

Modul Pra-praktikum

IF2230 Jaringan Komputer

2 - Static & Dynamic Routing, NAT, dan Port Forwarding

Dipersiapkan oleh Sister'21

Waktu Mulai :

Selasa, 1 Oktober 2024, 15:00 WIB

Waktu Akhir :

Selasa, 8 Oktober 2024, 13:00 WIB

I. Daftar Revisi

1. Menambahkan beberapa bagian yang tidak lengkap pada NAT

II. Latar Belakang dan Peraturan

Tugas ini ditujukan untuk mempersiapkan peserta untuk praktikum pertama kuliah ini. Dengan menyelesaikan tugas ini, praktikan diharapkan memiliki persiapan dan pengetahuan dasar terhadap materi yang dibutuhkan.

Berikut topik-topik yang menjadi lingkup modul ini:

- Static Routing
- L3 Switch dan Inter-VLAN Routing
- Dynamic Routing
- NAT
- Port Forwarding

Kerjakan tugas ini dengan mengikuti peraturan-peraturan berikut:

1. **Pra-praktikum ini menjadi syarat untuk praktikum yang akan diadakan terkait modul ini. Tidak mengumpulkan tugas/modul ini akan menyebabkan nilai praktikum 0.**
2. Kumpulkan tugas Anda sesuai dengan arahan pengumpulan yang terdapat pada bagian "Deliverables". **Pengumpulan yang tidak sesuai dengan arahan akan mengurangi nilai praktikan.**
3. Praktikan diperbolehkan mengerjakan bersama-sama dengan praktikan lain dan menggunakan referensi & material yang dianggap sesuai ketentuan; namun, praktikan diharapkan memahami segala yang telah dikerjakan pada pengumpulan.
4. Praktikan tidak diperbolehkan untuk menyalin materi referensi atau pekerjaan praktikan lain secara langsung ke dalam pekerjaan praktikan.
5. Tanyakan segala pertanyaan terkait tugas ini pada sheet Q&A.
6. Revisi akan dilakukan secara langsung pada dokumen yang diberikan saat rilis dan akan ditambahkan pada bagian "Daftar Revisi". Bagian-bagian yang direvisi akan diberi warna khusus.

Segala bentuk kecurangan akademik (seperti mengganti nama dan mengumpulkan tugas praktikan lain, plagiarisme, dan sebagainya) akan mengakibatkan ketidaklulusan mata kuliah ini (dan sanksi-sanksi lain yang berlaku dalam lingkungan akademik ITB).

III. Deliverables

Kumpulkan tugas ini dengan mengikuti peraturan-peraturan berikut:

1. Buatlah salinan dari dokumen ini, dan kerjakan tugas-tugas ini pada salinan dokumen praktikan masing-masing.
2. Ikuti arahan dan instruksi yang diberikan pada setiap bagian untuk menyelesaikan pra-praktikum ini. Bagian-bagian yang perlu dikerjakan terdapat pada tabel-tabel dengan *header* kuning dan isi jawaban Anda pada bagian dengan label <Jawab>.
3. **Semua screenshot harus dapat dibaca dengan jelas. Segala screenshot yang tidak dapat dibaca dengan jelas dengan akibat apapun tidak akan dinilai.**
4. Simpan tugas Anda dengan format berikut:
5. Kumpulan tugas Anda melalui form ini. Upload dokumen Anda dengan format penamaan: IF2230_LabPrep[X]_<NIM>.pdf

IV. Modul Pra-praktikum

IV.1. Static Routing

Sebelumnya, kita mempelajari bahwa perangkat-perangkat di dua jaringan atau LAN berbeda tidak dapat saling berkomunikasi. Dalam kasus-kasus dimana kita ingin menghubungkan dua jaringan (seperti menghubungkan jaringan rumah ke internet), kita harus menggunakan ***routing***.

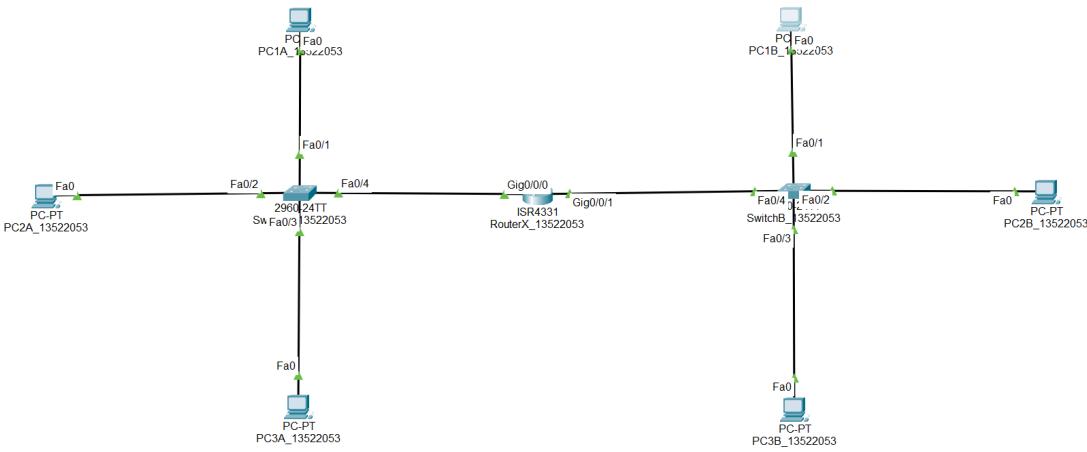
Singkatnya, ***routing*** adalah proses meneruskan ***packet*** dari sebuah jaringan ke jaringan lain. Hal ini dilakukan dengan cara memberikan setiap ***packet*** berbagai jalan yang dapat ditempuh untuk mencapai tujuannya, serta memilih dan mengarahkannya untuk mengikuti jalan yang paling optimal. Routing dilakukan oleh perangkat yang dinamakan ***router***, yang merupakan perangkat yang terhubung ke satu atau lebih jaringan dan meneruskan ***packet*** antar jaringan-jaringan tersebut. Dengan menggunakannya, kita dapat secara otomatis menghubungkan dua atau lebih jaringan (sehingga, memungkinkan pengiriman data antara keduanya), asalkan seluruhnya terhubung ke ***router*** yang sama. Perlu dicatat bahwa menghubungkan jaringan-jaringan yang tidak terhubung langsung ke ***router*** yang sama tidak dilakukan secara otomatis, dan membutuhkan konfigurasi lebih lanjut menggunakan metode-metode atau protokol-protokol yang akan dijelaskan selanjutnya.

Untuk mulai memanfaatkan kemampuan-kemampuan ***router***, pertama hubungkan seluruh perangkat (*host*) di sebuah jaringan ke ***router*** tersebut, lalu **jadikan alamat IP *router* tersebut sebagai default gateway**. ***Default gateway*** adalah alamat yang dituju oleh semua ***packet*** dengan alamat tujuan yang tidak termasuk dalam rentang alamat yang sama dengan *host* pengirim, dan yang diasumsikan akan meneruskan ***packet-packet*** tersebut ke tujuan yang seharusnya. Biasanya, alamat IP dari ***router*** (alias ***default gateway*** setiap *host*) merupakan alamat pertama atau alamat terakhir yang boleh digunakan pada rentang jaringan.

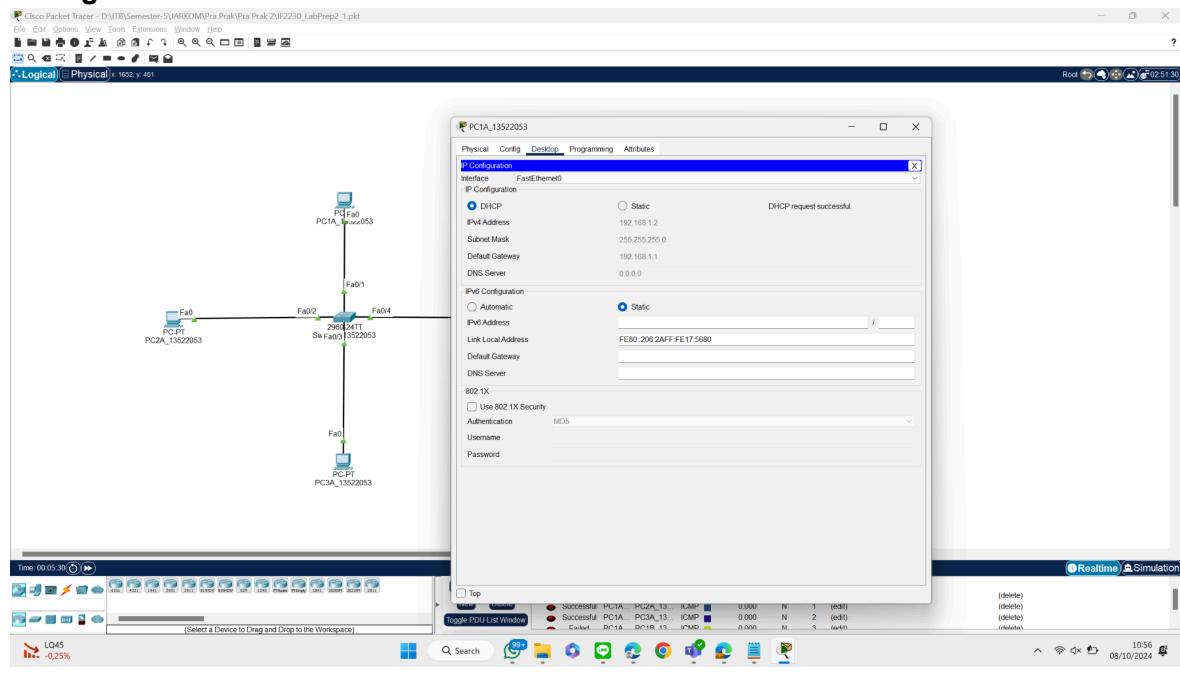
Misalnya, bayangkan sebuah jaringan sederhana 192.168.0.0/24. Alamat IP ***router*** (dan lantas, ***default gateway*** yang digunakan setiap *host*) biasanya adalah 192.168.0.1/24 atau 192.168.0.254/24. Jika sebuah komputer yang terhubung dengan jaringan tersebut hendak mengirimkan sebuah ***packet*** ke sebuah ***server*** dengan alamat 192.168.100.5/24, komputer tersebut akan mengirimkan ***packet*** tadi ke ***default gateway*-nya**, yaitu ***router*** dengan alamat 192.168.0.1/24. Dari sana, tanggung jawab meneruskan ***packet*** ke ***server*** tujuan berada pada ***router***.

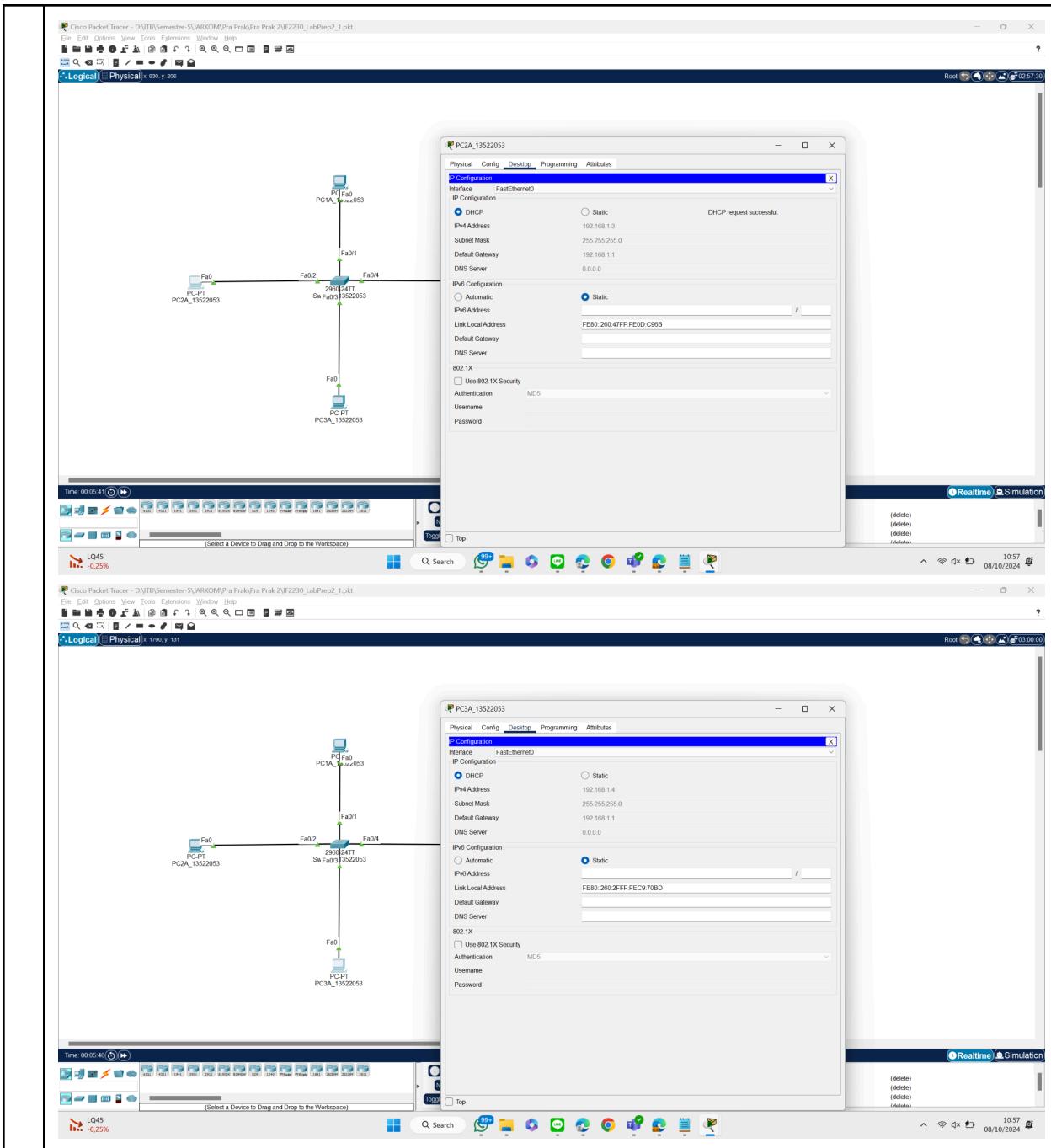
Tugas 1

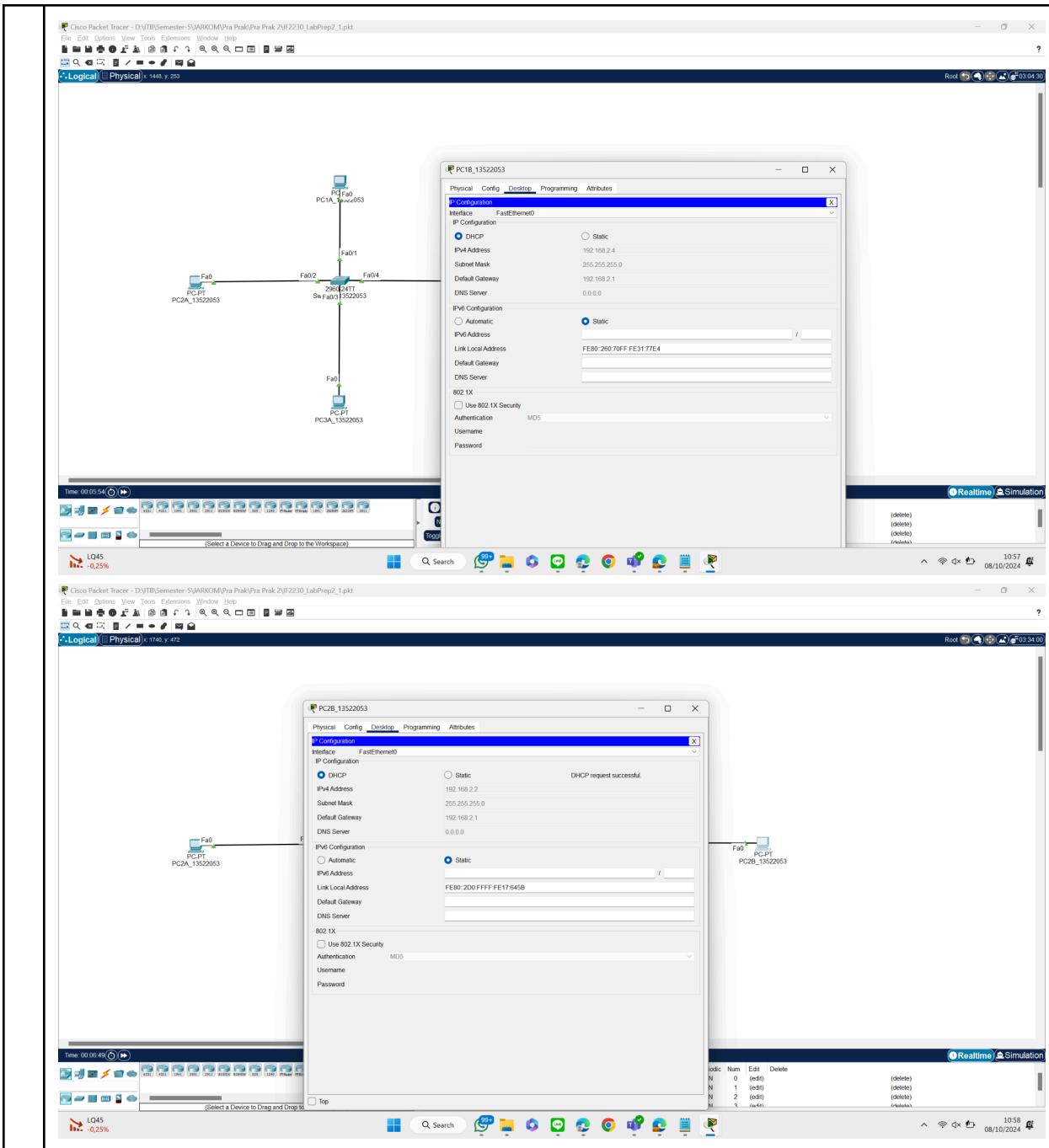
Q	<p>Di Cisco Packet Tracer, buatlah dua buah topologi bintang (A dan B), yang masing-masing terdiri atas satu <i>switch</i> 2960 yang terhubung ke tiga komputer. Kemudian, pasangkanlah sebuah <i>router</i> 4331, dan berikan <i>display name RouterX_<NIM></i>.</p> <p>Untuk topologi pertama, gunakan <i>display name</i> dan alamat IP sebagai berikut untuk setiap perangkat. Urutan penomoran PC dibebaskan:</p> <ul style="list-style-type: none"> • SwitchA_<NIM>: - • PC1A_<NIM>: DHCP • PC2A_<NIM>: DHCP • PC3A_<NIM>: DHCP <p>Untuk topologi kedua, gunakan <i>display name</i> dan alamat IP sebagai berikut untuk setiap perangkat. Urutan penomoran PC dibebaskan:</p> <ul style="list-style-type: none"> • SwitchB_<NIM>: - • PC1B_<NIM>: DHCP • PC2B_<NIM>: DHCP • PC3B_<NIM>: DHCP <p>Kemudian, hubungkan SwitchA dan SwitchB dengan RouterX sebagai berikut:</p> <ul style="list-style-type: none"> • SwitchA ke <i>interface GigabitEthernet0/0/0</i>, dan berikan alamat IP 192.168.1.1/24 • SwitchB ke <i>interface GigabitEthernet0/0/1</i>, dan berikan alamat IP 192.168.2.1/24 <p>Terakhir, konfigurasikan DHCP <i>pool</i> untuk masing-masing jaringan supaya komputer-komputer dalam masing-masing topologi dapat mendapatkan alamat IP secara otomatis. Informasi terkait DHCP dijelaskan di bawah.</p> <p>Lampirkan topologinya, kemudian coba ping semua PC dari PC1A dan PC1B. Apa yang terjadi? Lampirkan hasilnya dan jelaskan!</p>
A	<p>Konfigurasi pool DHCP</p> <pre>Router(config)#exit Router(config)#interface GigabitEthernet0/0/1 Router(config-if)#exit Router(config)#ip dhcp pool NetworkA Router(dhcp-config)#network 192.168.1.0 255.255.255.0 Router(dhcp-config)#default-router 192.168.1.1 Router(dhcp-config)#exit Router(config)#ip dhcp pool NetworkB Router(dhcp-config)#network 192.168.2.0 255.255.255.0 Router(dhcp-config)#default-router 192.168.2.1 Router(dhcp-config)#exit Router(config)#ip routing Router(config)# </pre> <p>Topologi</p>

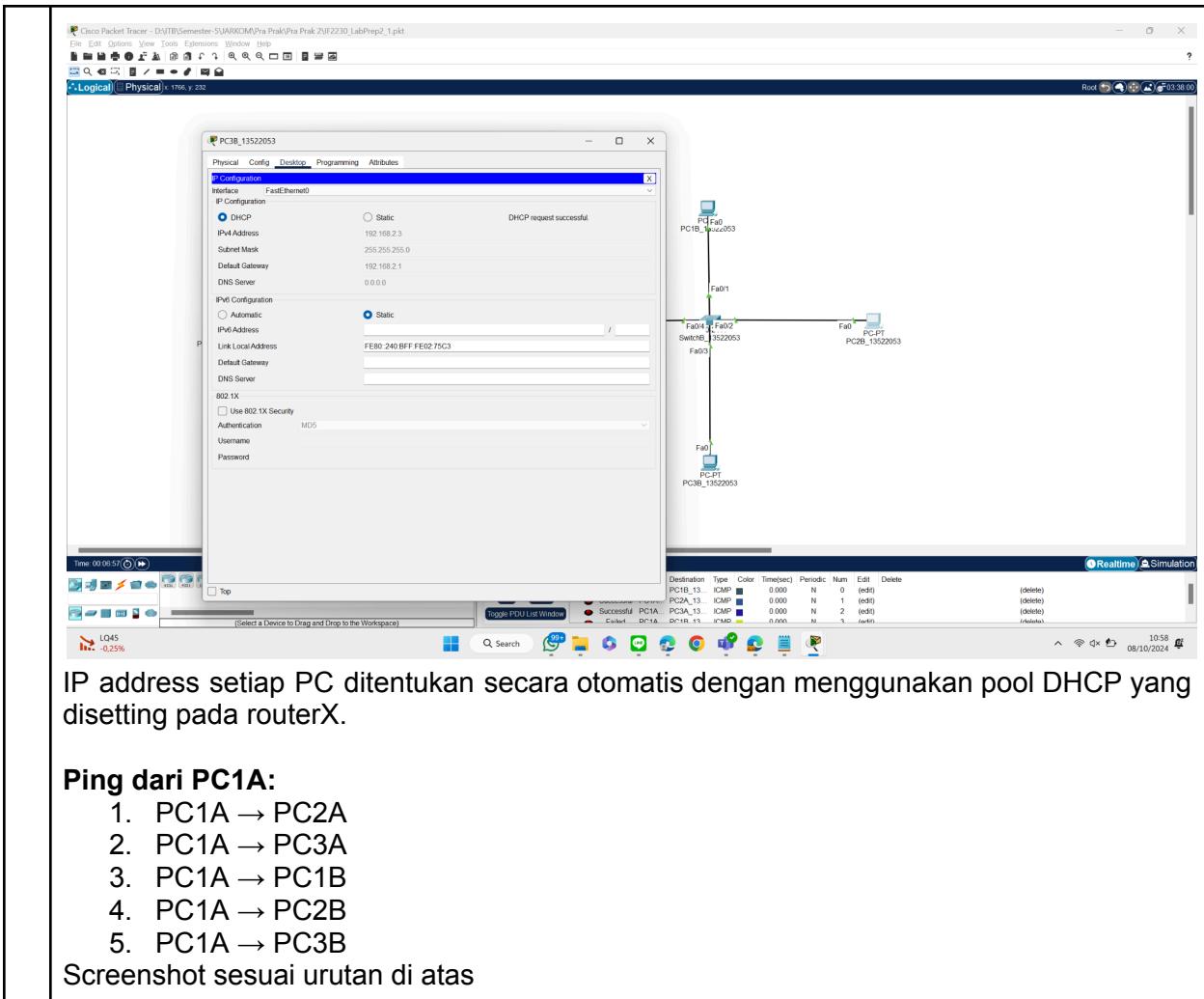


Konfigurasi IP:









IP address setiap PC ditentukan secara otomatis dengan menggunakan pool DHCP yang disetting pada routerX.

