

## Kata Pengantar

Bismillahirrahmanirrahim,

Segala puja dan puji bagi allah senantiasa kita ucapkan atas limpahan rahmat dan nikmatnya sehingga saya dapat menyelesaikan buku saya yang pertama yaitu **Abang Cisco**.

Tak lupa pula kita aturkan sholawat dan salam kepada Nabi Muhammad SAW. Idola kita, dan suri tauladan terbaik di dunia ini.

Alhamdulillah, setelah lama perjuangan saya menyelesaikan buku ini, akhirnya selesai juga. Buku ini ditujukan kepada kedua orangtua saya yang telah membesarkan saya dengan penuh kasih sayang, dan kepada guru TKJ saya yang telah mengajarkan kepada saya semua hal tentang Cisco CCNA

Pada buku saya yang pertama ini tentang Cisco CCNA, semoga kalian semua dapat mengambil ilmu/pelajaran yang saya tulis dalam buku ini. Semoga dapat membawa berkah dan dapat menjadi langkah kalian dalam menguasai Cisco CCNA .

Saya masih menyadari banyaknya kesalahan dalam buku ini, jika kalian mau memberi kritik/saran kalian bisa menghubungi saya di email : [adaffah6@gmail.com](mailto:adaffah6@gmail.com)

Selamat belajar dan membaca!

Pamijahan, Jawa Barat, Nov 2021

Ahmad Daffah

## DAFTAR ISI

<b>Kata Pengantar .....</b>	<b>1</b>
<b>Daftar Isi.....</b>	<b>2</b>
<b>Preparation .....</b>	<b>5</b>
<b>Network Fundamental .....</b>	<b>8</b>
OSI & TCP/IP LAYER .....	10
TCP & UDP .....	14
Network Protocol .....	17
Infrastruktur Jaringan .....	18
Network Device.....	21
Pyhsical Interface And Cable Type .....	23
Pengenalan Cisco Router dan Switch .....	27
Broadcast Domain & Collision Domain .....	30
Booting process .....	32
<b>IPv4 &amp; Subnetting.....</b>	<b>33</b>
Penulisan IPv4.....	33
Konversi Binary ke Desimal .....	34
Konversi Desimal ke Binary .....	35
Bagian pada IPv4 .....	37
<b>Basic Configuration .....</b>	<b>40</b>
Command Line Interface (CLI) Mode .....	41
8 Initial Configuration .....	43
<b>Switching.....</b>	<b>46</b>
Lab 1. Virtual Local Area Network (VLAN) .....	48
Lab 2. Trunk .....	55
Lab 3. Allowed Trunk .....	59
Lab 4. MLS Trunk .....	63
Lab 5. Intervlan Routing.....	67
Lab 6. SVI (Switch Interface Virtual) .....	72
Lab 7. VTP (Vlan Trunking Protocol).....	76
DHCP Introduction.....	82
Lab 8. DHCP VLAN .....	83
Lab 9. DHCP MLS .....	87
Lab 10. DHCP Excluded .....	91
Lab 11. Port Security .....	94
Lab 12. Telnet.....	98
Lab 13. SSH (Secure Shell Host).....	102

Lab 14. Spanning tree protocol (STP) .....	106
Lab 15. STP Portfast.....	110
Lab 16. STP Priority (Main Link) .....	111
Lab 17. Etherchannel.....	114
Lab 18. Switch Stacking.....	117
<b>Routing .....</b>	<b>118</b>
Routing Introduction.....	120
Routing Fundamental.....	120
Lab 19. Static Route .....	124
Lab 20. Static Routing 2 <sup>nd</sup> .....	127
Lab 21. Dynamic Routing EIGRP.....	131
Lab 22. EIGRP Authentication .....	135
<b>OSPF Introduction.....</b>	<b>138</b>
Lab 23. Dynamic Routing OSPF (Backbone) .....	139
OSPF Area Type .....	142
OSPF Router Type .....	143
Lab 24. Dynamic Routing OSPF (Non Backbone).....	145
Lab 25. OSPF Traffic Routing .....	150
Lab 26. OSPF Authentication.....	153
Lab 27. Redistribute EIGRP & OSPF.....	154
Lab 28. Dynamic Routing RIP .....	155
<b>Access List .....</b>	<b>159</b>
Access-List Introduction.....	161
Lab 29. Standard Access List .....	162
Lab 30. Standard Access-list 2 <sup>nd</sup> .....	166
Lab 31. Extended Access-list.....	170
Lab 32. Extended Access-list 2 <sup>nd</sup> .....	174
Lab 33. Named Extended Access-list .....	178
<b>NAT.....</b>	<b>183</b>
NAT Introduction.....	185
Lab 34. Static NAT.....	186
Lab 35. Dynamic NAT.....	190
Lab 36. NAT Overload .....	194
Lab 37. NTP (Network Time Protocol) .....	199
<b>Tunnel .....</b>	<b>201</b>
Lab 38. Tunnel GRE .....	202
Lab 39. Tunnel GRE With NAT .....	207
<b>FHRP .....</b>	<b>213</b>
FHRP Introduction .....	214

Lab 40. HSRP.....	215
Lab 41. Priority HSRP.....	220
Lab 42. VRRP.....	222
Lab 43. Priority VRRP.....	227
Lab 44. GLBP .....	229
<b>HDLC .....</b>	<b>235</b>
Lab 45. HDLC .....	236
<b>IPv6.....</b>	<b>239</b>
IPv6 Introduction.....	241
IPv6 Address Notation .....	242
IPv6 Compression .....	243
Lab 46. Peer to Peer IPv6.....	244
Lab 47. Static Route IPv6.....	246
Lab 48. Dynamic Routing EIGRP IPv6.....	248
<b>IPv6 Address Type .....</b>	<b>252</b>
IPv6 Anycast.....	252
IPv6 Multicast .....	252
IPv6 Unicast .....	253
<b>IPv6 Subnetting .....</b>	<b>254</b>
Konversi Desimal ke Binary .....	254
Konversi Binary ke Desimal .....	255
<b>Wireless .....</b>	<b>257</b>
Radio Frequency .....	257
Frequency.....	257
Frequency.....	257
Frequency Band .....	257
SSID .....	258
Wireless Authentication .....	258
Wireless Encryption .....	258
<b>Network Automation .....</b>	<b>259</b>
<b>Virtualization.....</b>	<b>260</b>
<b>About Writer .....</b>	<b>261</b>

# Preparation

Ibarat mengawali sebuah pembangunan, pasti kita membutuhkan perlengkapannya terlebih dahulu sebagai awalan. Jika sudah, tinggal kita menunggu proses, apakah akhirnya bangunan yang dibangun kokoh atau tidak, indah atau tidak. Itu tergantung usaha dan pemahaman kita. Maka dari itu, untuk mengawali Materi CCNA kali ini, maka disarankan untuk menggunakan perlengkapan berikut, agar kita bisa lebih memahami.

## 1. Cisco Packet Tracer.

- Pertama-tama, kita daftar netacad terlebih dahulu, agar kita bisa menggunakan dan mengunduh CPT
- Klik <https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer>
- Lalu klik ‘Sign up Today!’ dan klik ‘English’ untuk bahasa inggris.

Packet Tracer

## Introduction to Packet Tracer

Discover and troubleshoot using powerful networking simulation tool.

### Hands-On Practice

Enroll, download and start learning valuable tips and best practices for using our innovative, virtual simulation tool, Cisco Packet Tracer. This self-paced course is designed for beginners with no prior networking knowledge. It teaches basic operations of the tool with multiple hands-on activities helping you to visualize a network using everyday examples, including Internet of Things (IoT). This introductory course is extremely helpful for anyone who plans to take one of the Networking Academy courses which utilizes the powerful simulation tool. No prerequisites required!

You'll Learn These Core Skills:

- Simulate data interactions traveling through a network.
- Visualize the network in both logical and physical modes.
- Apply skills through practice, using labs and Cisco Packet Tracer activities.
- Develop critical thinking and problem-solving skills.

[Sign up today!](#)

Length: 10 hours

Cost: Free\*

Level: Beginning

Learning Type: Online self-paced

Achievements: Badge

Languages: English, Український

- Selanjutnya kita isi formulir dan verifikasi e-mail.
- Jika kita sudah, masuk ke homepage netacad

CISCO Networking Academy

Home / I'm Learning

Certification Exams & Discounts

Last login on 12/01/2021 at 20:57 PM

Find an Academy

Download Packet Tracer

All Resources

Alumni Courses

Refresh Status

Browse Course Catalog

Status

Search by Course name or ID

All Statuses

Showing 6

1 - 1 of 1

NETACAD-SMK-IDN-CNAV7-ITN-001-02  
CCNA-RS-V7-SMK-IDN-001-02  
SMK IDN

Week 6 of 8

20 Oct - 15 Dec 2021  
CCNAv7: Introduction to Networks  
Jurusan Teknik Komputer dan Jaringan - S...  
Please finish by 15 Dec 2021

<https://www.netacad.com/portal/resources/packet-tracer>

## Download

DOWLOADING, INSTALLING, OR USING THE CISCO PACKET TRACER SOFTWARE CONSTITUTES ACCEPTANCE OF THE [CISCO END USER LICENSE AGREEMENT](#) ("EULA") AND THE [SUPPLEMENTAL END USER LICENSE AGREEMENT FOR CISCO PACKET TRACER](#) ("SEULA"). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE EULA AND SEULA, PLEASE DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE.

To successfully install and run Cisco Packet Tracer 8.1.0, the following system requirements must be met:

1. Cisco Packet Tracer 8.1.0 ([64 bit](#)):
  - Computer with one of the following operating systems: Microsoft Windows 8.1, 10, 11 (64bit), Ubuntu 20.04 LTS (64bit) or macOS 10.14 or newer.
  - amd64(x86-64) CPU
  - 4GB of free RAM
  - 1.4 GB of free disk space

2. Cisco Packet Tracer 8.1.0 ([32 bit](#)):
  - Computer with one of the following operating systems: Microsoft Windows 8.1, 10, 11 (32bit)
  - x86 compatible CPU
  - 2GB of free RAM
  - 1.4 GB of free disk space

- For CCNA 7.0.2, Cisco Packet Tracer 8.1.0 64-bit is the minimum version for new activities and new PTSA to work properly
- Cisco Packet Tracer requires authentication with your email and password when you first use it and for each new OS login session (See footnote 1 below)
- For more information read the [FAQ](#) and view [Tutorials](#)

**Windows Desktop Version 8.1.0 English**  
[64 Bit Download](#)    [32 Bit Download](#)

**Ubuntu Desktop Version 8.1.0 English**  
[64 Bit Download](#)

- Lalu klik 'Resources' pada tab atas kemudian klik 'Download Packet Tracer'
- Disitu ada beberapa jenis Packet Tracer, unduhlah sesuai dengan OS atau system yang sedang digunakan.

---

**“MENUNTUT ILMU MERUPAKAN KEWAJIBAN BAGI  
SETIAP KAUM MUSLIMIN, BAIK LAKI LAKI DAN  
PEREMPUAN.”**

---

-Sabda Rasulullah SAW-

# **Network Fundamental**

# **Network Fundamental**

## **CONTENT :**

**OSI & TCP/IP LAYER**

**TCP & UDP**

**NETWORK PROTOCOL**

**INFRASTRUKTUR JARINGAN**

**NETWORK DEVICE**

**PHYSICAL INTERFACE AND CABLE TYPE**

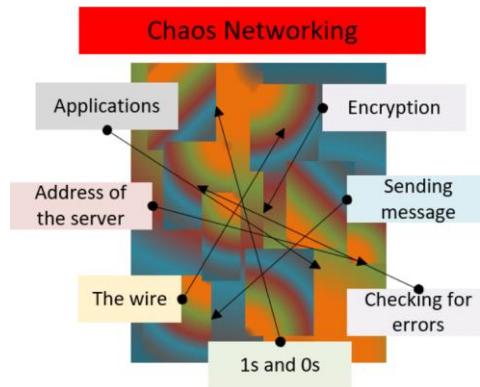
**PENGENALAN CISCO ROUTER DAN SWITCH**

**BROADCAST DOMAIN & COLLISION DOMAIN**

**BOOTING PROCESS**

## OSI & TCP/IP LAYER

Do you know?, bahwa jika ketika kita akan mengakses internet, ada suatu proses yang sangat panjang hingga akhirnya kita bisa mengakses email, menonton youtube dll. Semua hal tersebut dapat kita akses dengan mudah karena kemajuan teknologi. Bayangkan pada zaman dahulu, untuk internet sangat susah sekali, hal ini dikarenakan terjadinya Chaos Networking. Yaitu sebuah proses dimana semua proses saling bertabrakan, tidak termodel.



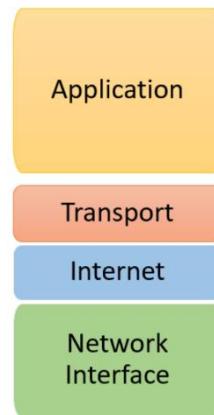
This network would be difficult to understand and implement

Dan susah untuk berkomunikasi. Hal ini juga dikarenakan tiap vendor pada networking memiliki protokol komunikasi yang berbeda-beda. Hal ini mengakibatkan antara vendor satu dan yang lain tidak bisa saling berkomunikasi.

Maka dari itu, pada tahun 1970-an DARPA membuat sebuah model protokol komunikasi yang disebut TCP/IP yang dapat digunakan oleh semua vendor networking sehingga dapat saling berkomunikasi. Ini merupakan kemajuan teknologi. TCP/IP sendiri merupakan singkatan dari Transmission Control Protocol/ Internet Protocol.

**TCP/IP terdiri dari 4 layer :**

1. Network Interface
2. Internet
3. Transport
4. Application



**OSI Layer**

Sementara itu, 10 tahun kemudian, pada tahun 1980-an. ISO atau Organisasi Standar Internasional membuat protocol komunikasi lain yang lebih kompleks dan jelas fungsinya dari TCP/IP. Protokol komunikasi itu disebut juga dengan OSI Layer. OSI Layer merupakan singkatan dari Open System Interconnection.

OSI Layer terdiri dari 7 layer :



1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

#### Lalu apa perbedaan dari TCP/IP dan OSI Layer?

Perbedaanya terletak pada layer-nya. Jika pada TCP/IP terdapat 4 Layer, maka pada OSI terdapat 7 layer. OSI layer, memecah satu layer pada TCP/IP menjadi beberapa layer. Secara fungsi pada tiap layer masing-masing protocol tidak ada perbedaan, hanya saja pada OSI Layer. Fungsi-fungsinya dibuat menjadi lebih kompleks dan lebih mudah dimengerti. Sehingga untuk secara keunggulan masih bagus OSI layer. Hanya saja, protocol yang kita

OSI Model	TCP/IP Model
Application Layer	
Presentation Layer	Application layer
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data link layer	
Physical layer	Link Layer

guna dari dulu sampai sekarang adalah TCP/IP. Hal ini dikarenakan TCP/IP dulu lah yang pertama keluar dan langsung digunakan oleh hampir semua vendor jaringan yang ada didunia.

### Fungsi tiap layer pada OSI

#### 1. Physical

Pada layer ini, kita mengirimkan data dari unsur terluar atau unsur fisik seperti kabel, antenna. Yang menghubungkan antar penyedia layanan internet (ISP) data yang dikirim berupa bit dan pengalamatannya menggunakan bit (101010101).

#### 2. Data Link

Setelah data (bit) tadi dikirim lewat kabel, setelah itu akan naik lagi ke layer 2. Pada layer 2, data diproses oleh hardware yang bernama switch, data yang dikirim berupa frame dan pengalamatannya berupa MAC Address.

#### 3. Network

Jika data tadi sudah diproses switch, maka selanjutnya akan diproses oleh router. Data yang dikirim berupa Packet dan pengalamatannya menggunakan IP address.

#### 4. Transport

Sebelum packet ini dikirim oleh router, maka akan dipilih packetnya berdasarkan protocol apa, ada TCP dan juga UDP .

#### 5. Session,Presentation, Application

Setelah packet itu dikirim ke IP Adress tujuan, selanjutnya akan diproses oleh software yang akan menghasilkan protocol baru, seperti DHCP (UDP no 67-68) atau telnet (TCP no 23) dan masih banyak lagi.

Atau lebih ringkasnya dapat dilihat di tabel berikut :

Layer	Nama	Perangkat	Data Unit	Pengalamatan
Layer 1	Physical	Hub	Bit	0111001110
Layer 2	Data Link	Switch	Frame	MAC Address
Layer 3	Network	Router	Paket	IP Address

Tabel 3 . 1 Daftar Pengalamatan

Apabila 7 OSI Layer susah untuk dihafal, maka sebagai seorang network engineer hafal Layer 1, 2 dan 3 adalah suatu keharusan, karena dapat menunjukkan bedanya antara Hub, Switch dan Router dimana ketiganya berada di layer yang berbeda sehingga memiliki cara kerja yang berbeda tentunya.

<b>Perangkat</b>	<b>Layer</b>	<b>Konektivitas</b>	<b>Pengiriman Data</b>	<b>Memory</b>
Hub	Layer 1	Antar network yang sama	Broadcast ke semua port	Tidak Punya
Switch	Layer 2	Antar network yang sama	Berdasar MAC Address Tujuan	MAC Address Tabel
Router	Layer 3	Antar network yang berbeda	Berdasar IP Address Tujuan	Routing Tabel

*Tabel 3 . 2 Daftar Konektivitas*

Berdasarkan tabel diatas dapat kita simpulkan bahwa pada layer 1 dan 2 bekerja pada network yang sama alias masih pada satu jaringan. Jika kita analogikan, layer 1 dan 2 ini masih bekerja di satu desa, sementara layer 3, dia bekerja di perbatasan desa. Jadi layer 3 ini, nanti fungsinya mengenalkan desa (network) nya kepada desa-desa lain (network lain).

## TCP & UDP

Fungsi dari layer 4 adalah untuk menerima data dari session layer, lalu dibagi menjadi segmen-segmen yang lebih kecil untuk diteruskan ke network layer. Transport layer juga memastikan setiap bit yang diterima adalah bit yang sama dengan bit yang dikirim tanpa ada modifikasi ataupun loss.

Jika terjadi error, maka transport layer harus memperbaiki error tersebut. Cara memperbaikinya, bisa dengan mengirim ulang data yang corrupt atau dengan mengirim semua data dari awal.

Berikut tabel perbandingan TCP & UDP :

No	TCP	UDP
1.	Beroperasi berdasarkan konsep koneksi.	Tidak berdasarkan konsep koneksi, jadi harus membuat kode sendiri.
2.	Jaminan pengiriman-penerimaan data akan reliable dan teratur.	Tidak ada jaminan bahwa pengiriman dan penerimaan data akan reliable dan teratur, sehingga paket data mungkin dapat kurang, terduplikat, atau bahkan tidak sampai sama sekali.
3.	Secara otomatis memecah data ke dalam paket-paket.	Pemecahan ke dalam paket-paket dan proses pengirimannya dilakukan secara manual.
4.	Tidak akan mengirimkan data terlalu cepat sehingga memberikan jaminan koneksi internet dapat menanganinya.	Harus membuat kepastian mengenai proses transfer data agar tidak terlalu cepat sehingga internet masih dapat menanganinya.
5.	Mudah untuk digunakan, transfer paket data seperti menulis dan membaca file.	Jika paket ada yang hilang, perlu dipikirkan di mana letak kesalahan yang terjadi dan mengirim ulang data yang diperlukan.

Mudahnya, jika kita analogikan dalam jaringan :

**TCP :**

Misalkan kita sebagai klien, mengirimkan 10 paket kepada server, jika waktu dijalankan paketnya hilang 5 (drop) dan sampai di server hanya 5. Maka klien akan mengirim 5 paket susulan agar 10 paket sempurna sampai di server atau mengoreksi paketnya kembali. Ini disebut juga dengan Reliable atau seimbang. Selain itu TCP justru lebih lambat daripada UDP dikarenakan adanya koreksi paket tersebut dan ukuran paket TCP juga lebih berat daripada UDP yaitu 20 bytes.

**UDP :**

Pada UDP, jika kita sebagai klien dan mengirim 10 data kepada server, jika waktu dijalankan paketnya hilang 5 (drop) dan sampai di server hanya 5. Maka klien tidak akan mengirim ulang karena dianggap urusan pengiriman paket itu sudah selesai. Ini disebut juga dengan non-

reliable atau tidak seimbang. Namun, UDP jauh lebih cepat pengiriman paketnya daripada TCP dikarenakan UDP sekali kirim dan ukuran paketnya jauh lebih kecil dari TCP yaitu 8 bytes.

## Port Numbers

Sementara itu, Port adalah nomor 16-bit yang digunakan untuk mengidentifikasi aplikasi dan layanan tertentu. TCP dan UDP menentukan nomor port sumber dan tujuan di header paket mereka dan informasi itu, bersama dengan alamat IP sumber dan tujuan dan protokol transport (TCP atau UDP), memungkinkan aplikasi yang berjalan pada host di jaringan TCP / IP untuk berkomunikasi. T

Terdapat 3 port number range :

- Well known port (0 - 1023): Untuk core services.
- Registered port number (1024 – 49151) : Untuk keperluan industri aplikasi dan process.
- Dynamic port number (49152 – 65535) : Digunakan untuk keperluan temporary untuk sebuah komunikasi yang spesifik.

## Contoh dari TCP dan UDP

### TCP :

Contohnya pada browser (HTTP & HTTPS). Pada saat kita berselancar di internet, saat kita mengakses situs, jika misalkan ada gambar/bagian dari situs itu yang kurang lengkap atau hilang, kita tinggal melakukan refresh agar gambar tersebut bisa muncul. Hal ini sama seperti protocol TCP yang mengirim ulang packet nya.

**UDP** : Contohnya ketika kita bertelpon menggunakan VOIP (Voice Over Internet Protocol). Pada saat kita menggunakan VOIP, pasti pernah kita merasakan suara lawan bicara kita putus-putus dikarenakan jaringan alias packet yang terkirim tidak sampai. Itu karena UDP hanya sekali mengirimkan packet. Jika VOIP menggunakan TCP, jika saat kita mengirimkan paket suara namun tidak sampai, maka suara tersebut akan dikirim ulang ke penerima dan terjadilah keterlambatan. Maka dari itu VOIP menggunakan UDP agar tidak terjadi keaneahan dan keterlambatan dalam bertelpon, lebih baik suara terputus daripada suara dikirim ulang disaat yang tidak tepat.

## COMMON PORTS

packetlife.net

TCP/UDP Port Numbers			
7 Echo	554 RTSP	2745 Bagle.H	6891-6901 Windows Live
19 Chargen	546-547 DHCPv6	2967 Symantec AV	6970 Quicktime
20-21 FTP	560 rmonitor	3050 Interbase DB	7212 GhostSurf
22 SSH/SCP	563 NNTP over SSL	3074 XBOX Live	7648-7649 CU-SeeMe
23 Telnet	587 SMTP	3124 HTTP Proxy	8000 Internet Radio
25 SMTP	591 FileMaker	3127 MyDoom	8080 HTTP Proxy
42 WINS Replication	593 Microsoft DCOM	3128 HTTP Proxy	8086-8087 Kaspersky AV
43 WHOIS	631 Internet Printing	3222 GLBP	8118 Privoxy
49 TACACS	636 LDAP over SSL	3260 iSCSI Target	8200 VMware Server
53 DNS	639 MSDP (PIM)	3306 MySQL	8500 Adobe ColdFusion
67-68 DHCP/BOOTP	646 LDP (MPLS)	3389 Terminal Server	8767 TeamSpeak
69 TFTP	691 MS Exchange	3689 iTunes	8866 Bagle.B
70 Gopher	860 iSCSI	3690 Subversion	9100 HP JetDirect
79 Finger	873 rsync	3724 World of Warcraft	9101-9103 Bacula
80 HTTP	902 VMware Server	3784-3785 Ventrilo	9119 MXit
88 Kerberos	989-990 FTP over SSL	4333 mSQL	9800 WebDAV
102 MS Exchange	993 IMAP4 over SSL	4444 Blaster	9898 Dabber
110 POP3	995 POP3 over SSL	4664 Google Desktop	9988 Rbot/Spybot
113 Ident	1025 Microsoft RPC	4672 eMule	9999 Urchin
119 NNTP (Usenet)	1026-1029 Windows Messenger	4899 Radmin	10000 Webmin
123 NTP	1080 SOCKS Proxy	5000 UPnP	10000 BackupExec
135 Microsoft RPC	1080 MyDoom	5001 Slingbox	10113-10116 NetIQ
137-139 NetBIOS	1194 OpenVPN	5001 iperf	11371 OpenPGP
143 IMAP4	1214 Kazaa	5004-5005 RTP	12035-12036 Second Life
161-162 SNMP	1241 Nessus	5050 Yahoo! Messenger	12345 NetBus
177 XDMCP	1311 Dell OpenManage	5060 SIP	13720-13721 NetBackup
179 BGP	1337 WASTE	5190 AIM/ICQ	14567 Battlefield
201 AppleTalk	1433-1434 Microsoft SQL	5222-5223 XMPP/Jabber	15118 Dipnet/Oddbob
264 BGMP	1512 WINS	5432 PostgreSQL	19226 AdminSecure
318 TSP	1589 Cisco VQP	5500 VNC Server	19638 Ensim
381-383 HP Openview	1701 L2TP	5554 Sasser	20000 Usermin
389 LDAP	1723 MS PPTP	5631-5632 pcAnywhere	24800 Synergy
411-412 Direct Connect	1725 Steam	5800 VNC over HTTP	25999 Xfire
443 HTTP over SSL	1741 CiscoWorks 2000	5900+ VNC Server	27015 Half-Life
445 Microsoft DS	1755 MS Media Server	6000-6001 X11	27374 Sub7
464 Kerberos	1812-1813 RADIUS	6112 Battle.net	28960 Call of Duty
465 SMTP over SSL	1863 MSN	6129 DameWare	31337 Back Orifice
497 Retrospect	1985 Cisco HSRP	6257 WinMX	33434+ traceroute
500 ISAKMP	2000 Cisco SCCP	6346-6347 Gnutella	Legend
512 rexec	2002 Cisco ACS	6500 GameSpy Arcade	Chat
513 rlogin	2049 NFS	6566 SANE	Encrypted
514 syslog	2082-2083 cPanel	6588 AnalogX	Gaming
515 LPD/LPR	2100 Oracle XDB	6665-6669 IRC	Malicious
520 RIP	2222 DirectAdmin	6679/6697 IRC over SSL	Peer to Peer
521 RIPng (IPv6)	2302 Halo	6699 Napster	Streaming
540 UUCP	2483-2484 Oracle DB	6881-6999 BitTorrent	

IANA port assignments published at <http://www.iana.org/assignments/port-numbers>

by Jeremy Stretch

v1.1

# Network Protocol

Dalam dunia jaringan, terdapat banyak jenis komunikasi yang berbeda-beda, namun itu semua sudah tertata rapi sesuai dengan protocol yang digunakan. Seperti ketika kita browsing di internet, kita menggunakan protocol HTTP dan HTTPS, lalu saat kita akan meremote router atau switch, kita menggunakan telnet maupun SSH.

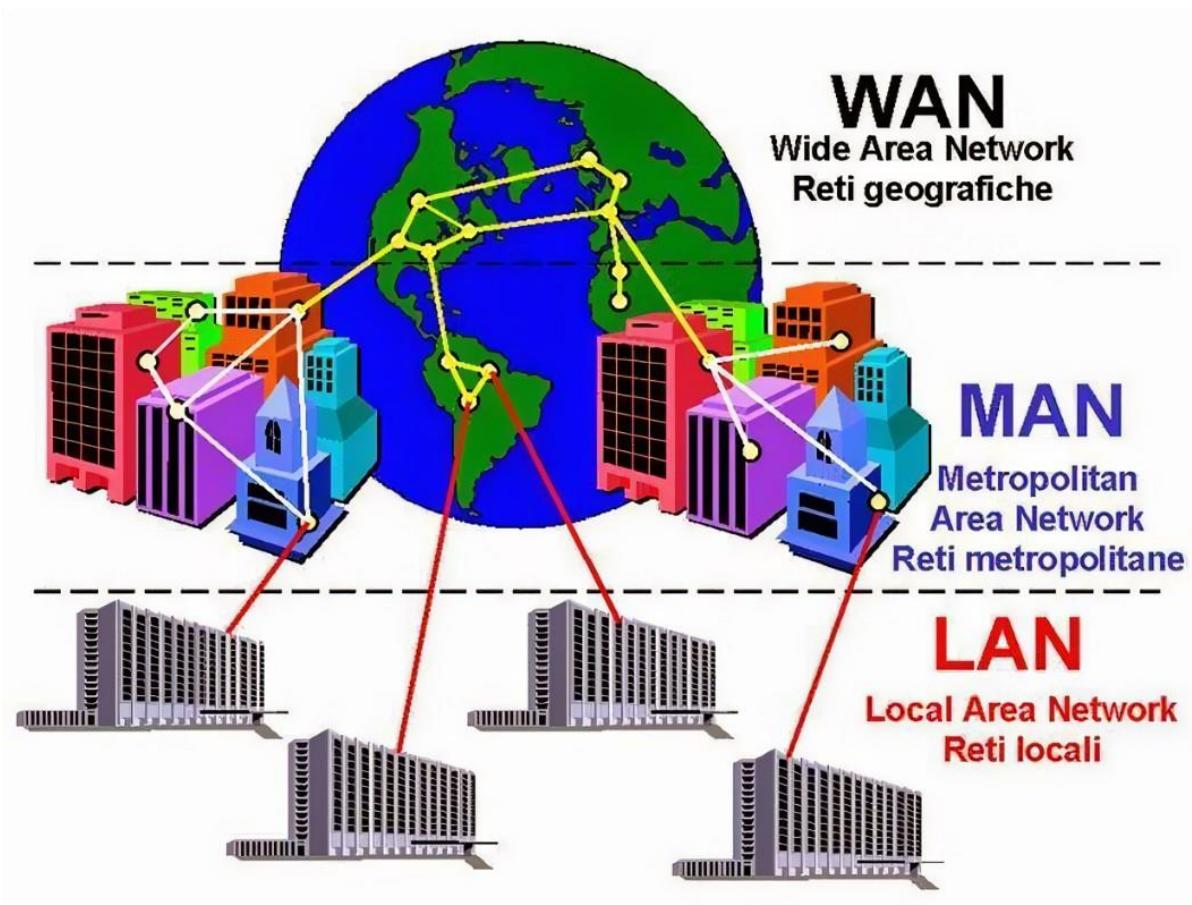
Jadi, fungsi dari Network Protocol, ialah mengatur jalannya komunikasi pada jaringan dengan protokol-protokol agar berjalan dengan lancar.

## Contoh Network Protocol

Berikut beberapa network protocol yang harus kita pahami :

Label on Column	Service Name	UDP and TCP Port Numbers Included
DNS	Domain Name Service – UDP	UDP 53
DNS TCP	Domain Name Service – TCP	TCP 53
HTTP	Web	TCP 80
HTTPS	Secure Web (SSL)	TCP 443
SMTP	Simple Mail Transport	TCP 25
POP	Post Office Protocol	TCP 109, 110
SNMP	Simple Network Management	TCP 161,162 UDP 161,162
TELNET	Telnet Terminal	TCP 23
FTP	File Transfer Protocol	TCP 20,21
SSH	Secure Shell (terminal)	TCP 22
AFP IP	Apple File Protocol/IP	TCP 447, 548

# Infrastruktur Jaringan



Dalam implementasinya, infrastruktur jaringan dibagi menjadi 2 :

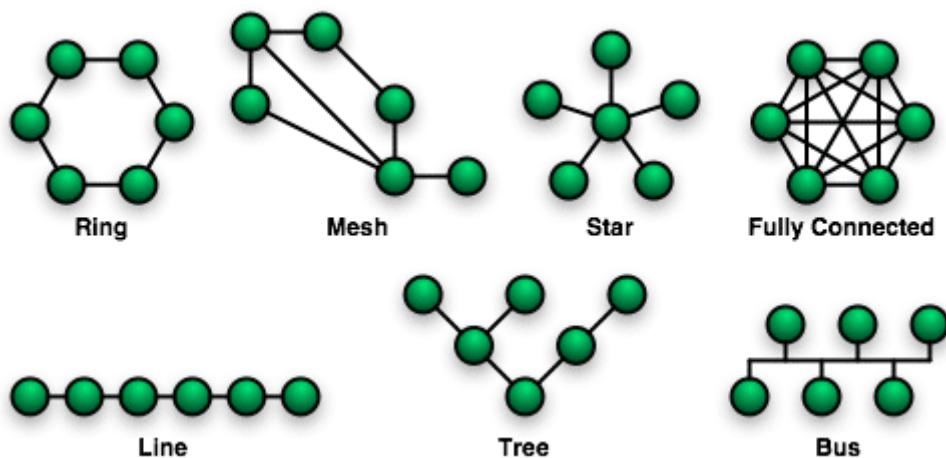
1. LAN (Local Area Network)- Merupakan jaringan skala kecil yang terdiri dari sekumpulan perangkat yang saling terhubung yang masih dalam ruang lingkup yang belum luas. Seperti jaringan pada Sekolah, Rumah, Warnet.
2. WAN (Wide Area Network)- Merupakan jaringan skala besar yang terdiri dari kumpulan LAN yang saling terhubung satu sama lain. Contohnya Internet.

Adapun beberapa istilah jaringan lain yang berkaitan :

1. WLAN (Wireless Local Area Network)- Merupakan jaringan skala kecil, sama seperti LAN. Namun dalam konektivitasnya menggunakan jaringan wireless (tanpa kabel).
2. MAN (Metropolitan Area Network)- Merupakan jaringan skala menengah, diantara WAN dan LAN. MAN ini sendiri merupakan kumpulan dari LAN dan diimplementasikan pada jaringan seperti kota.

## Topologi Jaringan

Dalam membangun sebuah jaringan, ada sebuah aspek penting yang harus diperhatikan, yaitu topologi. Topologi adalah sebuah cara bagaimana perangkat-perangkat jaringan ini dapat saling berkomunikasi, baik lewat menggunakan kabel maupun nirkabel. Tujuannya untuk mempermudah perangkat-perangkat tersebut saling bertukar informasi.



selain itu, efisien dalam memilih topologi yang digunakan juga dapat menghemat sumber daya perangkat dan juga pastinya lebih hemat dana.

Berikut ini penjelasan singkat beberapa topologi :

#### 1. Topologi Ring

Ini adalah metode topologi jaringan yang banyak digunakan di perusahaan. Sesuai dengan namanya, metode ini menghubungkan antarkomputer dengan cara membentuk rangkaian seperti sebuah lingkaran.

#### 2. Topologi Mesh/Fully Connected

Topologi jaringan mesh atau jala adalah sistem topologi di mana koneksi antar komputer saling terhubung secara langsung satu sama lain. Koneksi antarkomputer secara langsung seperti ini disebut dedicated link

#### 3. Topologi Star

Topologi jaringan berbentuk star atau bintang adalah jaringan dari beberapa komputer yang memiliki koneksi dengan node yang berada di jaringan pusat. Jadi, masing-masing perangkat memiliki koneksi dengan node yang berada di tengah sistem jaringan.

#### 4. Topologi Point to Point/Line

Jenis topologi linear sebenarnya merupakan perluasan dari jenis topologi bus, yang mana kabel utama di dalam jaringan harus dihubungkan dengan setiap titik-titik yang ada di komputer dengan T-Connector. Seperti yang dijelaskan sebelumnya, jaringan linear merupakan topologi jaringan yang memiliki layout cukup umum.

#### 5. Topologi Tree

Topologi jaringan berbentuk tree (pohon) merupakan bentuk gabungan dari sistem topologi bus dan star, di mana jaringan topologi bus menjadi konektor utama beberapa topologi star. Jika diibaratkan dengan bentuk seperti pohon, topologi bus adalah batang utama yang menghubungkan beberapa topologi star sebagai rantingnya.

#### 6. Topologi Bus

Topologi yang merupakan cara dalam jaringan komputer dalam menghubungkan suatu jaringan satu dengan yang lainnya menggunakan kabel tunggal yang menghubungkan ke client dan server. Metode topologi bus ini digunakan pada jaringan dengan skala

kecil yang semua perangkatnya saling terhubung dan membentuk sebuah bus, oleh karena itu disebut topologi bus.

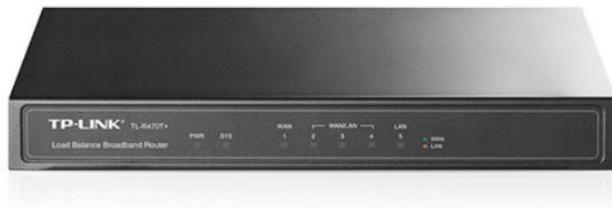
# Network Device

Sebelum kita dapat mengakses internet, terdapat sebuah proses panjang yang terjadi sehingga kita dapat menggunakan internet. Proses itu terjadi pada perangkat-perangkat jaringan berjalan disekitar kita. Perangkat-perangkat tersebut saling terhubung hingga seluruh perangkat yang ada di bumi. Sehingga terciptalah internet. Maka dari itu, perangkat jaringan ini merupakan komponen penting dalam terbentuknya internet yang tersebar diseluruh negara.

**Contoh Network Device dibawah ini :**

## 1. Router

Router termasuk kedalam perangkat WAN. Router sendiri merupakan perangkat Layer 3 – Network, yang bekerja berdasarkan IP Address. Data unit di perangkat router adalah Packet. Fungsi utamanya adalah untuk menghubungkan jaringan-jaringan yang berbeda. Dan juga sebagai penghubung antara jaringan LAN dan WAN.



## 2. Switch

Switch, pada dasarnya merupakan perangkat Layer 2 – Datalink, yang bekerja berdasarkan MAC Address. Data unit perangkat Switch adalah Frame. Switch digunakan untuk menghubungkan beberapa komputer dalam 1 broadcast domain / 1 jaringan.



## 3. Access-Point

Access Point merupakan perangkat jaringan yang bekerja menggunakan teknologi wireless, sehingga memungkinkan kita untuk mengkoneksikan perangkat kita ke Access Point tersebut tanpa harus menggunakan kabel.



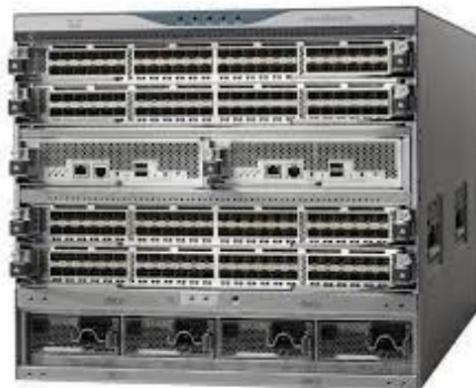
#### 4. Server

Server merupakan sebuah komputer atau perangkat yang menyediakan layanan atau fungsi untuk sebuah program atau perangkat lain yang biasa disebut klien. Tujuan dari server adalah untuk berbagi data serta sumber daya serta mendistribusikannya kepada klien yang ingin menggunakan data atau sumber daya tersebut.



#### 5. MLS

MLS adalah salah satu jenis switch yang bekerja pada 2 layer yaitu : Data Link dan Network, switch ini berfungsi sebagai layer-3 ketika mengaktifkan fungsi routernya yaitu ***ip routing*** dan MLS bisa memasang IP Address dengan mengaktifkan command ***no switchport***.



# Physical Interface And Cable Type

## Ethernet

Ethernet merupakan jenis perkabelan dan pemrosesan sinyal untuk data jaringan komputer. Ethernet merupakan sebuah teknologi yang sudah dikenal oleh masyarakat luas sebagai interface yang digunakan untuk koneksi perangkat komputer maupun laptop, hampir di setiap jaringan LAN (Local Area Network) di seluruh dunia. Ethernet menggunakan standar IEEE 802.3. Ethernet ini bisa menggunakan kabel twisted pair ataupun fiber optic.

## IEEE Ethernet

Standards ethernet didefinisikan dalam standar IEEE 802.3. Standar ini menentukan spesifikasi layer fisik dan data-link untuk Ethernet. Berfungsi sebagai standar LAN paling populer untuk framing dan menyiapkan data untuk transmisi ke media jaringan.

Standar 802.3 yang paling penting untuk diketahui diantaranya :

1. **10Base-T (IEEE 802.3)** -10 Mbps dengan kabel cat 3 UTP. Jangkauan hingga 100 meter.
2. **100Base-TX (IEEE 802.3u)** -dikenal juga sebagai Fast Ethernet, menggunakan kabel cat 5, 5E, atau cat 6 dengan jangkauan 100 meter.
3. **100Base-FX (IEEE 802.3u)** -versi Fast Ethernet yang menggunakan kabel fiber optic dengan jangkauan hingga 412 meter.
4. **100Base-CX (80002.3z)** -menggunakan kabel twisted-pair dengan jangkauan 25 meter.
5. **100Base-T (IEEE 802.3ab)** -Gigabit Ethernet yang menggunakan Kabel cat 5 UTP dengan jangkauan 100 meter.
6. **100Base-SX (IEEE 802.3z)** -1 Gigabit Ethernet yang berjalan menggunakan multimode kabel fiber optic.
7. **100Base-LX (IEEE 802.3z)** -1 Gigabit Ethernet yang berjalan single-mode kabel fiber optic.
8. **100Base-T (802.an)** -Koneksi dengan kecepatan 10 Gbps dengan kategori cat 5e, 6, 7 kabel UTP.

Jika kita perhatikan nomor pertama dari standar tersebut mewakilkan kecepatan dengan satuan megabits per detik. Bagian terakhir dari standard tersebut mengacu pada jenis kabel yang digunakan untuk membawa sinyal. Sebagai contoh, 1000Base-T berarti bahwa kecepatan jaringan up to 1000 Mbps, menggunakan sinyal baseband, dan menggunakan kabel twisted-pair (T sendiri melambangkan dari Twisted-pair).

Ada tiga jenis kabel yang biasa digunakan untuk pemasangan kabel Ethernet :

- **coaxial** (biasa digunakan untuk tv kabel)

- **twisted pair** (biasa digunakan untuk LAN)
- **fiber optic** (digunakan untuk jaringan yang dituntut berkinerja tinggi)

## Fiber Optic

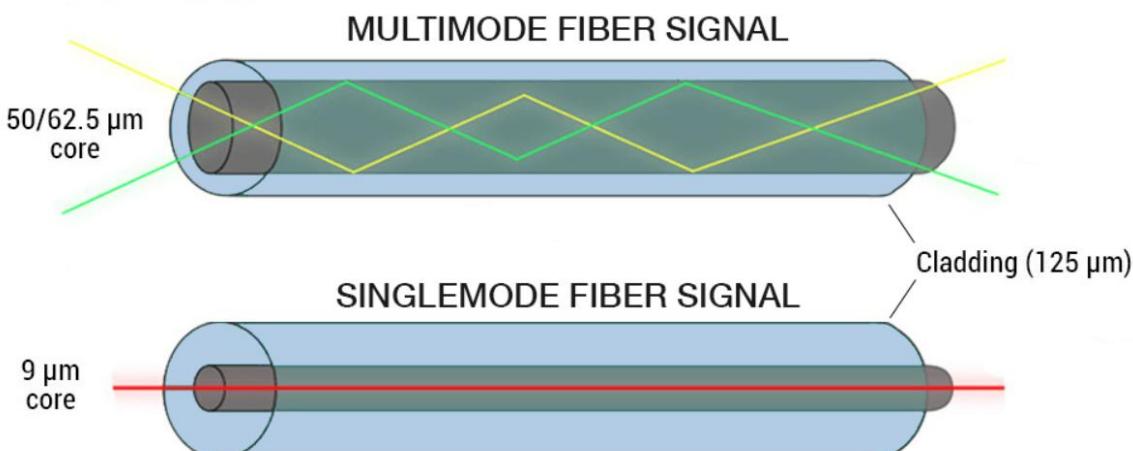
Berbeda dengan kabel twisted-pair, kabel fiber menggunakan Cahaya untuk transmisi data dan dengan alasan inilah Fiber Optic bekerja lebih baik dibandingkan twisted-pair yang menggunakan gelombang elektromagnetik untuk transmisi data.

Kelebihan dari Fiber Optic dibanding temannya twisted-pair ialah :

1. Jangkauan lebih jauh
2. Bandwidth lebih besar
3. Bebas gangguan interferensi gelombang elektromagnetik.

Namun walau begitu, menggunakan fiber optic tentunya ada kekurangannya juga. Biaya pemasangan yang tidak murah, pemasangan yang memerlukan keahlian khusus, dll.

Fiber Optic dibagi menjadi 2 jenis yaitu :



## PoE

Power Over Ethernet (PoE) adalah teknologi yang berfungsi untuk memberi daya pada perangkat melalui kabel jaringan Ethernet biasa. Kelebihan utama menggunakan PoE ialah flexibility, karena kita bisa menyimpan perangkat kita dimana saja, tanpa harus memikirkan electrical outlet. Namun tentu saja ada kekurangan menggunakan PoE, salah satu kendala utamanya ialah suhu perangkat yang tinggi.

Device yang menggunakan PoE diantaranya :

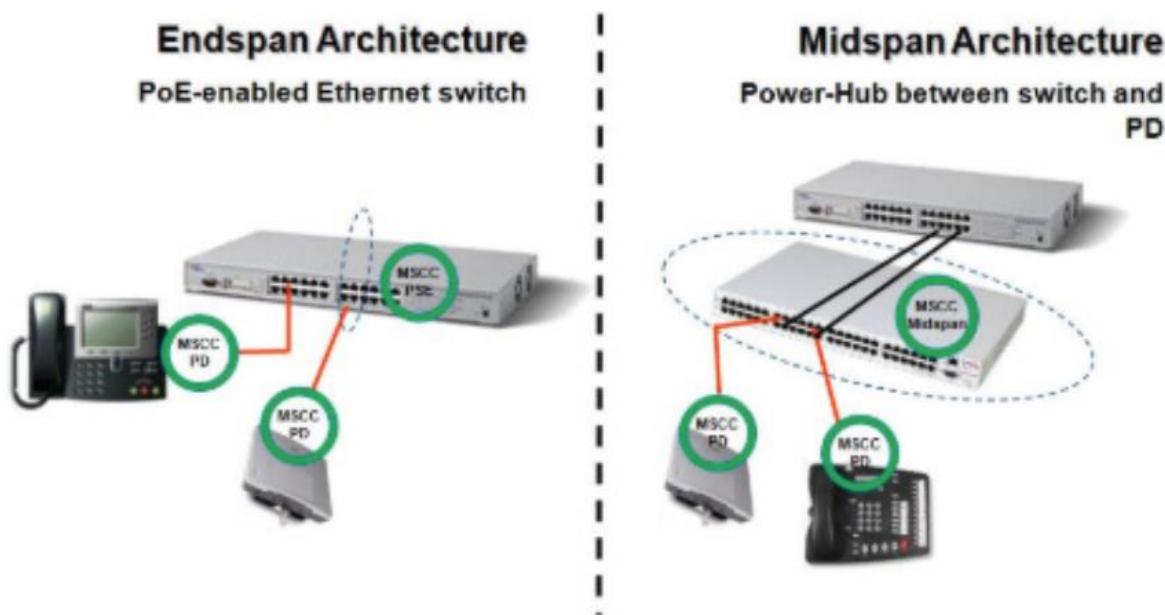
- VoIP phones
- IP cameras
- Wireless access points
- IoT devices
- Small routers and switches

Device yang diberi power oleh PoE disebut **Powered Device (PD)**.

Ada dua jenis penggunaan PoE, yaitu **endspan** dan **midspan**.

**Endspan**, artinya pada perangkat (switch, router, atau sejenisnya) sudah tersedia fitur PoE, sehingga perangkat bisa memberikan power (PoE out).

**Midspan**, artinya perangkat tidak bisa memberikan power. Di antara perangkat utama dengan perangkat tujuan dihubungkan dengan PoE injector (perangkat penengah) sebagai midspan.



How to choose?

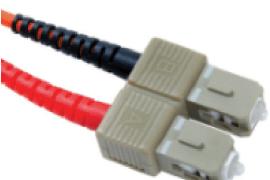
- Midspan memerlukan dua device untuk di manage. Memerlukan extra space di rack.
- Kalo switch-nya baru beli, dan ga support PoE mending pilih yang midspan. Ganti switch cuman buat.

PoE adalah solusi yang mahal

- Endspan walau keliatannya mantap, tapi tentu saja ada kekurangannya. Power yang tersedia terbatas, sehingga bisa saja setiap port tidak mendapat power yang maximum.

## PHYSICAL TERMINATIONS

packetlife.net

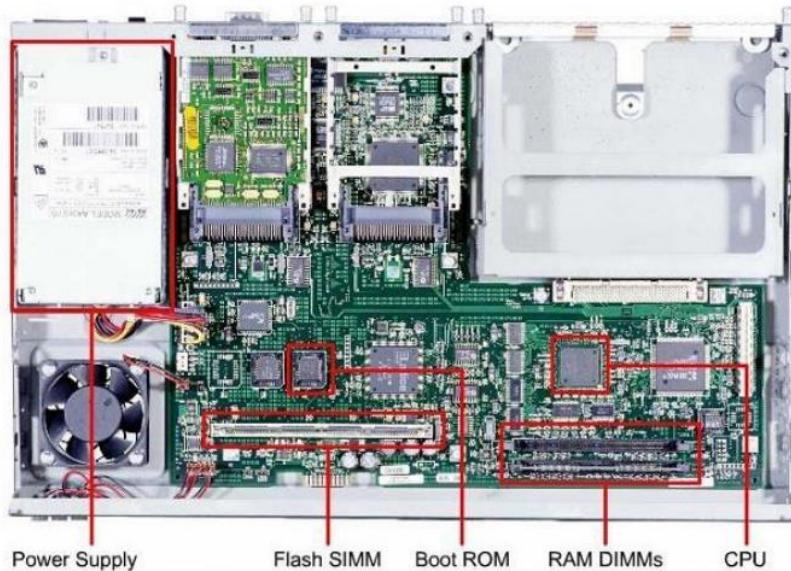
Optical Terminations	Copper Terminations	GBICs
		
		
		
		
<b>Wireless Antennas</b>		
		
		

by Jeremy Stretch

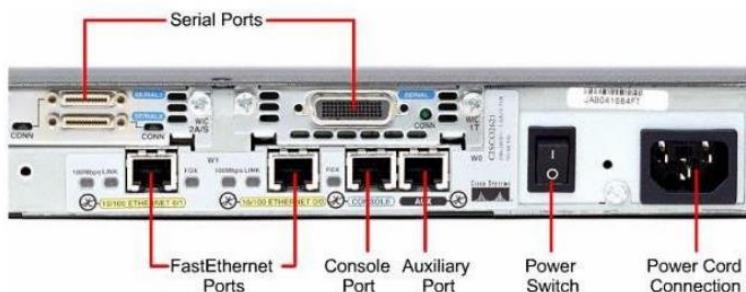
v1.1

# Pengenalan Cisco Router dan Switch

Cisco ini, terkenal dengan produk Router dan Switchnya, dan kita akan mempelajari bentuk dan komponen-komponen penyusun dari router. Berikut gambarnya :



Gambar 1 . 12 Komponen internal Cisco router 2600



Gambar 1 . 13 Komponen External Cisco router 2600

## Bagian utama router :

### 1. Power Supply

Power Supply, merupakan komponen yang memiliki tugas utama menyediakan sumber daya untuk pengoperasian komponen didalam router. Beberapa router memiliki beberapa power supply.

### 2. CPU

Ini adalah bagian inti dari riuter, yang fungsinya sebagai otak si router dalam melakukan routing.

### 3. RAM

Bagian ini berfungsi sebagai penyimpanan sementara dari routing tabel dan segala konfigurasi yang dijalankan di router.

#### 4. NVRAM

Merupakan tempat penyimpanan startup configuration yaitu penyimpanan konfigurasi yang di-save atau disimpan. Dan startup configuration berjalan ketika router pertama kali dinyalakan.

#### 5. FLASH

Flash merupakan tempat penyimpanan Os dari routernya yaitu Cisco IOS.

## Perbedaan Hub, Switch dan Router

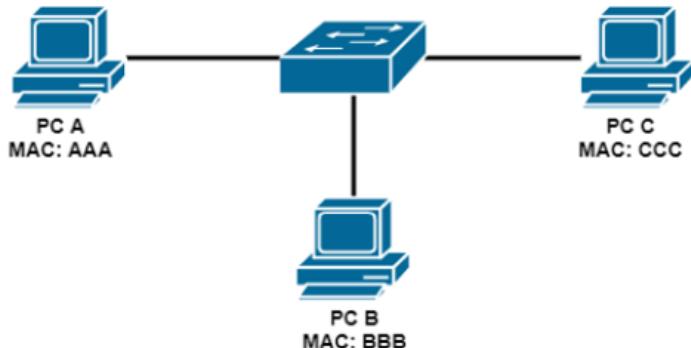
### A. Hub

Hub tidak lebih dari physical repeater yang bekerja pada layer 1 dan tidak punya intelijensi. Cara kerja hub adalah dengan menerima sinyal electric dari satu interface dan mengirimkannya ke semua interface kecuali ke source interface, butuh atau tidak butuh. Karena bekerja pada layer physical dengan half-duplex (satu mengirim, yang lain menunggu), maka dapat terjadi tabrakan (collision) ketika ada packet yang dikirimkan dalam waktu yang bersamaan. Area dimana dapat terjadi collision disebut dengan collision domain.

### B. Switch

Switch ini mirip dengan bridge, namun memiliki banyak kelebihan. Terdapat banyak port dan bermacam jenis.

### Cara kerja switch



- Switch mempunyai tabel MAC Address yang menyimpan MAC Address dari PC yang tersambung ke port-port pada switch. Misal ketika pertama kali ketika PC disambungkan ke switch, PC A ingin mengirimkan data ke C.

- Maka PC A membuat Ethernet frame berisi IP address, MAC address dan tujuannya dan mengirimkannya ke switch.

- Switch lalu membroadcastnya ke semua port kecuali source. Sampai sini, switch telah menyimpan MAC address A.

- Setelah dibroadcast, PC C akan mengirim reply berisi MAC addressnya dan ketika lewat switch, switch akan menyimpan MAC address C.

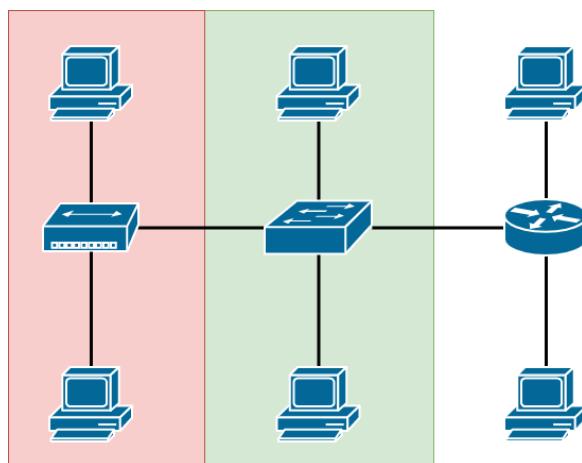
Catatan : Switch melakukan broadcast hanya ketika ada packet data yang destination MAC addressnya tidak terdapat pada tabel MAC address switch.

### C. Router

Jika switch dan hub hanya dapat menghubungkan pada satu jaringan saja. Maka router, adalah perangkat jaringan yang tugasnya menghubungkan antar jaringan yang berbeda.

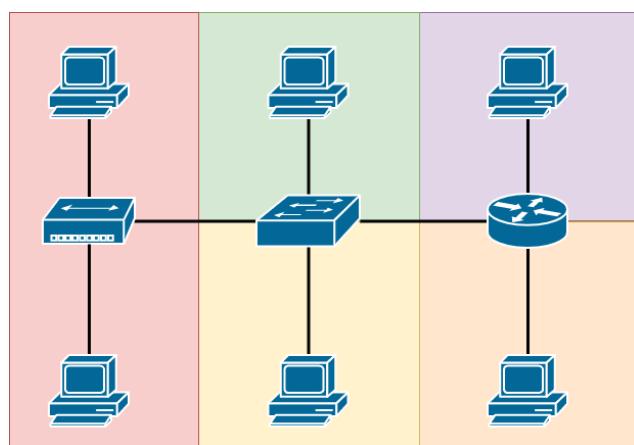
# Broadcast Domain & Collision Domain

## Broadcast Domain



Broadcast domain, adalah sebuah area pada suatu network, dimana ketika ada packet yang lewat, maka packet tersebut akan di broadcast (disebarluaskan) ke semua port. Hub dan Switch memiliki Broadcast domain yang sama, karena sama-sama membroadcast packet tersebut keseluruhan port yang dimilikinya, Sementara router tidak.

## Collision Domain



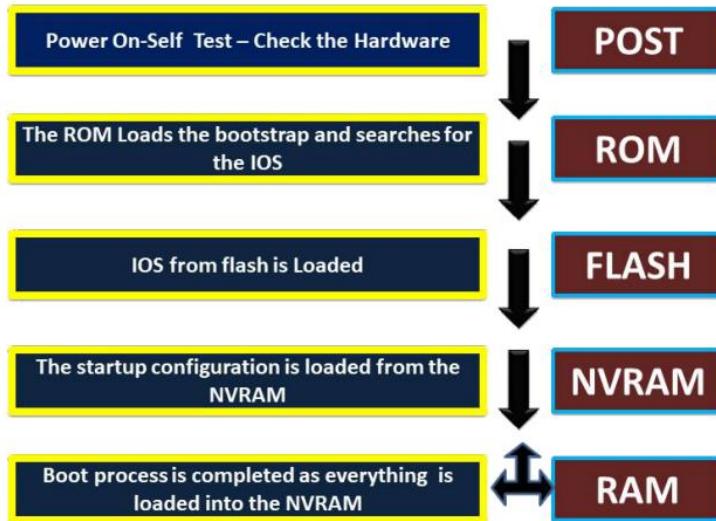
Collision domain, adalah sebuah area pada suatu network, dimana packet yang dikirimkan dapat mengalami tabrakan (collision) dikarenakan dikirim dalam waktu yang bersamaan. Hub memiliki collision domain 1 (besar) karena sifat hub half-duplex, sehingga dapat mengakibatkan terjadinya collision. Sementara itu, pada switch dan router, collision domain hanya terjadi pada tiap interface saja.

**Half Duplex** : Sebuah cara pengiriman data dengan cara menunggu satu data terkirim terlebih dahulu, barulah data yang lain bisa dikirim. Metode ini memungkinkan besanya terjadi tabrakan (collision). Contoh: Hub

**Full Duplex** : Sebuah cara pengiriman data dengan data bebas dikirim kemana saja, karena tiap data memiliki jalurnya masing-masing. Metode ini kecuali kemungkinannya terjadi tabrakan (collision). Contoh: Switch.

## Booting process

Router akan mengalami beberapa process booting sebelum dapat digunakan, berikut penjelasannya.



- **POST (Power on Self-Test)**

Power on Self-Test (POST) merupakan proses yang biasa dilakukan hampir disemua komputer, khususnya saat menjalankan prosedur bootup. Proses POST dilakukan untuk memeriksa perangkat keras (hardware) yang terdapat pada sebuah router. Ketika router dinyalakan, perangkat lunak (software) pada chip ROM melakukan POST.

- **ROM Bootstrap**

Setelah proses POST, program bootstrap akan di-copy dari ROM ke RAM. Setelah program bootstrap berada didalam RAM, processor akan menjalankan instruksi yang terdapat pada program bootstrap tersebut. Fungsi utama program bootsrap adalah mencari lokasi keberadaan dari Cisco IOS (operating system) dan kemudian memuat IOS tersebut kedalam RAM.

- **IOS Load**

Biasanya Internetwork Operating System (IOS) disimpan didalam “flash memory”, tetapi dapat juga disimpan pada media lainnya, contohnya pada TFTP server (Trivial File Transfer Protocol).

- **Configuration Load NVRAM**

Setelah IOS di-copy dari flash memory ke RAM, program bootstrap akan mencari file “startup configuration” atau biasanya disebut “startup-config”. Pada file ini terdapat perintah-perintah konfigurasi.

- **Running Config RAM**

Jika IOS menemukan startup-config pada NVRAM, selanjutnya IOS akan memuat startup-config kedalam RAM. Setelah dimuat ke dalam RAM, startup-config akan disebut sebagai running-config.

# IPv4 & Subnetting

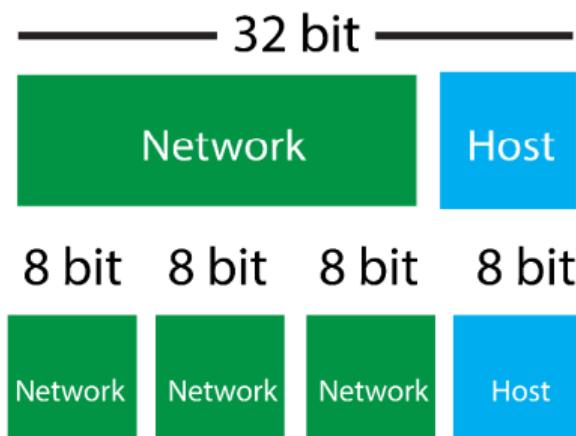
Secara dasar, dalam sebuah jaringan kita pasti membutuhkan sebuah alamat atau address agar semuanya bisa saling berkomunikasi atau terhubung. Atau bisa disebut juga, kita membutuhkan destinasi/tujuan kemana packet-packet yang kita kirimkan akan sampai. Hal seperti itu pasti membutuhkan yang namanya Sender/Pengirim dan Receiver/Penerima. Dan jangan lupa, IP Address ini merupakan pengalaman yang bekerja di layer 3 atau layer network pada OSI Layer.

Karakteristik IP (Internet Protocol) :

1. Beroperasi pada Layer Network di OSI Model.
2. Connectionless protocol: IP tidak meng-setup sebuah koneksi, sehingga untuk mengirim data kita memerlukan “transport” layer dan menggunakan TCP dan UDP.
3. Hierarkis : IP address memiliki aturan penyusunannya sendiri, pembahasannya akan dibahas pada pembahasan subnetting dan subnet mask IPv4 Address total bit-nya adalah 32-bit dan terdiri dari 2 bagian, Network dan Host.

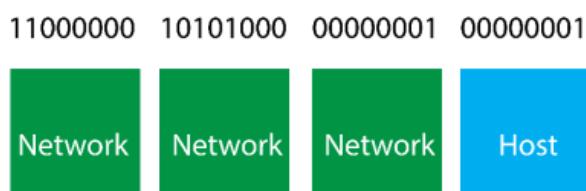
## Penulisan IPv4

Namun, dalam penulisannya, IPv4 dibagi menjadi 8 blok, yang masing-masing blok itu berjumlah 8 bit, bit ini yang sering juga dicebut dengan byte. Jadi  $8 \times 4 = 32$  bit.



Gambar 1 . 3 Total bit IPv4

Maksud dari 8 bit ini, pada tiap blok memiliki 8 bilangan biner (0/1) Seperti gambar dibawah ini.



Gambar 1 . 4 Biner pada 4 blok IPv4

## Konversi Binary ke Desimal

Agar IPv4 bisa digunakan pada perangkat, maka kita harus mengonversi IPv4 ini menjadi bilangan desimal terlebih dahulu. Cara mengonversinya jika tidak menggunakan kalkulator, dapat menggunakan tabel dibawah ini.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1. 5 Konversi Biner ke Desimal

Pada tabel diatas terdapat 8 kolom yang diisi oleh 8 angka biner. Sementara angka yang berada diatasnya merupakan hasil pembagian dari  $2^8$ .

Cara menggunakannya, tinggal mengisi angka 8-bit tadi secara urut dari kiri kekanan. Lalu jumlahkan angka yang berada diatas angka biner 1, angka 0 tidak usah.

Menurut tabel diatas, kita jumlahkan  $128 + 64 = 192$ .

Berarti angka decimal dari biner 11000000 adalah 192.

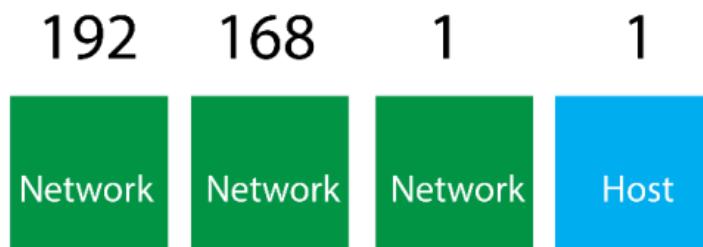
Kita lanjut dari ke blok selanjutnya dengan biner **10101000**. Caranya masih sama jika menggunakan tabel.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1. 5 Konversi Biner ke Desimal

Berdasarkan tabel diatas, kita tinggal menjumlahkan  $128 + 32 + 8 /$  angka diatas biner 1. Maka hasilnya adalah **168**.

Berarti decimal dari **10101000** adalah **168**.



