

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

Laporan Akhir Praktikum Jaringan Komputer

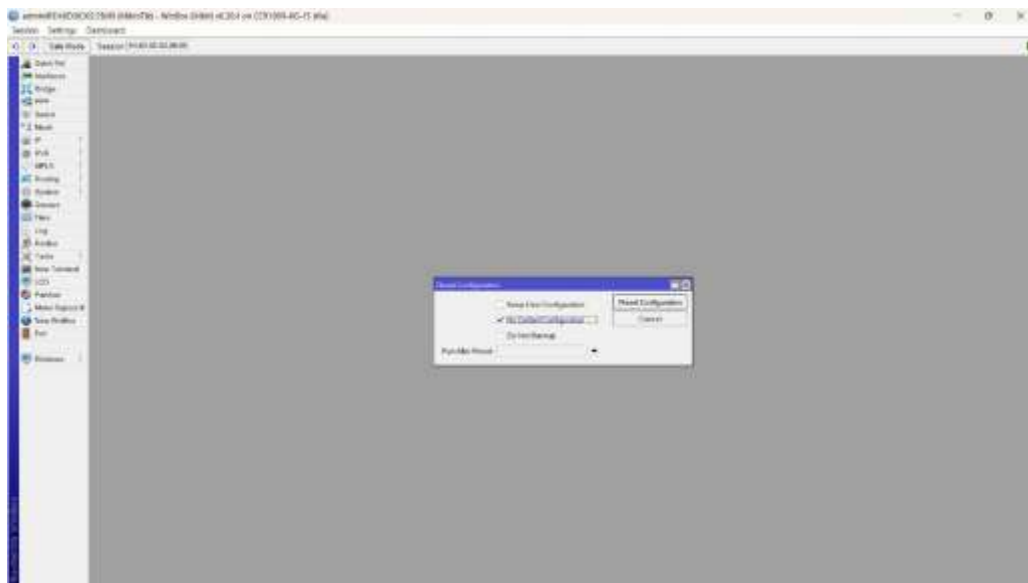
Firewall & NAT

Theo Kawalisa Pinem - 5024231008

2025

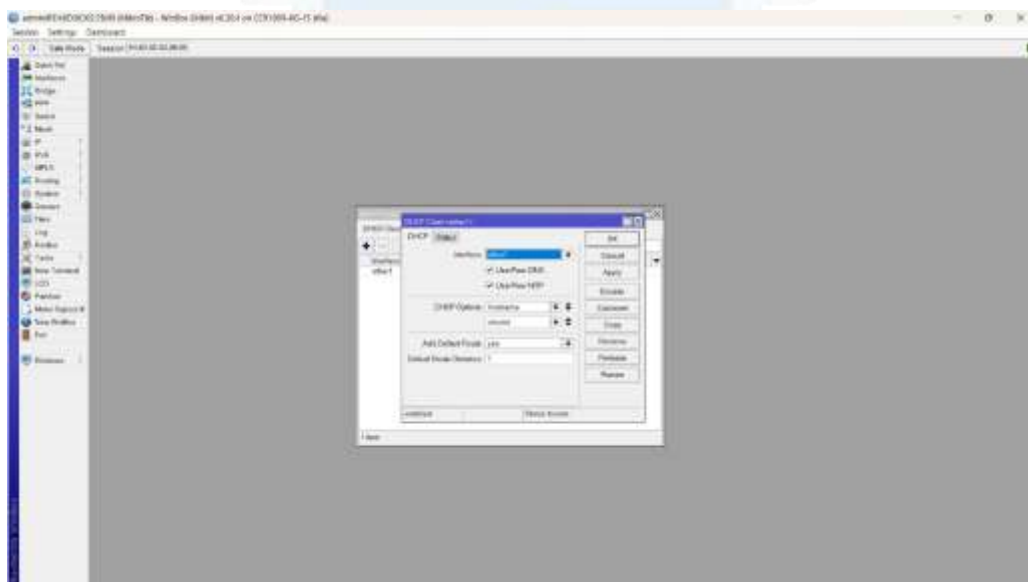
1 Langkah-Langkah Percobaan

Praktikum ini dimulai dengan menghubungkan dua laptop dengan dua router menggunakan kabel LAN, kemudian lakukan login, namun kita melakukan reset dulu terhadap router sebelum digunakan.



