



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

Laporan Akhir Praktikum Jaringan Komputer

VPN dan QoS

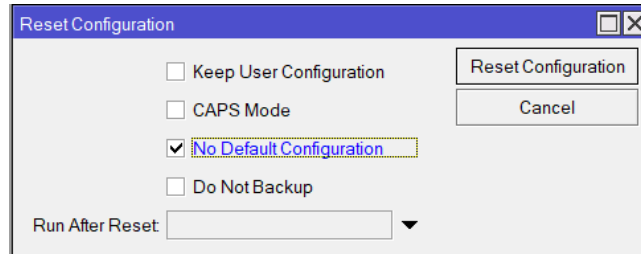
Muhammad Tamim Nugraha - 5024231060

2025

1 Langkah-Langkah Percobaan

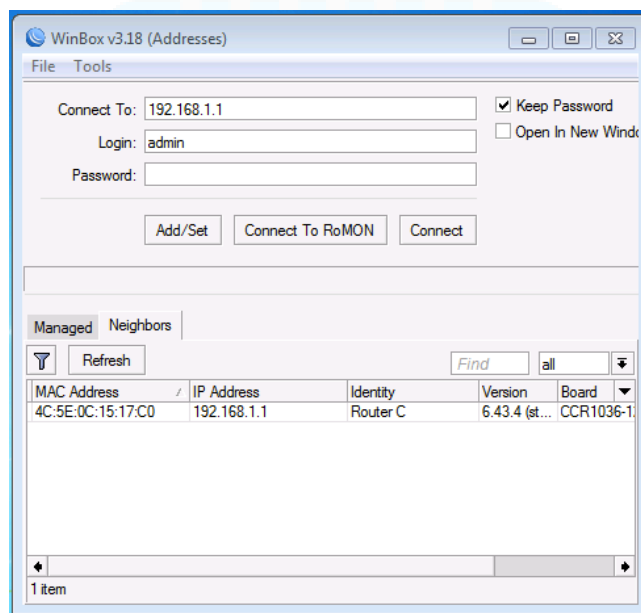
1.1 Konfigurasi VPN

1. Lakukan reset pada router untuk mengembalikannya ke konfigurasi pabrik guna menghindari potensi konflik pengaturan.



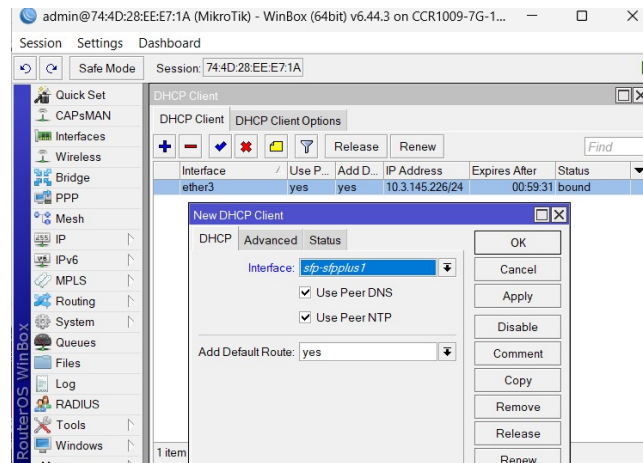
Gambar 1: Proses reset router

2. Akses router menggunakan Winbox dengan memasukkan alamat IP-nya, lalu masuk dengan nama pengguna "admin".



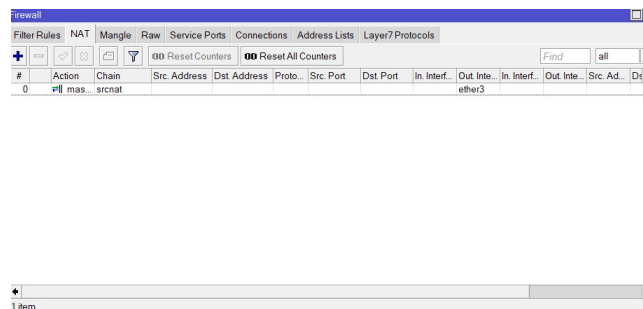
Gambar 2: Login ke router via Winbox

