COMPUTER ENGINEERING

Laboratorium
Multimedia dan Internet of Things
Departemen Teknik Komputer
Institut Teknologi Sepuluh Nopember

Praktikum
Jaringan Komputer

Tunneling

Ahmad Arfian Syamsa - 5024231072

04 Juni 2025

1 Pendahuluan

1.1 Latar Belakang

Sekarang ini, cara orang bercerita udah nggak kayak dulu yang cuma lewat satu arah, misalnya nulis di buku atau ngomong di depan banyak orang. Di era digital, cerita bisa nyebar lewat berbagai platform kayak Instagram, Twitter, YouTube, bahkan TikTok. Nah, konsep kayak gini disebut nutelling atau network storytelling, yaitu menyampaikan cerita yang saling terhubung lewat banyak media dan bisa dikembangkan bareng-bareng. Nutelling ini muncul karena gaya hidup kita yang makin sering online dan aktif di berbagai platform digital. Orang nggak cuma jadi pendengar, tapi juga bisa ikut nyumbang atau nyebarin cerita dari sudut pandang mereka sendiri. Cerita jadi lebih kaya dan berkembang karena banyak orang terlibat.

Fenomena ini penting banget dipahami, apalagi buat kita sebagai mahasiswa. Nggak cuma buat tugas kuliah atau bikin konten, tapi juga bisa dipakai buat hal yang lebih besar—kayak edukasi, kampanye sosial, atau bahkan promosi produk. Karena itu, kita perlu ngerti gimana cara kerja nutelling ini, gimana cara bikin narasi yang kuat, dan gimana nyebarin pesan yang berdampak lewat banyak channel digital.

2 Dasar Teori

2.1 Tunneling

Apa sih itu tunneling? Tunneling adalah bisa dibayangkan seperti "menyembunyikan" data agar bisa lewat jalur internet yang biasanya tidak bisa dilalui langsung. Jadi bisa diilustrasikan seperti lagi ngirim paket lewat jalan tol, tapi jalan itu cuma bisa dilalui mobil tertentu. Nah, agat paket bisa nyampe, kita perlu bungkus dulu paketnya menggunakan label “mobil legal” biar bisa lewat jalan tol itu. Di ujung jalan, bungkusnya dibuka lagi, dan isi paketnya dilanjutkan ke tujuan aslinya. Kurang lebih seperti itulah prinsip dasar tunneling.

2.1.1 Cara kerja Tuneling

1. Komputer A bikin paket data ke komputer B.
2. Paket ini dimasukin ke dalam bingkai Ethernet dan dikirim ke router M1.
3. Di router M1, data dibungkus lagi pake format WAN, dan dikirim ke router M2.
4. Di router M2, bungkus WAN dibuka, dan data dikirim ke komputer B dalam bentuk asli.

2.1.2 Jenis-Jenis Protokol Tunneling

1. **GRE (Generic Routing Encapsulation)**
    - Bungkus IP packet dengan header tambahan dan ngirim lewat “terowongan”. Cuma router tertentu yang bisa ngerti isi bungkusan ini.
2. **IPSec (Internet Protocol Security)**

- Tunneling yang aman banget. Pake enkripsi biar data nggak bisa dibaca orang iseng, cocok buat koneksi sensitif.

3. **IP-in-IP**
   - IP dimasukin ke dalam IP. Simpel tapi efektif buat ngelewatin jaringan beda.
4. **SSH (Secure Shell)**
   - Buat akses jarak jauh secara aman, kayak kamu login ke server tapi datanya dienkripsi.
5. **PPTP (Point-to-Point Tunneling Protocol)**
   - Salah satu protokol VPN paling awal. Udah lama dipakai di Windows, juga bisa jalan di Mac dan Linux.
6. **SSTP (Secure Socket Tunneling Protocol)**
   - Punya Microsoft. Pakai SSL untuk jamin keamanan koneksi, tapi cuma buat Windows.
7. **L2TP (Layer 2 Tunneling Protocol)**
   - Gabungan kekuatan dari PPTP-nya Microsoft dan L2F-nya Cisco. Cocok buat VPN di banyak sistem.
8. **VXLAN (Virtual Extensible LAN)**
   - Ini buat virtualisasi jaringan, cocok buat lingkungan cloud atau data center besar. Bisa bikin jaringan virtual seolah-olah menyatu meskipun fisiknya berjauhan.

2.2 IPsec (IP Security)

IPsec (Internet Protocol Security) adalah sebuah protokol keamanan jaringan yang digunakan untuk mengamankan komunikasi antar perangkat di jaringan IP, terutama saat data dikirim melalui internet atau jaringan publik.

