan IMS. Penelitian ini akan menguji pengaruh dari penerepan VPN PPTP dan VPN L2TP yang melakukan layanan VoIP pada jaringan IMS terhadap paket QoS.

BAB 3
PERANCANGAN SISTEM

Pada penulisan skripsi ini akan digunakan sebuah virtual mesin, yaitu virtuabox sebagai penghematan komponen-komponen yang akan digunakan. Di dalam virtualbox ini akan diinstal beberapa Sistem Operasi yang digunakan untuk keperluan skripsi ini, antara lain: Ubuntu OS sebagai server open IMS dan server ENUM, Vyatta OS sebagai VPN router, dan Windows sebagai IMS klien. Berikut topologi system yang akan digunakan:



Gambar 3.1 Topologi Sistem

Pada skripsi ini akan dilakukan tiga pengujian. [1] Klien 1 (alice@telkom.co.id) akan melakukan layanan VoIP tanpa menggunakan VPN ke klien 2 (bob@telkom.co.id) untuk mengetahui protokol RTP VoIP yang tertangkap oleh Wireshark. [2] Klien 1 akan melakukan layanan VoIP dengan menggunakan VPN PPTP ke klien 2 untuk mengetahui apakah protokol RTP VoIP terenkripsi oleh protokol PPP atau tidak serta melihat QoS-nya untuk dibandingkan dengan VPN L2TP. [3] Klien 1 akan melakukan layanan VoIP dengan menggunakan VPN L2TP ke klien 2 untuk mengetahui apakah protokol tersebut terenkripsi oleh protokol ESP atau tidak serta melihat QoS-nya untuk dibandingkan dengan VPN PPTP. Untuk melakukan pengujian (*testbed*) digunakan sebuah software yang dapat menangkap (*capture*) paket-paket yang bersebaran di udara, yaitu Wireshark. Dengan Wireshark maka akan terlihat apakah sistem yang digunakan benar-benar dapat mengamankan data-data klien atau tidak. Selain itu Wireshark digunakan sebagai tool untuk mengukur parameter-parameter QoS sistem yang dirancang.

3.1 Instalasi dan Konfigurasi Komponen IMS Core

Pada penulisan skripsi ini akan digunakan perangkat lunak bebas OpenIMSCore. Berikut langkah-langkah instalasi OpenIMSCore[15] :

1. Masuk ke terminal Ubuntu sebagai root.
2. Update repositori Ubuntu.
3. Unduh Subversion package.
4. Membuat direktori OpenIMSCore.
5. Membuat direktori CSCF dan FhoSS.
6. Unduh source code CSCF dan FHoSS versi terakhir.
7. Install package-package yang dibutuhkan.
8. Copy open-ims DNS file ke folder bind.

9. Ubah file named.conf.local

   Lalu tambahkan kata-kata berikut ke dalam file tersebut:

   zone “open-ims.test” {

   type master;

   file “/etc/bind/open-ims.dnszone”;

   };

10. Ubah file resolv.conf.

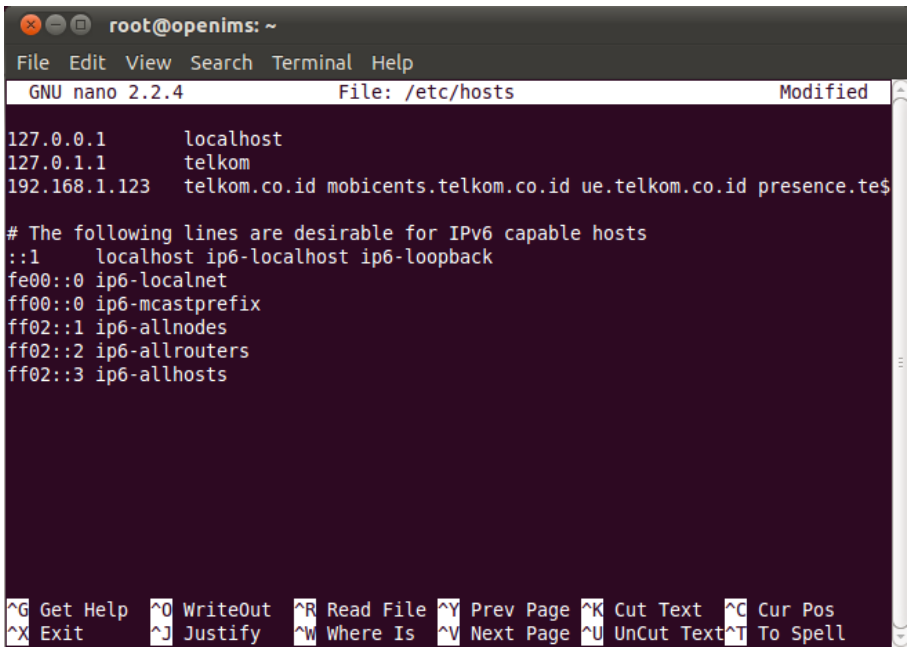
    Masukan domain dan nameserver sesuai yang diinginkan, dalam skripsi ini digunakan domain open-ims.test dan namesever 10.14.18.216. Maka edit file resolv.conf tersebut seperti ini:

    domain open-ims.test

    search open-ims.test

    nameserver 10.14.18.216

11. Ubah file hosts.



Gambar 3.2 Hosts Open IMS

Replace domain dan IP address server (domain "telkom.co.id" dan IP address "192.168.1.123") sesuai dengan domain dan IP address server yang digunakan (misalnya domainnya "open-ims.test dan IP addressnya "10.14.18.216"). Dalam skripsi ini digunakan dua domain yang berbeda, yaitu telkom.co.id dan open-ims.test.