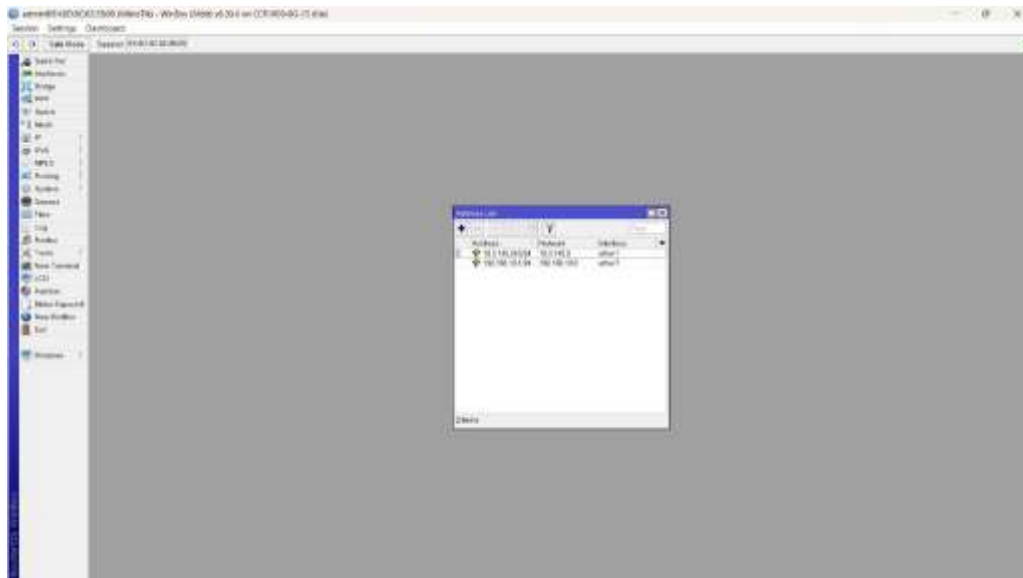
Gambar 1: Reset Konfigurasi Router

Setelah router di reset, sambungkan kabel internet ke ether 1 pada Router A dan lakukan konfigurasi DHCP Client dengan cara mengakses menu IP -> DHCP Client, kemudian klik ikon "+", dan pilih ether1 sebagai interface dan klik "apply" serta pastikan status koneksi sudah dalam "bound".



Gambar 2: Konfigurasi DHCP Client pada Router A

Lalu tambahkan alamat IP pada ether7 yang dimana adalah konektivitas dengan Switch atau Router B dengan ke menu IP lalu Addresses, klik ikon "+", masukkan address 192.168.10.1/24, pilih interface ether7 dan klik "apply" kemudian "ok".



Gambar 3: Penambahan Alamat IP pada Ether 7

Kemudian lakukan konfigurasi DHCP Server dengan cara mengakses menu IP, lalu DHCP server, klik tombol "DHCP Setup" dan pastikan konfigurasinya sudah sesuai pada gambar - gambar berikut ini.



