

*"Connecting Knowledge"*  
Agus Setiawan

# CCNA

Cisco Certified Network Associate

**Lab Guide**

Exam 200-120 | 1st Edition



[www.nixtrain.com](http://www.nixtrain.com)

## Kata Pengantar

Segala puji dan syukur penulis panjatkan kepada Allah S.W.T yang telah melimpahkan karunia-Nya, serta atas pencerahan dan hidayah-Nya lah, penulis dapat menyelesaikan buku ini yang berjudul “CCNA Lab Guide: 1<sup>st</sup> Edition”.

Melalui buku ini, saya ingin mengucapkan terima kasih kepada guru-guru saya : Achmad Mardiansyah, Andry M. Hartawan, Dedi Gunawan, Danu Wiyoto, Fathur Ridho, Miftah Rahman, Wahyu M. Sun, Deny Julianti dan masih banyak yang lainnya.. dan juga teman-teman di group facebook Nixtrain, Road to CCNA, dan Komunitas Cisco Bandung atas dukungan dan motivasinya sehingga saya bisa menyelesaikan karya buku ini.

Latar belakang penulisan buku ini diawali untuk membantu penulis dalam menyampaikan materi lab di training center Nixtrain. Penulis mengucapkan terima kasih atas saran dan masukkannya kepada team Nixtrain : Toni, Rama, Sufyan. You are my best team.. (y)

Untuk menggunakan buku ini cukup memakai Packet Tracer atau GNS3 sebagai tool nge-labnya.. didesain dengan ulasan yang sistematis dan terdapat pesan tersembunyi, sehingga mengharuskan pembaca teliti dalam mengikuti petunjuk dibuku ini.. pembaca akan diuji dengan pertanyaan review disetiap akhir lab.

Semoga buku ini membawa manfaat buat pembaca dalam mempelajari basic networking. Apabila terdapat kesalahan dalam penulisan atau ingin memberikan saran/feedback, silahkan kirimkan kepada penulis melalui email : agussetiawan@nixtrain.com

Jika ada kesulitan dalam mengerjakan lab-nya dan ingin mendapatkan support gratis, silahkan bergabung di group facebook Road to CCNA. Kami dengan senang hati akan membantu kesulitan pembaca.

Selamat belajar dan ikuti perkembangan terupdate tentang penulisan buku edisi selanjutnya di group facebook Road to CCNA.

Sebagai penutup kata pengantar ini, penulis menyadari masih terdapat banyak kekurangan disana-sini dalam penulisan buku ini. Oleh karena itu, penulis tetap mengharapkan kritik dan masukan bagi perbaikan buku ini.

Bandung, Januari 2015

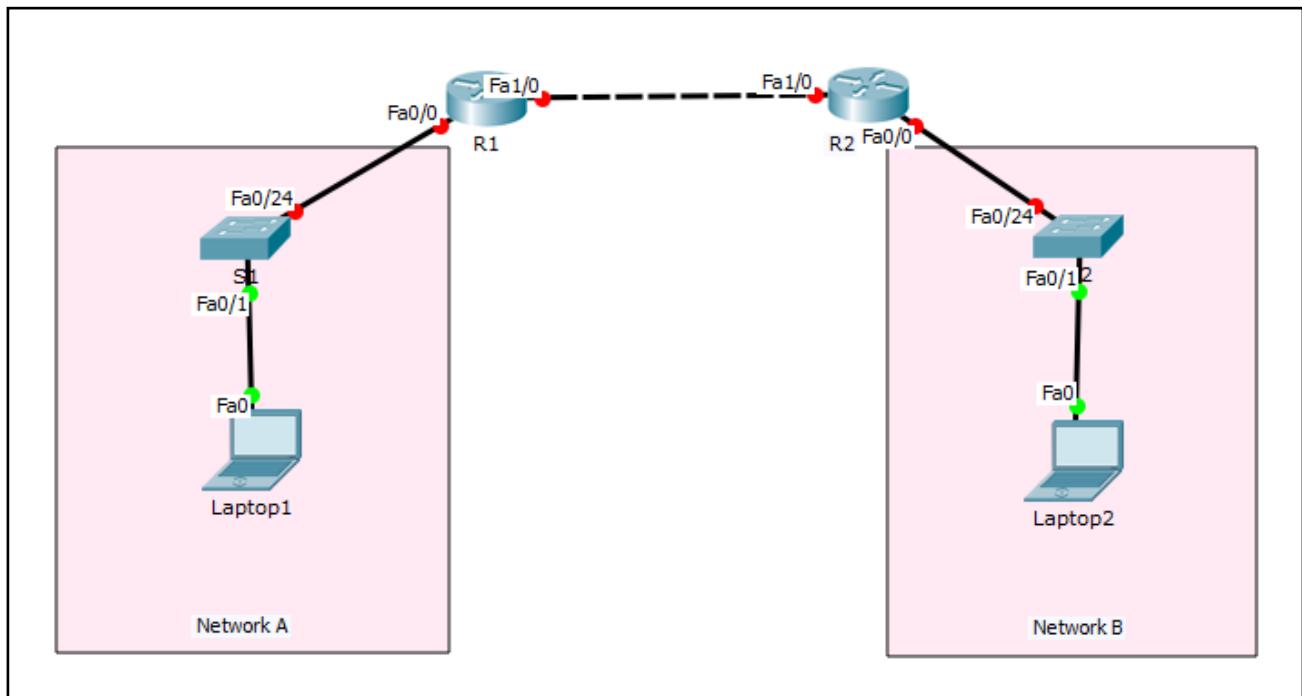
Penulis,  
Agus Setiawan

## Daftar Lab

Kategori	Lab	Nama Lab	Halaman
Basic Router	1	Basic Router Configuration	1
	2	Remote Access Telnet Router	5
	3	Managing Router Configuration	9
Routing	4	Static Routing	15
	5	Static Default Route	24
	6	RIPv2	32
	7	EIGRP	40
	8	OSPF	50
ACL	9	ACL Standar	65
	10	ACL Extended	72
NAT	11	NAT Static	80
	12	NAT Dynamic	87
	13	NAT Dynamic Overload (PAT)	93
	14	NAT Dynamic Overload (PAT with Exit-Interface)	99
Basic Switch	15	Basic Switch Configuration	104
Switching	16	VLAN	111
	17	VLAN Trunking	120
	18	InterVLAN Routing	126
	19	STP	132
HA	20	EtherChannel	139
	21	HSRP	146
IP Services	22	DHCP	150
WAN	23	PPP	153

# Lab 1. Basic Router Configuration

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting basic router

## Konsep Dasar

Router memiliki 6 mode :

### 1. Setup mode

- ✓ Router masuk setup mode jika NVRAM kosong alias tidak memiliki konfigurasi. Biasanya kondisi ini terjadi ketika kita mengaktifkan router baru atau setelah melakukan reset konfigurasi.

### 2. User mode

- ✓ Hanya terdapat beberapa command untuk monitoring
- ✓ Command show terbatas, ping dan traceroute
- ✓ Ditandai dengan : Router>

### 3. Privileged mode

- ✓ Terdapat beberapa command monitoring dan troubleshooting
- ✓ Terdapat semua command show, ping, trace, copy, erase
- ✓ Ditandai dengan : Router#

### 4. Global Configuration mode

- ✓ Untuk mensetting keseluruhan router misalnya hostname, konfigurasi routing
- ✓ Semua konfigurasi yang kita inputkan berlaku global di router
- ✓ Ditandai dengan : Router(config)#

### 5. Interface mode

- ✓ Untuk konfigurasi interface secara spesifik, misal Interface fa0/0, Interface Fa0/1

### 6. Rommon mode

- ✓ Untuk recovery password
- ✓ Jika lupa password console dan telnet, atau lupa password enable maka gunakan rommon mode untuk melakukan recovery password dengan mengubah nilai confreg

## Konektivitas Console

Untuk koneksi router menggunakan console, membutuhkan kabel console dan converter DB-9 to USB. Proses remote console dapat dilakukan dengan aplikasi putty atau hyperterminal untuk sistem operasi Windows. Sedangkan di Linux dapat menggunakan minicom -s.

## Konfigurasi

Untuk mensetting basic router R1 dan R2, gunakan akses console dari Laptop1 dan Laptop2. Setelah itu, ketikkan command basic router dibawah ini di R1 dan R2.

- a. Setelah login telnet ketikkan enable privileged EXEC mode.

```
Router> enable
Router#
```

- b. Masuk global configuration mode.

```
Router# config terminal
Router(config) #
```

- c. Memberikan nama device router.

```
Router(config) # hostname R1
```

- d. Disable DNS lookup untuk mencegah router melakukan translasi command yang salah ketik.

```
R1(config) # no ip domain-lookup
```

- e. Setting semua password dengan minimum karakter 6.

```
R1(config) # security passwords min-length 6
```

- f. Setting password privilege terenkripsi ciscosec

```
R1(config) # enable secret ciscosec
```

- g. Setting password console ciscocon. Aktifkan timeout command sehingga jika selama 5 menit 0 second tidak ada aktifitas maka akan logout sendiri.

```
R1(config) # line console 0
R1(config-line) # password ciscocon
```

```
R1(config-line)# exec-timeout 5 0  
R1(config-line)# login
```

- h. Setting password vty **ciscovty**. Aktifkan timeout command sehingga jika selama 5 menit 0 second tidak ada aktifitas maka akan logout sendiri.

```
R1(config)# line vty 0 4  
R1(config-line)# password ciscovty  
R1(config-line)# exec-timeout 5 0  
R1(config-line)# login
```

- i. Enable enkripsi clear text passwords.

```
R1(config)# service password-encryption
```

- j. Buat banner yang memberikan informasi kepada user yang tidak memiliki otorisasi dilarang login router.

```
R1(config)# banner motd #Unauthorized access prohibited!#
```

- k. Setting IP address dan interface description. Aktifkan interface router dengan sub-command no shutdown.

```
R1(config)# int fa1/0  
R1(config-if)# description Connection to R2  
R1(config-if)# ip address 12.12.12.1 255.255.255.0  
R1(config-if)# no shutdown  
R1(config-if)# exit  
R1(config)# exit  
R1#
```

- l. Setting clock di router; contoh seperti dibawah:

```
R1# clock set 10:00:00 3 Jan 2015
```

- m. Simpan konfigurasi file running-configuration ke startup-configuration.

```
R1# copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
R1#
```

Ketika kita mensetting router, maka konfigurasi akan disimpan sementara di file running-configuration (RAM), oleh karena itu proses menyimpan penting untuk dilakukan agar saat router reboot atau shutdown file konfigurasi router masih tetap disimpan di startup-configuration (NVRAM).

**Note: ulangi langkah yang sama diatas untuk mensetting basic router R2 dan setting IP interface router yang belum disetting di R1 maupun R2**

## **Verifikasi**

Setelah mensetting basic router R1 dan R2, langkah selanjutnya lakukan verifikasi bahwa konfigurasi yang kita inputkan sudah benar dengan command **show running-config** dan **show ip interface brief**.

Lakukan tes Ping :

- dari Laptop1 ke Fa0/0 R1
- dari Laptop2 ke Fa0/0 R2
- dari Fa1/0 R1 ke Fa1/0 R2

Pastikan tes Ping diatas berhasil semua. Gunakan CMD di Laptop untuk tes Ping, caranya klik **LaptopX** -> pilih tab **Desktop** -> pilih **Command Prompt** -> ketikkan **ping IP\_Tujuan** (Enter).

### Menampilkan informasi full konfigurasi router

```
R1# show running-config
Building configuration...

Current configuration : 1742 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 6
enable secret 4 3mxoP2KRPf3sFHY16Vm6.ssJJi9tOJqqb6DMG/YH5No
!
no aaa new-model
!
(skip)
```

- Gunakan tombol **Enter** untuk menampilkan per baris
- Gunakan tombol **Space** untuk menampilkan per screen
- Gunakan tombol **q** untuk exit dari tampilan konfigurasi router

Cek konfigurasi yang sudah diinputkan apakah ada yang salah atau tidak.

### Menampilkan informasi interface

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.1.254  YES manual up        up
FastEthernet1/0    12.12.12.1     YES manual up        up
```

Dari tampilan informasi interface, cek apakah IP yang sudah diconfig sudah sesuai tabel addressing atau belum.

### Tes konektivitas antar router R1 dan R2

Lakukan tes Ping dari R1 ke R2 dan sebaliknya. Ping pertama success rate masih 80%.

```
R1#ping 12.12.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/986/3944 ms
```

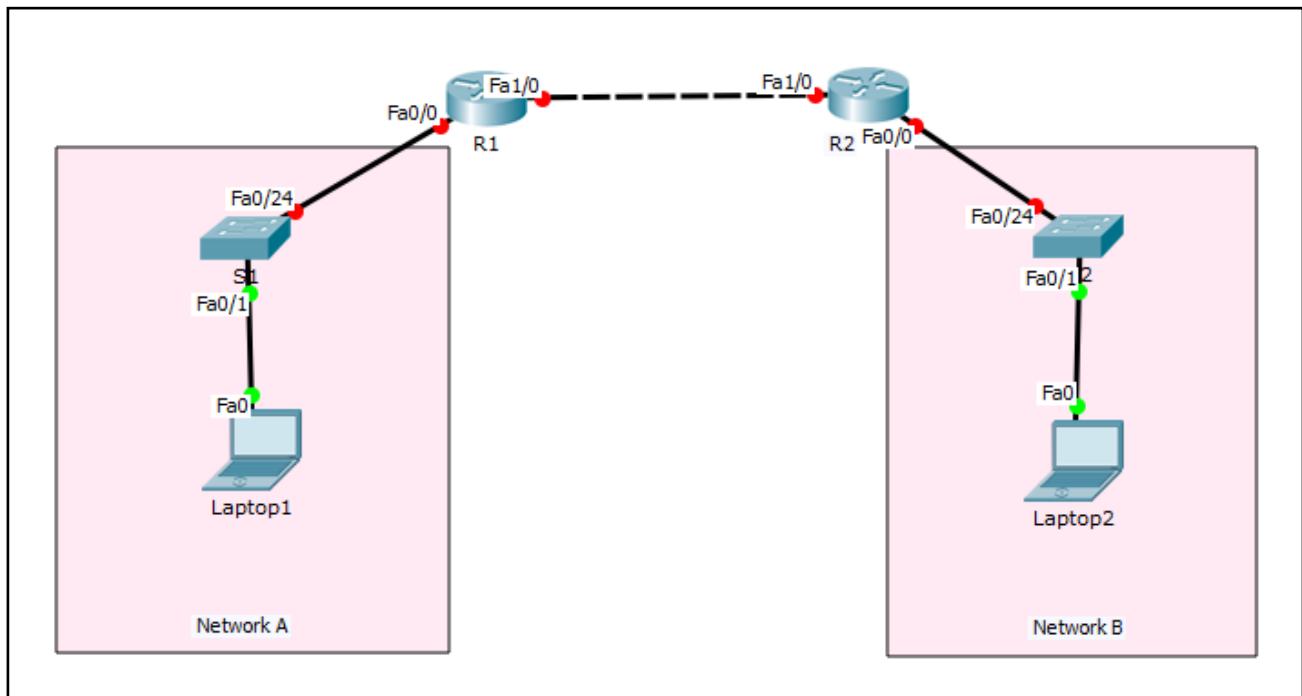
Ulangi tes Ping sampai success rate 100%.

### Review

1. Tes Ping dari Laptop1 ke Laptop2, apakah berhasil? Jika menjawab Ya/Tidak, jelaskan kenapa?

## Lab 2. Remote Access Telnet Router

### Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

### Tujuan

- Remote access R1 dan R2 menggunakan telnet dari Laptop1 dan Laptop2

### Konsep Dasar

Untuk mensetting router menggunakan command line dapat kita lakukan dengan tiga cara yaitu :

- **Console**

Koneksi membutuhkan kabel console dan tidak memerlukan settingan IP address pada sisi router maupun Laptop

- **Telnet**

Koneksi membutuhkan kabel UTP dan memerlukan settingan IP address pada sisi router maupun Laptop. Komunikasi telnet bersifat clear-text protocol, sehingga masih ada kekurangan dari sisi keamanan yaitu password dapat dengan mudah dilihat menggunakan packet sniffer.

- **SSH**

Koneksi membutuhkan kabel UTP dan memerlukan settingan IP address pada sisi router maupun Laptop. Komunikasi SSH bersifat encrypted protocol (enkripsi), sehingga lebih aman dibandingkan dengan telnet.

## **Konfigurasi**

Untuk mensetting telnet di router, berikut ini command yang diperlukan :

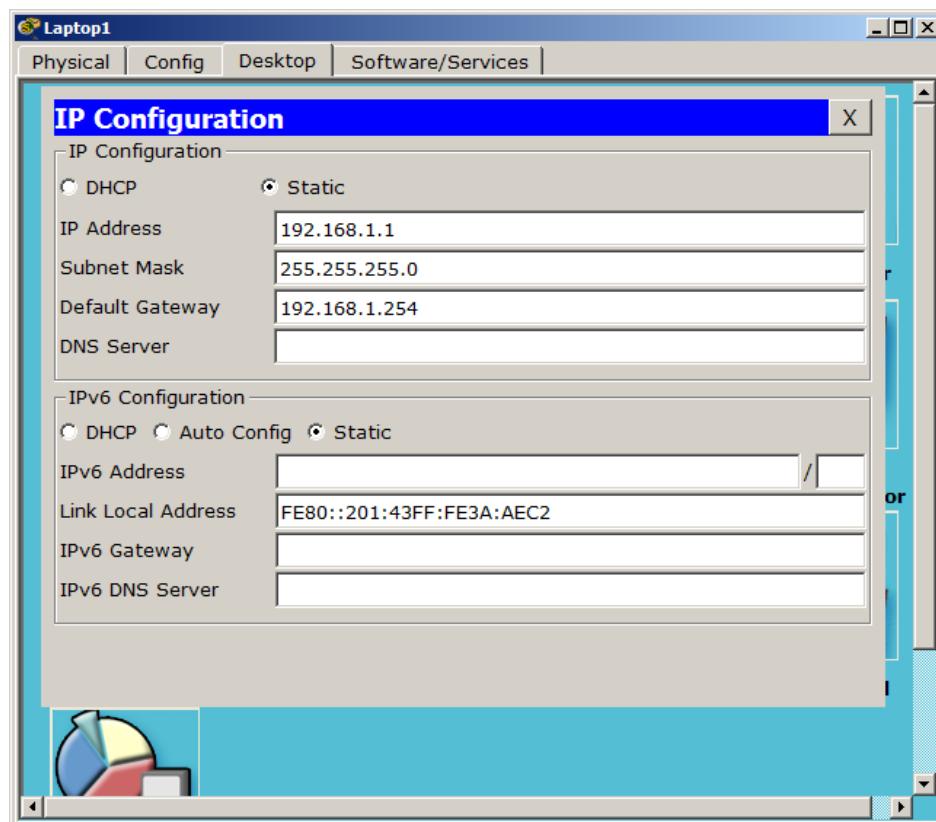
```
R1(config)#line vty 0 4
R1(config-line)#password <password>
R1(config-line)#login
```

Agar kita dapat melakukan akses telnet ke router, command `enable password` atau `enable secret` harus disetting terlebih dahulu.

Pada settingan gambar topologi diatas, R1 dan R2 diasumsikan sudah disetting akses telnet dengan password ciscovty dan enable secret ciscosec (*Lihat Lab 1-Basic Cisco Configuration*). Oleh karena itu, kita langsung dapat meremote telnet R1 dan R2. Akan tetapi, sebelum Laptop1 dan Laptop2 meremote router menggunakan telnet, Laptop1 dan Laptop2 harus disetting IP addressnya sesuai dengan tabel addressing diatas. Kemudian lakukan tes Ping dari Laptop1 ke R1 dan Laptop2 ke R2 dan pastikan berhasil tes konektivitasnya antara Laptop dan router.

### **Setting IP address Laptop1**

Klik **Laptop1** -> Pilih tab **Desktop** -> Klik **IP Configuration** -> Inputkan **IP address** sesuai tabel addressing diatas.



## **Verifikasi**

Setelah disetting IP address Laptop1, kemudian lakukan tes Ping dari Laptop1 ke interface Fa0/0 R1 menggunakan command prompt. Interface Fa0/0 R1 berfungsi sebagai gateway Laptop1.

### **Tampilkan konfigurasi Laptop1**

```
Laptop1>ipconfig
```

```
FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::201:43FF:FE3A:AEC2
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.254
```

Dan hasil tes Ping tampil reply seperti dibawah ini.

```
Laptop1>ping 192.168.1.254
```

```
Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=1ms TTL=255
Reply from 192.168.1.254: bytes=32 time=0ms TTL=255
Reply from 192.168.1.254: bytes=32 time=0ms TTL=255
Reply from 192.168.1.254: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

### **Telnet dari Laptop1 ke R1**

Setelah berhasil terhubung ke service telnet router, inputkan password telnet **ciscovty** dan ketikkan command **enable**, kemudian inputkan password **ciscosec**.

```
Laptop1>telnet 192.168.1.254
```

```
Trying 192.168.1.254 ...Open
```

```
Unauthorized access prohibited!
```

```
User Access Verification
```

```
Password:
```

```
R1>enable
```

```
Password:
```

```
R1#
```

Muncul login access dan banner yang isinya “**Unauthorized access prohibited!**”.

Akses telnet dari Laptop1 ke R1 sudah berhasil. Dengan telnet kita bisa meremote router dari mana saja asalkan ada koneksi dari user ke router.

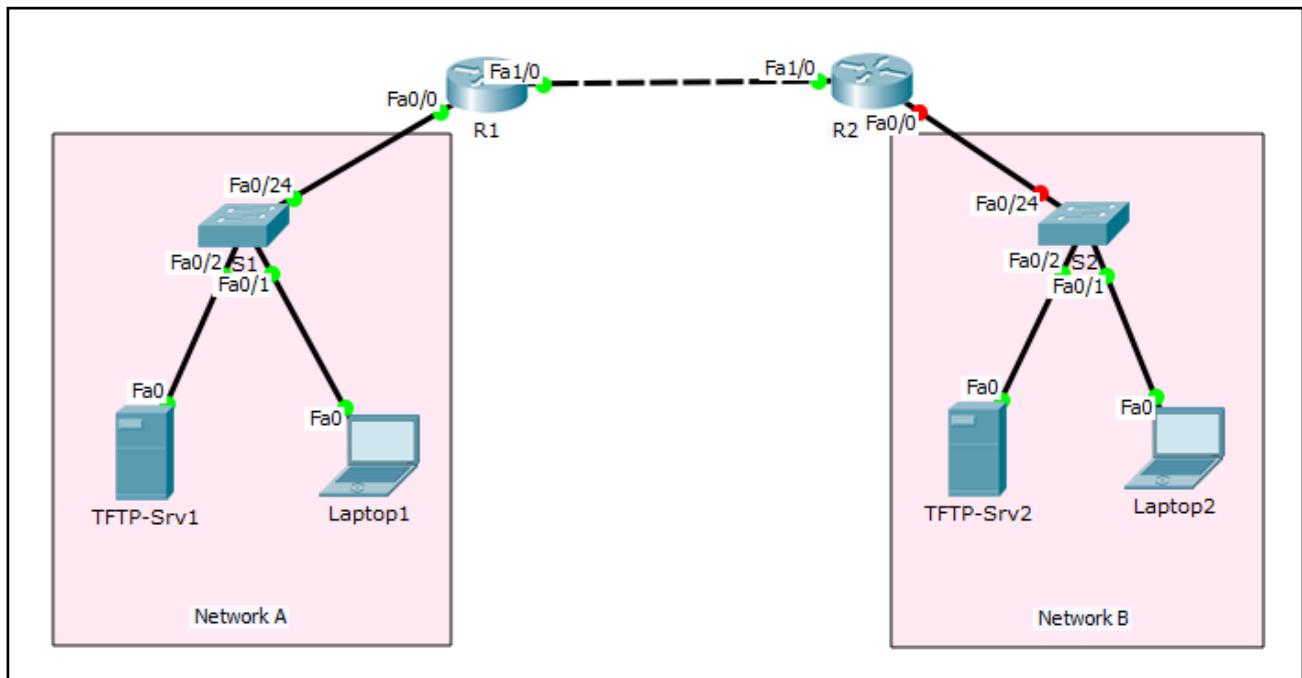
**Note: ulangi langkah yang sama diatas untuk meremote telnet R2 dari Laptop2.**

## **Review**

1. Bagaimana caranya agar saat telnet router tidak hanya ditanyakan password saja, akan tetapi ditanyakan username juga? Jadi saat telnet kita harus tahu username dan passwordnya, jika tidak tahu maka akses telnet tidak bisa dilakukan.

# Lab 3. Managing Router Configuration

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254
TFTP-Srv1	NIC	192.168.1.11	255.255.255.0	192.168.1.254
TFTP-Srv2	NIC	192.168.2.11	255.255.255.0	192.168.1.254

## Tujuan

- Setting SSH di R1 dan R2
- Backup dan restore konfigurasi router
- Menampilkan informasi hardware dan software router

## Konsep Dasar

Tujuan mensetting SSH di router yaitu untuk meningkatkan keamanan akses router, karena dengan SSH komunikasi antar Laptop dan router dienkripsi sehingga menyulitkan proses sniffing password dengan menggunakan packet sniffer.

Setelah kita mensetting basic router dan router sudah berjalan operasional, langkah selanjutnya yaitu melakukan backup konfigurasi. Untuk menyimpan hasil backup ini dibutuhkan server TFTP. Proses backup tidak hanya untuk file konfigurasi, namun bisa juga dilakukan untuk backup Cisco IOS. Keuntungan melakukan backup yaitu jika suatu saat konfigurasi missing atau Cisco IOS corrupt, maka kita bisa dengan mudah melakukan restore konfigurasi atau Cisco IOS yang sudah kita simpan di server TFTP sebelumnya.

Agar tidak terjadi kehilangan konfigurasi router, biasakan setelah mensetting router untuk menjalankan command `copy run start` atau `write memory` untuk menyimpan konfigurasi.

Untuk mengetahui informasi hardware dan software router kita bisa menggunakan beberapa command, contohnya `show version` atau `show interface`. Hasil output command tersebut berupa informasi Ethernet cable, RAM, NVRAM, dan masih banyak lainnya.

## **Konfigurasi**

Login console ke R1 atau R2 untuk mempraktikkan **Lab 3-Managing Router Configuration**.

### **Setting SSH di router R1 dan R2.**

Langkah mengaktifkan SSH di router:

1. Setting domain router
2. Setting username dan password login
3. Setting transport input ssh di line vty
4. Generate crypto rsa key 1024

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-name NIXTRAIN.com
R1(config)#username admin secret ciscossh
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#crypto key generate rsa [ENTER]
The name for the keys will be: R1.NIXTRAIN.com
Choose the size of the key modulus in the range of 360 to 2048 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]

R1(config)#exit
*Mar 3 2:27:58.564: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#
```

### **Backup konfigurasi R1**

Sebelum proses backup dilakukan, pastikan koneksi antara router R1 dan TFTP-Srv1 tidak ada masalah. Untuk mengeceknya gunakan tes Ping.

Setelah koneksi dari R1 ke TFTP-Srv1 sukses, langkah selanjutnya yaitu eksekusi command di R1.

Ketikkan command backup berikut di R1 :

```
R1#copy running-config tftp  
Address or name of remote host []? 192.168.1.11  
Destination filename [R1-config]?  
  
Writing running-config....!!  
[OK - 828 bytes]  
  
828 bytes copied in 3.005 secs (275 bytes/sec)
```

## Backup Cisco IOS R1

Tampilkan lokasi penyimpanan Cisco IOS yang akan dibackup

```
R1#show flash  
System flash directory:  
File Length Name/status  
3 5571584 pt1000-i-mz.122-28.bin  
2 28282 sigdef-category.xml  
1 227537 sigdef-default.xml  
[5827403 bytes used, 58188981 available, 64016384 total]  
63488K bytes of processor board System flash (Read/Write)
```

## Proses Backup Cisco IOS R1

```
R1#copy flash tftp  
Source filename []? pt1000-i-mz.122-28.bin  
Address or name of remote host []? 192.168.1.11  
Destination filename [pt1000-i-mz.122-28.bin]?  
  
Writing pt1000-i-mz.122-  
28.bin...!!!!!!!!!!!!!!  
[OK - 5571584 bytes]  
  
5571584 bytes copied in 0.29 secs (4402126 bytes/sec)
```

**Note: ulangi langkah yang sama untuk backup config dan Cisco IOS di R2.**

## Restore konfigurasi R1

Perbedaan proses backup dan restore, kalo backup menyimpan konfigurasi router ke TFTP, sedangkan restore yaitu download konfigurasi dari TFTP ke router.

Misalkan kita ingin mengconfig router dengan konfigurasi yang identik, maka kita bisa menggunakan konfigurasi yang sudah disimpan di TFTP. Dengan mensetting koneksi TFTP dan router, maka kita bisa mendownload config di TFTP diarahkan ke router dan mengubah settingan yang berbeda kemudian disesuaikan dengan konfigurasi yang sudah direncanakan.

Yang perlu diingat dari backup dan restore ini adalah source dan destination. Kalo backup berarti sourcenya router dan destinationnya TFTP, sedangkan restore yang berfungsi sebagai sourcenya TFTP dan destinationnya router.

## Command restore di R1

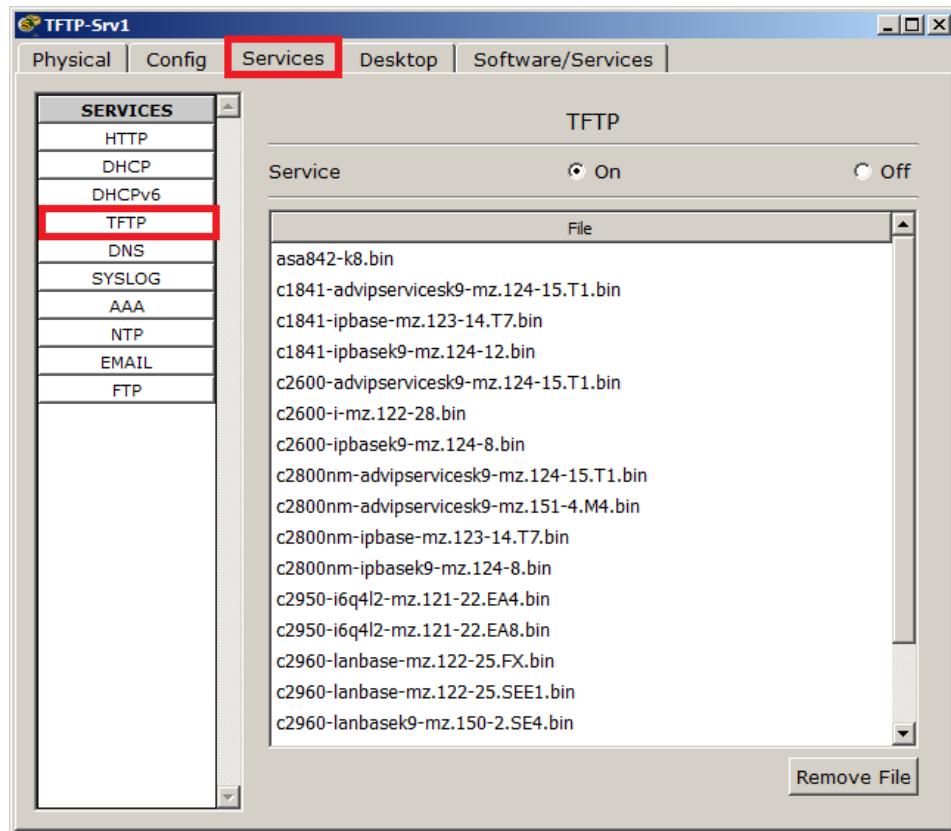
```
R1#copy tftp running-config
Address or name of remote host []? 192.168.1.11
Source filename []? R1-config
Destination filename [running-config]?

Accessing tftp://192.168.1.11/R1-config...
Loading R1-config from 192.168.1.11: !
[OK - 828 bytes]

828 bytes copied in 0.001 secs (828000 bytes/sec)
R1#
```

**Note: ulangi langkah yang sama untuk restore config R2.**

Untuk melihat hasil backup Cisco IOS dan R1-config, klik **TFTP-Srv1** -> pilih tab **Services** -> pilih **TFTP**



Gunakan scroll kebawah untuk melihat hasil backup terbaru

## Verifikasi

### Remote login SSH ke R1 dan R2

Setelah mensetting SSH di router R1 dan R2, gunakan putty untuk melakukan koneksi SSH ke router dari Laptop1 dan Laptop2 jika menggunakan real device.

- Ketikkan IP address R1 dan R2 pada bagian Hostname (or IP address)
- Pilih connection type SSH

- Klik Open

### Remote Akses SSH dari Laptop1 ke R1

```
Laptop1>ipconfig
```

```
FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::201:43FF:FE3A:AEC2
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.254
```

```
Laptop1>ssh -l admin 192.168.1.254
```

```
Open
```

```
Password:
```

```
Unauthorized access prohibited!
```

```
R1#show users
```

```
Line User Host(s) Idle Location
0 con 0 idle 00:01:49
*134 vty 0 admin idle 00:00:00
```

```
Interface User Mode Idle Peer Address
```

```
R1#
```

**admin** pada command SSH adalah username yang dibuat sebelumnya dan juga passwordnya.

**Note: ulangi langkah yang sama untuk remote SSH dari Laptop2 ke R2.**

## Menampilkan informasi hardware dan software R1

Gunakan command `show version`

```
R1#show version
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:pt1000-i-mz.122-28.bin"

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

R1#
```

Dari output diatas kita bisa mengetahui versi Cisco IOS, jumlah RAM, FastEthernet cable, Serial cable, NVRAM, Flash, confreg, dsb.

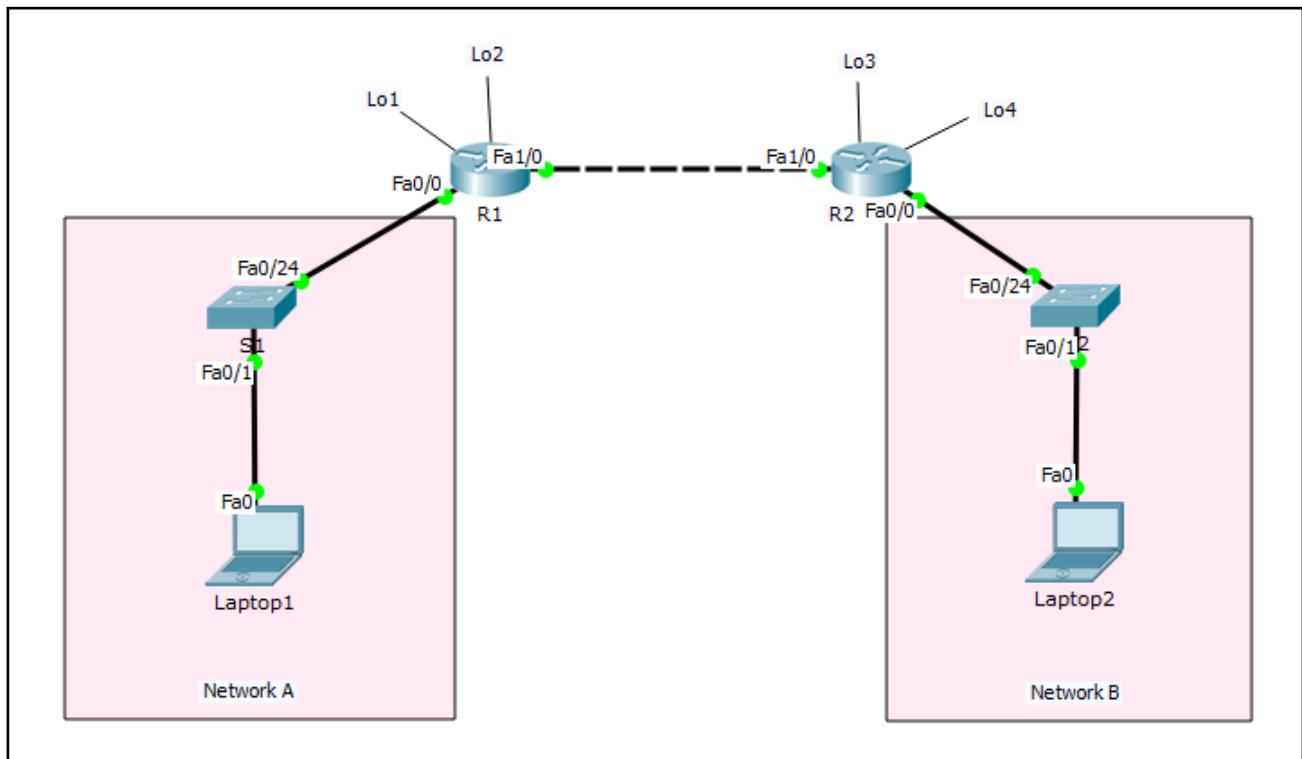
**Note: ulangi langkah yang sama untuk `show version` di R2.**

## Review

1. Coba lakukan akses telnet dari Laptop1 ke R1 dan Laptop2 ke R2, apakah berhasil atau tidak?
2. Bagaimana caranya agar user dapat melakukan akses telnet dan SSH sekaligus?
3. Apa bedanya FTP dan TFTP?

# Lab 4. Static Routing

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting static routing

## Konsep Dasar

### Routing

- Forwarding paket dari satu network ke network lainnya dengan memilih jalur yang terbaik dari routing table
- Routing memungkinkan dua network atau lebih dapat berkomunikasi dengan network lainnya
- Routing table hanya terdiri dari jalur terbaik untuk masing-masing network destination

### Static routing

- Konfigurasi routing dilakukan secara manual
- Membutuhkan informasi network destination
- Setiap network destination disetting manual
- Digunakan oleh organisasi kecil
- Memiliki administrative distance 0 atau 1

## Konfigurasi

Login console ke R1 atau R2 untuk mempraktikkan **Lab 4-Static Routing**.

### Setting interface loopback di R1

Ketikkan command berikut di R1

```
R1>enable
R1#configure terminal
R1(config)#interface lo1
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#
R1(config-if)#interface lo2
R1(config-if)#ip address 172.16.2.2 255.255.255.0
R1(config-if)#
R1(config-if)#end
```

Interface loopback secara default tidak ada, untuk membuat interface loopback gunakan command diatas. Fungsi interface loopback ini seperti logical interface untuk merepresentasikan sebuah subnet. Manfaat lain interface loopback untuk testing. Jika memiliki keterbatasan resources untuk membuat LAN saat ngelab, gunakan interface loopback sebagai LAN. Interface loopback sudah UP secara otomatis, sehingga tidak perlu memberikan sub-command no shutdown.

**Note:** ulangi langkah yang sama diatas untuk pembuatan interface loopback di R2.

### Tampilkan interface yang sudah disetting di R1

Untuk melakukan verifikasi apakah IP address yang sudah kita setting apakah sudah sesuai atau belum. Gunakan command dibawah ini.