Gambar 1 . 4 Desimal pada 4 blok subnet

Dan untuk 2 blok terakhir, karena binernya sama maka kita tinggal menghitung

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1. 5 Konversi Biner ke Desimal

Sudah terlihat hasilnya, berarti decimal dari **00000001** adalah **1**. Hasilnya jika angka biner dari 4 blok diatas kita susun dalam bentuk decimal, maka akan diperoleh IP Address: **192.168.1.1**  
Begitulah cara konversi IPv4 dari biner ke decimal.

## Konversi Desimal ke Binary

Setelah kita mengetahui bagaimana mengonversi binary ke decimal, kita juga harus mengetahui bagaimana caranya mengonversi Desimal ke Binary/biner. Misalkan mengonversi decimal 105, berapakah binernya?

### Cara Pertama

Caranya adalah dengan membagi 2 tiap bilangan, jika bisa dibagi alias genap maka kita tandai dengan angka 0, jika tidak bisa dibagi alias ganjil, kita tandai dengan angka satu dan kita kurangi 1 pada angka ganjil tersebut, sehingga dapat dibagi. Terus dibagi hingga angka tersebut habis. Jika sudah kita urutkan tanda (0/1) yang telah kita tandai dari tiap pembagian. Kita urutkan dari bawah, maka disitu sudah terlihat angka binernya.

Caranya bisa dilihat pada gambar berikut



Gambar 1 . 5 Cara konversi decimal ke binary

Jika dijabarkan, seperti ini :

1.  $105/2$  : karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1. Maka  $(105-1)/2$ , hasilnya adalah 52 .
2.  $52/2$  : karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 26.
3.  $26/2$  : karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 13.
4.  $13/2$  : karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1. Maka  $(13-1)/2$ , hasilnya adalah 6.
5.  $6/2$  : karena bisa dibagi kita tandai dengan angka 0, hasilnya adalah 3
6.  $3/2$  : karena tidak bisa (ganjil) kita kurangi 1 (agar bisa dibagi) dan kemudian kita tandai 1. Maka  $(3-1)/2$ , hasilnya adalah 1
7.  $1/2$  : karena tidak bisa dibagi dan sudah habis, kita tandai saja dengan angka 1
8. Seperti yang kita lihat, pembagiannya sudah habis, sementara itu jumlah angka biner nya (0/1) belum mencapai 8 alias 8-bit. Maka dari itu, kita tambahkan saja angka 0 dibelakang hingga mencapai 8-bit.
9. Jika sudah, kita urutkan tanda biner yang telah kita buat dari bawah keatas, maka kita akan mendapatkan **1101001 + 0** (melengkapi 8-bit).

Kita coba satu contoh konversi lagi.

Kita konversi decimal 11, berapakah binernya?

1.  $11/2: (11-1)/2 = 5$  (1) -> tandanya
2.  $5/2: (5-1)/2 = 2$  (1) -> tandanya
3.  $2/2= 1$  (0) -> tandanya
4.  $1/2:$  sudah habis dan tidak bisa dibagi (1) -> tandanya
5. Kita urutkan tandanya dari bawah keatas. Maka biner dari 11 adalah 1011 + 0000 (untuk melengkapi 8-bit).

Berdasarkan cara konversi diatas, mungkin akan timbul pertanyaan, Mengapa harus 8-bit?

Alasannya simpel. Kita kembali ke materi penulisan IPv4. Karena, setiap blok pada IPv4 (yang terdiri dari 4 blok) itu terdiri atas 8-bit angka biner, oleh karena itu kita hanya mencari 8-bit angka biner agar dapat kita masukkan dalam sebuah blok pada IPv4.

### Cara kedua

Caranya adalah dengan menggunakan tabel yang kita gunakan untuk mengonversi dari biner ke decimal.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1.5 Konversi Biner ke Desimal

Untuk menggunakan tabel diatas, kita harus bisa menggunakan logika. Misalkan kita mencari biner dari **75**. Maka kita mencari, penjumlahan berapa tambah berapakah dengan bilangan diatas agar mendapatkan angka **75**.

Didapat :  $75 = 64 + 8 + 2 + 1$ . Maka binernya adalah: **01001011**

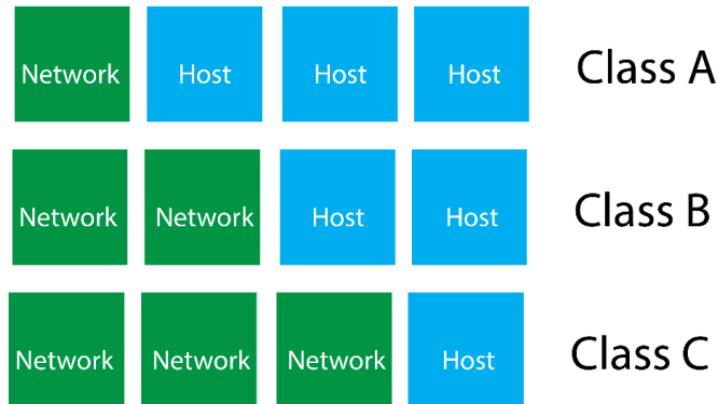
128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Tabel 1.5 Konversi Biner ke Desimal

Begitulah cara konversi dari decimal ke biner, menurut kalian mudah yang mana? Cara pertama atau kedua?

### Klasifikasi IPv4

IPv4 ini, dalam kegunaannya dibagi menjadi tiga kelas A, Kelas B, dan Kelas C.



Gambar 1 . 6 Pembagian kelas IPv4

## Bagian pada IPv4

Bagian Network memberi tahu kita, ID dari Network yang kita gunakan. Bagian Host adalah angka unik yang berbeda di setiap perangkat yang mengidentifikasi perangkat kita. Subnet mask berfungsi untuk memberi tahu komputer, mana bagian Network dan mana bagian Host.

- Kelas A, Kelas A bit pertamanya pasti 0.
- Kelas B, Kelas B 2-bit pertamanya pasti 10.
- Kelas C, Kelas C 3-bit pertamanya pasti 110.

Jika di konversi ke desimal maka kita dapat range IP Address :

- Kelas A = 0.0.0.0 - 126.255.255.255 <> USED FOR VERY LARGE NETWORK
- Kelas B = 128.0.0.0 - 191.255.255.255 <> USED FOR MEDIUM NETWORK
- Kelas C = 192.0.0.0 - 223.255.255.255 <> USED FOR SMALL NETWORKS

Ada pula kelas D dan E namun mereka tidak digunakan untuk penggunaan host :

- Kelas D = 224.0.0.0 - 239.255.255.255 <> USED FOR MULTICAST
- Kelas E = 240.0.0.0 - 247.255.255.255 <> USED FOR EXPERIMENTAL

Range IPv4 Private :

Kelas	Range IP	Subnet	Jumlah IP
A	10.0.0.0 – 10.255.255.255	255.0.0.0	16.777.212
B	172.16.0.0 – 172.16.31.255	255.255.0.0	8.190
C	192.168.0.0 – 192.168.255.255	255.255.255.0	65.354

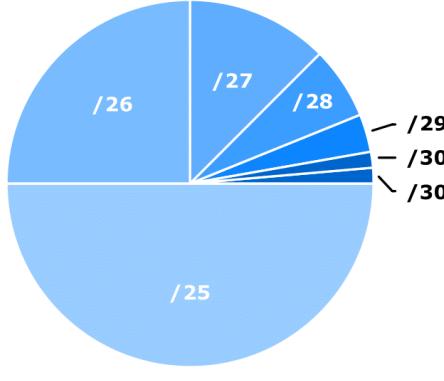
Tabel 3 . 8 Daftar range IP Private IPv4

Ada juga range IP khusus yang digunakan untuk keperluan tertentu :

- 127.X.X.X = Digunakan untuk IP Loopback.
- 0.0.0.0 = Digunakan untuk routing seluruh network yang ada didunia (default route).
- 169.254.0.0/16 = Digunakan untuk Link Local Address(APIPA).

# IPv4 SUBNETTING

packetlife.net

Subnets				Decimal to Binary			
CIDR	Subnet Mask	Addresses	Wildcard	Subnet Mask		Wildcard	
/32	255.255.255.255	1	0.0.0.0	255	1111 1111	0 0000 0000	
/31	255.255.255.254	2	0.0.0.1	254	1111 1110	1 0000 0001	
/30	255.255.255.252	4	0.0.0.3	252	1111 1100	3 0000 0011	
/29	255.255.255.248	8	0.0.0.7	248	1111 1000	7 0000 0111	
/28	255.255.255.240	16	0.0.0.15	240	1111 0000	15 0000 1111	
/27	255.255.255.224	32	0.0.0.31	224	1110 0000	31 0001 1111	
/26	255.255.255.192	64	0.0.0.63	192	1100 0000	63 0011 1111	
/25	255.255.255.128	128	0.0.0.127	128	1000 0000	127 0111 1111	
/24	255.255.255.0	256	0.0.0.255	0	0000 0000	255 1111 1111	
/23	255.255.254.0	512	0.0.1.255	Subnet Proportion			
/22	255.255.252.0	1,024	0.0.3.255				
/21	255.255.248.0	2,048	0.0.7.255				
/20	255.255.240.0	4,096	0.0.15.255				
/19	255.255.224.0	8,192	0.0.31.255				
/18	255.255.192.0	16,384	0.0.63.255				
/17	255.255.128.0	32,768	0.0.127.255				
/16	255.255.0.0	65,536	0.0.255.255				
/15	255.254.0.0	131,072	0.1.255.255				
/14	255.252.0.0	262,144	0.3.255.255				
/13	255.248.0.0	524,288	0.7.255.255				
/12	255.240.0.0	1,048,576	0.15.255.255				
/11	255.224.0.0	2,097,152	0.31.255.255				
/10	255.192.0.0	4,194,304	0.63.255.255	Classful Ranges			
/9	255.128.0.0	8,388,608	0.127.255.255	A	0.0.0.0 - 127.255.255.255		
/8	255.0.0.0	16,777,216	0.255.255.255	B	128.0.0.0 - 191.255.255.255		
/7	254.0.0.0	33,554,432	1.255.255.255	C	192.0.0.0 - 223.255.255.255		
/6	252.0.0.0	67,108,864	3.255.255.255	D	224.0.0.0 - 239.255.255.255		
/5	248.0.0.0	134,217,728	7.255.255.255	E	240.0.0.0 - 255.255.255.255		
/4	240.0.0.0	268,435,456	15.255.255.255	Reserved Ranges			
/3	224.0.0.0	536,870,912	31.255.255.255	RFC 1918	10.0.0.0 - 10.255.255.255		
/2	192.0.0.0	1,073,741,824	63.255.255.255	localhost	127.0.0.0 - 127.255.255.255		
/1	128.0.0.0	2,147,483,648	127.255.255.255	RFC 1918	172.16.0.0 - 172.31.255.255		
/0	0.0.0.0	4,294,967,296	255.255.255.255	RFC 1918	192.168.0.0 - 192.168.255.255		

## Terminology

### CIDR

Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

### VLSM

Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes

by Jeremy Stretch

v2.0

# **Basic Configuration**

## Basic Configuration

### Command Line Interface (CLI) Mode

Router>

Ketika tanda ‘>’ ini pada posisi user mode

Router#

Ketika tanda ‘#’ ini adalah pada posisi privilege mode

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Ketika muncul ‘router(config)#’ ini pada posisi global config mode. Dari global config mode, jika ingin kembali ke privilege mode, kita tinggal mengetik command “exit”.

**Enable** : Perintah di mode user untuk memasuki mode privilege

**Configure terminal** : Perintah di mode privilege untuk memasuki mode global

**Router(config)#** : Tanda bahwa kita sudah masuk di mode global.

Ada 3 mode yang harus network engginner pahami :

#### User mode

Dalam user mode, kita hanya dibataskan beberapa perintah untuk monitoring. Merupakan mode pertama saat kita mengaktifkan perangkat Cisco.

#### Privilege mode

Pada mode ini, kita hanya dapat melihat konfigurasi, tanpa menambahkan konfigurasi.

#### Global configuration mode

Pada mode ini, kita sudah dapat menambahkan, mengubah, dan menghapus konfigurasi. Merupakan mode dimana kita dapat mengakses router secara keseluruhan.

#### Perintah show

Perintah ‘show’ ini digunakan untuk melakukan pengecekan di mode privilege namun ketika di mode global pengecekannya ditambah **do** contohnya ‘**do show run**’

Router#show version

Router#show flash

Router#show start

Router#show run

Perintah “show run” untuk melihat konfigurasi yang sedang berjalan , bisa juga di ketik router#show running-config. Atau diketik router#show run (tekan tombol tab, maka akan auto complete).

Berikut contoh melihat konfigurasi :

```
Router#show run
Building configuration...

Current configuration : 852 bytes
!
version 12.4
service timestamps debug datetime msec s
service timestamps log datetime msec no
service password-encryption
!
hostname Router >>> Hostname dari router
! boot-start-marker boot-end-marker
! no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable ip
cef
! no ip domain lookup
!
multilink bundle-name authenticated
! archive log config
idekeys
!!
ip tcp synwait-time 5
!
interface FastEthernet0/0 >>> nama interface
no ip address >>> IP address shutdown
>>>> Status port duplex auto speed auto
!
interface FastEthernet0/1 >>> nama interface
no ip address >>> IP address shutdown
>>>> Status port duplex auto speed auto
! no ip http server no ip
http secure-server
!!
control-plane ! line con 0 exec-timeout 0 0 privilege level 15 logging
synchronous line aux 0 exec-timeout 0 0
privilege level 15 logging synchronous
line vty 0 4 login ! ! end
```

## 8 Initial Configuration

1. **Hostname** : -Digunakan untuk menamai device yang kita konfigurasi, biasanya sebagai tanda pengenal untuk lebih mudah membedakan antara device satu dan yang lain.

Berikut konfigurasinya :

```
Router>enable  
Router#conf t  
Router(config)#hostname Router-Core --> Mengganti hostname  
Router-Core (config) #
```

2. **Password** : -Digunakan untuk memberikan keamanan pada device, agar device tersebut tidak bisa sembarangan di remote oleh orang, namun kurang aman (tidak terenkripsi).

Berikut konfigurasinya :

```
Router-Core(config)#enable password 123
```

3. **Secret** : -Fungsinya sama seperti password, namun keamanan secret jauh lebih tinggi dibanding password dan terenkripsi, jika kita lihat pada command show run maka password akan kelihatan, namun secret tidak.

Berikut konfigurasinya :

```
Router-Core(config)#enable secret 321
```

4. **Banner** : -Fungsinya memberi kata sambutan ketika kita mulai meremote device yang diberi command banner.

Berikut konfigurasinya :

```
Router-Core (config)#banner motd Z  
Enter TEXT message. End with the character 'Z'.  
Selamat pagi bro!! Z -> Setelah selesai masukkan huruf 'Z'
```

Catatan : kita bisa mengganti 'Z' dengan huruf lain, seperti banner motd K, maka pada akhir kalimat masukkan huruf 'K'.

Untuk melihat hasilnya, kita kembali ke mode user, ketik **exit**.

```
Selamat pagi bro!!  
Router-Core>
```

5. **Remote Access** : -Fungsinya untuk memberi akses remote device menggunakan protocol Telnet maupun SSH, jadi tidak perlu menggunakan console lagi. Lebih lengkapnya dibahas setelah ini.

Kemudian coba kita lihat pada show run dan bandingkan dengan password.

```
Router-Core(config)#do show run
Building configuration...

Current configuration : 627 bytes
!
version 12.4 no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router-Core
!
!
!
enable secret 5 $1$mERr$DadO.ZoS.MDbWMQdR.LSo0
enable password 123
```

Hasilnya secret tidak terlihat karena terenkripsi sementara password tidak.

6. **Menyimpan Konfigurasi** : -Setelah kita melakukan banyak konfigurasi di router maupun di switch jangan lupa untuk menyimpan konfigurasinya, konfigurasi itu disimpan di tempat yang biasa kita kenal dengan **Nvram**. Bisa dilakukan dengan melakukan perintah “**do write**”

Berikut perintahnya :

```
Router-Core (config)#do write
do write Building configuration...
[OK]
```

7. **Menghapus Konfigurasi** : -Perintah ini dilakukan/diterapkan jika kita ingin menghapus seluruh konfigurasi router maupun switch yaitu dengan melakukan perintah “**do write erase**”

Berikut perintahnya :

```
Router-Core (config)#do write erase
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

8. **Merestart Router/Switch** : -Ketika kita ingin merestart ulang konfigurasi dari awal, perintahnya adalah “**do reload**”

Berikut perintahnya :

```
Router-Core (config)#do reload
System configuration has been modified. Save? [yes/no]:no
Proceed with reload? [confirm]
```

Kalian bisa pilih **no** untuk merestart ulang device.

---

“BARANGSIAPA YANG ENGGAN MERASAKAN  
PAHITNYA MENUNTUT ILMU, MAKA BERSIAPLAH  
UNTUK MENERIMA HINANYA KEBODOHAN.”

---

-Imam Syafi'i-

# Switching

# Switching

## CONTENT :

VLAN (VIRTUAL LAN)

TRUNK

Allowed Trunk

MLS TRUNK

INTERVLAN ROUTING

SVI (SWITCH INTERFACE VIRTUAL)

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

PORt SECURITY

TELNET

SSH (SECURE SHELL HOST)

STP (SPANNING TREE PROTOCOL)

ETHERCHANNEL

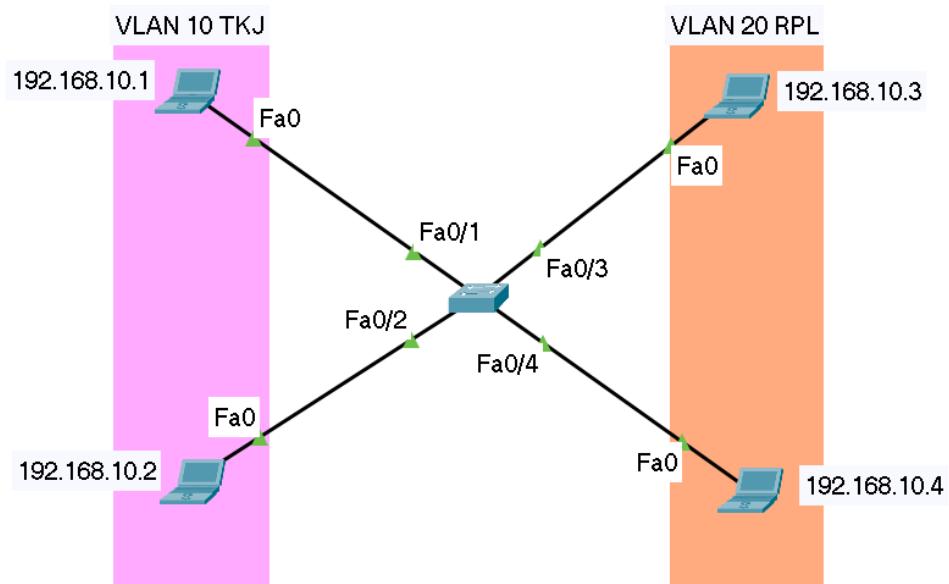
SWITCH STACKING

## Lab 1. Virtual Local Area Network (VLAN)

VLAN merupakan singkatan dari **Virtual Local Area Network**, yang berarti membuat sebuah LAN buatan dalam perangkat jaringan, yang maksudnya dapat memecah satu network menjadi beberapa bagian yang dimana tiap bagian ini tidak dapat saling berkomunikasi padahal sudah satu network.

Hal ini dikarenakan VLAN tadi yang memecah jaringan networknya dan VLAN ini berjalan/hanya bisa dikonfigurasi di switch yang bekerja di layer-2 yaitu **data link**. Karena switch sendiri merupakan perangkat yang bisa menghubungkan satu jaringan saja. Istilah lain dalam VLAN yaitu adalah VLAN **default** yang mana itu adalah kondisi awal port sebelum dimasukan ke dalam VLAN tertentu.

Misalkan kita menggunakan **switch unmanagable**, switch-switch harga murahan, maka semua portnya hanya bisa digunakan untuk dikoneksikan ke PC/laptop yang networknya sama. Nah pada **switch managable**, kita bisa membuat pada sebuah switch untuk digunakan network yang berbeda. Setiap network memiliki LAN sendiri, sehingga pada sebuah switch seolah-olah terdapat beberapa LAN. Kiita akan mengkonfigurasikan VLAN di topologi dibawah ini :



Dengan adanya VLAN ini, maka kita bisa memisahkan atau mengelompokkan user sesuai kebutuhannya masing-masing.misalkan kita membuat VLAN TKJ,VLAN RPL bisa juga berdasarkan lantai,misalkan VLAN 10 buat lantai 1 dan VLAN 20 buat lantai 2 DLL.

Langkah Langkah :

- A. Konfigurasi di Switch
  1. Mengganti nama hostname

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-IDN
```

2. Membuat VLAN 10 dan VLAN 20

```
SW-IDN(config)#vlan 10  
SW-IDN(config)#name TKJ
```

```
SW-IDN(config)#vlan 20  
SW-IDN(config)#name RPL
```

**Vlan 10** : Adalah perintah untuk membuat VLAN, 20 hanya angka penomoran VLAN (Angka bebas).

**Name TKJ** : Memberi nama VLAN tersebut yaitu TKJ.

3. Memasukan interface kedalam VLAN

```
SW-IDN(config)#interface fa0/1  
SW-IDN(config)#switchport mode access  
SW-IDN(config)#switchport access vlan 10
```

```
SW-IDN(config)#interface fa0/2  
SW-IDN(config)#switchport mode access  
SW-IDN(config)#switchport access vlan 10
```

```
SW-IDN(config)#interface fa0/3  
SW-IDN(config)#switchport mode access  
SW-IDN(config)#switchport access vlan 20
```

```
SW-IDN(config)#interface fa0/4  
SW-IDN(config)#switchport mode access  
SW-IDN(config)#switchport access vlan 20
```

**Interface fa0/1** : Adalah interface yang akan kita pilih untuk dimasukan kedalam VLAN 10.

**Switchport mode access** : Perintah untuk memberikan access kepada interface tersebut.

**Switchport access vlan 10** : Perintah agar interface yang telah ditentukan masuk kedalam VLAN 10.

Jika sudah, kita cek terlebih dahulu dengan perintah **do show vlan**, kita pastikan port fa0/1 dan fa0/2 sudah menjadi member VLAN 10 dan port VLAN fa0/3 da fa0/4 menjadi member VLAN 20. Biasakan setelah konfigurasi lakukan cek terlebih dahulu

B. Pengecekan

1. Pengecekan interface sebelum dimasukan kedalam VLAN

```
SW-IDN(config)#do show vlan
```

SW-IDN(config-if-range)#do 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 Fa0/20 Fa0/24	
10 TKJ	active		
20 RPL	active		
1002 fddi-default	active		
1003 token-ring-default	active		
1004 fddinet-default	active		
1005 trnet-default	active		

Dalam SS an diatas terlihat bahwa kita sudah mengkonfigurasi sebuah VLAN tetapi belum memasukan sebuah interface kedalamnya. Interface interface itu masuk kedalam VLAN default nya switch yaitu VLAN 1.

## 2. Pengecekan interface sesudah dimasukan kedalam VLAN

SW-IDN(config)#do show vlan			
SW-IDN(config)#do show vlan			
VLAN Name	Status	Ports	
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/20 Fa0/24	
10 TKJ	active	Fa0/1, Fa0/2	
20 RPL	active	Fa0/3, Fa0/4	
1002 fddi-default	active		
1003 token-ring-default	active		
1004 fddinet-default	active		
1005 trnet-default	active		

Dalam SS an selanjutnya bisa dilihat bahwa kita sudah memasukan interface ke dalam VLAN yang sudah ditentukan, interface yang sudah dimasukan kedalam VLAN sudah resmi menjadi anggota/member dari VLAN itu sendiri. Sedangkan jika kita ingin menghapus interface yang berada didalam VLAN perintahnya sebagai berikut :

```
SW-IDN(config)#interface fa0/1
SW-IDN(config)#no switchport mode access
SW-IDN(config)#no switchport access vlan 10
```

Misalkan seperti perintah diatas jika kita ingin menghapus interface fa0/1 yang berada didalam VLAN 10 **perintah pertama** pilih interface mana yang ingin kalian hapus, setelah itu jika ingin menambahkan VLAN, kan perintahnya switchport mode access nah jika kita ingin menghapus perintahnya ditambahkan **no**

begitupun perintah seterusnya. Maka interface fa0/1 sudah tidak menjadi anggota/member dari VLAN 10.

Setelah itu hal yang paling terpenting adalah memasang IP Address untuk laptop, karena **IP Address** dapat berfungsi sebagai identitas diri dari suatu perangkat. **IP Address** ini dapat menyimpan data penting seperti lokasi atau bahkan tempat tinggal kalian saat ini.

C. Konfigurasi IP Address laptop :

1. Laptop A

**IP Configuration**

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

2. Laptop B

**IP Configuration**

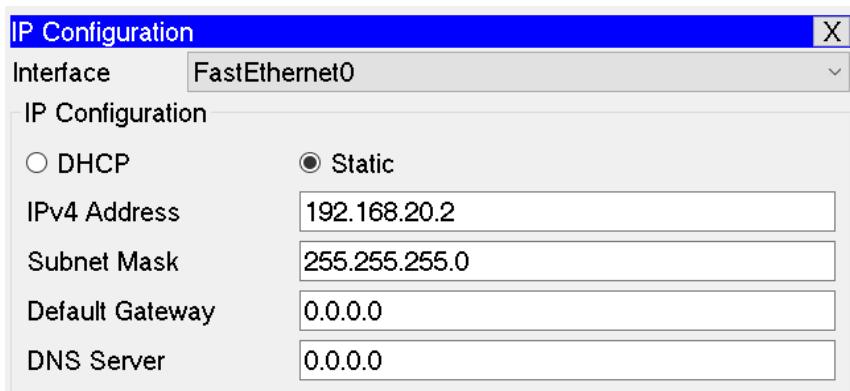
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

3. Laptop C

**IP Configuration**

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

4. Laptop D

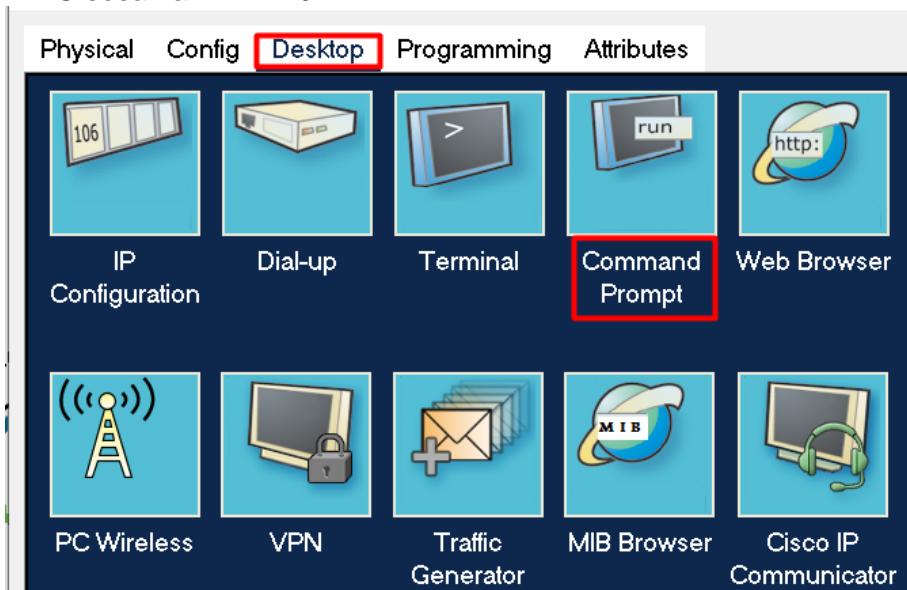


**Keterangan :** Laptop A dan B adalah laptop yang berada di VLAN 10 dan laptop C dan D adalah yang berada di VLAN 20.

Setelah memasang IP Address yaitu melakukan pengecekan dengan melakukan ping sesama VLAN dan antar VLAN.

#### D. Test PING

##### 1. PING sesama VLAN 10



Buka laptop VLAN 10 yang atas, kemudian pilih desktop setelah itu klik command prompt.

```
Command Prompt
X

Packet Tracer PC Command Line 1.0
C:\>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<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms 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
```

Tampilannya seperti gambar diatas kemudian masukan IP Address VLAN 10 yang bawah, setelah itu klik enter aja jika ada tulisan **reply from blablabla** seperti tulisan diatas itu berarti PING telah berhasil/success.

2. PING VLAN 10 dan 20

```
C:\>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),  
  
C:\>
```

Laptop gagal melakukan PING/**request timed out** karena laptop sudah berbeda network, Jadi pertanyaannya adalah kapan kita menggunakan VLAN? jawabannya adalah disaat kita ingin membagi/memecah network. Dan VLAN hanya bisa dibuat di switch managable

E. Lab VLAN telah selesai.

# VLANs

packetlife.net

Trunk Encapsulation					Trunk Types	
ISL	26 ISL Header	6 Dest MAC	6 Source MAC	2 Type	4 FCS	802.1Q ISL
Untagged		Dest MAC	Source MAC	Type		Header Size 4 bytes Trailer Size N/A Standard IEEE Maximum VLANs 4094
802.1Q	6 Dest MAC	6 Source MAC	4 802.1Q	2 Type		26 bytes 4 bytes Cisco 1000
VLAN Creation					VLAN Numbers	
Switch(config)# vlan 100 Switch(config-vlan)# name Engineering					0 Reserved	1004 fdnet
					1 default	1005 trnet
					1002 fddi-default	1006-4094 Extended
					1003 tr	4095 Reserved
Access Port Configuration					Terminology	
Switch(config-if)# switchport mode access Switch(config-if)# switchport nonegotiate Switch(config-if)# switchport access vlan 100 Switch(config-if)# switchport voice vlan 150					Trunking Carrying multiple VLANs over the same physical connection	
Trunk Port Configuration					Native VLAN By default, frames in this VLAN are untagged when sent across a trunk	
Switch(config-if)# switchport mode trunk Switch(config-if)# switchport trunk encapsulation dot1q Switch(config-if)# switchport trunk allowed vlan 10,20-30 Switch(config-if)# switchport trunk native vlan 10					Access VLAN The VLAN to which an access port is assigned	
SVI Configuration					Voice VLAN If configured, enables minimal trunking to support voice traffic in addition to data traffic on an access port	
Switch(config)# interface vlan100 Switch(config-if)# ip address 192.168.100.1 255.255.255.0					Dynamic Trunking Protocol (DTP) Can be used to automatically establish trunks between capable ports (insecure)	
VLAN Trunking Protocol (VTP)					Switched Virtual Interface (SVI) A virtual interface which provides a routed gateway into and out of a VLAN	
<b>Domain</b> Common to all switches participating in VTP					Switch Port Modes	
<b>Server Mode</b> Generates and propagates VTP advertisements to clients; default mode on unconfigured switches					trunk	Forms an unconditional trunk
<b>Client Mode</b> Receives and forwards advertisements from servers; VLANs cannot be manually configured on switches in client mode					dynamic desirable	Attempts to negotiate a trunk with the far end
<b>Transparent Mode</b> Forwards advertisements but does not participate in VTP; VLANs must be configured manually					dynamic auto	Forms a trunk only if requested by the far end
<b>Pruning</b> VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic					access	Will never form a trunk
VTP Configuration					Troubleshooting	
Switch(config)# vtp mode {server   client   transparent} Switch(config)# vtp domain <name> Switch(config)# vtp password <password> Switch(config)# vtp version {1   2} Switch(config)# vtp pruning					show vlan show interface [status   switchport] show interface trunk show vtp status show vtp password	

by Jeremy Stretch

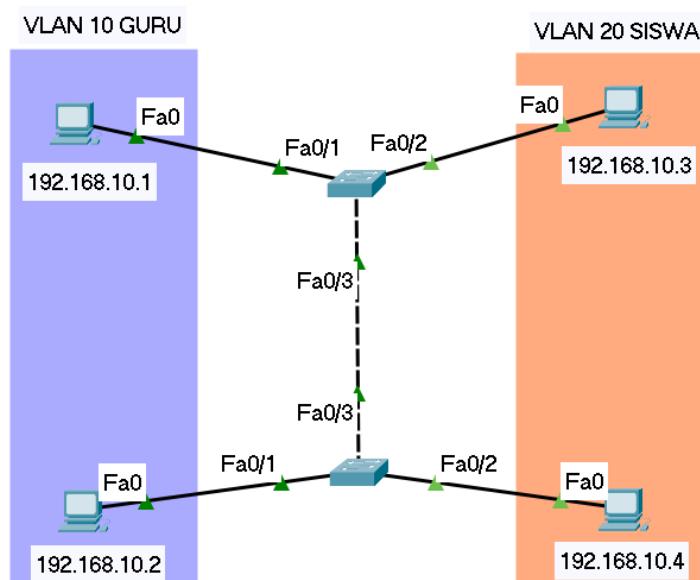
v2.0

## Lab 2. Trunk

Bagaimana caranya jika kita ingin menghubungkan 2 buah laptop pada network dan VLAN yang sama, di-2 switch yang berbeda? Caranya dengan menggunakan Trunk, pada dasarnya trunk adalah sebuah protocol pada interface switch yang digunakan untuk menyalurkan informasi VLAN.

Ada 2 jenis protocol trunk :

1. **ISL** (Cisco Propetary)- Protokol encapsulasi trunk yang hanya dikhususkan untuk switch cisco.
2. **dot1q** (Open Standard)- Protokol encapsulasi trunk standar yang bisa digunakan disemua jenis dan merek switch.



Berdasarkan topologi diatas, agar kedua buah switch bisa saling tethubung, kita konfigurasikan trunk pada interface yang mengarah ke switch lain.

Langkah Langkah :

A. Konfigurasi di Switch atas

1. Mengganti nama hostname

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-ATAS
```

2. Membuat VLAN 10 dan VLAN 20

```
SW-ATAS(config)#vlan 10  
SW-ATAS(config)#name GURU
```

```
SW-ATAS(config)#vlan 20  
SW-ATAS(config)#name SISWA
```

3. Memasukan interface ke dalam VLAN

```
SW-ATAS(config)#interface fa0/1  
SW-ATAS(config)#switchport mode access
```

```
SW-ATAS(config)#switchport acces vlan 10
```

```
SW-ATAS(config)#interface fa0/2
```

```
SW-ATAS(config)#switchport mode access
```

```
SW-ATAS(config)#switchport access vlan 20
```

4. Melakukan trunk di switch atas

```
SW-ATAS(config)#interface fa0/3
```

```
SW-ATAS(config)#switchport mode trunk
```

**Switchport mode trunk** : Adalah perintah untuk mengaktifkan protocol trunk.

B. Konfigurasi di Switch bawah

1. Mengganti nama hostname

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#hostname SW-BAWAH
```

2. Membuat VLAN 10 dan VLAN 20

```
SW-BAWAH(config)#vlan 10
```

```
SW-BAWAH(config)#name GURU
```

```
SW-BAWAH(config)#vlan 20
```

```
SW-BAWAH(config)#name SISWA
```

3. Memasukan interface ke dalam VLAN

```
SW-BAWAH(config)#interface fa0/1
```

```
SW-BAWAH(config)#switchport mode access
```

```
SW-BAWAH(config)#switchport acces vlan 10
```

```
SW-BAWAH(config)#interface fa0/1
```

```
SW-BAWAH(config)#switchport mode access
```

```
SW-BAWAH(config)#switchport access vlan 20
```

4. Melakukan trunk di switch bawah

```
SW-BAWAH(config)#interface fa0/3
```

```
SW-BAWAH(config)#switchport mode trunk
```

Untuk mengecek apakah trunk yang kita konfigurasikan sudah berjalan atau belum pengecekannya sebagai berikut :

C. Pengecekan

1. Pengecekan trunk di switch atas

```
SW-ATAS(config)#do show interface trunk
```

```
SW-ATAS(config)#do show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/3	on	802.1q	trunking	1

```
Port Vlans allowed on trunk
```

```
Fa0/3 1-1005
```

```
Port Vlans allowed and active in management domain
```

```
Fa0/3 1,10,20
```

```
Port Vlans in spanning tree forwarding state and not pruned
```

```
Fa0/3 1,10,20
```

2. Pengecekan trunk di switch atas

```

SW-ATAS(config)#do show interface trunk
SW-BAWAH(config) # do show interface trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/3    on        802.1q         trunking     1

Port      Vlans allowed on trunk
Fa0/3    1-1005

Port      Vlans allowed and active in management domain
Fa0/3    1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/3    1,10,20

```

Protocol trunk sendiri hanya bisa dilakukan oleh switch ke 3 network device ini yaitu router, sesama switch, dan switch MLS.

#### D. Konfigurasi IP Address laptop

##### 1. Laptop A

**IP Configuration**

Interface FastEthernet0

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

##### 2. Laptop B

**IP Configuration**

Interface FastEthernet0

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

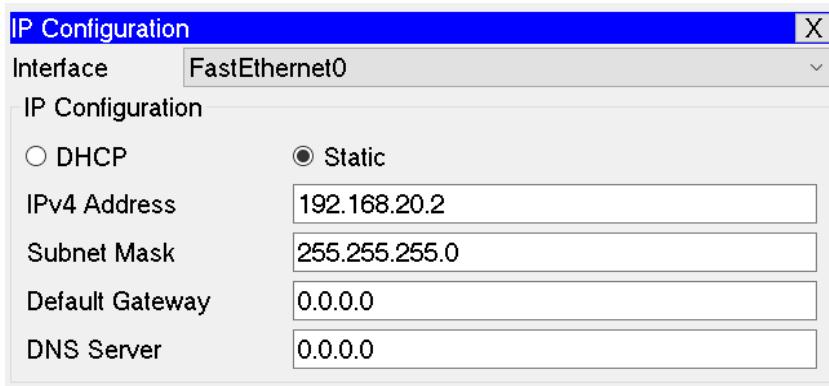
##### 3. Laptop C

**IP Configuration**

Interface FastEthernet0

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

##### 4. Laptop D



Untuk pengetesannya, lakukan tes ping ke PC lain yang masih dalam satu network yang sama namun berbeda switch dan pastikan berhasil mendapatkan Reply.

#### E. Test PING

1. Sesama VLAN switch atas dan bawah

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<lms TTL=128
Reply from 192.168.10.2: bytes=32 time=lms TTL=128
Reply from 192.168.10.2: bytes=32 time<lms TTL=128
Reply from 192.168.10.2: bytes=32 time<lms TTL=128

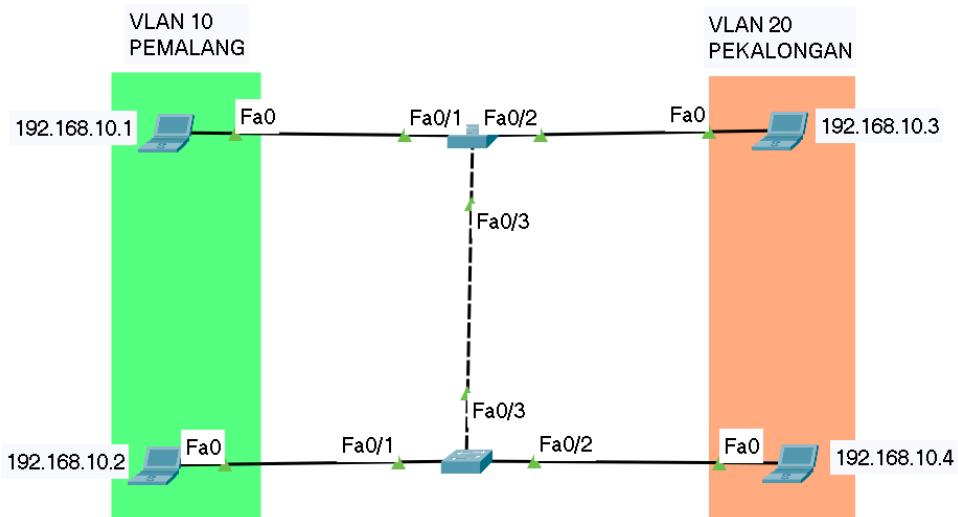
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = lms, Average = 0ms
```

Terlihat bahwa kita sudah melakukan PING sesama VLAN switch atas dan bawah hasilnya success karena kita sudah menerapkan protocol trunking ini. Nah jadi pertanyaanya adalah kapan kita menggunakan protocol trunking? jawabannya ketika kita mempunyai 2 switch atau lebih dalam satu VLAN dan switch itu ingin terhubung sesama lain maka trunk solusinya.

#### F. Lab Trunk telah selesai.

## Lab 3. Allowed Trunk

Filtering VLAN saat menggunakan trunk sering kali harus dilakukan. Karena secara default mode trunking pada Cisco akan allow semua VLAN dan pada case-case tertentu kita ingin filter beberapa VLAN agar tidak dilewatkan ke switch lainnya. Dengan topologi dibawah kita akan mencoba untuk filtering VLAN 20 agar tidak dilewatkan ke Switch atas.



Caranya dengan masuk ke interface trunk, Lalu memilih VLAN mana yang akan di perbolehkan atau VLAN mana yang akan di filter, ikuti Langkah Langkah berikut ini :

Langkah Langkah :

A. Konfigurasi di switch atas

1. Mengganti nama hostname

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-ATAS
```

2. Membuat VLAN 10 dan VLAN 20

```
SW-ATAS(config)#vlan 10  
SW-ATAS(config)#name GURU
```

```
SW-ATAS(config)#vlan 20  
SW-ATAS(config)#name SISWA
```

3. Memasukan interface ke dalam VLAN

```
SW-ATAS(config)#interface fa0/1  
SW-ATAS(config)#switchport mode access  
SW-ATAS(config)#switchport acces vlan 10
```

```
SW-ATAS(config)#interface fa0/2  
SW-ATAS(config)#switchport mode access  
SW-ATAS(config)#switchport access vlan 20
```

4. Melakukan trunk di switch atas

```
SW-ATAS(config)#interface fa0/3  
SW-ATAS(config)#switchport mode trunk
```

5. Memasang Konfigurasi Allowed Trunk

```
SW-ATAS(config)#interface fa0/3  
SW-ATAS(config)#switchport trunk allowed vlan 20
```

**Switchport trunk allowed vlan 20** : Perintah untuk mengizinkan VLAN 20 untuk melakukan sinkronisasi, tetapi jika kita mempunyai 3 VLAN/lebih dan hanya ingin mengizinkan 2 VLAN yang melakukan sinkronisasi contoh perintahnya adalah **switchport trunk allowed vlan 20,30**. begitupula seterusnya.

B. Konfigurasi di switch bawah

1. Mengganti nama hostname

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-BAWAH
```

2. Membuat VLAN 10 dan VLAN 20

```
SW-BAWAH(config)#vlan 10  
SW-BAWAH(config)#name GURU
```

```
SW-BAWAH(config)#vlan 20  
SW-BAWAH(config)#name SISWA
```

3. Memasukan interface ke dalam VLAN

```
SW-BAWAH(config)#interface fa0/1  
SW-BAWAH(config)#switchport mode access  
SW-BAWAH(config)#switchport acces vlan 10
```

```
SW-BAWAH(config)#interface fa0/2  
SW-BAWAH(config)#switchport mode access  
SW-BAWAH(config)#switchport access vlan 20
```

4. Melakukan trunk di switch atas

```
SW-BAWAH(config)#interface fa0/3  
SW-BAWAH(config)#switchport mode trunk
```

5. Memasang Konfigurasi Allowed Trunk

```
SW-BAWAH(config)#interface fa0/3  
SW-BAWAH(config)#switchport trunk allowed vlan 20
```

Untuk pengecekan allowed trunk sebagai berikut :

C. Pengecekan

1. Pengecekan allowed trunk switch atas

```
SW-ATAS(config)#do show interface trunk  
SW-ATAS(config)#do show int trunk  
Port      Mode       Encapsulation  Status      Native vlan  
Fa0/3     on        802.1q         trunking      1  
  
Port      Vlans allowed on trunk  
Fa0/3     20  
  
Port      Vlans allowed and active in management domain  
Fa0/3     20  
  
Port      Vlans in spanning tree forwarding state and not pruned  
Fa0/3     20
```

2. Pengecekan allowed trunk switch bawah

```
SW-BAWAH(config)#do show int trunk
SW-BAWAH(config-if)#do show interface trunk
Port      Mode       Encapsulation  Status        Native vlan
Fa0/3    auto       n-802.1q      trunking      1

Port      Vlans allowed on trunk
Fa0/3    20

Port      Vlans allowed and active in management domain
Fa0/3    20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/3    20
```

Dapat dilihat bahwa kita sudah menerapkan allowed trunk untuk VLAN 20 switch atas dan bawah, selanjutnya adalah memasang IP Address laptop.

D. Konfigurasi IP Address laptop

1. Laptop A

IP Configuration

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

2. Laptop B

IP Configuration

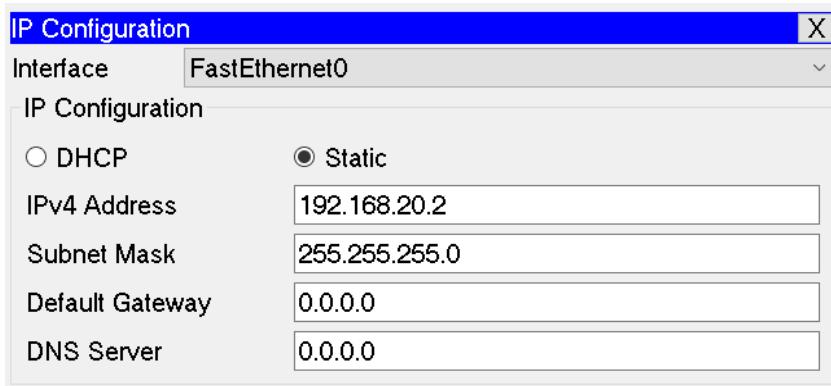
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

3. Laptop C

IP Configuration

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

4. Laptop D



Setelah memasang IP Address Langkah selanjutnya kita akan melakukan test PING tetapi bukan sesama VLAN 10, karena kita tadi sudah mengkonfigurasi untuk mengizinkan VLAN 20 saja untuk sinkronisasi,

#### E. Test PING

##### 1. Sesama VLAN 10

```
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

##### 2. Sesama VLAN 20

```
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.2
Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time=lms TTL=128
Reply from 192.168.20.2: bytes=32 time<lms TTL=128
Reply from 192.168.20.2: bytes=32 time<lms TTL=128
Reply from 192.168.20.2: bytes=32 time=lms 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 = lms, Average = 0ms
```

Bisa dilihat PING sesama VLAN 10 hasilnya gagal sedangkan PING sesama VLAN 20 berhasil, artinya allowed trunk tadi sudah berhasil diterapkan oleh switch. Jadi fungsi allowed trunk disini adalah untuk mengizinkan beberapa VLAN saja yang melakukan sinkronisasi.

#### F. Lab Allowed Trunk telah selesai.

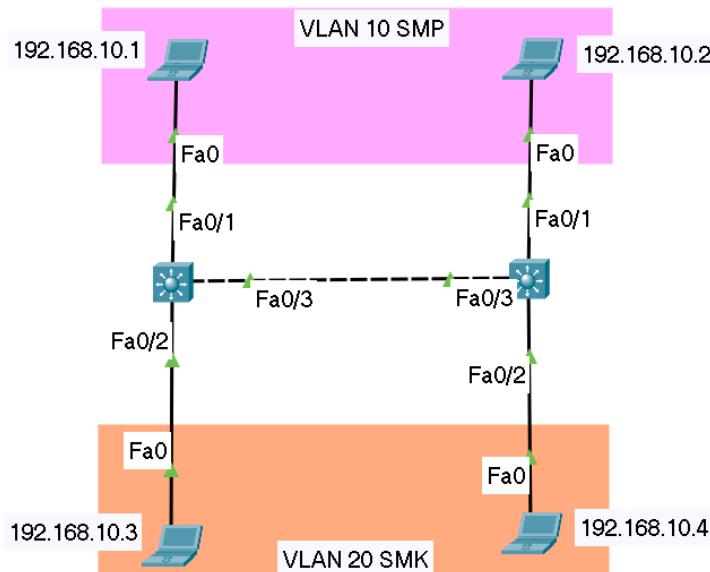
## Lab 4. MLS Trunk

MLS (Multi-Layer Switch) adalah salah satu hardware yang mirip dengan router karena MLS sendiri mempunyai fungsi layer-3, dan uniknya MLS mempunyai layer-2 juga seperti namanya sendiri **Multi-Layer**. Dan MLS bisa menambahkan IP Address dan melakukan routing.

Untuk MLS protocol trunk nya menggunakan dot1q kenapa tidak menggunakan trunk ISL karena trunk ISL hanya untuk (cisco proprietary). Sedangkan dot1q untuk open standard jadi bisa digunakan untuk seluruh merek.

Kenapa kita menggunakan switch MLS jawabannya adalah :

- Switch MLS bisa berfungsi sebagai router.
- Berbeda dengan switch biasanya.
- Jika kita mempunyai minus budget dan ingin membeli alat yang mempunyai 2 fungsi maka MLS adalah solusinya.



Baik kita akan mengkonfigurasi MLS Trunk pada topologi di atas langkah langkah sebagai berikut :

Langkah Langkah :

- A. Konfigurasi di Switch MLS kiri
  1. Mengganti hostname MLS

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-KIRI
```

2. Membuat VLAN 10 dan 20

```
SW-KIRI(config)#vlan 10  
SW-KIRI(config)#name SMP
```

```
SW-KIRI(config)#vlan 20  
SW-KIRI(config)#name SMK
```

3. Memasukan interface ke VLAN

```
SW-KIRI(config)#interface fa0/1
SW-KIRI(config)#switchport mode access
SW-KIRI(config)#switchport access vlan 10
```

```
SW-KIRI(config)#interface fa0/2
SW-KIRI(config)#switchport mode access
SW-KIRI(config)#switchport access vlan 20
```

4. Melakukan Trunk dot1q

```
SW-KIRI(config #interface fa0/3
SW-KIRI(config #switchport trunk encapsulation dot1q
SW-KIRI(config #switchport mode trunk
```

**Switchport trunk encapsulation dot1q** : Perintah trunk melakukan trunk di switch MLS

B. Konfigurasi di Switch MLS kanan

1. Mengganti hostname MLS

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-KIRI
```

2. Membuat VLAN 10 dan 20

```
SW-KANAN(config)#vlan 10
SW-KANAN(config)#name SMP
```

```
SW-KANAN(config)#vlan 20
SW-KANAN(config)#name SMK
```

3. Memasukan interface ke VLAN

```
SW-KANAN(config)#interface fa0/1
SW-KANAN(config)#switchport mode access
SW-KANAN(config)#switchport access vlan 10
```

```
SW-KANAN(config)#interface fa0/2
SW-KANAN(config)#switchport mode access
SW-KANAN(config)#switchport access vlan 20
```

4. Melakukan Trunk dot1q

```
SW-KANAN(config #interface fa0/3
SW-KANAN(config #switchport trunk encapsulation dot1q
SW-KANAN(config #switchport mode trunk
```

Setelah melakukan konfigurasi trunk yaitu melakukan pengecekan apakah trunk sudah berhasil diterapkan.

C. Pengecekan

1. Pengecekan trunk switch MLS kiri

```
SW-KIRI(config)#do show interface trunk
```

```

SW-KIRI(config)#do show interface trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/3    on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/3    1-1005

Port      Vlans allowed and active in management domain
Fa0/3    1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/3    1,10,20

```

2. Pengecekan trunk switch MLS kanan

```

SW-KANAN(config)#do show interface trunk
SW-KANAN(config)#do show interface trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/3    on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/3    1-1005

Port      Vlans allowed and active in management domain
Fa0/3    1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/3    1,10,20

```

Terlihat bahwa trunk sudah berhasil di jalankan oleh switch MLS. Setelah itu kita akan lanjut memasang IP Address untuk laptop.

D. Konfigurasi IP Address

1. Laptop A

**IP Configuration**

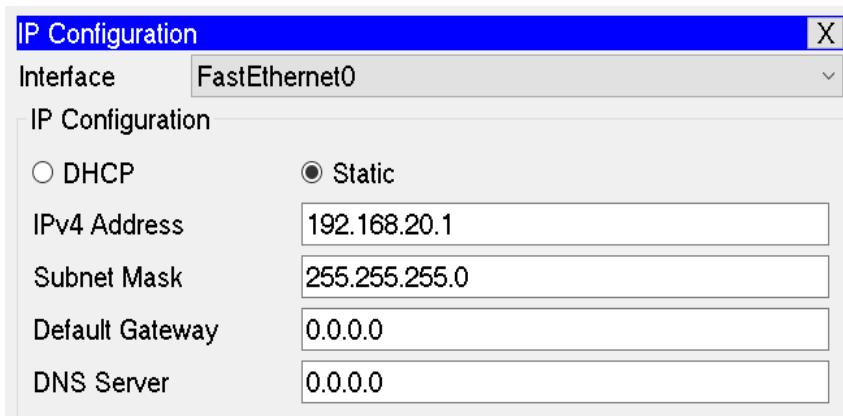
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

2. Laptop B

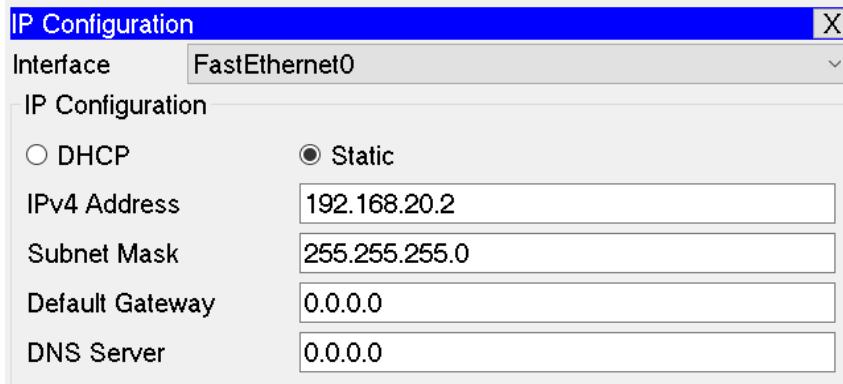
**IP Configuration**

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

3. Laptop C



#### 4. Laptop D



Setelah itu kita akan coba melakukan test PING.

#### E. Test PING

##### 1. Sesama VLAN 10

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>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<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms 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
```

##### 2. Antar VLAN

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

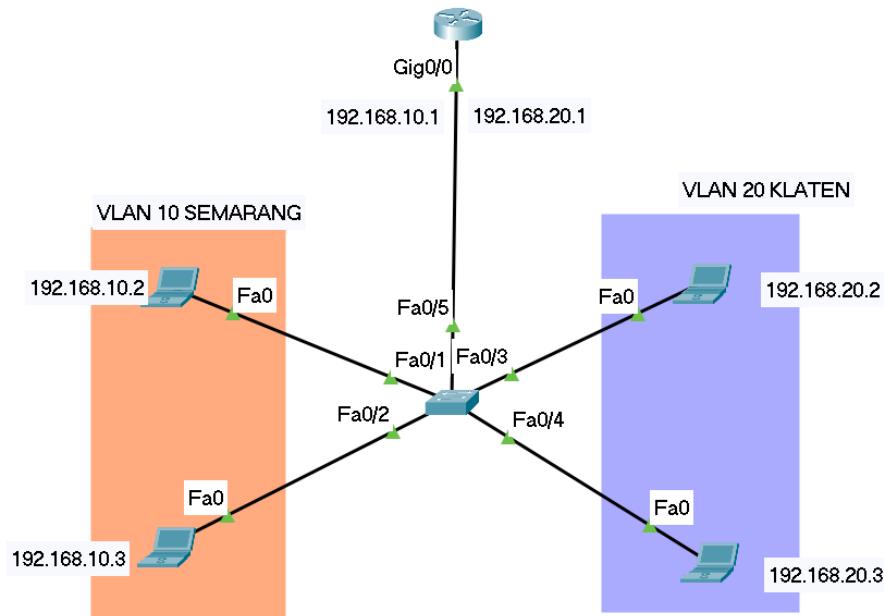
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

#### F. Lab MLS Trunk telah selesai.

## Lab 5. Intervlan Routing

Seperti yang kita ketahui, jika memecah satu network menjadi beberapa vlan menggunakan switch. Maka antar VLAN yang berbeda tidak akan bisa saling berkomunikasi. Namun, kita bisa membuat agar antar VLAN tersebut, dapat berkomunikasi satu sama lain, dengan bantuan perangkat layer 3 yang berfungsi sebagai gateway. Hal seperti ini biasa disebut dengan nama Intervlan Routing.



Apabila kita menghubungkan switch ke router dimana ada beberapa VLAN yang perlu dilewatkan diantaranya, maka pada switch disetting trunk. Namun bila pada switch hanya terdapat 1 VLAN saja maka cukup disetting access. Kali ini karena kita ingin melewatkkan beberapa VLAN yakni VLAN 10 dan 20, maka di sisi switch disetting trunk.

Langkah Langkah :

A. Konfigurasi pada Router

1. Mengganti nama Router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-IDN
```

2. Mengaktifkan interface Gig0/0

```
R-IDN(config)#interface gig0/0  
R-IDN(config-if)#no shutdown
```

**Interface gig0/0** : Adalah interface yang akan kita nyalakan/aktifkan.

**No shutdown** : Perintah untuk mengaktifkan sebuah interface.

3. Membuat Sub interface

```
R-IDN(config)#interface gig0/0.10  
R-IDN(config-subif)#encapsulation dot1q 10  
R-IDN(config-subif)#ip add 192.168.10.1 255.255.255.0
```

```
R-IDN(config-subif)#interface gig0/0.20
R-IDN(config-subif)#encapsulation dot1q 20
R-IDN(config-subif)#ip add 192.168.20.1 255.255.255.0
```

Pada router kita membuat sub interface sejumlah VLAN yang dilewatkan, dalam hal ini karena hanya ada 2 VLAN, maka kita akan membuat 2 subinterface pada router, yakni dengan menambahkan simbol titik pada interface utamanya diikuti dengan nomor VLAN nya.

gig0/0 = main interface □ gig0/0.10 dan gig0/0.20 = subinterface.

**Sub-Interface:** -Kalau misalnya kita ingin menghubungkan VLAN ke VLAN lain, pasti dibutuhkan gateway. Namun interface yang terkoneksi ke switch hanya satu, jika satu interface untuk satu VLAN, pasti akan repot. Oleh karena itu digunakan yang namanya sub-interface. Dengan adanya sub interface, maka kita membuat interface palsu pada router untuk membuat gateway dari VLAN. Dengan begitu antar vlan pada switch dapat saling terkoneksi.

B. Konfigurasi pada Switch

1. Mengganti hostname Switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-BAWAH
```

2. Membuat VLAN 10 dan 20

```
SW-BAWAH(config)#vlan 10
SW-BAWAH(config-vlan)#name SEMARANG
```

```
SW-BAWAH(config-vlan)#VLAN 20
SW-BAWAH(config-vlan)#name KLATEN
```

3. Memasukan interface ke VLAN

```
SW-BAWAH(config)#interface fa0/1
SW-BAWAH(config)#switchport mode access
SW-BAWAH(config)#switchport access vlan 10
```

```
SW-BAWAH(config)#interface fa0/2
SW-BAWAH(config)#switchport mode access
SW-BAWAH(config)#switchport access vlan 10
```

```
SW-BAWAH(config)#interface fa0/3
SW-BAWAH(config)#switchport mode access
SW-BAWAH(config)#switchport access vlan 20
```

```
SW-BAWAH(config)#interface fa0/4
SW-BAWAH(config)#switchport mode access
SW-BAWAH(config)#switchport access vlan 20
```

4. Mengaktifkan interface Trunk yang mengarah ke Router

```
SW-BAWAH(config)#interface fa0/5
SW-BAWAH(config)#switchport mode trunk
```

C. Konfigurasi IP Address laptop

1. Laptop VLAN 10

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.10.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 0.0.0.0

2. Laptop VLAN 10

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.10.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 0.0.0.0

3. Laptop VLAN 20

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.20.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.20.1

DNS Server 0.0.0.0

4. Laptop VLAN 20

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.20.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.20.1

DNS Server 0.0.0.0

Pada lab kali ini laptop membutuhkan gateway untuk berkomunikasi ke VLAN lain. Untuk IP Gateway sendiri adalah IP yang di pasang pada konfigurasi sub interface tadi, selanjutnya kita akan melakukan pengecekan.

D. Pengecekan

1. Pengecekan IP Address yang di pasang di router

```
R-IDN(config)#do show ip interface brief
R-IDN(config)#do show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0  unassigned     YES NVRAM   up
GigabitEthernet0/0.10 192.168.10.1 YES manual  up
GigabitEthernet0/0.20 192.168.20.1 YES manual  up
GigabitEthernet0/1    unassigned     YES NVRAM   administratively down down
Vlan1               unassigned     YES unset   administratively down down
```

2. Pengecekan trunk di switch bawah

```
R-IDN(config)#do show ip interface brief
SW-BAWAH(config)#do show int trunk
Port      Mode       Encapsulation  Status        Native vlan
Fa0/5    on         802.1q        trunking      1

Port      Vlans allowed on trunk
Fa0/5    1-1005

Port      Vlans allowed and active in management domain
Fa0/5    1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/5    1,10,20
```

Setelah semua sudah di konfigurasi IP Address pun sudah di pasang langkah terakhir adalah melakukan PING.

E. Test PING

1. Sesama VLAN 10

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=2ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

3. Antar VLAN

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time=1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

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
```

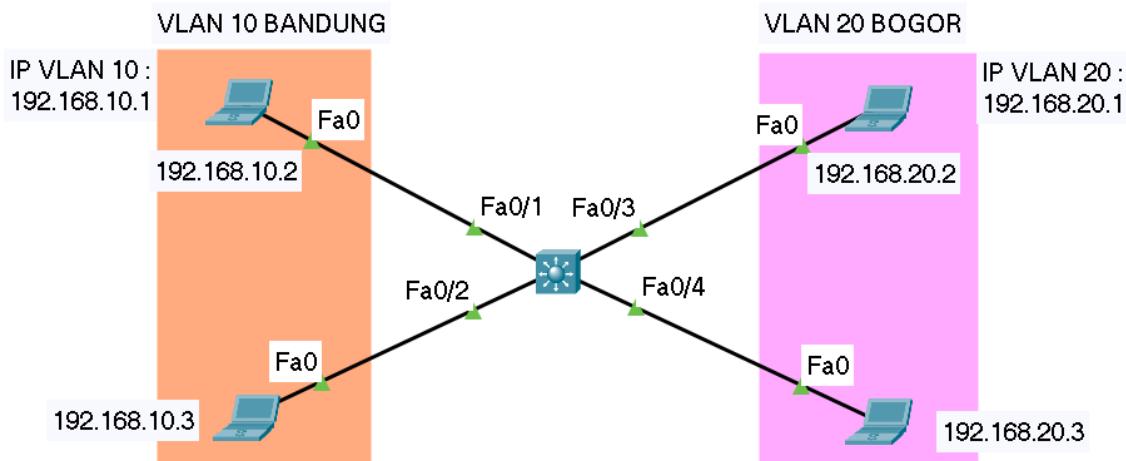
Kenapa PING antar VLAN success??? karena kita sudah menerapkan intervlan routing yang dimana fungsinya sendiri dapat memungkinkan kita berkomunikasi antar VLAN dengan bantuan router.

F. Lab Intervlan Routing telah selesai.

## Lab 6. SVI (Switch Interface Virtual)

SVI (Switch Interface Virtual) adalah protocol kembaran dari intervlan routing, fungsinya sama seperti pada bab sebelumnya yaitu memungkinkan kita dapat terhubung ke VLAN yang berbeda. Hal yang membedakannya lagi adalah jika intervlan menggunakan router nah sedangkan SVI menggunakan switch MLS.

Switch MLS sendiri dapat menambahkan IP Address, agar antar VLAN bisa saling terhubung maka di switch MLS perlu IP Address yang mana akan di gunakan client/laptop sebagai gateway.



Kita akan mengkonfigurasi SVI pada topologi di atas, untuk langkah langkah nya sebagai berikut :

Langkah Langkah :

A. Konfigurasi di switch MLS

1. Mengganti hostname MLS

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname MLS-CORE
```

2. Membuat VLAN 10 dan 20

```
MLS-CORE(config)#vlan 10  
MLS-CORE(config-vlan)#name BANDUNG
```

```
MLS-CORE(config-vlan)#vlan 20  
MLS-CORE(config-vlan)#name BOGOR
```

3. Memasukan interface ke VLAN

```
MLS-CORE(config)#interface fa0/1  
MLS-CORE(config)#switchport mode access  
MLS-CORE(config)#switchport access vlan 10
```

```
MLS-CORE(config)#interface fa0/2  
MLS-CORE(config)#switchport mode access  
MLS-CORE(config)#switchport access vlan 10
```

```
MLS-CORE(config)#interface fa0/3
MLS-CORE(config)#switchport mode access
MLS-CORE(config)#switchport access vlan 20
```

```
MLS-CORE(config)#interface fa0/4
MLS-CORE(config)#switchport mode access
MLS-CORE(config)#switchport access vlan 20
```

4. Membuat interface VLAN (SVI)

```
MLS-CORE(config)#interface vlan 10
MLS-CORE(config)#ip address 192.168.10.1 255.255.255.0
```

```
MLS-CORE(config)#interface vlan 20
MLS-CORE(config)#ip address 192.168.20.1 255.255.255.0
```

**Interface vlan 10** : Perintah untuk membuat interface virtual/sub interface vlan 10.

5. Mengaktifkan fungsi router

```
MLS-CORE(config)#ip routing
```

**Ip routing** : Perintah untuk melakukan routing, harus ada 2 network yang ingin saling terhubung.

Setelah mengkonfigurasi SVI jangan lupa untuk memasang IP Address dan gateway laptop pada setiap VLAN.