Ping dari PC1A:

1. PC1A → PC2A
2. PC1A → PC3A
3. PC1A → PC1B
4. PC1A → PC2B
5. PC1A → PC3B

Screenshot sesuai urutan di atas

PC1A_13522053

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time=3ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

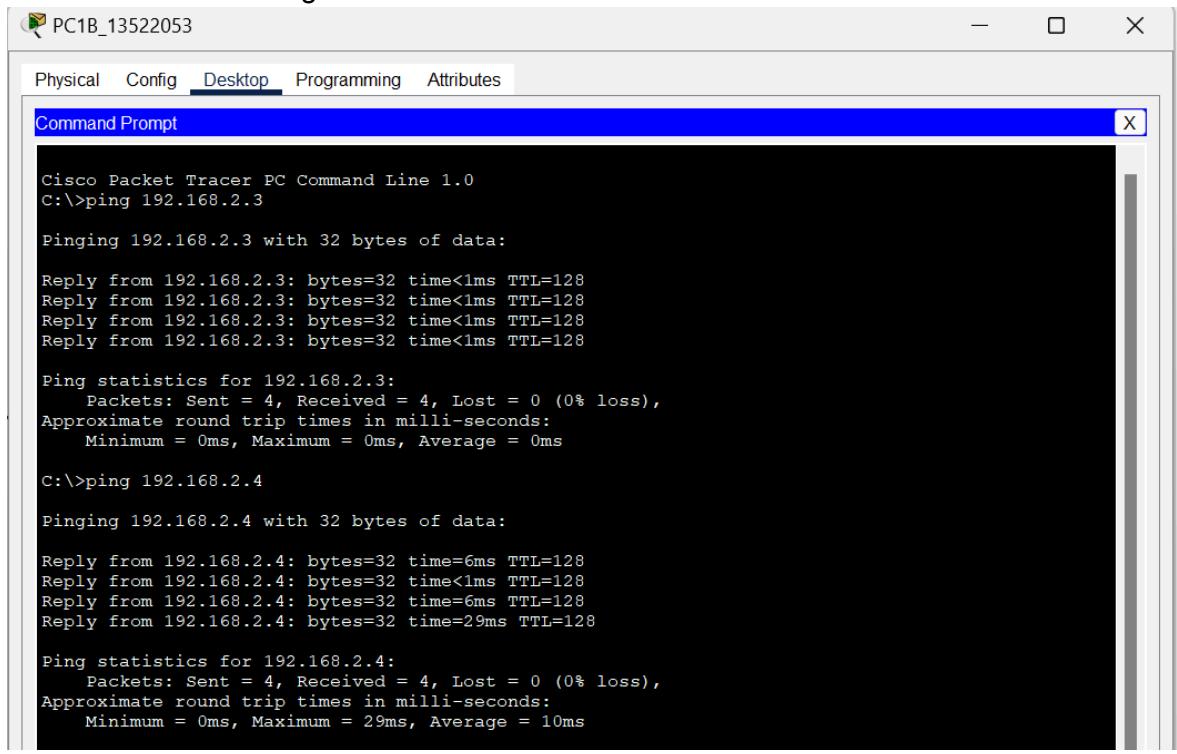
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127
Reply from 192.168.2.4: bytes=32 time=1ms TTL=127
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ping dari PC1B:

1. PC1B → PC2B
2. PC1B → PC3B
3. PC1B → PC1A
4. PC1B → PC2A
5. PC1B → PC3A

Screenshot sesuai dengan urutan di atas



The screenshot shows a Cisco Packet Tracer Command Prompt window titled "PC1B_13522053". The window has tabs for Physical, Config, Desktop (which is selected), Programming, and Attributes. The command prompt area displays the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=6ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time=6ms TTL=128
Reply from 192.168.2.4: bytes=32 time=29ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 29ms, Average = 10ms
```

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=2ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.4: bytes=32 time<1ms TTL=127
Reply from 192.168.1.4: bytes=32 time=1ms TTL=127
Reply from 192.168.1.4: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC1A dapat berkomunikasi dengan semua PC termasuk dengan PC1B, PC2B, PC3B walaupun berbeda subnet, berarti router tersebut berhasil berfungsi sebagai penghubung antara dua subnet yang berbeda, memungkinkan komunikasi lintas subnet. Begitu pula yang terjadi saat ping dari PC1B.

Dalam tugas di atas, kita telah berhasil menghubungkan dua buah jaringan dan memungkinkan komunikasi diantaranya dengan menghubungkannya ke router yang sama. Namun, bagaimana jika kita ingin menghubungkan dua jaringan yang tidak langsung terhubung seperti ini? Untuk melakukan hal tersebut, kita harus menggunakan **bentuk-bentuk dan protokol-protokol routing**. Banyak jenis yang tersedia, namun salah satu yang paling sederhana adalah **static routing**.

Static routing adalah bentuk **routing** dimana kita secara manual dan langsung memberi tahu **router** jalan yang digunakan untuk mengirim **packet** menuju alamat jaringan atau **host spesifik**. Hal ini dilakukan dengan cara menambahkan **entry** ke **routing table router**. Sebuah **entry** dalam **routing table** memberi tahu **router** ke alamat IP mana sebuah **packet** harus dikirimkan, apabila alamat tujuan **packet** sama dengan alamat pada **entry**.

Contohnya, sebuah perusahaan memiliki dua buah bangunan, A dan B. Setiap jaringan memiliki sebuah jaringan komputer dengan **router** (192.168.100.0/24 untuk A dan 192.168.200.0/24 untuk B); **router-router** ini saling terhubung satu sama lain dalam jaringan 192.168.0.0/24

(asumsikan dalam jaringan ini, *router A* memiliki alamat 192.168.0.1/24 dan *router B* memiliki alamat 192.168.0.2/24). Dalam kasus tersebut, **secara default, packet dari jaringan A tidak dapat mencapai perangkat-perangkat dalam jaringan B, dan begitu pula sebaliknya**. Untuk memungkinkan perangkat-perangkat di bangunan A untuk mengirimkan *packet*-*packet* ke perangkat-perangkat di bangunan B, **kita harus menambahkan entry static routing di router A**, supaya *router A* meneruskan seluruh *packet* yang ditujukan ke jaringan B ke alamat *router B*. Untuk itu, kita dapat menggunakan perintah berikut:

```
RouterA(config)# ip route 192.168.200.0 255.255.255.0 192.168.0.2
```

Kita dapat mengecek apakah perintah telah berhasil dengan melihat seluruh *entry static routing* di sebuah *router*, yang dapat dilakukan menggunakan GUI atau CLI dengan perintah berikut:

```
RouterA# show ip route static
```

Perhatikan bahwa konfigurasi ini tidak bekerja sebaliknya (memungkinkan host di bangunan B untuk mengirimkan packet ke bangunan A); untuk itu, kita juga harus mengkonfigurasikan atau menambahkan entry sesuai di router B.

Tugas 2

Q	<p>Gunakan hasil tugas sebelumnya.</p> <p>Pasang sebuah <i>router</i> 4331 baru, dan berikan <i>display name</i> RouterY_<NIM>. Kemudian, hubungkan <i>interface</i> GigabitEthernet0/0/0 di RouterY dengan <i>interface</i> GigabitEthernet0/0/3 di RouterX.</p> <p>Berikan alamat-alamat IP berikut untuk setiap <i>interface</i> yang baru dihubungkan:</p> <ul style="list-style-type: none">• RouterX_<NIM>: 192.168.0.1/24• RouterY_<NIM>: 192.168.0.2/24 <p>Kemudian, buatlah sebuah topologi bintang baru yang terdiri atas satu <i>switch</i> 2960 yang terhubung ke tiga komputer. gunakan <i>display name</i> dan alamat IP sebagai berikut untuk setiap perangkat. Urutan penomoran PC dibebaskan:</p> <ul style="list-style-type: none">• SwitchC_<NIM>: -• PC1C_<NIM>: DHCP• PC2C_<NIM>: DHCP• PC3C_<NIM>: DHCP <p>Kemudian, hubungkan SwitchC dengan RouterY sebagai berikut:</p>
---	--

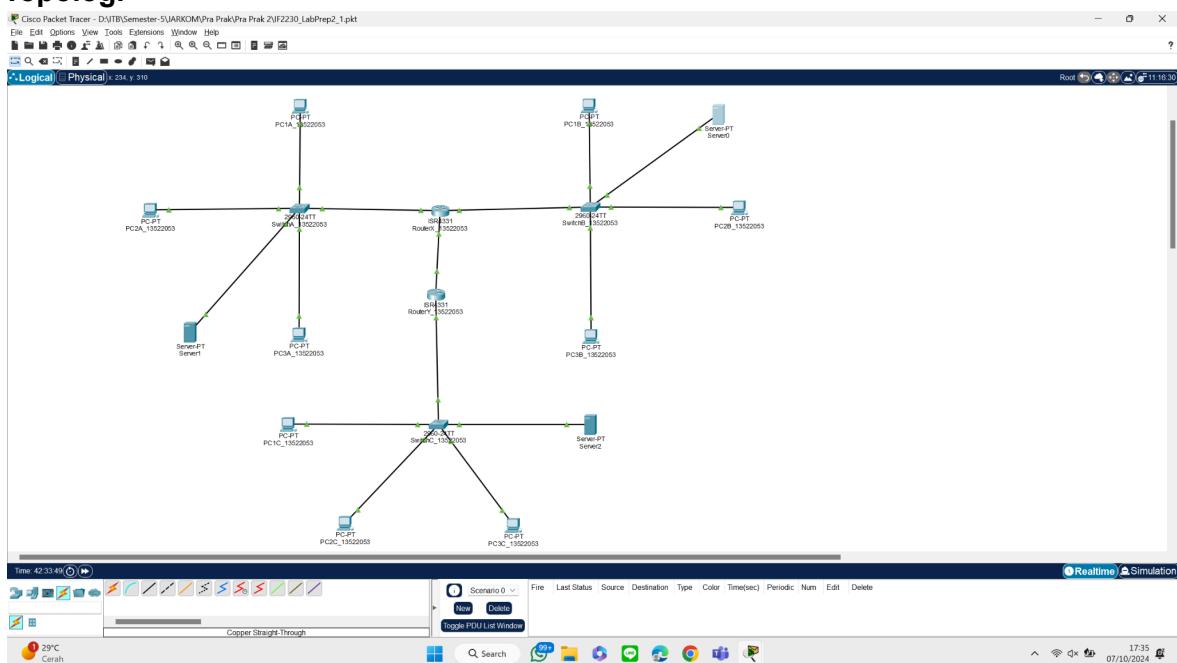
- SwitchC ke *interface GigabitEthernet0/0/2*, dan berikan alamat IP 192.168.3.1/24

Konfigurasikan DHCP *pool* untuk jaringan C supaya komputer-komputer dalam topologi C dapat mendapatkan alamat IP secara otomatis. Informasi terkait DHCP dijelaskan di bawah.

Terakhir, tambahkan konfigurasi *static routing* supaya Anda dapat melakukan ping terhadap komputer-komputer dalam topologi C dari komputer-komputer dalam topologi A.

Lampirkan topologinya, kemudian coba ping PC1C dari PC1A. Kemudian, coba ping PC1C dari PC1B. Apa yang terjadi? Lampirkan hasilnya dan jelaskan!

A Topologi



Konfigurasi DHCP pool jaringan C

PC1C_13522053

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

DHCP Static

IPv4 Address 192.168.3.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.3.2

DNS Server 0.0.0.0

IPv6 Configuration

Automatic Static

IPv6 Address /

Link Local Address FE80::20A:F3FF:FE4E:683

Default Gateway

DNS Server

802.1X

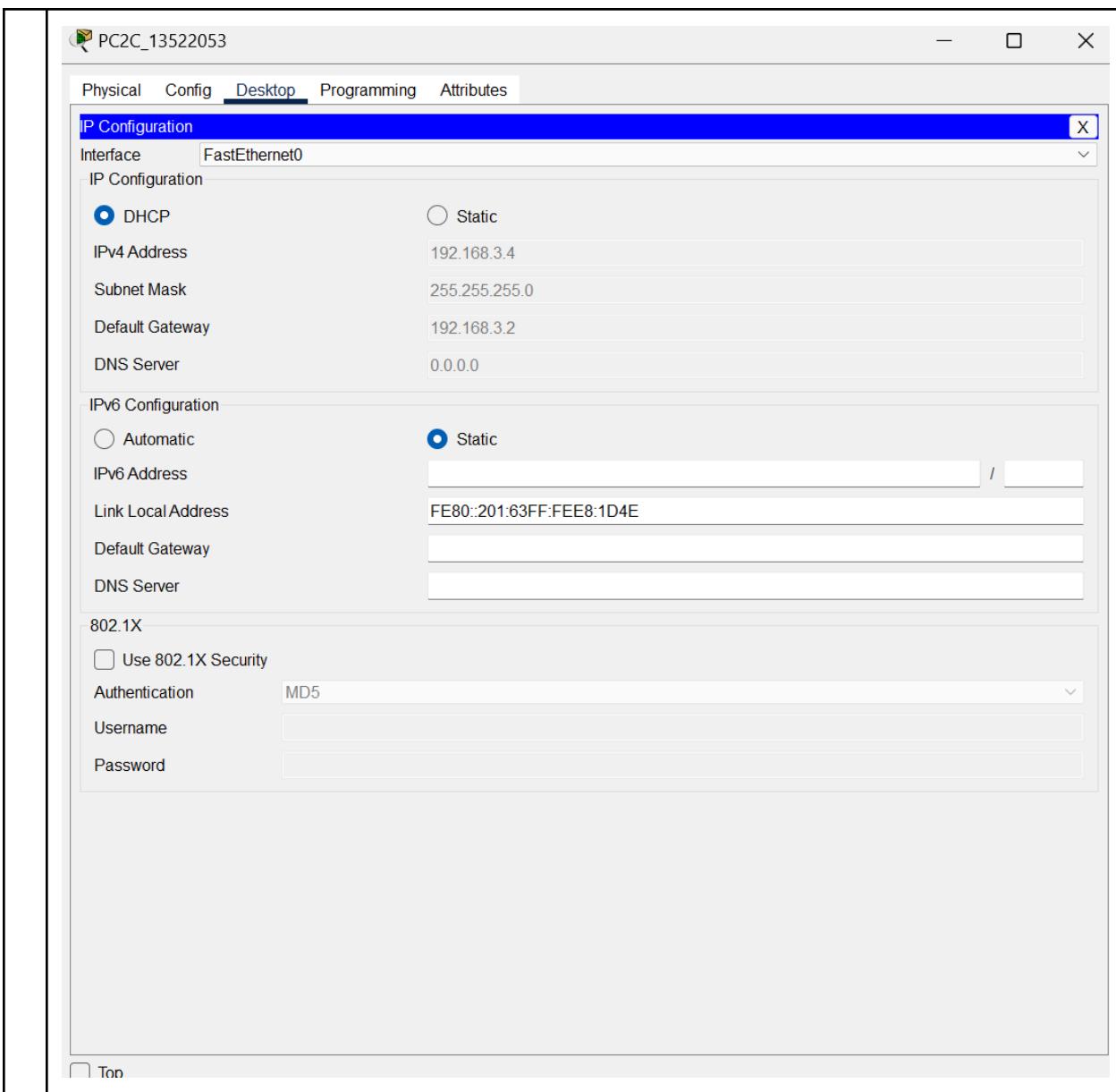
Use 802.1X Security

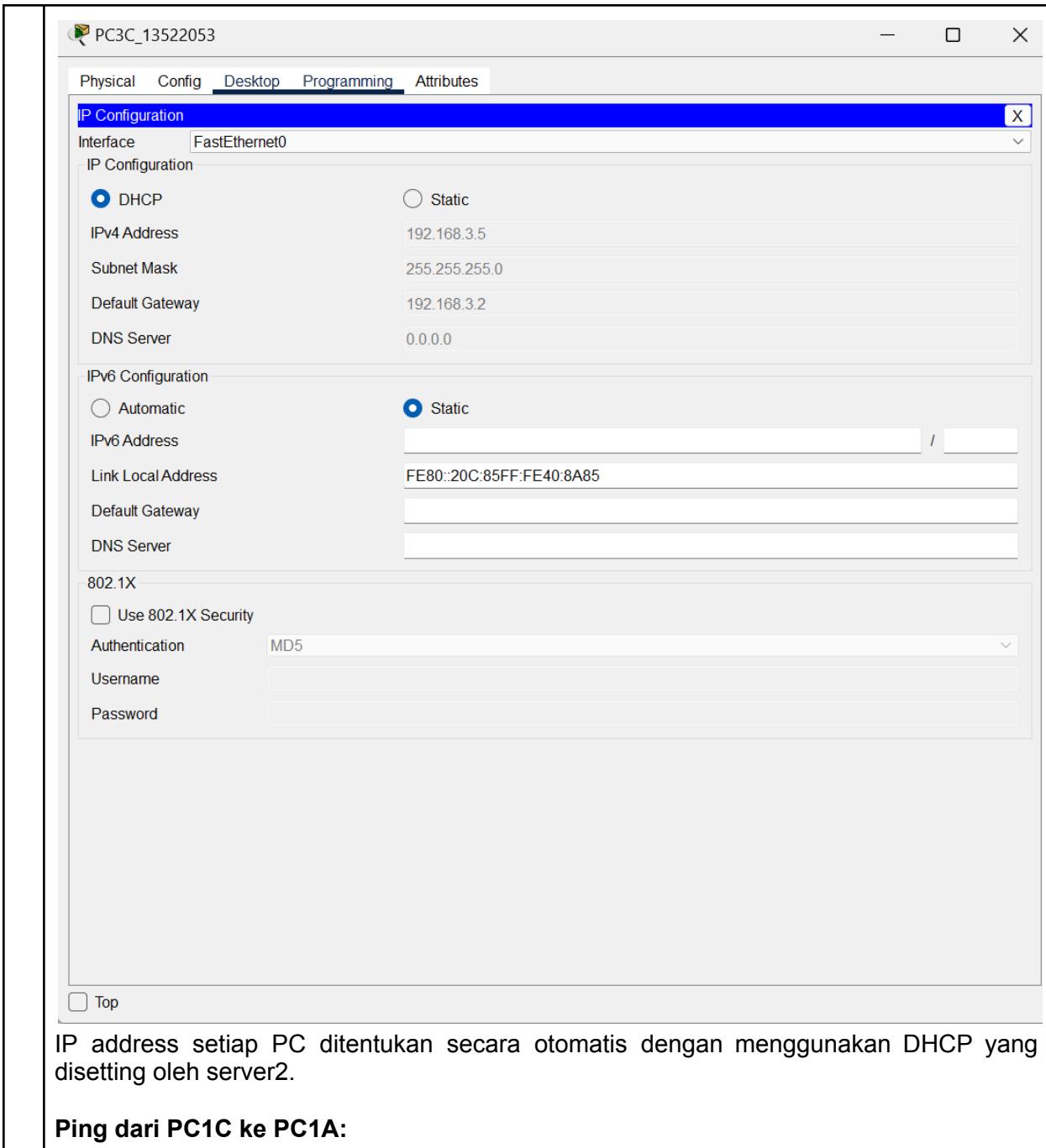
Authentication MD5

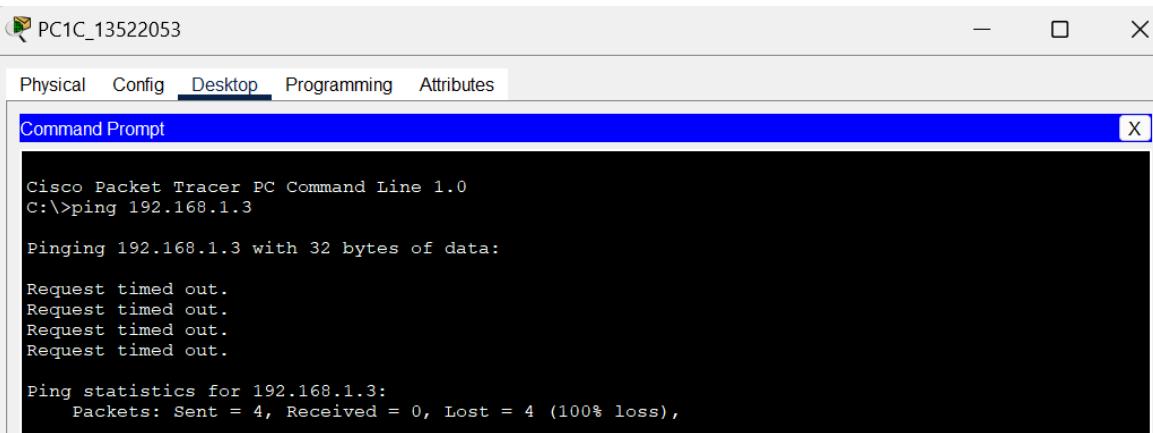
Username

Password

Top







```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 192.168.1.3

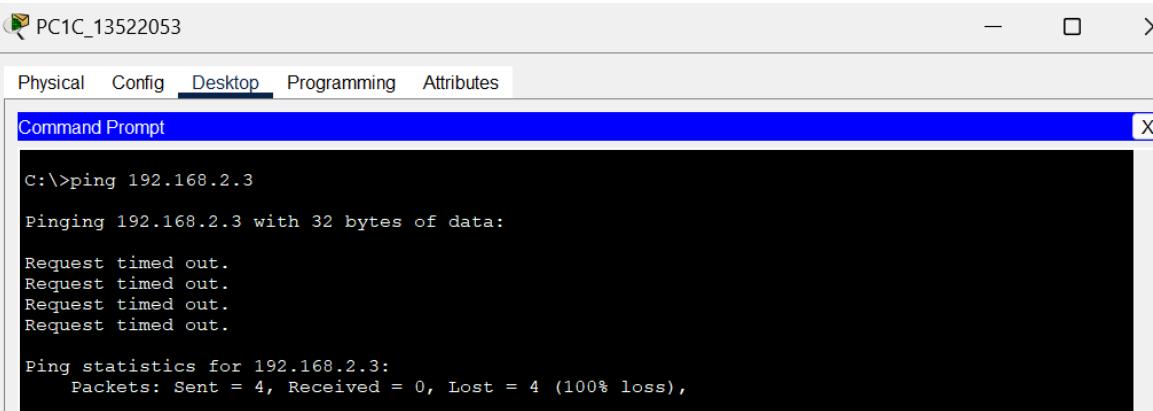
Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC1C tidak bisa melakukan ping ke PC1A karena memiliki subnet yang berbeda, dimana PC1A memiliki subnet 192.168.1.X sedangkan PC1C memiliki subnet 192.168.3.X sehingga PC1C tidak bisa berkomunikasi dengan PC1A dan sebaliknya.

Ping dari PC1C ke PC1B:



```
C:>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

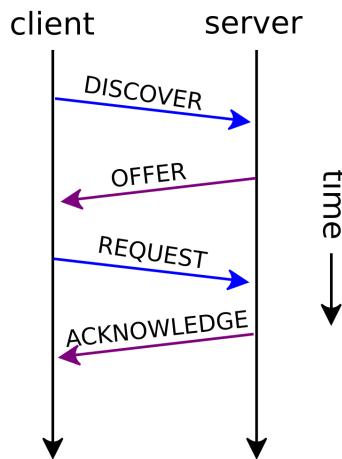
Ping statistics for 192.168.2.3:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC1C tidak bisa melakukan ping ke PC1B karena memiliki subnet yang berbeda, dimana PC1B memiliki subnet 192.168.2.X sedangkan PC1C memiliki subnet 192.168.3.X sehingga PC1C tidak bisa berkomunikasi dengan PC1B dan sebaliknya.

Alamat IP sebuah perangkat dapat ditentukan secara manual; jika dilakukan seperti ini, alamat tersebut dinamakan **IP statis**. Di jaringan-jaringan yang lebih besar, perangkat-perangkat dapat mendapatkan alamat-alamat IP secara otomatis menggunakan protokol [DHCP](#). Menggunakan ini, sebuah *router* "menyewakan" sebuah jangkauan alamat IP yang boleh digunakan oleh perangkat-perangkat dalam jaringan tersebut, dan memberikan juga *default gateway* dan alamat [DNS](#) yang dapat digunakan bersamanya.

Penyewaan alamat DHCP dilakukan dalam empat langkah. Dalam langkah DHCP Discovery, klien mengirimkan *broadcast* untuk menemukan server DHCP yang tersedia dalam jaringan tersebut. Kemudian, dalam langkah DHCP Offer, server mengirimkan pesan *unicast* yang berisi tawaran sewaan ke klien. Kemudian, DHCP Request, klien mengirimkan *broadcast* yang

meminta alamat yang telah ditawarkan, dan terakhir DHCP Acknowledgement dimana server mengirimkan durasi sewa dan informasi konfigurasi lainnya yang diminta.



Gambar 1. Proses penyewaan DHCP.

Penggunaan DHCP cukup umum ditemui di jaringan-jaringan yang bersifat publik dan dinamis. Ketika kita menggunakan "obtain IP address automatically" di sebuah *interface* di Windows, DHCP digunakan.

Di *router-router* Cisco, klien-klien DHCP dapat dikonfigurasikan menggunakan perintah berikut:

```
Router0(config)# interface f0/0
Router0(config-if)# ip address dhcp
```

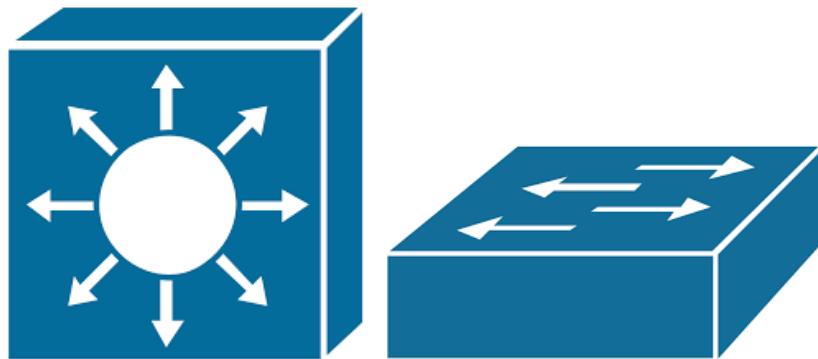
Sementara itu, *server-server* DHCP dapat dikonfigurasikan dengan membuat DHCP Pool yang mengkonfigurasikan alamat jaringan, alamat terlarang, *default gateway*, alamat-alamat DNS, serta informasi lainnya untuk klien-klien.