3. Atur DHCP Client agar router dapat menerima alamat IP dan koneksi internet secara dinamis dari penyedia layanan.



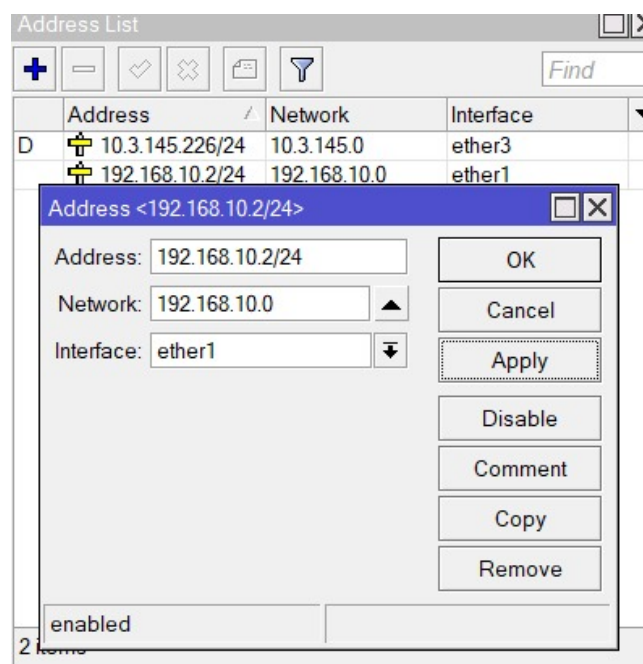
Gambar 3: Pengaturan DHCP Client untuk koneksi internet

4. Buat aturan NAT pada firewall untuk mengizinkan perangkat di jaringan lokal yang terhubung melalui ether3 dapat mengakses internet.



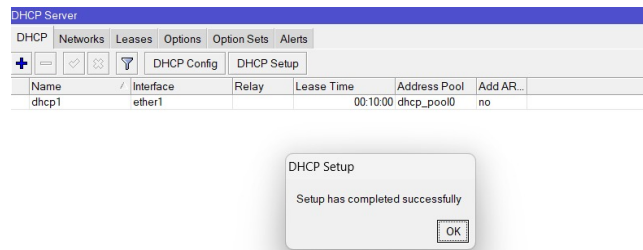
Gambar 4: Konfigurasi NAT pada firewall

5. Tetapkan alamat IP untuk antarmuka ether1 yang akan berfungsi sebagai gerbang untuk jaringan lokal (LAN).



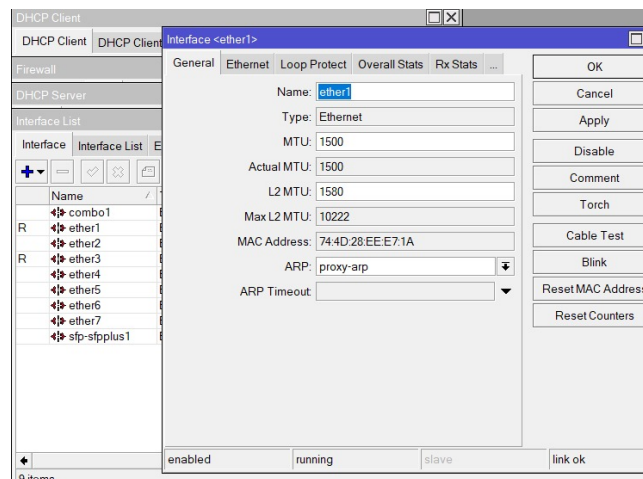
Gambar 5: Penambahan alamat IP untuk LAN

6. Lakukan pengaturan DHCP Server pada antarmuka ether1 untuk menyediakan alamat IP secara otomatis kepada klien seperti PC atau laptop.