```
R1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 192.168.1.254 YES manual up up
FastEthernet1/0 12.12.12.1 YES manual up up
Loopback1 172.16.1.1 YES manual up up
```

```
Loopback2 172.16.2.2 YES manual up up
R1#
```

### Tampilkan interface yang sudah disetting di R2

```
R2#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 192.168.2.254 YES manual up up
FastEthernet1/0 12.12.12.2 YES manual up up
Loopback0 172.16.3.3 YES manual up up
Loopback1 172.16.4.4 YES manual up up
R2#
```

Pastikan status interface **UP UP** semua.

### Tampilkan routing table di R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R1#
```

Dari output routing table R1 dapat dilihat :

- Routing table diatas yang ditampilkan hanya network directly connected (jaringan yang terhubung langsung) ditandai dengan kode C (Connected).
- Secara default, router tidak mengetahui network yang tidak terhubung langsung dan itulah alasan mengapa Network A dan Network B tidak bisa berkomunikasi (Jawaban Review **Lab 1. Basic Router Configuration**)
- Untuk mengatasi hal tersebut, maka dibutuhkanlah routing protocol dengan berbagai tipe contohnya static routing atau dynamic routing.

### Setting static routing di R1

Untuk mensetting static routing dapat dilakukan dengan dua cara:

1. Next-hop IP address
2. Exit-interface

Istilah lain static routing :

1. Recursive static route = menggunakan next-hop ip address
2. Directly static route = menggunakan exit-interface

## Konfigurasi static routing:

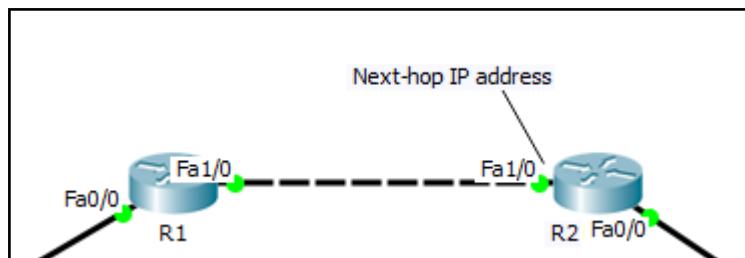
```
R1(config)#ip route <network-destination> <subnet-mask network-destination>
<next-hop ip address>
R1(config)#ip route <network-destination> <subnet-mask network-destination>
<exit-interface>
```

**network destination:** network tujuan yang tidak terhubung langsung (remotely connected network)

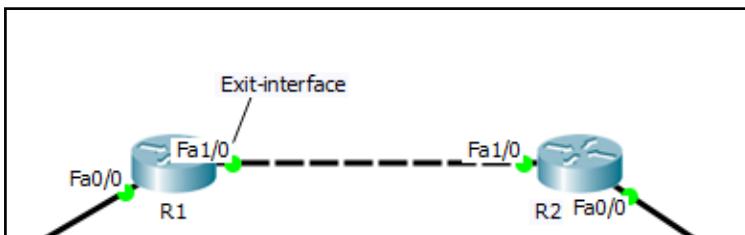
**next-hop ip address:** ip address yang terletak didepan router lokal menuju network destination

**exit-interface:** interface yang ada di router lokal untuk menuju network destination

Dari R1, untuk menuju network Fa0/0 R2, yang menjadi next-hop ip address yaitu IP address Fa1/0 R2.



Dari R1, untuk menuju network Fa0/0 R2, yang menjadi exit-interface yaitu interface Fa1/0 R1.



### Setting static routing di R1

```
R1(config)#
R1(config)#ip route 192.168.2.0 255.255.255.0 12.12.12.2
R1(config)#ip route 172.16.3.0 255.255.255.0 12.12.12.2
R1(config)#ip route 172.16.4.0 255.255.255.0 12.12.12.2
R1(config) #
```

### Setting static routing di R2

```
R2(config)#
R2(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
R2(config)#ip route 172.16.1.0 255.255.255.0 12.12.12.1
R2(config)#ip route 172.16.2.0 255.255.255.0 12.12.12.1
R2(config) #
```

### Verifikasi

Setelah melakukan setting static routing, lakukan verifikasi dengan beberapa command dibawah ini. Tes Ping antara Laptop1 dan Laptop2 pastikan berhasil. Lakukan tracert dari Laptop1 untuk melihat router mana saja yang dilewati ketika menuju ke Laptop2.

## Tampilkan routing table R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 4 subnets
C 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
S 172.16.3.0 [1/0] via 12.12.12.2
S 172.16.4.0 [1/0] via 12.12.12.2
C 192.168.1.0/24 is directly connected, FastEthernet0/0
S 192.168.2.0/24 [1/0] via 12.12.12.2
R1#
```

Dari output command static routing yang kita inputkan diatas, akan tampil kode S di routing table, artinya routing yang aktif yaitu static routing.

```
S 192.168.2.0/24 [1/0] via 12.12.12.2
```

### Penjelasan baris routing table diatas:

Dari output routing table diatas, dibagi menjadi 4 kolom :

- Kolom 1 = S : kode static routing, untuk menuju network destination digunakan static routing, atau routing protocol yang aktif di routing table adalah static routing.
- Kolom 2 = 192.168.2.0/24 : network destination, alamat network destination yang akan dituju oleh router. Network destination tampil di routing table setelah kita mengaktifkan routing protocol.
- Kolom 3 = [1/0] : 1 menyatakan nilai Administrative Distance (AD), 0 menyatakan nilai metric.
- Kolom 4 = via 12.12.12.2 : next-hop ip address yang akan digunakan oleh router local untuk memforward paket ke network destination

**Administrative Distance (AD)** menyatakan tingkat prioritas routing protocol ketika router menjalankan lebih dari satu routing protocol secara bersamaan. AD dengan nilai terkecil yang akan dipilih oleh router. Misalkan kita mengaktifkan protocol routing dynamic OSPF dan RIP, maka yang akan dipilih oleh router yaitu OSPF karena memiliki nilai AD lebih kecil (110), sedangkan RIP memiliki nilai AD lebih besar (120).

**Metric** menyatakan nilai dari hasil perhitungan routing protocol. Untuk RIP, metric terbaik dinilai dari hop terkecil, sehingga path (jalur) terbaik menurut RIP yaitu route dengan jumlah hop terkecil.

AD untuk membandingkan prioritas routing protocol yang satu dengan yang lainnya, sedangkan Metric untuk membandingkan value (nilai perhitungan) di dalam routing protocol tertentu.

### Cisco default administrative distances

Routing protocol or source	Administrative distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Unknown	255

## Ping dari Laptop1 ke Laptop2

```
Laptop1>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=126
```

```
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
```

```
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
```

```
Reply from 192.168.2.1: bytes=32 time=1ms TTL=126
```

```
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 = 1ms, Average = 0ms
```

Ping berhasil dari Laptop1 ke Laptop2.

## Tampilkan routing table R2

```
R2#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, 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
```

```
12.0.0.0/24 is subnetted, 1 subnets
```

```
C 12.12.12.0 is directly connected, FastEthernet1/0
```

```
172.16.0.0/24 is subnetted, 4 subnets
```

```
S 172.16.1.0 [1/0] via 12.12.12.1
```

```
S 172.16.2.0 [1/0] via 12.12.12.1
```

```
C 172.16.3.0 is directly connected, Loopback0
```

```
C 172.16.4.0 is directly connected, Loopback1
```

```
S 192.168.1.0/24 [1/0] via 12.12.12.1
```

```
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R2#
```

## Ping dari Laptop2 ke Laptop1

```
Laptop2>ping 192.168.1.1
```

Pinging 192.168.1.1 with 32 bytes of data:

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126  
Reply from 192.168.1.1: bytes=32 time=12ms TTL=126  
Reply from 192.168.1.1: bytes=32 time=10ms TTL=126
```

Ping statistics for 192.168.1.1:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:

```
Minimum = 0ms, Maximum = 12ms, Average = 5ms
```

## Lakukan trace route dari Laptop1 ke Laptop2

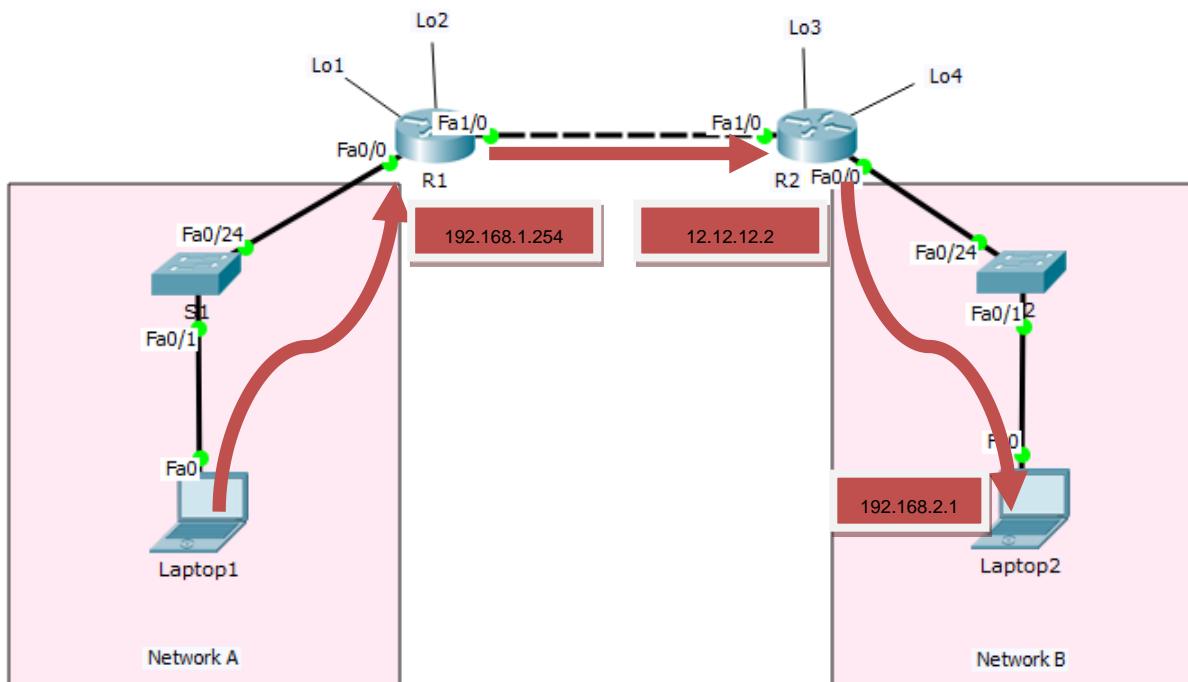
Untuk mengetahui jalur mana yang dilewati, bisa kita cek dengan command **tracert** di Laptop.

```
Laptop1>tracert 192.168.2.1
```

Tracing route to 192.168.2.1 over a maximum of 30 hops:

```
1 7 ms 1 ms 0 ms 192.168.1.254  
2 0 ms 0 ms 0 ms 12.12.12.2  
3 1 ms 0 ms 0 ms 192.168.2.1  
Trace complete.
```

Dari output diatas, untuk menuju Laptop2 dari Laptop1 melewati 3 hop.



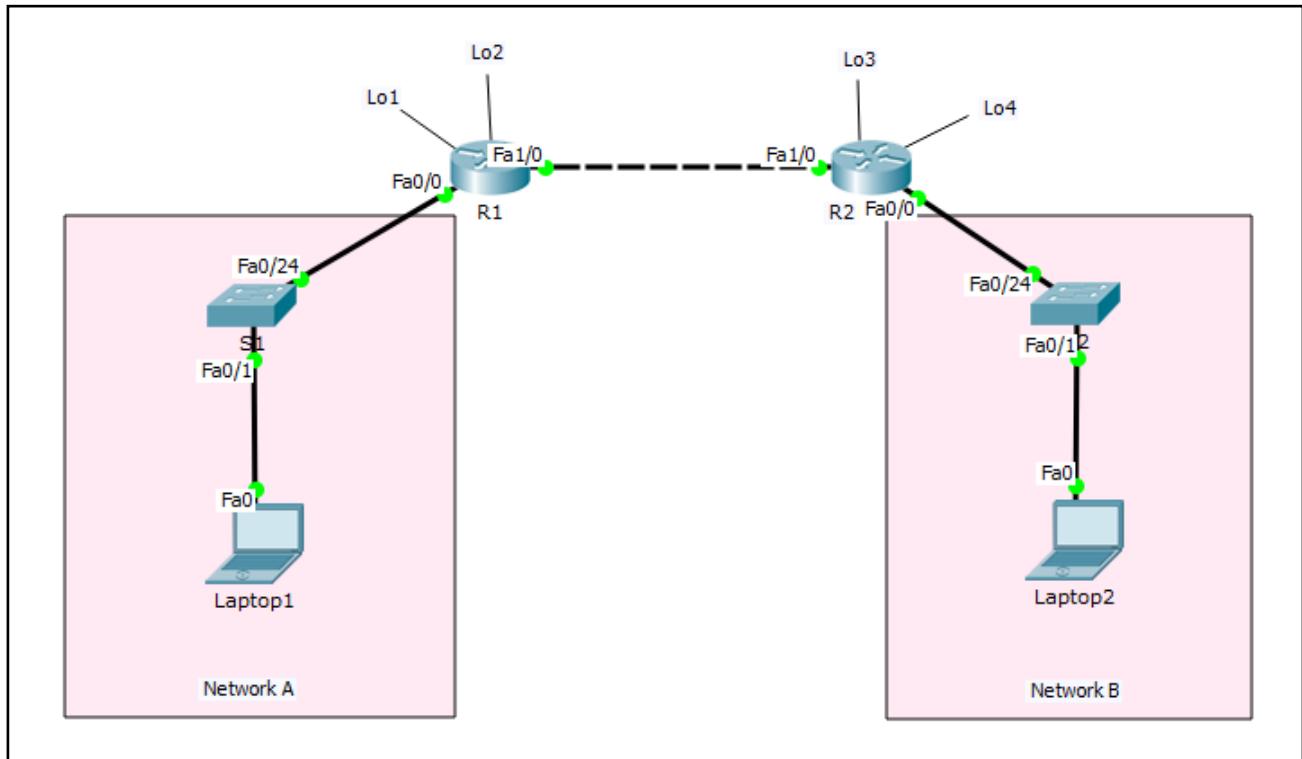
Note: ulangi langkah yang sama diatas untuk traceroute dari Laptop2 ke Laptop1.

## **Review**

1. Setelah mengetahui static routing dengan next-hop ip address, sekarang coba kerjakan static routing menggunakan exit-interface di R1 dan R2?
2. Lebih baik menggunakan next-hop ip address atau exit-interface untuk implementasi static routing? Jelaskan alasannya kenapa?

# Lab 5. Static Default Route

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting static default route

## Konsep Dasar

Static default route adalah static route dengan network address destination 0.0.0.0 dan subnet mask 0.0.0.0. Dikenal juga sebagai “quad zero” route. Static default route melakukan identifikasi gateway yang akan digunakan oleh router untuk mengirimkan semua paket IP untuk network destination yang tidak diketahui di routing table, sehingga akan diforward ke route 0.0.0.0/0.

Untuk konfigurasi static default route dapat menggunakan next-hop ip address atau exit-interface.

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address or exit-intf}
```

Static default route:

- Default route dapat digunakan ketika network destination tidak diketahui (Internet)
- Default route dapat digunakan ketika hanya ada satu jalur keluar untuk semua network destination
- Dapat mengurangi ukuran routing table
- Jika router tidak menemukan entry network destination di routing table, maka router akan memforward paket ke default route
- Menjadi route pilihan terakhir di routing table

## Konfigurasi

Login console ke R1 atau R2 untuk mempraktikkan **Lab-5 Static Default Route**.

Setelah mengerjakan Lab 4, gunakan kembali topologi Lab 4 beserta solutionnya untuk mempraktikkan Lab 5.

Untuk mensimulasikan default route di R1, hapus terlebih dahulu static route di R1 sedangkan R2 masih seperti semula. Setelah disetting static default route di R1 kemudian tes Ping dari Laptop1 ke Laptop2. Sebaliknya, untuk mencoba default route di R2, hapus static route di R2 dan setting ulang static route di R1 seperti di Lab 4. Kemudian tes Ping dari Laptop2 ke Laptop1.

### **Hapus static route di R1**

```
R1(config)#
R1(config)#no ip route 192.168.2.0 255.255.255.0 12.12.12.2
R1(config)#no ip route 172.16.3.0 255.255.255.0 12.12.12.2
R1(config)#no ip route 172.16.4.0 255.255.255.0 12.12.12.2
R1(config)#

```

### **Setting static default route di R1**

Command untuk mensetting static default route menggunakan next-hop ip address.

```
R1(config)#
R1(config)# ip route 0.0.0.0 0.0.0.0 12.12.12.2
R1(config)#

```

Command untuk mensetting static default route menggunakan exit-interface

```
R1(config)#
R1(config)# ip route 0.0.0.0 0.0.0.0 fa1/0
R1(config)#

```

Pilih salah satu command diatas apakah ingin menggunakan next-hop ip address atau exit-interface.

### Tampilkan routing table di R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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 12.12.12.2 to network 0.0.0.0

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
C 192.168.1.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 12.12.12.2
```

Tanda **S\*** menandakan static default route. Setiap network destination yang tidak diketahui dirouting table akan diforward ke 12.12.12.2. Lihat juga pada bagian **Gateway of last resort** yang menyatakan bahwa untuk menuju network 0.0.0.0 gunakan gatewaynya 12.12.12.2.

### Tes Ping dari Laptop1 ke Laptop2

```
Laptop1>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=126
Reply from 192.168.2.1: bytes=32 time=1ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126

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 = 1ms, Average = 0ms
```

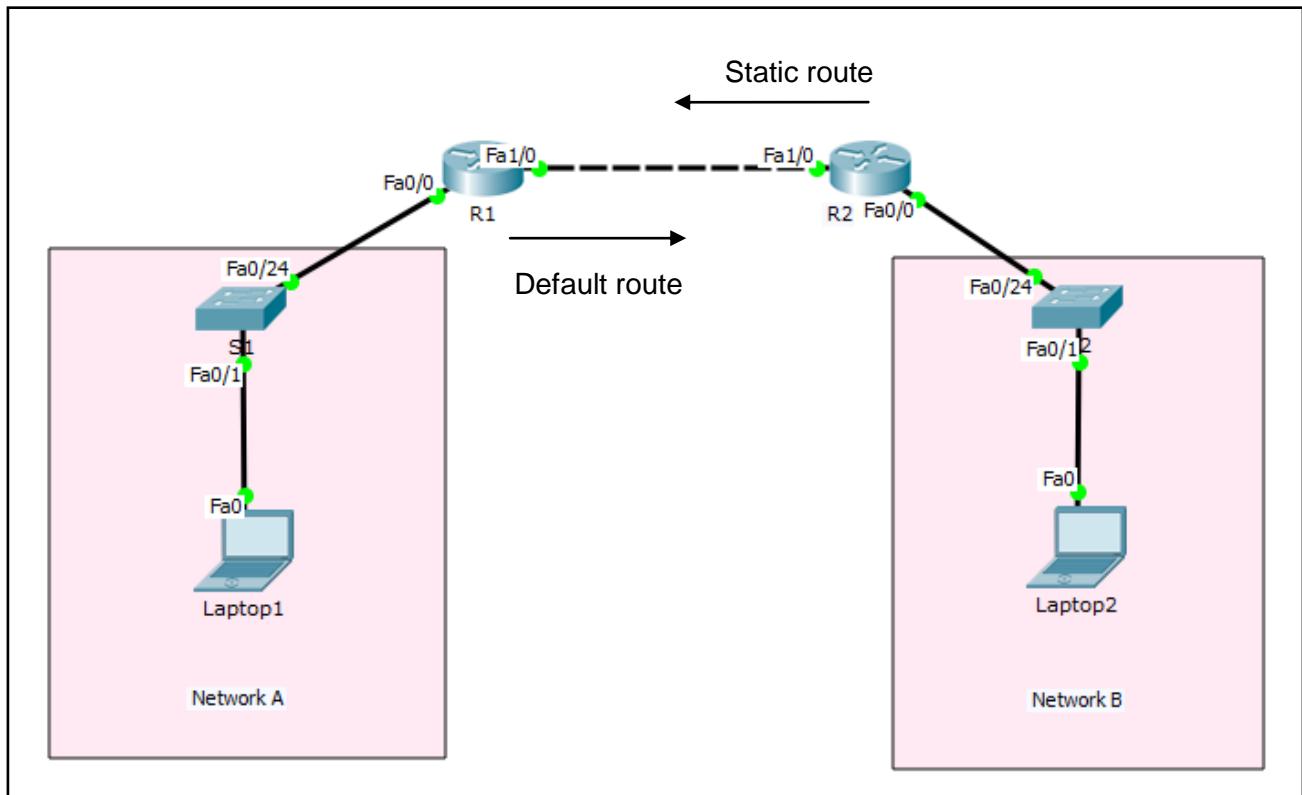
### Traceroute dari Laptop1 ke Laptop2

```
Laptop1>tracert 192.168.2.1
Tracing route to 192.168.2.1 over a maximum of 30 hops:

1 1 ms 0 ms 0 ms 192.168.1.254
2 0 ms 0 ms 0 ms 12.12.12.2
3 0 ms 0 ms 0 ms 192.168.2.1

Trace complete.
```

Lab static default route di R1 sudah berhasil. Konfigurasi eksisting saat ini R1 menggunakan static default route dan R2 menggunakan static route.



### Tampilan routing table di R2

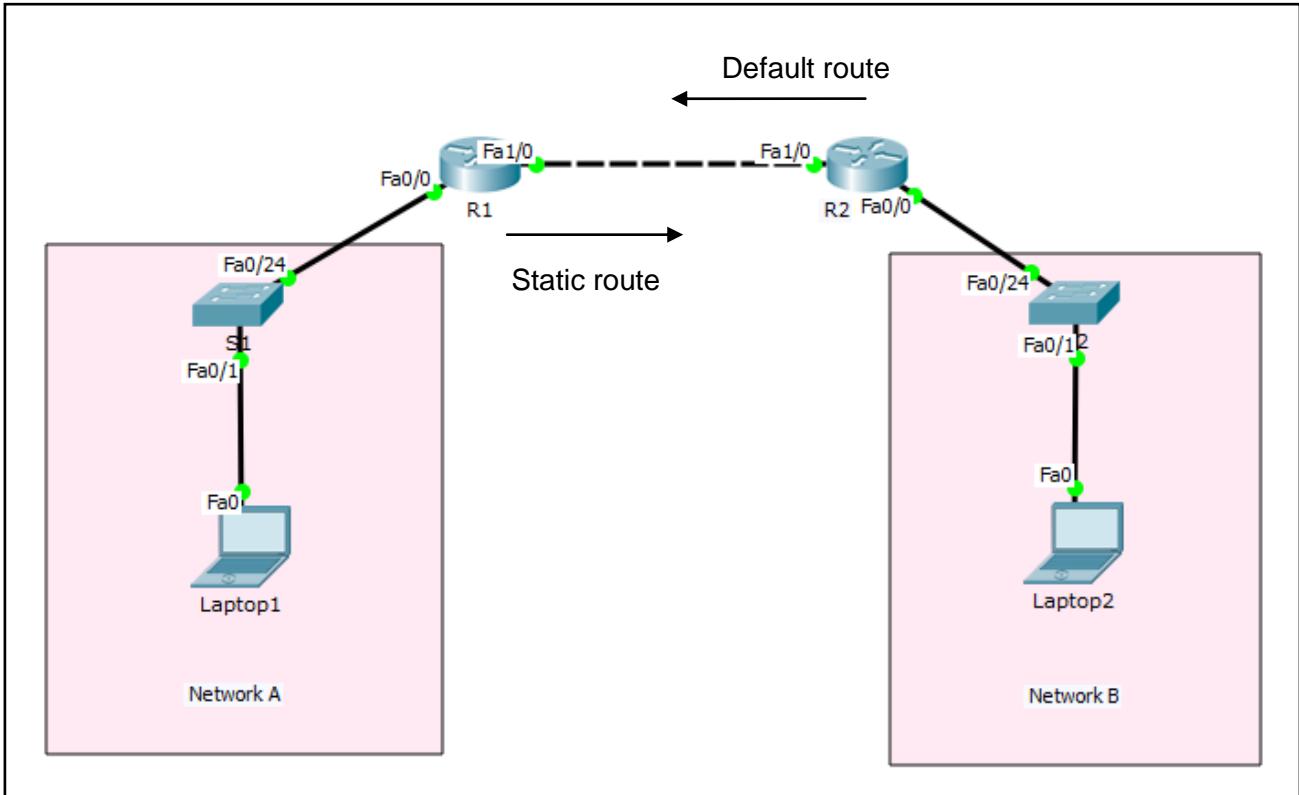
```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 4 subnets
S 172.16.1.0 [1/0] via 12.12.12.1
S 172.16.2.0 [1/0] via 12.12.12.1
C 172.16.3.0 is directly connected, Loopback0
C 172.16.4.0 is directly connected, Loopback1
S 192.168.1.0/24 [1/0] via 12.12.12.1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

Dari tampilan diatas dapat dilihat bahwa R2 menggunakan static route dengan kode **S**. Sedangkan di R1 static default route dengan kode **S\***. Perhatikan perbedaannya ada \* di R1.

Sekarang kita akan mencoba static default route di R2, berarti di R1 harus disetting static route terlebih dahulu dan hapus konfigurasi static default route yang ada. Cek kembali solution Lab 4.



### Hapus static default route di R1

Command untuk menghapus settingan static default route menggunakan next-hop ip address.

```
R1(config)#
R1(config)#no ip route 0.0.0.0 0.0.0.0 12.12.12.2
R1(config)#

```

Command untuk menghapus settingan static default route menggunakan exit-interface

```
R1(config)#
R1(config)#no ip route 0.0.0.0 0.0.0.0 fa1/0
R1(config)#

```

### Setting static route di R1

```
R1(config)#
R1(config)#ip route 192.168.2.0 255.255.255.0 12.12.12.2
R1(config)#ip route 172.16.3.0 255.255.255.0 12.12.12.2
R1(config)#ip route 172.16.4.0 255.255.255.0 12.12.12.2
R1(config)#

```

Sebelum melanjutkan langkah berikutnya, hapus terlebih dahulu static route di R2. Dan tampilkan hasilnya menggunakan `show ip route`, pastikan hanya C saja yang masih ada di routing table R2.

### Setting static default route di R2

Command untuk mensetting static default route menggunakan next-hop ip address.

```
R2(config)#
R2(config) # ip route 0.0.0.0 0.0.0.0 12.12.12.1
R2(config)#

```

Command untuk mensetting static default route menggunakan exit-interface

```
R2(config)#
R2(config)# ip route 0.0.0.0 0.0.0.0 fa1/0
R2(config)#
```

Pilih salah satu command diatas apakah ingin menggunakan next-hop ip address atau exit-interface.

### Tampilkan routing table di R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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 12.12.12.1 to network 0.0.0.0

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.3.0 is directly connected, Loopback0
C 172.16.4.0 is directly connected, Loopback1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 12.12.12.1
R2#
```

Tanda **S\*** menandakan static default route. Setiap network destination yang tidak diketahui dirouting table akan diforward ke 12.12.12.1. Lihat juga pada bagian **Gateway of last resort** yang menyatakan bahwa untuk menuju network 0.0.0.0 gunakan gatewaynya 12.12.12.1.

### Tes Ping dari Laptop2 ke Laptop1

```
Laptop2>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126
Reply from 192.168.1.1: bytes=32 time=11ms TTL=126
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

## Traceroute dari Laptop2 ke Laptop1

```
Laptop2>tracert 192.168.1.1
```

```
Tracing route to 192.168.1.1 over a maximum of 30 hops:
```

```
1 1 ms 0 ms 0 ms 192.168.2.254  
2 0 ms 0 ms 0 ms 12.12.12.1  
3 1 ms 11 ms 11 ms 192.168.1.1
```

```
Trace complete.
```

**Note:** langkah diatas harus dijalankan secara bergantian agar bisa mensimulasikan static default route di R1 maupun R2.

## Verifikasi

Proses konfigurasi diatas sekaligus dilakukan proses verifikasi. Untuk melihat hasil settingan, gunakan command show running-config.

### Tampilkan routing table R2

```
R2#show ip route  
Codes: C - connected, S - static, I - IGRP, 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 12.12.12.1 to network 0.0.0.0
```

```
12.0.0.0/24 is subnetted, 1 subnets  
C 12.12.12.0 is directly connected, FastEthernet1/0  
172.16.0.0/24 is subnetted, 2 subnets  
C 172.16.3.0 is directly connected, Loopback3  
C 172.16.4.0 is directly connected, Loopback4  
C 192.168.2.0/24 is directly connected, FastEthernet0/0  
S* 0.0.0.0/0 [1/0] via 12.12.12.1
```

Dari output diatas ditampilkan full routing table di R2. Jika ingin menampilkan misalnya yang connected atau static saja, gunakan tambahan sub-command **connected** atau **static**.

### Tampilkan routing table static R2

```
R2#show ip route static  
S* 0.0.0.0/0 [1/0] via 12.12.12.1  
R2#
```

## Tampilkan routing table connected R2

```
R2#show ip route connected
C 12.12.12.0/24 is directly connected, FastEthernet1/0
C 172.16.3.0/24 is directly connected, Loopback3
C 172.16.4.0/24 is directly connected, Loopback4
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

## Opsi menampilkan routing table

Ada beberapa pilihan untuk menampilkan routing table, apakah ingin menampilkan static saja atau yang lainnya. Gunakan tanda ? untuk melihat opsi yang tersedia.

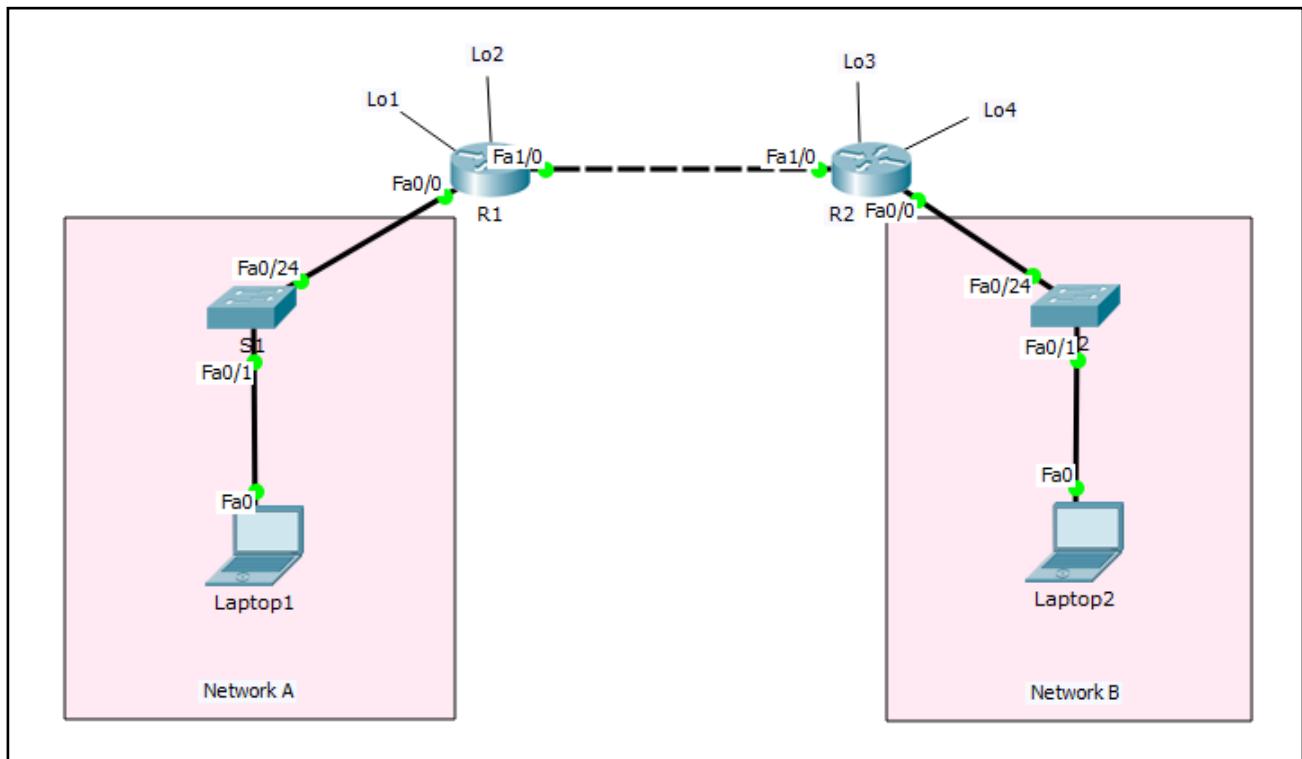
```
R2#show ip route ?
WORD Network to display information about or hostname
bgp Border Gateway Protocol (BGP)
connected Connected
eigrp Enhanced Interior Routing Protocol (EIGRP)
ospf Open Shortest Path First (OSPF)
rip Routing Information Protocol (RIP)
static Static routes
summary Summary of all routes
<cr>
R2#
```

## Review

1. Static default route cocok untuk network tipe stub-network, jelaskan apa yang di maksud tipe stub-network?
2. Router bisa menjalankan routing protocol static dan dynamic secara bersamaan. Static default route sering digunakan sebagai backup routing protocol dynamic jika bermasalah, bagaimana cara mensetting agar static default route menjadi backup routing protocol OSPF jika routing protocol OSPF down?

# Lab 6. RIPv2

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting RIPv2
- Debug RIPv2
- Setting passive-interface RIPv2

## Konsep Dasar

Keuntungan menggunakan dynamic routing dibandingkan static routing:

- Tidak perlu tahu network destination
- Perlu melakukan advertise network yang terhubung langsung
- Update perubahan topologi secara dinamis
- Pekerjaan network admin jadi berkurang
- Digunakan di industri besar
- Neighbor router melakukan pertukaran informasi routing dan membangun routing table secara otomatis
- Lebih mudah dibandingkan menggunakan static routing

## RIPv2

- Open standar protocol (Cisco atau non-Cisco)
- Classless routing protocol (support default atau sub-networks)
- Mendukung VLSM
- Mendukung Autentikasi
- Menggunakan multicast address 224.0.0.9
- Administrative distance: 120
- Metric: hop count (terbaik = yang paling kecil)
- Hop ke-16 unreachable
- Load balancing 4 equal path
- Digunakan untuk organisasi kecil
- Update secara periodic dan pertukaran keseleruhan informasi routing tabel setiap 30 second

**Dua langkah mudah setting routing protocol dinamis secara umum:**

1. Pilih routing protocol
2. Advertise directly connected network (jaringan yang terhubung langsung dengan router)

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network <Network ID>
Router(config-router)# no auto-summary
```

network <Network-ID> : untuk advertise network yang terhubung langsung dengan router (directly connected network).

## Keuntungan RIPv2

- Mudah dikonfigurasi
- Tidak memerlukan design seperti OSPF
- Tidak kompleks
- Less overhead

## Kerugian RIPv2

- Utilisasi bandwidth sangat tinggi karena diperlukan untuk broadcast setiap 30 second (RIPv1)
- Terbatas pada jumlah hop (bukan bandwidth)
- Tidak scalable, hop count hanya 15
- Konvergensi rendah

**Waktu konvergensi:** waktu yang dibutuhkan oleh router untuk menggunakan route alternative ketika best route down.

## Konfigurasi

Login console ke R1 atau R2 untuk mempraktikkan **Lab 6-RIPv2**.

### Tampilkan routing table sebelum disetting RIPv2 di R1

```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R1#
```

### Tampilkan routing table sebelum disetting RIPv2 di R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.3.0 is directly connected, Loopback0
C 172.16.4.0 is directly connected, Loopback1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

## Setting RIPv2 di R1

Command untuk mensetting RIPv2.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 12.12.12.0
R1(config-router)#network 172.16.1.0
R1(config-router)#network 172.16.2.0
R1(config-router)#network 192.168.1.0
R1(config-router)#no auto-summary
R1(config-router)#

```

## Setting RIPv2 di R2

Command untuk mensetting RIPv2.

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 12.12.12.0
R2(config-router)#network 172.16.3.0
R2(config-router)#network 172.16.4.0
R2(config-router)#network 192.168.2.0
R2(config-router)#no auto-summary
R2(config-router)#

```

## Verifikasi

### Tampilkan routing table setelah disetting RIPv2 di R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
R 172.16.0.0/16 [120/1] via 12.12.12.2, 00:00:55, FastEthernet1/0
C 172.16.1.0/24 is directly connected, Loopback1
C 172.16.2.0/24 is directly connected, Loopback2
R 172.16.3.0/24 [120/1] via 12.12.12.2, 00:00:02, FastEthernet1/0
R 172.16.4.0/24 [120/1] via 12.12.12.2, 00:00:02, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R 192.168.2.0/24 [120/1] via 12.12.12.2, 00:00:02, FastEthernet1/0
R1#

```

**Note: ulangi langkah yang sama diatas untuk menampilkan routing table di R2**

### Tes Ping dari Laptop1 ke Laptop2

```
Laptop1>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=126  
Reply from 192.168.2.1: bytes=32 time=1ms TTL=126  
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126  
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
```

```
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 = 1ms, Average = 0ms
```

Ping dari Laptop1 ke Laptop2 berhasil.

### Traceroute dari Laptop1 ke Laptop2

```
Laptop1>tracert 192.168.2.1
```

```
Tracing route to 192.168.2.1 over a maximum of 30 hops:
```

```
1 1 ms 0 ms 0 ms 192.168.1.254  
2 0 ms 0 ms 0 ms 12.12.12.2  
3 0 ms 0 ms 0 ms 192.168.2.1
```

```
Trace complete.
```

Untuk menuju Laptop2 dari Laptop1 membutuhkan 3 hop.

### Tes Ping dari Laptop2 ke Laptop1

```
Laptop2>ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.1: bytes=32 time=11ms TTL=126  
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
```

```
Ping statistics for 192.168.1.1:
```

```
PACKets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Ping dari Laptop2 ke Laptop1 berhasil.

## Traceroute dari Laptop2 ke Laptop1

```
Laptop2>tracert 192.168.1.1
```

```
Tracing route to 192.168.1.1 over a maximum of 30 hops:
```

```
1 1 ms 0 ms 0 ms 192.168.2.254  
2 0 ms 0 ms 0 ms 12.12.12.1  
3 1 ms 11 ms 11 ms 192.168.1.1
```

```
Trace complete.
```

## Tampilkan informasi routing protocol yang digunakan di R1

```
R1#show ip protocols  
Routing Protocol is "rip"  
  Sending updates every 30 seconds, next due in 12 seconds  
  Invalid after 180 seconds, hold down 180, flushed after 240  
  Outgoing update filter list for all interfaces is not set  
  Incoming update filter list for all interfaces is not set  
  Redistributing: rip  
  Default version control: send version 2, receive 2  
  Interface Send Recv Triggered RIP Key-chain  
    FastEthernet1/0 2 2  
    Loopback1 2 2  
    Loopback2 2 2  
    FastEthernet0/0 2 2  
  Automatic network summarization is not in effect  
  Maximum path: 4  
  Routing for Networks:  
    12.0.0.0  
    172.16.0.0  
    192.168.1.0  
  Passive Interface(s):  
  Routing Information Sources:  
    Gateway Distance Last Update  
    12.12.12.2 120 00:00:15  
  Distance: (default is 120)
```

**Note: ulangi langkah yang sama diatas untuk menampilkan routing information di R2**

Berdasarkan output routing information di R1, kita bisa lihat bahwa R1 menggunakan RIP version 2 untuk network 12.0.0.0, 172.16.0.0, dan 192.168.1.0. RIP memiliki **Administrative Distance** (AD) 120. Terdapat 4 interface yang mengaktifkan RIP yaitu Fa1/0, Fa0/0, Lo1, Lo2.

## Debug RIP di R1

Dengan mengaktifkan fitur debug, kita bisa tahu apakah RIP sudah berjalan atau belum.

```
R1#debug ip rip
RIP protocol debugging is on
R1#
RIP: received v2 update from 12.12.12.2 on FastEthernet1/0
172.16.3.0/24 via 0.0.0.0 in 1 hops
172.16.4.0/24 via 0.0.0.0 in 1 hops
192.168.2.0/24 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via FastEthernet1/0 (12.12.12.1)
RIP: build update entries
172.16.1.0/24 via 0.0.0.0, metric 1, tag 0
172.16.2.0/24 via 0.0.0.0, metric 1, tag 0
192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Loopback1 (172.16.1.1)
RIP: build update entries
12.12.12.0/24 via 0.0.0.0, metric 1, tag 0
172.16.2.0/24 via 0.0.0.0, metric 1, tag 0
172.16.3.0/24 via 0.0.0.0, metric 2, tag 0
172.16.4.0/24 via 0.0.0.0, metric 2, tag 0
192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
192.168.2.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Loopback2 (172.16.2.2)
RIP: build update entries
12.12.12.0/24 via 0.0.0.0, metric 1, tag 0
172.16.1.0/24 via 0.0.0.0, metric 1, tag 0
172.16.2.0/24 via 0.0.0.0, metric 1, tag 0
172.16.3.0/24 via 0.0.0.0, metric 2, tag 0
172.16.4.0/24 via 0.0.0.0, metric 2, tag 0
192.168.2.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0 (192.168.1.254)
```

Dari output debug RIP, kita bisa lihat bahwa RIP sudah running di router R1. Untuk menghentikan output debug, gunakan command **undebbug ip rip** atau **undebbug all**.

**Note: ulangi langkah yang sama diatas untuk menampilkan output debug RIP di R2**

## **Setting passive-interface di R1**

Untuk menghentikan routing updates yang dikirimkan ke Network A, maka aktifkan command **passive-interface** di interface fa0/0 R1 yang menuju Network A. Hal ini tidak mempengaruhi advertise Network A. Jadi, Network A masih tetap dikenali oleh R2 dan masih tampil di routing table R2. Di routing protocol RIPv2, mengaktifkan **passive-interface** mencegah multicast update melalui interface spesifik dan masih bisa mendapatkan update dari RIP neighbor yang lain.

```
R1(config)#router rip
R1(config-router)#passive-interface fa0/0
R1(config-router) #
```

## **Tampilkan routing information di R1**

```
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 3 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive 2
  Interface Send Recv Triggered RIP Key-chain
    FastEthernet1/0 2 2
    Loopback1 2 2
    Loopback2 2 2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    12.0.0.0
    172.16.0.0
    192.168.1.0
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway Distance Last Update
    12.12.12.2 120 00:00:08
    Distance: (default is 120)
R1#
```

Passive-interface fa0/0 R1 sudah berhasil kita setting.

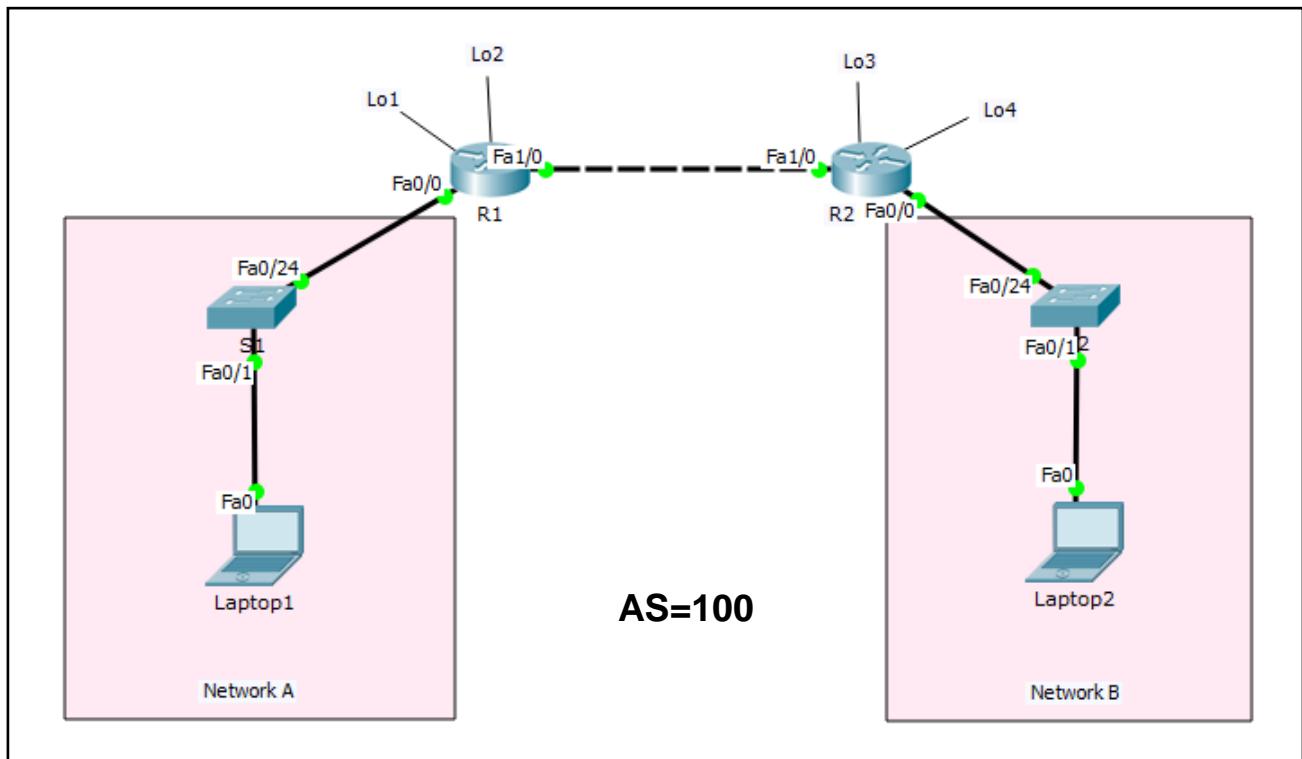
**Note: ulangi langkah yang sama diatas untuk setting passive-interface di R2**

## **Review**

1. Jelaskan fungsi dari no-auto summary pada sub-command RIPv2?
2. Command apa yang berfungsi untuk mengaktifkan passive-interface RIPv2 di semua interface R1 hanya dengan satu input command saja?
3. Gunakan jawaban No.2 untuk mengaktifkan passive-interface di semua interface di R1 dan R2? Kemudian lihat hasil output RIPv2 menggunakan command **debug ip rip** dan **show ip route**, apa yang terjadi?

# Lab 7. EIGRP

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting EIGRP
- Debug EIGRP
- Setting passive-interface EIGRP

## Konsep Dasar

EIGRP disebut juga sebagai routing protocol distance vector, terkadang disebut juga advanced distance vector atau routing protocol hybrid.

Berikut ini beberapa fitur dari EIGRP :

- Cisco open standar protocol (sebelumnya proprietary)
- Termasuk classless routing protocol
- Update perubahan topologi secara dinamis
- Metric (32 bit) : Composite Metric (BW + Delay + Load + MTU + Reliability)
- Administrative Distance: 90
- Update menggunakan multicast: 224.0.0.10
- Jumlah maksimum hop count: 255 (default 100)
- Mendukung protocol IP, IPX, Apple Talk
- Hello packet dikirim setiap 5 second (dead interval 15 second)
- Konvergensi cepat
- Menggunakan algoritma DUAL (Diffusing Update Algorithm)
- Mendukung equal dan unequal cost load balancing

**EIGRP memaintain tiga tabel**

1. Neighbor table
  - Menampilkan informasi directly connected router
  - Command: `show ip eigrp neighbor`
2. Topology table
  - Menampilkan semua best route yang dipelajari dari masing-masing neighbor
  - Command: `show ip eigrp topology`
3. Routing table
  - Menampilkan best route menuju network destination
  - Command: `show ip route`

**Notes EIGRP**

- EIGRP menggunakan autonomous system number (ASN) untuk mengidentifikasi router-router yang sharing informasi route
- Hanya router yang memiliki ASN sama yang bisa sharing informasi route

**Dua step menggunakan routing protocol dinamis secara umum:**

1. Pilih routing protocol
2. Advertise directly connected network (jaringan yang terhubung langsung dengan router)

**Konfigurasi EIGRP**

```
Router(config)# router eigrp 100
Router(config-router)# network <Network ID>
Router(config-router)# network <Network ID> <Wildcard Mask>
Router(config-router)# no auto-summary
```

network <Network-ID> : untuk advertise network yang terhubung langsung dengan router (directly connected network).

**Keuntungan EIGRP**

- Terdapat backup route jika best route down (successor=primary, feasible successor=backup)
- Mendukung VLSM

## Konfigurasi

Login console ke R1 atau R2 untuk mempraktikkan **Lab 7-EIGRP**.

### Tampilkan routing table sebelum disetting EIGRP di R1

```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R1#
```

### Tampilkan routing table sebelum disetting EIGRP di R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.3.0 is directly connected, Loopback0
C 172.16.4.0 is directly connected, Loopback1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

Dari output diatas, hanya menampilkan directly connected network pada masing-masing router yang ditandai dengan kode C. Untuk menghubungkan router agar bisa berkomunikasi dengan network remote (yang tidak terhubung langsung dengan router) maka perlu disetting routing protocol, salah satu contohnya yaitu EIGRP.

## Setting EIGRP di R1

Command untuk mensetting EIGRP.

```
R1(config)#router eigrp 100
R1(config-router)#network 12.12.12.0
R1(config-router)#network 172.16.1.0
R1(config-router)#network 172.16.2.0
R1(config-router)#network 192.168.1.0
R1(config-router)#no auto-summary
R1(config-router)#

```

## Setting EIGRP di R2

Command untuk mensetting EIGRP.

```
R2(config)#router eigrp 100
R2(config-router)#network 12.12.12.0
R2(config-router)#network 172.16.3.0
R2(config-router)#network 172.16.4.0
R2(config-router)#network 192.168.2.0
R2(config-router)#no auto-summary
R2(config-router)#

```

## Verifikasi

### Tampilkan routing table setelah disetting EIGRP di R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 4 subnets
C 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
D 172.16.3.0 [90/156160] via 12.12.12.2, 00:00:17, FastEthernet1/0
D 172.16.4.0 [90/156160] via 12.12.12.2, 00:00:17, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
D 192.168.2.0/24 [90/30720] via 12.12.12.2, 00:00:17, FastEthernet1/0
R1#

```

**Note: ulangi langkah yang sama diatas untuk menampilkan routing table di R2**

### Tes Ping dari Laptop1 ke Laptop2

```
Laptop1>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=126
```

```
Reply from 192.168.2.1: bytes=32 time=1ms TTL=126
```

```
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
```

```
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
```

```
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 = 1ms, Average = 0ms
```

Ping dari Laptop1 ke Laptop2 berhasil.

### Traceroute dari Laptop1 ke Laptop2

```
Laptop1>tracert 192.168.2.1
```

```
Tracing route to 192.168.2.1 over a maximum of 30 hops:
```

```
1 1 ms 0 ms 0 ms 192.168.1.254
```

```
2 0 ms 0 ms 0 ms 12.12.12.2
```

```
3 0 ms 0 ms 0 ms 192.168.2.1
```

```
Trace complete.
```

Untuk menuju Laptop2 dari Laptop1 membutuhkan 3 hop.

### Tes Ping dari Laptop2 ke Laptop1

```
Laptop2>ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
```

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126
```

```
Reply from 192.168.1.1: bytes=32 time=11ms TTL=126
```

```
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
```

```
Ping statistics for 192.168.1.1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Ping dari Laptop2 ke Laptop1 berhasil.

## Traceroute dari Laptop2 ke Laptop1

```
Laptop2>tracert 192.168.1.1
```

```
Tracing route to 192.168.1.1 over a maximum of 30 hops:
```

```
1 1 ms 0 ms 0 ms 192.168.2.254  
2 0 ms 0 ms 0 ms 12.12.12.1  
3 1 ms 11 ms 11 ms 192.168.1.1
```

```
Trace complete.
```

## Tampilkan neighbor table R1

```
R1#show ip eigrp neighbors  
IP-EIGRP neighbors for process 100  
H Address Interface Hold Uptime SRTT RTO Q Seq  
(sec) (ms) Cnt Num  
0 12.12.12.2 Fa1/0 10 00:02:23 40 1000 0 32
```

```
R1#
```

Dari output neighbor table dapat diketahui bahwa R1 memiliki neighbor router 12.12.12.2 (IP address R2).

## Tampilkan topologi table di R1

```
R1#show ip eigrp topology  
IP-EIGRP Topology Table for AS 100  
  
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  
r - Reply status  
  
P 12.12.12.0/24, 1 successors, FD is 28160  
via Connected, FastEthernet1/0  
P 172.16.1.0/24, 1 successors, FD is 128256  
via Connected, Loopback1  
P 172.16.2.0/24, 1 successors, FD is 128256  
via Connected, Loopback2  
P 172.16.3.0/24, 1 successors, FD is 156160  
via 12.12.12.2 (156160/128256), FastEthernet1/0  
P 172.16.4.0/24, 1 successors, FD is 156160  
via 12.12.12.2 (156160/128256), FastEthernet1/0  
P 192.168.1.0/24, 1 successors, FD is 28160  
via Connected, FastEthernet0/0  
P 192.168.2.0/24, 1 successors, FD is 30720  
via 12.12.12.2 (30720/28160), FastEthernet1/0  
R1#
```

**Note: ulangi langkah yang sama diatas untuk menampilkan neighbor table dan topologi table di R2**

## Tampilkan informasi routing EIGRP di R1

```
R1#show ip protocols

Routing Protocol is "eigrp 100"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
12.0.0.0
172.16.0.0
192.168.1.0
Routing Information Sources:
Gateway Distance Last Update
12.12.12.2 90 160431022
Distance: internal 90 external 170

R1#
```

Berdasarkan output routing information di R1, kita bisa lihat bahwa R1 menggunakan EIGRP dengan ASN 100 untuk network 12.0.0.0, 172.16.0.0, dan 192.168.1.0. EIGRP memiliki Administrative Distance 120. Secara default hop-count EIGRP 100.

## Tampilkan informasi interface EIGRP di R1

```
R1#show ip eigrp interfaces

IP-EIGRP interfaces for process 100

Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
Fa1/0 1 0/0 1236 0/10 0 0
Lo1 0 0/0 1236 0/10 0 0
Lo2 0 0/0 1236 0/10 0 0
Fa0/0 0 0/0 1236 0/10 0 0

R1#
```

Terdapat 4 interface yang disetting EIGRP yaitu Fa1/0, Fa0/0, Lo1, Lo2.

## Debug EIGRP R2

Pada saat kita mensetting EIGRP di R2 step sebelumnya pada **Halaman 43**, di R2 akan tampil output seperti dibawah ini :

```
R2(config)#router eigrp 100
R2(config-router)#network 12.12.12.0
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 12.12.12.1 (FastEthernet1/0) is up:
new adjacency

R2(config-router)#network 172.16.3.0
R2(config-router)#network 172.16.4.0
R2(config-router)#network 192.168.2.0
R2(config-router)#no auto-summary
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 12.12.12.1 (FastEthernet1/0) resync:
summary configured

R2(config-router)#end
R2#
```

Setelah selesai setting EIGRP di R1, kemudian kita mensetting EIGRP di R2, setelah input network 12.12.12.0 di R2, muncul pesan **neighbor adjacency** yang ditambahkan ke dalam routing process EIGRP. Oleh karena itu, saat kita verifikasi **show ip eigrp neighbors** R2 akan memiliki neighbor 12.12.12.1 seperti tampilan dibawah ini :

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 12.12.12.1 Fa1/0 10 00:23:38 40 1000 0 16
```

R2#

Selain itu juga terjadi proses resync saat kita mengetikkan command **no auto-summary**.

Untuk mengaktifkan debug paket EIGRP, gunakan command dibawah ini :

```
R2#debug eigrp packets
EIGRP Packets debugging is on
(UPDATE, REQUEST, QUERY, REPLY, HELLO, ACK )
EIGRP: Received HELLO on FastEthernet1/0 nbr 12.12.12.1
AS 100, Flags 0x0, Seq 17/0 idbQ 0/0

EIGRP: Sending HELLO on Loopback4
AS 100, Flags 0x0, Seq 36/0 idbQ 0/0 iidbQ un/rely 0/0

EIGRP: Received HELLO on Loopback4 nbr 172.16.4.4
AS 100, Flags 0x0, Seq 36/0 idbQ 0/0

EIGRP: Packet from ourselves ignored
```

```

EIGRP: Sending HELLO on Loopback3
AS 100, Flags 0x0, Seq 36/0 idbQ 0/0 iidbQ un/rely 0/0

EIGRP: Received HELLO on Loopback3 nbr 172.16.3.3
AS 100, Flags 0x0, Seq 36/0 idbQ 0/0

EIGRP: Packet from ourselves ignored

EIGRP: Sending HELLO on FastEthernet0/0
AS 100, Flags 0x0, Seq 36/0 idbQ 0/0 iidbQ un/rely 0/0

EIGRP: Sending HELLO on FastEthernet1/0
AS 100, Flags 0x0, Seq 36/0 idbQ 0/0 iidbQ un/rely 0/0

EIGRP: Received HELLO on FastEthernet1/0 nbr 12.12.12.1
AS 100, Flags 0x0, Seq 17/0 idbQ 0/0

```

Untuk menghentikan debug EIGRP packets, gunakan command berikut : **no debug eigrp packets**

### **Setting passive-interface di R1**

```

R1(config)#router eigrp 100
R1(config-router)#passive-interface fa0/0
R1(config-router)#

```

Dari output debug packet EIGRP, kita bisa lihat bahwa EIGRP menggunakan paket hello untuk membentuk relationship dengan router tetangga (adjacent router). Apabila kita mengaktifkan command **passive-interface** di interface maka akan menghentikan pengiriman paket hello sehingga akan mencegah update outgoing dan incoming.

Karena Network A dan Network B tidak memerlukan paket hello, maka kita perlu mengaktifkan **passive-interface** untuk interface di R1 dan R2 yang menuju Network A dan Network B.

**Note: ulangi langkah yang sama diatas untuk setting passive-interface EIGRP di R2**

### **Review**

1. Apakah yang dimaksud dengan wildcard mask?
2. Jelaskan perbedaannya saat kita mensetting routing EIGRP tanpa menggunakan wildcard mask dan menggunakan wildcard mask? Untuk membandingkan keduanya, gunakan solution lab sebelumnya **Halaman 43** yang tanpa wildcard mask dan solution dibawah ini yang menggunakan wildcard mask.

### Command untuk mensetting EIGRP di R1

```

R1(config)#router eigrp 100
R1(config-router)#network 12.12.12.0 0.0.0.255
R1(config-router)#network 172.16.1.0 0.0.0.255
R1(config-router)#network 172.16.2.0 0.0.0.255
R1(config-router)#network 192.168.1.0 0.0.0.255

```

```
R1(config-router)#no auto-summary
```

Command untuk mensetting EIGRP di R2

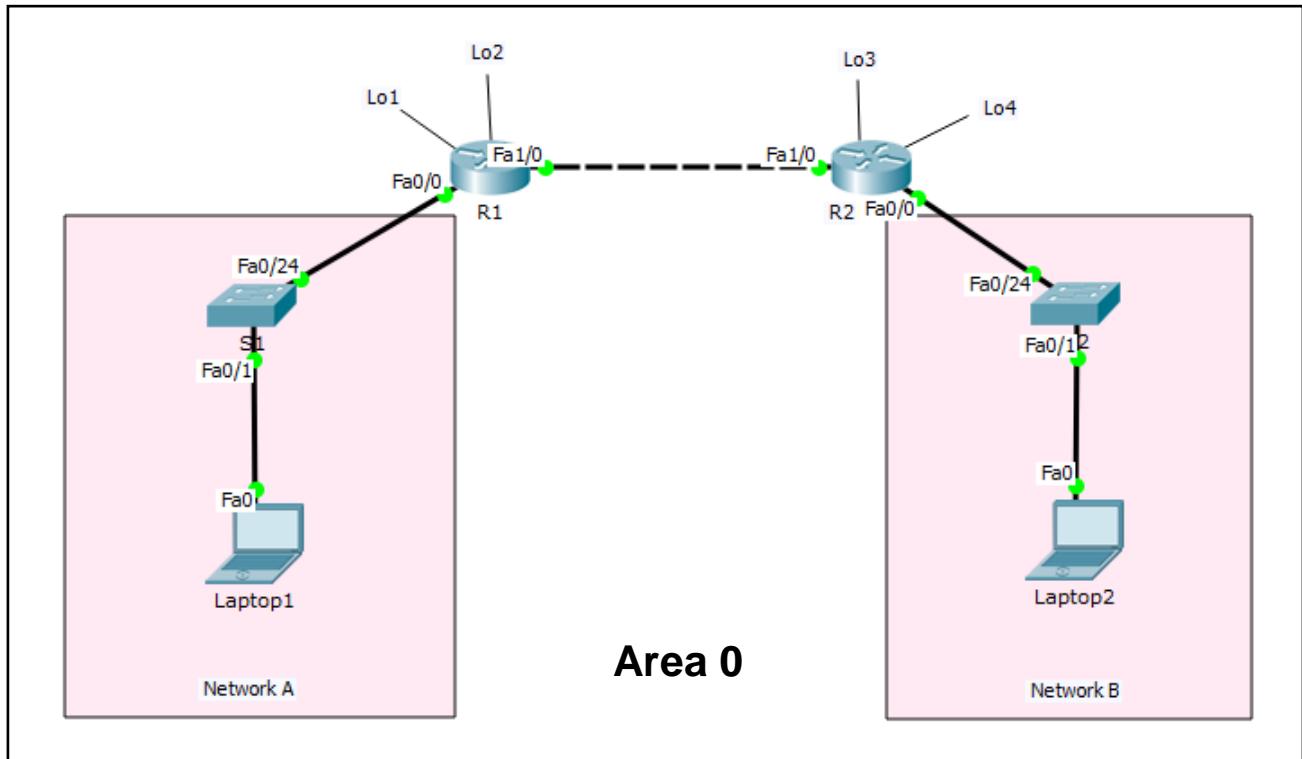
```
R2(config)#router eigrp 100
R2(config-router)#network 12.12.12.0 0.0.0.255
R2(config-router)#network 172.16.3.0 0.0.0.255
R2(config-router)#network 172.16.4.0 0.0.0.255
R2(config-router)#network 192.168.2.0 0.0.0.255
R2(config-router)#no auto-summary
```

3. Untuk membentuk relationship neighbor antar router di EIGRP, apa sajakah kriteria yang diperlukan ? Isi **Ya** atau **Tidak** table dibawah ini.

Requirement	EIGRP
Status interface harus UP UP	
Interface harus berada pada subnet yang sama	
Harus lolos autentikasi (jika disetting autentikasinya)	
Harus menggunakan ASN yang sama disettingan command <b>router eigrp</b>	
Hello dan hold/dead timers harus sama	
IP MTU harus sama	
Router ID harus unik	
K-values harus sama	
Harus berada dalam area yang sama	

# Lab 8. OSPF

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting OSPF
- Setting router-id OSPF
- Setting passive-interface dan network type loopback OSPF

## Konsep Dasar

- OSPF singkatan dari Open Shortest Path First
- OSPF merupakan routing protocol open standar yang diimplementasikan oleh berbagai macam vendor, termasuk Cisco
- Link-state protocol
- OSPF bekerja dengan menggunakan algoritma Dijkstra
- Hop count unlimited
- Metric: cost ( $\text{cost} = 10^8 / \text{BW}$ )
- Administrative Distance: 110
- Classless routing protocol
- Mendukung VLSM dan CIDR
- Hanya mendukung equal cost load balancing
- Terdapat konsep area untuk memudahkan manajemen dan control traffic
- Menyediakan design hierarki dengan multiple area
- Harus memiliki satu area yang disebut sebagai area 0 atau backbone area
- Semua area selain 0 (non-backbone area) harus terhubung ke area 0
- Dari scalabilitas lebih baik dibandingkan dengan protocol distance vector
- Mendukung autentikasi
- Update melalui multicast address: 224.0.0.5
- Konvergensi cepat
- Mengirimkan hello packet setiap 10 second
- Trigger/Incremental updates
  - Router mengirimkan update hanya jika terjadi perubahan dan tidak mengirimkan semua routing table pada periodic update

## **OSPF memaintain tiga tabel**

1. Neighbor table
  - Dikenal juga sebagai adjacency database
  - Menampilkan informasi directly connected router (neighbors)
  - Command: `show ip ospf neighbor`
2. Database table
  - Disebut juga sebagai LSDB (link state database)
  - Menampilkan semua kemungkinan informasi route menuju network dalam satu area
  - Command: `show ip ospf database`
3. Routing table
  - Menampilkan best route menuju network destination
  - Command: `show ip route`

## **Dua step menggunakan routing protocol dinamis secara umum:**

1. Pilih routing protocol
2. Advertise directly connected network (jaringan yang terhubung langsung dengan router)

## **Konfigurasi OSPF**

```
Router(config)# router ospf <process-id>
Router(config-router)# network <network-id> <wildcard-mask> area <area-id>
Router(config-router)# network <network-id> <wildcard-mask> area <area-id>
```

network <Network-ID> : untuk advertise network yang terhubung langsung dengan router (directly connected network).

wildcard-mask : inverse subnet-mask

## Keuntungan OSPF

- Open standard
- Tidak ada batasan jumlah hop
- Loop free
- Konvergensi lebih cepat

## Kerugian OSPF

- Mengkonsumsi lebih banyak resource CPU
- Kompleks dalam hal design dan implementasi
- Hanya mendukung equal load balancing
- Hanya mendukung protocol IP

## Konfigurasi

Login console ke R1 atau R2 untuk mempraktikkan **Lab 8-OSPF**.

### Tampilkan routing table sebelum disetting OSPF di R1

```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R1#
```

Dari output diatas, hanya terdapat directly connected network yang ditandai dengan kode C.

## Tampilkan routing table sebelum disetting OSPF di R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.3.0 is directly connected, Loopback0
C 172.16.4.0 is directly connected, Loopback1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

Agar proses routing berhasil, harus disetting OSPF disemua router terlebih dulu. Setelah itu baru diverifikasi dengan tes Ping end-to-end device-nya.

## Setting OSPF di R1

Command untuk menseetting OSPF.

```
R1(config)#router ospf 1
R1(config-router)#network 12.12.12.0 0.0.0.255 area 0
R1(config-router)#network 172.16.1.0 0.0.0.255 area 0
R1(config-router)#network 172.16.2.0 0.0.0.255 area 0
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#

```

## Setting OSPF di R2

Command untuk menseetting OSPF.

```
R2(config)#router ospf 1
R2(config-router)#network 12.12.12.0 0.0.0.255 area 0
R2(config-router)#network 172.16.3.0 0.0.0.255 area 0
R2(config-router)#network 172.16.4.0 0.0.0.255 area 0
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0

```

## Verifikasi

### Tampilkan routing table setelah disetting OSPF di R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Loopback1
C 172.16.2.0/24 is directly connected, Loopback2
O 172.16.3.3/32 [110/2] via 12.12.12.2, 00:01:31, FastEthernet1/0
O 172.16.4.4/32 [110/2] via 12.12.12.2, 00:01:31, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
O 192.168.2.0/24 [110/2] via 12.12.12.2, 00:00:40, FastEthernet1/0
R1#
```

### Tampilkan routing table setelah disetting OSPF di R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O 172.16.1.1/32 [110/2] via 12.12.12.1, 00:02:07, FastEthernet1/0
O 172.16.2.2/32 [110/2] via 12.12.12.1, 00:02:07, FastEthernet1/0
C 172.16.3.0/24 is directly connected, Loopback0
C 172.16.4.0/24 is directly connected, Loopback1
O 192.168.1.0/24 [110/2] via 12.12.12.1, 00:02:07, FastEthernet1/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

### Tampilkan informasi neighbor OSPF di R1

```
R1#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
172.16.4.4 1 FULL/DROTHER 00:00:35 12.12.12.2 FastEthernet1/0
R1#
```

### Tampilkan informasi neighbor OSPF di R2

```
R2#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
172.16.2.2 1 FULL/DR 00:00:31 12.12.12.1 FastEthernet1/0
R2#
```

### Tampilkan informasi routing protocol di R1

```
R1#show ip protocol
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 172.16.2.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
12.12.12.0 0.0.0.255 area 0
172.16.1.0 0.0.0.255 area 0
172.16.2.0 0.0.0.255 area 0
192.168.1.0 0.0.0.255 area 0
Routing Information Sources:
Gateway Distance Last Update
172.16.2.2 110 00:07:22
172.16.4.4 110 00:06:07
Distance: (default is 110)
R1#
```

Dari informasi routing diatas, R1 menjalankan OSPF dengan proses ID 1. Ada 4 network yang diroutingkan oleh R1. Administrative distance 110. R1 memiliki router ID 172.16.2.2.

R1 memiliki neighbor 172.16.4.4 (IP Loopback R2) . 172.16.4.4 merupakan router-ID R2.

**Note:** ulangi langkah yang sama diatas untuk menampilkan informasi neighbor dan informasi routing protocol di R2

## Tampilkan informasi database OSPF di R1

```
R1#show ip ospf database
OSPF Router with ID (172.16.2.2) (Process ID 1)

Router Link States (Area 0)

Link ID ADV Router Age Seq# Checksum Link count
172.16.2.2 172.16.2.2 472 0x80000005 0x00e483 4
172.16.4.4 172.16.4.4 397 0x80000004 0x00ba9c 4

Net Link States (Area 0)
Link ID ADV Router Age Seq# Checksum
12.12.12.1 172.16.2.2 472 0x80000001 0x00720b
R1#
```

Di area 0 hanya terdapat 2 router dengan ID : 172.16.2.2 dan 172.16.4.4.

## Tes Ping dari Laptop1 ke Laptop2

```
Laptop1>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=126
Reply from 192.168.2.1: bytes=32 time=1ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126

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 = 1ms, Average = 0ms
```

Ping dari Laptop1 ke Laptop2 berhasil.

## Traceroute dari Laptop1 ke Laptop2

```
Laptop1>tracert 192.168.2.1

Tracing route to 192.168.2.1 over a maximum of 30 hops:

1 1 ms 0 ms 0 ms 192.168.1.254
2 0 ms 0 ms 0 ms 12.12.12.2
3 0 ms 0 ms 0 ms 192.168.2.1

Trace complete.
```

Untuk menuju Laptop2 dari Laptop1 membutuhkan 3 hop.

## Tes Ping dari Laptop2 ke Laptop1

```
Laptop2>ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126
Reply from 192.168.1.1: bytes=32 time=11ms TTL=126
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
```

```
Ping statistics for 192.168.1.1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

## Traceroute dari Laptop2 ke Laptop1

```
Laptop2>tracert 192.168.1.1
```

```
Tracing route to 192.168.1.1 over a maximum of 30 hops:
```

```
1 1 ms 0 ms 0 ms 192.168.2.254
2 0 ms 0 ms 0 ms 12.12.12.1
3 1 ms 11 ms 11 ms 192.168.1.1
```

```
Trace complete.
```

## Tampilkan routing table spesifik OSPF di R1 dan R2

```
R1#show ip route ospf
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O 172.16.3.3 [110/2] via 12.12.12.2, 00:05:11, FastEthernet1/0
O 172.16.4.4 [110/2] via 12.12.12.2, 00:05:11, FastEthernet1/0
O 192.168.2.0 [110/2] via 12.12.12.2, 00:04:20, FastEthernet1/0
R1#
```

```
R2#show ip route ospf
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O 172.16.1.1 [110/2] via 12.12.12.1, 00:05:05, FastEthernet1/0
O 172.16.2.2 [110/2] via 12.12.12.1, 00:05:05, FastEthernet1/0
O 192.168.1.0 [110/2] via 12.12.12.1, 00:05:05, FastEthernet1/0
R2#
```

## Debug OSPF di R1

```
05:53:59: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.4.4 on FastEthernet1/0 from
LOADING to FULL, Loading Done
```

Setelah selesai setting OSPF di R2 step **Halaman 53**, di R1 maupun R2 akan muncul output **adjacent router** OSPF. Dari output debug OSPF diatas R1 memiliki neighbor 172.16.4.4. 172.16.4.4 adalah router ID dari R2. Berarti R1 dan R2 telah menjalin relationship neighbor (adjacency) sehingga routing update akan saling dikirimkan.

## Setting router-id OSPF di R1

```
R1(config)#router ospf 1
R1(config-router)#router-id 111.111.111.111
R1(config-router)#Reload or use "clear ip ospf process" command, for this to
take effect
R1(config-router)#

```

## Setting router-id OSPF di R2

```
R2(config)#router ospf 1
R2(config-router)#router-id 222.222.222.222
R2(config-router)#Reload or use "clear ip ospf process" command, for this to
take effect
R2(config-router)#

```

Setelah menjalankan command **router-id** diatas, jalankan command **clear ip ospf process** untuk mereset proses OSPF di R1 maupun R2, sehingga router-id OSPF akan berubah.

