



Hands-On Tutorial – H03

# ***Network Address Translation (NAT) & Open Shortest Path First (OSPF)***

Penulis : AAM  
Versi : 1 (20241028-0800)



© 2024, Fakultas Ilmu Komputer Universitas Indonesia  
This work is licensed under [Creative Commons Attribution-ShareAlike 4.0 International \(CC BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/) license.

## Riwayat Versi

Versi	Timestamp	Halaman	Perubahan
1	20241028-0800	Semua	Rilis Pertama
2	20241028-1230	12 & 14	Merevisi gambar code konfigurasi NAT dan menegaskan kembali instruksi DHCP pada alokasi IP
3	20241028-1750	16	Merevisi nilai slash, subnetmask, dan last ip address pada tabel alokasi IP.
4	20241028-2008	16	Merevisi beberapa kolom pada tabel router interface
5	20241029-0955	16	Merevisi beberapa entri terkait <i>first address</i> dan alamat IP <i>interface</i>
6	20241029-1510	15	Memberikan klarifikasi terhadap process-id Router Publik pada Spesifikasi
7	20241030-0925	8 & 14	Merevisi penggunaan interface
8	20241030-1645	16	Merevisi lokasi device untuk dianalisis

## Daftar Isi

Riwayat Versi .....	2
Daftar Isi .....	3
Informasi Umum .....	4
Ekspektasi Hasil Pembelajaran .....	4
Prasyarat.....	4
Deskripsi.....	4
Memahami Cisco IOS Console Modes .....	4
Network Address Translation (NAT) .....	5
Dynamic NAT Configuration .....	5
Open Shortest Path First (OSPF).....	7
Routing Protocol OSPF Configuration .....	7
Simulasi Sederhana: Tech Innovators .....	8
Topologi.....	8
Alokasi IP .....	10
Konfigurasi OSPF .....	11
Konfigurasi NAT .....	12
Spesifikasi.....	13
[8 Poin] Topologi .....	13
[2 Poin] Nilai X .....	14
[10 Poin] Alokasi IP .....	14
[29 Poin] Konfigurasi OSPF .....	15
[29 Poin] Konfigurasi NAT .....	15
[10 Poin] Uji Konektivitas .....	16
[12 Poin] Analisis .....	16
Informasi Terkait Pengumpulan Berkas .....	17
Peraturan .....	17
Keterlambatan .....	17
Plagiarisme .....	17

## Hands-On Tutorial – H03

### Network Address Translation (NAT) & Open Shortest Path First (OSPF)

#### Informasi Umum

- Tipe Tugas : Individu
- Batas Waktu Pengumpulan : Jumat, 1 November 2024 Jam 17.00 Waktu SCoLE
- Format Penamaan Berkas : **H03\_[NPM].pdf** dan **H03\_[NPM].pkt**
- *Template* Lembar Jawaban : [H03 - Kerangka Laporan](#)

#### Ekspektasi Hasil Pembelajaran

Peserta dapat menyimulasikan (C3) konfigurasi NAT dan OSPF pada jaringan menggunakan Packet Tracer.

#### Prasyarat

Sebelum mengerjakan tutorial ini, Anda diharapkan untuk mereview A01b terkait Packet Tracer dan H02 terkait IP Addressing. Selain itu, Anda juga perlu untuk mereview materi kelas terkait Network Address Translation (NAT) dan Open Shortest Path First (OSPF).

#### Deskripsi

Pada tutorial ini Anda akan mengimplementasikan dynamic NAT dan OSPF pada sebuah topologi di Packet Tracer.

Penjelasan berikutnya merupakan sejumlah panduan konfigurasi NAT dan OSPF pada Packet Tracer. Sebelum memulai konfigurasi, kita perlu memahami terlebih dahulu terkait Cisco IOS Console Modes.

#### Memahami Cisco IOS Console Modes

Cisco Internetworking Operating System (IOS) merupakan default operating system yang digunakan pada semua perangkat Cisco, dimana setiap interaksinya sebagian besar dilakukan melalui konsolnya. Sebagian besar perangkat dikontrol dari serial console, sementara beberapa perangkat terbaru dapat dikontrol melalui SSH setelah jaringan berhasil dikonfigurasi sepenuhnya.

Pada kasus ini, kita akan menggunakan serial console sebagai backwards compatibility dengan menggunakan serial console, SSH, atau metode apapun (termasuk penggunaan didalam Cisco Packet Tracer). Terdapat beberapa modes yang dapat anda gunakan untuk berinteraksi dengan jaringan pada perangkat. Hal ini ditunjukkan dengan sebuah tanda yang berada tepat disebelah kanan host name pada console interface. Sebagai contoh, pada prompt tertulis “Router>”, penanda mode ditunjukkan oleh “>”. Sebagian besar perintah hanya akan bekerja pada modes tertentu, sehingga sangat penting untuk mengetahui mode apa yang sedang anda gunakan dan cara navigasi antar mode. Berikut adalah beberapa mode yang umumnya dijumpai:

No	Mode	Penanda Mode	Perintah yang perlu diberikan (berdasarkan mode sebelumnya)
1	EXEC Mode Merupakan default mode yang ditemukan setelah proses booting.	> Contoh: Router>	-
2	Privileged EXEC Mode Merupakan mode dimana anda dapat menginstruksikan perintah query (biasanya dimulai dengan sh, misal: sh ip int br, sh vlan br, dll).	# Contoh: Router#	enable
3	Configuration Mode Mode ini adalah mode dimana anda dapat melakukan konfigurasi apa saja terkait dengan perangkat.	(config)# Contoh: Router(config)#	conf t
4	Specific Configuration Mode Mode ini ditemukan ketika anda sedang mengonfigurasi aspek tertentu pada perangkat, seperti: interface, DHCP, VLAN, etc.	(config-xxxx)# Contoh: Router(config-dhcp)#	Bervariasi tergantung pada masing-masing aspek

Pada tiap modes, anda dapat kembali pada mode sebelumnya secara berurutan dengan mengetik perintah “exit”. Sebagai contoh, anda menggunakan perintah ini untuk berpindah dari Configuration Mode ke Privileged EXEC mode.

## Network Address Translation (NAT)

NAT merupakan pemetaan atau proses translasi Private IP Address menjadi Public IP Address. Terdapat tiga tipe NAT yang umumnya ditemukan, yaitu:

1. Static NAT: Merupakan pemetaan yang dilakukan secara manual.
2. Dynamic NAT: Merupakan pemetaan yang dilakukan secara otomatis melalui pool dari IP Address. Pool IP Address yang dimaksud merupakan rentang IP Address yang dapat digunakan pada suatu jaringan. Contoh: subnet dengan IP Address 192.168.10.65 dan subnet mask 255.255.255.224, memiliki 2 PC yaitu PC A dan PC B. Apabila anda menggunakan konfigurasi Dynamic NAT, maka masing-masing perangkat yaitu PC A akan secara otomatis mendapatkan IP 192.168.10.66 dan PC B 192.168.10.67.
3. Port Address Translation (PAT): merupakan pemetaan yang dilakukan secara otomatis pada tingkatan port.

Pada dynamic NAT, setiap kali anda melakukan pemetaan antara private-public, hasil dari pemetaannya akan selalu tersimpan selama router masih berada dalam lalu lintas antara dua private address. Apabila tidak ada lalu lintas pada periode waktu tertentu, maka pemetaan akan terhapus. Sehingga IP Address dapat selalu digunakan oleh berbagai host dan client.

## Dynamic NAT Configuration

Berikut ini adalah serangkaian perintah yang dapat anda gunakan untuk meng-konfigurasi NAT pada router di Packet Tracer.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config) #ip nat pool <pool-name> <first-ip> <last-ip> netmask <subnet-mask>
Router(config) #access-list <access-list-number> permit <ip-address> <wildcard-mask>
Router(config) #ip nat inside source list <access-list-number> pool <pool-name>
Router(config) #interface <interface-name-and-number>
Router(config-if) #ip nat inside
Router(config-if) #exit
Router(config) #interface <interface-name-and-number>
Router(config-if) #ip nat outside
Router(config-if) #end
Router #
```

Penjelasan untuk tiap perintah diatas:

- **ip nat pool** <pool-name> <first-ip> <last-ip> **netmask** <subnet-mask>
  - **Tujuan:** untuk mendefinisikan rentang dari Public IP Address yang dapat digunakan oleh klien.
  - **Pool name:** merupakan nama pool yang akan digunakan (bebas, namun unik untuk masing-masing pool).
  - **First-ip** dan **last-ip:** rentang IP yang dapat digunakan oleh klien.
  - **Subnet-mask:** subnet mask yang digunakan sebagai NAT.
  - **Example:**  
**ip nat pool** my\_pool 192.168.10.64 192.168.10.95 **netmask** 255.255.255.224
- **access-list** <access-list-number> **permit** <ip-address> <wildcard-mask>
  - **Tujuan:** untuk mendefinisikan IP Address yang akan dipetakan.
  - **Access-list-number:** digunakan untuk menspesifikasikan IP Address source mana yang seharusnya ditranslasikan menjadi global IP Address. Umumnya, standar nomor IP yang digunakan yaitu diantara 1-99.
  - **Ip-address:** merupakan alamat jaringan pada subnet
  - **Wildcard-mask:** merupakan inverse dari subnet mask.
    - Berikut cara menemukan wildcard mask:
      - Misal, anda memiliki subnet mask = 255.255.255.224, maka wildcard = 0.0.0.31.
      - Sedangkan, subnet mask = 255.255.255.0, memiliki wildcard = 0.0.0.255.
    - Jika wildcard-nya adalah 0.0.0.255 dan IP Address-nya adalah 192.168.10.\*\*\*, maka NAT akan menerima segala IP yang addressnya berasal dari header 192.168.10 untuk ditranslasikan dari private ke public IP. Untuk penjelasan lebih lengkap, Cisco telah menyediakan referensi [disini](#).
- **Ip nat inside/ip nat outside**
  - **Tujuan:** menetapkan interface mana yang terhubung ke jaringan private dan interface mana yang terhubung ke jaringan publik .

- **ip nat inside source list** <access-list-number> **pool** <pool-name>
  - **Tujuan:** mengaktifasi NAT berdasarkan <access-list-number> dan <pool-name> yang telah dibuat.

## Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) salah satu algoritma yang digunakan untuk menentukan jarak tercepat dan terpendek pada suatu jaringan. OSPF merupakan link-state routing protocol algorithm yang berarti setiap router akan melakukan broadcast terkait routing table yang dimilikinya kepada setiap router yang berada pada area yang sama. Dengan kata lain, setiap router saling berbagi informasi satu sama lain.

### Routing Protocol OSPF Configuration

OSPF pada Packet Tracer butuh diaktifasi secara manual dengan mengetikan perintah pada Command Line Interface (CLI) router. Berikut ini adalah perintah konfigurasi OSPF yang dapat anda jalankan pada router di Packet Tracer.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config) #router ospf <process-id>
Router(config-router) #network <network-address> <wildcard-mask> area <area-id>
Router(config-router) #end
Router #
```

Berikut adalah penjelasan pada tiap baris perintah diatas:

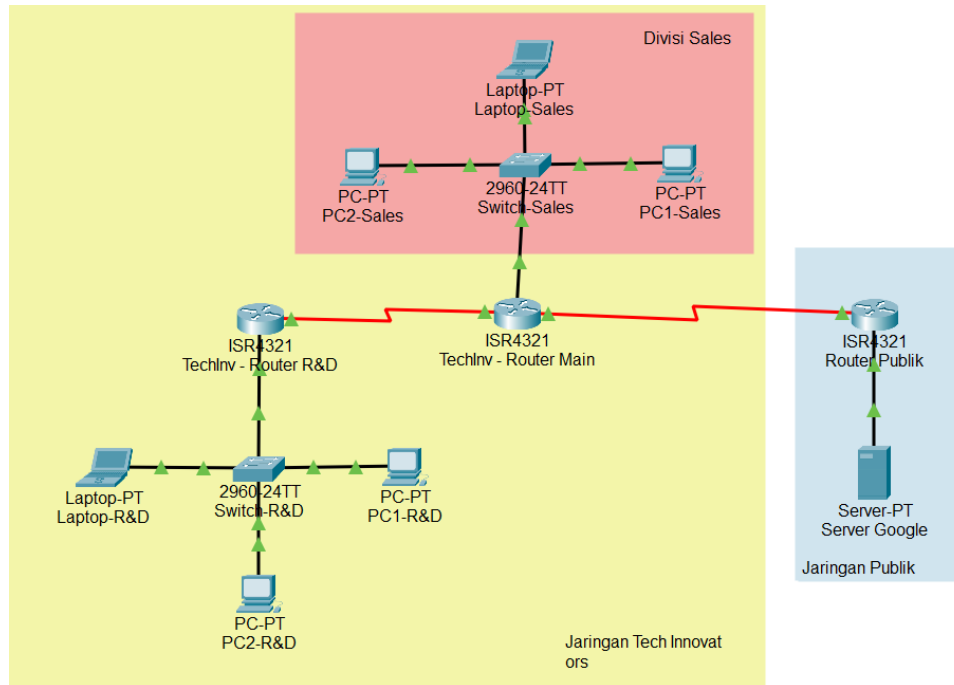
- **router ospf** <process-id>
  - **process-id:** Process id dapat diisi dengan memilih bilangan bulat positif secara acak diantara 1 hingga 65535 di Cisco Packet Tracer. Process id pada tiap router tidak perlu mirip.
  - **Tujuan:** aktivasi OSPF dan instruksi router untuk memasuki mode konfigurasi.
- **network** <network-address> <wildcard-mask> **area** <area-id>
  - **area-id:** karena kita tidak akan menggunakan hirarki pada router private, anda dapat mengatur nilainya menjadi 0 (backbone) pada seluruh router yang telah mengaktifasi OSPF.
  - **network-address:** network address dari jaringan yang akan dihubungkan.
  - **Tujuan:** mendefinisikan jaringan mana yang akan dihubungkan pada router.
  - **Beberapa catatan:**
    - Pastikan seluruh network address terhubung pada router.
    - Pastikan area-id diatur menjadi 0 untuk router-config.

## Simulasi Sederhana: Tech Innovators

**! Bagian ini tidak termasuk ke dalam penilaian, namun menjadi prasyarat untuk mengerjakan bagian spesifikasi.**

Sebuah perusahaan teknologi bernama "Tech Innovators" memiliki dua divisi yang berbeda, yaitu R&D (Research and Development) dan Sales. Masing-masing divisi memerlukan koneksi ke internet untuk mengakses layanan internet seperti Google.

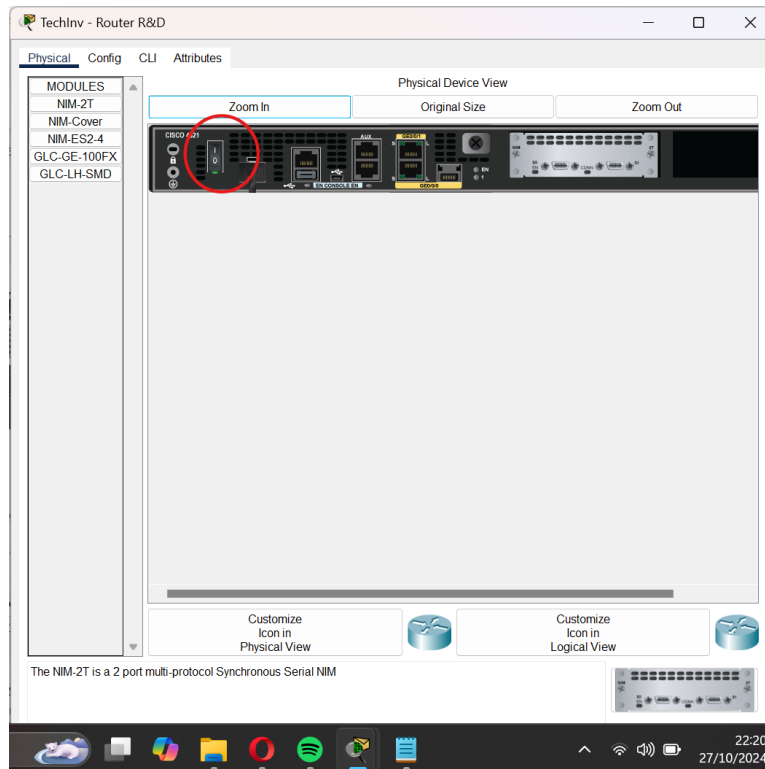
### Topologi



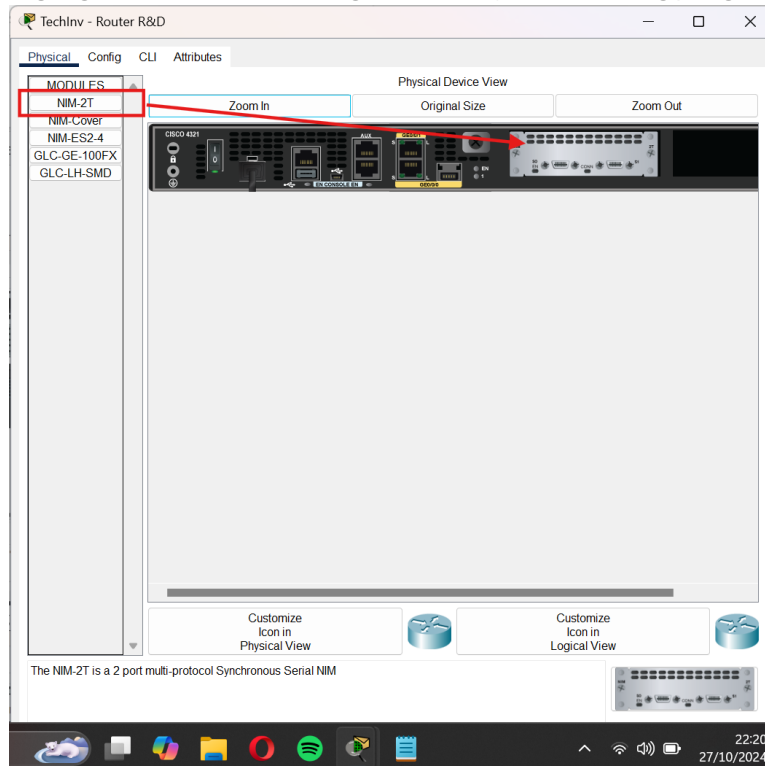
Adapun ketentuan yang berlaku pada jaringan ini, yaitu:

- Jumlah End-Device:  
Pada Divisi R&D terdapat 110 devices dalam mendukung efektivitas kegiatannya. Sedangkan Divisi Sales membutuhkan 221 devices.
- Perangkat Jaringan:
  - a. Router Perusahaan & Publik: ISR4321
  - b. Switch Perusahaan & Publik: Switch-2960
- Tipe Perkabelan:
  - a. Copper Straight Through untuk menghubungkan PC/Laptop– Switch melalui interface FastEthernet, sedangkan Switch – Router dan Router – Server melalui GigabitEthernet.
  - b. Serial DTE untuk menghubungkan Router – Router melalui interface Serial.
- Informasi Tambahan:  
Terdapat penambahan **satu modul NIM-2T pada Router**.  
Berikut adalah tata cara penambahan modul pada router:
  - a. Matikan Router terlebih dahulu.



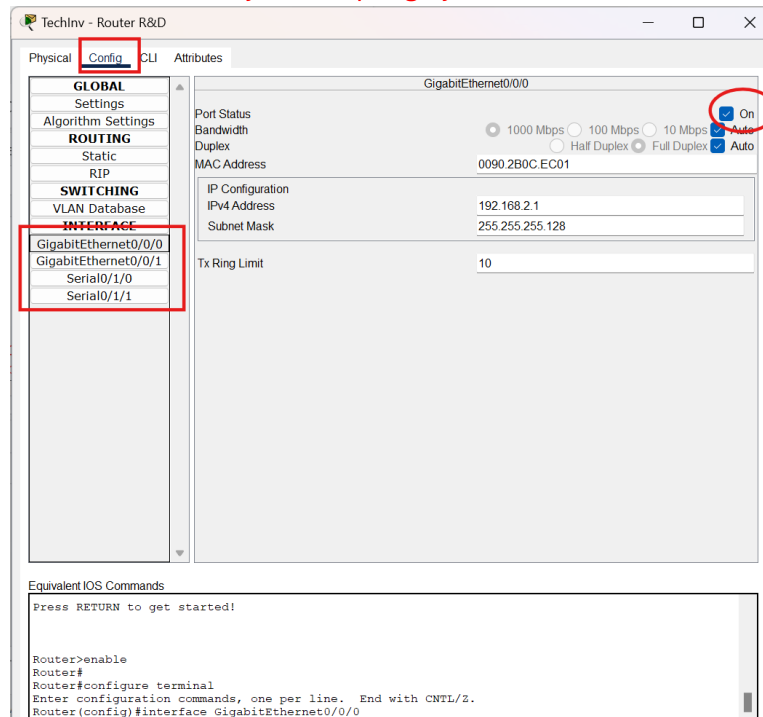


- b. Pilih modul yang ingin ditambahkan dan geser menuju slot kosong yang tersedia.



- c. Setelah terpasang, kembali nyalakan router seperti tahap 1. Kemudian aktifkan masing-masing interface pada router melalui menu “Config” dan pilih interface yang ingin

dinyalakan. **Perhatian! Mematikan router dapat menghapus seluruh konfigurasi anda!**  
**Pastikan modul ditambahkan sejak awal pengerjaan.**



## Alokasi IP

Adapun network address yang digunakan oleh jaringan perusahaan Tech Innovators yaitu 192.168.1.0/23. Dimana kebutuhannya akan dibagi menjadi 2 subnet yaitu Divisi R&D dan Divisi Sales. Selain itu, jaringan publik untuk perusahaan memiliki network address 203.0.112.0/22. Perlu diperhatikan! Rentang dari IP jaringan publik harus memetakan seluruh kebutuhan IP jaringan private.

Sedangkan distribusi IP address yang dimiliki oleh jaringan publik:

- Server Google adalah 35.191.0.0/16.

Pada Divisi R&D terdapat 110 devices dan Divisi Sales membutuhkan 221 devices. Dalam menentukan subnet, dilakukan metode VLSM pada kasus ini. Berikut adalah tabel subnettingnya.

Pada tahapan ini, pastikan anda mengimplementasikan DHCP untuk mendistribusikan IP Address pada tiap end-device dengan mengkonfigurasikannya pada tiap router. Pastikan nama pool dhcp mengikuti nama subnet yang disediakan (bukan IPD). Contoh: rnd, sales, dan publik. Untuk menghubungkan tiap router, diperlukan subnetting sebagai identitas yang dibutuhkan dalam routing table, sehingga pada tahapan ini anda perlu mempertimbangkan subnetting antar router, namun tidak perlu melakukan DHCP antar routernya.

Catatan: Meskipun pada topologi hanya tergambar dengan 3 perangkat pada tiap subnetnya, namun aturan pengalokasian IP Address tetap mengikuti ketentuan yang diberikan.