12. Restart bind server

13. Cek apakah step 7 sampai 11 sudah benar. Lihat apakah ping mendapat response, atau tidak. Pada answer section harus tertulis alamat IP addres yang digunakan.
14. Masuk ke directory OpenIMSCore dan *replace* domain dan IP address server yang dengan menjalankan file ***./configurator.sh***.
    Dilayar akan muncul:
    Domain Name:
    IP Address:
    Isi domain dan IP address yang digunakan.

15. Atur database mysql.
16. Compile source code (CSCF dan FHoSS).
17. Copy configuration file ke folder OpenIMSCore.
18. Jalankan OpenIMSCore. Jalankan setiap CSCF dan FHOSS pada satu tab terminal.

Tabel 3.1 Daftar Element dan Port IMS Core

Element	Port Number
P-CSCF	4060
I-CSCF	5060
S-CSCF	6060
Diameter	3868; 3869; 3870

Untuk mengetahui data user did alam database yang telah tersimpan, maka buka halaman berikut : 10.14.18.216:8080.

Username: hssAdmin (untuk admin) untuk member “hss”

Password: hss

3.2 Konfigurasi ENUM Server

Pad skripsi ini akan digunakan ENUM server untuk memetakan nomor-nomor telepon klien Open IMS ke dalam alamat DNS URI. Berikut langkah-langkah dalam membuat ENUM server:

1. Masuk ke terminal Ubuntu.
2. Masuk sebagai root.
3. Edit file resolv.conf untuk memasukkan ip address name server.
4. Edit file ”/etc/bind/named.conf.local”.
5. Buat file baru sebagai database dan masukkan nomor-nomor telepon yang ingin dipetakan di ENUM server.

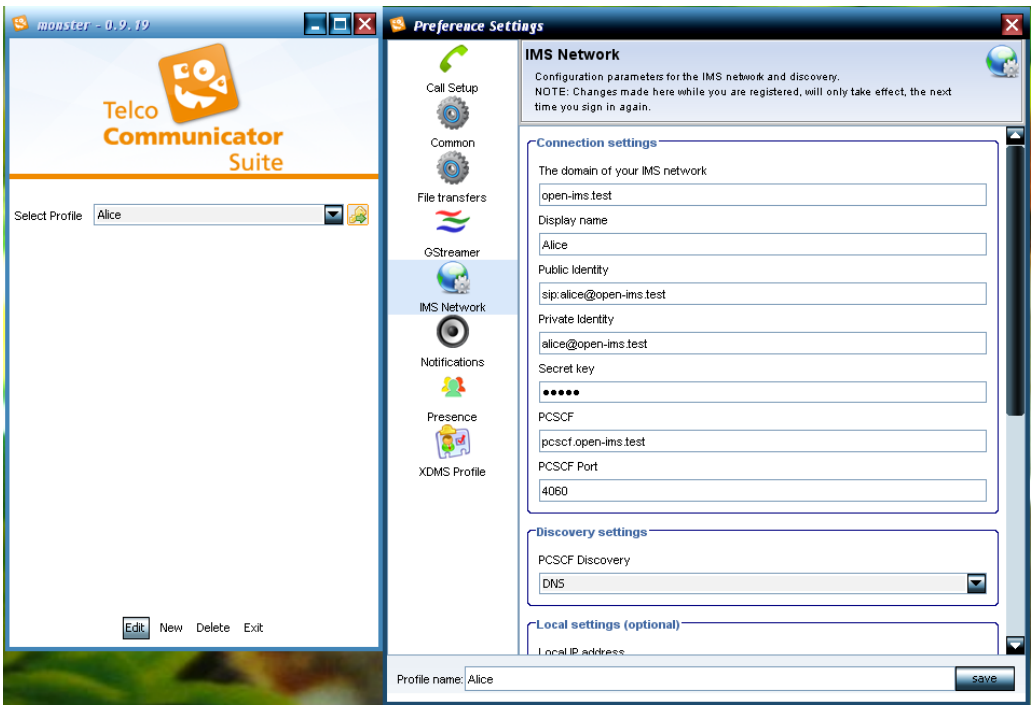
3.3 Konfigurasi VPN PPTP dan L2TP pada Vyatta OS

Pada skripsi ini akan dibuat remote acces VPN dengan dua protokol keamanan yang disediakan oleh Vyatta OS, yaitu PPTP dan L2TP. Kedua protokol ini akan mengenkripsi data-data user saat melakukan suatu layanan VoIP. Berikut langkah-langkah untuk menngkonfigurasi VPN PPTP dan L2TP di Vyatta OS:

1. Masuk sebagai super admin (root).
2. Atur IP address pada interface yang ingin digunakan.
3. Buat *routing protokol table* agar paket yang ingin dikirim ter-*forward* - sampai dengan tujuan.
4. SetupVPN PPTP dan L2TP dengan memberikan username dan password yang nantinya akan digunakan klien dalam membuat koneksi. Untuk L2TP jangan lupa untuk mengatur *pre-shared-secret* yang nantinya akan digunakan klien sebagai kunci untuk membentuk *tunnel*.
5. Setup *service* NAT agar IP address user tidak terdeteksi oleh *sniffer tools*.

