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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall dan NAT

Muhammad Azzikri - 5024221029

2025

1 Langkah-Langkah Percobaan

Praktikum ini melibatkan serangkaian konfigurasi pada dua perangkat MikroTik RouterBoard, yaitu Router A yang berfungsi sebagai router utama dengan kapabilitas NAT dan Firewall, serta Router B yang dikonfigurasi sebagai perangkat bridge. Pengujian fungsionalitas dilakukan pada perangkat laptop yang terhubung ke infrastruktur jaringan yang dibangun.

1.1 Konfigurasi Router A (MikroTik)

Reset Konfigurasi Router

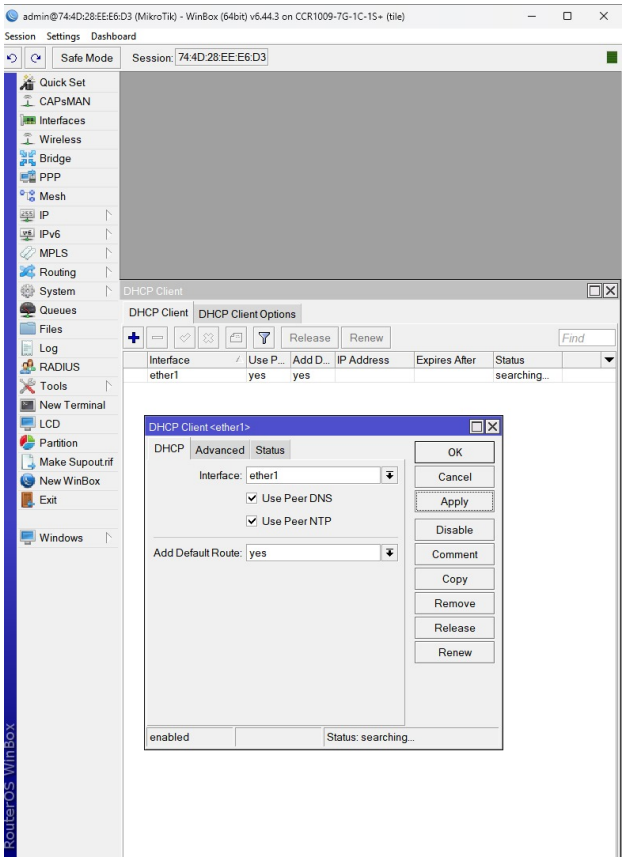
Tahap awal dalam praktikum ini adalah memastikan Router A berada dalam kondisi konfigurasi default guna menghindari potensi konflik pengaturan sebelumnya. Proses ini diawali dengan mengakses router menggunakan aplikasi Winbox. Setelah terhubung, navigasi dilakukan ke menu `System > Reset Configuration`. Penting untuk mengaktifkan opsi `"No Default Configuration"` dengan mencentangnya sebelum mengeksekusi perintah `"Reset Configuration"` untuk memulai proses reset.

Akses Router via Winbox

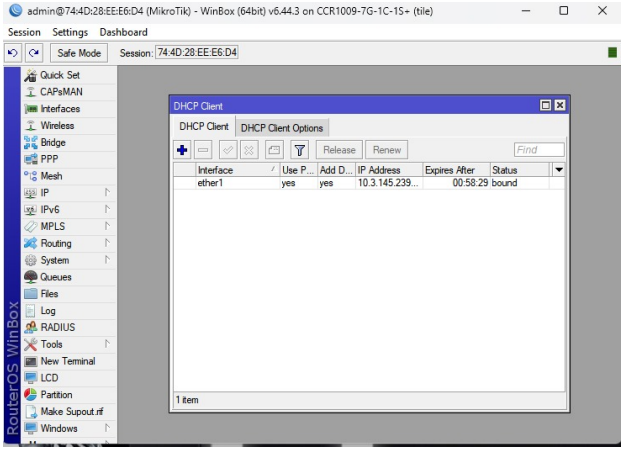
Setelah proses reset selesai, router dapat diakses kembali melalui aplikasi Winbox. Koneksi dapat dibangun baik melalui MAC address perangkat maupun alamat IP default. Login dilakukan menggunakan username `"admin"` tanpa kata sandi.

Konfigurasi DHCP Client pada Ether 1

Konektivitas internet Router A diinisiasi dengan menghubungkan kabel internet ke antarmuka `ether1`. Selanjutnya, konfigurasi DHCP Client dilakukan untuk memperoleh alamat IP secara otomatis dari penyedia layanan internet. Prosedur ini mencakup akses ke menu `IP > DHCP Client`, penambahan entri baru dengan memilih `"ether1"` sebagai antarmuka, dan aplikasi konfigurasi. Verifikasi keberhasilan ditandai dengan status koneksi yang menunjukkan `"bound"`.



