

## ANALISIS PERFORMANSI DAN KEAMANAN VOIP OVER VIRTUAL PRIVATE NETWORK (VPN)

### THE ANALYSIS OF PERFORMANCE AND SECURITY VOIP OVER VIRTUAL PRIVATE NETWORK (VPN)

Pande Putu Rambo Sadewa<sup>1</sup>, Gunawan Adi<sup>2</sup>, Nyoman Bogi Aditya Karna<sup>3</sup>

<sup>1</sup>Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

---

#### Abstrak

Seiring dengan perkembangan teknologi, banyak layanan multimedia telah dikembangkan di internet. Salah satu dari layanan itu adalah VoIP. Teknologi VoIP sangat menguntungkan karena menggunakan jaringan berbasis IP yang sudah memiliki jaringan kuat di dunia sehingga biaya untuk melakukan panggilan jauh lebih efisien daripada menggunakan telepon analog. Tetapi VoIP memiliki kelemahan yaitu keamanan yang tidak terjamin. Karena berbasis IP, maka siapapun bisa melakukan penyadapan dan perekaman terhadap data VoIP. Dari sinilah muncul suatu pemikiran tentang bagaimana caranya untuk mengamankan data VoIP tanpa mengurangi performansi dari jaringan VoIP itu sendiri. Salah satu cara adalah dengan menggunakan VPN (Virtual Private Network). VPN sendiri telah diketahui sebagai salah satu metoda yang handal dalam menangani masalah keamanan jaringan, terutama untuk pengiriman data penting. Untuk mengimplementasikan pemikiran tersebut maka dibuatlah suatu sistem VoIP over VPN. Kemudian dianalisa bagaimana performansi dan keamanan VoIP sebelum dan sesudah menggunakan VPN. Apakah voice yang dihasilkan oleh VoIP over VPN masih memenuhi standar ITU-T berdasarkan delay, jitter dan packet loss. Dari pengujian dengan menggunakan codec G729 didapatkan bahwa untuk bitrate 96 kbps maka performansi (delay, jitter dan packet loss) dengan menggunakan VPN tidak terlalu berubah (adanya peningkatan sekitar 1%- 8%). Tetapi ketika bitrate dibuat dibawah 64 kbps maka performansi VoIP menurun drastis (delay meningkat 1000%, jitter 100% dan packet loss meningkat sekitar 83% sampai 87% ) sedangkan untuk keamanan data VoIP, VPN dapat mengamankan data dari ancaman keamanan. Sebelum menggunakan VPN data VoIP dapat direkam dan dimainkan ulang. Data payloadnya juga dapat ditangkap dan dilihat tetapi setelah menggunakan VPN VoIP tidak dapat direkam dan data payloadnya tidak terlihat.

Kata Kunci :

---

Telkom  
University

### Abstract

With the development of technology, many multimedia services has developed in the internet. One of these service is VoIP. VoIP technology has lot of benefit because its uses IP based network that has complex networking in the world. Therefore the cost to make long distance call is more efficient than using analog telephone. But VoIP have weakness which is there no guarantee of security. Because of its IP based, then everone can sniffed and record VoIP data traffic. From this case, a research on how to make VoIP data securer without reducing the performance of the VoIP network itself came to our thought. One of it was Virtual Private Network Method. VPN itself has known as one of the powerful method to handle security problem, especially securing important data. To implement this idea than a VoIP over VPN system is made. Than the performance and security of VoIP before and after using the VPN is analyzed. Wheater the voice that created by VoIP over VPN system is fulfil the ITU-T standar based on delay, jitter and packet loss. From the testing with G.729 codec, the performance with 96 kbps bitrate (delay, jitter and packet loss ) with VPN sebelum dan sesudah menggunakan VPN. Apakah voice yang dihasilkan oleh VoIP over VPN isn't significantly change (there is increase for 1% until 8%). But when bitrate setting is below 64 kbps then the performace of VoIP is decrease drastically. (delay is increasing 1000%, jitter 100% and packet loss increase to 83% - 87%). Meanwhile for the security of VoIP data, VPN can secure VoIP data from security threat. Before using VPN, VoIP data can be recorded and replay with audio player. The payload data is captureable and visible but after using VPN, VoIP data can't be record and the payload data is invisible.

