



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

Laporan Akhir Praktikum Jaringan Komputer

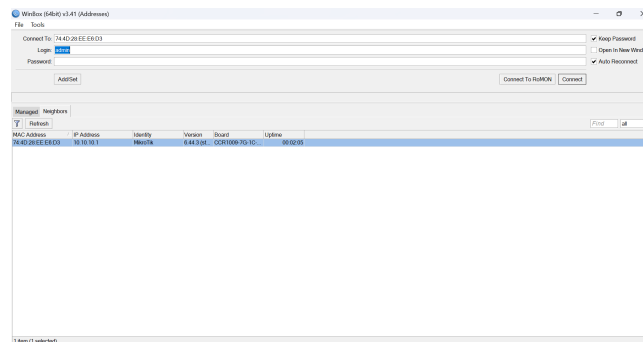
Jaringan Wireless

Ernita Kartika Weni - 5024231013

2025

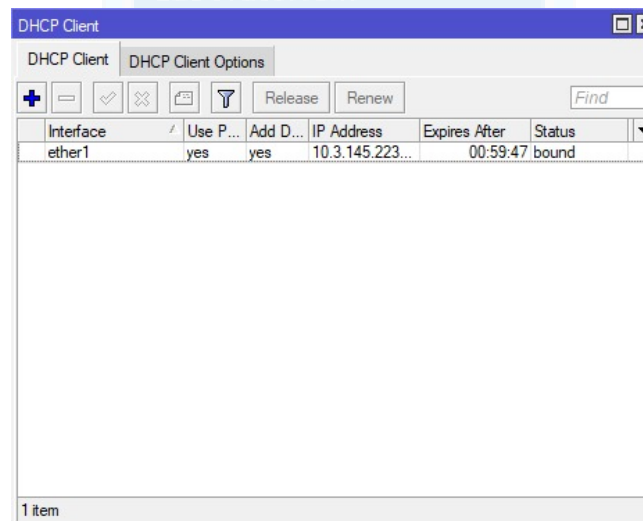
1 Langkah-Langkah Percobaan

1. Login ke Router Gunakan Winbox untuk mengakses router melalui MAC address tanpa password.



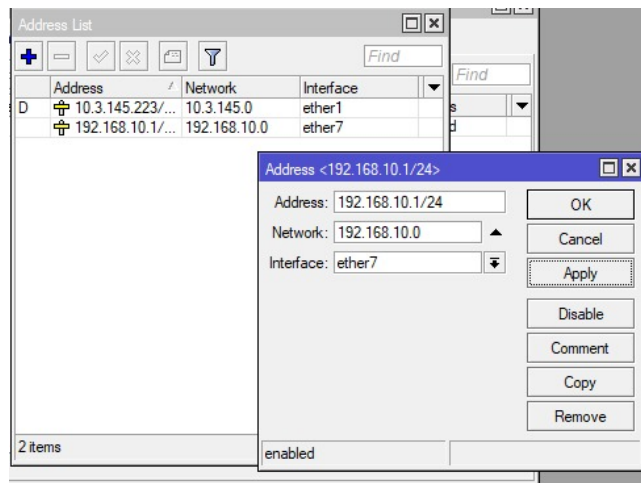
Gambar 1: Login ke Router melalui Winbox

2. Reset Router melalui winbox pada menu system → reset konfigurasi → cek list no default konfigurasi. Setelah sudah di reset, masuk kembali menggunakan MAC address.
3. Konfigurasi DHCP Client pada Router A interface ether 1. Konfigurasi di menu IP > DHCP Client. Klik ikon "+" untuk menambah entri baru selanjutnya pilih "ether1" sebagai interface lalu klik "Apply" dan pastikan status koneksi menunjukkan "bound".



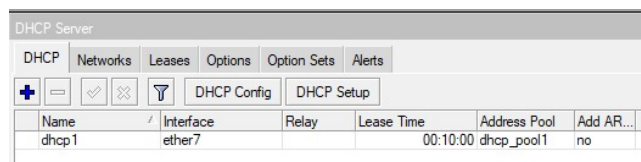
Gambar 2: Konfigurasi DHCP Client Router A untuk Ether 1

4. Konfigurasi IP address router A untuk interface ether 7. Konfigurasi pada menu IP > Addresses. Klik ikon "+" untuk menambahkan alamat IP. Selanjutnya Masukkan Address: 192.168.10.1/24 dan pilih Interface: "ether7" serta Klik "Apply" kemudian "OK".



