Laporan Praktikum

Desain dan Manajemen Jaringan Komputer

TUGAS 6

Akademik ITK

Disusun Oleh :

Rayhan Iqbal **10231080**

<11 MARET 2025>

📝 Kriteria Penilaian

1. Konfigurasi DHCP & DNS (30%):
    - DHCP server berfungsi dan klien menerima IP dinamis.
    - DNS server dapat melakukan resolusi nama.
2. Implementasi NAT/PAT (40%):
    - NAT overload berjalan, PC di LAN dapat mengakses IP publik.
    - show ip nat translations menampilkan hasil translasi dengan benar.
3. Simple Firewall (ACL) (30%):
    - ACL berhasil membatasi trafik tertentu (misal ICMP).
    - Dokumentasi rule ACL dan hasil uji ping.

Jawaban

1. **Persiapan & Pembuatan Topologi**

   Tarik (Drag) Perangkat:

   - **Router1 (R1): Cisco 2811 (atau 1841)**
   - **Router2 (R2): Cisco 2811 (sebagai "Internet" simulasi)**
   - **Switch: Cisco 2960**
   - **Server: Untuk DHCP & DNS**
   - **2 PC: Sebagai klien di LAN**

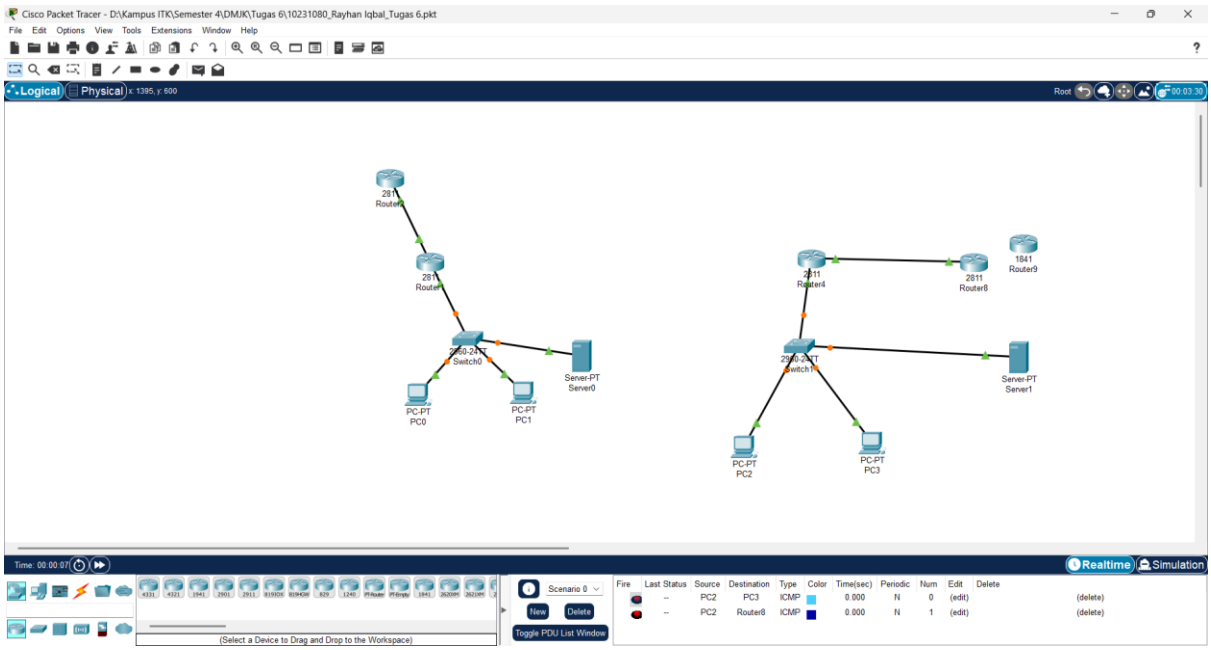
   Pengkabelan Dasar:

   - **Router1 Fa0/0 → Switch Fa0/1 (straight-through cable)**
   - **Switch Fa0/2 → Server**
   - **Switch Fa0/3 → PC0**
   - **Switch Fa0/4 → PC1**
   - **Router1 Fa0/1 → Router2 Fa0/0 (straight-through cable untuk link WAN)**

   Tujuan Utama:

   - **Jaringan LAN: 192.168.10.0/24**
   - **Router1 mengelola DHCP & DNS (didukung oleh Server di LAN).**
   - **Router1 (Fa0/1) punya IP Publik: 203.0.113.1/30 → terhubung ke Router2.**
   - **Router2 (Fa0/0) punya IP Publik: 203.0.113.2/30 → mewakili "Internet."**

   Lampu LED di setiap port harus hijau (menandakan link up).

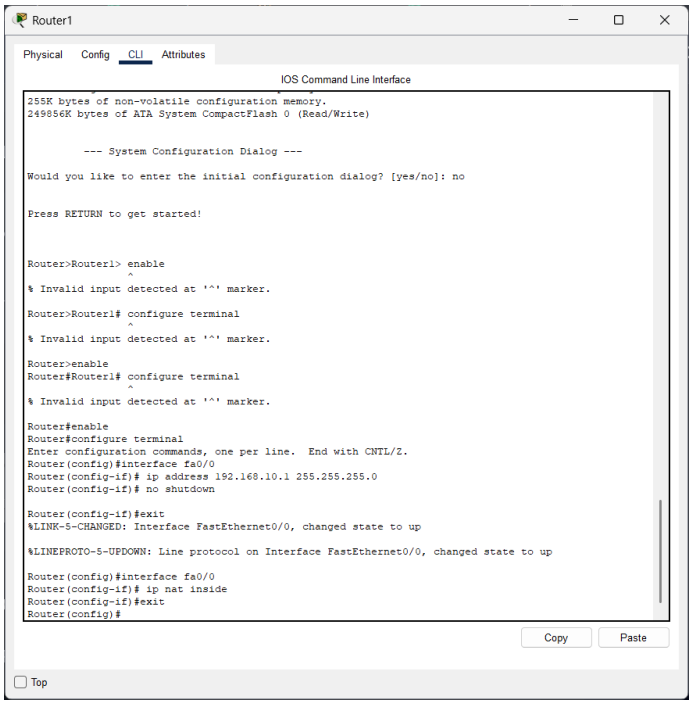


Kiri Udah Firewall dan Kanan Belum Firewalll

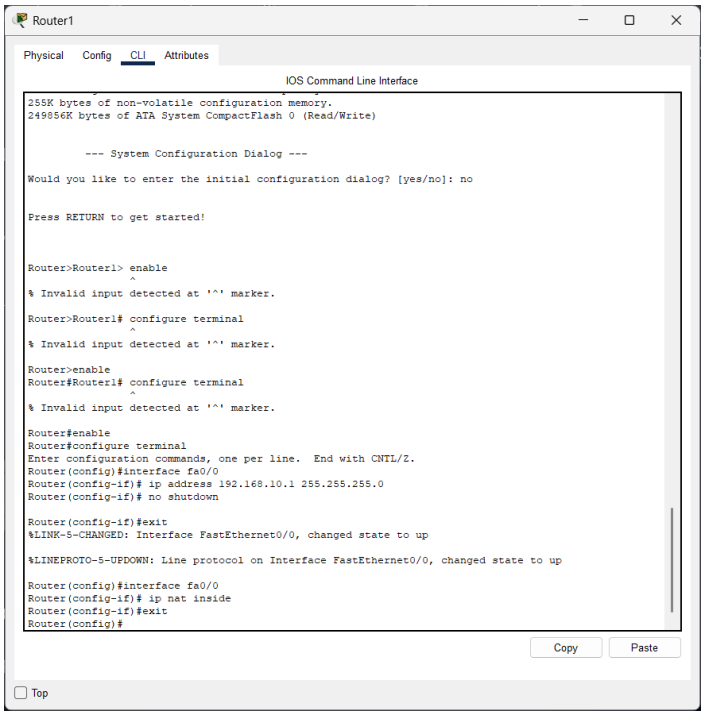
2. Konfigurasi Router1 (R1)

a. Interface LAN (Fa0/0)