```
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

R1#
06:12:37: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.4.4 on FastEthernet1/0 from FULL
to DOWN, Neighbor Down: Adjacency forced to reset

06:12:37: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.4.4 on FastEthernet1/0 from FULL
to DOWN, Neighbor Down: Interface down or detached

R1#
06:12:41: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.4.4 on FastEthernet1/0 from
LOADING to FULL, Loading Done

```

## Tampilkan neighbor table OSPF di R1

```
R1#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
222.222.222.222 1 FULL/DR 00:00:36 12.12.12.2 FastEthernet1/0
R1#

```

Dari output neighbor table di R1, bisa kita lihat di kolom neighbor ID terdapat 222.222.222.222, dimana 222.222.222.222 adalah router-id R2. Dengan demikian, setting router-id OSPF di R2 telah berhasil.

**Note:** ulangi langkah yang sama diatas untuk mereset process OSPF dan tampilkan neighbor table OSPF di R2, pastikan neighbor ID R1 111.111.111.111

## Setting passive-interface OSPF di R1

```
R1(config)#router ospf 1
R1(config-router)#passive-interface fa0/0
R1(config-router) #
```

## Tampilkan routing information OSPF di R1

```
R1#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 111.111.111.111
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
12.12.12.0 0.0.0.255 area 0
172.16.1.0 0.0.0.255 area 0
172.16.2.0 0.0.0.255 area 0
192.168.1.0 0.0.0.255 area 0
Passive Interface(s):
FastEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
111.111.111.111 110 00:11:04
172.16.2.2 110 00:30:11
172.16.4.4 110 00:11:38
222.222.222.222 110 00:11:04
Distance: (default is 110)
```

Passive-interface fa0/0 telah berhasil ditambahkan di OSPF R1.

## Tampilkan interface OSPF di R1

```
R1#show ip ospf interface

FastEthernet1/0 is up, line protocol is up
Internet address is 12.12.12.1/24, Area 0
Process ID 1, Router ID 111.111.111.111, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 222.222.222.222, Interface address 12.12.12.2
Backup Designated Router (ID) 111.111.111.111, Interface address 12.12.12.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 222.222.222.222 (Designated Router)
```

```

Suppress hello for 0 neighbor(s)

Loopback1 is up, line protocol is up
Internet address is 172.16.1.1/24, Area 0
Process ID 1, Router ID 111.111.111.111, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host

Loopback2 is up, line protocol is up
Internet address is 172.16.2.2/24, Area 0
Process ID 1, Router ID 111.111.111.111, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host

FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.254/24, Area 0
Process ID 1, Router ID 111.111.111.111, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
Index 4/4, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

**Passive-interface** OSPF memiliki kemiripan dengan EIGRP. Dengan mengaktifkan **passive-interface** di interface OSPF, maka akan menghentikan pengiriman paket hello sehingga akan mencegah router membentuk relationship neighbor antar router, akibatnya router akan berhenti melakukan update outgoing dan incoming (tidak dapat mengirimkan update routing dan tidak dapat dikirimi update routing).

OSPF dan EIGRP sama-sama menggunakan paket hello sebelum membentuk relationship antar router. Perhatikan informasi interface OSPF Fa0/0 dan Fa1/0 R1 diatas. Fa0/0 sudah diaktifkan command **passive-interface** sehingga tidak ada lagi paket hello. Beda dengan Fa1/0 yang ada keterangan **Hello due in..**

```

FastEthernet0/0 is up, line protocol is up
No Hellos (Passive interface)

```

```

FastEthernet1/0 is up, line protocol is up
Hello due in 00:00:07

```

Karena Network A dan Network B merupakan jaringan LAN dimana tidak membutuhkan relationship neighbor antar router OSPF sehingga tidak jadi masalah ketika interface Fa0/0 diaktifkan command **passive-interface**-nya. Lain halnya dengan interface Fa1/0 ketika diaktifkan command **passive-interface**, maka akan menimbulkan masalah yaitu R1 tidak dapat membentuk relationship dengan R2, sehingga OSPF tidak dapat berjalan normal.

OSPF secara default memiliki hello interval = 10 second, dan dead interval = 40 second.

## Interface Loopback di OSPF

Perhatikan sekali lagi output routing table di R1 dan R2. Apakah ada masalah dengan interface loopback?

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Loopback1
C 172.16.2.0/24 is directly connected, Loopback2
O 172.16.3.3/32 [110/2] via 12.12.12.2, 00:38:50, FastEthernet1/0
O 172.16.4.4/32 [110/2] via 12.12.12.2, 00:38:50, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
O 192.168.2.0/24 [110/2] via 12.12.12.2, 00:38:50, FastEthernet1/0
```

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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
```

```
12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O 172.16.1.1/32 [110/2] via 12.12.12.1, 00:41:42, FastEthernet1/0
O 172.16.2.2/32 [110/2] via 12.12.12.1, 00:41:42, FastEthernet1/0
C 172.16.3.0/24 is directly connected, Loopback3
C 172.16.4.0/24 is directly connected, Loopback4
O 192.168.1.0/24 [110/2] via 12.12.12.1, 00:41:42, FastEthernet1/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R2#
```

Dari output **show ip ospf interface Halaman 60** dan **show ip route Halaman 61** kita bisa lihat bahwa loopback yang sebelumnya kita buat untuk tujuan imitasi subnet atau testing menjadi sebuah network sendiri di R1 maupun di R2 berubah menjadi stub host dengan prefix /32 dan network type LOOPBACK.

```
Loopback1 is up, line protocol is up
.
Process ID 1, Router ID 111.111.111.111, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host

Loopback2 is up, line protocol is up
.
Process ID 1, Router ID 111.111.111.111, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host

Loopback3 is up, line protocol is up
.
Process ID 1, Router ID 222.222.222.222, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host

Loopback4 is up, line protocol is up
.
Process ID 1, Router ID 222.222.222.222, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host

O 172.16.3.3/32 [110/2] via 12.12.12.2, 00:38:50, FastEthernet1/0
O 172.16.4.4/32 [110/2] via 12.12.12.2, 00:38:50, FastEthernet1/0

O 172.16.1.1/32 [110/2] via 12.12.12.1, 00:41:42, FastEthernet1/0
O 172.16.2.2/32 [110/2] via 12.12.12.1, 00:41:42, FastEthernet1/0
```

Semua loopback, yaitu Loopback1, Loopback2, Loopback3, Loopback4 menjadi stub host dengan network type LOOPBACK. Stub host memang tampil di routing table dengan prefix /32, akan tetapi tidak dapat digunakan untuk forwarding.

Agar semua loopback dapat di advertise oleh OSPF sebagai network dengan prefix aslinya yaitu /24, caranya dengan mengubah network type loopback menjadi point-to-point.

### Ubah Network Type Interface Loopback OSPF di R1 dan R2

```
R1(config)#interface lo1
R1(config-if)#ip ospf network point-to-point
R1(config-if)#
R1(config-if)#interface lo2
R1(config-if)#ip ospf network point-to-point
R1(config-if)#

```

```
R2(config)#interface lo3
R2(config-if)#ip ospf network point-to-point
R2(config-if)#
R2(config-if)#interface lo4
R2(config-if)#ip ospf network point-to-point
R2(config-if)#

```

## Tampilkan routing table OSPF terupdate di R1 dan R2

```
R1#show ip route
```

Codes: C - connected, S - static, I - IGRP, 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

```
12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 4 subnets
C 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
O 172.16.3.0 [110/2] via 12.12.12.2, 00:01:00, FastEthernet1/0
O 172.16.4.0 [110/2] via 12.12.12.2, 00:00:50, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
O 192.168.2.0/24 [110/2] via 12.12.12.2, 01:17:07, FastEthernet1/0
R1#
```

```
R2#show ip route
```

Codes: C - connected, S - static, I - IGRP, 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

```
12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/24 is subnetted, 4 subnets
O 172.16.1.0 [110/2] via 12.12.12.1, 00:04:33, FastEthernet1/0
O 172.16.2.0 [110/2] via 12.12.12.1, 00:04:23, FastEthernet1/0
C 172.16.3.0 is directly connected, Loopback3
C 172.16.4.0 is directly connected, Loopback4
O 192.168.1.0/24 [110/2] via 12.12.12.1, 01:18:04, FastEthernet1/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

Dari output diatas, semua loopback telah diadvertis sebagai network dengan prefix /24. Selanjutnya kita akan tes Ping dari Loopback1 di R1 ke Loopback3 di R2.

## Tes Ping dari Loopback1 di R1 ke Loopback3 di R2

Untuk mencoba tes Ping dari Loopback, gunakan extended-ping di router.

```
R1#ping
Protocol [ip]: ip
Target IP address: 172.16.3.3
Repeat count [5]: [ENTER]
Datagram size [100]: [ENTER]
Timeout in seconds [2]: [ENTER]
Extended commands [n]: y
Source address or interface: loopback1
Type of service [0]: [ENTER]
Set DF bit in IP header? [no]: [ENTER]
Validate reply data? [no]: [ENTER]
Data pattern [0xABCD]: [ENTER]
Loose, Strict, Record, Timestamp, Verbose[none] :
Sweep range of sizes [n]: [ENTER]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

**Note:** ulangi langkah yang sama diatas untuk tes Ping dari Loopback4 di R2 ke Loopback2 di R1.

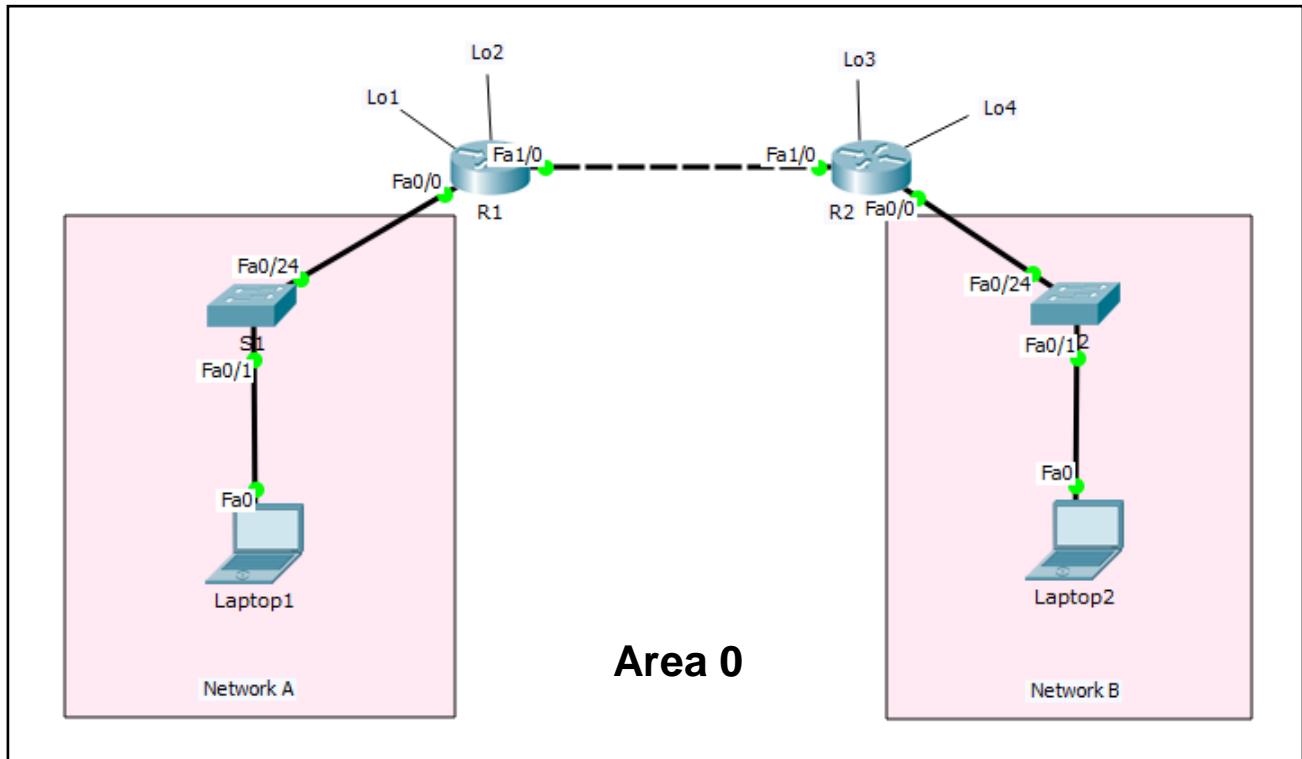
## Review

1. Jelaskan bagaimana mekanisme pemilihan router-id OSPF?
2. Apa yang terjadi jika router memiliki router-id yang sama dengan router yang lain dalam satu area yang sama?
3. Untuk membentuk relationship neighbor antar router di OSPF, apa sajakah kriteria yang diperlukan ? Isi **Ya** atau **Tidak** table dibawah ini.

Requirement	OSPF
Status interface harus UP UP	
Interface harus berada pada subnet yang sama	
Harus lolos autentikasi (jika disetting autentikasinya)	
Harus menggunakan ASN yang sama disettingan command <b>router ospf</b>	
Hello dan hold/dead timers harus sama	
IP MTU harus sama	
Router ID harus unik	
K-values harus sama	
Harus berada dalam area yang sama	

# Lab 9. ACL Standard

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting ACL Standard

## Konsep Dasar

Karakteristik ACL secara umum

- Menentukan tipe traffic yang akan di control
- Menentukan karakteristik traffic
- Mengidentifikasi traffic dengan permit atau deny
- Dapat men-denry traffic spesifik atau secara keseluruhan
- **Terdapat implisit deny any pada akhir baris access list secara default**
- Masing-masing baris hanya untuk satu protokol spesifik
- Masing-masing interface router maksimal hanya punya dua access list untuk masing-masing protocol, satu incoming traffic dan satu outgoing traffic
- Ketika access list di assign untuk interface, tentukan apakah untuk incoming atau outgoing
- Access list sifatnya global di router, tapi filter traffic hanya berlaku di interface yang di assign access list
- Masing-masing access list dapat di assign ke beberapa interface
- Akan tetapi tiap interface hanya boleh satu incoming dan satu outgoing
- Access list dapat digunakan untuk nge-log traffic yang match dengan access list statement
- Access list yang di applied ke inbound traffic dilakukan sebelum routing decision
- Access list yang di applied ke outbound traffic dilakukan setelah routing decision
- Ketikkan rule access list secara berurutan, dengan statement paling restrictive berada di atas

### ACL Standard

1. Nomor : 1-99
2. Digunakan untuk filter source IP address
3. Permit / Deny semua protocol suite TCP/IP
4. Tips : **assign pada router yang terdekat dengan destination (close to the destination router)**

### Konfigurasi ACL

Untuk melakukan setting ACL di router, pertama setting rule ACL terlebih dahulu di mode global router, kemudian langkah kedua assign rule ACL tersebut di interface.

```
Router(config)# access-list 1 permit/deny source hostname/ip/network
Router(config)# access-list 1 permit/deny any

Router(config)# interface fa0/0
Router(config)# ip access-group 1 in/out
```

### Contoh Konfigurasi ACL

Rule ACL : allow akses VTY line 0-4 dari internal network 192.168.1.0/24 :

```
Router(config)# access-list 12 permit 192.168.1.0 0.0.0.255
Router(config)# line vty 0 4
Router(config)# access-class 12 .in
```

Untuk menyatakan match sebuah host bisa menggunakan 2 cara :

- Dengan wildcard mask “0.0.0.0”, misal 192.168.1.1 0.0.0.0
- Dengan keyword “host”, misal host 192.168.1.1

**Untuk menyatakan match semua host bisa menggunakan 2 cara :**

- Dengan wildcard mask “255.255.255.255”, misal 0.0.0.0 255.255.255.255
- Dengan keyword “any”, misal any source atau destination

## **Konfigurasi**

Login console ke R1 atau R2 untuk mempraktikkan **Lab 9-ACL Standard**.

Sebelum menerapkan ACL, setting OSPF Area 0 terlebih dahulu topologi diatas. Lihat solution **Lab 8-OSPF**.

**#1. Buat rule ACL standard seperti dibawah ini:**

1. Deny host 192.168.1.1 berkomunikasi dengan network 192.168.2.0
2. Deny network 172.16.1.0 berkomunikasi dengan network 192.168.2.0
3. Permit semua trafik lainnya

Gunakan ACL number 1 untuk rule 1-3 diatas.

**Tampilkan ipconfig Lapopt1 sebelum disetting ACL**

```
Laptop1>ipconfig
FastEthernet0 Connection: (default port)
Link-local IPv6 Address.....: FE80::201:43FF:FE3A:AEC2
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.254
```

**Laptop1 dapat melakukan tes Ping ke Laptop2 yang berada di network 192.168.2.0**

```
Laptop1>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=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126

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 = 1ms, Average = 0ms
```

**Setting ACL Standar di R2**

```
R2(config)#access-list 1 deny 192.168.1.1 0.0.0.0
R2(config)#access-list 1 deny 172.16.1.0 0.0.0.255
R2(config)#access-list 1 permit any
```

ACL telah disetting di R2 sesuai urutan rule nomor 1-3 di atas. Mengapa menempatkan ACL-nya di R2? Agar rule tersebut berjalan normal saat di eksekusi, maka kita taruh di dekat router tujuan. Ingat konsep ACL standar : **close to the destination router**.

Setelah mensetting rule ACL di R2, langkah selanjutnya yaitu menempatkan ACL tersebut di interface agar bekerja efektif. ACL ditempatkan di interface outgoing menuju network 192.168.2.0.

### Apply ACL di Interface Fa0/0 R2

```
R2(config)#interface fa0/0
R2(config-if)#ip access-group 1 out
```

### Verifikasi

#### Tampilkan access-list standard yang sudah dibuat di R2

```
R2#show access-list
Standard IP access list 1
10 deny host 172.16.1.1
20 deny 192.168.1.0 0.0.0.255
30 permit any
R2#
```

#### Tes Ping dari Laptop1 ke Laptop2

```
Laptop1>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 12.12.12.2: Destination host unreachable.

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

ACL sudah berjalan sesuai dengan rule diatas bahwa host 192.168.1.1 tidak boleh berkomunikasi dengan network 192.168.2.0. Kemudian kita akan tes dengan IP selain 192.168.1.1.

#### Tes Ping dari Laptop1 ke Laptop2 dengan mengubah IP address Laptop1 selain 192.168.1.1

```
Laptop1>ipconfig
FastEthernet0 Connection: (default port)
Link-local IPv6 Address.....: FE80::201:43FF:FE3A:AEC2
IP Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.254
```

```

Laptop1>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=11ms TTL=126
Reply from 192.168.2.1: bytes=32 time=11ms TTL=126
Reply from 192.168.2.1: bytes=32 time=1ms TTL=126
Reply from 192.168.2.1: bytes=32 time=0ms TTL=126

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 = 11ms, Average = 5ms

```

Dengan IP 192.168.1.3 ternyata berhasil tes Ping host yang berada di network 192.168.2.0. Dengan demikian rule ACL baris ke-1 sudah berhasil memfilter host 192.168.1.1 saat mengakses network 192.168.2.0.

### Tes Ping dari Loopback1 ke Laptop2

```

R1#ping
Protocol [ip]: [ENTER]
Target IP address: 192.168.2.1
Repeat count [5]: [ENTER]
Datagram size [100]: [ENTER]
Timeout in seconds [2]: [ENTER]
Extended commands [n]: y
Source address or interface: loopback1
Type of service [0]: [ENTER]
Set DF bit in IP header? [no]: [ENTER]
Validate reply data? [no]: [ENTER]
Data pattern [0xABCD]: [ENTER]
Loose, Strict, Record, Timestamp, Verbose[none]: [ENTER]
Sweep range of sizes [n]: [ENTER]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
UUUUU
Success rate is 0 percent (0/5)

```

Tes Ping dari Loopback1 ke Laptop2 hasilnya 0 percent dan ditampilkan kode U (unreachable). Berarti rule ACL baris ke-2 sudah berhasil.

Untuk verifikasi rule ACL baris ke-3 yaitu permit semua trafik lainnya, kita akan mencoba tes Ping dari Loopback2 ke Laptop2 dengan extended ping.

```

R1#ping
Protocol [ip]: [ENTER]
Target IP address: 192.168.2.1
Repeat count [5]: [ENTER]
Datagram size [100]: [ENTER]
Timeout in seconds [2]: [ENTER]
Extended commands [n]: y
Source address or interface: loopback2
Type of service [0]: [ENTER]
Set DF bit in IP header? [no]: [ENTER]
Validate reply data? [no]: [ENTER]
Data pattern [0xABCD]: [ENTER]
Loose, Strict, Record, Timestamp, Verbose[none]: [ENTER]
Sweep range of sizes [n]: [ENTER]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

```

Dari hasil tes Ping extended dari Loopback2 ke Laptop2 memberikan success rate 100%. Berarti rule ACL baris ke-3 sudah berhasil diimplementasikan.

### Tampilkan interface access-list standard di R2

```

R2#show ip interface fa0/0
FastEthernet0/0 is up, line protocol is up (connected)
Internet address is 192.168.2.254/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is 1
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
...

```

Dari output interface access-list diatas, di Fa0/0 R2 terdapat outgoing access-list dengan number 1.

## #2. Buat rule ACL standard seperti dibawah ini untuk R1:

1. Deny host 192.168.2.1 berkomunikasi dengan network 192.168.1.0
2. Deny network 172.16.3.0 berkomunikasi dengan network 192.168.1.0
3. Permit semua trafik lainnya

Untuk mempraktikkan rule ACL standard diatas, hapus ACL yang telah disetting di R2. Cara menghapus rule ACL dengan command : `no access-list [number-acl]`. Dan hapus juga di interface yang dipasang ACL dengan command : `no ip access-group [number-acl] out`.

**Note: ulangi langkah yang sama seperti di Halaman 67 untuk menerapkan ACL di R1 sesuai dengan rule #2 diatas.**

## Review

1. Jika ada kesalahan penulisan rule di numbered ACL standar, bagaimana cara melakukan pengeditan rule-nya?
2. Jelaskan perbedaan antara numbered ACL dan named ACL?
3. Praktikkan rule ACL diatas (#1 maupun #2) menggunakan named ACL secara bergantian?
4. Buatlah rule ACL dibawah ini di R1 maupun R2 dan aplikasikan rule ACL tersebut di R1 maupun R2? Verifikasi rule tersebut dengan mencoba akses telnet dari Laptop1 dan Laptop2.

### R1

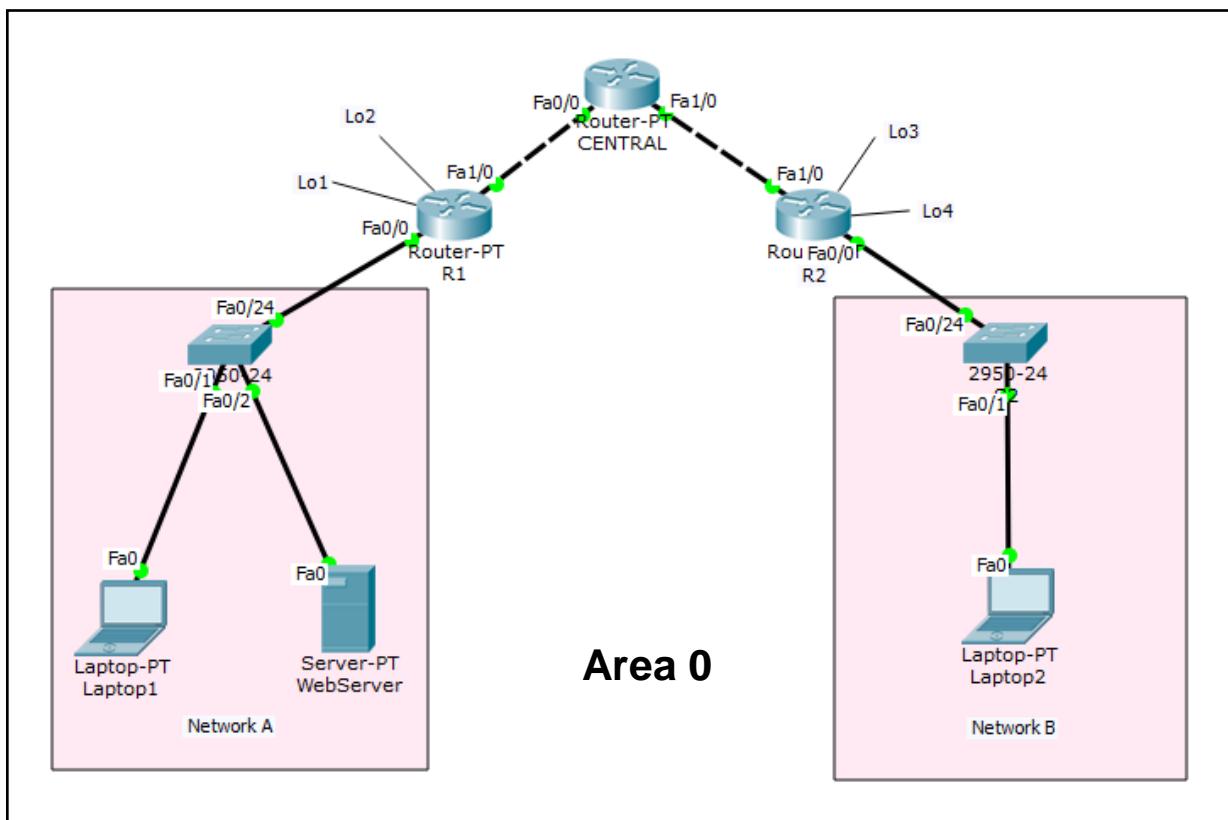
- Hanya Laptop2 yang boleh akses telnet R1
- Host lainnya tidak diperbolehkan akses telnet R1

### R2

- Hanya Laptop1 yang boleh akses telnet R2
- Host lainnya tidak diperbolehkan akses telnet R2

# Lab 10. ACL Extended

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	10.10.10.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	20.20.20.1	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
CENTRAL	Fa0/0	10.10.10.2	255.255.255.0	N/A
	Fa1/0	20.20.20.2	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254
WebServer	NIC	192.168.1.11	255.255.255.0	192.168.1.254

## Tujuan

- Setting ACL Extended

## Konsep Dasar

Karakteristik ACL secara umum

- Menentukan tipe traffic yang akan di control
- Menentukan karakteristik traffic
- Mengidentifikasi traffic dengan permit atau deny
- Dapat men-denry traffic spesifik atau secara keseluruhan
- ***Terdapat implisit deny any pada akhir baris access list secara default***
- Masing-masing baris hanya untuk satu protokol spesifik
- Masing-masing interface router maksimal hanya punya dua access list untuk masing-masing protocol, satu incoming traffic dan satu outgoing traffic
- Ketika access list di assign untuk interface, tentukan apakah untuk incoming atau outgoing
- Access list sifatnya global di router, tapi filter traffic hanya berlaku di interface yang di assign access list
- Masing-masing access list dapat di assign ke beberapa interface
- Akan tetapi tiap interface hanya boleh satu incoming dan satu outgoing
- Access list dapat digunakan untuk nge-log traffic yang match dengan access list statement
- Access list yang di applied ke inbound traffic dilakukan sebelum routing decision
- Access list yang di applied ke outbound traffic dilakukan setelah routing decision
- Ketikkan rule access list secara berurutan, dengan statement paling restrictive berada di atas

## **ACL Extended**

1. Nomor : 100-199
2. Digunakan untuk filter source dan destination IP address
3. Dapat memfilter spesifik protocol IP dan port number
4. Tips : **assign pada router yang terdekat dengan source (close to the source router)**

## **Konfigurasi ACL**

Untuk melakukan setting ACL di router, pertama setting rule ACL terlebih dahulu di mode global router, kemudian langkah kedua assign rule ACL tersebut di interface.

```
Router(config)# access-list 100 permit/deny protocol source_IP destination_IP
Router(config)# access-list 100 permit/deny protocol source_IP port
destination_IP port
Router(config)# access-list 100 permit/deny protocol any any

Router(config)# interface fa0/0
Router(config)# ip access-group 1 in/out
```

**Untuk menyatakan match sebuah host bisa menggunakan 2 cara :**

- Dengan wildcard mask “0.0.0.0”, misal 192.168.1.1 0.0.0.0
- Dengan keyword “host”, misal host 192.168.1.1

**Untuk menyatakan match semua host bisa menggunakan 2 cara :**

- Dengan wildcard mask “255.255.255.255”, misal 0.0.0.0 255.255.255.255
- Dengan keyword “any”, misal any source atau destination

## **Konfigurasi**

Login console ke R1 atau R2 untuk mempraktikkan **Lab 10-ACL Extended**.

Sebelum menerapkan ACL, setting OSPF Area 0 terlebih dahulu topologi diatas. Lihat solution **Lab 8-OSPF**.

**#1. Buat rule ACL extended seperti dibawah ini:**

1. Allow host 192.168.2.1 mengakses service SSH R1
2. Allow network R2 mengakses service HTTP ke mana saja
3. Deny semua trafik lainnya

Gunakan ACL number 100 untuk rule 1-3 diatas.

**Tampilkan ipconfig Laptop2 sebelum disetting ACL**

```
Laptop2>ipconfig
FastEthernet0 Connection: (default port)
Link-local IPv6 Address.....: FE80::260:2FFF:FE42:A6D3
IP Address.....: 192.168.2.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.254
```

**Laptop2 dapat melakukan tes Ping ke Laptop1 yang berada di network 192.168.1.0**

```
Laptop2>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=13ms TTL=125
Reply from 192.168.1.1: bytes=32 time=12ms TTL=125
Reply from 192.168.1.1: bytes=32 time=13ms TTL=125
Reply from 192.168.1.1: bytes=32 time=7ms TTL=125

Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 7ms, Maximum = 13ms, Average = 11ms
```

**Setting ACL Extended di R2**

```
R2(config)#access-list 100 permit tcp host 192.168.2.1 host 10.10.10.1 eq 22
R2(config)#access-list 100 permit tcp any any eq 80
```

ACL telah disetting di R2 sesuai urutan rule nomor 1-3 di atas. Mengapa menempatkan ACL-nya di R2? Agar rule tersebut berjalan normal saat di eksekusi, maka kita taruh di dekat router source. Ingat konsep ACL extended : **close to the source router**. Karena **implicit deny** ada dibaris terakhir ACL, maka kita tidak perlu menuliskan rule ACL tersebut.

Setelah mensetting rule ACL di R2, langkah selanjutnya yaitu menempatkan ACL tersebut di interface agar bekerja efektif. Rule ACL ditempatkan di interface outgoing menuju network luar di Fa1/0 R2.

### Apply ACL di Interface Fa1/0 R2

```
R2(config)#interface fa1/0
R2(config-if)#ip access-group 100 out
```

### Verifikasi

#### Tampilkan access-list extended yang sudah dibuat di R2

```
R2#show access-list
Extended IP access list 100
10 permit tcp host 192.168.2.1 host 10.10.10.1 eq 22
20 permit tcp any any eq www
R2#
```

#### Tes Ping dari Laptop2 ke Laptop1

```
Laptop2>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.2.254: Destination host unreachable.

Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ACL sudah berjalan sesuai dengan rule nomer 3 diatas, deny semua traffic lainnya termasuk ping dari Laptop2 ke Laptop1. Perhatikan yang memberikan reply dari router R2 (192.168.2.254).

#### Tes Ping dari Laptop2 ke Laptop1 dengan mengubah IP address Laptop2 selain 192.168.2.1

```
Laptop2>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::260:2FFF:FE42:A6D3
IP Address.....: 192.168.2.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.254
```

```
Laptop2>ping 192.168.1.1  
  
Pinging 192.168.1.1 with 32 bytes of data:  
  
Reply from 192.168.2.254: Destination host unreachable.  
  
Ping statistics for 192.168.1.1:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Dengan IP 192.168.2.3 ternyata tidak berhasil tes Ping host yang berada di network 192.168.1.0.

### Tes Ping dari Laptop2 ke R1

```
Laptop2>ping 10.10.10.1  
  
Pinging 10.10.10.1 with 32 bytes of data:  
  
Reply from 192.168.2.254: Destination host unreachable.  
  
Ping statistics for 10.10.10.1:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Tes Ping dari Laptop2 ke R1 gagal.