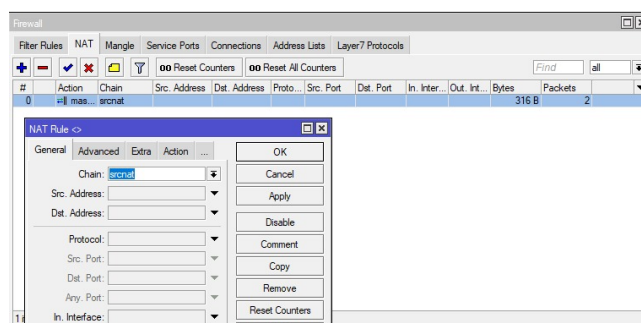
Gambar 3: Konfigurasi IP address Router A untuk Ether 7

- Konfigurasi DHCP Server pada Router untuk interface ether 7 supaya alamat IP dapat terdistribusi secara otomatis kepada perangkat client yang terhubung.

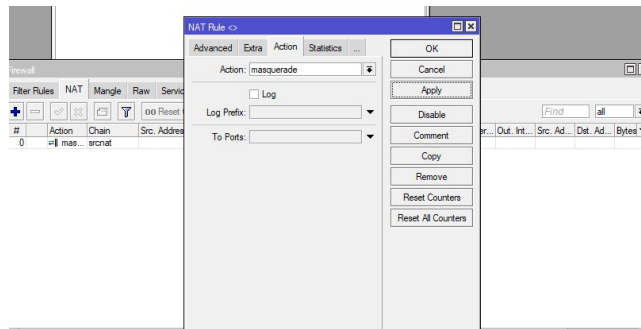


Gambar 4: Konfigurasi DHCP Server Router A untuk Ether 7

- Konfigurasi NAT (Network Address Translation) untuk menyediakan konektivitas internet. Konfigurasi pada menu IP > Firewall > NAT. Klik ikon "+" untuk membuat aturan baru selanjutnya pada tab "General", atur Chain: "src-nat". Pada tab "Action", atur Action: "masquerade" setelah itu klik "Apply" kemudian "OK".



Gambar 5: Konfigurasi NAT Tab General



Gambar 6: Konfigurasi NAT Tab Action

7. Konfigurasi Firewall

(a) Konfigurasi firewall untuk pemblokiran ICMP (Internet Control Message Protocol).

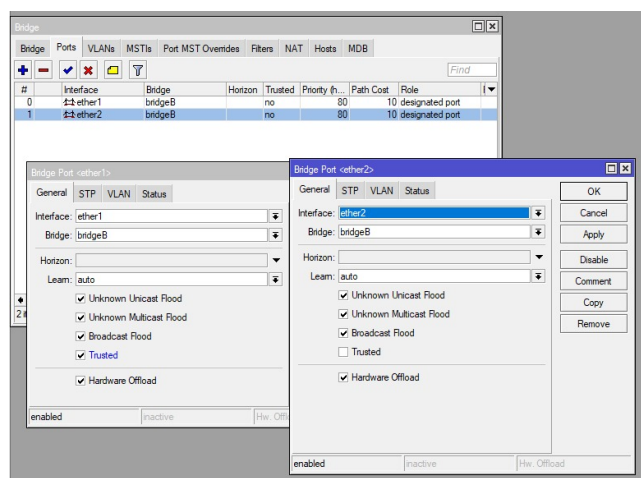
Konfigurasi firewall pada menu IP > Firewall > Filter Rule. Klik ikon "+" untuk menambahkan aturan baru. Pada tab "General", atur Chain: "forward"; Protocol: "icmp"; In. Interface: "ether7" dan pada tab "Action", atur Action: "drop".

(b) Konfigurasi firewall untuk Pemblokiran Akses Situs Web Berdasarkan Konten (Content Blocking).

Konfigurasi firewall pada menu IP > Firewall > Filter Rule. Klik ikon "+" untuk menambahkan aturan baru. Pada tab "General", atur Chain: "forward"; Protocol: "tcp"; Dst. Port: "80,443", In. Interface: "ether7", Out. Interface: "ether1", Content: "youtube" dan pada tab "Action", atur Action: "drop".