1. **Masuk CLI Router1:**

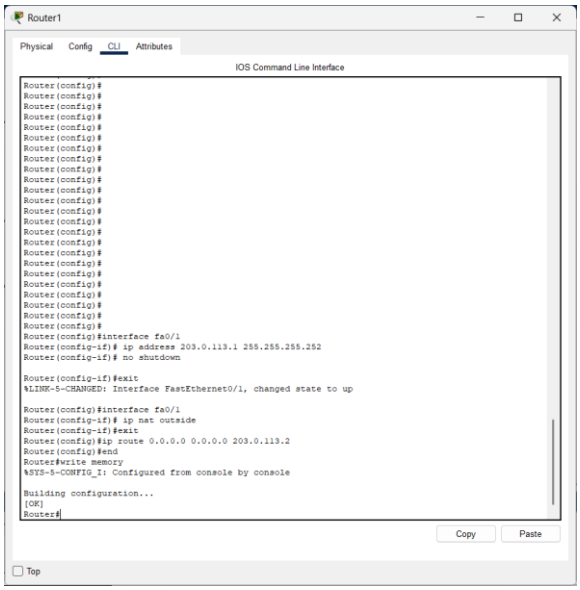


2. **Tandai interface (untuk NAT):**



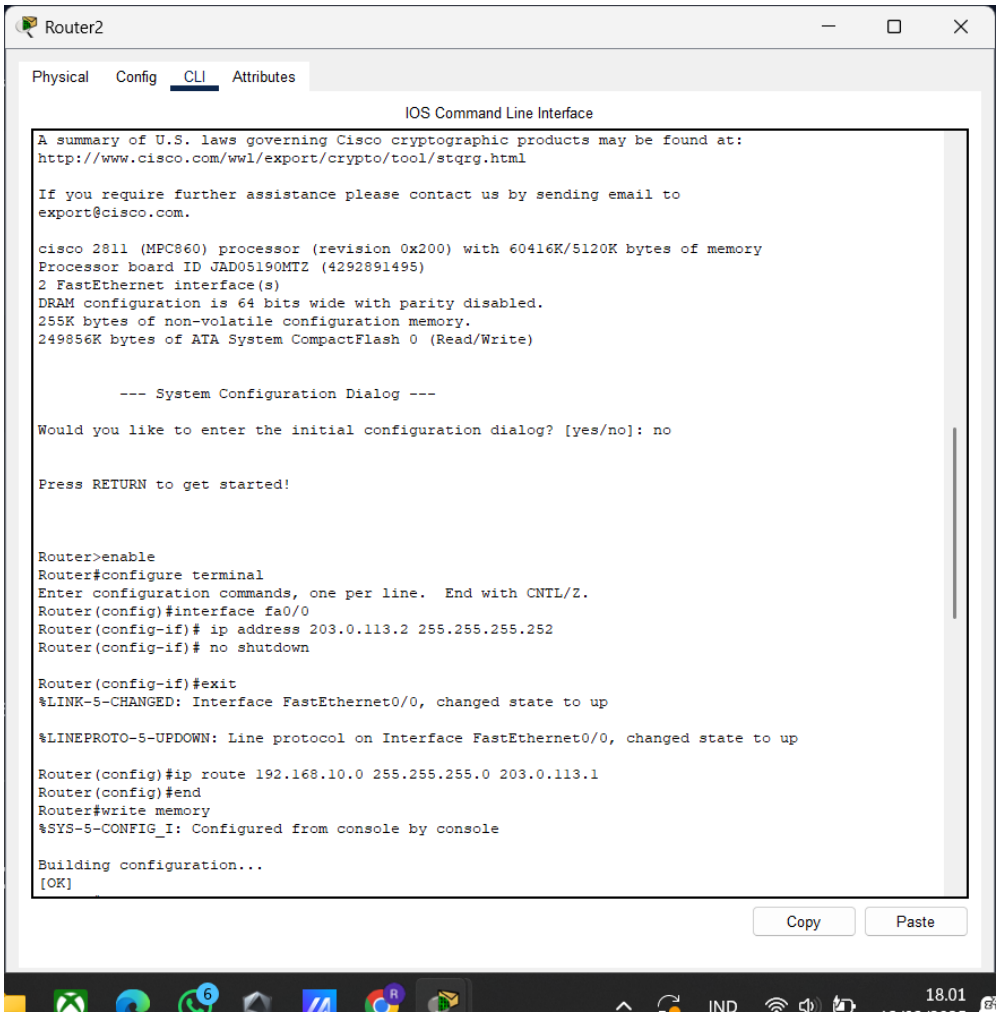
b. Interface WAN (Fa0/1)

1. **Set IP Publik (203.0.113.1/30):**
2. **Tandai interface (untuk NAT):**
3. **Buat Default Route (menuju Router2):**
4. **ip route 0.0.0.0 0.0.0.0 203.0.113.2**

