

Modul Pra-praktikum IF2230 Jaringan Komputer

3 - Wireless Router, DNS, SSH, Network Access Control List, dan IPv6

Dipersiapkan oleh Sister'21

Waktu Mulai :

Selasa, 8 Oktober 2024, 15:00 WIB

Waktu Akhir :

Selasa, 15 Oktober 2024, 13:00 WIB

I. Daftar Revisi

1.

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:

- Wireless Router
- DNS
- SSH
- Network Access Control List
- IPv6 (and tunneling with IPv4)

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 ketidakkululusan 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. Kumpulan tugas Anda melalui form [ini](#). Upload dokumen Anda dengan format penamaan: **IF2230_LabPrep[X]_<NIM>.pdf**

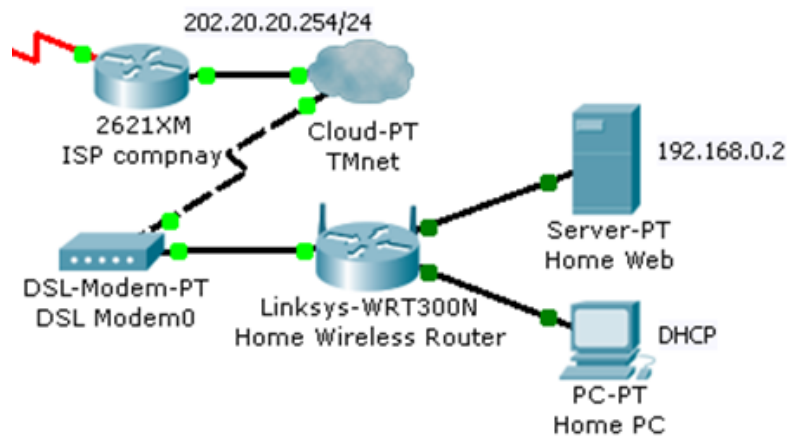
IV. Modul Pra-praktikum

IV.1. Wireless Router

Terdapat berbagai jenis perangkat keras jaringan nirkabel, masing-masing memiliki tujuan dan kemampuan sendiri. Salah satu perangkat tersebut adalah *wireless router* (perangkat lainnya termasuk *access point*, *repeater*, dan beberapa perangkat nirkabel lainnya). Wireless router berfungsi sebagai router dan juga sebagai access point.

Tugas 1

Q Download file [NAT-start.pkt](#) dari Packet Tracer yang telah kami siapkan.



Atur jaringan rumah dengan Server dan PC seperti pada gambar di atas.

Mulailah dengan mengkonfigurasi wireless router dengan pengaturan berikut (**pastikan untuk menyimpan pengaturan dengan tombol “save settings” di bawah ini**):

Network Setup

Router IP

DHCP Server Settings

IP Address:

192

168

0

1

Subnet Mask:

255.255.255.0

DHCP Server:

☒ Enabled
☐ Disabled

DHCP Reservation

Start IP Address:

192.168.0.

100

Maximum number of Users:

50

IP Address Range:
192.168.0. 100 - 149

Client Lease Time:

0

minutes (0 means one day)

Static DNS 1:

11

11

11

11

Static DNS 2:

0

0

0

0

Static DNS 3:

0

0

0

0

WINS:

0

0

0

0

Dan, di tab “wireless”, ubah nama SSID jaringan tanpa kabel Anda menjadi “Home network” (biarkan pengaturan lainnya seperti adanya, atau pastikan mereka diisi dengan nilai default seperti berikut):

Basic Wireless Settings

Network Mode:

Mixed

Network Name (SSID):

Home network

Radio Band:

Auto

Wide Channel:

Auto

Standard Channel:

1 - 2.412GHz

SSID Broadcast:

☒ Enabled
☐ Disabled

Kemudian, konfigurasi PC untuk menggunakan DHCP, dan server rumah dengan konfigurasi jaringan berikut:

IP Address	192.168.0.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	11.11.11.11

Tambahkan Laptop, lalu di konfigurasi Fisik, tukar antarmuka ethernet dengan antarmuka tanpa kabel (WPC300N). Kemudian hubungkan ke router nirkabel melalui aplikasi “PC Wireless” di tab desktop (temukan jaringan nirkabel dengan nama yang sama yang telah Anda konfigurasi sebelumnya). Cobalah untuk melakukan ping ke Home PC dan Home Server melalui laptop dan pastikan ping berhasil.

Periksa alamat IP publik yang diberikan kepada router nirkabel di tab “status” dalam menu GUI. Ambil tangkapan layar dan tampilkan hasilnya!

Setelah mengetahui alamat IP router, lakukan ping ke PC0 dan Ganesha Server di ITB Ganesha melalui laptop menggunakan alamat publik mereka (perangkat di ITB Ganesha memiliki alamat mereka yang dipetakan secara statis ke alamat publik mereka).

Setelah ping berhasil, akses situs web Ganesha Server dengan peramban web laptop (gunakan alamat publik Ganesha Server), kemudian tampilkan tabel NAT dari router ITB Ganesha! Ambil tangkapan layar hasilnya, dan jelaskan alamat mana yang mewakili alamat laptop di tabel NAT!

A Konfigurasi Home PC dan Home Server

The screenshot shows the 'Home PC' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing settings for the 'FastEthernet0' interface. The 'DHCP' option is selected under 'IP Configuration'. The 'IPv6 Configuration' section shows 'Static' selected. The '802.1X' section shows 'Use 802.1X Security' unchecked, 'Authentication' set to 'MD5', and 'Username' and 'Password' fields empty.

Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.0.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	11.11.11.11
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::201:63FF:FE2A:9C2D
Default Gateway	
DNS Server	
802.1X	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5
Username	
Password	

Home Web

PhysicalConfigServicesDesktopProgrammingAttributes

IP Configuration

IP Configuration

DHCP

Static

IPv4 Address192.168.0.2

Subnet Mask255.255.255.0

Default Gateway192.168.0.1

DNS Server11.11.11.11

IPv6 Configuration

Automatic

Static

IPv6 Address

Link Local AddressFE80::201:43FF:FE69:6AB0

Default Gateway

DNS Server

802.1X

Use 802.1X Security

AuthenticationMD5

Username

Password

Ping dari Laptop ke Home PC dan Home Server

Laptop0

PhysicalConfigDesktopProgrammingAttributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=51ms TTL=128
Reply from 192.168.0.100: bytes=32 time=22ms TTL=128
Reply from 192.168.0.100: bytes=32 time=15ms TTL=128
Reply from 192.168.0.100: bytes=32 time=33ms TTL=128

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 51ms, Average = 30ms

C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=31ms TTL=128
Reply from 192.168.0.2: bytes=32 time=24ms TTL=128
Reply from 192.168.0.2: bytes=32 time=22ms TTL=128
Reply from 192.168.0.2: bytes=32 time=26ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 31ms, Average = 25ms
```

Status Home Wireless Router

Home Wireless Router

PhysicalConfigGUIAttributes

Wireless-N Broadband Router

Firmware Version: v0.93.3

Status

SetupWirelessSecurityAccess RestrictionsApplications & GamingAdministrationStatus

RouterLocal NetworkWireless Network

Router Information

Firmware Version:v0.93.3

Current Time:Not Available

Internet MAC Address:00E0.F985.7801

Host Name:

Domain Name:

Internet Connection

Connection Type:Automatic Configuration - DHCP

Internet IP Address:202.20.20.1

Subnet Mask:255.255.255.0

Default Gateway:202.20.20.254

DNS1:11.11.11.11

DNS2:11.11.11.11

DNS3:

MTU:1500

DHCP Lease Time:1 days 0:0:0

IP Address Release

IP Address Renew

Help...

Ping ke PC0 dan Ganesha Server di ITB Ganesha melalui laptop menggunakan alamat publik mereka

```
C:\>ping 201.10.10.11

Pinging 201.10.10.11 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 201.10.10.11: bytes=32 time=52ms TTL=124
Reply from 201.10.10.11: bytes=32 time=50ms TTL=124

Ping statistics for 201.10.10.11:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 52ms, Average = 51ms

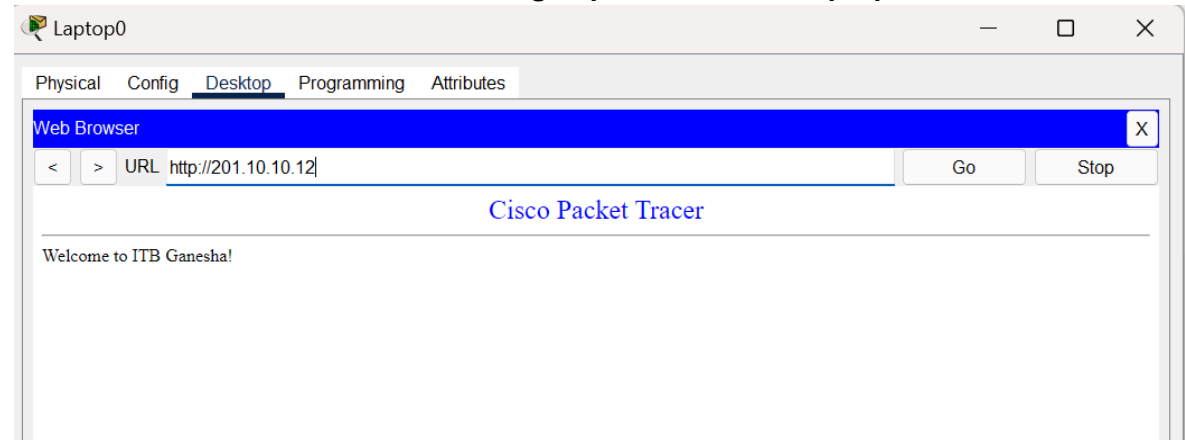
C:\>ping 201.10.10.12

Pinging 201.10.10.12 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 201.10.10.12: bytes=32 time=51ms TTL=124
Reply from 201.10.10.12: bytes=32 time=51ms TTL=124

Ping statistics for 201.10.10.12:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 51ms, Maximum = 51ms, Average = 51ms
```

Akses situs web Ganesha Server dengan peramban web laptop



Tabel NAT dari router ITB 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      ---                ---
tcp 201.10.10.12:80     192.168.10.2:80   202.20.20.1:1025   202.20.20.1:1025
```

Alamat 202.20.20.1:1025 pada tabel NAT ini adalah representasi dari laptop yang mengakses Ganesha Server (201.10.10.12) pada port 80 (HTTP).

- Q Sekarang, kita akan mengonfigurasi server rumah agar dapat diakses dari luar jaringan rumah. Mulailah dengan mengatur permintaan HTTP di server untuk menyajikan index.html dengan konten berikut:

```
<html>
```

```
<center><font      size='+2'      color='blue'>Cisco      Packet
Tracer</font></center>
<hr>Welcome to my home server!
```

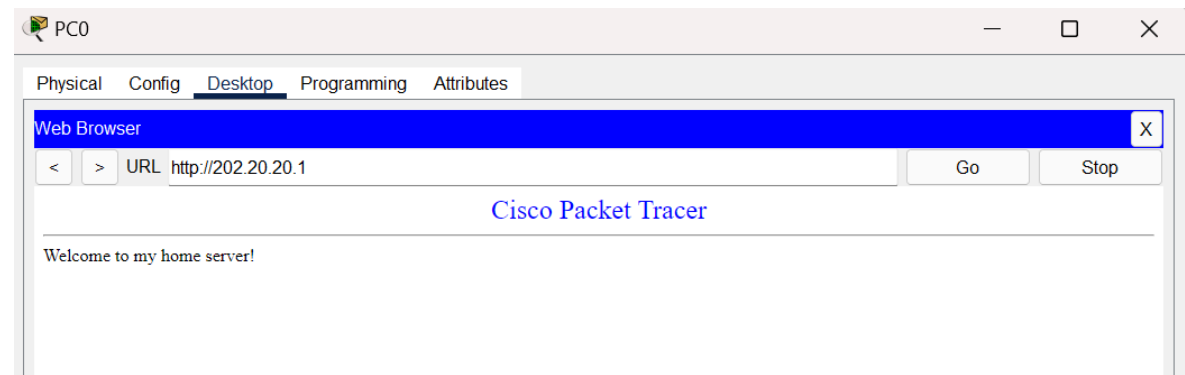
Selanjutnya, konfigurasi pengalihan port server rumah di router nirkabel dengan konfigurasi berikut (di tab “applications and gaming” dan **pastikan untuk menyimpan pengaturan dengan tombol “save settings” di bagian bawah halaman**):

Single Port					
Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
None	—	—	—	192.168.0. 0	<input type="checkbox"/>
None	—	—	—	192.168.0. 0	<input type="checkbox"/>
None	—	—	—	192.168.0. 0	<input type="checkbox"/>
None	—	—	—	192.168.0. 0	<input type="checkbox"/>
None	—	—	—	192.168.0. 0	<input type="checkbox"/>
	80	80	Both	192.168.0. 2	<input checked="" type="checkbox"/>
	0	0	Both	192.168.0. 0	<input type="checkbox"/>

Server rumah Anda seharusnya dapat diakses dari internet publik sekarang!

