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

# Laporan Sementara
# Praktikum Jaringan Komputer

## VPN QoS

Akhmad Rizqullah Ridloi - 5024231037

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Pada praktikum ini dilakukan percobaan VPN dan QOS, di mana VPN dan QOS adalah salah satu perihal yang umum pada konteks jaringan komputer, sehingga praktikum ini diperlukan agar praktikan mampu mengaplikasikan VPN dan QOS saat digunakan

## 1.2 Dasar Teori

Tunneling dalam jaringan komputer adalah teknik untuk mengirimkan data dari satu jaringan ke jaringan lain yang berbeda jenis melalui sebuah "terowongan digital". Konsep ini mirip seperti mengirim paket dari rumah A ke rumah B melewati berbagai jenis jalan—data dari satu perangkat dibungkus (encapsulated) menggunakan protokol tertentu agar bisa melewati jaringan perantara, dan kemudian dibuka kembali di tujuan. Pertama cara kerja tunneling, komputer pengirim membuat data yang ingin dikirimkan ke komputer penerima, lalu paket akan dimasukkan ke dalam bingkai ethernet dan dikirimkan ke router pengirim, lalu pada router pengirim, data dibungkus menggunakan format WAN, dan dikirim ke router penerima, lalu pada router penerima bungkus WAN dibuka dan paket dikirimkan ke komputer penerima.

Berbagai protokol tunneling digunakan tergantung pada kebutuhan. GRE (Generic Routing Encapsulation) digunakan untuk membungkus paket IP tanpa enkripsi. IPSec (Internet Protocol Security) menyediakan keamanan tinggi melalui enkripsi dan autentikasi, sering digunakan dalam koneksi VPN untuk melindungi data dari pihak ketiga. Protokol lain seperti PPTP, L2TP, dan SSTP juga digunakan untuk VPN, masing-masing dengan kelebihan dan keterbatasannya. SSH dapat digunakan untuk tunneling yang aman melalui koneksi remote, sementara VXLAN memungkinkan virtualisasi jaringan dalam skala besar seperti di data center atau lingkungan cloud.

Salah satu protokol yang paling penting dalam tunneling adalah IPSec. IPSec memberikan perlindungan data melalui fitur-fitur seperti autentikasi, enkripsi, integritas data, dan manajemen kunci. IPSec dapat bekerja dalam dua mode: Transport Mode dan Tunnel Mode, dengan perbedaan pada bagian paket IP yang dienkripsi. IPSec memanfaatkan protokol tambahan seperti ESP (Encapsulation Security Payload) dan AH (Authentication Header) untuk menjamin keamanan dan keaslian data.

MikroTik menyediakan dua metode utama yaitu Simple Queue dan Queue Tree. Simple Queue digunakan untuk pengaturan bandwidth per user atau per IP dengan cara yang mudah dan cepat, cocok untuk jaringan kecil. Sebaliknya, Queue Tree memberikan kontrol yang lebih kompleks dan fleksibel untuk jaringan besar dengan struktur bertingkat dan kemampuan pengelompokan trafik berdasarkan port, protokol, atau VLAN, namun memerlukan konfigurasi mangle terlebih dahulu. Kedua metode ini memungkinkan pengaturan prioritas trafik agar layanan penting seperti VPN dan video conference mendapat bandwidth lebih besar saat jaringan padat.

Pengaturan prioritas trafik sangat penting dalam menjaga kualitas layanan jaringan, terutama saat jaringan sedang padat. Dengan menggunakan fitur Quality of Service (QoS) atau sistem antrian seperti Queue Tree, administrator jaringan dapat memastikan bahwa trafik penting mendapat prioritas lebih tinggi dibanding aktivitas yang tidak mendesak seperti streaming atau download file besar. Dengan demikian, kinerja jaringan tetap optimal dan layanan penting tetap berjalan lancar.