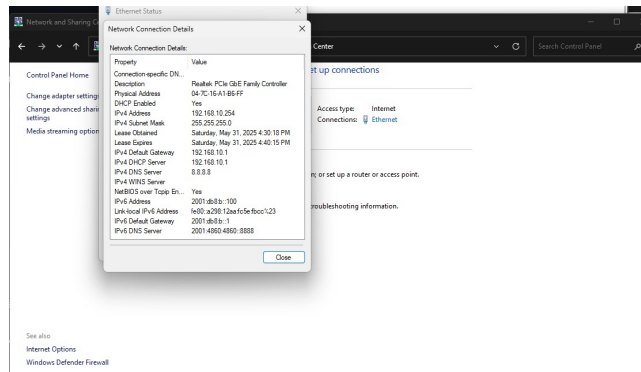
8. Selanjutnya konfigurasi bridge pada Router B untuk mengubah fungsi Router B menjadi hub. Konfigurasi bridge pada menu Bridge. Klik ikon "+" untuk membuat bridge baru selanjutnya klik "Apply" kemudian "OK".

9. Setelah membuat bridge dilanjutkan dengan menambahkan port ke dalam bridge yang telah dibuat. Port ditambahkan pada menu Bridge > Port. Klik ikon "+" untuk menambahkan port selanjutnya pilih interface yang terhubung ke perangkat laptop serta interface yang terhubung ke Router A yaitu ether1 dan ether2.



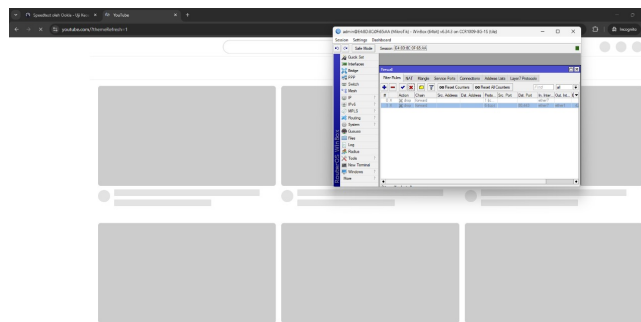
Gambar 7: Konfigurasi Bridge Router B

10. Konfigurasi IP address pada laptop secara otomatis melalui DHCP, selanjutnya mengverifikasi alamat IP yang diperoleh.

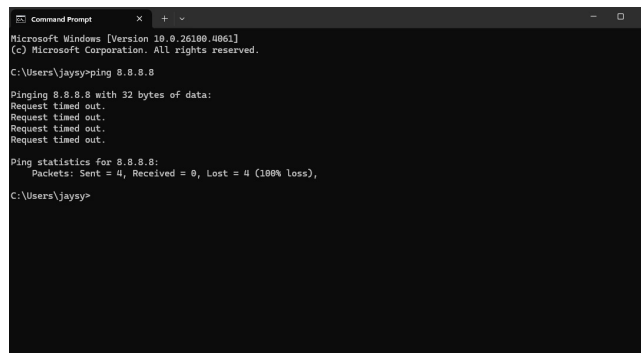


Gambar 8: Konfigurasi IP address melalui DHCP pada laptop

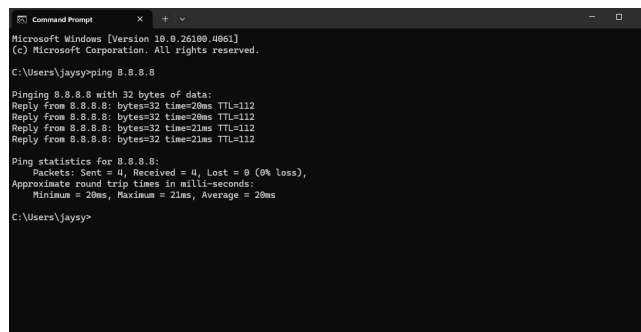
11. Pengujian



Gambar 9: Pengujian Pemblokiran Konten



Gambar 10: Pengujian Konektivitas (ICMP) Firewall Aktif

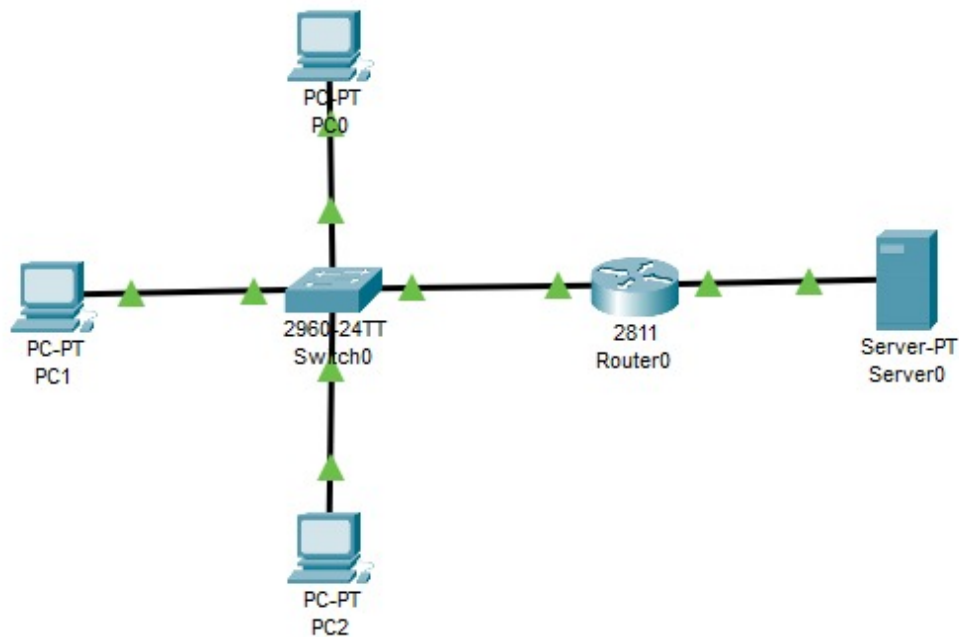


Gambar 11: Pengujian Konektivitas (ICMP) Firewall Tidak Aktif

2 Analisis Hasil Percobaan

Berdasarkan langkah-langkah konfigurasi yang telah dilakukan, seluruh tahapan berhasil dilaksanakan dengan baik sesuai dengan tujuan yang telah ditetapkan, yaitu membangun jaringan dengan distribusi IP otomatis, konektivitas internet, serta implementasi firewall untuk kontrol lalu lintas jaringan. Pada tahap awal, proses login dan reset konfigurasi router berjalan tanpa kendala. Konfigurasi DHCP Client pada interface ether1 memungkinkan Router A untuk memperoleh alamat IP dari sumber jaringan utama. Selanjutnya, konfigurasi IP statis dan DHCP Server pada interface ether7 berhasil memungkinkan perangkat klien (laptop) memperoleh IP secara otomatis. Implementasi NAT pada Router A juga telah berhasil, dibuktikan dengan perangkat klien yang dapat mengakses internet. Selain itu, konfigurasi bridge pada Router B berhasil mengubah fungsinya menjadi hub, memungkinkan perangkat klien tetap terhubung ke jaringan meskipun melalui perantara Router B. Pengujian firewall menunjukkan hasil yang sesuai. Aturan filter rule untuk pemblokiran protokol ICMP efektif memblokir permintaan ping dari perangkat klien ke internet saat firewall dalam kondisi aktif, dan sebaliknya saat firewall dinonaktifkan. Namun, terdapat kendala pada saat melakukan konfigurasi firewall untuk pemblokiran konten. Awalnya, pengujian pemblokiran konten direncanakan menggunakan layanan speedtest.net. Akan tetapi, mekanisme pemuatan konten situs tersebut tidak terdeteksi oleh fitur content filtering pada MikroTik RouterOS. Oleh karena itu, situs youtube.com dipilih sebagai alternatif untuk pengujian. Setelah aturan firewall dikonfigurasi dengan parameter konten berisi kata kunci "youtube", pengujian menunjukkan bahwa pemblokiran berhasil, yang ditandai dengan kegagalan akses ke situs tersebut. Secara keseluruhan, konfigurasi jaringan yang dilakukan dapat berfungsi dengan baik sesuai dengan skenario yang dirancang, dengan satu penyesuaian minor pada bagian pemblokiran konten situs.

3 Hasil Tugas Modul



Gambar 12: Hasil Tugas Modul

4 Kesimpulan

Konfigurasi DHCP Client dan DHCP Server berhasil dilakukan sehingga perangkat klien dapat memperoleh alamat IP secara otomatis. Implementasi Network Address Translation (NAT) juga berhasil memberikan akses internet kepada klien yang terhubung ke jaringan lokal. Selain itu, konfigurasi bridge pada Router B mampu mengubah fungsinya menjadi hub, yang memungkinkan lalu lintas jaringan dapat diteruskan tanpa proses routing. Penerapan firewall untuk pemblokiran protokol ICMP dan konten situs juga berjalan sesuai dengan harapan, menunjukkan efektivitas fitur keamanan yang dimiliki oleh MikroTik. Kendala yang ditemui dalam pengujian pemblokiran konten terhadap situs speedtest.net diselesaikan dengan mengganti target pemblokiran menjadi situs youtube.com, yang kemudian berhasil diblokir oleh sistem.

5 Lampiran

5.1 Dokumentasi saat praktikum



Gambar 13: Dokumentasi Praktikum