3.4 Instalasi myMONSTER sebagai IMS Client

Pada skripsi ini software yang digunakan sebagai IMS Client adalah myMONSTER versi 0.9.19 bersifat opensource. Untuk proses instalasi user hanya perlu mendownload software tersebut dari website Telco Communicator Suite (TCS). Berikut tampilan dari myMONSTER:



Gambar 3.3 IMS Client

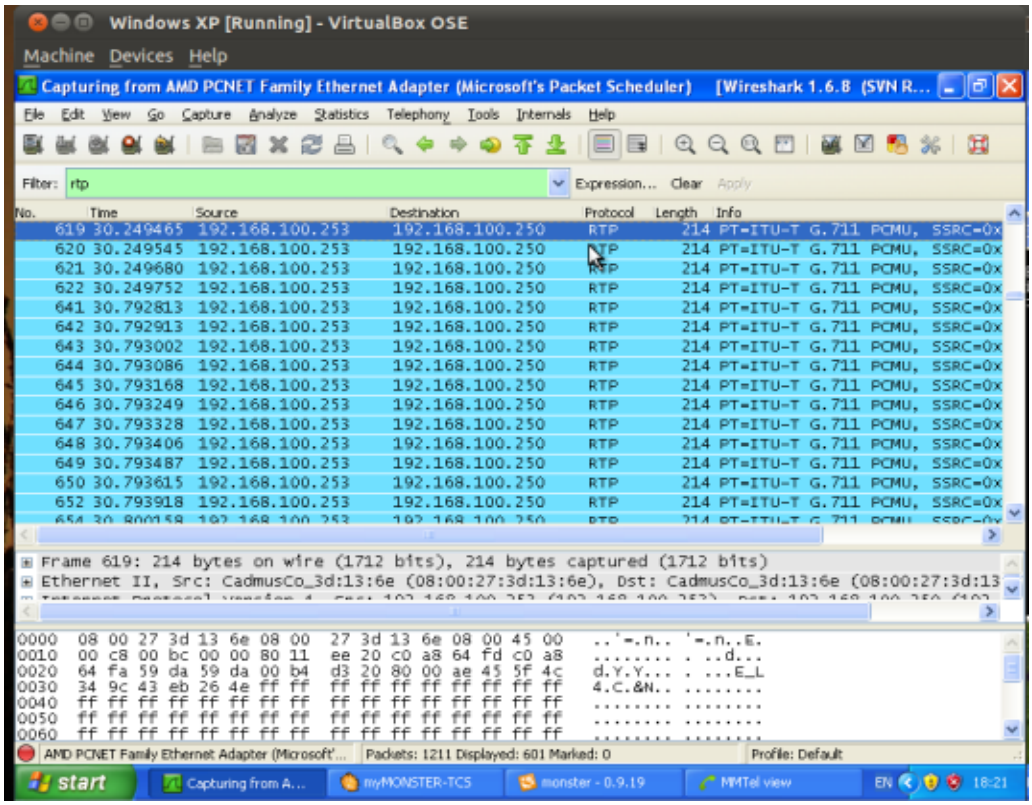
Dari gambar diatas, masukan *The domain of your IMS network* dengan nama domain yang digunakan. Pada skripsi ini nama domain yang digunakan adalah telkom.co.id. Setelah masukan nama user yang ingin ditampilkan pada aplikasi di kotak *Display Name.* Masukan IMPU (*IP Multimedia Public Identity*) dan IMPI (*IP Multimedia Private Identity*) di kotak *Public Identity* dan *Private Identity* masing-masing. Masukan *Secret Key* yang diberikan oleh ISP. Untuk alice@telkom.co.id maka passwordnya adalah “alice”, sedangkan untuk bob@telkom.co.id passwordnya adalah “bob”. Masukan alamat PCSCF yang digunakan oleh system, yaitu pcscf.telkom.co.id dan portnya 4060. Setelah itu, selesai simpan dengan nama yang dinginkan.

BAB 4
Implementasi dan Analisis Sistem

Seperti yang telah dijelaskan pada bab sebelumnya bahwa akan dilakukan tiga pengujian skenario pada skripsi ini.

4.1 Pengujian Layanan VoIP IMS Tanpa VPN

Pada pengujian ini akan dilakukan sebuah layanan IMS berupa VoIP tanpa menerapkan VPN. Pengujian ini dimaksudkan untuk menunjukkan protokol RTP yang tertangkap oleh Wireshark saat user melakukan layanan VoIP. Berikut gambar dari hasil penjejakan paket pada Wireshark.



Gambar 4.1 Penjejakan Paket VoIP IMS Tanpa VPN

Pada gambar diatas dapat terlihat bahwa protokol RTP yang merupakan protokol terpenting dalam layanan VoIP dapat ditangkap dengan jelas oleh Wireshark. Protokol RTP merupakan protokol yang dapat dibaca dan diubah oleh seorang *hacker* dengan membaca isi dari *payload* protokol tersebut dengan menggunakan suatu perangkat lunak tertentu.

Selain itu, pada gambar diatas juga IP dari klien yang menggunakan layanan VoIP dapat terbaca juga oleh Wireshark. Hal ini cukup berbahaya karena dengan mengetahui alamat IP si user maka seorang hacker juga dapat mengetahui keberadaan si klien.