## 2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut

1. Untuk membangun koneksi yang aman antara kantor pusat dan kantor cabang sebuah perusahaan, VPN (Virtual Private Network) jenis IPSec site-to-site menjadi solusi yang umum digunakan. Proses ini dilakukan melalui dua fase utama, yaitu IKE (Internet Key Exchange) Phase 1 dan Phase 2. Pada **IKE Phase 1**, kedua perangkat (router kantor pusat dan cabang) bertukar informasi guna membentuk Secure Association (SA) awal menggunakan algoritma kriptografi yang disepakati. Fase ini bertujuan untuk mengaeutentikasi identitas masing-masing pihak dan membuat tunnel aman untuk pertukaran kunci. Parameter penting dalam fase ini mencakup algoritma enkripsi seperti AES-256, metode autentikasi seperti pre-shared key (PSK) atau digital certificate, serta lifetime key, misalnya 86400 detik (1 hari).

   Selanjutnya, **IKE Phase 2** digunakan untuk membuat SA kedua yang akan digunakan untuk enkripsi dan dekripsi data aktual. Dalam fase ini, protokol ESP (Encapsulation Security Payload) biasanya digunakan, dengan parameter keamanan seperti algoritma enkripsi (misalnya AES-128), algoritma hashing (SHA-256), dan parameter lifetime yang lebih pendek, seperti 3600 detik (1 jam), untuk meningkatkan keamanan. Kedua fase ini saling bergantung dan harus disesuaikan pada kedua perangkat yang terlibat.

   Untuk konfigurasi sederhana pada router MikroTik untuk IPSec site-to-site, langkah-langkah umum adalah sebagai berikut:

   - Konfigurasi Phase 1 (Proposal, Policy, dan Peer):

     ```
     /ip ipsec proposal
     add name=ph1-proposal auth-algorithms=sha256 enc-algorithms=aes-256-cbc lifetime=1d

     /ip ipsec peer
     add address=REMOTE_IP exchange-mode=main secret=SharedKey name=branch-peer
     ```

   - Konfigurasi Phase 2 (Policy):

     ```
     /ip ipsec policy
     add src-address=192.168.1.0/24 dst-address=192.168.2.0/24 \
      sa-dst-address=REMOTE_IP sa-src-address=LOCAL_IP tunnel=yes \
      proposal=ph1-proposal
     ```

   **Referensi**:

   - MikroTik Documentation: `https://help.mikrotik.com/docs/display/ROS/IPsec`

2. Untuk manajemen bandwidth di sebuah sekolah dengan total kapasitas 100 Mbps, digunakan metode Queue Tree pada MikroTik RouterOS. Skema ini memungkinkan pembagian lalu lintas berdasarkan jenis layanan, dengan pendekatan hierarchical queue. Pertama-tama, semua trafik diberi parent queue dengan max-limit 100 Mbps. Kemudian dilakukan packet marking

pada masing-masing jenis trafik menggunakan fitur `/ip firewall mangle`. Trafik ke e-learning dapat ditandai dengan `mark-packet=e-learning`, guru dan staf dengan `mark-packet=guru-staf`, dan seterusnya. Berikut adalah Parent Queue dan Chold Queues:

- Parent Queue:

```
/queue tree
add name=Total parent=global max-limit=100M
```

- Child Queues:

```
add name=e-learning parent=Total packet-mark=e-learning max-limit=40M priority=1
add name=guru-staf parent=Total packet-mark=guru-staf max-limit=30M priority=2
add name=siswa parent=Total packet-mark=siswa max-limit=20M priority=3
add name=cctv-sistem parent=Total packet-mark=cctv-sistem max-limit=10M priority=4
```

Konfigurasi mangle seperti berikut:

```
/ip firewall mangle
add chain=forward dst-address=192.168.10.0/24 action=mark-packet \
    new-packet-mark=e-learning passthrough=yes

add chain=forward dst-address=192.168.20.0/24 action=mark-packet \
    new-packet-mark=guru-staf passthrough=yes

add chain=forward dst-address=192.168.30.0/24 action=mark-packet \
    new-packet-mark=siswa passthrough=yes

add chain=forward dst-address=192.168.40.0/24 action=mark-packet \
    new-packet-mark=cctv-sistem passthrough=yes
```

**Referensi**:


- MikroTik Queue Tree Documentation: `https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues`