



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

Laporan Akhir Praktikum Jaringan Komputer

Firewall & NAT

Ahmad Faiq Fawwaz - 5024231032

2025

1 Langkah-Langkah Percobaan

2 Langkah-Langkah Percobaan

1. Reset Router

Pastikan perangkat router telah dikembalikan ke konfigurasi awal untuk mencegah potensi konflik dalam pengaturan selanjutnya.

- Akses router menggunakan aplikasi Winbox.
- Navigasikan ke menu System > Reset Configuration.
- Aktifkan opsi No Default Configuration dengan mencentangnya.
- Klik Reset Configuration untuk memulai proses reset.

2. Login ke Router

Lakukan proses login untuk mengakses antarmuka router.

- Gunakan Winbox untuk melakukan koneksi ke router.
- Login dapat dilakukan melalui MAC address atau IP default perangkat.
- Gunakan username admin (kata sandi tidak diperlukan jika belum diatur).

3. Konfigurasi DHCP Client pada Router A (Ether1)

Sambungkan kabel internet ke ether1 pada Router A, kemudian lakukan konfigurasi DHCP Client.

- Akses menu IP > DHCP Client.
- Klik ikon + untuk menambah entri baru.
- Pilih ether1 sebagai interface.
- Klik Apply dan pastikan status koneksi menunjukkan bound.

4. Penambahan Alamat IP pada Ether7

Tambahkan alamat IP pada ether7 untuk konektivitas dengan Switch.

- Navigasikan ke menu IP > Addresses.
- Klik ikon + untuk menambahkan alamat IP.
- Masukkan Address: 192.168.10.1/24.
- Pilih Interface: ether7.
- Klik Apply kemudian OK.

5. Konfigurasi DHCP Server pada Router MikroTik

Konfigurasi DHCP Server digunakan untuk secara otomatis mendistribusikan alamat IP kepada perangkat klien.

- Akses menu IP > DHCP Server.

- Klik tombol DHCP Setup.
- Pilih interface ether7, klik Next.
- Verifikasi network address: 192.168.10.0/24, klik Next.
- Verifikasi gateway: 192.168.10.1, klik Next.
- Tentukan rentang IP: 192.168.10.2-192.168.10.254, klik Next.
- Masukkan DNS Server: 8.8.8.8 dan 8.8.4.4, klik Next.
- Atur lease time: 00:10:00, klik Next.
- Setelah selesai, klik OK.

6. Konfigurasi NAT

Lakukan konfigurasi NAT (Network Address Translation) untuk menyediakan konektivitas internet.

- Akses menu IP > Firewall > NAT.
- Klik ikon + untuk membuat aturan baru.
- Pada tab General, atur Chain: src-nat.
- Pada tab Action, atur Action: masquerade.
- Klik Apply kemudian OK.
- Untuk uji koneksi, buka terminal di Winbox dan gunakan perintah ping 8.8.8.8.

7. Konfigurasi Firewall

Tambahkan aturan filter (Filter Rules) pada firewall.

- **Pemblokiran ICMP:**
 - Akses menu IP > Firewall > Filter Rule.
 - Klik ikon + untuk menambahkan aturan baru.
 - Pada tab General, atur Chain: forward, Protocol: icmp, dan In. Interface: ether7.
 - Pada tab Action, atur Action: drop.
- **Pemblokiran Konten Web (Content Blocking):**
 - Tambahkan aturan baru pada tab Filter Rule.
 - Pada tab General, atur Chain: forward, Protocol: tcp, Dst. Port: 80,443, In. Interface: ether7, dan Out. Interface: ether1.
 - Pada tab Advanced, atur Content: speedtest.
 - Pada tab Action, atur Action: drop.

8. Konfigurasi Bridge pada Router B

Lakukan konfigurasi bridge untuk menjadikan Router B sebagai hub.

- Akses menu Bridge.
- Klik ikon + untuk membuat bridge baru, lalu klik Apply dan OK.
- Akses menu Bridge > Port.

- Tambahkan interface yang terhubung ke perangkat laptop dan interface yang terhubung ke Router A.

9. Konfigurasi Alamat IP pada Laptop

- Atur pengaturan jaringan pada laptop agar menggunakan DHCP (otomatis).
- Buka Command Prompt (CMD).
- Gunakan perintah `ipconfig` untuk memverifikasi alamat IP yang diperoleh.

