

# Praktikum Jaringan Komputer



NRP	: 3223600017
Nama	: Muhammad Alfarrel Arya Mahardika
Materi	: Dynamic NAT & Port Address Translation (PAT)
Tanggal	: 30 April 2025

## 1. Tujuan

- 1.1. Mahasiswa mampu menjelaskan konsep dan cara kerja Dynamic NAT
- 1.2. Mahasiswa mampu melakukan konsep dan cara kerja NAT Overload
- 1.3. Mahasiswa mampu menjelaskan konfigurasi dynamic NAT dan PAT pada router

## 2. Dasar Teori

Dynamic NAT (Network Address Translation) dan Port Address Translation (PAT) adalah dua teknik dalam NAT yang digunakan untuk memungkinkan perangkat dalam jaringan lokal mengakses jaringan eksternal seperti internet, meskipun menggunakan alamat IP privat. Meskipun keduanya memiliki tujuan serupa, yaitu untuk menghemat penggunaan alamat IP publik, keduanya bekerja dengan cara yang sedikit berbeda. Dynamic NAT menggunakan pool alamat IP publik dan memetakan alamat IP privat ke alamat IP publik dari pool yang tersedia secara dinamis, sementara PAT memungkinkan banyak perangkat internal untuk berbagi satu alamat IP publik dengan membedakan sesi koneksi menggunakan nomor port.

Pada Dynamic NAT, setiap perangkat di jaringan lokal akan diberi alamat IP publik dari pool yang ada saat melakukan akses ke luar jaringan. Setelah sesi komunikasi selesai, alamat IP publik yang digunakan akan dikembalikan ke pool dan dapat digunakan oleh perangkat lain. Teknik ini berguna ketika banyak perangkat internal yang memerlukan koneksi keluar, tetapi jumlah alamat IP publik terbatas. Namun, Dynamic NAT tidak mendukung koneksi masuk dari luar jaringan karena pemetaan antara alamat IP privat dan publik bersifat sementara dan tidak konsisten.

Sementara itu, Port Address Translation (PAT), yang juga dikenal sebagai NAT Overload, adalah variasi dari NAT yang lebih efisien dalam memanfaatkan satu alamat IP publik. PAT bekerja dengan cara yang mirip dengan Dynamic NAT, tetapi alih-alih memberikan satu alamat IP publik untuk setiap perangkat internal, PAT menggunakan satu alamat IP publik untuk banyak perangkat dengan membedakan setiap koneksi menggunakan nomor port yang unik. Dengan demikian, banyak perangkat dalam jaringan lokal dapat berbagi satu alamat IP publik saat mengakses internet, tetapi masih dapat membedakan setiap sesi komunikasi berdasarkan kombinasi alamat IP dan nomor port.

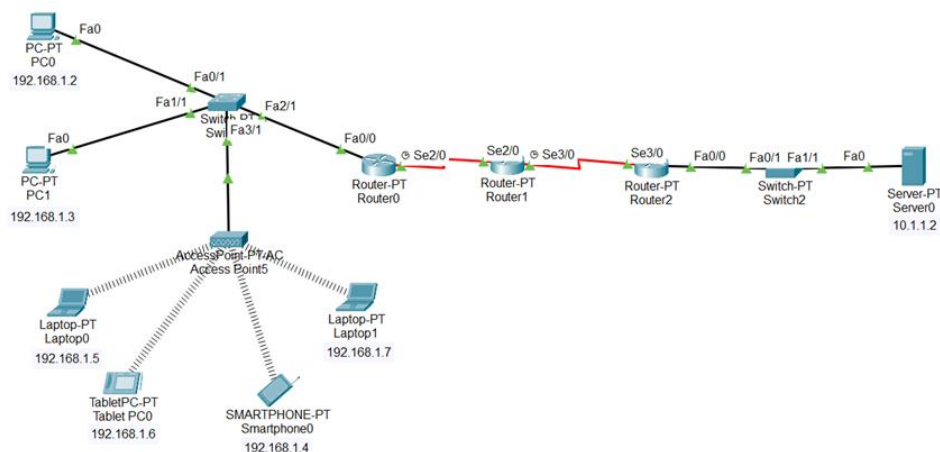
Keuntungan utama PAT adalah penghematan besar dalam jumlah alamat IP publik yang dibutuhkan. Hal ini sangat penting, terutama pada jaringan besar atau pada organisasi yang memiliki banyak perangkat yang membutuhkan akses ke internet, namun memiliki jumlah IP publik yang terbatas. PAT memungkinkan ribuan perangkat internal untuk berbagi satu alamat IP publik yang sama, yang menjadikannya solusi yang lebih efisien daripada Dynamic NAT dalam banyak skenario.

Namun, baik Dynamic NAT maupun PAT memiliki kelemahan. Keduanya tidak mendukung akses langsung dari luar jaringan ke perangkat internal (inbound connections) karena pemetaan antara IP privat dan publik tidak bersifat tetap. Jika perangkat dalam jaringan lokal perlu diakses dari luar, misalnya untuk hosting server web atau aplikasi lainnya, konfigurasi tambahan seperti port forwarding atau menggunakan teknik NAT yang lebih canggih diperlukan. Meskipun demikian, kedua teknik ini tetap sangat berguna dalam mengoptimalkan penggunaan IP publik dan meningkatkan efisiensi jaringan.