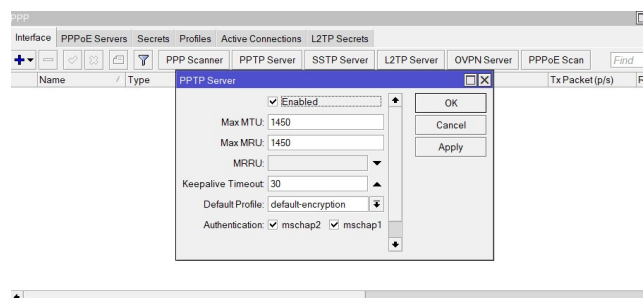
Gambar 6: Proses setup DHCP Server

7. Pastikan konfigurasi DHCP Server telah selesai sehingga klien yang terhubung ke ether1 akan mendapatkan IP secara otomatis.



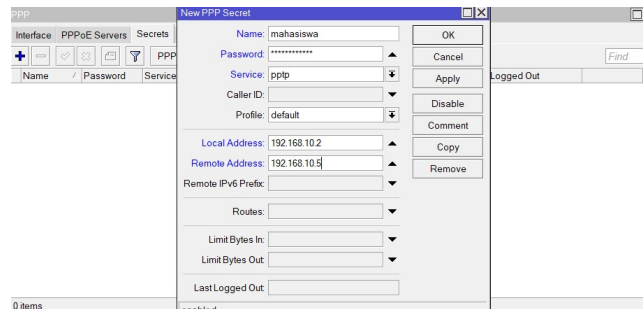
Gambar 7: Menyelesaikan setup DHCP Server

8. Pada antarmuka yang terhubung ke internet, aktifkan mode Proxy ARP untuk memfasilitasi proses bridging dan routing.



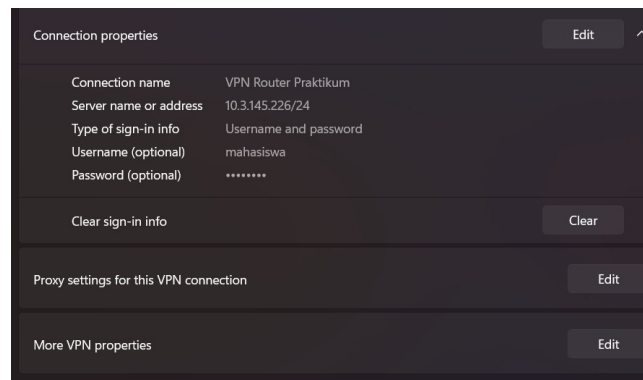
Gambar 8: Mengaktifkan Proxy ARP

9. Mulai konfigurasi PPTP VPN Server dengan mengaktifkan layanan tersebut pada router.



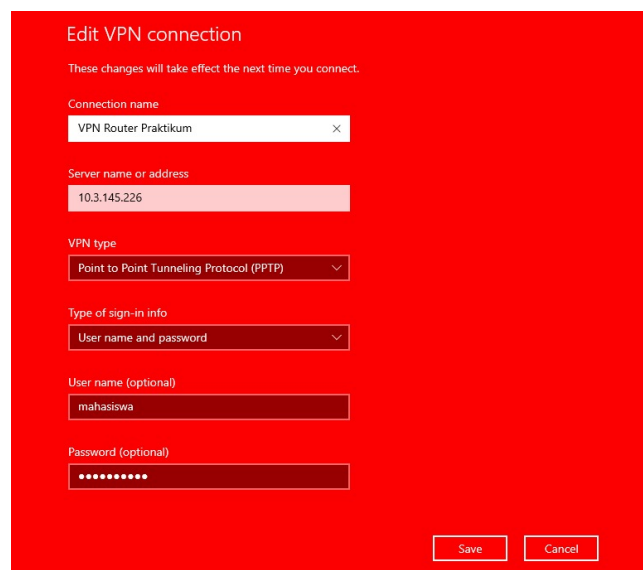
Gambar 9: Aktivasi layanan PPTP Server

10. Lanjutkan konfigurasi PPTP Server dengan membuat akun pengguna (user dan password) pada bagian *secrets* yang akan digunakan klien untuk otentikasi VPN.