Gambar 1: Konfigurasi DHCP Client pada Ether 1



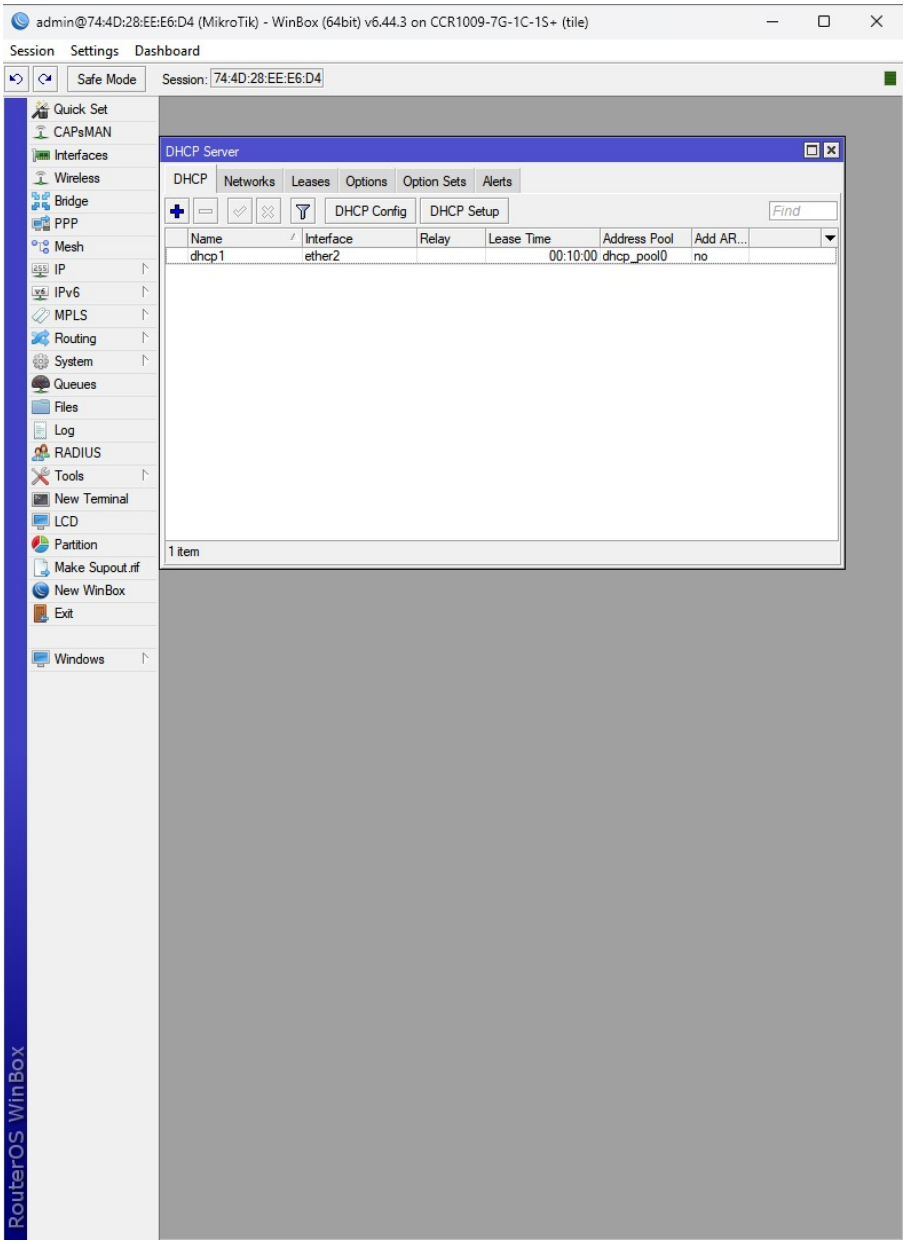
Gambar 2: Status DHCP Client "bound" pada Ether 1

Penambahan Alamat IP pada Ether 7

Untuk memfasilitasi konektivitas dengan jaringan lokal melalui Switch, alamat IP ditambahkan pada antarmuka `ether7` Router A. Prosedur ini melibatkan navigasi ke menu `IP > Addresses`, penambahan alamat IP `192.168.10.1/24`, dan pemilihan `"ether7"` sebagai antarmuka. Konfigurasi kemudian diterapkan dan disimpan.

Konfigurasi DHCP Server

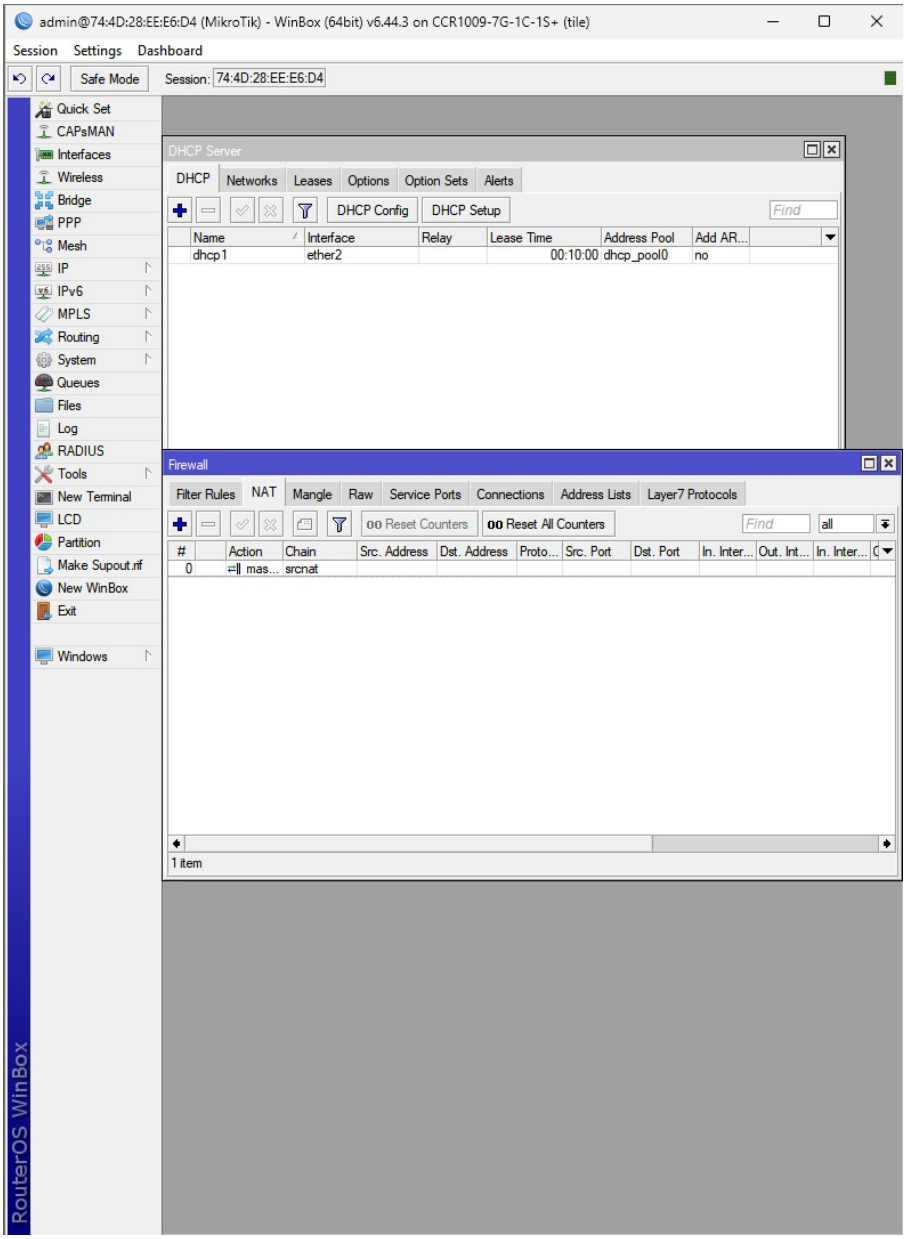
Distribusi alamat IP secara otomatis kepada perangkat klien di jaringan lokal dilakukan melalui konfigurasi DHCP Server pada Router A. Proses ini diawali dengan akses ke menu `IP > DHCP Server` dan penggunaan fitur `"DHCP Setup"`. Langkah-langkah selanjutnya meliputi pemilihan `"ether7"` sebagai antarmuka DHCP Server, verifikasi ruang alamat DHCP (`192.168.10.0/24`), penetapan gateway (`192.168.10.1`), penentuan rentang IP yang akan didistribusikan (`192.168.10.2-192.168.10.254`), serta konfigurasi DNS Server (`8.8.8.8` dan `8.8.4.4`) dan waktu lease (`00:10:00`). Konfigurasi berhasil apabila muncul pesan `"Setup has completed successfully"`.