### 3. Prosedur

3.1. Buatlah topologi Dynamic NAT & PAT menggunakan simulator Packet Tracer, dimana perangkat yang dibutuhkan yaitu:

- End devices: PC
- Network devices: Switch, Router
- Connections: Copper Straight-Through, Serial, Wireless



3.2. Lakukan konfigurasi IP Address, subnetmask, dan default gateway pada semua end device. Anda dapat menggunakan konfigurasi IP statis atau mengkonfigurasi router sebagai DHCP server, kemudian end device akan menggunakan konfigurasi IP DHCP

End devices	IP address	Subnetmask	Default Gateway
PC0	192.168.1.2	255.255.255.0	192.168.1.1
PC1	192.168.1.3	255.255.255.0	192.168.1.1
Laptop0	192.168.1.5	255.255.255.0	192.168.1.1
Tablet PC0	192.168.1.6	255.255.255.0	192.168.1.1
Smartphone0	192.168.1.4	255.255.255.0	192.168.1.1
Laptop1	192.168.1.7	255.255.255.0	192.168.1.1
Server0	10.1.1.2	255.0.0.0	10.1.1.1

3.3. Lakukan konfigurasi interface pada semua router baik melalui CLI atau Router Config:

Router	Interface	IP address	Subnetmask
Router0	Fa0/0	192.168.1.1	255.255.255.0
	Se2/0	200.1.1.251	255.255.255.0
Router1	Se2/0	200.1.1.252	255.255.255.0
	Se3/0	200.1.2.251	255.255.255.0
Router2	Fa0/0	10.1.1.1	255.0.0.0
	Se2/0	200.1.2.252	255.255.255.0

a. Router 0

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
```

```
interface Serial2/0
ip address 200.1.1.251 255.255.255.0
no shutdown
```

b. Router 1

```
interface Serial2/0
ip address 200.1.1.252 255.255.255.0
no shutdown
```

```
interface Serial3/0
ip address 200.1.2.251 255.255.255.0
no shutdown
```

c. Router 2

```
interface FastEthernet0/0
ip address 10.1.1.1 255.0.0.0
no shutdown
```

```
interface Serial3/0
ip address 200.1.2.252 255.255.255.0
no shutdown
```

3.4. Lakukan konfigurasi pada interface yang menjadi sisi inside

a. Router 0

```
Router(config)# int fa0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip nat inside
```

b. Router 1

```
Router(config)# int fa0/0
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# ip nat inside
```

Hasil Konfigurasi:

a. Router 0

```
interface FastEthernet0/0
ip nat inside
```

- b. Router 1

```
interface FastEthernet0/0
ip nat inside
```

3.5. Lakukan konfigurasi pada interface yang menjadi sisi inside pada:

- a. Router 0

```
Router(config)# interface Serial2/0
Router(config-if)# ip address 200.1.1.251 255.255.255.0
Router(config-if)# ip nat outside
```

- b. Router 2

```
Router(config)# interface Serial3/0
Router(config-if)# ip address 200.1.2.252 255.255.255.0
Router(config-if)# ip nat outside
```

Hasil Konfigurasi

- a. Router 0

```
interface Serial2/0
ip nat outside
```

- b. Router 2

```
interface Serial3/0
ip nat outside
```

Note: Pada prosedur 6 – 8 dilakukan pada Router0. Sedangkan untuk Router2 dapat dilakukan konfigurasi static NAT ataupun dynamic NAT. Bila diasumsikan menggunakan konfigurasi static NAT, maka dapat menjalankan perintah berikut:

```
Router(config)# ip nat inside source static 10.1.1.2 200.10.0.2
Router(config)# ex
Router# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 200.10.0.2 10.1.1.2 --- ---
```

3.6. Lakukan konfigurasi ACL untuk mencocokkan paket yang masuk ke inside interface

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

3.7. Lakukan konfigurasi untuk pool Alamat IP public yang terdaftar

```
Router(config)# ip nat pool dynpool 200.1.1.1 200.1.1.5 netmask 255.255.255.0
```

3.8. Lakukan konfigurasi untuk mengaktifkan dynamic NAT

```
Router(config)# ip nat inside source list 1 pool dynpool
```

3.9. Lakukan konfigurasi static routing

- a. Router 0

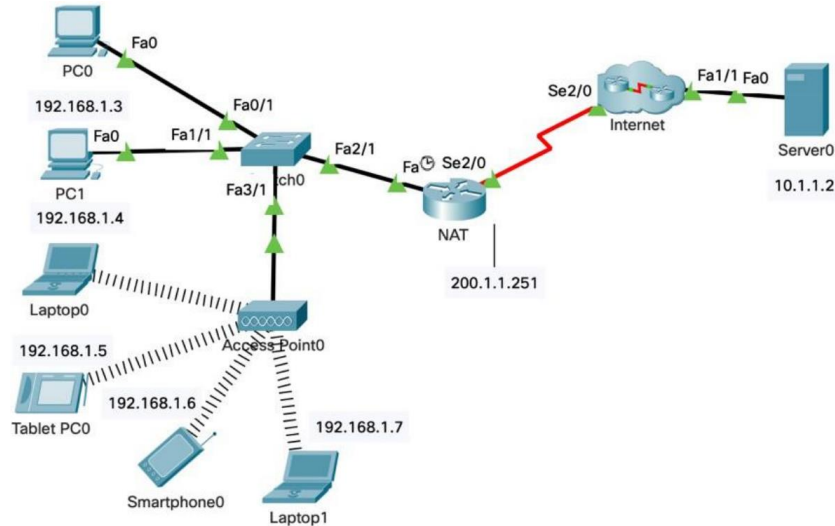
```
Router(config)# ip route 200.1.2.0 255.255.255.0 200.1.1.252
Router(config)# ip route 200.10.0.0 255.255.255.0 200.1.2.252
```

b. Router 1

```
Router(config)# ip route 200.10.0.0 255.255.255.0 200.1.2.252
```

c. Router 2

```
Router(config)# ip route 200.1.1.0 255.255.255.0 200.1.2.251
```



3.10. Lakukan verifikasi pada router NAT baik sebelum membangkitkan trafik dengan perintah berikut:

```
Router# show ip nat translations
Router# show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial2/0
Inside Interfaces: FastEthernet0/0
Hits: 0 Misses: 0
Expired translations: 24
Dynamic mappings:
-- Inside Source
access-list 1 pool dynpool refCount 0
pool dynpool: netmask 255.255.255.0
start 200.1.1.1 end 200.1.1.5
type generic, total addresses 5 , allocated 0 (0%), misses 0
```

Hasil Verifikasi:

```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router#show ip nat translations
Router#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial2/0
Inside Interfaces: FastEthernet0/0
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool dynpool refCount 0
pool dynpool: netmask 255.255.255.0
start 200.1.1.1 end 200.1.1.5
type generic, total addresses 5 , allocated 0 (0%), misses 0
```

- 3.11. Lakukan pengujian melalui sejumlah end device yang berada di private network menuju ke server dengan IP tujuan 200.10.0.2, anda dapat menguji melalui command prompt untuk tes ping, ftp, dan lainnya, ataupun melalui web browser seperti pada percobaan praktikum sebelumnya di bab Static NAT. lampirkan screenshot pengujian anda dan lakukan analisa. Bandingkan dengan percobaan pada Langkah 10.

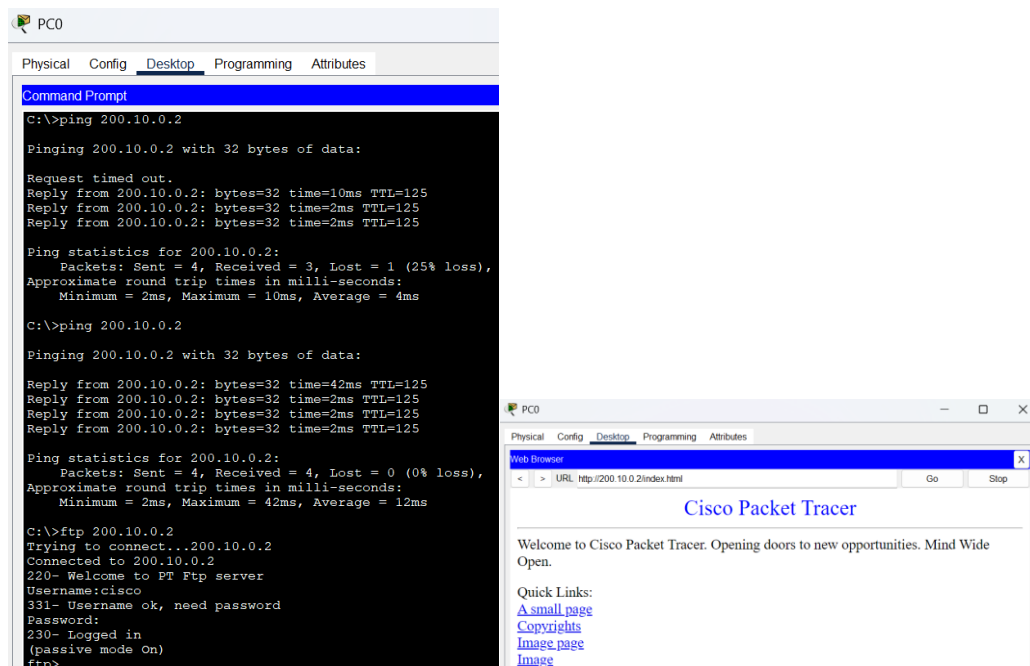
Maka setelah ada trafik, contohnya akan tampil seperti berikut:

```
Router# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 200.1.1.1:1 192.168.1.5:1 200.10.0.2:1 200.10.0.2:1
icmp 200.1.1.1:2 192.168.1.5:2 200.10.0.2:2 200.10.0.2:2
icmp 200.1.1.1:3 192.168.1.5:3 200.10.0.2:3 200.10.0.2:3
icmp 200.1.1.1:4 192.168.1.5:4 200.10.0.2:4 200.10.0.2:4
tcp 200.1.1.3:1025 192.168.1.2:1025 200.10.0.2:21 200.10.0.2:21
tcp 200.1.1.4:1027 192.168.1.3:1027 200.10.0.2:80 200.10.0.2:80
tcp 200.1.1.5:1028 192.168.1.4:1028 200.10.0.2:21 200.10.0.2:21