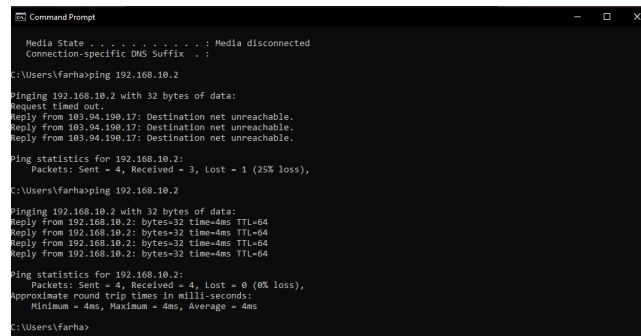
Gambar 10: Pembuatan akun user pada PPTP secrets

11. Pada perangkat laptop (OS Windows), buat koneksi PPTP Client baru untuk terhubung ke server VPN yang sudah dibuat.



Gambar 11: Pengaturan koneksi PPTP Client di Windows

12. Lakukan verifikasi pada PC1 yang terkoneksi melalui VPN dengan melakukan uji ping ke alamat IP lokal milik router.



```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 
C:\Users\Farha>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.2: Destination net unreachable.
Reply from 192.168.10.2: Destination net unreachable.
Reply from 192.168.10.2: Destination net unreachable.

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

C:\Users\Farha>ping 192.168.10.2

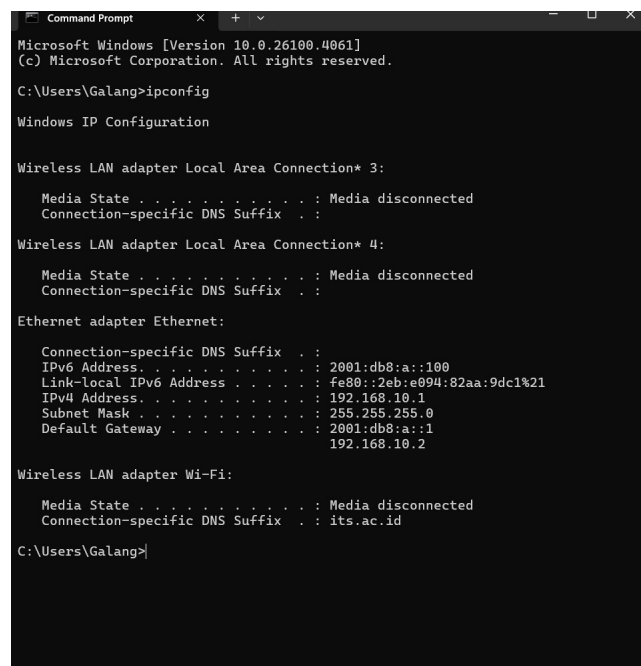
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=4ms TTL=64
Reply from 192.168.10.2: bytes=32 time=4ms TTL=64
Reply from 192.168.10.2: bytes=32 time=4ms TTL=64
Reply from 192.168.10.2: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\Farha>
```

Gambar 12: Verifikasi koneksi dari klien VPN (PC1)

13. Lakukan verifikasi serupa pada PC2 yang terhubung langsung ke ether1 dengan melakukan uji ping.



```
Microsoft Windows [Version 10.0.26100.4061]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Galang>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:db8:a::100
    Link-local IPv6 Address . . . . . : fe80::2eb:e094:82aa:9dc1%21
    IPv4 Address. . . . . : 192.168.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 2001:db8:a::1
                               192.168.10.2

Wireless LAN adapter Wi-Fi:

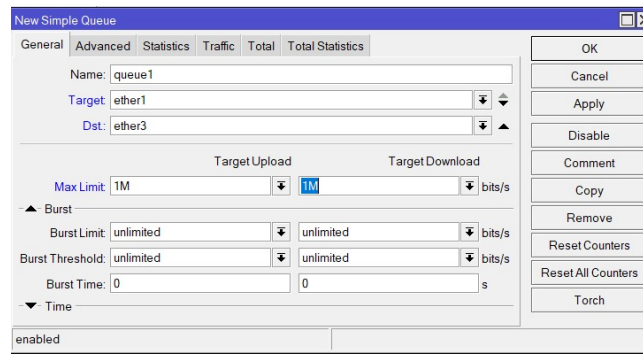
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : its.ac.id

C:\Users\Galang>
```