Gambar 3: Tampilan Konfigurasi DHCP Server pada Router A

Konfigurasi NAT

NAT (Network Address Translation) dikonfigurasi untuk memungkinkan perangkat di jaringan lokal mengakses internet. Konfigurasi ini dilakukan melalui menu `IP > Firewall > NAT`. Aturan baru ditambahkan dengan Chain `"src-nat"` pada tab `"General"`, dan Action `"masquerade"` pada tab `"Action"`. Implementasi NAT ini esensial untuk penerjemahan alamat IP privat ke alamat IP publik.

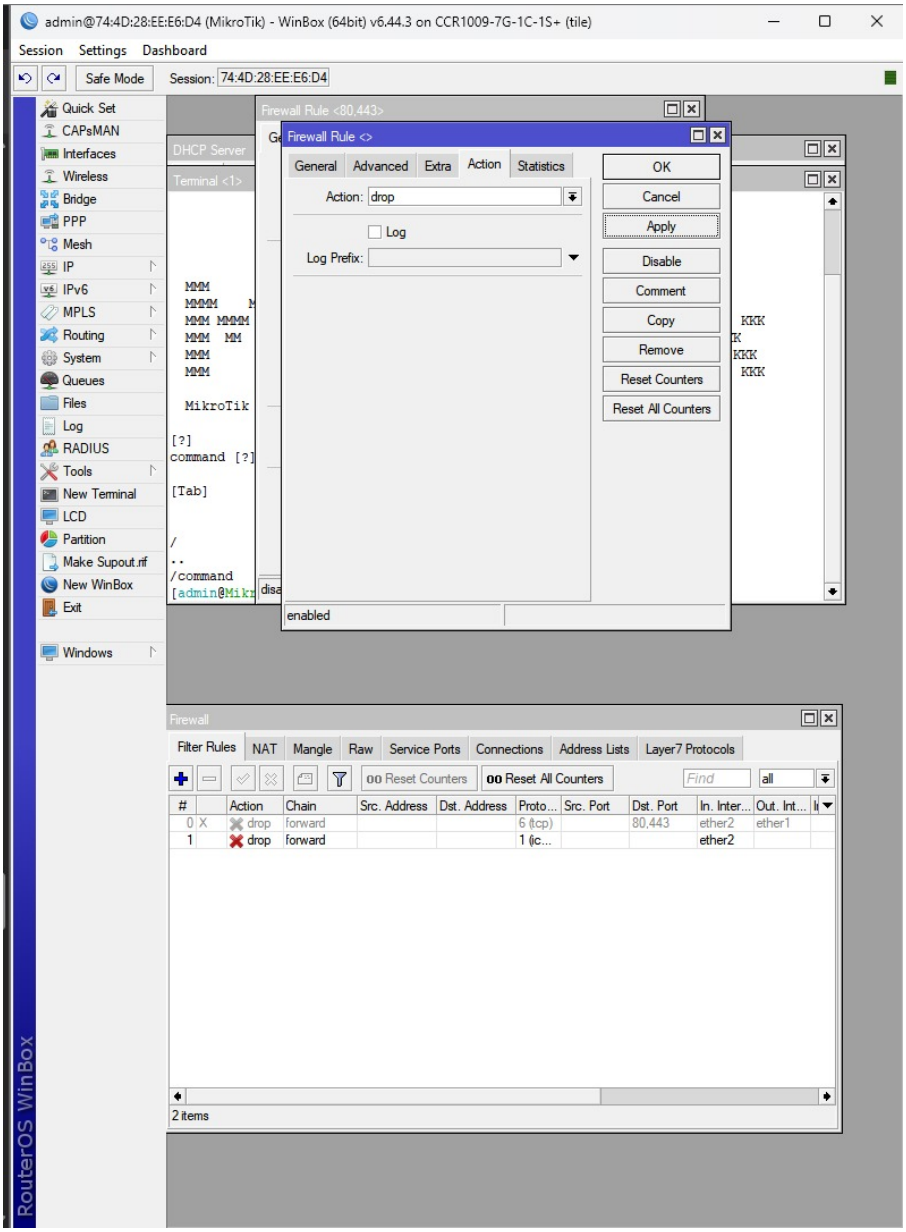


Gambar 4: Tampilan Konfigurasi NAT pada Router A

Konfigurasi Firewall (Filter Rules)