4.2 Pengujian Layanan VoIP IMS Menggunakan VPN PPTP

Pada pengujian ini akan dilakukan sebuah layanan VoIP dari klien IMS1 (alice@telkom.co.id) ke klien IMS1 lainnya (bob@telkom.co.id) dengan menggunakan VPN PPTP. Dari pengujian yang telah dilakukan diperoleh data sebagai berikut:

Tabel 4.1 QoS Pengujian Menggunakan VPN PPTP

Pengukuran ke-	Delay (ms)	Jitter (ms)	Throughput (packet/sec)
1	5,2361	1,21	190,979
2	5,2059	1,18	192,091
3	5,1995	1,10	192,327
4	5,1860	1,05	192,639
5	5,1838	0,97	192,908
6	5,1808	0,90	193,022
7	5,1754	0,85	193,221
8	5,1714	0,79	193,370
9	5,1655	0,75	193,593
10	5,1620	0,71	193,726
Rata-rata	5,1866	0,95	192,788

4.3 Pengujian Layanan VoIP IMS Menggunakan VPN L2TP

Pada pengujian ini akan dilakukan sebuah layanan IMS berupa VoIP dari klien IMS1 (alice@telkom.co.id) ke klien IMS1 lainnya (bob@telkom.co.id) dengan menggunakan VPN L2TP. Dari hasil pengujian diperoleh data sebagai berikut:

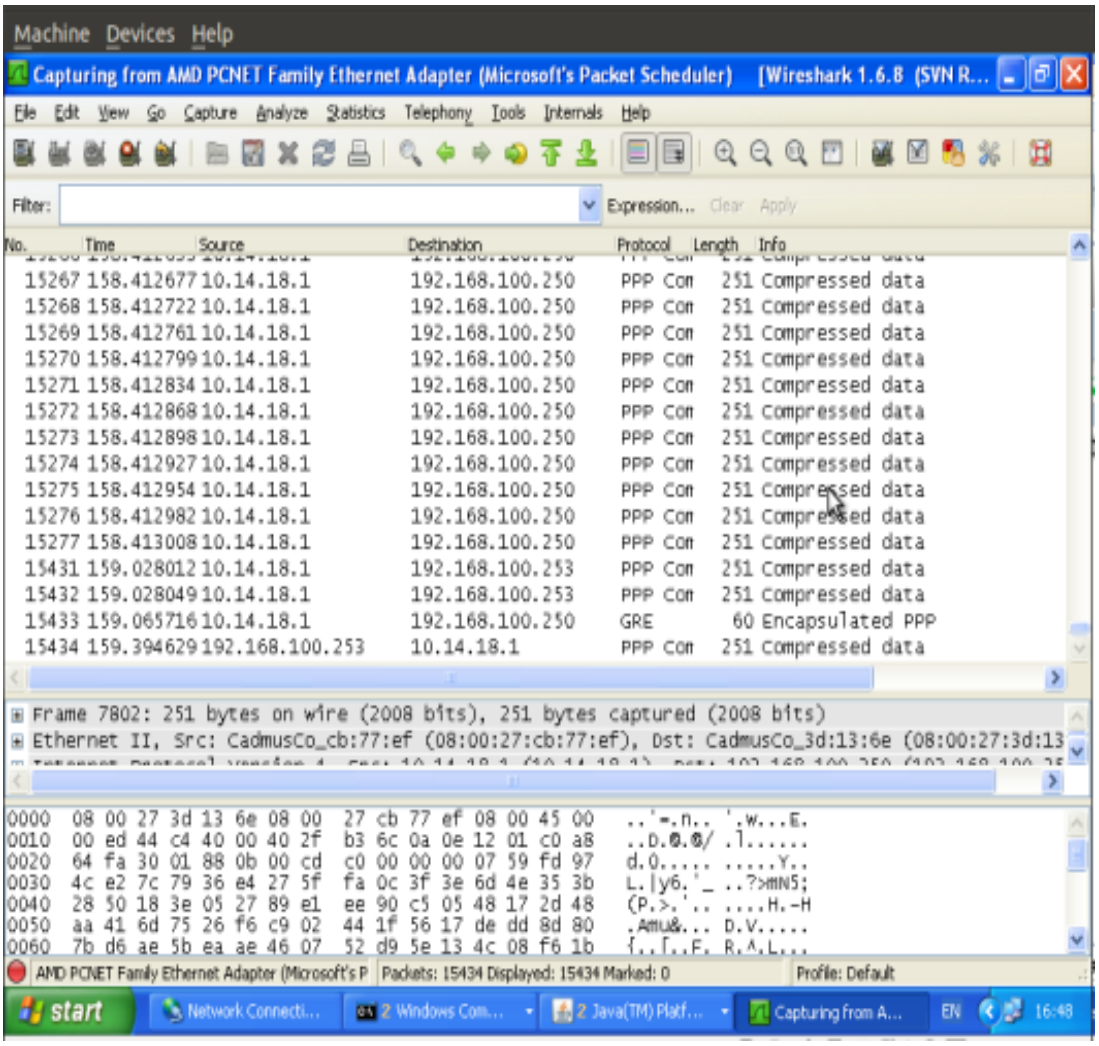
Tabel 4.2 QoS Pengujian Menggunakan VPN L2TP