Subnet	Network Address	Slash	Subnet Mask	First Device IP Address	Last Device IP Address	Default Gateway
Divisi Sales	192.168.1.0	/24	255.255.255.0	192.168.1.2	192.168.1.254	192.168.1.1
Divisi R&D	192.168.2.0	/25	255.255.255.128	192.168.2.2	192.168.2.126	192.168.2.1

Berikut adalah alokasi IP Address untuk tiap router:

Router	Interface	IPv4 Address	Subnet Mask
Router-R&D	Serial0/1/0	192.168.2.129	255.255.255.252
	GigabitEthernet0/0/0	192.168.2.1	255.255.255.128
Router-Main	Serial0/1/0	192.168.2.130	255.255.255.252
	GigabitEthernet0/0/0	192.168.1.1	255.255.255.0
	Serial0/1/1	203.0.112.1	255.255.252.0
Router Publik	Serial0/1/1	203.0.112.2	255.255.252.0
	GigabitEthernet0/0/0	35.191.0.1	255.255.0.0

## Konfigurasi OSPF

Pada bagian ini, anda akan mengkonfigurasi OSPF pada seluruh router. Berikut adalah konfigurasi pada tiap routernya.

- Router R&D:

```
Router(config)#router ospf 1
Router(config-router)# network 192.168.2.0 0.0.0.127 area 0
Router(config-router)# network 192.168.2.128 0.0.0.3 area 0
```

- Router Main:

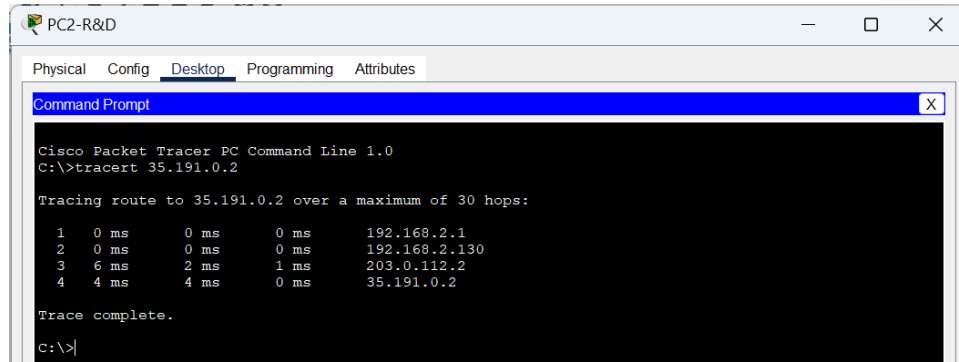
```
Router(config)#router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 203.0.112.0 0.0.3.255 area 0
Router(config-router)# network 192.168.2.128 0.0.0.3 area 0
```

- Router Publik:

```
Router(config)#router ospf 1
Router(config-router)# network 203.0.112.0 0.0.3.255 area 0
Router(config-router)# network 35.191.0.0 0.0.255.255 area 0
```

Perhatikan, pastikan jaringan yang anda masukkan ke konfigurasi ospf yang berada pada suatu router merupakan jaringan yang terhubung secara langsung pada router tersebut.

Untuk memastikan apakah konfigurasi anda berhasil, anda perlu melakukan uji coba sederhana dengan menggunakan perintah "tracert <ip address tujuan>". Berikut adalah contoh ketika anda berhasil mengkonfigurasi OSPF yang menghubungkan PC2-R&D ke Server Google:



```
PC2-R&D
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 35.191.0.2

Tracing route to 35.191.0.2 over a maximum of 30 hops:

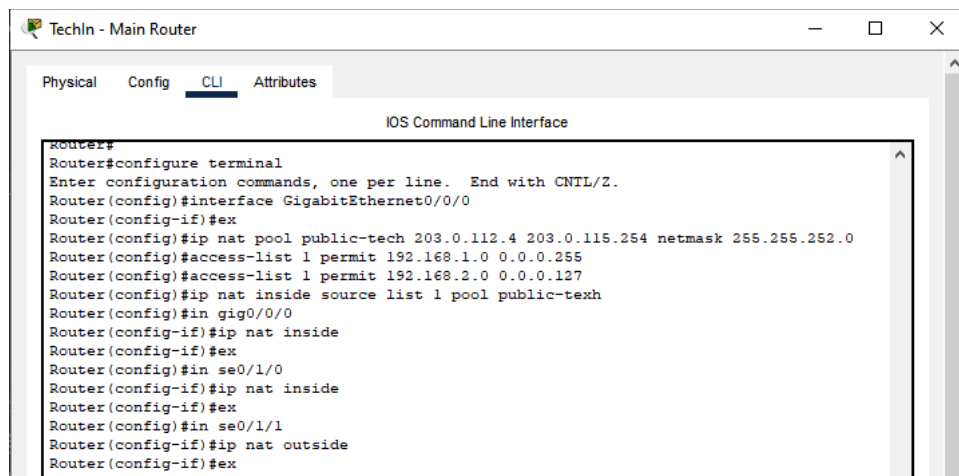
  0  0 ms    0 ms    0 ms    192.168.2.1
  1  0 ms    0 ms    0 ms    192.168.2.130
  2  6 ms    2 ms    1 ms    203.0.112.2
  3  4 ms    4 ms    0 ms    35.191.0.2

Trace complete.

C:\>|
```

## Konfigurasi NAT

Pada bagian ini, anda akan mengkonfigurasi NAT pada Main-Router. Berikut adalah konfigurasinya:



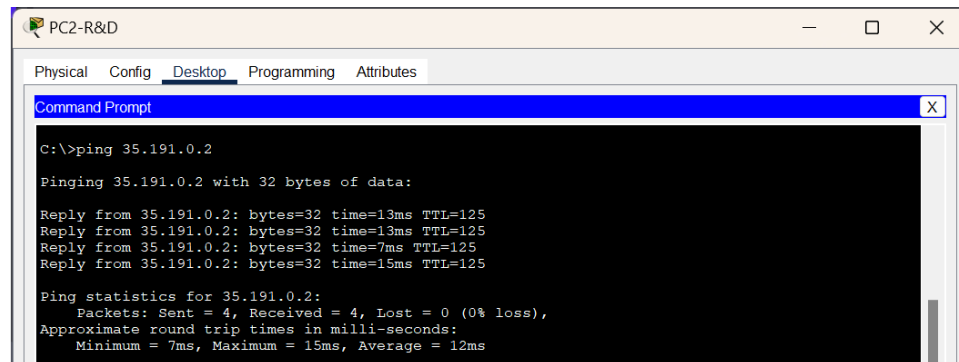
```
TechIn - Main Router
Physical Config CLI Attributes
IOS Command Line Interface

Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ex
Router(config)#ip nat pool public-tech 203.0.112.4 203.0.115.254 netmask 255.255.252.0
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 1 permit 192.168.2.0 0.0.0.127
Router(config)#ip nat inside source list 1 pool public-tech
Router(config)#in gig0/0/0
Router(config-if)#ip nat inside
Router(config-if)#ex
Router(config)#in se0/1/0
Router(config-if)#ip nat inside
Router(config-if)#ex
Router(config)#in se0/1/1
Router(config-if)#ip nat outside
Router(config-if)#ex
```

Penjelasan:

- Baris 4: membuat pool dengan nama “public-tech” yang memuat alamat IP Publik dari jaringan perusahaan Tech Innovators. Perlu diperhatikan bahwa range IP Address yang diberikan diatas mungkin tidak sesuai dengan alokasi pada subnetmasknya karena range yang ditetapkan tidak menginclude IP yang digunakan pada antar-router. Selain itu, anda dapat juga memperkecil range IP-nya sesuai dengan range IP yang ingin digunakan untuk translasi.
- Baris 5-6: membuat access-list dengan id “1” yang memuat alamat IP Lokal/ Private dari jaringan perusahaan Tech Innovators.
- Baris 7: Mendeklarasikan bahwa jaringan lokal berada pada access-list dengan ID “1” dan akan ditranslasikan pada jaringan pool dengan nama “public-tech”
- Baris 8-16: Mendeklarasikan interface mana saja yang terhubung ke jaringan lokal perusahaan dan interface mana saja yang terhubung ke jaringan publik.

Untuk memastikan apakah konfigurasi anda berhasil, anda perlu melakukan uji coba sederhana dengan menggunakan perintah “ping <ip address tujuan>”. Berikut adalah contoh ketika anda berhasil mengkonfigurasi NAT yang menghubungkan PC2-R&D ke Server Google:



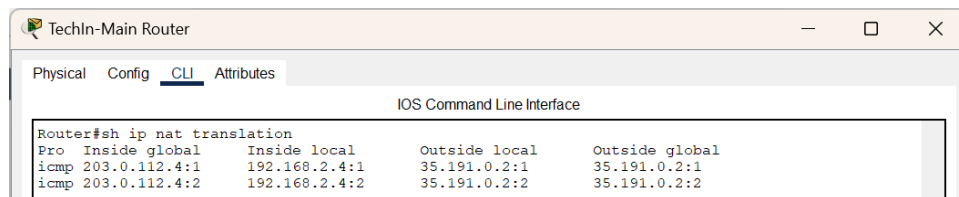
```
PC2-R&D
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 35.191.0.2

Pinging 35.191.0.2 with 32 bytes of data:

Reply from 35.191.0.2: bytes=32 time=13ms TTL=125
Reply from 35.191.0.2: bytes=32 time=13ms TTL=125
Reply from 35.191.0.2: bytes=32 time=7ms TTL=125
Reply from 35.191.0.2: bytes=32 time=15ms TTL=125

Ping statistics for 35.191.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 15ms, Average = 12ms
```

Kemudian, periksa lah hasil translasi yang dilakukan oleh Main-Router melalui CLI dengan menggunakan perintah “sh ip nat translation”. Berikut adalah contohnya:



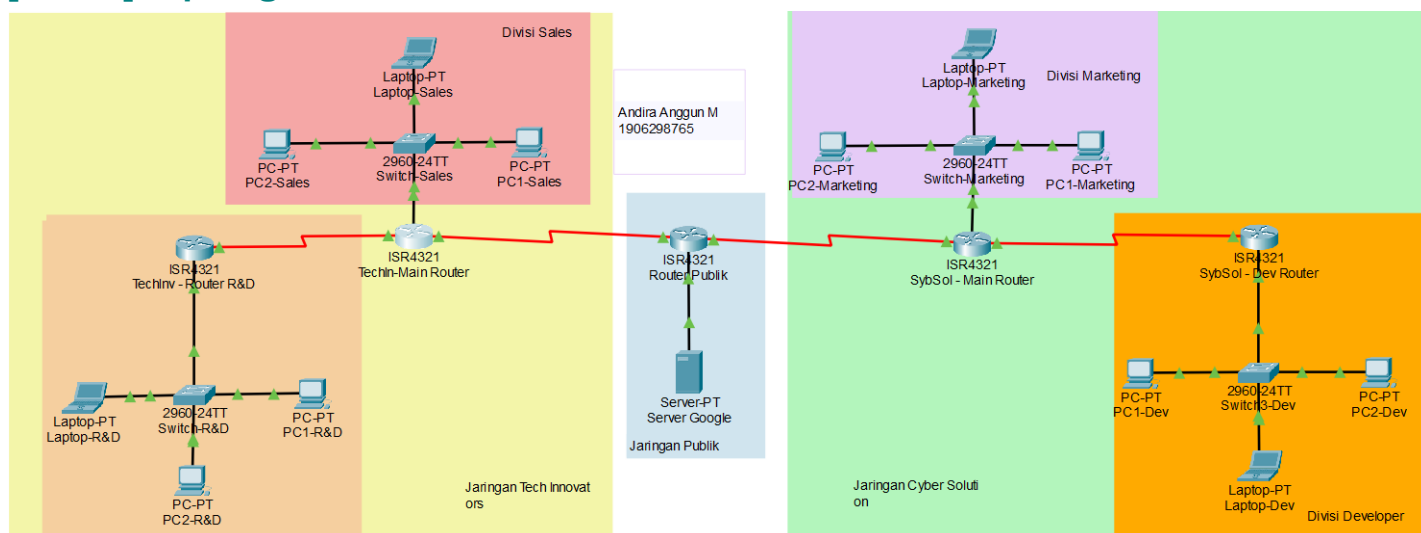
```
TechIn-Main Router
Physical Config CLI Attributes
IOS Command Line Interface

Router#sh ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 203.0.112.4:1      192.168.2.4:1      35.191.0.2:1       35.191.0.2:1
icmp 203.0.112.4:2      192.168.2.4:2      35.191.0.2:2       35.191.0.2:2
```