B. Konfigurasi pada Laptop agar dipasang Gateway pada setiap VLAN

1. Laptop VLAN 10

IP Configuration

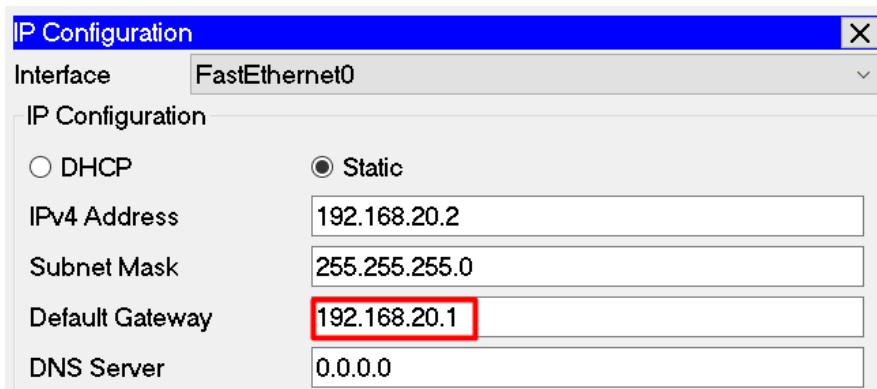
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

2. Laptop VLAN 10

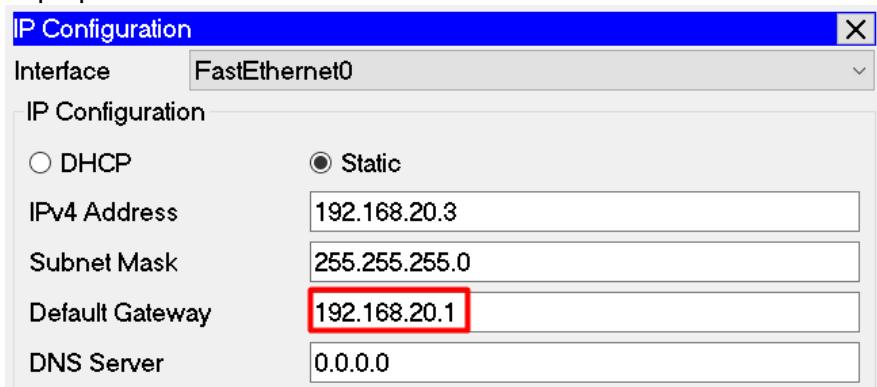
IP Configuration

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

3. Laptop VLAN 20



#### 4. Laptop VLAN 20



Pada lab kali ini laptop membutuhkan gateway untuk berkomunikasi ke VLAN lain. Untuk IP Gateway sendiri adalah IP yang di pasang pada konfigurasi sub interface tadi, selanjutnya kita akan melakukan pengecekan.

### C. Pengecekan

#### 1. Pengecekan VLAN

MLS-CORE(config)#do show vlan			
MLS-CORE(config) #do show vlan			
VLAN	Name	Status	Ports
1	default	active	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		Gig0/1, Gig0/2
10	SMP	active	Fa0/1, Fa0/2
20	SMK	active	Fa0/3, Fa0/4
1002	fdmi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

#### 2. Pengecekan VLAN

MLS-CORE(config)#do show vlan					
Vlan1	unassigned	YES	unset	administratively	down down
Vlan10	192.168.10.1	YES	manual	up	up
Vlan20	192.168.20.1	YES	manual	up	up

#### D. Test PING

##### 1. Sesama VLAN 10

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=2ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

##### 2. Antar VLAN

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time=1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

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
```

Dengan konfigurasi SVI maka PING antar laptop yang berbeda VLAN pun, bisa saling terhubung.

#### E. Lab SVI telah selesai.

## Lab 7. VTP (Vlan Trunking Protocol)

VTP ( Vlan Trunking Protocol) adalah salah satu protocol yang dapat memudahkan kita dalam me-management data VLAN. Jika kita menerapkan VTP maka kita akan lebih mudah me-manage switch, misalkan kita hanya membuat satu VLAN di satu switch dan switch lainnya akan mengikuti secara otomatis.

Ada 3 mode jenis VTP :

1. **VTP Server** : Jenis VTP ini adalah jenis VTP yang bisa membuat VLAN, mengurangi VLAN, menambahkan VLAN.
2. **VTP Client** : Jenis VTP ini Cuma bisa mensinkronisasikan VLAN dan memforwading VLAN, **Sinkronisasi** berarti menerima dan menyamakan VLAN dari server, sedangkan **forwading** berarti meneruskan VLAN yang telah dibuat.
3. **VTP Transparent** : Jenis VTP ini bisa membuat VLAN tetapi untuk dirinya sendiri jadi jenis VTP ini tidak menerima data VLAN dari VTP server (only local). Dan VTP ini bisa memforwading VLAN.

VTP Modes			
	VTP Server	VTP Client	VTP Transparent
Description	Manage Domain and VLAN configurations	Updates VTP configurations VTP client switches cannot change VLAN configurations.	Able to manage local VLAN configurations. Local VLAN configurations not shared with VTP network
Respond to VTP advertisements?	Participates fully	Participates fully	Only Forwards VTP advertisements
Global VLAN configuration preserved on restart?	Yes, global configurations stored in NVRAM	No, global configurations stored in RAM, not in NVRAM	No, local VLAN configuration only is stored in NVRAM
Update other VTP enabled switches?	Yes	Yes	No



Untuk melakukan konfigurasi VTP, kita harus pastikan bahwa switch saling terhubung ke switch yang lainnya yaitu dengan melakukan trunk di setiap switch.

Langkah Langkah :

A. Konfigurasi di switch 1

1. Mengganti hostname switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-1
```

2. Melakukan Trunk di interface yang mengarah ke switch

```
SW-1(config)#Interface fa0/1
SW-1(config)#switchport mode trunk
```

3. Membuat VTP

```
SW-1(config)#vtp mode server
```

```
SW-1(config)#vtp domain IDN  
SW-1(config)#vtp password 123
```

Hal yang harus di perhatikan dalam melakukan konfigurasi VTP adalah mode VTP, domain, dan password, Domain dan password wajib sama agar VTP bisa berjalan.

**VTP mode server** : Perintah membuat/merubah switch ke mode server

**VTP domain IDN** : Perintah untuk menambahkan domain di VTP, IDN hanya sebagai nama domain saja (Nama bebas).

**VTP password 123** : Perintah untuk menambahkan password .

4. Membuat VLAN 10,20 dan 30

```
SW-1(config)#vlan 10  
SW-1(config)#name TKJ
```

```
SW-1(config)#vlan 20  
SW-1(config)#name RPL
```

```
SW-1(config)#vlan 30  
SW-1(config)#name MM
```

B. Konfigurasi di switch 2

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-2
```

2. Melakukan Trunk di interface yang mengarah ke switch

```
SW-2(config)#Interface range fa0/1-2  
SW-2(config)#switchport mode trunk
```

**Interface Range** : Perintah untuk mengakses beberapa interface dengan secara bersamaan.

3. Membuat VTP

```
SW-2(config)#vtp mode client  
SW-2(config)#vtp domain IDN  
SW-2(config)#vtp password 123
```

**VTP mode client** : Perintah membuat/merubah switch ke mode client

Untuk domain dan password di samakan dengan VTP mode server.

C. Konfigurasi di switch 3

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-3
```

2. Melakukan Trunk di interface yang mengarah ke switch

```
SW-3(config)#Interface range fa0/1  
SW-3(config)#switchport mode trunk
```

3. Membuat VTP

```
SW-3(config)#vtp mode transparent  
SW-3(config)#vtp domain IDN  
SW-3(config)#vtp password 123
```

VTP mode transparent : Perintah membuat/merubah switch ke mode transparent

4. Membuat VLAN 100 dan 200

```
SW-3(config)#vlan 100  
SW-3(config)#name AAA
```

```
SW-3(config)#vlan 200  
SW-3(config)#name BBB
```

Kenapa VTP transparent membuat VLAN lagi???jawabannya karena VTP jenis ini seperti penjelasan di atas bahwa VTP mode transparent tidak bisa melakukan sinkronisasi/menyamakan data VLAN dari VTP server, maka dari itu disini kita membuat VLAN lagi. Untuk membuktikan bahwa VTP di setiap switch berhasil di konfigurasi kita akan melakukan pengecekan di setiap switch tersebut.

D. Pengecekan

1. Pengecekan VTP status switch 1

```
SW-1(config)#do show vtp status  
SW-1(config)#do show vtp status  
VTP Version capable : 1 to 2  
VTP version running : 2  
VTP Domain Name : IDN  
VTP Pruning Mode : Disabled  
VTP Traps Generation : Disabled  
Device ID : 00D0.BC02.8600  
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:09  
Local updater ID is 0.0.0.0 (no valid interface found)  
  
Feature VLAN :  
-----  
VTP Operating Mode : Server  
Maximum VLANs supported locally : 255  
Number of existing VLANs : 8  
Configuration Revision : 6  
MD5 digest : 0xCF 0x09 0xF9 0xD4 0x6B 0x89 0xB1 0x96  
0x64 0xFF 0xED 0x84 0xC6 0xD3 0x88 0xAE
```

2. Pengecekan VTP status switch 2

```
SW-2(config)#do show vtp status
```

```

SW-2(config)#do show vtp status
VTP Version capable : 1 to 2
VTP version running : 2
VTP Domain Name : IDN
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0001.C9CD.3500
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:09

Feature VLAN :
-----
VTP Operating Mode : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
Configuration Revision : 6
MD5 digest : 0xCF 0x09 0xF9 0xD4 0x6B 0x89 0xB1 0x96
              0x64 0xFF 0xED 0x84 0xC6 0xD3 0x88 0xAE

```

### 3. Pengecekan VTP status switch 3

```

SW-3(config)#do show vtp status
SW-3(config)#do show vtp status
VTP Version capable : 1 to 2
VTP version running : 2
VTP Domain Name : IDN
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 000C.85CC.3200
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN :
-----
VTP Operating Mode : Transparent
Maximum VLANs supported locally : 255
Number of existing VLANs : 7
Configuration Revision : 0
MD5 digest : 0x74 0x00 0xC6 0xAF 0x89 0x05 0xE0 0xC2
              0x4B 0xBD 0x0B 0xA6 0xA9 0xD6 0x9B 0x6B

```

Kemudian kita akan mengecek data VLAN di setiap masing masing switch.

### 1. Chek data VLAN di switch server

```

SW-1(config)#do show vlan
SW-1(config)#do show vlan

VLAN Name          Status    Ports
---- -----
1     default       active   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,
Gig0/1
                      Gig0/2
10    TKJ           active
20    RPL           active
30    MM            active
1002  raai-default active
1003  token-ring-default active
1004  fddinet-default active
1005  trnet-default active

```

Untuk pengecekan pertama kita mengecek data VLAN dari switch server, terlihat bahwa kita tadi telah mengkonfigurasi VLAN 10, 20, dan 30. Setelah itu kita akan melakukan pengecekan switch client apakah akan melakukan sinkronisasi atau tidak.

## 2. Chek data VLAN di switch client

```
SW-1(config)#do show vlan
SW-2 (config)#do show vlan

VLAN Name          Status    Ports
--- --- 
1      default      active   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, Gig0/1,
                           Gig0/2
10     TKJ          active
20     RPL          active
30     MM           active
1002  rada-default active
1003  token-ring-default active
1004  fddinet-default active
1005  trnet-default active
```

Terlihat bahwa kita tadi tidak melakukan konfigurasi VLAN pada switch 2/client, tapi switch 2 menerima data VLAN dari switch server, karena kita sudah berhasil menerapkan VTP mode client di switch ini. Jadi switch otomatis akan melakukan sinkronisasi.

## 3. Chek data VLAN di switch transparent

```
SW-1(config)#do show vlan
SW-3 (config)#do show vlan

VLAN Name          Status    Ports
--- --- 
1      default      active   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,
                           Gig0/1
                           Gig0/2
100   AAA           active
200   BBB           active
1002  rada-default active
1003  token-ring-default active
1004  fddinet-default active
1005  trnet-default active
```

Switch transparent tidak melakukan sinkronisasi data VLAN dari server, karena switch ini membuat VLAN (Only local)/untuk dirinya sendiri.

E. Lab VTP telah selesai.

# DHCP Introduction

DHCP merupakan singkatan dari (Dynamic Host Configuration Protocol). adalah protocol yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan.

Fungsinya adalah untuk mempermudah pendapatan IP Address pada suatu jaringan. Misalnya jika pada suatu jaringan tidak dipasang DHCP Server, maka pengalamatan pada klien harus dikonfigurasi secara manual, sedangkan jika kita pasang DHCP Server pada suatu jaringan, maka klien akan mendapatkan IP Address secara otomatis dari DHCP Server tanpa harus mengonfigurasi secara manual.

Pada DHCP terdapat 3 peran, yaitu:

## 1. DHCP Server

DHCP Server berfungsi untuk membuat daftar IP Address (IP Pool) dan kemudian memberikannya kepada klien.

## 2. DHCP Client

DCHP Client berfungsi untuk menerima IP Address yang diberikan oleh DHCP Server.

## 3. DHCP Relay

DHCP Relay berfungsi untuk meneruskan DHCP dari satu router ke router lain, sehingga dalam beberapa jaringan, kita dapat menggunakan satu DHCP server.

### ➤ Proses DHCP

Beginilah proses yang terjadi pada DHCP antara Server dan Client yang kita kenal dengan istilah DORA.

#### Discover

Client/laptop melakukan broadcast ke networknya sendiri, mencari DHCP server menggunakan IP 0.0.0.0 ke 255.255.255.255.

#### Offer

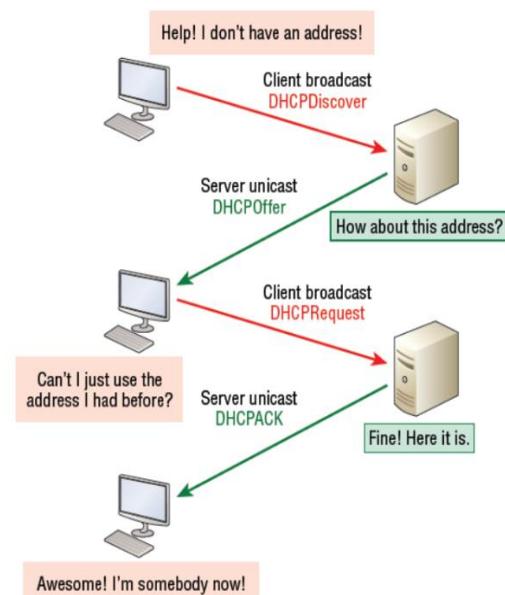
Membalas pesan tadi dengan mengirim *DHCP offer message*, pesan offer ini yang berisikan konfigurasi jaringan yang tersedia untuk si client.

#### Request

Negosiasi peminjaman IP dari server ke client

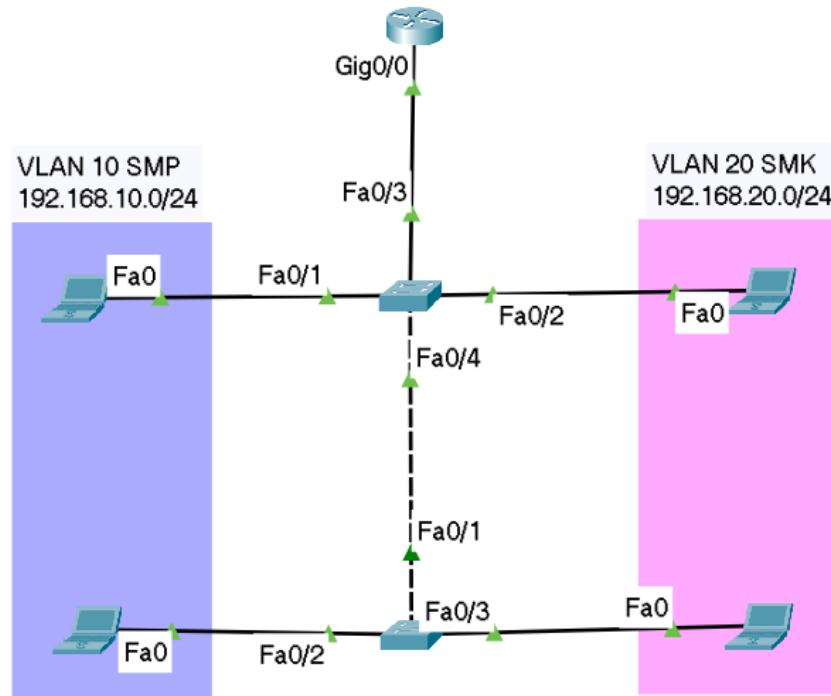
#### Acknowledge

Client sudah diberikan IP dan menjadi bagian dari Jaringan DHCP Server.



## Lab 8. DHCP VLAN

Setelah tau apa itu DHCP selanjutnya kita akan mempraktekan nya pada topologi dibawah ini. Karena DHCP memerlukan fungsi dari OSI layer-3 yaitu network, maka kita memerlukan router pada topology.



Langkah Langkah :

A. Konfigurasi di Router

1. Mengganti nama Router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-IDN
```

2. Mengaktifkan interface Gig0/0

```
R-IDN(config)#interface gig0/0  
R-IDN(config-if)#no shutdown
```

3. Membuat Sub interface

```
R-IDN(config)#interface gig0/0.10  
R-IDN(config-subif)#encapsulation dot1q 10  
R-IDN(config-subif)#ip add 192.168.10.1 255.255.255.0  
  
R-IDN(config-subif)#interface gig0/0.20  
R-IDN(config-subif)#encapsulation dot1q 20  
R-IDN(config-subif)#ip add 192.168.20.1 255.255.255.0
```

4. Membuat DHCP pada Sub interface

```
R-IDN(config)#ip dhcp pool SMP  
R-IDN(config)#network 192.168.10.0 255.255.255.0
```

```
R-IDN(config)#default-router 192.168.10.1
R-IDN(config)#dns-server 8.8.8.8

R-IDN(config)#ip dhcp pool SMK
R-IDN(config)#network 192.168.20.0 255.255.255.0
R-IDN(config)#default-router 192.168.20.1
R-IDN(config)#dns-server 8.8.8.8
```

- **Ip dhcp** command dari DHCP
- **pool** (nama pool) contoh pool SMP
- **network 192.168.10.0** network yang diberikan ke klien
- **dns-server 8.8.8.8** DNS server yang akan diberikan oleh server
- **default-router 192.168.10.1** gateway yang akan diberikan server

#### B. Konfigurasi pada Switch atas

##### 1. Mengganti nama Switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-ATAS
```

##### 2. Membuat VLAN

```
SW-ATAS(config)#vlan 10
SW-ATAS(config)#name SMP
```

```
SW-ATAS(config)#vlan 20
SW-ATAS(config)#name SMK
```

##### 3. Memasukan interface kedalam VLAN

```
SW-ATAS(config)#interface fa0/1
SW-ATAS(config)#switchport mode access
SW-ATAS(config)#switchport access vlan 10
```

```
SW-ATAS(config)#interface fa0/2
SW-ATAS(config)#switchport mode access
SW-ATAS(config)#switchport access vlan 20
```

##### 4. Melakukan Trunk

```
SW-ATAS(config)#interface fa0/3
SW-ATAS(config)#switchport mode trunk
```

```
SW-ATAS(config)#interface fa0/4
SW-ATAS(config)#switchport mode trunk
```

#### C. Konfigurasi pada Switch atas

##### 1. Mengganti nama Switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-BAWAH
```

##### 2. Membuat VLAN

```
SW-BAWAH(config)#vlan 10
SW-BAWAH(config)#name SMP
```

```
SW-BAWAH(config)#vlan 20
SW-BAWAH(config)#name SMK
```

##### 3. Memasukan interface ke VLAN

```
SW-BAWAH (config)#interface fa0/2
```

```
SW-BAWAH(config)#switchport mode access  
SW-BAWAH(config)#switchport access vlan 10
```

```
SW-BAWAH(config)#interface fa0/3  
SW-BAWAH(config)#switchport mode access  
SW-BAWAH(config)#switchport access vlan 20
```

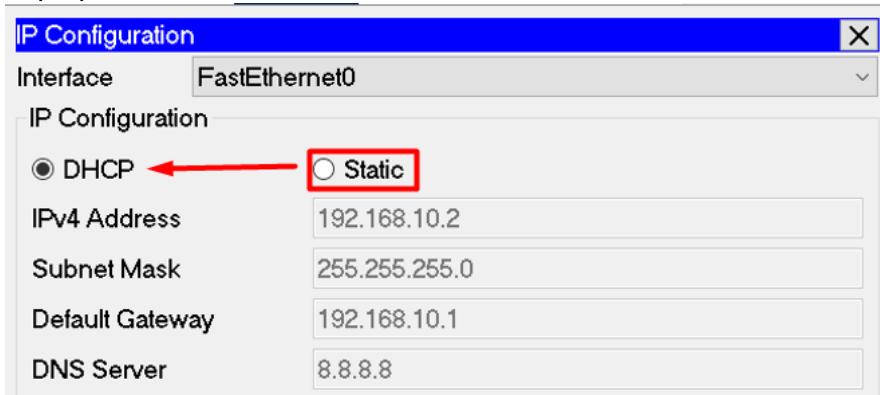
4. Melakukan Trunk

```
SW-BAWAH(config)#interface fa0/1  
SW-BAWAH(config)#switchport mode trunk
```

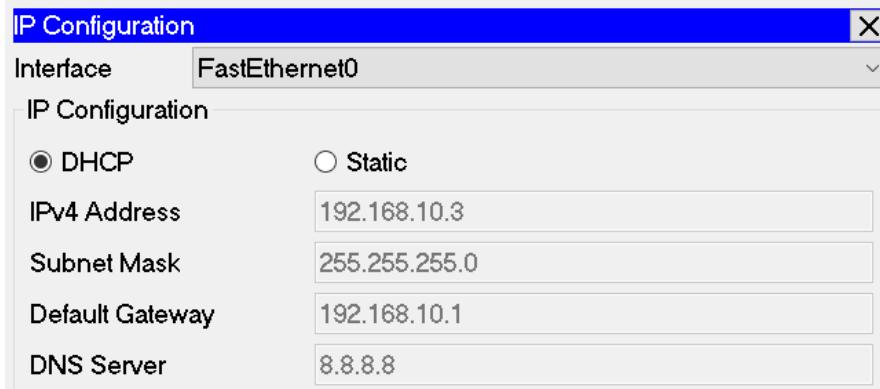
Selanjutnya rubah settingan IP pada laptop menjadi dynamic, untuk mengetahui apakah DHCP sudah berhasi

D. Konfigurasi Laptop yang sudah diberikan DHCP

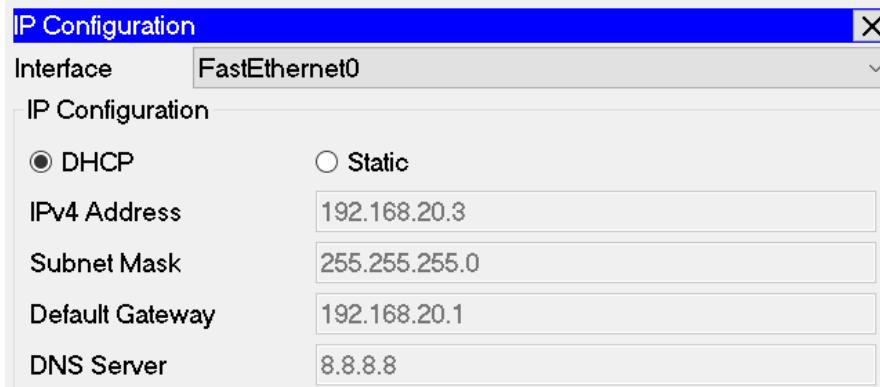
1. Laptop VLAN 10



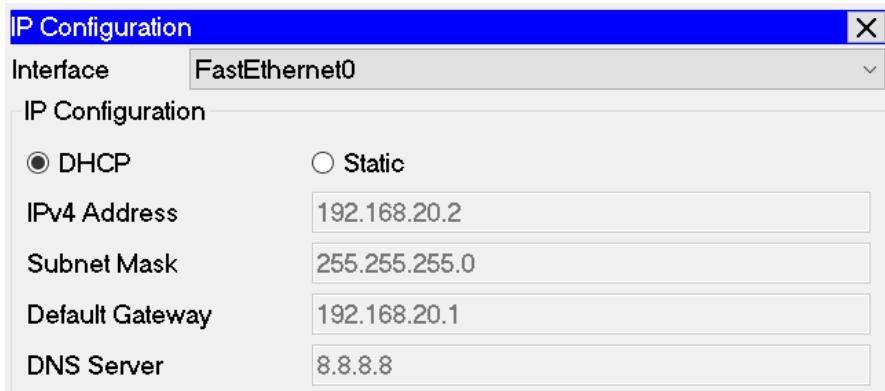
2. Laptop VLAN 10



3. Laptop VLAN 20



4. Laptop VLAN 20



Setelah semua laptop mendapatkan IP addressnya, pada Router ketikkan perintah berikut untuk mengetahui laptop siapa dan mendapatkan IP berapa.

Pengecekan IP yang sudah diberikan DHCP oleh router

```
R-IDN(config)#do show ip dhcp binding
R-IDN(config)#do show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.10.2 00D0.BA2C.D97E --
192.168.10.3 0006.2AE0.AAA4 --
192.168.20.2 0001.63C3.553E --
192.168.20.3 00E0.F96D.050B --
```

#### E. Test PING

##### 1. Sesama VLAN 10

```
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

##### 2. Antar VLAN

```
C:\>ping 192.168.20.2

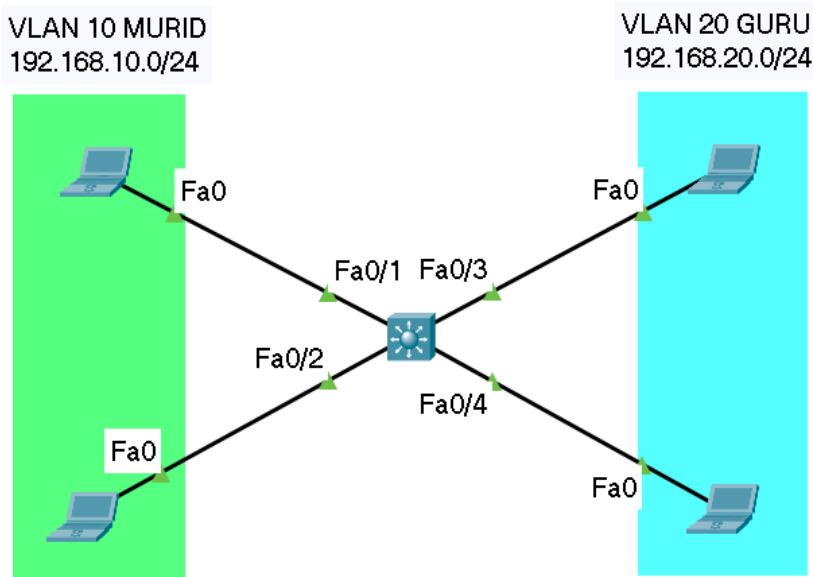
Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time=lms TTL=127
Reply from 192.168.20.2: bytes=32 time<lms TTL=127
Reply from 192.168.20.2: bytes=32 time<lms TTL=127
Reply from 192.168.20.2: bytes=32 time<lms TTL=127

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
```

#### F. Lab DHCP VLAN telah selesai

## Lab 9. DHCP MLS

Lab kali ini sama seperti lab sebelumnya bedanya sekarang kita menggunakan MLS sebagai layer-3 nya karena MLS sendiri adalah switch yang mempunyai layer-3 yaitu network.



Kita harus membuat interface virtual (SVI) pada lab kali ini agar antar VLAN bisa saling terhubung. Untuk langkah-langkahnya sebagai berikut :

Langkah Langkah :

A. Konfigurasi di MLS

1. Mengganti hostname MLS

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname MLS-IDN
```

2. Membuat VLAN

```
MLS-IDN(config)#vlan 10  
MLS-IDN(config)#name SMP
```

```
MLS-IDN(config)#vlan 20  
MLS-IDN(config)#name SMK
```

3. Memasukan interface kedalam VLAN

```
MLS-IDN(config)#interface range fa0/1-2  
MLS-IDN(config)#switchport mode access  
MLS-IDN(config)#switchport access vlan 10
```

```
MLS-IDN(config)#interface range fa0/3-4  
MLS-IDN(config)#switchport mode access  
MLS-IDN(config)#switchport access vlan 20
```

3. Membuat interface VLAN (SVI)

```
MLS-IDN(config)#interface vlan 10  
MLS-IDN(config)#ip add 192.168.10.1 255.255.255.0
```

```
MLS-IDN(config)#interface vlan 20  
MLS-IDN(config)#ip add 192.168.20.1 255.255.255.0
```

Dengan adanya SVI yang kita telah buat tadi maka kita bisa lanjut untuk mengkonfigurasi DHCP Server di switch MLS.

##### 5. Membuat DHCP Server

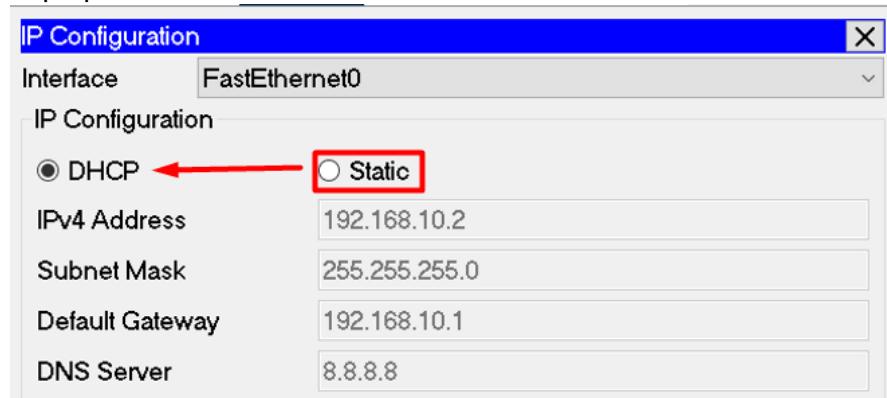
```
R-IDN(config)#ip dhcp pool MURID
R-IDN(config)#network 192.168.10.0 255.255.255.0
R-IDN(config)#default-router 192.168.10.1
R-IDN(config)#dns-server 8.8.8.8

R-IDN(config)#ip dhcp pool GURU
R-IDN(config)#network 192.168.20.0 255.255.255.0
R-IDN(config)#default-router 192.168.20.1
R-IDN(config)#dns-server 8.8.8.8
```

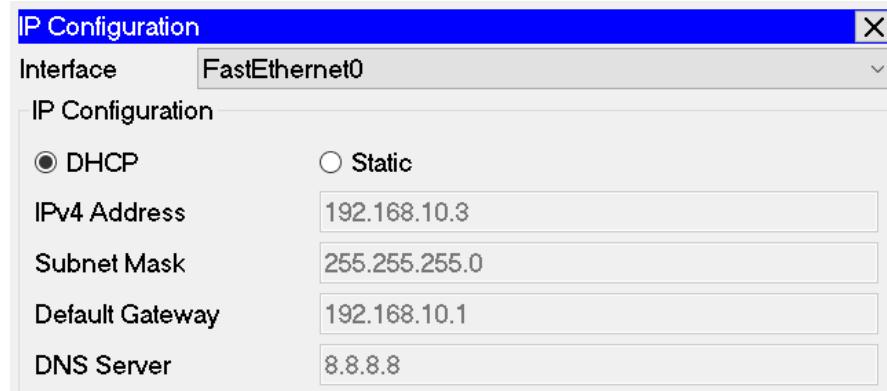
Selanjutnya rubah settingan IP pada laptop menjadi dynamic, untuk mengetahui apakah DHCP sudah berhasi

##### B. Konfigurasi Laptop yang sudah diberikan DHCP

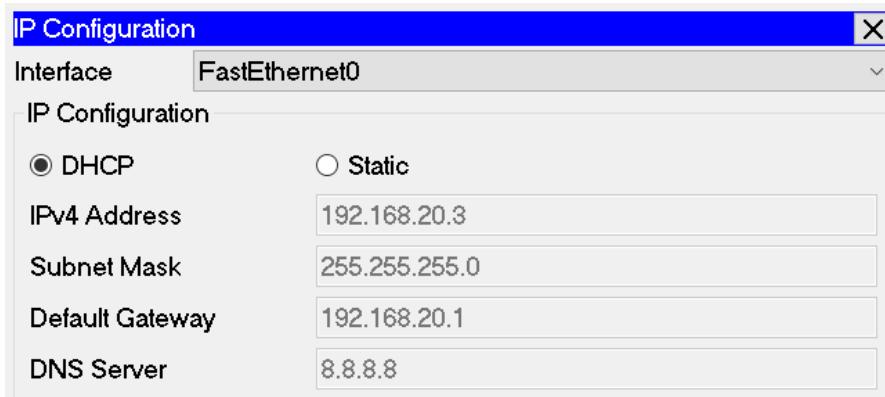
###### 1. Laptop VLAN 10



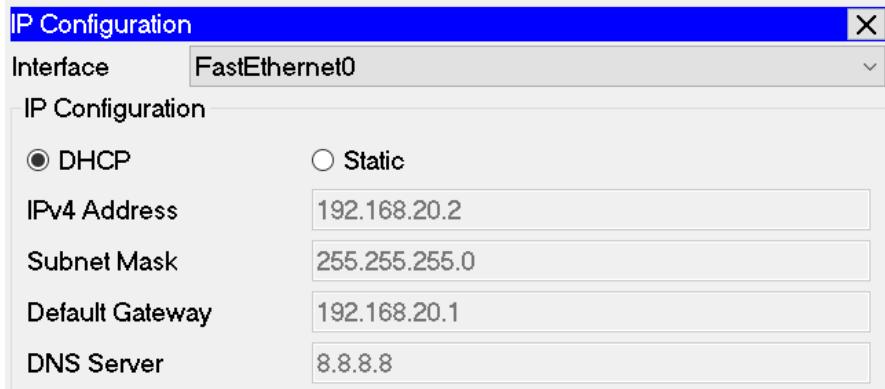
###### 2. Laptop VLAN 10



###### 3. Laptop VLAN 20



4. Laptop VLAN 20



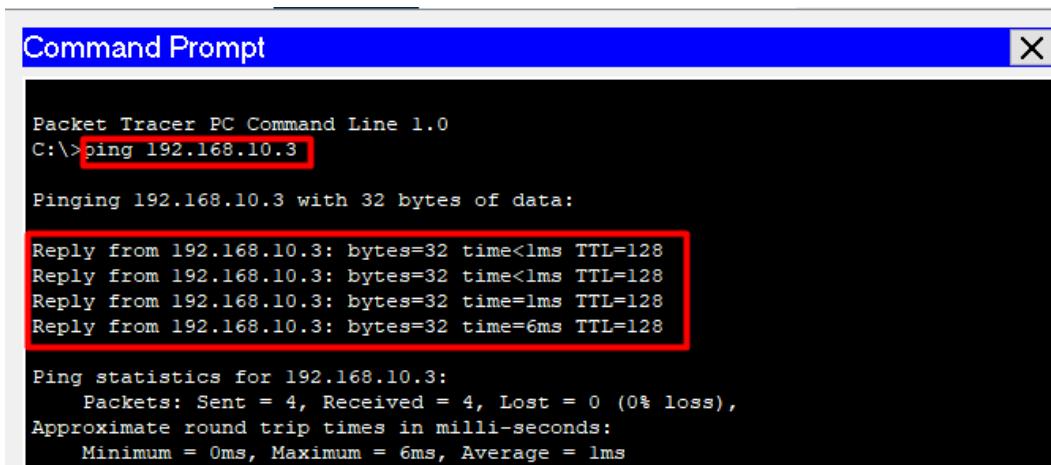
Setelah semua laptop mendapatkan IP addressnya, pada Router ketikkan perintah berikut untuk mengetahui laptop siapa dan mendapatkan IP berapa

Pengecekan IP yang sudah diberikan DHCP oleh MLS

MLS-IDN(config)#do show ip dhcp binding				
IP address	Client-ID/ Hardware address	Lease expiration	Type	
192.168.10.2	0001.43D5.06BC	--	Automatic	
192.168.10.3	0001.96B3.30A8	--	Automatic	
192.168.20.2	00D0.5830.746A	--	Automatic	
192.168.20.3	000A.4145.A20D	--	Automatic	

C. Test PING

1. Sesama VLAN 10



2. Antar VLAN

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

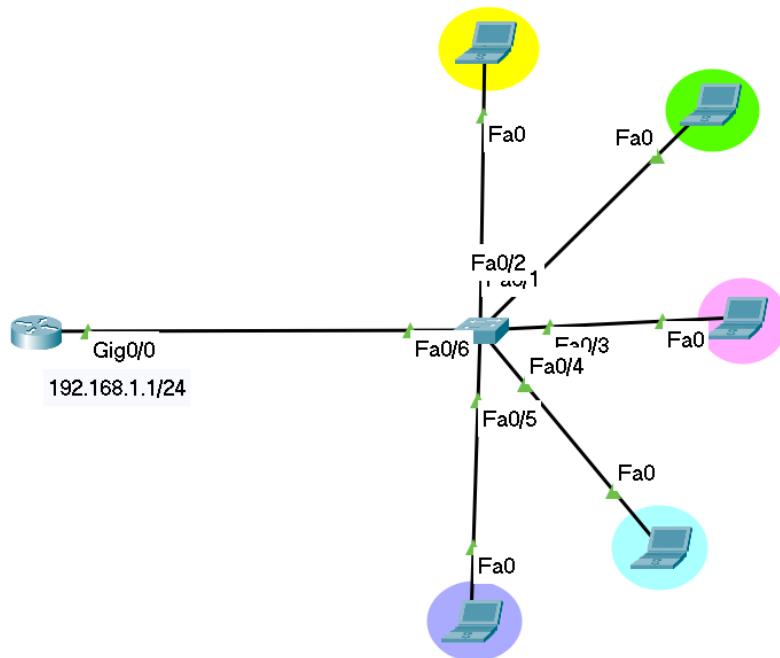
Reply from 192.168.20.2: bytes=32 time=lms TTL=127
Reply from 192.168.20.2: bytes=32 time<lms TTL=127
Reply from 192.168.20.2: bytes=32 time<lms TTL=127
Reply from 192.168.20.2: bytes=32 time<lms TTL=127

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 = lms, Average = 0ms
```

D. Lab DHCP MLS telah selesai.

## Lab 10. DHCP Excluded

Excluded Address adalah salah satu perintah agar pemberian DHCP bisa di manajemen, lebih tepatnya IP Address yang kita setting sebagai IP Excluded Address tidak akan diberikan kepada client. Misalnya kita excluded IP 192.168.1.2 192.168.1.100, nah berarti pemberian DHCP/IP yang bisa kita gunakan mulai dari IP 101 dan seterusnya sampai IP host 254 jika kita menggunakan prefix 24.



Kita akan mengkonfigurasi DHCP Excluded di topologi diatas tanpa adanya VLAN, perintahnya sama seperti membuat DHCP pada umumnya. Perintah Excluded Address sendiri setelah kita mengkonfigurasi DHCP Server.

Langkah Langkah :

A. Konfigurasi di Router

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-IDN
```

2. Mengaktifkan interface Gig0/0 dan memasang IP Address

```
R-IDN(config)#interface gig0/0  
R-IDN(config)#no shutdown  
R-IDN(config)#ip address 192.168.1.1 255.255.255.0
```

Jika tidak ada VLAN maka tidak perlu mengkonfigurasi sub interface, langsung membuat DHCP Server nya di router

3. Membuat DHCP Server

```
R-IDN(config)#ip dhcp pool TKJ
```

```
R-IDN(config)#network 192.168.1.0 255.255.255.0  
R-IDN(config)#default-router 192.168.1.1  
R-IDN(config)#dns-server 8.8.8.8
```

#### 4. Konfigurasi IP Excluded Address

```
R-IDN(config)#ip dhcp excluded-address 192.168.1.2 192.168.1.100
```

Adalah perintah untuk tidak memberikan IP Address mulai dari IP 192.168.11.2 sampai 192.168.11.100. Setelah itu mari kita cek konfigurasi laptop dan rubah settingan menjadi dynamic.

#### B. Pengecekan IP Address laptop

##### 1. Laptop A

IP Configuration

Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.1.101
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	8.8.8.8

##### 2. Laptop B

IP Configuration

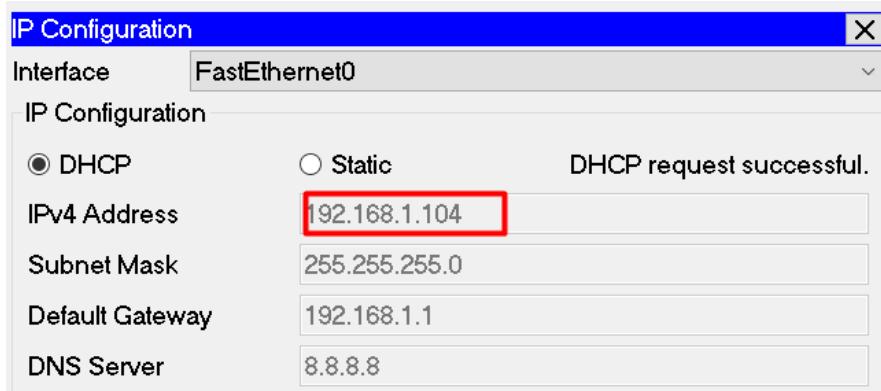
Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.1.102
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	8.8.8.8

##### 3. Laptop C

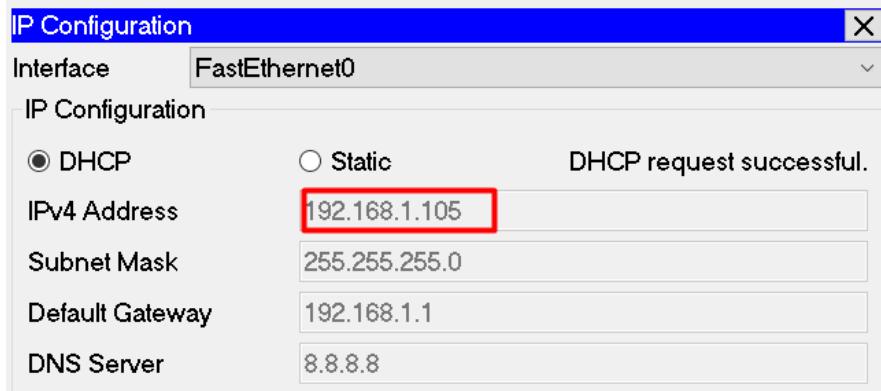
IP Configuration

Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.1.103
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	8.8.8.8

##### 4. Laptop D



5. Laptop E



Bisa dilihat bahwa IP Address yang diberikan oleh DHCP Server dimulai dari IP 101 dan seterusnya karena kita sudah mengkonfigurasi Excluded Address.

Pengecekan IP yang sudah diberikan DHCP oleh MLS

R-IDN(config)#do show ip dhcp binding				
IP address	Client-ID/ Hardware address	Lease expiration	Type	
192.168.1.101	00D0.58ED.004D	--	Automatic	
192.168.1.102	0090.2BAC.D183	--	Automatic	
192.168.1.103	0050.0F99.E249	--	Automatic	
192.168.1.104	0004.9A0A.7815	--	Automatic	
192.168.1.105	0004.9AD1.32D3	--	Automatic	

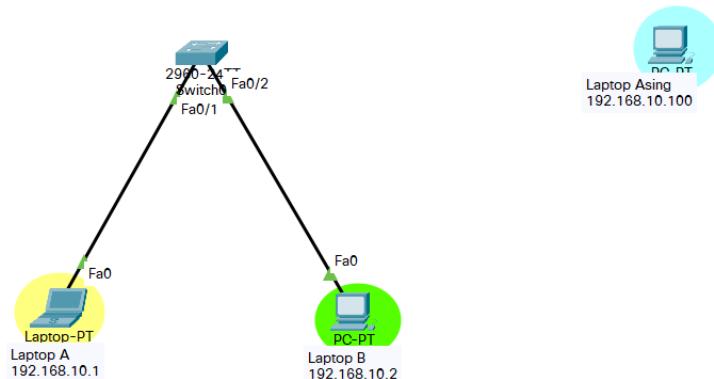
C. Lab DHCP Excluded telah selesai.

## Lab 11. Port Security

Port security merupakan sebuah cara untuk mengamankan port pada switch kita dari orang-orang yang tidak bertanggung jawab, seperti ketika ada seorang hacker yang mencoba menjebol PC Server. Untuk mengantisipasi, kita dapat menggunakan Port Security.

Pada Port Security terdapat 3 peran yaitu :

- **Shutdown:** Ketika port switch terhubung pada PC yang bukan Mac addressnya, maka port tersebut akan mati secara otomatis.
- **Protect:** Ketika port switch terhubung pada PC yang bukan mac addressnya, maka ketika ada packet keluar/masuk dari port tersebut, semuanya akan dibuang (drop).
- **Restrict:** Ketika port switch terhubung pada PC yang bukan mac addressnya, maka ketika ada packet keluar/masuk dari port tersebut, semuanya akan dibuang (drop) dan akan memunculkan pesan notifikasi SNMP (Simple Network Monitoring Protocol).



Kita akan mengkonfigurasi port security pada topologi atas, untuk langkah langkah sebagai berikut :

Langkah Langkah :

A. Konfigurasi di Switch

1. Mengganti nama Switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-IDN
```

2. Mengaktifkan command port security di interface

```
SW-IDN(config)#interface fa0/1
SW-IDN(config)#switchport mode access
SW-IDN(config)#switchport port-security
```

Berarti kita akan memilih *interface fa0/1* untuk menjalankan port security, Lalu, kita konfigurasikan agar switch mencatat mac address dari pc-nya. Terdapat 2 pilihan dalam mencatatnya, yaitu secara STATIC dan STICKY. STATIC adalah, kita mengisi secara manual mac address PC-nya. Jika STICKY, maka switch akan mencatat mac address yang ada di port tersebut berdasarkan mac address table.

Maka dari itu, jika mac address table masih kosong, kita harus melakukan ping antar pc agar ada traffic yang lewat pada switch tersebut.

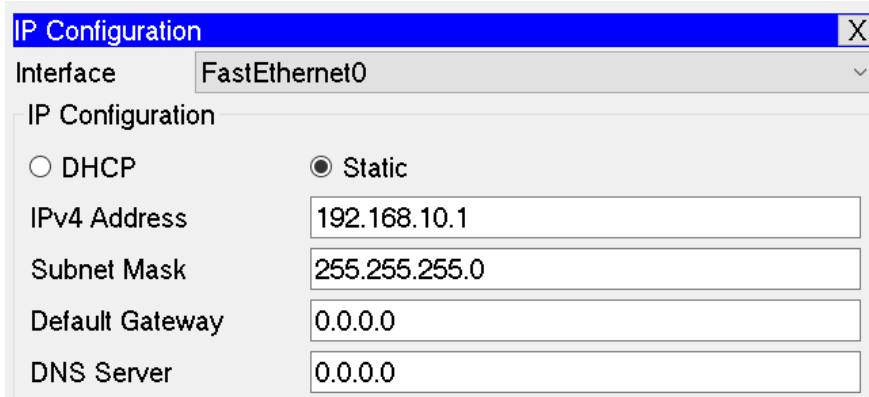
3. Menentukan jenis mencatatnya dan port securitynya

```
SW-IDN(config)#switchport port-security mac-address sticky  
SW-IDN(config)#switchport port-security violation shutdown
```

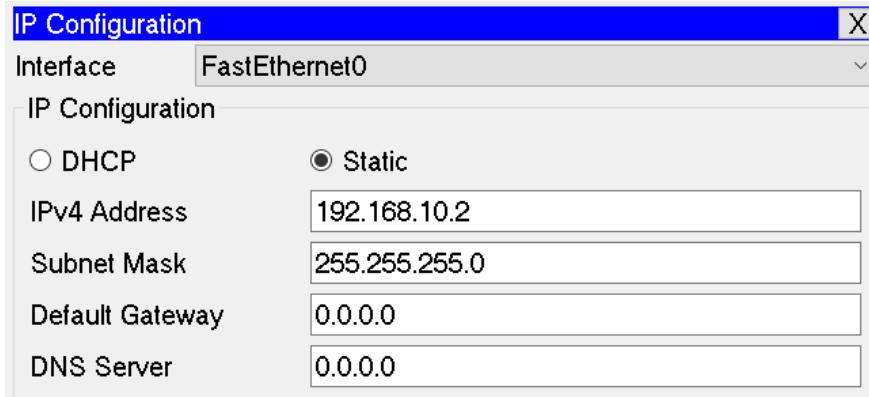
Jenis mencatat yang kita pilih yaitu STICKY yang mana switch akan mencatat mac address yang ada di port secara manual, dan memilih shutdown sebagai jenis violationnya. Kita juga bisa mengatur berapa banyak mac address yang bisa tercatat dalam satu interface. Secara default Port Security hanya membolehkan satu mac address dalam satu interface.

B. Konfigurasi IP Address Laptop

1. Laptop A



2. Laptop B



Setelah memasang IP Address yaitu kita akan melakukan status interface yang menjalankan port security.

C. Pengecekan

1. Pengecekan status interface yang menjalankan port-security

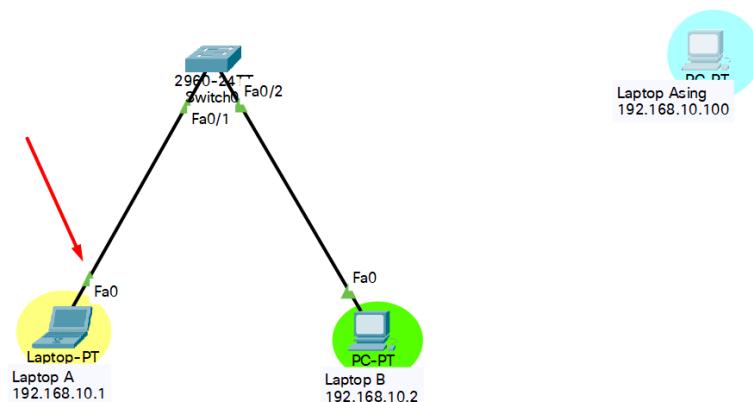
```
SW-IDN(config)#do show port-security  
SW-IDN(config-if)#do show port-security  
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action  
(Count) (Count) (Count)  
Fa0/1 1 1 0 Shutdown
```

2. Pengecekan mac address table

```
SW-IDN(config)#do show mac address-table
```

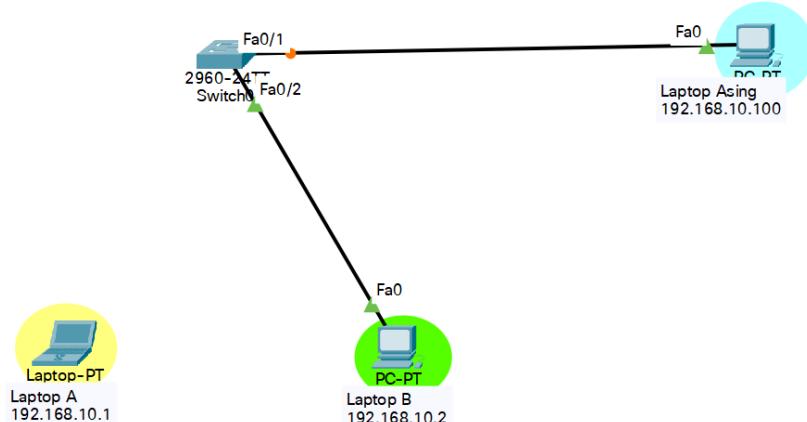
Mac Address Table			
Vlan	Mac Address	Type	Ports
1	000a.4179.b630	DYNAMIC	Fa0/2
1	000d.bd52.ceb0	STATIC	Fa0/1

3. Pengecekan interface fa0/1 sebelum di pindah ke laptop asing



Bisa dilihat bahwa interface fa0/1 sebelum di pindah ke laptop asing masih aktif, setelah itu kita akan mencoba interface fa0/1 dipindah ke laptop asing. Caranya tinggal drag interface fa0/1 ke laptop asing.

4. Pengecekan interface sesudah di pindah ke laptop asing



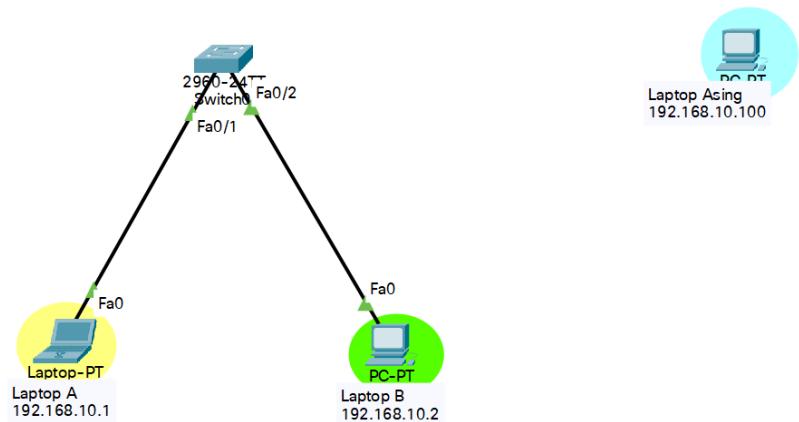
Bisa dilihat ketika interface fa0/1 dihubungkan ke laptop asing maka interface akan otomatis mati.

Setelah itu port dari laptop asing dipindah lagi ke laptop A

```

SW-IDN(config)#interface fa0/1
SW-IDN(config)#shutdown
SW-IDN(config)#no shutdown

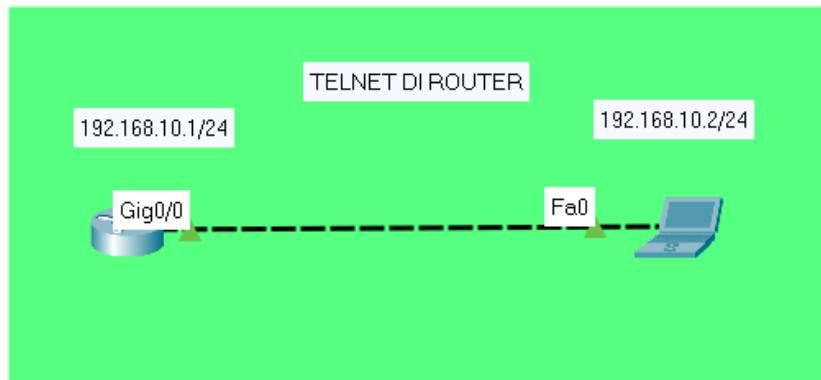
```



D. Lab Port Security telah selesai

## Lab 12. Telnet

Selain menggunakan kabel console, untuk mengakses router bisa juga by remote. Kita bisa meremote router kita menggunakan protocol telnet/SSH. Metode ini membutuhkan menggunakan IP Address. Untuk mengaktifkan telnet, yang akan kita config adalah line vty, telnet sendiri menggunakan protocol TCP/23, Berikut ini adalah cara mengkonfigurasinya :



Langkah Langkah :

A. Konfigurasi di Router

1. Mengganti nama Router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-TKJ
```

2. Mengaktifkan interface Gig0/0 dan memasang IP Address

```
R-TKJ(config)#interface gig0/0  
R-TKJ(config)#ip address 192.168.10.1 255.255.255.0  
R-TKJ(config)#no shutdown
```

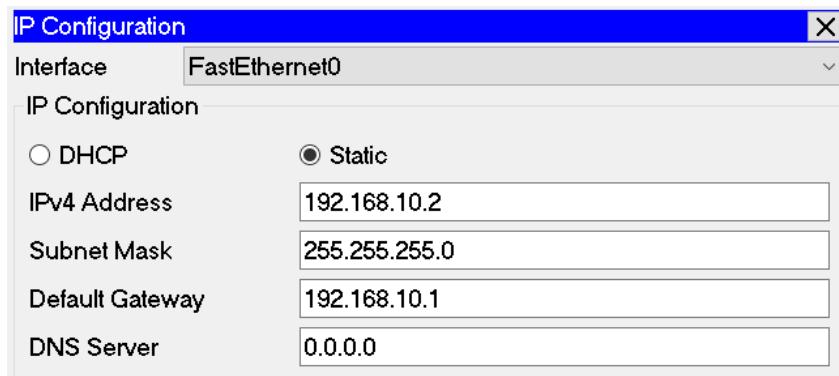
3. Konfigurasi Telnet di Router

```
R-TKJ(config)#username TKJ password 123  
R-TKJ(config)#line vty 0 4  
R-TKJ(config)#login local  
R-TKJ(config)#enable password 456
```

Angka 0 4 artinya perangkat tersebut bisa diremote oleh 5 orang secara bersamaan. "Login local" berarti saat seseorang akan melakukan remote, maka dia harus menggunakan username dan password yang ada di router. "login local" bisa diganti dengan "login" saja. Kalau kita menggunakan "login" maka tidak perlu menggunakan username, cukup memasukkan password saja. Jika menggunakan konfigurasi seperti di atas, maka 5 orang yang melakukan remote itu semuanya menggunakan jenis authentikasi yang sama. Untuk username sendiri bisa dibuat sesuai jumlah orang yang akan mengakses.

4. Konfigurasi IP Address laptop

1. Laptop A



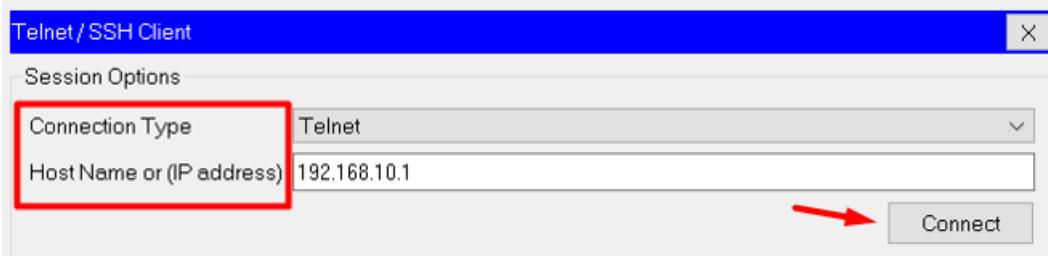
Selanjutnya kita akan melakukan pengecekan pada laptop untuk menjalankan telnet.

## B. Pengecekan

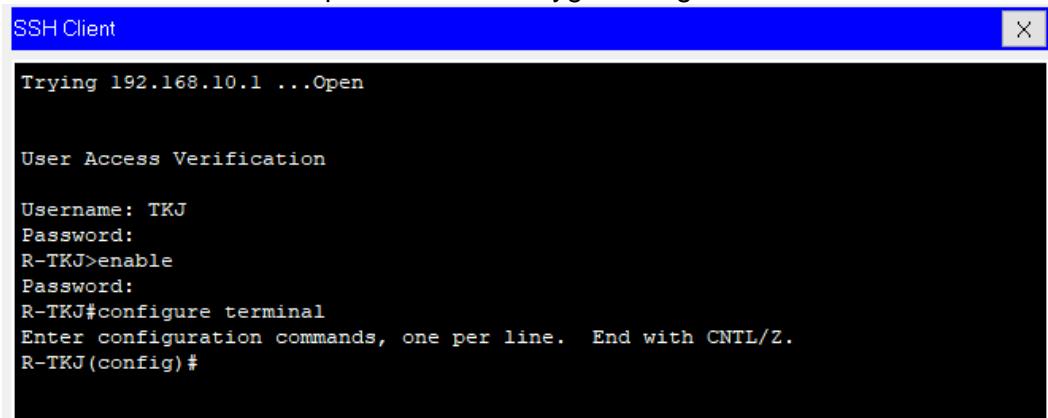
### 1. Pengecekan laptop untuk mentelnet Router



### 2. Ubah **connection type** menjadi telnet dan masukan ip target yang akan di telnet

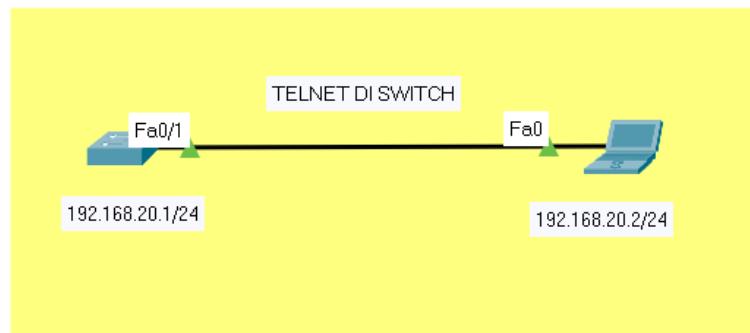


### 3. Masukan username dan password sesuai yg dikonfigurasikan di Router



### 4. Router berhasil di Telnet oleh laptop....

**Setelah mengkonfigurasi Telnet di Router, disini kita akan mengkonfigurasi Telnet di Switch**



Sama dengan router bedanya kita harus menambahkan interface virtual pada switch.  
Untuk langkah langkahnya sebagai berikut :

Langkah Langkah :

A. Konfigurasi di Switch

1. Mengganti nama Switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#host SW-KANTOR
```

2. Membuat interface VLAN 1 dan memasang ip address untuk gateway laptop

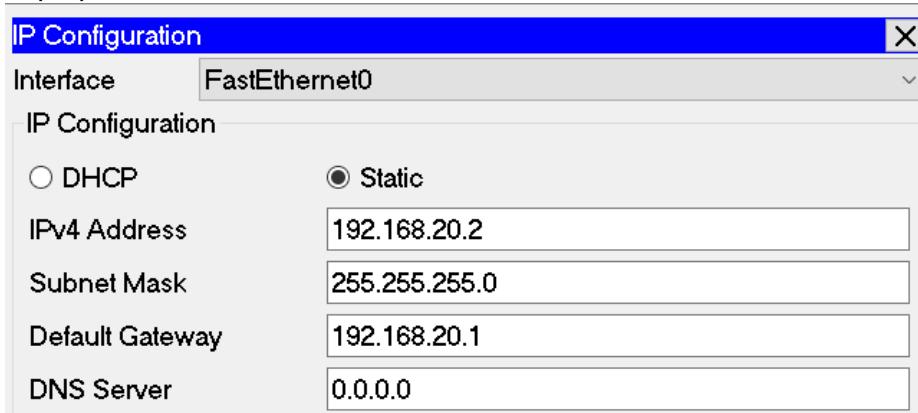
```
SW-KANTOR(config)#interface vlan 1  
SW-KANTOR(config)#ip address 192.168.20.1 255.255.255.0  
SW-KANTOR(config)#no shutdown
```

3. Konfigurasi Telnet di Switch

```
SW-KANTOR(config)#username IDN password 123  
SW-KANTOR(config)#line vty 0 4  
SW-KANTOR(config)#login local  
SW-KANTOR(config)#enable password 456
```