Keywords : Kata Kunci : VoIP, VPN, delay,jitter,packet loss



## BAB I

### PENDAHULUAN

#### 1.1 Latar Belakang

Teknologi komunikasi berbasis IP berkembang dengan begitu cepatnya seiring dengan kemajuan teknologi. Saat ini jaringan internet tidak hanya terfokus pada layanan paket data dan aplikasi standar seperti WWW (world wide web), http, smtp, ftp, atau layanan data lainnya yang bersifat non real-time dan tidak memiliki *QoS*. Saat ini kebutuhan akan layanan atau aplikasi berbasis multimedia melewati jaringan IP telah menjadi sesuatu yang mungkin. Pada dasarnya jaringan IP dibuat untuk tidak melewati data yang bersifat *real time*. Tetapi dengan ditemukannya teknologi penunjang *QoS* jaringan seperti RTP, *streaming* via internet, RSVP, dan MPLS membuat jaringan IP menjadi *reliable* untuk mengirim data yang bersifat *real time* seperti voice, video.

Kemajuan – kemajuan inilah yang membuat berbagai layanan multimedia berbasis IP muncul di masyarakat. VoIP adalah salah satunya. Teknologi ini melewati suara (*speech*) ke dalam jaringan. Dengan teknologi VoIP biaya untuk melakukan telekomunikasi antara satu user ke user lainnya menjadi lebih efisien. Hal ini disebabkan karena VoIP tidak tergantung pada jarak. Sehingga membuat layanan bertelekomunikasi menggunakan PC menjadi lebih murah. Skype, Yahoo Messenger with Voice dan masih banyak lagi provider layanan VoIP menawarkan jasa pelayanan VoIP ini.

Berkembangnya layanan *voice* ini bukan berarti bahwa tidak akan ada masalah yang muncul di masa yang akan datang. Salah satu kelemahan jaringan internet adalah bahwa data yang terkirim tidak terjamin kerahasiaannya sehingga siapapun dapat menangkap dan memanipulasi data tersebut. Jika data yang ditangkap ternyata rahasia maka akan menjadi kerugian bagi kita jika data tersebut diketahui orang lain atau bahkan digunakan untuk hal yang dapat merugikan. Dalam tugas akhir ini

---

ANALISIS PERFORMANSI DAN KEAMANAN VoIP OVER VPN

dianalisis mengenai keamanan aplikasi VoIP di jaringan. Seberapa amankah telekomunikasi menggunakan VoIP? Apakah perlu untuk mengamankan jaringan VoIP? Dan bagaimana perubahan performansi dari jaringan voip jika data tersebut kita amankan dengan suatu metoda keamanan? Apakah perubahan tersebut masih sesuai dengan standar VoIP yang telah ditetapkan oleh ITU-T? Dimana pada tugas akhir kali ini metoda yang akan digunakan adalah VPN (Virtual Private Network).

### 1.2 Maksud dan Tujuan

Penyusunan Tugas Akhir ini dimaksudkan untuk memenuhi salah satu syarat kelulusan pendidikan Strata 1 di Sekolah Tinggi Teknologi Telkom Jurusan Teknik Elektro. Sedangkan tujuan dari penyusunan tugas akhir ini adalah:

1. Mengetahui celah keamanan pada voip dan performansi VoIP dalam jaringan
2. Mengetahui kualitas suara dan keamanan yang dihasilkan dari konfigurasi VoiP over VPN dengan melakukan perekaman dan diputar ulang.
3. Mengetahui bagaimanakah perubahan performansi dari VoIP sebelum dan sesudah diamankan dengan VPN dengan menganalisa *delay*, *packet loss*, dan *jitter*.
4. Mengetahui *Bandwidth* optimum yang sesuai untuk aplikasi VoIP dan VoIP over VPN
5. Mengetahui Codec Optimum yang dapat digunakan untuk Jaringan VoIP over VPN

### 1.3. Perumusan Masalah

Rumusan masalah pada pembuatan tugas akhir ini adalah sebagai berikut

1. Amankah suatu pembicaraan melalui VoIP yang melalui jaringan IP? Mengingat sifat dari data *packet switch* yang dapat di *taping*, dan dilihat isi datanya.
2. Berapakah *Bandwidth* optimum yang baik digunakan untuk melewati jaringan VoIP?