## Spesifikasi

Pada bagian ini, anda akan melanjutkan topologi diatas dan menghubungkannya dengan jaringan pada Perusahaan Cyber Solution. Selain itu, anda akan diminta untuk mengimplementasikan konfigurasi OSPF dan NAT pada jaringan tersebut. Pastikan juga anda membaca template lembar jawaban terlebih dahulu untuk membantu anda mengidentifikasi kebutuhan apa saja yang diminta pada tugas ini.

## [8 Poin] Topologi



Pada bagian ini, lanjutkan topologi sebelumnya menjadi topologi seperti gambar di atas. Lampirkan tangkapan layarnya pada lembar jawaban. Perhatikan bahwa:

- 1) Berikan nama dan npm pada topologi. **Anda tidak akan mendapatkan skor untuk nomor ini jika tidak ada nama dan npm pada topologi.**
- 2) Pastikan setiap perangkat memiliki nama yang sama seperti contoh
- 3) Pastikan tipe perangkat yang digunakan:
  - a. Router Perusahaan: ISR4321
  - b. Switch Perusahaan: 2960
- 4) Pastikan tipe kabel yang digunakan:
  - a. Copper Straight Through untuk menghubungkan PC/Laptop– Switch melalui interface FastEthernet, sedangkan Switch – Router dan Router – Server melalui GigabitEthernet.
  - b. Serial DTE untuk menghubungkan Router – Router melalui interface Serial.
- 5) Sebelum menggunakan kabel DTE, pastikan pada Router Security Solution sudah dipasang modul 2T dan router sudah dinyalakan kembali.

## [2 Poin] Nilai X

Pada tugas ini, anda akan diminta untuk mengganti variabel X dengan suatu nilai konstan dengan cara mengambil hasil modulo 256 dari tiga digit terakhir NPM kamu. Misalnya, jika NPM kamu adalah 2006123456, maka tiga digit terakhirnya adalah 456 dan nilai X yang akan kamu gunakan adalah  $456 \bmod 256 = 200$ .

## [10 Poin] Alokasi IP

Adapun network address yang digunakan oleh jaringan perusahaan Cyber Solution yaitu 10.X.0.0/21. Dimana kebutuhannya akan dibagi menjadi 2 subnet yaitu Divisi Developer dan Divisi Marketing. Selain itu, jaringan publik untuk perusahaan memiliki network address 198.X.96.0/20. Perlu diperhatikan! Rentang dari IP jaringan publik harus memetakan seluruh kebutuhan IP jaringan private.

Pada Divisi Developer terdapat 180 PC, 20 Printer, dan 180 Laptop. Sedangkan Divisi Marketing membutuhkan 350 Laptop, 50 Printer, dan 200 PC. Dalam menentukan subnet, dilakukan metode VLSM pada kasus ini. Berikut adalah tabel subnettingnya. Jangan lupa untuk melengkapi tabel dibawah ini terlebih dahulu.

Pada tahapan ini, pastikan anda mengimplementasikan DHCP untuk mendistribusikan IP Address pada tiap end-device dengan mengkonfigurasikannya pada tiap router. Pastikan nama pool dhcp mengikuti nama subnet yang disediakan (bukan IPD). Contoh: marketing, developer, dan publik. Untuk menghubungkan tiap router, diperlukan subnetting sebagai identitas yang dibutuhkan dalam routing table, sehingga pada tahapan ini anda perlu mempertimbangkan subnetting antar router, namun tidak perlu melakukan DHCP antar routernya.

Catatan: Meskipun pada topologi hanya tergambar dengan 3 perangkat pada tiap subnetnya, namun aturan pengalokasian IP Address tetap mengikuti ketentuan yang diberikan.

Subnet	Network Address	Slash	Subnet Mask	First Device IP Address	Last Device IP Address	Default Gateway
Divisi Marketing	10.X.0.0	/22		10.X.0.2	10.X.3.254	
Divisi Developer		/22	255.255.252.0	10.X.4.2		10.X.4.1

Berikut adalah alokasi IP Address untuk tiap router:

Router	Interface	IPv4 Address	Subnet Mask
Router-CybSol-Developer	Serial0/1/1	10.X.8.1	255.255.255.252
	GigabitEthernet0/0/0	10.X.4.1	255.255.252.0
Router-CybSol-Main	Serial0/1/1	10.X.8.2	255.255.255.252
	GigabitEthernet0/0/0	10.X.0.1	255.255.252.0
	Serial0/1/0	198.X.96.1	255.255.240.0
Router Publik	Serial0/1/0	198.X.96.2	255.255.240.0

Jangan lupa masukkan tangkapan layar hasil konfigurasi alamat IP setiap perangkat di lembar jawaban.