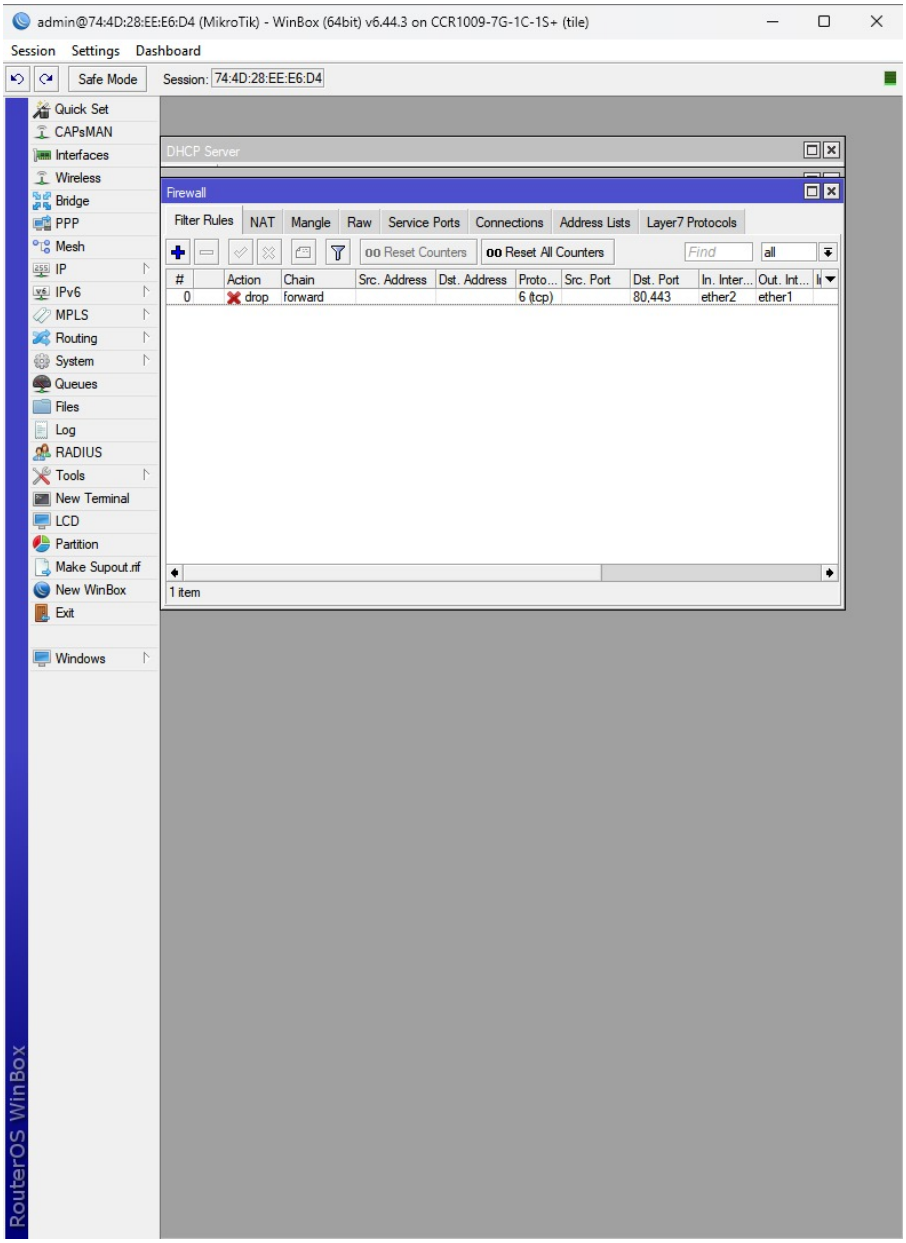
Penerapan aturan filter (Filter Rules) pada firewall bertujuan untuk mengatur lalu lintas jaringan dan meningkatkan keamanan. Ini diatur melalui menu `IP > Firewall > Filter Rule`.

Untuk pemblokiran ICMP (Internet Control Message Protocol), aturan baru ditambahkan dengan Chain `"forward"`, Protocol `"icmp"`, dan In. Interface `"ether7"` pada tab `"General"`. Pada tab `"Action"`, Action diatur menjadi `"drop"`. Konfigurasi ini dirancang untuk memblokir permintaan ping yang masuk dari jaringan lokal ke luar.



Gambar 5: Tampilan Konfigurasi Firewall untuk Pemblokiran ICMP

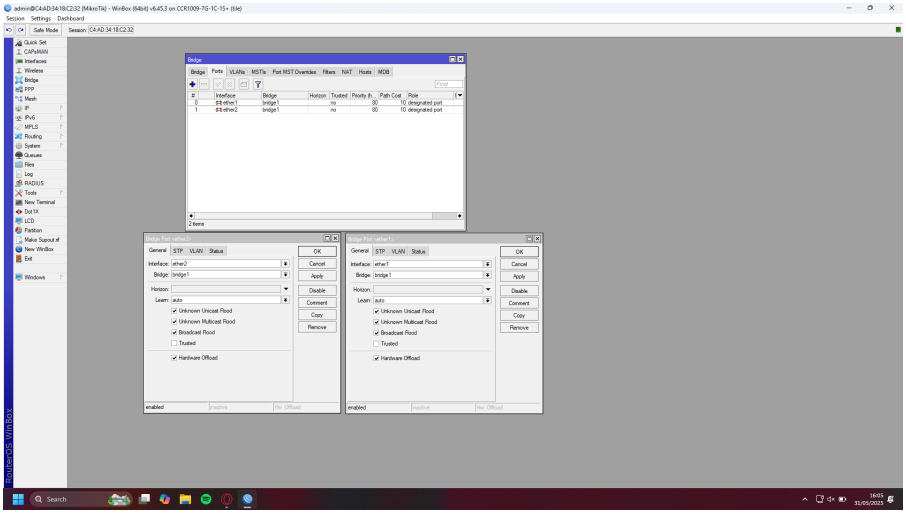
Selanjutnya, untuk pemblokiran akses situs web berdasarkan konten spesifik (misalnya, "speedtest"), aturan firewall lainnya ditambahkan. Aturan ini memiliki Chain `"forward"`, Protocol `"tcp"`, dan Dst. Port `"80,443"` pada tab `"General"`. In. Interface diatur ke `"ether7"` dan Out. Interface ke `"ether1"`. Pada tab `"Advanced"`, Content diatur ke `"speedtest"`, dan Action diatur menjadi `"drop"`. Aturan ini berfungsi untuk memblokir akses ke situs web yang mengandung kata kunci "speedtest" dalam lalu lintas HTTP/HTTPS.