Akses server rumah Anda melalui PC0 di ITB Ganesha (cek alamat publiknya dengan cara yang sama seperti tugas sebelumnya)! Ambil tangkapan layar hasilnya!

A Akses server rumah melalui PC0 di ITB Ganesha



IV.2. DNS

Dalam praktikum sebelumnya, kita sudah mengeksplorasi topik alamat IP, routing, dan translasi alamat. Namun, manusia mengakses informasi secara online melalui nama yang lebih mudah dibaca seperti 'google.com'. Sistem ini disebut **domain name system (DNS)**. Server DNS menghilangkan kebutuhan bagi manusia untuk mengingat alamat IP seperti 192.168.1.1.

Proses resolusi DNS melibatkan **konversi nama host menjadi alamat IP yang dapat dibaca oleh komputer**. Sebuah translasi harus terjadi antara permintaan pengguna hingga alamat yang dapat dibaca oleh mesin yang diperlukan untuk menemukan sumber daya yang ditetapkan pada nama host oleh pemilik domain melalui pendaftar domain ([domain registrar](#)) diterima.

Ada 8 langkah dalam pencarian DNS:

1. Seorang pengguna mengetik 'example.com' ke dalam aplikasi klien dan kueri tersebut melakukan perjalanan ke Internet dan diterima oleh resolver DNS rekursif.
2. Resolver kemudian menanyakan server nama akar DNS (.).
3. Server akar kemudian merespons resolver dengan alamat server DNS Tingkat Atas (TLD) (.com atau .net), yang menyimpan informasi untuk domain-domainnya. Ketika mencari example.com, permintaan kita diarahkan menuju TLD .com.
4. Resolver kemudian mengajukan permintaan ke TLD .com.
5. Server TLD kemudian merespons dengan alamat IP dari nameserver domain, example.com.
6. Terakhir, resolver rekursif mengirim kueri ke nameserver domain.
7. Alamat IP untuk example.com kemudian dikembalikan ke resolver dari nameserver.
8. Resolver DNS kemudian merespons klien dengan alamat IP dari domain yang diminta sebelumnya.

Entri DNS mungkin disimpan dalam router lokal, browser, atau sistem operasi. Ini membuat akses lebih cepat dengan melewati langkah-langkah pencarian, namun juga memungkinkan serangan seperti pencemaran DNS ([DNS poisoning](#)).

Menambahkan sumber daya di server DNS dilakukan dengan menambahkan entri DNS yang mungkin bervariasi tergantung pada platform DNS yang digunakan. Cloudflare adalah salah satu penyedia layanan pendaftaran DNS yang paling dikenal dengan alamat server DNS 1.1.1.1. Gambar di bawah ini menunjukkan antarmuka manajemen catatan DNS Cloudflare.

DNS management for [REDACTED]

Review, add, and edit DNS records. Edits will go into effect once saved.

DNS Setup: Full ⓘ Import and Export ▼ Dashboard Display Settings

Search DNS Records

[Add filter](#) [Search](#) [Add record](#)

[name] points to [IPv4 address] and has its traffic proxied through Cloudflare.

Type: Name (required): IPv4 address (required): Proxy status: ☒ Proxied TTL:

Record Attributes [Documentation](#)

The information provided here will not impact DNS record resolution and is only meant for your reference.

Comment

[Cancel](#) [Save](#)

<input type="checkbox"/>	Type ⓘ	Name ⓘ	Content ⓘ	Proxy status ⓘ	TTL ⓘ	Actions
<input type="checkbox"/>	A	[REDACTED]	[REDACTED]	Proxied	Auto	Edit
<input type="checkbox"/>	A	[REDACTED]	[REDACTED]	DNS only	Auto	Edit
<input type="checkbox"/>	A	[REDACTED]	[REDACTED]	DNS only - reserved IP	Auto	Edit
<input type="checkbox"/>	A	[REDACTED]	[REDACTED]	DNS only	Auto	Edit
<input type="checkbox"/>	A	[REDACTED]	[REDACTED]	Proxied	Auto	Edit
<input type="checkbox"/>	AAAA	[REDACTED]	[REDACTED]	DNS only	Auto	Edit
<input type="checkbox"/>	CNAME	[REDACTED]	[REDACTED]	Proxied	Auto	Edit
<input type="checkbox"/>	MX	[REDACTED]	[REDACTED]	DNS only	Auto	Edit
<input type="checkbox"/>	TXT	[REDACTED]	[REDACTED]	DNS only	Auto	Edit
<input type="checkbox"/>	TXT	[REDACTED]	[REDACTED]	DNS only	Auto	Edit

Gambar 1. Cloudflare DNS record management interface

Begitu pula, menambahkan entri catatan DNS di server DNS Cisco Packet Tracer dapat dilakukan di antarmukanya.

Server1

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☐ On ☒ Off

Resource Records

Name Type

Address

[Add](#) [Save](#) [Remove](#)

No.	Name	Type	Detail
-----	------	------	--------

Gambar 2. Antarmuka manajemen catatan DNS server Cisco Packet Tracer

Ada berbagai jenis catatan DNS ([DNS records](#)), di antaranya adalah catatan A, catatan AAAA, dan CNAME. Catatan A menyimpan alamat IP dari sebuah domain; catatan AAAA menyimpan alamat IPv6 untuk sebuah domain, berbeda dengan catatan A yang mencantumkan alamat IPv4; sedangkan catatan CNAME meneruskan satu domain atau subdomain ke domain lain

alih-alih memberikan alamat IP. Jenis catatan domain lainnya mungkin ada atau tidak dalam lingkup lab kita.

Apakah Anda pernah mempertimbangkan untuk membeli domain sendiri untuk mengarah ke server Anda sendiri? Beberapa [domain](#) sangat murah, dengan yang termurah di Indonesia harganya kurang dari dua dolar per tahun!

Tugas 2

Q Melanjutkan dari Tugas 1, Anda mungkin merasa kurang familiar dengan mengakses situs web menggunakan alamat IP server web secara langsung. Di sinilah server DNS yang Anda tetapkan dalam konfigurasi sebelumnya berperan.

Di server DNS dengan alamat yang terdaftar dalam konfigurasi Anda, tambahkan catatan DNS dengan `ganesha.itb.ac.id` sebagai nama domain, yang menunjuk ke alamat Ganesha Server (alamat publik).

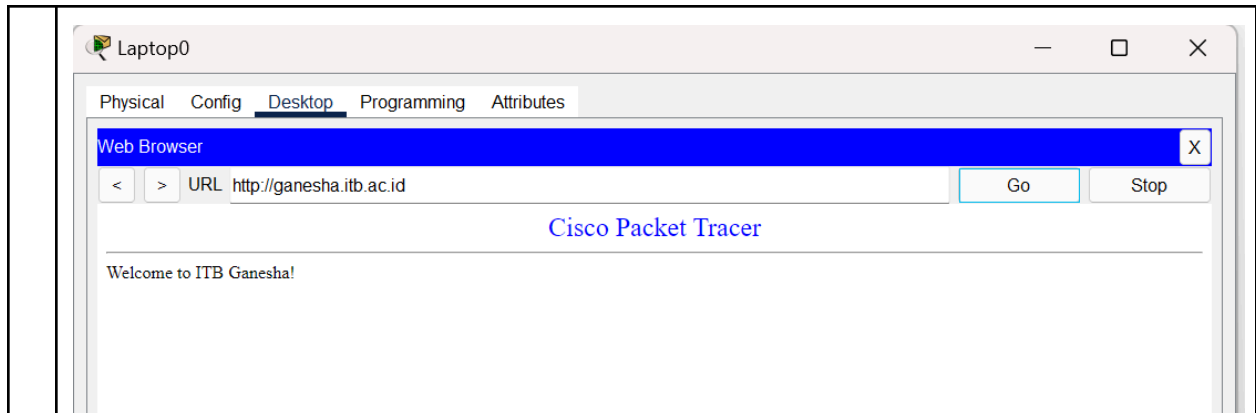
Tampilkan tabel DNS yang baru. Setelah mengatur DNS, coba akses `ganesha.itb.ac.id` dari laptop rumah dan PC Publik (tentu saja melalui peramban web)! Terakhir, amati paket yang dikirim untuk permintaan web tersebut, dan jelaskan prosesnya!

A **Tabel DNS yang baru**

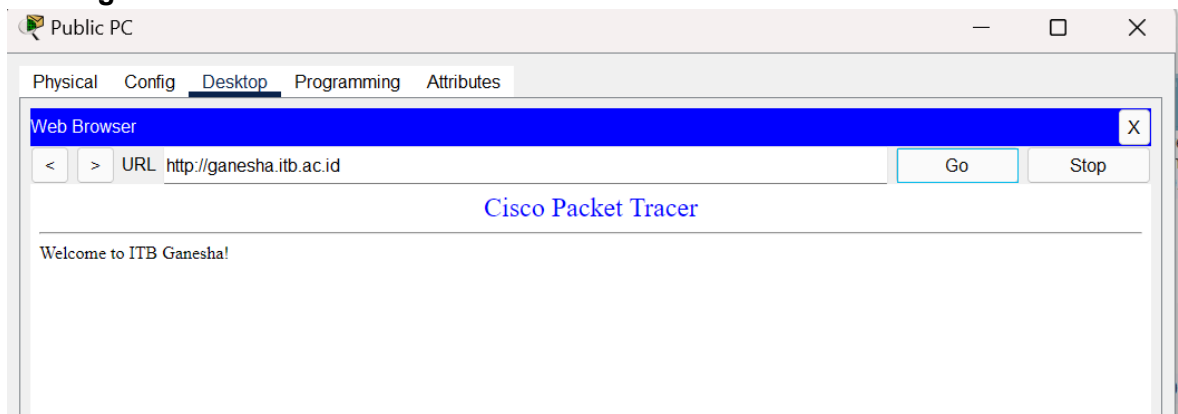
The screenshot shows the 'Public DNS' configuration window. The 'Services' tab is selected, and the 'DNS' service is turned 'On'. Below the service controls, there is a section for 'Resource Records' with a 'Name' field, a 'Type' dropdown set to 'A Record', and an 'Address' field. At the bottom, there are 'Add', 'Save', and 'Remove' buttons. A table displays the current resource records:

No.	Name	Type	Detail
0	Bandung.com	A Record	180.1.1.1
1	ganesha.itb.ac.id	A Record	201.10.10.12
2	jatinangor.itb.ac.id	A Record	11.11.100.123
3	publicteln.net.com	A Record	11.11.100.100

Akses `ganesha.itb.ac.id` dari laptop rumah



Akses ganesha.itb.ac.id dari PC Publik



Simulation paket dari laptop rumah

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.204	--	Laptop0	DNS
	0.205	Laptop0	Home Wireless Router	DNS
	0.206	Home Wireless Router	DSL Modem0	DNS
	0.207	DSL Modem0	TMnet	DNS
	0.208	TMnet	ISP company	DNS
	0.209	ISP company	Internet	DNS
	0.209	--	Home Wireless Router	DNS
	0.210	Home Wireless Router	Laptop0	DNS
	0.210	Internet	Public Router 2	DNS
	0.211	Public Router 2	Switch1	DNS
	0.212	Switch1	Public DNS	DNS
	0.213	Public DNS	Switch1	DNS
	0.214	Switch1	Public Router 2	DNS
	0.215	Public Router 2	Internet	DNS
	0.216	Internet	ISP company	DNS
	0.217	ISP company	TMnet	DNS
	0.218	TMnet	DSL Modem0	DNS
	0.219	DSL Modem0	Home Wireless Router	DNS
	0.220	Home Wireless Router	Laptop0	DNS
	0.220	--	Laptop0	TCP
	0.223	--	Laptop0	TCP
	0.224	Laptop0	Home Wireless Router	TCP
	0.225	Home Wireless Router	DSL Modem0	TCP
	0.226	DSL Modem0	TMnet	TCP
	0.227	TMnet	ISP company	TCP
	0.227	--	Home Wireless Router	TCP
	0.228	Home Wireless Router	Laptop0	TCP
	0.228	ISP company	Internet	TCP
	0.229	Internet	Public Router 1	TCP
	0.230	Public Router 1	ITB Ganesha	TCP
	0.231	ITB Ganesha	Switch2	TCP
	0.232	Switch2	Ganesha Server	TCP
	0.233	Ganesha Server	Switch2	TCP
	0.234	Switch2	ITB Ganesha	TCP
	0.235	ITB Ganesha	Public Router 1	TCP
	0.236	Public Router 1	Internet	TCP
	0.237	Internet	ISP company	TCP
	0.238	ISP company	TMnet	TCP
	0.239	TMnet	DSL Modem0	TCP
	0.240	DSL Modem0	Home Wireless Router	TCP
	0.241	Home Wireless Router	Laptop0	TCP
	0.241	--	Laptop0	HTTP
	0.244	--	Laptop0	TCP

Reset Simulation
☒ Constant Delay
Captured to: 0.244 s

0.232

Switch2

Ganesha Server

TCP

0.233

Ganesha Server

Switch2

TCP

0.234

Switch2

ITB Ganesha

TCP

0.235

ITB Ganesha

Public Router 1

TCP

0.236

Public Router 1

Internet

TCP

0.237

Internet

ISP company

TCP

0.238

ISP company

TMnet

TCP

0.239

TMnet

DSL Modem0

TCP

0.240

DSL Modem0

Home Wireless Router

TCP

0.241

Home Wireless Router

Laptop0

TCP

0.241

--

Laptop0

HTTP

0.244

--

Laptop0

TCP

Reset Simulation
☒ Constant Delay
Captured to: 0.244 s

Permintaan DNS:

- Laptop0 mengirim permintaan DNS melalui Home Wireless Router untuk

menyelesaikan nama ganesha.itb.ac.id.