### [29 Poin] Konfigurasi OSPF

Pada bagian ini, lakukan konfigurasi OSPF pada Router Developer dan Router Main milik perusahaan Cyber Solution. **Perhatikan, pada bagian process-id gunakan 3 digit dari NPM anda. Jika NPM anda 2206700023, maka process-id yang digunakan adalah 23.**

Selain itu, jangan lupa untuk memperbarui routing table yang berada pada Router Publik. **Catat bahwa process-id pada Router Publik tetap menggunakan process-id pada Simulasi Sederhana, yaitu 1 (bukan 3 digit NPM).** Cantumkan juga tangkapan layar dari konfigurasi anda di ketiga router tersebut pada lembar jawaban.

Selanjutnya, lakukan uji konektivitas menggunakan Simple PDU antara:

- PC2-Dev ke Server Google
- PC1-Marketing ke PC1-Sales

Cantumkan tangkapan layar dari hasil uji konektivitas yang dilakukan pada lembar jawaban anda. Selain itu, cantumkan juga tangkapan layar dari hasil ICMP OSI model pada uji coba pertama (PC2-Dev ke Server Google) tepatnya saat paket berada pada Server Google. Pastikan bahwa tangkapan layar anda lengkap dan terbaca secara jelas.

### [29 Poin] Konfigurasi NAT

Pada bagian ini, lakukan konfigurasi NAT pada Router Main milik perusahaan Cyber Solution. **Gunakan NPM anda sebagai nama dari NAT pool.**

Selanjutnya, lakukan uji konektivitas menggunakan Simple PDU antara:

- PC2-Marketing ke Server Google
- PC1-Dev ke PC1-R&D

Cantumkan tangkapan layar dari uji konektivitas yang dilakukan pada lembar jawaban anda. Selain itu, cantumkan juga tangkapan layar dari hasil ICMP OSI model pada uji coba pertama (PC2-Marketing ke Server Google) tepatnya saat paket berada pada Server Google. Pastikan bahwa tangkapan layar anda lengkap dan terbaca secara jelas.

### [10 Poin] Uji Konektivitas

Lakukan uji konektivitas sesuai dengan permintaan pada lembar jawaban. Jangan lupa untuk mencantumkan tangkapan layar.

### [12 Poin] Analisis

1. Pada CybSol-Router Main, interface mana yang berperan sebagai ip nat inside dan interface mana yang berperan sebagai ip nat outside? Apa yang terjadi jika keduanya ditukar?
2. Lihat OSI model pada uji coba menggunakan Simple PDU dari PC2-Dev ke Server google pada posisi At Device Router CybSol-Main dan posisi At Device Router Publik (observasi bagian In Layer nya) .
  - a. Apakah terdapat perbedaan? Jika ya, tunjukkan perbedaannya.
  - b. Jelaskan mengapa berbeda atau tidak berbeda.
3. Lakukan uji coba menggunakan Simple PDU dari PC1-R&D ke PC1-Dev.
  - a. Apakah berhasil atau gagal? Tunjukkan hasilnya.
  - b. Jelaskan mengapa hal tersebut bisa terjadi. Sertakan juga buktinya.

Hint: Lakukan analisis pada OSI Model.



## Informasi Terkait Pengumpulan Berkas

Pada tutorial ini, dokumen yang perlu Anda submit adalah:

1. Laporan (.pdf) berupa lembar jawaban yang telah diisi dengan hasil pekerjaan Anda untuk tutorial ini
2. Dokumen Packet Tracer (.pkt) hasil pengerjaan tutorial ini

Format penamaan: **H03\_[NPM Anda].pkt** dan **H03\_[NPM Anda].pdf**

## Peraturan

### Keterlambatan

Anda diharapkan dapat mengumpulkan hasil pekerjaan yang dilakukan sebelum batas waktu pengumpulan. Jika terdapat kondisi di mana Anda terpaksa terlambat mengumpulkan hasil pekerjaan, terdapat jangka waktu tambahan di mana Anda masih diperbolehkan mengumpulkan hasil pekerjaan dengan konsekuensi tertentu. Jika  $X$  adalah durasi setelah batas waktu pengumpulan yang ditetapkan sampai waktu Anda mengumpulkan hasil pekerjaan, Anda akan menerima penalti nilai pekerjaan sebagaimana diatur pada peraturan berikut ini:

- |   |  |
|---|--|
| • $X < 10$ menit                            | : Tidak ada penalti                            |
| • $10 \text{ menit} \leq X < 2 \text{ jam}$ | : 25% penalti                                  |
| • $2 \text{ jam} \leq X < 4 \text{ jam}$    | : 50% penalti                                  |
| • $4 \text{ jam} \leq X < 6 \text{ jam}$    | : 75% penalti                                  |
| • $X \geq 6 \text{ jam}$                    | : Cut-off (Pekerjaan anda tidak akan diterima) |

### Plagiarisme

Anda diperbolehkan berdiskusi tentang pekerjaan Anda dengan peserta kuliah lain atau pihak lainnya, namun Anda harus memastikan bahwa **semua pekerjaan yang dikumpulkan adalah murni hasil pekerjaan Anda sendiri**. Anda dilarang keras melakukan tindak plagiarisme atau kecurangan akademik lainnya. Menurut kamus daring Merriam-Webster, plagiarisme berarti:

- Mencuri dan mengklaim (ide atau kata orang lain) sebagai milik sendiri
- Menggunakan hasil (karya/pekerjaan orang lain) sebagai milik sendiri
- Melakukan pencurian literatur/sastra
- Merepresentasikan ulang sebuah ide/produk yang sudah ada sebagai sesuatu yang bersifat baru dan orisinal.

Tim pengajar memiliki hak untuk meminta klarifikasi terkait dugaan ketidakjujuran akademik, terutama plagiarisme, dan memberikan konsekuensi berupa **pengurangan nilai hasil pekerjaan atau pencabutan nilai (nilai diubah menjadi nol) untuk hasil pekerjaan yang terkonfirmasi dikerjakan secara tidak jujur**.