```
Router0(config)# ip dhcp pool <name>
Router0(dhcp-config)# network <Network-IP> <Mask>
Router0(dhcp-config)# dns-server <DNS-IP> (optional)
Router0(dhcp-config)# default-router <Default-IP> (optional)
Router0(dhcp-config)# exit
Router0(config)# ip dhcp excluded-address <Bottom-IP> <Top-IP>
```

Konflik DHCP mungkin terjadi bila dua atau lebih perangkat diberikan alamat yang sama. Hal ini dapat diselesaikan dengan me-reset klien DHCP dan meminta penyewaan baru.

IV.2. L3 Switch dan Inter-VLAN Routing

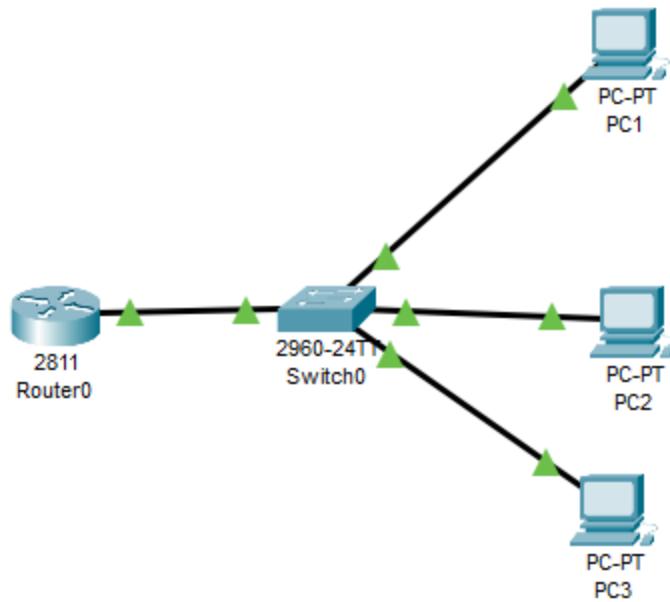
Dari pra-praktikum sebelumnya mengenai *frame switching*, kita tahu bahwa *switch* beroperasi pada *layer 2* dan tidak memerlukan alamat IP untuk beroperasi. Namun, beberapa switch dapat memiliki kemampuan *routing* dalam bentuk alamat IP dan *routing table*. Switch ini disebut dengan **L3 Switch** atau Multilayer switch. *Switch Layer 3* ditandai menggunakan simbol yang berbeda dalam diagram - diagram dibandingkan dengan *switch layer 2* seperti yang ditunjukkan di bawah.



Gambar 2. L3 Switch (kiri), L2 Switch (kanan)

Salah satu cara untuk melakukan *routing* antar-VLAN adalah dengan menggunakan konfigurasi **router on a stick** dengan sebuah switch terhubung pada router melalui satu kabel, melakukan *trunking* semua VLAN ke dalam router dan menggunakan router untuk mengelola rute antar VLAN. Router memiliki *interface* dan alamat IP di setiap VLAN dengan **mengkonfigurasi subinterface** pada router. Konfigurasi dapat dilakukan dengan perintah - perintah di bawah dengan `f0/0.x` sebagai *subinterface* dan `x` dapat berupa angka apa saja. Praktik yang baik adalah mengatur `.x` agar sama dengan ID VLAN. Sebagai contoh, pengaturan *subinterface* untuk ID VLAN 10 dapat dilakukan sebagai berikut

```
Router0(config)# interface f0/0
Router0(config-if)# interface f0/0.10
Router0(config-subif)# encapsulation dot1q 10
Router0(config-subif)# ip address ... (set the ip address)
```



Gambar 3. Contoh konfigurasi router on a stick

Tugas 3

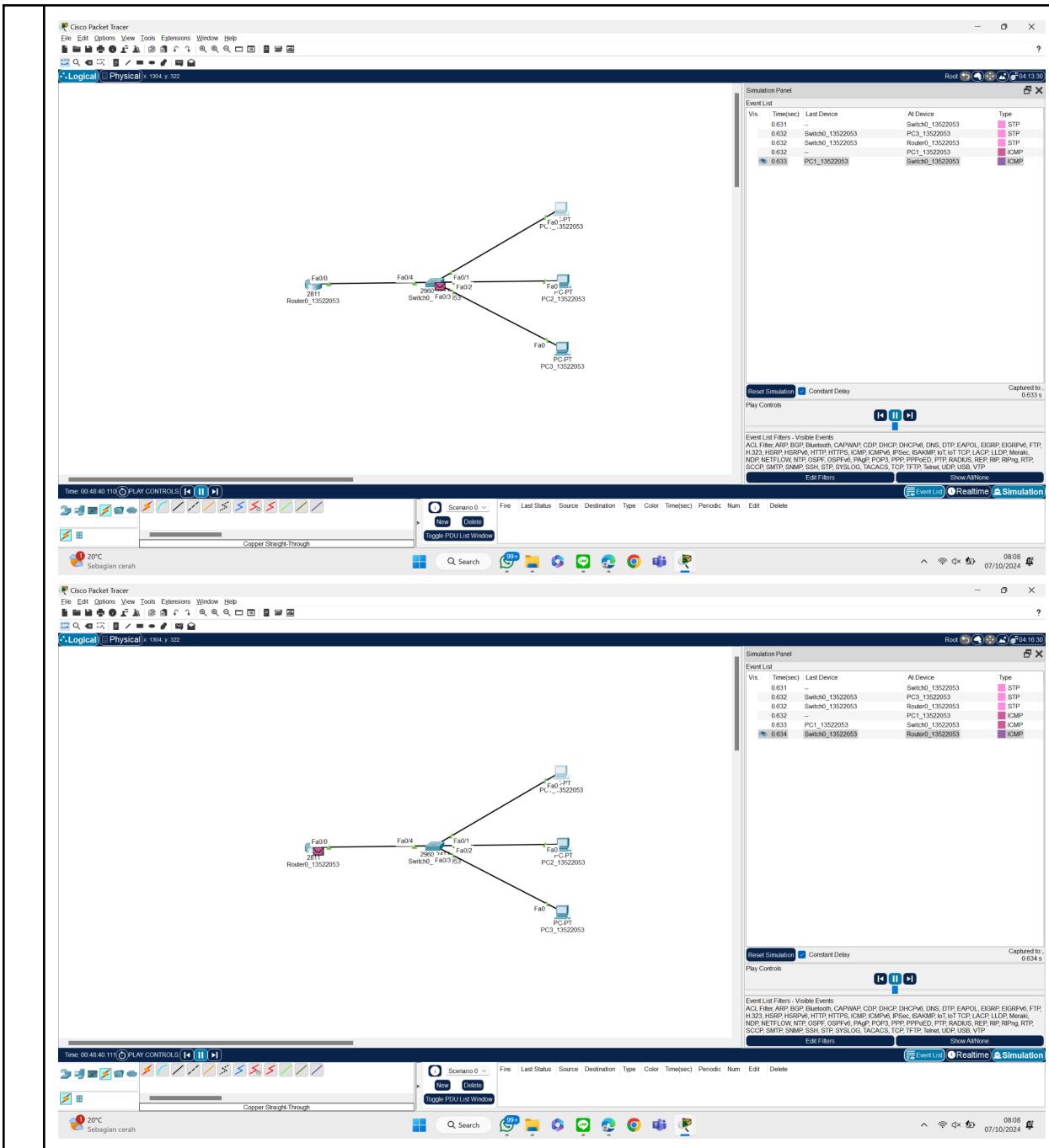
Q Di Cisco Packet Tracer, buatlah konfigurasi *router on a stick* sederhana dengan 3 PC, sebuah switch, dan sebuah router (lihat Gambar 3. Contoh konfigurasi *router on a stick*).

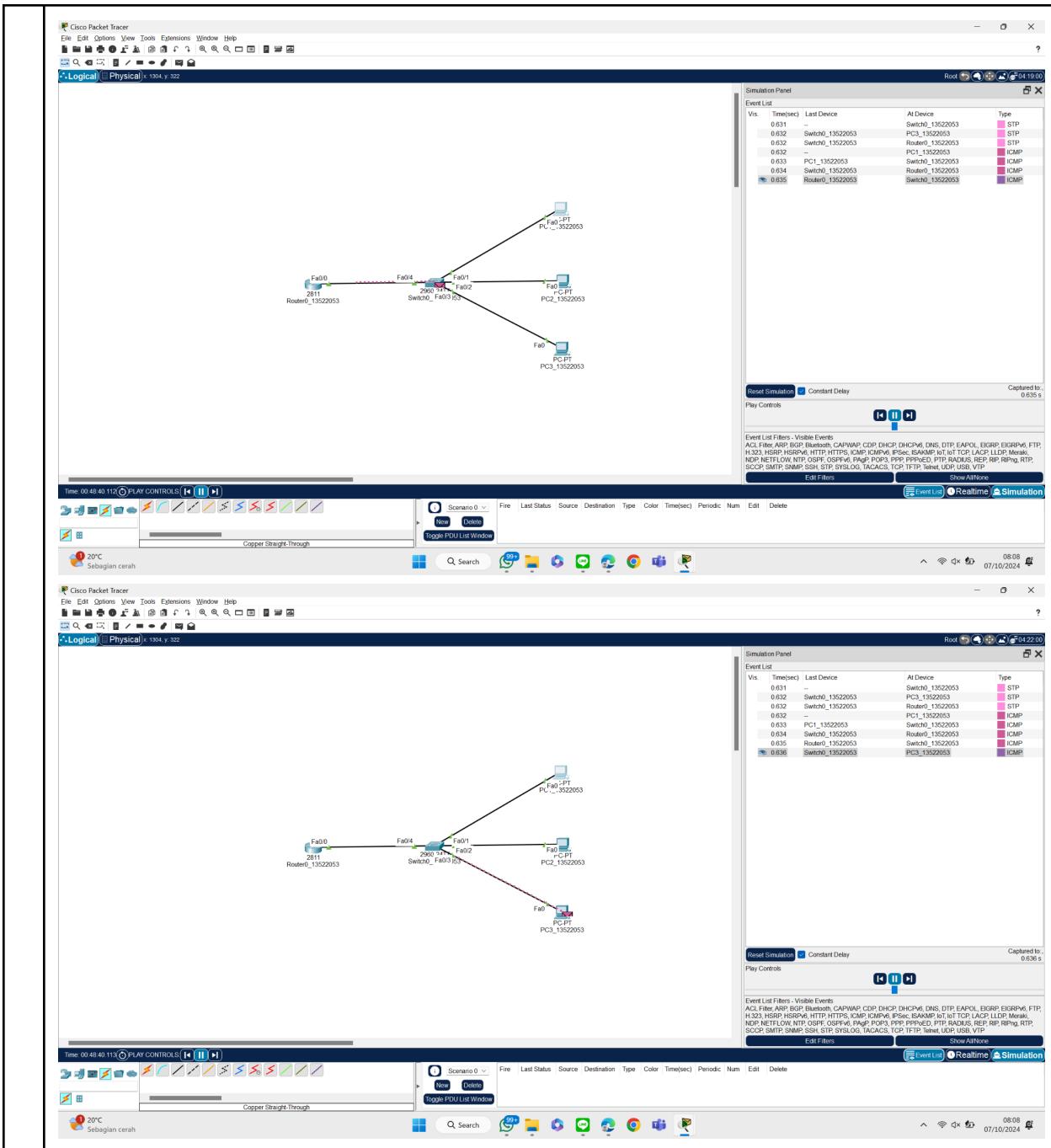
Gunakan konfigurasi berikut:

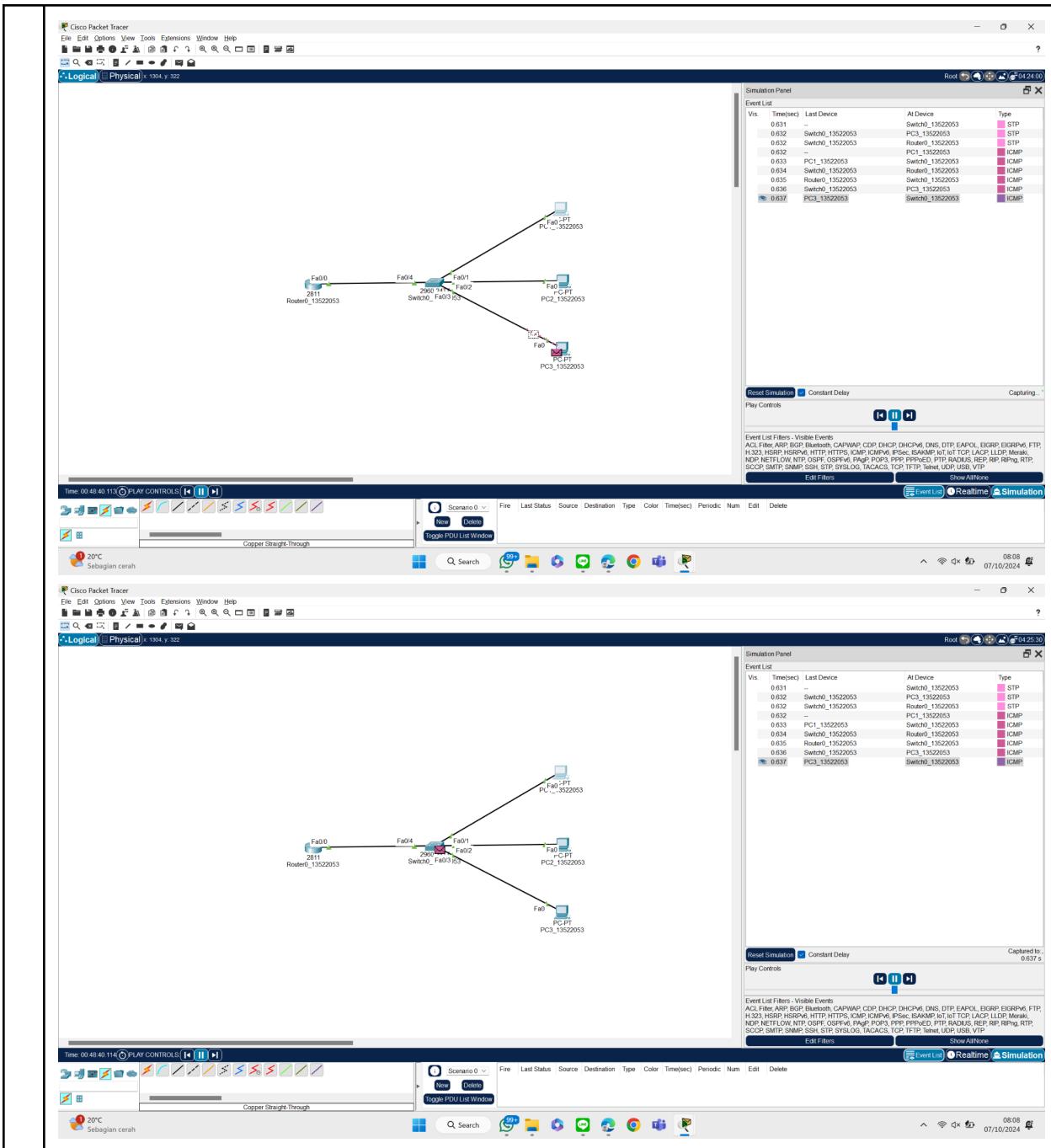
- Switch0_<NIM>: -
- PC1_<NIM>:
 - 192.168.1.1/24, VLAN 10
 - Default Gateway 192.168.1.254
- PC2_<NIM>:
 - 192.168.2.1/24, VLAN 20
 - Default Gateway 192.168.2.254
- PC3_<NIM>:
 - 192.168.3.1/24, VLAN 30
 - Default Gateway 192.168.3.254
- Router0_<NIM>
 - Subinterface f0/0.10: 192.168.1.254/24
 - Subinterface f0/0.20: 192.168.2.254/24
 - Subinterface f0/0.30: 192.168.3.254/24

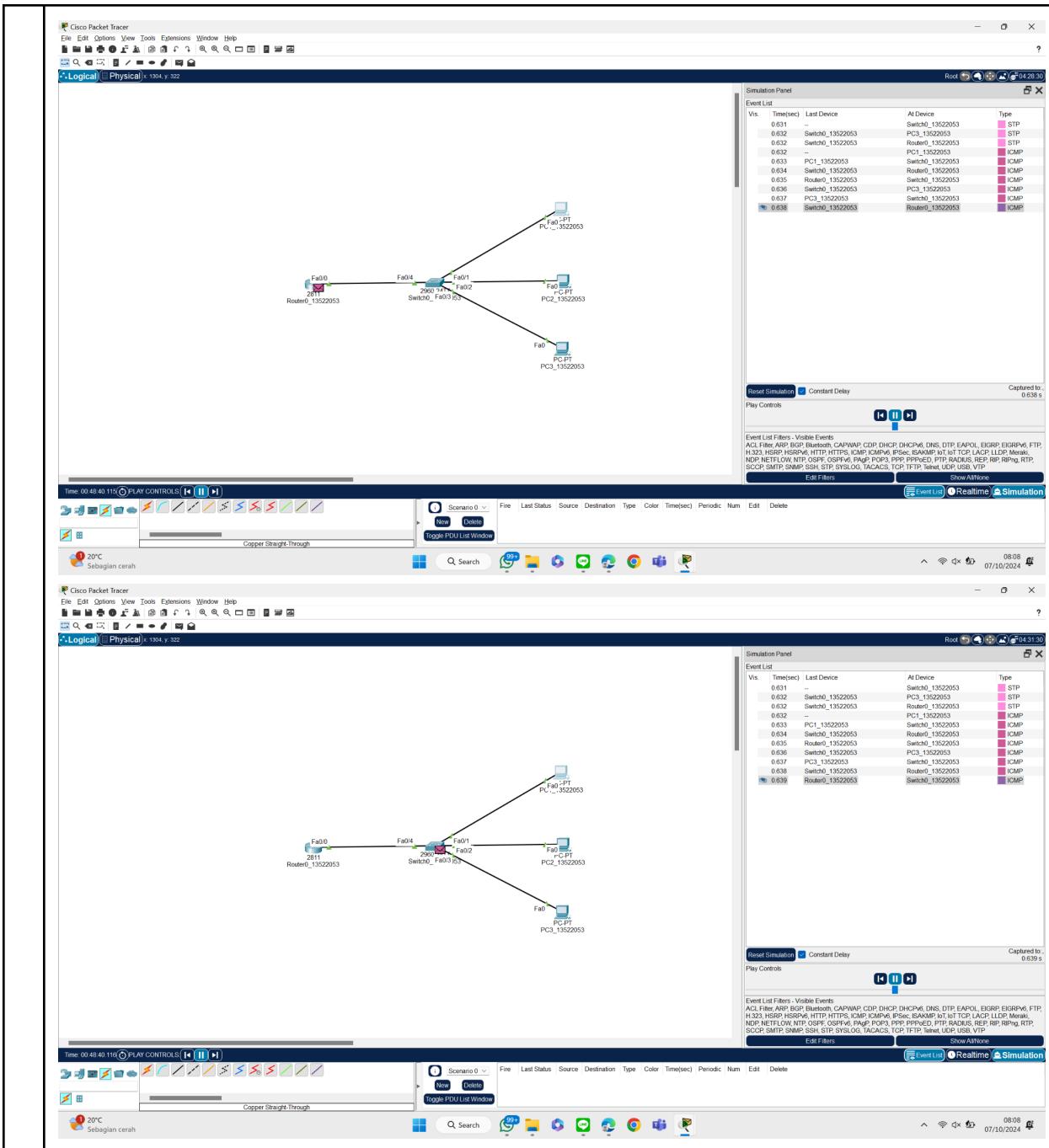
Lalu amati jalur ping dari PC1 ke PC3, ping tersebut seharusnya melewati router sebelum menuju ke PC3.

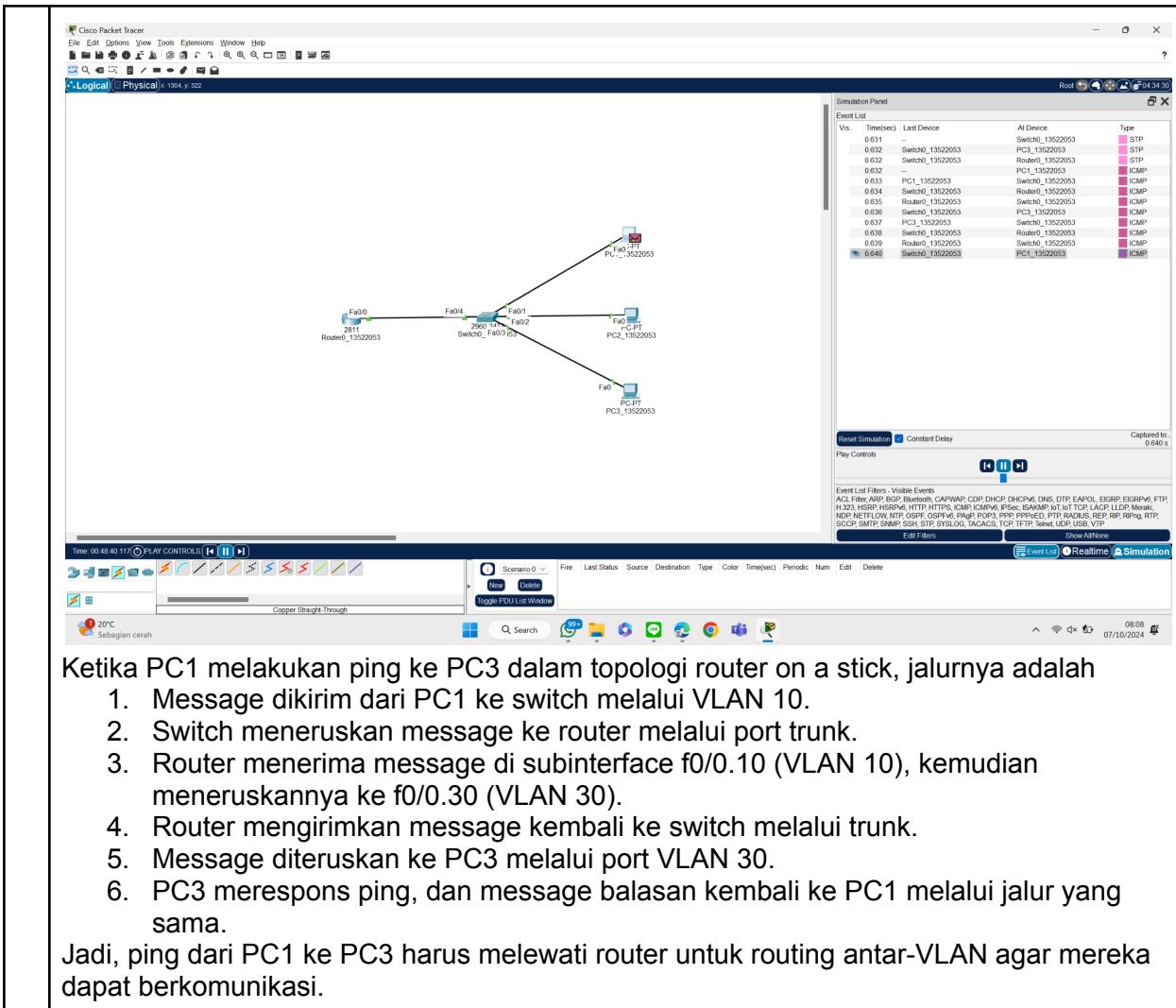
	<p>Lampiran topologi dan jelaskan jalur ping di area di bawah (gunakan fitur simulasi packet tracer!).</p>
A	<p>Topologi</p> <pre> graph TD Router[Router0_13522053] --- Switch[Switch0_13522053] Router --- PC1[PC-PT PC1_13522053] Router --- PC2[PC-PT PC2_13522053] Router --- PC3[PC-PT PC3_13522053] Switch --- PC1 Switch --- PC2 Switch --- PC3 </pre> <p>Jalur ping</p>









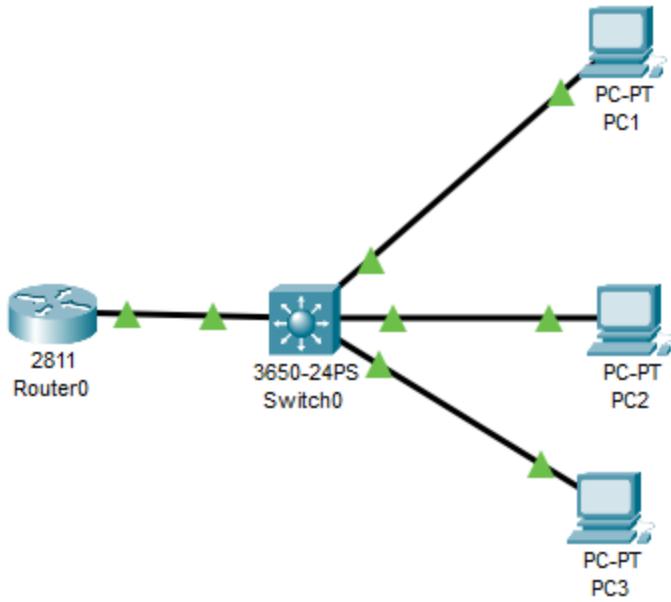


Ketika PC1 melakukan ping ke PC3 dalam topologi router on a stick, jalurnya adalah

1. Message dikirim dari PC1 ke switch melalui VLAN 10.
2. Switch meneruskan message ke router melalui port trunk.
3. Router menerima message di subinterface f0/0.10 (VLAN 10), kemudian meneruskannya ke f0/0.30 (VLAN 30).
4. Router mengirimkan message kembali ke switch melalui trunk.
5. Message diteruskan ke PC3 melalui port VLAN 30.
6. PC3 merespons ping, dan message balasan kembali ke PC1 melalui jalur yang sama.

Jadi, ping dari PC1 ke PC3 harus melewati router untuk routing antar-VLAN agar mereka dapat berkomunikasi.

L3 Switch dapat digunakan untuk menyederhanakan konfigurasi ini dengan memungkinkan *routing* antar-VLAN untuk terjadi di *switch* dan bukan di *router*. Hal ini mengurangi jumlah *hop* dalam jaringan, sehingga mengurangi *congestion* dan latensi. *L3 Switch* dapat memiliki antarmuka dalam VLAN yang disebut dengan **Switch Virtual Interface (SVI)**.



Gambar 4. Konfigurasi antar-VLAN menggunakan L3 switch

Fungsi routing pada *L3 Switch* dapat diaktifkan menggunakan perintah berikut

```
Switch0(config)# ip routing
```

Kemudian masing - masing *port* pada *switch* dapat dikonfigurasi menjadi *routed port* dan bukan *switchport* menggunakan perintah berikut.

```
Switch0(config-if)# no switchport
```

Setelah itu, alamat IP dapat diatur ke *interface* tersebut layaknya sebuah *router*.

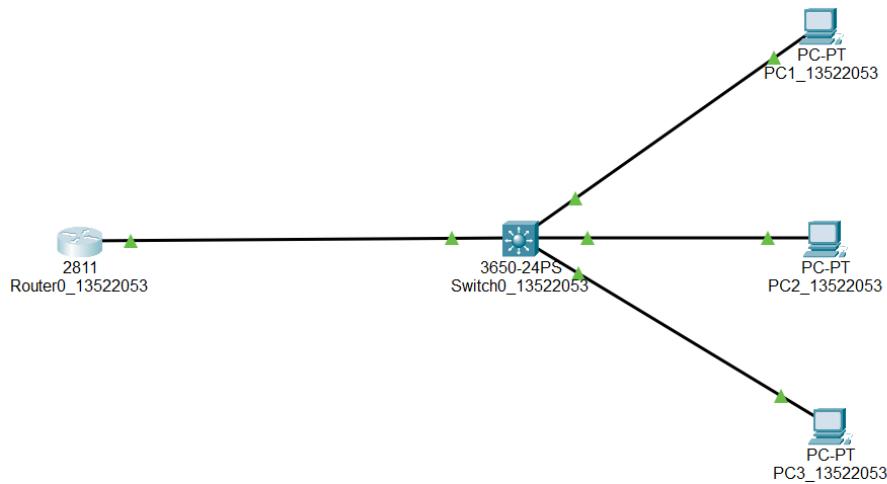
Di sisi lain, *SVI* dapat dikonfigurasi menggunakan perintah berikut, contohnya mengatur alamat IP untuk *SVI* dengan ID *VLAN 10*.