Gambar 6: Tampilan Konfigurasi Firewall untuk Pemblokiran Konten "speedtest"

1.2 Konfigurasi Bridge pada Router B

Router B dikonfigurasi sebagai perangkat bridge untuk berfungsi sebagai hub yang mentransmisikan lalu lintas antar antarmuka tanpa melakukan routing. Konfigurasi ini diawali dengan mengakses menu `Bridge` dan membuat bridge baru. Setelah bridge berhasil dibuat, port-port yang terhubung ke perangkat laptop dan Router A ditambahkan ke dalam bridge melalui menu `Bridge > Port`.



Gambar 7: Tampilan Konfigurasi Bridge pada Router B

1.3 Konfigurasi Alamat IP pada Laptop

Sebagai bagian dari pengujian, konfigurasi alamat IP pada laptop diatur untuk memperoleh alamat secara otomatis melalui DHCP. Verifikasi perolehan alamat IP dilakukan dengan membuka Command Prompt (CMD) dan mengeksekusi perintah `ipconfig`.

2 Analisis Hasil Percobaan

Pengujian fungsionalitas NAT dan Firewall dilakukan setelah seluruh konfigurasi perangkat selesai. Analisis ini membahas hasil dari setiap pengujian yang dilakukan.

2.1 Pengujian Konektivitas (NAT)

Pengujian konektivitas internet dilakukan untuk memverifikasi fungsi NAT setelah konfigurasi DHCP Client, IP Addresses, DHCP Server, dan NAT pada Router A. Dengan mengeksekusi perintah `ping 8.8.8.8` dari Terminal Winbox, diperoleh balasan (`reply`) dari `8.8.8.8`. Hasil ini mengindikasikan bahwa Router A berhasil memperoleh koneksi internet dari penyedia layanan dan fungsi NAT berjalan dengan baik, memungkinkan penerjemahan alamat IP privat dari jaringan lokal ke alamat IP publik untuk akses internet.

2.2 Pengujian Firewall (ICMP)

Pengujian terhadap aturan pemblokiran ICMP (ping) dilakukan dari perangkat laptop ke internet. Tabel di bawah merangkum hasil pengujian:

Tabel 1: Hasil Pengujian Firewall ICMP

Kondisi Firewall	Tindakan/Perintah	Hasil
Firewall ICMP Aktif	`ping 8.8.8.8` dari Laptop	`Request Timed Out (RTO)`
Firewall ICMP Nonaktif	Aturan firewall ICMP didisable	Mendapatkan balasan (`reply`)

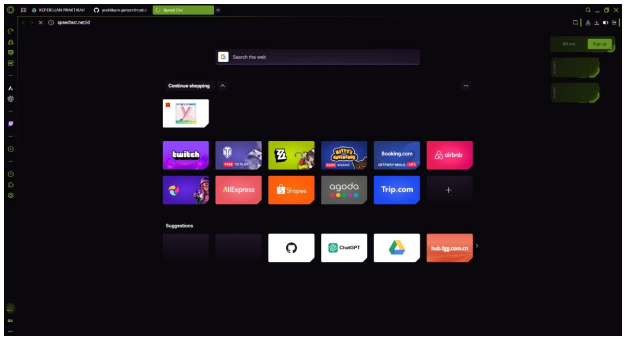
Berdasarkan hasil tersebut, dapat disimpulkan bahwa aturan firewall untuk ICMP berfungsi secara efektif. Ketika aturan aktif, lalu lintas ping berhasil diblokir, menghasilkan `Request Timed Out`. Sebaliknya, ketika aturan dinonaktifkan, lalu lintas ping diizinkan dan menghasilkan balasan normal. Hal ini memvalidasi kemampuan firewall dalam mengontrol lalu lintas ICMP.

2.3 Pengujian Firewall (Pemblokiran Konten)

Pengujian selanjutnya adalah verifikasi aturan pemblokiran situs web berdasarkan konten, khususnya kata kunci "speedtest". Tabel berikut menampilkan hasil pengujian:

Tabel 2: Hasil Pengujian Firewall Konten

Kondisi Firewall	**Tindakan/Perintah**	**Hasil**
Firewall Konten Aktif	Akses `www.speedtest.net` dari Laptop	Situs web tidak dapat diakses atau terus memuat tanpa menampilkan konten.
Firewall Konten Nonaktif	Aturan firewall konten di-disable	Situs web dapat diakses dengan normal, menampilkan hasil speedtest.



Gambar 8: Firewall konten aktif

Gambar 9: Firewall ketika konten nonaktif

Hasil pengujian ini mengkonfirmasi bahwa firewall konten berhasil memblokir akses ke situs web yang mengandung kata kunci "speedtest" saat aturan diaktifkan, dan mengizinkan akses normal ketika aturan dinonaktifkan. Ini menunjukkan efektivitas firewall dalam melakukan penyaringan konten berbasis kata kunci.