2.2.1 Fitur IPSec

1. **Autentikasi** : Pastikan data emang dari pengirim aslinya.
2. **Enkripsi**: Data diacak supaya gak bisa dibaca sembarangan.
3. **Integritas**: Data dicek biar gak ada yang berubah/korup selama perjalanan.
4. **Manajemen Kunci**: Nentuin kunci enkripsi rahasia buat komunikasi.
5. **Tunneling**: Bisa bikin “terowongan aman” buat data lewat internet.
6. **Fleksibel**: Bisa dipakai dari skala kecil (antar komputer) sampai besar (antar cabang perusahaan). Bisa jalan di berbagai sistem dan perangkat karena pakai standar terbuka.

2.2.2 Cara Kerja IPSec

1. Dua perangkat kirim sinyal duluan buat bikin koneksi aman.
2. Mereka tukar-tukaran kunci rahasia lewat proses yang disebut IKE (Internet Key Exchange).
3. Setelah sepakat, mereka bikin “terowongan” aman.
4. Data dikirim lewat terowongan itu: terenkripsi dan dicek keasliannya.
5. Setelah selesai, koneksi ditutup.

2.2.3 Mode dalam IPSec

Untuk mode terdapat 2 mode, yaitu **Tunnel Mode** : Bungkus seluruh paket (termasuk alamat IP-nya). Cocok buat koneksi antar kantor atau cabang. Kemudian, **Transport Mode** : Bungkus seluruh paket (termasuk alamat IP-nya). Cocok buat koneksi antar kantor atau cabang.

2.2.4 Protokol dalam IPSec

1. **ESP (Encapsulation Security Payload)**: Enkripsi isi data + autentikasi.
2. **AH (Authentication Header)**: Cuma autentikasi dan integritas, tanpa enkripsi.
3. **IKE (Internet Key Exchange)**: Buat saling tukar kunci dan negosiasi pengamanan.

2.3 Simple Queue V.S. Queue Tree

2.3.1 Definisi Simple Queue dan Queue Tree

1. **Simple Queue**: Merupakan cara paling gampang buat ngatur bandwidth per user atau per IP. Cocok buat pemula atau buat jaringan kecil.

   Ciri-cirinya:

   - Mudah disetting, cukup masukin IP atau interface.
   - Bisa langsung atur kecepatan upload/download (limit-at dan max-limit).
   - Kerjanya lebih "langsung", satu queue = satu user/IP/interface.
   - Bisa diatur urutan prioritas juga, tapi terbatas.

2. **Queue Tree**: Merupakan cara buat kamu yang butuh pengaturan bandwidth lebih kompleks dan fleksibel. Cocok buat jaringan besar, ISP, atau kamu yang mau pisahin bandwidth berdasarkan port, protokol, VLAN, dll.

   Ciri-cirinya:

   - Harus pakai mangle (mark connection atau mark packet dulu).
   - Bisa bikin struktur bertingkat (parent-child).
   - Lebih fleksibel, bisa gabungin trafik dari banyak IP, protokol, atau interface ke satu queue.
   - Cocok buat ngatur total bandwidth dan bagi rata ke banyak user.

2.4 Prioritas Trafik bandwith

Fungsi manajemen bandwidth dan prioritas trafik berperan. Ibaratnya kayak jalan tol digital, sistem ini bantu ngatur siapa aja yang lebih dulu boleh lewat. Jadi, misalnya ada data penting kayak Zoom meeting dosen atau upload tugas, itu bakal dikasih jalur prioritas. Sedangkan aktivitas yang kurang penting kayak download film atau update aplikasi bisa "disuruh" nunggu dulu biar nggak ganggu performa jaringan.

2.4.1 Mengapa Trafik Dibutuhkan?

Trafik dibutuhkan karena,

1. **Biar komunikasi penting tetap lancar**, walaupun jaringan lagi rame Misalnya: meeting online, VoIP, atau live video call nggak boleh ngelag. Nah, ini dikasih jalur prioritas tinggi biar nggak terganggu sama yang lain kayak update software atau browsing santai.
2. **Siap siaga kalau jaringan bermasalah**. Kadang ada link putus atau server error. Di kondisi kayak gini, sistem harus bisa milih trafik mana yang penting dan dikasih jalan dulu. Misalnya, backup data atau VPN kantor tetap jalan, sedangkan YouTube bisa ditunda dulu.
3. **Ngirit bandwidth kalau jaringan terbatas**. Kalau nggak bisa nambah kecepatan internet atau bikin jalur baru, kita bisa atur prioritas layanan penting (kayak akses ke sistem kantor, database, atau VPN) dibanding aktivitas lain kayak buka TikTok, streaming, atau download film.

