BAB I
PENDAHULUAN

1.1 Latar Belakang

Industri telekomunikasi sedang berada dalam perubahan fundamental yang akan merubah secara drastis dunia berkomunikasi. Inti dari perubahan ini adalah penyatuan dari gambar, suara, data, dan jasa-jasa wireless dalam satu network. Sebagai hasilnya para penyedia servis VoIP menghadapi tantangan baru dan karena semakin meningkatnya persaingan industri, disamping terbukanya kesempatan yang besar dalam peningkatan dan keuntungan di dunia informasi. Teknologi telekomunikasi selalu mengalami perkembangan, bukan saja dari segi kemampuannya tetapi juga dari berbagai jenis layanan yang bisa diberikan ke pelanggan seiring dengan semakin majunya masyarakat yang selalu mendambakan kemudahan dan kualitas yang baik dalam berkomunikasi. Layanan komunikasi multimedia-multipoint (*conferencing*) audio dan video yang real-time sudah menjadi trend di masyarakat. Teknologi conference berbasis IP khususnya protokol H.323 telah lama dikembangkan dan saat ini bisa dikatakan telah siap pakai.

Standar H.323 memberikan fondasi bagi komunikasi audio, video, dan data melalui jaringan IP, termasuk Internet. Setiap produk multimedia yang dibuat oleh berbagai vendor yang mengikuti standar H.323 bisa saling berinteroprasi, sehingga user bisa berkomunikasi tanpa menghawatirkan masalah kompatibiliti. H.323 bisa digunakan untuk terminal dengan kemampuan audio saja dan juga bisa digunakan pada terminal yang memiliki kemampuan video. H.323 bisa digunakan dalam point-to-point call dan juga bisa digunakan dalam aplikasi multipoint conference. H.323 juga mengatur masalah call control, multimedia management, bandwidth management dan juga interface antar LAN dan interface ke jaringan lainnya (jaringan PSTN, ISDN, dll).

Pada tugas akhir ini akan dibahas mengenai sistem keamanan (*sekuritas*) dari protokol H.323 dengan metode *authentication* dan *key switch*, dikarenakan seiring dengan semakin pesatnya teknologi telekomunikasi dibutuhkan pula jaminan akan keamanan pelanggan agar dapat saling bertukar informasi dengan bebas tanpa adanya kebocoran informasi.

1.2 Tujuan

Tujuan dari penelitian pada tugas akhir ini adalah :

1. Merancang skema video conference menggunakan protokol H.323 ke protokol SIP dan membangun sistem keamanan jaringan menggunakan metode *authentication* dan *key switch – diffie hellman.*
2. Menganalisa sistem keamanan jaringan video conference yang telah dirancang untuk mendapatkan perbandingan, kelebihan serta kekurangan dari metode authentication dan key switch - diffie hellman yang digunakan.
3. Mengetahui bagaimana metode authentication dan key switch – diffie hellman bereaksi terhadap gangguan-gangguan dalam hubungan video conference.
4. Mendapatkan skema awal sistem video conference yang aman dengan perpaduan antara metode *authentication* dengan metode *key switch*.

1.3 Rumusan Masalah

Permasalahan yang dibahas pada tugas akhir ini adalah :

1. Bagaimana Merancang skema video conference menggunakan protokol H.323 ke protokol lainnya dalam membangun sistem keamanan jaringan video conference menggunakan metode *authentication* dan *key switch*
2. Bagaimana analisa sistem keamanan jaringan video conference yang telah dirancang untuk mendapatkan perbandingan, kelebihan serta kekurangan dari tiap metode yang digunakan dengan data-data hasil pengukuran yang didapatkan
3. Bagaimana gangguan-gangguan pada komunikasi video conference dapat diamankan oleh metode *authentication* dan *key switch*
4. Bagaimanakah idealnya sebuah sistem video conference yang aman untuk saling bertukar informasi di masa mendatang