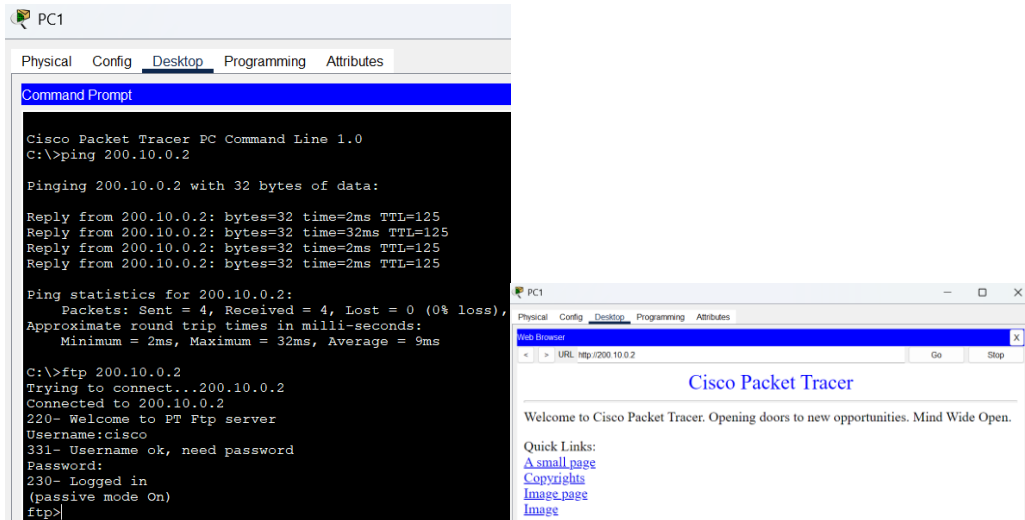
Router# show ip nat statistics
Total translations: 7 (0 static, 7 dynamic, 7 extended)
Outside Interfaces: Serial2/0
Inside Interfaces: FastEthernet0/0
Hits: 74 Misses: 50
Expired translations: 28
Dynamic mappings:
-- Inside Source
access-list 1 pool dynpool refCount 7
pool dynpool: netmask 255.255.255.0
start 200.1.1.1 end 200.1.1.5
type generic, total addresses 5 , allocated 3 (60%), misses 0
```

Hasil Pengujian:

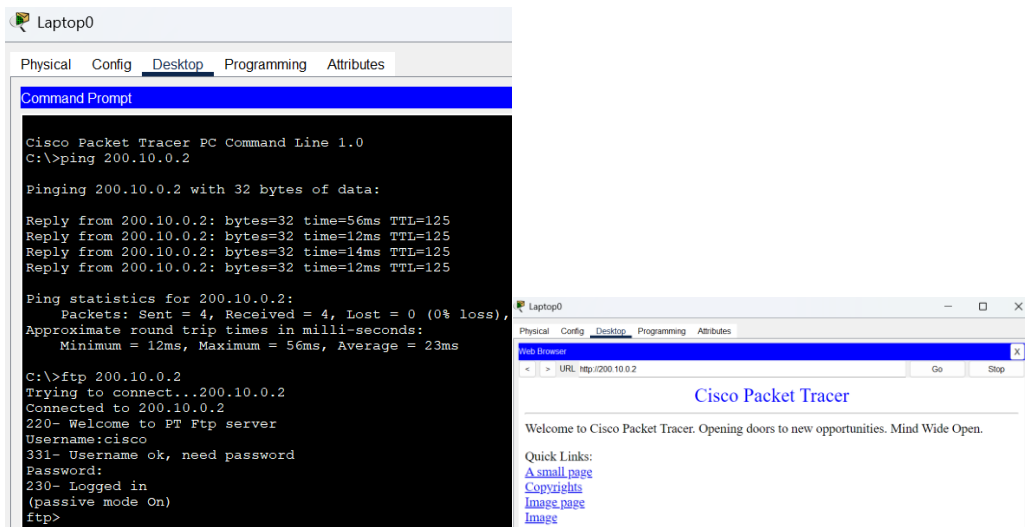
- a. PC0 ke Server0



b. PC1 ke Server0

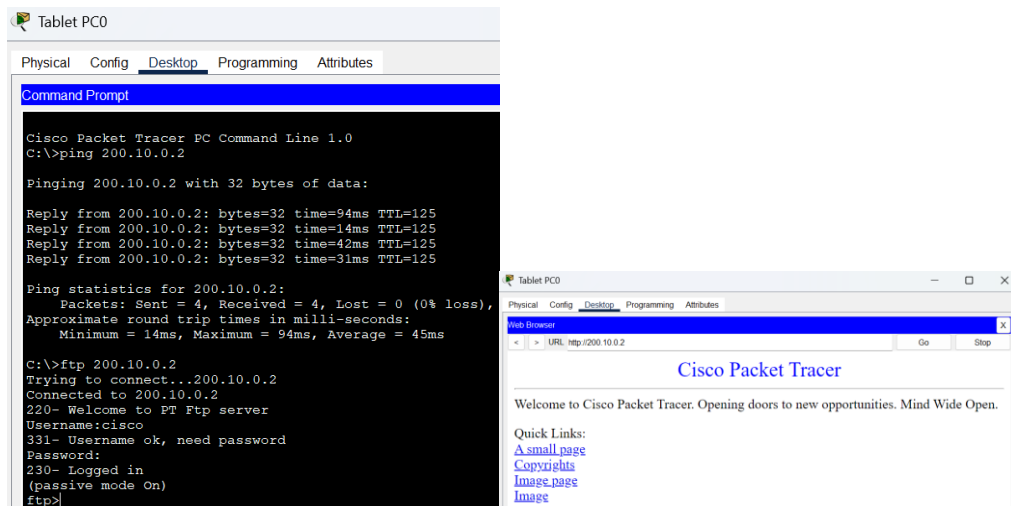


c. Laptop0 ke Server0

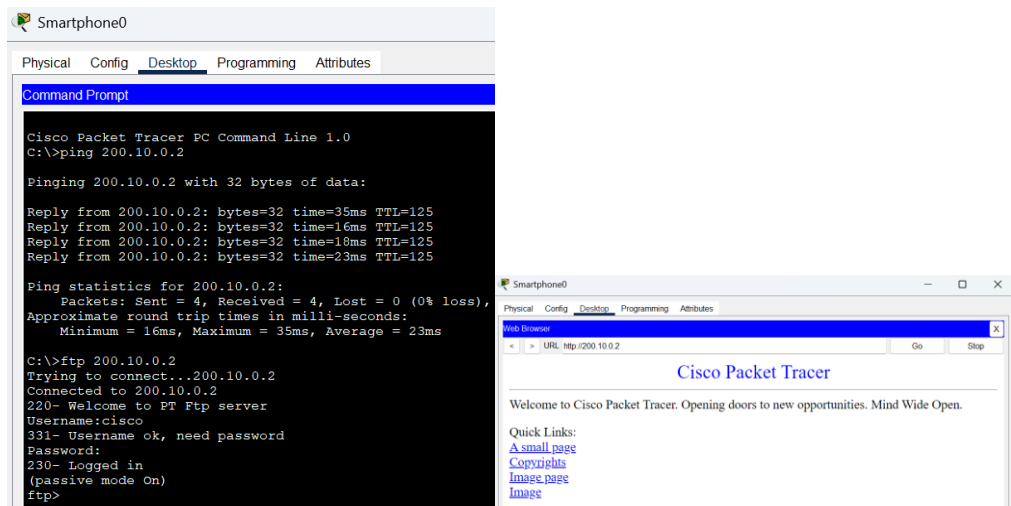




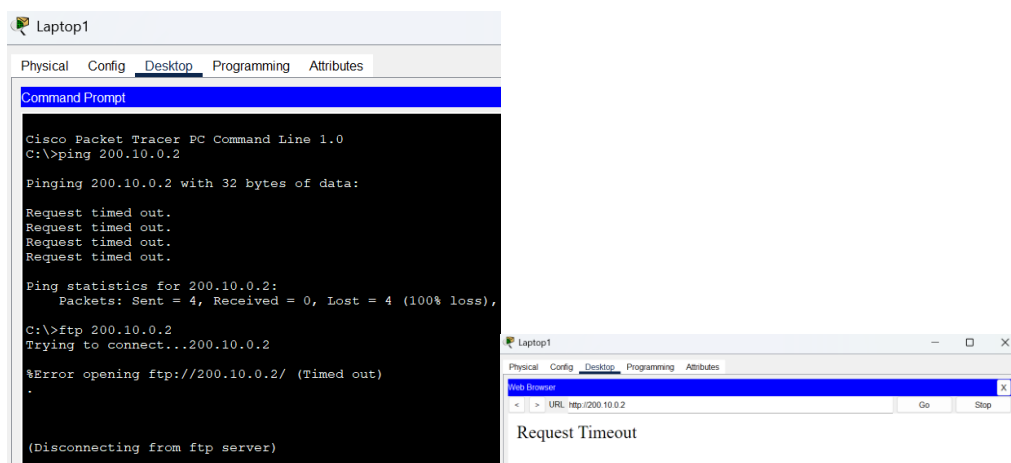
d. Tablet PC0 ke Server0




e. Smartphone0 ke Server0



f. Laptop1 ke Server0




 Router0
 

Physical
 Config
 CLI
 Attributes

 IOS Command Line Interface
 

