# MODUL 8
# ANALISA QoS PADA VPN

## TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang VPN
2. Mengenalkan pada mahasiswa tentang konfigurasi VPN pada Cisco Router

## DASAR TEORI

**Parameter QoS**

A. Packet Loss

Paket *lost* dapat disebabkan oleh sejumlah faktor, mencakup penurunan signal dalam media jaringan, melebihi batas saturasi jaringan, paket yang *corrupt* yang menolak untuk transit, kesalahan *hadware* jaringan.

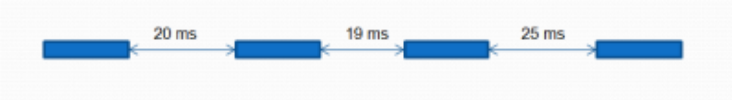
$$Packet\ loss\ = \frac{(Packets\ \_\ trasnsmitted - Packets\ \_\ received)}{Packets\ \_\ trasnmitted} x100\%$$

B. Delay

Waktu yang dibutuhkan untuk sebuah paket untuk mencapai tujuan, karena adanya antrian yang panjang, atau mengambil rute yang lain untuk menghindari kemacetan. Delay dapat di cari dengan membagi antara panjang paket (L, *packet length* (bit/s)) di bagi dengan *link bandwith* (R, *link bandwith* (bit/s)).

C. Jitter

Perbedaan waktu kedatangan dari suatu paket ke penerima dengan waktu yang diharapkan. *Jitter* dapat menyebabkan sampling di sisi penerima menjadi tidak tepat sasaran, sehingga informasi menjadi rusak., jitter dapat dihitung dengan menggunakan persamaan seperti berikut, J(i) = J(i-1) + ( |D(i-1,i)| - J(i-1) )/16. Contoh jitter seperti gambar dibawah ini.




**Gambar 1** Contoh dari jitter

D. Troughput

Pada bagian ini akan dibahas tentang analisa *throughput* pada jaringan *mpls*. *Throughput* adalah kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data. Biasanya *throughput* selalu dikaitkan dengan *bandwidth*. Karena *throughput* memang bisa disebut juga dengan *bandwidth* dalam kondisi yang sebenarnya. *Bandwidth* lebih bersifat fix sementara *throughput* sifatnya adalah dinamis tergantung trafik yang sedang terjadi.

Rumus *throughput* = $\frac{Jumlah\ data\ yang\ dikirim}{Waktu\ pengiriman\ data}$

# TUGAS PENDAHULUAN

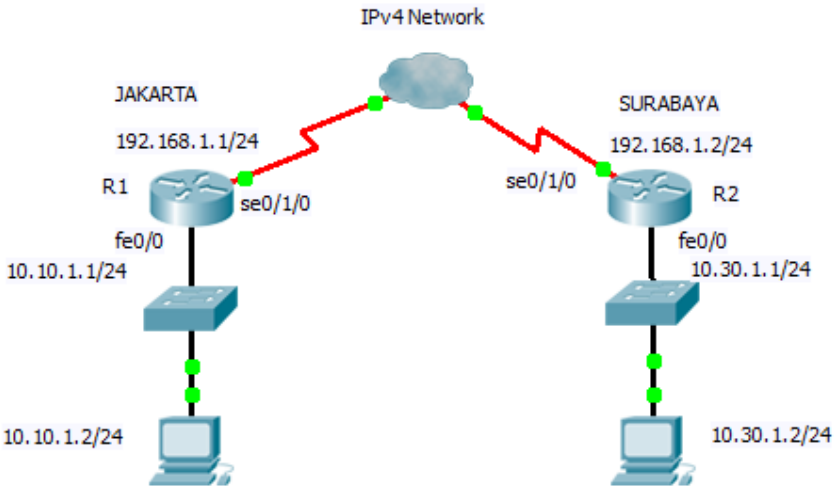
1. Jelaskan sistem kerja jaringan VPN yang anda ketahui.
2. Siapkan file berukuran 10Mbyte, 20Mbyte dan 30Mbyte.

# PERCOBAAN

## A. Membangun Jaringan Tunneling

Untuk membangun simulasi ini ada beberapa langkah yang harus dilakukan untuk mendisain beberapa subnet jaringan berbasis IPv6 yang saling tehubung dalam satu jaringan melalui Ipv4.

