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

Laporan Akhir
Praktikum Jaringan Komputer

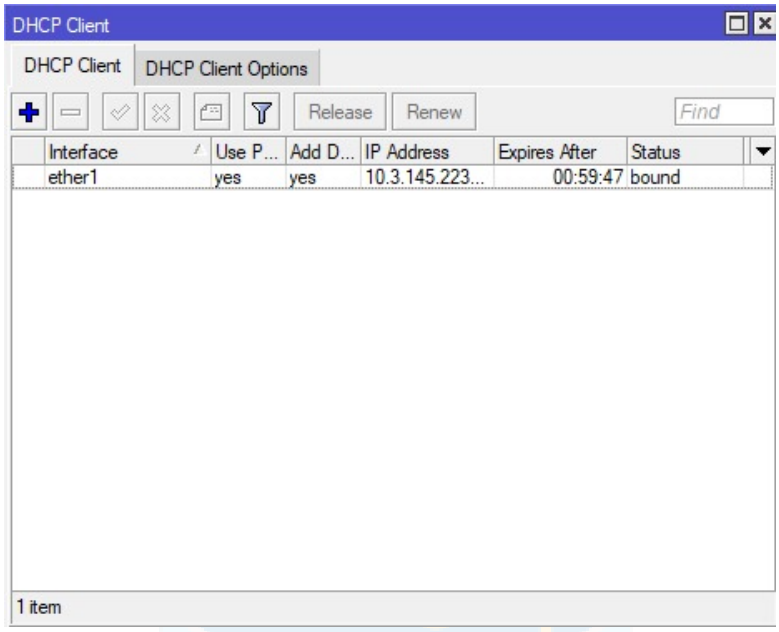
Firewall dan NAT

Muhammad Jaysyurrahman - 5024231057

2025

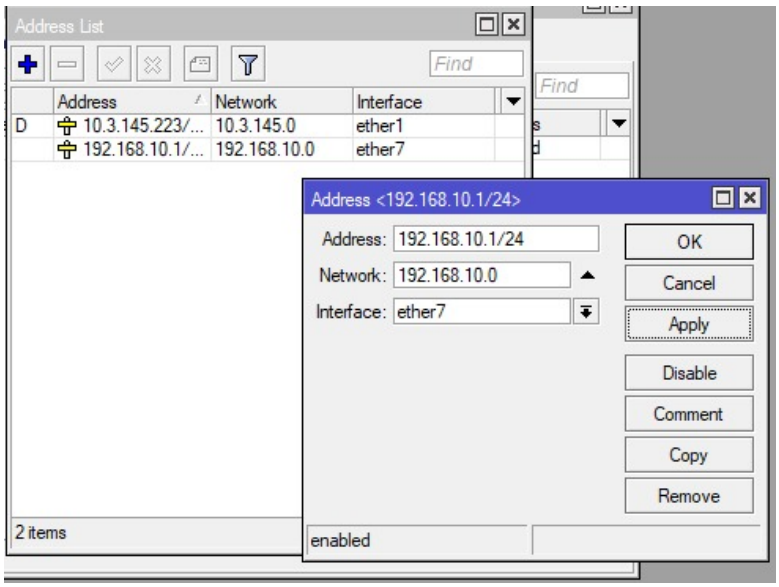
1 Langkah-Langkah Percobaan

1. Hubungkan laptop ke router A di ether 1 dan switch di ether 7
2. masuk aplikasi winbox
3. login ke router (Gunakan username "admin")
4. reset router dengan klik menu System > Reset Configuration. Aktifkan opsi "No Default Configuration" lalu klik reset configuration
5. Konfigurasi DHCP Client pada Router A yang terhubung di ether 1 dengan klik menu IP > DHCP Client. Klik ikon "+" untuk menambah entri baru. Pilih "ether1" sebagai Interface lalu klik "Apply"