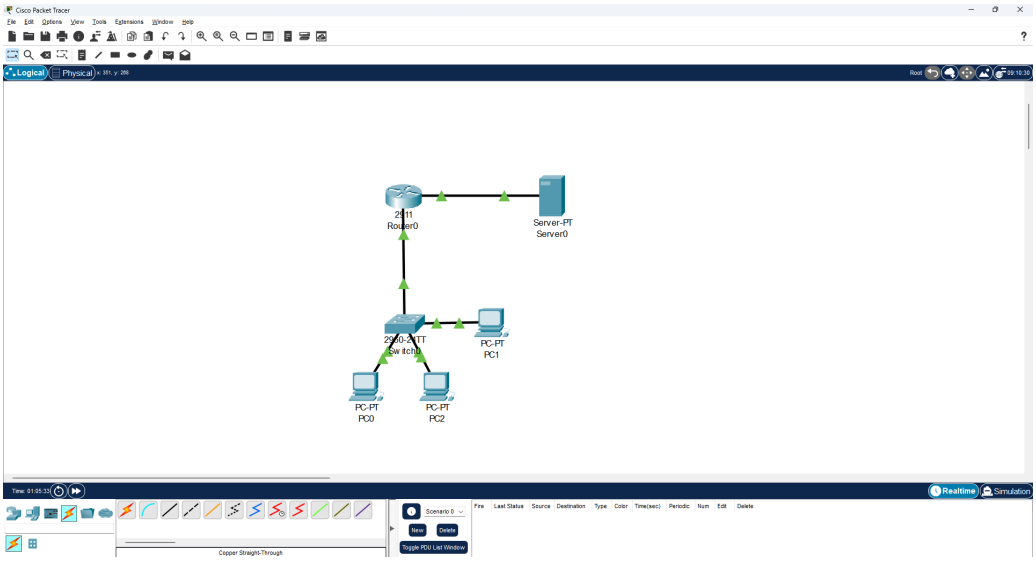
3 Hasil Tugas Modul

Tugas ini meliputi pembangunan topologi jaringan sederhana, konfigurasi NAT (Network Address Translation), dan implementasi firewall menggunakan Access Control Lists (ACLs) di Cisco Packet Tracer. Pengujian konektivitas dilakukan untuk memvalidasi setiap konfigurasi.

Topologi Jaringan

Topologi yang dibangun terdiri dari satu Router (`2911`), satu Switch (`2960`), tiga PC (`PC0`, `PC1`, `PC2`) yang terhubung dalam satu jaringan LAN, dan satu Server (`Server0`) yang disimulasikan sebagai internet/jaringan publik.

- **Router Interface Gig0/0 (LAN)**: `192.168.1.1/24`
- **Router Interface Gig0/1 (Public)**: `200.10.10.1/24`
- **PC0 IP**: `192.168.1.10/24`, Gateway: `192.168.1.1`
- **PC1 IP**: `192.168.1.11/24`, Gateway: `192.168.1.1`
- **PC2 IP**: `192.168.1.12/24`, Gateway: `192.168.1.1`
- **Server0 IP**: `200.10.10.2/24`, Gateway: `200.10.10.1`



Gambar 10: Diagram Topologi Jaringan

Konfigurasi NAT (Network Address Translation)

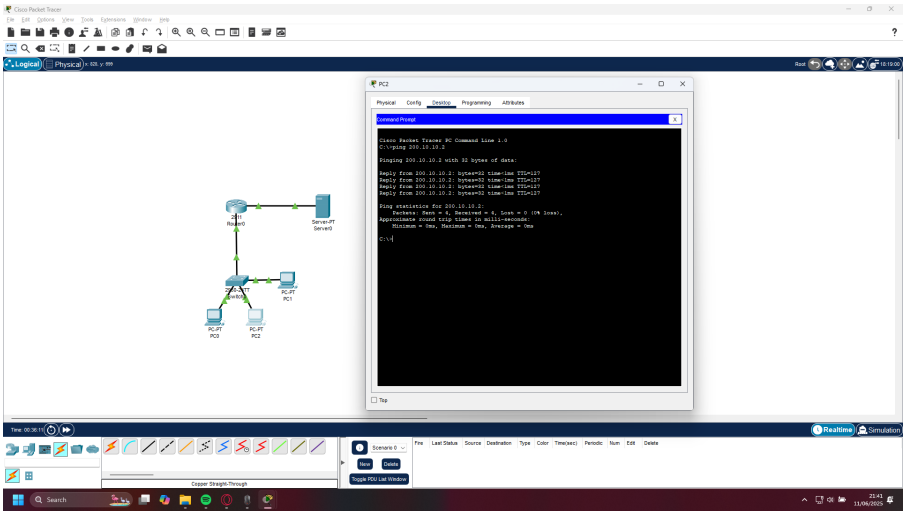
NAT dikonfigurasi untuk memungkinkan semua PC di jaringan LAN (IP private `192.168.1.x`) mengakses Server (`200.10.10.2`) menggunakan IP publik Router (`200.10.10.1`). Konfigurasi menggunakan NAT Overload (PAT) diterapkan pada Router.

- `access-list 1 permit 192.168.1.0 0.0.0.255`
- `ip nat inside source list 1 interface GigabitEthernet0/1 overload`
- `interface GigabitEthernet0/0`: `ip nat inside`
- `interface GigabitEthernet0/1`: `ip nat outside`

Hasil Pengujian Konektivitas Setelah NAT:

- PC0 → `ping 200.10.10.2`: **Berhasil**
- PC1 → `ping 200.10.10.2`: **Berhasil**
- PC2 → `ping 200.10.10.2`: **Berhasil**

Semua PC di LAN berhasil mengakses Server, memverifikasi fungsi NAT.



Gambar 11: Hasil Ping ke Server Setelah Konfigurasi NAT (Contoh dari PC2)

Konfigurasi Firewall (ACL)

Dua skenario ACL diimplementasikan dan diuji untuk mengontrol akses PC ke Server. ACL diterapkan pada `interface GigabitEthernet0/0` dengan arah `in` (masuk dari LAN ke router) untuk mengontrol lalu lintas yang keluar dari LAN.

Skenario 1: Izinkan Hanya PC1 Mengakses Server

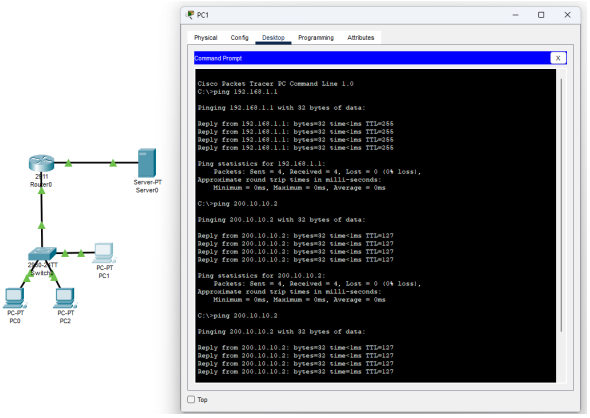
Dalam skenario ini, ACL dikonfigurasi untuk secara eksplisit mengizinkan hanya `PC1` (`192.168.1.11`) untuk mengakses `Server0` (`200.10.10.2`). Aturan `deny any` implisit pada ACL akan memblokir PC lainnya. Untuk skenario ini, NAT static digunakan untuk `PC1` agar tetap bisa berkomunikasi setelah ACL diaktifkan.