Gambar 13: Verifikasi koneksi dari klien LAN (PC2)

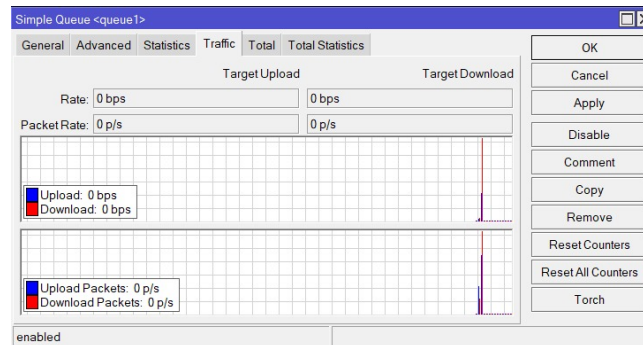
1.2 Konfigurasi QoS

Buat sebuah aturan *Simple Queue* untuk membatasi kecepatan unduh dan unggah yang dapat digunakan oleh klien di jaringan.



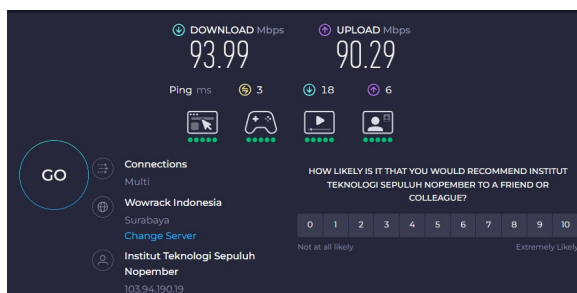
Gambar 14: Pembuatan aturan pembatasan bandwidth

- 1.
2. Lakukan pemantauan pada lalu lintas data untuk mengobservasi dan memastikan bahwa aturan *simple queue* telah berfungsi dengan benar.

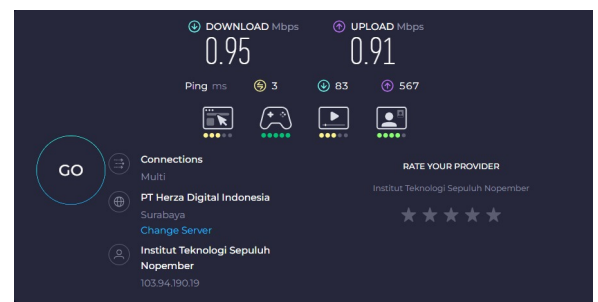


Gambar 15: Pemantauan lalu lintas data pada queue

3. Lakukan pengujian kecepatan internet untuk membandingkan hasilnya sebelum dan sesudah *queue* diaktifkan, serta saat *queue* dimatikan dan dinyalakan kembali.