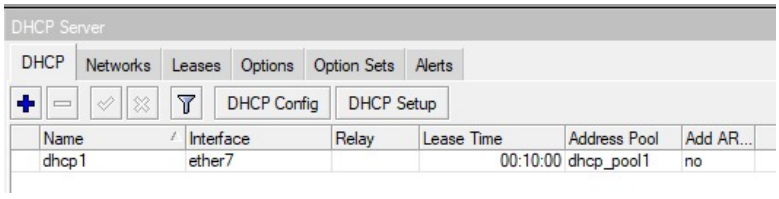
Gambar 1: Konfigurasi DHCP Client

6. Menambah alamat IP pada ether 7 untuk konektivitas dengan switch dengan klik menu IP > Addresses. Klik "+" untuk menambahkan alamat IP.
   Masukkan Address: 192.168.10.1/24.
   Pilih Interface: "ether7".
   Klik "Apply" lalu "OK".



Gambar 2: Penambahan alamat IP ether 7

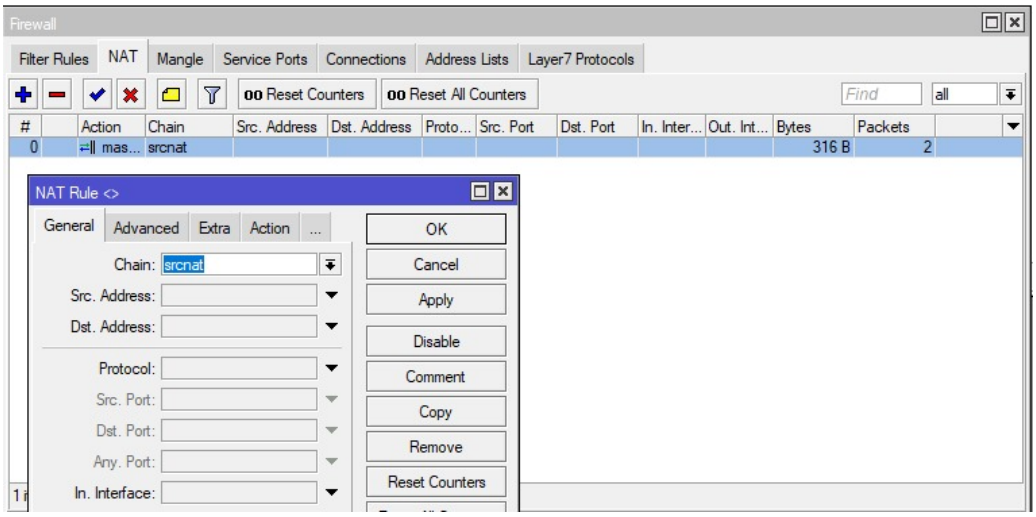
7. Konfigurasi DHCP Server router agar otomatis mendistribusikan alamat IP kepada perangkat klien yang terhubung :
   Akses menu IP > DHCP Server.
   Klik tombol "DHCP Setup".
   Pada jendela "DHCP Server Interface":
   Pilih interface ether7 lalu klik "Next".
   Pada jendela "DHCP Address Space":
   Verifikasi network address 192.168.10.0/24. Klik "Next".
   Pada jendela "Gateway for DHCP Network":
   Verifikasi gateway 192.168.10.1. Klik "Next".
   Pada jendela "Addresses to Give Out":
   Tentukan rentang alamat IP 192.168.10.2-192.168.10.254. Klik "Next".
   Pada jendela "DNS Servers":
   Masukkan alamat DNS Server 8.8.8.8 dan 8.8.4.4. Klik "Next".
   Pada jendela "Lease Time":
   Atur durasi waktu lease IP address 00:10:00 untuk 10 menit. Klik "Next".
   Setelah semua langkah selesai, akan muncul pesan "Setup has completed successfully". Klik "OK".



Gambar 3: Konfigurasi DHCP server

8. Konfigurasi NAT untuk menyediakan konektivitas internet. Klik menu IP > Firewall > NAT, lalu Klik "+" untuk membuat aturan baru.

