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

# Laporan Sementara
# Praktikum Jaringan Komputer

## VPN & QoS

Nadhif Basyara - 502423147

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Seiring meningkatnya kompleksitas dan kebutuhan komunikasi data dalam jaringan komputer, aspek keamanan dan manajemen kualitas layanan menjadi hal yang sangat krusial. Virtual Private Network (VPN) merupakan salah satu solusi yang digunakan untuk menciptakan koneksi jaringan yang aman melalui media publik seperti internet, dengan membentuk jalur komunikasi terenkripsi yang hanya dapat diakses oleh pihak yang memiliki otorisasi. Hal ini sangat penting dalam menjaga integritas dan kerahasiaan data, terutama dalam skenario kerja jarak jauh atau komunikasi antar-cabang organisasi.

Di sisi lain, Quality of Service (QoS) memainkan peran penting dalam mengatur lalu lintas data di dalam jaringan agar berbagai jenis layanan seperti video call, streaming, dan transfer file besar dapat berjalan dengan optimal tanpa saling mengganggu. Dengan menerapkan QoS, administrator jaringan dapat menetapkan prioritas dan pengaturan bandwidth sesuai kebutuhan masing-masing jenis trafik.

## 1.2 Dasar Teori

VPN (Virtual Private Network) adalah suatu jaringan privat (biasanya untuk instansi atau kelompok tertentu) di dalam jaringan internet (publik), dimana jaringan privat ini seolah-olah sedang mengakses jaringan lokalnya tapi menggunakan jaringan publik. VPN merupakan salah satu teknik pengamanan jaringan dengan cara membuat suatu tunnel, misalkan pada jaringan publik atau internet sehingga bersifat private dan aman. VPN dikatakan bersifat private karena ketika dibutuhkan sebuah koneksi VPN membutuhkan autentikasi untuk memastikan bahwa kedua ujung dalam koneksi adalah user yang sesuai dengan yang diberikan kewenangan untuk mengakses suatu user.

Quality of Service (QoS) atau Kualitas layanan adalah metode pengukuran yang digunakan untuk menentukan kemampuan sebuah jaringan seperti; aplikasi jaringan, host atau router dengan tujuan memberikan network service yang lebih baik dan terencana sehingga dapat memenuhi kebutuhan suatu layanan. Quality of Service (QoS) merupakan sebuah arsitektur end-to-end dan bukan merupakan sebuah fitur yang dimiliki oleh jaringan. QoS suatu jaringan merujuk pada tingkat kecepatan dan kehandalan penyampaian berbagai jenis data di dalam suatu komunikasi. Melalui QoS seorang network administrator dapat memberikan prioritas trafik tertentu. QoS menawarkan kemampuan untuk mendefinisikan atribut-atribut layanan yang disediakan, baik secara kualitatif maupun kuantitatif. Tujuan QoS menyediakan kualitas layanan yang berbeda-beda berdasarkan kebutuhan layanan di dalam jaringan.

# 2 Tugas Pendahuluan

1. **Studi kasus untuk konfigurasi VPN IPSec**

   - Fase negosiasi IPSec
     IKE Phase 1 dan IKE Phase 2. Pada IKE Phase 1, tujuan utamanya adalah membangun jalur komunikasi yang aman antara dua peer melalui pertukaran kunci kriptografi dan pembentukan Security Association (SA). Fase ini bisa dijalankan dalam mode Main atau Aggressive. Selanjutnya, pada IKE Phase 2, dilakukan negosiasi untuk membentuk IPSec

SA yang digunakan untuk mengenkripsi dan mengautentikasi data yang dikirimkan. Protokol yang digunakan biasanya ESP (Encapsulating Security Payload) yang mendukung enkripsi dan autentikasi data.

- Parameter keamanan yang harus disepakati
  AES-256 atau 3DES, SHA-256 atau MD5, pre-shared key atau digital signature (RSA).
- Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site
  Pada perangkat MikroTik, pengguna perlu mengatur peer VPN dengan menentukan alamat IP tujuan, mode pertukaran kunci (misalnya IKEv2), serta identitas autentikasi dan proposal keamanan. Selanjutnya, dibuat pula kebijakan IPSec (IPSec Policy) untuk menentukan jaringan sumber dan tujuan, serta tunnel yang digunakan.

Referensi: https://wiki.mikrotik.com/wiki/Manual:IP/IPsec

2. **Skema Queue Tree Berdasarkan Pembagian Bandwidth Sekolah**

   Membuat parent queue yang mengatur total bandwidth (100 Mbps) pada interface WAN (misalnya ether1). Kemudian, dibuat child queue untuk setiap kategori trafik berdasarkan kebutuhan alokasi bandwidth. Untuk membedakan trafik dari masing-masing kategori, digunakan metode marking dengan aturan mangle di firewall. Misalnya, alamat IP subnet e-learning ditandai dengan packet-mark=e-learning, guru dan staf dengan packet-mark=guru-staf, siswa dengan packet-mark=siswa, dan CCTV dengan packet-mark=cctv. Penandaan ini penting agar queue dapat mengatur lalu lintas secara spesifik.

   Setelah proses marking dilakukan, masing-masing child queue dikonfigurasikan dengan parameter limit-at (alokasi minimum) dan max-limit (batas maksimum), sesuai pembagian bandwidth yang diinginkan. E-learning diberi prioritas tertinggi (priority=1) karena dianggap sebagai trafik utama, disusul oleh guru dan staf (priority=2), siswa (priority=3), dan terakhir CCTV serta update sistem (priority=4). Dengan konfigurasi ini, sistem akan memastikan bahwa e-learning selalu mendapat bandwidth yang cukup, sementara trafik lain tetap mendapat jatah sesuai kebutuhannya dan tidak saling mengganggu.

   Referensi:

   https://wiki.mikrotik.com/wiki/Manual:Queues

   https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Mangle