### Tes Ping dari Laptop2 ke router CENTRAL

```
Laptop2>ping 20.20.20.2  
  
Pinging 20.20.20.2 with 32 bytes of data:  
  
Reply from 192.168.2.254: Destination host unreachable.  
  
Ping statistics for 20.20.20.2:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Dari hasil tes Ping Laptop2 ke router CENTRAL juga gagal.

## Tampilkan interface access-list extended di R2

```
R2#show ip interface fa1/0
FastEthernet1/0 is up, line protocol is up (connected)
Internet address is 20.20.20.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is 100
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
...
...
```

Dari output interface access-list diatas, di Fa1/0 R2 terdapat outgoing access-list dengan number 100.

## Tampilkan Akses SSH dari Laptop2 ke R1

```
Laptop2>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::260:2FFF:FE42:A6D3
IP Address.....: 192.168.2.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.254

PC>
```

```
Laptop2>ssh -l admin 10.10.10.1
```

```
Open
```

```
Password:
```

```
Unauthorized access prohibited!
```

```
R1>enable
```

```
Password:
```

```
R1#
```

```
R1#
```

Akses SSH dari Laptop2 ke R1 berhasil. Hal ini sesuai dengan rule ACL extended nomer 1.

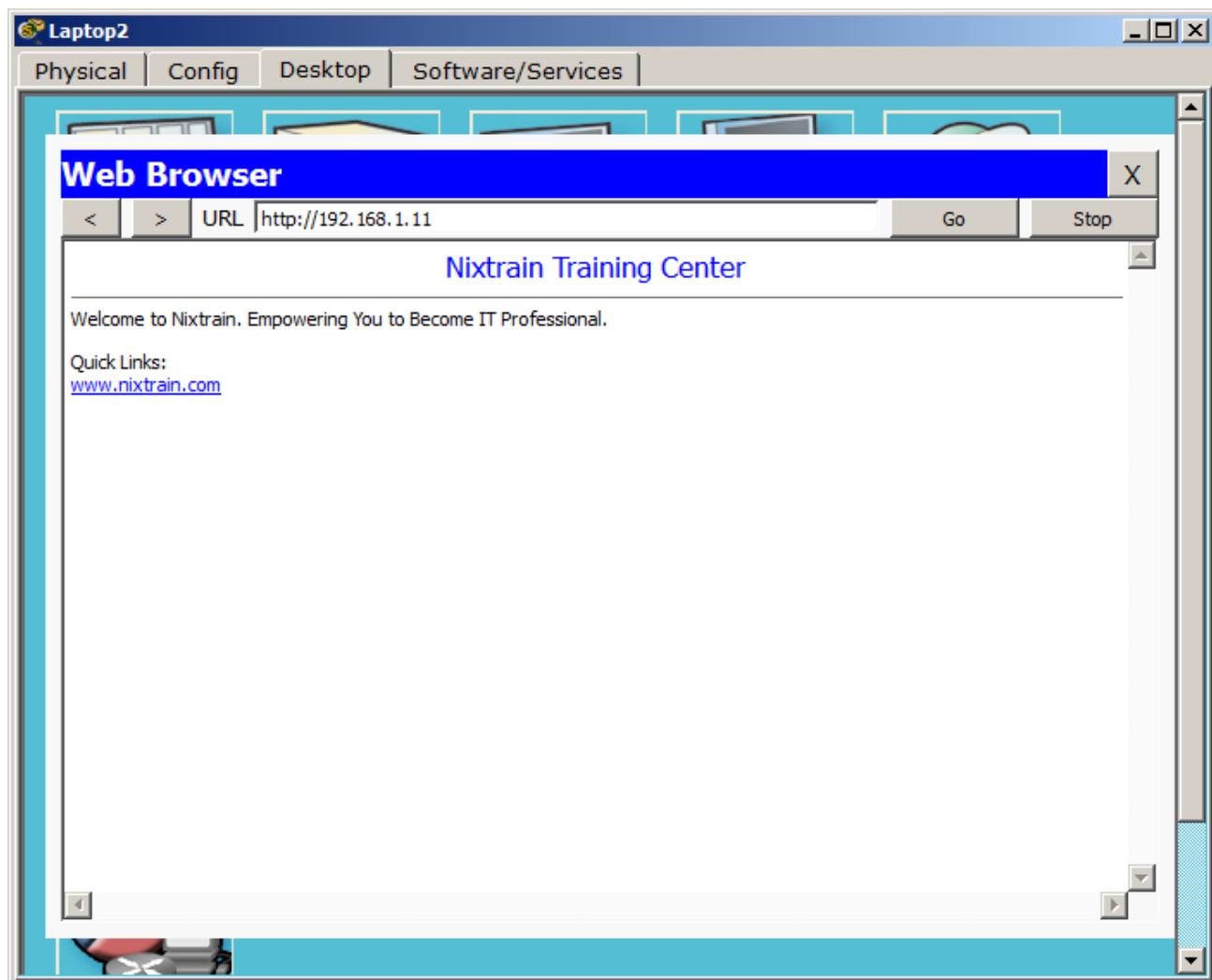
#### Tampilkan access-list extended setelah di jalankan akses SSH ke R1

```
R2#show access-list
Extended IP access list 100
10 permit tcp host 192.168.2.1 host 10.10.10.1 eq 22 (154 match(es))
20 permit tcp any any eq www
R2
```

Perhatikan pada baris pertama rule ACL terdapat 154 match(es) artinya jumlah **attempt** yang match dengan rule baris ke-1 dimana Laptop2 diperbolehkan mengakses service SSH ke R1. Jumlah match akan terus naik seiring dengan jumlah koneksi SSH dari Laptop2 ke R1.

#### Jalankan Web Browser di Laptop2 untuk Mengakses Web Server di Network A

Klik **Laptop2** -> Pilih tab **Desktop** -> Klik **Web Browser** -> Isikan IP Web Server : **192.168.1.11** -> ENTER.



Service HTTP WebServer berhasil diakses dari Laptop2. Coba ganti IP address Laptop2 selain 192.168.2.1, kemudian akses WebServer dan pastikan berhasil karena service HTTP memang diperbolehkan diakses dari network R2 mana saja.

## Tampilkan access-list extended setelah mengakses Web Server di R1

```
R2#show access-list
Extended IP access list 100
10 permit tcp host 192.168.2.1 host 10.10.10.1 eq 22 (155 match(es))
20 permit tcp any any eq www (11 match(es))
R2#
```

Dari output baris rule nomor 2 diatas, bagian akhir baris terdapat 11 match(es) artinya jumlah **attempt** yang dilakukan oleh **source any** ketika mengakses HTTP.

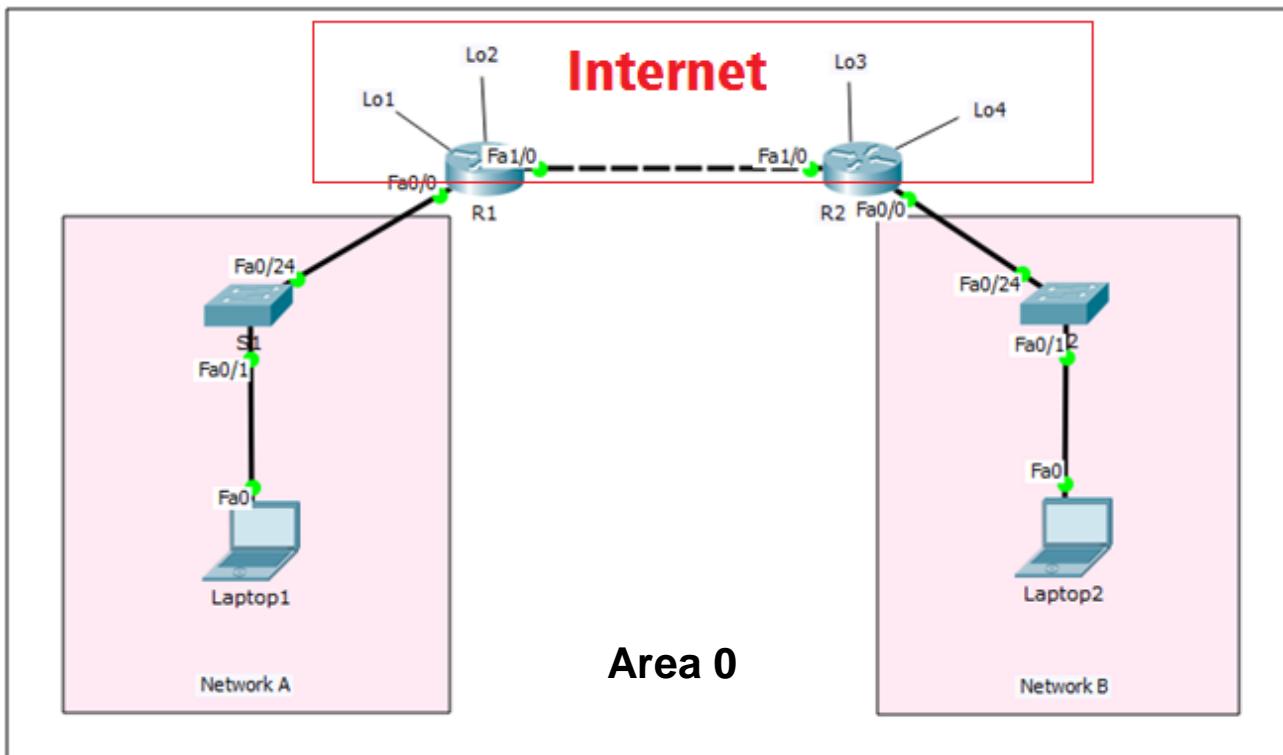
Dari informasi output **show access-list** dapat disimpulkan bahwa ACL yang telah kita buat sudah berhasil melewatkkan traffic SSH dan HTTP.

## Review

1. Praktikkan akses SSH dari Laptop2 ke router CENTRAL? Apakah berhasil atau tidak?
2. Apabila tidak berhasil, buatlah rule ACL agar akses SSH dari Laptop2 ke router CENTRAL dapat dilakukan?
3. Buatlah ACL dengan tipe named menggunakan rule ACL yang telah di lab-kan di Halaman 74?

# Lab 11. NAT Static

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting NAT Static

## Konsep Dasar

### Pengertian NAT

NAT adalah metode translasi IP private menjadi IP public. Agar dapat berkomunikasi dengan Internet kita harus terregistrasi menggunakan IP public.

### Tujuan NAT

- Mengurangi keterbatasan IPv4
- Menyembunyikan skema network internal

### Tipe NAT

1. NAT Static
2. NAT Dynamic
3. PAT (Port Address Translation)

### Terminologi NAT

1. **Inside Local Adress** : source address sebelum translasi (IP private)
2. **Outside Local Address** : destination address sebelum translasi (IP private)
3. **Inside Global Address** : inside host setelah translasi (IP public)
4. **Outside Global Address** : outside destination host setelah translasi (IP public)

### IP Private

Yaitu IP yang digunakan oleh organisasi secara internal dan tidak dapat dirutekan di Internet.

Class	Range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

- Perusahaan kecil biasanya mendapatkan IP public dari ISP
- ISP mendapatkan alokasi IP public dari IANA (Internet Assigned Numbers Authority)
- Device yang dapat melakukan translation biasanya berupa firewall, router, server.

### Keuntungan NAT

- Menghemat alamat IP secara legal
- Mengurangi overlap pengalaman
- Meningkatkan fleksibilitas ketika berkomunikasi ke internet
- Mengurangi pemotongan kembali jika terjadi perubahan network

### Kerugian NAT

- Terdapat delay pada proses switching
- Tidak dapat melakukan trace end-to-end IP
- Terdapat beberapa aplikasi yang tidak berfungsi ketika implementasi NAT

### NAT Static

- Termasuk jenis *one-to-one* NAT, satu IP private ditranslate menjadi satu IP public
- Ingat, untuk NAT static tiap host menggunakan IP public sendiri
- Bisa inisiasi komunikasi dari network outside global

## **Konfigurasi**

Login console ke R1 atau R2 untuk mempraktikkan **Lab 11-NAT Static**.

Untuk mempraktikkan konsep NAT Static ini, kita asumsikan bahwa area Internet menggunakan routing OSPF. Network A dan Network B pada R1 dan R2 tidak diadvertise oleh OSPF sehingga masuk Network Private, sehingga untuk mengakses Internet dibutuhkan NAT. Agar Network A dan Network B tidak diadvertise oleh OSPF berarti kita tidak perlu memasukkan Network A dan Network B pada command OSPF di R1 maupun R2.

### **Tampilan routing table R1**

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Loopback1
C 172.16.2.0/24 is directly connected, Loopback2
O 172.16.3.3/32 [110/2] via 12.12.12.2, 00:17:33, FastEthernet1/0
O 172.16.4.4/32 [110/2] via 12.12.12.2, 00:17:33, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

### **Tampilan routing table R2**

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O 172.16.1.1/32 [110/2] via 12.12.12.1, 00:18:24, FastEthernet1/0
O 172.16.2.2/32 [110/2] via 12.12.12.1, 00:18:24, FastEthernet1/0
C 172.16.3.0/24 is directly connected, Loopback0
C 172.16.4.0/24 is directly connected, Loopback1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

Dari output kedua routing table di R1 dan R2, sudah tidak terlihat lagi route menuju masing-masing Network A dan Network B.

**Tabel NAT R1**

Private IP	Public IP
192.168.1.1	12.12.12.11
192.168.1.2	12.12.12.22
192.168.1.3	12.12.12.33

**Tabel NAT R2**

Private IP	Public IP
192.168.2.1	12.12.12.44
192.168.2.2	12.12.12.55
192.168.2.3	12.12.12.66

Langkah sederhana setting NAT Static:

1. Tentukan interface NAT inside
2. Tentukan interface NAT outside
3. Buat translasi NAT dari source Private IP ke destination Public IP

### **Setting NAT Static di R1**

Command untuk mensetting NAT Static.

```
R1(config)#interface fa0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#interface fa1/0
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#exit
R1(config)#ip nat inside source static 192.168.1.1 12.12.12.11
R1(config)#ip nat inside source static 192.168.1.2 12.12.12.22
R1(config)#ip nat inside source static 192.168.1.3 12.12.12.33
R1(config)#+
```

## Setting NAT Static di R2

Command untuk mensetting NAT Static.

```
R2(config)#interface fa0/0
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#interface fa1/0
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#exit
R2(config)#
R2(config)#ip nat inside source static 192.168.2.1 12.12.12.44
R2(config)#ip nat inside source static 192.168.2.2 12.12.12.55
R2(config)#ip nat inside source static 192.168.2.3 12.12.12.66
R2(config)#+
```

## Verifikasi

### Tes Ping dari Laptop1 ke Lo3

```
Laptop1>ping 172.16.3.3

Pinging 172.16.3.3 with 32 bytes of data:

Reply from 172.16.3.3: bytes=32 time=1ms TTL=254
Reply from 172.16.3.3: bytes=32 time=0ms TTL=254
Reply from 172.16.3.3: bytes=32 time=1ms TTL=254
Reply from 172.16.3.3: bytes=32 time=0ms TTL=254

Ping statistics for 172.16.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

### Tes Ping dari Laptop1 ke Lo4

```
Laptop1>ping 172.16.4.4

Pinging 172.16.4.4 with 32 bytes of data:

Reply from 172.16.4.4: bytes=32 time=1ms TTL=254
Reply from 172.16.4.4: bytes=32 time=0ms TTL=254
Reply from 172.16.4.4: bytes=32 time=0ms TTL=254
Reply from 172.16.4.4: bytes=32 time=2ms TTL=254

Ping statistics for 172.16.4.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Dari tampilan diatas dapat diketahui bahwa Laptop1 yang berada di Private Network dapat berkomunikasi dengan Lo3 dan Lo4 yang berada di **Internet**.

## Tampilan NAT table di R1

```
R1#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 12.12.12.11:87 192.168.1.1:87 172.16.4.4:87 172.16.4.4:87
icmp 12.12.12.11:88 192.168.1.1:88 172.16.4.4:88 172.16.4.4:88
icmp 12.12.12.11:89 192.168.1.1:89 172.16.4.4:89 172.16.4.4:89
icmp 12.12.12.11:90 192.168.1.1:90 172.16.4.4:90 172.16.4.4:90
--- 12.12.12.11 192.168.1.1 --- ---
--- 12.12.12.22 192.168.1.2 --- ---
--- 12.12.12.33 192.168.1.3 --- ---

R1#
```

Dari tampilan NAT tabel di R1 dapat dilihat proses translasi dari host 192.168.1.1 menjadi 12.12.12.11. Sebelum packet di forward ke **Internet**, terlebih dahulu source host 192.168.1.1 diubah menjadi 12.12.12.11 agar bisa dikenal di **Internet**. Karena Private IP tidak dikenal di **Internet** dan tidak dirutekan di **Internet**.

**Note:** ulangi langkah verifikasi diatas untuk tes Ping dari Laptop2 ke Lo1 dan Lo2 dan tampilkan NAT table di R2.

## Traceroute dari Laptop1 ke Lo4

```
Laptop1>tracert 172.16.4.4
Tracing route to 172.16.4.4 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.1.254
2 0 ms 0 ms 0 ms 172.16.4.4

Trace complete.
```

Perhatikan hasil tracert dari Laptop1 ke Lo4.

Dimulai dari Laptop1 ke Gateway 192.168.1.254, kemudian source IP Laptop1 diubah menjadi 12.12.12.11 sehingga masuk ke directly connected network R1 dan R2, langsung di teruskan sampe di Lo4 (172.16.4.4).

## Traceroute dari Laptop2 ke Lo2

```
Laptop2>tracert 172.16.2.2
Tracing route to 172.16.2.2 over a maximum of 30 hops:
1 0 ms 1 ms 0 ms 192.168.2.254
2 * 0 ms 0 ms 172.16.2.2

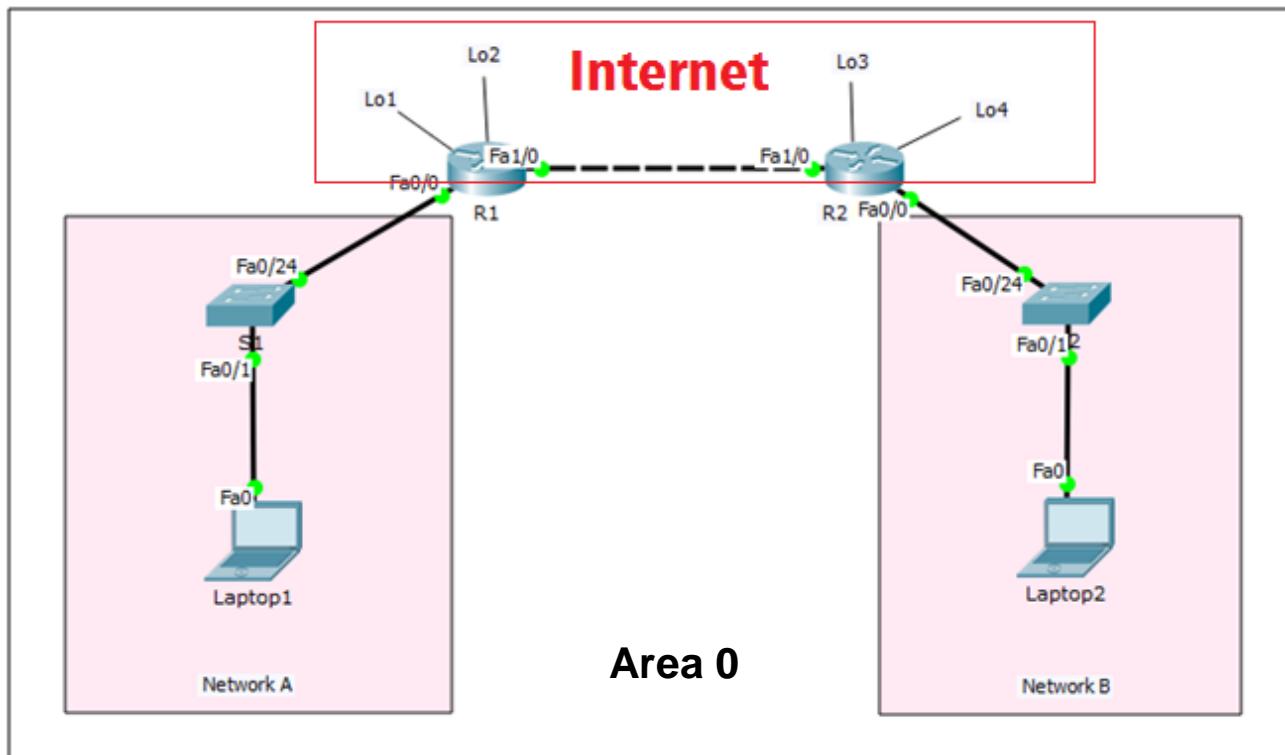
Trace complete.
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

## **Review**

1. Dengan konfigurasi NAT Static di R1 dan R2, apakah Laptop1 dapat melakukan tes Ping ke Laptop2 menggunakan Public IP yang dimiliki Laptop1 dan Laptop2?
2. Tambahkan WebServer pada Network A dan berikan IP address 192.168.1.3. Dengan asumsi NAT static telah disetting seperti pada Halaman 83, coba akses WebServer dari Laptop2 menggunakan IP Public yang telah diberikan untuk WebServer yaitu 12.12.12.33.
  - Apakah Laptop2 dapat mengakses WebServer di Network A?
  - Apakah Laptop2 dapat melakukan tes Ping ke WebServer di Network A?
3. Sebutkan kelebihan dan kekurangan NAT Static?

# Lab 12. NAT Dynamic

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting NAT Dynamic

## Konsep Dasar

### NAT Dynamic

- Termasuk tipe *many-to-many* NAT, IP private dalam jumlah banyak kemudian ditranslate menjadi IP public yang banyak juga dengan menyediakan sebuah pool IP public
- Kita tidak perlu melakukan translate satu per satu, cukup sediakan IP public sesuai jumlah user yang akan terkoneksi ke Internet

## Konfigurasi

Login console ke R1 atau R2 untuk mempraktikkan **Lab 12-NAT Dynamic**.

Untuk mempraktikkan konsep NAT Static ini, kita asumsikan bahwa area Internet menggunakan routing OSPF. Network A dan Network B pada R1 dan R2 tidak diadvertise oleh OSPF sehingga masuk Network Private, sehingga untuk mengakses Internet dibutuhkan NAT. Agar Network A dan Network B tidak diadvertise oleh OSPF berarti kita tidak perlu memasukkan Network A dan Network B pada command OSPF di R1 maupun R2.

### Tampilan routing table R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Loopback1
C 172.16.2.0/24 is directly connected, Loopback2
O 172.16.3.3/32 [110/2] via 12.12.12.2, 00:17:33, FastEthernet1/0
O 172.16.4.4/32 [110/2] via 12.12.12.2, 00:17:33, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

## Tampilan routing table R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O 172.16.1.1/32 [110/2] via 12.12.12.1, 00:18:24, FastEthernet1/0
O 172.16.2.2/32 [110/2] via 12.12.12.1, 00:18:24, FastEthernet1/0
C 172.16.3.0/24 is directly connected, Loopback0
C 172.16.4.0/24 is directly connected, Loopback1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

Dari output kedua routing table di R1 dan R2, sudah tidak terlihat lagi route menuju masing-masing Network A dan Network B. Oleh karena itu, agar Network A dan Network B bisa berkomunikasi dengan Internet langkah selanjutnya yaitu setting NAT.

### Pool NAT R1

Private IP (ACL 1)	Public IP (POOLR1)
192.168.1.0/24	12.12.12.11-12.12.12.20

### Pool NAT R2

Private IP (ACL 1)	Public IP (POOLR2)
192.168.2.0/24	12.12.12.21-12.12.12.30

Langkah sederhana setting NAT Dynamic:

1. Tentukan interface NAT inside
  2. Tentukan interface NAT outside
  3. Tentukan permit ACL Private Network
  4. Tentukan pool Public IP
  5. Buat translasi NAT dari source ACL ke destination pool Public IP

## Setting NAT Dynamic di R1

Command untuk mensetting NAT Dynamic.

```
R1(config)#interface fa0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#interface fa1/0
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#
R1(config)#ip nat pool POOLR1 12.12.12.11 12.12.12.20 netmask 255.255.255.0
R1(config)#
R1(config)#ip nat inside source list 1 pool POOLR1
R1(config)#

```

## Setting NAT Dynamic di R2

Command untuk mensetting NAT Dynamic.

```
R2(config)#interface fa0/0
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#interface fa1/0
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#exit
R2(config)#
R2(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R2(config)#
R2(config)#ip nat pool POOLR2 12.12.12.21 12.12.12.30 netmask 255.255.255.0
R2(config)#
R2(config)#ip nat inside source list 1 pool POOLR2
R2(config)#+
```

## Verifikasi

### Tes Ping dari Laptop1 ke Lo3

```
Laptop1>ping 172.16.3.3
```

Pinging 172.16.3.3 with 32 bytes of data:

```
Reply from 172.16.3.3: bytes=32 time=1ms TTL=254  
Reply from 172.16.3.3: bytes=32 time=0ms TTL=254  
Reply from 172.16.3.3: bytes=32 time=1ms TTL=254  
Reply from 172.16.3.3: bytes=32 time=0ms TTL=254
```

Ping statistics for 172.16.3.3:

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

### Tes Ping dari Laptop1 ke Lo4

```
Laptop1>ping 172.16.4.4
```

Pinging 172.16.4.4 with 32 bytes of data:

```
Reply from 172.16.4.4: bytes=32 time=1ms TTL=254  
Reply from 172.16.4.4: bytes=32 time=0ms TTL=254  
Reply from 172.16.4.4: bytes=32 time=0ms TTL=254  
Reply from 172.16.4.4: bytes=32 time=2ms TTL=254
```

Ping statistics for 172.16.4.4:

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

Dari tampilan diatas dapat diketahui bahwa Laptop1 yang berada di Private Network dapat berkomunikasi dengan Lo3 dan Lo4 yang berada di **Internet**.

### Tampilan NAT table di R1

```
R1#show ip nat translation  
Pro Inside global Inside local Outside local Outside global  
icmp 12.12.12.11:101 192.168.1.1:101 172.16.4.4:101 172.16.4.4:101  
icmp 12.12.12.11:102 192.168.1.1:102 172.16.4.4:102 172.16.4.4:102  
icmp 12.12.12.11:103 192.168.1.1:103 172.16.4.4:103 172.16.4.4:103  
icmp 12.12.12.11:104 192.168.1.1:104 172.16.4.4:104 172.16.4.4:104  
icmp 12.12.12.11:105 192.168.1.1:105 172.16.3.3:105 172.16.3.3:105  
icmp 12.12.12.11:106 192.168.1.1:106 172.16.3.3:106 172.16.3.3:106  
icmp 12.12.12.11:107 192.168.1.1:107 172.16.3.3:107 172.16.3.3:107  
icmp 12.12.12.11:108 192.168.1.1:108 172.16.3.3:108 172.16.3.3:108  
icmp 12.12.12.11:109 192.168.1.1:109 172.16.4.4:109 172.16.4.4:109  
icmp 12.12.12.11:110 192.168.1.1:110 172.16.4.4:110 172.16.4.4:110  
icmp 12.12.12.11:111 192.168.1.1:111 172.16.4.4:111 172.16.4.4:111  
icmp 12.12.12.11:112 192.168.1.1:112 172.16.4.4:112 172.16.4.4:112
```

Dari tampilan NAT tabel di R1 dapat dilihat proses translasi dari host 192.168.1.1 menjadi 12.12.12.11 dengan tujuan host 172.16.4.4 dan 172.16.3.3.

**Note: ulangi langkah verifikasi diatas untuk tes Ping dari Laptop2 ke Lo1 dan Lo2 dan tampilkan NAT table di R2.**

### Traceroute dari Laptop1 ke Lo4

```
Laptop1>tracert 172.16.4.4
```

Tracing route to 172.16.4.4 over a maximum of 30 hops:

```
1 0 ms 0 ms 0 ms 192.168.1.254  
2 0 ms 0 ms 0 ms 172.16.4.4
```

Trace complete.

### Traceroute dari Laptop2 ke Lo2

```
Laptop2>tracert 172.16.2.2
```

Tracing route to 172.16.2.2 over a maximum of 30 hops:

```
1 0 ms 1 ms 0 ms 192.168.2.254  
2 * 0 ms 0 ms 172.16.2.2
```

Trace complete.

Approximate round trip times in milli-seconds:

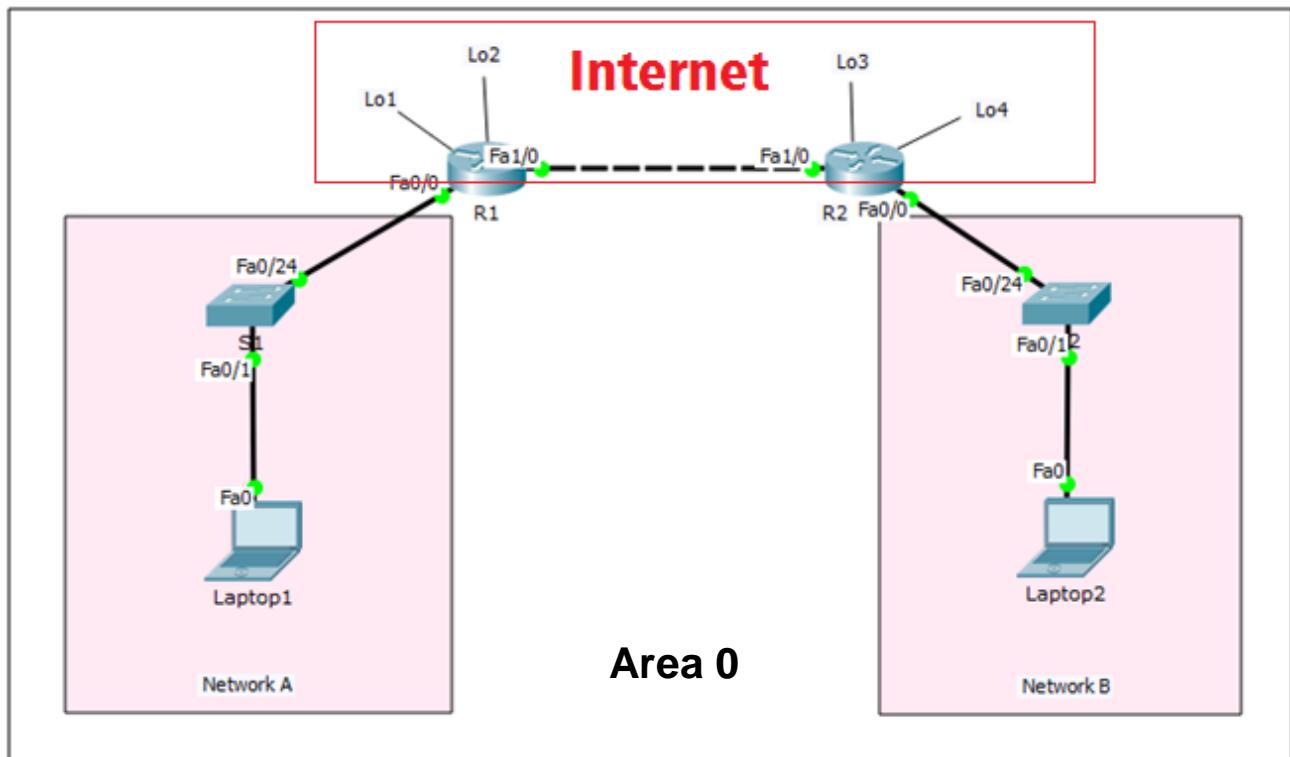
Minimum = 0ms, Maximum = 11ms, Average = 3ms

## Review

1. Apa perbedaannya antara NAT Static dan NAT Dynamic dilihat dari show ip nat translation ?
2. Apa saja kelebihan dan kekurangan NAT Dynamic?

# Lab 13. NAT Dynamic Overload (PAT)

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting PAT

## Konsep Dasar

### PAT

- Tipe NAT yang paling popular
- Termasuk tipe *many-to-one* NAT
- Dengan menyediakan satu IP public dapat mentranslate IP private yang banyak dengan menggunakan pembeda yaitu port
- Disebut juga sebagai NAT Dynamic Overload, Port Address Translation (PAT), atau NAT Overload

## Konfigurasi

Di lab ini akan dibagi menjadi dua bagian yang pertama tentang Port Address Translation dan kedua tentang Port Address Translation menggunakan exit-interface.

### Bagian 1. Port Address Translation

Login console ke R1 atau R2 untuk mempraktikkan **Lab 13-NAT Dynamic Overload (PAT)**.

Untuk mempraktikkan konsep NAT Static ini, kita asumsikan bahwa area Internet menggunakan routing OSPF. Network A dan Network B pada R1 dan R2 tidak diadvertis oleh OSPF sehingga masuk Network Private, sehingga untuk mengakses Internet dibutuhkan NAT. Agar Network A dan Network B tidak diadvertis oleh OSPF berarti kita tidak perlu memasukkan Network A dan Network B pada command OSPF di R1 maupun R2.

#### Tampilan routing table R1

```
R1#show ip route
...
Gateway of last resort is not set

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Loopback1
C 172.16.2.0/24 is directly connected, Loopback2
O 172.16.3.3/32 [110/2] via 12.12.12.2, 00:17:33, FastEthernet1/0
O 172.16.4.4/32 [110/2] via 12.12.12.2, 00:17:33, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

### Tampilan routing table R2

```
R2#show ip route
...
Gateway of last resort is not set

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O 172.16.1.1/32 [110/2] via 12.12.12.1, 00:18:24, FastEthernet1/0
O 172.16.2.2/32 [110/2] via 12.12.12.1, 00:18:24, FastEthernet1/0
C 172.16.3.0/24 is directly connected, Loopback0
C 172.16.4.0/24 is directly connected, Loopback1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

Dari output kedua routing table di R1 dan R2, sudah tidak terlihat lagi route menuju masing-masing Network A dan Network B.

### Pool NAT R1

Private IP (ACL 1)	Public IP (POOLR1)
192.168.1.0/24	12.12.12.11

### Pool NAT R2

Private IP (ACL 1)	Public IP (POOLR2)
192.168.2.0/24	12.12.12.22

Langkah sederhana setting NAT Dynamic PAT:

1. Tentukan interface NAT inside
  2. Tentukan interface NAT outside
  3. Tentukan permit ACL Private Network
  4. Tentukan pool Public IP (terdiri dari single Public IP)
  5. Buat translasi NAT dari source ACL ke destination pool Public IP

## Setting NAT Dynamic PAT di R1

Command untuk mensetting NAT Dynamic PAT.

```
R1(config)#interface fa0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#interface fa1/0
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#
R1(config)#ip nat pool POOLR1 12.12.12.11 12.12.12.11 netmask 255.255.255.0
R1(config)#
R1(config)#ip nat inside source list 1 pool POOLR1 overload
R1(config)#

```

## Setting NAT Dynamic PAT di R2

Command untuk mensetting NAT Dynamic PAT.

```
R2(config)#interface fa0/0
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#interface fa1/0
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#exit
R2(config)#
R2(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R2(config)#
R2(config)#ip nat pool POOLR2 12.12.12.22 12.12.12.22 netmask 255.255.255.0
R2(config)#
R2(config)#ip nat inside source list 1 pool POOLR2 overload
R2(config)#
```

## Verifikasi

### Tes Ping dari Laptop1 ke Lo3

```
Laptop1>ping 172.16.3.3
```

Pinging 172.16.3.3 with 32 bytes of data:

```
Reply from 172.16.3.3: bytes=32 time=1ms TTL=254  
Reply from 172.16.3.3: bytes=32 time=0ms TTL=254  
Reply from 172.16.3.3: bytes=32 time=1ms TTL=254  
Reply from 172.16.3.3: bytes=32 time=0ms TTL=254
```

Ping statistics for 172.16.3.3:

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

### Tes Ping dari Laptop1 ke Lo4

```
Laptop1>ping 172.16.4.4
```

Pinging 172.16.4.4 with 32 bytes of data:

```
Reply from 172.16.4.4: bytes=32 time=1ms TTL=254  
Reply from 172.16.4.4: bytes=32 time=0ms TTL=254  
Reply from 172.16.4.4: bytes=32 time=0ms TTL=254  
Reply from 172.16.4.4: bytes=32 time=2ms TTL=254
```

Ping statistics for 172.16.4.4:

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

Dari tampilan diatas dapat diketahui bahwa Laptop1 yang berada di Private Network dapat berkomunikasi dengan Lo3 dan Lo4 yang berada di **Internet**.

### Tampilan NAT table di R1

```
R1#show ip nat translation  
Pro Inside global Inside local Outside local Outside global  
icmp 12.12.12.11:123 192.168.1.1:123 172.16.3.3:123 172.16.3.3:123  
icmp 12.12.12.11:124 192.168.1.1:124 172.16.3.3:124 172.16.3.3:124  
icmp 12.12.12.11:125 192.168.1.1:125 172.16.3.3:125 172.16.3.3:125  
icmp 12.12.12.11:126 192.168.1.1:126 172.16.3.3:126 172.16.3.3:126  
icmp 12.12.12.11:127 192.168.1.1:127 172.16.3.3:127 172.16.3.3:127  
icmp 12.12.12.11:128 192.168.1.1:128 172.16.3.3:128 172.16.3.3:128  
icmp 12.12.12.11:129 192.168.1.1:129 172.16.3.3:129 172.16.3.3:129  
icmp 12.12.12.11:130 192.168.1.1:130 172.16.3.3:130 172.16.3.3:130  
icmp 12.12.12.11:131 192.168.1.1:131 172.16.4.4:131 172.16.4.4:131  
icmp 12.12.12.11:132 192.168.1.1:132 172.16.4.4:132 172.16.4.4:132
```

Dari tampilan NAT tabel di R1 dapat dilihat proses translasi dari host 192.168.1.1 menjadi 12.12.12.11 dengan tujuan host 172.16.4.4 dan 172.16.3.3. Dengan menggunakan single-IP address Public, maka yang membedakan tiap sessionnya yaitu port, contoh 123, 124, 125, dst.

**Note:** ulangi langkah verifikasi diatas untuk tes Ping dari Laptop2 ke Lo1 dan Lo2 dan tampilkan NAT table di R2.

### Traceroute dari Laptop1 ke Lo4

```
Laptop1>tracert 172.16.4.4
```

Tracing route to 172.16.4.4 over a maximum of 30 hops:

```
1 0 ms 0 ms 0 ms 192.168.1.254  
2 0 ms 0 ms 0 ms 172.16.4.4
```

Trace complete.

### Traceroute dari Laptop2 ke Lo2

```
Laptop2>tracert 172.16.2.2
```

Tracing route to 172.16.2.2 over a maximum of 30 hops:

```
1 0 ms 1 ms 0 ms 192.168.2.254  
2 * 0 ms 0 ms 172.16.2.2
```

Trace complete.

Approximate round trip times in milli-seconds:

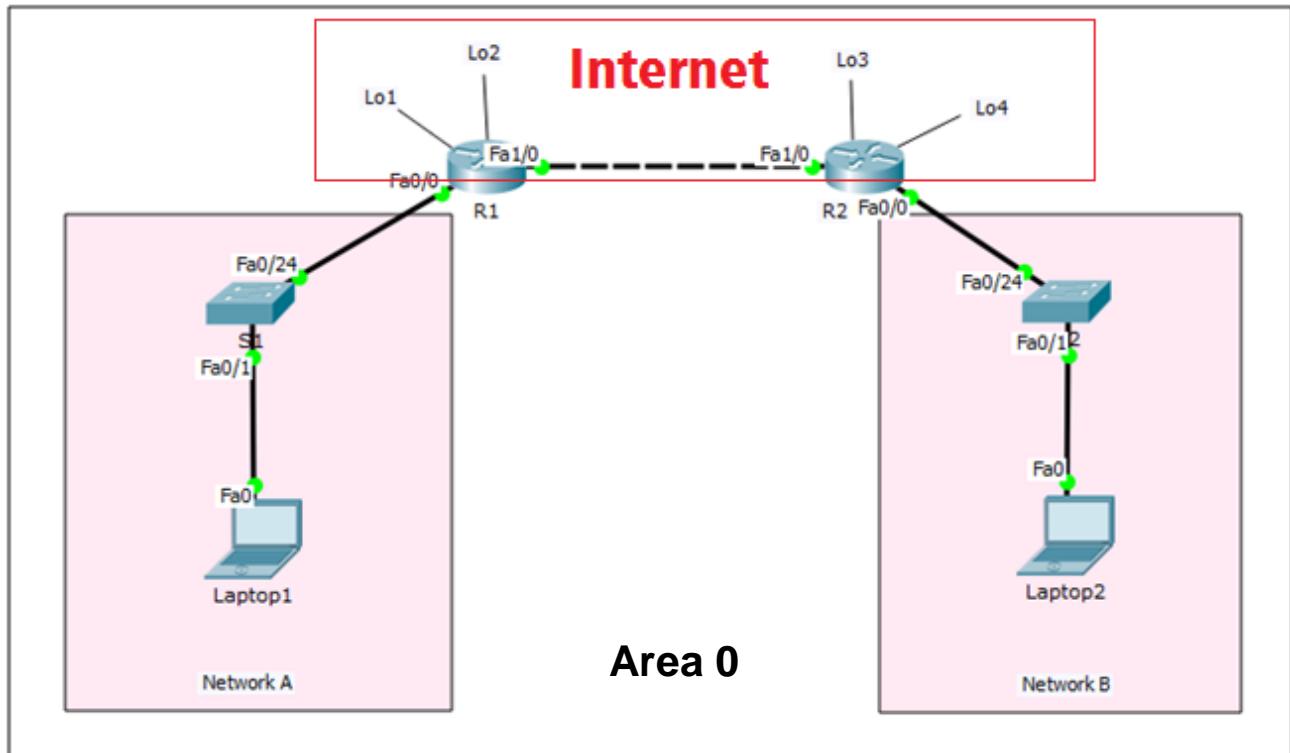
Minimum = 0ms, Maximum = 11ms, Average = 3ms

## Review

1. Apa saja keuntungan menggunakan NAT Dynamic PAT ini?

# Lab 14. NAT Dynamic Overload (PAT) with Exit Interface

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting PAT with Exit-Interface

## Konsep Dasar

### PAT

- Tipe NAT yang paling popular
- Termasuk tipe *many-to-one* NAT
- Dengan menyediakan satu IP public dapat mentranslate IP private yang banyak dengan menggunakan pembeda yaitu port
- Disebut juga sebagai NAT Dynamic Overload, Port Address Translation (PAT), atau NAT Overload

## Konfigurasi

### Bagian 2. Port Address Translation with Exit-Interface

Login console ke R1 atau R2 untuk mempraktikkan **Lab 14-NAT Dynamic Overload (PAT) with Exit-Interface**.