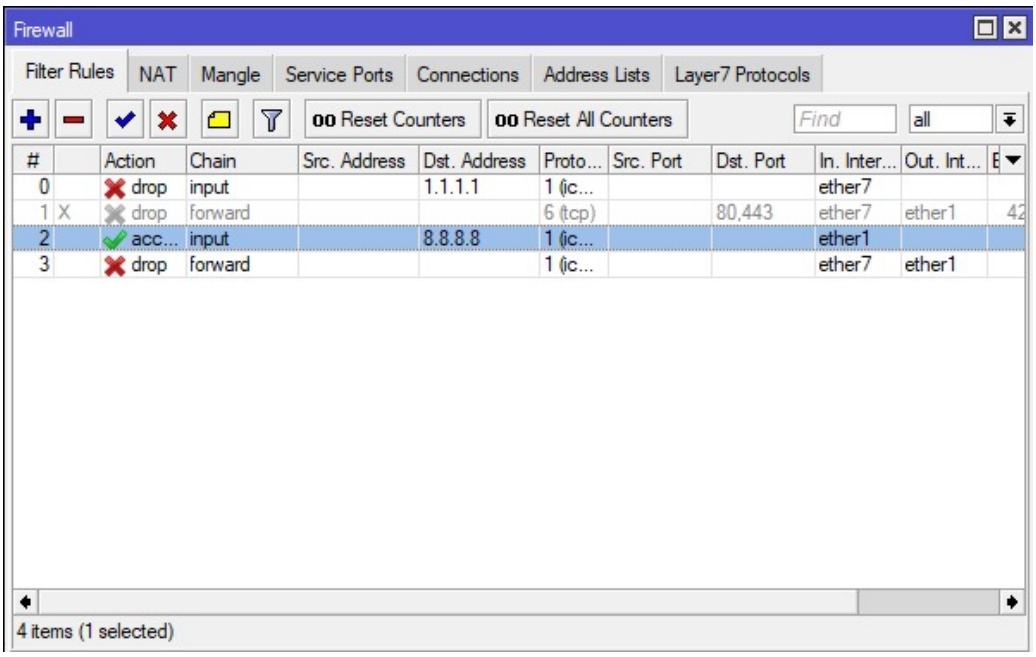
Pada tab "General", atur Chain: "src-nat".
Pada tab "Action", atur Action: "masquerade".
Klik Apply dan OK.



Gambar 4: Konfigurasi NAT

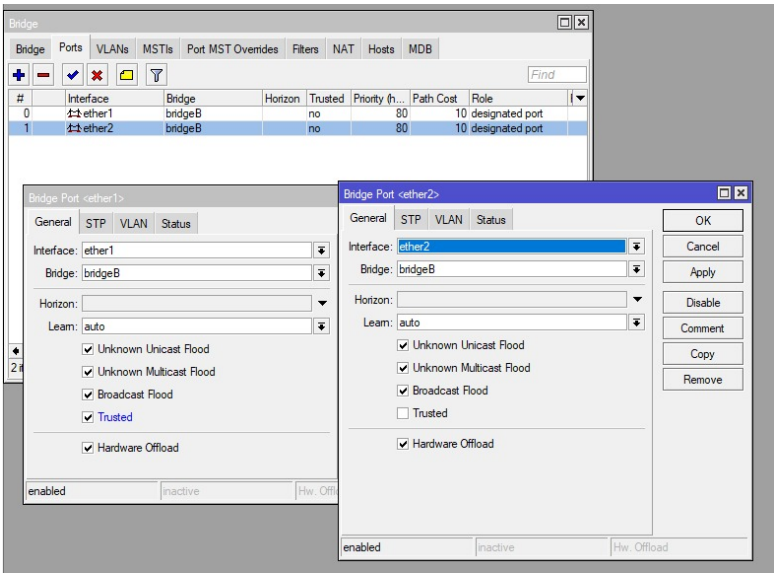
9. Konfigurasi Firewall. Tambahkan aturan filter (Filter Rules) pada firewall. Klik menu IP > Firewall > Filter Rule lalu Klik "+" untuk menambahkan aturan baru.
   Untuk Pemblokiran ICMP (Internet Control Message Protocol):
   Pada tab "General", atur Chain: "forward".
   Pada tab "General", atur Protocol: "icmp".
   Pada tab "General", atur In. Interface: "ether7".
   Pada tab "Action", atur Action: "drop".