Pengukuran ke-	Delay (ms)	Jitter (ms)	Throughput (packet/sec)
	5,4643	1,24	183,007
2	5,4450	1,20	183,651
3	5,4345	1,17	184,011
4	5,4222	1,10	184,427
5	5,4101	0,98	184,841
6	5,3976	0,92	185,266
7	5,3884	0,86	185,582
8	5,3791	0,79	185,903
9	5,3700	0,75	186,211
10	5,3614	0,70	186,519
Rata-rata	5,4072	0,97	184,942

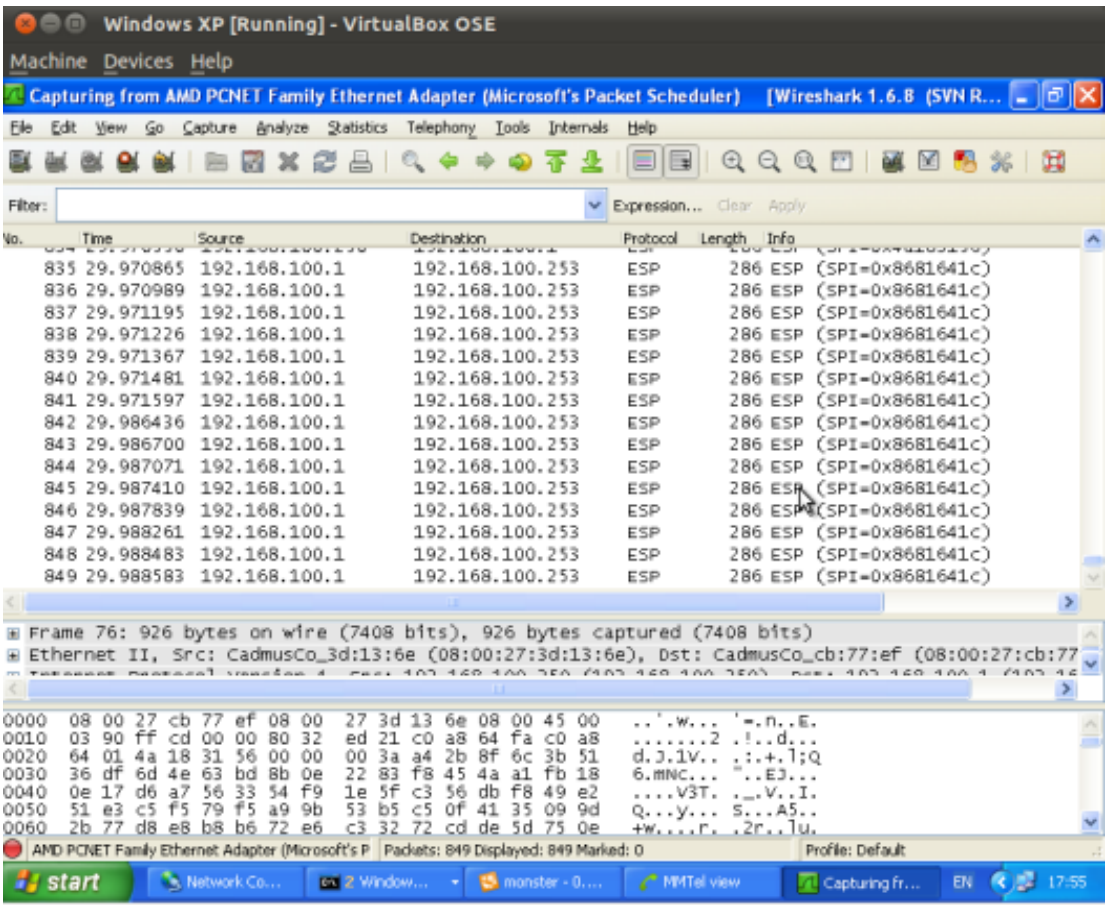
4.4 Analisis Perbandingan Layanan VoIP IMS VPN PPTP dengan VPN L2TP

Setelah diperoleh hasil dari seluruh pengujian, dapat dilihat bahwa dengan diterapkannya VPN maka data-data user yang melakukan layanan VoIP dienkripsi sesuai dengan protokol yang digunakan. Hal ini terjadi karena pada jaringan IMS over VPN terdapat metode *tunneling* Pada sistem yang tidak menerapkan VPN maka *payload* yang ada pada protokol RTP terlihat secara transparan oleh perangkat lunak Wireshark (lihat Gambar 4.1). Sedangkan pada sistem yang menerapkan VPN, data *payload* protokol RTP tidak terlihat karena protokol RTP tersebut telah diubah ke dalam protokol GRE/PPP untuk VPN PPTP dan diubah ke dalam protokol ESP untuk

VPN L2TP. Data-data dari kedua protokol tersebut beserta dengan data *payload*-nya tidak dapat terlihat oleh Wireshark (lihat Gambar 4.2 dan Gambar 4.3).