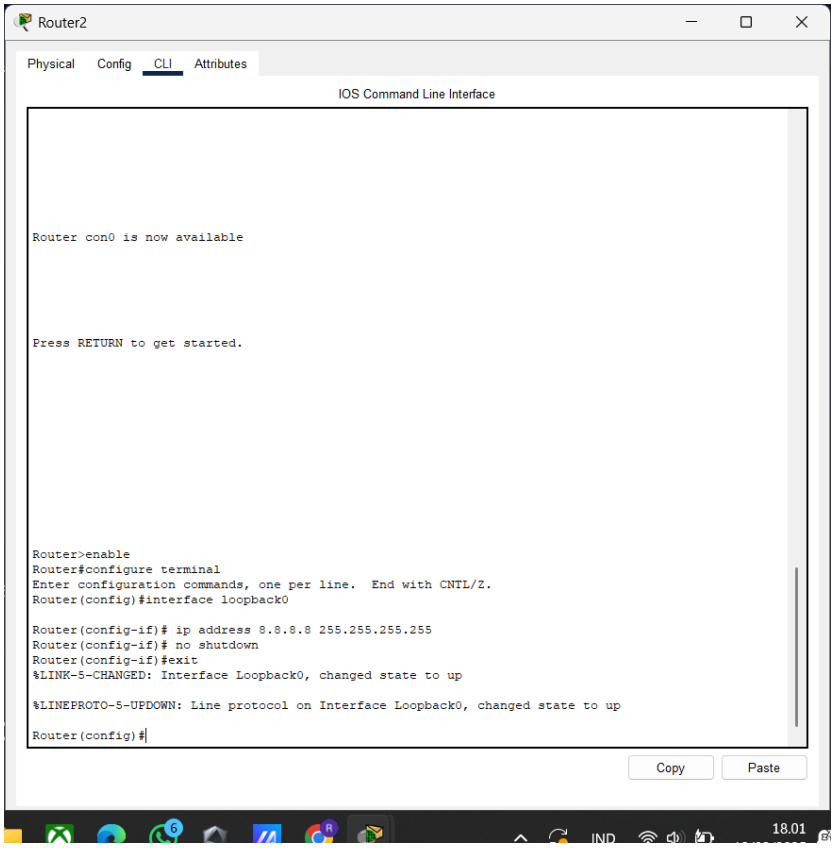


3. Konfigurasi Router2 (R2) Sebagai "Internet"

1. **Masuk CLI Router2:**
2. **Interface Fa0/0 (203.0.113.2/30):**
3. **Opsional: Tambahkan Route Balik (Jika ingin ping ke LAN R1 dari R2):**



4. **(Opsional) Tambah Loopback:**

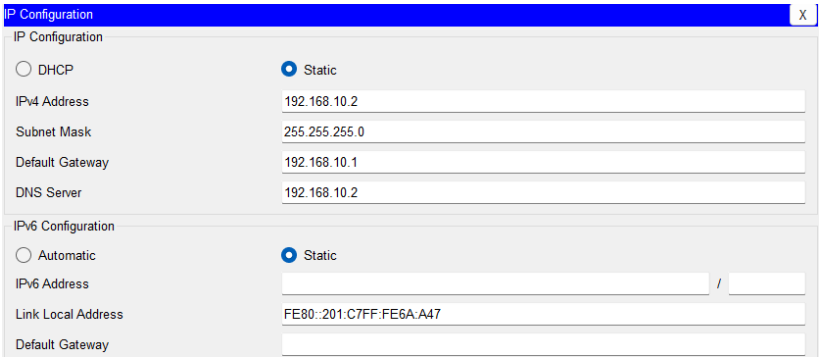


Berguna untuk simulasi IP publik tambahan.

4. Konfigurasi DHCP & DNS pada Server (di LAN)

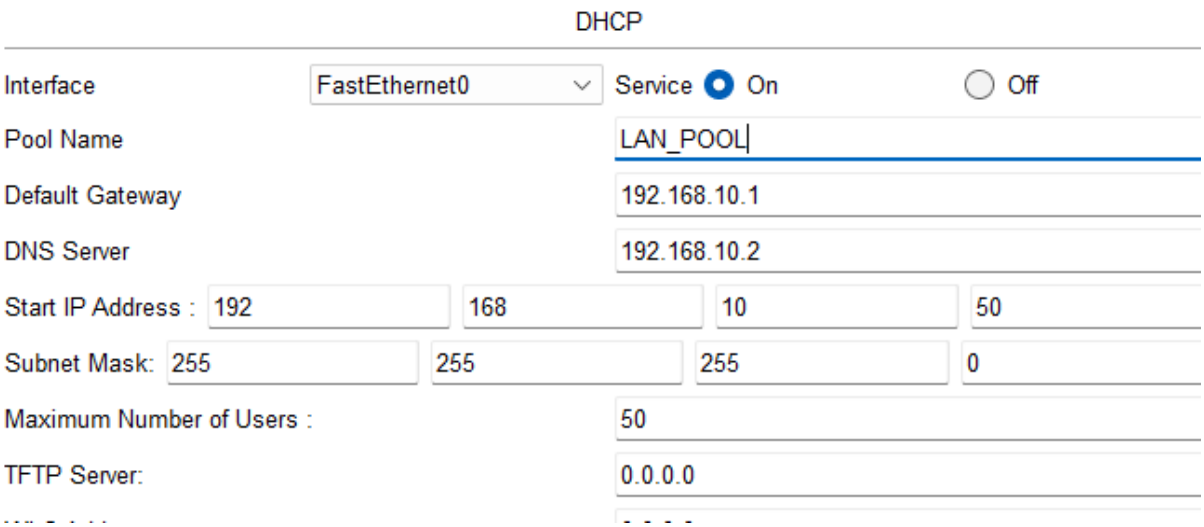
a. Set IP Server (Statik):

- **Klik Server → Tab Desktop → IP Configuration:**



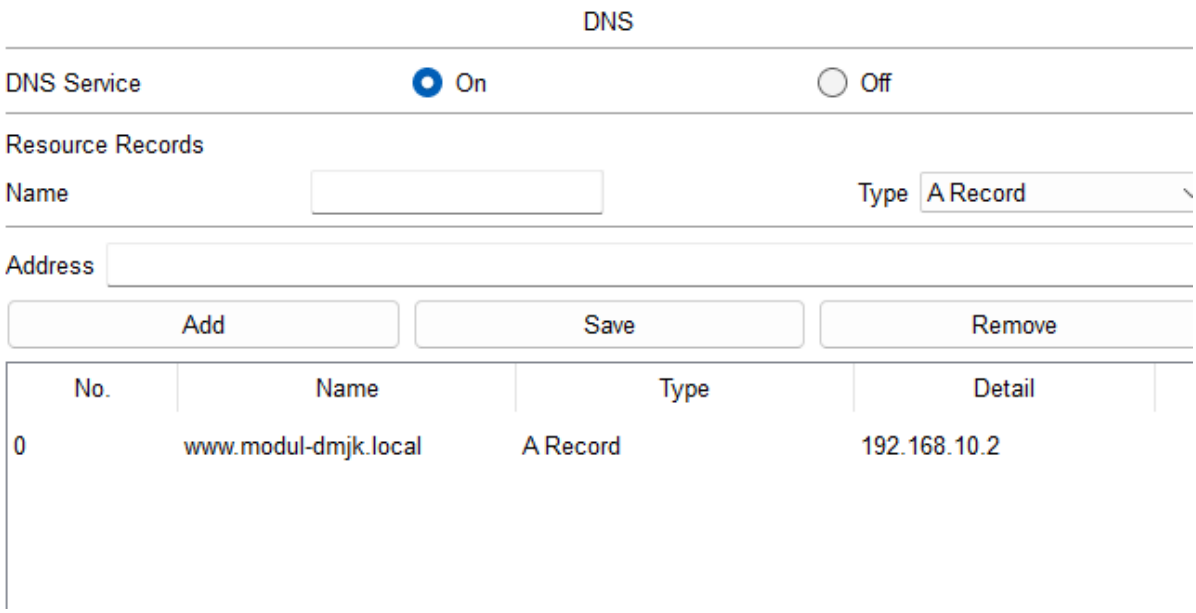
b. Menyiapkan DHCP:

1. **Server → Tab Services → DHCP:**



c. Menyiapkan DNS:

1. **Server → Tab Services → DNS:**



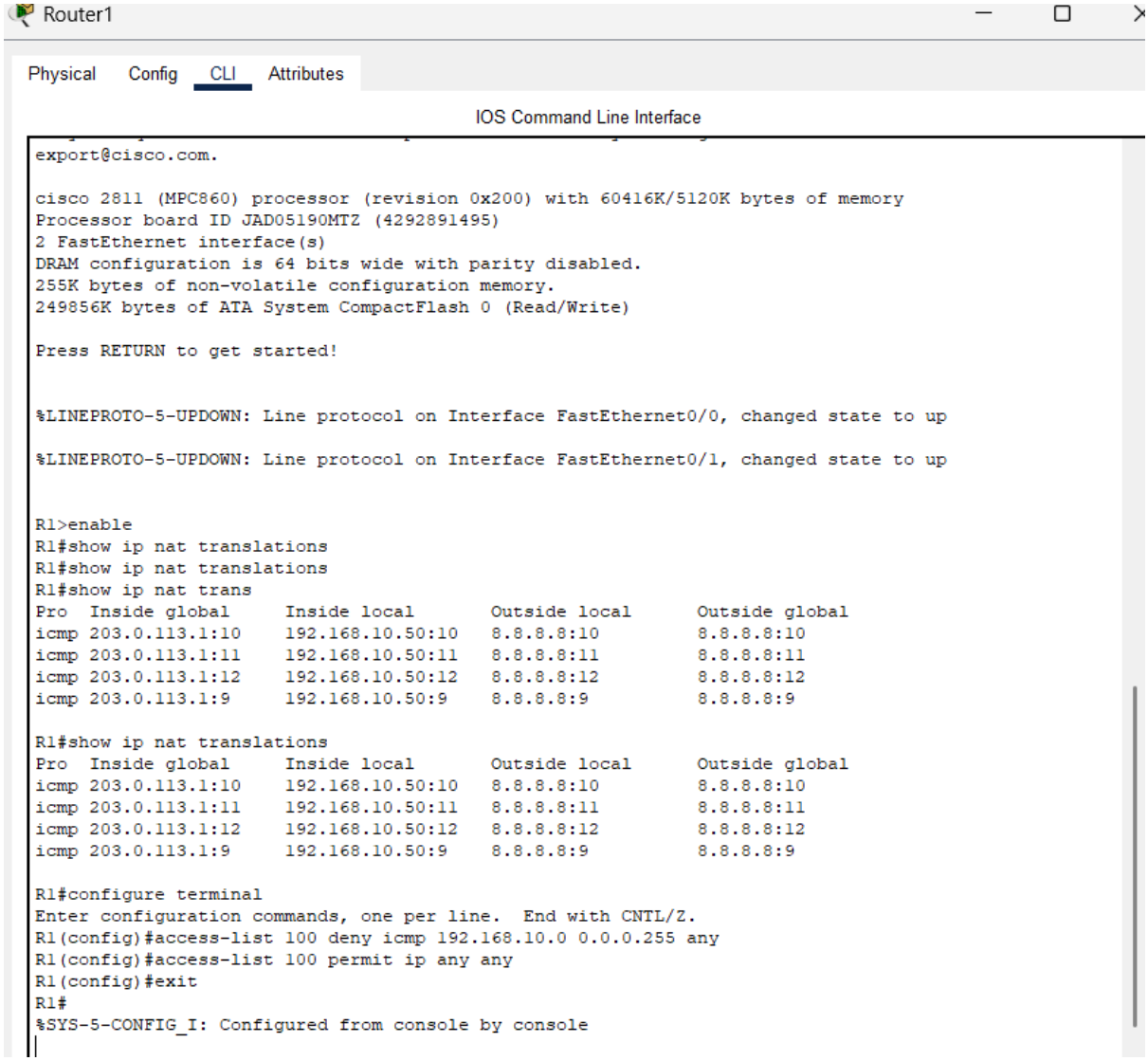
5. Konfigurasi NAT Overload (PAT) di Router1

1. Buat ACL untuk subnet LAN:

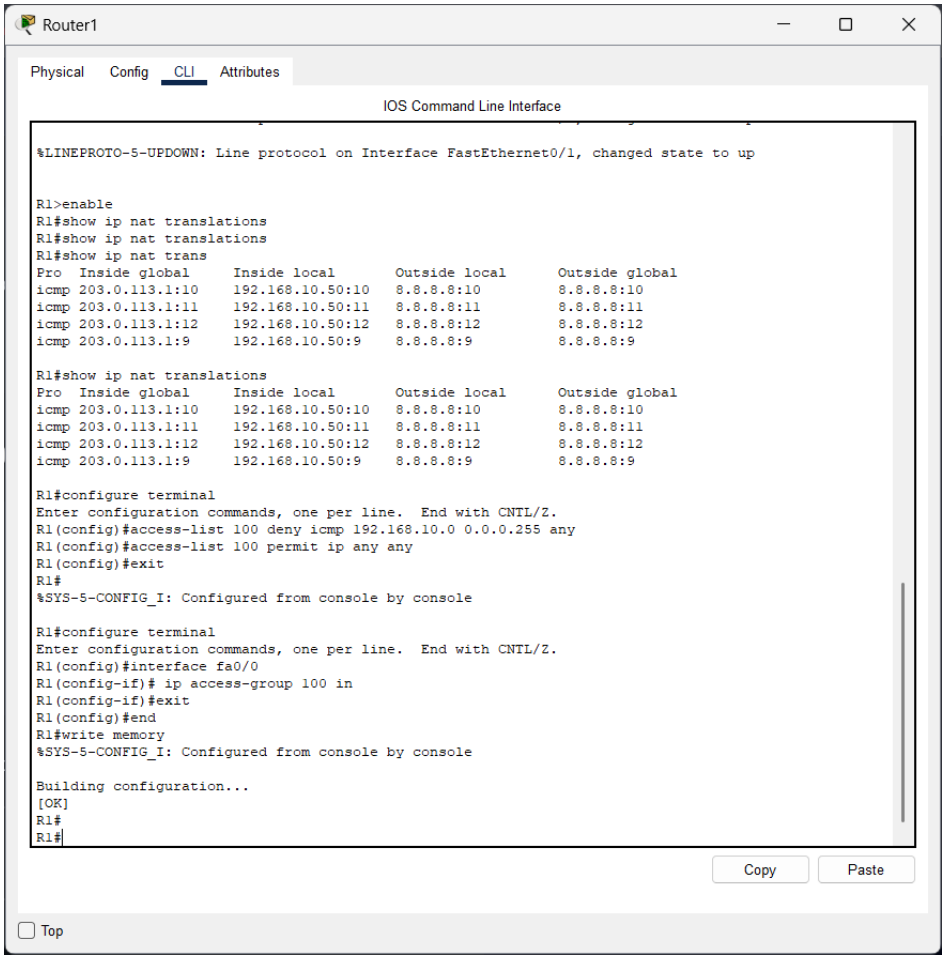
Ini memastikan LAN (192.168.10.x) akan keluar ke WAN (203.0.113.x) memakai IP Router1 (203.0.113.1).