   Untuk Pemblokiran Akses Situs Web Berdasarkan Konten (Content Blocking):
   Pada tab "General", atur Chain: "forward".
   Pada tab "General", atur Protocol: "tcp".
   Pada tab "General", atur Dst. Port: "80,443".
   Pada tab "General", atur In. Interface: "ether7".
   Pada tab "General", atur Out. Interface: "ether1".
   Pada tab "Advanced", atur Content: "speedtest".
   Pada tab "Action", atur Action: "drop".



Gambar 5: Konfigurasi Firewall

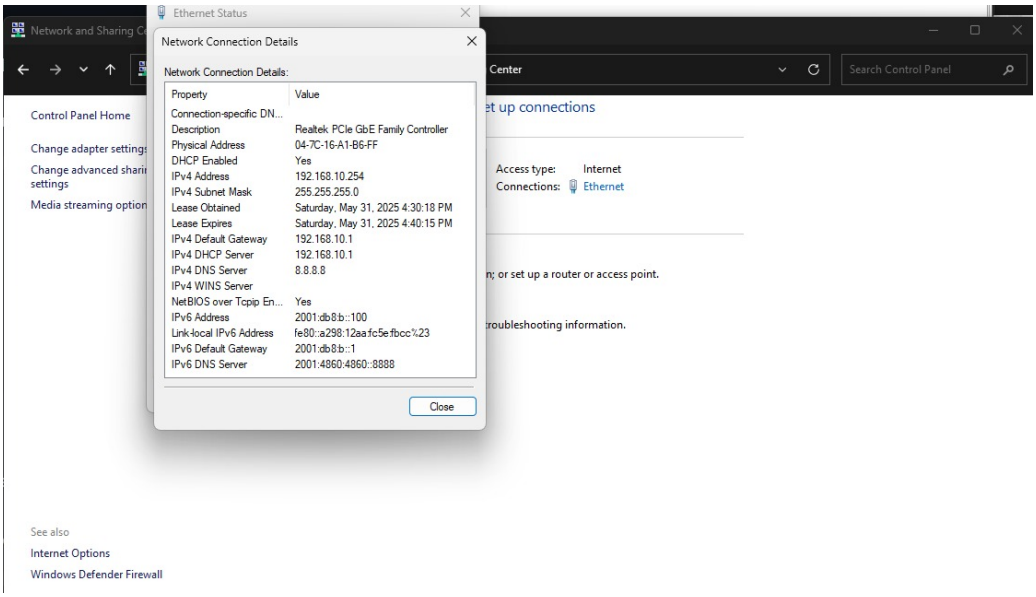
10. Konfigurasi Bridge pada Router B untuk mengubahnya menjadi hub dengan cara :
    Masuk ke menu Bridge.
    Klik "+" untuk membuat bridge baru.
    Klik "Apply" kemudian "OK".
    Lalu tambahkan port ke dalam bridge dengan cara :
    Masuk ke tab Port pada Bridge
    Klik ikon "+" untuk menambahkan port.
    Pilih interface ether1 (Laptop).
    Pilih interface ether2 (Router A).



Gambar 6: Menambah Port Bridge

11. Konfigurasi Alamat IP pada Laptop

Pada pengaturan sistem operasi laptop (melalui Settings atau Control Panel), pastikan konfigurasi jaringan diatur ke DHCP (Automatic).
Buka Command Prompt (CMD).
Gunakan perintah ipconfig untuk memeriksa dan mengonfirmasi alamat IP yang telah diterima oleh laptop.