---

ANALISIS PERFORMANSI DAN KEAMANAN VoIP OVER VPN

3. Bagaimanakah performansi yang dihasilkan ketika kita menambahkan suatu metoda keamanan pada VoIP? Seberapa besar pengaruhnya terhadap keamanan VoIP
4. Apakah sistem VoIP over VPN masih dapat memenuhi syarat untuk standar ITU-T untuk komunikasi suara melalui jaringan IP?

#### 1.4 Batasan Masalah

1. Paket yang dianalisa adalah paket RTP, paket lain yang tertangkap bersama paket RTP akan dibuang dan tidak masuk perhitungan analisa.
2. Codec yang digunakan untuk analisis VoIP ada 3 buah yakni GSM, G.711, dan G.729. sedangkan untuk analisis VoIP over VPN akan digunakan codec yang memiliki performansi terbaik diantara ketiganya.
3. Analisis performansi tidak menentukan MOS. Untuk MOS digunakan referensi dari ITU – T.
4. Jaringan yang akan diamankan adalah jaringan diantara 2 VPN server, sedangkan jaringan di belakang server, diasumsikan aman
5. Range Bandwidth yang digunakan dari 32 kbps – 256 kbps, terbagi menjadi 5 bagian. 32 kbps, 64 kbps, 96 kbps, 128 kbps dan 256 kbps.
6. Hasil – hasil yang didapat pada percobaan tugas akhir adalah dengan mengasumsikan jaringan berada pada kondisi ideal.

#### 1.5 Metoda Penyelesaian Masalah

berikut ini adalah tahap-tahap penyelesaian masalah yang akan dilakukan.

1. Mengumpulkan dan mempelajari literatur hasil penelitian sebelumnya
2. Merancang sistem jaringan VoIP melalui VPN *tunelling*
3. Mengimplementasikan jaringan
4. Analisa hasil percobaan dan evaluasi

## **1.6 Sistematika Penulisan**

Berikut ini sistematika penulisan Tugas Akhir yang akan disusun.

### **BAB I PENDAHULUAN**

Memuat latar belakang, maksud dan tujuan, baasan masalah, metode penyelesaian masalah, serta sistematika penulisan.

### **BAB II LANDASAN TEORI**

Memuat berbagai materi yang diperlukan untuk mendasari pemahaman pada bagian-bagian selanjutnya dan yang akan digunakan untuk mencapai tujuan Tugas Akhir ini.

### **BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM**

Memuat perancangan keseluruhan sistem VoIP via VPN *tunelling*

### **BAB IV PENGUJIAN DAN ANALISA SISTEM**

Memuat laporan realisasi dan penerapan rancangan yang sebelumnya telah dilakukan sekaligus mengevaluasi hasil yang diperoleh.

### **BAB V PENUTUP**

Memuat kesimpulan dan kemungkinan pengembangan untuk penelitian selanjutnya.

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

- Aplikasi komunikasi menggunakan VoIP relatif tidak aman, karena pembicaraan yang terjadi dapat direkam dan dimainkan ulang
- Performansi VoIP paling baik jika menggunakan codec G729. codec ini memiliki nilai delay, jitter dan packet loss paling rendah dan kualitas suara yang cukup bagus.
- Penggunaan VPN mengurangi performansi VoIP. Delay, packet loss dan jitter meningkat ketika menggunakan VPN. *Bitrate* minimal agar performansi VoIP over VPN mendekati performansi VoIP tanpa VPN adalah 96 kbps dengan codec G729.
- Penggunaan kunci Enkripsi yang berbeda (tetapi panjang kunci sama) tidak terlalu mempengaruhi performansi dari jaringan VoIP over VPN. Tetapi performansi jaringan VoIP over VPN terbaik diperoleh jika kita menggunakan kunci enkripsi Blowfish.
- Untuk performansi dan keamanan optimal dalam komunikasi VoIP dapat digunakan VPN dengan *bitrate* minimal 96 kbps dan codec G729

#### 5.2. Saran

1. Pembatasan Bit rate dibuat dengan rentang pengukuran yang lebih kecil lagi sehingga hasil pengukuran bisa lebih presisi lagi dalam mengetahui penurunan performansi dan peningkatan performansi VoIP dan VoIP over VPN.