6. Firewall Dasar (ACL Extended) [Opsional]

1. Buat Extended ACL



2. Terapkan di Interface Fa0/0 (LAN)

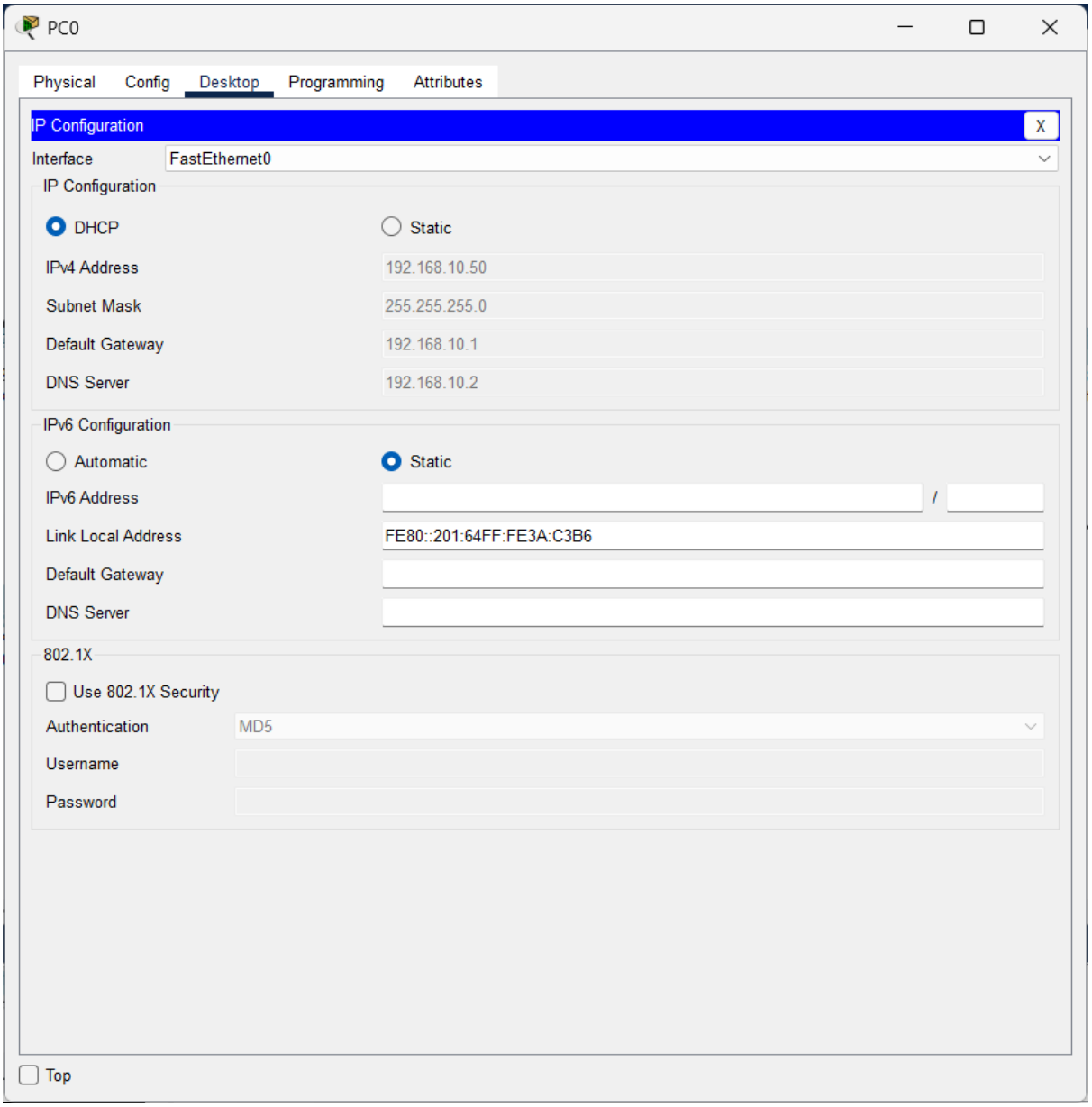


Penjelasan: Di sini paket ICMP diblok sebelum alamat source di-NAT. Hasil: Dari PC LAN (192.168.10.x) → ping ke 203.0.113.2 (WAN) akan gagal dengan "Destination host unreachable" (atau sejenis).