- `ip nat inside source static 192.168.1.11 200.10.10.1`
- `access-list 100 permit ip host 192.168.1.11 host 200.10.10.2`
- `access-list 100 deny ip any host 200.10.10.2`
- `interface GigabitEthernet0/0`: `ip access-group 100 in`

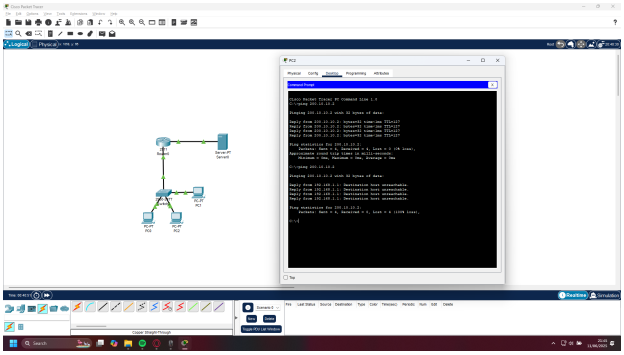
Hasil Pengujian Konektivitas Skenario 1:

- `PC1` → `ping 200.10.10.2`: **Berhasil**
- `PC0` → `ping 200.10.10.2`: **Gagal** (Request timed out)
- `PC2` → `ping 200.10.10.2`: **Gagal** (Request timed out)
- `PCx` → `ping 192.168.1.x` (antar PC LAN): **Berhasil** (Komunikasi LAN tidak terpengaruh)

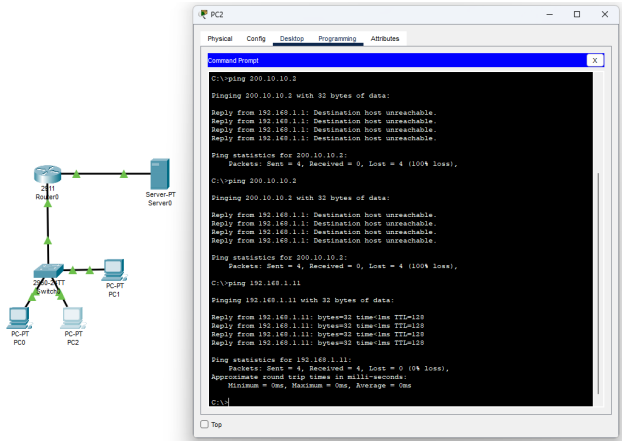
Pengujian ini menunjukkan bahwa hanya `PC1` yang diizinkan mengakses Server, sesuai dengan konfigurasi ACL.



Gambar 12: Hasil Ping dari PC1 ke Server (Skenario 1)



Gambar 13: Hasil Ping dari PC2 ke Server (Skenario 1 - Gagal)



Gambar 14: Hasil Ping Antar PC di LAN (Tidak Terpengaruh ACL)

Skenario 2: Blokir PC1 dan PC2 Mengakses Server

Pada skenario ini, ACL dikonfigurasi untuk secara eksplisit memblokir `PC1` (`192.168.1.11`) dan `PC2` (`192.168.1.12`) dari mengakses `Server0`. Aturan `permit ip any any` ditambahkan di akhir ACL untuk memastikan PC lainnya (`PC0`) tetap dapat mengakses Server. NAT overload untuk seluruh LAN diaktifkan kembali.

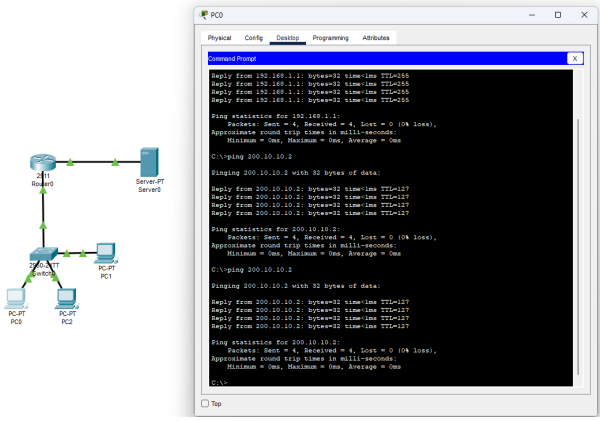
- `access-list 101 deny ip host 192.168.1.11 host 200.10.10.2`
- `access-list 101 deny ip host 192.168.1.12 host 200.10.10.2`
- `access-list 101 permit ip any any`
- `interface GigabitEthernet0/0`: `ip access-group 101 in`

Hasil Pengujian Konektivitas Skenario 2:

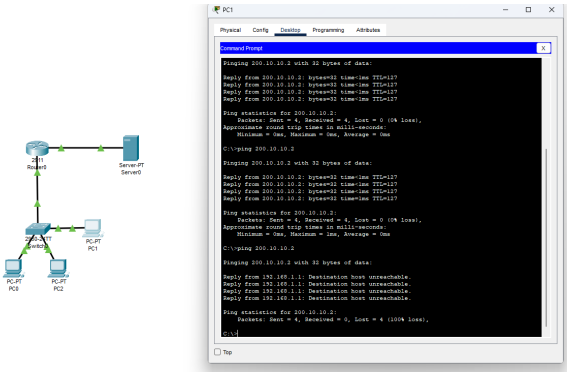
- `PC0` → `ping 200.10.10.2`: **Berhasil**
- `PC1` → `ping 200.10.10.2`: **Gagal** (Request timed out)
- `PC2` → `ping 200.10.10.2`: **Gagal** (Request timed out)

- `PCx` → `ping 192.168.1.x` (antar PC LAN): **Berhasil** (Komunikasi LAN tidak terpengaruh)

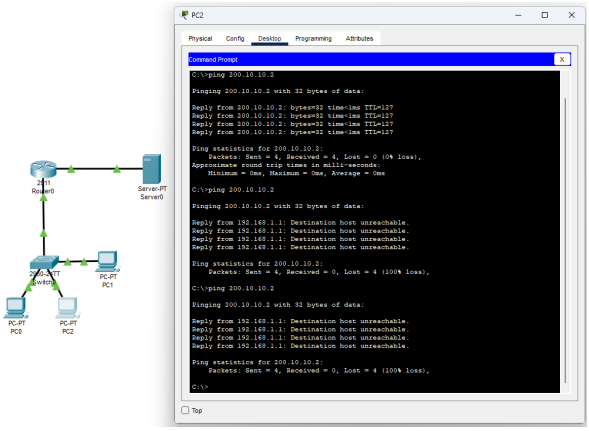
Hasil pengujian ini mengkonfirmasi bahwa `PC1` dan `PC2` berhasil diblokir dari mengakses Server, sementara `PC0` tetap memiliki akses, menunjukkan keefektifan ACL.