Untuk mempraktikkan konsep NAT Static ini, kita asumsikan bahwa area Internet menggunakan routing OSPF. Network A dan Network B pada R1 dan R2 tidak diadvertise oleh OSPF sehingga masuk Network Private, sehingga untuk mengakses Internet dibutuhkan NAT. Agar Network A dan Network B tidak diadvertise oleh OSPF berarti kita tidak perlu memasukkan Network A dan Network B pada command OSPF di R1 maupun R2.

#### Tampilan routing table R1

```
R1#show ip route
..
Gateway of last resort is not set

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Loopback1
C 172.16.2.0/24 is directly connected, Loopback2
O 172.16.3.3/32 [110/2] via 12.12.12.2, 00:17:33, FastEthernet1/0
O 172.16.4.4/32 [110/2] via 12.12.12.2, 00:17:33, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

#### Tampilan routing table R2

```
R2#show ip route
..
Gateway of last resort is not set

12.0.0.0/24 is subnetted, 1 subnets
C 12.12.12.0 is directly connected, FastEthernet1/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O 172.16.1.1/32 [110/2] via 12.12.12.1, 00:18:24, FastEthernet1/0
O 172.16.2.2/32 [110/2] via 12.12.12.1, 00:18:24, FastEthernet1/0
C 172.16.3.0/24 is directly connected, Loopback0
C 172.16.4.0/24 is directly connected, Loopback1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

Dari output kedua routing table di R1 dan R2, sudah tidak terlihat lagi route menuju masing-masing Network A dan Network B.

### Pool NAT R1

Private IP (ACL 1)	Interface Public
192.168.1.0/24	Fa1/0

### Pool NAT R2

Private IP (ACL 1)	Public IP (POOLR2)
192.168.2.0/24	Fa1/0

Langkah sederhana setting NAT Dynamic Overload (PAT with Exit-Interface):

1. Tentukan interface NAT inside
2. Tentukan interface NAT outside
3. Tentukan permit ACL Private Network
4. Tentukan interface Public (Fa1/0)
5. Buat translasi NAT dari source ACL ke destination Interface Public

### Setting NAT Dynamic PAT di R1

Command untuk mensetting NAT Dynamic PAT.

```
R1(config)#interface fa0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#interface fa1/0
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#
R1(config)#
R1(config)#ip nat inside source list 1 interface fa1/0 overload
R1(config)#

```

## **Setting NAT Dynamic PAT di R2**

Command untuk mensetting NAT Dynamic PAT.

```
R2(config)#interface fa0/0
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#interface fa1/0
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#exit
R2(config)#
R2(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R2(config)#
R2(config)#ip nat inside source list 1 interface fa1/0 overload
R2(config)#

```

## **Verifikasi**

### **Tes Ping dari Laptop1 ke Lo3**

```
Laptop1>ping 172.16.3.3

Pinging 172.16.3.3 with 32 bytes of data:

Reply from 172.16.3.3: bytes=32 time=1ms TTL=254
Reply from 172.16.3.3: bytes=32 time=0ms TTL=254
Reply from 172.16.3.3: bytes=32 time=1ms TTL=254
Reply from 172.16.3.3: bytes=32 time=0ms TTL=254

Ping statistics for 172.16.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

### **Tes Ping dari Laptop1 ke Lo4**

```
Laptop1>ping 172.16.4.4

Pinging 172.16.4.4 with 32 bytes of data:

Reply from 172.16.4.4: bytes=32 time=1ms TTL=254
Reply from 172.16.4.4: bytes=32 time=0ms TTL=254
Reply from 172.16.4.4: bytes=32 time=0ms TTL=254
Reply from 172.16.4.4: bytes=32 time=2ms TTL=254

Ping statistics for 172.16.4.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms

```

Dari tampilan diatas dapat diketahui bahwa Laptop1 yang berada di Private Network dapat berkomunikasi dengan Lo3 dan Lo4 yang berada di **Internet**.

### Tampilan NAT table di R1

```
R1#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 12.12.12.1:155 192.168.1.1:155 172.16.4.4:155 172.16.4.4:155
icmp 12.12.12.1:156 192.168.1.1:156 172.16.4.4:156 172.16.4.4:156
icmp 12.12.12.1:157 192.168.1.1:157 172.16.4.4:157 172.16.4.4:157
icmp 12.12.12.1:158 192.168.1.1:158 172.16.4.4:158 172.16.4.4:158
icmp 12.12.12.1:159 192.168.1.1:159 172.16.3.3:159 172.16.3.3:159
icmp 12.12.12.1:160 192.168.1.1:160 172.16.3.3:160 172.16.3.3:160
icmp 12.12.12.1:161 192.168.1.1:161 172.16.3.3:161 172.16.3.3:161
```

Dari tampilan NAT tabel di R1 dapat dilihat proses translasi dari host 192.168.1.1 menjadi 12.12.12.11 dengan tujuan host 172.16.4.4 dan 172.16.3.3. Dengan menggunakan single-IP address Public, maka yang membedakan tiap sessionnya yaitu port address, contoh 155, 156, 159, dst.

**Note:** ulangi langkah verifikasi diatas untuk tes Ping dari Laptop2 ke Lo1 dan Lo2 dan tampilkan NAT table di R2.

### Traceroute dari Laptop1 ke Lo4

```
Laptop1>tracert 172.16.4.4
Tracing route to 172.16.4.4 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.1.254
2 0 ms 0 ms 0 ms 172.16.4.4
Trace complete.
```

### Traceroute dari Laptop2 ke Lo2

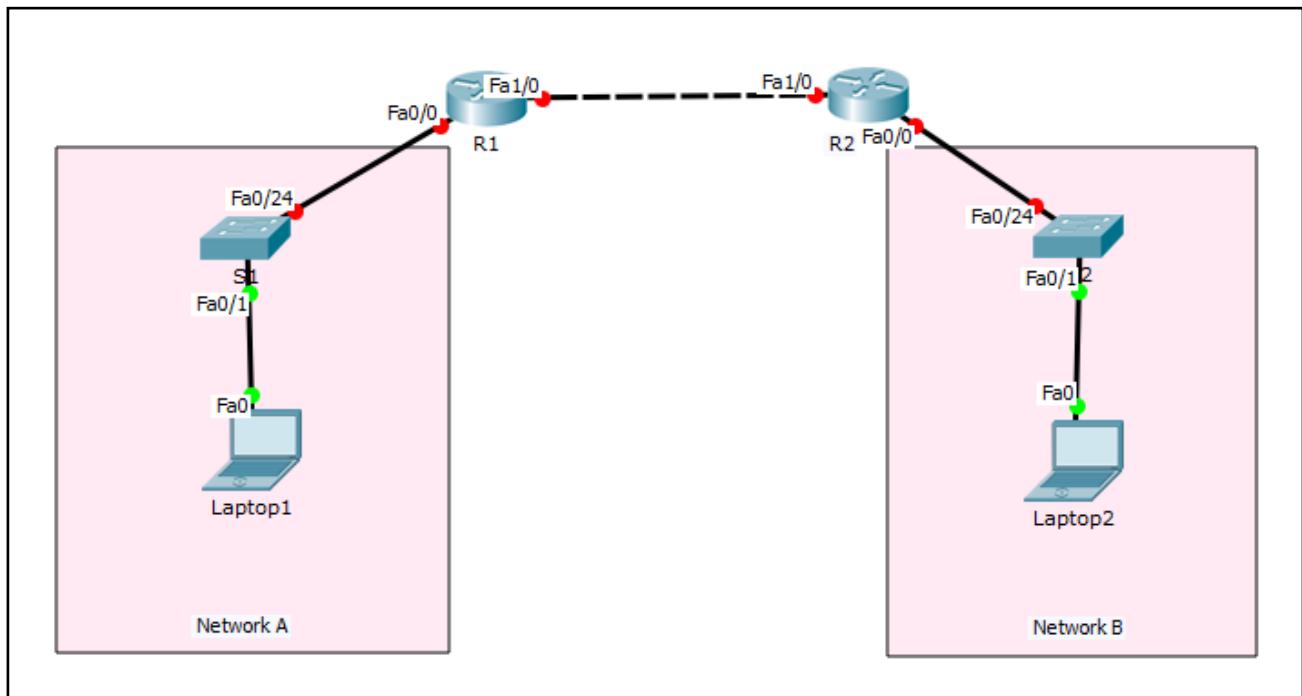
```
Laptop2>tracert 172.16.2.2
Tracing route to 172.16.2.2 over a maximum of 30 hops:
1 0 ms 1 ms 0 ms 192.168.2.254
2 * 0 ms 0 ms 172.16.2.2
Trace complete.
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

## Review

1. Dari segi reliabilitas, mana yang lebih recommended antara NAT Dynamic Overload dengan Single-IP Public atau Exit-Interface?
2. Dengan menggunakan PAT with Exit-Interface, apakah bisa dilakukan inisiasi komunikasi dari network luar menuju Network A atau B? Misal Loopback3 ingin tes Ping ke Laptop1 atau Loopback1 ingin tes Ping ke Laptop2?

# Lab 15. Basic Switch Configuration

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.254
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254

## Tujuan

- Setting basic switch

## Konsep Dasar

Switch memiliki 5 mode :

### 1. Setup mode

- ✓ Switch masuk setup mode jika NVRAM kosong alias tidak memiliki konfigurasi. Biasanya kondisi ini terjadi ketika kita mengaktifkan switch baru atau setelah melakukan reset konfigurasi.

### 2. User mode

- ✓ Hanya terdapat beberapa command untuk monitoring
- ✓ Command show terbatas, ping dan traceroute
- ✓ Ditandai dengan : **Switch>**

### 3. Privileged mode

- ✓ Terdapat beberapa command monitoring dan troubleshooting
- ✓ Terdapat semua command show, ping, trace, copy, erase
- ✓ Ditandai dengan : **Switch#**

### 4. Global Configuration mode

- ✓ Untuk mensetting keseluruhan switch misalnya hostname, konfigurasi switching
- ✓ Semua konfigurasi berlaku global di switch
- ✓ Ditandai dengan : **Switch(config) #**

### 5. Switch ROM

- ✓ Untuk mereset password

## Konektivitas Console

Untuk koneksi switch menggunakan console, membutuhkan kabel console dan converter DB-9 to USB. Proses remote dapat dilakukan dengan aplikasi putty atau hyperterminal untuk sistem operasi Windows. Sedangkan di Linux dapat menggunakan minicom -s.

## Konfigurasi

Untuk mensetting basic switch S1 dan S2, gunakan akses console dari Laptop1 dan Laptop2. Setelah itu, ketikkan command basic switch dibawah ini di S1 dan S2.

- a. Setelah login console ketikkan enable privileged EXEC mode.

```
Switch> enable
Switch#
```

- b. Masuk global configuration mode.

```
Switch# config terminal
Switch(config) #
```

- c. Memberikan nama device switch.

```
Switch(config)# hostname S1
```

- d. Disable DNS lookup untuk mencegah switch melakukan translasi command yang salah ketik.

```
S1(config)# no ip domain-lookup
```

- e. Setting password privilege terenkripsi **ciscosec**

```
S1(config)# enable secret ciscosec
```

- f. Setting password console **ciscocon**. Aktifkan timeout command sehingga jika selama 5 menit 0 second tidak ada aktifitas maka akan logout sendiri.

```
S1(config)# line con 0
S1(config-line)# password ciscocon
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
```

- g. Setting password vty **ciscovty**. Aktifkan timeout command sehingga jika selama 5 menit 0 second tidak ada aktifitas maka akan logout sendiri.

```
S1(config)# line vty 0 4
S1(config-line)# password ciscovty
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
```

- h. Enable enkripsi clear text passwords.

```
S1(config)# service password-encryption
```

- i. Buat banner yang memberikan informasi kepada user yang tidak memiliki otorisasi dilarang login switch.

```
S1(config)# banner motd #Unauthorized access is strictly
prohibited!#
```

- j. Setting IP address dan interface description. Aktifkan interface vlan 1 dengan sub-command no-shutdown.

```
S1(config)# int vlan 1
S1(config-if)# description Connection to VLAN 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# exit
S1#
```

- k. Setting default gateway

```
S1(config)# ip default-gateway 192.168.1.254
```

- l. Simpan konfigurasi file running-configuration ke startup-configuration.

```
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Ketika kita mensetting switch, maka konfigurasi akan disimpan sementara di file running-configuration (RAM), oleh karena itu proses menyimpan penting untuk dilakukan agar saat switch reboot atau shutdown file konfigurasi switch masih tetap disimpan di startup-configuration (NVRAM). Cara lain menyimpan konfigurasi yaitu menggunakan command **write memory** atau **wr mem**.

**Note: ulangi langkah yang sama untuk mensetting basic switch S2.**

## **Verifikasi**

Setelah mensetting basic switch S1 dan S2, langkah selanjutnya melakukan verifikasi bahwa konfigurasi yang sudah kita setting benar.

### **Menampilkan informasi full konfigurasi switch**

```
S1#show run
Building configuration...

Current configuration : 1285 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$thF1sEHJ9Dl2J3WzXxyZ1/
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
```

```

interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
description Connection to VLAN 1
ip address 192.168.1.11 255.255.255.0
!
ip default-gateway 192.168.1.254
!
banner motd ^CUnauthorized access is strictly prohibited!^C
!
!
!
line con 0
password 7 0822455D0A1606181C
login
exec-timeout 5 0
!
line vty 0 4
exec-timeout 5 0
password 7 0822455D0A1613030B
login
line vty 5 15
login
!
!
end

```

- Gunakan tombol **Enter** untuk menampilkan per baris
- Gunakan tombol **Space** untuk menampilkan per screen

- Gunakan tombol **q** untuk exit dari tampilan konfigurasi switch

Cek konfigurasi yang sudah diinputkan apakah ada yang salah atau tidak.

### Menampilkan informasi interface

```
S1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual down down
FastEthernet0/2 unassigned YES manual down down
FastEthernet0/3 unassigned YES manual down down
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
FastEthernet0/6 unassigned YES manual down down
FastEthernet0/7 unassigned YES manual down down
FastEthernet0/8 unassigned YES manual down down
FastEthernet0/9 unassigned YES manual down down
FastEthernet0/10 unassigned YES manual down down
FastEthernet0/11 unassigned YES manual down down
FastEthernet0/12 unassigned YES manual down down
FastEthernet0/13 unassigned YES manual down down
FastEthernet0/14 unassigned YES manual down down
FastEthernet0/15 unassigned YES manual down down
FastEthernet0/16 unassigned YES manual down down
FastEthernet0/17 unassigned YES manual down down
FastEthernet0/18 unassigned YES manual down down
FastEthernet0/19 unassigned YES manual down down
FastEthernet0/20 unassigned YES manual down down
FastEthernet0/21 unassigned YES manual down down
FastEthernet0/22 unassigned YES manual down down
FastEthernet0/23 unassigned YES manual down down
FastEthernet0/24 unassigned YES manual down down
Vlan1 192.168.1.11 YES manual up up
```

Dari tampilan informasi interface, dicek apakah IP yang sudah diconfig sudah benar atau belum.

### Tes konektivitas dari Laptop1 ke S1

Lakukan tes Ping dari Laptop1 ke S1 dan sebaliknya.

```
Laptop1>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.11: bytes=32 time=0ms TTL=255
Reply from 192.168.1.11: bytes=32 time=0ms TTL=255
Reply from 192.168.1.11: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.11:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Dari output diatas, reply pertama diawali timed out kemudian dilanjutkan reply dari IP VLAN 1 S1.

### Tes konektivitas dari S1 ke R1

```
S1#ping 192.168.1.254
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
S1#ping 192.168.1.254
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
S1#
```

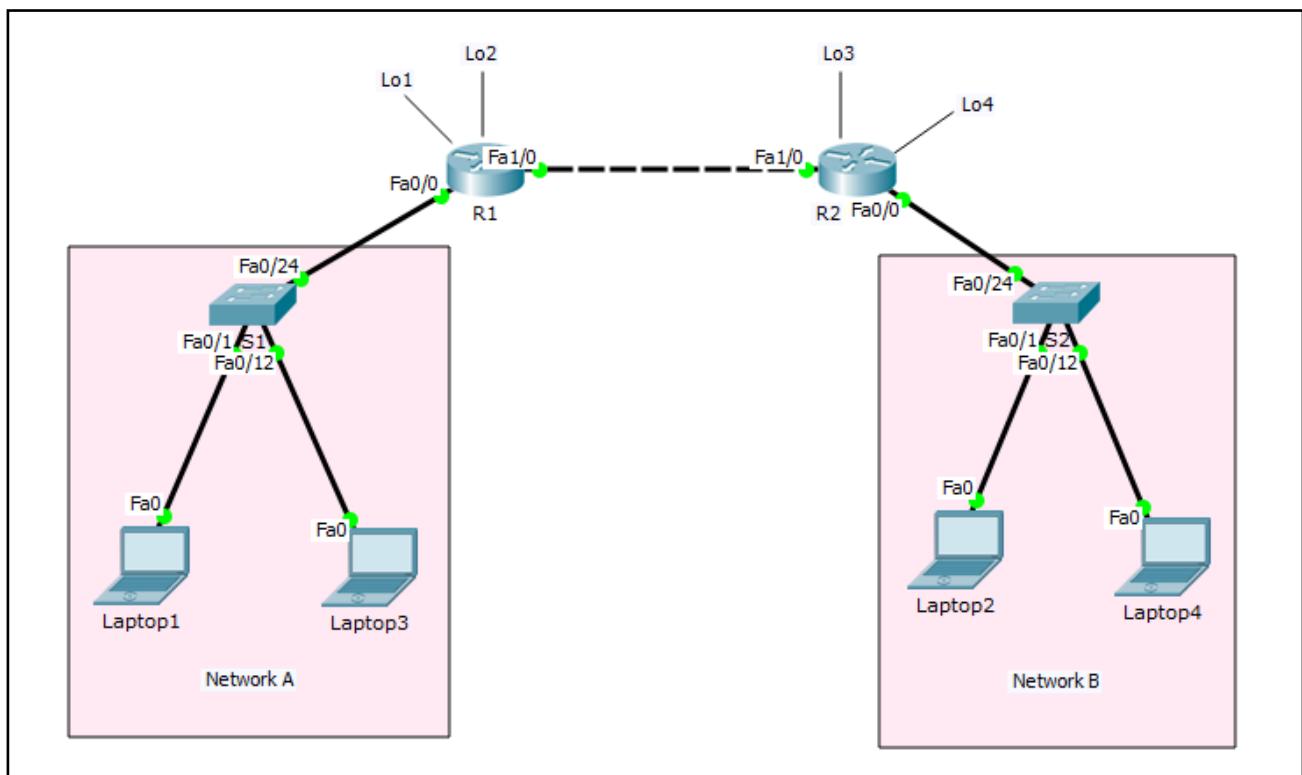
Dari hasil ping yang pertama success rate masih 80%, kemudian dilanjutkan yang kedua menjadi 100%.

### Review

1. Secara default, apa bedanya status interface antara Switch dan Router?

# Lab 16. VLAN

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop3	NIC	192.168.1.3	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254
Laptop4	NIC	192.168.2.3	255.255.255.0	192.168.2.254

## Tujuan

- Setting VLAN

## Konsep Dasar

### VLAN

- Membagi single broadcast domain menjadi beberapa broadcast domain
- Security layer 2
- Secara default semua port switch masuk VLAN 1
- VLAN 1 dikenal juga sebagai Administrative VLAN atau Management VLAN
- VLAN bisa dibuat dari nomor 2 – 1001
- VLAN hanya bisa dikonfigurasi pada Manageable Switch saja
- 2 tipe VLAN :
  - Static VLAN
  - Dynamic VLAN
- VLAN meningkatkan security network
- VLAN meningkatkan jumlah broadcast domain dan menurunkan size broadcast domain

### Static VLAN

- Static VLAN berdasarkan port
- Dilakukan secara manual untuk assign port ke VLAN
- Disebut juga sebagai Port-Based VLAN
- Satu port hanya bisa untuk satu VLAN

Dua cara membuat VLAN :

#### 1. Membuat VLAN di config mode

```
Switch (config) # vlan <no>
Switch (config-vlan) # name <name>
Switch (config-vlan) # exit
```

Assign port di VLAN

```
Switch (config) # interface <interface type> <interface no.>
Switch (config-if) # switchport mode access
Switch (config-if) # switchport access vlan <no>
```

#### 2. Membuat VLAN menggunakan command database

```
Switch (config) # vlan database
Switch (config-vlan) # vlan <vlan id> name <vlan name>
Switch (config-vlan) # exit
```

Assign port di VLAN

```
Switch (config) # interface <interface type> <interface no.>
Switch (config-if) # switchport mode access
Switch (config-if) # switchport access vlan <no>
```

## Verifikasi VLAN

```
Switch # show vlan
```

## **Dynamic VLAN**

- Berdasarkan MAC address PC
- Switch secara otomatis assign port ke VLAN
- Masing-masing port bisa menjadi lebih dari satu member VLAN
- Untuk konfigurasi VLAN dibutuhkan software VMPS (VLAN Membership Policy Server)

## **Konfigurasi**

Login console ke S1 atau S2 untuk mempraktikkan **Lab 16-VLAN**.

Sebelum implementasi VLAN di S1 maupun S2, Laptop1 dan Laptop3 masih bisa saling Ping, begitu juga Laptop2 dan Laptop4 karena masih dalam satu VLAN yang sama yaitu VLAN 1.

### **Tes Ping Laptop1 ke Laptop3**

```
Laptop1>ipconfig
```

```
FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::201:43FF:FE3A:AEC2
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.254
```

```
Laptop3>ipconfig
```

```
FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::2D0:97FF:FE5C:503B
IP Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.254
```

```
Laptop1>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=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms 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
```

## Tes Ping Laptop2 ke Laptop4

```
Laptop2>ipconfig
```

```
FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::260:2FFF:FE42:A6D3
IP Address.....: 192.168.2.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.254
```

```
Laptop4>ipconfig
```

```
FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::20A:F3FF:FE4B:1E76
IP Address.....: 192.168.2.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.254
```

```
Laptop2>ping 192.168.2.3
```

```
Pinging 192.168.2.3 with 32 bytes of data:
```

```
Reply from 192.168.2.3: bytes=32 time=63ms TTL=128
Reply from 192.168.2.3: bytes=32 time=8ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms TTL=128
Reply from 192.168.2.3: bytes=32 time=0ms 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 = 63ms, Average = 17ms
```

## Tabel VLAN

Switch	VLAN	VLAN NAME	Interface	Network VLAN
S1	VLAN 10	IT	Fa0/1-Fa0/12	192.168.10.0/24
	VLAN 20	Admin	Fa0/13-Fa0/24	192.168.20.0/24
	Interface VLAN10			192.168.10.10
S2	VLAN 10	IT	Fa0/1-Fa0/12	192.168.10.0/24
	VLAN 20	Admin	Fa0/13-Fa0/24	192.168.20.0/24
	Interface VLAN10			192.168.10.10

Setting VLAN di S1 dan S2 sesuai dengan tabel VLAN diatas dan setting IP address untuk interface VLAN 10 agar S1 atau S2 dapat diremote melalui telnet.

## Setting VLAN di S1

### Tampilkan VLAN default di S1

```
S1#show vlan

VLAN Name Status Ports
-----
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
1 enet 100001 1500 - - - - 0 0
1002 fddi 101002 1500 - - - - 0 0
1003 tr 101003 1500 - - - - 0 0
1004 fdnet 101004 1500 - - ieee - 0 0
1005 trnet 101005 1500 - - ibm - 0 0

Remote SPAN VLANs
-----
-----
```

Primary Secondary Type Ports

```
-----
```

S1#

### Command membuat VLAN di S1

```
S1(config)#
S1(config)#vland 10
S1(config-vlan)#name IT
S1(config-vlan)#vland 20
S1(config-vlan)#name Admin
S1(config-vlan)#
S1(config-vlan)#interface range fa0/1-12
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#
S1(config-if-range)#interface range fa0/13-24
S1(config-if-range)#switchport mode access
```

```
S1(config-if-range)#switchport access vlan 20
S1(config-if-range)#
S1(config-if-range)#end
```

### Command setting IP address interface VLAN 10 di S1

```
S1(config)#
S1(config)#interface vlan 10
S1(config-if)#ip address 192.168.10.10 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#
S1(config-if)#ip default-gateway 192.168.10.254
S1(config)#

```

Note : ulangi langkah yang sama diatas untuk membuat VLAN dan Interface VLAN di S2

## Verifikasi

### Tampilkan show vlan brief setelah disetting VLAN di S1

```
S1#show vlan brief

VLAN Name Status Ports
-----
1 default active
10 IT active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
20 Admin active Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
S1#
```

### Tampilkan show vlan brief setelah disetting VLAN di S2

```
S2#show vlan brief

VLAN Name Status Ports
-----
1 default active
10 IT active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
20 Admin active Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default active
1003 token-ring-default active
```

```
1004 fddinet-default active  
1005 trnet-default active  
S2#
```

Dari hasil output `show vlan brief` diatas, kita telah berhasil membuat VLAN 10 dan VLAN 20 di S1 dan S2. Dengan status Active pada masing-masing VLAN dan interface VLAN sudah sesuai dengan tabel VLAN yang diberikan.

**Tampilkan `show ip interface brief` di S1**

```
S1#show ip interface brief  
Interface IP-Address OK? Method Status Protocol  
FastEthernet0/1 unassigned YES manual up up  
...  
FastEthernet0/24 unassigned YES manual up up  
Vlan1 unassigned YES manual administratively down down  
Vlan10 192.168.10.10 YES manual up up  
S1#
```

**Tampilkan `show ip interface brief` di S2**

```
S2#show ip interface brief  
Interface IP-Address OK? Method Status Protocol  
FastEthernet0/1 unassigned YES manual up up  
...  
FastEthernet0/24 unassigned YES manual up up  
Vlan1 unassigned YES manual administratively down down  
Vlan10 192.168.10.10 YES manual up up  
S2#
```

Dari hasil output diatas, interface VLAN 10 telah berhasil disetting IP address. Langkah selanjutnya meremote S1 dari Laptop1. Setting IP Laptop1 terlebih dahulu agar sesuai dengan network VLAN 10. IP address Laptop1 = 192.168.10.1/24. Diasumsikan switch telah disetting basic switch configuration misalnya hostname, enable secret, telnet, dll, lihat solution **Lab 15-Basic Switch Configuration**.

```
Laptop1>ipconfig  
  
FastEthernet0 Connection: (default port)  
  
Link-local IPv6 Address.....: FE80::201:43FF:FE3A:AEC2  
IP Address.....: 192.168.10.1  
Subnet Mask.....: 255.255.255.0  
Default Gateway.....: 192.168.10.254
```

### Tes Ping dari Laptop1 ke S1

```
Laptop1>ping 192.168.10.10
```

```
Pinging 192.168.10.10 with 32 bytes of data:
```

```
Reply from 192.168.10.10: bytes=32 time=1ms TTL=255  
Reply from 192.168.10.10: bytes=32 time=0ms TTL=255  
Reply from 192.168.10.10: bytes=32 time=0ms TTL=255  
Reply from 192.168.10.10: bytes=32 time=0ms TTL=255
```

```
Ping statistics for 192.168.10.10:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

### Telnet dari Laptop1 ke S1

```
Laptop1>telnet 192.168.10.10
```

```
Trying 192.168.10.10 ...Open
```

```
User Access Verification
```

```
Password:
```

```
S1>enable
```

```
Password:
```

```
S1#
```

**Note: ulangi langkah yang sama diatas untuk tes Ping dari Laptop2 ke S2 dan akses telnet ke S2**

Setelah selesai disetting VLAN, maka Laptop1 dan Laptop3 di S1, Laptop2 dan Laptop4 di S2 tidak bisa melakukan Ping karena beda VLAN. Oleh karena itu untuk mengkoneksikan VLAN yang berbeda membutuhkan device layer 3 yaitu router dan L3 switch.

- Laptop1 & Laptop2 menjadi member VLAN10
- Laptop3 & Laptop4 menjadi member VLAN 20

**Tabel Addressing setelah VLAN disetting**

Device	Interface	IP Address	Subnet Mask	Default Gateway
Laptop1	NIC	192.168.10.1	255.255.255.0	192.168.10.254
Laptop3	NIC	192.168.20.1	255.255.255.0	192.168.20.254
Laptop2	NIC	192.168.10.2	255.255.255.0	192.168.10.254
Laptop4	NIC	192.168.20.2	255.255.255.0	192.168.20.254

Dari tabel diatas ada yang memiliki network address yang sama, hal ini tidak menjadi masalah karena VLAN terletak beda lokasi yang satu di Network A dan lainnya di Network B. Dan VLAN ini tidak dikoneksikan menggunakan routing protocol sehingga tidak menyebabkan overlap network.

### Tes Ping dari Laptop1 ke Laptop3 setelah disetting VLAN di S1

```
Laptop1>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

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

Ping statistics for 192.168.20.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

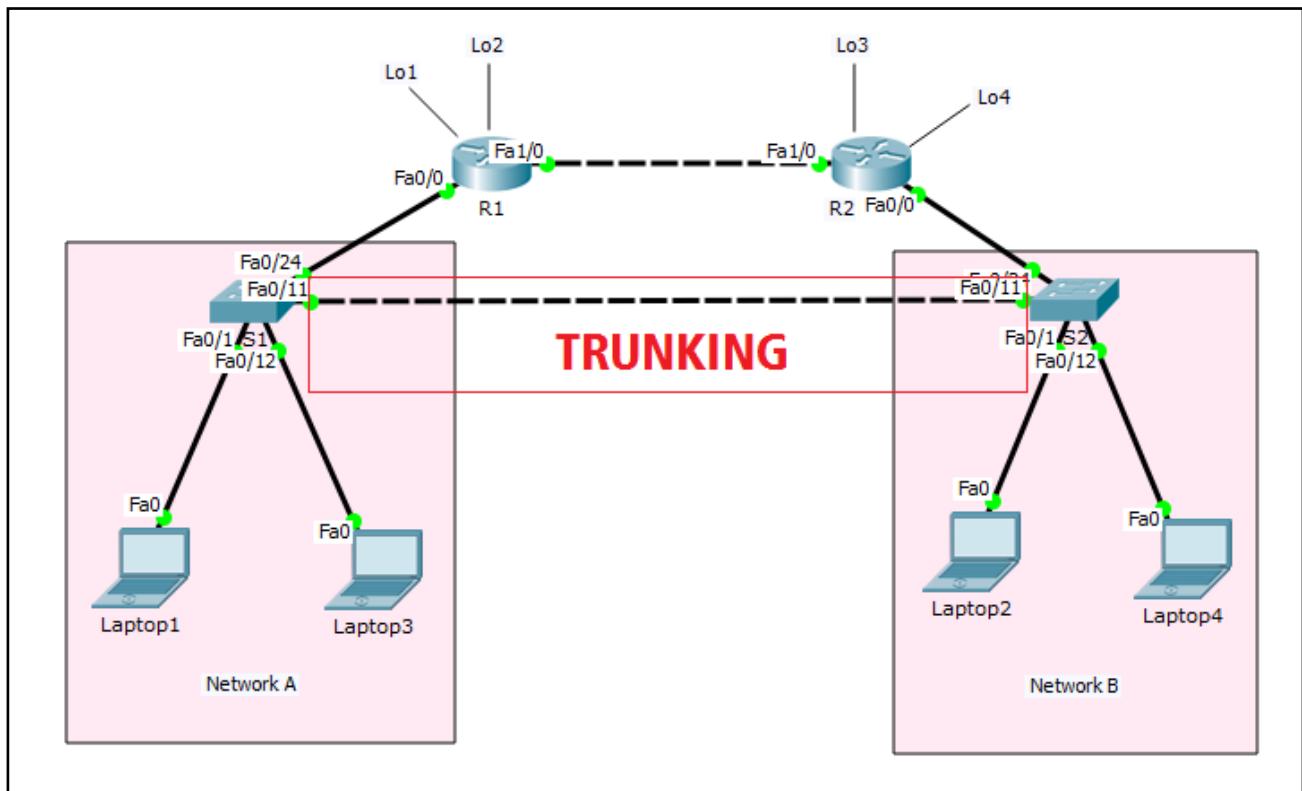
Tes Ping gagal dari Laptop1 ke Laptop3 karena beda VLAN dan belum terdapat gateway diantara masing-masing VLAN. Untuk mengatasi hal ini maka diperlukan InterVLAN menggunakan interface physical router atau sub-interface router (Router-on-Stick).

### Review

1. Command apa yang digunakan untuk menghapus VLAN di swith?
2. Hapus VLAN 1 di S1 maupun S2? Bagaimana hasilnya, berhasil atau tidak? Jelaskan?
3. Ubah interface router Fa0/0 R1 dan R2 menjadi 192.168.10.254, kemudian lakukan tes Ping dari S1 dan S2? Bagaimana hasilnya? Jelaskan?

# Lab 17. VLAN Trunking

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
Laptop3	NIC	192.168.1.3	255.255.255.0	192.168.1.254
Laptop2	NIC	192.168.2.1	255.255.255.0	192.168.2.254
Laptop4	NIC	192.168.2.3	255.255.255.0	192.168.2.254

## Tujuan

- Setting VLAN Trunking

## Konsep Dasar

### Tipe Link/Port

#### 1. Access Port

- Hanya mampu memuat satu VLAN
- Digunakan oleh end-device
- Tidak aware dengan VLAN membership, hanya sebagai member broadcast domain tertentu
- Tidak memiliki pemahaman tentang jaringan fisik
- Switch akan menghapus informasi VLAN dari frame sebelum dikirimkan ke access link

#### 2. Trunk Port

- Dapat melakukan carrier multiple VLAN
- Digunakan oleh point-to-point antara dua switch, antara switch dan router, atau antara switch dan server
- Mampu memuat trafik multiple VLAN dari VLAN 1 sampai 1005 pada satu waktu

### Frame Tagging

- Single VLAN bisa di span untuk multiple switch
- Untuk memastikan komunikasi antar member VLAN yang sama di switch yang berbeda membutuhkan metode frame tagging di trunk link
- Tag ditambahkan sebelum frame dikirimkan dan diremove saat diterima disisi trunk link
- Frame tagging hanya terjadi di trunk link
- VLAN ID digunakan oleh switch untuk mengetahui semua frame melalui trunk link
- Dua trunking protocol yang bertanggung jawab untuk proses frame tagging :
  - Inter-Switch Link (ISL)
  - IEEE 802.1Q

### ISL

- Cisco proprietary
- Bekerja di Ethernet, Token Ring, FDDI
- Menambahkan 30 byte tagging
- Semua VLAN ditag
- Frame tidak dimodifikasi

### IEEE 802.1Q

- Open standar, kita dapat menggunakan switch vendor manapun
- Hanya bekerja di Ethernet
- Hanya menambahkan 4 byte kedalam frame aslinya
- Tidak seperti ISL, 802.1Q tidak mengenkapsulasi frame, tetapi memodifikasi eksisting frame untuk menambahkan VLAN ID

## Konfigurasi Trunking

```
Switch(config)# interface <interface type> <interface no.>
Switch(config-if) # switchport mode trunk
Switch(config-if) # switchport trunk encapsulation dot1q/ISL
```

## Konfigurasi

Login console ke S1 atau S2 untuk mempraktikkan **Lab 17-VLAN Trunking**.

**Tabel VLAN**

Switch	VLAN	VLAN NAME	Interface	IP VLAN
S1	VLAN 10	IT	Fa0/1-Fa0/12	192.168.10.0/24
	VLAN 20	Admin	Fa0/13-Fa0/24	192.168.20.0/24
	Interface VLAN10			192.168.10.10
S2	VLAN 10	IT	Fa0/1-Fa0/12	192.168.10.0/24
	VLAN 20	Admin	Fa0/13-Fa0/24	192.168.20.0/24
	Interface VLAN10			192.168.10.10

**Tabel Addressing setelah VLAN disetting**

VLAN	Device	Interface	IP Address	Subnet Mask	Default Gateway
VLAN 10	Laptop1	NIC	192.168.10.1	255.255.255.0	192.168.10.254
	Laptop2	NIC	192.168.20.1	255.255.255.0	192.168.20.254
VLAN 20	Laptop3	NIC	192.168.10.2	255.255.255.0	192.168.10.254
	Laptop4	NIC	192.168.20.2	255.255.255.0	192.168.20.254

Dari tabel diatas ada yang memiliki network address yang sama, hal ini tidak menjadi masalah karena VLAN terletak beda lokasi yang satu di Network A dan lainnya di Network B. Dan VLAN ini tidak dikoneksikan menggunakan routing protocol sehingga tidak menyebabkan overlap network.

Dengan settingan VLAN seperti tabel VLAN dan tabel addressing diatas, untuk menghubungkan antar VLAN yang sama pada switch yang berbeda kita membutuhkan port dengan mode **Trunk** antara S1 dan S2. Sedangkan untuk mengkoneksikan VLAN yang berbeda membutuhkan device layer 3 yaitu router dan L3 switch, walaupun VLAN yang berbeda terletak pada switch yang sama.