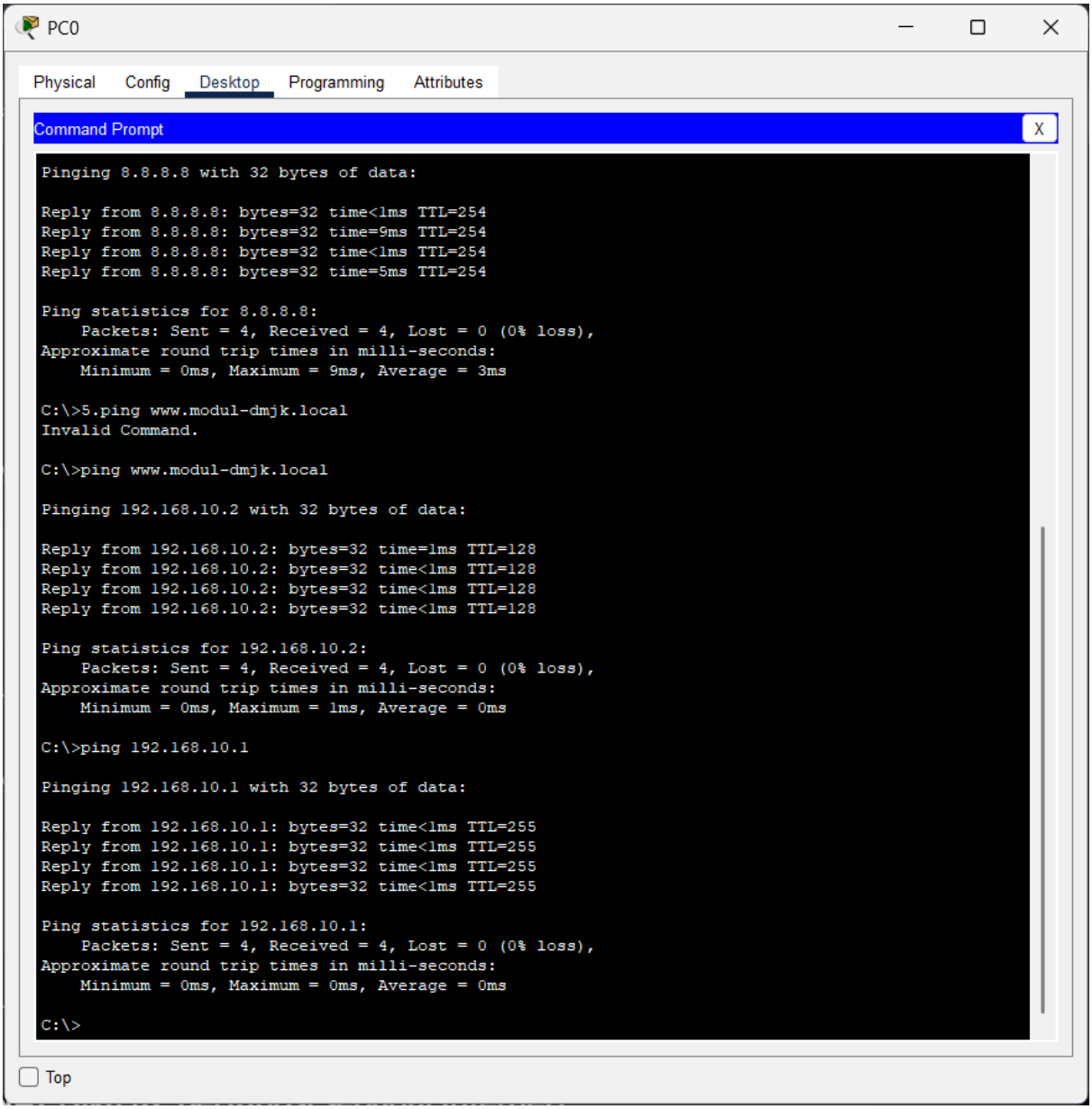
7. Verifikasi & Uji Konektivitas

a. PC di LAN

- **Set PC ke DHCP:**

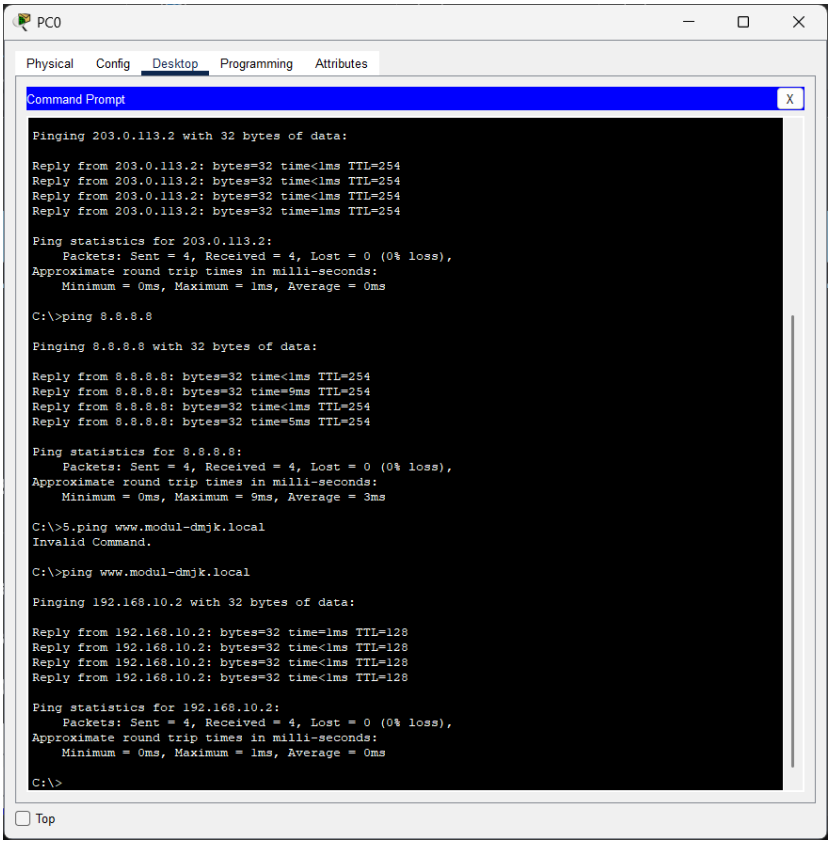


- **Ping Router:**



Harus Reply

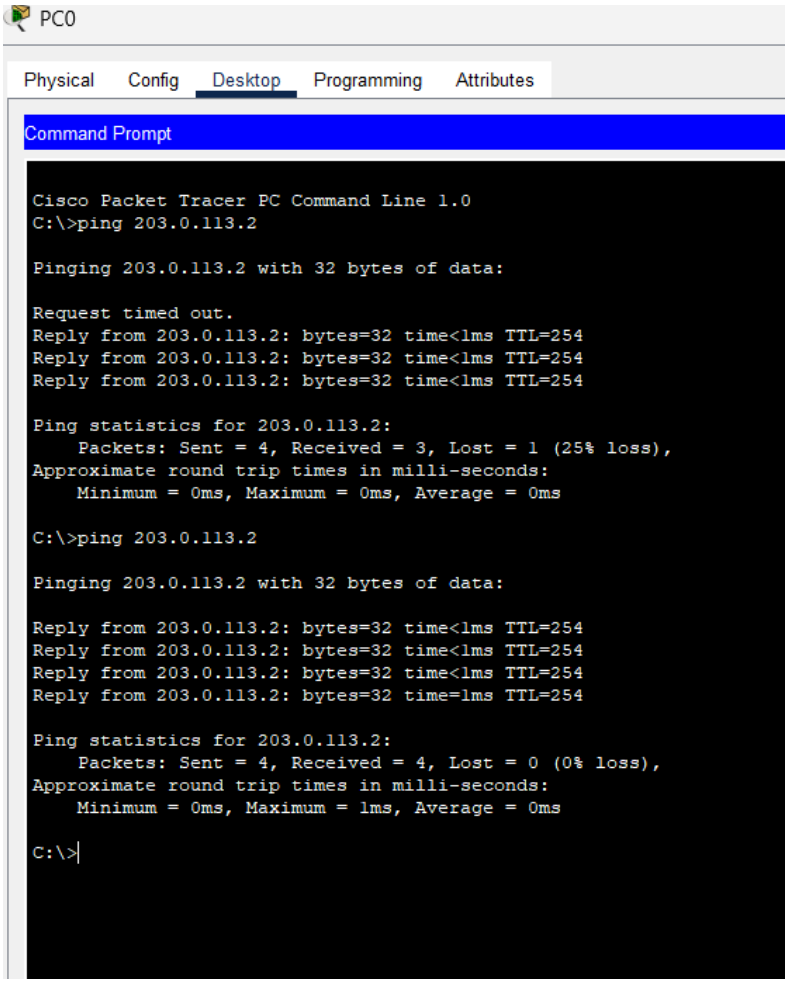
- **Ping DNS:**



Harus Reply dari 192.168.10.2

b. Uji NAT (Jika R2 Berfungsi sebagai Internet)

- **Dari PC0: ping 203.0.113.2**



- **Harus Reply jika firewall ACL tidak memblok.**

- **Lihat Translasi di R1:**

```
R1>enable
R1#show ip nat translations
R1#show ip nat translations
R1#show ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
icmp 203.0.113.1:10    192.168.10.50:10   8.8.8.8:10         8.8.8.8:10
icmp 203.0.113.1:11    192.168.10.50:11   8.8.8.8:11         8.8.8.8:11
icmp 203.0.113.1:12    192.168.10.50:12   8.8.8.8:12         8.8.8.8:12
icmp 203.0.113.1:9     192.168.10.50:9    8.8.8.8:9          8.8.8.8:9

R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 203.0.113.1:10    192.168.10.50:10   8.8.8.8:10         8.8.8.8:10
icmp 203.0.113.1:11    192.168.10.50:11   8.8.8.8:11         8.8.8.8:11
icmp 203.0.113.1:12    192.168.10.50:12   8.8.8.8:12         8.8.8.8:12
icmp 203.0.113.1:9     192.168.10.50:9    8.8.8.8:9          8.8.8.8:9

R1#
```