B. Konfigurasi ip di laptop

1. Laptop A

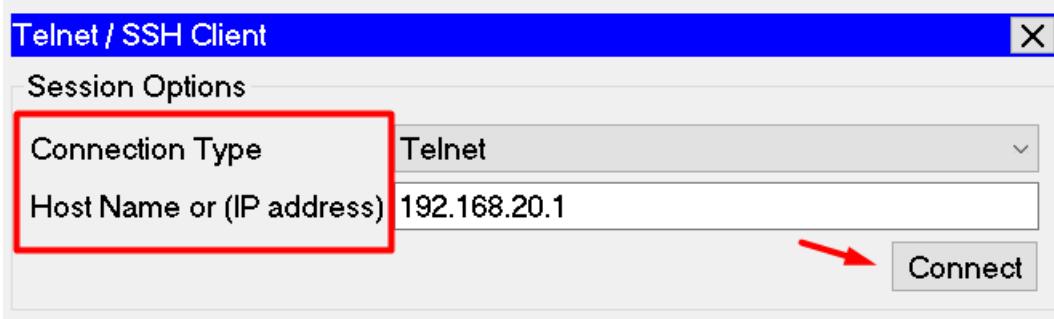


C. Pengecekan

1. Pengecekan laptop untuk telnet Switch



2. Ubah **connection type** menjadi telnet dan masukan ip target yang akan di telnet



3. Masukan username dan password sesuai yg dikonfigurasikan di Router

```
Trying 192.168.20.1 ...Open

User Access Verification

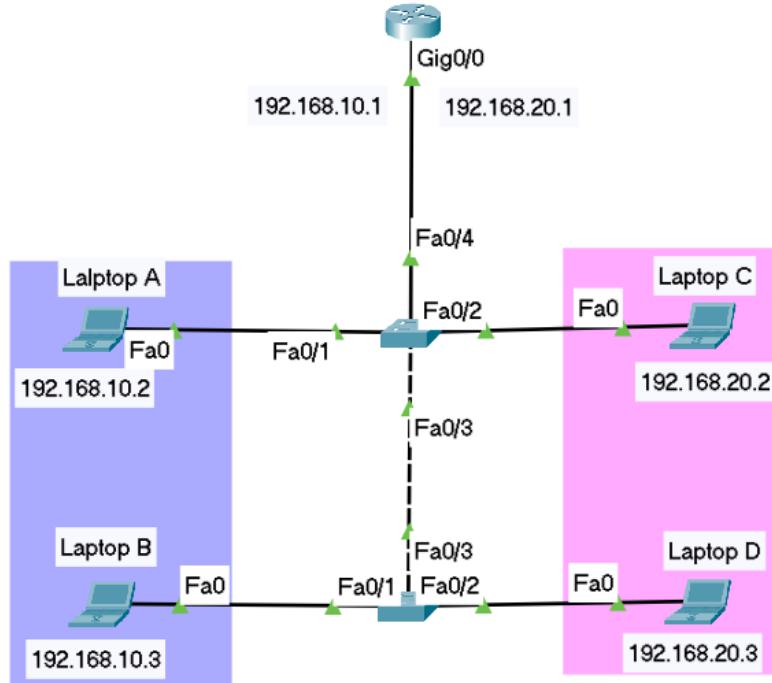
Username: IDN
Password:
SW-KANTOR>enable
Password:
SW-KANTOR#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-KANTOR(config) #
```

4. Switch berhasil di telnet oleh laptop

D. Lab Telnet telah selesai

## Lab 13. SSH (Secure Shell Host)

Sama dengan telnet SSH memiliki fungsi mengakses/meremote perangkat, SSH sendiri menggunakan protocol TCP/22, bedanya SSH lebih aman daripada telnet karena menggunakan enkripsi. Kita akan mengkonfigurasi SSH di topologi dibawah ini :



Langkah Langkah :

A. Konfigurasi di router

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-TKJ
```

2. Mengaktifkan interface Gig0/0

```
R-CORE(config)#interface gig0/0  
R-CORE(config)#no shutdown
```

3. Membuat sub interface

```
R-CORE(config)#interface gig0/0.10  
R-CORE(config)#encapsulation dot1q  
R-CORE(config)#ip address 192.168.10.1 255.255.255.0
```

4. Konfigurasi SSH (Membuat SSH)

```
R-CORE (config)#username tkj password 123  
R-CORE(config)#ip domain-name idn.id  
R-CORE(config)#crypto key generate rsa  
R-CORE(config)#enable password 456  
(Klik enter beberapa kali)
```

**Ip domain-name idn.id** maksudnya adalah kita membuat IP domain dengan nama idn.id, **crypto key generate rsa** maksudnya kita mengaktifkan enkripsi pada SSH, **enable password 456** maksudnya ketika seseorang hendak melakukan mengkonfigurasi router mereka harus memasukan password terlebih dahulu.

5. Konfigurasi SSH (Memasang SSH)

```
R-CORE(config)#line vty 0 4  
R-CORE(config)#transport input ssh  
R-CORE(config)#login local
```

jadi disini kita akan menggunakan laptop D untuk mentelnet Router, sebenarnya bisa menggunakan laptop mana saja tapi disini kita akan menggunakan laptop D saja untuk mentelnet Router.

B. Konfigurasi switch atas

1. Mengganti nama hostname

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-ATAS
```

2. Membuat VLAN 10 dan VLAN 20

```
SW-ATAS(config)#vlan 10  
SW-ATAS(config)#name GURU
```

```
SW-ATAS(config)#vlan 20  
SW-ATAS(config)#name SISWA
```

3. Memasukan interface ke dalam VLAN

```
SW-ATAS(config)#interface fa0/1  
SW-ATAS(config)#switchport mode access  
SW-ATAS(config)#switchport acces vlan 10
```

```
SW-ATAS(config)#interface fa0/2  
SW-ATAS(config)#switchport mode access  
SW-ATAS(config)#switchport access vlan 20
```

4. Melakukan trunk di switch atas

```
SW-ATAS(config)#interface range fa0/4-6  
SW-ATAS(config)#switchport mode trunk
```

C. Konfigurasi switch bawah

1. Mengganti nama hostname

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-BAWAH
```

2. Membuat VLAN 10 dan VLAN 20

```
SW-BAWAH(config)#vlan 10  
SW-BAWAH(config)#name GURU
```

```
SW-BAWAH(config)#vlan 20  
SW-BAWAH(config)#name SISWA
```

3. Memasukan interface ke dalam VLAN

```
SW-BAWAH(config)#interface fa0/1  
SW-BAWAH(config)#switchport mode access  
SW-BAWAH(config)#switchport acces vlan 10
```

```
SW-BAWAH(config)#interface fa0/2  
SW-BAWAH(config)#switchport mode access  
SW-BAWAH(config)#switchport access vlan 20
```

4. Melakukan trunk di switch atas

```
SW-BAWAH(config)#interface fa0/3  
SW-BAWAH(config)#switchport mode trunk
```

D. Konfigurasi IP Address laptop

1. Laptop A

IP Configuration

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

2. Laptop B

IP Configuration

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

3. Laptop C

IP Configuration

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.20.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	0.0.0.0

4. Laptop D

IP Configuration

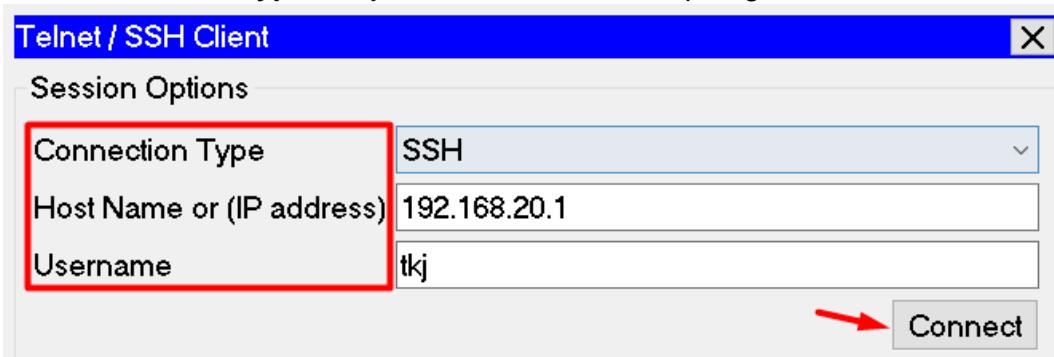
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.20.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	0.0.0.0

## E. Pengecekan

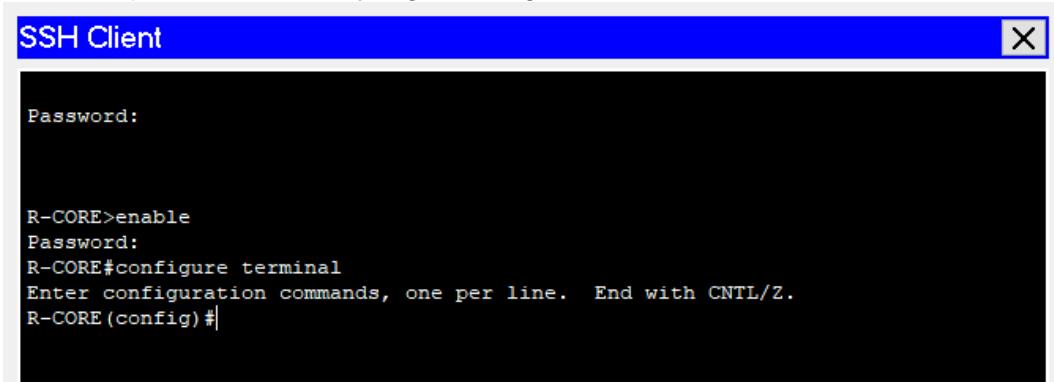
### 1. Pengecekan laptop D untuk SSH Router



### 2. Ubah **connection type** menjadi SSH dan masukan ip target dan username



### 3. Masukan password sesuai yang di konfigurasi di Router

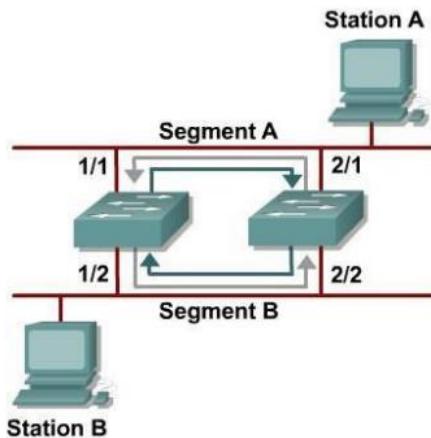


### 4. Router berhasil di SSH oleh laptop D

## F. Lab SSH telah selesai

## Lab 14. Spanning tree protocol (STP)

Secara garis besar, STP/Spanning Tree Protocol adalah protocol dalam switch yang berfungsi untuk mencegah terjadinya switching looping.



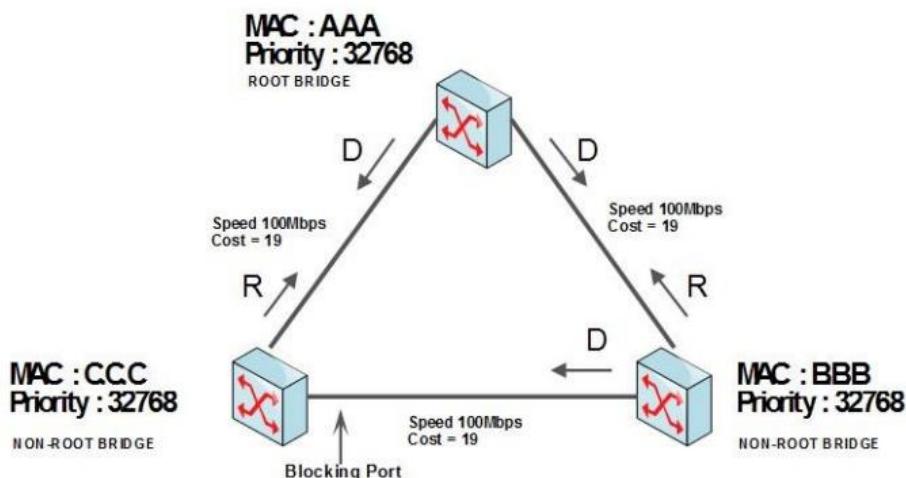
Misalkan pada switch kiri mau mengirim sebuah data yang tidak ada destinasinya pada tabel mac addressnya, sehingga switchnya akan membroadcast ke semua port hingga sampailah ke switch kanan. Sementara di switch kanan juga sama, dia juga tidak tahu destinasinya kemana sehingga dibroadcast ulang dan sampai ke switch kiri, di switch kiri terulang lagi dan dibroadcast lagi ke switch kanan, dan begitulah seterusnya hingga networknya down.

Dengan adanya STP, maka salah satu port tadi akan diblok, sehingga hanya satu jalur yang digunakan agar tidak terjadi loop. Namun jika salah satunya down, maka port yang diblok tadi akan forward kembali.

Jenis STP:

- Open Standard: STP (802.1D), Rapid STP (802.1W), Multiple Spanning Tree/MST (802.1S)
- Cisco Proprietary: Per-Vlan Spanning Tree/PVST, PVST +, Rapid PVST

### Proses dalam STP



- Root Bridge dan Non-Root Bridge

Root bridge: Merupakan switch yang menjadi “Raja.” Diantara switch-switch lain dalam satu STP. Switch ini dipilih berdasarkan priority terendah, jika priority sama, maka dipilih berdasar mac address terendah, sementara switch dengan mac address terbesar akan menjadi port blocking.

Non-Root bridge: Merupakan switch yang tidak menjadi “raja.” Dan hanya menjadi switch yang meneruskan jalan dari sang “raja”.

- Designated port, root port dan Alternate/blocking port.

Designated Port: Merupakan port forwarding/ port aktif yang dapat menyalurkan data, posisi port ini menjauhi sang “raja.”

Root Port: Merupakan port forwarding/port aktif yang dapat menyalurkan data, namun posisinya mendekat/menuju sang “raja.”

Blocking port: Merupakan port yang non-aktif/mati/terblokir. Port ini merupakan port cadangan jika designated port yang aktif tiba-tiba down/mati.

- Cost pada tiap jalur:

Ethernet: 100

Fast Ethernet: 19

Gigabyte Ethernet: 4

# SPANNING TREE • PART 1

packetlife.net

Spanning Tree Protocols						
	Legacy STP	PVST	PVST+	RSTP	RPVST+ & MST	
<b>Algorithm</b>	Legacy ST	Legacy ST	Legacy ST	Rapid ST	Rapid ST	
<b>Defined By</b>	802.1D-1998	Cisco	Cisco	802.1w, 802.1D-2004	Cisco	
<b>Instances</b>	1	Per VLAN	Per VLAN	1	Per VLAN	
<b>Trunking</b>	N/A	ISL	802.1Q, ISL	N/A	802.1Q, ISL	
Spanning Tree Instance Comparison						
<span style="color: black;">■ All VLANs</span> <span style="color: red;">■ VLAN 1</span> <span style="color: green;">■ VLAN 10</span> <span style="color: blue;">■ VLAN 20</span> <span style="color: orange;">■ VLAN 30</span> <span style="color: red;">■ MSTI 0 (1, 10)</span> <span style="color: blue;">■ MSTI 1 (20, 30)</span>						
BPDU Format		Spanning Tree Specifications			Link Costs	
Field	Bits	802.1s	802.1Q-2003	802.1Q-2005	Bandwidth	Cost
Protocol ID	16				4 Mbps	250
Version	8				10 Mbps	100
BPDU Type	8	802.1D-1998		802.1D-2004	16 Mbps	62
Flags	8		802.1Q-1998		45 Mbps	39
Root ID	64				100 Mbps	19
Root Path Cost	32				155 Mbps	14
Bridge ID	64	ISL	PVST	PVST+	622 Mbps	6
Port ID	16				1 Gbps	4
Message Age	16				10 Gbps	2
Max Age	16				20+ Gbps	1
Hello Time	16					
Forward Delay	16					
Default Timers		IEEE	<b>IEEE 802.1D-1998</b> · Deprecated legacy STP standard <b>IEEE 802.1w</b> · Introduced RSTP <b>IEEE 802.1D-2004</b> · Replaced legacy STP with RSTP <b>IEEE 802.1s</b> · Introduced MST <b>IEEE 802.1Q-2003</b> · Added MST to 802.1Q <b>IEEE 802.1Q-2005</b> · Most recent 802.1Q revision			Port States
Hello	2s	Cisco	PVST	PVST+	RPVST+	Legacy ST      Rapid ST
Forward Delay	15s					Disabled
Max Age	20s					Blocking      Discarding
						Listening
						Learning      Learning
						Forwarding      Forwarding
Spanning Tree Operation						Port Roles
<b>1 Determine root bridge</b>	The bridge advertising the lowest bridge ID becomes the root bridge					Legacy ST      Rapid ST
<b>2 Select root port</b>	Each bridge selects its primary port facing the root					Root      Root
<b>3 Select designated ports</b>	One designated port is selected per segment					Designated      Designated
<b>4 Block ports with loops</b>	All non-root and non-designated ports are blocked					Blocking      Alternate
						Blocking      Backup

by Jeremy Stretch

v3.0

# SPANNING TREE • PART 2

packetlife.net

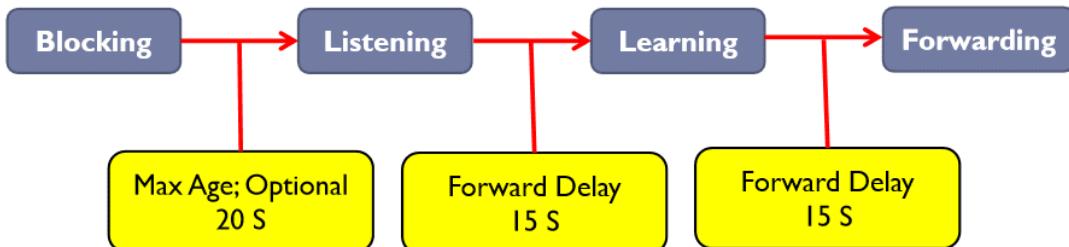
PVST+ and RPVST+ Configuration	Bridge ID Format						
<pre>spanning-tree mode {pvst   rapid-pvst}  ! Bridge priority spanning-tree vlan 1-4094 priority 32768  ! Timers, in seconds spanning-tree vlan 1-4094 hello-time 2 spanning-tree vlan 1-4094 forward-time 15 spanning-tree vlan 1-4094 max-age 20  ! PVST+ Enhancements spanning-tree backbonefast spanning-tree uplinkfast  ! Interface attributes interface FastEthernet0/1   spanning-tree [vlan 1-4094] port-priority 128   spanning-tree [vlan 1-4094] cost 19  ! Manual link type specification spanning-tree link-type {point-to-point   shared}  ! Enables PortFast if running PVST+, or ! designates an edge port under RPVST+ spanning-tree portfast  ! Spanning tree protection spanning-tree guard {loop   root   none}  ! Per-interface toggling spanning-tree bpdufilter enable spanning-tree bpdufilter enable</pre>	<table border="1"> <tr> <td style="text-align: center;">4</td> <td style="text-align: center;">12</td> <td style="text-align: center;">48</td> </tr> <tr> <td>Pri</td> <td>Sys ID Ext</td> <td>MAC Address</td> </tr> </table> <p><b>Priority</b> 4-bit bridge priority (configurable from 0 to 61440 in increments of 4096)</p> <p><b>System ID Extension</b> 12-bit value taken from VLAN number (IEEE 802.1t)</p> <p><b>MAC Address</b> 48-bit unique identifier</p>	4	12	48	Pri	Sys ID Ext	MAC Address
4	12	48					
Pri	Sys ID Ext	MAC Address					
MST Configuration	Path Selection						
<pre>spanning-tree mode mst  ! MST Configuration spanning-tree mst configuration   name MyTree   revision 1  ! Map VLANs to instances   instance 1 vlan 20, 30   instance 2 vlan 40, 50  ! Bridge priority (per instance) spanning-tree mst 1 priority 32768  ! Timers, in seconds spanning-tree mst hello-time 2 spanning-tree mst forward-time 15 spanning-tree mst max-age 20  ! Maximum hops for BPDU spanning-tree mst max-hops 20  ! Interface attributes interface FastEthernet0/1   spanning-tree mst 1 port-priority 128   spanning-tree mst 1 cost 19</pre>	<ol style="list-style-type: none"> <li>1 Bridge with lowest root ID becomes the root</li> <li>2 Prefer the neighbor with the lowest cost to root</li> <li>3 Prefer the neighbor with the lowest bridge ID</li> <li>4 Prefer the lowest sender port ID</li> </ol>						
	Optional PVST+ Enhancements						
	<p><b>PortFast</b> Enables immediate transition into the forwarding state (designates edge ports under MST)</p> <p><b>UplinkFast</b> Enables switches to maintain backup paths to root</p> <p><b>BackboneFast</b> Enables immediate expiration of the Max Age timer in the event of an indirect link failure</p>						
	Spanning Tree Protection						
	<p><b>Root Guard</b> Prevents a port from becoming the root port</p> <p><b>BPDU Guard</b> Error-disables a port if a BPDU is received</p> <p><b>Loop Guard</b> Prevents a blocked port from transitioning to listening after the Max Age timer has expired</p> <p><b>BPDU Filter</b> Blocks BPUDUs on an interface (disables STP)</p>						
	RSTP Link Types						
	<p><b>Point-to-Point</b> Connects to exactly one other bridge (full duplex)</p> <p><b>Shared</b> Potentially connects to multiple bridges (half duplex)</p> <p><b>Edge</b> Connects to a single host; designated by PortFast</p>						
	Troubleshooting						
	<pre>show spanning-tree [summary   detail   root] show spanning-tree [interface   vlan] show spanning-tree mst [...]</pre>						

by Jeremy Stretch

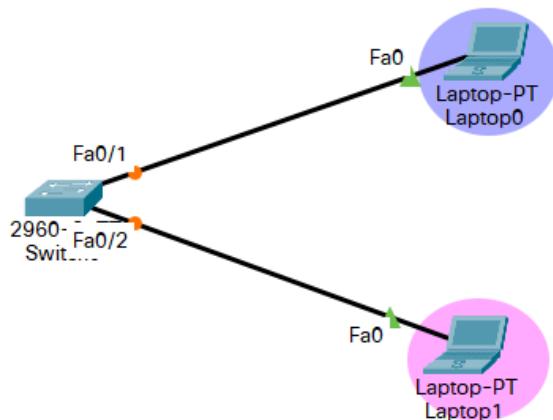
v3.0

## Lab 15. STP Portfast

Bila kita colokkan kabel ke switch maka biasanya butuh waktu agak lama portnya dari oranye menjadi hijau. Total waktu yang dibutuhkan adalah 50 detik.



Dengan memasukan STP Portfast, port fa0/1 dan fa0/2 ketika terkoneksi dengan pc akan langsung bisa forwarding data sehingga tidak perlu listening dan learning dulu yang biasanya akan memakan waktu 50 detik. Portfast, tidak dapat berjalan dengan trunk. Sehingga, jika kita ingin menggunakan portfast, maka kita harus mematikan fungsi trunk terlebih dahulu. biasanya portfast diimplementasikan pada port yang mengarah ke end device.



Langkah Langkah :

- Konfigurasi Switch
  - Mengganti hostname switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-IDN
```

2. Konfigurasi STP Portfast

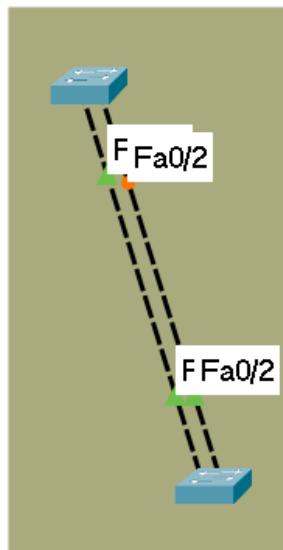
```
SW-IDN(config)#interface range fa0/1-2
SW-IDN(config)#spanning-tree portfast
```

Dengan adanya konfigurasi portfast interface akan langsung melewati tahapan tahapan forwading dan interface langsung berwarna hijau.

- B. Lab STP Portfast telah selesai.

## Lab 16. STP Priority (Main Link)

Bagaimana caranya agar kita bisa menentukan switch mana yang menjadi root bridge? yaitu dengan merubah nilai prioritynya menjadi lebih kecil. Karena switch dengan nilai prioritynya terkecil akan menjadi switch root bridge.



Pada topologi diatas ini switch yang menjadi root bridge adalah switch bawah, nah kita akan mengkonfigurasi STP Priority agar switch atas menjadi root bridge.

Langkah Langkah :

A. Konfigurasi di switch atas

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-ATAS
```

2. Konfigurasi STP Priority,mengubah nilai priority Switch atas

```
SW-ATAS(config)#spanning-tree vlan 1 priority 4096
```

B. Konfigurasi di Switch bawah

1. Mengganti nama Switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-BAWAH
```

2. Konfigurasi STP Priority,mengubah nilai priority Switch bawah

```
SW-BAWAH(config)#spanning-tree vlan 1 priority 61440
```

C. Pengecekan

1. Pengecekan Switch atas untuk melihat nilai priority yang sudah diubah

```
SW-ATAS(config)#do show spanning-tree
```

```

SW-ATAS(config)# do show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Priority    4097
            Address   00D0.D375.EC88
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority    4097 (priority 4096 sys-id-ext 1)
            Address   00D0.D375.EC88
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/1          Desg FWD 19        128.1    P2p
  Fa0/2          Desg FWD 19        128.2    P2p

```

2. Pengecekan Switch bawah untuk melihat nilai priority yang sudah diubah

```

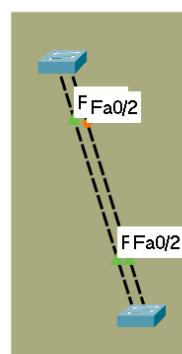
SW-BAWAH(config)#do show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Priority    4097
            Address   00D0.D375.EC88
            Cost      19
            Port      1(FastEthernet0/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority    61441 (priority 61440 sys-id-ext 1)
            Address   0060.7070.8930
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

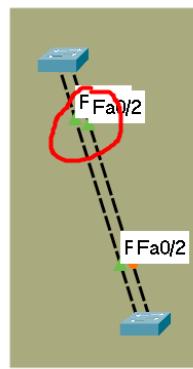
  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/1          Root FWD 19        128.1    P2p
  Fa0/2          Altn BLK 19        128.2    P2p

```

Dikondisi awal sebelum dikonfigurasi STP Priority, switch yang menjadi root bridge adalah switch bawah. Bisa dilihat pada topologi dibawah ini :



kedua switch tersebut memiliki nilai priority yang sama jadi penentuan switch yang akan menjadi root bridge adalah melalui nilai mac address terendah diantara kedua switch tersebut. Setelah dikonfigurasi STP Priority yaitu dengan merubah nilai priority dikedua switch di switch atas nilai priority nya adalah 4096 dan di switch bawah nilai priority 61440 maka switch akan mengambil switch atas yang mempunyai nilai priority terendah.



Kalian dapat menentukan nilai priority dengan syarat, boleh menggunakan 0 dan kelipatan 4096 misalnya 0,4096,8192 dan seterusnya.

D. Lab STP Priority telah selesai.

## Lab 17. Etherchannel

Pada switch bila kita koneksi beberapa kabel, maka karena mekanisme spanning tree, tidak semua link digunakan untuk mengirimkan data dikarenakan salah satu portnya blocking. Untuk itu kita bisa gunakan etherchannel, yakni dengan membundling link tersebut sehingga seolah-olah menjadi 1 link saja. Dengan demikian semua linknya aktif digunakan untuk mengirimkan data.

Terdapat 3 jenis Etherchannel :

- **LACP (Link Aggregation Control Protocol)**

Open Standard IEEE 802.1AD Etherchannel, terdapat 2 mode :

- Active: Protocol LACP yang mengajak untuk menjadi etherchannel

- Passive: Protocol LACP yang menunggu untuk menjadi etherchannel

- **PAGP (Port Aggregation Protocol)**

Cisco Proprietary, hanya bekerja ada sesama switch Cisco, terdapat 2 mode :

- Desirable: Protocol PAGP yang mengajak untuk menjadi etherchannel

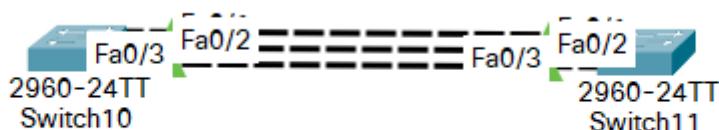
- Auto: Protocol PAGP yang menunggu untuk diajak etherchannel

- **Layer 3 Etherchannel**

Protocol Etherchannel yang dapat dilakukan di MLS, hanya terdapat 1 mode :

- ON: Protocol Etherchannel layer 3 yang mengajak untuk menjadi etherchannel

Berikut adalah Lab Etherchannel :



Kita konfigurasi etherchannel layer-2 (LACP)

1. Perintah etherchannel LACP switch kiri

```
SW-KIRI(config)#interface range fa0/1-3
SW-KIRI(config)#switchport mode trunk
SW-KIRI(config)#channel-group 1 mode active
```

2. Perintah etherchannel LACP switch kanan

```
SW-KANAN (config)#interface range fa0/1-3
SW-KANAN(config)#switchport mode trunk
SW-KANAN(config)#channel-group 1 mode passive
```

Agar etherchannel dapat terbentuk, kita harus menggunakan mode yang saling mengajak, ataupun yang satu mengajak, yang satu menunggu diajak. Karena,

etherchannel tidak akan terbentuk jika keduanya menggunakan mode yang menunggu diajak.

Berikut command untuk melihat etherchannel yang dijalankan :

1. Pengecekan etherchannel yang dijalankan di switch kiri

```
SW-KIRI(config)#do show etherchannel summary
SW-KIRI(config)#do show etherchannel summary
Flags: D - down          P - 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
      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)       LACP        Fa0/1(P)  Fa0/2(P)  Fa0/3(P)
```

2. Pengecekan etherchannel yang dijalankan di switch kanan

```
SW-KANAN(config)#do show etherchannel summary
SW-KANAN(config)#do show etherchannel summary
Flags: D - down          P - 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
      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)       LACP        Fa0/1(P)  Fa0/2(P)  Fa0/3(P)
```

Berdasarkan command diatas, terdapat etherchannel aktif, protocolnya LACP dan menggunakan 3 port yaitu fa0/1, fa0/2, dan fa0/3.

Sementara itu, berikut konfigurasi etherchannel layer-2 (PAGP)

```
SW-KIRI(config)#interface range fa0/1-3
SW-KIRI(config)#switchport mode trunk
SW-KIRI(config)#channel-group 1 mode desirable
```

```
SW-KANAN (config)#interface range fa0/1-3
SW-KANAN(config)#switchport mode trunk
SW-KANAN(config)#channel-group 1 mode auto
```

Secara konfigurasi, memang tidak jauh berbeda, hal ini dikarenakan LACP dan PAGP masih satu layer, yaitu layer 2. Namun cara agar etherchannelnya terbentuk

masih sama, gunakan mode yang saling mengajak, atau yang satu mengajak yang satu menunggu.

Berikut konfigurasi etherchannel layer-2 (MLS)

```
MLS-KIRI (config)#interface range fa0/1-3
MLS-KIRI(config)#switchport mode trunk
MLS-KIRI(config)#channel-group 1 mode on
MLS-KIRI(config)#no switchport
MLS-KIRI(config)#interface port-channel 1
MLS-KIRI(config)#ip address 10.10.10.1 255.255.255.0
```

```
MLS-KANAN (config)#interface range fa0/1-3
MLS-KANAN(config)#switchport mode trunk
MLS-KANAN(config)#channel-group 1 mode on
MLS-KANAN(config)#no switchport
MLS-KANAN(config)#interface port-channel 1
MLS-KANAN(config)#ip address 10.10.10.2 255.255.255.0
```

Pada etherchannel layer 3, terdapat beberapa perbedaan. Etherchannel layer 3, hanya didukung oleh perangkat MLS (MultiLayer Switch) yang bekerja di layer 2 dan 3.

Berdasarkan konfigurasi diatas, setelah kita konfigurasikan etherchannelnya, kita masukkan command **no switchport**. Fungsi dari command ini adalah untuk menghilangkan fungsi switch pada port tersebut. Karena, etherchannel yang dikonfigurasikan bekerja di layer 3 dan sementara switch, berjalan di layer 2. Namun etherchannel layer 3 merupakan layanan pada switch, namun hanya pada Layer 3 switch, yaitu MLS.

Kemudian mengapa kita masukkan IP Address kedalam port channelnya? Karena etherchannel layer 3 menggunakan IP Address sebagai identitasnya agar antar port channel dapat saling mengetahui.

## Lab 18. Switch Stacking

Switch stacking adalah penggabungan/penumpukan beberapa switch menjadi sebuah switch tunggal. Keuntungan dan fungsi Switch Stacking : Menyederhanakan manajemen, Scalability, Menambah port pada switch.



Apabila sudah di sambungkan dengan kabel stacking, kita hanya sedikit mengkonfigurasi reload pada switch.

```
SW-STACKING(config)#do reload
```

# Routing

# **ROUTING**

**CONTENT :**

**STATIC ROUTE**

**DYNAMIC ROUTING EIGRP**

**EIGRP AUTHENTICATION**

**DYNAMIC ROUTING OSPF**

**OSPF AUTHENTICATION**

**REDISTRIBUTE EIGRP & OSPF**

**DYNAMIC ROUTING RIP**

## Routing Introduction

Secara garis besar, routing merupakan sebuah cara untuk menghubungkan antar jaringan yang berbeda dengan skala yang berbeda, mulai dari skala kecil (LAN), skala menengah (MAN) hingga skala besar (WAN). Routing ini bekerja pada layer ke-3 pada OSI Layer yang pengalamatannya berdasarkan IP address.

Dan cara kerjanya. Router, sebagai device yang bekerja, mengenalkan jaringan yang dia miliki kepada router lain sehingga antar kedua jaringan yang terdapat di kedua router tersebut dapat saling berkomunikasi.

Itulah pengenalan routing, tentang bagaimana antar kedua buah atau bahkan lebih jaringan diseluruh dunia ini bisa saling berkomunikasi. Dan selanjutnya, kita akan membahas tentang routing secara detail.

## Routing Fundamental

### Route Type

Dalam berkomunikasi, routing ini terbagi menjadi 3 tipe:

#### 1. Static Route

Adalah router yang memiliki kabel routing statis yang settingannya diatur oleh administrasi jaringan secara manual yaitu dengan menentukan destination dan gateway secara manual.

#### 2. Dynamic Route

Adalah router yang membuat tabel routing secara otomatis, dengan membaca lalu lintas jaringan dan tentu juga dengan saling berhubungan dengan router yang lain. Routing dinamis adalah routing yang paling mudah daripada routing default dan static.

#### 3. Default Route

adalah jalur default untuk paket yang mempunyai alamat network tujuan tertentu tapi tidak terdapat di routing table router yang disinggahi. Jika terdapat default route yang di-set pada router tersebut, maka paket tersebut akan mengikuti rute default yang telah ditetapkan, jika tidak ada default route maka paket akan dibuang/discard. Default route didefinisikan dengan alamat : 0.0.0.0/0 . Default route pada routing table ditandai dengan flag "S\*".

## Routing Table

Sebuah Router akan forwarding paket berdasarkan informasi yang terdapat pada sebuah routing table. Jadi jika kita ingin mengirim sebuah paket ke Network tertentu, pastikan informasi network tersebut ada di Routing Table.

Yang artinya jika kita mencoba melakukan ping terhadap network selain network yang berada di routing table, maka hasilnya akan RTO (Request Time Out) alias gagal karena router tidak/belum mengenali network tersebut. Lalu, bagaimana kita mengisi routing table.

Lalu bagaimana kita mengisi routing table?

## Best Route

Router akan memilih sebuah jalur terbaik (mengisi informasi table routing) berdasarkan kriteria berikut:

### 1. Longest prefix match

Router akan memilih prefix paling spesifik ke destination address untuk memforward packet.

Contoh, jika dalam table routing terdapat entry:

- a. 192.168.0.0/16
- b. 192.168.12.0/24
- c. 192.0.0.0/10

Maka jika kita ingin mengirim paket ke 192.168.12.1, router akan mengirim ke prefix yang paling spesifik yaitu 192.168.12.0/24.

### 2. Distance

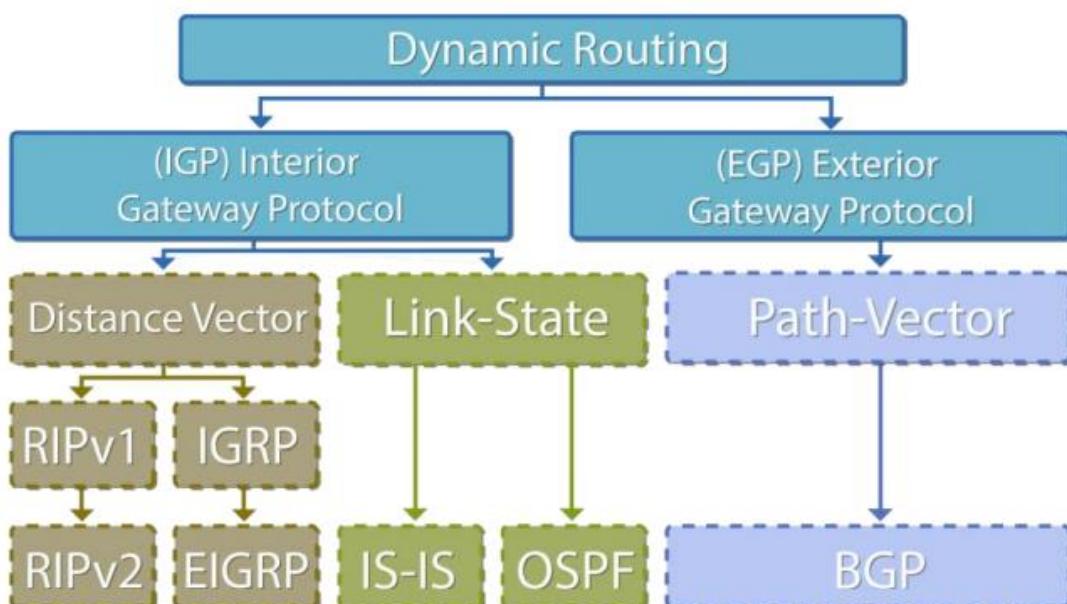
Router akan memilih nilai distance yang paling kecil).

### 3. Round Robin

Random Apabila Rule tersebut sama-sama spesifik dan memiliki nilai distance yang sama. Biasa disebut sebagai Load Balance).

## Routing Protocol

Routing protocol akan digunakan oleh router jika router tersebut menggunakan Routing Dynamic, Routing protocol merupakan Protocol yang di gunakan oleh Router router untuk saling bertukar informasi Routing, pertukaran infromasi akan dilakukan secara Dynamic, sehingga jika terjadi perubahan pada jaringan,maka Protocol tersebut akan memberitahukan perubahan tersebut kepada router-router lain yang ada di dalam jaringan tersebut.



Terdapat 2 jenis routing protocol pada dynamic routing:

### 1. IGP (Interior Gateway Protocol)

IGP, merupakan jenis routing protocol yang berjalan didalam sebuah instansi/Area lokal atau yang biasa disebut dengan AS (Autonomous System). Didalam IGP, dibagi lagi menjadi 2 algoritma :

- **Distance Vector**

Distance Vector, merupakan tipe routing protocol yang dalam konektivitasnya pada sebuah jaringan, dia akan memilih jalur routing dengan loncatan/hop count tersedikit atau routing dengan jalur terpendek daripada jalur routing yang memiliki bandwidth terbesar walaupun jaraknya jauh.

- **Link-State**

Sedangkan Link-State, merupakan kebalikan dari Distance Vector. Dalam konektivitasnya pada suatu jaringan, dia lebih memilih jalur routing dengan bandwidth terbesar walaupun jaraknya jauh, daripada jalur dengan hop count terpendek.

### 2. EGP (Exterior Gateway Protocol)

Sedangkan EGP, merupakan routing protocol, yang berjalan diluar AS (Autonomous System) tujuan dari EGP ini, untuk menghubungkan antar area lokal/AS tadi agar bisa saling berkomunikasi. EGP ini, merupakan routing protocol yang besar sekali perannya, karena dengan EGP ini, kita bisa menikmati internet. Dalam EGP ada sebuah sebuah algoritma :

- **Path Vector**

Satu-satunya algoritma pada EGP, yang dalam konektivitasnya, dia menggunakan gabungan antara jarak terpendek dan Bandwidth terbesar serta dilengkapi dengan attributes/penanda dalam proses menemukan jalur terbaiknya.

## Administrative Distance (AD)

Administrative distance merupakan suatu fitur yang digunakan oleh router untuk menentukan pemilihan jalur terbaik jika terdapat dua atau lebih jalur menuju ke tujuan yang sama dari dua routing protokol yang berbeda. Dengan adanya Administrative Distance maka router bisa dengan jelas menentukan protocol apakah yang akan ia pakai jika terdapat lebih dari satu protocol.

Sebagai contoh, dalam sebuah jaringan, terdapat router-A dan router B. Misalkan terdapat 2 jalur jika router-A ingin berkomunikasi dengan router-B, jalur pertama lewat router-C dan menggunakan protokol RIP, sementara jalur kedua lewat router-D dan menggunakan protokol OSPF, disinilah Administrative Distance bekerja. Jika kita perhatikan, kedua jalur memiliki protokol routing yang berbeda, kanan menggunakan RIP, kiri menggunakan OSPF. AD dari OSPF adalah 110, sementara RIP adalah 120. Maka jalur yang dipilih oleh router untuk berkomunikasi dengan router-B adalah lewat router-D yaitu OSPF, hal ini dikarenakan AD dari OSPF lebih kecil daripada RIP, semakin kecil Administrative Distance maka itulah yang akan dipilih router.

Sementara itu, jalur kanan atau RIP, akan digunakan oleh router jika jalur yang diutamakan -OSPF mati.

Berikut adalah daftar dari Administrative Distance :

Administrative Distance Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unknown	255

## Metric

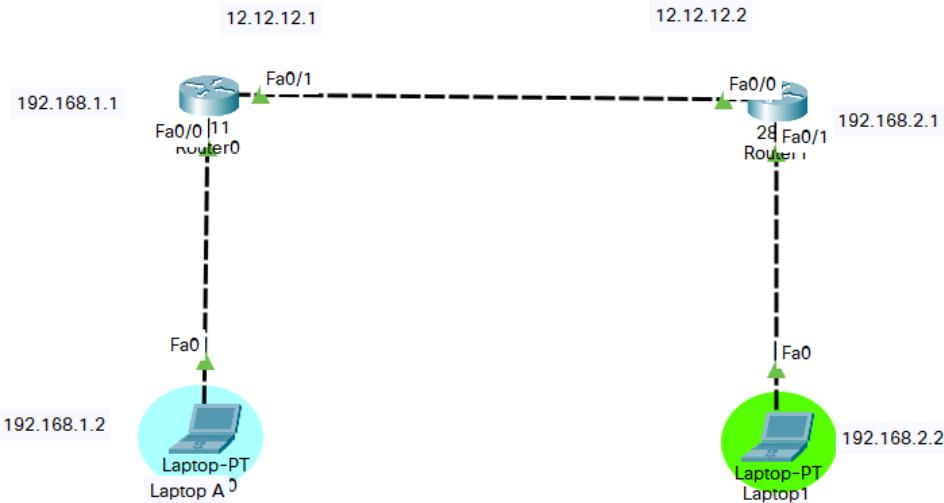
Metric adalah suatu nilai yang digunakan untuk mencapai suatu jaringan. Semakin nilai metrik maka akan memiliki jalur terbaik.

Beberapa jenis metric yang digunakan beberapa routing protokol adalah:

1. Hop count  
Metode ini menghitung jumlah router yang harus dilalui paket sebelum sampai ke tujuan. Setiap router bernilai satu hop
2. Bandwidth  
Penggunaan Bandwidth sebagai Metric hampir sama dengan penggunaan cost. Protocol Routing akan menghitung bandwidth pada setiap path dan akan menjadikan path dengan bandwidth terbesar sebagai Best Path .
3. Cost  
Metric ini akan memberikan harga (cost) pada setiap Link yang ada dalam jaringan. Path yang memiliki Cost terkecil maka akan menjadi Best Path.
4. Load  
Jika Load dijadikan Metric maka protocol Routing akan menghitung beban dari setiap path dan akan menjadikan beban terkecil sebagai Best Path.
5. Delay  
Delay adalah waktu yang diperlukan untuk mengirimkan paket data dari setiap path, path dengan delay terkecil akan menjadi Best Path.
6. Reliability  
Reliability adalah nilai kehandalan dari sebuah Path, misalnya sering tidak terjadi Error atau kegagalan dalam link tersebut. Nilai reliability tertinggi akan menjadi Best Path.

## Lab 19. Static Route

Static route adalah routing yang path/jalurnya ditentukan oleh Network Administrator ke dalam router untuk menentukan bagaimana router akan sampai ke subnet tertentu dengan menggunakan jalur tertentu.



Berikut adalah Lab Static Routing, kita akan menghubungkan Router kiri dan Router kanan agar klien/PC dapat berkomunikasi.

Pertama-tama kita konfigurasikan hostname dan IP Address terlebih dahulu.

### A. Konfigurasi Router Kiri

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KIRI
R-KIRI(config)#interface fa0/1
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 12.12.12.1 255.255.255.0
R-KIRI(config)#interface fa0/0
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0
```

### B. Konfigurasi Router Kanan

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KANAN
R-KANAN(config)#interface fa0/1
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 12.12.12.1 255.255.255.0
R-KANAN(config)#interface fa0/0
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 192.168.1.1 255.255.255.0
```

Jika keduanya sudah, selanjutnya kita konfigurasi static route-nya

Berikut confignya :

Pada Router KIRI, kita konfigurasikan routing ke network 192.168.2.0 yaitu network PC pada Router KANAN.

Sementara pada Router KANAN, kita konfigurasikan routing ke network 192.168.1.0 yaitu network PC pada Router KIRI.

Router Kiri

```
R-KIRI(config)#ip route 192.168.2.0 255.255.255.0 12.12.12.2
```

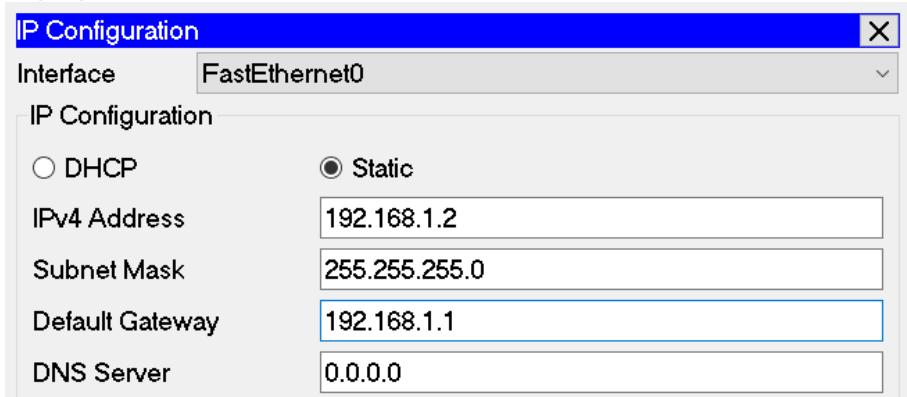
Router Kanan

```
R-KANAN(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
```

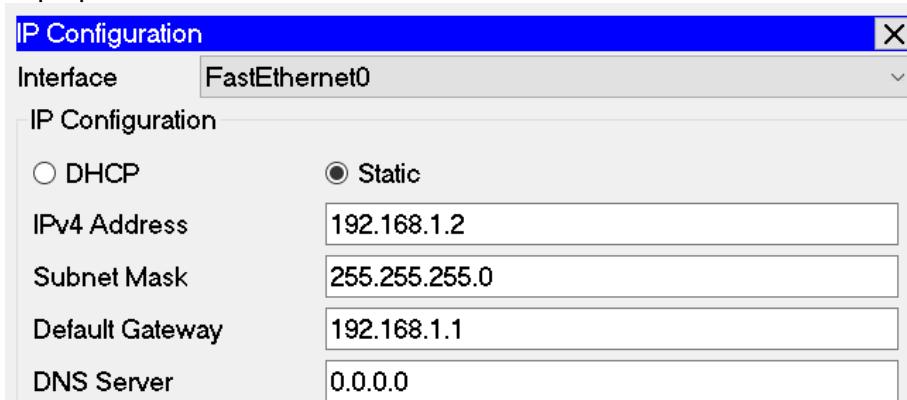
Ip route A.B.C.D (destination network/host) A.B.C.D (subnet mask) A.B.C.D (Next Hop/IP Tetangga )

#### C. Konfigurasi IP Address laptop

##### 1. Laptop A



##### 2. Laptop B



Untuk melihat routing table dan Admisitrative Distance suatu routing kita bisa menggunakan command, **do show ip route**

Router Kiri

```
R-KIRI(config)#do show ip route
```

```

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

Gateway of last resort is not set

      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, FastEthernet0/1
L        12.12.12.1/32 is directly connected, FastEthernet0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/0
L        192.168.1.1/32 is directly connected, FastEthernet0/0
S        192.168.2.0/24 [1/0] via 12.12.12.2

```

### Router Kanan

```

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

Gateway of last resort is not set

      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, FastEthernet0/0
L        12.12.12.2/32 is directly connected, FastEthernet0/0
S        192.168.1.0/24 [1/0] via 12.12.12.1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, FastEthernet0/1
L        192.168.2.1/32 is directly connected, FastEthernet0/1

```

Untuk Static Routing, ditandai dengan "S" dan Administravite Distancenya "1", Untuk pengetesan, coba lakukan PING laptop kiri dan laptop kanan, pastikan reply.

```

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=20ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=21ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126

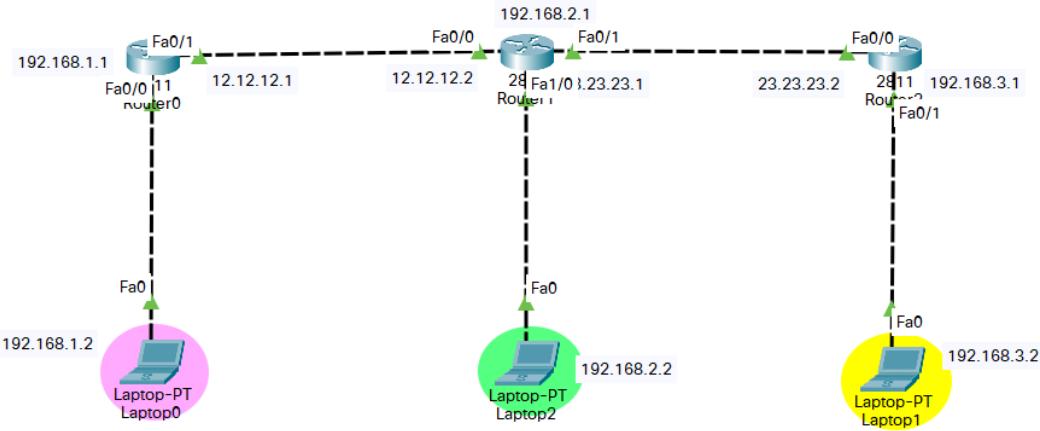
Ping statistics for 192.168.2.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 21ms, Average = 10ms

```

D. Lab Static Route 1<sup>st</sup> telah selesai

## Lab 20. Static Routing 2<sup>nd</sup>

Selanjutnya kita akan membahas static routing lagi, namun dengan lab yang berbeda. Di lab kali ini, kita akan menghubungkan antar PC yang terdapat pada tiap router



Pertama-tama kita konfigurasikan hostname dan IP Address terlebih dahulu.

### A. Konfigurasi Router kiri

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KIRI
R-KIRI(config)#interface fa0/1
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 12.12.12.1 255.255.255.0
R-KIRI(config)#interface fa0/0
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0
```

### B. Konfigurasi Router tengah

```
Router>enable
Router#configure terminal
Router(config)#hostname R-TENGAH
R-TENGAH(config)#interface fa0/0
R-TENGAH(config)#no shutdown
R-TENGAH(config)#ip address 12.12.12.2 255.255.255.0
R-TENGAH(config)#interface fa1/0
R-TENGAH(config)#no shutdown
R-TENGAH(config)#ip address 192.168.2.1 255.255.255.0
R-TENGAH(config)#interface fa0/1
R-TENGAH(config)#no shutdown
R-TENGAH(config)#ip address 23.23.23.1 255.255.255.0
```

### C. Konfigurasi Router kanan

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KIRI
R-KIRI(config)#interface fa0/0
R-KIRI(config)#no shutdown
```

```
R-KANAN(config)#ip address 23.23.23.2 255.255.255.0
R-KANAN(config)#interface fa0/1
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 192.168.3.1 255.255.255.0
```

Selanjutnya kita konfigurasikan static routing pada tiap router

Router Kiri

```
R-KIRI(config)#ip route 23.23.23.0 255.255.255.0 12.12.12.2
R-KIRI(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.2
R-KIRI(config)#ip route 192.168.3.0 255.255.255.0 12.12.12.2
```

Router tengah

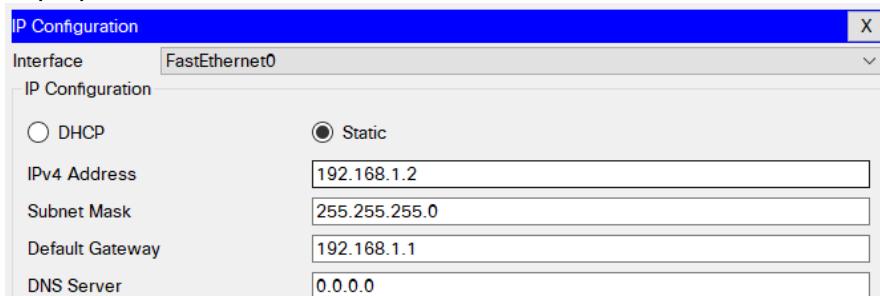
```
R-KANAN(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
R-KANAN(config)#ip route 192.168.3.0 255.255.255.0 23.23.23.2
```

Router Kiri

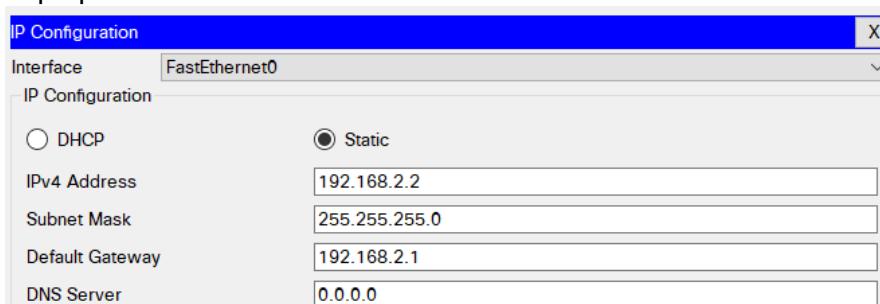
```
R-KANAN(config)#ip route 12.12.12.0 255.255.255.0 12.12.12.2
R-KANAN(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.2
R-KANAN(config)#ip route 192.168.2.0 255.255.255.0 12.12.12.2
```

D. Konfigurasi laptop untuk dipasang ip address dan ip gateway

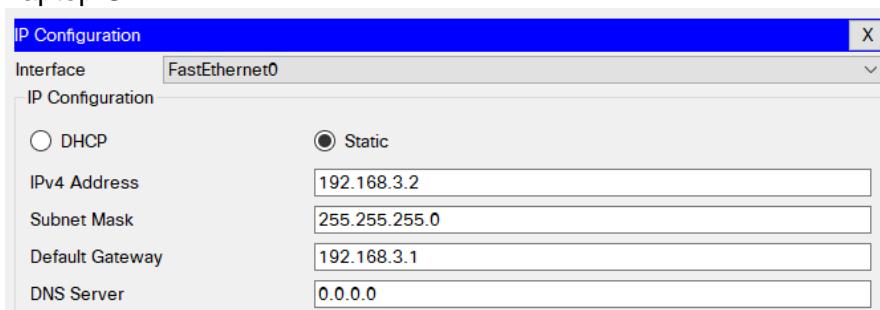
1. Laptop A



2. Laptop B



3. Laptop C



Untuk melihat routing table dan Admisitrative Distance suatu routing kita bisa menggunakan command, **do show ip route**

### Router Kiri

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

Gateway of last resort is not set

    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/24 is directly connected, FastEthernet0/1
L       12.12.12.1/32 is directly connected, FastEthernet0/1
    23.0.0.0/24 is subnetted, 1 subnets
S       23.23.23.0/24 [1/0] via 12.12.12.2
        192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/0
L       192.168.1.1/32 is directly connected, FastEthernet0/0
S       192.168.2.0/24 [1/0] via 12.12.12.2
S       192.168.3.0/24 [1/0] via 12.12.12.2
```

### Router Tengah

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

Gateway of last resort is not set

    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.12.12.0/24 is directly connected, FastEthernet0/0
L       12.12.12.2/32 is directly connected, FastEthernet0/0
    23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       23.23.23.0/24 is directly connected, FastEthernet0/1
L       23.23.23.1/32 is directly connected, FastEthernet0/1
S       192.168.1.0/24 [1/0] via 12.12.12.1
        192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, FastEthernet1/0
L       192.168.2.1/32 is directly connected, FastEthernet1/0
S       192.168.3.0/24 [1/0] via 23.23.23.2
```

### Router Kanan

```
R-KANAN(config)#do show ip route
```

```

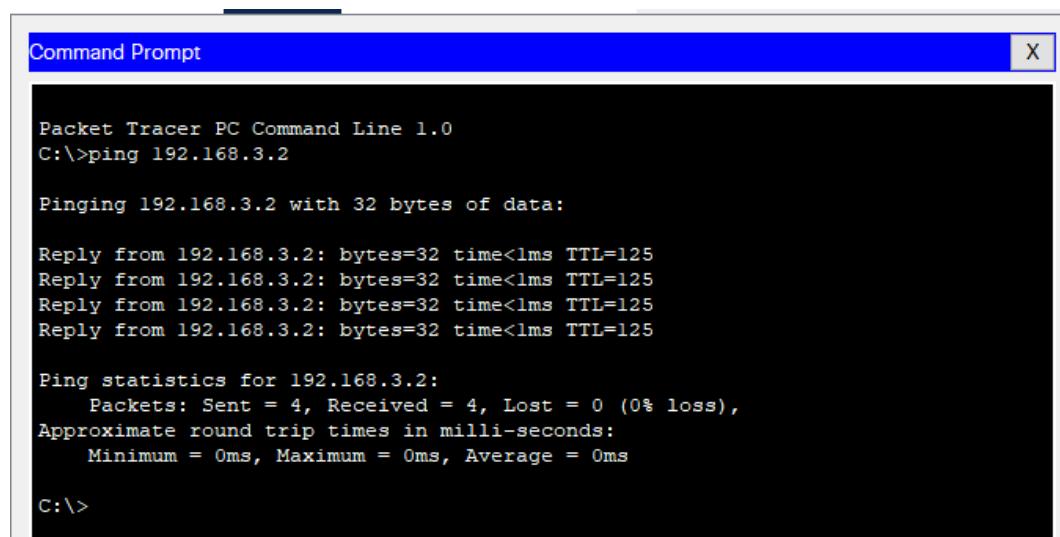
R-KANAN(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type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

Gateway of last resort is not set

      12.0.0.0/24 is subnetted, 1 subnets
S       12.12.12.0/24 [1/0] via 23.23.23.1
      23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         23.23.23.0/24 is directly connected, FastEthernet0/0
L         23.23.23.2/32 is directly connected, FastEthernet0/0
S       192.168.1.0/24 [1/0] via 23.23.23.1
S       192.168.2.0/24 [1/0] via 23.23.23.1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.3.0/24 is directly connected, FastEthernet0/1
L         192.168.3.1/32 is directly connected, FastEthernet0/1

```

Untuk pengetesan lakukan PING laptop kiri dan laptop kanan, pastikan reply



```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

E. Lab Static Routing 2<sup>nd</sup> telah selesai

## Lab 21. Dynamic Routing EIGRP

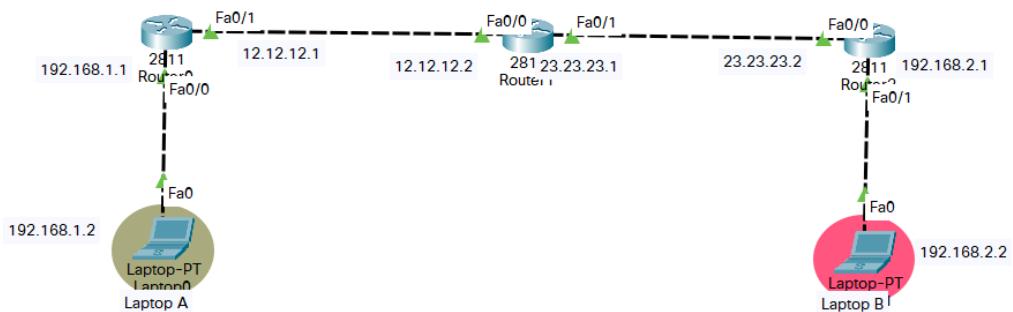
EIGRP (Enhanced Interior Gateway Routing Protocol) adalah routing protocol yang hanya digunakan oleh router Cisco atau sering disebut sebagai proprietary protocol pada CISCO. Dimana EIGRP ini hanya bisa digunakan sesama router CISCO saja dan routing ini tidak didukung dalam jenis router yang lain.

Router EIGRP juga termasuk kedalam router jenis Distance Vector protocol. Dalam pengertian bahwa routing EIGRP sebenarnya merupakan distance vector protocol tetapi prinsip kerjanya menggunakan link-states protocol. Sehingga EIGRP disebut sebagai Hybrid-distance-vector, mengapa dikatakan demikian karena prinsip kerjanya sama dengan link-states protocol yaitu mengirimkan semacam Hello Packet.

Dalam Static Routing tadi kita akan melakukan routing dengan cara mendaftarkan network yang tidak dimiliki sedangkan dynamic routing seperti EIGRP, kita akan mendaftarkan network yang dimiliki kedalam protocol routing atau biasa disebut dengan (Advertise Network).

### Kelebihan Routing EIGRP :

- Mendukung IP, IPX, dan AppleTalk melalui modul-modul yang bersifat protocol dependent
- Pencarian network tetangga yang dilakukan dengan efisien
- Komunikasi melalui Reliable Transport Protocol (RTP)
- Pemilihan jalur terbaik melalui Diffusing Update Algorithms (DUAL)



Berikut adalah Lab Dynamic Routing (EIGRP), kita akan menghubungkan Router kiri dan Router kanan agar klien/PC dapat berkomunikasi.

Pertama-tama kita konfigurasikan hostname dan IP Address terlebih dahulu

#### A. Konfigurasi Router Kiri

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KIRI
R-KIRI(config)#interface fa0/1
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 12.12.12.1 255.255.255.0
R-KIRI(config)#interface fa0/0
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0
```

## B. Konfigurasi Router Tengah

```
Router>enable
Router#configure terminal
Router(config)#hostname R-TENGAH
R-TENGAH(config)#interface fa0/0
R-TENGAH(config)#no shutdown
R-TENGAH(config)#ip address 12.12.12.2 255.255.255.0
R-TENGAH(config)#interface fa0/0
R-TENGAH(config)#no shutdown
R-TENGAH(config)#ip address 23.23.23.1 255.255.255.0
```

## C. Konfigurasi Router Kanan

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KANAN
R-KANAN(config)#interface fa0/0
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 23.23.23.2 255.255.255.0
R-KANAN(config)#interface fa0/1
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 192.168.2.1 255.255.255.0
```

Selanjutnya kita konfigurasikan EIGRP pada tiap router

Router Kiri

```
R-KIRI(config)#router eigrp 123
R-KIRI(config)#network 192.168.1.0 0.0.0.255
R-KIRI(config)#network 12.12.12.0 0.0.0.255
R-KIRI(config)#no auto-summary
```

Router Tengah

```
R-TENGAH(config)#router eigrp 123
R-TENGAH(config)#network 12.12.12.0 0.0.0.255
R-TENGAH(config)#network 23.23.23.0 0.0.0.255
R-TENGAH(config)#no auto-summary
```

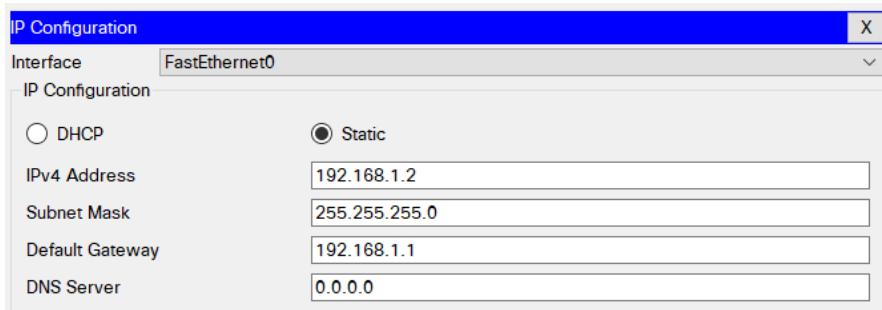
Router Kanan

```
R-KANAN(config)#router eigrp 123
R-KANAN(config)#network 23.23.23.0 0.0.0.255
R-KANAN(config)#network 192.168.2.0 0.0.0.255
R-KANAN(config)#no auto-summary
```

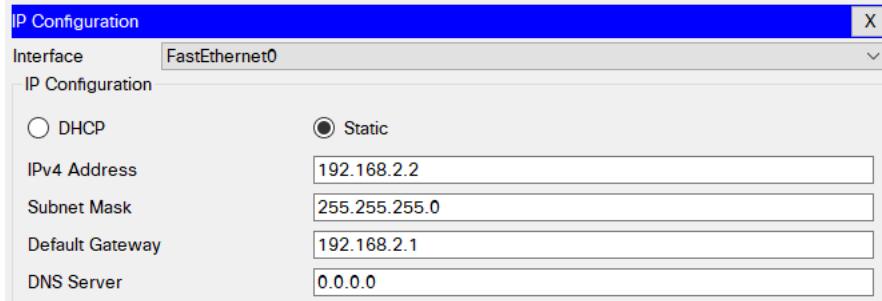
Maksud/Makna dari “no auto summary” adalah perintah agar IP tidak diringkas, perintah “router eigrp 123” adalah perintah untuk mengkonfigurasi route EIGRP “123” adalah nomor Administrative Distance (AD), kita harus sama saat memasukan AS number nya apabila berbeda maka router tidak akan bisa bertukar informasi routingnya.

## D. Konfigurasi IP Address di laptop

1. Laptop A



## 2. Laptop B



Setelah melakukan Routing EIGRP, kita bisa melakukan do show ip route, untuk melihat tabel routing router yang sudah menjalankan EIGRP.

### Router Kiri

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

Gateway of last resort is not set

      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, FastEthernet0/1
L        12.12.12.1/32 is directly connected, FastEthernet0/1
      23.0.0.0/24 is subnetted, 1 subnets
D        23.23.23.0/24 [90/30720] via 12.12.12.2, 00:46:34, FastEthernet0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/0
L        192.168.1.1/32 is directly connected, FastEthernet0/0
D        192.168.2.0/24 [90/33280] via 12.12.12.2, 00:46:34, FastEthernet0/1
```

### Router Tengah

```
R-TENGAH(config)#do show ip route
```

```

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

Gateway of last resort is not set

      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, FastEthernet0/0
L        12.12.12.2/32 is directly connected, FastEthernet0/0
      23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        23.23.23.0/24 is directly connected, FastEthernet0/1
L        23.23.23.1/32 is directly connected, FastEthernet0/1
D        192.168.1.0/24 [90/30720] via 12.12.12.1, 00:00:21, FastEthernet0/0
D        192.168.2.0/24 [90/30720] via 23.23.23.2, 00:00:21, FastEthernet0/1

```

### Router Kanan

```

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

Gateway of last resort is not set

      12.0.0.0/24 is subnetted, 1 subnets
D        12.12.12.0/24 [90/30720] via 23.23.23.1, 00:05:30, FastEthernet0/0
      23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        23.23.23.0/24 is directly connected, FastEthernet0/0
L        23.23.23.2/32 is directly connected, FastEthernet0/0
D        192.168.1.0/24 [90/33280] via 23.23.23.1, 00:05:30, FastEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, FastEthernet0/1
L        192.168.2.1/32 is directly connected, FastEthernet0/1

```

Untuk Routing EIGRP, ditandai dengan “D” dan Administravite Distancenya “9”, Untuk pengetesan, coba lakukan PING laptop kiri dan laptop kanan, pastikan reply.

```

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<lms TTL=125

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

```

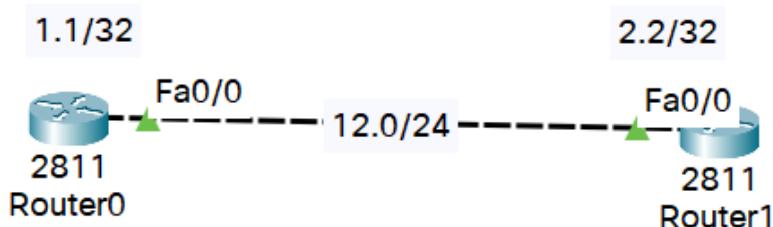
E. Lab Dynamic Routing EIGRP telah selesai

## Lab 22. EIGRP Authentication

EIGRP Authentication adalah jenis authnentifikasi & enskripsi yang cukup aman dan banyak digunakan oleh protocol routing. Authentifikasi di EIGRP biasa dikenal dengan MD5 Authentifikasi, sebenarnya jenis authentifikasi bisa digunakan oleh protocol EIGRP dan OSPF, namun kita akan mempraktekkannya di protocol routing EIGRP.