Gambar 4: Konfigurasi Interface



Gambar 5: Konfigurasi Address Space



Gambar 6: Konfigurasi Gateway



Gambar 7: Konfigurasi Address to Give Out

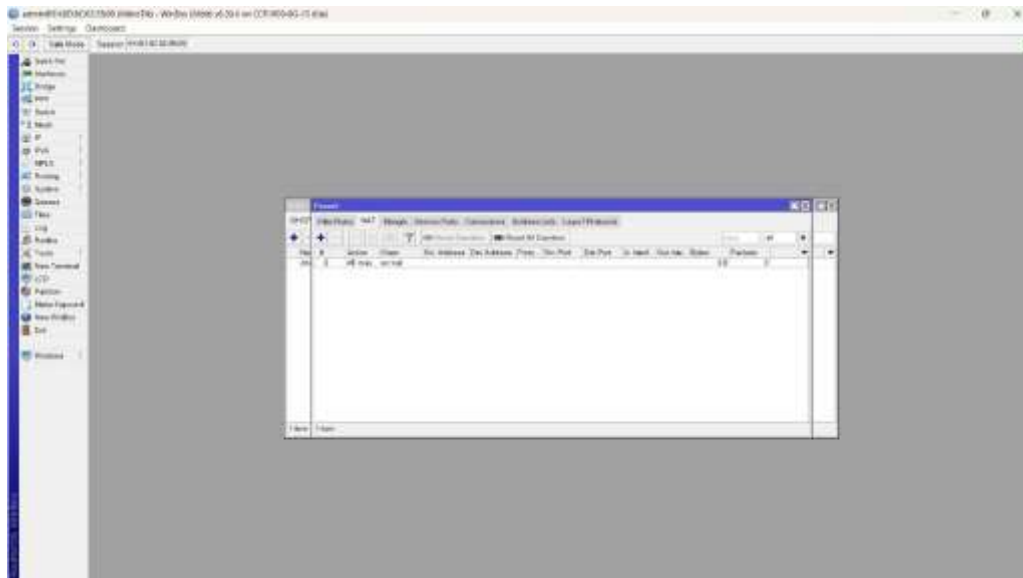


Gambar 8: Konfigurasi DNS



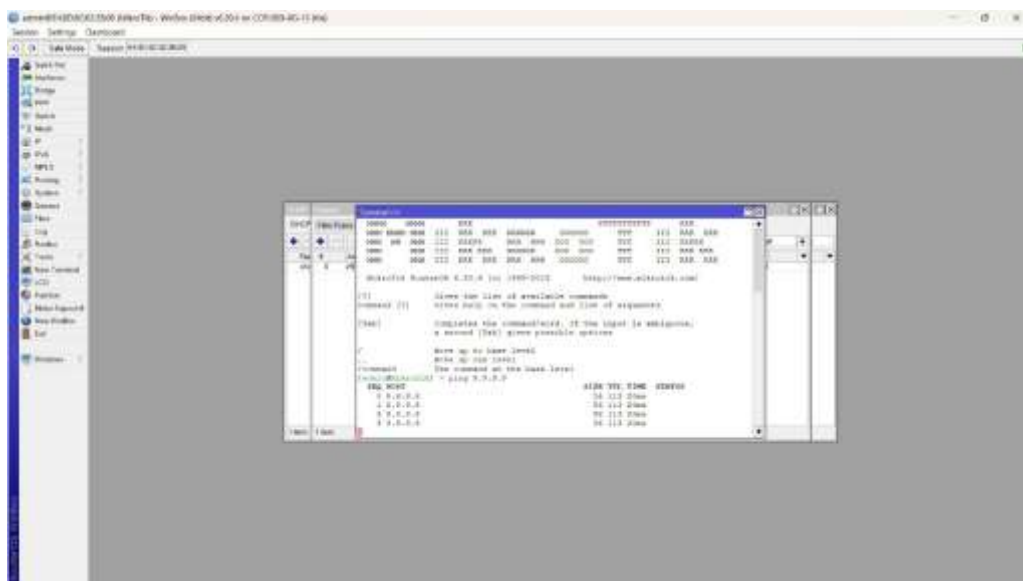
Gambar 9: Konfigurasi Lease Time

Lalu lakukan konfigurasi NAT dengan mengakses menu IP lalu Firewall lalu NAT, klik ikon "+", pada tab "General", atur menjadi "src-nat", pada tab "Action", atur menjadi "masquarade", klik "apply" dan "ok".



Gambar 10: Konfigurasi NAT

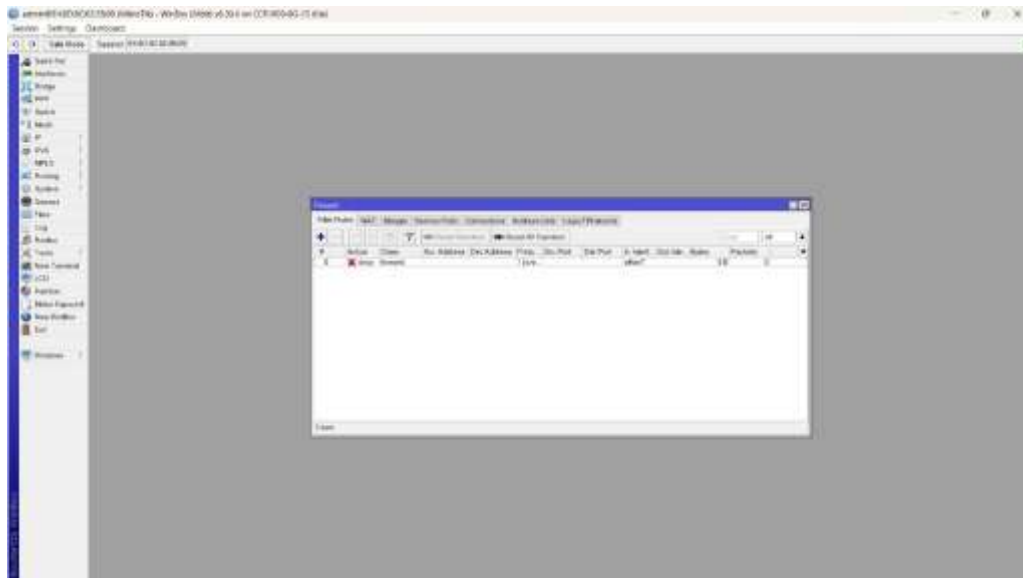
Kemudian lakukan tes koneksi dengan membuka terminal baru dan lakukan ping dengan ping 8.8.8.8.