---

*ANALISIS PERFORMANSI DAN KEAMANAN VoIP OVER VPN*

2. Sebaiknya dicoba menggunakan metoda pengamanan komunikasi VoIP yang memiliki performansi yang lebih baik dari VPN, sehingga bandwidth requirement untuk layanan tersebut memerlukan bitrate yang lebih kecil dari VoIP over VPN.
3. penambahan MOS (Mean Opinion Score) pada analisis VoIP over VPN untuk mengetahui apakah ada penurunan kualitas suara.sebelum dan sesudah menggunakan VPN. MOS bisa melalui perhitungan atau dengan mendengarkan suara dari sistem VoIP..



Telkom  
University

## DAFTAR PUSTAKA

- [1] Gupta Meeta, "Building a Virtual Private Network", Premier Press 2645 Erie Avenue, Suite 41 Cincinnati , Ohio 45208 , 2003
- [2]Cisco System. "*Understanding Delay in Packet Voice Networks*". USA : Cisco Press. 2004.
- [3] "Building and Integrating Virtual Private Network With Openswan", Wouter Paul, Bantoft Ken, Packet Publishing Ltd, Birmingham,2006 page 67
- [4] <http://www.xten.com/index.php?menu=Products&smenu=eyeBeam>
- [5] "Building Telephony System with Asterisk", Gomillion David, Dempster Barrie, Packet Publishing Ltd, Birmingham, 2005, page 22
- [6] Kashnabhis Bhumi "Implementing Voice over IP", Willey-Interscience Hoboken New Jersey, 2003
- [7] Kent S, Atkinson R, "Security Architecture for the Internet Protocol", RFC 2401, Internet Engineering Task Force (IETF)
- [8] Handley, M., Schulzrinne, H., Schooler, E. and J. Rosenberg. "*SIP : Session Initiation Protocol*", RFC 2543. Maret 1999.
- [9] Prasetyo Budi,"Analisis Implementasi Voice over IP (VoIP) pada Jaringan Wireless LAN Berbasis Session Initiation Protocol (SIP)", Tugas Akhir Teknik Elektro STT Telkom, Bandung, 2006
- [10] Cain and Abel software password recovery, [www.oxid.it/cain.html](http://www.oxid.it/cain.html)
- [11] Ethereal a network protocol Analyzer, [www.ethereal.com](http://www.ethereal.com)
- [12] Sukaridhoto Sritrusta, Dutono Titon Nonot Harsono, Iwan Sarif, "Teknik Keamanan pada VoIP dengan Virtual Private Networking dan Kriptografi Serta Korelasi Terhadap Bandwidth dan Intelligibility Suara", (EEPIS), Institut Teknologi Sepuluh Nopember (ITS), Surabaya
- [13] Addison Wesley,"RTP: Audio and Video for Internet", Pearson Education, Inc 75 Arlington Street, Suite 300 Boston, MA 02116, 2003
- [14] Kent S, Atkinson R, "IP Encapsulation Service Payload ", RFC 2406, Internet

---

*ANALISIS PERFORMANSI DAN KEAMANAN VoIP OVER VPN*

Engineering Task Force (IETF)

- [15] H. Schulzrinne, S. Casner, R. Frederick, “RTP : A Transport Protocol For Real Time Applications”, (RFC) 3550, Internet Engineering Task Force (IETF),2003
- [16] 3DES encryption method, [www.wikipedia.org](http://www.wikipedia.org)
- [17] AES encryption method, [www.wikepedia.org](http://www.wikepedia.org)
- [18] Blowfish encryption method, [www.wikipedia.org](http://www.wikipedia.org)



Telkom  
University