10. Uji Coba Konfigurasi

- **Pengujian Konektivitas (ICMP):**
 - Buka terminal pada laptop.
 - Jalankan perintah `ping 8.8.8.8`.
 - Jika firewall ICMP aktif, hasil yang diharapkan adalah `Request Timed Out`.
 - Nonaktifkan aturan firewall ICMP dengan menekan tanda "X" (disable).
 - Ulangi ping untuk memastikan koneksi berhasil.
- **Pengujian Pemblokiran Konten Web:**
 - Akses situs web dengan kata kunci `speedtest` (misalnya: `www.speedtest.net`).
 - Jika firewall konten aktif, akses akan gagal atau tidak memuat sempurna.
 - Nonaktifkan aturan firewall konten untuk menguji akses normal kembali.

3 Analisis Hasil Percobaan

Dari hasil percobaan yang dilakukan, dapat disimpulkan bahwa seluruh tahapan konfigurasi router MikroTik berjalan dengan baik dan sesuai ekspektasi. Proses reset router memastikan perangkat dalam kondisi bersih tanpa konfigurasi sebelumnya, sehingga meminimalkan potensi konflik konfigurasi. Proses login melalui Winbox juga tidak mengalami kendala, memungkinkan praktikan langsung mengakses pengaturan router.

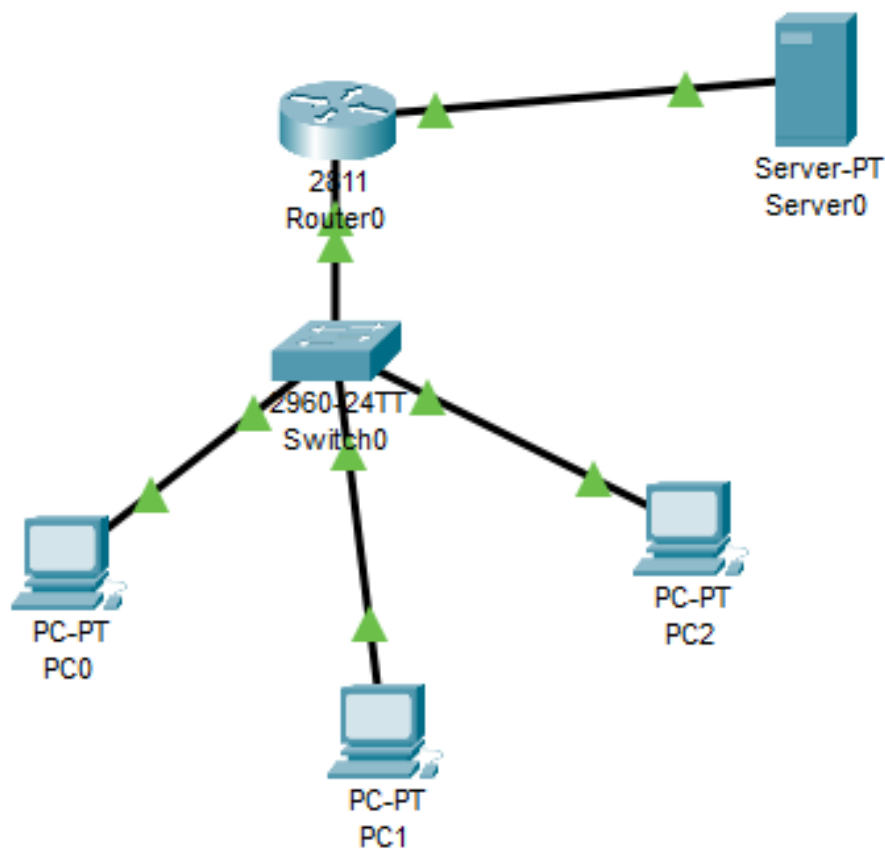
Konfigurasi DHCP Client pada `ether1` berhasil dilakukan dan router memperoleh IP publik dari jaringan luar, yang menjadi dasar agar perangkat di jaringan lokal dapat terkoneksi ke internet. Selanjutnya, konfigurasi alamat IP statis pada `ether7` serta pengaktifan DHCP Server menunjukkan bahwa router mampu membagikan IP secara otomatis ke klien melalui jaringan lokal, dibuktikan dengan klien berhasil mendapatkan IP dari rentang yang telah ditentukan.

Penerapan NAT menggunakan metode `masquerade` juga terbukti efektif, di mana klien dapat mengakses internet menggunakan IP publik yang dimiliki router. Hal ini dibuktikan melalui uji coba perintah `ping 8.8.8.8` yang berhasil mendapatkan balasan. Pengujian firewall menunjukkan bahwa aturan pemblokiran dapat bekerja sesuai dengan konfigurasi. Ketika aturan pemblokiran ICMP diaktifkan, klien tidak dapat melakukan ping, dan saat aturan dinonaktifkan, koneksi kembali berjalan normal. Begitu juga dengan pemblokiran akses terhadap konten tertentu seperti "speedtest" yang berhasil membatasi akses sesuai filter yang diterapkan.