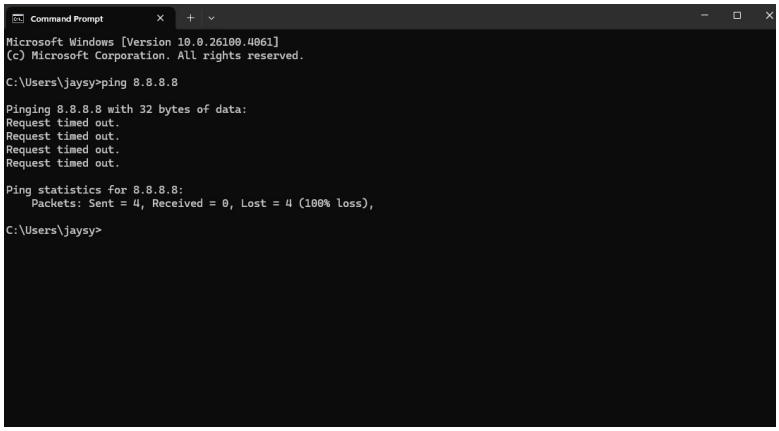


Gambar 7: Konfigurasi Jaringan

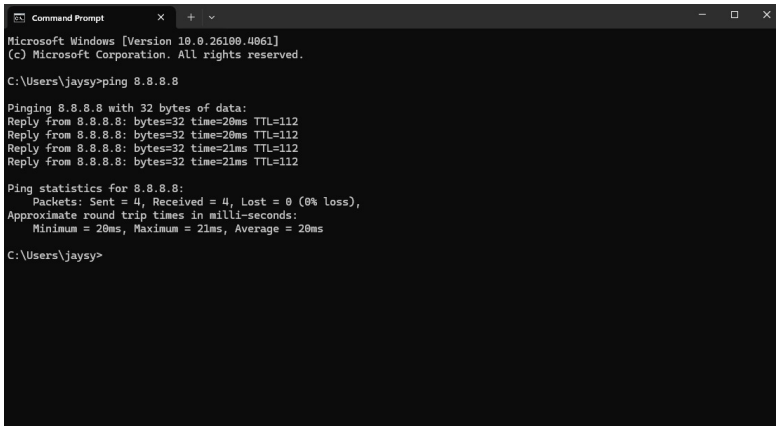
12. Uji Coba Konfigurasi
Pengujian Konektivitas (ICMP):

Buka Terminal pada laptop.
Lakukan perintah ping 8.8.8.8.
Saat firewall aktif, responnya Request Timed Out (RTO).
Nonaktifkan firewall ICMP dengan menekan tanda "X" (disable) pada aturan terkait di Filter Rules.
Ulangi perintah ping 8.8.8.8. Koneksi terhubung kembali
Pengujian Pemblokiran Konten (Browse):

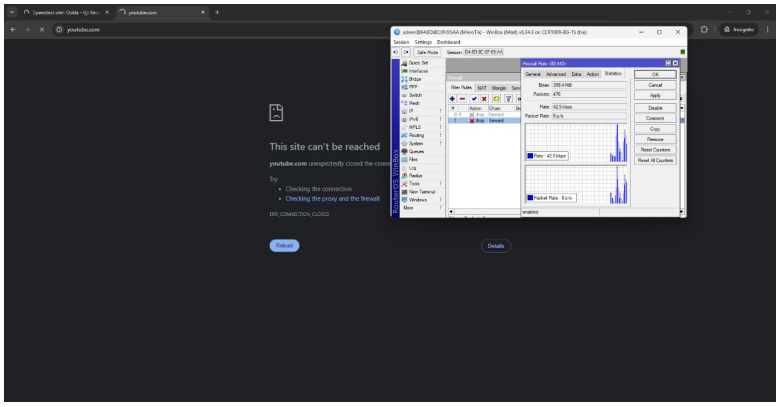
akses situs web www.speedtest.net melalui peramban web.
Saat firewall konten aktif, situs web tidak dapat diakses atau terus memuat tanpa menampilkan konten, menandakan bahwa firewall telah berhasil bekerja.
Nonaktifkan firewall konten dengan menekan tanda "X" (disable) pada aturan terkait di Filter Rules.
Situs web dapat diakses kembali.