```

Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
tcp  200.1.1.1:1026     192.168.1.2:1026  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1027     192.168.1.2:1027  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1028     192.168.1.2:1028  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1029     192.168.1.2:1029  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1030     192.168.1.2:1030  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1031     192.168.1.2:1031  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1032     192.168.1.2:1032  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1033     192.168.1.2:1033  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1034     192.168.1.2:1034  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1035     192.168.1.2:1035  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.1:1036     192.168.1.2:1036  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.2:1026     192.168.1.3:1026  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.3:1025     192.168.1.6:1025  200.10.0.2:21      200.10.0.2:21
tcp  200.1.1.3:1026     192.168.1.6:1026  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.4:1025     192.168.1.7:1025  200.10.0.2:21      200.10.0.2:21
tcp  200.1.1.4:1026     192.168.1.7:1026  200.10.0.2:80      200.10.0.2:80
tcp  200.1.1.5:1025     192.168.1.4:1025  200.10.0.2:21      200.10.0.2:21
tcp  200.1.1.5:1026     192.168.1.4:1026  200.10.0.2:80      200.10.0.2:80
  
```

 Router0
 

Physical
 Config
 CLI
 Attributes

 IOS Command Line Interface
 

```

Router#show ip nat statistics
Total translations: 18 (0 static, 18 dynamic, 18 extended)
Outside Interfaces: Serial2/0
Inside Interfaces: FastEthernet0/0
Hits: 200 Misses: 72
Expired translations: 26
Dynamic mappings:
-- Inside Source
access-list 1 pool dynpool refCount 18
pool dynpool: netmask 255.255.255.0
start 200.1.1.1 end 200.1.1.5
type generic, total addresses 5 , allocated 4 (80%), misses 28
  
```

3.12. Untuk menghapus dynamic entreies anda dapat menggunakan perintah

Router# clear ip nat translation \*

3.13. Untuk menampilkan pesan yang mendeskripsikan tiap paket anda dapat menggunakan perintah

Router# debug ip nat

3.14. Lanjutkan percobaan untuk NAT overload dengan menggunakan mekanisme Port Address Translation (PAT), dimana anda dapat menambahkan perintah berikut

Router(config)#ip nat inside source list 1 interface se2/0 overload

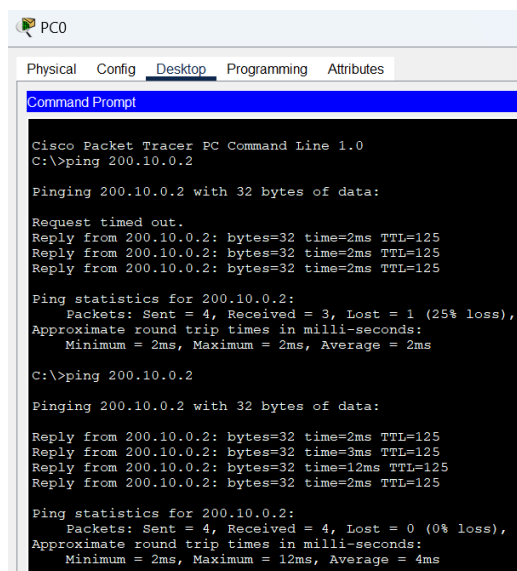
- 3.15. Kemudian bangkitkan trafik untuk melakukan pengujian, dan bandingkan dengan hasil pada prosedur 11. Lampirkan screenshot pengujian anda dan lakukan analisa