Secara keseluruhan, percobaan ini menunjukkan bahwa MikroTik dapat dikonfigurasi untuk mengatur distribusi IP, koneksi internet melalui NAT, serta pembatasan akses melalui firewall. Hal ini membuktikan bahwa router MikroTik adalah perangkat yang fleksibel dan dapat diandalkan dalam manajemen jaringan skala kecil hingga menengah. Praktikum ini memberikan pemahaman langsung mengenai konsep dasar jaringan dan implementasinya secara praktis.

4 Hasil Tugas Modul

4.1 Topologi Jaringan



4.2 Konfigurasi NAT

```
1 # Langkah 1: Tentukan interface 'inside' (dari LAN) dan 'outside' (ke Public)
2 interface FastEthernet0/0
3   ip nat inside
4 exit
5
6 interface FastEthernet0/1
7   ip nat outside
8 exit
9
10 # Langkah 2: Buat Access Control List (ACL) untuk mengidentifikasi trafik dari LAN
    yang boleh di-NAT
11 # ACL Standar nomor 1 ini mengizinkan semua IP dari jaringan 192.168.10.0
```

```

12 access-list 1 permit 192.168.10.0 0.0.0.255
13
14 # Langkah 3: Terapkan aturan NAT
15 # Perintah ini menerjemahkan IP sumber (source) yang cocok dengan ACL 1
16 # ke alamat IP pada interface FastEthernet0/1 secara overload (PAT)
17 ip nat inside source list 1 interface FastEthernet0/1 overload

```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server0	ICMP		0.000	N	6	(edit)	
	Successful	PC2	Server0	ICMP		0.000	N	7	(edit)	
	Successful	PC0	Server0	ICMP		0.000	N	8	(edit)	
	Successful	PC1	PC2	ICMP		0.000	N	9	(edit)	

4.3 Konfigurasi Firewall Access Control List (ACL)

```

1 # Buat ACL Extended dengan nama 'FIREWALL_SERVER'
2 ip access-list extended FIREWALL_SERVER
3
4 # Aturan 1: Izinkan PC1 (192.168.10.11) mengakses protokol apa pun (ip) ke Server
   (200.100.50.2)
5 permit ip host 192.168.10.11 host 200.100.50.2
6
7 # Aturan 2: Tolak/Blokir PC0 (192.168.10.10) mengakses Server
8 deny ip host 192.168.10.10 host 200.100.50.2
9
10 # Aturan 3: Tolak/Blokir PC2 (192.168.10.12) mengakses Server
11 deny ip host 192.168.10.12 host 200.100.50.2
12
13 # Aturan 4: Izinkan semua trafik lain yang berasal dari LAN
14 # Ini penting agar proses NAT untuk PC1 tetap berjalan dan tidak terblokir
15 permit ip 192.168.10.0 0.0.0.255 any
16
17 # Terapkan ACL ini pada interface yang mengarah ke Server (Public)
18 # Arahnya 'in' karena kita menyaring paket yang MASUK ke interface ini dari sisi LAN
19 interface FastEthernet0/0
20 ip access-group FIREWALL_SERVER in
21 exit

```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC2	Server0	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC0	Server0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	3	(edit)	(delete)

5 Kesimpulan

Berdasarkan hasil percobaan yang telah dilakukan, dapat disimpulkan bahwa router MikroTik mampu dikonfigurasi secara efektif untuk memenuhi kebutuhan jaringan lokal, mulai dari distribusi alamat IP secara otomatis menggunakan DHCP Server, konektivitas internet melalui konfigurasi NAT, hingga pengaturan keamanan akses menggunakan firewall. Semua fitur utama berjalan dengan baik dan dapat diuji langsung oleh perangkat klien, baik dari sisi konektivitas maupun pembatasan akses.

Konfigurasi NAT memungkinkan perangkat di jaringan lokal untuk menggunakan satu IP publik dalam mengakses internet, sedangkan fitur firewall memberikan kontrol penuh terhadap lalu lintas data yang masuk maupun keluar. Dengan demikian, percobaan ini memberikan gambaran nyata tentang bagaimana perangkat MikroTik dapat

6 Lampiran

6.1 Dokumentasi saat praktikum

Menunggu kiriman dari temannya didan karena laptop yang dipake pas praktikum dicod