- Permintaan DNS melewati beberapa perangkat jaringan hingga mencapai Public DNS.
- Public DNS mengembalikan alamat IP 201.10.10.12 untuk ganesha.itb.ac.id.

Permintaan HTTP (TCP):

- Laptop0 menggunakan alamat IP yang diterima dan mengirim permintaan HTTP melalui TCP ke Ganesha Server.
- Permintaan melewati jaringan hingga mencapai Ganesha Server di ITB Ganesha.

Respons dari Ganesha Server:

- Ganesha Server menerima permintaan HTTP dan mengirimkan halaman web kembali ke Laptop0.

Proses berhasil melalui resolusi DNS dan koneksi TCP/HTTP dari Laptop0 ke Ganesha Server.

Simulation paket dari PC Publik

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.033	Public PC	Switch0	DNS
	0.034	Switch0	Public Router 2	DNS
	0.035	Public Router 2	Switch1	DNS
	0.036	Switch1	Public DNS	DNS
	0.037	Public DNS	Switch1	DNS
	0.038	Switch1	Public Router 2	DNS
	0.039	Public Router 2	Switch0	DNS
	0.040	Switch0	Public PC	DNS
	0.040	--	Public PC	TCP
	0.041	Public PC	Switch0	TCP
	0.042	Switch0	Public Router 2	TCP
	0.043	Public Router 2	Internet	TCP
	0.044	Internet	Public Router 1	TCP
	0.045	Public Router 1	ITB Ganesha	TCP
	0.046	ITB Ganesha	Switch2	TCP
	0.047	Switch2	Ganesha Server	TCP
	0.048	Ganesha Server	Switch2	TCP
	0.049	Switch2	ITB Ganesha	TCP
	0.050	ITB Ganesha	Public Router 1	TCP
	0.051	Public Router 1	Internet	TCP
	0.052	Internet	Public Router 2	TCP
	0.053	Public Router 2	Switch0	TCP
	0.054	Switch0	Public PC	TCP

Permintaan DNS:

- Public PC mengirimkan permintaan DNS untuk menyelesaikan nama ganesha.itb.ac.id.
- Permintaan mencapai Public DNS, yang mengembalikan alamat IP 201.10.10.12 ke Public PC.

	<p>Permintaan HTTP (TCP):</p> <ul style="list-style-type: none"> - Public PC mengirimkan permintaan HTTP menggunakan protokol TCP ke alamat IP 201.10.10.12 (Ganesha Server). - Ganesha Server menerima permintaan dan mengirimkan halaman web ke Public PC. <p>Aliran Paket:</p> <ul style="list-style-type: none"> - Paket DNS dikirim dari Public PC ke Public DNS dan kembali ke Public PC. - Paket TCP/HTTP dikirim dari Public PC ke Ganesha Server dan halaman web dikembalikan ke Public PC. <p>Proses berhasil dengan DNS yang menyelesaikan nama domain dan TCP/HTTP yang mengantarkan halaman web ke Public PC.</p>
--	--

IV.3. SSH

Secure Shell ([SSH](#)) adalah metode untuk mengirimkan perintah secara aman ke komputer melalui jaringan yang tidak aman, biasanya untuk mengontrol server dari jarak jauh, mengelola infrastruktur, dan untuk mentransfer file. SSH menggunakan [kriptografi](#) untuk mengautentikasi dan mengenkripsi koneksi antara perangkat. Port default untuk SSH adalah 22.

SSH aman karena mengintegrasikan enkripsi dan autentikasi melalui proses yang disebut kriptografi kunci publik ([public key cryptography](#)). Kriptografi kunci publik adalah cara untuk mengenkripsi data menggunakan kunci asimetris. Salah satu kunci, yaitu kunci publik, tersedia untuk digunakan siapa saja. Kunci lainnya, yaitu kunci privat, disimpan rahasia oleh pemiliknya. Karena kedua kunci saling berhubungan, penetapan identitas pemilik kunci memerlukan kepemilikan kunci privat yang sesuai dengan kunci publik, karena **data yang dienkripsi dengan kunci publik memerlukan kunci privat untuk dekripsi dan sebaliknya**. Dalam koneksi SSH, kedua pihak memiliki sepasang kunci publik/privat, dan masing-masing pihak mengautentikasi satu sama lain menggunakan kunci-kunci ini.

Kunci asimetris ini memungkinkan kedua pihak dalam koneksi untuk merundingkan kunci simetris yang identik dan bersama untuk enkripsi lebih lanjut melalui saluran tersebut. **Setelah negosiasi ini selesai, kedua pihak menggunakan kunci simetris untuk mengenkripsi data yang mereka tukar karena enkripsi dan dekripsi menggunakan kunci simetris lebih cepat.** Terdapat banyak algoritma enkripsi dan lebih banyak rinciannya mengenai kriptografi yang akan dibahas dalam IF4020 Kriptografi. Salah satu algoritma yang paling menonjol digunakan untuk enkripsi asimetris adalah [RSA](#) dengan panjang kunci minimum 2048. Sementara itu, [AES](#) dengan panjang kunci 256 digunakan untuk enkripsi simetris.

Untuk mengonfigurasi server SSH di router Cisco, diperlukan nama host yang bukan default dan nama domain. Atur nama host dan nama domain menggunakan perintah di bawah ini.

```
Router(config)# hostname <name>  
Router(config)# ip domain-name <name>
```

Setelah itu, dibutuhkan pengguna dan kata sandi. Perintah berikut dapat digunakan untuk membuat pengguna di router.

```
Router(config)# username <name> privilege <level> secret <password>
```

Tingkat hak akses menentukan perintah yang akan diotorisasi untuk dijalankan oleh pengguna pada perangkat; penjelasan lebih lanjut dapat diakses di sini. Ketahui bahwa 1 adalah yang terendah dan 15 adalah yang tertinggi. Untuk saat ini, gunakan 15 untuk akses SSH. Enkripsi dan versi SSH juga dapat dikonfigurasi, tetapi PC harus mendukung algoritma hash dan versi SSH yang dipilih, yang seringkali menambah tantangan dalam penerapannya. Untuk menyederhanakan, biarkan semuanya pada default.

Setelah membuat pengguna, generate kunci yang akan digunakan untuk pertukaran kunci. Perintah yang digunakan untuk membuat kunci adalah sebagai berikut, dengan prompt yang meminta spesifikasi lebih lanjut pada implementasi yang mungkin diperlukan tergantung pada pilihan algoritma Anda.

```
Router(config)# crypto key generate <algorithm>
```

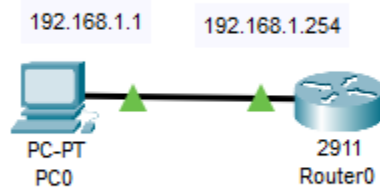
Terakhir, atur sebuah line untuk memungkinkan SSH ke dalam router.

```
Router(config)# line vty 0 15  
Router(config-line)# login local  
Router(config-line)# transport input ssh
```

Dengan cara ini, koneksi SSH dapat dipertahankan menggunakan kunci yang disimpan di router.

Tugas 3

Q Using the following topology



- Atur nama host dan nama domain Router0 menjadi Nomor Induk Mahasiswa Anda.
- Siapkan server SSH di router dengan nama pengguna 'cisco' dan kata sandi 'cisco'.
- Kemudian, sambungkan ke router menggunakan SSH dari PC0.
- Jalankan perintah 'show ip interface brief' dari koneksi SSH.
- Jalankan perintah 'exit' untuk menutup koneksi SSH.

Cantumkan hasil dari perintah 'show ip interface brief' dan 'exit' dari koneksi SSH di area di bawah ini.

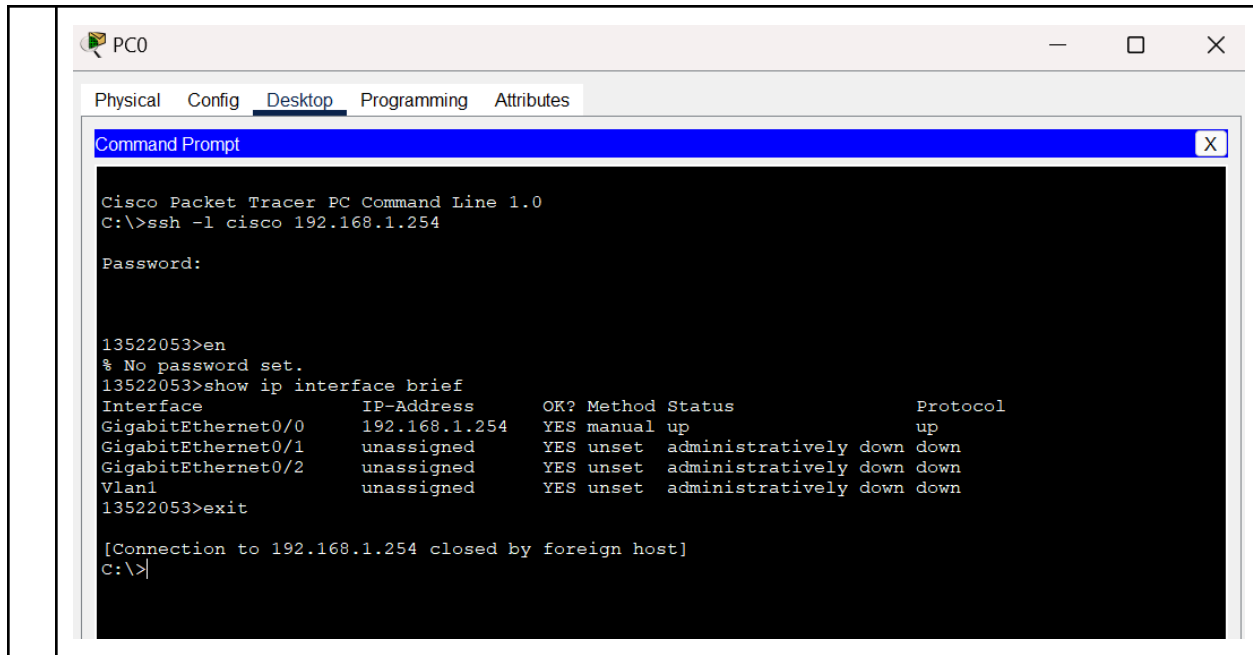
A **Konfigurasi domain dan server SSH**

```
13522053(config)#ip domain-name 13522053.local
13522053(config)#username cisco password cisco
13522053(config)#crypto key generate rsa
The name for the keys will be: 13522053.13522053.local
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

13522053(config)#line vty 0 4
*Mar 1 0:5:40.103: %SSH-5-ENABLED: SSH 1.99 has been enabled
13522053(config-line)#login local
13522053(config-line)#transport input ssh
13522053(config-line)#ip ssh version 2
13522053(config)#ip ssh version 2
13522053(config)#exit
13522053#
```

Hasil 'show ip interface brief' dan 'exit'



Materi dari bagian ini hingga akhir bagian ini berada di luar cakupan Cisco Packet Tracer.

Cara yang lebih tepat untuk mengaktifkan SSH ke router dari PC adalah dengan menghasilkan sepasang kunci di komputer dan kemudian memasukkan kunci publik yang dihasilkan ke router. Ini dapat dilakukan dengan memasuki mode konfigurasi keychain, menentukan pengguna yang terkait dengan kunci, dan memasukkan key-string.