1.4 Batasan Masalah

Batasan masalah dalam penulisan tugas akhir ini adalah :

1. Protokol yang digunakan adalah H.323.
2. Metode pengamanan yang digunakan adalah metode *authentication* dan *key switch.*

3. Software yang digunakan adalah *Skype, SkyStone* dan *ViCon*.
4. Skenario *video conference* yang digunakan adalah *multipoint call.*
5. Pada metode Key Switch, metode yang digunakan adalah algoritma Diffie_Hellman.
6. Software yang digunakan untuk meng-analisa dan mengambil data pada jaringan secara *Real Time* adalah *OPNET* dan *Wireshark.*
7. Parameter ukur QoS pada jaringan *video conference* adalah *troughput, packet loss, jitter* dan *delay.*

1.5 Metodologi Penulisan

Metode yang akan digunakan untuk menyelesaikan tugas akhir ini adalah:

1. Studi Literatur

   Pada tahap ini, dilakukan pendalaman materi-materi yang terkait melalui literatur dan referensi yang tersedia di berbagai sumber.
2. Proses Perancangan

   Pada tahap ini, dilakukan proses perancangan sistem jaringan yang akan digunakan untuk melakukan video conference .menggunakan protokol H.323.
3. Simulasi dan Optimasi

   Pada tahap ini, dilakukan simulasi desain sistem menggunakan software *OPNET* yang telah dirancang dengan menggunakan 4 buah laptop beserta software *Skype, SkyStone,* dan *ViCon*.
4. Proses Realisasi

   Pada tahap ini, dilakukan proses realisasi pengamanan komunikasi *video conference* menggunakan metode *authentication* dan *key switch.*
5. Proses Pengambilan Data

   Pada tahap ini, dilakukan pengambilan data / capture data pada kedua metode menggunakan *wireshark* dan *OPNET* untuk membaca dan menangkap paket-paket data yang ada pada jaringan.
6. Analisa

Pada tahap ini, dilakukan analisa terhadap sistem keamanan jaringan *video conference* yang menggunakan metode *authentication* dengan yang menggunakan metode *key switch*.

7. Pembuatan Laporan

   Tahap akhir dari penelitian ini adalah pembuatan laporan Tugas Akhir dan Sidang Tugas Akhir.

1.6 Sistematika Penulisan

Secara umum sistematika penulisan tugas akhir ini adalah sebagai berikut :

- BAB I : PENDAHULUAN

  Bab ini berisi uraian mengenai latar belakang permasalahan Tugas Akhir, tujuan, rumusan masalah, batasan masalah, metodologi penelitian, serta sistematika penulisan.

- BAB II : LANDASAN TEORI

  Bab ini mambahas uraian dasar teori *video conference* dan protokol H.323 serta menjelaskan metode pengamanan yang akan digunakan, juga beberapa kendala/gangguan yang bisa dihadapi pada saat proses *video conference* berlangsung.

- BAB III : PEMODELAN DAN SIMULASI

  Pada bab ini disajikan bentuk pemodelan melalui simulasi dengan menggunakan *Skype* dan untuk melihat proses kerja dari sistem keamanan *video conference* yang dirancang. Lalu disajikan hasil capture/pengambilan data pada kedua metode tersebut yang telah diujikan dengan 3 gangguan yang sama menggunakan *Wireshark* dan *OPNET*.

- BAB IV : ANALISIS DAN PERBANDINGAN

  Berisikan data hasil analisis dan perbandingan data hasil pengamanan dari hasil simulasi. Analisis dilakukan secara kualitatif dan kuantitatif terhadap parameter-parameter uji protokol yang menjalankan komunikasi *video conference*.

- BAB V : KESIMPULAN DAN SARAN

Pada bab terakhir ini berisikan kesimpulan dan saran dari perancangan dan analisis pengamanan jaringan *video conference* yang telah dibuat sehingga dapat dilakukan pengembangan terhadap topik yang bersangkutan.