Gambar 16: Pengujian kecepatan saat queue aktif



Gambar 17: Pengujian kecepatan saat queue nonaktif

2 Analisis Hasil Percobaan

Pada sesi praktikum ini, dilakukan dua jenis konfigurasi inti, yaitu penyiapan Virtual Private Network (VPN) dan penerapan Quality of Service (QoS). Seluruh rangkaian prosedur, mencakup pengaturan DHCP Client dan Server, definisi alamat IP, NAT, hingga konfigurasi spesifik untuk VPN PPTP serta QoS, berhasil diimplementasikan tanpa kendala berarti. Router sukses memperoleh alamat IP secara dinamis dari ISP melalui DHCP Client, dan sebaliknya, perangkat klien juga berhasil mendapatkan IP dari DHCP Server yang telah disiapkan. Aturan NAT berfungsi secara efektif untuk menyediakan koneksi internet bagi jaringan lokal. Layanan VPN PPTP juga berhasil dibangun, memungkinkan klien terhubung ke jaringan internal secara aman lewat koneksi yang terenkripsi. Uji konektivitas dengan perintah ping memberikan respons yang sukses, mengindikasikan komunikasi antarperangkat berjalan lancar. Dalam implementasi QoS, aturan *simple queue* terbukti mampu membatasi alokasi bandwidth untuk klien sesuai dengan nilai yang ditetapkan. Perbedaan kecepatan yang signifikan teramati antara sebelum dan sesudah *queue* diaktifkan, yang menjadi bukti bahwa manajemen bandwidth bekerja sesuai harapan. Meskipun sempat ditemukan beberapa kendala kecil selama pengujian, semua masalah tersebut dapat diselesaikan dengan baik dan tidak mengganggu jalannya praktikum.

3 Hasil Tugas Modul

1. Membuat sebuah simulasi jaringan pada Cisco Packet Tracer yang melibatkan dua router yang saling terhubung melalui protokol PPTP VPN. Setiap router terhubung ke satu PC klien. Seluruh perangkat dikonfigurasi dengan alamat IP, dan koneksi PPTP antar-router diatur agar kedua PC dapat saling melakukan ping secara aman. Disertakan topologi jaringan, bukti hasil uji ping, dan deskripsi singkat mengenai fungsi PPTP.


```

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=7ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126
Reply from 192.168.2.10: bytes=32 time=5ms TTL=126
Reply from 192.168.2.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 3ms

```

Hasil Ping dari PC1 ke PC2

```

C:\>ping 192.168.1.10

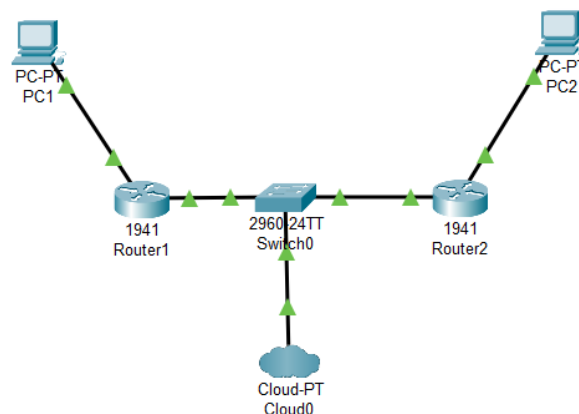
Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=6ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

```

Hasil Ping dari PC2 ke PC1



Desain Topologi Jaringan

2. PPTP (Point-to-Point Tunneling Protocol) adalah protokol yang digunakan untuk membangun koneksi VPN yang aman melintasi jaringan publik. Protokol ini bekerja dengan cara mengenkripsi data yang dikirimkan antara dua titik, sehingga memungkinkan dua jaringan di lokasi yang berbeda untuk terhubung seolah-olah berada dalam satu jaringan lokal (LAN) yang sama.

4 Kesimpulan

Berdasarkan keseluruhan rangkaian praktikum, dapat ditarik kesimpulan bahwa konfigurasi jaringan pada perangkat MikroTik—meliputi DHCP Client dan Server, NAT, Firewall, VPN PPTP, dan QoS—telah berhasil diimplementasikan sesuai rancangan. Setiap elemen jaringan sudah diatur dengan benar

dan terverifikasi dapat berfungsi secara optimal. Hasil dari pengujian menunjukkan bahwa perangkat di dalam jaringan mampu terhubung ke internet serta dapat berkomunikasi satu sama lain tanpa masalah. Implementasi QoS juga terbukti efektif dalam mengelola lalu lintas data sesuai dengan kebijakan yang telah ditetapkan. Semua konfigurasi yang dilakukan berkontribusi dalam mendukung keamanan, efisiensi, dan stabilitas koneksi jaringan sebagaimana yang menjadi tujuan praktikum.

5 Lampiran

5.1 Dokumentasi saat praktikum



Gambar 18: Foto Dokumentasi Praktikum Modul 5