```
Switch0(config)# interface vlan10
Switch0(config-if)# ip address ...
Switch0(config-if)# no shutdown
```

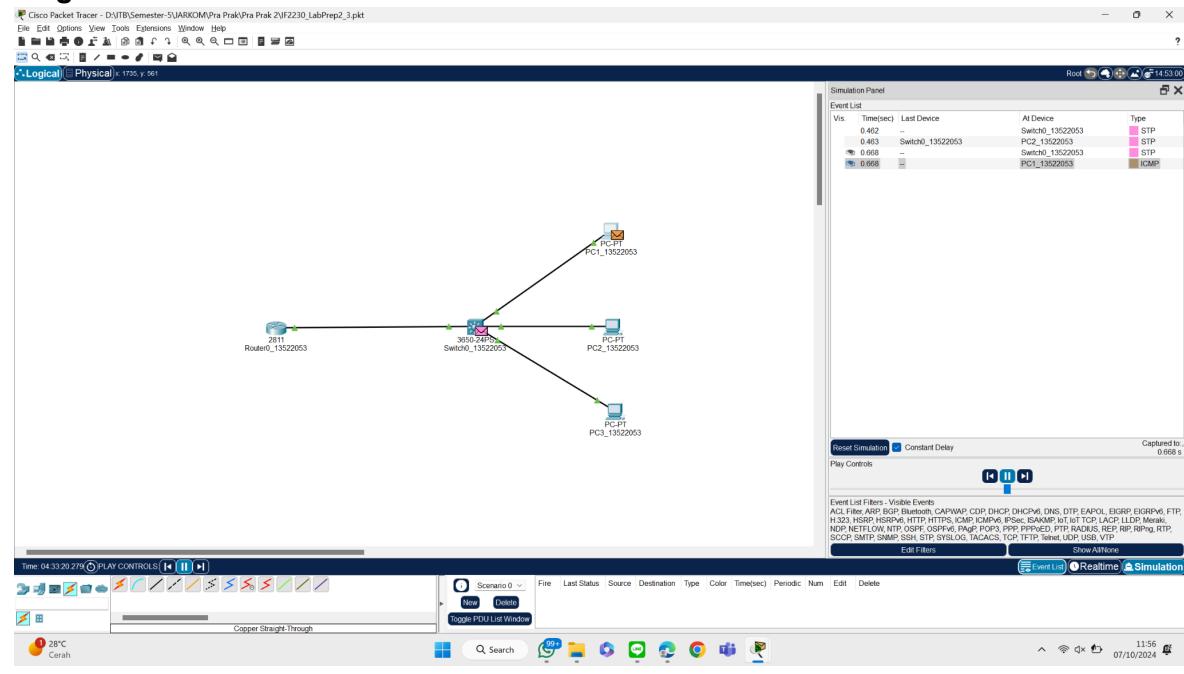
Perhatikan bahwa membutuhkan setidaknya satu port akses di *VLAN* dalam keadaan *up/up* dan/atau port *trunk* yang memperbolehkan *VLAN* tersebut dalam keadaan *up/up* serta *VLAN*

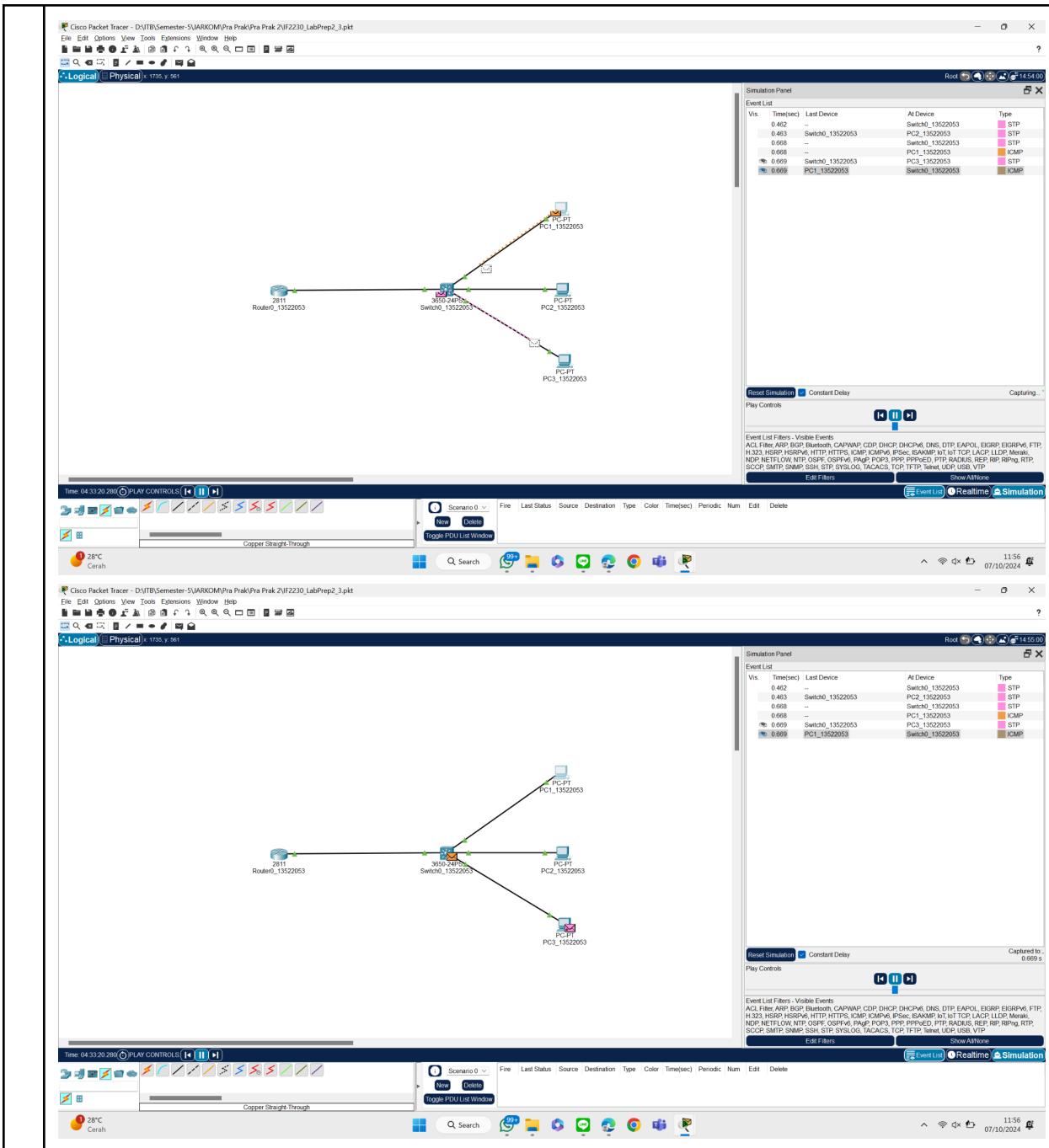
yang digunakan SVI tersebut harus ada dan tidak dimatikan dalam *switch* agar SVI dalam kondisi menyala.

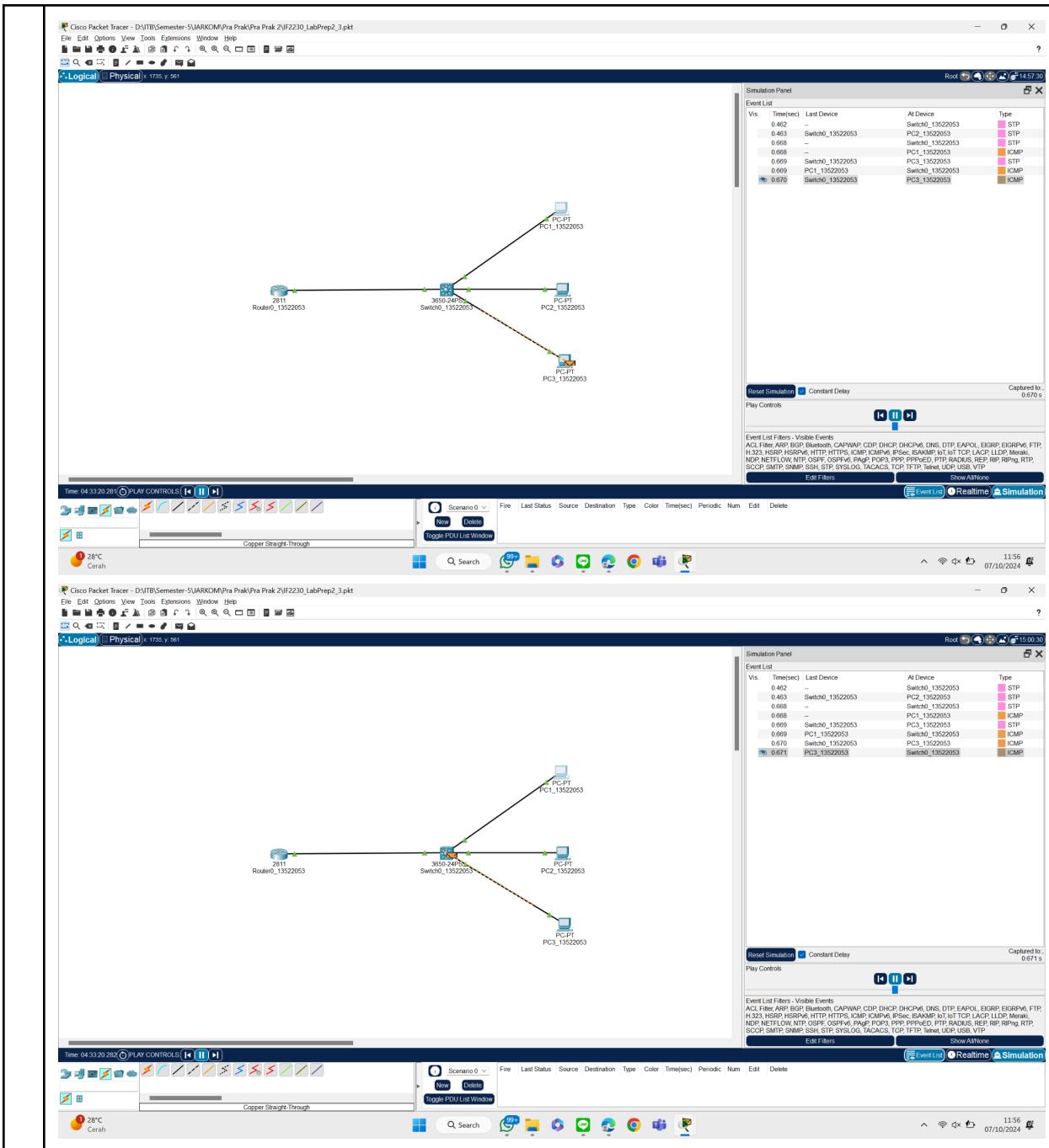
Tugas 4	
Q	<p>Salin konfigurasi dari tugas sebelumnya, ubah <i>switch</i> menjadi sebuah <i>multilayer switch</i> (lihat <i>Gambar 4. Konfigurasi antar-VLAN menggunakan L3 switch</i>), kemudian lakukan hal berikut:</p> <ul style="list-style-type: none">• Hapus semua <i>subinterface</i> di Router0• Atur alamat IP f0/0 Router0 menjadi 192.168.4.254/24• Atur <i>interface</i> Switch0 yang terhubung pada <i>router</i> menjadi <i>routed port</i> dan atur alamat IP-nya menjadi 192.168.4.1/24• Atur <i>default gateway</i> Switch0 menjadi alamat IP f0/0 milik Router0• Atur Router0 agar memiliki <i>static route</i> seperti berikut:<ul style="list-style-type: none">◦ 192.168.1.0/24 via 192.168.4.1◦ 192.168.2.0/24 via 192.168.4.1◦ 192.168.3.0/24 via 192.168.4.1• Atur SVI berikut di Switch0:<ul style="list-style-type: none">◦ VLAN 10: 192.168.1.254/24◦ VLAN 20: 192.168.2.254/24◦ VLAN 30: 192.168.3.254/24 <p>Kemudian amati jalur ping dari PC1 ke PC3, ping tersebut seharusnya tidak melewati router sebelum ke PC3. Selain itu, lakukan ping dari PC1 ke Router0</p> <p>Lampiran topologi dan jelaskan jalur ping di area di bawah (gunakan fitur simulasi packet tracer!).</p>
A	Topologi

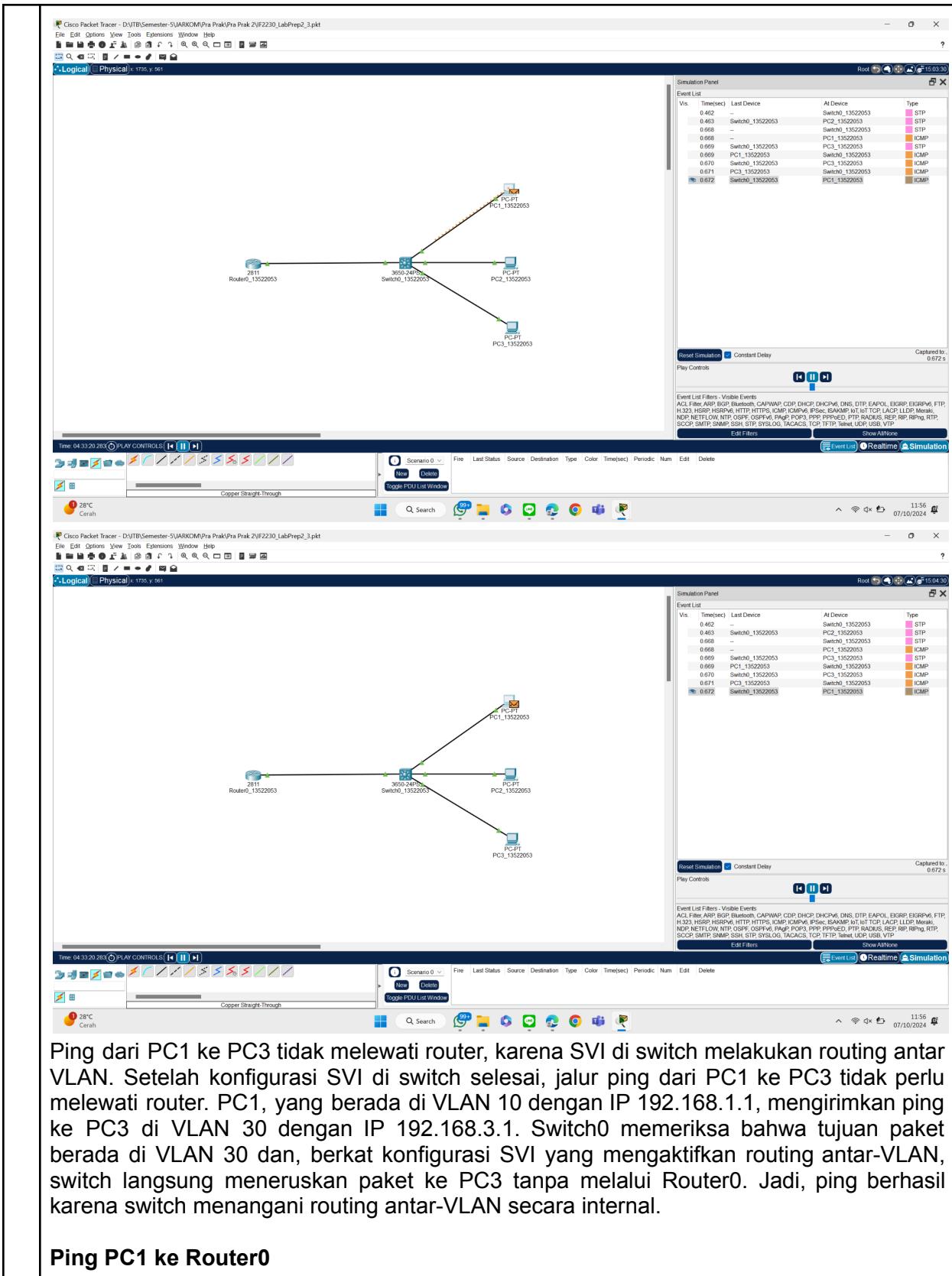


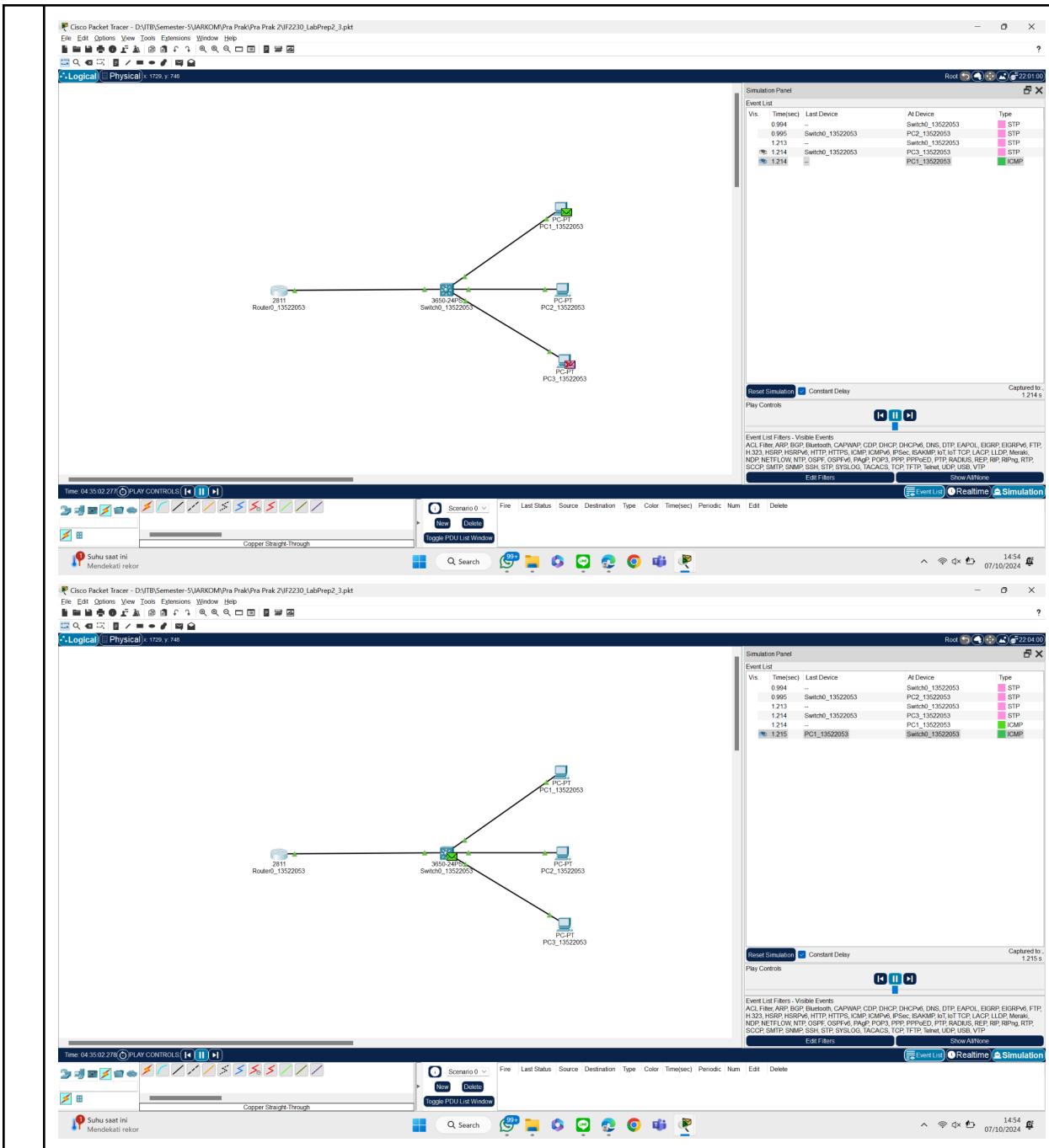
Ping PC1 ke PC3

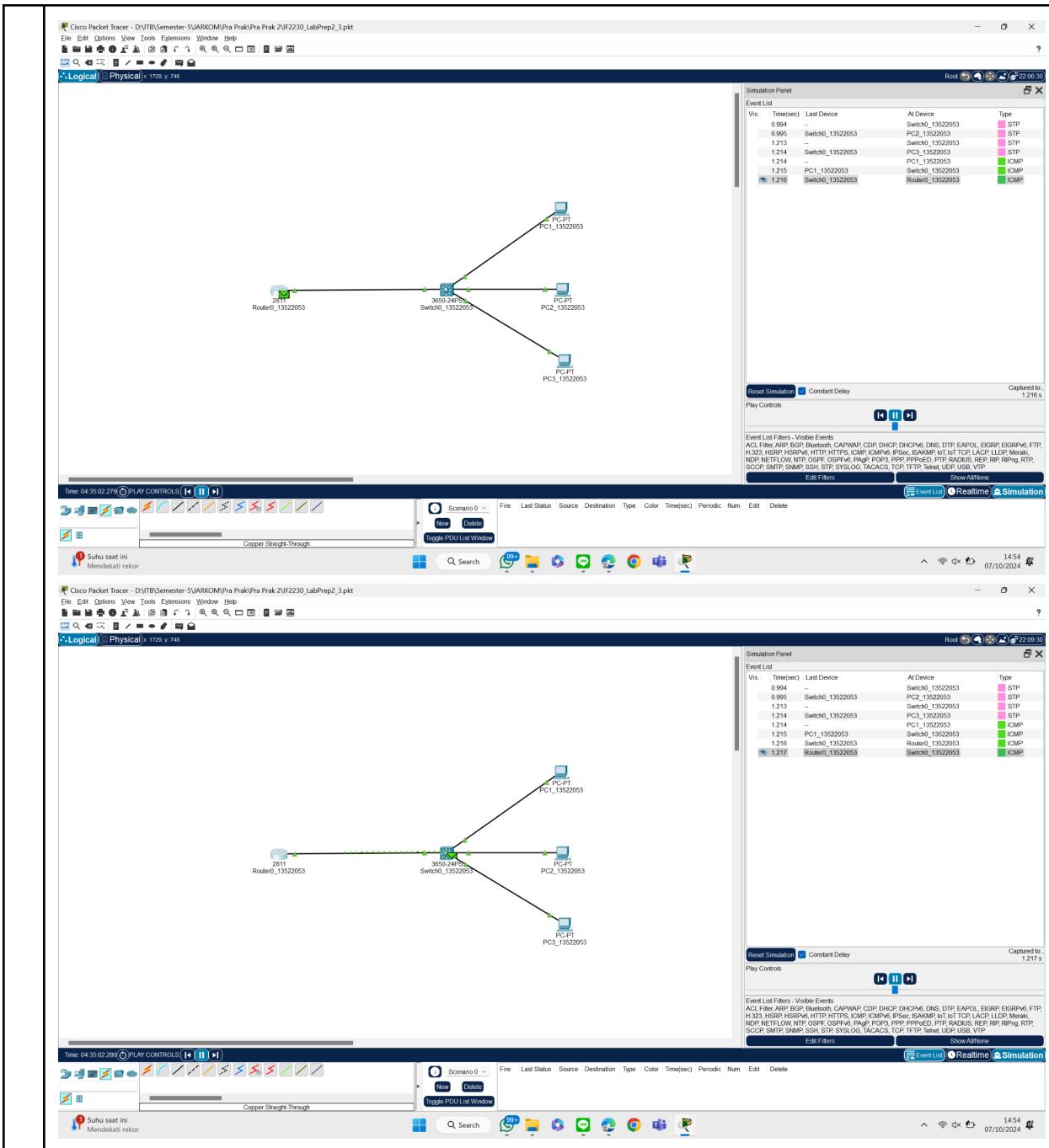


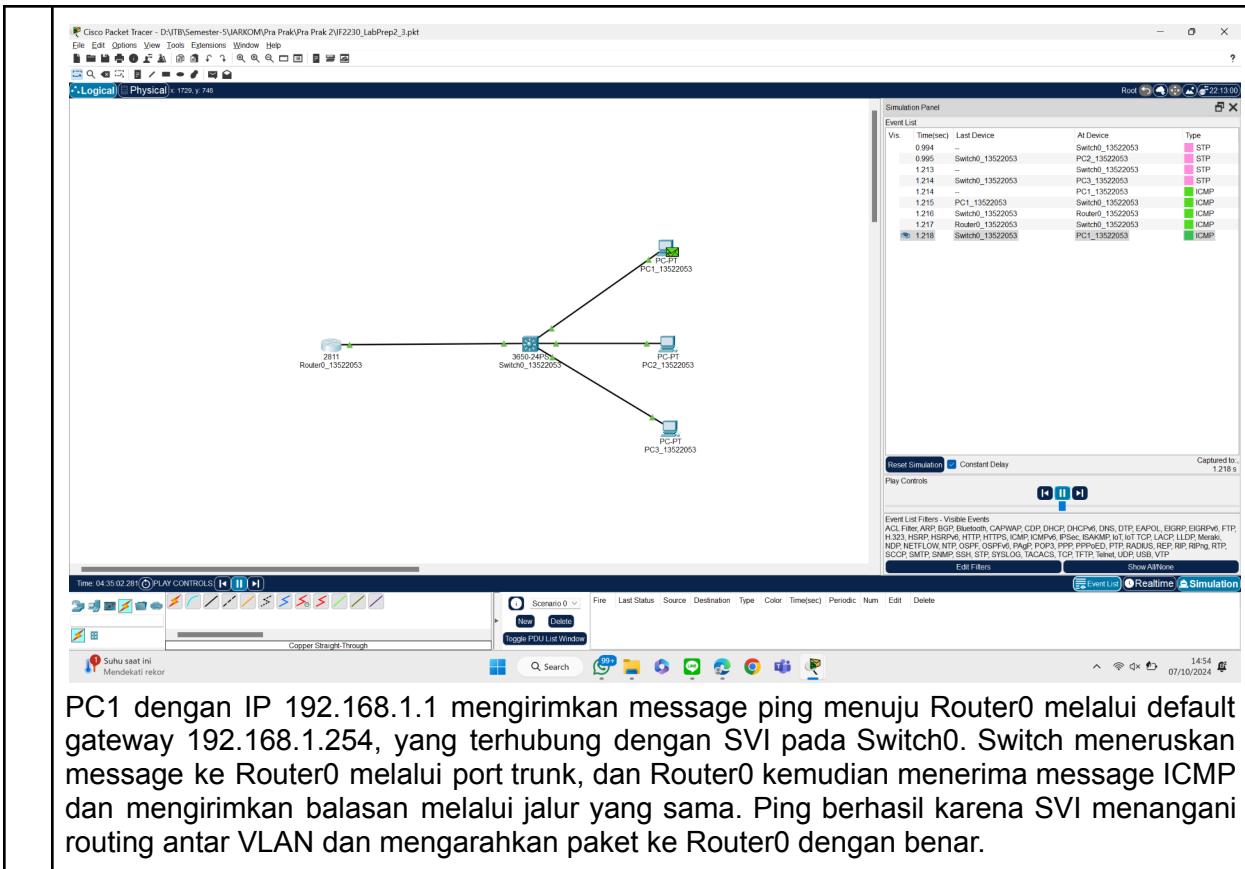












PC1 dengan IP 192.168.1.1 mengirimkan message ping menuju Router0 melalui default gateway 192.168.1.254, yang terhubung dengan SVI pada Switch0. Switch meneruskan message ke Router0 melalui port trunk, dan Router0 kemudian menerima message ICMP dan mengirimkan balasan melalui jalur yang sama. Ping berhasil karena SVI menangani routing antar VLAN dan mengarahkan paket ke Router0 dengan benar.

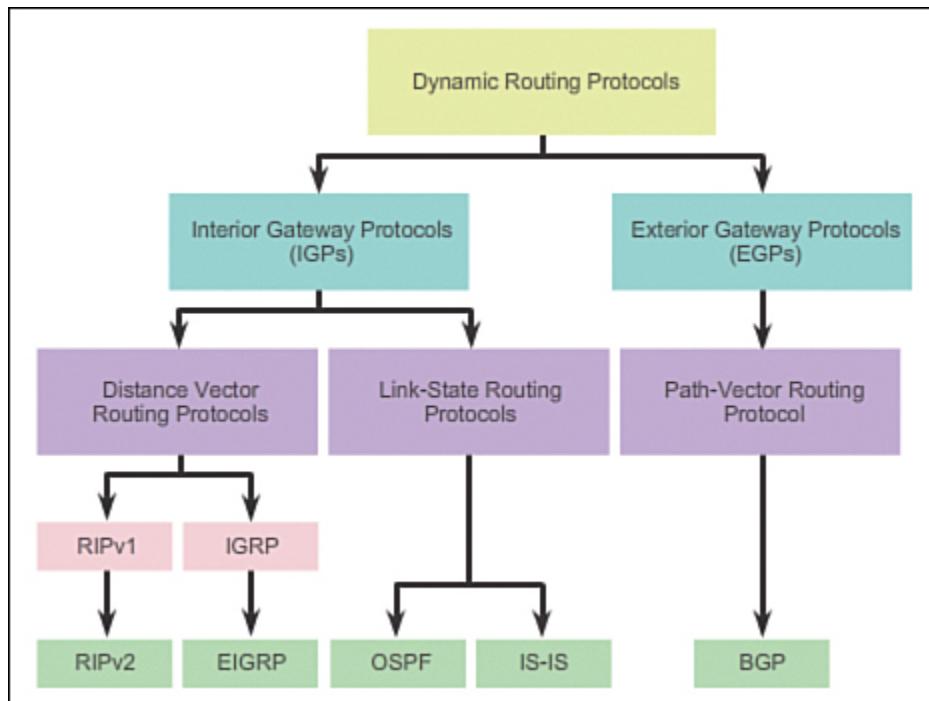
Ketika sebuah *switch* memiliki alamat IP dan *routing table*, secara teknis *switch* tersebut telah menjadi *router*. Perhatikan bahwa **layer 2 ditunjukkan dengan penggunaan MAC address sedangkan layer 3 ditunjukkan dengan penggunaan alamat IP**. Lalu, apa perbedaan antara *L3 Switch* dan *router*? Sebagai alat yang didesain khusus untuk keperluan *routing*, *router* memiliki kemampuan *routing* yang lebih canggih dengan *routing table* yang lebih besar, protokol yang lebih canggih, dan fitur keamanan. Namun, hal ini bergantung pada jenis *switch* dan *router*. *Router* yang lebih tua bisa saja memiliki kemampuan *routing* yang lebih buruk dibandingkan *L3 Switch* yang lebih baru.

IV.3. Dynamic Routing

Pada bagian IV.1 Static Routing, kita telah belajar menambahkan rute ke *routing table* alat jaringan secara manual. Namun, mengkonfigurasi rute secara manual tidak efisien dalam konfigurasi jaringan yang kompleks. Untuk mengatasi masalah tersebut, rute dapat dibuat secara dinamis menggunakan protokol dengan algoritma tertentu untuk menemukan rute terbaik.

Ada dua kategori *dynamic routing*, yaitu *interior gateway protocol* dan *exterior gateway protocol*. *Interior gateway protocol* secara dinamis bertukar informasi *routing* dan keterjangkauan di dalam sebuah *autonomous system*, sedangkan *exterior gateway protocol* bertukar informasi *routing* dan keterjangkauan ke luar sebuah *autonomous system*.

Algoritma yang digunakan untuk menghasilkan rute mengklasifikasikan protokol yang ada lebih lanjut. [Distance-vector routing protocol](#) menggunakan metrik seperti *hop count*, *bandwidth*, *delay*, dan lainnya untuk menentukan rute terbaik melalui tetangganya; [Link-state routing protocol](#) memetakan seluruh jaringan sambil tetap mempertimbangkan metrik tertentu untuk menentukan rute terbaik; dan [Path-vector routing protocol](#) menyimpan jalur yang digunakan untuk mencapai tujuan tertentu untuk menentukan penambahan suatu rute. Perhatikan bahwa *path-vector routing protocol* berbeda dari yang lain dengan berfokus lebih pada ketersediaan rute daripada memeriksa rute terbaik yang mungkin menggunakan metrik tertentu, hal ini disebabkan penggunaannya sebagai *exterior gateway protocol*.



Gambar 5. Klasifikasi dynamic routing protocol ([source](#))

Untuk menentukan rute terbaik ke tujuan yang sama, protokol menggunakan metrik tertentu untuk membandingkan satu rute dengan rute lainnya. Jika sebuah perangkat memiliki rute dari beberapa *routing protocol* ke suatu tujuan, rute - rute tersebut akan diprioritaskan berdasarkan **administrative distance (AD)** terkecil.

Route Source	Administrative Distance	Default Metric(s)
Connected	0	0
Static	1	0
EIGRP Summary Route	5	
External BGP	20	Value assigned by Admin
Internal EIGRP	90	Bandwidth, Delay
IGRP	100	Bandwidth, Delay
OSPF	110	Link cost (bandwidth)
IS-IS	115	Link cost (Value assigned by admin)
RIP	120	Hop count
External EIGRP	170	
Internal BGP	200	Value assigned by Admin

Gambar 6. AD dan metrik dynamic routing protocol default pada perangkat Cisco ([source](#))

Administrative distance ini dapat diubah secara manual untuk memprioritaskan sebuah protokol dibandingkan yang lainnya. *Static route* juga dapat diatur secara manual untuk memiliki *administrative distance* yang lebih tinggi yang disebut ***floating static route***. *Floating static route* dapat digunakan sebagai rute cadangan jika terjadi kegagalan pada *dynamic routing*.