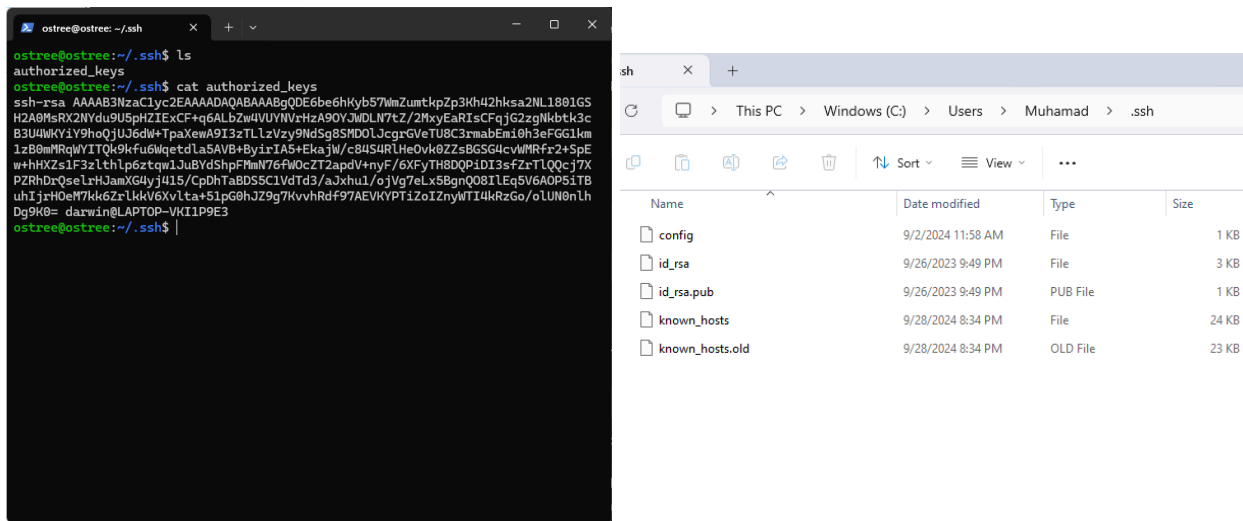
```
Router(config)# ip ssh pubkey-chain
Router(conf-ssh-pubkey)# username <name>
Router(conf-ssh-pubkey-user)# key string
Router(conf-ssh-pubkey-data)# <key, 254 chars at a time>
Router(conf-ssh-pubkey-data)# exit
```

Ini memungkinkan login tanpa kata sandi jika mode autentikasi mengizinkan kunci publik. **Login tanpa kata sandi kurang rentan terhadap rekayasa sosial, sementara menyimpan kunci di perangkat pengguna membuat pengguna terautentikasi dengan benar.** Autentikasi kunci publik kemudian dapat dipaksa lebih lanjut dengan menonaktifkan login menggunakan kata sandi.

```
Router(config)# no ip ssh server authenticate user password
```

Sayangnya, Cisco Packet Tracer memiliki batasan. Tidak mungkin untuk menghasilkan sepasang kunci di PC Cisco Packet Tracer ([Tutorial on how to do it on actual PCs](#)) maupun untuk mengonfigurasi keychain router. Namun, ini adalah pengetahuan yang baik karena koneksi ke server dilakukan dengan cara yang sama dengan menyalin kunci publik Anda ke dalam keychain pengguna. **Di openssh GNU/Linux, itu berada di ~/.ssh/ dengan**

kunci akses publik terletak di file `authorized_keys`. Sementara di Windows, itu terletak di `%USER%.ssh`.



Gambar 3. openssh keychain (kiri), Windows SSH keychain (kanan)

Ini mungkin tidak digunakan dalam lab kita, tetapi perlu diingat bahwa Anda akan menggunakan ini sangat sering. Juga, tidak, saya tidak mengorbankan sistem saya dengan menunjukkan kunci publik saya ([read more](#)).

IV.4. Network Access Control List

Network access-control list (ACL) adalah sekumpulan aturan yang mengizinkan atau menolak akses ke sumber daya komputer pada tingkat jaringan. *Network access control list* dapat berfungsi sebagai penyaring paket, yang menginstruksikan router untuk mengizinkan atau membuang lalu lintas tertentu. ACL dapat menyaring lalu lintas berdasarkan alamat IP sumber/tujuan, port sumber/tujuan, protokol, dan lain sebagainya. **ACL dievaluasi dari atas ke bawah**, sehingga jika suatu permintaan memenuhi beberapa aturan dalam ACL, aturan teratas akan diterapkan. Di sisi lain, jika suatu permintaan tidak memenuhi aturan mana pun dalam ACL, maka akan jatuh pada aturan default yang diterapkan pada ACL. Aturan default dalam ACL bisa berupa penolakan implisit di mana paket selalu dibuang atau pengizinan implisit di mana paket selalu diizinkan.

Secara umum, ada dua jenis ACL IP di router Cisco, yaitu **ACL IP standar** dan **ACL IP extended**. ACL IP standar hanya menyaring lalu lintas berdasarkan alamat IP sumber paket; sedangkan ACL IP *extended* dapat menyaring lalu lintas berdasarkan lebih banyak parameter seperti protokol, port, dan alamat sumber serta tujuan.

Mengonfigurasi ACL IP standar dan diperluas di router Cisco dapat dilakukan dengan secara berurutan membuat entri daftar akses bernomor atau bernama dan kemudian menetapkan

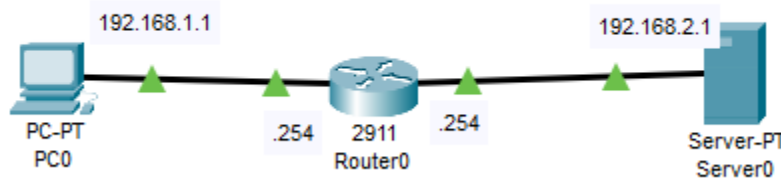
pada suatu antarmuka. Misalnya, entri ACL IP standar yang sederhana dapat ditambahkan di mode konfigurasi global dengan menjalankan perintah berikut.

```
RouterA(config)# access-list <number> {permit | deny} <IP> <Wildcard Mask>
```

Dengan parameter nomor yang merupakan ID dari daftar dan jika wildcard tidak ditambahkan, secara default akan menjadi 0.0.0.0 atau /32.

Tugas 4

Q Menggunakan topologi berikut



Dengan gateway default pada kedua perangkat yang diatur menuju antarmuka router di setiap jaringan.

- Terapkan ACL masuk pada antarmuka 192.168.1.254 Router0 tanpa aturan apa pun.
- Kemudian tambahkan satu aturan yang menolak 192.168.1.1/0 pada ACL yang sama.

Cantumkan perbedaan saat melakukan ping ke Server0 dari PC0 tanpa aturan apa pun dan dengan aturan yang mengizinkan ditambahkan.

A Ping ke Server0 dari PC0 tanpa aturan apa pun

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=127
Reply from 192.168.2.1: bytes=32 time=1ms TTL=127
Reply from 192.168.2.1: bytes=32 time=5ms TTL=127
Reply from 192.168.2.1: bytes=32 time=26ms TTL=127

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 26ms, Average = 8ms
```

Ping ke Server0 dari PC0 dengan aturan yang mengizinkan ditambahkan

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Di sisi lain, entri ACL IP yang diperluas yang sederhana dapat ditambahkan di mode konfigurasi global dengan menjalankan perintah sebagai berikut.

```
RouterA(config)# access-list <number> {permit | deny} <Source> <Destination>
```

Extended IP ACL jauh lebih rinci dibandingkan dengan standard IP ACL dengan konfigurasi yang detail mungkin dilakukan dengan menentukan port sumber/tujuan dan/atau protokol yang digunakan, sehingga bisa sangat panjang. Misalnya, kita bisa mengizinkan host di 172.16.1.0/24 untuk menggunakan port sumber TCP lebih besar dari 9999 untuk mengakses semua port TCP pada server 4.4.4.4/32 kecuali port 23 pada nomor ACL 100 dengan memasukkan perintah berikut.

```
RouterA(config)# access-list 1 permit tcp 172.16.1.0 0.0.0.255 gt 9999 host 4.4.4.4 neq 23
```

Internet Assigned Numbers Authority (IANA) bertanggung jawab untuk memelihara penetapan resmi nomor port untuk penggunaan tertentu. **Tabel resmi untuk port default dapat diakses di [sini](#).** Dalam praktiknya, port yang digunakan untuk aplikasi dan layanan mungkin bervariasi dan dapat digunakan secara bergantian. Penggunaan port default bahkan tidak dianjurkan dalam konteks keamanan jaringan.

Daftar akses kemudian dapat diterapkan pada suatu antarmuka dengan menggunakan perintah berikut, di mana 'in' menyaring paket yang diterima pada antarmuka dan 'out' menyaring paket yang dikirim dari antarmuka.

```
RouterA(config-if)# ip access-group 1 {in | out}
```

Standard dan extended IP access lists dibedakan melalui nomor ID yang digunakan selama pembuatan dengan rentang berikut. Penggunaan nama string sebagai pengganti nomor juga dimungkinkan.

Type	Range
------	-------

Standard IP	1-99 & 1300-1999
Extended IP	100-199 & 2000-2699

Cara yang lebih baik untuk menambahkan ACL adalah dengan memasukkan mode konfigurasi daftar kontrol akses jaringan saat membuat daftar dan menambahkan entri individual di dalamnya. Memasuki mode konfigurasi daftar kontrol akses jaringan dapat dilakukan dengan menggunakan perintah ini.

```
RouterA(config)# ip access-group {standard | extended} {number | name}
RouterA(config-{std | ext}-nacl)# {sequence number} {permit | deny} <Source>
<Destination>
```

Mode konfigurasi daftar akses jaringan lebih baik karena memungkinkan spesifikasi nomor urutan untuk prioritas dan penghapusan entri daftar individual.

Tugas 5	
Q	<p>Menggunakan topologi dari tugas sebelumnya</p> <ul style="list-style-type: none"> - Hapus ACL yang ditambahkan pada tugas sebelumnya. - Buat daftar kontrol akses yang diperluas dengan nama atau nomor yang sembarangan. - Terapkan ACL keluar pada antarmuka 192.168.2.254 Router0 tanpa aturan apa pun. - Tambahkan entri yang menolak akses TCP dari PC0 ke port 80 Server0. - Tambahkan entri yang mengizinkan akses TCP dari PC0 ke port 80 Server0 dengan nomor urutan yang lebih kecil. <p>Cantumkan hasil saat melakukan ping dan mengakses web Server0 dari PC0 sebelum dan setelah menambahkan aturan kedua.</p>
A	Sebelum menambah aturan kedua

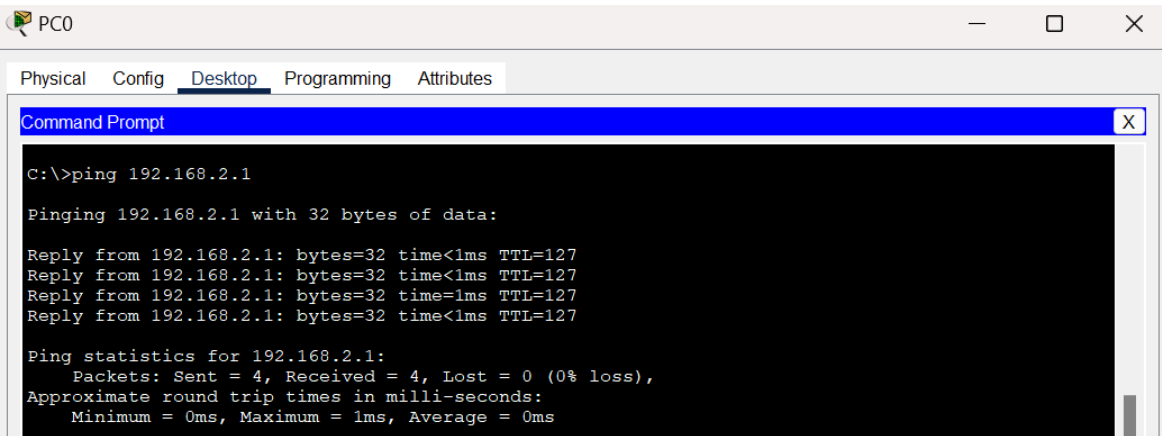
```

13522053>en
13522053#interface Gig0/0
^
% Invalid input detected at '^' marker.