```
Router# show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
icmp 200.1.1.251:13 192.168.1.3:13 200.10.0.2:13 200.10.0.2:13
icmp 200.1.1.251:14 192.168.1.3:14 200.10.0.2:14 200.10.0.2:14
icmp 200.1.1.251:15 192.168.1.3:15 200.10.0.2:15 200.10.0.2:15
icmp 200.1.1.251:16 192.168.1.3:16 200.10.0.2:16 200.10.0.2:16
tcp 200.1.1.251:1024 192.168.1.5:1027 200.10.0.2:80 200.10.0.2:80
tcp 200.1.1.251:1027 192.168.1.2:1027 200.10.0.2:21 200.10.0.2:21
tcp 200.1.1.251:1029 192.168.1.4:1029 200.10.0.2:21 200.10.0.2:21
```

Hasil Pengujian:

- a. PC0



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.10.0.2

Pinging 200.10.0.2 with 32 bytes of data:

Request timed out.
Reply from 200.10.0.2: bytes=32 time=2ms TTL=125
Reply from 200.10.0.2: bytes=32 time=2ms TTL=125
Reply from 200.10.0.2: bytes=32 time=2ms TTL=125

Ping statistics for 200.10.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

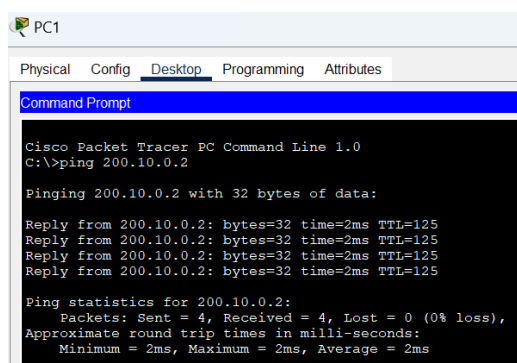
C:\>ping 200.10.0.2

Pinging 200.10.0.2 with 32 bytes of data:

Reply from 200.10.0.2: bytes=32 time=2ms TTL=125
Reply from 200.10.0.2: bytes=32 time=3ms TTL=125
Reply from 200.10.0.2: bytes=32 time=12ms TTL=125
Reply from 200.10.0.2: bytes=32 time=2ms TTL=125

Ping statistics for 200.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 4ms
```

- b. PC1



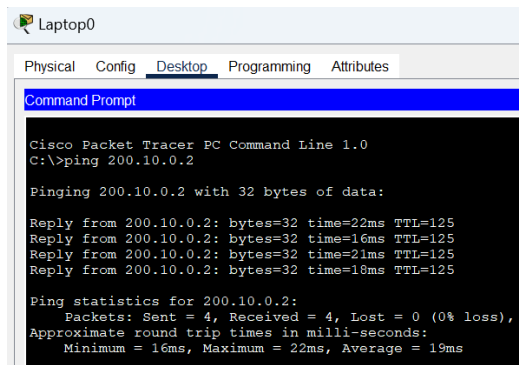
```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.10.0.2

Pinging 200.10.0.2 with 32 bytes of data:

Reply from 200.10.0.2: bytes=32 time=2ms TTL=125
Reply from 200.10.0.2: bytes=32 time=2ms TTL=125
Reply from 200.10.0.2: bytes=32 time=2ms TTL=125
Reply from 200.10.0.2: bytes=32 time=2ms TTL=125

Ping statistics for 200.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

c. Laptop0



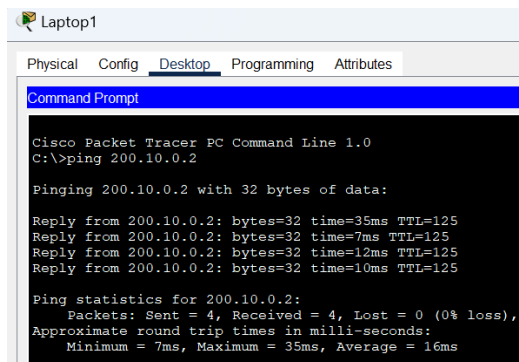
```
Laptop0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.10.0.2

Pinging 200.10.0.2 with 32 bytes of data:

Reply from 200.10.0.2: bytes=32 time=22ms TTL=125
Reply from 200.10.0.2: bytes=32 time=16ms TTL=125
Reply from 200.10.0.2: bytes=32 time=21ms TTL=125
Reply from 200.10.0.2: bytes=32 time=18ms TTL=125

Ping statistics for 200.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 22ms, Average = 19ms
```

d. Laptop1



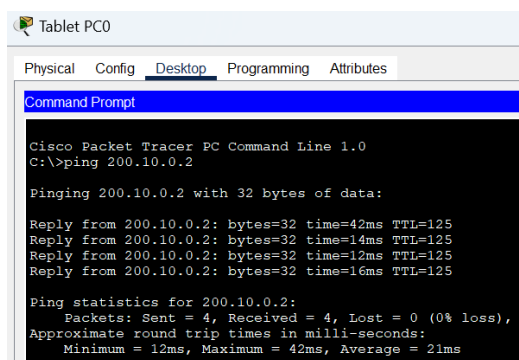
```
Laptop1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.10.0.2

Pinging 200.10.0.2 with 32 bytes of data:

Reply from 200.10.0.2: bytes=32 time=35ms TTL=125
Reply from 200.10.0.2: bytes=32 time=7ms TTL=125
Reply from 200.10.0.2: bytes=32 time=12ms TTL=125
Reply from 200.10.0.2: bytes=32 time=10ms TTL=125

Ping statistics for 200.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 35ms, Average = 16ms
```

e. Tablet PC0



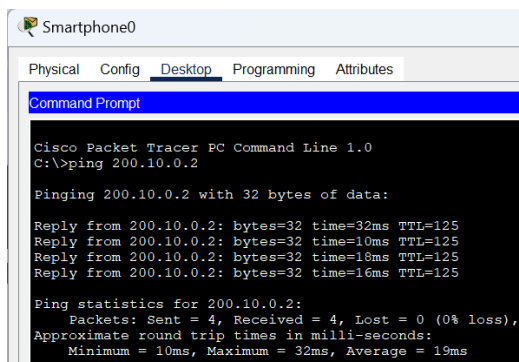
```
Tablet PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.10.0.2

Pinging 200.10.0.2 with 32 bytes of data:

Reply from 200.10.0.2: bytes=32 time=42ms TTL=125
Reply from 200.10.0.2: bytes=32 time=14ms TTL=125
Reply from 200.10.0.2: bytes=32 time=12ms TTL=125
Reply from 200.10.0.2: bytes=32 time=16ms TTL=125

Ping statistics for 200.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 42ms, Average = 21ms
```

f. Smartphone0