```

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   10.8.0.0/24 is directly connected, GigabitEthernet0/2
L   10.8.0.1/32 is directly connected, GigabitEthernet0/2
172.16.0.0/24 is subnetted, 1 subnets
S     172.16.1.0/24 [1/0] via 10.8.0.2
B   192.168.1.0/24 [20/2] via 192.168.2.1, 00:00:00
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.2.0/24 is directly connected, GigabitEthernet0/1
L     192.168.2.3/32 is directly connected, GigabitEthernet0/1
B   192.168.3.0/24 [20/2] via 192.168.2.1, 00:00:00
192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.4.0/24 is directly connected, GigabitEthernet0/0
L     192.168.4.3/32 is directly connected, GigabitEthernet0/0

```

Gambar 7. Contoh *routing table* dengan berbagai *routing configuration* pada perangkat Cisco

Dalam *routing table* Cisco, sebuah rute biasanya dicatat seperti berikut.

```
S 172.16.1.0/24 [1/0] via 10.8.0.2
```

Huruf paling kiri menunjukkan asal rute dengan 'S' adalah '*Static*', Penjelasan mengenai kode lain selalu tersedia di atas *routing table* ketika memanggil show ip route. Di sisi lain, *administrative distance* dan metrik ditampilkan di dalam kurung siku - siku dengan bersesuaian. Sebagai contoh, rute di atas memiliki [1/0] yang berarti *administrative distance* bernilai 1 dan metrik bernilai 0. **Rute dari protokol berbeda dibandingkan menggunakan *administrative***

distance sementara rute dari protokol yang sama dibandingkan menggunakan metrik. Hal ini di luar aturan *most specific route first*, rute di atas masih bisa didahului oleh rute ke tujuan yang lebih spesifik (/25, /26).

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route
```

Gambar 8. Kode - kode route pada perangkat Cisco

Karena *static route* tidak memiliki metrik untuk dihitung, **pengaturan *distance metric* pada *static route* sebenarnya mengganti *administrative distance* rute tersebut.** *Distance metric* pada *static route* dapat diatur ketika menambahkan *static route* dengan sebagai berikut.

```
Router0(config)# ip route 172.16.1.0 255.255.255.0 10.8.0.2 <AD>
```

Sementara itu, mengubah *administrative distance* pada *dynamic route* umumnya dilakukan dengan menggunakan perintah *distance* dalam menu konfigurasinya.

```
Router0(config)# router ospf 1  
Router0(config-router)# distance <AD>
```

Open Shortest Path First (OSPF) adalah salah satu *link state interior gateway protocol*. OSPF membangun peta topologi jaringan dengan mengumpulkan informasi keterhubungan dari *router - router* yang tersedia. **Algoritma mendasar yang digunakan untuk melakukan hal tersebut adalah dengan menghitung *shortest path tree* untuk setiap *router* menggunakan metode yang didasari oleh algoritma Dijkstra.** Selain itu, OSPF dapat mendeteksi kegagalan hubungan dan menghasilkan struktur rute bebas loop yang baru.

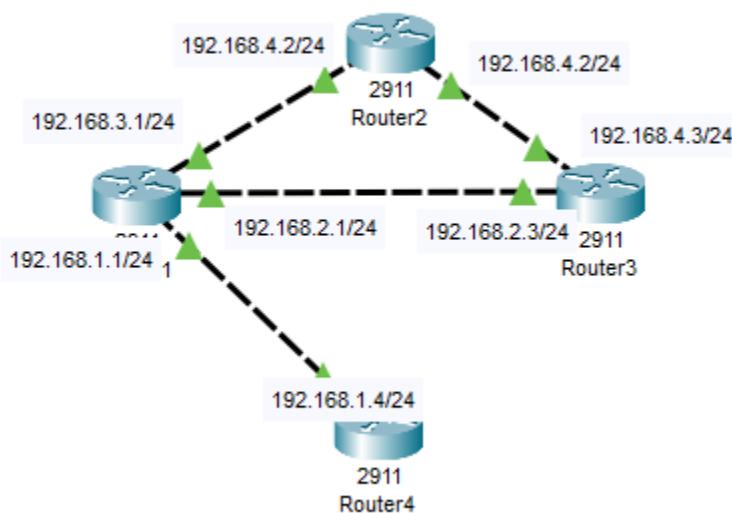
OSPF dikonfigurasi pada [router Cisco](#) dengan menentukan *process-id* dan alamat IP dari *area-id* tertentu. Konfigurasi *process-id* 100, *area-id* 1, dan alamat 192.168.1.0/24 dapat dilakukan seperti berikut.

```
Router0(config)# router ospf 100  
Router0(config-router)# network 192.168.1.0 0.0.0.255 area 1
```

Process-id digunakan sebagai ID konfigurasi untuk membedakan proses OSPF berbeda pada *router* yang sama. *Process-id* tidak harus sama dengan *router* lainnya agar OSPF dapat mengenali satu jaringan. **Yang harus sama dengan *router* lain adalah *area-id*.**

Tugas 5

Q Buatlah topologi *router* seperti di bawah ini.



Konfigurasikan OSPF pada semua *router* dengan setiap *router* mem-*broadcast* semua jaringannya, contoh: Router1 mem-*broadcast* 192.168.1.0/24, 192.168.2.0/24, dan 192.168.3.0/24. Gunakan nomor berapa saja sebagai *process-id* dan 1 sebagai *area-id*.

Protip! Cara lain untuk melacak rute atau jalur ping adalah dengan menggunakan perintah trace <ip>.

Lampirkan dan jelaskan *routing table* pada setiap router dan jelaskan jalur dari Router3 ke Router4 dengan 192.168.2.3 dalam kondisi menyala dan mati.

A **Konfigurasi OSPF**
Router 1

Router1_13522053

Physical Config **CLI** Attributes

IOS Command Line Interface

```

L    192.168.3.1/32 is directly connected, GigabitEthernet0/0
O    192.168.4.0/24 [110/2] via 192.168.2.3, 00:03:51, GigabitEthernet0/1

Router#
00:49:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.4.2 on GigabitEthernet0/0 from LOADING to FULL,
Loading Done

Router#show ip ospf neighbor
^
% Invalid input detected at '^' marker.

Router#show ip ospf neighbor
^
% Invalid input detected at '^' marker.

Router#show ip ospf neighbor

Neighbor ID      Pri  State          Dead Time     Address          Interface
192.168.4.2       1    FULL/BDR      00:00:35     192.168.3.2    GigabitEthernet0/0
192.168.4.3       1    FULL/BDR      00:00:37     192.168.2.3    GigabitEthernet0/1
192.168.1.4       1    FULL/BDR      00:00:36     192.168.1.4    GigabitEthernet0/2

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/2
L        192.168.1.1/32 is directly connected, GigabitEthernet0/2
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/1
L        192.168.2.1/32 is directly connected, GigabitEthernet0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0
O    192.168.4.0/24 [110/2] via 192.168.2.3, 00:02:29, GigabitEthernet0/1
                [110/2] via 192.168.3.2, 00:02:29, GigabitEthernet0/0

Router#

```

Top

C: Menunjukkan jaringan yang directly connected ke Router1 (192.168.1.0, 192.168.2.0, 192.168.3.0).

O: Menunjukkan rute yang diperoleh melalui OSPF, dalam hal ini Router1 memiliki dua jalur menuju jaringan 192.168.4.0/24 melalui Router2 (192.168.2.3) dan Router3 (192.168.3.2).

Router 2

Router2 memiliki dua jaringan yang directly connected (192.168.3.0/24 dan 192.168.4.0/24).

Rute OSPF (dengan AD 110) menunjukkan bahwa Router2 mengetahui rute menuju jaringan 192.168.1.0/24 dan 192.168.2.0/24 melalui Router1. Router2 juga mengetahui rute menuju jaringan 192.168.2.0/24 melalui Router3.

Router 3

Router3_13522053

Physical Config **CLI** Attributes

IOS Command Line Interface

Press RETURN to get started.

```
Router>
Router>
Router>
Router>en
Router#show ip ospf neighbor

Neighbor ID      Pri      State        Dead Time     Address          Interface
192.168.4.2      1      FULL/DR      00:00:36     192.168.4.2      GigabitEthernet0/0
192.168.3.1      1      FULL/DR      00:00:37     192.168.2.1      GigabitEthernet0/1
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O   192.168.1.0/24 [110/2] via 192.168.2.1, 00:28:57, GigabitEthernet0/1
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.2.0/24 is directly connected, GigabitEthernet0/1
L     192.168.2.3/32 is directly connected, GigabitEthernet0/1
O   192.168.3.0/24 [110/2] via 192.168.2.1, 00:19:32, GigabitEthernet0/1
    [110/2] via 192.168.4.2, 00:19:32, GigabitEthernet0/0
    192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.4.0/24 is directly connected, GigabitEthernet0/0
L     192.168.4.3/32 is directly connected, GigabitEthernet0/0
Router#
```

Top

Copy Paste

Router3 memiliki dua jaringan yang directly connected (192.168.2.0/24 dan 192.168.4.0/24).
Rute OSPF (dengan AD 110) menunjukkan bahwa Router3 mengetahui rute menuju jaringan 192.168.1.0/24 dan 192.168.3.0/24 melalui Router1.

Router 4

Router4_13522053

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show i
00:39:34: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on GigabitEthernet0/0 from LOADING to FULL,
Loading Done
% Incomplete command.
Router#show ospf neighbor
^
% Invalid input detected at '^' marker.

Router#show ip ospf neighbor

Neighbor ID      Pri      State          Dead Time     Address          Interface
192.168.3.1      1      FULL/DR        00:00:38    192.168.1.1      GigabitEthernet0/0
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.4/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/2] via 192.168.1.1, 00:00:45, GigabitEthernet0/0
O    192.168.3.0/24 [110/2] via 192.168.1.1, 00:00:45, GigabitEthernet0/0
O    192.168.4.0/24 [110/3] via 192.168.1.1, 00:00:45, GigabitEthernet0/0

Router#

```

Top

Router4 hanya memiliki satu jaringan yang directly connected (192.168.1.0/24). Semua rute lainnya didapat dari OSPF, dengan jalur utama ke jaringan 192.168.2.0/24, 192.168.3.0/24, dan 192.168.4.0/24 melalui Router1.

Jalur dari Router3 ke Router4 dengan 192.168.2.3 dalam kondisi menyala

Dalam kondisi normal di mana interface 192.168.2.3 menyala, Router3 memiliki jalur langsung menuju Router4 melalui jaringan 192.168.4.0/24 dimana jalur ini adalah jalur terpendek dan paling efisien.

Jalur utama adalah Router3 → Router4 melalui jaringan 192.168.4.0/24 menggunakan interface GigabitEthernet0/1 dari Router3 untuk langsung menuju Router4.

Jalur dari Router3 ke Router4 dengan 192.168.2.3 dalam kondisi mati

Jika interface 192.168.2.3 pada Router3 mati, Router3 tidak dapat menggunakan jalur langsung ke Router4 melalui jaringan 192.168.4.0/24. Dalam kasus ini, OSPF akan mencari jalur alternatif melalui jaringan lain. Jalur alternatif yang tersedia adalah melalui Router1. Jalur alternatifnya adalah Router3 → Router1 → Router4. Rute ini akan melalui jaringan 192.168.2.0/24 dari Router3 ke Router1, kemudian Router1 akan meneruskan paket ke Router4 melalui jaringan 192.168.1.0/24.

Border gateway protocol (BGP) adalah sebuah *path-vector exterior gateway protocol*. Protokol ini bekerja dengan mengiklankan jaringan dan *host* yang tersedia dalam *autonomous system* ke *autonomous system* lainnya. BGP juga digunakan secara internal dalam topologi fabric untuk memungkinkan konfigurasi yang lebih sederhana dan modular, sering kali di pusat data.

BGP dikonfigurasi pada [router Cisco](#) yang diiklankan dan alamat IP tetangga yang juga mengiklankan BGP. Konfigurasi dapat dilakukan menggunakan perintah berikut untuk *autonomous system* bernomor 100 dengan tetangga yang memiliki *autonomous system* bernomor 200.

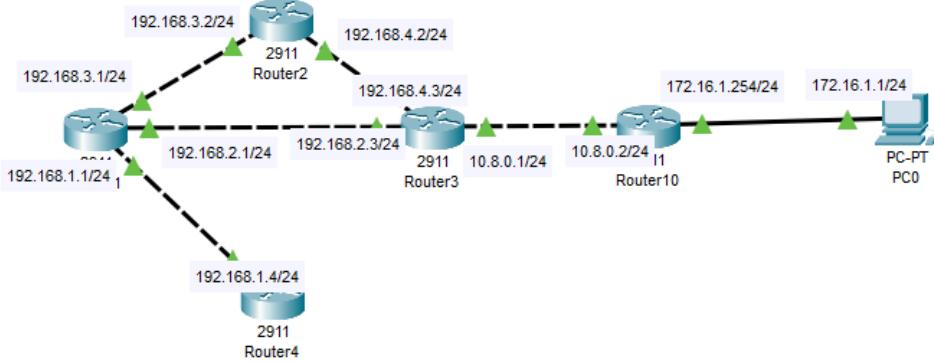
```
Router0(config)# router bgp 100
Router0(config-router)# neighbor 192.168.1.1 remote-as 200
```

Kemudian jaringan dapat diiklankan menggunakan perintah berikut.

```
Router0(config-router)# network 192.168.2.0 mask 255.255.255.0
```

Tugas 6

- | | | |
|--|---|--|
| | Q | Kembangkan topologi pada Tugas 5 untuk menyertakan <i>router</i> lain yang terhubung ke Router3 dengan sebuah PC terhubung ke <i>router</i> tersebut |
|--|---|--|



Konfigurasikan Router3 dan Router10 untuk menghubungkan semua jaringan yang dimilikinya satu sama lain menggunakan BGP, kemudian lakukan ping 192.168.2.3 dari PC0 (Jangan lupa untuk mengatur *default gateway* PC0 ke 172.16.1.254). Gunakan nomor sembarang sebagai nomor *autonomous system* pada Router3 dan Router10 selama berbeda.

Lampirkan dan jelaskan *routing table* pada Router3 dan Router10 serta jelaskan jalur dari PC0 ke 192.168.2.3

A	Konfigurasi PC0
---	------------------------

PC0_13522053

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

DHCP Static

IPv4 Address: 172.16.1.1

Subnet Mask: 255.255.0.0

Default Gateway: 172.16.1.254

DNS Server: 0.0.0.0

IPv6 Configuration

Automatic Static

IPv6 Address: /

Link Local Address: FE80::20C:CFEE:FEA7:1DCB

Default Gateway:

DNS Server:

802.1X

Use 802.1X Security

Authentication: MD5

Username:

Password:

Top

Route Table Router3

Router>en

```
Router#show ip bgp summary
BGP router identifier 192.168.4.3, local AS number 100
BGP table version is 6, main routing table version 6
5 network entries using 660 bytes of memory
5 path entries using 260 bytes of memory
2/1 BGP path/bestpath attribute entries using 276 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1276 total bytes of memory
BGP activity 4/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor      V     AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.8.0.2        4    200       6       3       6     0     0 00:01:58          4

Router#show ip bgp
BGP table version is 6, local router ID is 192.168.4.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric LocPrf Weight Path
*> 10.8.0.0/24    0.0.0.0             0       0 32768 i
*           10.8.0.2             0       0     0 200 i
*> 172.16.1.0/24  10.8.0.2             0       0     0 200 i
*> 192.168.2.0/24 0.0.0.0             0       0 32768 i
*> 192.168.4.0/24 0.0.0.0             0       0 32768 i

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.8.0.0/24 is directly connected, GigabitEthernet0/2
L    10.8.0.1/32 is directly connected, GigabitEthernet0/2
      172.16.0.0/24 is subnetted, 1 subnets
B      172.16.1.0/24 [20/0] via 10.8.0.2, 00:00:00
O    192.168.1.0/24 [110/2] via 192.168.2.1, 00:01:37, GigabitEthernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.2.0/24 is directly connected, GigabitEthernet0/1
L      192.168.2.3/32 is directly connected, GigabitEthernet0/1
O    192.168.3.0/24 [110/2] via 192.168.4.2, 00:01:37, GigabitEthernet0/0
      [110/2] via 192.168.2.1, 00:01:37, GigabitEthernet0/1
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.4.0/24 is directly connected, GigabitEthernet0/0
L      192.168.4.3/32 is directly connected, GigabitEthernet0/0
```

Connected Routes (C):

- 10.0.0.0/8: Terhubung langsung via GigabitEthernet0/2.
- 192.168.2.0/24: Terhubung langsung via GigabitEthernet0/1.
- 192.168.4.0/24: Terhubung langsung via GigabitEthernet0/0.

Local Routes (L):

- 10.8.0.1/32: IP lokal di GigabitEthernet0/2.
- 192.168.2.1/32: IP lokal di GigabitEthernet0/1.
- 192.168.4.3/32: IP lokal di GigabitEthernet0/0.

BGP Routes (B):

- 10.8.0.0/24: Dipelajari dari Router10 via Next Hop 10.8.0.2.
- 172.16.1.0/24: Dipelajari dari Router10 via Next Hop 10.8.0.2.

Route Table Router10

Router10_13522053

Physical Config **CLI** Attributes

```
Router>en
Router#show ip bgp summary
BGP router identifier 172.16.1.254, local AS number 200
BGP table version is 6, main routing table version 6
5 network entries using 660 bytes of memory
5 path entries using 260 bytes of memory
3/2 BGP path/bestpath attribute entries using 460 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1460 total bytes of memory
BGP activity 4/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor      V     AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.8.0.1        4    100       9       5         6     0     0 00:03:28        4

Router#show ip bgp
BGP table version is 6, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
*> 10.8.0.0/24      0.0.0.0                  0     0 32768 i
*           10.8.0.1                  0     0     0 100 i
*> 172.16.1.0/24      0.0.0.0                  0     0 32768 i
*> 192.168.2.0/24    10.8.0.1                  0     0     0 100 i
*> 192.168.4.0/24    10.8.0.1                  0     0     0 100 i

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.8.0.0/24 is directly connected, GigabitEthernet0/0
L        10.8.0.2/32 is directly connected, GigabitEthernet0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/1
L        172.16.1.254/32 is directly connected, GigabitEthernet0/1
B        192.168.2.0/24 [20/0] via 10.8.0.1, 00:00:00
B        192.168.4.0/24 [20/0] via 10.8.0.1, 00:00:00
```

Connected Routes (C):

10.0.0.0/8: Terhubung langsung via GigabitEthernet0/0.
172.16.1.0/24: Terhubung langsung via GigabitEthernet0/1.

Local Routes (L):

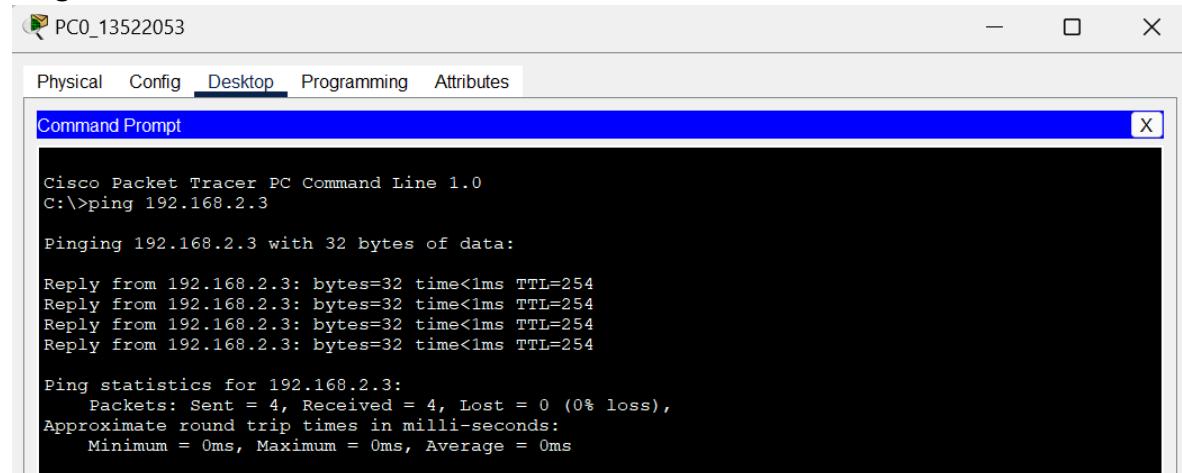
10.8.0.2/32: IP lokal di GigabitEthernet0/0.
172.16.1.254/32: IP lokal di GigabitEthernet0/1.

BGP Routes (B):

192.168.2.0/24: Dipelajari dari Router3 via Next Hop 10.8.0.1.

192.168.4.0/24: Dipelajari dari Router3 via Next Hop 10.8.0.1.

Ping dari PC0 ke 192.168.2.3



The screenshot shows a Cisco Packet Tracer window titled "Ping dari PC0 ke 192.168.2.3". The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with Desktop selected. A Command Prompt window is open, showing the output of a ping command:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Message dari PC0 (172.16.1.1) dikirim ke Router10 sebagai gateway default, lalu Router10 meneruskannya ke Router3 melalui 10.8.0.1 karena rute ke 192.168.2.0/24 dipelajari melalui BGP. Setelah menerima message, Router3 mengetahui bahwa 192.168.2.0/24 terhubung langsung melalui GigabitEthernet0/1 dan meneruskan message ke 192.168.2.3. Balasan dari 192.168.2.3 mengikuti jalur yang sama kembali ke PC0.

Seperti yang ditunjukkan dari tugas sebelumnya, Router10 tidak memiliki rute ke 192.168.1.0/24. Meskipun penambahan pengiklanan rute di BGP Router3 dapat dilakukan secara manual, rute antar protokol dapat didistribusikan secara dinamis satu sama lain menggunakan **route redistribution**. Secara umum, *route redistribution* dilakukan dengan masuk ke konfigurasi rute lalu menggunakan perintah `redistribute`. Sebagai contoh, untuk mendistribusikan rute BGP ke perangkat yang terhubung melalui OSPF, perintah berikut dapat digunakan.