Sifat MD5 Authentication :

1. Authentication MD5 pasti dipasang pada interface router
2. Authentication protocol routing wajib peer to peer yang berarti wajib dipasang ke router tetangga dan harus sama.



Konfigurasi pertama yaitu mengganti hostname setelah itu memasang IP Address dan mengkonfigurasi interface loopback.

Langkah Langkah :

- A. Konfigurasi MD5 Authentication (Router Kiri)

```
R-KIRI(config)#key chain TKJ
R-KIRI(config)#key 1
R-KIRI(config)#key-string idn123

R-KIRI(config)#interface fa0/0
R-KIRI(config)#ip authentication mode eigrp 123 md5
R-KIRI(config)#ip authentication key-chain eigrp 123 TKJ
```

**Key chain TKJ** : Membuat nama authentication dengan nama TKJ

**Key 1** : Urutan nomor authentication (Nomor Bebas)

**Key-string idn123** : Membuat password pada authentication TKJ

**Interface fa0/0** : interface yang akan kita pilih untuk dikonfigurasi MD5

**ip authentication mode eigrp 123 md5** : Memasang MD5 pada EIGRP

**ip authentication key-chain eigrp 123 TKJ** : Memasang Authentication dengan chain yang sudah dibuat

- B. Konfigurasi MD5 Authentication (Router Kanan)

```
R-KIRI(config)#key chain TKJ
R-KIRI(config)#key 1
R-KIRI(config)#key-string idn123

R-KIRI(config)#interface fa0/0
R-KIRI(config)#ip authentication mode eigrp 123 md5
```

```
R-KIRI(config)#ip authentication key-chain eigrp 123 TKJ
```

Di router kanan perintahnya harus sama bedanya pada interface. interface yang digunakan adalah interface yang mengarah ke router peer to peer.

C. Lab EIGRP Authentication telah selesai

# EIGRP

packetlife.net

Protocol Header				Attributes
8	16	24	32	Type Distance Vector
Version	Opcode	Checksum		Algorithm DUAL
Flags				Internal AD 90
Sequence Number				External AD 170
Acknowledgment Number				Summary AD 5
Autonomous System Number				Standard Cisco proprietary
Type	Length			Protocols IP, IPX, Appletalk
Value				Transport IP/88
Metric Formula				Authentication MD5
$\frac{256 * (K_1 * \text{bw} + K_2 * \text{delay})}{256 - \text{load}} + K_3 * \text{delay} * \frac{K_5}{\text{rel} + K_4}$				Multicast IP 224.0.0.10
· bw = $10^7 / \text{minimum path bandwidth in kbps}$ · delay = interface delay in $\mu\text{secs} / 10$				Hello Timers 5/60
				Hold Timers 15/180
EIGRP Configuration				K Defaults
<pre> ! Enable EIGRP router eigrp &lt;ASN&gt;  ! Add networks to advertise network &lt;IP address&gt; &lt;wildcard mask&gt;  ! Configure K values to manipulate metric formula metric weights 0 &lt;k1&gt; &lt;k2&gt; &lt;k3&gt; &lt;k4&gt; &lt;k5&gt;  ! Disable automatic route summarization no auto-summary  ! Designate passive interfaces passive-interface (&lt;interface&gt;   default)  ! Enable stub routing eigrp stub [receive-only   connected   static   summary]  ! Statically identify neighboring routers neighbor &lt;IP address&gt; &lt;interface&gt; </pre>				Packet Types
				<b>K</b> <b>Defaults</b>
				<b>K<sub>1</sub></b> 1 <b>1</b> Update
				<b>K<sub>2</sub></b> 0 <b>3</b> Query
				<b>K<sub>3</sub></b> 1 <b>4</b> Reply
				<b>K<sub>4</sub></b> 0 <b>5</b> Hello
				<b>K<sub>5</sub></b> 0 <b>8</b> Acknowledge
Interface Configuration				Terminology
<pre> ! Set maximum bandwidth EIGRP can consume ip bandwidth-percent eigrp &lt;AS&gt; &lt;percentage&gt;  ! Configure manual summarization of outbound routes ip summary-address eigrp &lt;AS&gt; &lt;IP address&gt; &lt;mask&gt; [&lt;AD&gt;]  ! Enable MD5 authentication ip authentication mode eigrp &lt;AS&gt; md5 ip authentication key-chain eigrp &lt;AS&gt; &lt;key-chain&gt;  ! Configure hello and hold timers ip hello-interval eigrp &lt;AS&gt; &lt;seconds&gt; ip hold-time eigrp &lt;AS&gt; &lt;seconds&gt;  ! Disable split horizon for EIGRP no ip split-horizon eigrp &lt;AS&gt; </pre>				Reported Distance
				The metric for a route advertised by a neighbor
Protocol Configuration				Feasible Distance
<pre> ! Enable EIGRP router eigrp &lt;ASN&gt;  ! Add networks to advertise network &lt;IP address&gt; &lt;wildcard mask&gt;  ! Configure K values to manipulate metric formula metric weights 0 &lt;k1&gt; &lt;k2&gt; &lt;k3&gt; &lt;k4&gt; &lt;k5&gt;  ! Disable automatic route summarization no auto-summary  ! Designate passive interfaces passive-interface (&lt;interface&gt;   default)  ! Enable stub routing eigrp stub [receive-only   connected   static   summary]  ! Statically identify neighboring routers neighbor &lt;IP address&gt; &lt;interface&gt; </pre>				The distance advertised by a neighbor plus the cost to get to that neighbor
Stub Router				Stuck In Active (SIA)
				The condition when a route becomes unreachable and not all queries for it are answered; adjacencies with unresponsive neighbors are reset
Passive Interface				Passive Interface
				An interface which does not participate in EIGRP but whose network is advertised
Troubleshooting				Stub Router
				A router which advertises only a subset of routes, and is omitted from the route query process
<pre> show ip eigrp interfaces show ip eigrp neighbors show ip eigrp topology show ip eigrp traffic clear ip eigrp neighbors debug ip eigrp [packet   neighbors] </pre>				Troubleshooting

by Jeremy Stretch

v2.1

## OSPF Introduction

OSPF merupakan singkatan dari Open Shortest Path First. Sebuah routing protokol yang ber algoritma Djikstra.

OSPF mempunyai fitur-fitur :

- Terbagi menjadi area area dan Process-ID
- meminimalkan routing update traffic
- Allows scalability • Supports VLSM/CIDR
- Unlimited hop count
- Open Standard/ multi-vendor deployment

OSPF adalah link-state routing protocol, Router tahu persis topologi dari network sehingga memperkecil kesalahan dalam keputusan melakukan routing.

OSPF punya banyak features dan semua itu untuk menjadikan protocol yang cepat dan scalable. OSPF idealnya di desain secara hierarchical, yang intinya kita dapat membagi network yang besar kedalam network yang lebih kecil disebut area.

Alasan OSPF di desain secara hierarchical :

- Menurunkan routing overhead
- Mempercepat convergence
- membatasi network yang tidak stabil agar tidak menyebar ke area yang lain.

OSPF menggunakan Cost untuk menentukan jalur terbaiknya rumusnya : reference bandwidth / bandwidth yang di konfigur di interface dalam kbps di Cisco routers, default reference bandwidth 100000 kbps.

## OSPF Packet Type

Dalam pembentukan jaringan, OSPF menggunakan beberapa packet multicast khusus:

-**Hello**: sebagai neighbor discovery saat protokol berjalan dan sebagai penjaga stabilitas agar jaringan OSPF berjalan dengan baik.

-**DBD**: digunakan untuk mengecek LSDB jika ada ada 2 router yang sama. DBD merupakan ringkasan dari LSDB

-**LSR**: untuk meminta Link-State records yang spesifik

-**LSU**: untuk mengirim Link-State records yang diminta

-**LSA**: Dalam pembentukan jaringan, OSPF membuat paket yang bernama LSA yang berisi link/jalur yang dia ketahui dan dibagikan ke router lain sehingga dapat saling mengetahui

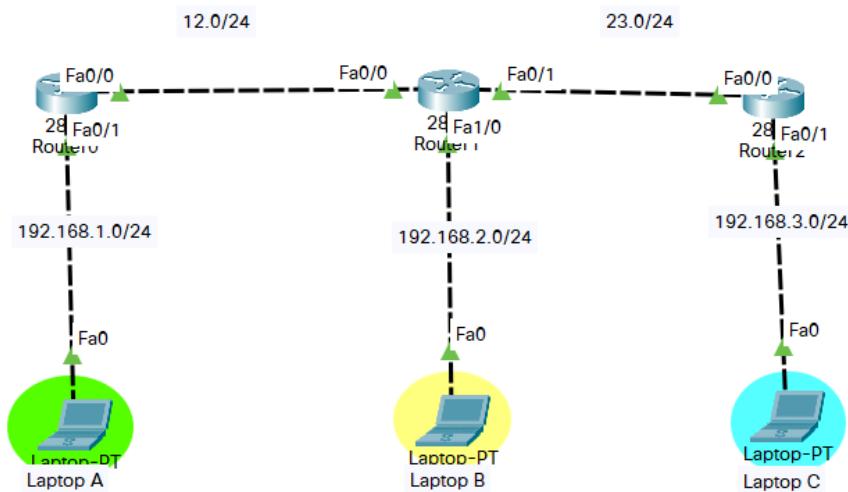
-**LSDB**: Setelah LSA terkumpul, maka akan diambilah jalur-jalur terbaik sehingga menghasilkan suatu database yang dinamakan LSDB

## Lab 23. Dynamic Routing OSPF (Backbone)

Area Backbone adalah area router yang bertanggung jawab mendistribusikan informasi routing antara non-backbone area. Semua sub-area harus terhubung dengan backbone secara logical.

Backbone :

1. Pusat dari area OSPF
2. Penghubung antar area
3. Non Backbone (Selain Backbone)



Berikut adalah Lab Dynamic Routing (OSPF), kita akan memasukan semua router kedalam area backbone.

Langkah Langkah :

A. Konfigurasi OSPF Router Kiri

```
R-KIRI(config)#router ospf 1
R-KIRI(config)#network 192.168.1.0 0.0.0.255 area 0
R-KIRI(config)#network 12.12.12.0 0.0.0.255 area 0
```

B. Konfigurasi OSPF Router Kanan

```
R-TENGAH(config)#router ospf 1
R-TENGAH(config)#network 192.168.2.0 0.0.0.255 area 0
R-TENGAH(config)#network 12.12.12.0 0.0.0.255 area 0
R-TENGAH(config)#network 23.23.23.0 0.0.0.255 area 0
```

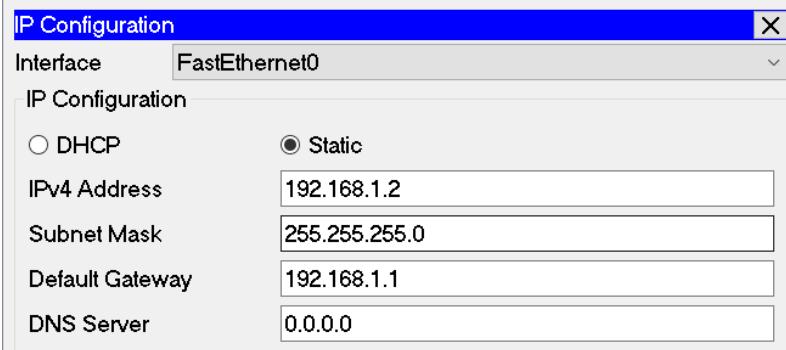
C. Konfigurasi OSPF Router Kanan

```
R-KANAN(config)#router ospf 1
R-KANAN(config)#network 192.168.3.0 0.0.0.255 area 0
R-KANAN(config)#network 23.23.23.0 0.0.0.255 area 0
```

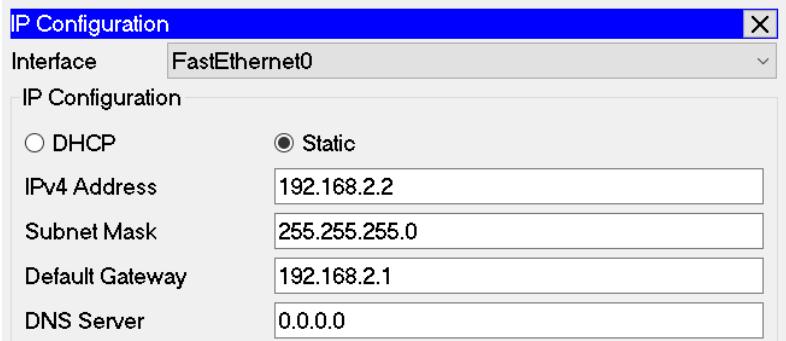
Pada OSPF dan EIGRP, digunakan wildcard mask, wildcard mask merupakan kebalikan dari subnet mask. Rumus **wildcard mask 255-Oktet terakhir subnet**, misalkan kita menggunakan prefix 25 yang subnetnya 255.255.255.128 maka wildcard masknya adalah  $255 - 128 = 127$

## D. Konfigurasi IP Address laptop

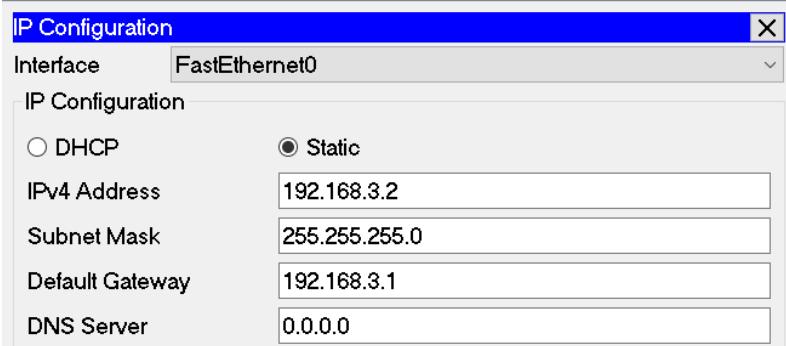
### 1. Laptop A



### 2. Laptop B



### 3. Laptop C



Setelah melakukan Routing OSPF, kita bisa melakukan pengecekan terhadap salah satu router yang telah menjalankan protocol OSPF, untuk melihat tabel routing router yang sudah menjalankan OSPF commandnya **do show ip route**

### Router Kiri

```
R-KIRI(config)#do show ip route
```

```

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

Gateway of last resort is not set

      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, FastEthernet0/0
L        12.12.12.1/32 is directly connected, FastEthernet0/0
      23.0.0.0/24 is subnetted, 1 subnets
O        23.23.23.0/24 [110/2] via 12.12.12.2, 00:27:43, FastEthernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/1
L        192.168.1.1/32 is directly connected, FastEthernet0/1
O        192.168.2.0/24 [110/2] via 12.12.12.2, 00:27:43, FastEthernet0/0
O        192.168.3.0/24 [110/3] via 12.12.12.2, 00:27:33, FastEthernet0/0

```

Kode huruf O adalah Route untuk OSPF satu area, 110 adalah Admistrative Distance dari OSPF, 2 adalah COST ke tujuan rumus dari OSPF cost adalah **[reference bandwidth / configured bandwidth of interface in kbps]**.

```

R-KIRI(config)#do show ip ospf neighbor

Neighbor ID      Pri   State          Dead Time     Address           Interface
192.168.2.1       1     FULL/DR      00:00:38      12.12.12.2

```

```

R-KIRI(config)#do show ip ospf database
              OSPF Router with ID (1.1.1.1) (Process ID 1)

              Router Link States (Area 0)

Link ID        ADV Router      Age        Seq#      Checksum Link count
1.1.1.1        1.1.1.1        1618      0x80000005 0x00aad7 2
192.168.3.1    192.168.3.1    1614      0x80000005 0x00cla8 2
192.168.2.1    192.168.2.1    1613      0x80000007 0x00fd12 3

              Net Link States (Area 0)
Link ID        ADV Router      Age        Seq#      Checksum
12.12.12.2     192.168.2.1    1617      0x80000002 0x009f40
23.23.23.2     192.168.3.1    1614      0x80000002 0x002039

```

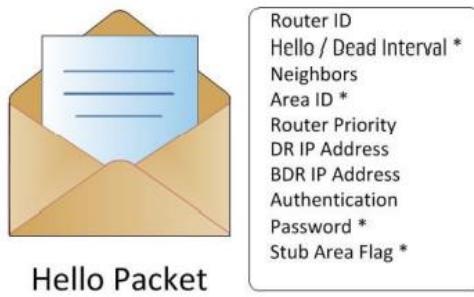
#### Cara Kerja OSPF :

Setelah melakukan LAB diatas, terdapat banyak sekali cara kerja OSPF, akan kita bahas semuanya :

Pada OSPF terdapat 7 keadaan sebelum akhirnya bisa menjadi neighbor :

1. **Down** -> Tidak terdapat OSPF neighbor saat itu.
2. **Init** -> Hello Packet diterima.
- Two-way** -> Terdapat router-id pada hello packet
3. **Exstart** -> Pembentukan role pada OSPF (DR, BDR)
4. **Exchange** -> Database Description Packet (DBD) telah dikirim secara multicast kesemua router OSPF
5. **Loading** -> Pertukaran packet dari LSR (Link State Requests) dan LSU (Link State Update) Full : Router OSPF sekarang sudah terbentuk sebagai adjacency.

Dari pembahasan neighbor discovery diatas, kita dapat melihat bahwa ada istilah Hello packet. Hello packet sendiri merupakan salah satu OSPF packet yang berperan sangat penting agar sebuah topologi OSPF bisa terbentuk.



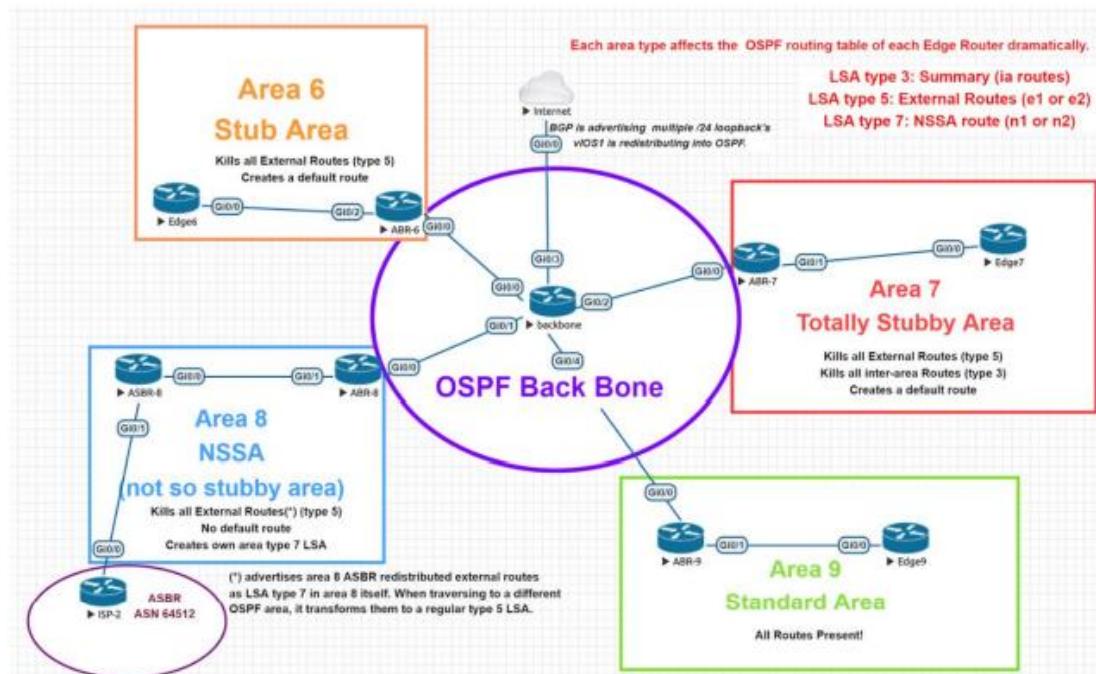
Nantinya setiap hello packet akan membawa informasi seperti pada ilustrasi disamping. Banyak informasi yang dibawa oleh hello packet ini, tapi yang bisa kita highlight untuk saat ini ialah Router ID, Hello/Dead Interval, Area ID.

**Router ID** – merupakan identitas unik dari sebuah router yang formatnya 32 bit (sama seperti IPv4). Router ID biasanya didapat dari IP loopback tertinggi atau jika tidak terdapat IP loopback, maka interface dengan IP tertinggilah yang akan dijadikan sebagai Router ID.

**Hello/Dead Interval** – (Hello timer) berapa kali paket hello akan dikirimkan, dan jika dalam beberapa detik tidak mengirimkan sebuah Hello paket maka neighbor akan dinyatakan down (Dead timer).

**Area ID** – Informasi area dari router yang mengirimkan hello paket. Area ID harus sama dengan router tetangganya.

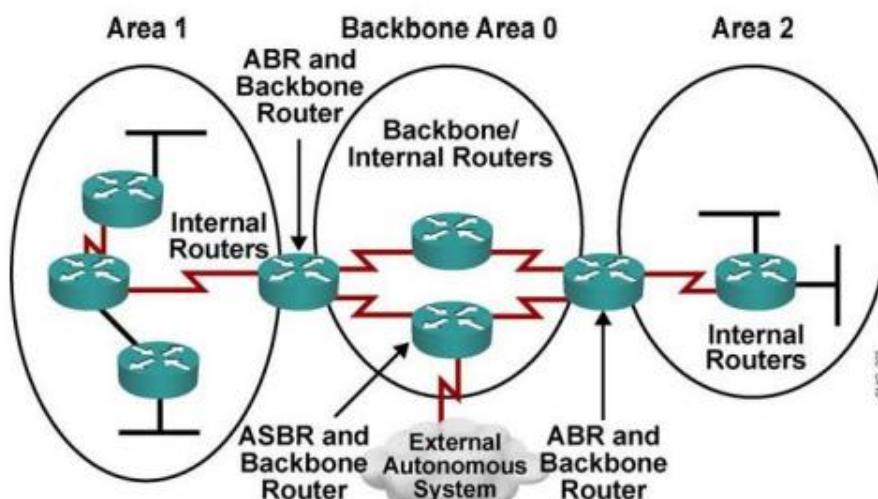
## OSPF Area Type



Pada OSPF, konektivitas networknya dibagi di tiap jaringan, terdapat beberapa tipe area pada OSPF seperti berikut.

- **Backbone - Area 0 (Area ID 0.0.0.0)** -> Bertanggung jawab mendistribusikan informasi routing antara non-backbone area. Semua sub-Area harus terhubung dengan backbone secara logikal.
- **Standart/Default Area** -> Merupakan sub-Area dari Area 0. Area ini menerima LSA intra-area dan inter-area dar ABR yang terhubung dengan area 0 (Backbone area).
- **Stub Area** -> Area yang paling "ujung". Area ini tidak menerima advertise external route (digantikan default area).
- **Not So Stubby Area (NSSA)** -> Stub Area yang tidak menerima external route (digantikan default route) dari area lain tetapi masih bisa mendapatkan external route dari router yang masih dalam 1 area.
- **Totally Stubby Area** -> Area ini lebih dari Stub area lain, dikarenakan selain tidak menerima external route dari area lain, ditambah tidak menerima external router dari luar. Sehingga router didalam area ini hanya mengenali router yang berada di area tersebut.

## OSPF Router Type



Dalam koneksi OSPF, terdapat sejumlah tipe router tertentu yang bekerja. Berikut tipe router dalam OSPF.

- **IR (Internal Router)** adalah router yang tergabung dalam sebuah area, jumlah maksimal IR dalam satu area adalah 80 router.
- **ABR (Area Border Router)** adalah router yang menjembatani area satu dengan area yang lain.
- **ASBR (Autonomous System Border Router)** adalah sebuah router yang terletak di perbatasan sebuah AS (Router terluar dari sebuah AS) dan bertugas untuk menjembatani antara router yang ada di dalam AS dengan Network lain (Berbeda AS).
- **ASBR** juga bisa berarti sebuah router anggota OSPF yang menjembatani routing OSPF dengan Routing protocol yang lain (RIP, BGP dll)

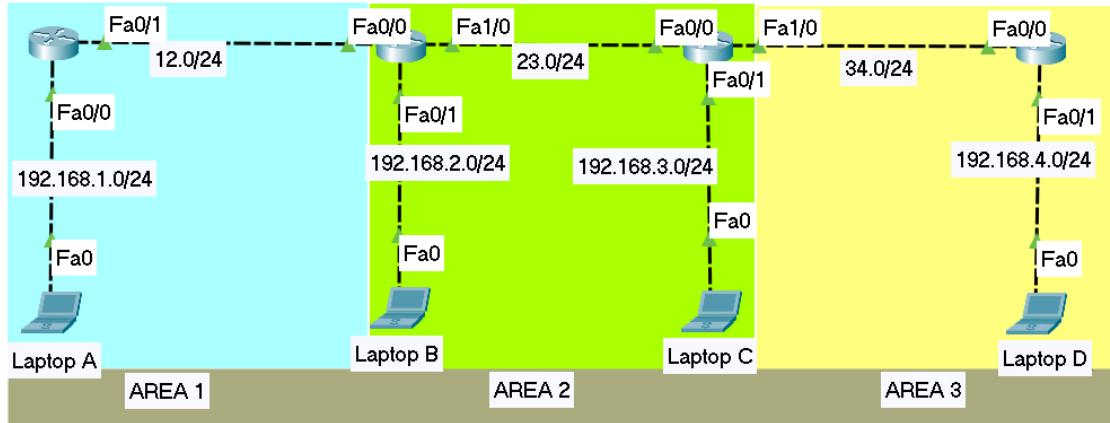
## **DR/BDR**

Dalam jaringan OSPF, DR (Designated Router) dan BDR (Backup Designated Router) sangatlah diperlukan. DR dan BDR akan menjadi pusat komunikasi seputar informasi OSPF dalam jaringan tersebut. Semua paket pesan yang ada dalam proses OSPF akan disebarluaskan oleh DR dan BDR.

Router dengan nilai Priority tertinggi akan menang dalam pemilihan dan langsung menjadi DR. Router dengan nilai Priority di urutan kedua akan dipilih menjadi BDR. Secara default, semua router OSPF akan memiliki nilai Priority 1. Range Priority ini adalah mulai dari 0 hingga 255. Nilai 0 akan menjamin router tersebut tidak akan menjadi DR atau BDR, sedangkan nilai 255 menjamin router untuk menjadi DR.

## Lab 24. Dynamic Routing OSPF (Non Backbone)

Area Non Backbone adalah area router selain Area Backbone, yaitu area ini bukan area pusat dari OSPF, bukan juga penghubung antar area, intinya bukan OSPF yang diarea 0, kalau area itu 0 maka itu bukan termasuk Area Non Backbone melainkan Area Backbone.



Berikut adalah Lab Dynamic Routing (OSPF), kita akan memasukan semua router kedalam area non-backbone.

Langkah Langkah :

- Konfigurasi OSPF Router 1

```
R-1 (config)#router ospf 1  
R-1(config)#network 192.168.1.0 0.0.0.255 area 1  
R-1(config)#network 12.12.12.0 0.0.0.255 area 1
```

- Konfigurasi OSPF Router 2

```
R-2(config)#router ospf 1  
R-2(config)#network 192.168.2.0 0.0.0.255 area 2  
R-2(config)#network 12.12.12.0 0.0.0.255 area 1  
R-2(config)#network 23.23.23.0 0.0.0.255 area 2
```

- Konfigurasi OSPF Router 3

```
R-3(config)#router ospf 1  
R-3(config)#network 192.168.3.0 0.0.0.255 area 2  
R-3(config)#network 23.23.23.0 0.0.0.255 area 2  
R-3(config)#network 34.34.34.0 0.0.0.255 area 3
```

- Konfigurasi OSPF Router 4

```
R-3(config)#router ospf 1  
R-3(config)#network 192.168.4.0 0.0.0.255 area 3  
R-3(config)#network 34.34.34.0 0.0.0.255 area 3
```

- Konfigurasi laptop untuk dipasang ip address dan ip gateway

- Laptop A

**IP Configuration**

Interface FastEthernet0

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

2. Laptop B

**IP Configuration**

Interface FastEthernet0

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0

3. Laptop C

**IP Configuration**

Interface FastEthernet0

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.3.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
DNS Server	0.0.0.0

4. Laptop D

**IP Configuration**

Interface FastEthernet0

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.4.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.1
DNS Server	0.0.0.0

Setelah itu kita akan mengecek salah satu router apakah routing OSPF sudah berhasil dijalankan

**Router Kiri**

```
R-KIRI(config)#do show ip route
```

```

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

Gateway of last resort is not set

      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, FastEthernet0/1
L        12.12.12.1/32 is directly connected, FastEthernet0/1
23 0 0 0/24 is subnetted, 1 subnets
O IA    23.23.23.0/24 [110/2] via 12.12.12.2, 00:20:56, FastEthernet0/1
34 0 0 0/24 is subnetted, 1 subnets
O IA    34.34.34.0/24 [110/3] via 12.12.12.2, 00:20:56, FastEthernet0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/0
I        192.168.1.1/32 is directly connected, FastEthernet0/0
O IA    192.168.2.0/24 [110/2] via 12.12.12.2, 00:20:56, FastEthernet0/1
O IA    192.168.3.0/24 [110/3] via 12.12.12.2, 00:20:56, FastEthernet0/1
O IA    192.168.4.0/24 [110/4] via 12.12.12.2, 00:20:56, FastEthernet0/1

```

Kode **O IA** di atas adalah kode dimana router menjangkau network router lain yang berbeda area. Namun ketika area router itu **sama** kode itu tidak ada. Setelah itu kita akan melakukan pengetesan dengan melakukan PING dari R-1 Ke R-4, pastikan reply.

```

C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time<1ms TTL=124
Reply from 192.168.4.2: bytes=32 time<1ms TTL=124
Reply from 192.168.4.2: bytes=32 time=25ms TTL=124
Reply from 192.168.4.2: bytes=32 time=10ms TTL=124

Ping statistics for 192.168.4.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 25ms, Average = 8ms

```

## F. Lab Dynamic Routing OSPF Non Backbone telah selesai

# OSPF • PART 1

packetlife.net

Protocol Header				Attributes			
Version	Type	Length	Data	Type Link-State			
Router ID				Algorithm Dijkstra			
Area ID				Metric Cost (Bandwidth)			
Checksum	Instance ID	Reserved					
Data				AD 110			
Link State Advertisements				Standard RFC 2328, 2740			
<b>Router Link (Type 1)</b> Lists neighboring routers and the cost to each; flooded within an area				Protocols IP			
<b>Network Link (Type 2)</b> Generated by a DR; lists all routers on an adjacent segment; flooded within an area				Transport IP/89			
<b>Network Summary (Type 3)</b> Generated by an ABR and advertised among areas				Authentication Plaintext, MD5			
<b>ASBR Summary (Type 4)</b> Injected by an ABR into the backbone to advertise the presence of an ASBR within an area				AllSPF Address 224.0.0.5			
<b>External Link (Type 5)</b> Generated by an ASBR and flooded throughout the AS to advertise a route external to OSPF				AllDR Address 224.0.0.6			
<b>NSSA External Link (Type 7)</b> Generated by an ASBR in a not-so-stubby area; converted into a type 5 LSA by the ABR when leaving the area				Metric Formula			
				$\text{cost} = \frac{100,000 \text{ Kbps}^*}{\text{link speed}}$			
				* modifiable with <code>ospf auto-cost reference-bandwidth</code>			
Router Types				Adjacency States			
<b>Internal Router</b> All interfaces reside within the same area	Area Types			1 Down      5 Exstart			
<b>Backbone Router</b> A router with an interface in area 0 (the backbone)	<b>Standard Area</b> Default OSPF area type			2 Attempt    6 Exchange			
<b>Area Border Router (ABR)</b> Connects two or more areas	<b>Stub Area</b> External link (type 5) LSAs are replaced with a default route			3 Init       7 Loading			
<b>AS Boundary Router (ASBR)</b> Connects to additional routing domains; typically located in the backbone	<b>Totally Stubby Area</b> Type 3, 4, and 5 LSAs are replaced with a default route			4 2-Way     8 Full			
<b>Not So Stubby Area (NSSA)</b> A stub area containing an ASBR; type 5 LSAs are converted to type 7 within the area				DR/BDR Election			
				<ul style="list-style-type: none"> <li>The DR serves as a common point for all adjacencies on a multiaccess segment</li> <li>The BDR also maintains adjacencies with all routers in case the DR fails</li> <li>Election does not occur on point-to-point or multipoint links</li> <li>Default priority (0-255) is 1; highest priority wins; 0 cannot be elected</li> <li>DR preemption will not occur unless the current DR is reset</li> </ul>			
External Route Types				Virtual Links			
<b>E1</b> · Cost to the advertising ASBR plus the external cost of the route				<ul style="list-style-type: none"> <li>Tunnel formed to join two areas across an intermediate</li> </ul>			
<b>E2 (Default)</b> · Cost of the route as seen by the ASBR				<ul style="list-style-type: none"> <li>Both end routers must share a common area</li> <li>At least one end must reside in area 0</li> <li>Cannot traverse stub areas</li> </ul>			
Troubleshooting							
show ip [route   protocols]	show ip ospf border-routers						
show ip ospf interface	show ip ospf virtual-links						
show ip ospf neighbor	debug ip ospf [...]						

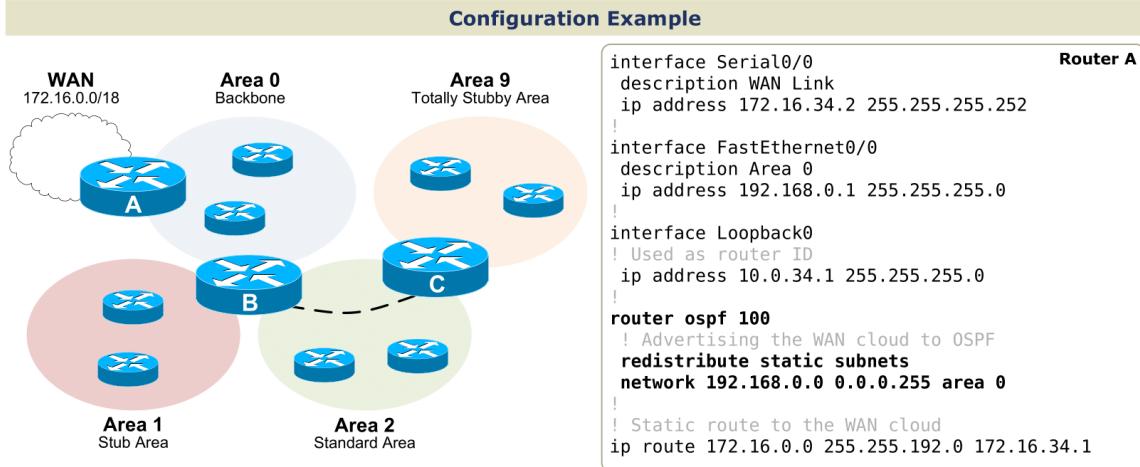
by Jeremy Stretch

v2.1

# OSPF • PART 2

packetlife.net

	Network Types				
	Nonbroadcast (NBMA)	Multipoint Broadcast	Multipoint Nonbroadcast	Broadcast	Point-to-Point
<b>DR/BDR Elected</b>	Yes	No	No	Yes	No
<b>Neighbor Discovery</b>	No	Yes	No	Yes	Yes
<b>Hello/Dead Timers</b>	30/120	30/120	30/120	10/40	10/40
<b>Defined By</b>	RFC 2328	RFC 2328	Cisco	Cisco	Cisco
<b>Supported Topology</b>	Full Mesh	Any	Any	Full Mesh	Point-to-Point



Router A	Router B	Router C
<pre> interface Serial0/0 description WAN Link ip address 172.16.34.2 255.255.255.252  interface FastEthernet0/0 description Area 0 ip address 192.168.0.1 255.255.255.0  interface Loopback0 ! Used as router ID ip address 10.0.34.1 255.255.255.0  router ospf 100 ! Advertising the WAN cloud to OSPF redistribute static subnets network 192.168.0.0 0.0.0.255 area 0 ! ! Static route to the WAN cloud ip route 172.16.0.0 255.255.192.0 172.16.34.1 </pre>	<pre> interface Ethernet0/0 description Area 0 ip address 192.168.0.2 255.255.255.0 ip ospf 100 area 0 ! interface Ethernet0/1 description Area 2 ip address 192.168.2.1 255.255.255.0 ip ospf 100 area 2 ! Optional MD5 authentication configured ip ospf authentication message-digest ip ospf message-digest-key 1 md5 FooBar ! Give B priority in DR election ip ospf priority 100 ! interface Ethernet0/2 description Area 1 ip address 192.168.1.1 255.255.255.0 ip ospf 100 area 1 ! interface Loopback0 ip address 10.0.34.2 255.255.255.0 ! router ospf 100 ! Define area 1 as a stub area area 1 stub ! Virtual link from area 0 to area 9 area 2 virtual-link 10.0.34.3 </pre>	<pre> interface Ethernet0/0 description Area 9 ip address 192.168.9.1 255.255.255.0 ip ospf 100 area 9 ! interface Ethernet0/1 description Area 2 ip address 192.168.2.2 255.255.255.0 ip ospf 100 area 2 ! Optional MD5 authentication configured ip ospf authentication message-digest ip ospf message-digest-key 1 md5 FooBar ! Give C second priority (BDR) in election ip ospf priority 50 ! ! ! ! interface Loopback0 ip address 10.0.34.3 255.255.255.0 ! router ospf 100 ! Define area 9 as a totally stubby area area 9 stub no-summary ! Virtual link from area 9 to area 0 area 2 virtual-link 10.0.34.2 </pre>

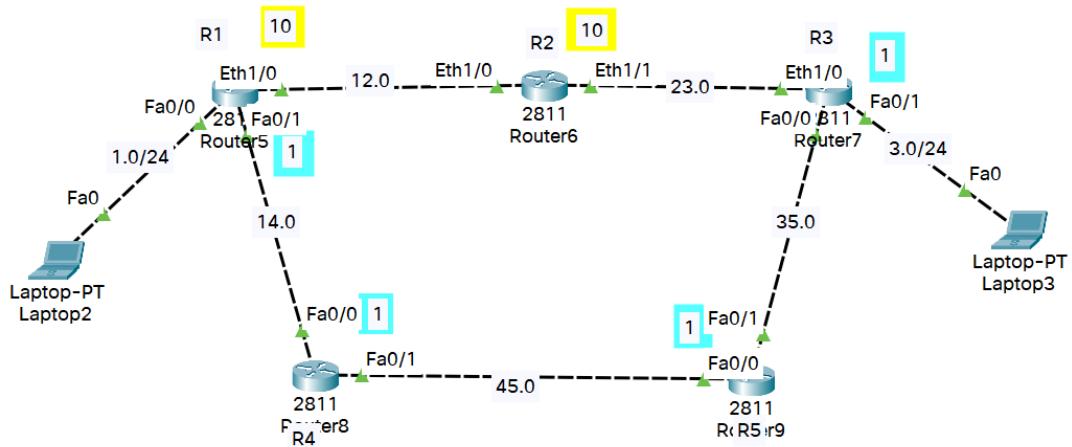
by Jeremy Stretch

v2.1

## Lab 25. OSPF Traffic Routing

Pada lab kali ini, kita akan membahas tentang OSPF Traffic Routing, yaitu kita akan membuktikan bahwa OSPF menentukan jalur utama pada jalur yang memiliki cost yang lebih kecil. Sebagaimana pada penjelasan lab sebelumnya.

Pada topology dibawah kita akan menggunakan satu jalur dimana jalur tersebut hanya berisi interface Ethernet dan satu jalur lagi akan menggunakan Fast Ethernet.



Seperti dengan lab-lab sebelumnya, kita akan melakukan konfigurasi IP Address terhadap masing-masing perangkat sesuai dengan topology.

Langkah Langkah :

### A. Konfigurasi IP Address R1

```
R1(config)#interface range fa0/0-1
R1(config-if-range)#no shutdown
R1(config-if-range)#interface eth1/0
R1(config-if)#no shutdown
R1(config-if)#interface fa0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#interface fa0/1
R1(config-if)#ip add 14.14.14.1 255.255.255.0
R1(config-if)#interface eth1/0
R1(config-if)#ip add 12.12.12.1 255.255.255.0
```

### B. Konfigurasi IP Address R2

```
R2(config)#interface eth1/0
R2(config-if-range)#no shutdown
R2(config-if-range)#interface eth1/0
R2(config-if)#no shutdown
R2(config-if)#interface eth1/0
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#interface eth1/1
R2(config-if)#ip add 23.23.23.1 255.255.255.0
```

### C. Konfigurasi IP Address R3

```
R3(config)#interface eth1/0
R3(config-if-range)#no shutdown
R3(config-if-range)#interface fa0/1
R3(config-if)#no shutdown
```

```
R3(config-if)#interface eth1/0
R3(config-if)#ip add 23.23.23.2 255.255.255.0
R3(config-if)#interface fa0/1
R3(config-if)#ip add 192.168.3.1 255.255.255.0
```

D. Konfigurasi IP Address R4

```
R4(config)#interface fa0/0
R4(config-if-range)#no shutdown
R4(config-if-range)#interface fa0/1
R4(config-if)#no shutdown
R4(config-if)#interface fa0/0
R4(config-if)#ip add 14.14.14.2 255.255.255.0
R4(config-if)#interface fa0/1
R4(config-if)#ip add 45.45.45.1 255.255.255.0
```

E. Konfigurasi IP Address R4

```
R4(config)#interface fa0/0
R4(config-if-range)#no shutdown
R4(config-if-range)#interface fa0/1
R4(config-if)#no shutdown
R4(config-if)#interface fa0/0
R4(config-if)#ip add 45.45.45.2 255.255.255.0
R4(config-if)#interface fa0/1
R4(config-if)#ip add 35.35.35.1 255.255.255.0
```

Setelah menambahkan IP pada semua interface, langkah selanjutnya yaitu untuk melakukan routing OSPF dengan mendaftarkan network yang router miliki.

Routing OSPF R1

```
R1(config)#router ospf 10
R1(config)#network 192.168.1.0 0.0.0.255 area 0
R1(config)#network 12.12.12.0 0.0.0.255 area 0
```

Routing OSPF R2

```
R2(config)#router ospf 10
R2(config)#network 23.23.23.0.0.0.255 area 0
R2(config)#network 12.12.12.0 0.0.0.255 area 0
```

Routing OSPF R3

```
R3(config)#router ospf 10
R3(config)#network 23.23.23.0.0.0.255 area 0
R3(config)#network 192.168.3.0 0.0.0.255 area 0
```

Routing OSPF R4

```
R4(config)#router ospf 10
R4(config)#network 14.14.14.0.0.0.255 area 0
R4(config)#network 45.45.45.0 0.0.0.255 area 0
```

Routing OSPF R5

```
R5(config)#router ospf 10
R5(config)#network 45.45.45.0.0.0.255 area 0
R5(config)#network 35.35.35.0 0.0.0.255 area 0
```

Jika sudah melakukan konfigurasi diatas, selanjutnya kita akan mencoba traceroute dari **PC1** ke **PC2** agar jalur yang dilewati oleh packet terlihat.

#### Tracert PC1 > PC 2

```
C:\>tracert 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops:
1  0 ms      0 ms      0 ms      192.168.1.1
2  0 ms      0 ms      0 ms      14.14.14.2
3  0 ms      0 ms      1 ms      45.45.45.2
4  0 ms      0 ms      0 ms      35.35.35.2
5  10 ms     11 ms     11 ms     192.168.3.2

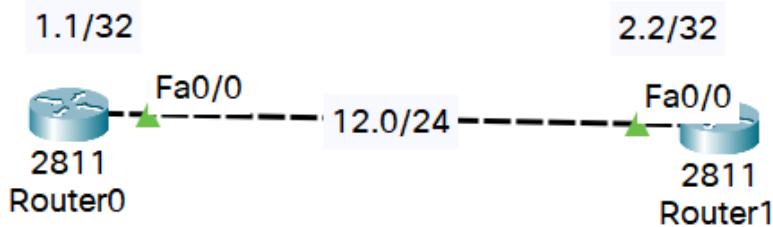
Trace complete.
```

Packet akan melewati jalur yang digunakan oleh Fast Ethernet karena Fast Ethernet memiliki cost lebih kecil dibandingkan dengan Ethernet.

- F. Lab OSPF Traffic Routing telah selesai

## Lab 26. OSPF Authentication

OSPF Authentication adalah jenis authnentifikasi & enskripsi yang cukup aman dan banyak digunakan oleh protocol routing. Authentifikasi di OSPF biasa dikenal dengan Plain text Authentifikasi, jenis authentifikasi ini digunakan untuk OSPF saja.



Konfigurasi pertama yaitu mengganti hostname setelah itu memasang IP Address dan mengkonfigurasi interface loopback.

Langkah Langkah :

- Konfigurasi OSPF Authentication (Router Kiri)

```
R-KIRI(config)#interface fa0/0
R-KIRI(config)#ip ospf authentication
R-KIRI(config)#ip ospf authentication-key TKJ
```

**Interface fa0/0** : interface yang akan kita konfigurasi plaintext authentifikasi

**Ip ospf authentication** : Perintah untuk membuat ospf authentifikasi jenis plaintext

**Ip ospf authentication-key TKJ** : Perintah untuk membuat ospf authentifikasi dengan nama TKJ

- Konfigurasi OSPF Authentication (Router Kanan)

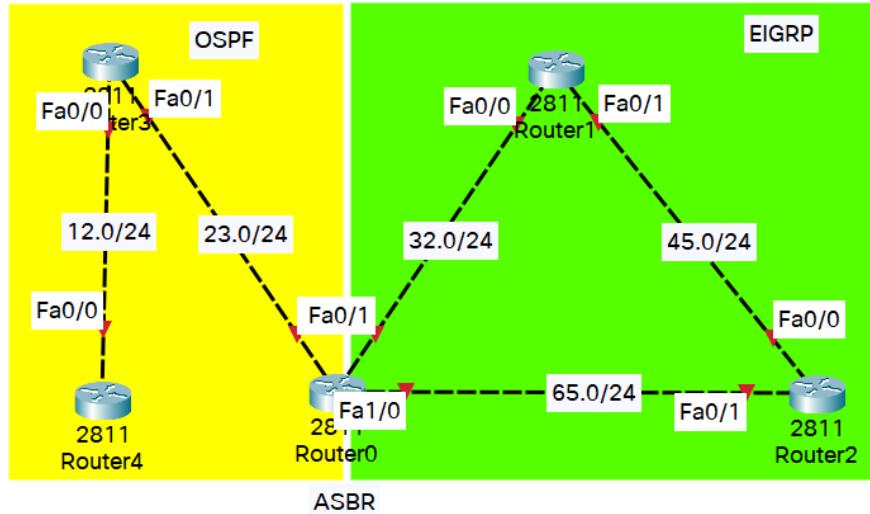
```
R-KANAN(config)#interface fa0/0
R-KANAN(config)#ip ospf authentication
R-KANAN(config)#ip ospf authentication-key TKJ
```

Di router kanan perintahnya harus sama bedanya pada interface. interface yang digunakan adalah interface yang mengarah ke router peer to peer.

- Lab OSPF Authentication telah selesai

## Lab 27. Redistribute EIGRP & OSPF

Fungsinya adalah untuk menghubungkan 2 protocol routing agar tabel routing saling sinkron dan terhubung. Contoh : Menghubungkan protocol routing EIGRP dan OSPF. Dikonfigurasikan hanya di router yang menjembatani antar protocol (Router ASBRI routing yang berarti 1 router tsb memiliki 2 protocol routing).



Kita akan mengkonfigurasi redistribute pada topologi diatas, tujuan kita agar kedua protocol bisa saling berkomunikasi.

Langkah Langkah :

- Konfigurasi Redistribute EIGRP Ke OSPF

```
R-ASBR(config)#router eigrp 123  
R-ASBR(config)#redistribute ospf 100 metric 1 1 1 1 1
```

**Router eigrp 123** : Jenis route yang akan kita redistribute  
**redistribute ospf 100 metric 1 1 1 1 1** : Meredistribute ke OSPF 100, metric 1 1 1 1 1 adalah K-Value.

- Konfigurasi Redistribute OSPF Ke EIGRP

```
R-ASBR(config)#router ospf 200  
R-ASBR(config)#redistribute eigrp 123 subnets
```

Perintahnya sama namun bedanya EIGRP Ke OSPF menggunakan **metric**, tapi kalau OSPF Ke EIGRP pake **subnets**.

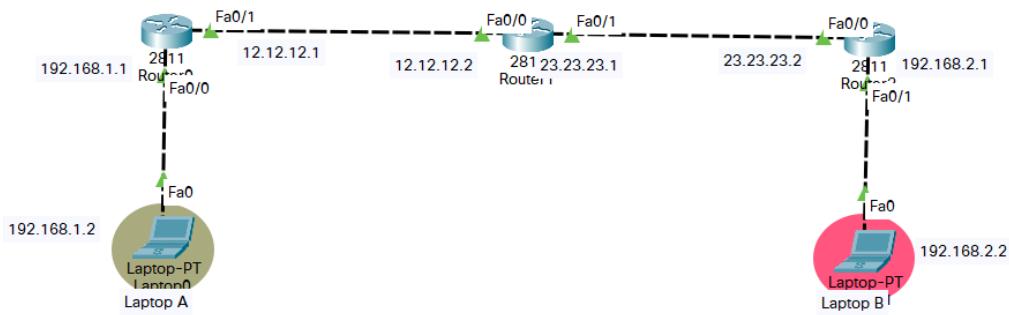
- Lab Redistribute EIGRP & OSPF telah selesai

## Lab 28. Dynamic Routing RIP

**Routing Information Protocol (RIP)** adalah sebuah protokol routing dinamis yang digunakan dalam jaringan LAN (Local Area Network) dan WAN (Wide Area Network). Oleh karena itu protokol ini diklasifikasikan sebagai Interior Gateway Protocol (IGP). Protoko routing ini menggunakan algoritme Distance-Vector Routing.

Ada 3 jenis protocol RIP :

1. RIPv1
2. RIPv2
3. RIPIpv6 (RIP-Next Generation)



Berikut adalah Lab Dynamic Routing (RIP), kita akan menghubungkan Router kiri dan Router kanan agar klien/PC dapat berkomunikasi.

Langkah Langkah :

A. Konfigurasi Router Kiri

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KIRI
R-KIRI(config)#interface fa0/1
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 12.12.12.1 255.255.255.0
R-KIRI(config)#interface fa0/0
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0
```

B. Konfigurasi Router Tengah

```
Router>enable
Router#configure terminal
Router(config)#hostname R-TENGAH
R-TENGAH(config)#interface fa0/0
R-TENGAH(config)#no shutdown
R-TENGAH(config)#ip address 12.12.12.2 255.255.255.0
R-TENGAH(config)#interface fa0/1
R-TENGAH(config)#no shutdown
R-TENGAH(config)#ip address 23.23.23.1 255.255.255.0
```

C. Konfigurasi Router Kanan

```
Router>enable
```

```
Router#configure terminal
Router(config)#hostname R-KANAN
R-KANAN(config)#interface fa0/0
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 23.23.23.2 255.255.255.0
R-KANAN(config)#interface fa0/1
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 192.168.2.1 255.255.255.0
```

Selanjutnya kita konfigurasikan EIGRP pada tiap router

Router Kiri

```
R-KIRI(config)#router rip
R-KIRI(config)#version 2
R-KIRI(config)#network 12.12.12.0
R-KIRI(config)#network 192.168.1.0
```

Router Tengah

```
R-TENGAH(config)#router rip
R-TENGAH(config)#version 2
R-TENGAH(config)#network 23.23.23.0
R-TENGAH(config)#network 12.12.12.0
```

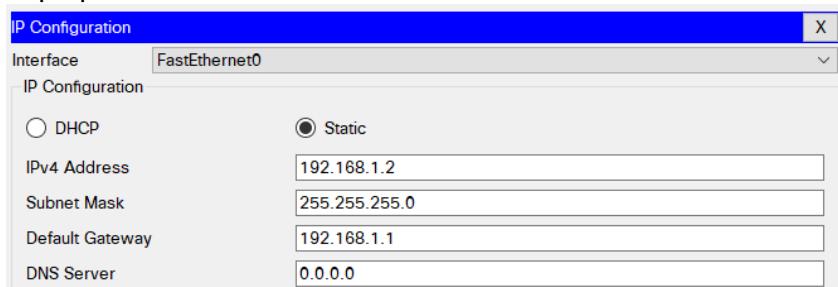
Router Kanan

```
R-KANAN(config)#router rip
R-KANAN(config)#version 2
R-KANAN(config)#network 23.23.23.0
R-KANAN(config)#network 192.168.2.0
```

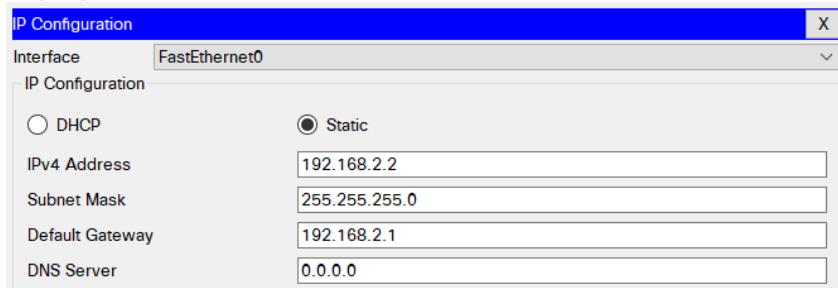
Maksud perintah “**router rip**” adalah kita mengaktifkan protocol routing RIP. “**version 2**” maksudnya mengaktifkan protocol routing RIP versi 2, untuk protocol routing RIP tidak menggunakan wildcard mask jadi mencantumkan IP Networknya saja.

#### D. Konfigurasi IP Address di laptop

##### 1. Laptop A



##### 3. Laptop B



Setelah melakukan Routing EIGRP, kita bisa melakukan **do show ip route**, untuk melihat tabel routing router yang sudah menjalankan EIGRP.

### Router Kiri

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

Gateway of last resort is not set

      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, FastEthernet0/1
L        12.12.12.1/32 is directly connected, FastEthernet0/1
R  23.0.0.0/8 [120/1] via 12.12.12.2, 00:00:05, FastEthernet0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/0
L        192.168.1.1/32 is directly connected, FastEthernet0/0
```

### Router Tengah

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

Gateway of last resort is not set

      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, FastEthernet0/0
L        12.12.12.2/32 is directly connected, FastEthernet0/0
      23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        23.23.23.0/24 is directly connected, FastEthernet0/1
L        23.23.23.1/32 is directly connected, FastEthernet0/1
R  192.168.1.0/24 [120/1] via 12.12.12.1, 00:00:00, FastEthernet0/0
```

### Router Kanan

```
R-KANAN(config)#do show ip route
```

```

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

Gateway of last resort is not set

R    12.0.0.0/8 [120/1] via 23.23.23.1, 00:00:15, FastEthernet0/0
      23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        23.23.23.0/24 is directly connected, FastEthernet0/0
L        23.23.23.2/32 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/2] via 23.23.23.1, 00:00:15, FastEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, FastEthernet0/1
L        192.168.2.1/32 is directly connected, FastEthernet0/1

```

Untuk Routing RIP, ditandai dengan “R” dan Administravite Distancenya “120”, Untuk pengetesan, coba lakukan PING laptop kiri dan laptop kanan, pastikan reply.

```

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<lms TTL=125

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

```

## E. Lab Dynamic Routing EIGRP telah selesai

# Access List

# **ACCESS LIST**

**CONTENT :**

**STANDARD ACCESS LIST**

**EXTENDED ACCESS LIST**

**NAMED EXTENDED ACCESS LIST**

## Access-List Introduction

Dalam sebuah jaringan, kita dapat melakukan sebuah penyaringan packet yang berjalan melewati router, dengan adanya penyaringan ini, kita dapat mengatur packet mana yang boleh lewat dan yang tidak.

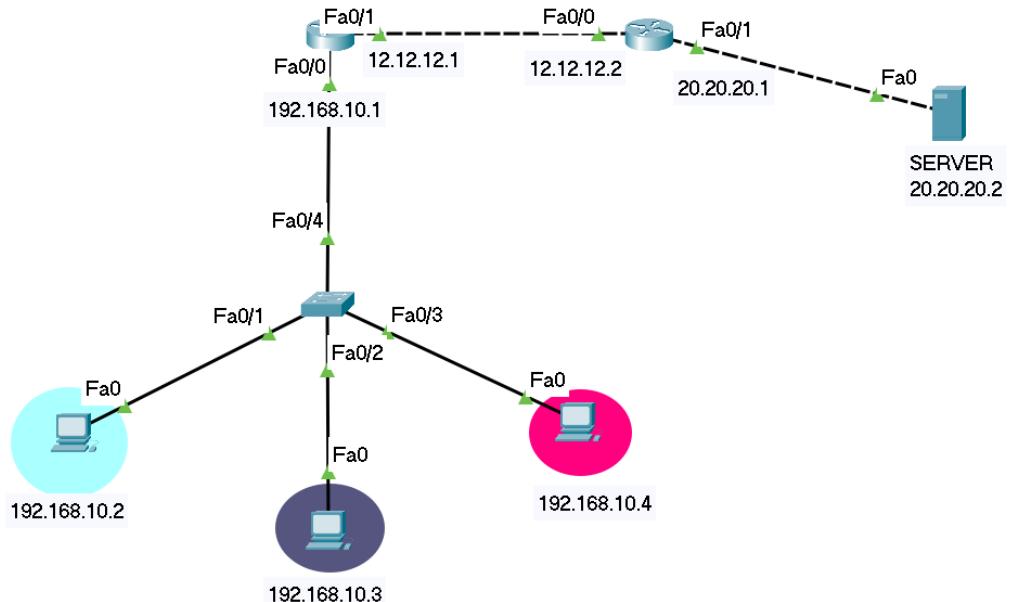
ACL terbagi menjadi 2, Standard Access List dan Extended Access List, yang tiap Access List memiliki keunggulan dan perbedaannya.

Berikut perbedaan pada Standard Access List dan Extended Access List: Standard Access List Extended Access List :

Standard Access List	Extended Access List
Nomer ACL antara 1-99	Nomer ACL antara 100-199
Bisa memblokir network, host dan subnet.	Bisa membolehkan/melarang network, host, subnet, service dan protocol.
Semua service diblokir	Bisa memilih service mana yang mau diblokir
Dikonfigurasikan sedekat mungkin dengan <i>destination</i> .	Dikonfigurasikan sedekat mungkin dengan <i>destination</i> .
Penyaringan hanya berdasarkan <i>source IP Address</i> .	Penyaringan berdasarkan <i>source IP Address, destination IP Address, jenis protocol dan port number</i> .

## Lab 29. Standard Access List

Seperti yang dijelaskan pada perbandingan diatas, Standard ACL memiliki perbandingan yang jauh berbeda daripada Extended ACL. Meskipun memiliki kekurangan dibagian filtering namun konfigurasi serta penerapan Standard ACL ini lebih mudah daripada Extended ACL.



Pada lab ini kita akan memblokir akses PING laptop 192.168.10.2 terhadap web server menggunakan Standard Access List.

Langkah Langkah :

A. Konfigurasi Switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-BAWAH  
SW-BAWAH(config)#interface fa0/4  
SW-BAWAH(config)#switchport mode trunk
```

B. Konfigurasi Router Kiri

```
R-1(config)#interface fa0/0  
R-1(config)#no shutdown  
R-1(config)#ip address 192.168.10.1 255.255.255.0  
  
R-1(config)#interface fa0/1  
R-1(config)#no shutdown  
R-1(config)#ip address 12.12.12.1 255.255.255.0
```

C. Konfigurasi Router Kanan

```
R-2(config)#interface fa0/0  
R-2(config)#no shutdown  
R-2(config)#ip address 12.12.12.2 255.255.255.0  
  
R-2(config)#interface fa0/1  
R-2(config)#no shutdown  
R-2(config)#ip address 20.20.20.1 255.255.255.0
```

Setelah itu gunakan routing agar antar network bisa saling terhubung

R-1/Router Kiri

```
R-1(config)#router eigrp 123
R-1(config)#network 12.12.12.0 0.0.0.255
R-1(config)#network 192.168.10.0 0.0.0.255
R-1(config)#no auto-summary
```

R-2/Router Kanan

```
R-2(config)#router eigrp 123
R-2(config)#network 12.12.12.0 0.0.0.255
R-2(config)#network 20.20.20.0 0.0.0.255
R-2(config)#no auto-summary
```

Pastikan antar laptop dan server bisa saling berkomunikasi, selanjutnya kita set Access-List nya di R-2 (Terdekat dengan tujuan).

R-2/Router Kanan

```
R-2(config)#access-list 1 deny host 192.168.10.2
R-2(config)#access-list 1 permit any
```

-Kita gunakan Standard Access List nomer 1  
-Konfigurasikan deny host ‘menolak’ host 192.168.10.2  
-Kita masukkan command permit any karena secara default, ketika kita masukkan deny maka akan menolak semuanya.