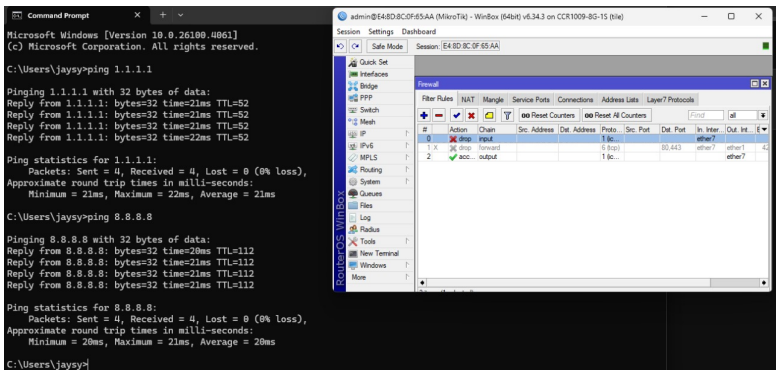
Gambar 8: Ping 8.8.8.8 firewall aktif



Gambar 9: Ping 8.8.8.8 firewall nonaktif



Gambar 10: Block Youtube



Gambar 11: Unblock 1.1.1.1

2 Analisis Hasil Percobaan

Pada praktikum ini, langkah-langkah yang dilakukan meliputi konfigurasi jaringan di router dan firewall untuk menguji pemblokiran situs dan konektivitas internet. Berdasarkan hasil yang diperoleh, konfigurasi router dan firewall berhasil diimplementasikan dengan baik, sesuai dengan langkah yang sudah dipersiapkan dalam praktikum.

Hasil percobaan terkait pemblokiran situs web dan konektivitas ICMP sesuai dengan ekspektasi. Pengujian ICMP menunjukkan bahwa saat firewall aktif, perintah ping 8.8.8.8 memberikan respons "Request Timed Out", yang menunjukkan bahwa koneksi terblokir. Setelah firewall dinonaktifkan, koneksi kembali terhubung dengan sukses, seperti terlihat pada Gambar 8 dan 9. Hal ini mengonfirmasi bahwa konfigurasi firewall telah berhasil untuk memblokir dan mengizinkan koneksi sesuai dengan aturan yang diterapkan.

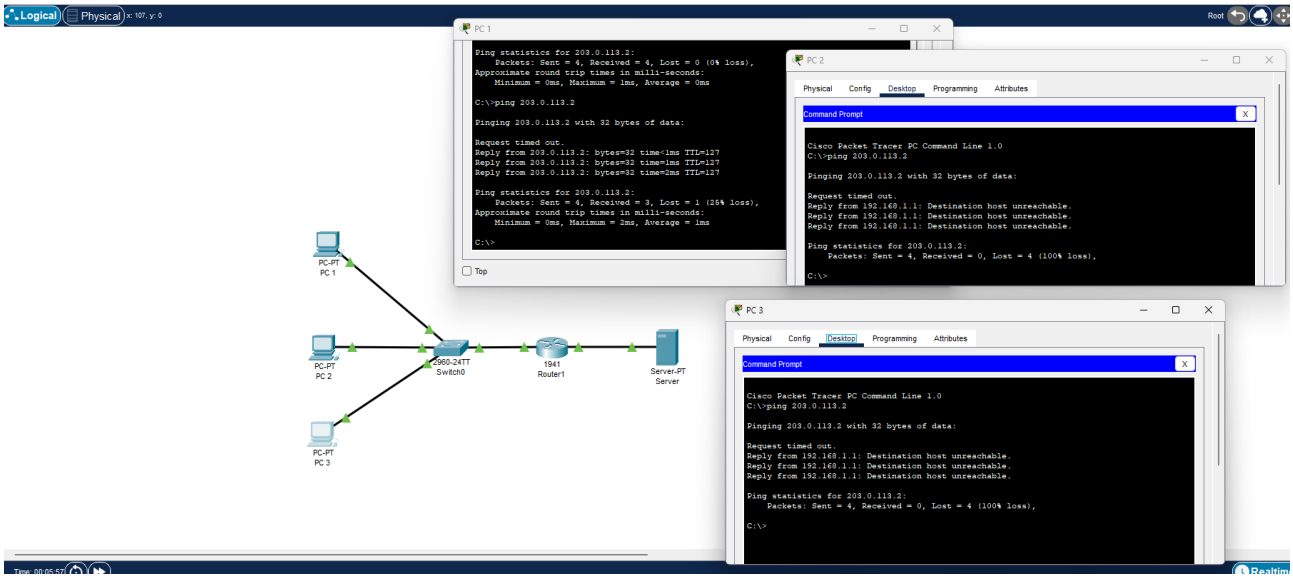
Demikian pula, pengujian pemblokiran konten situs web dengan mengakses www.youtube.com menunjukkan bahwa situs tidak dapat diakses saat firewall konten aktif (Gambar 10). Setelah firewall konten dinonaktifkan, situs dapat diakses kembali, menunjukkan keberhasilan firewall dalam mengendalikan akses sesuai dengan konten yang diblokir.