Gambar 4.2 Penjejakan Paket VoIP IMS VPN PPTP



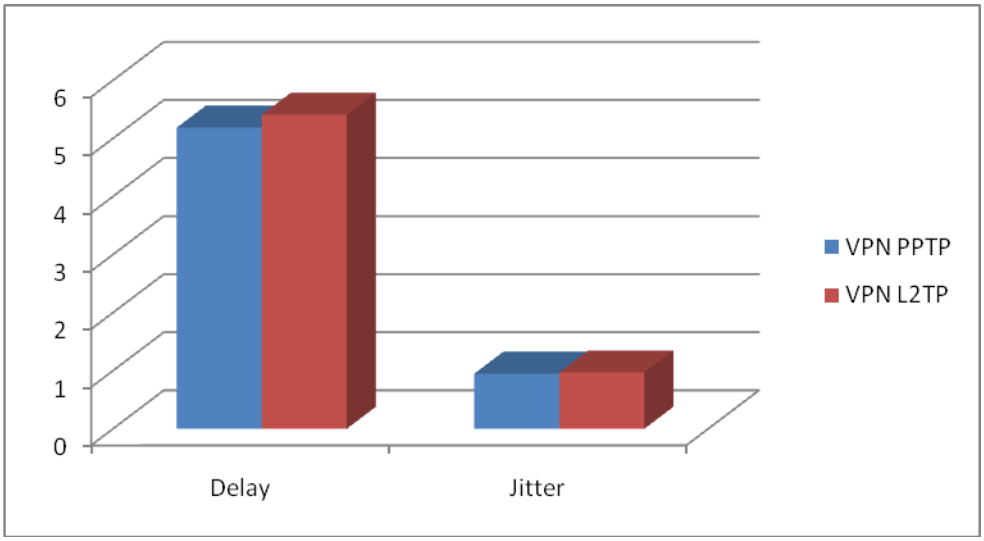
Gambar 4.3 Penjejakan Paket VoIP IMS VPN L2TP

Selain itu, dengan adanya VPN ini IP address si klien dan IMS server tidak terlihat oleh Wireshark karena telah digantikan oleh IP address milik VPN server. Dengan ini maka kemungkinan sulit bagi *hacker* untuk melacak keberadaan si klien dan IMS server.

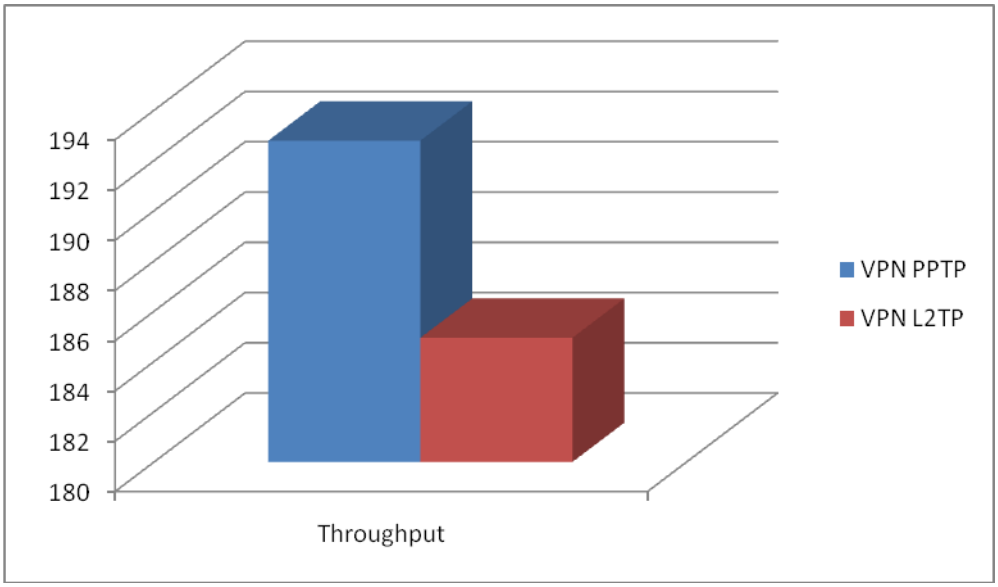
Untuk analisis perbandingan QoS jaringan IMS yang menerapkan VPN PPTP dengan VPN L2TP dapat dilihat secara ringkas dari tabel dan grafikberikut:

Tabel 4.3 Perbandingan QoS VPN PPTP dan L2TP

	Delay (ms)	Jitter (ms)	Throughput (packet/sec)
VPN PPTP	5,1866	0,95	192,788
VPN L2TP	5,4072	0,97	184,942



Gambar 4.4 Perbandingan Nilai Delay dan Jitter



Gambar 4.5 Perbandingan Nilai Throughput VPN PPTP dan VPN L2TP

Berdasarkan tabel dan grafik diatas, perbandingan QoS VPN PPTP dengan VPN L2TP terbukti seperti apa yang telah dikatakan oleh Ahmed A. Joha pada papernya bahwa nilai throughput dan jitter pada VPN PPTP lebih baik dibandingkan VPN

L2TP. Hal ini dapat dilihat dari tabel 4.3 bahwa nilai delay dan jitter pada VPN PPTP lebih kecil dibandingkan dengan delay dan jitter pada VPN L2TP. Nilai delay pada VPN PPTP lebih baik 4.08% daripada VPN L2TP. Nilai jitter pada VPN PPTP lebih baik 2.06% daripada VPN L2TP. Hal ini dikarenakan pada VPN L2TP mengalami dua kali proteksi data, yaitu dalam pengenkapsulasian paket dengan menggunakan *pre-shared-secret* dan pengesahan paket validasi *user* dengan menggunakan *username* dan *password*. *Pre-shared-secret* ini digunakan L2TP untuk menjaga data dengan cara mengenkripsi data yang ditransmisi dengan menambahkan header L2TP. Sedangkan *username* dan *password* L2TP digunakan untuk menjamin integritas data bahwa data yang dikirimkan benar dari user yang melakukan pengirimin data. Jadi setiap ada data yang masuk ke *tunnel* L2TP dijamin dari user yang bersangkutan. Hal ini menyebabkan delay dan jitter user yang menggunakan L2TP ini bernilai lebih besar dibandingkan yang menggunakan PPTP. Sedangkan untuk nilai throughput pada VPN PPTP lebih besar dibandingkan nilai throughput pada VPN L2TP. Nilai throughput pada VPN PPTP lebih baik 4.07% daripada VPN L2TP. Hal ini dikarenakan nilai delay pada VPN PPTP lebih kecil dibandingkan dengan nilai delay pada VPN L2TP. Seperti yang dijelaskan sebelumnya bahwa nilai delay selalu berbanding terbalik dengan nilai throughput.