Gambar 11: Tes Koneksi

Lalu lakukan konfigurasi firewall dengan mengakses menu IP, lalu firewall, lalu filter rule dan klik ikon "+". Untuk pemblokiran ICMP bisa dilakukan dengan mengatur :

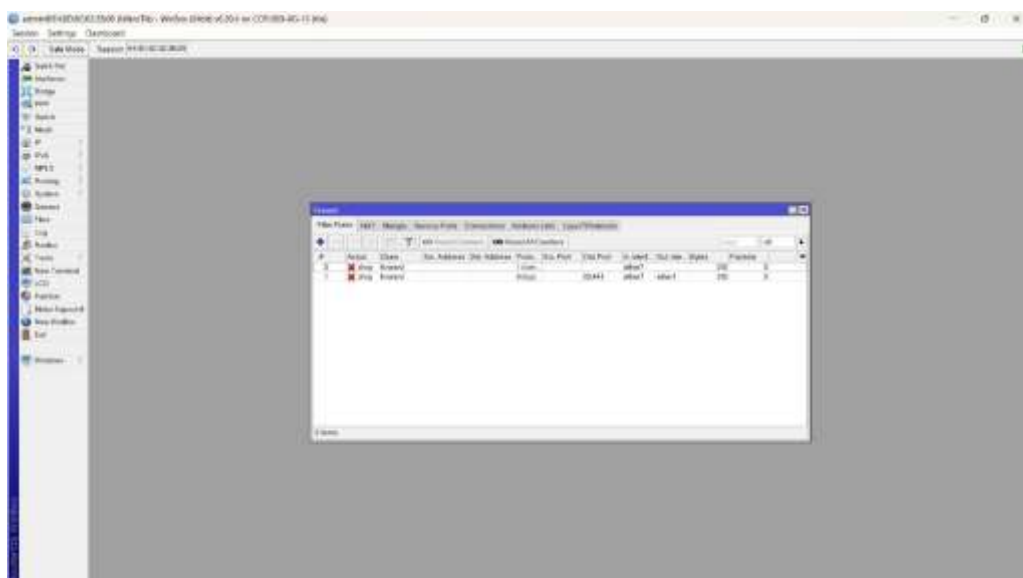
1. Pada tab "General", atur Chain: "forward".
2. Pada tab "General", atur Protocol: "icmp".
3. Pada tab "General", atur In. Interface: "ether7".
4. Pada tab "Action", atur Action: "drop".



Gambar 12: Konfigurasi Pemblokiran ICMP

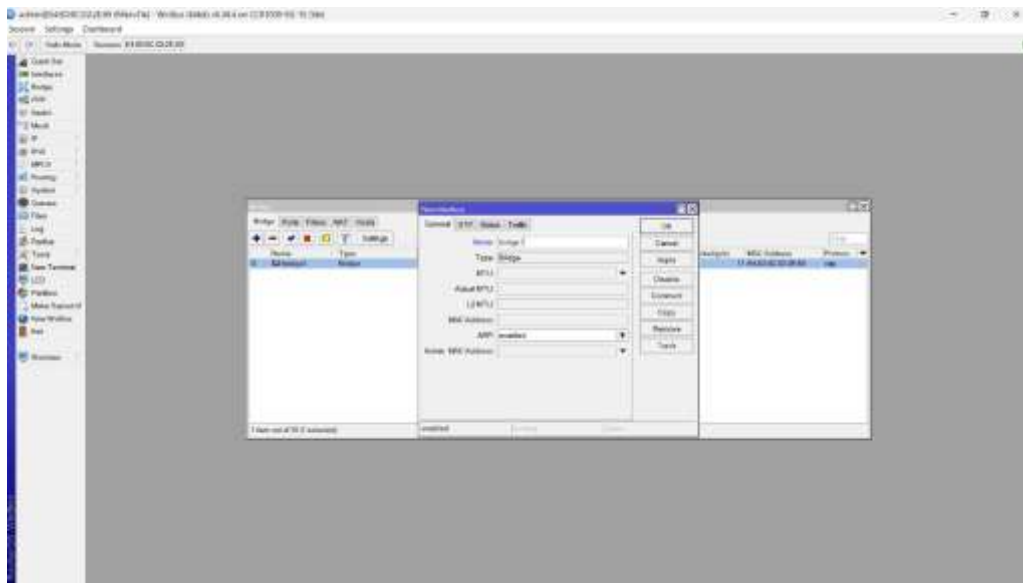
Untuk pemblokiran akses situs web berdasarkan konten atau content blocking bisa dengan mengatur :