## Setting port trunk di S1 dan S2

Dari gambar topologi diatas, S1 dan S2 terhubung melalui port Fa0/11 dimasing-masing switch. Oleh karena itu, kita akan mensetting port trunk di port Fa0/11 di S1 dan S2.

```
S1(config)#
S1(config)#interface fa0/11
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan all
S1(config-if)#

```

```
S2(config)#
S2(config)#interface fa0/11
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan all
S2(config-if)#

```

### Tampilkan interface trunk di S1

```
S1#show interface trunk
Port Mode Encapsulation Status Native vlan
Fa0/11 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/11 1-1005

Port Vlans allowed and active in management domain
Fa0/11 1,10,20

Port Vlans in spanning tree forwarding state and not pruned
Fa0/11 1,10,20
S1#

```

### Tampilkan interface trunk di S2

```
S2#show interface trunk
Port Mode Encapsulation Status Native vlan
Fa0/11 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/11 1-1005

Port Vlans allowed and active in management domain
Fa0/11 1,10,20

Port Vlans in spanning tree forwarding state and not pruned
Fa0/11 1,10,20
S2#

```

Setelah mensetting trunk di S1 dan S2, kita akan tes Ping antar Laptop yang memiliki VLAN sama dan pastikan berhasil.

## Tes Ping dari Laptop1 ke Laptop2

```
Laptop1>ping 192.168.10.2
```

```
Pinging 192.168.10.2 with 32 bytes of data:
```

```
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
```

```
Ping statistics for 192.168.10.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

## Tes Ping dari Laptop3 ke Laptop4

```
Laptop3>ping 192.168.20.2
```

```
Pinging 192.168.20.2 with 32 bytes of data:
```

```
Reply from 192.168.20.2: bytes=32 time=0ms TTL=128
Reply from 192.168.20.2: bytes=32 time=0ms TTL=128
Reply from 192.168.20.2: bytes=32 time=1ms TTL=128
Reply from 192.168.20.2: bytes=32 time=0ms TTL=128
```

```
Ping statistics for 192.168.20.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

## Verifikasi

### Tampilkan show interface trunk di S1

```
S1#show interface trunk
```

```
Port Mode Encapsulation Status Native vlan
Fa0/11 on 802.1q trunking 1
```

```
Port Vlans allowed on trunk
Fa0/11 1-1005
```

```
Port Vlans allowed and active in management domain
Fa0/11 1,10,20
```

```
Port Vlans in spanning tree forwarding state and not pruned
Fa0/11 1,10,20
S1#
```

### Tampilkan show interface trunk di S2

```
S2#show interface trunk
Port Mode Encapsulation Status Native vlan
Fa0/11 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/11 1-1005

Port Vlans allowed and active in management domain
Fa0/11 1,10,20

Port Vlans in spanning tree forwarding state and not pruned
Fa0/11 1,10,20
S2#
```

Dari hasil output `show interface trunk` diatas, kita telah berhasil menghubungkan VLAN yang sama namun berada pada lokasi switch yang berbeda. Port trunk memungkinkan komunikasi lebih dari satu VLAN.

Ketika port switch disetting menjadi port trunk, maka di tampilan `show vlan brief` sudah tidak tampak lagi port switchnya.

### Tampilkan show vlan brief di S1

```
S1#show vlan brief
VLAN Name Status Ports
-----
1 default active
10 IT active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/12
20 Admin active Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
S1#
```

Perhatikan output diatas, port Fa0/11 sudah tidak lagi menjadi member VLAN 10.

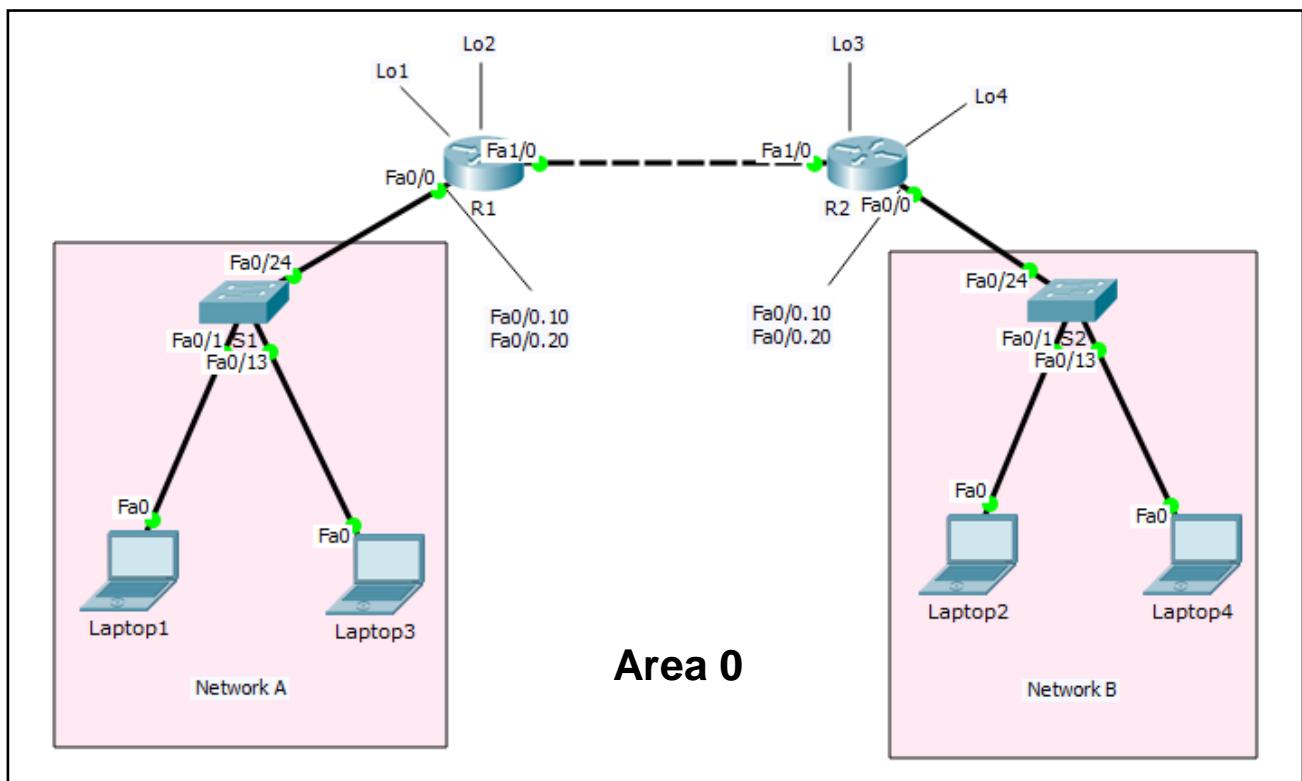
**Note: ulangi langkah yang sama diatas show vlan brief di S2**

### Review

1. Apa yang dimaksud dengan Native VLAN?
2. Apa yang terjadi jika S1 dan S2 memiliki Native VLAN yang berbeda? Jelaskan?
3. Bagaimana cara menambahkan, mengurangi, menghapus VLAN di port TRUNK?

# Lab 18. InterVLAN Routing

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0.10	192.168.10.254	255.255.255.0	N/A
	Fa0/0.20	192.168.20.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
	Lo1	172.16.1.1	255.255.255.0	N/A
	Lo2	172.16.2.2	255.255.255.0	N/A
R2	Fa0/0.10	192.168.30.254	255.255.255.0	N/A
	Fa0/0.20	192.168.40.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
	Lo3	172.16.3.3	255.255.255.0	N/A
	Lo4	172.16.4.4	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	192.168.10.1	255.255.255.0	192.168.10.254
Laptop2	NIC	192.168.20.2	255.255.255.0	192.168.20.254
Laptop3	NIC	192.168.30.3	255.255.255.0	192.168.30.254
Laptop4	NIC	192.168.40.4	255.255.255.0	192.168.40.254

## Tujuan

- Setting InterVLAN Routing

## Konsep Dasar

Bagaimana interVLAN routing bekerja?

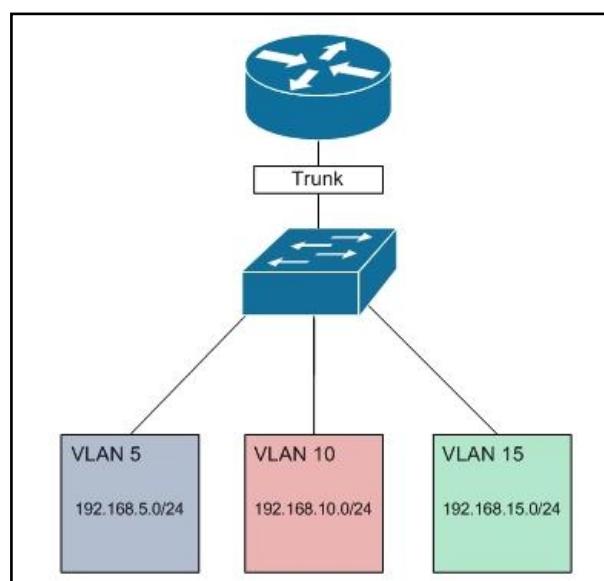
- Device network yang berbeda VLAN tidak dapat berkomunikasi dengan device lainnya tanpa router dan L3 switch, yang berfungsi untuk merutekan trafik antar VLAN
- Konfigurasi VLAN bermanfaat untuk mengontrol size broadcast domain dan menjaga trafik local
- Untuk mengkoneksikan end-devices didalam satu VLAN dengan VLAN lainnya dibutuhkan komunikasi InterVLAN
- InterVLAN membutuhkan interface fisik router atau sub-interface router sebagai gateway masing-masing VLAN dan L3 switch
- Penggunaan sub-interface router untuk InterVLAN disebut juga sebagai Router-on-Stick
- Sub-interface router untuk InterVLAN membutuhkan protocol trunking ISL atau 802.1Q

## **Konfigurasi Router-On-Stick**

1. Pilih Interface router
2. Setting sub-interface
3. Setting protocol trunking ISL atau 802.1Q

```
Router(config)# interface fa0/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip address <ip> <subnetmask>
Router(config-if)#
Router(config)# interface fa0/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip address <ip> <subnetmask>
Router(config-if)#
Router(config-if)# exit
Router(config)# interface fa0/0
Router(config)# no shutdown
```

**Contoh ilustrasi InterVLAN routing dengan ROS (Router-on-Stick) :**



## Konfigurasi

Login console ke S1 atau S2 untuk mempraktikkan **Lab 18-InterVLAN Routing**.

**Tabel VLAN**

Switch	VLAN	VLAN NAME	Interface	Network VLAN
S1	VLAN 10	IT	Fa0/1-Fa0/12	192.168.10.0/24
	VLAN 20	Admin	Fa0/13-Fa0/24	192.168.20.0/24
	Interface VLAN10			192.168.10.10
S2	VLAN 10	IT	Fa0/1-Fa0/12	192.168.30.0/24
	VLAN 20	Admin	Fa0/13-Fa0/24	192.168.40.0/24
	Interface VLAN10			192.168.30.10

**Tabel Addressing setelah VLAN disetting**

VLAN	Device	Interface	IP Address	Subnet Mask	Default Gateway
VLAN 10	Laptop1	NIC	192.168.10.1	255.255.255.0	192.168.10.254
	Laptop2	NIC	192.168.20.2	255.255.255.0	192.168.20.254
VLAN 20	Laptop3	NIC	192.168.30.3	255.255.255.0	192.168.30.254
	Laptop4	NIC	192.168.40.4	255.255.255.0	192.168.40.254

Dengan settingan VLAN seperti tabel VLAN dan tabel addressing diatas, untuk menghubungkan antar VLAN yang sama pada switch yang berbeda kita membutuhkan port switch dengan mode **Trunk**. Sedangkan untuk menghubungkan VLAN yang berbeda kita membutuhkan router atau L3 switch. Untuk menghemat resource interface router, maka kita akan menggunakan sub-interface untuk gateway masing-masing VLAN.

- Gateway VLAN 10 = Fa0/0.10
- Gateway VLAN 20 = Fa0/0.20

Trunking selain digunakan untuk switch-to-switch harus disetting juga di switch yang terhubung ke router untuk melewaskan lebih dari satu trafik VLAN. Di sisi port switch disetting mode trunk, di port router disetting trunking protocol misalnya dengan encapsulation dot1q.

Setelah mensetting trunk di S1 dan S2, kemudian setting encapsulation di Fa0/0 di R1 dan R2, agar VLAN 10 dan VLAN 20 yang berada di S1 dan S2 dapat saling berkomunikasi. Hal itu dibuktikan dengan tes Ping yang berhasil antar masing-masing Laptop di VLAN yang berbeda.

## Setting port trunk di S1

Dari gambar topologi diatas, S1 dan R1 terhubung melalui port Fa0/24 di switch dan Fa0/0 di R1. Oleh karena itu, kita akan mensetting port trunk di port Fa0/24 di S1.

```
S1(config)#
S1(config)#interface fa0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan all
S1(config-if)#

```

```
S2(config)#
S2(config)#interface fa0/24
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan all
S2(config-if)#

```

## Tampilkan interface trunk di S1

```
S1#show interface trunk
Port Mode Encapsulation Status Native vlan
Fa0/24 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/24 1-1005

Port Vlans allowed and active in management domain
Fa0/24 1,10,20

Port Vlans in spanning tree forwarding state and not pruned
Fa0/24 1,10,20
S1#

```

## Tampilkan interface trunk di S2

```
S2#show interface trunk
Port Mode Encapsulation Status Native vlan
Fa0/24 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/24 1-1005

Port Vlans allowed and active in management domain
Fa0/24 1,10,20

Port Vlans in spanning tree forwarding state and not pruned
Fa0/24 1,10,20
S2#

```

Setelah mensetting trunk di S1 dan S2, kita akan mensetting encapsulation dot1q di R1 dan R2.

## **Setting sub-interface di R1**

```
R1(config)#interface fa0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.254 255.255.255.0
R1(config-subif)#
R1(config-subif)#interface fa0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.30.254 255.255.255.0
R1(config-subif)#
R1(config-subif)#interface fa0/0
R1(config-if)#no shutdown
R1(config-if)#

```

## **Setting sub-interface di R2**

```
R2(config)#interface fa0/0.10
R2(config-subif)#encapsulation dot1q 10
R2(config-subif)#ip address 192.168.20.254 255.255.255.0
R2(config-subif)#
R2(config-subif)#interface fa0/0.20
R2(config-subif)#encapsulation dot1q 20
R2(config-subif)#ip address 192.168.40.254 255.255.255.0
R2(config-subif)#
R2(config-subif)#interface fa0/0
R2(config-if)#no shutdown
R2(config-if)#

```

Setelah gateway masing-masing VLAN di R1 dan R2 disetting, maka langkah selanjutnya yaitu tes Ping dari VLAN yang berbeda. Berdasarkan gambar topologi diatas, maka kita akan tes Ping dari Laptop1 ke Laptop3 dan dari Laptop2 ke Laptop4.

### **Tes Ping dari Laptop1 ke Laptop3 di Network A**

```
Laptop1>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=0ms TTL=127
Reply from 192.168.30.3: bytes=32 time=0ms TTL=127
Reply from 192.168.30.3: bytes=32 time=1ms TTL=127
Reply from 192.168.30.3: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.30.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

**Note: ulangi langkah yang sama diatas untuk tes Ping dari Laptop2 ke Laptop4 di Network B**

## Verifikasi

**Tampilkan** show ip interface brief **di R1**

```
R1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES NVRAM up up
FastEthernet0/0.10 192.168.10.254 YES manual up up
FastEthernet0/0.20 192.168.30.254 YES manual up up
FastEthernet1/0 12.12.12.1 YES manual up up
Loopback1 172.16.1.1 YES manual up up
Loopback2 172.16.2.2 YES manual up up
```

**Tampilkan** show ip interface brief **di R2**

```
R2#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES NVRAM up up
FastEthernet0/0.10 192.168.20.254 YES manual up up
FastEthernet0/0.20 192.168.40.254 YES manual up up
FastEthernet1/0 12.12.12.2 YES manual up up
Loopback1 172.16.3.3 YES manual up up
Loopback2 172.16.4.4 YES manual up up
```

Dari output yang dihasilkan **show ip interface brief** diatas, masing-masing VLAN yaitu VLAN 10 dan VLAN 20 telah memiliki gateway sendiri dan sudah bisa tes Ping antara VLAN 10 dan VLAN 20 di network internal S1 maupun S2.

## Review

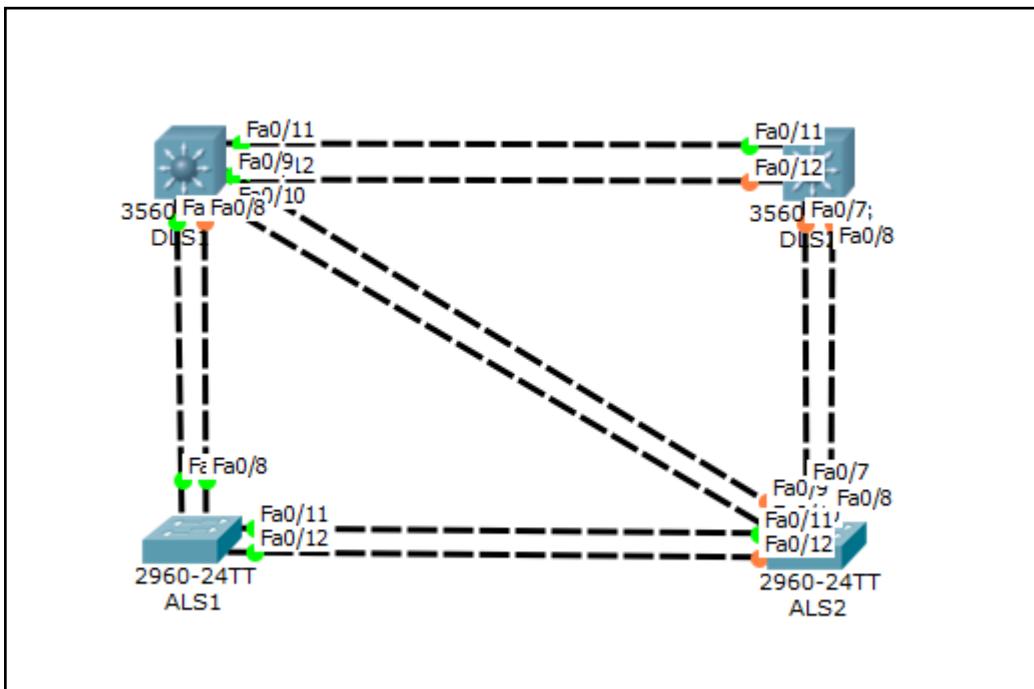
1. Dari lab InterVLAN Routing ini, VLAN 10 dan VLAN 20 hanya bisa berkomunikasi di satu network saja yaitu VLAN 10 bisa berkomunikasi di VLAN 20 di Network A saja atau VLAN 10 hanya bisa berkomunikasi dengan VLAN 20 di Network B saja.  
Bagaimana caranya supaya VLAN 10 di Network A bisa berkomunikasi dengan VLAN 10 di Network B, begitu juga dengan VLAN 20 di Network A bisa berkomunikasi dengan VLAN 20 di Network B?

Untuk menjawab pertanyaan no.1, gunakan solution **Lab 8-OSPF** dengan informasi Area 0 seperti gambar topologi diatas.

2. Praktikkan InterVLAN Routing dengan interface fisik router.
  - Gunakan topologi dan solution pada **Lab 17-VLAN Trunking**
  - Setting Trunking antara S1 dan S2
  - Setting interface Fa0/0 R1 sebagai Gateway VLAN 10
  - Setting interface Fa0/0 R2 sebagai Gateway VLAN 20
  - Terapkan static routing untuk menghubungkan VLAN 10 dan VLAN 20
  - Tes Ping antar VLAN yang berbeda
  - **Notes:** untuk mensetting interface fisik router sebagai gateway VLAN tidak membutuhkan konfigurasi protocol trunking ISL atau 802.1Q

# Lab 19. STP

## Topologi



## Tujuan

- Observasi STP

## Konsep Dasar

4 switch telah disetting seperti gambar topologi diatas terdiri dari 2 distribution layer switch seri 3560 dan 2 access layer switch seri 2960. Terdapat redundansi antara switch distribution dan access layer. Untuk menghindari kemungkinan terjadinya loop layer 2, maka STP secara logical menonaktifkan beberapa redundant link. Port switch warna hijau menandakan port aktif dan warna orange menandakan port non-aktif.

Secara default, spanning-tree aktif disetiap port. Ketika link baru aktif, kemudian spanning-tree akan melakukan listening dan learning sebelum akhirnya berpindah status menjadi forwarding. Pada saat itu switch sedang discover apakah terkoneksi ke switch lain atau end-device.

Dari topologi switch diatas, salah satu akan menjadi root bridge. Dan akan terjadi agreement switch mana yang akan aktif semua portnya dan sementara yang lainnya di non-aktif untuk menghindari loop. Komunikasi switch untuk menentukan mana yang menjadi root bridge dan mana yang non-root bridge dengan saling mengirimkan BPDU (Bridge Protocol Data Unit). Operasi spanning-tree berdasarkan mac-address switch.

## Verifikasi

### Tampilkan informasi spanning-tree disemua switch

Tampilan spanning-tree bisa saja berbeda untuk masing-masing topologi. Karena memang operasi spanning-tree berdasarkan mac-address switch. Dan switch memiliki mac-address yang berbeda-beda.

#### Tampilan spanning-tree DLS1

```
DLS1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000C.8560.A349
Cost 19
Port 7(FastEthernet0/7)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000C.CF75.B926
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/11 Desg FWD 19 128.11 P2p
Fa0/12 Desg FWD 19 128.12 P2p
Fa0/7 Root FWD 19 128.7 P2p
Fa0/8 Altn BLK 19 128.8 P2p
Fa0/10 Desg FWD 19 128.10 P2p
Fa0/9 Desg FWD 19 128.9 P2p

DLS1#
```

## Tampilan spanning-tree DLS2

```
DLS2#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000C.8560.A349
Cost 38
Port 11(FastEthernet0/11)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0060.5CAA.5A03
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/7 Altn BLK 19 128.7 P2p
Fa0/8 Altn BLK 19 128.8 P2p
Fa0/11 Root FWD 19 128.11 P2p
Fa0/12 Altn BLK 19 128.12 P2p

DLS2#
```

## Tampilan spanning-tree ALS1

```
ALS1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000C.8560.A349
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000C.8560.A349
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/7 Desg FWD 19 128.7 P2p
Fa0/8 Desg FWD 19 128.8 P2p
Fa0/11 Desg FWD 19 128.11 P2p
Fa0/12 Desg FWD 19 128.12 P2p

ALS1#
```

## Tampilan spanning-tree ALS2

```
ALS2#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000C.8560.A349
Cost 19
Port 11(FastEthernet0/11)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 00E0.8F21.2D8B
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/12 Altn BLK 19 128.12 P2p
Fa0/11 Root FWD 19 128.11 P2p
Fa0/10 Altn BLK 19 128.10 P2p
Fa0/9 Altn BLK 19 128.9 P2p
Fa0/8 Desg FWD 19 128.8 P2p
Fa0/7 Desg FWD 19 128.7 P2p
```

ALS2#

**sts** menyatakan status port, **FWD** = forwarding, **BLK** = blocking

Dari output diatas :

- Port antar switch-to-switch terdapat minimal satu port yang non-aktif (BLK) kecuali root bridge
- Port non-aktif atau blocking bisa terjadi di switch distribution atau access-layer
- Apabila semua port memiliki settingan default, interface dengan nomor interface yang lebih tinggi yang akan berubah status menjadi blocking
- Port menjadi blocking karena switch mendeteksi dua jalur antar switch yang sama
- Bridging loop akan terjadi ketika salah satu switch tidak mendisable link secara logical

## Review

### 1. Tampilkan kembali spanning-tree di ALS1

```
ALS1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000C.8560.A349
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000C.8560.A349
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/7 Desg FWD 19 128.7 P2p
Fa0/8 Desg FWD 19 128.8 P2p
Fa0/11 Desg FWD 19 128.11 P2p
Fa0/12 Desg FWD 19 128.12 P2p

ALS1#
```

Setelah melihat output diatas, coba jawab pertanyaan berikut ini :

- a) Switch yang mana yang menjadi root bridge?
- b) Bagaimana cara mengidentifikasi root bridge?
- c) Mengapa switch tersebut terpilih menjadi root bridge?
- d) Apa penyebab port switch menjadi blocking?

### 2. Apabila root bridge dihilangkan dari topology switch diatas, mana yang akan menjadi root bridge? Pilihlah jawaban dibawah ini: a, b, ataukah c?

```
ALS1(config)#int range fa0/1-24
ALS1(config-if-range)#shutdown
```

#### a. DLS1

```
DLS1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000C.CF75.B926
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000C.CF75.B926
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Fa0/11 Desg FWD 19 128.11 P2p  
Fa0/12 Desg FWD 19 128.12 P2p  
Fa0/10 Desg FWD 19 128.10 P2p  
Fa0/9 Desg FWD 19 128.9 P2p
```

```
DLS1#
```

### b. DLS2

```
DLS2#show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee  
Root ID Priority 32769  
Address 000C.CF75.B926  
Cost 19  
Port 11(FastEthernet0/11)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)  
Address 0060.5CAA.5A03  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 20
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Fa0/7 Desg FWD 19 128.7 P2p  
Fa0/8 Desg FWD 19 128.8 P2p  
Fa0/11 Root FWD 19 128.11 P2p  
Fa0/12 Altn BLK 19 128.12 P2p
```

```
DLS2#
```

### c. ALS2

```
ALS2#show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee  
Root ID Priority 32769  
Address 000C.CF75.B926  
Cost 19  
Port 9(FastEthernet0/9)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)  
Address 00E0.8F21.2D8B  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 20
```

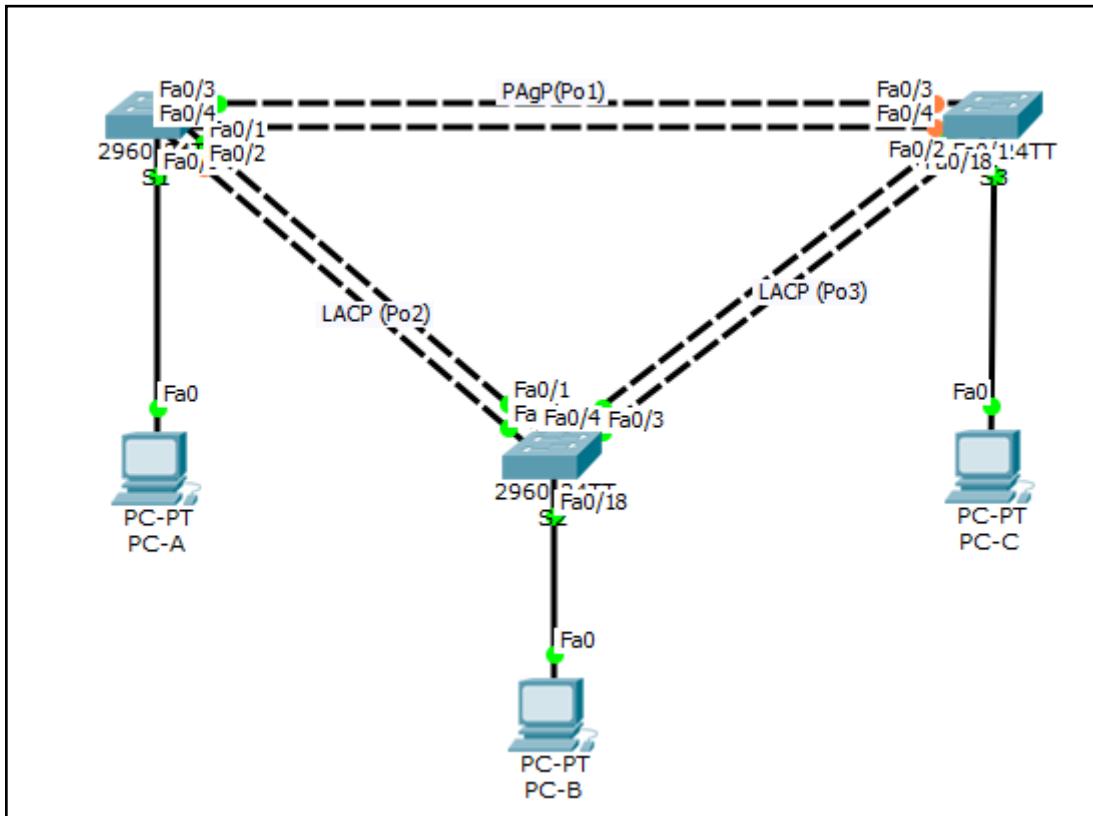
```
Interface Role Sts Cost Prio.Nbr Type
```

```
Fa0/10 Altn BLK 19 128.10 P2p
Fa0/9 Root FWD 19 128.9 P2p
Fa0/8 Altn BLK 19 128.8 P2p
Fa0/7 Altn BLK 19 128.7 P2p
```

```
ALS2#
```

# Lab 20. EtherChannel

## Topologi



Tabel addressing

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.99.11	255.255.255.0
S2	VLAN 99	192.168.99.12	255.255.255.0
S3	VLAN 99	192.168.99.13	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.10.2	255.255.255.0
PC-C	NIC	192.168.10.3	255.255.255.0

## Tujuan

- Part 1: Setting basic switch
- Part 2: Setting PAgP
- Part 3: Setting LACP

## Konsep Dasar

### EtherChannel

- EtherChannel digunakan untuk menggabungkan multiple interface fisik menjadi satu interface logical dengan tujuan load sharing dan redundancy
- EtherChannel bisa dikonfigurasi :
  - Secara manual/static
  - Dinamis melalui PAgP (Port Aggregation Protocol)
  - Dinamis melalui LACP (IEEE 802.1AD – Link Aggregation Control Protocol)
- Cisco 3560 support 8 EtherChannel interface (800 Mbps dengan FastEthernet Interface atau 8 Gbps dengan Gigabit Interface)

**Protocol dynamic EtherChannel tergantung dari keyword berikut :**

- PAgP : Auto dan Desirable
- LACP : Passive dan Active

### Konfigurasi

#### Part 1: Konfigurasi Basic Switch

- a. Matikan semua switchports kecuali yang terkoneksi ke PC
- b. Konfigurasi VLAN 99 dan beri nama **Management**
- c. Konfigurasi VLAN 10 dan beri nama **Staff**
- d. Konfigurasi switch ports yang terkoneksi ke PC dengan VLAN 10
- e. Setting IP address PC sesuai tabel addressing diatas
- f. Simpan konfigurasi

#### Part 2: Konfigurasi PAgP

PAgP adalah protocol link aggregation buatan Cisco. Pada bagian ini, link antara S1 dan S3 akan disetting EtherChannel menggunakan PAgP.

#### Step 1: Konfigurasi PAgP di S1 dan S3

Untuk link antara S1 dan S3, konfigurasi port di S1 dengan mode PAgP desirable dan port di S3 mode PAgP auto. Aktikan port setelah mode PAgP selesai disetting.

```
S1(config)# interface range f0/3-4
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown
```

```
S3(config)# interface range f0/3-4
S3(config-if-range)# channel-group 1 mode auto
S3(config-if-range)# no shutdown
```

#### Step 2: Tampilkan output konfigurasi

Sekarang interface F0/3, F0/4, dan Po1 (Port-channel1) pada S1 dan S3 sudah berfungsi dengan secara operasional dengan mode administrative dynamic auto. Verifikasi konfigurasi menggunakan perintah **show run interface interface-id** dan **show interfaces interface-id switchport**.

```
S1# show run interface f0/3
```

```
Building configuration...
```

```
Current configuration : 103 bytes
```

```
!
```

```
interface FastEthernet0/3
```

```
  channel-group 1 mode desirable
```

```
S1# show interfaces f0/3 switchport
```

```
Name: Fa0/3
```

```
Switchport: Enabled
```

```
Administrative Mode: dynamic auto
```

```
Operational Mode: static access (member of bundle Po1)
```

```
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: native
```

```
Negotiation of Trunking: On
```

```
Access Mode VLAN: 1 (default)
```

```
Trunking Native Mode VLAN: 1 (default)
```

```
Administrative Native VLAN tagging: enabled
```

```
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
```

```
Administrative private-vlan mapping: none
```

```
Administrative private-vlan trunk native VLAN: none
```

```
Administrative private-vlan trunk Native VLAN tagging: enabled
```

```
Administrative private-vlan trunk encapsulation: dot1q
```

```
Administrative private-vlan trunk normal VLANs: none
```

```
Administrative private-vlan trunk associations: none
```

```
Administrative private-vlan trunk mappings: none
```

```
Operational private-vlan: none
```

```
Trunking VLANs Enabled: ALL
```

```
Pruning VLANs Enabled: 2-1001
```

```
Capture Mode Disabled
```

```
Capture VLANs Allowed: ALL
```

```
Protected: false
```

```
Unknown unicast blocked: disabled
```

```
Unknown multicast blocked: disabled
```

```
Appliance trust: none
```

### Step 3: Verifikasi bahwa port sudah di aggregasi

```
S1# show etherchannel summary
```

```
Flags: D - down P - bundled in port-channel
```

```
I - stand-alone S - suspended
```

```
H - Hot-standby (LACP only)
```

```
R - Layer3 S - Layer2
```

```
U - in use f - failed to allocate aggregator
```

```
M - not in use, minimum links not met
```

```
u - unsuitable for bundling
```

```
w - waiting to be aggregated
```

```
d - default port
```

```
Number of channel-groups in use: 1
```

```
Number of aggregators: 1
```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	PAgP	Fa0/3 (P) Fa0/4 (P)

```
S3# show etherchannel summary
Flags: D - down P - bundled in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3 S - Layer2
      U - in use f - failed to allocate aggregator

      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
```

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	PAgP	Fa0/3 (P) Fa0/4 (P)

Dari output diatas,

- S menyatakan port-channel Layer 2 EtherChannel
- U menyatakan EtherChannel sedang digunakan
- P menyatakan port yang dibundle dengan port-channel

#### Step 4: Konfigurasi trunk port.

Setelah port di aggregasi, kemudian kita konfigurasi port Po1 di S1 dan S3 sebagai trunk dan setting Po1 menjadi native VLAN 99.

```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
```

```
S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
```

#### Step 5: Verifikasi bahwa port-channel sudah dikonfigurasi sebagai trunk.

Ketikkan perintah `show run interface interface-id` di S1 dan S3. Perhatikan, ketika kita mensetting port-channel menjadi trunk akan memberikan efek terhadap member link bundle.

```
S1# show run interface po1
Building configuration...

Current configuration : 92 bytes
!
interface Port-channel1
```

```

switchport trunk native vlan 99
switchport mode trunk
end

```

```

S1# show run interface f0/3
Building configuration...

Current configuration : 126 bytes
!
interface FastEthernet0/3
    switchport trunk native vlan 99
    switchport mode trunk
    channel-group 1 mode desirable
end

```

## Part 3: Konfigurasi LACP

LACP adalah protocol link aggregation yang bersifat open source dan dikembangkan oleh IEEE. Pada bagian 3, link antara S1 dan S2, dan link antara S2 dan S3 akan dikonfigurasi menggunakan LACP. Link individu akan dikonfigurasi trunk sebelum link dimasukkan ke link bundle sebagai EtherChannel.

### Step 1: Konfigurasi LACP antara S1 dan S2.

```

S1(config)# interface range f0/1-2
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99
S1(config-if-range)# channel-group 2 mode active
S1(config-if-range)# no shutdown

```

```

S2(config)# interface range f0/1-2
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 2 mode passive
S2(config-if-range)# no shutdown

```

### Step 2: Verifikasi bahwa port sudah diaggregasi.

```

S1# show etherchannel summary
Flags: D - down          P - bundled in port-channel
      I - stand-alone   s - suspended
      H - Hot-standby   (LACP only)
      R - Layer3         S - Layer2
      U - in use         f - failed to allocate aggregator

      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 2
Number of aggregators:           2

```

Group	Port-channel	Protocol	Ports

1	Po1 (SU)	PAgP	Fa0/3 (P)	Fa0/4 (P)
2	Po2 (SU)	LACP	Fa0/1 (P)	Fa0/2 (P)

```
S2# show etherchannel summary
```

Flags: D - down P - bundled in port-channel  
I - stand-alone s - suspended  
H - Hot-standby (LACP only)  
R - Layer3 S - Layer2  
U - in use f - failed to allocate aggregator  
M - not in use, minimum links not met  
u - unsuitable for bundling  
w - waiting to be aggregated  
d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

2	Po2 (SU)	LACP	Fa0/1 (P) Fa0/2 (P)
---	----------	------	---------------------

### Step 3: Konfigurasi LACP antara S2 dan S3.

- Konfigurasi link antara S2 dan S3 sebagai Po3 dan menggunakan LACP sebagai link aggregation protocol.

```
S2(config)# interface range f0/3-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 3 mode active
S2(config-if-range)# no shutdown
```

```
S3(config)# interface range f0/1-2
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
S3(config-if-range)# channel-group 3 mode passive
S3(config-if-range)# no shutdown
```

- Verifikasi bahwa EtherChannel sudah terbentuk.