```
Router0(config)# router ospf 1
Router0(config-router)# redistribute bgp 100 subnets
```

Sementara itu, distribusi rute OSPF ke perangkat yang terhubung melalui BGP, perintah berikut dapat digunakan.

```
Router0(config)# router bgp 100
Router0(config-router)# redistribute ospf 1
```

Rute lain seperti *connected* dan *static route* juga dapat didistribusikan menggunakan metode yang serupa dengan ini.

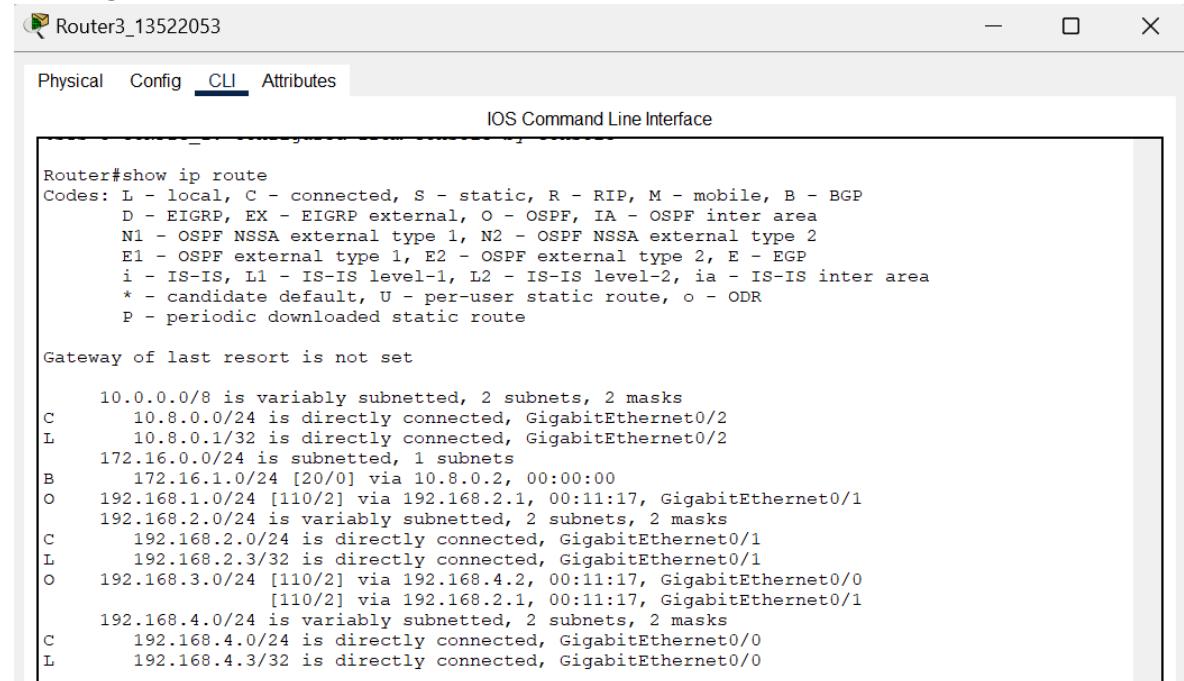
Tugas 7

- Q Gunakan topologi sebelumnya dari Tugas 6. Pada Router3, distribusikan rute BGP ke OSPF dan sebaliknya, kemudian coba lakukan ping ke Router4 dari PC0.

Lampirkan dan amati *routing table* pada Router3 dan Router10 sebelum dan sesudah redistribusi rute. Setelah itu, jelaskan jalur dari PC0 ke Router4.

- A **Routing table sebelum redistribusi rute**
Terlampir pada Tugas 6

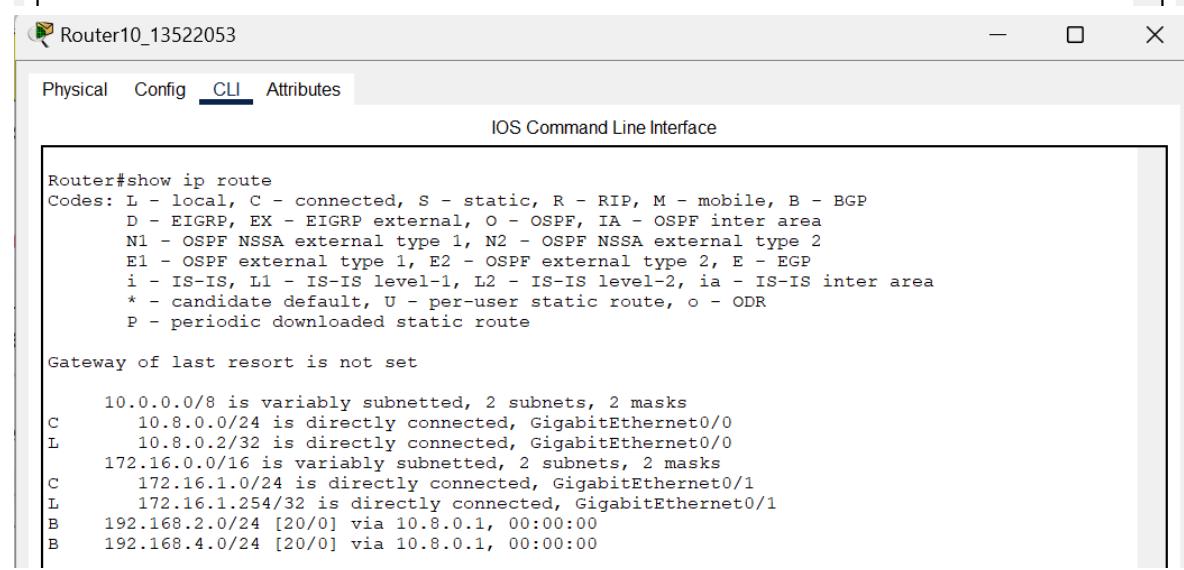
Routing table setelah redistribusi rute



```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.8.0.0/24 is directly connected, GigabitEthernet0/2
L        10.8.0.1/32 is directly connected, GigabitEthernet0/2
  172.16.0.0/24 is subnetted, 1 subnets
B          172.16.1.0/24 [20/0] via 10.8.0.2, 00:00:00
O        192.168.1.0/24 [110/2] via 192.168.2.1, 00:11:17, GigabitEthernet0/1
          192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.2.0/24 is directly connected, GigabitEthernet0/1
L          192.168.2.3/32 is directly connected, GigabitEthernet0/1
O        192.168.3.0/24 [110/2] via 192.168.4.2, 00:11:17, GigabitEthernet0/0
          [110/2] via 192.168.2.1, 00:11:17, GigabitEthernet0/1
          192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.4.0/24 is directly connected, GigabitEthernet0/0
L          192.168.4.3/32 is directly connected, GigabitEthernet0/0
```

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.8.0.0/24 is directly connected, GigabitEthernet0/0
L        10.8.0.2/32 is directly connected, GigabitEthernet0/0
  172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C          172.16.1.0/24 is directly connected, GigabitEthernet0/1
L          172.16.1.254/32 is directly connected, GigabitEthernet0/1
B        192.168.2.0/24 [20/0] via 10.8.0.1, 00:00:00
B        192.168.4.0/24 [20/0] via 10.8.0.1, 00:00:00
```

Ping dari PC0 ke Router4

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=252

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Message dari PC0 dikirim ke Router10 melalui default gateway 172.16.1.254, kemudian Router10 meneruskan message ke Router3 melalui rute BGP. Setelah redistribusi BGP ke OSPF dilakukan, Router3 mengetahui rute menuju Router4 melalui protokol OSPF, sehingga message diteruskan ke Router4 di jaringan 192.168.1.0/24, dan ping berhasil tanpa kehilangan paket.

Protokol *dynamic routing* lainnya selain OSPF dan BGP seperti Intermediate System to Intermediate System ([IS-IS](#)), Enhanced Interior Gateway Routing Protocol ([EIGRP](#)), dan Routing Information Protocol ([RIP](#)) bisa ada atau tidak ada di dalam cakupan lab ini.

IV.4. Network Address Translation (NAT)

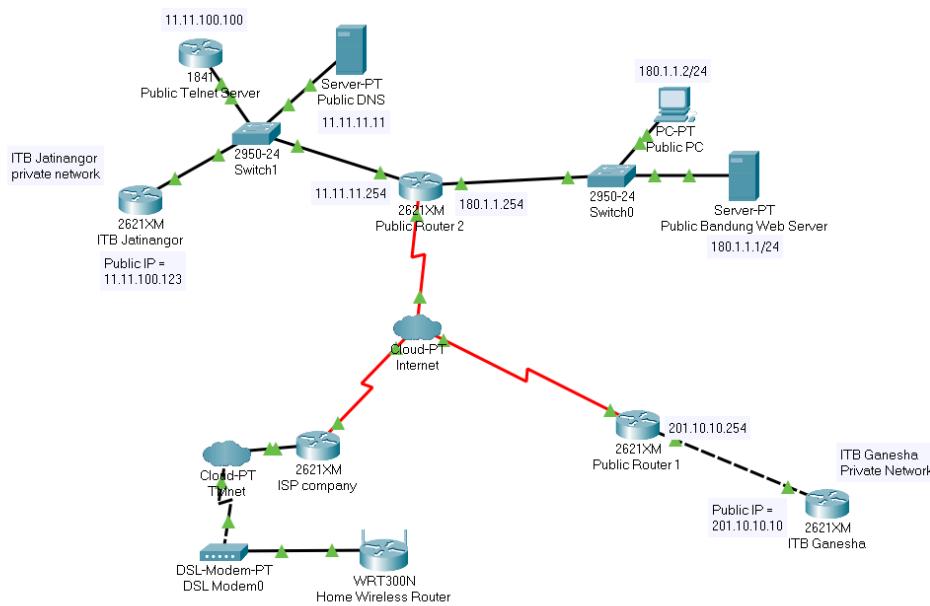
Network Address Translation (NAT) adalah metode memetakan *IP address* dari sebuah jaringan ke *IP address* lain. Hal ini dilakukan dengan mengubah *IP address* pada *header* paket ketika ketika diterima perangkat NAT, sebelum meneruskan paket tersebut ke jaringan. Berdasarkan penjelasan tersebut, hal ini dilakukan pada **network layer** (atau pada **transport layer pada PAT**). NAT digunakan dalam banyak hal, contohnya untuk mengurangi kebutuhan mengkonfigurasi *IP address host* setiap terdapat perubahan pada jaringan (yang menyebabkan perubahan *IP address*), mengurangi penggunaan *IPv4 address*, dan juga dapat berfungsi sebagai *load balancer* (yang tidak termasuk dalam topik kuliah ini, namun menarik untuk dieksplorasi). Sebagai catatan, terdapat beberapa metode *mapping* NAT, yang sebagian akan dibahas pada modul ini.

1. Setting up

Tugas pada bagian ini akan sedikit berbeda dari tugas-tugas lain untuk membantu praktikan memulai dengan lebih cepat dan memberi contoh yang lebih relevan terkait penggunaan NAT dan konfigurasi-konfigurasi lainnya.

Tugas 8

- | | |
|---|---|
| Q | Download file Packet Tracer NAT-start.pkt yang telah kami persiapkan. |
|---|---|

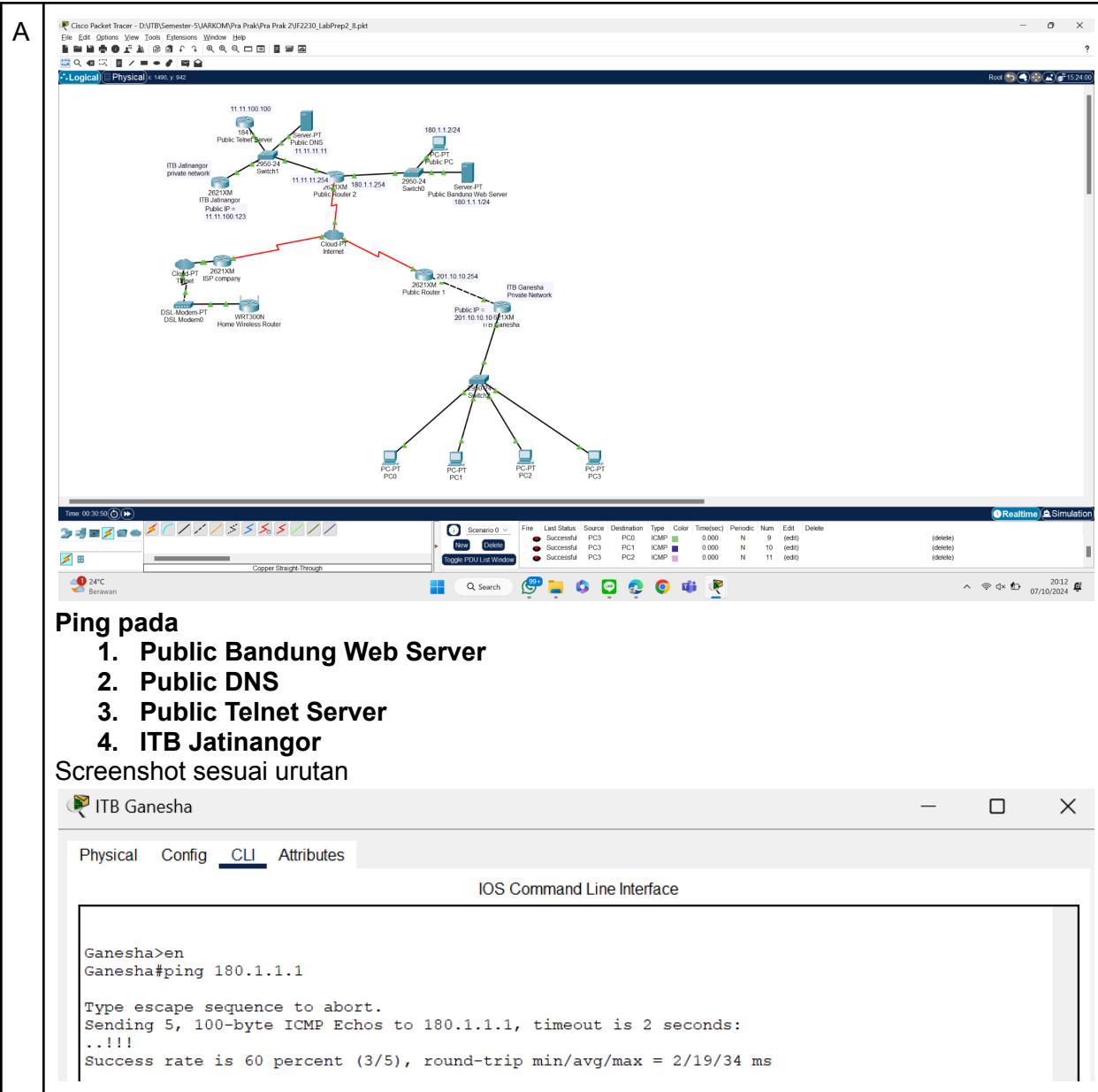


Gambar IV.4.1.1. Jaringan Awal

Jaringan awal yang disediakan telah memiliki router dan server yang telah dikonfigurasi, dan Anda dapat menganggap jaringan ini sebagai bagian dari Internet atau jaringan *public*. Tugas Anda adalah mengkonfigurasi jaringan *private* ITB.

Gunakan router ITB Ganesha untuk melakukan ping pada (i) Public Bandung Web Server; (ii) Public DNS; (iii) Public Telnet Server; dan (iv) ITB Jatinangor. Lakukan hal ini untuk memeriksa perangkat-perangkat pada jaringan berfungsi dengan baik.

Setelah memeriksa *connectivity*, hubungkan 4 PC (PC0-3) dengan static IP (192.168.10.1 - 192.168.10.4) dan gunakan 11.11.11.11 sebagai IP DNS (ingat konfigurasi default gateway). Setiap konfigurasi menggunakan subnet mask /24. Setelah melakukan persiapan, periksa *connectivity* dengan melakukan ping antar PC dalam jaringan ITB Ganesha. Setelah itu, coba akses Public Bandung Web Server pada <http://bandung.com> dari salah satu PC melalui *web browser*. **What happened? Explain!**



```

Ganesha#ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/17/37 ms

Ganesha#ping 11.11.100.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.100.100, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/17/36 ms

Ganesha#ping 11.11.100.123
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.100.123, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/25/37 ms

Ganesha#

```

Top

Semua ping berhasil, maka perangkat-perangkat pada jaringan berfungsi dengan baik.

Periksa connectivity dengan melakukan ping antar PC dalam jaringan ITB Ganesha

1. PC0 → PC1, PC2, PC3

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC1	ICMP	teal	0.000	N	0	(edit)	
●	Successful	PC0	PC2	ICMP	dark brown	0.000	N	1	(edit)	
●	Successful	PC0	PC3	ICMP	green	0.000	N	2	(edit)	

2. PC1 → PC0, PC2, PC3

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC1	PC0	ICMP	green	0.000	N	3	(edit)	
●	Successful	PC1	PC2	ICMP	dark green	0.000	N	4	(edit)	
●	Successful	PC1	PC3	ICMP	dark purple	0.000	N	5	(edit)	

3. PC2 → PC0, PC1, PC3

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC2	PC0	ICMP	magenta	0.000	N	6	(edit)	
●	Successful	PC2	PC1	ICMP	light green	0.000	N	7	(edit)	
●	Successful	PC2	PC3	ICMP	dark brown	0.000	N	8	(edit)	

4. PC3 → PC0, PC1, PC2

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC3	PC0	ICMP	green	0.000	N	9	(edit)	
●	Successful	PC3	PC1	ICMP	dark blue	0.000	N	10	(edit)	
●	Successful	PC3	PC2	ICMP	purple	0.000	N	11	(edit)	

Semua ping yang dilakukan oleh antar PC di dalam jaringan ITB Ganesha berhasil.

Akses Public Bandung Web Server pada <http://bandung.com> dari salah satu PC melalui web browser



2. Static NAT

Pada bagian ini, kita akan mengatasi beberapa masalah yang dialami pada bagian sebelumnya menggunakan NAT (dimulai dari static NAT, kemudian menggunakan jenis NAT lain pada bagian-bagian selanjutnya). Static LAN dilakukan dengan memetakan *IP address* lokal secara statik dengan *IP address* eksternal (yang bisa saja merupakan *IP address* global). Selain itu, bagian ini akan menggunakan pemetaan *one-to-one*, yang memetakan masing-masing *IP*

address lokal ke sebuah *IP address* global (ada beberapa metode *mapping static NAT* lain, silakan dieksplorasi). Salah satu contoh penggunaan static NAT adalah memungkinkan sebuah perangkat pada jaringan lokal terekspos pada jaringan *public* (Internet) namun tetap mengenkapsulasi jaringan *private*.

Tugas 9	
Q	<p>Melanjutkan dari tugas sebelumnya, konfigurasi NAT router ITB Ganeshha.</p> <p>Mulailah dengan mengkonfigurasi <i>interface</i> router yang akan digunakan sebagai <i>inside interface</i> & <i>outside interface</i> pada <i>address translation</i> (dengan <i>outside interface</i> merupakan <i>interface</i> yang terhubung ke Internet).</p> <p>Hint: konfigurasi mode NAT <i>interface</i> dengan mengaktifkan mode <i>interface config</i>, kemudian gunakan command <code>ip nat ...</code></p> <p>Setelah mengkonfigurasi <i>inside/outside interface</i> dari <i>address translation</i>, saatnya mengkonfigurasi <i>address translation</i> dari <i>inside interface</i>. Menggunakan static NAT, petakan <i>IP address</i> lokal PC dengan <i>IP address</i> global.</p> <p>Petakan <i>address translation</i> dengan <i>one-to-one mapping</i> berikut:</p> <ul style="list-style-type: none"> • 192.168.10.1 : 201.10.10.11 • 192.168.10.2 : 201.10.10.12 • 192.168.10.3 : 201.10.10.13 <p>Hint: konfgurasi <i>inside address translation</i> pada <i>config mode</i> dengan command <code>ip nat ...</code></p> <p>Screenshoot <i>command-command</i> konfigurasi, kemudian lakukan hal-hal berikut:</p> <ul style="list-style-type: none"> • Akses http://bandung.com melalui web browser PC0. • Lakukan telnet melalui PC1 ke publictelnet.com dengan password “cisco”, kemudian ping http://bandung.com dalam sesi telnet, kemudian keluar dari sesi telnet. • Ping bandung.com dan jatinangor.itb.ac.id dari PC2 • Ping PC0 dan bandung.com dari PC3 <p>Tunjukkan hasilnya, kemudian jelaskan mengapa hal tersebut berhasil/tidak. Tunjukkan juga tabel NAT router.</p>
A	Konfigurasi

ITB Ganesha

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Ganesha#config t
Enter configuration commands, one per line. End with CNTL/Z.
Ganesha(config)#interface FastEthernet0/0
Ganesha(config-if)#ip nat outside
Ganesha(config-if)#exit
Ganesha(config)#interface FastEthernet0/1
Ganesha(config-if)#ip nat inside
Ganesha(config-if)#exit
Ganesha(config)#ip nat inside source static 192.168.10.1 201.10.10.11
Ganesha(config)#ip nat inside source static 192.168.10.2 201.10.10.12
Ganesha(config)#ip nat inside source static 192.168.10.3 201.10.10.13
Ganesha(config)#exit
```

Ping dari PC1 ke bandung.com melalui telnet

PC1

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>telnet publictelnet.com
Trying 11.11.100.100 ...Open

User Access Verification

Password:
TelnetServer>ping bandung.com
Translating "bandung.com"...domain server (255.255.255.255)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

TelnetServer>exit
[Connection to 11.11.100.100 closed by foreign host]
C:\>
```

NAT bekerja dengan baik. IP lokal PC1 (192.168.10.2) dipetakan ke IP publik (201.10.10.12) melalui Static NAT sehingga koneksi Telnet dari PC1 ke publictelnet.com bisa diterima oleh server publik. Ping ke bandung.com dari dalam sesi Telnet berhasil karena PC1 (dengan IP publik 201.10.10.12) sudah berkomunikasi dengan publictelnet.com. Permintaan ping dikirim dari publictelnet.com ke bandung.com, dan jika NAT dan DNS dikonfigurasi dengan benar, server bandung.com merespons.

Ping dari PC2 ke bandung.com dan jatinangor.itb.ac.id

Cisco Packet Tracer PC Command Line 1.0
C:\>ping bandung.com
Pinging 180.1.1.1 with 32 bytes of data:
Reply from 180.1.1.1: bytes=32 time=69ms TTL=125
Reply from 180.1.1.1: bytes=32 time=2ms TTL=125
Reply from 180.1.1.1: bytes=32 time=3ms TTL=125
Reply from 180.1.1.1: bytes=32 time=4ms TTL=125
Ping statistics for 180.1.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 69ms, Average = 19ms
C:\>ping jatinangor.itb.ac.id
Pinging 11.11.100.123 with 32 bytes of data:
Request timed out.
Reply from 11.11.100.123: bytes=32 time=3ms TTL=252
Reply from 11.11.100.123: bytes=32 time=3ms TTL=252
Reply from 11.11.100.123: bytes=32 time=2ms TTL=252
Ping statistics for 11.11.100.123:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms

NAT bekerja dengan benar pada PC2 (192.168.10.3 dipetakan ke 201.10.10.13). PC2 dapat menjangkau server eksternal seperti bandung.com dan jatinangor.itb.ac.id. DNS menerjemahkan domain dengan benar dan tidak ada masalah pada rute atau firewall.

Ping dari PC3 ke PC0 dan bandung.com

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time=18ms TTL=128
Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 18ms, Average = 4ms
C:\>ping bandung.com
Ping request could not find host bandung.com. Please check the name and try again.

PC3 (192.168.10.4) dan PC0 (192.168.10.1) terhubung dengan baik di dalam jaringan lokal ITB Ganesha tanpa perlu melewati NAT. Semua perangkat di subnet yang sama dapat berkomunikasi satu sama lain tanpa masalah jaringan internal.