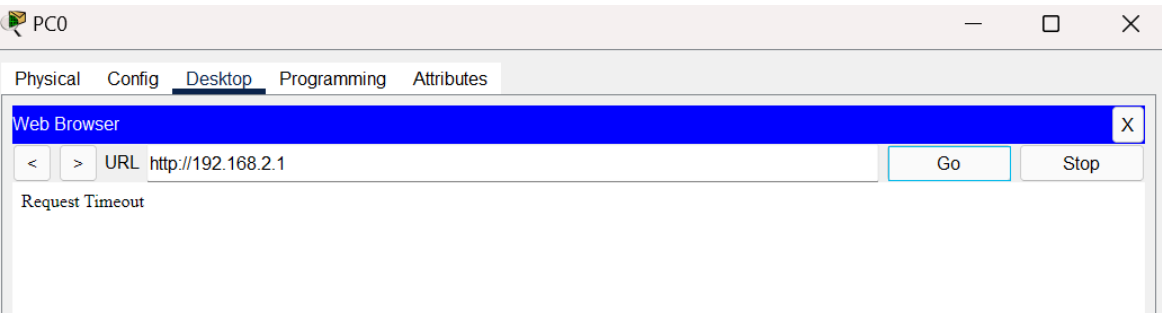
13522053#config t
Enter configuration commands, one per line. End with CNTL/Z.
13522053(config)#interface Gig0/0
13522053(config-if)#no ip access-group 1 in
13522053(config-if)#ip access-list extended 100
13522053(config-ext-nacl)#20 deny tcp host 192.168.1.1 host 192.168.2.1 eq 80
13522053(config-ext-nacl)#30 permit ip any any
13522053(config-ext-nacl)#exit
13522053(config)#interface Gig0/1
13522053(config-if)#ip access-group 100 out
13522053(config-if)#exit
13522053(config)#exit
13522053#
%SYS-5-CONFIG_I: Configured from console by console

13522053#show access-lists 100|
Extended IP access list 100
    deny tcp host 192.168.1.1 host 192.168.2.1 eq www
    permit ip any any (8 match(es))

```



Ping berhasil, karena ACL saat ini hanya memblokir akses ke port 80 (HTTP), sedangkan ICMP tidak termasuk dalam aturan ACL.



Akses gagal, karena ada aturan dalam ACL yang memblokir akses TCP dari PC0 ke port 80 Server0.

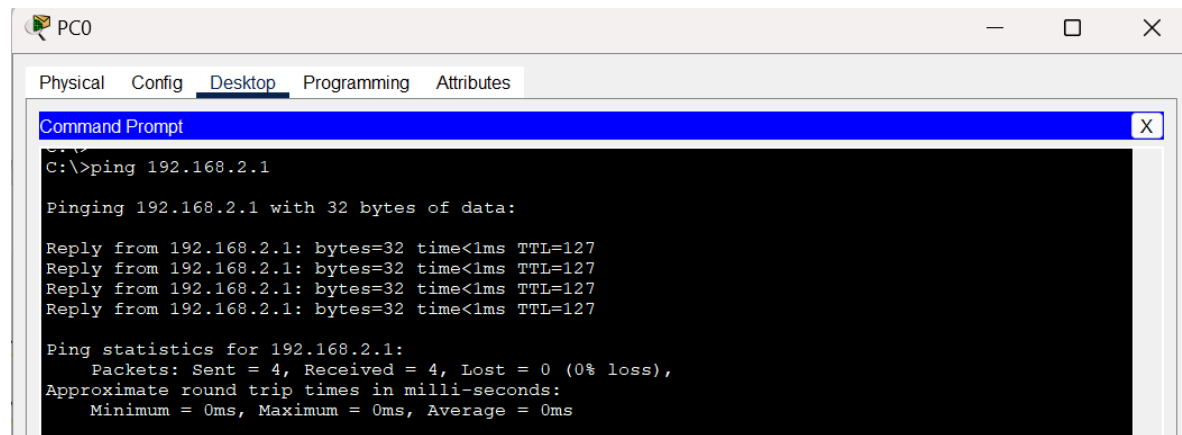
Sesudah menambah aturan kedua

```

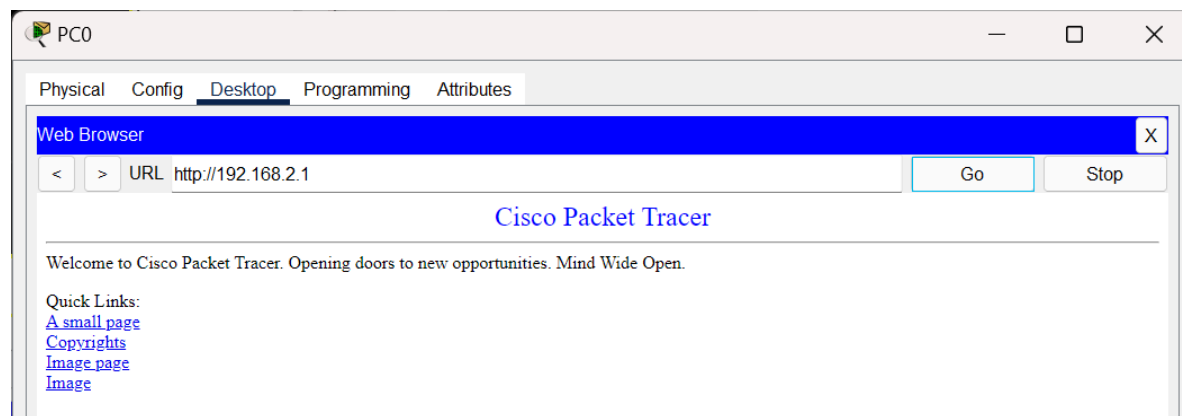
13522053#config t
Enter configuration commands, one per line. End with CNTL/Z.
13522053(config)#ip access-list extended 100
13522053(config-ext-nacl)#10 permit tcp host 192.168.1.1 host 192.168.2.1 eq 80
13522053(config-ext-nacl)#exit
13522053(config)#exit
13522053#
%SYS-5-CONFIG_I: Configured from console by console

13522053#show access-lists 100
Extended IP access list 100
    permit tcp host 192.168.1.1 host 192.168.2.1 eq www
    deny tcp host 192.168.1.1 host 192.168.2.1 eq www (28 match(es))
    permit ip any any (8 match(es))

```



Ping tetap berhasil, karena ping (ICMP) tidak dibatasi oleh ACL.



Akses web berhasil, karena aturan baru yang mengizinkan akses ke port 80 berada di urutan lebih tinggi dibanding aturan yang menolaknya.

Selain itu, daftar kontrol akses IPv6 juga dapat ditambahkan dengan cara yang serupa dengan memasukkan 'ipv6' sebagai pengganti 'ip' dalam perintah dengan satu tipe ACL yang tersedia di IPv6 mirip dengan extended IP ACL pada IPv4 dan hanya menggunakan nama string sebagai pengenal.

```
RouterA(config)# ipv6 access-group {name}
```

Apa itu IPv6? Pertanyaan bagus, silakan lanjut ke bagian berikutnya.

IV.5. IPv6

Internet Protocol versi 6 (IPv6) adalah versi baru dari pengalamatan IP (dan saat ini merupakan yang terbaru). Ini memperluas bit alamat dari 32 bit menjadi 128 bit, yang menyediakan jauh lebih banyak alamat dibandingkan pendahulunya (IPv4), lebih dari cukup untuk memberikan alamat unik bagi setiap perangkat yang terhubung ke jaringan yang ada. IPv6 bekerja dengan cara yang mirip dengan IPv4, dengan kemampuan yang lebih luas.

Address Format

Alamat IPv6 direpresentasikan sebagai serangkaian bidang heksadesimal 16-bit yang dipisahkan oleh titik dua (:) dalam format: **x:x:x:x:x:x:x**. Karena ruang alamat yang besar dan urutan yang panjang, alamat IPv6 dapat dipadatkan dengan mengompresi bidang heksadesimal nol yang berurutan (bagian 16-bit yang hanya berisi 0) menggunakan double colon (::). Kompresi dapat dilakukan di awal, tengah, atau akhir alamat. Misalnya, alamat loopback **0:0:0:0:0:0:1** dapat dipadatkan menjadi **::1**, atau alamat yang tidak ditentukan **0:0:0:0:0:0:0:0** dapat dipadatkan menjadi **::**. **Perlu dicatat bahwa Anda tidak dapat menggunakan double colon lebih dari sekali dalam satu alamat IPv6 (mengapa?).**

Mirip dengan subnet IPv4, IPv6 menggunakan prefix untuk merepresentasikan blok-blok yang berurutan secara bit dari seluruh ruang alamat. Karena prefix dapat menjadi cukup panjang dan oleh karena itu sulit untuk diekspresikan seperti subnet mask di IPv4, **IPv6 menggunakan format ipv6-prefix/prefix-length**. Di mana panjang prefix menentukan berapa banyak bit yang berurutan dari tinggi yang merupakan prefix (bagian jaringan dari alamat, sama seperti notasi CIDR di IPv4).

Tugas 6

Q Download file [IPv6-start.pkt](#) yang telah kami siapkan. Mulailah dengan menetapkan alamat IPv6 ke setiap perangkat seperti yang tercatat dalam file packet tracer.

Penetapan alamat IPv6 pada PC dan Server dapat dilakukan melalui aplikasi alamat IP, menggunakan kolom IPv6 di bawah kolom IPv4. Pastikan untuk mengisi gateway default dan server DNS dengan benar (gunakan server “DNS Server” sebagai server DNS untuk semua perangkat).

Untuk mengkonfigurasi alamat IPv6 pada router, konfigurasi di mode antarmuka dengan cara yang mirip dengan mengkonfigurasi alamat IPv4 di modul sebelumnya:

```
Router(config)#interface {interface_id}
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address {ipv6_address}/{prefix_length}
```

```
Router(config-if)#no shutdown
```

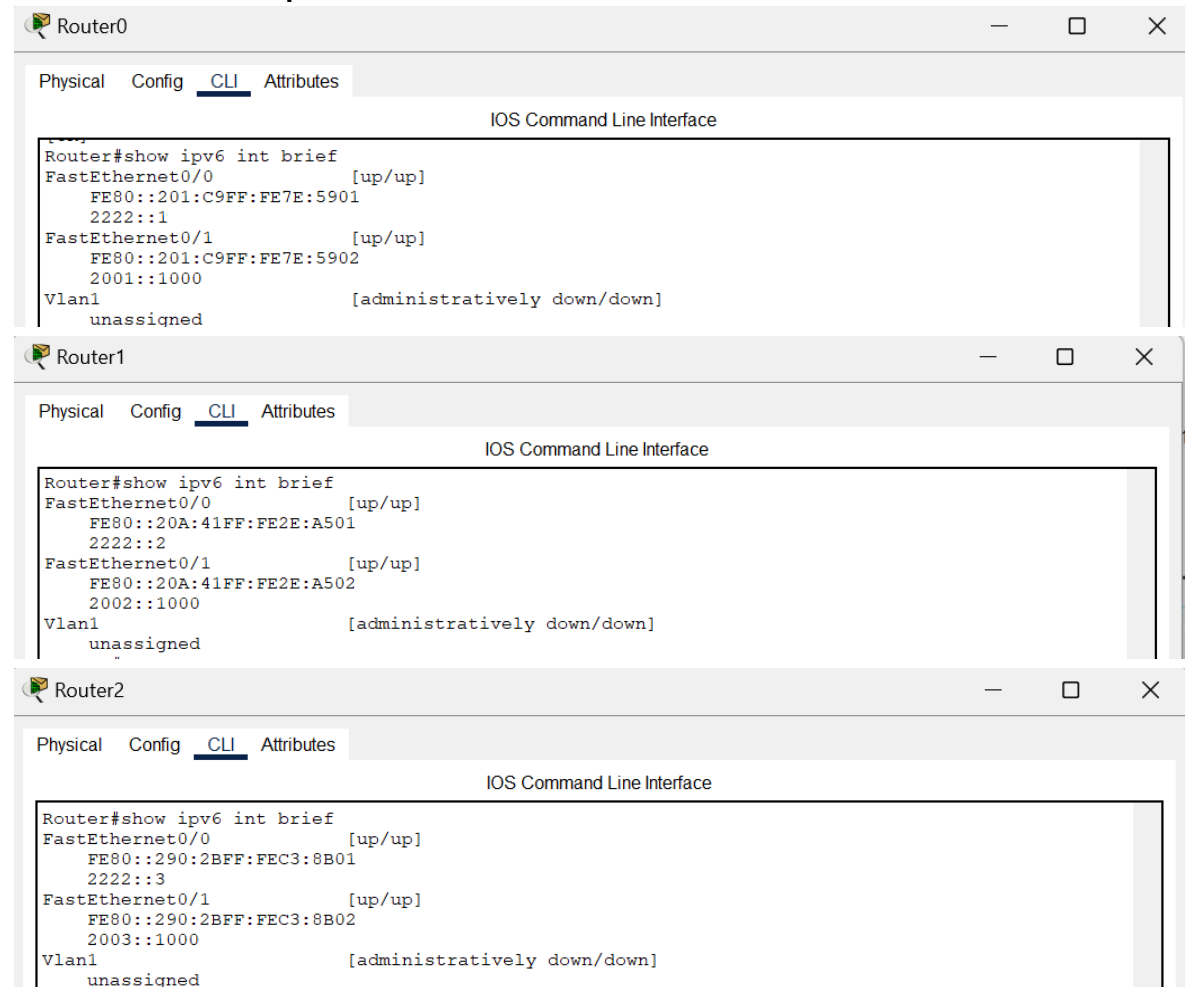
Hint: untuk menampilkan alamat IPv6 di antarmuka, gunakan:

```
show ipv6 int brief
```

Simpan kemajuan Anda saat ini ke file baru, untuk memudahkan pengaturan ulang konfigurasi routing untuk tugas berikutnya (jangan lupa untuk menyimpan konfigurasi yang sedang berjalan dari router ke konfigurasi awal!)

Cobalah untuk melakukan ping ke router yang berdekatan dari setiap PC (router yang terhubung langsung ke PC), dan lakukan ping ke setiap router lainnya dari Router0, dan tampilkan hasilnya!

A Alamat IPv6 di setiap router

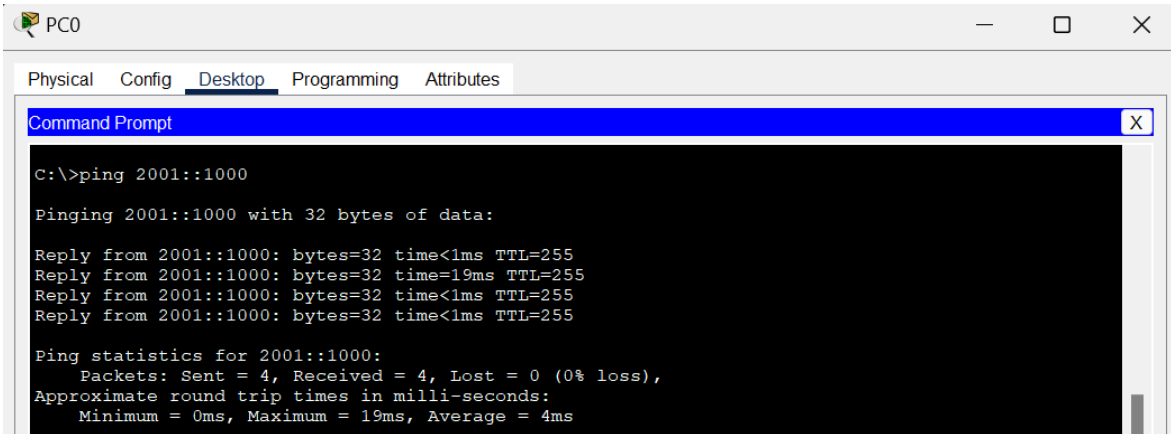


```
Router0
Router#show ipv6 int brief
FastEthernet0/0      [up/up]
  FE80::201:C9FF:FE7E:5901
  2222::1
FastEthernet0/1      [up/up]
  FE80::201:C9FF:FE7E:5902
  2001::1000
Vlan1                 [administratively down/down]
  unassigned

Router1
Router#show ipv6 int brief
FastEthernet0/0      [up/up]
  FE80::20A:41FF:FE2E:A501
  2222::2
FastEthernet0/1      [up/up]
  FE80::20A:41FF:FE2E:A502
  2002::1000
Vlan1                 [administratively down/down]
  unassigned

Router2
Router#show ipv6 int brief
FastEthernet0/0      [up/up]
  FE80::290:2BFF:FEC3:8B01
  2222::3
FastEthernet0/1      [up/up]
  FE80::290:2BFF:FEC3:8B02
  2003::1000
Vlan1                 [administratively down/down]
  unassigned
```

Ping dari PC0 ke Router0



PC0

Physical Config Desktop Programming Attributes

Command Prompt

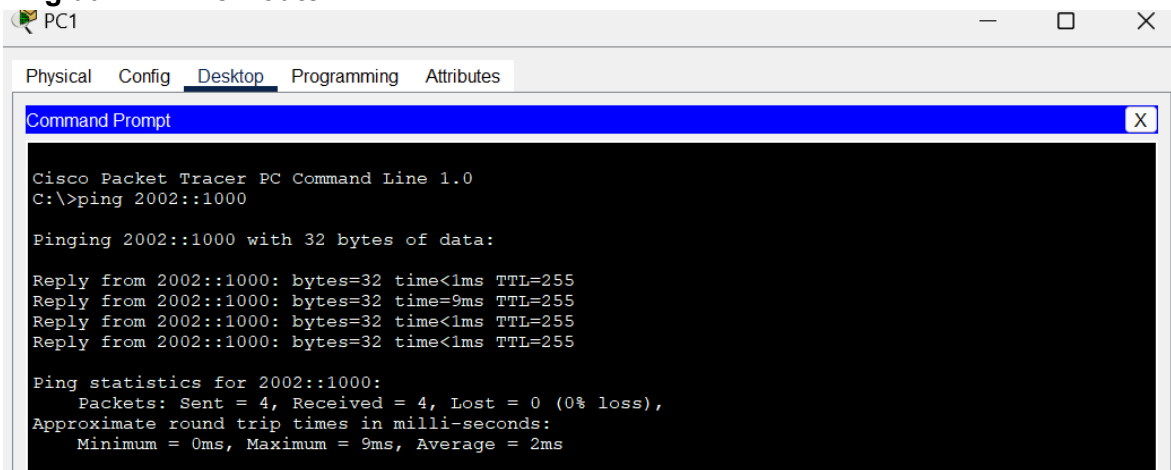
```
C:\>ping 2001::1000

Pinging 2001::1000 with 32 bytes of data:

Reply from 2001::1000: bytes=32 time<1ms TTL=255
Reply from 2001::1000: bytes=32 time=19ms TTL=255
Reply from 2001::1000: bytes=32 time<1ms TTL=255
Reply from 2001::1000: bytes=32 time<1ms TTL=255

Ping statistics for 2001::1000:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

Ping dari PC1 ke Router1



PC1

Physical Config Desktop Programming Attributes

Command Prompt

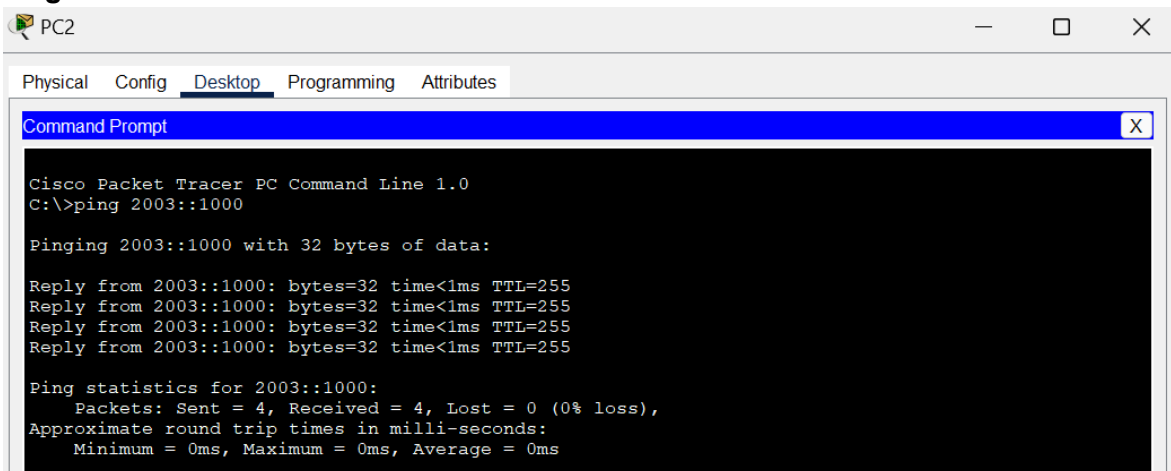
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2002::1000

Pinging 2002::1000 with 32 bytes of data:

Reply from 2002::1000: bytes=32 time<1ms TTL=255
Reply from 2002::1000: bytes=32 time=9ms TTL=255
Reply from 2002::1000: bytes=32 time<1ms TTL=255
Reply from 2002::1000: bytes=32 time<1ms TTL=255

Ping statistics for 2002::1000:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 2ms
```

Ping dari PC2 ke Router2



PC2

Physical Config Desktop Programming Attributes

Command Prompt

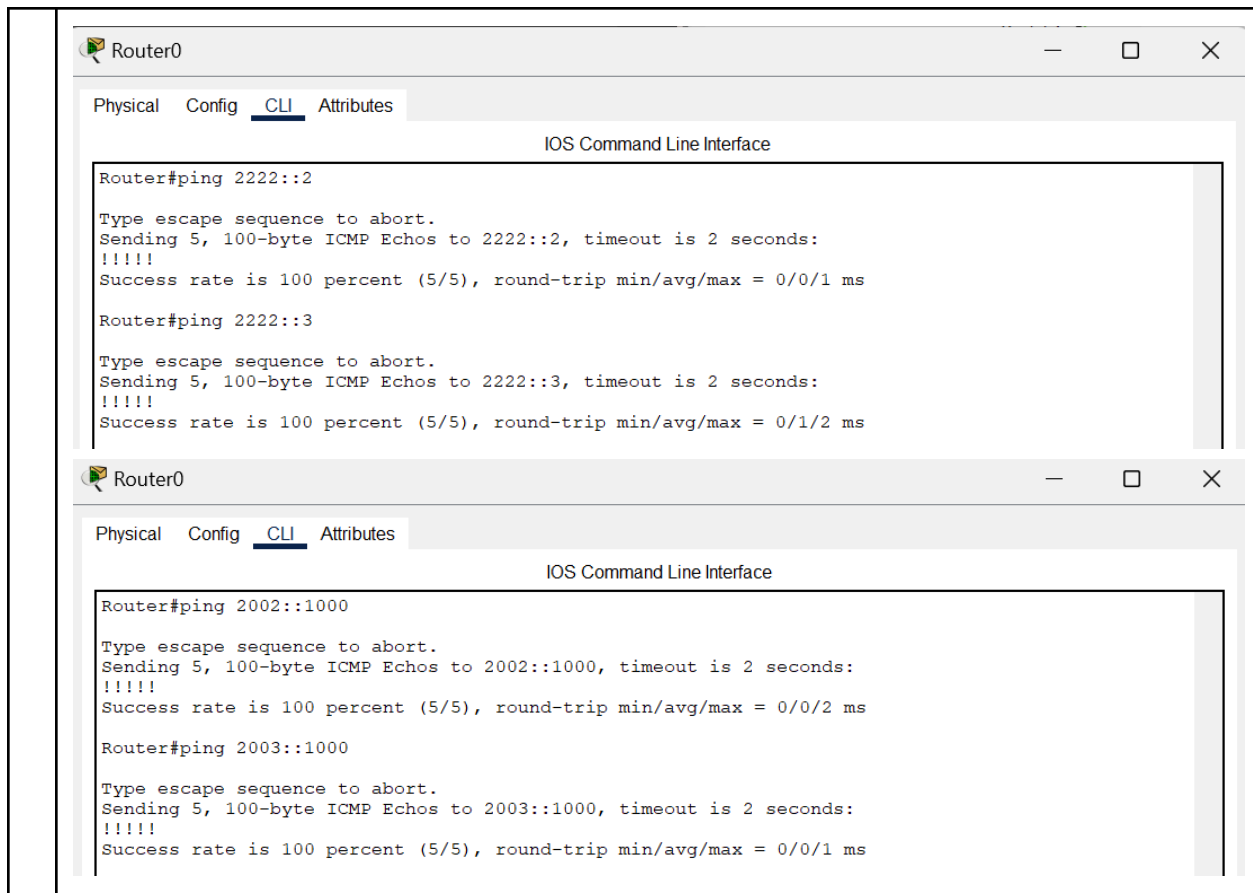
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2003::1000

Pinging 2003::1000 with 32 bytes of data:

Reply from 2003::1000: bytes=32 time<1ms TTL=255
Reply from 2003::1000: bytes=32 time<1ms TTL=255
Reply from 2003::1000: bytes=32 time<1ms TTL=255
Reply from 2003::1000: bytes=32 time<1ms TTL=255

Ping statistics for 2003::1000:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping dari Router0 ke Router1 (2222::2 dan 2002::1000) dan Router2 (2222::3 dan 2003::1000)



Addressing and Routing

Unicast IPv6 routing dilakukan dengan cara yang sama seperti routing IPv4. Kita telah membahas beberapa dynamic routing protocols dalam aktivitas laboratorium sebelumnya, dan kita hanya akan menggunakan RIP untuk dynamic routing dalam tugas ini.

Tugas 7

Q Melanjutkan dari [Tugas 6](#), kita akan mengkonfigurasi routing statik IPv6 di jaringan.

Untuk memulai, kita perlu mengaktifkan routing unicast di router.

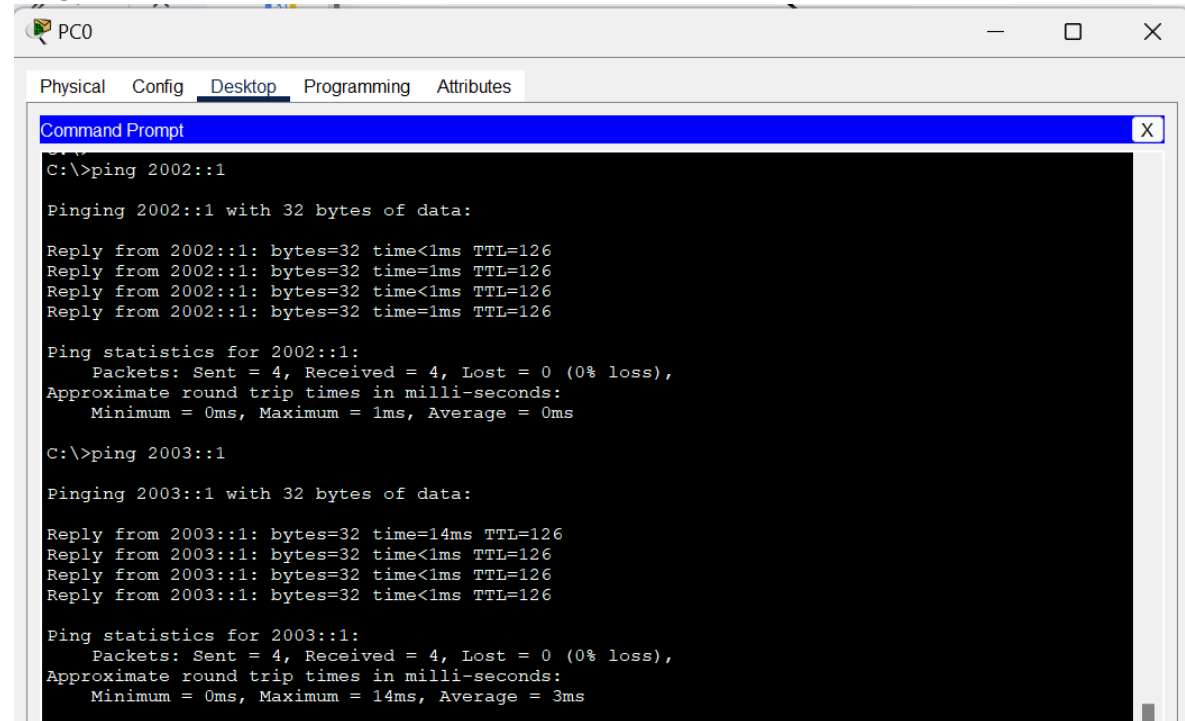
```
Router(config)#ipv6 unicast-routing
```

Kemudian, daftar routing statis dengan cara yang sama seperti routing statik IPv4 menggunakan