Gambar 15: Hasil Ping dari PC0 ke Server (Skenario 2)



Gambar 16: Hasil Ping dari PC1 ke Server (Skenario 2 - Gagal)



Gambar 17: Hasil Ping dari PC2 ke Server (Skenario 2 - Gagal)

3.1 Kesimpulan Hasil Tugas Modul

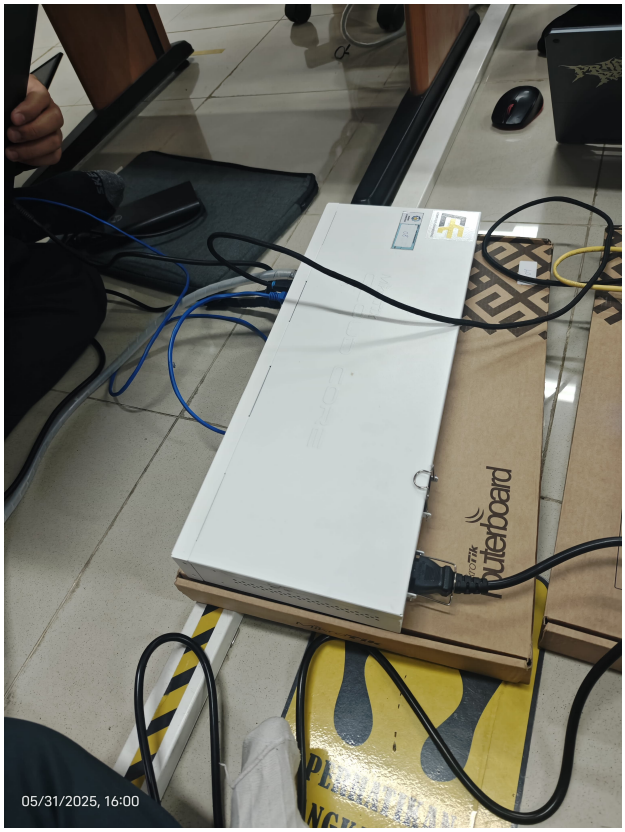
Berdasarkan serangkaian percobaan yang telah dilakukan, semua konfigurasi (topologi dasar, NAT, dan ACL) berhasil diimplementasikan dan diverifikasi di Cisco Packet Tracer. NAT berhasil memungkinkan komunikasi dari jaringan privat ke publik, dan ACLs secara efektif mengontrol akses spesifik antar perangkat, sekaligus mempertahankan konektivitas internal LAN.

4 Kesimpulan

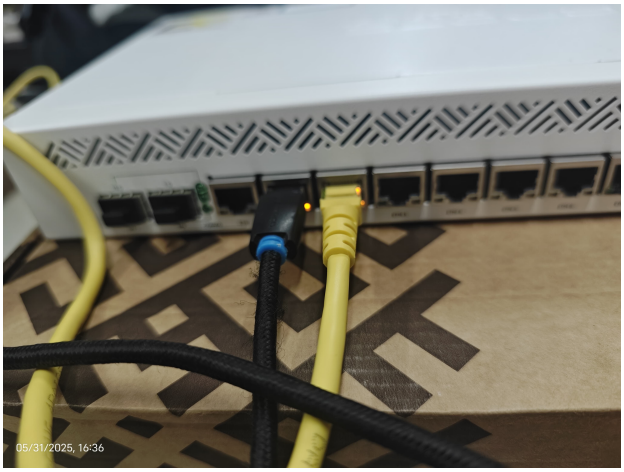
Praktikum ini berhasil mengimplementasikan dan memverifikasi fungsionalitas Network Address Translation (NAT) dan Firewall pada perangkat MikroTik RouterBoard. Konfigurasi NAT terbukti efektif dalam menyediakan konektivitas internet bagi perangkat di jaringan lokal. Sementara itu, implementasi Firewall dengan filter rules berhasil memblokir lalu lintas ICMP dan akses ke situs web yang mengandung konten spesifik. Router B juga berhasil dikonfigurasi sebagai bridge, memfasilitasi koneksi

perangkat ke jaringan lokal dan perolehan alamat IP dari DHCP Server di Router A. Secara keseluruhan, hasil pengujian menunjukkan bahwa seluruh konfigurasi yang dilakukan bekerja sesuai tujuan, menegaskan pemahaman komprehensif mengenai manajemen jaringan dasar dan keamanan.

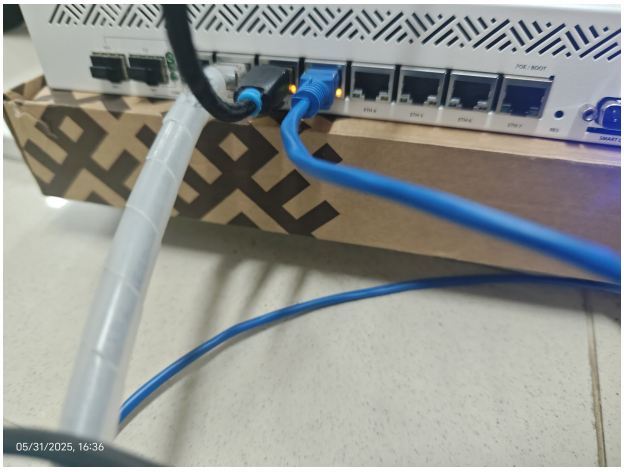
5 Lampiran



Gambar 18: Koneksi Kabel pada Router A



Gambar 19: Detail Koneksi Kabel Router B



Gambar 20: Detail Koneksi Kabel Router A