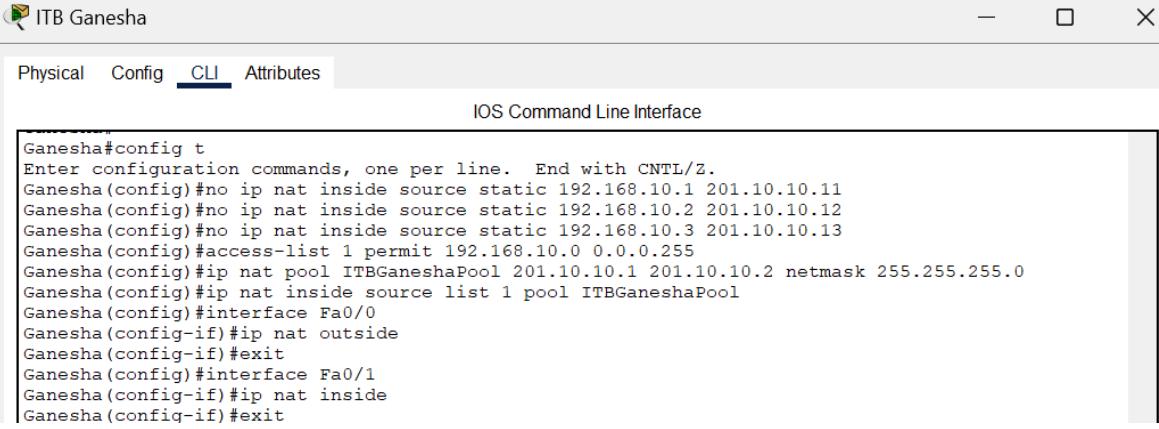
Ping dari PC3 ke bandung.com gagal karena PC3 tidak memiliki IP publik yang dipetakan melalui NAT. Hanya PC yang memiliki pemetaan one-to-one (seperti PC0, PC1, dan PC2) yang dapat melakukan koneksi ke server eksternal.

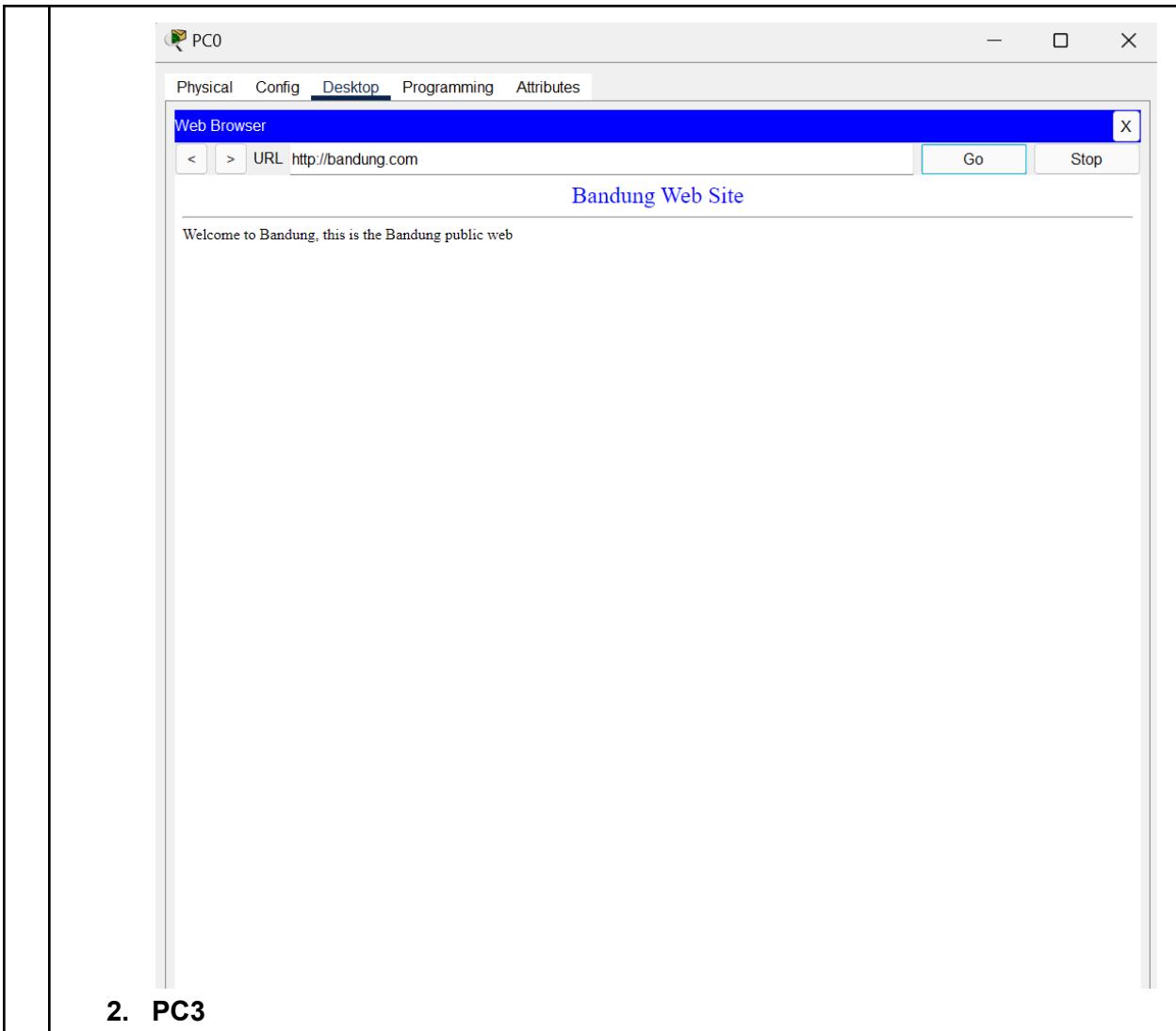
Tabel NAT router	
 ITB Ganeshha	— □ ×
Physical Config CLI Attributes IOS Command Line Interface <pre>Ganesha# Ganesha#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 201.10.10.11 192.168.10.1 --- --- --- 201.10.10.12 192.168.10.2 --- --- --- 201.10.10.13 192.168.10.3 --- --- tcp 201.10.10.12:1025 192.168.10.2:1025 11.11.100.100:23 11.11.100.100:23</pre>	

3. Dynamic NAT

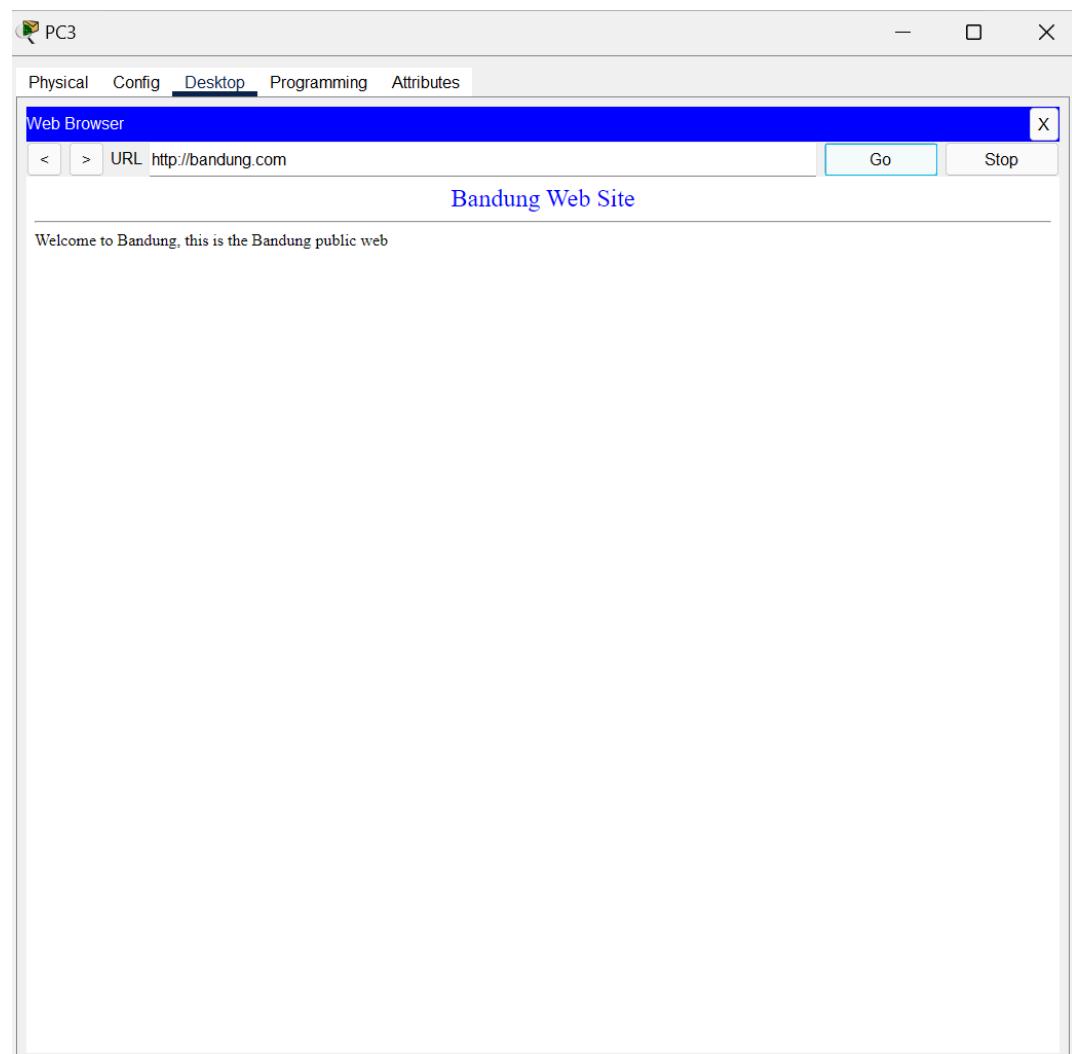
Dengan banyaknya PC dalam sebuah jaringan *private*, terkadang dynamic NAT dibutuhkan, dan static NAT tidak cukup untuk memenuhi kebutuhan tersebut. Dengan dynamic NAT, perangkat-perangkat dalam jaringan *private* dipetakan ke *public IP address* yang dikhususkan (untuk sementara). Pemetaan ini memungkinkan komunikasi 2 arah seperti halnya pada static NAT (sederhananya, dynamic NAT membuat static NAT sementara pada *IP addresses pool*). Berdasarkan cara kerja dynamic NAT, hal ini bermanfaat jika tidak dibutuhkan pemetaan eksplisit antar *address* (tidak ada keterhubungan yang perlu ditetapkan secara *strict* antara alamat *private* dan *public*).

Tugas 10	
Q Dari tugas sebelumnya, konfigurasi NAT router ITB Ganeshha Hapus konfigurasi static NAT dari tugas sebelumnya. Hint: void/hapus <i>address translation</i> pada <i>config mode</i> dengan <i>command no ...</i> (atau restart routernya jika konfigurasi belum di-save pada <i>start config</i>) Setelah menghapus konfigurasi static NAT, konfigurasi kembali <i>inside/outside interface address translation</i> (seperti pada Task 9). Setelah mengkonfigurasi <i>interface-interface</i> tersebut, saatnya mengkonfigurasi dynamic NAT. Pertama, buat <i>address list</i> untuk <i>inside local addresses</i> . Hint: buatlah <i>address list</i> menggunakan <i>access list</i> <code>access-list {X} permit {network address} {wildcard bits} ...</code> Dengan X adalah nomor <i>list</i> , network address adalah <i>address</i> yang akan dilakukan <i>matching</i> , dan wildcard bits adalah bagian dari address yang bisa bernilai apa saja. Selanjutnya, definisikan <i>address pool</i> untuk dynamic NAT yang berisi <i>address</i> 201.10.10.1/24 - 201.10.10.2/24	

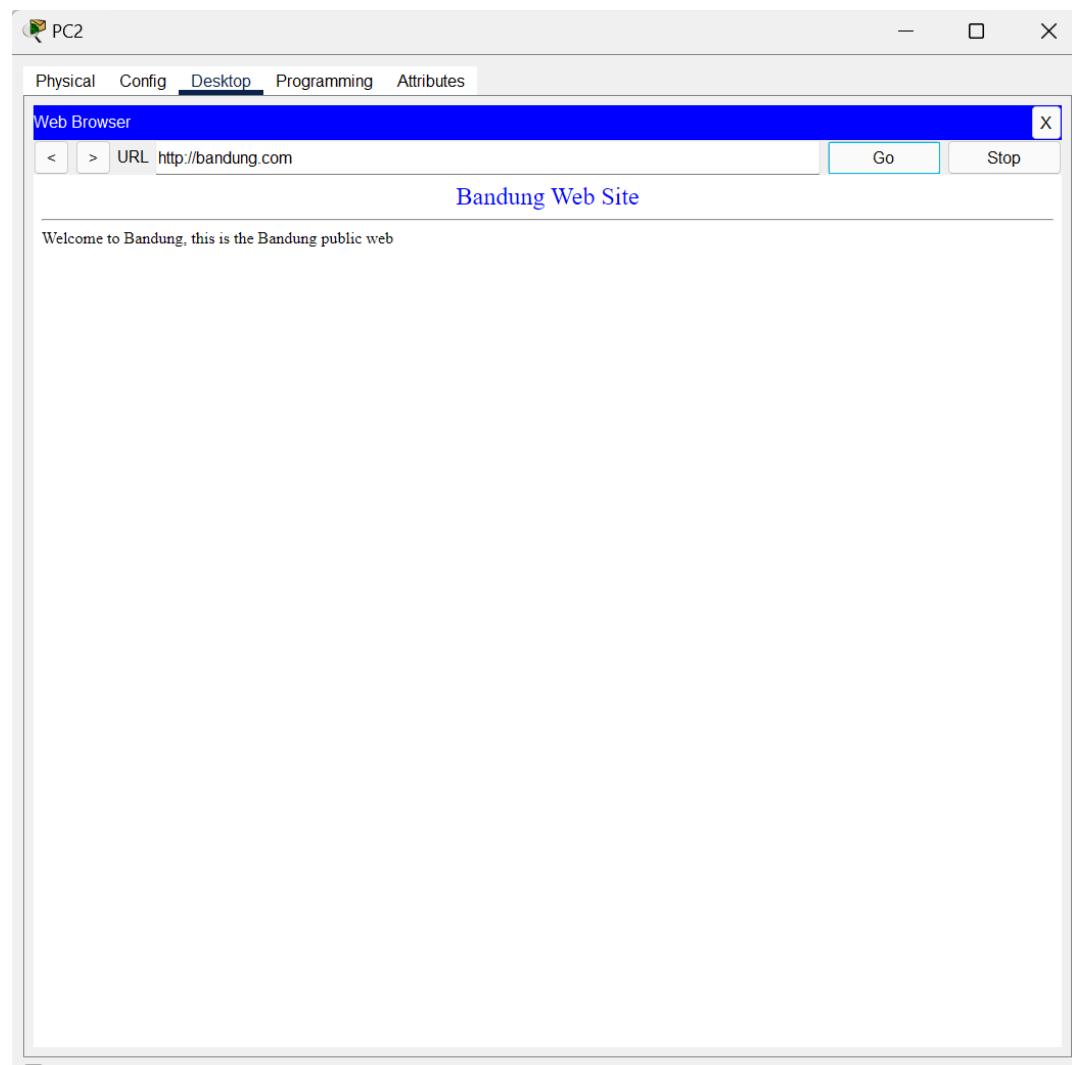
	<p>Hint: buat pendefinisian <i>address pool</i> dengan command ip nat pool ...</p> <p>Kemudian, petakan <i>address list</i> dengan <i>address pool</i> yang telah dikonfigurasi sebelumnya</p> <p>Hint: konfigurasi <i>inside interface</i> NAT dengan command serupa pada konfigurasi static NAT pada tugas sebelumnya.</p> <p>Setelah mengkonfigurasi NAT, lakukan hal-hal berikut ini secara berurutan:</p> <ul style="list-style-type: none"> ● Akses http://bandung.com dari semua web browser PC dengan urutan: PC0 - PC3 - PC2 - PC1. ● Kosongkan NAT table, dan tutup semua web browser PC ● Akses http://bandung.com dari semua web browser PC dengan urutan: PC1 - PC3 - PC2 - PC0. <p>Tampilkan hasilnya dan jelaskan mengapa hal-hal tersebut berhasil/tidak!</p>
A	<h3>Konfigurasi</h3>  <pre>Ganeshा#config t Enter configuration commands, one per line. End with CNTL/Z. Ganeshा(config)#no ip nat inside source static 192.168.10.1 201.10.10.11 Ganeshা(config)#no ip nat inside source static 192.168.10.2 201.10.10.12 Ganeshা(config)#no ip nat inside source static 192.168.10.3 201.10.10.13 Ganeshা(config)#access-list 1 permit 192.168.10.0 0.0.0.255 Ganeshা(config)#ip nat pool ITBGaneshaPool 201.10.10.1 201.10.10.2 netmask 255.255.255.0 Ganeshা(config)#ip nat inside source list 1 pool ITBGaneshaPool Ganeshা(config)#interface Fa0/0 Ganeshা(config-if)#ip nat outside Ganeshা(config-if)#exit Ganeshা(config)#interface Fa0/1 Ganeshা(config-if)#ip nat inside Ganeshা(config-if)#exit</pre> <p>Akses http://bandung.com dari semua web browser PC dengan urutan:</p> <ol style="list-style-type: none"> 1. PC0