BAB 5
KESIMPULAN

1. Berdasarkan hasil percobaan yang telah dilakukan, penggunaan layanan IMS berupa VoIP tanpa menggunakan *remote access* VPN dapat tertangkap jelas data-data si klien yang melakukan suatu layanan IMS dengan merekam protokol RTP.
2. Berdasarkan hasil percobaan yang telah dilakukan, VPN PPTP dan VPN L2TP dapat mengamankan data-data klien IMS yang melakukan layanan VoIP dengan mengenkripsi protokol RTPnya.
3. Berdasarkan hasil pecobaan yang telah dilakukan, nilai parameter QoS (delay, jitter, dan throughput) VPN PPTP pada layanan VoIP jaringan Open IMS lebih baik dibandingkan dengan nilai parameter QoS VPN L2TP. Nilai delay pada VPN PPTP lebih baik 4.08% daripada VPN L2TP. Nilai jitter pada VPN PPTP lebih baik 2.06% daripada VPN L2TP. Dan nilai throughput pada VPN PPTP lebih baik 4.07% daripada VPN L2TP.
4. Berdasarkan hasil percobaan yang telah dilakukan, penerapan VPN PPTP dan VPN L2TP dapat diterapkan pada jaringan Open IMS sesuai dengan standar ITU-T G.104 mengenai standar layanan VoIP, yaitu nilai delay lebih kecil daripada 150ms dan nilai jitter lebih kecil daripada 30ms.

DAFTAR REFERENSI

[1]. Rachmana, Nana dan Praditya, Dhata. "Analisis dan Simulasi Model Trafik Next Generation Network". Bandung : Institut Teknologi Bandung.

[2]. T.C., Henni., Djanali, Supeno., Husni, M. "Kualitas Layanan IP Multimedia Subsystem". Surabaya : Institut Teknologi Surabaya.

[3]. Zacharias, JM. (2006)."Seamless Mobility". http://www.jmzacharias.com/seamless.htm diakses pada 29 November 2011.

[4]. FOKUS OPEN IMS PLAYGROUND. Open Testbed for IMS Technologies. http://www.fokus.fraunhofer.de/en/fokus_testbeds/open_ims_playground/components/osims/index.html diakses pada 13 Desember 2011.

[5]. Magedanz, Th. "IMS – the IP Multimedia Subsystem as NGN Service Delivery Platform".

[6]. OPENSOURCEIMS core. http://openimscore.org/ diakses pada 13 Desember 2011.

[7]. Wright, James. "SIP – An Introduction". Konektik.

[8]. Stallings, p.214. "SIP Request Messages".

[9]. Johnston, Alan B. 2004. *Understanding Session Initiation Protocol, 2nd Edition*. Norwood, MA. Artech House.

[10]. Gupta Meeta."Building a Virtual Private Network". Premier Press 2645 Erie Avenue, Suite 41 Cincinnati, Ohio 45208, 2003.

[11]. Stallings, p.214-215. "SIP Response Messages"

[12]. Ardiyansyah, Bambang. "Implementasi IPSec Pada VPN". Palembang : Universitas Sriwijaya.

[13]. 3GPP (2003) : 3rd Generation Partnership Project, TS 33.210: Release 5, 3G Security, Network Domain Security, IP Network Layer Security.

[14]. Alex. (2010). INSTALASI OPENIMSCORE. http://alexatmana.wordpress.com/2010/12/30/instalasi-openimscore/ diakses pada 26 Desember 2011.

[15]. Implementasi ENUM Server. (2010,May). http://opensource.telkomspeedy.com/ diakses pada Mei 2012.

[16]. Ardiansyah. "Implementasi dan Analisis QoS Pada PPTP dan L2TP Remote Access VPN untuk Layanan Secured Mobile IP based Video Telephony". Depok : Universitas Indonesia.

[17]. Derianto, Erix. "Perbandingan Tunneling pada Komunikasi VPN". Palembang : Universitas Indonesia".