Beberapa faktor yang memengaruhi hasil adalah ketelitian dalam mengikuti langkah-langkah konfigurasi dan penggunaan alat yang tepat, seperti router dan perangkat firewall. Selain itu, pengaturan DHCP dan NAT juga berperan penting dalam memastikan perangkat terhubung dengan jaringan yang telah dikonfigurasi.

3 Hasil Tugas Modul

Dalam tugas modul ini, membuat topologi jaringan sederhana menggunakan Cisco Packet Tracer yang terdiri dari satu buah Router (1941), satu Switch (2960-24TT), tiga PC yang terhubung dalam jaringan LAN (192.168.1.0/24), serta satu Server yang mewakili jaringan publik (203.0.113.2/30). Konfigurasi jaringan dilakukan secara menyeluruh agar ketiga PC dapat terhubung ke internet melalui Router yang memiliki IP publik pada interface GigabitEthernet0/1 (203.0.113.1).

Langkah pertama adalah melakukan konfigurasi NAT (Network Address Translation) dengan teknik NAT overload agar seluruh perangkat di jaringan LAN dapat mengakses server publik menggunakan satu IP publik milik router. NAT ini memungkinkan IP privat dari PC1, PC2, dan PC3 untuk



Gambar 12: Hasil Tugas Modul

diterjemahkan ke IP publik router saat mengakses server, sehingga komunikasi ke jaringan luar dapat dilakukan tanpa konflik IP.

Selanjutnya, menerapkan konfigurasi ACL (Access Control List) pada router untuk mengatur hak akses ke server. Sesuai dengan ketentuan soal, hanya PC1 (192.168.1.11) yang diizinkan mengakses server, sedangkan PC2 (192.168.1.12) dan PC3 (192.168.1.13) diblokir. ACL ditempatkan pada interface GigabitEthernet0/1 (arah keluar menuju internet) dengan urutan aturan: permit hanya untuk IP PC1 ke server, deny untuk semua akses ke server dari IP lain, dan permit sisanya untuk memastikan LAN tetap bisa saling terhubung. Hasil pengujian melalui perintah ping menunjukkan bahwa hanya PC1 yang berhasil terhubung ke server, sedangkan PC2 dan PC3 mendapatkan respon “Destination host unreachable”, yang menandakan ACL berjalan sesuai konfigurasi.

4 Kesimpulan

Praktikum ini berhasil dilaksanakan dengan baik, dan tujuan untuk memblokir akses situs dan mengatur konektivitas internet dapat tercapai dengan sukses. Berdasarkan hasil yang didapat, pemblokiran akses situs seperti yang diuji pada situs web dan pengujian ICMP, hasilnya sesuai dengan teori yang ada mengenai cara kerja firewall dalam memfilter lalu lintas jaringan.

Pembelajaran yang diperoleh adalah pentingnya konfigurasi yang tepat dalam penerapan firewall dan pengaturan jaringan, serta pemahaman tentang bagaimana masing-masing aturan dapat memengaruhi akses internet. Praktikan telah memahami cara kerja DHCP, NAT, dan firewall untuk mengelola konektivitas serta pembatasan akses.

5 Lampiran

5.1 Dokumentasi saat praktikum

Gambar 13: Dokumentasi saat praktikum