



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

# **Laporan Sementara Praktikum Jaringan Komputer**

**VPN & QoS**

Atria Caesariano Tinto - 5024231068

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Seiring dengan meningkatnya ketergantungan terhadap jaringan komputer dalam berbagai aspek kehidupan, baik untuk keperluan pribadi, pendidikan, maupun industri, kebutuhan akan koneksi jaringan yang aman, stabil, dan efisien menjadi semakin krusial. Permasalahan umum yang sering muncul dalam lingkungan jaringan adalah transmisi data melalui media jaringan yang berbeda-beda, serta ketidakseimbangan penggunaan bandwidth yang menyebabkan lambatnya akses layanan penting. Oleh karena itu, pemahaman dan penerapan konsep tunneling menjadi vital agar komunikasi data antar perangkat tetap lancar meskipun melewati jaringan heterogen. Selain itu, untuk mengoptimalkan kinerja jaringan, dibutuhkan pengelolaan bandwidth secara cerdas, termasuk penentuan prioritas trafik agar aplikasi yang bersifat kritis seperti video conference atau akses VPN tetap berjalan lancar tanpa terganggu oleh aktivitas lain yang kurang prioritas. Penggunaan protokol keamanan seperti IPSec serta fitur manajemen bandwidth seperti Simple Queue dan Queue Tree pada perangkat jaringan modern menjadi kunci dalam membangun sistem komunikasi data yang handal dan aman di era digital saat ini.

## 1.2 Dasar Teori

Dalam dunia jaringan komputer, pertukaran data tidak selalu terjadi dalam satu jenis jaringan atau media yang sama. Oleh karena itu, diperlukan suatu mekanisme yang memungkinkan data dapat berjalan melalui berbagai jenis jaringan secara aman dan efisien. Salah satu mekanisme tersebut adalah tunneling, yaitu proses mengenkapsulasi paket data agar dapat dikirim melalui jaringan yang berbeda sebelum akhirnya dikembalikan ke bentuk semula di tujuan. Berbagai protokol seperti GRE, IPSec, hingga SSL Tunneling digunakan untuk menjamin keamanan dan kompatibilitas proses ini. Salah satu protokol yang paling aman dan sering digunakan untuk membuat jaringan pribadi virtual (VPN) adalah IPSec, yang menyediakan enkripsi, autentikasi, serta integritas data selama transmisi. Di sisi lain, dalam manajemen jaringan, pengaturan bandwidth dan prioritas trafik menjadi penting untuk memastikan efisiensi penggunaan sumber daya jaringan. Fitur seperti Simple Queue dan Queue Tree di MikroTik menjadi solusi untuk mengatur pembagian dan prioritas bandwidth berdasarkan IP, jenis trafik, maupun protokol tertentu, sehingga memastikan layanan penting mendapatkan prioritas yang layak di tengah lalu lintas jaringan yang padat.

# 2 Tugas Pendahuluan

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

- **Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2):**

- **IKE Phase 1:** Membangun saluran aman (ISAKMP SA) antara dua router. Proses ini melakukan pertukaran informasi awal (IP, metode enkripsi, autentikasi) dan menghasilkan kunci bersama (shared key).
- **IKE Phase 2:** Digunakan untuk membuat tunnel IPSec. Di sini, trafik antar kantor akan dienkripsi menggunakan parameter yang sudah disepakati.

- **Parameter Keamanan yang Disepakati:**

- **Enkripsi:** AES-256 atau 3DES
- **Autentikasi:** Pre-shared key atau digital certificate
- **Hash/Integrity:** SHA-256
- **Diffie-Hellman Group:** Group 14 (2048-bit)
- **Lifetime:** 3600 detik (1 jam)

- **Contoh Konfigurasi Router (Cisco-like):**

```
crypto isakmp policy 10
  encr aes
  hash sha256
  authentication pre-share
  group 14
  lifetime 3600

crypto isakmp key mysecretkey address 192.168.2.1

crypto ipsec transform-set TS esp-aes esp-sha-hmac

crypto map VPN-MAP 10 ipsec-isakmp
  set peer 192.168.2.1
  set transform-set TS
  match address 101

interface GigabitEthernet0/0
  crypto map VPN-MAP

access-list 101 permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255
```

## 2. Skema Queue Tree (Bandwidth Management pada Sekolah):

- **Struktur Queue Tree:**

```
Root Queue (100 Mbps)
|- eLearning Queue (40 Mbps)
|- Staff Queue (30 Mbps)
|  |- Email (10 Mbps)
|  |- Cloud Storage (20 Mbps)
|- Student Queue (20 Mbps)
|- CCTV & Update Queue (10 Mbps)
```

- **Penjelasan Marking dan Prioritas:**

- Trafik ditandai (marking) dengan mangle rule berdasarkan port atau IP.
- Parent Queue adalah Root dengan 100 Mbps total.
- Setiap child queue diberi limit rate, priority (opsional), dan burst.

- **Contoh Mikrotik Simple Queue Tree:**

### Listing 1: Contoh Mikrotik Simple Queue Tree

```
1 /queue tree
2 add name="eLearning" parent=global queue=default limit-at=40M max-limit=40M packet-mark=
  eLearning
3 add name="Email" parent="Staff" queue=default limit-at=10M max-limit=10M packet-mark=email
4 add name="Cloud" parent="Staff" queue=default limit-at=20M max-limit=20M packet-mark=cloud
5 add name="Staff" parent=global queue=default limit-at=30M max-limit=30M
6 add name="Student" parent=global queue=default limit-at=20M max-limit=20M packet-mark=
  student
7 add name="CCTV-Update" parent=global queue=default limit-at=10M max-limit=10M packet-mark=
  cctv
```

## Referensi

- Cisco. (2024). *IPSec VPN Configuration Guide*. <https://www.cisco.com>
- MikroTik. (2024). *Queue Tree Manual*. <https://wiki.mikrotik.com/wiki/Manual:Queue>