```
S2# show etherchannel summary
```

Flags: D - down P - bundled in port-channel  
I - stand-alone s - suspended  
H - Hot-standby (LACP only)  
R - Layer3 S - Layer2  
U - in use f - failed to allocate aggregator  
M - not in use, minimum links not met  
u - unsuitable for bundling  
w - waiting to be aggregated  
d - default port

Number of channel-groups in use: 2

```

Number of aggregators: 2

Group Port-channel Protocol Ports
-----+-----+-----+
2     Po2 (SU)      LACP    Fa0/1 (P)   Fa0/2 (P)
3     Po3 (SU)      LACP    Fa0/3 (P)   Fa0/4 (P)

```

```

S3# show etherchannel summary

Flags: D - down      P - bundled in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use       f - failed to allocate aggregator

      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

```

```

Number of channel-groups in use: 2
Number of aggregators: 2

Group Port-channel Protocol Ports
-----+-----+-----+
1     Po1 (SU)      PAgP    Fa0/3 (P)   Fa0/4 (P)
3     Po3 (SU)      LACP    Fa0/1 (P)   Fa0/2 (P)

```

## Verifikasi

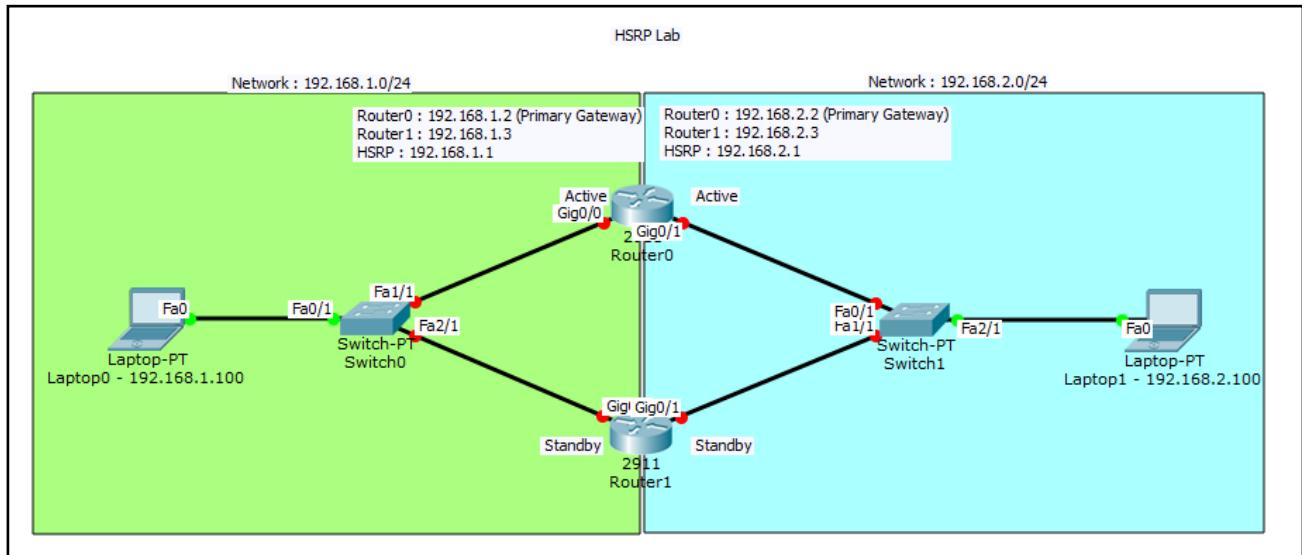
Verifikasi semua device bisa saling ping pada VLAN yang sama. Jika gagal, lakukan troubleshooting sampai bisa normal konektivitas end-to-end-nya.

## Review

1. Apakah load sharing di EtherChannel akan sama rata disetiap interface membernya?

# Lab 21. HSRP

## Topologi



## Tabel addressing

- Network 192.168.1.0/24
  - Router0 : 192.168.1.2 (GigabitEthernet 0/0)
  - Router1 : 192.168.1.3 (GigabitEthernet 0/0)
- Network 192.168.2.0/24
  - Router0 : 192.168.2.2 (GigabitEthernet 0/1)
  - Router1 : 192.168.2.3 (GigabitEthernet 0/1)

## HSRP group

- HSRP Group 1 :
  - IP address : 192.168.1.1
  - Router0 with priority 120 (preemption enabled)
  - Router1 with HSRP default priority (100)
- HSRP Group 2 :
  - IP address : 192.168.2.1
  - Router0 with priority 120 (preemption enabled)
  - Router1 with HSRP default priority (100)

## Tujuan

- Setting HSRP

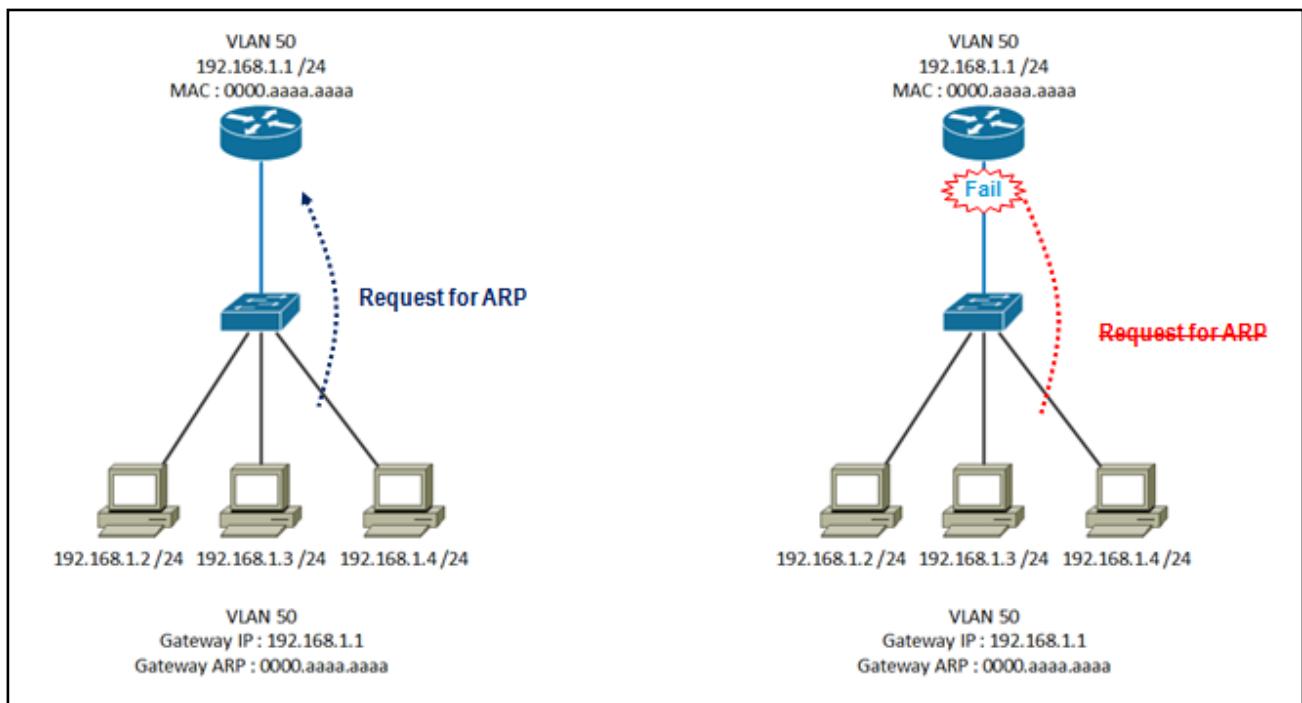
## Konsep Dasar

### HSRP

- Redundancy Gateway, meningkatkan availibilitas gateway dalam jaringan
- Teknologi Cisco Proprietary, hanya perangkat Cisco
- Implementasi dua perangkat Router/Switch L3 dalam satu grup HSRP
- Salah satu Router/Switch L3 berperan sebagai Gateway (HSRP Active/Primary)
- Verifikasi keberadaan member group dengan saling bertukar Hello Message (multicast 224.0.0.2)
- Interface fisik atau Interface VLAN sebagai Gateway

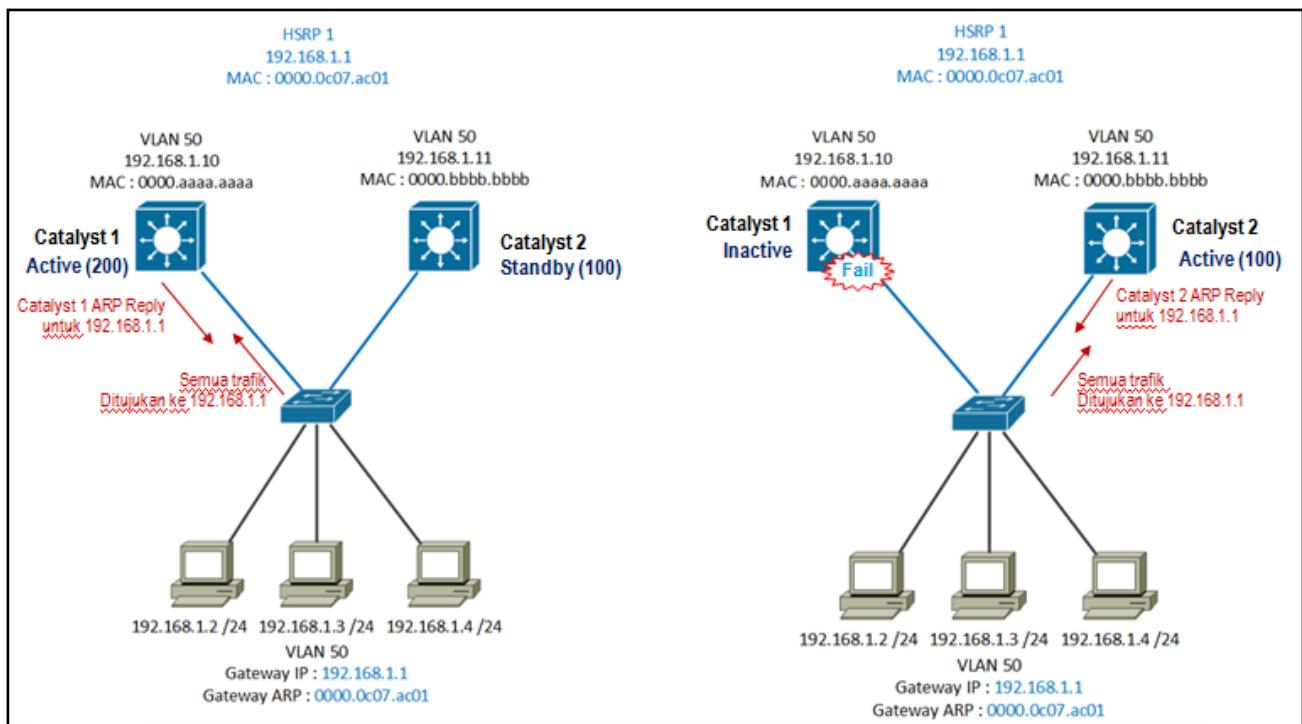
### Contoh implementasi single gateway LAN

Apabila gateway down, maka koneksi tidak dapat dilakukan



Oleh karena itu, redundancy gateway sangat dibutuhkan untuk network yang critical.

## Contoh implementasi redundancy gateway



Koneksi pertama dilakukan melalui Catalyst 1 sebagai primary gateway, kemudian terjadi down di Catalyst 1 dan komunikasi dialihkan secara otomatis ke Catalyst 2. Tingkat prioritas HSRP yang tinggi yang akan menjadi primary gateway. Apabila Catalyst 1 sudah kembali normal, maka komunikasi akan kembali seperti semula yaitu melalui Catalyst 1.

### 4 Langkah mudah setting HSRP basic

1. Setting IP address router / VLAN interface
2. Setting Standby Group dan Virtual IP
3. Setting priority HSRP
4. Setting preempt (opsional)

```
Router(config)# interface Vlan 50
Router(config-if)# ip address 192.168.1.10 255.255.255.0

Router(config-if)# standby 1 ip 192.168.1.1

Router(config-if)# standby 1 priority 200

Router(config-if)# standby 1 preempt
```

## Konfigurasi

### **Setting HSRP di Router0**

```
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 1 ip 192.168.1.1
 standby 1 priority 120
 standby 1 preempt
!
interface GigabitEthernet0/1
 ip address 192.168.2.2 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 2 ip 192.168.2.1
 standby 2 priority 120
 standby 2 preempt
```

### **Setting HSRP di Router1**

```
interface GigabitEthernet0/0
 ip address 192.168.1.3 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 1 ip 192.168.1.1
!
interface GigabitEthernet0/1
 ip address 192.168.2.3 255.255.255.0
 duplex auto
 speed auto
 standby version 2
 standby 2 ip 192.168.2.1
```

## Verifikasi

Untuk memverifikasi konfigurasi yang sudah kita setting benar atau belum, lakukan tes berikut ini :

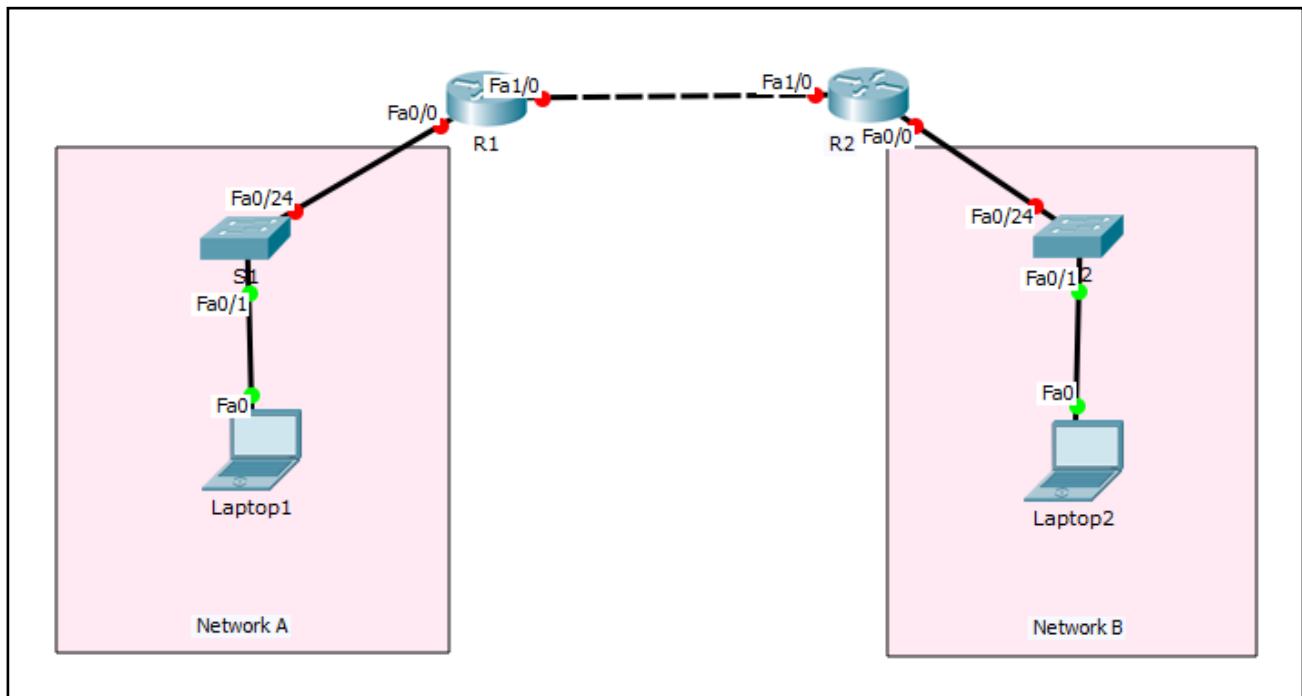
- i) Tes Ping dari Laptop0 ke Laptop1
- ii) Komunikasi normal akan melalui Router0
- iii) Tes Ping lagi dari Laptop0 ke Laptop1 dan secara bersamaan matikan semua interface Router0
- iv) Perhatikan output debug di Router1, maka akan tampil output bahwa Router1 akan menjadi Active HSRP

## Review

1. Apa bedanya HSRP version 1 dan version 2?

# Lab 22. DHCP

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.254	255.255.255.0	N/A
	Fa1/0	12.12.12.1	255.255.255.0	N/A
R2	Fa0/0	192.168.2.254	255.255.255.0	N/A
	Fa1/0	12.12.12.2	255.255.255.0	N/A
S1	N/A	VLAN 1	N/A	N/A
S2	N/A	VLAN 1	N/A	N/A
Laptop1	NIC	DHCP	-	-
Laptop2	NIC	DHCP	-	-

## Tujuan

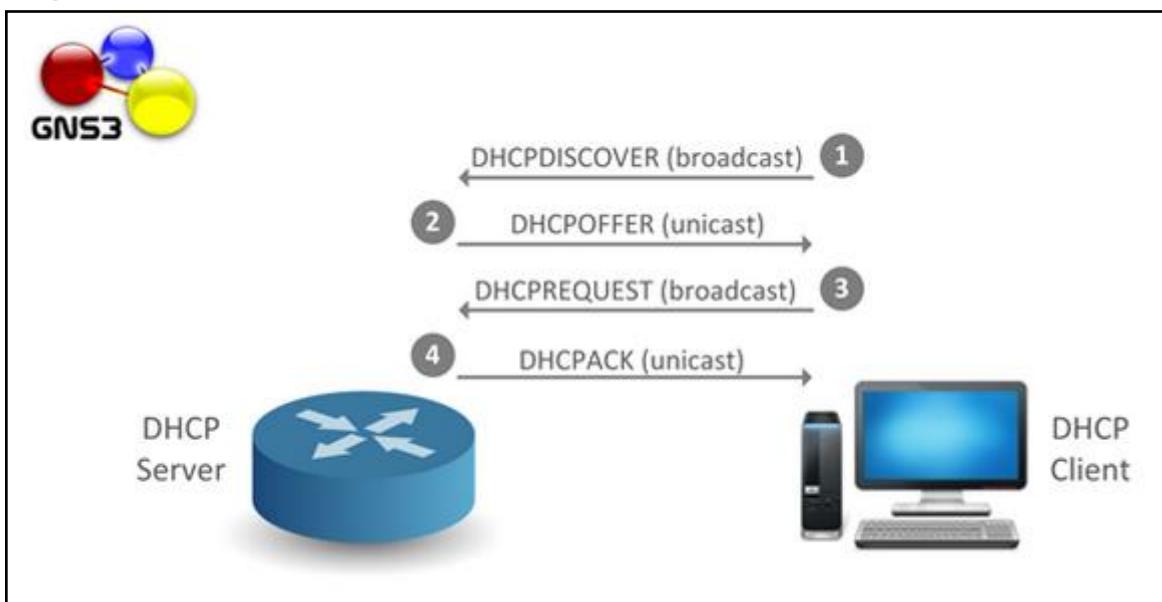
- Setting DHCP

## Konsep Dasar

### DHCP

- DHCP (Dynamic Host Configuration Protocol)
- Berfungsi memberikan IP address kepada host secara dinamis
- DHCP beroperasi secara klien-server

### Proses pertukaran data antara DHCP Server dan DHCP klien



## Konfigurasi

Login console ke R1 dan R2 untuk mempraktikkan **Lab 22-DHCP**.

Untuk mensetting DHCP di R1, berikut ini command yang digunakan :

```
R1(config)#ip dhcp excluded-address 192.168.1.10 192.168.1.50
R1(config)#
R1(config)#ip dhcp pool Pool_R1
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.254
R1(dhcp-config)# dns-server 192.168.1.254
R1(dhcp-config)# lease 0 23 59
R1(dhcp-config)# domain-name NIXTRAIN.com
R1(dhcp-config)#

```

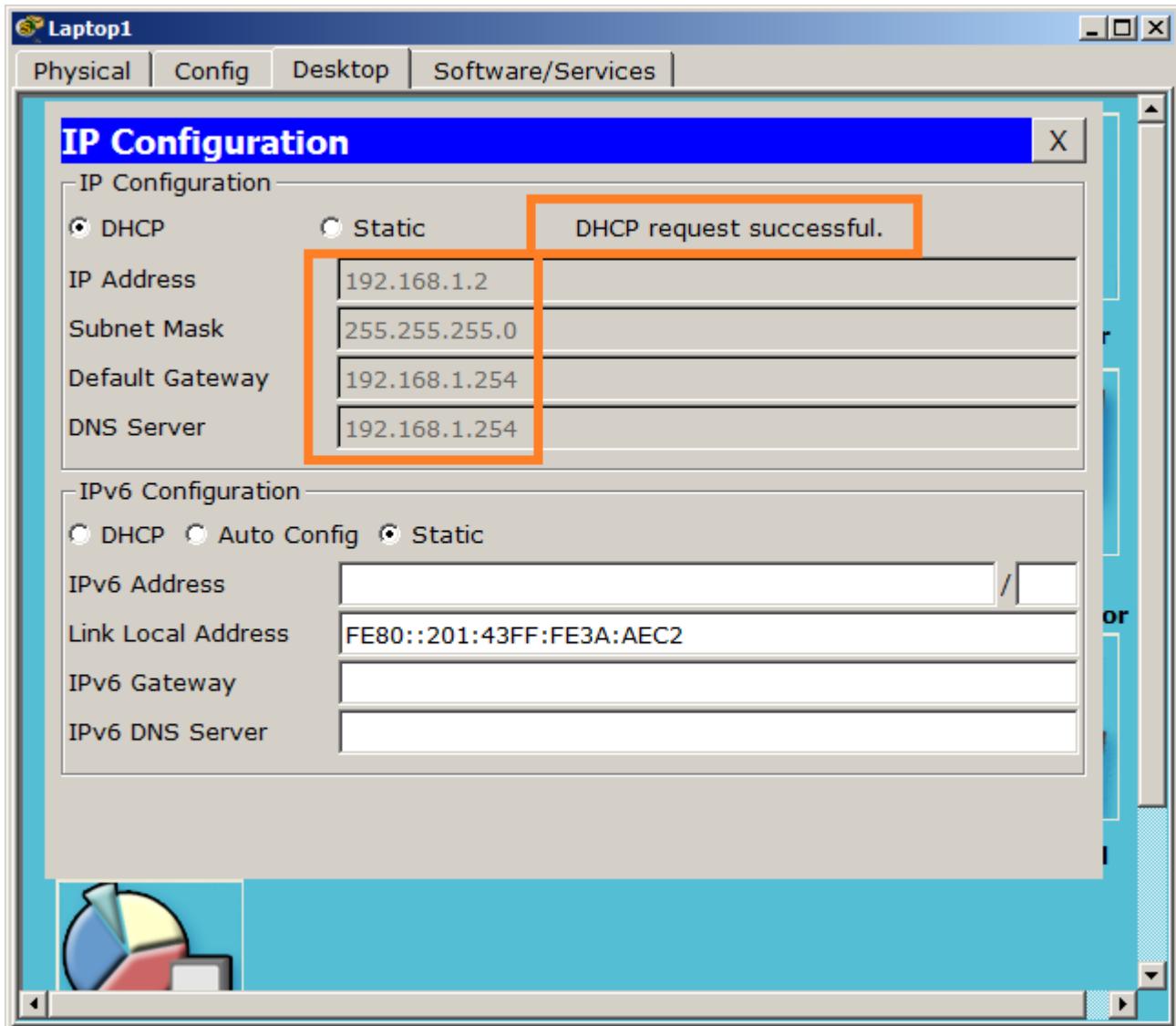
Keterangan:

**excluded-address** : untuk menentukan IP yang tidak boleh di lease oleh DHCP, biasanya berupa IP static untuk server / printer  
**pool** : tentukan nama pool DHCP, misal untuk network 192.168.1.0 namanya Pool\_R1  
**network** : menentukan network DHCP  
**default-router** : menentukan default gateway untuk klien  
**dns-server** : menentukan dns server untuk klien  
**lease** : lama waktu penggunaan IP dhcp  
**domain-name** : menentukan nama domain

**Note: ulangi langkah yang sama diatas untuk mensetting DHCP server di R2**

## **Verifikasi**

Klik Laptop1 -> Pilih Desktop -> Pilih IP Configuration -> Pilih DHCP



Dari tampilan diatas, DHCP telah berhasil disetting di R1.

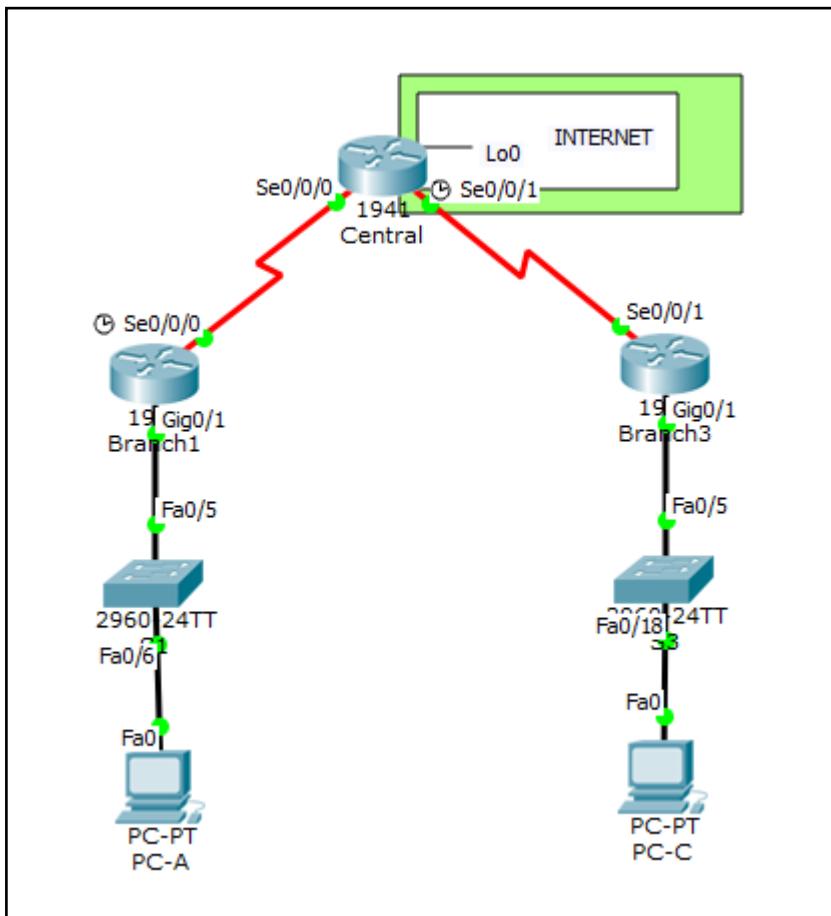
**Note: ulangi langkah yang sama diatas untuk menampilkan DHCP klien di Laptop2**

## **Review**

1. Terkait DHCP, cisco router dapat digunakan menjadi berapa tipe DHCP?
2. Apa yang dimaksud dengan DHCP relay agent? Praktikkan dengan topologi diatas, lokasi DHCP server berada di Network B/R2, dan klien berada di Network A?

# Lab 23. PPP

## Topologi



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
Branch1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
Central	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
Branch3	Lo0	209.165.200.225	255.255.255.224	N/A
	G0/1	192.168.3.1	255.255.255.0	N/A
PC-A	S0/0/1	10.2.2.1	255.255.255.252	N/A
	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

## Tujuan

Part 1: Setting routing

Part 2: Setting enkapsulasi PPP

## Konfigurasi

### Part 1. Setting routing

Setting routing OSPF Area 1

- i) Aktifkan OSPF single-area pada semua router dan menggunakan proses ID 1. Tambahkan semua network ke dalam proses OSPF kecuali 209.165.200.224/27.
- ii) Konfigurasi default route ke Internet pada router Central menggunakan Lo0 sebagai exit interface dan lakukan redistribusi default route ke dalam proses OSPF.
- iii) Verifikasi konfigurasi router OSPF

### Part 2. Setting enkapsulasi PPP

#### 1. Tampilkan enkapsulasi default serial

Di router, ketikkan perintah `show interfaces serial` untuk menampilkan enkapsulasi serial yang sedang dipakai.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
    Keepalive set (10 sec)
    Last input 00:00:02, output 00:00:05, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
      1003 packets input, 78348 bytes, 0 no buffer
      Received 527 broadcasts (0 IP multicasts)
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      1090 packets output, 80262 bytes, 0 underruns
      0 output errors, 0 collisions, 3 interface resets
      0 unknown protocol drops
      0 output buffer failures, 0 output buffers swapped out
      2 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

**Note:** Harap diingat bahwa HDLC sebagai default enkapsulasi pada serial router Cisco.

## 2. Ubah enkapsulasi serial menjadi PPP.

- i) Ketikkan command **encapsulation ppp** di interface S0/0/0 interface pada router Branch1 untuk mengubah enkapsulasi HDLC menjadi PPP.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
Branch1(config-if)#

```

- ii) Ketikkan perintah untuk menampilkan line status dan line protocol di interface S0/0/0 pada router Branch1. Line protocol statusnya down karena enkapsulasi di router Central yang mengarah ke Branch1 belum dikonfigurasi.

```
Branch1# show ip interface brief
Line status is up, and line protocol is down.
Branch1# show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned    YES unset administratively down down
GigabitEthernet0/0   unassigned    YES unset administratively down down
GigabitEthernet0/1   192.168.1.1  YES manual up           up
Serial0/0/0          10.1.1.1     YES manual up           down
Serial0/0/1          unassigned    YES unset administratively down down

```

- iii) Ketikkan perintah **encapsulation ppp** di interface S0/0/0 pada router Central router untuk mengatasi enkapsulasi “*problem mismatch encapsulation*”. Back-to-back koneksi serial harus memiliki enkapsulasi yang sama agar bisa berkomunikasi.

```
Central(config)# interface s0/0/0
Central(config-if)# encapsulation ppp
Central(config-if)#

```

- iv) Verifikasi di interface S0/0/0 antara router Branch1 dan Central apakah line status dan line protocolnya sudah up/up dan enkapsulasinya PPP?

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
    Keepalive set (10 sec)
    Last input 00:00:00, output 00:00:00, output hang never
    Last clearing of "show interface" counters 00:03:58
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo

```

```

Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    77 packets input, 4636 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    117 packets output, 5800 bytes, 0 underruns
    0 output errors, 0 collisions, 8 interface resets
    22 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    18 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

```

```

Central# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
    Hardware is WIC MBRD Serial
    Internet address is 10.1.1.2/30
    MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
    Open: IPCP, CDPCP, loopback not set
    Keepalive set (10 sec)
    Last input 00:00:02, output 00:00:03, output hang never
    Last clearing of "show interface" counters 00:01:20
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
        41 packets input, 2811 bytes, 0 no buffer
        Received 0 broadcasts (0 IP multicasts)
        0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        40 packets output, 2739 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 unknown protocol drops
        0 output buffer failures, 0 output buffers swapped out
        0 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

```

**Note :** Harap diingat enkapsulasi serial antar router harus sama. Jika tidak, maka koneksi tidak bisa terbentuk alias interface tetap down.

- v) Ketikkan perintah **encapsulation ppp** di interface S0/0/0 pada router Branch1 router untuk memperbaiki enkapsulasi yang mismatch (tidak sama).

```

Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp

```

- vi) Ketikkan perintah **show ip interface brief** pada router Branch1 dan Central setelah network konvergen. Lihat pada line status dan line protocol, pastikan semua up/up.

```
Branch1# show ip interface brief
Interface IP-Address OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned YES unset administratively down down
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 192.168.1.1 YES manual up up
Serial0/0/0 10.1.1.1 YES manual up up
Serial0/0/1 unassigned YES unset administratively down down
```

```
Central# show ip interface brief
Interface IP-Address OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned YES unset administratively down down
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 10.1.1.2 YES manual up up
Serial0/0/1 10.2.2.2 YES manual up up
Loopback0 209.165.200.225 YES manual up up
```

- vii) Verifikasi interface S0/0/0 di router Branch1 dan Central menggunakan PPP.

```
Branch1# show interfaces s0/0/0
Central# show interfaces s0/0/0
```

- viii) Konfigurasi enkapsulasi serial antara router Central dengan Branch3 menjadi PPP.

```
Central(config)# interface s0/0/1
Central(config-if)# encapsulation ppp
Central(config-if)#
```

```
Branch3(config)# interface s0/0/1
Branch3(config-if)# encapsulation ppp
Branch3(config-if)#
```

## Verifikasi

Verifikasi konektivitas end-to-end dengan cara tes Ping antar PC-A dan PC-C. Pastikan bisa saling ping antara router Central dan Branch3 dan Routing OSPF berjalan normal.

## Review

1. Apa yang dimaksud dengan PPP?
2. Jelaskan tujuan kita mensetting PPP pada WAN?
3. Dengan menggunakan topologi dan addressing yang sama, praktikkan enkapsulasi PPP dengan CHAP?
4. Jelaskan perbedaan PPP dengan enkapsulasi WAN Frame Relay?
5. Selain PPP dan Frame Relay, sebutkan dan jelaskan jenis enkapsulasi WAN lainnya?

## Sumber Referensi

- [01] [www.cisco.com](http://www.cisco.com)
- [02] [learningnetwork.cisco.com](http://learningnetwork.cisco.com)
- [03] [www.netacad.com](http://www.netacad.com)
- [04] [www.gns3.net](http://www.gns3.net)
- [05] [blog.ine.com](http://blog.ine.com)
- [06] [networklessons.com](http://networklessons.com)
- [07] [www.networkonlineacademy.com](http://www.networkonlineacademy.com)
- [08] [www.networkers-online.com](http://www.networkers-online.com)
- [09] [routemyworld.com](http://routemyworld.com)
- [10] [www.micronicstraining.com](http://www.micronicstraining.com)
- [11] [www.jawdat.com](http://www.jawdat.com)
- [12] [blog.initialdraft.com](http://blog.initialdraft.com)
- [13] [it-certification-network.blogspot.com](http://it-certification-network.blogspot.com)
- [14] [sysnetnotes.blogspot.com](http://sysnetnotes.blogspot.com)
- [15] [simplecisco.wordpress.com](http://simplecisco.wordpress.com)
- [16] [mycciegeekblog.wordpress.com](http://mycciegeekblog.wordpress.com)
- [17] [cciepursuit.wordpress.com](http://cciepursuit.wordpress.com)
- [18] [cciethebeginning.wordpress.com](http://cciethebeginning.wordpress.com)
- [19] [certificationkits.com](http://certificationkits.com)
- [20] [www.freeccnaworkbook.com](http://www.freeccnaworkbook.com)
- [21] [himawan.blogsome.com](http://himawan.blogsome.com)
- [22] [community.spiceworks.com](http://community.spiceworks.com)
- [23] [www.packetu.com](http://www.packetu.com)
- [24] [www.ccie.net](http://www.ccie.net)
- [25] [www.thebryantadvantage.com](http://www.thebryantadvantage.com)
- [26] [www.routerlabs.de](http://www.routerlabs.de)
- [27] [blog.alwaysthenetwork.com](http://blog.alwaysthenetwork.com)
- [28] [www.ccie-study.com](http://www.ccie-study.com)
- [29] [www.packettracernetwork.com](http://www.packettracernetwork.com)
- [30] [blog.pluralsight.com](http://blog.pluralsight.com)
- [31] [resources.intenseschool.com](http://resources.intenseschool.com)

## Biografi Penulis



Nama lengkap Agus Setiawan, biasa dipanggil Agus atau Wawan. Saat ini aktif menjadi pengajar tidak tetap di salah satu kampus di Bandung, Jawa Barat. Selain mengajar di kampus, Agus juga menjadi trainer sekaligus CEO & Founder di training center Nixtrain. Berbekal dari pengalaman yang dimilikinya, Agus memberanikan diri membuka usaha IT Solution dan Training Center yang menjadi passionnya sejak mahasiswa.

Di awali dari hobi dan kesenangannya ngoprek Linux/Unix saat semester 3, kemudian ngoprek network sampai memiliki sertifikasi SCSAS (Sun Certified Solaris Associate), CCAI (Cisco Certified Academy Instructor) dan MTCAT (MikroTik Certified Academy Trainer), ternyata bagi Agus belum memberikan kenyamanan tersendiri dan merasa masih ada yang kurang yaitu belum berbagi ke sesama, oleh karena itu, Agus mencoba membuat komunitas group facebook "Road to CCNA" tahun 2013 untuk saling bertukar pengetahuan dan pengalamannya agar dapat membantu orang-orang yang ingin belajar networking.

Dengan perkembangan member group yang semakin banyak dan minimnya bahan bacaan mengenai CCNA di Indonesia, Agus meluangkan waktunya untuk membuat ebook "CCNA Lab Guide" yang dibagikan gratis kepada para pembaca yang berminat mempelajari networking dengan harapan semakin banyak orang yang terbantu dengan adanya ebook tersebut.

CCNA saat ini masih menjadi sertifikasi yang paling banyak dicari oleh perusahaan, oleh karena itu penting bagi pembaca yang tertarik mempelajari CCNA agar mengikuti ujian internasionalnya. Sehingga tidak hanya mempelajari konsepnya saja, tetapi juga harus dibuktikan dengan mengikuti ujian internasional CCNA.

Apabila pembaca mendapatkan manfaat dari ebook ini, beritahukan kepada sahabat pembaca untuk mendownloadnya secara gratis di [www.bukainter.net](http://www.bukainter.net). Semoga dengan adanya ebook ini makin banyak pemuda/pemudi Indonesia yang menjadi network expert di masa mendatang.