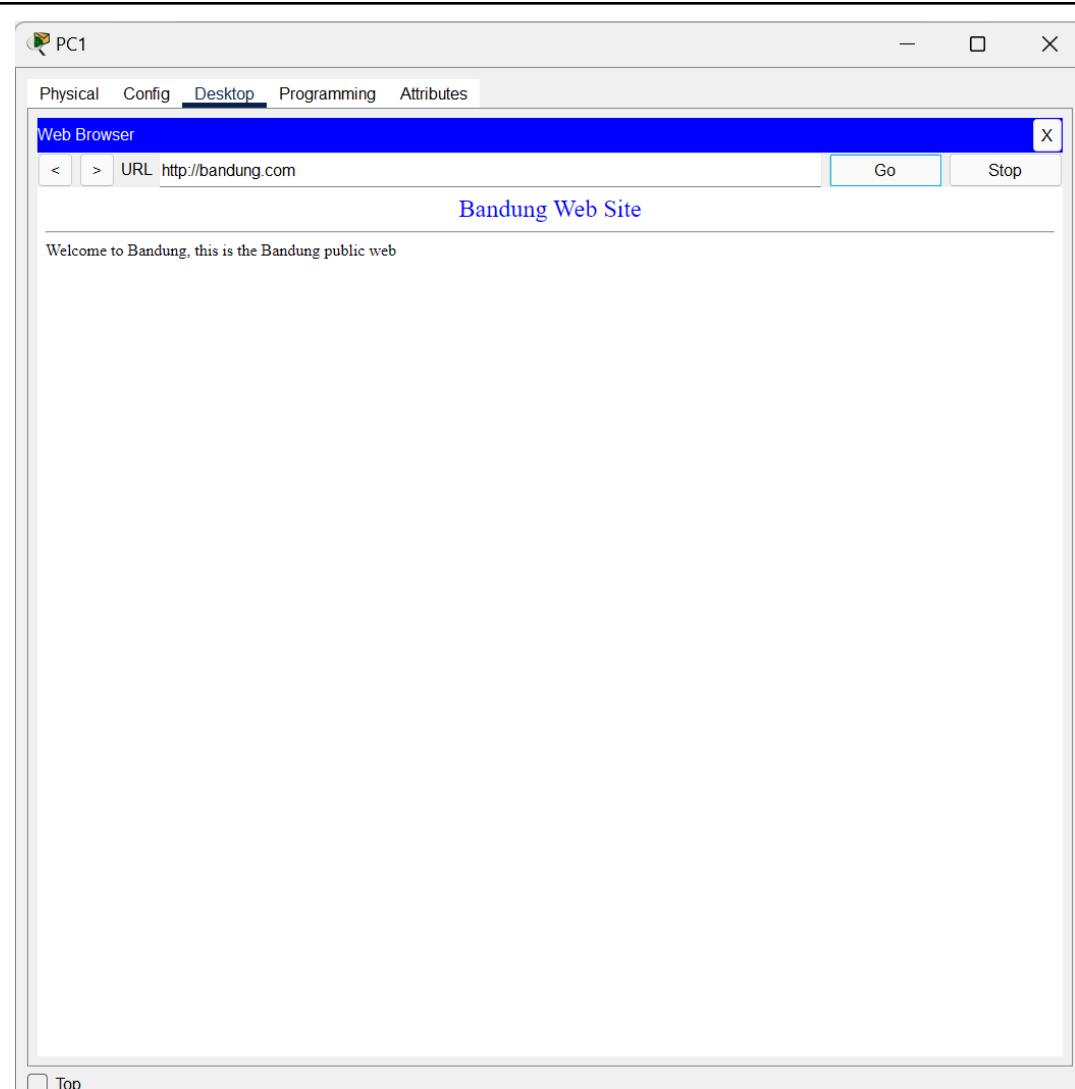
2. PC3



3. PC2



4. PC1

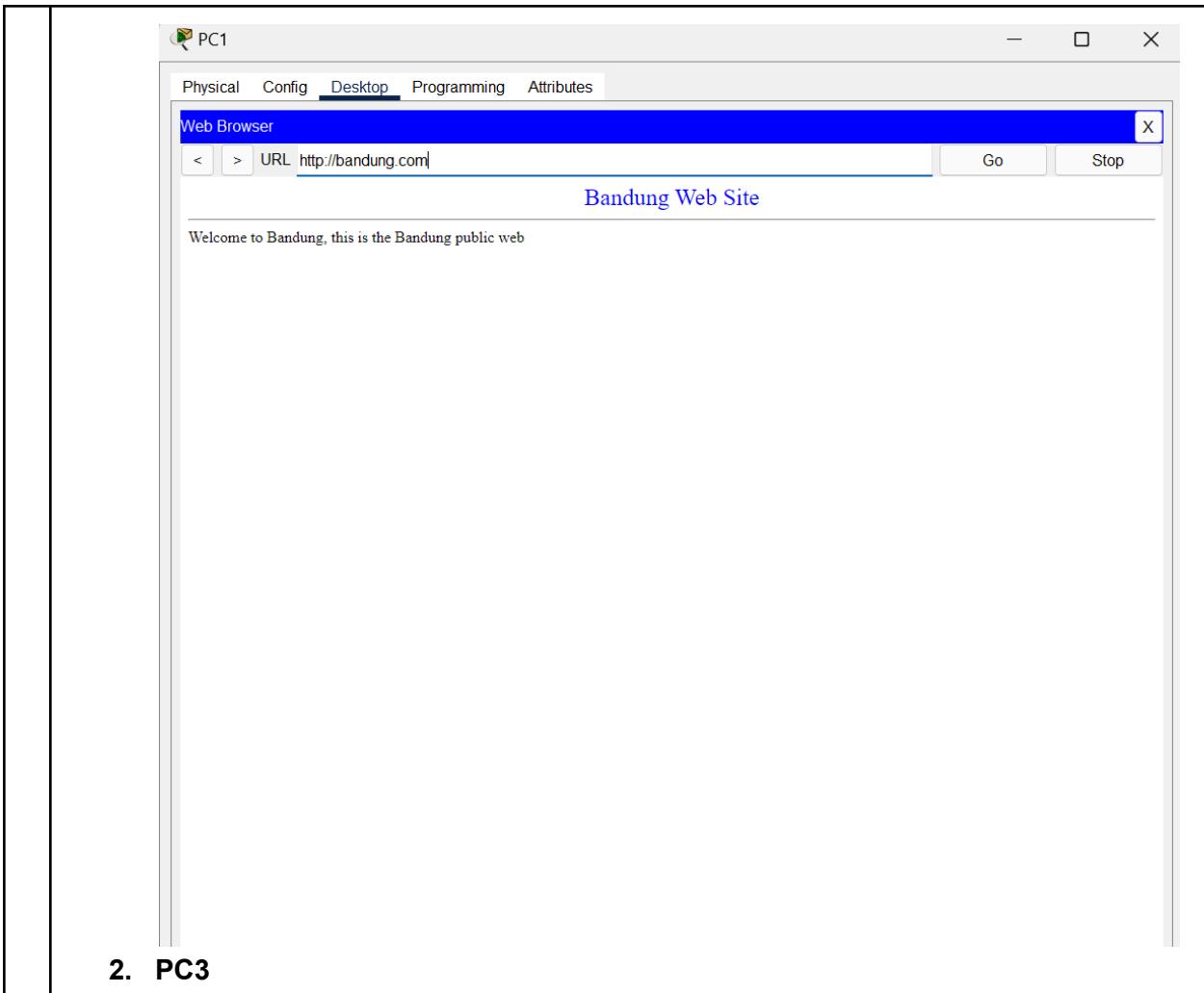


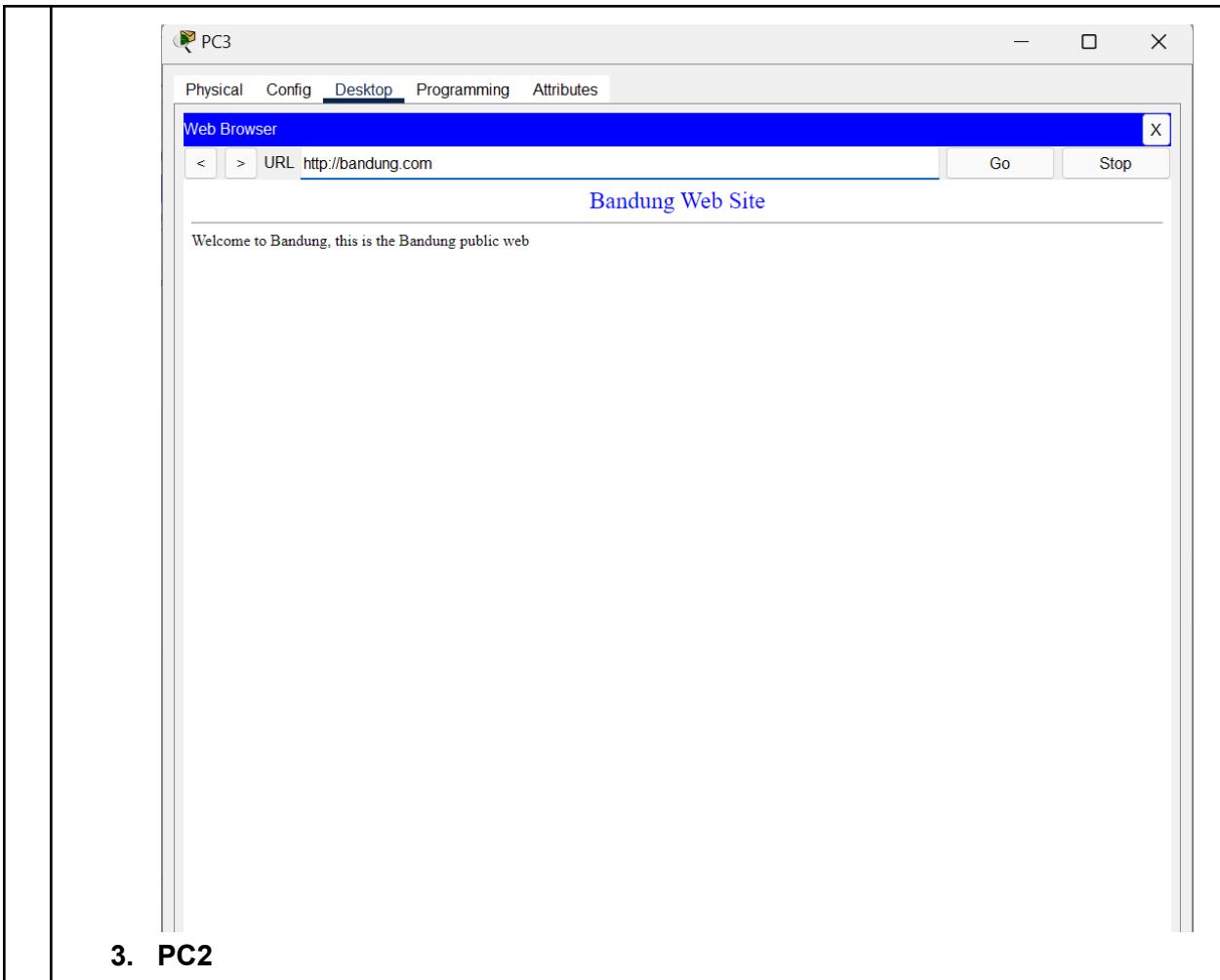
Mengosongkan NAT table

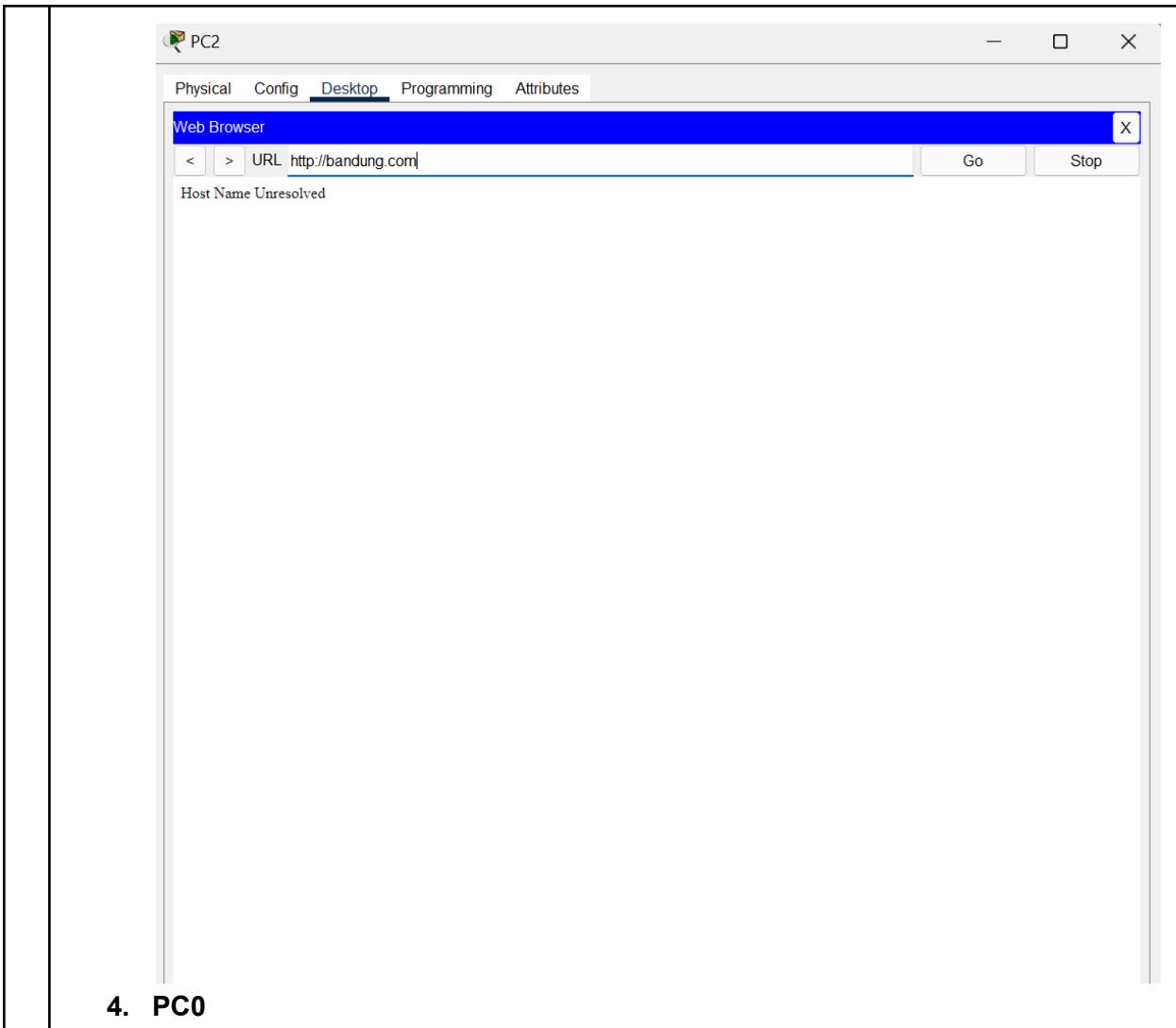
```
Ganesha#clear ip nat translation *
Ganesha#show ip nat translations
Pro Inside global      Inside local        Outside local        Outside global
--- 201.10.10.12      192.168.10.1      ---                ---
--- 201.10.10.13      192.168.10.1      ---                ---
```

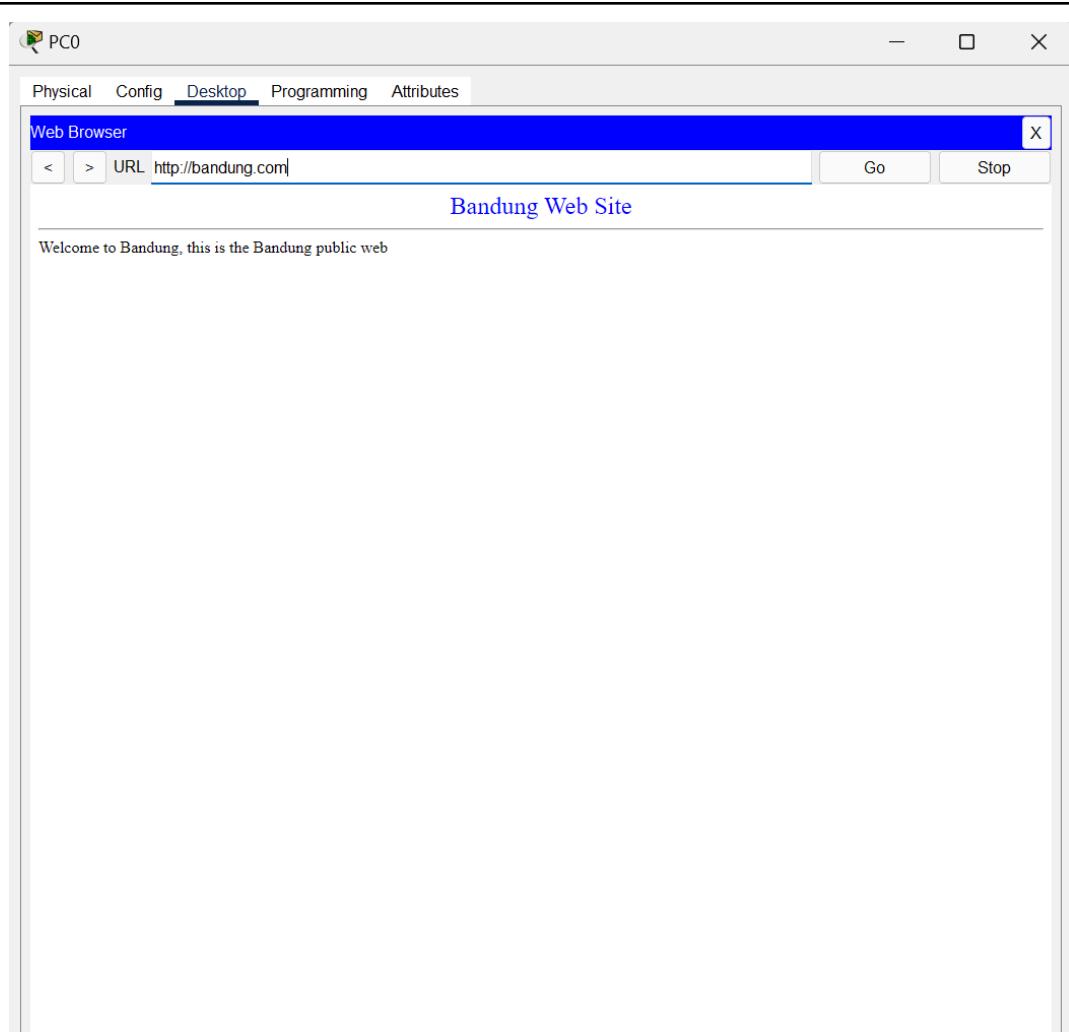
Akses <http://bandung.com> dari semua web browser PC dengan urutan:

1. PC1









Setiap PC akan mendapatkan salah satu dari dua IP publik yang tersedia di pool NAT (201.10.10.1 atau 201.10.10.2). Karena pool hanya memiliki dua IP publik, setelah dua PC mengakses bandung.com, NAT akan menggunakan IP publik yang sama untuk PC lain. Ini berarti IP publik dapat digunakan oleh lebih dari satu PC secara bergantian. PC0 dan PC3 mungkin menggunakan 201.10.10.1, sedangkan PC2 dan PC1 menggunakan 201.10.10.2. Setelah tabel NAT dikosongkan, NAT akan memulai kembali dari nol, dan IP publik dapat dipetakan ulang untuk urutan yang berbeda. Proses ini berhasil karena dynamic NAT sudah terkonfigurasi dengan benar, dan router dapat memetakan IP lokal ke IP publik dari pool yang tersedia. Dengan dynamic NAT, beberapa perangkat dapat menggunakan satu atau dua IP publik secara bergantian, asalkan tidak ada masalah dengan konfigurasi NAT atau routing di jaringan.

4. Port Address Translation (PAT)

Menggunakan NAT bisa bermanfaat, namun terdapat beberapa masalah pada bagian sebelumnya terkait penggunaan NAT. Hal ini lebih besar dengan keterbatasan jumlah *IPv4 address*. Untuk mengatasi hal ini, digunakan PAT, yang memetakan alamat menggunakan *IP*

address dan port number (logical port number) yang digunakan pada **transport layer**, dan bukan *port fisik* dari perangkat). Hal ini membantu mengurangi penggunaan *IPv4 address*, namun mengaburkan pemisahan *network layer* dan *transport layer* pada OSI model.

Tugas 11	
Q	<p>Melanjutkan dari tugas sebelumnya, Anda menyadari keterbatasan jumlah <i>IPv4 address</i>, dan Anda mendapat peringatan dari ICANN karena menggunakan 3 <i>public IP address</i> meskipun Anda hanya disediakan 1 <i>public IP address</i>. Berdasarkan penjelasan pada bagian ini, Anda dapat menyelesaikan persoalan ini.</p> <p>Mulai dengan menghapus konfigurasi dynamic NAT dari bagian sebelumnya (jangan hapus <i>access list</i>).</p> <p>Selanjutnya, konfigurasi router ITB Ganesha (yang memiliki fitur PAT) untuk memetakan <i>access list</i> yang telah dikonfigurasi ke <i>interface</i> router yang terhubung ke Internet Hint: konfigurasi <i>inside interface</i> NAT dengan <i>command</i> serupa dengan konfigurasi static NAT, tetapi petakan menuju sebuah <i>interface</i> dari router. Gunakan opsi overload untuk mengaktifkan PAT</p> <p style="padding-left: 2em;">... overload</p> <p>Lakukan hal-hal berikut:</p> <ul style="list-style-type: none">• Ping bandung.com dari PC0• Akses bandung.com melalui web browser PC1• Lakukan telnet melalui PC2 menuju publictelnet.com dengan password “cisco”, kemudian keluar dari sesi telnet.• Ping bandung.com dari PC3 <p>Kemudian segera tampilkan NAT table router</p> <p>Tunjukkan NAT table router. Kemudian, berdasarkan NAT table yang ditampilkan, jawablah pertanyaan-pertanyaan berikut:</p> <ol style="list-style-type: none">1. Apa <i>public source IP</i> ITB Ganesha?2. Apa layanan udp yang diakses 192.168.10.3?3. Apa layanan tcp yang diakses 192.168.10.?4. Apa fungsi dari <i>port number</i> protokol icmp pada NAT table?
A	NAT Table Router

```

ITB Ganesha
Physical Config CLI Attributes
IOS Command Line Interface

Ganesha#show ip nat translations
Pro Inside global     Inside local      Outside local      Outside global
icmp 201.10.10.10:10   192.168.10.4:10  180.1.1.1:10    180.1.1.1:10
icmp 201.10.10.10:11   192.168.10.4:11  180.1.1.1:11    180.1.1.1:11
icmp 201.10.10.10:8    192.168.10.4:8   180.1.1.1:8     180.1.1.1:8
icmp 201.10.10.10:9    192.168.10.4:9   180.1.1.1:9     180.1.1.1:9
udp 201.10.10.10:1030  192.168.10.3:1030 11.11.11.11:53  11.11.11.11:53
udp 201.10.10.10:1031  192.168.10.4:1031 11.11.11.11:53  11.11.11.11:53
udp 201.10.10.10:1040  192.168.10.2:1040 11.11.11.11:53  11.11.11.11:53
udp 201.10.10.13:1036  192.168.10.1:1036 11.11.11.11:53  11.11.11.11:53
--- 201.10.10.12      192.168.10.1       ---           ---
--- 201.10.10.13      192.168.10.1       ---           ---
tcp 201.10.10.1:1028  192.168.10.4:1028 180.1.1.1:80    180.1.1.1:80
tcp 201.10.10.1:1029  192.168.10.4:1029 180.1.1.1:80    180.1.1.1:80
tcp 201.10.10.10:1027 192.168.10.3:1027 11.11.100.100:23 11.11.100.100:23
tcp 201.10.10.10:1030 192.168.10.2:1030 180.1.1.1:80    180.1.1.1:80
tcp 201.10.10.13:1035 192.168.10.1:1035 180.1.1.1:80    180.1.1.1:80
tcp 201.10.10.2:1028  192.168.10.2:1028 180.1.1.1:80    180.1.1.1:80
tcp 201.10.10.2:1029  192.168.10.2:1029 180.1.1.1:80    180.1.1.1:80

```

Jawaban Pertanyaan

1. Apa public source IP ITB Ganesha?

Public source IP yang digunakan oleh perangkat ITB Ganesha adalah 201.10.10.x. Terlihat dari kolom “Inside global” yang menunjukkan alamat 201.10.10.x untuk setiap entri.

2. Apa layanan udp yang diakses 192.168.10.3?

Layanan UDP yang diakses oleh 192.168.10.3 adalah DNS (port 53) → kolom Outside local dan Outside global menunjukkan 11.11.11.53

3. Apa layanan tcp yang diakses 192.168.10.?

Layanan TCP yang diakses oleh 192.168.10.x adalah HTTP (port 80).

4. Apa fungsi dari port number protokol icmp pada NAT table?

Membedakan sesi ping/echo request yang unik dari setiap perangkat, sehingga router dapat menerjemahkan dan melacak setiap sesi dengan benar.

- Q Setelah mempelajari PAT, saatnya mencoba PAT dengan lebih dari satu *IP addresses*. ITB Ganesha telah mendaftarkan 3 *public IP address* tambahan (201.10.10.1 - 201.10.10.3). Seperti saat mengkonfigurasi PAT pada bagian sebelumnya, konfigurasi PAT untuk menggunakan *pool mode*. Hint: konfigurasi *inside interface* NAT dengan *command* serupa dengan konfigurasi dynamic NAT, tetapi dengan langkah tambahan pada saat konfigurasi PAT
- Lakukan hal-hal berikut:
- Ping bandung.com dari PC0
 - Akses bandung.com melalui web browser PC1
 - Lakukan telnet melalui PC2 menuju publictelnet.com dengan password “cisco”, kemudian keluar dari sesi telnet.
 - Ping bandung.com dari PC3

	<p>Kemudian segera tampilkan NAT table router</p> <p>Tunjukkan NAT table. Kemudian, berdasarkan NAT table yang ditampilkan, jawablah pertanyaan-pertanyaan berikut:</p> <ol style="list-style-type: none"> 1. Apa <i>public source IP</i> ITB Ganeshaa?? 2. Apa perbedaan <i>pool mode</i> PAT dan dynamic NAT dengan membandingkan NAT table kedua mode NAT tersebut? 3. Berikan beberapa contoh (kasus) yang mengakibatkan NAT table menggunakan <i>public IP address</i> lebih pada konfigurasi dynamic PAT
A	<p>NAT Table Router</p> <pre>Ganesha#show ip nat translations Pro Inside global Inside local Outside local Outside global icmp 201.10.10.3:12 192.168.10.4:12 180.1.1.1:12 180.1.1.1:12 icmp 201.10.10.3:13 192.168.10.4:13 180.1.1.1:13 180.1.1.1:13 icmp 201.10.10.3:14 192.168.10.4:14 180.1.1.1:14 180.1.1.1:14 icmp 201.10.10.3:15 192.168.10.4:15 180.1.1.1:15 180.1.1.1:15 udp 201.10.10.13:1037 192.168.10.1:1037 11.11.11.11:53 11.11.11.11:53 udp 201.10.10.3:1031 192.168.10.3:1031 11.11.11.11:53 11.11.11.11:53 udp 201.10.10.3:1032 192.168.10.4:1032 11.11.11.11:53 11.11.11.11:53 udp 201.10.10.3:1041 192.168.10.2:1041 11.11.11.11:53 11.11.11.11:53 udp 201.10.10.3:1042 192.168.10.2:1042 11.11.11.11:53 11.11.11.11:53 --- 201.10.10.12 192.168.10.1 --- --- --- 201.10.10.13 192.168.10.1 --- --- tcp 201.10.10.1:1028 192.168.10.4:1028 180.1.1.1:80 180.1.1.1:80 tcp 201.10.10.1:1029 192.168.10.4:1029 180.1.1.1:80 180.1.1.1:80 tcp 201.10.10.10:1027 192.168.10.3:1027 11.11.100.100:23 11.11.100.100:23 tcp 201.10.10.10:1030 192.168.10.2:1030 180.1.1.1:80 180.1.1.1:80 tcp 201.10.10.13:1035 192.168.10.1:1035 180.1.1.1:80 180.1.1.1:80 tcp 201.10.10.2:1028 192.168.10.2:1028 180.1.1.1:80 180.1.1.1:80 tcp 201.10.10.2:1029 192.168.10.2:1029 180.1.1.1:80 180.1.1.1:80 tcp 201.10.10.3:1028 192.168.10.3:1028 11.11.100.100:23 11.11.100.100:23 tcp 201.10.10.3:1031 192.168.10.2:1031 180.1.1.1:80 180.1.1.1:80 tcp 201.10.10.3:1032 192.168.10.2:1032 180.1.1.1:80 180.1.1.1:80</pre> <p>Jawaban Pertanyaan</p> <ol style="list-style-type: none"> 1. Apa public source IP ITB Ganeshaa?? Public source IP yang digunakan adalah 201.10.10.1, 201.10.10.2, dan 201.10.10.3. Terlihat di kolom Inside global, ini adalah IP publik yang diterjemahkan dari IP lokal (192.168.10.x). 2. Apa perbedaan pool mode PAT dan dynamic NAT dengan membandingkan NAT table kedua mode NAT tersebut? Dalam PAT pool mode, beberapa alamat IP publik (dalam kasus ini, 201.10.10.1 - 201.10.10.3) digunakan secara bersamaan oleh banyak perangkat di jaringan lokal. Setiap perangkat atau sesi menggunakan port yang berbeda sehingga beberapa perangkat bisa berbagi satu IP publik yang sama. Pada tabel NAT, terlihat ada beberapa Inside local (misalnya, 192.168.10.4 dan 192.168.10.2) yang menggunakan satu IP publik yang sama (201.10.10.1) tetapi dengan port yang berbeda. Dalam dynamic NAT, alamat IP publik dari sebuah pool diberikan kepada perangkat lokal secara dinamis, tetapi setiap perangkat atau sesi mendapatkan satu IP publik eksklusif dari pool (tanpa berbagi port dengan perangkat lain). Jadi, setiap perangkat akan menggunakan satu IP publik secara unik hingga sesi selesai. Tabel NAT pada dynamic NAT akan menunjukkan satu Inside local yang dipetakan ke satu Inside global tanpa ada overload (berbagi port). Intinya, perbedaan utama antara pool mode PAT dan dynamic NAT adalah pada

	<p>penggunaan port. Pool mode PAT memungkinkan banyak perangkat menggunakan satu IP publik dengan port yang berbeda (overload), sementara dynamic NAT memberikan satu IP publik unik per perangkat, tanpa overload.</p> <p>3. Berikan beberapa contoh (kasus) yang mengakibatkan NAT table menggunakan public IP address lebih pada konfigurasi dynamic PAT</p> <ul style="list-style-type: none"> - Banyak perangkat yang mengakses Internet secara bersamaan. - Aplikasi yang membuka banyak sesi atau menggunakan banyak port. - Keterbatasan jumlah port yang bisa digunakan oleh satu IP publik dalam mode overload.
--	---

5. Port Forwarding

Setelah mempelajari penggunaan PAT, dan bagaimana PAT dapat digunakan untuk menerjemahkan beberapa *local address* secara dinamik ke satu atau beberapa *public address*. Namun, ketika kita ingin mengkonfigurasi server yang melakukan *listen* koneksi dan bukan melakukan *request* (misalnya ping, http request, DNS lookup), hal ini menjadi tidak dapat dilakukan (karena tidak ada *endpoint* yang *fixed* untuk menerima koneksi). Untuk memetakan port statik yang menerima koneksi, perangkat di jaringan *private* harus memiliki jalur “khusus” untuk menerima *request* dari alamat publik melalui perangkat NAT. Untuk melakukan hal ini, digunakan port forwarding, untuk memetakan alamat tertentu secara statik sehingga perangkat di jaringan *private* memiliki alamat “khusus” yang terekspos ke Internet.

Tugas 12

Q	<p>Melanjutkan dari bagian sebelumnya, Anda diminta untuk men-deploy server pada jaringan <i>private</i> di Jatinangor, dan memungkinkan server tersebut agar dapat diakses melalui Internet.</p> <p>Tambahkan sebuah Server dalam jaringan ITB Jatinangor. Beri <i>IP address</i> statik 192.168.10.1/24 dan gunakan 192.168.10.254 sebagai gateway-nya.</p> <p>Kemudian, konfigurasi server pada tab “services” di bagian atas. Pilih tab HTTP di bagian kiri, kemudian edit file index.html dengan isi berikut</p> <pre><html> <center>Cisco Packet Tracer</center> <hr>Welcome to ITB Jatinangor >:D </html></pre> <p>Kemudian, konfigurasi <i>inside & outside interface</i> router untuk <i>address translation</i> seperti pada tugas-tugas sebelumnya.</p>
---	---

Setelah itu, konfigurasi *port forwarding* dengan memetakan protokol tcp dari *local address* server pada port 80 ke *global address* pada port 80 (*global address* dari router) secara **static**.

Tunjukkan NAT table. Kemudian, menggunakan salah satu PC dalam jaringan ITB Ganesha, akses webpage dari web server ITB Jatinangor (akses menggunakan *global IP address* server tersebut)

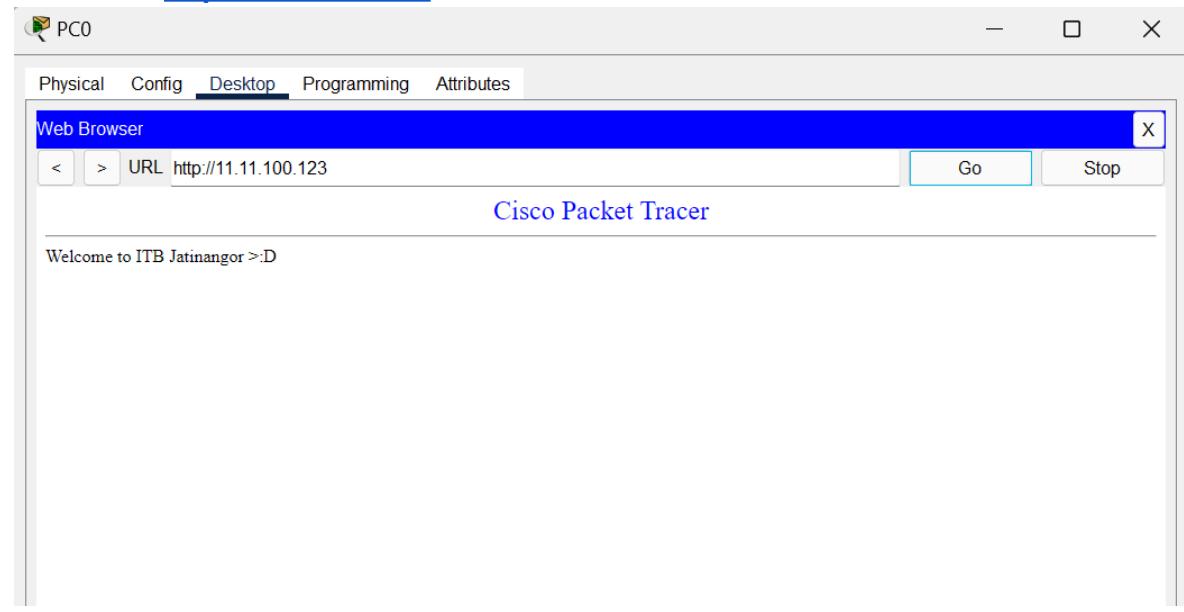
A **Konfigurasi**

```
Jatinangor(config)#interface FastEthernet0/0
Jatinangor(config-if)#ip nat outside
Jatinangor(config-if)#exit
Jatinangor(config)#ip nat outside
% Incomplete command.
Jatinangor(config)#interface FastEthernet0/1
Jatinangor(config-if)#ip nat inside
Jatinangor(config-if)#exit
Jatinangor(config)#ip nat inside source static tcp 192.168.10.1 80 11.11.100.123 80
Jatinangor(config)#exit
Jatinangor#
```

NAT Table

```
Jatinangor#show ip nat translations
Pro Inside global      Inside local        Outside local      Outside global
tcp 11.11.100.123:80  192.168.10.1:80    ---              ---
```

PC0 akses <http://11.11.100.123>



Referensi

Cisco. (n.d.). *Cisco Networking Academy*. <https://www.netacad.com>

Lammle, T. (2020). *CCNA certification study guide: Exam 200-301*. Sybex.