Kemudian kita masukkan konfigurasi Access List tersebut pada interface.

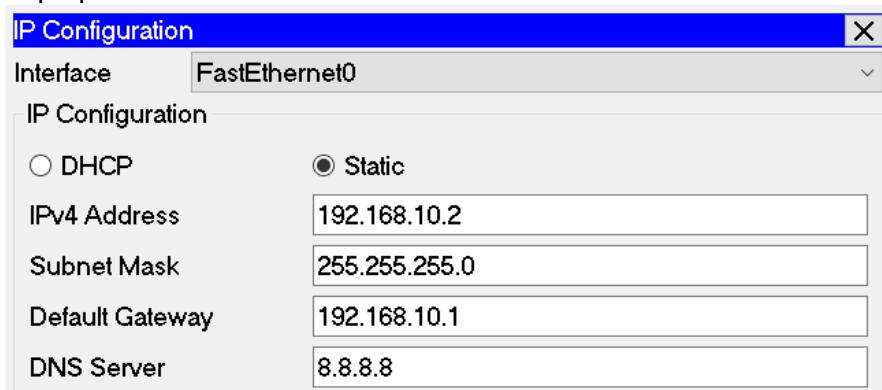
R-2/Router Kanan

```
R-2(config)#interface fa0/1
R-2(config)#ip access-group 1 out
```

**Access-group 1 out** digunakan untuk menandai bahwa dari sini packet akan keluar dari router yang kita konfigurasi access list.

#### D. Konfigurasi Laptop dan Server

##### 1. Laptop Kiri



##### 2. Laptop Tengah

**IP Configuration**

Interface **FastEthernet0**

**IP Configuration**

DHCP       Static

IPv4 Address **192.168.10.3**

Subnet Mask **255.255.255.0**

Default Gateway **192.168.10.1**

DNS Server **8.8.8.8**

3. Laptop Kanan

**IP Configuration**

Interface **FastEthernet0**

**IP Configuration**

DHCP       Static

IPv4 Address **192.168.10.4**

Subnet Mask **255.255.255.0**

Default Gateway **192.168.10.1**

DNS Server **8.8.8.8**

4. Server

**IP Configuration**

**IP Configuration**

DHCP       Static

IPv4 Address **20.20.20.2**

Subnet Mask **255.255.255.0**

Default Gateway **20.20.20.1**

DNS Server **8.8.8.8**

E. Pengecekan

1. Pengecekan Konfigurasi Access-list

```
R-2(config)#do show access-list
R-2(config)#do show access-list
Standard IP access list 1
  10 deny host 192.168.10.2
  20 permit any
```

Kondisi dimana Router sudah menerapkan Access-list tapi belum di PING

2. Pengecekan Penerapan interface fa0/1 yang menjalankan Access-list

```
R-2(config)#do show access-list
interface FastEthernet0/1
  ip address 20.20.20.1 255.255.255.0
  ip access-group 1 out
  duplex auto
  speed auto
```

Setelah itu kita akan coba melakukan PING dari IP Host yang sudah kita blokir tadi ke arah server.

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 12.12.12.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Hasilnya gagal karena kita sudah menerapkan Access-list memblokir IP 192.168.10.2 kearah server.

#### Pengecekan Tabel Access-List sesudah di PING

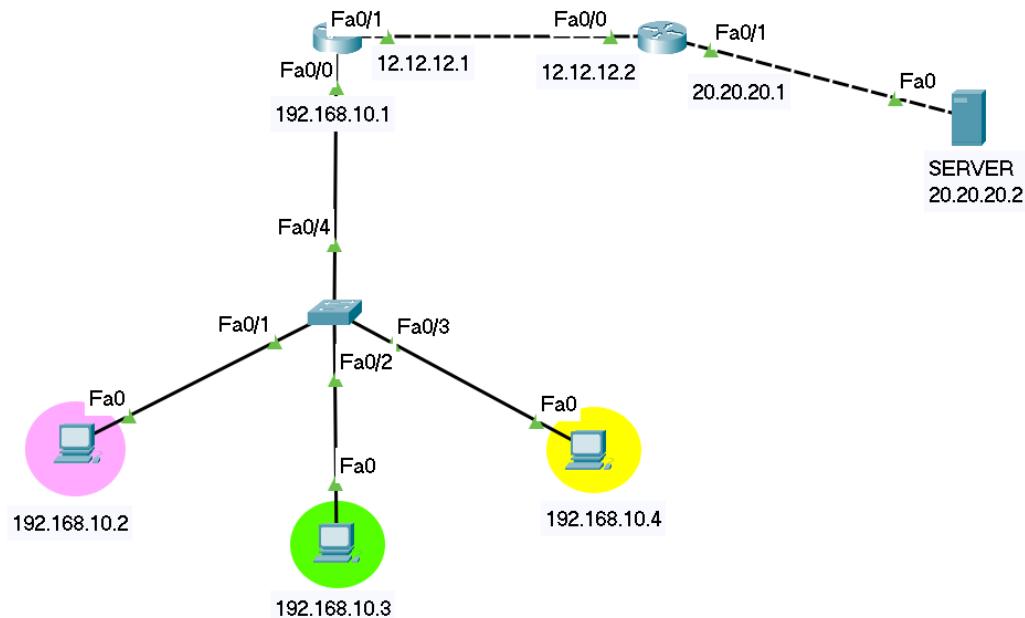
```
R-2(config)#do show access-list
R-2(config)#do show access-list
Standard IP access list 1
    10 deny host 192.168.10.2 (3 match(es))
    20 permit any
```

Terlihat ketika kita melakukan PING dari IP yang di Access-list ke Server setelah itu di cek kembali muncul Tanda seperti gambar diatas.itu Berarti Client sudah melakukan PING sebanyak 3 kali begitupula seterusnya.

F. Lab Standard Access-list telah selesai

## Lab 30. Standard Access-list 2<sup>nd</sup>

Sama aja seperti lab sebelumnya tetapi pada lab kali kita akan memblokir network IP Address untuk mengakses tujuan (server). Berikut adalah topologi nya kita akan memblokir network 192.168.10.0 agar tidak bisa melakukan PING terhadap server.



Langkah Langkah :

A. Konfigurasi Switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-BAWAH
SW-BAWAH(config)#interface fa0/4
SW-BAWAH(config)#switchport mode trunk
```

B. Konfigurasi Router Kiri

```
R-1(config)#interface fa0/0
R-1(config)#no shutdown
R-1(config)#ip address 192.168.10.1 255.255.255.0

R-1(config)#interface fa0/1
R-1(config)#no shutdown
R-1(config)#ip address 12.12.12.1 255.255.255.0
```

C. Konfigurasi Router Kanan

```
R-2(config)#interface fa0/0
R-2(config)#no shutdown
R-2(config)#ip address 12.12.12.2 255.255.255.0

R-2(config)#interface fa0/1
R-2(config)#no shutdown
R-2(config)#ip address 20.20.20.1 255.255.255.0
```

Setelah itu gunakan routing agar antar network bisa saling terhubung

#### R-1/Router Kiri

```
R-1(config)#router eigrp 123  
R-1(config)#network 12.12.12.0 0.0.0.255  
R-1(config)#network 192.168.10.0 0.0.0.255  
R-1(config)#no auto-summary
```

#### R-2/Router Kanan

```
R-2(config)#router eigrp 123  
R-2(config)#network 12.12.12.0 0.0.0.255  
R-2(config)#network 20.20.20.0 0.0.0.255  
R-2(config)#no auto-summary
```

Pastikan antar laptop dan server bisa saling berkomunikasi, selanjutnya kita set Access-List nya di R-2 (Terdekat dengan tujuan).

#### R-2/Router Kanan

```
R-2(config)#access-list 1 deny 192.168.10.0 0.0.0.255  
R-2(config)#access-list 1 permit any
```

- Kita gunakan Standard Access List nomer 1
- Konfigurasikan deny 'menolak' network 192.168.10.2 dan 0.0.0.255 (wildcard dari 255.255.255.0)
- Kita masukkan command permit any karena secara default, ketika kita masukkan deny maka akan menolak semuanya.

Kemudian kita masukkan konfigurasi Access List tersebut pada interface.

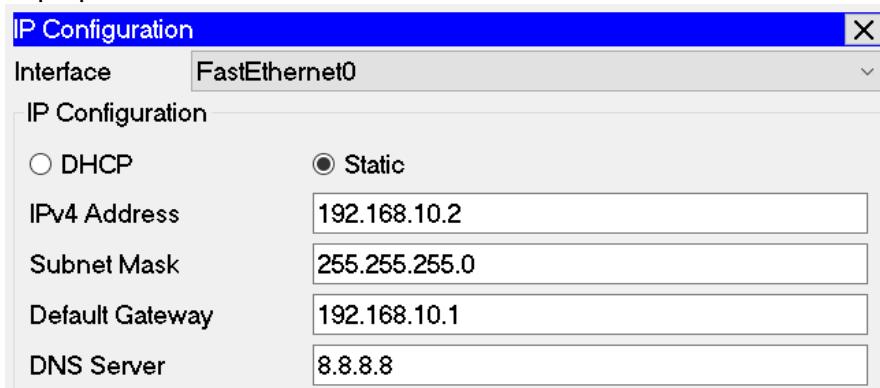
#### R-2/Router Kanan

```
R-2(config)#interface fa0/1  
R-2(config)#ip access-group 1 out
```

**Access-group 1 out** digunakan untuk menandai bahwa dari sini packet akan keluar dari router yang kita konfigurasi access list.

#### D. Konfigurasi Laptop dan Server

##### 1. Laptop Kiri



##### 2. Laptop Tengah

**IP Configuration**

Interface **FastEthernet0**

**IP Configuration**

DHCP       Static

IPv4 Address **192.168.10.3**

Subnet Mask **255.255.255.0**

Default Gateway **192.168.10.1**

DNS Server **8.8.8.8**

3. Laptop Kanan

**IP Configuration**

Interface **FastEthernet0**

**IP Configuration**

DHCP       Static

IPv4 Address **192.168.10.4**

Subnet Mask **255.255.255.0**

Default Gateway **192.168.10.1**

DNS Server **8.8.8.8**

4. Server

**IP Configuration**

**IP Configuration**

DHCP       Static

IPv4 Address **20.20.20.2**

Subnet Mask **255.255.255.0**

Default Gateway **20.20.20.1**

DNS Server **8.8.8.8**

E. Pengecekan

1. Pengecekan Konfigurasi Access-list

```
R-2(config)#do show access-list
R-2 (config)#do show access-list
Standard IP access list 1
  10 deny 192.168.10.0 0.0.0.255
  20 permit any
```

2. Pengecekan Penerapan interface fa0/1 yang menjalankan Access-list

```
R-2(config)#do show access-list
interface FastEthernet0/1
  ip address 20.20.20.1 255.255.255.0
  ip access-group 1 out
  duplex auto
  speed auto
```

Setelah itu kita akan coba melakukan PING dari IP salah satu Host network 192.168.10.0 yang sudah kita blokir tadi ke arah server.

```
C:\>ping 20.20.20.2  
Pinging 20.20.20.2 with 32 bytes of data:  
  
Reply from 12.12.12.2: Destination host unreachable.  
  
Ping statistics for 20.20.20.2:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gagal karena kita sudah memblokir network dari IP host tersebut

Pengecekan Tabel Access-List sesudah di PING

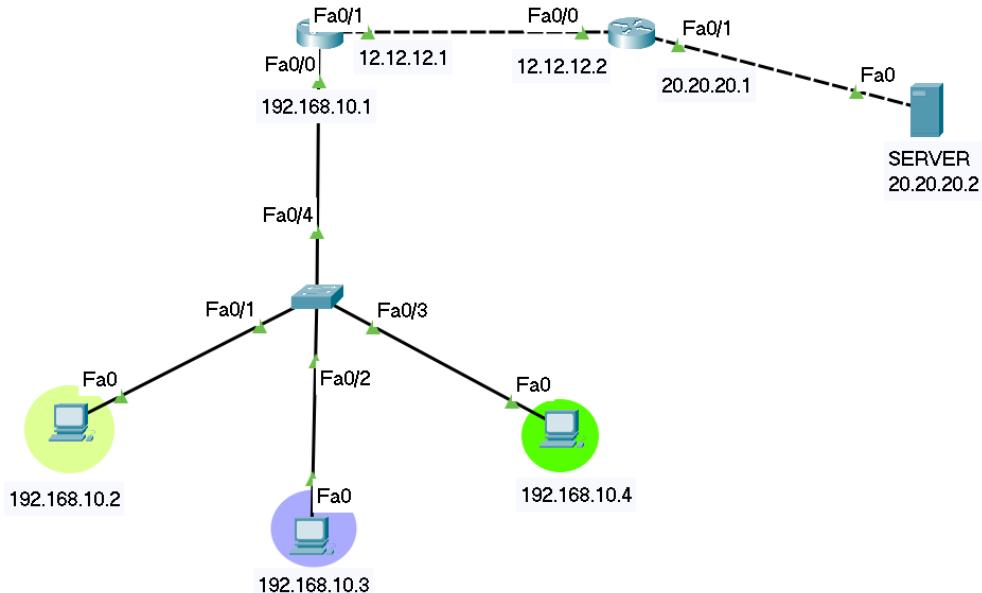
```
R-2(config)#do show access-list  
R-2(config)#do show access-list  
Standard IP access list 1  
    10 deny 192.168.10.0 0.0.0.255 (6 match(es))  
    20 permit any
```

Jumlah PING yang dilakukan oleh IP Client Network 192.168.10.0 adalah 6 kali

F. Lab Standard Access-list 2<sup>nd</sup> telah selesai

## Lab 31. Extended Access-list

Pada Extended Access List, kita dapat filtering lebih dari sekedar source address, tapi juga bisa destination address, bahkan protocol dan port number seperti Telnet, SSH, DHCP dll. Pada Lab ini kita akan memblokir akses host terhadap web (TCP port 80) pada server.



A. Konfigurasi Switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-BAWAH
SW-BAWAH(config)#interface fa0/4
SW-BAWAH(config)#switchport mode trunk
```

B. Konfigurasi Router Kiri

```
R-1(config)#interface fa0/0
R-1(config)#no shutdown
R-1(config)#ip address 192.168.10.1 255.255.255.0

R-1(config)#interface fa0/1
R-1(config)#no shutdown
R-1(config)#ip address 12.12.12.1 255.255.255.0
```

C. Konfigurasi Router Kanan

```
R-2(config)#interface fa0/0
R-2(config)#no shutdown
R-2(config)#ip address 12.12.12.2 255.255.255.0

R-2(config)#interface fa0/1
R-2(config)#no shutdown
R-2(config)#ip address 20.20.20.1 255.255.255.0
```

Setelah itu gunakan routing agar antar network bisa saling terhubung

#### R-1/Router Kiri

```
R-1(config)#router eigrp 123
R-1(config)#network 12.12.12.0 0.0.0.255
R-1(config)#network 192.168.10.0 0.0.0.255
R-1(config)#no auto-summary
```

#### R-2/Router Kanan

```
R-2(config)#router eigrp 123
R-2(config)#network 12.12.12.0 0.0.0.255
R-2(config)#network 20.20.20.0 0.0.0.255
R-2(config)#no auto-summary
```

Pastikan antar laptop dan server bisa saling berkomunikasi, selanjutnya kita set Access-List nya di R-2 (Terdekat dengan tujuan).

#### R-2/Router Kanan

```
R-2(config)#access-list 100 deny tcp host 192.168.10.3 host 20.20.20.2 eq 80
R-2(config)#access-list 100 deny tcp host 192.168.10.4 host 20.20.20.2 eq 80
R-2(config)#access-list 100 permit ip any any
```

- Extended Access List dimulai dari nomer 100-199
- Selain memblokir protocol TCP, kita dapat memblokir protocol lain seperti UDP, ICMP dll.
- Kita bisa memblokir destination pada Extended Access List
- Pada command eq 80 bermaksud port number yang spesifik dari protocol yang kita pilih, berdasarkan diatas, berarti TCP port 80 alias HTTP.
- Karena default Access List yaitu deny maka kita harus permit any any. **Any yang pertama** untuk membolehkan semua source address, **any yang kedua** untuk membolehkan semua destination address.

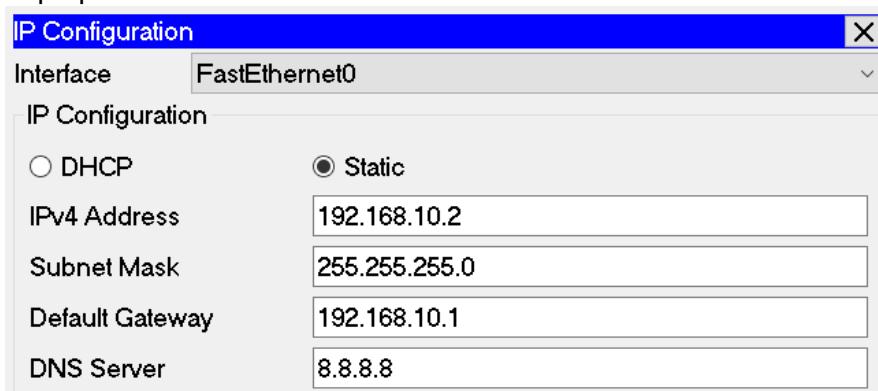
Kemudian kita masukkan konfigurasi Access List tersebut pada interface.

#### R-2/Router Kanan

```
R-2(config)#interface fa0/1
R-2(config)#ip access-group 100 out
```

### D. Konfigurasi Laptop dan Server

#### 1. Laptop Kiri



#### 2. Laptop Tengah

**IP Configuration**

Interface **FastEthernet0**

**IP Configuration**

DHCP       Static

IPv4 Address **192.168.10.3**

Subnet Mask **255.255.255.0**

Default Gateway **192.168.10.1**

DNS Server **8.8.8.8**

3. Laptop Kanan

**IP Configuration**

Interface **FastEthernet0**

**IP Configuration**

DHCP       Static

IPv4 Address **192.168.10.4**

Subnet Mask **255.255.255.0**

Default Gateway **192.168.10.1**

DNS Server **8.8.8.8**

4. Server

**IP Configuration**

**IP Configuration**

DHCP       Static

IPv4 Address **20.20.20.2**

Subnet Mask **255.255.255.0**

Default Gateway **20.20.20.1**

DNS Server **8.8.8.8**

E. Pengecekan

1. Pengecekan Konfigurasi Access-list

```
R-2(config)#do show access-list
R-2(config)#do show access-list
Extended IP access list 100
 10 deny icmp host 192.168.10.3 host 20.20.20.2
 20 deny tcp host 192.168.10.4 host 20.20.20.2 eq www
 30 permit ip any any
```

Kondisi dimana Router sudah menerapkan Extended Access-list tapi belum di Ping.

2. Pengecekan Penerapan interface fa0/1 yang menjalankan Access-list

```
R-2(config)#do show run
interface FastEthernet0/1
  ip address 20.20.20.1 255.255.255.0
  ip access-group 100 out
  duplex auto
  speed auto
```

Untuk pengetesan, apabila kita mencoba PING ke server dari PC maka hasilnya reply, namun jika kita mencoba mengakses web, maka hasilnya gagal.

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

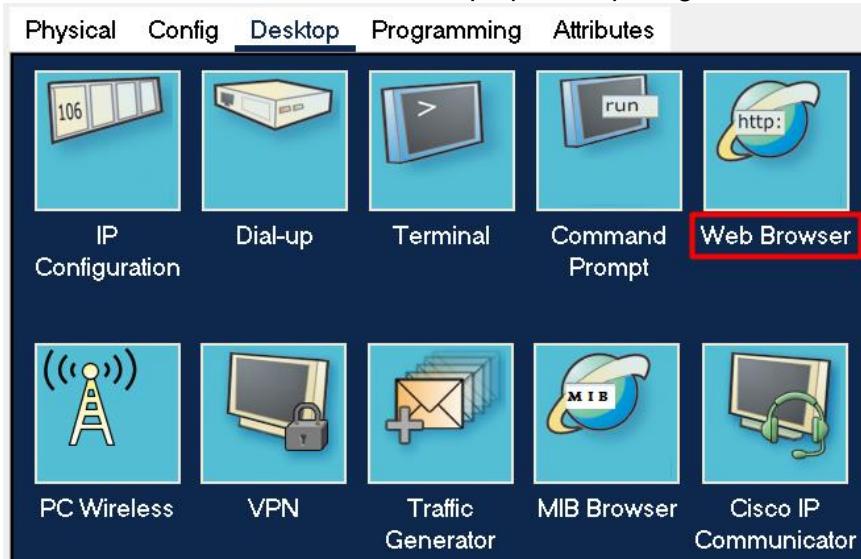
Reply from 12.12.12.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Setelah itu kita coba melakukan pengetesan akses web

#### F. Cara membuka Web Server

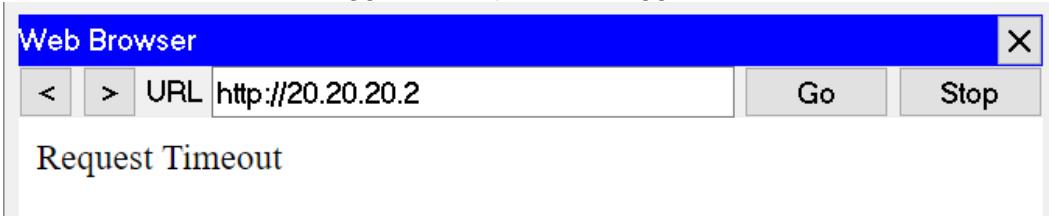
1. Membuka menu Web Browser di Laptop kiri seperti gambar dibawah



2. Klik dan masukan IP target/IP tujuan sesuai Konfigurasi tadi



3. Setelah itu klik Go dan tunggu beberapa saat hingga muncul

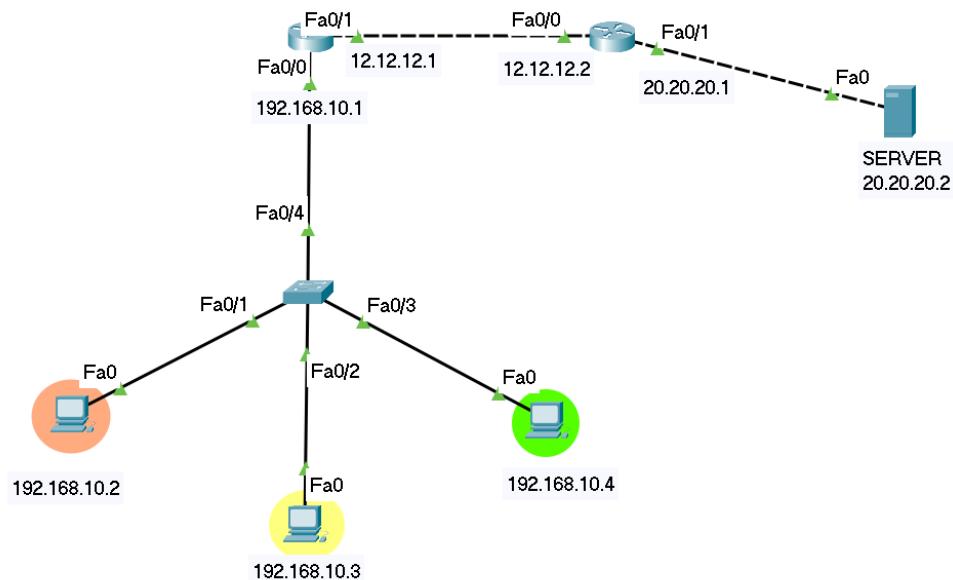


Bisa dilihat Request Timeout karena kita memblokir Laptop 192.168.10.3 untuk mengakses web dari IP tujuan 20.20.20.2.

#### G. Lab Extended Access-list telah selesai

## Lab 32. Extended Access-list 2<sup>nd</sup>

Sama saja seperti lab sebelumnya tetapi pada lab kali kita akan memblokir 2 port sekaligus yaitu (HTTP dan HTTPS). Berikut adalah topologi nya kita akan memblokir network 192.168.10.3 agar tidak bisa melakukan akses web .



Langkah Langkah :

A. Konfigurasi Switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-BAWAH  
SW-BAWAH(config)#interface fa0/4  
SW-BAWAH(config)#switchport mode trunk
```

B. Konfigurasi Router Kiri

```
R-1(config)#interface fa0/0  
R-1(config)#no shutdown  
R-1(config)#ip address 192.168.10.1 255.255.255.0  
  
R-1(config)#interface fa0/1  
R-1(config)#no shutdown  
R-1(config)#ip address 12.12.12.1 255.255.255.0
```

C. Konfigurasi Router Kanan

```
R-2(config)#interface fa0/0  
R-2(config)#no shutdown  
R-2(config)#ip address 12.12.12.2 255.255.255.0  
  
R-2(config)#interface fa0/1  
R-2(config)#no shutdown  
R-2(config)#ip address 20.20.20.1 255.255.255.0
```

Setelah itu gunakan routing agar antar network bisa saling terhubung

#### R-1/Router Kiri

```
R-1(config)#router eigrp 123
R-1(config)#network 12.12.12.0 0.0.0.255
R-1(config)#network 192.168.10.0 0.0.0.255
R-1(config)#no auto-summary
```

#### R-2/Router Kanan

```
R-2(config)#router eigrp 123
R-2(config)#network 12.12.12.0 0.0.0.255
R-2(config)#network 20.20.20.0 0.0.0.255
R-2(config)#no auto-summary
```

Pastikan antar laptop dan server bisa saling berkomunikasi, selanjutnya kita set Access-List nya di R-2 (Terdekat dengan tujuan).

#### R-2/Router Kanan

```
R-2(config)# access-list 100 deny tcp host 192.168.10.3 host 20.20.20.2 range
80 443
R-2(config#access-list 100 permit ip any any
```

**Range 80 443** : Perintah memblokir 2 port sekaligus secara bersamaan yaitu HTTP dan HTTPS

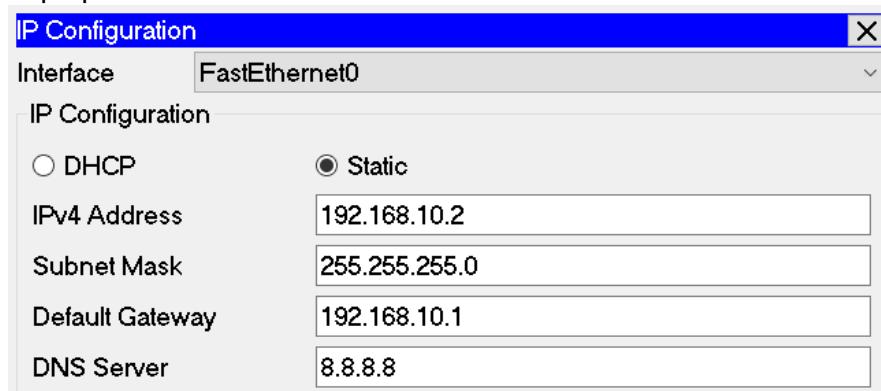
Kemudian kita masukkan konfigurasi Access List tersebut pada interface.

#### R-2/Router Kanan

```
R-2(config)#interface fa0/1
R-2(config)#ip access-group 100 out
```

### D. Konfigurasi Laptop dan Server

#### 1. Laptop Kiri



#### 2. Laptop Tengah

**IP Configuration**

Interface **FastEthernet0**

**IP Configuration**

DHCP       Static

IPv4 Address **192.168.10.3**

Subnet Mask **255.255.255.0**

Default Gateway **192.168.10.1**

DNS Server **8.8.8.8**

3. Laptop Kanan

**IP Configuration**

Interface **FastEthernet0**

**IP Configuration**

DHCP       Static

IPv4 Address **192.168.10.4**

Subnet Mask **255.255.255.0**

Default Gateway **192.168.10.1**

DNS Server **8.8.8.8**

4. Server

**IP Configuration**

**IP Configuration**

DHCP       Static

IPv4 Address **20.20.20.2**

Subnet Mask **255.255.255.0**

Default Gateway **20.20.20.1**

DNS Server **8.8.8.8**

E. Pengecekan

1. Pengecekan Konfigurasi Access-list

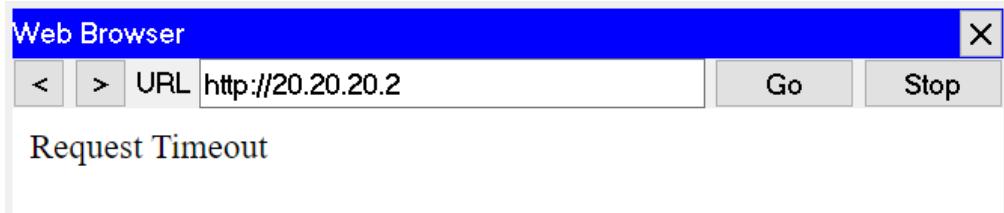
```
R-2(config)#do show access-list
R-2(config)#do show access-list
Extended IP access list 100
    10 deny tcp host 192.168.10.2 host 20.20.20.2 eq www
    20 deny tcp host 192.168.10.3 host 20.20.20.2 range www 443
    30 permit ip any any
```

2. Pengecekan Penerapan interface fa0/1 yang menjalankan Access-list

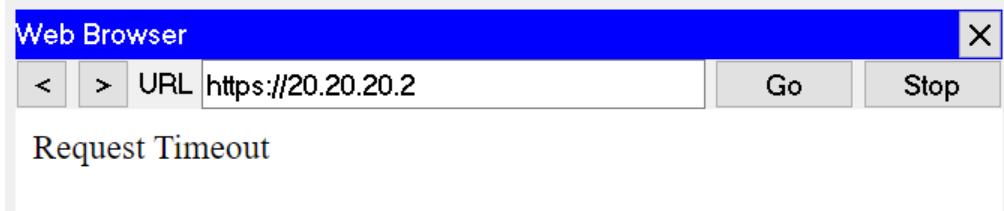
```
R-2(config)#do show run
interface FastEthernet0/1
  ip address 20.20.20.1 255.255.255.0
  ip access-group 100 out
  duplex auto
  speed auto
```

Kita akan melakukan pengetesan web HTTP dan HTTPS untuk IP Address yang sudah kita blokir tadi.

### Pengetesan Web HTTP



### Pengetesan Web HTTPS



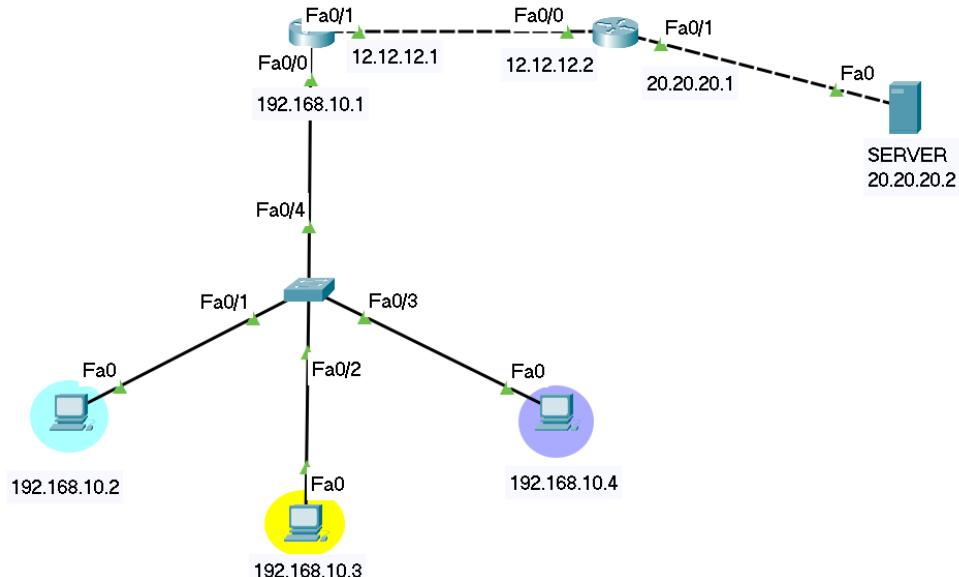
IP 192.168.10.2 gagal melakukan akses web HTTP dan HTTPS karena kita sudah memblokir IP untuk mengakses kedua web itu.

F. Lab Extended Access-list 2<sup>nd</sup> telah selesai

## Lab 33. Named Extended Access-list

Named Access-list adalah jenis Extended Access-List yang dapat memudahkan dalam me-manage ACL yang dibuat. Dengan NACL, kita bisa membuat daftar nama aturan sesuai dengan nama yang diinginkan dan pada nama daftar tersebut berisi nomor urutan access-list dalam 1 nama NACL dan nomor urutan terakhir harus perintah **#permit ip any any**

Alasan kenapa kita menggunakan NACL adalah agar lebih mudah ketika ada penambahan aturan baru dalam ACL sehingga kita tidak perlu repot-repot menghapus seluruh ACL, cukup menambahkan ACL baru dengan nomor sesuai pada daftar tetapi jangan nomor setelah nomor yang pertama.



Langkah Langkah :

A. Konfigurasi Switch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-BAWAH
SW-BAWAH(config)#interface fa0/4
SW-BAWAH(config)#switchport mode trunk
```

B. Konfigurasi Router Kiri

```
R-1(config)#interface fa0/0
R-1(config)#no shutdown
R-1(config)#ip address 192.168.10.1 255.255.255.0

R-1(config)#interface fa0/1
R-1(config)#no shutdown
R-1(config)#ip address 12.12.12.1 255.255.255.0
```

C. Konfigurasi Router Kanan

```
R-2(config)#interface fa0/0
R-2(config)#no shutdown
R-2(config)#ip address 12.12.12.2 255.255.255.0

R-2(config)#interface fa0/1
R-2(config)#no shutdown
```

```
R-2(config)#ip address 20.20.20.1 255.255.255.0
```

Setelah itu gunakan routing agar antar network bisa saling terhubung

R-1/Router Kiri

```
R-1(config)#router eigrp 123
R-1(config)#network 12.12.12.0 0.0.0.255
R-1(config)#network 192.168.10.0 0.0.0.255
R-1(config)#no auto-summary
```

R-2/Router Kanan

```
R-2(config)#router eigrp 123
R-2(config)#network 12.12.12.0 0.0.0.255
R-2(config)#network 20.20.20.0 0.0.0.255
R-2(config)#no auto-summary
```

Pastikan antar laptop dan server bisa saling berkomunikasi, selanjutnya kita set Access-List nya di R-2 (Terdekat dengan tujuan).

R-2/Router Kanan

```
R-2(config)#ip access-list extended TKJ-IDN
R-2(config)#10 deny tcp host 192.168.10.3 host 20.20.20.2 eq 80
R-2(config)#15 deny tcp host 192.168.10.4 host 20.20.20.2 eq 80
R-2(config)#20 permit ip any any
```

**Extended** : Perintah untuk membuat access-list jenis extended

**TKJ-IDN** : Nama Access-list yang aka kita gunakan (Nama bebas)

Kemudian kita masukkan konfigurasi Access List tersebut pada interface.

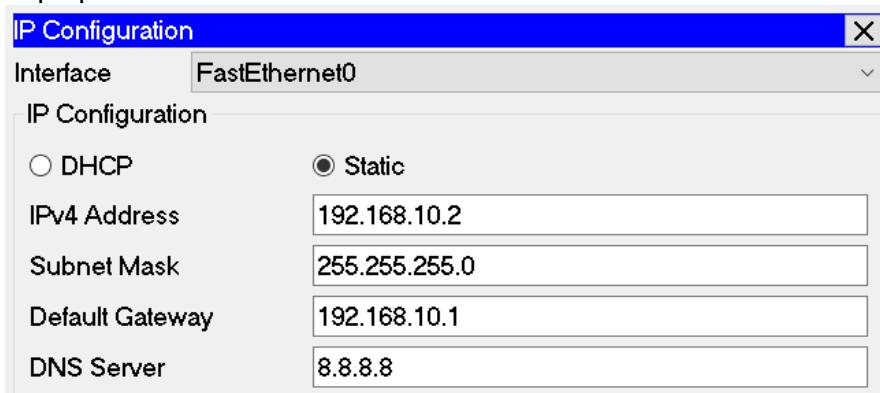
R-2/Router Kanan

```
R-2(config)#interface fa0/1
R-2(config)#ip access-group TKJ-IDN out
```

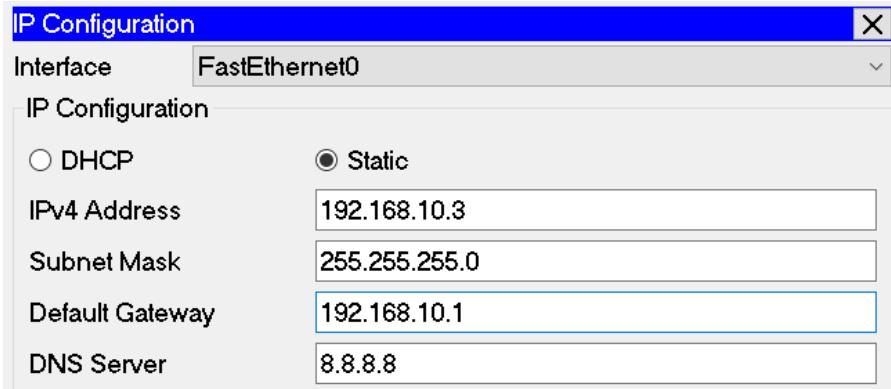
Jika di Access-List biasa menggunakan number,tapi kalau di Named Access-list kita menggunakan nama dari ACL tersebut sesuai yang kita config tadi

#### D. Konfigurasi Laptop dan Server

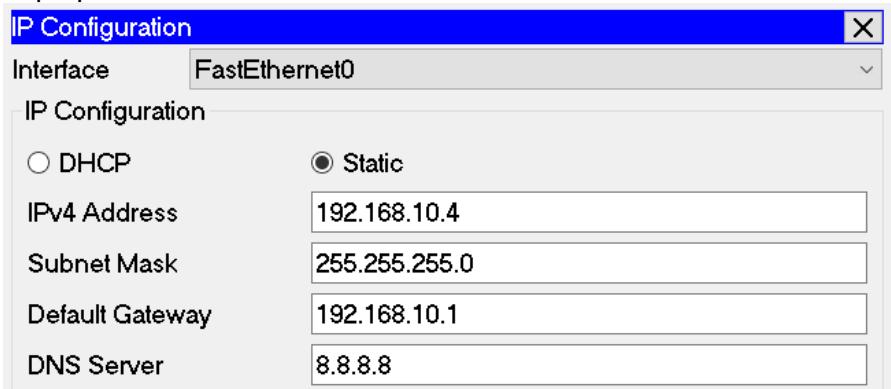
##### 1. Laptop Kiri



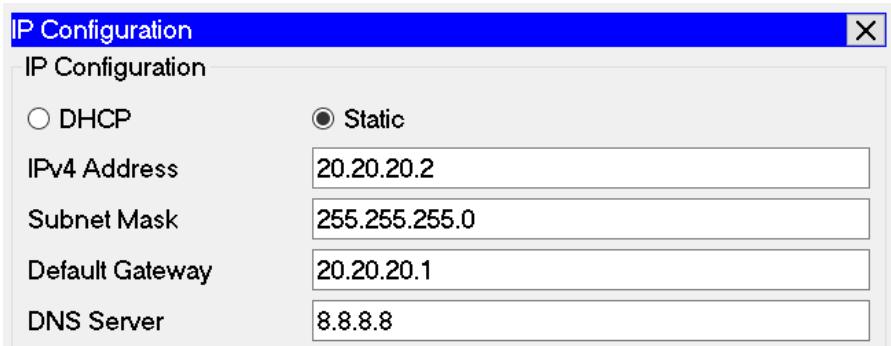
##### 2. Laptop Tengah



### 3. Laptop Kanan



### 4. Server



## E. Pengecekan

### 1. Pengecekan Konfigurasi Access-list

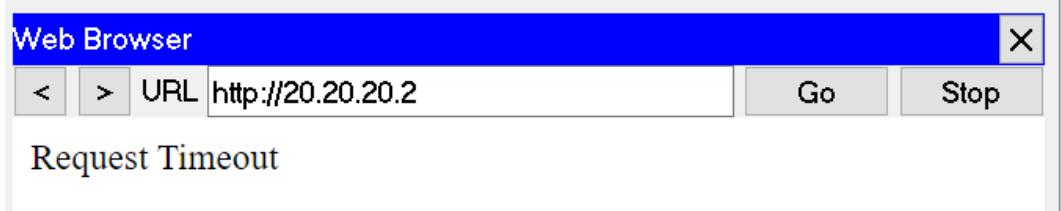
```
R-2(config)#do show access-list
R-2(config-if)#do show access-list
Extended IP access list TKJ-IDN
  15 deny icmp host 192.168.10.3 host 20.20.20.2
  20 deny tcp host 192.168.10.4 host 20.20.20.2 eq www
  25 permit ip any any
```

Terlihat bahwa kita telah mengkonfigurasi NACL TKJ-IDN

### 2. Pengecekan Penerapan interface fa0/1 yang menjalankan NACL

```
R-2(config)#do show run
interface FastEthernet0/1
  ip address 20.20.20.1 255.255.255.0
  ip access-group TKJ-IDN out
  duplex auto
  speed auto
```

Kita akan coba melakukan pengetesan web untuk IP Address 192.168.10.4



F. Lab Named Access-list telah selesai

# IOS IPv4 ACCESS LISTS

packetlife.net

Standard ACL Syntax		Actions
<pre>! Legacy syntax access-list &lt;number&gt; {permit   deny} &lt;source&gt; [log]</pre>		<b>permit</b> Allow matched packets
<pre>! Modern syntax ip access-list standard {&lt;number&gt;   &lt;name&gt;} [&lt;sequence&gt;] {permit   deny} &lt;source&gt; [log]</pre>		<b>deny</b> Deny matched packets
		<b>remark</b> Record a configuration comment
		<b>evaluate</b> Evaluate a reflexive ACL
Extended ACL Syntax		
<pre>! Legacy syntax access-list &lt;number&gt; {permit   deny} &lt;protocol&gt; &lt;source&gt; [&lt;ports&gt;] &lt;destination&gt; [&lt;ports&gt;] [&lt;options&gt;]</pre>		
<pre>! Modern syntax ip access-list extended {&lt;number&gt;   &lt;name&gt;} [&lt;sequence&gt;] {permit   deny} &lt;protocol&gt; &lt;source&gt; [&lt;ports&gt;] &lt;destination&gt; [&lt;ports&gt;] [&lt;options&gt;]</pre>		
ACL Numbers	Source/Destination Definitions	
1-99	any Any address	
1300-1999 IP standard	host <address> A single address	
100-199 IP extended	<network> <mask> Any address matched by the wildcard mask	
2000-2699		
200-299 Protocol	IP Options	
300-399 DECnet	dscp <DSCP> Match the specified IP DSCP	
400-499 XNS	fragments Check non-initial fragments	
500-599 Extended XNS	option <option> Match the specified IP option	
600-699 Appletalk	precedence {0-7} Match the specified IP precedence	
700-799 Ethernet MAC	ttl <count> Match the specified IP time to live (TTL)	
800-899 IPX standard	TCP/UDP Port Definitions	
900-999 IPX extended	eq <port> Equal to	
1000-1099 IPX SAP	neq <port> Not equal to	
1100-1199 MAC extended	lt <port> Less than	
1200-1299 IPX summary	gt <port> Greater than	
	range <port> <port> Matches a range of port numbers	
TCP Options	Miscellaneous Options	
ack Match ACK flag	reflect <name> Create a reflexive ACL entry	
fin Match FIN flag	time-range <name> Enable rule only during the given time range	
psh Match PSH flag		
rst Match RST flag	Applying ACLs to Restrict Traffic	
syn Match SYN flag	interface FastEthernet0/0	
urg Match URG flag	ip access-group {<number>   <name>} {in   out}	
established Match packets in an established session		
Logging Options	Troubleshooting	
log Log ACL entry matches	show access-lists [<number>   <name>]	
log-input Log matches including ingress interface and source MAC address	show ip access-lists [<number>   <name>]	
	show ip access-lists interface <interface>	
	show ip access-lists dynamic	
	show ip interface [<interface>]	
	show time-range [<name>]	

by Jeremy Stretch

v2.0

# NAT

(Network Address Translation)

# NAT

**CONTENT :**

**STATIC NAT**

**DYNAMIC NAT**

**NAT OVERLOAD**

**NTP (NETWORK TIME PROTOCOL)**

## NAT Introduction

Network Address Translation (NAT) adalah sebuah proses dimana IP Private diterjemahkan menjadi IP Public oleh router agar klien yang menggunakan IP Private ini, dapat mengakses internet yang menggunakan IP public. NAT beroperasi pada router dan firewall pada jaringan.

Terdapat 2 NAT:

- **Static NAT**

Static NAT adalah NAT yang harus kita konfigurasikan secara manual, baik dari IP private maupun IP publicnya. Sehingga pada tiap satu IP public untuk satu IP private alias one to one mapping.

- **Dynamic NAT**

Dynamic NAT merupakan NAT yang berjalan secara otomatis sejak pertama kali kita konfigurasikan. Dynamic NAT sendiri ada dua versi, **Dynamic NAT Pool** dan **Dynamic NAT Overload**. Pada Dynamic NAT Pool, router akan membuat sebuah daftar IP Public yang akan dialokasikan sesuai dengan rules yang sudah dibuat kepada IP private. Pada Dynamic NAT Overload, kita hanya butuh satu buah IP Public untuk digunakan oleh banyak IP Private dengan syarat, satu interface untuk satu IP Public sehingga semua IP Private yang berada di port tersebut dapat menggunakan IP Public tersebut.

### Interface NAT

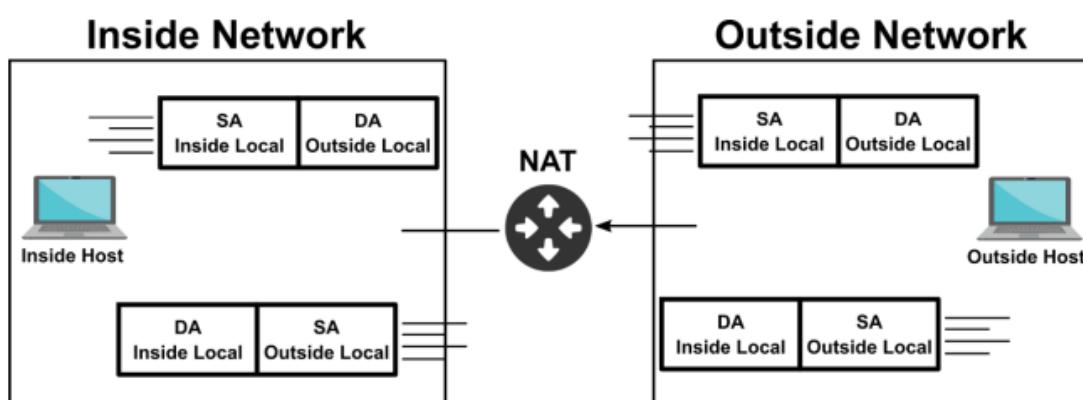
Saat membuat NAT router harus memasangnya pada interface, terdapat 2 jenis traffic :

1. **Inside**

Dipasang pada interface yang mengarah ke jaringan local/LAN/IP Private

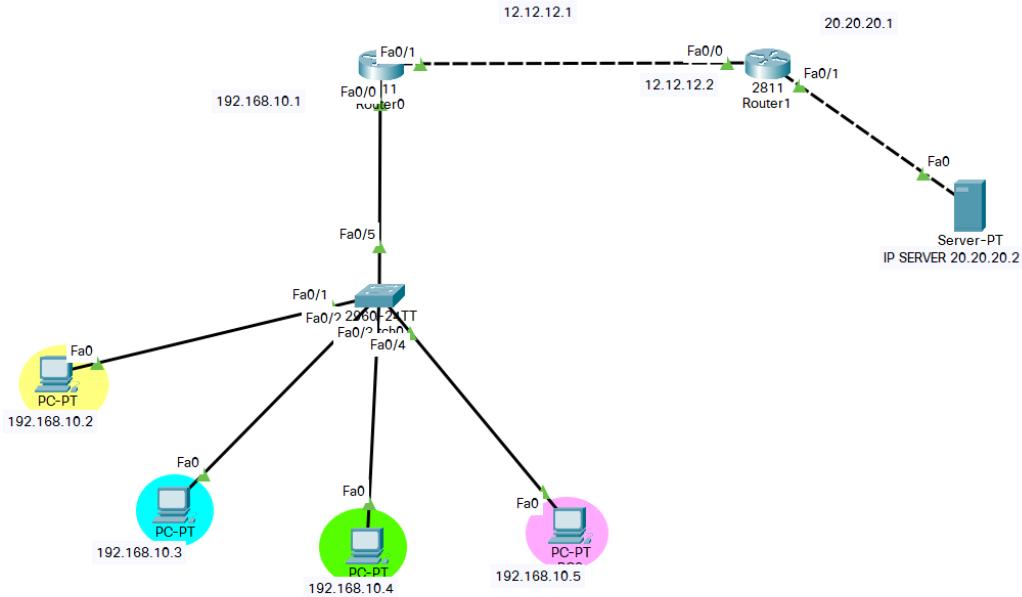
2. **Outside**

Dipadang pada interface yang mengarah ke jaringan Public/Internet



## Lab 34. Static NAT

Static NAT seperti yang sudah dijelaskan diatas, Static NAT adalah NAT yang kita harus konfigurasi secara manual.



Langkah Langkah :

A. Konfigurasi di Switch

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-KANTOR
```

2. Melakukan Trunk

```
SW-KANTOR(config)#interface fa0/5  
SW-KANTOR(config)#switchport mode trunk
```

B. Konfigurasi di Router Local

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-LOCAL
```

2. Mengaktifkan interface dan memasang ip address Router Local

```
R-LOCAL(config)#interface fa0/0  
R-LOCAL(config)#no shutdown  
R-LOCAL(config)#ip address 192.168.10.1 255.255.255.0  
  
R-LOCAL(config)#interface fa0/1  
R-LOCAL(config)#no shutdown  
R-LOCAL(config)#ip address 12.12.12.1 255.255.255.0
```

C. Konfigurasi di Router Public

1. Mengganti hostname router

```
Router>enable
```

```
Router#configure terminal  
Router(config)#hostname R-PUBLIC
```

2. Mengaktifkan interface dan memasang ip address Router Public

```
R-PUBLIC(config)#interface fa0/0  
R-PUBLIC(config)#no shutdown  
R-PUBLIC(config)#ip address 12.12.12.2 255.255.255.0
```

```
R-PUBLIC(config)#interface fa0/1  
R-PUBLIC(config)#no shutdown  
R-PUBLIC(config)#ip address 20.20.20.1 255.255.255.0
```

#### Konfigurasi Static NAT

```
R-LOCAL(config)#ip nat inside source static 192.168.10.2 12.12.12.3
```

Jadi maksud dari konfigurasi NAT static di atas adalah 1 IP Local di terjemahkan menggunakan 1 IP Public atau one to one NAT. Bisa dilihat IP Local 192.168.10.2 diterjemahkan menggunakan IP Public 12.12.12.3.

#### Konfigurasi Default-Route

```
R-LOCAL(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.2
```

**IP route** : Membuat Static Route

**0.0.0.0**: Network tujuan (0.0.0.0 (yang pertama) adalah IP yang mewakili semua IP network di internet)

**0.0.0.0**: Subnetmask tujuan (0.0.0.0(yang kedua) adalah subnetmask yang mewakili semua subnetmask di internet)

**12.12.12.2** : Gateaway/IP Router tetangga

#### Menentukan IP Inside/IP Outside di Router Local

```
R-LOCAL(config)#interface fa0/0  
R-LOCAL(config)#ip nat inside
```

```
R-LOCAL(config)#interface fa0/1  
R-LOCAL(config)#ip nat outside
```

**IP Nat inside** : Dipasang pada interface yang mengarah ke jaringan local/LAN/IP private

**IP Nat outside** : Dipasang pada interface yang mengarah ke jaringan public/internet

#### D. Konfigurasi IP Laptop dan Server

1. Laptop A

**IP Configuration**

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	8.8.8.8

2. Laptop B

**IP Configuration**

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	8.8.8.8

3. Laptop C

**IP Configuration**

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	8.8.8.8

4. Laptop D

**IP Configuration**

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	8.8.8.8

E. Pengecekan

- Pengecekan IP Local yang sudah diterjemahkan

```
R-LOCAL(config)#do show nat transalation
```

```
R-LOCAL(config-if)#do sh ip nat trans
Pro Inside global     Inside local      Outside local      Outside global
--- 12.12.12.3        192.168.10.2    ---               ---
--- 12.12.12.4        192.168.10.3    ---               ---
--- 12.12.12.5        192.168.10.4    ---               ---
--- 12.12.12.6        192.168.10.5    ---               ---
```

Kondisi dimana NAT sudah diterapkan tapi belum di PING ke Server

## 2. Pengecekan IP Local yang sudah Ping kearah Server

```
R-LOCAL(config)#do show nat translation
R-LOCAL(config)#do show ip nat translation
Pro Inside global     Inside local      Outside local      Outside global
icmp 12.12.12.4:5    192.168.10.3:5   20.20.20.2:5    20.20.20.2:5
icmp 12.12.12.4:6    192.168.10.3:6   20.20.20.2:6    20.20.20.2:6
icmp 12.12.12.5:1    192.168.10.4:1   20.20.20.2:1    20.20.20.2:1
icmp 12.12.12.5:2    192.168.10.4:2   20.20.20.2:2    20.20.20.2:2
icmp 12.12.12.5:3    192.168.10.4:3   20.20.20.2:3    20.20.20.2:3
icmp 12.12.12.6:1    192.168.10.5:1   20.20.20.2:1    20.20.20.2:1
icmp 12.12.12.6:2    192.168.10.5:2   20.20.20.2:2    20.20.20.2:2
--- 12.12.12.3        192.168.10.2    ---               ---
--- 12.12.12.4        192.168.10.3    ---               ---
--- 12.12.12.5        192.168.10.4    ---               ---
--- 12.12.12.6        192.168.10.5    ---               ---
```

Bisa dilihat bahwa IP Local 192.168.10.3 melakukan ICMP(PING) menggunakan IP Public 12.12.12.4 begitu pula seterusnya. Setelah itu kita akan melakukan test PING dari salah satu laptop kearah server.

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 12.12.12.2: Destination host unreachable.

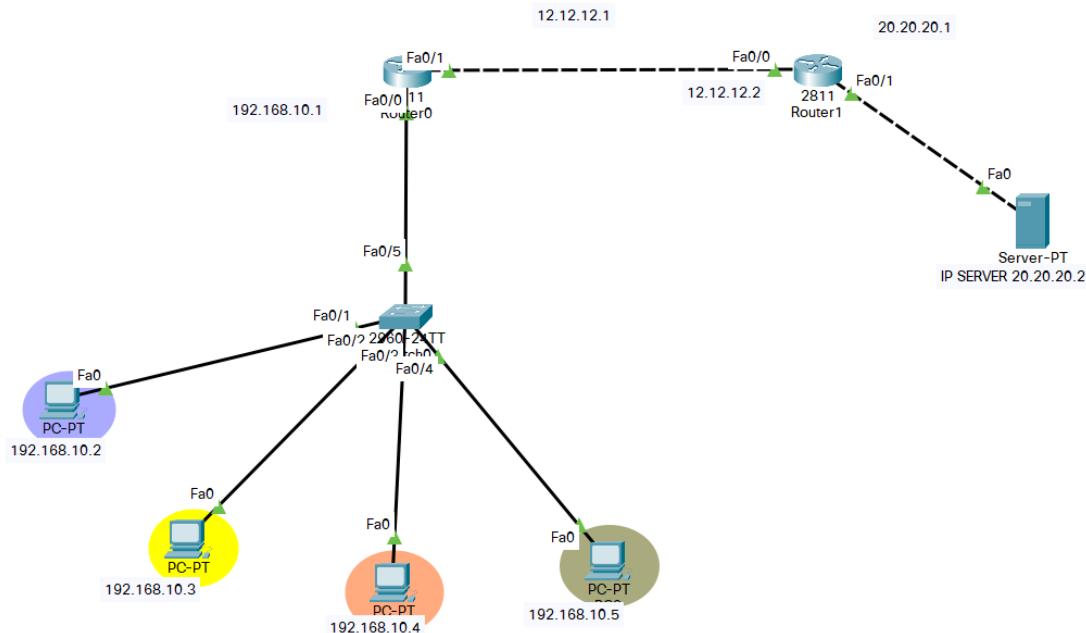
Ping statistics for 20.20.20.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Success karena Laptop sudah berhasil kita NAT,Jika ingin menambahkan Laptop lagi maka laptop itu harus di NAT lagi dengan menggunakan IP Public yang berbeda.

F. Lab Static NAT telah selesai.

## Lab 35. Dynamic NAT

Dynamic NAT yaitu jumlah IP Public sama dengan jumlah IP Private, jenis NAT ini jarang digunakan, misalkan ada 5 IP Private maka ada 5 IP Public juga, pemberian IP Public nya tergantung dengan routernya, biasanya Dynamic NAT diimplementasikan menggunakan range. Baik kita akan mengkonfigurasi Dynamic NAT pada topologi dibawah ini :



Langkah Langkah :

A. Konfigurasi di Switch

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-KANTOR
```

2. Melakukan Trunk

```
SW-KANTOR(config)#interface fa0/5  
SW-KANTOR(config)#switchport mode trunk
```

B. Konfigurasi di Router Local

1. Mengganti hostname switch

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-LOCAL
```

2. Mengaktifkan interface dan memasang ip address Router Local

```
R-LOCAL(config)#interface fa0/0  
R-LOCAL(config)#no shutdown  
R-LOCAL(config)#ip address 192.168.10.1 255.255.255.0
```

```
R-LOCAL(config)#interface fa0/1  
R-LOCAL(config)#no shutdown  
R-LOCAL(config)#ip address 12.12.12.1 255.255.255.0
```

### C. Konfigurasi di Router Public

1. Mengganti hostname switch

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-PUBLIC
```

2. Mengaktifkan interface dan memasang ip address Router Public

```
R-PUBLIC(config)#interface fa0/0  
R-PUBLIC(config)#no shutdown  
R-PUBLIC(config)#ip address 12.12.12.2 255.255.255.0
```

```
R-PUBLIC(config)#interface fa0/1  
R-PUBLIC(config)#no shutdown  
R-PUBLIC(config)#ip address 20.20.20.1 255.255.255.0
```

### Konfigurasi Dynamic NAT (Router Kiri)

```
R-LOCAL(config)#ip nat pool TKJ 12.12.12.10 12.12.12.20 net 255.255.255.0  
R-LOCAL(config)#ip nat inside source list 1 pool TKJ  
R-LOCAL(config)#access-list 1 permit 192.168.10.0 0.0.0.255
```

#### IP NAT Pool TKJ

Membuat daftar IP dengan nama daftar TKJ

**12.12.12.10 12.12.12.20**

Sejumlah range alamat IP Public yang berada pada daftar TKJ.

**Netmask 255.255.255.0**

Subnetmask/prefix yang digunakan oleh IP Public tsb.

**IP NAT Inside Source list 1 pool TKJ**

Membuat NAT nya yang berisi daftar IP Public TKJ

**Access-list 1 permit 192.168.10.0 0.0.0.255**

Membuat access-list untuk mengizinkan network dari IP Address tsb untuk di NAT

### Mengkonfigurasi Default Route

```
R-LOCAL(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.2
```

Menentukan IP Inside/IP Outside di Router Local

```
R-LOCAL(config)#interface fa0/0  
R-LOCAL(config)#ip nat inside
```

```
R-LOCAL(config)#interface fa0/1  
R-LOCAL(config)#ip nat outside
```

### D. Konfigurasi IP Laptop dan Server

1. Laptop A

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.10.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 8.8.8.8

2. Laptop B

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.10.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 8.8.8.8

3. Laptop C

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.10.4

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 8.8.8.8

4. Laptop D

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.10.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 8.8.8.8

E. Pengecekan

1. Pengecekan IP Local yang sudah diterjemahkan (Dynamic NAT)

R-LOCAL(config)#do show nat transalation

Protocol	Inside global	Inside local	Outside local	Outside global
icmp	12.12.12.10:1	192.168.10.3:1	20.20.20.2:1	20.20.20.2:1
icmp	12.12.12.10:2	192.168.10.3:2	20.20.20.2:2	20.20.20.2:2
icmp	12.12.12.10:3	192.168.10.3:3	20.20.20.2:3	20.20.20.2:3
icmp	12.12.12.11:10	192.168.10.5:10	20.20.20.2:10	20.20.20.2:10
icmp	12.12.12.11:8	192.168.10.5:8	20.20.20.2:8	20.20.20.2:8
icmp	12.12.12.11:9	192.168.10.5:9	20.20.20.2:9	20.20.20.2:9
icmp	12.12.12.12:1	192.168.10.4:1	20.20.20.2:1	20.20.20.2:1
icmp	12.12.12.12:2	192.168.10.4:2	20.20.20.2:2	20.20.20.2:2
icmp	12.12.12.13:15	192.168.10.2:15	20.20.20.2:15	20.20.20.2:15
icmp	12.12.12.13:16	192.168.10.2:16	20.20.20.2:16	20.20.20.2:16

## 2. Pengecekan penerapan NAT di interface

R-LOCAL(config)#do show run

```
interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
  ip nat inside
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 12.12.12.1 255.255.255.0
  ip nat outside
  duplex auto
  speed auto
!
```

Setelah itu kita akan melakukan test PING dari salah satu laptop kearah server.

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

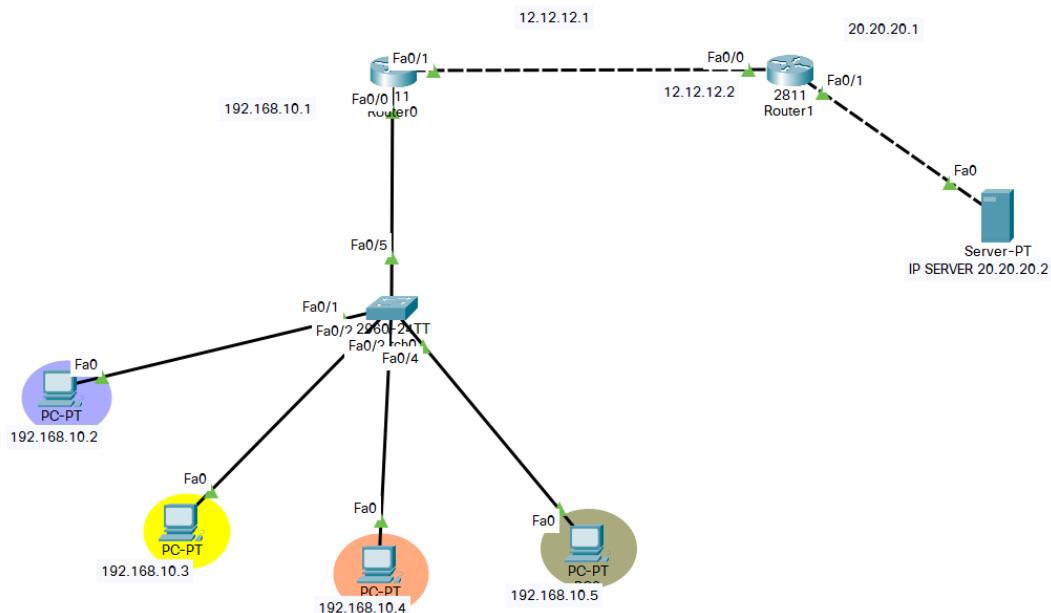
Reply from 12.12.12.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

## F. Lab Dynamic NAT telah selesai

## Lab 36. NAT Overload

Sama seperti yang dijelaskan sebelumnya, Dynamic NAT merupakan suatu cara untuk mengonfigurasi NAT secara otomatis pada suatu router. Pada Lab ini, kita akan mengonfigurasikan Dynamic NAT Overload atau biasa disebut dengan PAT (Port Address Translation) karena dapat menerjemahkan satu IP public untuk IP private pada satu port. Kita akan menggunakan topologi yang sama pada lab sebelumnya.