```
ipv6 route {destination_network} {next_hop}
```

Setelah mengkonfigurasi routing di ketiga router, coba ping semua PC dari PC0, dan coba akses itb.ac.id dari PC1 (rekaman DNS telah dikonfigurasi sebelumnya untuk Anda gunakan). Tunjukkan hasilnya!

A Ping semua PC dari PC0



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2002::1

Pinging 2002::1 with 32 bytes of data:

Reply from 2002::1: bytes=32 time<1ms TTL=126
Reply from 2002::1: bytes=32 time=1ms TTL=126
Reply from 2002::1: bytes=32 time<1ms TTL=126
Reply from 2002::1: bytes=32 time=1ms TTL=126

Ping statistics for 2002::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

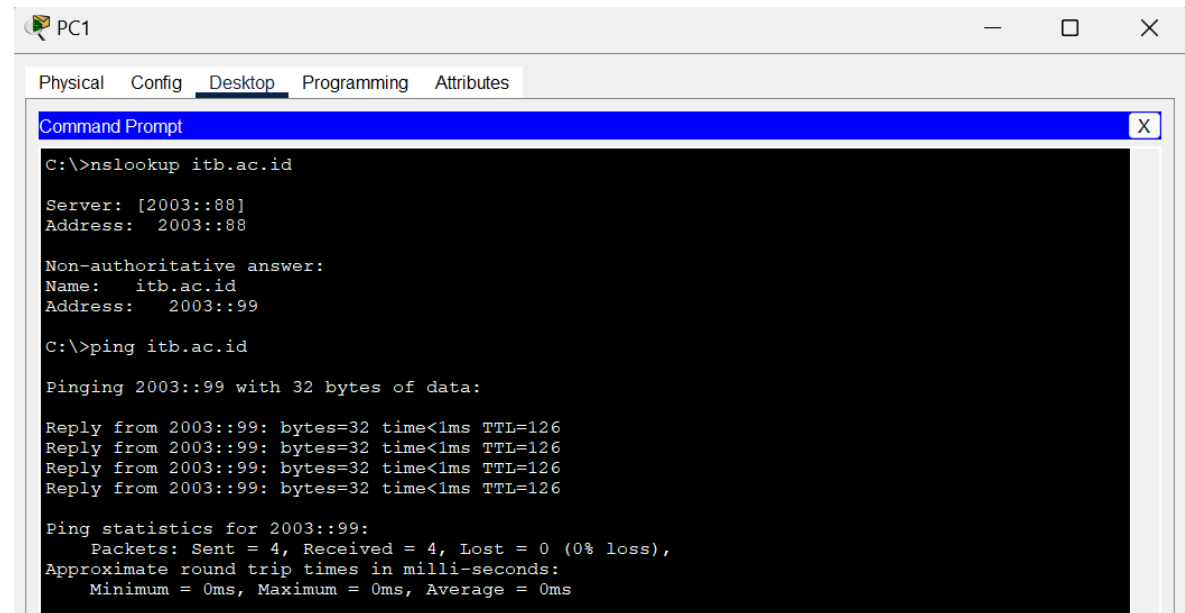
C:\>ping 2003::1

Pinging 2003::1 with 32 bytes of data:

Reply from 2003::1: bytes=32 time=14ms TTL=126
Reply from 2003::1: bytes=32 time<1ms TTL=126
Reply from 2003::1: bytes=32 time<1ms TTL=126
Reply from 2003::1: bytes=32 time<1ms TTL=126

Ping statistics for 2003::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms
```

Akses itb.ac.id dari PC1



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>nslookup itb.ac.id

Server: [2003::88]
Address: 2003::88

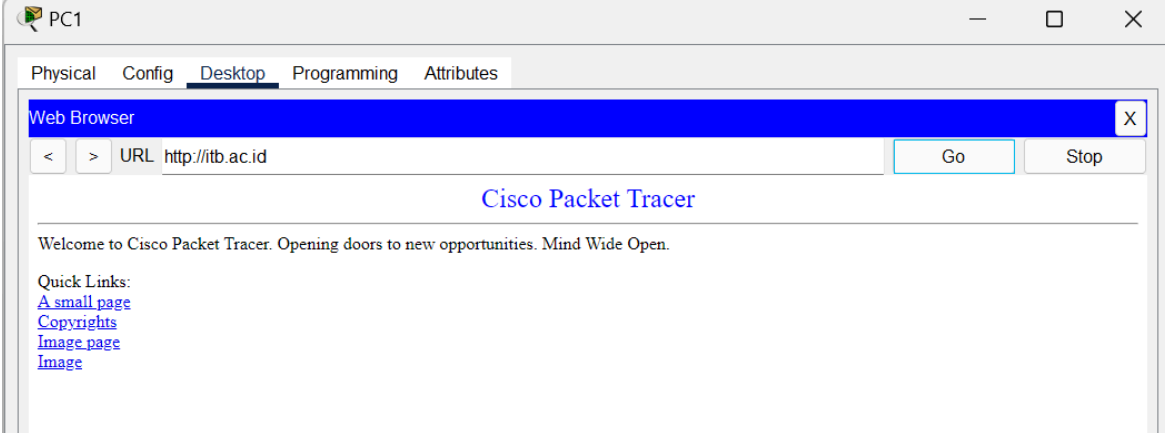
Non-authoritative answer:
Name: itb.ac.id
Address: 2003::99

C:\>ping itb.ac.id

Pinging 2003::99 with 32 bytes of data:

Reply from 2003::99: bytes=32 time<1ms TTL=126
Reply from 2003::99: bytes=32 time<1ms TTL=126
Reply from 2003::99: bytes=32 time<1ms TTL=126
Reply from 2003::99: bytes=32 time<1ms TTL=126

Ping statistics for 2003::99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


	 <p>The screenshot shows a PC1 window with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a 'Web Browser' window. The browser's address bar shows 'http://itb.ac.id' with 'Go' and 'Stop' buttons. The page content includes the title 'Cisco Packet Tracer', a welcome message, and quick links to 'A small page', 'Copyrights', 'Image page', and 'Image'.</p>
Q	<p>Setelah mencoba routing statik IPv6, sekarang saatnya mencoba routing dinamis. Sebelum melanjutkan, bersihkan semua konfigurasi routing statis (Anda dapat menggunakan “Power Cycle Devices” (restart semua perangkat) dengan alt+s) atau restart Packet Tracer tanpa menyimpan jika Anda secara tidak sengaja menyalin konfigurasi berjalan ke konfigurasi awal).</p> <p>Mulailah dengan menginisialisasi protokol RIP menggunakan</p> <pre>ipv6 router rip {rip_name}</pre> <p>Konfigurasikan setiap antarmuka router untuk mengaktifkan routing RIP dengan perintah</p> <pre>ipv6 rip {rip_name} enable</pre> <p>..dan itu saja! Konfigurasikan semua antarmuka router yang menghubungkan setiap jaringan dengan langkah-langkah konfigurasi yang sama untuk menyelesaikan proses ini.</p> <p><i>Hint:</i> untuk menampilkan tabel routing IPv6, gunakan</p> <pre>show ipv6 route</pre> <p>Setelah mengkonfigurasi routing di ketiga router, coba lakukan ping ke semua PC dari PC0, dan coba akses itb.ac.id dari PC1 (record DNS telah dipra-konfigurasi untuk Anda gunakan). Tampilkan hasilnya!</p>
A	<p>Konfigurasi routing di Router0</p>

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router rip RIPng1
Router(config-rtr)#exit
Router(config)#interface fa0/0
Router(config-if)#ipv6 rip RIPng1 enable
Router(config-if)#exit
Router(config)#interface fa0/1
Router(config-if)#ipv6 rip RIPng1 enable
Router(config-if)#exit
Router(config)#exit
Router#

Router#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C 2001::/64 [0/0]
   via FastEthernet0/1, directly connected
L 2001::1000/128 [0/0]
   via FastEthernet0/1, receive
R 2002::/64 [120/2]
   via FE80::20A:41FF:FE2E:A501, FastEthernet0/0
R 2003::/64 [120/2]
   via FE80::290:2BFF:FEC3:8B01, FastEthernet0/0
C 2222::/64 [0/0]
   via FastEthernet0/0, directly connected
L 2222::1/128 [0/0]
   via FastEthernet0/0, receive
L FF00::/8 [0/0]
   via Null0, receive
```

Konfigurasi routing di Router1

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router rip RIPng1
Router(config-rtr)#exit
Router(config)#interface fa0/0
Router(config-if)#ipv6 rip RIPng1 enable
Router(config-if)#exit
Router(config)#interface fa0/1
Router(config-if)#ipv6 rip RIPng1 enable
Router(config-if)#exit
Router(config)#exit
```

```

Router#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R  2001::/64 [120/2]
   via FE80::201:C9FF:FE7E:5901, FastEthernet0/0
C  2002::/64 [0/0]
   via FastEthernet0/1, directly connected
L  2002::1000/128 [0/0]
   via FastEthernet0/1, receive
R  2003::/64 [120/2]
   via FE80::290:2BFF:FEC3:8B01, FastEthernet0/0
C  2222::/64 [0/0]
   via FastEthernet0/0, directly connected
L  2222::2/128 [0/0]
   via FastEthernet0/0, receive
L  FF00::/8 [0/0]
   via Null0, receive

```

Konfigurasi routing di Router2

Router2

Physical Config CLI Attributes

IOS Command Line Interface

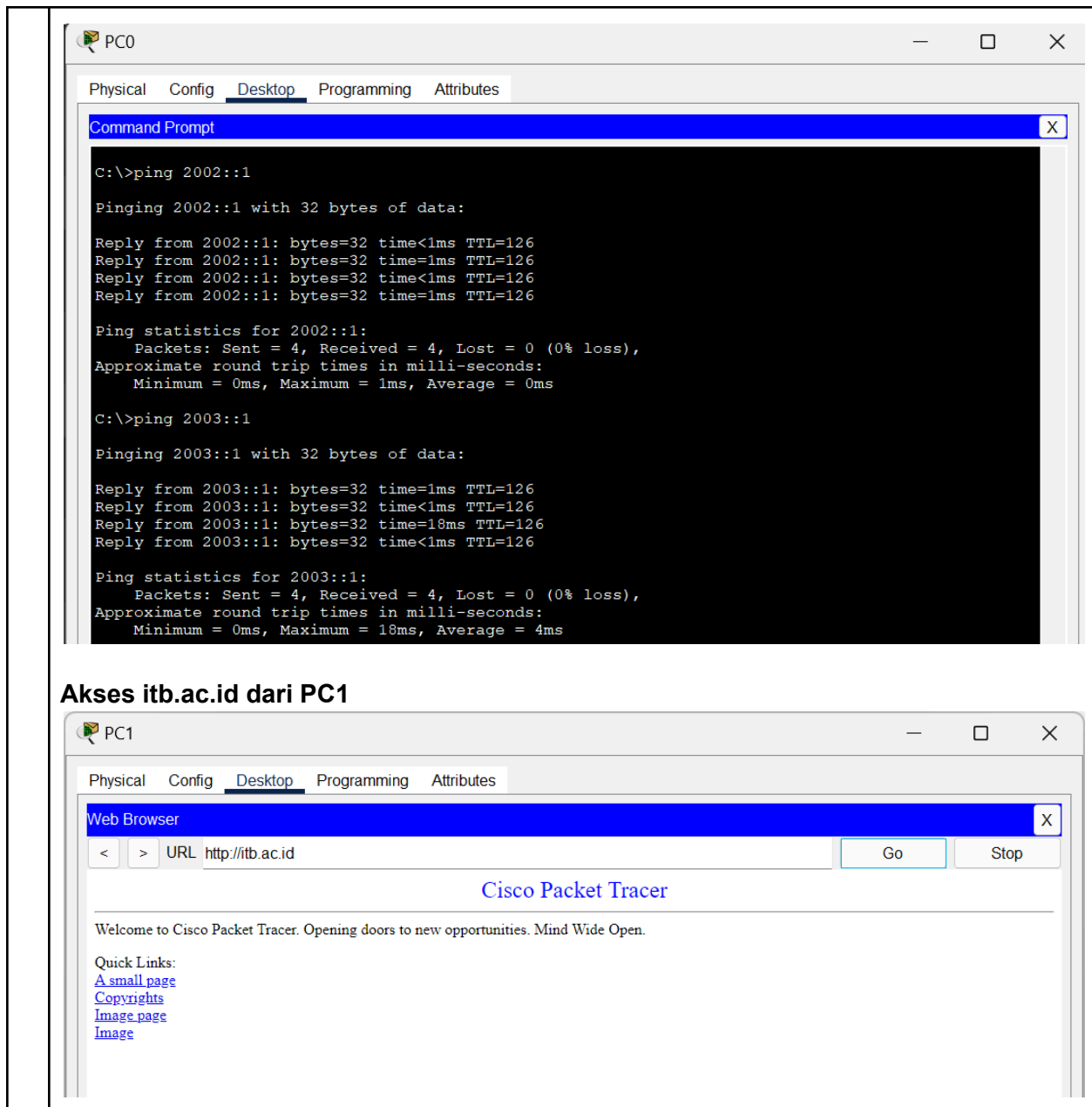
```

Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router rip RIPng1
Router(config-rtr)#exit
Router(config)#interface fa0/0
Router(config-if)#ipv6 rip RIPng1 enable
Router(config-if)#exit
Router(config)#interface fa0/1
Router(config-if)#ipv6 rip RIPng1 enable
Router(config-if)#exit
Router(config)#exit

Router#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R  2001::/64 [120/2]
   via FE80::201:C9FF:FE7E:5901, FastEthernet0/0
R  2002::/64 [120/2]
   via FE80::20A:41FF:FE2E:A501, FastEthernet0/0
C  2003::/64 [0/0]
   via FastEthernet0/1, directly connected
L  2003::1000/128 [0/0]
   via FastEthernet0/1, receive
C  2222::/64 [0/0]
   via FastEthernet0/0, directly connected
L  2222::3/128 [0/0]
   via FastEthernet0/0, receive
L  FF00::/8 [0/0]
   via Null0, receive