LAMPIRAN 1 KONFIGURASI OPEN IMS CORE

#sudo -i

apt-get update

apt-get install subversion

mkdir /opt/OpenIMSCore/
#chown -R username /opt/OpenIMSCore/

cd /opt/OpenIMSCore
mkdir ser_ims
mkdir FHoSS

svn checkout

http://svn.berlios.de/svnroot/repos/openimscore/ser_ims/trunk

ser_ims

svn checkout http://svn.berlios.de/svnroot/repos/openimscore/FHoSS/trunk

FHoSS

#apt-get install sun-java6-jdk mysql-server libmysqlclient15-dev libxml2 libxml2-dev bind9 ant flex bison curl.h

#cp /opt/OpenIMSCore/ser_ims/cfg/open-ims.dnszone /etc/bind/

nano /etc/bind/named.conf.local

zone “open-ims.test” {

type master;

file “/etc/bind/open-ims.dnszone”;

};

#nano /etc/resolv.conf

#nano /etc/hosts

#/etc/init.d/bind9 restart

#ping pcscf.open-ims.test

```
#dig open-ims.test
#cd /opt/OpenIMSCore/
#./configurator.sh  pcscf.cfg  pcscf.xml  icscf.cfg  icscf.xml
scscf.cfg           scscf.xml           /ser_ims/cfg/icscf.sql
/FHoSS/deploy/hss.properties  /FHoSS/deploy/DiameterPeerHSS.xml
/FHoSS/scripts/hss_db.sql /FHoSS/scripts/userdata.sql
#mysql      -uroot      -p      -h      localhost            <
/opt/OpenIMSCore/ser_ims/cfg/icscf.sql
#mysql       -uroot       -p       -h       localhost       <
/opt/OpenIMSCore/FHoSS/scripts/hss_db.sql
#mysql       -uroot       -p       -h       localhost       <
/opt/OpenIMSCore/FHoSS/scripts/userdata.sql
# cd /opt/OpenIMSCore/ser_ims
#make install-libs all
# cd /opt/OpenIMSCore/ser_ims
# ant compile deploy
# cp /opt/OpenIMSCore/ser_ims/cfg/* /opt/OpenIMSCore/
# cd /opt/OpenIMSCore/
# ./pcscf.sh
# ./icscf.sh
# ./scscf.sh
# cd /opt/OpenIMSCore/FhoSS/deply/
# export JAVA_HOME=/usr/lib/jvm/java-6-sun
# ./startup.sh
```

LAMPIRAN 2 KONFIGURASI ENUM SERVER

```
#sudo –i

#gedit /etc/bind/named.conf.local

      zone "5.2.6.e164.id" {

            type master;

            file "/etc/bind/5.2.6.e164.id.db";

      };

#gedit /etc/bind/5.2.6.e164.id.db

$TTL 86400

@     IN SOA           ns.telkom.co.id. root.telkom.co.id. (

                  42    ; Serial

                  3H    ; Refresh

                  15M   ; Retry

                  1H    ; Expiry

                  1D )  ; Minimum of TTL


            IN NS ns.telkom.co.id

0.0.0.1     NAPTR 10 100     "u" "E2U+sip"
"!.^*$!sip:alice@telkom.co.id!".

1.0.0.1     NAPTR 10 100     "u" "E2U+sip"
"!.^*$!sip:bob@telkom.co.id!".

#/etc/init.d/bind9 restart
```

LAMPIRAN 3 KONFIGURASI PPTP DAN L2TP VYATTA ROUTER

```
interfaces {
      ehternet eth0 {
            address 192.168.100.1/24
                  }
      ethernet eth1 {
            address 10.14.18.1/24
                  }
      loopback lo {
                  }
      tunnel tun0 {
            address 20.200.200.1/24
            encapsulation sit
            local-ip 200.200.200.2/24
            remote-ip 200.200.200.1/24
                  }
      }
protocols {
      ospf {
            }
      rip {
            network 10.14.18.0/24
            network 192.168.100.0/24
            network 200.200.200.0/24
            redistribute {
                  connected {
                        }
```

```
                static {
                        }
                }
        }
    ripng {
        interface eth0
        interface eth1
                redistribute {
                        connected {
                                }
                        }
        }
    static {
        route 0.0.0.0/24 {
                next-hop 192.168.100.1 {
                                }
                        }
        }
    }
nat {
    rule 1 {
        outbound-interface eth0
        source {
                address 10.14.18.0/24
                }
        type masquerade
    }
```

```
        rule 10 {
                outbound interface eth0
                outside-address {
                        address 192.168.100.1
                                }
                source {
                        address 192,168.1.0/24
                        }
                type source
                }
}
system {
        flow-accounting {
                interface eth0
                }
        login {
                uservyatta {
                        authentication {
                                encrypted-password **************
                                }
                }
        }
        name-server 10.18.14.215
        ntp-server 0.vyatta.pool.ntp.org
        syslog {
                global {
                        facility all {
```

```
                level notice
                }
            facility protocols {
                level debug
                }
            }
        }
vpn {
    ipsec {
        ipsec-interfaces {
            interface eth0
            }
        }
        nat-network {
            allowed-networks 10.14.18.0/24 {
                }
            }
        nat-tranversal enable
        }
    l2tp {
        remote-access {
            authentication {
                local-user {
                    username hari {
                        password ********
                        }
```

```
                        username hawabu {
                              }
                        }
                  mode local
                  }
            client-ip-pool {
                  start 192.168.2.50
                  stop 192.168.2.200
                  }
            ipsec-setting {
                  authentication {
                        mode pre-shared-secret
                        pre-shared-secret ********
                        }
                  }
            outside-address 192.168.100.1
            outside-nexthop 10.14.18.1
            }
pptp {
      remote-access {
            authentication {
                  local-users {
                        username alice {
                              password *********
                              }
                        username bob {
                              password *********
```

```
                        }
                    }
                mode local
                )
            client-ip-pool {
                start 192.168.1.1
                stop 192.168.1.1
                }
            outside-address 192.168.100.1
            }
        }
}
```