Tampil Inside local 192.168.10.50 → Inside global 203.0.113.1

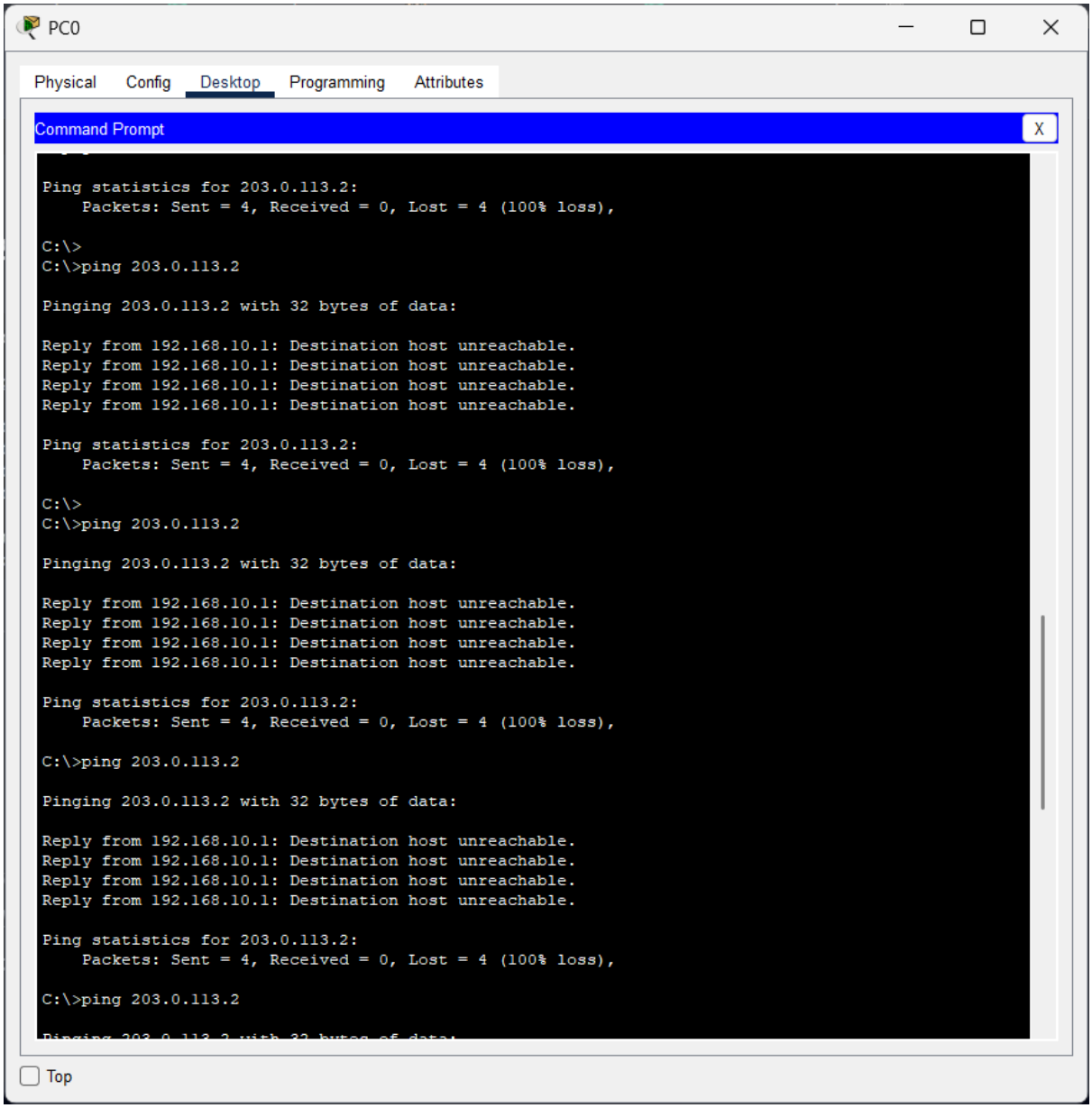
- **Ping Loopback R2 (Opsional):**

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
Reply from 8.8.8.8: bytes=32 time=9ms TTL=254
Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
Reply from 8.8.8.8: bytes=32 time=5ms TTL=254