```

Ping dari PC0 ke PC1 (2002::1) dan PC2 (2003::1)

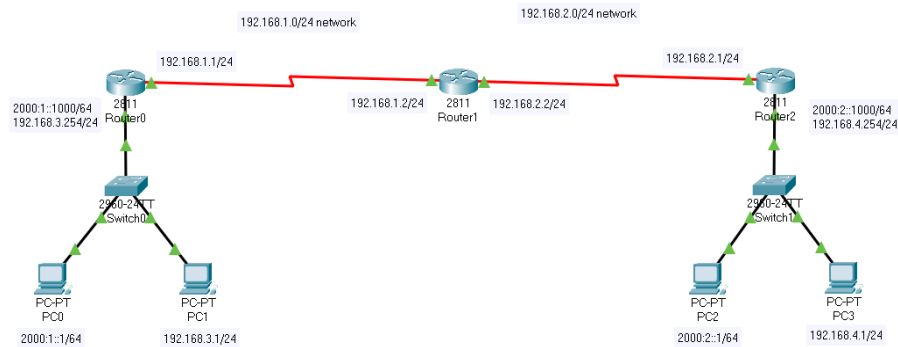


IV.1. IPv6 Tunneling over IPv4

Implementasi IPv6 memerlukan kerja keras untuk diterapkan pada infrastruktur jaringan saat ini, dan kedua skema pengalamatan tidak kompatibel satu sama lain. Jadi, implementasi IPv6 hanya dapat dilakukan dengan rolling deployment. Untuk menjaga agar jaringan tetap berjalan di IPv4 dan tetap terhubung dengan jaringan yang sudah berjalan di IPv6, kita perlu cara untuk menjembatani kedua skema pengalamatan dan routing-nya. Solusi yang banyak digunakan adalah IPv6 tunneling over IPv4.

Tugas 8

Q Download file [IPv6-tunnel-start.pkt](#) yang telah kami siapkan.



Dalam file tersebut, terdapat infrastruktur jaringan IPv4 yang sudah berjalan, dengan PC (PC0 & PC2) yang menggunakan IPv6 ditambahkan di setiap jaringan akhir. Semua perangkat telah dikonfigurasi dengan benar, tetapi router hanya dikonfigurasi untuk jaringan IPv4. Sebelum melanjutkan, pastikan jaringan berfungsi dengan baik dengan ping dari PC1 ke PC3.

Sekarang, kita ingin menghubungkan PC0 ke PC2 dengan infrastruktur jaringan yang sudah ada tanpa merusak jaringan untuk PC1 & PC3. Untuk melakukan ini, kita perlu mengkonfigurasi IPv6 & tunneling IPv6 melalui IPv4 di router.

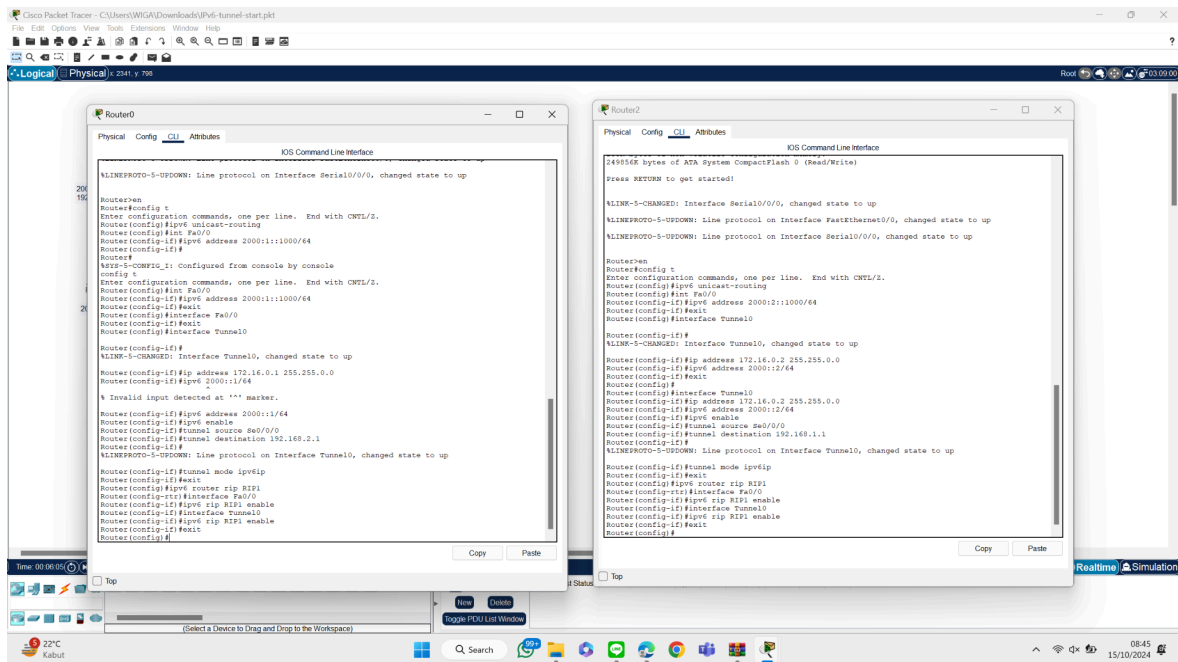
Untuk memulai, kita perlu mengaktifkan IPv6 & routing unicast di Router0 & Router3

```
Router(config)#ipv6 unicast-routing
Router(config)#int {interface_id}
Router(config-if)#ipv6 address {IPv6_address}
Router(config-if)#ipv6 enable
Router(config-if)#exit
```

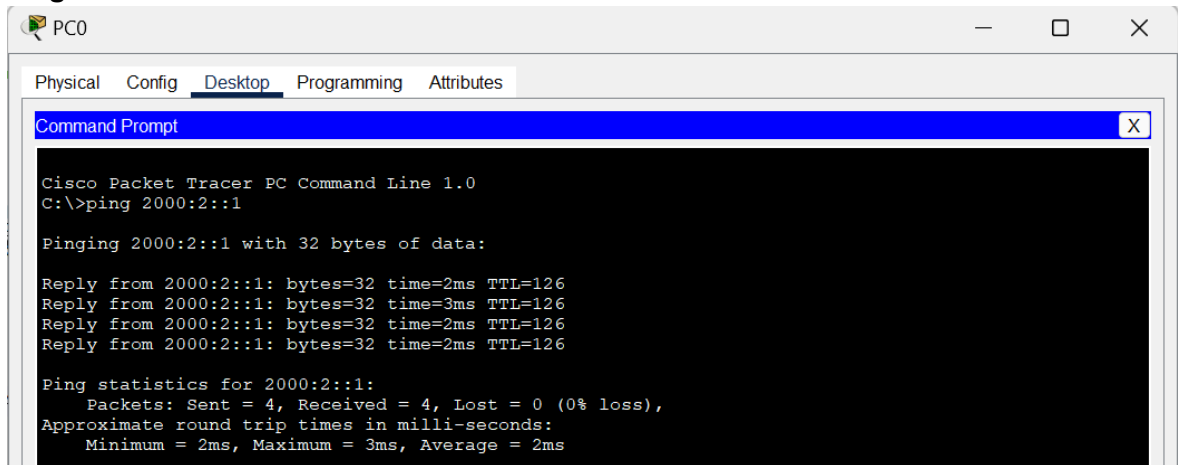
Setelah mengkonfigurasi alamat IPv6, kita perlu mengkonfigurasi antarmuka tunnel dan jaringannya. Mulailah dengan mengkonfigurasi antarmuka tunnel

```
Router(config)#interface Tunnel0
Router(config-if)#ip address {tunnel_address}{subnet_mask}
Router(config-if)#ipv6 address {tunnel_ipv6_address}
Router(config-if)#ipv6 enable
Router(config-if)#tunnel source Serial0/0/0
Router(config-if)#tunnel destination {target_router_address}
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#exit
```

	<p>Anda dapat menggunakan konfigurasi berikut, atau menggunakan nilai apa pun yang ingin Anda coba:</p> <ul style="list-style-type: none"> • Gunakan 172.16.0.0/16 sebagai jaringan antarmuka tunnel (misalnya dengan alamat 172.16.0.1/16 untuk Router0 & 172.16.0.2/16 untuk Router2). • Gunakan 2000::/64 sebagai prefix dari antarmuka tunnel (misalnya dengan alamat 2000::1/64 untuk Router0 & 2000::2/64 untuk Router2). <p>Sekarang bahwa antarmuka tunnel telah disetel di kedua perangkat, bagaimana dengan routing?</p> <p>Paket IPv4 (yang membungkus paket IPv6) sudah langsung diteruskan oleh alamat "tunnel source" dengan tujuan ke alamat "tunnel destination", yang telah dirutekan di atas routing IPv4 yang telah diatur sebelumnya. Dengan memeriksa field protokol dalam header IP (di mana 41 menandakan protokol enkapsulasi IPv6), paket kemudian akan dikirim ke antarmuka tunnel.</p> <p>Bagaimana dengan routing IPv6? Sekarang kita perlu mengkonfigurasi routing IPv6. Kita dapat menggunakan metode routing IPv6 apa pun, tetapi kita akan menggunakan RIP untuk tugas ini.</p> <p>Pertama, aktifkan protokol IPv6 RIP dengan</p> <pre>ipv6 router rip {rip_name}</pre> <p>Kemudian konfigurasikan setiap antarmuka (yaitu antarmuka Router yang terhubung ke PC, dan antarmuka tunnel) untuk berpartisipasi dalam protokol RIP yang sama dengan</p> <pre>ipv6 rip {rip_name} enable</pre> <p>Setelah mengkonfigurasi tunneling di kedua router, tampilkan hasil ping dari PC0 ke PC2! Jelaskan proses enkapsulasi/dekapsulasi paket dan proses routing!</p>
A	Konfigurasi



Ping dari PC0 ke PC2



Proses enkapsulasi/dekapsulasi paket dan proses routing:

1. PC0 mengirim paket IPv6 ke PC2 (2000:2::1).
2. Router0 melakukan enkapsulasi paket IPv6 ke dalam paket IPv4. Alamat IPv4: 192.168.1.1 sebagai sumber dan 192.168.2.1 sebagai tujuan.
3. Paket IPv4 dikirim melalui jaringan IPv4 dari Router0 ke Router2.
4. Router2 melakukan dekapsulasi paket IPv4 dan mengekstrak paket IPv6.
5. Paket IPv6 diteruskan ke PC2 yang merespons ping.
6. Routing IPv4 digunakan untuk mengirim paket yang terenkapsulasi.
7. Routing IPv6 (RIPng) digunakan untuk meneruskan paket IPv6 setelah dekapsulasi.

Referensi

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

IPv6 Addressing and Basic Connectivity Configuration Guide, Cisco IOS Release 15M&T.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/15-mt/ipv6b-15-mt-book.html

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