```
Smartphone0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.10.0.2

pinging 200.10.0.2 with 32 bytes of data:

Reply from 200.10.0.2: bytes=32 time=32ms TTL=125
Reply from 200.10.0.2: bytes=32 time=10ms TTL=125
Reply from 200.10.0.2: bytes=32 time=18ms TTL=125
Reply from 200.10.0.2: bytes=32 time=16ms TTL=125

Ping statistics for 200.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 32ms, Average = 19ms
```

```
Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 200.1.1.3:13       192.168.1.3:13    200.10.0.2:13      200.10.0.2:13
icmp 200.1.1.3:14       192.168.1.3:14    200.10.0.2:14      200.10.0.2:14
icmp 200.1.1.3:15       192.168.1.3:15    200.10.0.2:15      200.10.0.2:15
icmp 200.1.1.3:16       192.168.1.3:16    200.10.0.2:16      200.10.0.2:16
```

```
Router#show ip nat statistics
Total translations: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial2/0
Inside Interfaces: FastEthernet0/0
Hits: 47 Misses: 48
Expired translations: 44
Dynamic mappings:
-- Inside Source
access-list 1 pool dynpool refCount 4
pool dynpool: netmask 255.255.255.0
start 200.1.1.1 end 200.1.1.5
type generic, total addresses 5 , allocated 1 (20%), misses 0
```

#### 4. Analisa

Pada Praktikum Keenam ini juga dilakukan percobaan dynamic NAT dan PAT, yang mana konfigurasi translasi alamat IP secara dinamis dalam lingkungan jaringan yang kompleks dengan skenario yang mencakup berbagai jenis perangkat dan protokol. Topologi jaringan yang digunakan mencakup dua router utama yang menghubungkan jaringan privat ke jaringan publik dan perangkat end-device seperti PC, laptop, tablet, smartphone, dan server. Koneksi dilakukan melalui media kabel dan nirkabel wireless, meniru konfigurasi jaringan dunia nyata yang heterogen. IP address pada end device dikonfigurasi secara statis, namun terdapat opsi untuk menggunakan DHCP jika diperlukan. Tujuan utama dari praktik ini adalah mengevaluasi performa Dynamic NAT dan PAT dalam mengatur lalu lintas keluar dari jaringan lokal menuju jaringan publik. Melalui topologi ini, diharapkan dapat diamati bagaimana NAT bekerja dalam membatasi atau melancarkan akses keluar, serta bagaimana router menangani alokasi IP publik secara efisien.

Diawal konfigurasi difokuskan pada penetapan alamat IP pada masing-masing interface router serta pengaturan NAT. Interface yang mengarah ke jaringan lokal diberi peran sebagai ip nat inside, sedangkan interface yang mengarah ke jaringan luar sebagai ip nat outside. Router0, yang terhubung ke perangkat lokal, memiliki konfigurasi NAT inside pada FastEthernet0/0 dan NAT outside pada Serial2/0, sementara Router2 dikonfigurasi secara serupa sesuai perannya dalam topologi. Penetapan ini penting agar router dapat menentukan arah translasi alamat, dan menghindari kebingungan dalam pemrosesan paket masuk dan keluar. Kesalahan dalam penetapan inside dan outside interface dapat menyebabkan translasi gagal berjalan meskipun perintah NAT telah dikonfigurasi. Tahapan ini menjadi fondasi bagi proses translasi IP yang akan dilakukan pada prosedur selanjutnya.

Lalu untuk mengaktifkan Dynamic NAT, diperlukan konfigurasi access list (ACL) yang berfungsi menyaring lalu lintas dari jaringan privat. Access list yang dibuat mengizinkan trafik dari subnet 192.168.1.0/24, yang merupakan alamat jaringan privat semua perangkat end-user. Selain ACL, pool alamat IP publik didefinisikan dengan rentang tertentu, yakni 200.1.1.1 hingga 200.1.1.5, menyediakan lima alamat yang dapat dipinjam secara dinamis oleh perangkat privat saat melakukan akses ke luar. Hubungan antara ACL dan pool tersebut kemudian diikat melalui perintah ip nat inside source list 1 pool dynpool. Dengan konfigurasi ini, router hanya akan menerjemahkan alamat IP yang berasal dari subnet tertentu, ke dalam salah satu alamat publik dari pool yang tersedia. Hal

ini menunjukkan bahwa konfigurasi NAT tidak hanya tentang translasi, tetapi juga mencakup kontrol terhadap siapa yang boleh ditranslasikan.

Sebelum traffic dimulai, perintah `show ip nat translations` dan `show ip nat statistics` digunakan untuk melakukan verifikasi awal. Hasil menunjukkan bahwa tabel translasi masih kosong dan belum ada entri aktif, karena belum terdapat trafik yang men-trigger translasi. Ini sesuai dengan konsep dasar Dynamic NAT, yaitu translasi baru akan dibuat ketika ada permintaan dari host di dalam jaringan privat. Setelah dilakukan pengujian koneksi oleh perangkat-perangkat seperti PC, laptop, dan smartphone menuju Server0 (200.10.0.2), entri NAT mulai muncul pada tabel. Tercatat bahwa beberapa perangkat mendapatkan inside global dari pool secara dinamis, namun ketika lebih dari lima perangkat mencoba melakukan koneksi simultan, Laptop1 gagal mendapatkan IP publik karena pool telah habis. Hasil ini menegaskan bahwa Dynamic NAT sangat tergantung pada ketersediaan alamat IP publik dalam pool, dan memiliki keterbatasan dalam hal skalabilitas. Kondisi tersebut menjadi titik penting dalam analisa perbandingan dengan NAT Overload (PAT). Setelah perangkat keenam gagal, dilakukan konfigurasi PAT menggunakan perintah `ip nat inside source list 1 interface se2/0 overload`. Berbeda dengan Dynamic NAT biasa yang memerlukan beberapa alamat IP publik, PAT hanya membutuhkan satu alamat IP publik, dalam hal ini berasal dari interface Serial2/0. PAT memanfaatkan kombinasi alamat IP dan port unik untuk membedakan sesi koneksi dari banyak perangkat secara simultan. Hasil pengujian setelah konfigurasi PAT menunjukkan bahwa seluruh perangkat berhasil terkoneksi ke Server0 tanpa hambatan, termasuk Laptop1 yang sebelumnya gagal. Entri NAT yang tercatat memperlihatkan inside local yang sama-sama dipetakan ke satu inside global, namun dengan port yang berbeda, menunjukkan proses multiplexing yang dilakukan oleh router.