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 3ms

C:\>
```

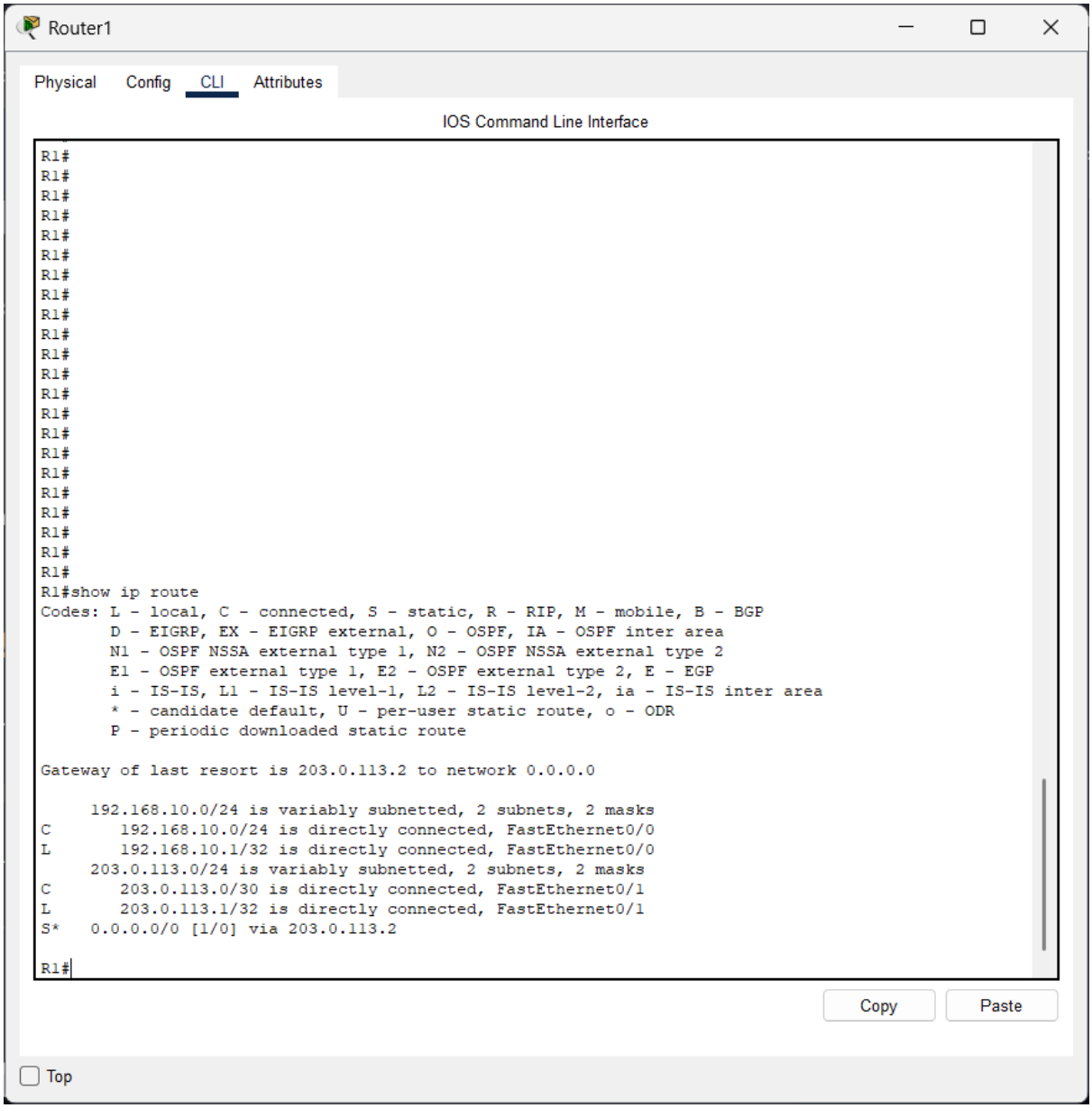
Jika loopback0 = 8.8.8.8, R2 perlu ip route 192.168.10.0/24 → 203.0.113.1 agar jalur balik ada.

c. Firewall Test (Jika ACL Diterapkan)

- **Dengan ACL extended deny icmp, ping ke 203.0.113.2 harus Request timed out, tapi protokol lain (TCP/UDP) masih berjalan (sesuai permit ip any any).**



- **Routing Table:**



Konsep Dasar Praktikum Jaringan (DHCP, DNS, NAT, Firewall)

Pada praktikum ini, kamu akan belajar beberapa layanan jaringan penting yang digunakan dalam infrastruktur IT, yaitu **DHCP, DNS, NAT/PAT, dan firewall dasar**. Berikut adalah pemahaman konsep dasarnya:

---

1. DHCP (Dynamic Host Configuration Protocol)

Fungsi:

- DHCP memungkinkan perangkat dalam jaringan mendapatkan **IP Address secara otomatis** tanpa perlu konfigurasi manual.
- Server DHCP akan memberikan **alamat IP, subnet mask, default gateway, dan DNS server** kepada klien yang memintanya.

Konsep Penting:

- **Lease**: Jangka waktu sewa IP address yang diberikan ke klien.
- **Scope**: Rentang alamat IP yang dapat diberikan oleh server DHCP.
- **Reservation**: Pemesanan IP address untuk perangkat tertentu berdasarkan **MAC Address**, sehingga IP-nya tetap sama setiap kali terhubung.

---

2. DNS (Domain Name System)

Fungsi:

- DNS mengonversi **nama domain (FQDN - Fully Qualified Domain Name)** menjadi **alamat IP**, sehingga pengguna bisa mengakses website atau layanan lain tanpa menghafal IP.
- Contoh: Saat kamu mengetik **www.google.com**, DNS akan menerjemahkannya ke alamat IP publik Google (misalnya **142.250.182.14**).

Proses Resolusi Nama:

1. **Client** meminta DNS Server untuk menerjemahkan nama domain.
2. Jika DNS Server memiliki informasi tersebut, maka langsung memberikan jawabannya.
3. Jika tidak, DNS Server akan bertanya ke **DNS Server lain** di internet sampai mendapatkan jawaban yang benar.

3. NAT/PAT (Network Address Translation / Port Address Translation)

Fungsi:

- NAT memungkinkan perangkat dengan **IP privat** (misalnya 192.168.x.x) dapat berkomunikasi dengan **internet publik** menggunakan satu IP publik.
- **PAT (Port Address Translation)** adalah bentuk NAT yang memungkinkan **banyak perangkat berbagi satu IP publik** dengan membedakan **nomor port**.

Jenis NAT:

- **Static NAT**: IP privat diterjemahkan ke satu IP publik tertentu.
- **Dynamic NAT**: IP privat diterjemahkan ke IP publik yang tersedia dari kumpulan IP yang ditetapkan.
- **PAT (NAT Overload)**: Banyak IP privat diterjemahkan ke **satu** IP publik, tetapi menggunakan **port yang berbeda**.

Contoh:

- **NAT tanpa PAT (1:1)**
    - 192.168.10.2 → 203.0.113.10
    - 192.168.10.3 → 203.0.113.11
- **NAT dengan PAT (1:banyak)**
    - 192.168.10.2:12345 → 203.0.113.1:54321
    - 192.168.10.3:12346 → 203.0.113.1:54322

---

4. Firewall Dasar (Access-List / Zone-Based Firewall)

Firewall berfungsi untuk **menyaring dan mengamankan lalu lintas jaringan** berdasarkan aturan yang telah ditentukan.

Access Control List (ACL)

ACL adalah **daftar aturan yang menentukan izin akses** berdasarkan sumber, tujuan, dan jenis lalu lintas.

Jenis ACL:

1. **Standard ACL** (Nomor 1-99):
    - Hanya bisa memfilter berdasarkan **IP sumber**.
    - Contoh:
    - access-list 1 deny 192.168.10.10
    - access-list 1 permit any
2. **Extended ACL** (Nomor 100-199):
    - Bisa memfilter berdasarkan **IP sumber, IP tujuan, dan protokol (ICMP, TCP, UDP, dll.)**.
    - Contoh:
    - access-list 100 deny icmp 192.168.10.0 0.0.0.255 any
    - access-list 100 permit ip any any
    - **ICMP diblokir**, tetapi trafik lainnya diizinkan.

Zone-Based Firewall (ZBF)

- ZBF lebih canggih dibanding ACL karena **mengelompokkan interface ke dalam zona** dan mengontrol lalu lintas antar zona.
- Contoh Zona:
    - **Inside**: Jaringan internal (192.168.10.x)
    - **Outside**: Internet (203.0.113.x)
    - **DMZ (Demilitarized Zone)**: Jaringan server publik

Konsep Utama:

- **Traffic dari Inside ke Outside → Allowed**
- **Traffic dari Outside ke Inside → Denied kecuali ada aturan khusus**

Kesimpulan

Dalam praktikum ini, kamu akan:

1. **Menggunakan DHCP** untuk mendistribusikan IP secara otomatis ke perangkat.

2. **Menggunakan DNS** agar klien dapat mengakses server berdasarkan nama, bukan IP.
3. **Mengimplementasikan NAT/PAT** agar perangkat di jaringan privat bisa mengakses internet.
4. **Menerapkan firewall dasar (ACL atau ZBF)** untuk mengamankan jaringan dengan aturan filtering trafik.

Tautan Github:

https://github.com/DeathMoonerg/DMJK-10231080