Langkah Langkah :

A. Konfigurasi di switch

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-KANTOR
```

2. Melakukan Trunk

```
SW-KANTOR(config)#interface fa0/5  
SW-KANTOR(config)#switchport mode trunk
```

B. Konfigurasi di Router Local

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-LOCAL
```

2. Mengaktifkan interface dan memasang ip address Router Local

```
R-LOCAL(config)#interface fa0/0  
R-LOCAL(config)#no shutdown  
R-LOCAL(config)#ip address 192.168.10.1 255.255.255.0
```

```
R-LOCAL(config)#interface fa0/1  
R-LOCAL(config)#no shutdown  
R-LOCAL(config)#ip address 12.12.12.1 255.255.255.0
```

### C. Konfigurasi di Router Public

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-PUBLIC
```

2. Mengaktifkan interface dan memasang ip address Router Public

```
R-PUBLIC(config)#interface fa0/0  
R-PUBLIC(config)#no shutdown  
R-PUBLIC(config)#ip address 12.12.12.2 255.255.255.0
```

```
R-PUBLIC(config)#interface fa0/1  
R-PUBLIC(config)#no shutdown  
R-PUBLIC(config)#ip address 20.20.20.1 255.255.255.0
```

### Konfigurasi NAT Overload

```
R-LOCAL(config)#access-list 1 permit any  
R-LOCAL(config)#ip nat inside source list 1 interface fa0/1 overload
```

- Access-list 1 permit 192.168.1.0 0.0.0.255 dalam menggunakan NAT Overload, kita perlu sebuah list daftar IP Address yang diperbolehkan

- Ip nat inside source list 1 interface fa0/1 overload kita terjemahkan kedalam (inside) kemudian kita gunakan access-list 1 sebagai daftarnya, kita pilih interface fa0/1 sebagai portnya, kemudian kita overload.

### Menentukan interface inside atau outside

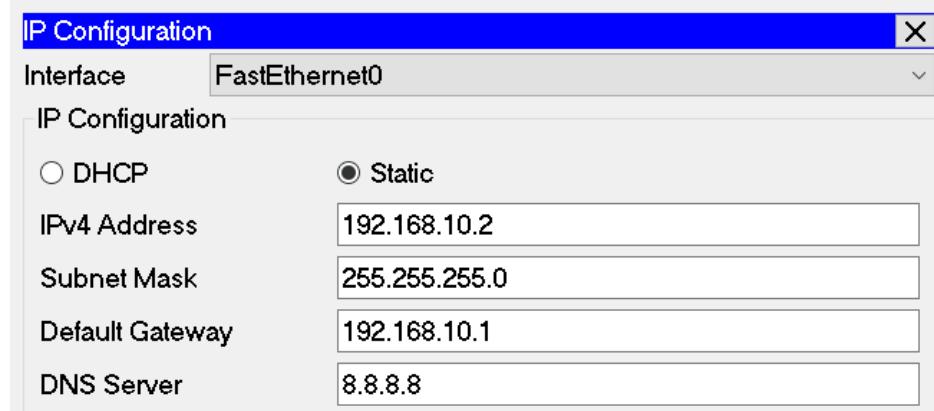
```
R-LOCAL(config)#interface fa0/0  
R-LOCAL(config)#ip nat inside  
R-LOCAL(config)#interface fa0/1  
R-LOCAL(config)#ip nat outside
```

### Mengkonfigurasi Default Route

```
R-LOCAL(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.2
```

### D. Konfigurasi IP Address Laptop dan Server

1. Laptop A



2. Laptop B

**IP Configuration**

Interface FastEthernet0

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	8.8.8.8

3. Laptop C

**IP Configuration**

Interface FastEthernet0

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	8.8.8.8

4. Laptop D

**IP Configuration**

Interface FastEthernet0

IP Configuration

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	8.8.8.8

E. Pengecekan

1. Pengecekan IP Local yang sudah diterjemahkan oleh router

R-LOCAL(config)#do show nat translation				
Protocol	Inside global	Inside local	Outside local	Outside global
icmp	12.12.12.1:1024	192.168.10.2:9	20.20.20.2:9	20.20.20.2:1024
icmp	12.12.12.1:10	192.168.10.4:10	20.20.20.2:10	20.20.20.2:10
icmp	12.12.12.1:11	192.168.10.4:11	20.20.20.2:11	20.20.20.2:11
icmp	12.12.12.1:12	192.168.10.4:12	20.20.20.2:12	20.20.20.2:12
icmp	12.12.12.1:1	192.168.10.3:1	20.20.20.2:1	20.20.20.2:1
icmp	12.12.12.1:9	192.168.10.4:9	20.20.20.2:9	20.20.20.2:9

Bisa dilihat semua IP Private diterjemahkan menggunakan 1 IP Public yaitu 12.12.12.1.

## 2. Pengecekan penerapan NAT di interface

```
R-LOCAL(config)#do show run
interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
  ip nat inside
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 12.12.12.1 255.255.255.0
  ip nat outside
  duplex auto
  speed auto
!
```

Setelah itu kita akan melakukan test PING dari salah satu laptop kearah server.

```
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 12.12.12.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

F. Lab NAT Overload telah selesai.

# NETWORK ADDRESS TRANSLATION

packetlife.net

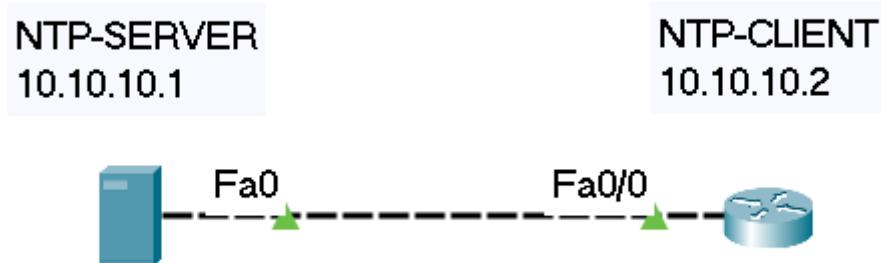
Example Topology		Address Classification			
<p>FastEthernet0 10.0.0.1/16 NAT Inside</p> <p>FastEthernet1 174.143.212.1/22 NAT Outside</p>		<b>Inside Local</b>	An actual address assigned to an inside host		
		<b>Inside Global</b>	An inside address seen from the outside		
		<b>Outside Global</b>	An actual address assigned to an outside host		
		<b>Outside Local</b>	An outside address seen from the inside		
NAT Boundary Configuration		Perspective			
<pre>interface FastEthernet0 ip address 10.0.0.1 255.255.0.0 ip nat inside ! interface FastEthernet1 ip address 174.143.212.1 255.255.252.0 ip nat outside</pre>		Location	Local	Global	
		Inside	Inside Local	Inside Global	
		Outside	Outside Local	Outside Global	
Static Source Translation		Terminology			
<pre>! One line per static translation ip nat inside source static 10.0.0.19 192.0.2.1 ip nat inside source static 10.0.1.47 192.0.2.2 ip nat outside source static 174.143.212.133 10.0.0.47 ip nat outside source static 174.143.213.240 10.0.2.181</pre>		<b>NAT Pool</b> A pool of IP addresses to be used as inside global or outside local addresses in translations			
Dynamic Source Translation		<b>Port Address Translation (PAT)</b> An extension to NAT that translates information at layer four and above, such as TCP and UDP port numbers; dynamic PAT configurations include the <b>overload</b> keyword			
<pre>! Create an access list to match inside local addresses access-list 10 permit 10.0.0.0 0.0.255.255 ! ! Create NAT pool of inside global addresses ip nat pool MyPool 192.0.2.1 192.0.2.254 prefix-length 24 ! ! Combine them with a translation rule ip nat inside source list 10 pool MyPool ! ! Dynamic translations can be combined with static entries ip nat inside source static 10.0.0.42 192.0.2.42</pre>		<b>Extendable Translation</b> The <b>extendable</b> keyword must be appended when multiple overlapping static translations are configured			
Port Address Translation (PAT)		<b>Special NAT Pool Types</b> <b>Rotary</b> Used for load balancing			
<pre>! Static layer four port translations ip nat inside source static tcp 10.0.0.3 8080 192.0.2.1 80 ip nat inside source static udp 10.0.0.14 53 192.0.2.2 53 ip nat outside source static tcp 174.143.212.4 23 10.0.0.8 23 ! ! Dynamic port translation with a pool ip nat inside source list 11 pool MyPool overload ! ! Dynamic translation with interface overloading ip nat inside source list 11 interface FastEthernet1 overload</pre>		<b>Match-Host</b> Preserves the host portion of the address after translation			
Inside Destination Translation		<b>Troubleshooting</b> show ip nat translations [verbose] show ip nat statistics clear ip nat translations			
<pre>! Create a rotary NAT pool ip nat pool LoadBalServers 10.0.99.200 10.0.99.203 prefix-length 24 type rotary ! ! Enable load balancing across inside hosts for incoming traffic ip nat inside destination list 12 pool LoadBalServers</pre>		<b>NAT Translations Tuning</b> ip nat translation tcp-timeout <seconds> ip nat translation udp-timeout <seconds> ip nat translation max-entries <number>			

by Jeremy Stretch

v1.0

## Lab 37. NTP (Network Time Protocol)

NTP (Network Time Protocol) berfungsi untuk menyinkronisasi waktu pada server, jaringan internet memiliki peraturan waktunya harus sesuai. NTP membantu peralatan jaringan agar bisa sinkron dengan suatu server NTP, server NTP bisa berada di jaringan local maupun di public/internet.



Langkah Langkah :

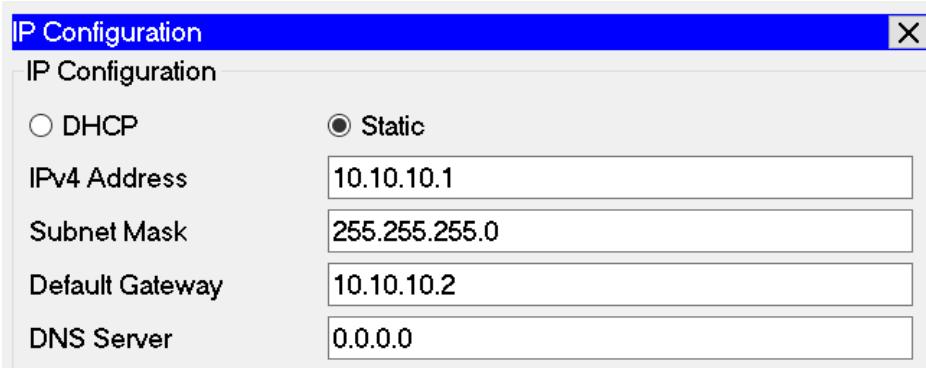
- Konfigurasi Router
  - Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-IDN
```

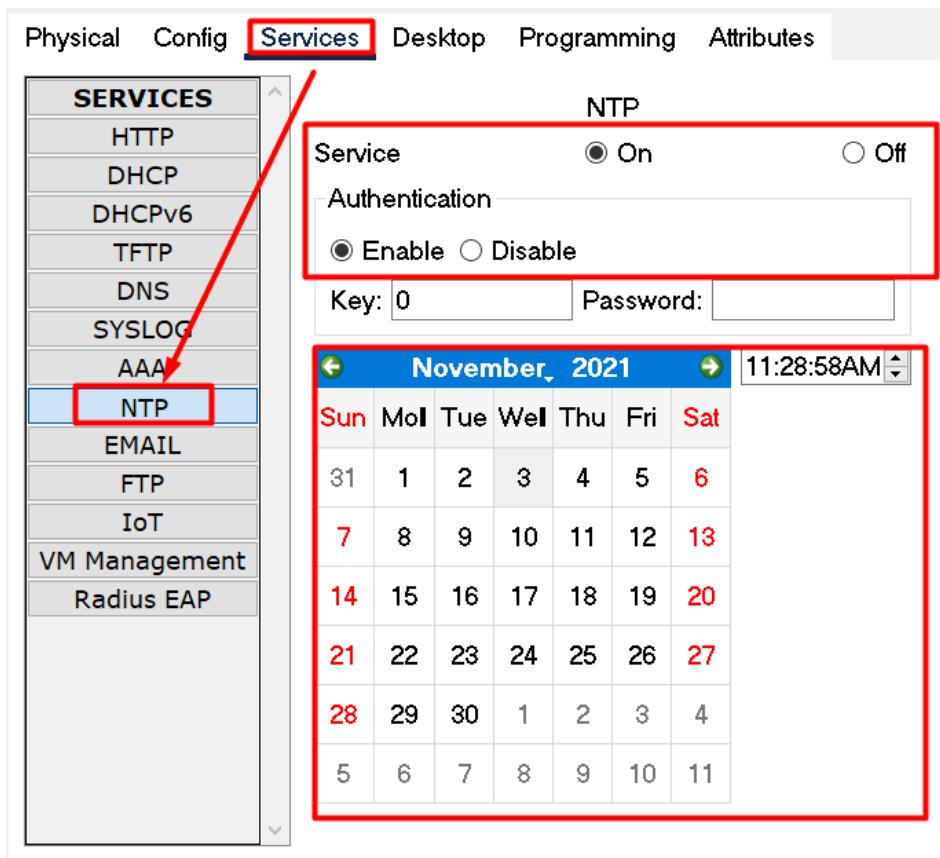
- Mengaktifkan interface dan memasang IP Address

```
R-IDN(config)#interface fa0/0  
R-IDN(config)#no shutdown  
R-IDN(config)#ip address 10.10.10.2 255.255.255.0
```

- Konfigurasi pada NTP Server
  - IP Server



- Mengaktifkan Service NTP pada Server



Untuk tanggal dan jam di sesuaikan pada saat kalian mengkonfigurasi NTP nya.

### 3. Mengaktifkan NTP Client pada Router

```
R-IDN(config)#ntp-server 10.10.10.1
R-IDN(config)#ntp update-calendar
```

### C. Pengecekan

#### 1. Perintah Pengecekan

```
R-LOCAL(config)#do show clock
```

Pada saat memasukkan perintah “do show clock” tanggal dan jam tidak langsung berubah harus memasukkan perintah “do show clock” berulang kali sampai tanggal dan jam berubah seperti gambar dibawah ini.

```
R-IDN(config)#do show clock
2:7:11.365 UTC Wed Nov 3 2021
```

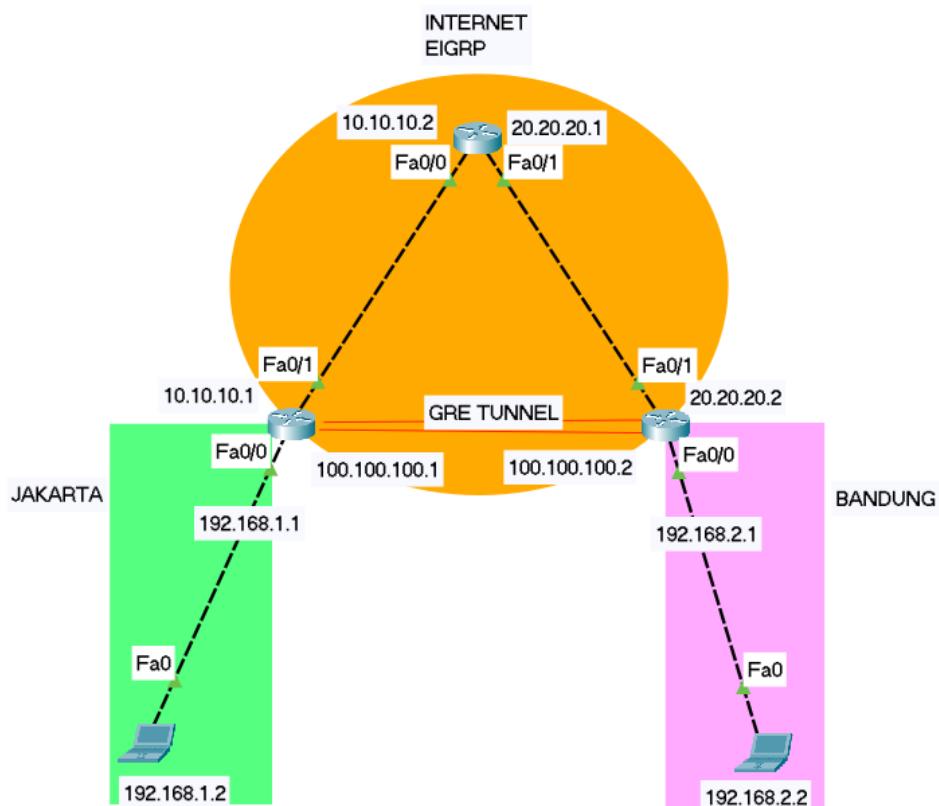
### D. Lab NTP telah selesai

# Tunnel

## Lab 38. Tunnel GRE

Dalam sebuah keperluan, biasanya sebuah instansi/perusahaan membutuhkan suatu koneksi yang sifatnya privat kesemua cabangnya yang terpisah dan letaknya berjauhan. Oleh karena itu, digunakanlah sebuah VPN (Virtual Private Network) agar komunikasi antar cabang tersebut aman. VPN ini dilewatkan lewat internet, jadi kita tidak perlu menarik kabel antar cabang yang jaraknya bisa mencapai puluhan bahkan ratusan kilo, cukup menggunakan VPN. Secara dasar, VPN membuat sebuah lubang atau tunnel pada internet sehingga keduanya dapat bertemu cara privat. singkatnya tunnel merupakan suatu layanan/service yang bertujuan membuat jalur pribadi. Pada Cisco sendiri sudah terdapat tunnel milik proprietary Cisco yaitu GRE tunnel.

Berikut Lab GRE Tunnel :



Langkah Langkah :

A. Konfigurasi di Router Kiri

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-KIRI
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KIRI(config)#interface fa0/0  
R-KIRI(config)#no shutdown  
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0  
  
R-KIRI(config)#interface fa0/1  
R-KIRI(config)#no shutdown  
R-KIRI(config)#ip address 10.10.10.1 255.255.255.0
```

### 3. Konfigurasi Route EIGRP

```
R-KIRI(config)#router eigrp 123  
R-KIRI(config)#network 10.10.10.0  
R-KIRI(config)#no auto summary
```

#### B. Konfigurasi di Router Kanan

##### 1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-KANAN
```

##### 2. Mengaktifkan interface dan memasang IP Address

```
R-KANAN(config)#interface fa0/0  
R-KANAN(config)#no shutdown  
R-KANAN(config)#ip address 192.168.2.1 255.255.255.0
```

```
R-KANAN(config)#interface fa0/1  
R-KANAN(config)#no shutdown  
R-KANAN(config)#ip address 20.20.20.2 255.255.255.0
```

##### 3. Konfigurasi Route EIGRP

```
R-KANAN(config)#router eigrp 123  
R-KANAN(config)#network 20.20.20.0  
R-KANAN(config)#no auto summary
```

#### C. Konfigurasi di Router Atas

##### 1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-ATAS
```

##### 2. Mengaktifkan interface dan memasang IP Address

```
R-ATAS(config)#interface fa0/0  
R-ATAS(config)#no shutdown  
R-ATAS(config)#ip address 10.10.10.2 255.255.255.0
```

```
R-ATAS(config)#interface fa0/1  
R-ATAS(config)#no shutdown  
R-ATAS(config)#ip address 20.20.20.1 255.255.255.0
```

##### 3. Konfigurasi Route EIGRP

```
R-ATAS(config)#router eigrp 123  
R-ATAS(config)#network 10.10.10.0  
R-ATAS(config)#no auto summary
```

#### D. Konfigurasi Tunnel GRE

##### 1. Router Kiri

```
R-KIRI(config)#interface tunnel 0  
R-KIRI(config)#ip address 100.100.100.1 255.255.255.252  
R-KIRI(config)#tunnel source fa0/1  
R-KIRI(config)#tunnel destination 20.20.20.2
```

##### 2. Router Kanan

```
R-KANAN(config)#interface tunnel 0  
R-KANAN(config)#ip address 100.100.100.2 255.255.255.252  
R-KANAN(config)#tunnel source fa0/1  
R-KANAN(config)#tunnel destination 10.10.10.1
```

#### Interface tunnel 0

Membuat interface pada tunnel 0

#### 100.100.100.0/24

IP Tunnel yang akan digunakan, kedua router harus memiliki IP yang berbeda

#### Tunnel source fa0/0

Tunnel source merupakan interface sumber yang berjalan diatas tunnel, yaitu interface yang terhubung ke internet.

#### Tunnel destination

IP tujuan yang mengarah ke internet, yang bukan IP tunnel dari router

Selanjutnya kita harus menambahkan routing ke jaringan local di interface tunnel kita

### E. Konfigurasi IP Route

#### 1. Router Kiri

```
R-KIRI(config)#ip route 192.168.2.0 255.255.255.0 100.100.100.2
```

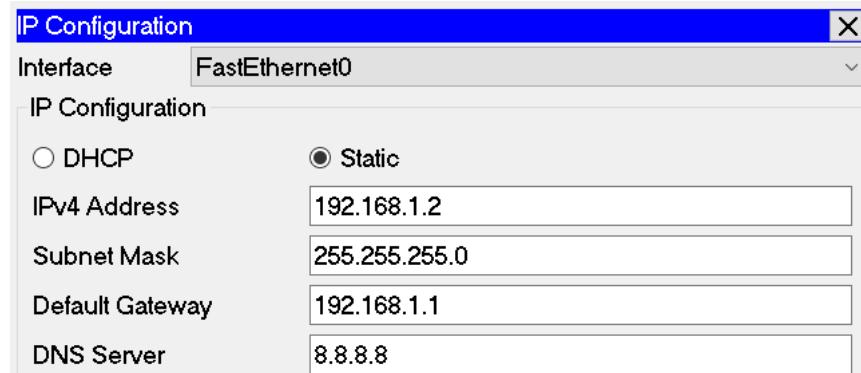
#### 2. Router Kanan

```
R-KANAN(config)#ip route 192.168.1.0 255.255.255.0 100.100.100.1
```

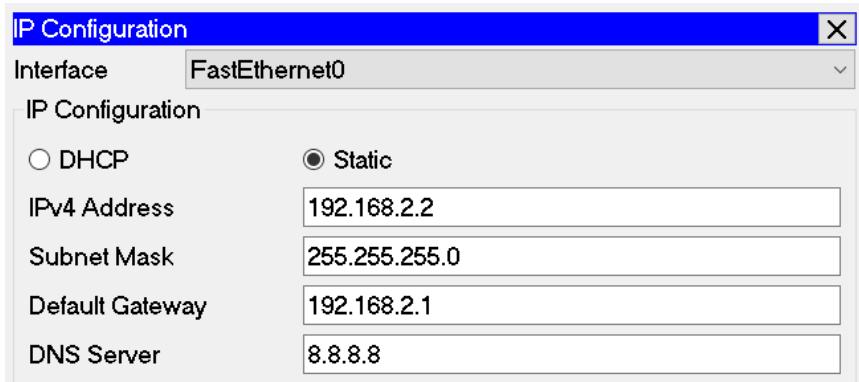
ip route (network local) (subnet mask) (gateway, IP Tunnel router lawan)

### F. Konfigurasi IP Address Laptop

#### 1. Laptop A



#### 2. Laptop B



Selanjutnya kita akan melakukan pengecekan apakah interface tunnel kita sudah berhasil dikonfigurasi/dijalankan.

#### G. Pengecekan

##### 1. Pengecekan interface tunnel Router Kiri

```
R-KIRI(config)#do show run
interface Tunnel0
ip address 100.100.100.1 255.255.255.252
mtu 1476
tunnel source FastEthernet0/1
tunnel destination 20.20.20.2
!
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.10.10.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router eigrp 10
network 10.0.0.0
!
ip classless
ip route 192.168.2.0 255.255.255.0 100.100.100.2
```

##### 2. Pengecekan interface tunnel Router Kanan

```
R-KANAN(config)#do show run
```

```

interface Tunnel0
 ip address 100.100.100.2 255.255.255.252
 mtu 1476
 tunnel source FastEthernet0/1
 tunnel destination 10.10.10.1
!
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 20.20.20.2 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 10
 network 20.0.0.0
!
in classless
ip route 192.168.1.0 255.255.255.0 100.100.100.1
!

```

Selanjutnya kita akan melakukan pengetesan dengan melakukan PING dan tracert, dan pastikan laptop menggunakan jalur tunnel kearah tujuan.

### Hasil PING Laptop A > Laptop B

```

C:\>ping 192.168.2.2

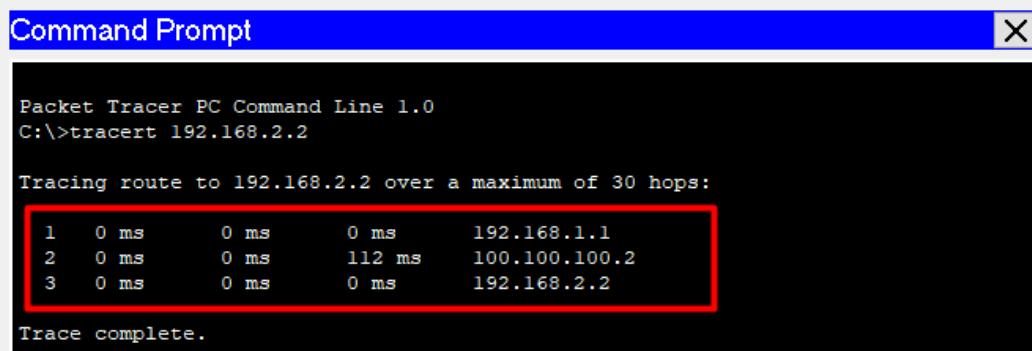
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=126

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

```

### Hasil Tracert Laptop A ➔ Laptop B



```

Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:
  1  0 ms      0 ms      0 ms      192.168.1.1
  2  0 ms      0 ms     112 ms    100.100.100.2
  3  0 ms      0 ms      0 ms    192.168.2.2

Trace complete.

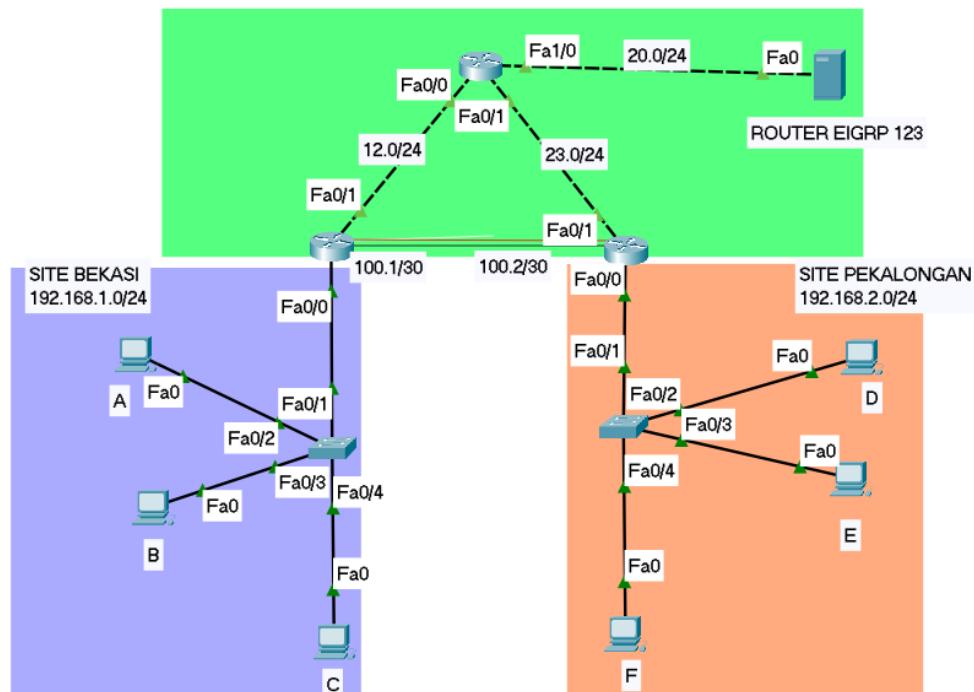
```

Bisa dilihat PING dari **Laptop A > Laptop B** menggunakan interface tunnel tandanya interface tunnel sudah berhasil diterapkan.

H. Lab Tunnel GRE telah selesai.

## Lab 39. Tunnel GRE With NAT

Pada lab sebelumnya kita hanya mengkonfigurasi tunnel saja, pada lab kali ini kita akan mengkonfigurasi tunnel dengan NAT agar tiap router memiliki akses internet.



Langkah Langkah :

A. Konfigurasi di Switch Kiri

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-KIRI
```

2. Melakukan Trunk

```
SW-KIRI(config)#interface fa0/1  
SW-KIRI(config)#do show trunk
```

B. Konfigurasi di Switch Kanan

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-KANAN
```

2. Melakukan Trunk

```
SW-KANAN(config)#interface fa0/1  
SW-KANAN(config)#do show trunk
```

C. Konfigurasi di Router Kiri

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal
```

- Router(config)#hostname R-KIRI
2. Mengaktifkan interface dan memasang IP Address

```
R-KIRI(config)#interface fa0/0
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0
```

```
R-KIRI(config)#interface fa0/1
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 12.12.12.1 255.255.255.0
```

3. Konfigurasi Route EIGRP

```
R-KIRI(config)#router eigrp 123
R-KIRI(config)#network 12.12.12.0 0.0.0.255
R-KIRI(config)#no auto-summary
```

D. Konfigurasi di Router Kanan

1. Mengganti hostname router

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KANAN
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KANAN(config)#interface fa0/0
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 192.168.2.1 255.255.255.0
```

```
R-KANAN(config)#interface fa0/1
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 23.23.23.2 255.255.255.0
```

3. Konfigurasi Route EIGRP

```
R-KANAN(config)#router eigrp 123
R-KANAN(config)#network 23.23.23.0 0.0.0.255
R-KANAN(config)#no auto-summary
```

E. Konfigurasi di Router Atas

1. Mengganti nama Router

```
Router>enable
Router#configure terminal
Router(config)#hostname R-ATAS
```

2. Mengaktifkan interface dan memasang IP Address

```
R-ATAS(config)#interface fa0/0
R-ATAS(config)#no shutdown
R-ATAS(config)#ip address 12.12.12.2 255.255.255.0
```

```
R-ATAS(config)#interface fa0/1
R-ATAS(config)#no shutdown
R-ATAS(config)#ip address 23.23.23.1 255.255.255.0
```

```
R-ATAS(config)#interface fa1/0
R-ATAS(config)#no shutdown
R-ATAS(config)#ip address 20.20.20.1 255.255.255.0
```

3. Konfigurasi Route EIGRP

```
R-ATAS(config)#router eigrp 123
```

```
R-ATAS(config)#network 23.23.23.0 0.0.0.255  
R-ATAS(config)#no auto-summary
```

Konfigurasi NAT Overload (Router Kiri)

```
R-KIRI(config)#access-list 1 permit any  
R-KIRI(config)#ip nat inside source list 1 interface fa0/1 overload
```

Konfigurasi NAT Overload (Router Kanan)

```
R-KANAN(config)#access-list 1 permit any  
R-KANAN(config)#ip nat inside source list 1 interface fa0/1 overload
```

Fungsi NAT disini agar semua client dapat mengakses internet, jenis NAT yang sekarang kita gunakan adalah NAT Overload.

Menentukan interface inside atau outside (Router Kiri)

```
R-KIRI(config)#interface fa0/0  
R-KIRI(config)#ip nat inside  
R-KIRI(config)#interface fa0/1  
R-KIRI(config)#ip nat outside
```

Menentukan interface inside atau outside (Router Kanan)

```
R-KANAN(config)#interface fa0/0  
R-KANAN(config)#ip nat inside  
R-KANAN(config)#interface fa0/1  
R-KANAN(config)#ip nat outside
```

## F. Konfigurasi Tunnel GRE

### 1. Router Kiri

```
R-ATAS(config)#interface tunnel 0  
R-ATAS(config)#ip address 100.100.100.1 255.255.255.252  
R-ATAS(config)#interface fa0/1  
R-ATAS(config)#tunnel destination 23.23.23.2
```

### 2. Router Kanan

```
R-ATAS(config)#interface tunnel 0  
R-ATAS(config)#ip address 100.100.100.2 255.255.255.252  
R-ATAS(config)#interface fa0/1  
R-ATAS(config)#tunnel destination 12.12.12.1
```

## G. Konfigurasi IP Route

### 1. Router Kiri

```
R-KIRI(config)#ip route 192.168.2.0 255.255.255.0 100.100.100.2
```

### 2. Router Kanan

```
R-KANAN(config)#ip route 192.168.1.0 255.255.255.0 100.100.100.1
```

## H. Konfigurasi IP Address Laptop

### 1. Laptop A

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP       Static

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 8.8.8.8

2. Laptop B

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP       Static

IPv4 Address 192.168.1.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 8.8.8.8

3. Laptop C

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP       Static

IPv4 Address 192.168.1.4

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 8.8.8.8

4. Laptop D

**IP Configuration**

Interface FastEthernet0

IP Configuration

DHCP       Static

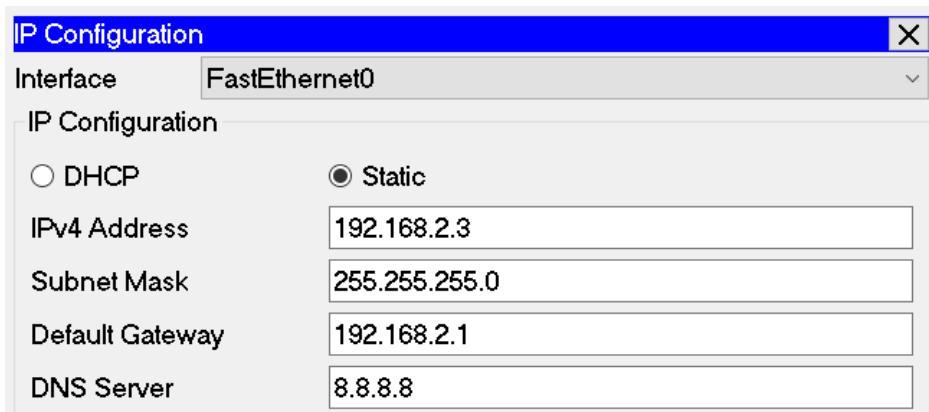
IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.0

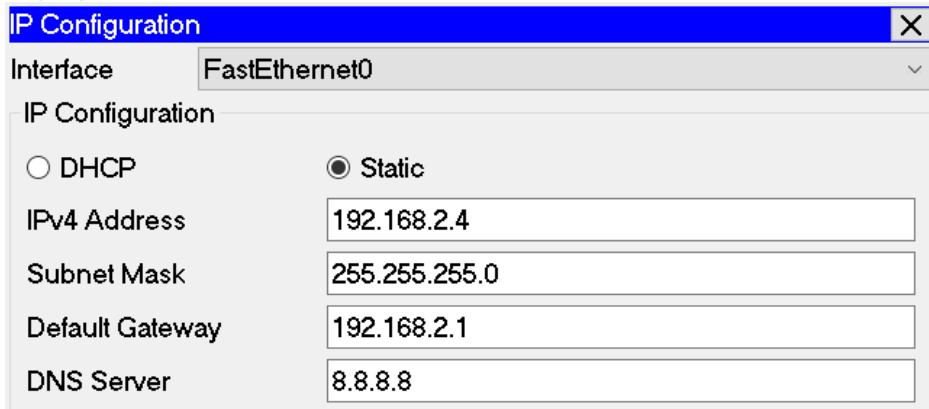
Default Gateway 192.168.2.1

DNS Server 8.8.8.8

5. Laptop E



#### 6. Laptop F



Selanjutnya kita akan melakukan pengecekan apakah interface tunnel kita sudah berhasil dikonfigurasi/dijalankan.

#### I. Pengecekan

##### 1. Pengecekan interface tunnel Router Kiri

```
R-KIRI(config)#do show run
interface Tunnel0
ip address 100.100.100.1 255.255.255.252
mtu 1476
tunnel source FastEthernet0/1
tunnel destination 23.23.23.2
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 12.12.12.1 255.255.255.0
ip nat outside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router eigrp 123
network 12.0.0.0
!
ip nat inside source list 1 interface FastEthernet0/1 overload
ip classless
ip route 192.168.2.0 255.255.255.0 100.100.100.2
```

## 2. Pengecekan interface tunnel Router Kanan

```
R-KANAN(config)#do show run
!
interface Tunnel0
 ip address 100.100.100.2 255.255.255.252
 mtu 1476
 tunnel source FastEthernet0/1
 tunnel destination 12.12.12.1
!
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 23.23.23.2 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 123
 network 23.0.0.0
!
ip nat inside source list 1 interface FastEthernet0/1 overload
ip classless
ip route 192.168.1.0 255.255.255.0 100.100.100.1
```

Selanjutnya kita akan melakukan pengetesan dengan melakukan PING dan tracert, dan pastikan laptop menggunakan jalur tunnel kearah tujuan.

### Hasil PING Laptop A > Laptop D

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 8ms
```

### Hasil Tracert Laptop A > Laptop D

```
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:
1  0 ms      0 ms      0 ms      192.168.1.1
2  0 ms      0 ms      0 ms      100.100.100.2
3  0 ms      0 ms      0 ms      192.168.2.2

Trace complete.
```

J. Lab Tunnel GRE With NAT telah selesai.

# **FHRP**

(First Hop Redundancy Protocol)

# FHRP Introduction

Pada sebuah instansi, perusahaan maupun jaringan lokal lainnya biasanya memiliki internet yang stabil, bagaimana jika gateway internet tersebut mati? Maka seluruh pegawai/karyawan terhambat proses kerjanya, maka dari itu biasanya di sebuah instansi memiliki gateway backup agar internet tetap stabil. Bisa dikatakan instansi tersebut memiliki 2 buah gateway internet, yang paling cepat menjadi prioritas, yang dibawahnya menjadi cadangan. Namun dengan 2 gateway pun masih tidak efisien, karena kita harus set satu persatu di tiap pc, gateway mana yang akan digunakan, jika salah satu gateway down, maka sebagian pc tidak bisa mengakses internet.

Dengan High Availability (HA), bisa dibuat seolah-olah ada satu IP gateway virtual. Sehingga walaupun salah gateway satunya down, pc client tetap dapat menggunakan internet.

Jenis First Hop Redudancy Protocol :

- HSRP (Hot Standby Redudancy Protocol) – Cisco Proprietary
- VRRP (Virtual Redudancy Router Protocol) -Multivendor
- GLBP (Gateway Load Balance Protocol) -Cisco Proprietary

Berikut Perbandingannya :

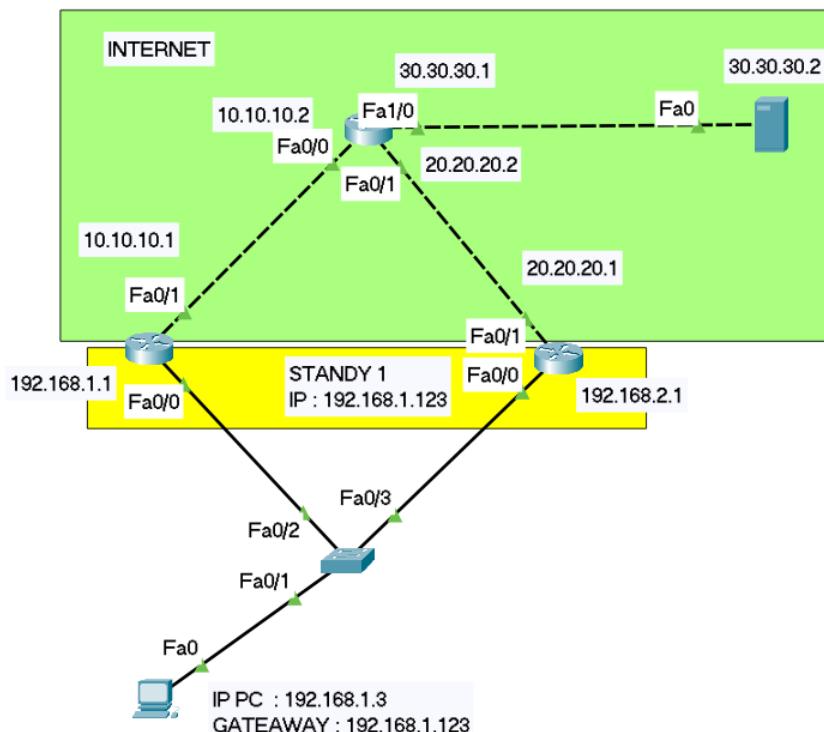
Protocol Features		HSRP (Hot Standby Router protocol)	VRRP (Virtual Redundancy Router Protocol)	GLBP (Gateway Load Balancing Protocol)
Router role		- 1 active router.- 1 standby router. - 1 or more listening routers.	- 1 master router.- 1 or more backup routers.	- 1 AVG (Active Virtual Gateway).- up to 4 AVF routers on the group (Active Virtual Forwarder) passing traffic.  - up to 1024 virtual routers (GLBP groups) per physical interface.
		- Use virtual ip address.	- Can use real router ip address, if not, the one with highest priority become master.	- Use virtual ip address.
Scope		Cisco proprietary	IEEE standard	Cisco proprietary
Election		Active Router: 1-Highest Priority 2-Highest IP (tiebreaker)	Master Router: 1-Highest Priority 2-Highest IP (tiebreaker)	Active Virtual Gateway: 1-Highest Priority 2-Highest IP (tiebreaker)
Optimization features	Tracking	yes	yes	yes
	Preempt	yes	yes	yes
	Timer adjustments	yes	yes	yes
Traffic type		224.0.0.2 – udp 1985 (version1) 224.0.0.102-udp 1985 (version2)	224.0.0.18 – udp 112	224.0.0.102 udp 3222
Timers		Hello – 3 seconds	Advertisement – 1 second	Hello – 3 seconds
		(Hold) 10 seconds	(Master Down Interval)3 * Advertisement + skew time	(Hold) 10 seconds
			(Skew time)(256-priority) / 256	
Load-balancing functionality		- Multiple HSRP group per interface/SVI/routed int.	- Multiple VRRP group per interface/SVI/routed int.	Load-balancing oriented- Weighted algorithm.  - Host-dependent algorithm.  - Round-Robin algorithm (default).
		Requires appropriate distribution of Virtual GW IP per Clients for optimal load-balancing.(generally through DHCP)	Requires appropriate distribution of Virtual GW IP per Clients for optimal load-balancing.(generally through DHCP)	Clients are transparently updated with virtual MAC according to load-balancing algorithm through ARP requesting a unique virtual gateway.

## Lab 40. HSRP

HSRP (Hot Standby Redundancy Protocol) merupakan protocol redundancy milik Cisco yang kini sudah menjadi multivendor. Menggunakan protokol UDP port number 1985 serta menggunakan IP Multicast 224.0.0.2 dalam berkomunikasi. Default **Hello-timer** dari HSRP adalah **3 detik** dengan **hold time 10 detik**.

Dalam HSRP, terdapat 3 istilah :

- Active Router: Router yang akan mengforward paket.
- Standby Router: Router yang akan backup jika Active Router mati.
- Standby Group: Kumpulan Router anggota HSRP.



Kita akan melakukan konfigurasi pada topologi diatas ini yang dimana terdapat 2 jalur gateway yang menuju internet.

Langkah Langkah :

A. Konfigurasi di Switch

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-GURU
```

2. Melakukan Trunk

```
SW-GURU(config)#interface fa0/2  
SW-GURU(config)#switchport mode trunk
```

```
SW-GURU(config)#interface fa0/3  
SW-GURU(config)#switchport mode trunk
```

B. Konfigurasi di Router Kiri

1. Mengganti hostname switch

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-KIRI
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KIRI(config)#interface fa0/0  
R-KIRI(config)#no shutdown  
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0
```

```
R-KIRI(config)#interface fa0/1  
R-KIRI(config)#no shutdown  
R-KIRI(config)#ip address 10.10.10.1 255.255.255.0
```

3. Konfigurasi Route EIGRP

```
R-KIRI(config)#router eigrp 123  
R-KIRI(config)#network 10.10.10.0  
R-KIRI(config)#no auto summary
```

Setelah itu gunakan routing agar antar network bisa saling terhubung

C. Konfigurasi di Router Kanan

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-KANAN
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KANAN(config)#interface fa0/0  
R-KANAN(config)#no shutdown  
R-KANAN(config)#ip address 192.168.2.1 255.255.255.0
```

```
R-KANAN(config)#interface fa0/1  
R-KANAN(config)#no shutdown  
R-KANAN(config)#ip address 20.20.20.1 255.255.255.0
```

3. Konfigurasi Route EIGRP

```
R-KANAN(config)#router eigrp 123  
R-KANAN(config)#network 10.10.10.0  
R-KANAN(config)#no auto summary
```

D. Konfigurasi di Router Atas

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-ATAS
```

2. Mengaktifkan interface dan memasang IP Address

```
R-ATAS(config)#interface fa0/0  
R-ATAS(config)#no shutdown  
R-ATAS(config)#ip address 192.168.2.1 255.255.255.0
```

```
R-ATAS(config)#interface fa0/1  
R-ATAS(config)#no shutdown  
R-ATAS(config)#ip address 20.20.20.1 255.255.255.0
```

### 3. Konfigurasi Route EIGRP

```
R-ATAS(config)#router eigrp 123  
R-ATAS(config)#network 10.10.10.0  
R-ATAS(config)#no auto summary
```

### E. Konfigurasi HSRP

#### 1. Router Kiri

```
R-KIRI(config)#interface fa0/0  
R-KIRI(config)#standby 1 ip 192.168.1.123  
R-KIRI(config)#standby 1 preempt
```

#### 2. Router Kanan

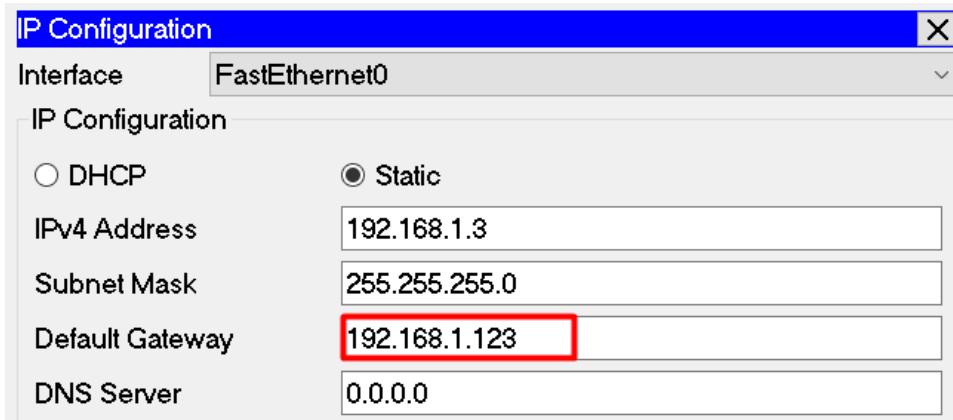
```
R-KANAN(config)#interface fa0/0  
R-KANAN(config)#standby 1 ip 192.168.1.123  
R-KANAN(config)#standby 1 preempt
```

### **SETTING HSRP DI R1 DAN R2 HSRP !**

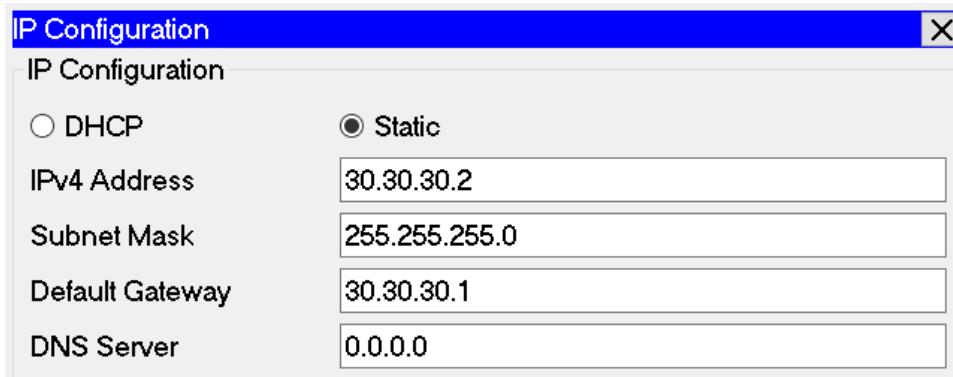
Diaktifkan di interface yang mengarah ke jaringan lokalnya, pada HSRP ini, kita dapat membuat sebuah IP gateway palsu yang akan digunakan oleh client. Router yang menjadi jalur utama harus memiliki priority yang lebih besar dari jalur lainnya. Default Priority: 100.

### F. Konfigurasi IP PC dan Server

#### 1. PC



#### 2. Server



Setelah itu melakukan pengecekan “**do show standby brief**” untuk memastikan HSRP sudah berhasil dikonfigurasi.

## G. Pengecekan HRRP

### 1. Router Kiri

```
R-KIRI(config)#do show stand brief
R-KIRI(config-if)#do sh stand brief
    P indicates configured to preempt.
    |
Interface  Grp   Pri  P State      Active          Standby        Virtual IP
Fa0/0       1     100  P Active    local           192.168.1.1    192.168.1.123
```

### 2. Router Kanan

```
R-KANAN(config)#do show stand brief
R-KANAN(config-if)#do show stand brief
    P indicates configured to preempt.
    |
Interface  Grp   Pri  P State      Active          Standby        Virtual IP
Fa0/0       1     100  P Standby   192.168.1.1    local          192.168.1.123
```

HSRP sudah berhasil diterapkan langkah selanjutnya yaitu melakukan pengetesan PING PC kearah server untuk mengetahui PC tersebut melewati jalur gateway yang mana.

### Hasil PING PC > Server

```
C:\>ping 30.30.30.2

Pinging 30.30.30.2 with 32 bytes of data:

Reply from 30.30.30.2: bytes=32 time<lms TTL=126

Ping statistics for 30.30.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

### Hasil Tracert PC > Server

```
C:\>tracert 30.30.30.2

Tracing route to 30.30.30.2 over a maximum of 30 hops:
    1  0 ms      0 ms      0 ms      192.168.1.1
    2  0 ms      0 ms      0 ms      10.10.10.2
    3  0 ms      0 ms      0 ms      30.30.30.2

Trace complete.
```

Bisa dilihat bahwa ping dari PC ke Server menggunakan IP Gateway 192.168.1.1. Setelah itu kita coba mematikan interface fa0/0 yaitu Router Kiri

Mematikan interface fa0/0

```
R-KIRI(config)#interface fa0/0
R-KIRI(config)#shutdown
```

### Hasil PING PC > Server lagi

```
C:\>ping 30.30.30.2

Pinging 30.30.30.2 with 32 bytes of data:

Reply from 30.30.30.2: bytes=32 time<1ms TTL=126

Ping statistics for 30.30.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

### Tracert PING PC > Server lagi

```
C:\>tracert 30.30.30.2

Tracing route to 30.30.30.2 over a maximum of 30 hops:
1  0 ms      0 ms      0 ms      192.168.1.2
2  0 ms      0 ms      0 ms      20.20.20.2
3  0 ms      0 ms      0 ms      30.30.30.2

Trace complete.
```

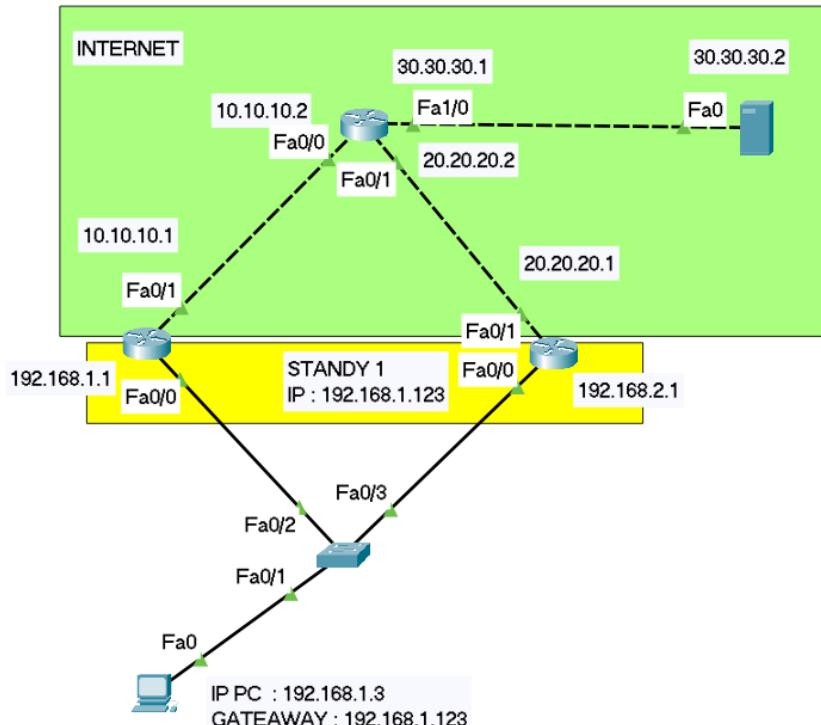
Bisa dilihat bahwa ketika interface salah satu jalur gateway mati maka PC akan melewati jalur cadangannya.

H. Lab HSRP telah selesai.

## Lab 41. Priority HSRP

Priority HSRP digunakan untuk menentukan router mana yang harus menjadi Active dan mana yang harus menjadi Standby, singkatnya menentukan jalur utama dan jalur cadangan. Secara default priority pada HSRP adalah 100 dan maksimalnya 255.

Jadi, dalam lab ini kita akan menentukan router mana yang akan menjadi Active dan mana yang akan menjadi Standby. Dan jika kedua router itu memiliki priority yang sama, router akan menentukannya sendiri melalui IP Address terkecil. Router yang memiliki priority tertinggi akan menjadi router utama (Active).



Kita akan menggunakan lab yang sama seperti yang sebelumnya, tujuan akhir kita merubah nilai priority di router kanan agar router tsb menjadi jalur utama (Active)

Langkah Langkah :

A. Konfigurasi Priority HSRP

1. Router Kiri

```
R-KIRI(config)#interface fa0/0
R-KIRI(config)#standby 1 priority 200
```

2. Router Kanan

```
R-KANAN(config)#interface fa0/0
R-KANAN(config)#standby 1 priority 250
```

B. Pengecekan

1. Pengecekan Status Priority Router Kiri

```
R-KIRI(config)#do show standby brief
```

```
R-KIRI(config)#do show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State      Active           Standby        Virtual IP
Fa0/0       1    200  P Standby   192.168.1.2     local          192.168.1.123
```

2. Pengecekan Status Priority Router Kanan

```
R-KANAN(config)#do show standby brief
R-KANAN(config)#do show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State      Active           Standby        Virtual IP
Fa0/0       1    250  P Active    local          192.168.1.1     192.168.1.123
```

Maka Router Kanan sudah menjadi jalur utama (Active) dan Router Kiri menjadi jalur cadangan (Standby).

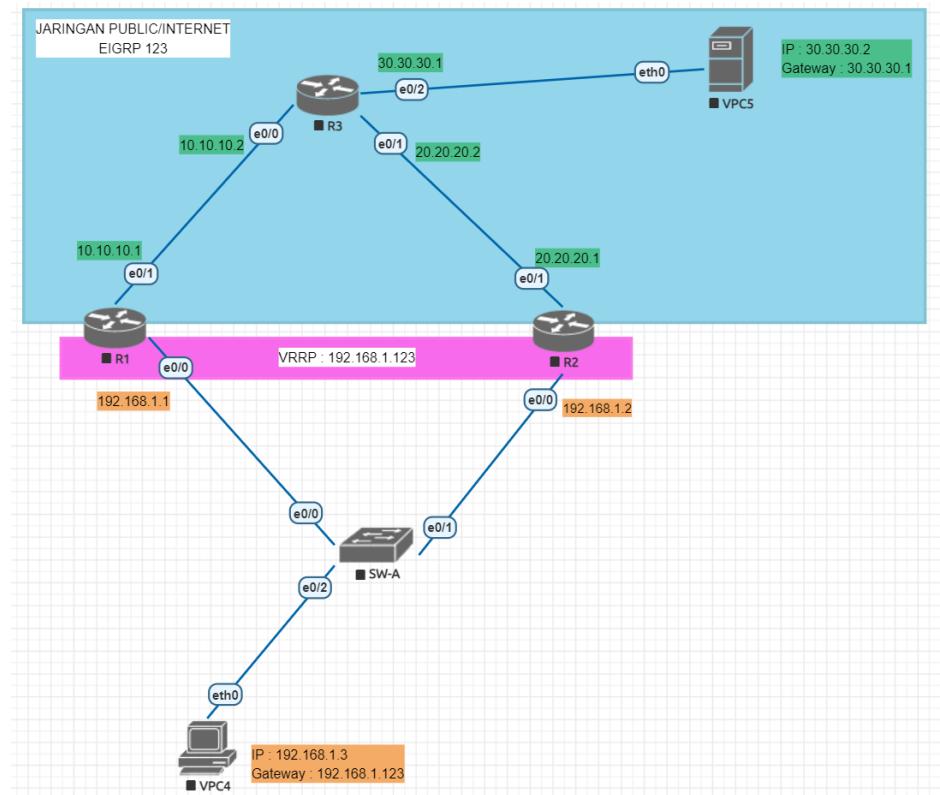
C. Lab Priority HSRP telah selesai.

## Lab 42. VRRP

VRRP (Virtual Redudancy Router Protocol) memiliki konsep yang sama seperti HSRP, hanya saja VRRP milik semua vendor alias multivendor, sedangkan HSRP hanya milik Cisco. VRRP ini dibuat oleh Lembaga internasional yakni IEEE dengan tujuan yang sama seperti HSRP yaitu Redudancy. Default **Hello-timer** dari VRRP adalah **1 detik**. Dan VRRP tidak support Cisco Packet Tracer maka dari itu kita menggunakan VMware Emulator.

Sama seperti HSRP, VRRP juga terdapat 3 istilah yang artinya sama :

- **Master Router:** Router yang akan mengforward paket.
- **Backup Router:** Router yang akan backup jika Active Router mati.
- **VRRP Group:** Kumpulan Router anggota HSRP.



Kita akan melakukan konfigurasi pada topologi diatas ini yang dimana terdapat 2 jalur gateway yang menuju internet.

Langkah Langkah :

A. Konfigurasi di Switch

1. Mengganti hostname switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-IDN
```

2. Melakukan Trunk

```
SW-IDN(config)#interface range e0/1-2  
SW-IDN(config)#switchport encapsulation dot1q  
SW-IDN(config)#switchport mode trunk
```

B. Konfigurasi di Router Kiri

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-KIRI
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KIRI(config)#interface e0/0  
R-KIRI(config)#no shutdown  
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0  
  
R-KIRI(config)#interface e0/1  
R-KIRI(config)#no shutdown  
R-KIRI(config)#ip address 10.10.10.1 255.255.255.0
```

#### C. Konfigurasi di Router Kanan

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-KANAN
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KANAN(config)#interface e0/0  
R-KANAN(config)#no shutdown  
R-KANAN(config)#ip address 192.168.1.2 255.255.255.0  
  
R-KANAN(config)#interface e0/1  
R-KANAN(config)#no shutdown  
R-KANAN(config)#ip address 20.20.20.1 255.255.255.0
```

#### D. Konfigurasi di Router Atas

1. Mengganti hostname router

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-ATAS
```

2. Mengaktifkan interface dan memasang IP Address

```
R-ATAS(config)#interface e0/0  
R-ATAS(config)#no shutdown  
R-ATAS(config)#ip address 10.10.10.2 255.255.255.0  
  
R-ATAS(config)#interface e0/1  
R-ATAS(config)#no shutdown  
R-ATAS(config)#ip address 20.20.20.2 255.255.255.0  
  
R-ATAS(config)#interface e0/2  
R-ATAS(config)#no shutdown  
R-ATAS(config)#ip address 30.30.30.1 255.255.255.0
```

#### Konfigurasi NAT Overload (Router Kiri)

```
R-KIRI(config)#access-list 1 permit any  
R-KIRI(config)#ip nat inside source list 1 interface e0/1 overload  
R-KIRI(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

Menentukan interface inside atau outside

```
R-KIRI(config)#interface e0/0
```

```
R-KIRI(config)#ip nat inside  
R-KIRI(config)#interface e0/1  
R-KIRI(config)#ip nat outside
```

#### Konfigurasi NAT Overload (Router Kanan)

```
R-KANAN(config)#access-list 1 permit any  
R-KANAN(config)#ip nat inside source list 1 interface e0/1 overload  
R-KANAN(config)#ip route 0.0.0.0 0.0.0.0 20.20.20.2  
Menentukan interface inside atau outside
```

```
R-KANAN(config)#interface e0/0  
R-KANAN(config)#ip nat inside  
R-KANAN(config)#interface e0/1  
R-KANAN(config)#ip nat outside
```

Fungsi NAT disini agar semua client dapat mengakses internet, jenis NAT yang sekarang kita gunakan adalah NAT Overload.

#### E. Konfigurasi VRRP

##### 1. Router Kiri

```
R-KIRI(config)#interface e0/0  
R-KIRI(config)#vrrp 1 ip 192.168.1.123  
R-KIRI(config)#vrrp 1 preempt
```

##### 2. Router Kanan

```
R-KANAN(config)#interface e0/0  
R-KANAN(config)#vrrp 1 ip 192.168.1.123  
R-KANAN(config)#vrrp 1 preempt
```

Pada lab **HSRP** perintahnya menggunakan “**standby**” dulu nah pada **VRRP** perintah “**vrrp**” dulu sesuai namanya begitupula seterusnya. Setelah itu kita setting IP Address nya, pada VMware cara setting IP Address nya sangat berbeda berikut cara kongifurasi IP Address di VMware :

#### F. Konfigurasi PC

##### 1. PC Bawah

- Cara memasang IP Address di VMware

```
VPCS> ip 192.168.1.3/24 gateway 192.168.1.123  
Checking for duplicate address...  
PC1 : 192.168.1.3 255.255.255.0 gateway 192.168.1.123
```

**Gateway yang dipakai adalah gateway dari VRRP yang di config tadi.**

- Cara mengecek IP yang sudah dipasang di PC tersebut

```
VPCS> show ip

NAME      : VPCS[1]
IP/MASK   : 192.168.1.3/24
GATEWAY   : 192.168.1.123
DNS       :
MAC       : 00:50:79:66:68:04
LPORT     : 20000
RHOST:PORT: 127.0.0.1:30000
MTU       : 1500
```

2. PC Atas

- Memasang IP Address dan Gateway

```
VPCS> ip 30.30.30.2/24 gateway 30.30.30.1
Checking for duplicate address...
PC1 : 30.30.30.2 255.255.255.0 gateway 30.30.30.1
```

- Mengecek IP Address dan Gateway

```
VPCS> show ip

NAME      : VPCS[1]
IP/MASK   : 30.30.30.2/24
GATEWAY   : 30.30.30.1
DNS       :
MAC       : 00:50:79:66:68:05
LPORT     : 20000
RHOST:PORT: 127.0.0.1:30000
MTU       : 1500
```

#### G. Pengecekan VRRP

1. Router Kiri

```
R-KIRI(config)#do show vrrp brief
R-KIRI(config-if)#do sh vrrp brief
Interface      Grp Pri Time  Own Pre State    Master addr      Group addr
Et0/0          1   100 3609      Y  Backup    192.168.1.2      192.168.1.123
```

2. Router Kanan

```
R-KANAN(config)#do show vrrp brief
R-KANAN(config-if)#do show vrrp brief
Interface      Grp Pri Time  Own Pre State    Master addr      Group addr
Et0/0          1   100 3609      Y  Master    192.168.1.2      192.168.1.123
```

Pengecekan VRRP hanya mengganti “**standby brief**” itu adalah perintah pengecekan HSRP “**vrrp brief**” adalah pengecekan untuk VRRP, setelah itu kita akan melakukan pengetesan dengan melakukan PING dari **PC > Server**.