Perbandingan antara Dynamic NAT dan PAT semakin jelas terlihat dari hasil pengamatan statistik NAT. Pada Dynamic NAT, penggunaan IP publik terbatas pada kapasitas pool, dan ketika pool habis maka koneksi baru akan ditolak. Sedangkan pada PAT, satu alamat publik dapat digunakan oleh banyak perangkat tanpa batasan jumlah selama nomor port masih tersedia. Statistik NAT menunjukkan peningkatan pada jumlah hits dan alokasi aktif setelah PAT diterapkan, serta berkurangnya jumlah miss karena seluruh perangkat mendapat kesempatan melakukan koneksi. Kondisi ini menjadikan PAT solusi yang sangat efisien untuk jaringan besar atau padat perangkat, seperti kantor, kampus, atau jaringan publik. Namun, perlu diperhatikan bahwa penggunaan satu IP publik untuk semua koneksi juga dapat meningkatkan beban pemrosesan pada router, karena harus mencocokkan setiap sesi berdasarkan tuple lengkap (IP dan port).

Selain efisiensi, PAT juga memberikan keunggulan dalam keamanan dan pengelolaan koneksi. Dengan adanya multiplexing melalui port, upaya penyerangan dari luar menjadi lebih sulit dilakukan karena setiap sesi memiliki kombinasi unik. Namun, di sisi lain, kompleksitas konfigurasi dan pengawasan koneksi meningkat. Kesalahan dalam alokasi port atau overload pada satu IP publik juga dapat menyebabkan konflik koneksi atau latensi. Oleh karena itu, penggunaan PAT dalam jaringan besar tetap harus dibarengi dengan manajemen dan pemantauan yang baik. Dalam praktik ini, PAT mampu menampung koneksi lebih banyak dibandingkan Dynamic NAT dengan hasil yang stabil, membuktikan kehandalannya dalam skenario jaringan dengan beban trafik tinggi. Secara keseluruhan, praktik ini membuktikan bahwa baik Dynamic NAT maupun PAT memiliki keunggulan dan keterbatasan masing-masing, yang harus disesuaikan dengan kebutuhan dan kondisi jaringan. Dynamic NAT memberikan pengendalian lebih terhadap alokasi IP, cocok untuk jaringan skala menengah dengan pool publik terbatas. Sementara PAT menawarkan solusi efisiensi maksimum dengan memungkinkan ribuan perangkat berbagi satu IP publik melalui nomor port.

Dalam praktik ini, keberhasilan seluruh konfigurasi sangat ditentukan oleh ketepatan ACL, penetapan inside-outside interface, ketersediaan IP pool, serta validitas jalur routing antar jaringan. percobaan ini juga memperlihatkan bagaimana setiap kesalahan kecil dalam konfigurasi dapat mengganggu seluruh proses translasi dan koneksi antar jaringan.

## 5. Kesimpulan

Berdasarkan hasil praktikum Dynamic NAT dan Port Address Translation (PAT), dapat disimpulkan bahwa kedua teknik translasi alamat IP ini berperan penting dalam menghubungkan jaringan privat ke jaringan publik dengan efisien. Dynamic NAT memungkinkan alokasi alamat IP publik secara sementara dari pool yang tersedia hanya saat dibutuhkan, sehingga penggunaan sumber daya dapat dikendalikan, namun terbatas oleh jumlah alamat yang tersedia. Sebaliknya, PAT menawarkan efisiensi yang jauh lebih tinggi dengan memungkinkan banyak perangkat berbagi satu alamat IP publik melalui perbedaan nomor port, menjadikannya sangat efektif untuk jaringan berskala besar. Praktikum ini menunjukkan bahwa keberhasilan implementasi NAT sangat bergantung pada konfigurasi yang tepat terhadap interface, ACL, pool IP, dan routing antar jaringan. Selain itu, perintah verifikasi seperti `show ip nat translations` dan `debug ip nat` terbukti membantu dalam memastikan translasi berjalan sesuai yang diharapkan. Dengan mempertimbangkan kelebihan dan keterbatasan masing-masing metode, pemilihan jenis NAT harus disesuaikan dengan kebutuhan skala jaringan dan efisiensi sumber daya yang tersedia.

## 6. Tugas

6.1. Jelaskan menurut anda bagaimana perbandingan static NAT pada praktikum sebelumnya dengan dynamic NAT dan NAT overload pada praktikum kali ini

Jawab:

Static NAT yang digunakan pada praktikum sebelumnya bekerja dengan pemetaan tetap antara alamat IP privat dan publik. Setiap perangkat mendapatkan alamat publik yang khusus dan tidak berubah, sehingga cocok untuk kebutuhan seperti server yang harus selalu tersedia dari luar jaringan. Sebaliknya, Dynamic NAT pada praktikum kali ini mengalokasikan alamat publik dari pool secara sementara hanya saat perangkat memulai komunikasi, yang memberikan fleksibilitas tapi rentan kehabisan alamat jika pool terbatas. Sedangkan, NAT Overload (PAT) mengizinkan banyak perangkat berbagi satu alamat publik melalui nomor port yang berbeda, yang menjadikannya solusi paling hemat sumber daya. Sehingga, Static NAT unggul dalam konsistensi, Dynamic NAT dalam fleksibilitas, dan PAT dalam efisiensi penggunaan alamat publik.