2.4.2 Contoh Penggunaan Prioritas Bandwidth

Trafik	Prioritas	Keterangan
VPN perusahaan	Tinggi	Akses ke sistem kerja, harus lancar
Video conference	Tinggi	Agar rapat online tidak buffering
Browsing	Sedang	Masih penting tapi bisa ditunda sedikit
Download game/software	Rendah	Boleh jalan tapi jangan ganggu yang lain
Streaming YouTube/Netflix	Rendah	Santai aja, kalau ada bandwidth lebih baru dikasih

2.4.3 Cara Mengatur Trafic Bandwidth

1. Di router atau mikrotik, kamu bisa pakai Simple Queue atau Queue Tree buat atur bandwidth per IP/user.
2. Bisa juga pakai marking untuk bedain trafik berdasarkan port, protokol, atau tujuan IP.
3. Beberapa perangkat bahkan punya fitur QoS (Quality of Service) otomatis buat langsung ngatur prioritas sesuai tipe trafik.

3 Tugas Pendahuluan

1. **Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu erusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:**

- Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)
- Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)
- Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

(a) **Fase Negosiasi IPSec (IKE Phase 1 Phase 2)**
IKE Fase 1 :

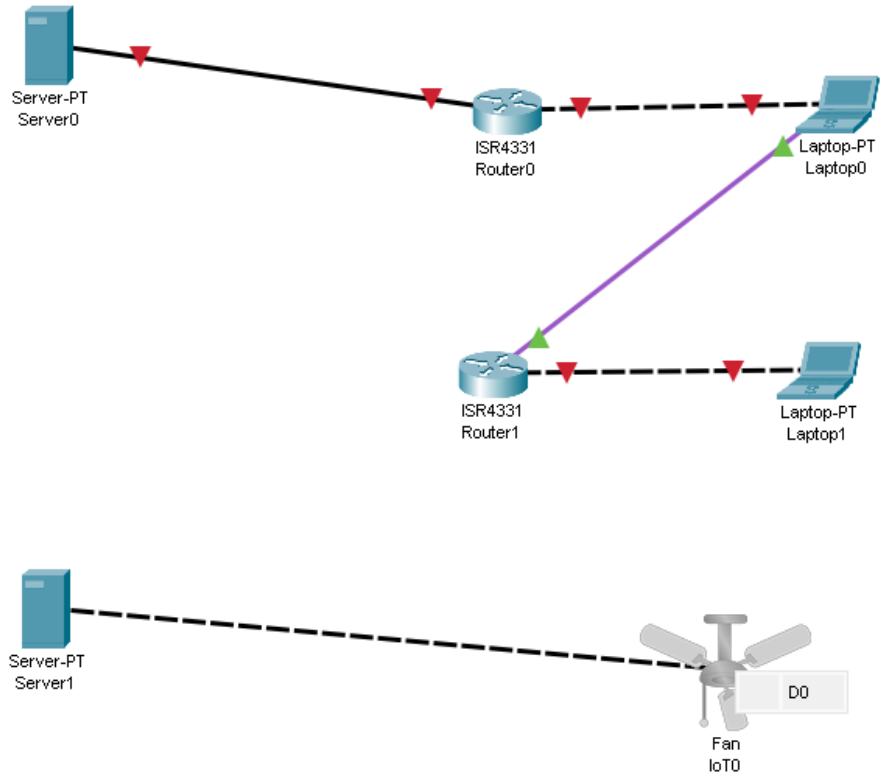
- Tujuan: Membangun secure channel (ISAKMP SA) antara dua router.
- Hasil: Terbentuk tunnel aman untuk negosiasi di fase berikutnya.
- Prosesnya :
  - Autentikasi antar perangkat (Pre-shared key / sertifikat digital)
  - Pertukaran parameter enkripsi dan hash
  - Tukar DH (Diffie-Hellman) key
  - Pembuatan enkripsi tunnel untuk IKE Phase 2Autentikasi antar perangkat (Pre-shared key / sertifikat digital)
  - Pertukaran parameter enkripsi dan hash
  - Tukar DH (Diffie-Hellman) ke Pembuatan enkripsi tunnel untuk IKE Phase 2

IKE Fase 2 :

- Tujuan: Negosiasi parameter untuk IPsec SA, yaitu tunnel data sebenarnya.
- Hasil: Data antar kantor bisa lewat tunnel aman.
- Proses :
  - Menentukan protokol (ESP atau AH)
  - Menentukan algoritma enkripsi dan hash
  - Menentukan mode (Tunnel atau Transport)
  - Menentukan lifetime dari IPsec SA

Sebuah sekolah memiliki bandwidth internet 100 Mbps yang dibagi menjadi:

- 40 Mbps untuk e-learning
- 30 Mbps untuk guru dan staf (akses email, cloud storage)
- 20 Mbps untuk siswa (browsing umum)
- 10 Mbps untuk CCTV dan update sistem


Server-PT
Server0
ISR4331
Router0
Laptop-PT
Laptop0
ISR4331
Router1
Laptop-PT
Laptop1
Server-PT
Server1
D0
Fan
IoT0