#### PC > Server

```
VPCS> ping 30.30.30.2
```

```
84 bytes from 30.30.30.2 icmp_seq=1 ttl=62 time=12.182 ms
84 bytes from 30.30.30.2 icmp_seq=2 ttl=62 time=5.152 ms
84 bytes from 30.30.30.2 icmp_seq=3 ttl=62 time=4.534 ms
84 bytes from 30.30.30.2 icmp_seq=4 ttl=62 time=4.169 ms
84 bytes from 30.30.30.2 icmp_seq=5 ttl=62 time=4.110 ms
```

#### Tracert PC > Server

```
VPCS> trace 30.30.30.2
```

```
trace to 30.30.30.2, 8 hops max, press Ctrl+C to stop
1 192.168.1.2 3.684 ms 2.181 ms 11.220 ms
2 20.20.20.2 4.316 ms 3.402 ms 2.989 ms
3 *30.30.30.2 3.649 ms (ICMP type:3, code:3, Destination port unreachable)
```

Bisa dilihat bahwa ping dari PC ke Server menggunakan IP Gateway 192.168.1.2  
Setelah itu kita coba mematikan **interface e0/0** yaitu Router Kanan

Mematikan interface e0/0

```
R-KANAN(config)#interface e0/0
R-KANAN(config)#shutdown
```

#### Hasil PING PC > Server lagi

```
VPCS> ping 30.30.30.2
```

```
84 bytes from 30.30.30.2 icmp_seq=1 ttl=62 time=6.735 ms
84 bytes from 30.30.30.2 icmp_seq=2 ttl=62 time=3.529 ms
84 bytes from 30.30.30.2 icmp_seq=3 ttl=62 time=3.312 ms
84 bytes from 30.30.30.2 icmp_seq=4 ttl=62 time=3.956 ms
84 bytes from 30.30.30.2 icmp_seq=5 ttl=62 time=3.851 ms
```

#### Tracert PC > Server lagi

```
VPCS> trace 30.30.30.2
```

```
trace to 30.30.30.2, 8 hops max, press Ctrl+C to stop
1 192.168.1.1 2.425 ms 2.576 ms 2.500 ms
2 10.10.10.2 2.887 ms 6.853 ms 2.504 ms
3 *30.30.30.2 7.196 ms (ICMP type:3, code:3, Destination port unreachable)
```

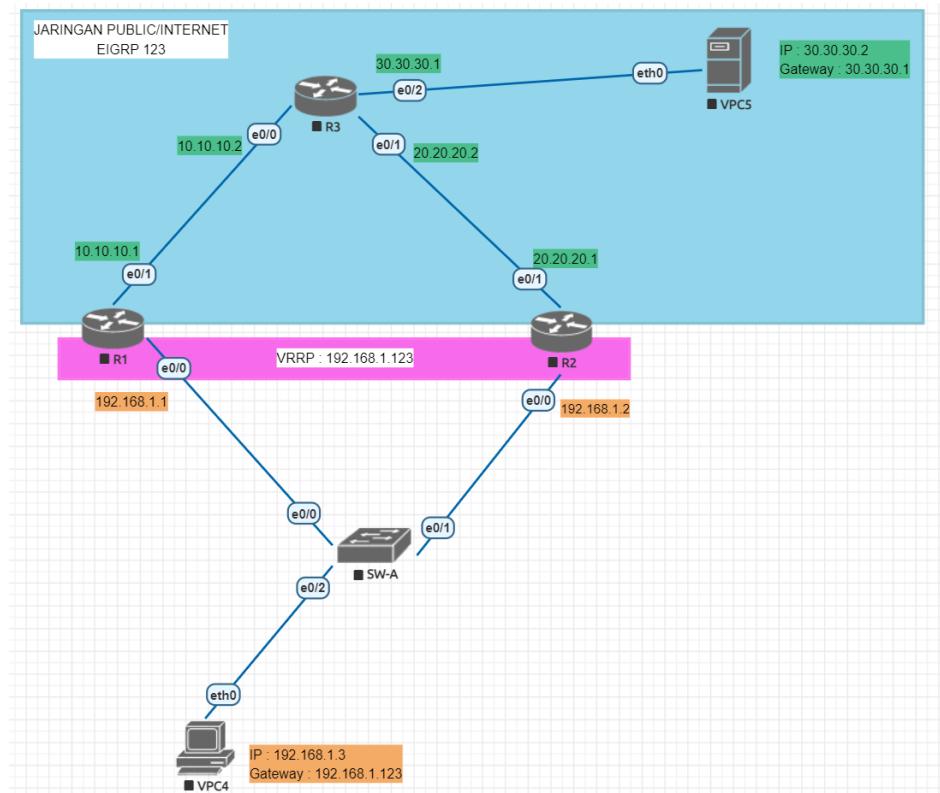
Bisa dilihat bahwa ketika interface salah satu jalur gateway mati maka PC akan melewati jalur cadangannya.

H. Lab VRRP telah selesai.

## Lab 43. Priority VRRP

Priority VRRP digunakan untuk menentukan router mana yang harus menjadi Active dan mana yang harus menjadi Standby, singkatnya menentukan jalur utama dan jalur cadangan. Secara default priority pada HSRP adalah 100 dan maksimalnya 255.

Jadi, dalam lab ini kita akan menentukan router mana yang akan menjadi Active dan mana yang akan menjadi Standby. Dan jika kedua router itu memiliki priority yang sama, router akan menentukannya sendiri melalui IP Address terkecil. Router yang memiliki priority tertinggi akan menjadi router utama (Active).



Kita akan menggunakan lab yang sama seperti yang sebelumnya, tujuan akhir kita merubah nilai priority di router kanan agar router tsb menjadi jalur utama (Active)

Langkah Langkah :

A. Konfigurasi Priority HSRP

1. Router Kiri

```
R-KIRI(config)#interface e0/0
R-KIRI(config)#standby 1 priority 200
```

2. Router Kanan

```
R-KANAN(config)#interface e0/0
R-KANAN(config)#standby 1 priority 250
```

B. Pengecekan

1. Pengecekan Status Priority Router Kiri

```
R-KIRI(config)#do show standby brief
```

```
R-KIRI(config)#do show vrrp brief
Interface      Grp Pri Time  Own Pre State    Master addr   Group addr
Et0/0          1   200 3218     Y Master    192.168.1.1   192.168.1.123
R-KIRI(config)#
R-KIRI(config)#

```

## 2. Pengecekan Status Priority Router Kanan

```
R-KANAN(config)#do show standby brief
R-KANAN(config)#do show vrrp brief
Interface      Grp Pri Time  Own Pre State    Master addr   Group addr
Et0/0          1   250 3023     Y Init      0.0.0.0    192.168.1.123
R-KANAN(config)#
R-KANAN(config)#

```

Maka Router Kanan sudah menjadi jalur utama (Init) dan Router Kiri menjadi jalur cadangan (Master).

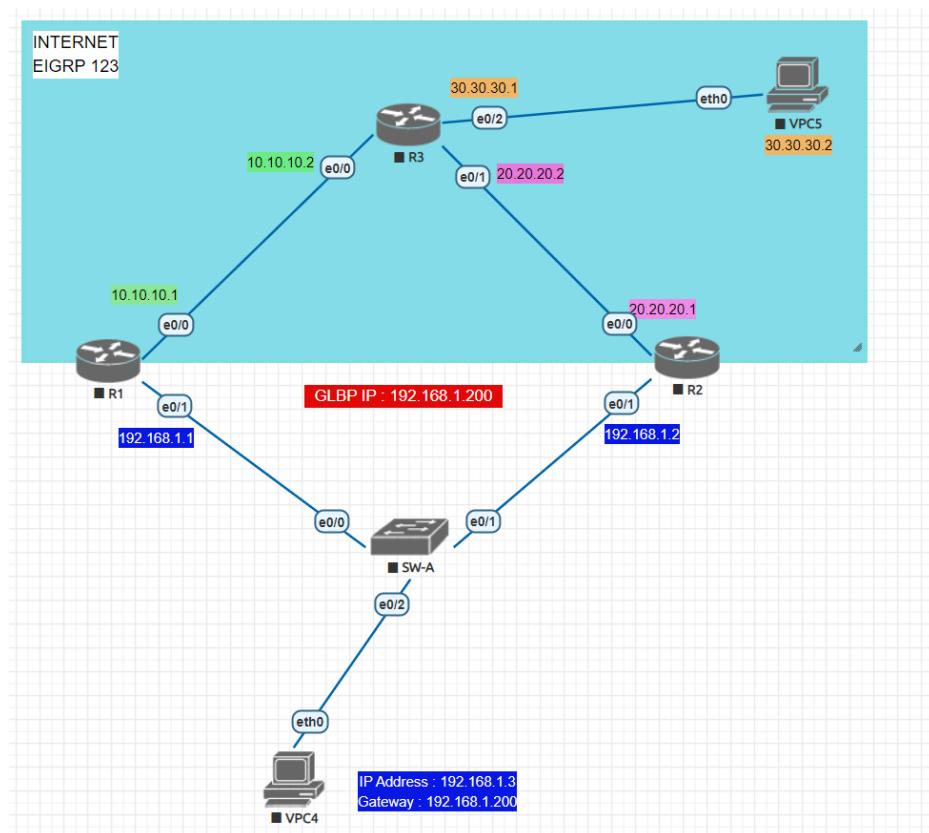
## C. Lab Priority HSRP telah selesai.

## Lab 44. GLBP

GLBP (Gateway Load Balancing Protocol) merupakan protokol redundancy milik Cisco, menggunakan menggunakan protokol UDP dengan port numbernya 3222 dengan IP multycat 224.0.0.102. Berbeda dengan HSRP, GLBP menggunakan tipe Load Balancing dalam redundansinya. Jika pada HSRP dan VRRP dapat membagi gateway menjadi jalur utama dan cadangan, maka GLBP justru menggunakan kedua gateway tersebut untuk digunakan dalam waktu bersamaan, hal ini disebut dengan load balancing. Default **Hello-timer** dari GLBP adalah **3 detik** dengan **hold time 10 detik**.

GLBP juga memiliki 3 istilah :

- **AVG** (Active Virtual Gateway): Menjadi gateway pengiriman packet, kemudian membagi clientnya dengan load balancing bersama AVF .
- **AVF** (Active Virtual Forwarder): Bertugas untuk mengirimkan packet untuk client tersebut
- **GLBP Group** : Kumpulan Router anggota HSRP.



Kita akan melakukan konfigurasi pada topologi diatas ini yang dimana terdapat 2 jalur gateway yang menuju internet.

Langkah Langkah :

- A. Konfigurasi di Switch
  1. Mengganti nama Switch

```
Switch>enable  
Switch#configure terminal  
Switch(config)#hostname SW-IDN
```

2. Melakukan Trunk

```
SW-IDN(config)#interface range e0/1-2
SW-IDN(config)#switchport encapsulation dot1q
SW-IDN(config)#switchport mode trunk
```

B. Konfigurasi di Router Kiri

1. Mengganti nama Router

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KIRI
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KIRI(config)#interface e0/0
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 192.168.1.1 255.255.255.0
```

```
R-KIRI(config)#interface e0/1
R-KIRI(config)#no shutdown
R-KIRI(config)#ip address 10.10.10.1 255.255.255.0
```

C. Konfigurasi di Router Kanan

1. Mengganti nama Router

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KANAN
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KANAN(config)#interface e0/0
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 192.168.1.2 255.255.255.0
```

```
R-KANAN(config)#interface e0/1
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 20.20.20.1 255.255.255.0
```

D. Konfigurasi di Router Kanan

1. Mengganti nama Router

```
Router>enable
Router#configure terminal
Router(config)#hostname R-KANAN
```

2. Mengaktifkan interface dan memasang IP Address

```
R-KANAN(config)#interface e0/0
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 10.10.10.2 255.255.255.0
```

```
R-KANAN(config)#interface e0/1
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 20.20.20.2 255.255.255.0
```

```
R-KANAN(config)#interface e0/2
R-KANAN(config)#no shutdown
R-KANAN(config)#ip address 30.30.30.1 255.255.255.0
```

Konfigurasi NAT Overload (Router Kiri)

```
R-KIRI(config)#access-list 1 permit any
```

```
R-KIRI(config)#ip nat inside source list 1 interface e0/1 overload
```

```
R-KIRI(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

Menentukan interface inside atau outside

```
R-KIRI(config)#interface ea0/0
```

```
R-KIRI(config)#ip nat inside
```

```
R-KIRI(config)#interface e0/1
```

```
R-KIRI(config)#ip nat outside
```

### Konfigurasi NAT Overload (Router Kanan)

```
R-KANAN(config)#access-list 1 permit any
```

```
R-KANAN(config)#ip nat inside source list 1 interface e0/1 overload
```

```
R-KANAN(config)#ip route 0.0.0.0 0.0.0.0 20.20.20.2
```

Menentukan interface inside atau outside

```
R-KANAN(config)#interface e0/0
```

```
R-KANAN(config)#ip nat inside
```

```
R-KANAN(config)#interface e0/1
```

```
R-KANAN(config)#ip nat outside
```

Fungsi NAT disini agar semua client dapat mengakses internet, jenis NAT yang sekarang kita gunakan adalah NAT Overload.

## E. Konfigurasi GLBP

### 1. Router Kiri

```
R-KIRI(config)#interface e0/1
```

```
R-KIRI(config)#glbp 1 ip 192.168.1.200
```

```
R-KIRI(config)#glbp 1 preempt
```

### 2. Router Kanan

```
R-KANAN(config)#interface e0/1
```

```
R-KANAN(config)#glbp 1 ip 192.168.1.200
```

```
R-KANAN(config)#glbp 1 preempt
```

Pada lab **HSRP** perintahnya menggunakan “**standby**” dulu, pada **VRRP** perintah pertama menggunakan “**vrrp**” dulu sesuai namanya begitupula seterusnya. Nah jika di **GLBP** pun sama seperti VRRP menggunakan perintah “**glbp**” dulu sesuai namanya.

## F. Konfigurasi PC

### 1. PC Bawah

```
VPCS> ip 192.168.1.3/24 gateway 192.168.1.200
```

```
Checking for duplicate address...
```

```
PC1 : 192.168.1.3 255.255.255.0 gateway 192.168.1.200
```

### 2. PC Atas

```
VPCS> ip 30.30.30.2/24 gateway 30.30.30.1
```

```
Checking for duplicate address...
```

```
PC1 : 30.30.30.2 255.255.255.0 gateway 30.30.30.1
```

## G. Pengecekan GLBP

### 1. Router Kiri

```
R-KIRI(config)#do show glbp brief
R-KIRI(config)#do show glbp brief
Interface  Grp  Fwd Pri State      Address          Active router   Standby router
Et0/1      1    -   100 Active     192.168.1.200 local           192.168.1.2
Et0/1      1    1   -   Active     0007.b400.0101 local           -
Et0/1      1    2   -   Listen      0007.b400.0102 192.168.1.2           -
```

### 2. Router Kanan

```
R-KANAN(config)#do show glbp brief
R-KANAN(config-if)#do show glbp brief
Interface  Grp  Fwd Pri State      Address          Active router   Standby router
Et0/1      1    -   100 Standby   192.168.1.200 192.168.1.1 local
Et0/1      1    1   -   Listen      0007.b400.0101 192.168.1.1           -
Et0/1      1    2   -   Active     0007.b400.0102 local           -
```

Pengecekan VRRP hanya mengganti “**standby brief**” itu adalah perintah pengecekan HSRP “**vrrp brief**” adalah pengecekan untuk VRRP, dan untuk “**glbp brief**” itu adalah perintah pengecekan untuk GLBP, setelah itu kita akan melakukan pengetesan dengan melakukan PING dari **PC > Server**.

### PC > Server

```
VPCS> ping 30.30.30.2
84 bytes from 30.30.30.2 icmp_seq=1 ttl=62 time=12.182 ms
84 bytes from 30.30.30.2 icmp_seq=2 ttl=62 time=5.152 ms
84 bytes from 30.30.30.2 icmp_seq=3 ttl=62 time=4.534 ms
84 bytes from 30.30.30.2 icmp_seq=4 ttl=62 time=4.169 ms
84 bytes from 30.30.30.2 icmp_seq=5 ttl=62 time=4.110 ms
```

### Tracert PC > Server

```
VPCS> trace 30.30.30.2
trace to 30.30.30.2, 8 hops max, press Ctrl+C to stop
1 192.168.1.2 3.684 ms 2.181 ms 11.220 ms
2 20.20.20.2 4.316 ms 3.402 ms 2.989 ms
3 *30.30.30.2 3.649 ms (ICMP type:3, code:3, Destination port unreachable)
```

Bisa dilihat bahwa ping dari PC ke Server menggunakan IP Gateway 192.168.1.2  
Setelah itu kita coba mematikan **interface e0/0** yaitu Router Kanan

Mematikan interface e0/0

```
R-KANAN(config)#interface e0/0
R-KANAN(config)#shutdown
```

### Hasil PING PC > Server lagi

```
VPCS> ping 30.30.30.2
84 bytes from 30.30.30.2 icmp_seq=1 ttl=62 time=6.735 ms
84 bytes from 30.30.30.2 icmp_seq=2 ttl=62 time=3.529 ms
84 bytes from 30.30.30.2 icmp_seq=3 ttl=62 time=3.312 ms
84 bytes from 30.30.30.2 icmp_seq=4 ttl=62 time=3.956 ms
84 bytes from 30.30.30.2 icmp_seq=5 ttl=62 time=3.851 ms
```

### Tracert PC > Server lagi

```
VPCS> trace 30.30.30.2
trace to 30.30.30.2, 8 hops max, press Ctrl+C to stop
1  192.168.1.1    2.425 ms  2.576 ms  2.500 ms
2  10.10.10.2    2.887 ms  6.853 ms  2.504 ms
3  *30.30.30.2   7.196 ms (ICMP type:3, code:3, Destination port unreachable)
```

Bisa dilihat bahwa ketika interface salah satu jalur gateway mati maka PC akan melewati jalur cadangannya.

H. Lab GLBP telah selesai.

# FIRST HOP REDUNDANCY

packetlife.net

Protocols		Attributes		
		HSRP	VRRP	GLBP
<b>Hot Standby Router Protocol (HSRP)</b>	Provides default gateway redundancy using one active and one standby router; standardized but licensed by Cisco Systems	<b>Standard</b> RFC 2281	RFC 3768	Cisco
<b>Virtual Router Redundancy Protocol (VRRP)</b>	An open-standard alternative to Cisco's HSRP, providing the same functionality	<b>Load Balancing</b> No	No	Yes
<b>Gateway Load Balancing Protocol (GLBP)</b>	Supports arbitrary load balancing in addition to redundancy across gateways; Cisco proprietary	<b>IPv6 Support</b> Yes	No	Yes
		<b>Transport</b> UDP/1985	IP/112	UDP/3222
		<b>Default Priority</b> 100	100	100
		<b>Default Hello</b> 3 sec	1 sec	3 sec
		<b>Multicast Group</b> 224.0.0.2	224.0.0.18	224.0.0.102
HSRP		VRP	GLBP	
HSRP Configuration				HSRP/GLBP Interface States
<pre>interface FastEthernet0/0 ip address 10.0.1.2 255.255.255.0 standby version {1   2} standby 1 ip 10.0.1.1 standby 1 timers &lt;hello&gt; &lt;dead&gt; standby 1 priority &lt;priority&gt; standby 1 preempt standby 1 authentication md5 key-string &lt;password&gt; standby 1 track &lt;interface&gt; &lt;value&gt; standby 1 track &lt;object&gt; decrement &lt;value&gt;</pre>		<b>Speak</b> · Gateway election in progress		
		<b>Active</b> · Active router/VG		
		<b>Standby</b> · Backup router/VG		
		<b>Listen</b> · Not the active router/VG		
VRRP Configuration		VRRP Interface States		
<pre>interface FastEthernet0/0 ip address 10.0.1.2 255.255.255.0 vrrp 1 ip 10.0.1.1 vrrp 1 timers {advertise &lt;hello&gt;   learn} vrrp 1 priority &lt;priority&gt; vrrp 1 preempt vrrp 1 authentication md5 key-string &lt;password&gt; vrrp 1 track &lt;object&gt; decrement &lt;value&gt;</pre>		<b>Master</b> · Acting as the virtual router		
		<b>Backup</b> · All non-master routers		
GLBP Configuration		GLBP Roles		
<pre>interface FastEthernet0/0 ip address 10.0.1.2 255.255.255.0 glbp 1 ip 10.0.1.1 glbp 1 timers &lt;hello&gt; &lt;dead&gt; glbp 1 timers redirect &lt;redirect&gt; &lt;time-out&gt; glbp 1 priority &lt;priority&gt; glbp 1 preempt glbp 1 forwarder preempt glbp 1 authentication md5 key-string &lt;password&gt; glbp 1 load-balancing &lt;method&gt; glbp 1 weighting &lt;weight&gt; lower &lt;lower&gt; upper &lt;upper&gt; glbp 1 weighting track &lt;object&gt; decrement &lt;value&gt;</pre>		<b>Active Virtual Gateway (AVG)</b> Answers for the virtual router and assigns virtual MAC addresses to group members		
		<b>Active Virtual Forwarder (AVF)</b> All routers which forward traffic for the group		
Troubleshooting		GLBP Load Balancing		
		<b>Round-Robin (default)</b> The AVG answers host ARP requests for the virtual router with the next router in the cycle		
		<b>Host-Dependent</b> Round-robin cycling is used while a consistent AVF is maintained for each host		
		<b>Weighted</b> Determines the proportionate share of hosts handled by each AVF		
		<b>show standby [brief]</b>	<b>show vrrp [brief]</b>	
		<b>show glbp [brief]</b>	<b>show track [brief]</b>	

by Jeremy Stretch

v2.0

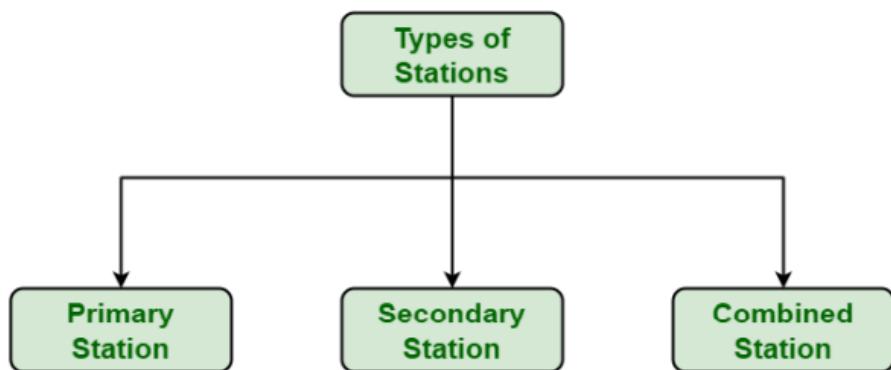
# **HDLC**

(High-Level Data Control)

## Lab 45. HDLC

High-level Data Link Control adalah protokol yang dapat digunakan dalam jaringan WAN (Wide Area Networks) yang dapat mengatasi kerugian-kerugian yang ada pada protokol yang berorientasi karakter seperti Bi-Synch. HDLC sendiri merupakan suatu protokol yang hanya dapat digunakan oleh Cisco (Cisco Proprietary) yang dikembangkan oleh ISO (International Organization for Standardization).

HDLC memungkinkan adanya komunikasi point-to-point menggunakan bit stuffing agar dapat terjadinya transparansi data pada Data Link Layer (DLL). Transparansi pada dasarnya adalah pemisahan data dari sinyal kontrol. HDLC diturunkan dari Synchronous Data Link Control (SDLC).



### Tipe-Tipe HDLC :

- **Primary Station**

- Merupakan master dan mengontrol operasi di Secondary Layer
- Menangani kesalahan pada Data Link Layer
- Mengontrol koneksi ke semua Secondary Layer

- **Secondary Station**

- Dibawah kontrol primary station
- Frame yg dibangkitkan disebut respons

- **Combined Station**

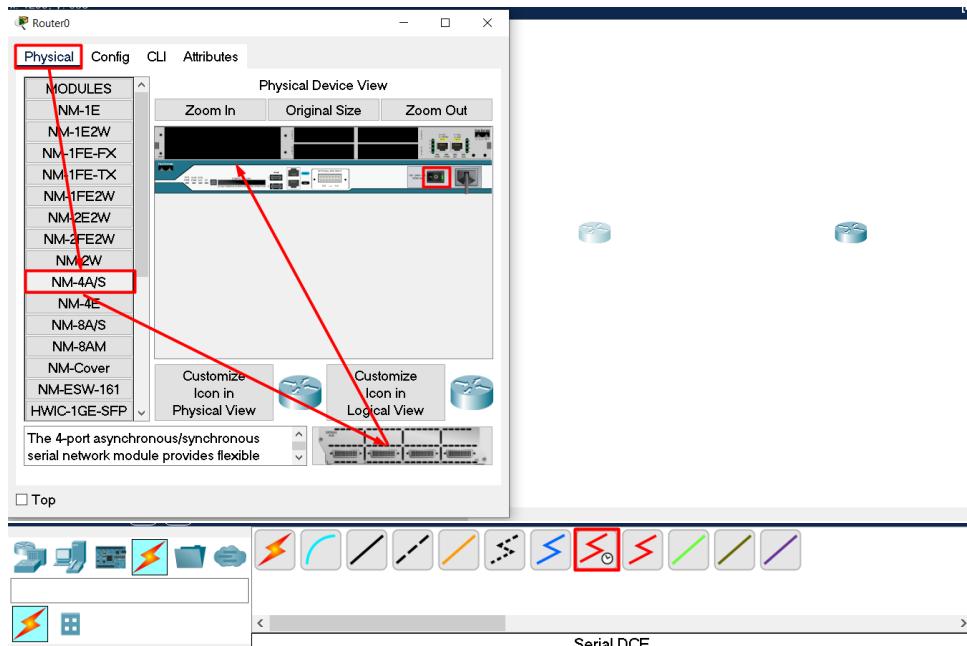
- Dapat membangkitkan command dan respons

Berikut adalah topologinya :

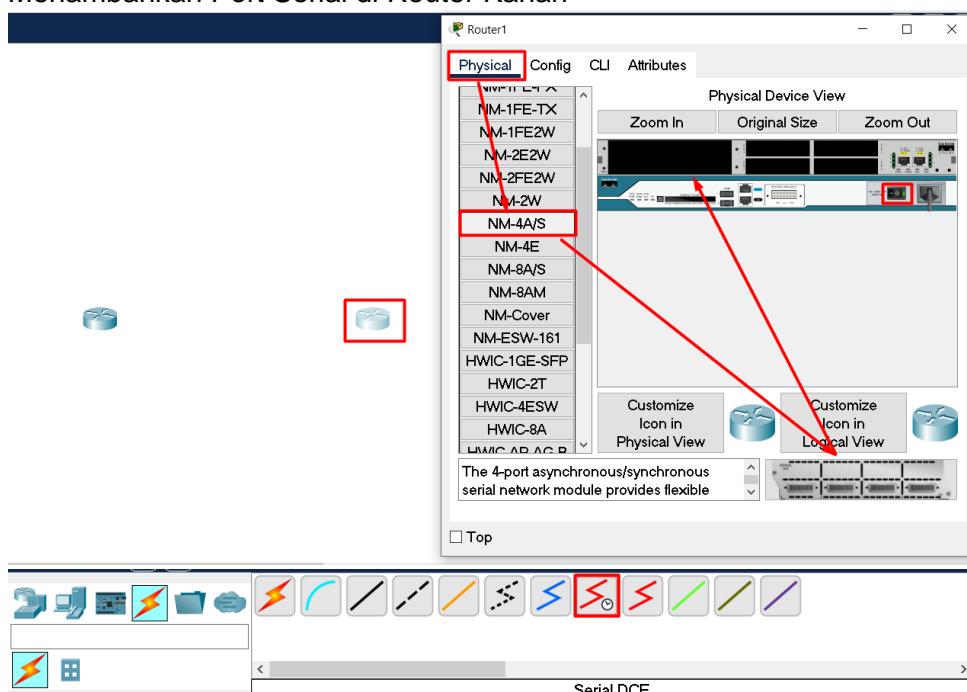


Langkah Langkah :

A. Cara menambahkan Port Serial di Router Kiri



B. Menambahkan Port Serial di Router Kanan



C. Konfigurasi Router Kiri

1. Mengaktifkan Interface Serial

```
R-KIRI(config)#interface se1/0  
R-KIRI(config)#shutdown
```

Kita dapat melihat bahwa interface serial sudah aktif dengan perintah “**do show interface se1/0**”

2. Pengecekan interface Serial

```
R-KIRI(config)#do show interface se1/0
```

```
R-KIRI(config)#do show interface sel/0
Serial1/0 is up, line protocol is up (connected)
Hardware is HD64570
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
```

D. Konfigurasi Router Kanan

1. Mengaktifkan Interface Serial

```
R-KANAN(config)#interface se1/0
R-KANAN(config)#shutdown
```

2. Pengecekan interface Serial

```
R-KANAN(config)#do show interface se1/0
R-KANAN(config)#do show int sel/0
Serial1/0 is up, line protocol is up (connected)
Hardware is HD64570
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
```

E. Lab HDLC telah selesai.

# **IPv6**

# **IPV6**

**CONTENT :**

**IPV6 INTRODUCTION**

**IPV6 ADDRESS NOTATION**

**IPV6 COMPRESSION**

**IPV6 ADDRESS TYPE**

**IPV6 SUBNETTING**

# IPv6 Introduction

Saat ini, IPv4 masih banyak dipakai untuk keperluan kita sehari-hari. Namun dari waktu ke waktu, dikarenakan jumlah IPv4 yang tak seberapa dan kini semakin habis, maka dari itu, organisasi dunia IETF (Internet Engineering Task Force) mengembangkan generasi terbaru dari IPv4, yaitu IPv6. Dengan jumlah yang bisa dibilang luar biasa banyaknya, dan beberapa fitur tambahan.

IPv6 memiliki jumlah empat kali lebih dibanding IPv4 dengan total IP address :

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$$

Dengan jumlah tersebut, memungkinkan setiap device memiliki IP Public pribadi sehingga tidak memerlukan NAT.

Perbandingan	IPv4	IPv6
Jumlah IP	$2^{32}$	$2^{128}$
Format IP	Desimal	Hexadesimal
Dynamic IP	DHCP	SLAAC/DHCPv6
IPSec	Optional	Required
Header Length	Variable	Fixed

Tabel 3 . 11 Perbandingan IPv4 dan IPv6

# IPv6 Address Notation

Jika sebelumnya IPv4 terdiri dari 4 fields dan tiap fieldsnya terdiri dari 8-bit, maka IPv6 terdiri dari 8 fields, setiap fields terdiri dari 16 bit.

IPv6 menggunakan bilangan Hexadesimal yang terdiri dari :

Desimal	Hexadesimal	Desimal	Hexadesimal		
1	1	8	8	15	F
2	2	9	9		
3	3	10	A		
4	4	11	B		
5	5	12	C		
6	6	13	D		
7	7	14	E		

Pada IPv6, penulisan pemisahan antar fields, dipisah menggunakan colon ":"

Berikut ini contoh dari IPv6 :

2001:aaaa:bbbb:cccc:1111:2222:3333:4444

Fields	Hexadesimal	Binary
1	2001	0010 0000 0000 0001
2	aaaa	1010 1010 1010 1010
3	bbbb	1011 1011 1011 1011
4	cccc	1100 1100 1100 1100
5	1111	0001 0001 0001 0001
6	2222	0010 0010 0010 0010
7	3333	0011 0011 0011 0011
8	4444	0100 0100 0100 0100

Berikut tata letak pada IPv6 :

2001:000C:0007:ABCD:0000:0000:0001/64

- 64 bit pertama 2001:000C:0007:ABCD merupakan address prefix
- 64 bit terakhir 0000:0000:0000:0001 merupakan interface ID
- /64 merupakan prefix length

# IPv6 Compression

Dalam penulisan IPv6, kita dipermudah dengan adanya Compression atau peringkasan. Hal ini merupakan suatu kemudahan bagi para Network Engineer untuk dapat mengkonfigurasi IPv6 dengan mudah.

Berikut beberapa compression dalam penulisan IPv6 :

**1. Menghapus angka “0” didepan.**

Misalkan ada IPv6 : **2001: F2C1:00E7:0000:0000:0000:0D71:34FE**

Kita dapat compress menjadi : **2001:F2C1:00E7:0000:0000:0000:0D71:34FE**

Hasilnya : **2001:F2C1:E7:0000:0000:D71:34FE**

**2. Mengganti angka 0000 menjadi 0.**

Misalkan ada IPv6 : **2001: F2C1:00E7:0000:0000:0000:0D71:34FE**

Kita dapat compress menjadi : **2001:F2C1:00E7:0000:0000:0000:0D71:34FE**

Hasilnya : **2001:F2C1:00E7:0:0:0D71:34FE**

**3. Mengganti angka 0000 yang berturut-turut menjadi “::” (double colon).**

Misalkan ada IPv6 : **2001:0000:0000:2F4D:5AC2:DE12:0000:0000**

Kita dapat compress menjadi : **2001::2F4D:5AC2:DE12:0000:0000**

Atau menjadi : **2001:0000:0000:2F4D:5AC2:DE12::**

Mengapa tidak menjadi: **2001::2F4D:5AC2:DE12::** ?

Jika kita membuat menjadi seperti diatas, maka router akan bingung dalam mengenali IPv6 tersebut.

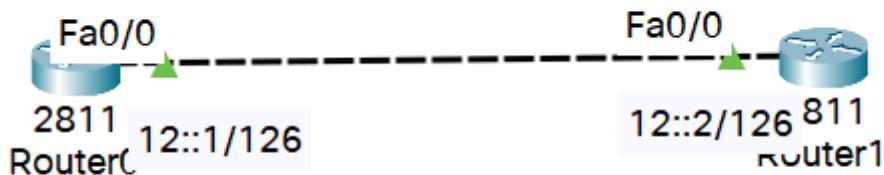
Bisa jadi dalam double colon pertama terdapat 3 “0000” sedangkan double colon kedua terdapat 4 “0000”. Maka dari itu, router akan sulit mengenalinya.



Namun jika hanya ada satu double colon router pasti dengan mudah dapat mengenalinya.

## Lab 46. Peer to Peer IPv6

Setelah kita belajar IPv6 tadi, kita akan mempraktekannya namun pada lab kali ini kita tidak akan mulai dengan yang susah susah dulu. Pada lab kali ini kita akan membuat lab peer to peer IPv6 yang mana cukup membutuhkan 2 router saja.



Kita mulai dengan mengganti hostname, setelah itu memasang IP Address di setiap router agar kedua router itu bisa saling berkomunikasi.

Langkah Langkah :

A. Konfigurasi Router Kiri

1. Mengganti hostname

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-KIRI
```

2. Mengaktifkan fungsi IPv6 dan memasang IPv6 di interface

```
R-KIRI(config)#ipv6 unicast-routing  
R-KIRI(config)#interface fa0/0  
R-KIRI(config)#ipv6 enable  
R-KIRI(config)#ipv6 address 12::1/126  
R-KIRI(config)#no shutdown
```

**Ipv6 unicast- routing** : Perintah untuk mengaktifkan fungsi dari IPv6 Unicast, merupakan IPv6 yang ditujukan untuk berkomunikasi antar kedua buah dengan salah satunya menjadi host.

**Ipv6 enable** : Perintah untuk mengaktifkan IPv6 di interface fa0/0

**Ipv6 address** : Perintah untuk memasang IP address 12::1/126

B. Konfigurasi Router Kanan

1. Mengganti hostname

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-KANAN
```

2. Mengaktifkan fungsi IPv6 dan memasang IPv6 di interface

```
R-KANAN(config)#ipv6 unicast-routing  
R-KANAN(config)#interface fa0/0  
R-KANAN(config)#ipv6 enable  
R-KANAN(config)#ipv6 address 12::2/126
```

```
R-KANAN(config)#no shutdown
```

Setalah itu kita coba melakukan pengetesan yaitu dengan PING dari Router Kiri ke Router Kanan.

```
R-1(config)#do ping 12::2
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 12::2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

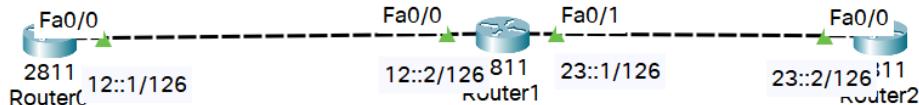
```
R-1(config)#
```

Kalau di IPv6 kita harus melakukan pengecekan PING dengan menggunakan CLI tidak bisa menggunakan PDU.

#### C. Lab Peer to Peer IPv6 telah selesai

## Lab 47. Static Route IPv6

Pada lab IPv4 sebelumnya kita sudah belajar Static Route yaitu dengan mendaftarkan network yang belum dimiliki oleh router, pada lab kali juga sama namun bedanya kita Static Route di IPv6.



Ditopologi atas terdapat 2 network yang mana kita harus mengkonfigurasi Route agar kedua network tsb bisa saling berkomunikasi. Konfigurasi pertama kita mengganti hostname di setiap router dan memasang IP Address, untuk IP Addressnya seperti topologi diatas.

Langkah Langkah :

- Konfigurasi Static Route (Router Kiri)

```
R-KIRI(config)#ipv6 route 23::0/126 12::2
```

**Ipv6 route** : Perintah melakukan routing jenis Static Route

**23::0/126** : Network tujuan dari routing

**12::2** : IP Gateway yang kita gunakan dalam melakukan routing

- Konfigurasi Static Route (Router Kanan)

```
R-KANAN(config)#ipv6 route 12::0/126 23::1
```

Setelah itu kita melakukan pengecekan tabel routing di setiap router, namun untuk perintah pengecekan tabel routing IPv6 berbeda yaitu dengan menambahkan perintah **IPv6**. Contohnya : “**do show ipv6 route**”

**Tabel Routing Router Kiri**

```
R-1(config)#do show ipv6 route
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
C    12::/126 [0/0]
      via FastEthernet0/0, directly connected
L    12::1/128 [0/0]
      via FastEthernet0/0, receive
S    23::/126 [1/0]
      via 12::2
L    FF00::/8 [0/0]
      via Null0, receive
```

### Tabel Routing Router Kanan

```
R-3(config)#do show ipv6 route
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP. EX - EIGRP external
S  12::/126 [1/0]
  via 23::1
C  23::/126 [0/0]
  via FastEthernet0/0, directly connected
L  23::2/128 [0/0]
  via FastEthernet0/0, receive
L  FF00::/8 [0/0]
  via Null0, receive
```

Setelah kita melakukan pengecekan tabel routing, hal selanjutnya kita melakukan PING dari Router Kiri ke Router Kanan.

### Hasil PING dari Router Kiri ke Router Kanan

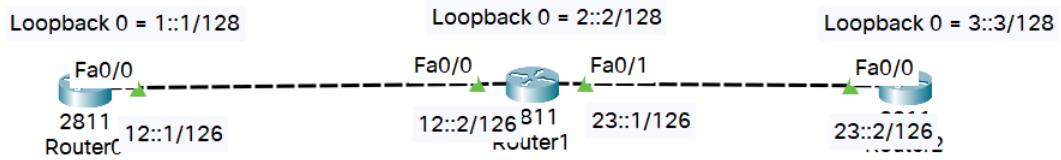
```
R-1(config)#do ping 23::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Bisa dilihat bahwa kita success melakukan PING dari Router Kiri ke Router Kanan karena kita sudah berhasil menjalankan Static Route.

C. Lab Static Route IPv6 telah selesai

## Lab 48. Dynamic Routing EIGRP IPv6

Lab kali ini kita akan belajar Dynamic Routing EIGRP lagi, pada lab sebelumnya pada bab IPv4 kita sudah belajar Dynamic Routing EIGRP, Intinya kalau Dynamic Routing itu kita mendaftarkan networknya sendiri atau yang biasa kita kenal sebagai (Advertise Network).



Di topologi atas kita akan mengkonfigurasi interface loopback juga pada setiap router, tujuan kita kali ini agar PING antar network bisa saling berkomunikasi.

Langkah Langkah :

A. Konfigurasi Router 1

1. Mengganti hostname

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-1
```

2. Mengaktifkan fungsi IPv6 dan memasang IPv6 di interface

```
R-1(config)#ipv6 unicast-routing  
R-1(config)#interface fa0/0  
R-1(config)#ipv6 enable  
R-1(config)#ipv6 address 12::1/126  
R-1(config)#no shutdown
```

3. Membuat dan memasang interface loopback

```
R-1(config)#interface loopback0  
R-1(config)#ipv6 address 1::1/128
```

4. Membuat EIGRP IPv6 AS 123

```
R-1(config)#ipv6 router eigrp 123  
R-1(config)#eigrp router-id 1.1.1.1  
R-1(config)#no shutdown
```

5. Memasukan interface ke EIGRP IPv6

```
R-1(config)#interface fa0/0  
R-1(config)#ipv6 eigrp 123  
  
R-1(config)#interface loopback0  
R-1(config)#ipv6 eigrp 123
```

B. Konfigurasi Router 2

1. Mengganti hostname

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-2
```

2. Mengaktifkan fungsi IPv6 dan memasang IPv6 di interface

```
R-2(config)#ipv6 unicast-routing  
R-2(config)#interface fa0/0
```

```
R-2(config)#ipv6 enable  
R-2(config)#ipv6 address 12::2/126  
R-2(config)#no shutdown
```

```
R-2(config)#ipv6 unicast-routing  
R-2(config)#interface fa0/1  
R-2(config)#ipv6 enable  
R-2(config)#ipv6 address 23::1/126  
R-2(config)#no shutdown
```

3. Membuat dan memasang interface loopback

```
R-2(config)#interface loopback0  
R-2(config)#ipv6 address 2::2/128
```

4. Membuat EIGRP IPv6 AS 123

```
R-2(config)#ipv6 router eigrp 123  
R-2(config)#eigrp router-id 2.2.2.2  
R-2(config)#no shutdown
```

5. Memasukan interface ke EIGRP IPv6

```
R-2(config)#interface fa0/0  
R-2(config)#ipv6 eigrp 123
```

```
R-2(config)#interface fa0/1  
R-2(config)#ipv6 eigrp 123
```

```
R-2(config)#interface loopback0  
R-2(config)#ipv6 eigrp 123
```

### C. Konfigurasi Router 3

1. Mengganti hostname

```
Router>enable  
Router#configure terminal  
Router(config)#hostname R-3
```

2. Mengaktifkan fungsi IPv6 dan memasang IPv6 di interface

```
R-3(config)#ipv6 unicast-routing  
R-3(config)#interface fa0/0  
R-3(config)#ipv6 enable  
R-3(config)#ipv6 address 23::2/126  
R-3(config)#no shutdown
```

3. Membuat dan memasang interface loopback

```
R-3(config)#interface loopback0  
R-3(config)#ipv6 address 3::3/128
```

4. Membuat EIGRP IPv6 AS 123

```
R-3(config)#ipv6 router eigrp 123  
R-3(config)#eigrp router-id 3.3.3.3  
R-3(config)#no shutdown
```

5. Memasukan interface ke EIGRP IPv6

```
R-2(config)#interface fa0/0  
R-2(config)#ipv6 eigrp 123
```

```
R-2(config)#interface loopback0  
R-2(config)#ipv6 eigrp 123
```

Setelah kita melakukan konfigurasi, kita akan melakukan pengecekan tabel routing dan tabel topologi EIGRP.

### Tabel Routing (Router 1)

```
R-1(config)#do show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
C   1::1/128 [0/0]
    via Loopback0, directly connected
D   2::2/128 [90/156160]
    via FE80::290:2BFF:FE4D:116E, FastEthernet0/0
D   3::3/128 [90/158720]
    via FE80::290:2BFF:FE4D:116E, FastEthernet0/0
D   12::/126 [90/30720]
    via FE80::290:2BFF:FE4D:116E, FastEthernet0/0
C   12::1/128 [0/0]
    via FastEthernet0/0, directly connected
D   23::/126 [90/33280]
    via FE80::290:2BFF:FE4D:116E, FastEthernet0/0
D   23::1/128 [90/30720]
    via FE80::290:2BFF:FE4D:116E, FastEthernet0/0
L   FF00::/8 [0/0]
    via Null0, receive
```

### Tabel Routing (Router 2)

```
R-2(config)#do show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
D   1::1/128 [90/156160]
    via FE80::209:7CFF:FE1B:97C, FastEthernet0/0
C   2::2/128 [0/0]
    via Loopback0, directly connected
D   3::3/128 [90/156160]
    via FE80::2D0:BAFF:FE02:5582, FastEthernet0/1
C   12::/126 [0/0]
    via FastEthernet0/0, directly connected
D   12::1/128 [90/30720]
    via FE80::209:7CFF:FE1B:97C, FastEthernet0/0
L   12::2/128 [0/0]
    via FastEthernet0/0, receive
D   23::/126 [90/30720]
    via FE80::2D0:BAFF:FE02:5582, FastEthernet0/1
C   23::1/128 [0/0]
    via FastEthernet0/1, directly connected
L   FF00::/8 [0/0]
    via Null0, receive
```

### Tabel Routing (Router 3)

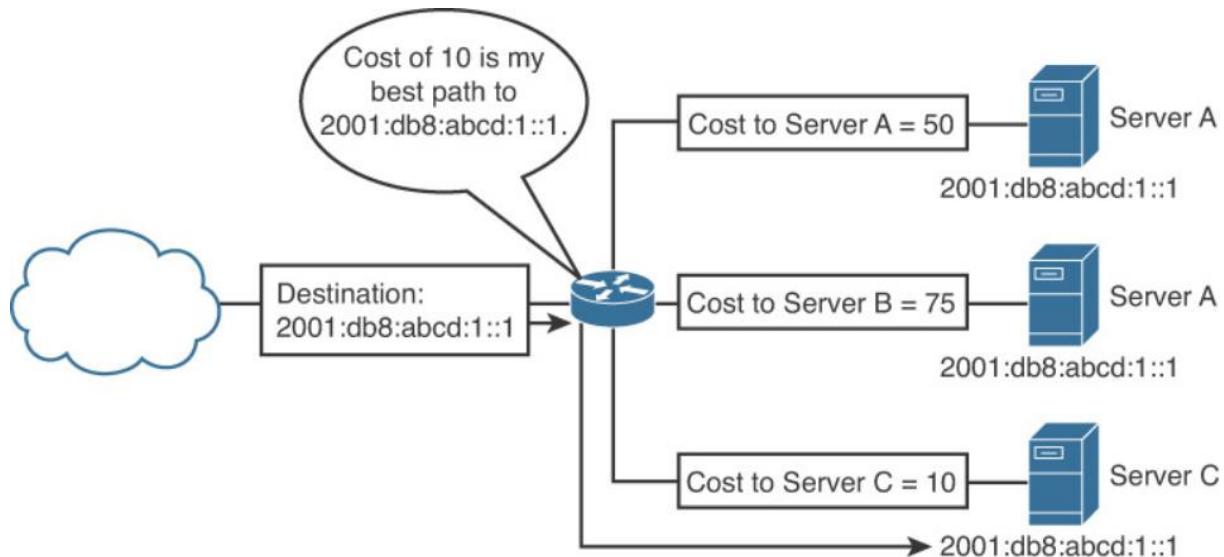
```
R-3(config)#do show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
D  1::1/128 [90/158720]
    via FE80::20A:F3FF:FEBA:E292, FastEthernet0/0
D  2::2/128 [90/156160]
    via FE80::20A:F3FF:FEBA:E292, FastEthernet0/0
C  3::3/128 [0/0]
    via Loopback0, directly connected
D  12::/126 [90/30720]
    via FE80::20A:F3FF:FEBA:E292, FastEthernet0/0
D  12::1/128 [90/33280]
    via FE80::20A:F3FF:FEBA:E292, FastEthernet0/0
C  23::/126 [0/0]
    via FastEthernet0/0, directly connected
D  23::1/128 [90/30720]
    via FE80::20A:F3FF:FEBA:E292, FastEthernet0/0
L  23::2/128 [0/0]
    via FastEthernet0/0, receive
L  FF00::/8 [0/0]
    via Null0, receive
```

D. Lab Dynamic Routing EIGRP IPv6 telah selesai

# IPv6 Address Type

## IPv6 Anycast

Anycast merupakan jenis komunikasi baru yang ada di IPv6, Anycast adalah jenis komunikasi jaringan IPv6 di mana Paket IPv6 dari sumber dialihkan ke perangkat terdekat (dalam hal jarak routing) dari server grup yang menyediakan layanan yang sama. Setiap server yang menyediakan layanan yang sama dikonfigurasi dengan alamat tujuan Anycast yang sama.



Dari gambar diatas, kita memiliki 3 server dengan services yang sama dan dikonfigurasikan IPv6 yang sama sehingga jika kita menggunakan komunikasi anycast, maka PC akan mengakses server yang paling bawah, ini dikarenakan PC akan diarahkan ke server terdekat.

## IPv6 Multicast

Secara default setiap host yang menggunakan IPv6, akan listen pada sebuah IP multicast FF02::1. Jika sebuah host ingin mengirimkan paket untuk seluruh host lain, maka host tersebut akan menggunakan IPv6 multicast FF02::1 sebagai tujuannya.

Jika sebuah host atau router ingin mengirim paket ke router, maka IPv6 multicast address yang digunakan ialah FF02::2. Maka dari itu setiap router akan listening pada IP Multicast FF02::2. Pada Router kita bisa mengetahui IP multicast berapa saja yang di listen, dengan menggunakan perintah berikut :

```
R1(config)#int f0/0
R1(config-if)#ipv6 enable
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#do show ipv6 int f0/0
FastEthernet0/0 is up, line protocol is down
  IPv6 is tentative, link-local address is FE80::201:C7FF:FE82:4B01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
```

```
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds ----
output filtered----
```

Dapat dilihat pada Interface Fa0/0 R1 listening ke IP multicast **FF02::1**. Tapi bukankah Router harusnya listening ke **FF02::2**? Mengapa hanya ada 1 IP Multicast saja yang di listen? Jawabannya, karena fitur routing pada Cisco Router secara default belum diaktifkan. Jika sudah diaktifkan, maka hasil dari show interface nya akan muncul sebagai berikut :

```
R1(config)#ipv6 unicast-routing
R1(config)#do show ipv6 int f0/0
FastEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::201:C7FF:FE82:4B01
No Virtual link-local address(es):
No global unicast address is configured
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF82:4B01
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
```

Dapat dilihat pada IP Multicast FF02::2 sudah terdaftar. Lalu dibawahnya ada IP FF02::1:FF82:4B01 yang mana IP tersebut merupakan sebuah Solicited Node Address yang berfungsi sebagai neighbor discovery.

## IPv6 Unicast

Unicast, merupakan IPv6 yang ditujukan untuk berkomunikasi antar kedua buah dengan salah satunya menjadi host.

Unicast ini terbagi menjadi 3 bagian :



# IPv6 Subnetting

## Konversi Desimal ke Binary

Pada IPv6, satu fieldsnya terdiri dari 16 bit bilangan hexadecimal. Misalkan hexadecimal dari 270F, kita konversikan menjadi 16 bit. Caranya dengan mengonversi satu-satu angka dari 4 angka hexadesimal (2-7-0-F) menjadi 4 bit, dan kemudian jika kita tambahkan keempat angka tersebut maka akan menjadi 16 bit. Berikut caranya dengan menggunakan tabel konversi yang masih sama caranya seperti konversi IPv4 :

-	-	-	-
8	4	2	1

Tabel yang diatas akan kita isi dengan angka 1 ketika angka yang berada dibawahnya menjadi angka yang dapat menjumlahkan angka tersebut dan isi dengan angka 0 jika angka dibawahnya tidak termasuk dari bilangan yang dapat menjumlahkannya. Sementara angka dibawahnya (8-4-2-1) jika kita jumlahkan menjadi angka maksimal dari hexadesimal yaitu F (15=F).

Kita konversikan angka “2” menjadi 4 bit :

0	0	1	0
8	4	2	1

Dari tabel tersebut, binary dari angka hexadesimal “2” adalah **0010**. Namun, tidak hanya sampai disini, kita harus mengonversi 3 angka yang lain hingga jika kita jumlahkan binarynya maka terdapat 16 binary.

Selanjutnya kita konversi angka hexadesimal “7” dengan menggunakan tabel konversi :

0	1	1	1
8	4	2	1

Jika dilihat dari hasil tabel diatas, binary dari angka hexadesimal “7” adalah **0111** yang merupakan hasil penjumlahan dari 4+2+1.

Selanjutnya kita konversi angka hexadesimal “0”. Nah untuk angka “0” ini kita tidak usah susah-susah mengonversinya ke binary karena, binary dari “0” ya “0”.

Maka 4 bit dari angka hexadesimal “0” adalah **0000**.

Kita lanjutkan konversi 4 bit terakhir pada field pertama, yaitu angka hexadesimal dari “F”. Angka “F” ini, jika kita konversi ke decimal menjadi angka 15.

1	1	1	1
8	4	2	1

Maka 4 bit dari angka hexadesimal “F” adalah 1111. Maka, jika satu field tadi (270F) kita tuliskan dalam bentuk binary maka akan membentuk angka :

**0010 0111 0000 1111 = 16 bit**

**2      7      0      F      = 1 Field**

Itu baru 1 field pertama, selanjutnya kita perlu mengonversi 7 fields lagi agar menjadi 128 bit, bagaimana, pusing??

## Konversi Binary ke Desimal

Baiklah, selanjutnya kita akan bahas konversi dari binary ke hexadesimalnya Caranya sama mudahnya seperti konversi hexadesimal ke binary, kita tinggal membalikkannya saja, seperti contoh berikut :

Misalkan ada binary **1010**

1	0	1	0
8	4	2	1

Maka kita tinggal menjumlahkan angka 8+2 karena binarynya 1. Maka hexadesimal dari **1010** adalah **A**. Mudah bukan?

Kita coba konversi satu field, **0010 1101 0011 1000**.

1. **0010: 2**

0	0	1	0
8	4	2	1

2. **1101: 8+4+1 = D**

1	1	0	1
8	4	2	1

3. **0011: 3**

0	0	1	1
8	4	2	1

4. **1000: 8**

1	0	0	0
8	4	2	1

Hasil dari konversi diatas adalah **2D38**. Pastinya jauh lebih mudah mengonversi dari binary ke hexadesimal daripada hexadesimal ke binary.

# IPv6

packetlife.net

Protocol Header				Address Notation									
8	16	24	32	<ul style="list-style-type: none"> <li>· Eliminate leading zeros from all two-byte sets</li> <li>· Replace up to one string of consecutive zeros with a double-colon (::)</li> </ul>									
Ver	Traffic Class	Flow Label		<b>Address Formats</b>									
Payload Length	Next Header	Hop Limit		<b>Global unicast</b>									
Source Address				Global Prefix	Subnet	Interface ID							
Destination Address				48	16	64							
<b>Version</b> (4 bits) · Always set to 6													
<b>Traffic Class</b> (8 bits) · A DSCP value for QoS													
<b>Flow Label</b> (20 bits) · Identifies unique flows (optional)													
<b>Payload Length</b> (16 bits) · Length of the payload in bytes													
<b>Next Header</b> (8 bits) · Header or protocol which follows													
<b>Hop Limit</b> (8 bits) · Similar to IPv4's time to live field													
<b>Source Address</b> (128 bits) · Source IP address													
<b>Destination Address</b> (128 bits) · Destination IP address													
Address Types													
<b>Unicast</b> · One-to-one communication													
<b>Multicast</b> · One-to-many communication													
<b>Anycast</b> · An address configured in multiple locations													
Multicast Scopes				EUI-64 Formation									
1 Interface-local	5 Site-local	8 Link-local	E Admin-local	MAC	00   0a   27   5c   88   19								
2 Link-local	8 Org-local												
4 Admin-local	E Global			EUI-64	02   0a   27   ff   fe   5c   88   19								
Special-Use Ranges													
::/0	Default route						· Insert 0xffffe between the two halves of the MAC						
::/128	Unspecified						· Flip the seventh bit (universal/local flag) to 1						
::1/128	Loopback												
::/96	IPv4-compatible*												
::FFFF:0:0/96	IPv4-mapped												
2001::/32	Teredo												
2001:DB8::/32	Documentation												
2002::/16	6to4												
FC00::/7	Unique local												
FE80::/10	Link-local unicast												
FEC0::/10	Site-local unicast*												
FF00::/8	Multicast												
<small>* Deprecated</small>													
Extension Headers													
<b>Hop-by-hop Options (0)</b>													
Carries additional information which must be examined by every router in the path													
<b>Routing (43)</b>													
Provides source routing functionality													
<b>Fragment (44)</b>													
Included when a packet has been fragmented by its source													
<b>Encapsulating Security Payload (50)</b>													
Provides payload encryption (IPsec)													
<b>Authentication Header (51)</b>													
Provides packet authentication (IPsec)													
<b>Destination Options (60)</b>													
Carries additional information which pertains only to the recipient													
Transition Mechanisms													
<b>Dual Stack</b>													
Transporting IPv4 and IPv6 across an infrastructure simultaneously													
<b>Tunneling</b>													
IPv6 traffic is encapsulated into IPv4 using IPv6-in-IP, UDP (Teredo), or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)													
<b>Translation</b>													
Stateless IP/ICMP Translation (SIIT) translates IP header fields, NAT Protocol Translation (NAT-PT) maps between IPv6 and IPv4 addresses													

by Jeremy Stretch

v2.0

# Wireless

Wireless berperan penting dalam kehidupan kita sekarang ini, karena hampir semua teknologi yang kita pakai dapat kita koneksi secara wireless. Tapi tahukah kamu apa itu wireless?

## Radio Frequency

Wireless jika kita analogikan seperti gelombang air yang berpencar kesegala arah, yang kemudian gelombang itu akan menabrak bebatuan/benda-benda lain, atau bahkan tidak menabrak benda dan akan hilang dengan sendirinya. Dalam wireless, gelombang air itu disebut dengan **Radio Frequency/frekuensi radio**, sementara yang menghasilkan gelombang air/radio frequency itu adalah **Transmitter/pemancar sinyal**, dan benda-benda yang ditabrak gelombang tersebut, menjadi **Receiver/penerima** dari sinyal radio tadi. Jika gelombang tidak menabrak apa-apa, maka sinyal yang dipancarkan akan terbuang.

## Frequency

Frequency merupakan banyaknya cycle/gelombang yang dipancarkan dalam waktu satu detik. Frequency ini berbentuk satuan Hz (Hertz).

Berikut konversinya :

<b>1 Hz: 1 cycle</b>	Turunan
<b>1 Kilo-Hz: 1.000 cycle</b>	
<b>1 Mega-Hz: 1.000.000 cycle</b>	
<b>1 Giga-Hz: 1.000.000.000 cycle</b>	

Tabel 6 . 1 Konversi Hertz

## Frequency Band

Kemudian, milyaran hertz/frekuensi tadi memiliki pengaturan lagi atau yang disebut **Frequency Band**. Dalam sehari-hari kita menggunakan band 2,4 GHz dan 5,8 GHz. Mengapa harus 2,4 dan 5,8? Karena pada standar jaringan wireless Indonesia, 2,4 dan 5,8 GHz sudah terstandar jadi tidak perlu menggunakan lisensi. Jika band yang digunakan bukan 2,4 atau 5,8 maka harus menggunakan lisensi. Contohnya kita memiliki perusahaan, dan kita ingin menggunakan wireless band yang berbeda, misalkan 2,8GHz. Maka kita harus memiliki lisensi terlebih dahulu untuk bisa menggunakan wireless band tersebut.

## 2,4GHz vs 5,8GHz

Berikut perbandingan 2,4GHz dan 5,8GHz :

Band	2,4GHz	5,8GHz
Jangkauan	Besar	Kecil
Protokol IEEE	802.11 b/g/n	802.11 a/n/ac
Konektivitas	Lebih lambat dari 5,8GHz	Lebih cepat dan stabil dari 2,4GHz

Tabel 6 . 2 Perbandingan 2,4GHz dan 5,8GHz

## **SSID**

SSID merupakan singkatan dari Service Set Identifier yang fungsinya untuk memberi nama pada setiap pancaran gelombang yang dipancarkan pada semua perangkat jaringan, contohnya seperti nama wifi.

SSID memiliki peraturan dalam pemberian namanya, yaitu dengan menggunakan karakter case-sensitive dan tidak boleh lebih dari 32 karakter.

## **Wireless Authentication**

Dalam jaringan wireless, kita dapat menggunakan autentikasi agar tidak ada orang lain yang dapat mengakses jaringan wireless kita, oleh karena itu dibuatlah wireless authentication.

## **Wireless Encryption**

Dalam keamanan wireless digunakan beberapa metode enkripsi :

- **Wired Equivalent Privacy (WEP)** – Pada awal penggunaan wireless network, tipe enkripsi inilah yang paling sering digunakan. Menggunakan algoritma RC4 dan sudah dianggap tidak aman lagi.
- **Wi-Fi Protected Access (WPA)** – Karena WEP dianggap sudah kurang bagus, maka dikembangkanlah WPA dengan menggunakan protocol (TKIP). Metode TKIP pun dianggap tidak aman karena sudah ditemukan kerentanan karena menggunakan beberapa mekanisme yang sama seperti yang dilakukan WEP.
- **Wi-Fi Protected Access 2 (WPA2)** - WPA2 menggantikan TKIP dengan Advanced Encryption Standard (AES); WPA2 juga umumnya sering disebut sebagai AES. Sampai saat ini metode enkripsi AES sangat sulit untuk di decrypt sehingga metode enkripsi ini aman untuk digunakan.

# Network Automation

Perkembangan teknologi berkembang pesat, sekarang semuanya dapat didapat secara instan, hal ini juga mempengaruhi perkembangan di dunia networking. Sebelumnya pada dunia jaringan, kita harus melakukan segalanya secara manual dan membutuh perhitungan serta koordinasi yang rumit. Sekarang kini semuanya dapat dilakukan secara otomatis, sehingga kita tidak perlu melakukan apapun tinggal program yang bekerja.

Dengan adanya Network Automation, segalanya menjadi mudah, berikut keuntungan dari Network Automation :

- 1. Mempercepat Pekerjaan**

Dengan adanya Network Automation, kita dapat meringkas sebuah pekerjaan yang tadinya butuh waktu satu bulan menjadi 2 minggu atau bahkan beberapa hari

- 2. Mengurangi Kesalahan**

Ketika semuanya dilakukan secara manual, kemungkinan pasti akan terjadi sebuah kesalahan oleh manusia, entah itu kelalaian hingga salah tekan, namun dengan adanya teknologi Network Automation, secara otomatis dapat menghilangkan kesalahan manusia/human error.

- 3. Meningkatkan Efisiensi**

Dengan menggunakan Network Automation, secara otomatis kita dapat melakukan semuanya sesuai dengan prosedur sehingga dapat meningkatkan efisiensinya, entah itu keuntungan naik, entah itu mendapat kepercayaan pelanggan.

# Virtualization

Virtualization adalah sebuah cara dimana sebuah hardware seperti server dibagi sehingga dapat menjalankan beberapa sistem operasi secara bersamaan.

Berikut keuntungan dari Virtualization :

**1. Kemudahan Backup & Recovery.**

Server-server yang dijalankan didalam sebuah mesin virtual dapat disimpan dalam 1 buah image yang berisi seluruh konfigurasi sistem. Jika satu saat server tersebut crash, kita tidak perlu melakukan instalasi dan konfigurasi ulang. Cukup mengambil salinan image yang sudah disimpan, merestore data hasil backup terakhir dan server berjalan seperti sedia kala. Hemat waktu, tenaga dan sumber daya.

**2. Kemudahan Deployment.**

Server virtual dapat dikloning sebanyak mungkin dan dapat dijalankan pada mesin lain dengan mengubah sedikit konfigurasi. Mengurangi beban kerja para staff IT dan mempercepat proses implementasi suatu system.

**3. Kemudahan Maintenance & Pengelolaan.**

Jumlah server yang lebih sedikit otomatis akan mengurangi waktu dan biaya untuk mengelola. Jumlah server yang lebih sedikit juga berarti lebih sedikit jumlah server yang harus ditangani.

**4. Standarisasi Hardware.**

Virtualisasi melakukan emulasi dan enkapsulasi hardware sehingga proses pengenalan dan pemindahan suatu spesifikasi hardware tertentu tidak menjadi masalah. Sistem tidak perlu melakukan deteksi ulang hardware sebagaimana instalasi pada sistem/komputer fisik.

Namun, ada juga beberapa kelemahan Virtualization :

**1. Satu Pusat Masalah.**

Virtualisasi bisa dianalogikan dengan menempatkan semua telur didalam 1 keranjang. Ini artinya jika server induk bermasalah, semua sistem virtual machine didalamnya tidak bisa digunakan. Hal ini bisa diantisipasi dengan menyediakan fasilitas backup secara otomatis dan periodik atau dengan menerapkan prinsip fail over/clustering.

**2. Spesifikasi Hardware.**

Virtualisasi membutuhkan spesifikasi server yang lebih tinggi untuk menjalankan server induk dan mesin virtual didalamnya.

**3. Satu Pusat Serangan.**

Penempatan semua server dalam satu komputer akan menjadikannya sebagai target serangan. Jika hacker mampu menerobos masuk kedalam sistem induk, ada kemungkinan ia mampu menyusup kedalam server-server virtual dengan cara menggunakan informasi yang ada pada server induk .

## About Writer



Beliau bernama Ahmad Daffah, lahir di Pemalang kecamatan petarukan desa temuireng. Biasa dipanggil Daffah, usianya masih enam belas tahun ketika menuliskan buku ini.

Sejak kecil ia sudah dikenalkan dengan berbagai macam teknologi yang menjadikan ia menyukai teknologi, hingga akhirnya pada saat lulus SMP, ia memutuskan untuk masuk kedalam SMK IDN demi memperdalam ilmunya dibidang teknologi, dengan ambisi yang beliau miliki ia akan membuktikan kepada semua orang, beliau akan menjadi orang terbaik dari yang terbaik, terhebat dari yang terhebat.

Buku ini adalah buku saya yang pertama yaitu CCNA, semoga kalian dapat paham tentang Cisco CCNA ini, bukan sekedar paham namun dapat mengajarkan ke orang lain.

Dan kini, diusianya yang masih dibilang muda, ia telah menyelesaikan buku pertamanya yang pada masanya anak SMK jarang membuat buku. Sekarang, ia masih duduk di bangku Sekolah SMK IDN Pamijahan.

Jika ingin bertanya atau ingin mengenal penulis lebih dalam, kalian bisa menghubunginya di :



Telepon

+6282134291560



Gmail

[adaffah6@gmail.com](mailto:adaffah6@gmail.com)



Instagram

ahmddaffah



Whatsapp

+6282134291560