1. Pada tab "General", atur Chain: "forward".
2. Pada tab "General", atur Protocol: "tcp".
3. Pada tab "General", atur Dst. Port: "80,443".
4. Pada tab "General", atur In. Interface: "ether7".
5. Pada tab "General", atur Out. Interface: "ether1".
6. Pada tab "Advanced", atur Content: "speedtest".
7. Pada tab "Action", atur Action: "drop".



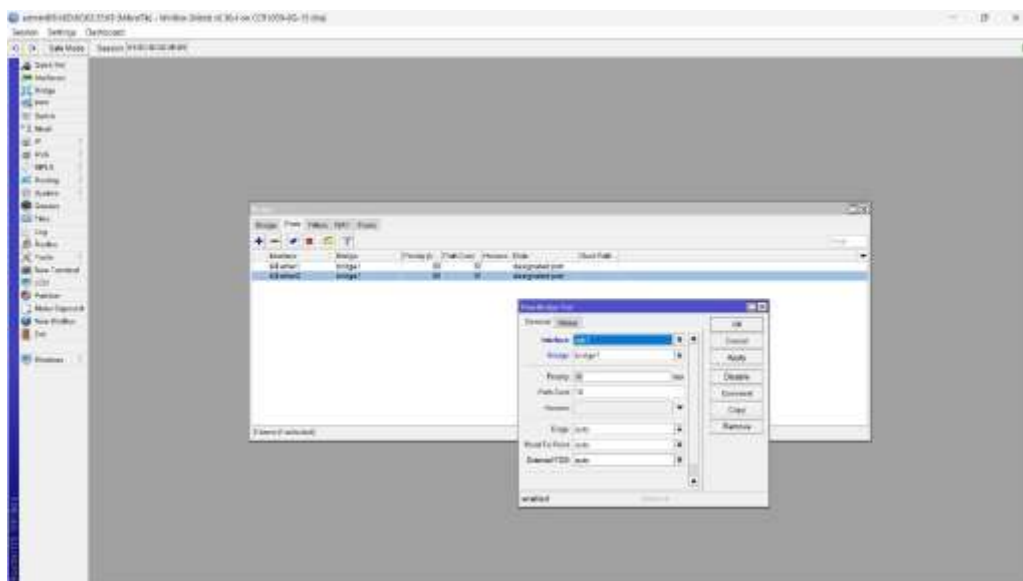
Gambar 13: Konfigurasi Content Blocking

Kemudian lakukan konfigurasi bridge pada Router B (Hub) dengan mengakses menu bridge, klik "+", "apply", dan "ok".



Gambar 14: Konfigurasi Bridge pada Router B

Lalu tambahkan port dalam bridge yang sudah dibuat dengan mengakses menu bridge lalu port, klik "+", pilih interface yang terhubung ke perangkat laptop, dan pilih interface yangn terhubung ke Router A.



Gambar 15: Konfigurasi Port dalam Bridge

Setelah itu, lakukan konfigurasi alamat IP pada laptop dengan IP yang sudah diatur tadi dan lakukan ping untuk menguji konektivitas ICMP dengan ping 8.8.8.8 pada command prompt.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\user> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=28ms TTL=112
Reply from 8.8.8.8: bytes=32 time=28ms TTL=112
Reply from 8.8.8.8: bytes=32 time=28ms TTL=112
Reply from 8.8.8.8: bytes=32 time=28ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 28ms, Average = 28ms
PS C:\Users\user>
```

Gambar 16: Pengujian Konektivitas ICMP

Hasil menunjukkan Request Timed Out (RTO) yang menandakan firewall sudah aktif. Untuk pengujian pemblokiran konten bisa dilakukan dengan melakukan browsing speedtest seperti pada gambar berikut.

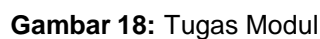


Gambar 17: Pengujian Content Blocking

2 Analisis Hasil Percobaan

Selama praktikum, semua tahapan konfigurasi berhasil dijalankan sesuai petunjuk. Setelah dilakukan pengaturan DHCP, NAT, dan firewall, perangkat klien bisa mendapatkan IP secara otomatis dan

3 Hasil Tugas Modul



7

5 Lampiran

5.1 Dokumentasi saat praktikum