1. Desain jaringan seperti gambar berikut:




Gambar 1. Desain Jaringan dengan VPN

Keterangan skenario gambar:

a. Pada gambar sekenario menunjukkan 2 subnet jaringan private yang berbeda, yaitu 10.10.1.0/24 dan 10.30.1.0/24 yang akan dihubungkan menggunakan VPN. Asumsikan 2 subnet jaringan tersebut terletak di Jakarta dan Surabaya, sedangkan IPv4 Network adalah jaringan milik ISP.

b. Masing-masing Router R1 dan R2 terhubung melalui kabel serial.

c. Pastikan tidak ada setting VPN pada router Cisco dengan perintah :
R1# show crypto ipsec sa

Dari perintah di atas, harusnya tidak muncul setting VPN-nya, kalau muncul setting VPN, hapus terlebih dahulu.

## B. Konfigurasi interface pada Cisco Router

**2. Konfigurasi interface pada Router 1**

a. Lakukan konfigurasi pada Router 1 dengan mengetikkan perintah berikut pada CLI:

```
R1> enable
R1#configure terminal
R1 (config)#interface fastethernet 0/0
R1 (config-if)#ip address 10.10.1.1 255.255.255.0
R1 (config-if)#no shutdown
R1(config-if)#exit

R1 (config)#interface serial 0/1/0
R1 (config-if)#ip address  192.168.1.1  255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#
```

b. Setting static routing ke jaringan 3

```
R1 (config)#ip route 10.30.1.0 255.255.255.0 192.168.1.2
R1 (config)#exit
```

c. Untuk melihat hasil konfigurasi :

```
R1#show ip interface brief
```

Amati dan catat hasil perintah di atas.

**3. Konfigurasi Router 2**

a. Lakukan hal yang sama pada Router 2:

```
R2> enable
R2#configure terminal
R2 (config)#interface fastethernet 0/0
R2 (config-if)#ip address 10.30.1.1 255.255.255.0
R2 (config-if)#no shutdown
R2(config-if)#exit

R2 (config)#interface serial 0/1/0
R2 (config-if)#ip address  192.168.1.2  255.255.255.0
R2(config-if)#clock rate 64000                    => asumsi bahwa posisi DCE di R2
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#
```

b. Setting static routing ke jaringan 1

```
R2 (config)#ip route 10.10.1.0 255.255.255.0 192.168.1.1
R2 (config)#exit
```

b. Untuk melihat hasil konfigurasi ketikan sebagai berikut:

```
R2# show ip  interface brief
```

Amati dan catat hasil perintah di atas.

## C. Konfigurasi pada PC Client

4. Lakukan setting secara manual pada PC Client
   a. Setting IP pada jaringan di Jakarta

```
# ifconfig eth0 10.10.1.2 netmask 255.255.255.0
```

Tambahkan default gatewaynya :

```
# route  add –net default gw 10.10.1.1
```

b. Lakukan setting juga pada client pada jaringan di Surabaya

```
# ifconfig eth0 10.30.1.2 netmask 255.255.255.0
```

Tambahkan default gatewaynya :

```
# route  add –net default gw 10.30.1.1
```

d. Lakukan ping dari jaringan di Jakarta ke jaringan di Surabaya, catat hasilnya

```
# ping  10.30.1.2
```

## D. QoS pada jaringan tanpa VPN

5. Lakukan pengukuran QoS dengan parameter delay . Lakukan tes koneksi dengan ftp dari PC di Jakarta (asumsi FTP Server di Surabaya)

```
# ftp  10.30.1.2
ftp> get  file10Mb          => untuk download dari server ke client
```

Catat hasilnya untuk waktu akses dan throughputnya seperti contoh di bawah ini.

```
226 Transfer complete
911455 bytes received in 5.33 secs (167.1 kB/s)
ftp>
```

| File size | Waktu (s) | Throughput (Kbps) |
|---|---|---|
| 10Mbyte | | |
| 20Mbyte | | |
| 30Mbyte | | |

## E. Setting Jaringan VPN

6. Tahapan untuk melakukan tunneling dari R1 ke R2 dengan melewati jaringan IPv4. Untuk melakukannya lakukan langkah sebagai berikut pad CLI:

**a. Pada Router 1:**

```
R1> enable
R1#configure terminal
Berikan access-list agar jaringan jkt-sby bisa saling interkoneksi
R1 (config)#ip access-list extended jkt-sby
R1 (config-ext-nacl)#permit ip 10.10.1.0  0.0.0.255  10.30.1.0  0.0.0.255
R1 (config-ext-nacl)#exit

Konfigurasi dengan VPN menggunakan isakmp, policy 1 adalah prioritasnya
R1 (config)#crypto isakmp policy 1
R1 (config-isakmp)#encr 3des
R1 (config-isakmp)#authentication pre-share
R1 (config-isakmp)#group 2
R1 (config-isakmp)#exit

Berikan nama kunci, dalam hal ini : vpnxyz  untuk koneksi ke 192.168.1.2 (Surabaya)
R1 (config)#crypto isakmp key vpnxyz address 192.168.1.2
R1 (config)#crypto ipsec transform-set 6 esp-3des esp-sha-hmac
R1 (cfg-crypto-trans)#exit

Setting crypto map dengan nama : vpn-ngn dengan nomor urut 1
R1 (config)#crypto map vpn-ngn 1 ipsec-isakmp
R1 (config-crypto-map)#set peer 192.168.1.2
R1 (config-crypto-map)#set transform-set 6
R1 (config-crypto-map)#match address jkt-sby
R1 (config-crypto-map)#exit

Berikan crypto map di atas pada interface serial 0/1/0
R1 (config)#interface serial0/1/0
R1 (config-if)#crypto map vpn-ngn
R1 (config-if)#exit
```

**b. Pada Router 2:**

```
R2> enable
R2#configure terminal
Berikan access-list agar jaringan sby-jkt bisa saling interkoneksi
R2 (config)#ip access-list extended sby-jkt
R2 (config-ext-nacl)#permit ip 10.30.1.0  0.0.0.255  10.10.1.0  0.0.0.255
R2 (config-ext-nacl)#exit

Konfigurasi dengan VPN menggunakan isakmp
R2 (config)#crypto isakmp policy 1
```

```
R2 (config-isakmp)#encr 3des
R2 (config-isakmp)#authentication pre-share
R2 (config-isakmp)#group 2
R2 (config-isakmp)#exit

Berikan nama kunci, dalam hal ini : vpnxyz  untuk koneksi ke 192.168.1.1 (Jakarta)
R2 (config)#crypto isakmp key vpnxyz address 192.168.1.1
R2 (config)#crypto ipsec transform-set 6 esp-3des esp-sha-hmac
R2 (cfg-crypto-trans)#exit

Setting crypto map dengan nama : vpn-ngn
R2 (config)#crypto map vpn-ngn 1 ipsec-isakmp
R2 (config-crypto-map)#set peer 192.168.1.1
R2 (config-crypto-map)#set transform-set 6
R2 (config-crypto-map)#match address sby-jkt
R2 (config-crypto-map)#exit

Berikan crypto map di atas pada interface serial 0/1/0
R2 (config)#interface serial0/1/0
R2 (config-if)#crypto map vpn-ngn
R2 (config-if)#exit
```

c. Untuk mengetahui jumlah paket yang dikirim, ketikkan perintah :
R1# show crypto ipsec sa

e. Lakukan ping dari client 10.30.1.2 ke 10.10.1.2 dan ulangi perintah 6.c, catat hasilnya dan amati perbedaannya.

## F. QoS pada jaringan dengan VPN

7. Lakukan pengukuran QoS dengan parameter delay . Lakukan tes koneksi dengan ftp dari PC di Jakarta (asumsi FTP Server di Surabaya)

```
# ftp  10.30.1.2
ftp> get  file10Mb          => untuk download dari server ke client
```

| File size | Waktu (s) | Throughput (Kbps) |
|---|---|---|
| 10Mbyte | | |
| 20Mbyte | | |
| 30Mbyte | | |

8. Bandingkan hasilnya table langkah ke-5. Buat grafik waktu dan throughputnya untuk perbandingannya.

## LAPORAN RESMI

Berikan kesimpulan hasil praktikum yang anda lakukan.