

# **HOW TO BASIC CISCO CCNA ENTERPRISE**

**MUHAMMAD ADIB AULIA NURKHAFIF**

# PREFACE

Bismillahirrahmanirrahim,

Pertama-tama saya ucapan puji syukur kepada Allah yang maha kuasa, berkat rahmat-Nya saya dapat menyelesaikan buku saya yang ketiga yaitu **HOW TO BASIC CISCO CCNA ENTERPRISE.**

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 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 ketiga 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: [adibnk11@gmail.com](mailto:adibnk11@gmail.com).

Selamat belajar dan membaca!

Batang, Jawa Tengah, Mei 2020

Muhammad Adib Aulia Nurkhafif



# DAFTAR ISI

<b>PREFACE</b>	<b>I</b>
<b>DAFTAR ISI</b>	<b>II</b>
<b>PREPARATION</b>	<b>VI</b>
<b>NETWORK FUNDAMENTAL</b>	<b>1</b>
<b>OSI &amp; TCP/IP LAYER</b>	<b>3</b>
SEJARAH	3
TCP/IP	4
OSI LAYER	4
<b>TCP &amp; UDP</b>	<b>7</b>
PERBANDINGAN TCP DAN UDP	7
PORT NUMBERS	9
CONTOH DARI TCP DAN UDP	9
<b>IPV4</b>	<b>12</b>
KONVERSI BINARY KE DESIMAL	13
KONVERSI DESIMAL KE BINARY	14
KLASIFIKASI IPv4	17
<b>NETWORK PROTOCOL</b>	<b>20</b>
CONTOH NETWORK PROTOCOL	20
<b>NETWORK COMPONENTS</b>	<b>21</b>
CONTOH NETWORK COMPONENT	22
<b>NETWORK TOPOLOGY ARCHITECTURE</b>	<b>24</b>
INFRASTRUKTUR JARINGAN	25
TOPOLOGI JARINGAN	26
<b>PHYSICAL INTERFACE AND CABLE TYPE</b>	<b>28</b>
ETHERNET	28
FIBER OPTIC	29
POE	30
<b>CISCO ROUTER &amp; SWITCH</b>	<b>33</b>
PERBEDAAN HUB, SWITCH DAN ROUTER	34
<b>BROADCAST DOMAIN &amp; COLLISION DOMAIN</b>	<b>36</b>
BROADCAST DOMAIN	36
COLLISION DOMAIN	36
<b>INITIAL CONFIGURATION</b>	<b>37</b>
CLI MODE	37
5 INITIAL CONFIGURATION	40

TIPS CLI	41
<b>REMOTE ACCESS</b>	<b>42</b>
REMOTE TELNET	42
REMOTE SSH	43
PERBEDAAN TELNET DAN SSH	44

## **SWITCHING SESSION** **47**

---

<b>VLAN</b>	<b>49</b>
<b>TRUNK</b>	<b>53</b>
<b>NATIVE VLAN</b>	<b>56</b>
<b>INTERVLAN</b>	<b>58</b>
ROUTER ON STICK	58
MULTILAYER SWITCH (MLS)	62
<b>NEIGHBOR DISCOVERY</b>	<b>64</b>
CDP	65
LLDP	65
<b>PORT SECURITY</b>	<b>66</b>
<b>SPANNING TREE PROTOCOL</b>	<b>69</b>
<b>SPANNING TREE PORTFAST</b>	<b>74</b>
<b>ETHERCHANNEL</b>	<b>75</b>

## **IPV6** **81**

---

<b>IPV6 INTRODUCTION</b>	<b>83</b>
<b>IPV6 ADDRESS NOTATION</b>	<b>84</b>
<b>IPV6 CONVERSION</b>	<b>85</b>
KONVERSI DESIMAL KE BINARY	85
KONVERSI BINARY KE DESIMAL	86
<b>IPV6 COMPRESSION</b>	<b>88</b>
<b>IPV6 ADDRESS TYPE</b>	<b>90</b>
IPv6 ANYCAST	90
IPv6 MULTICAST	91
IPv6 UNICAST	92
<b>IPV6 EUI-64</b>	<b>93</b>
<b>IPV6 ADDRESS CONFIGURATION</b>	<b>95</b>

## **ROUTING SESSION** **99**

---



<b>ROUTING INTRODUCTION</b>	<b>101</b>
<b>ROUTING FUNDAMENTAL</b>	<b>101</b>
ROUTE TYPE	101
ROUTING TABLE	102
BEST ROUTE	103
ROUTING PROTOCOL	103
ADMINISTRATIVE DISTANCE (AD)	105
METRIC	106
<b>STATIC ROUTING</b>	<b>108</b>
FLOATING STATIC ROUTE	113
DEFAULT STATIC ROUTE	113
STATIC ROUTE IPv6	114
<b>DYNAMIC ROUTE OSPF</b>	<b>119</b>
LAB OSPF	120
OSPF PACKET TYPE	122
OSPF AREA TYPE	124
OSPF ROUTER TYPE	125
DR/BDR	125

## **NETWORK MANAGEMENT** **131**

---

<b>QOS</b>	<b>133</b>
QOS VARIANT	135
<b>ACCESS LIST</b>	<b>136</b>
STANDARD ACCESS LIST	136
EXTENDED ACCESS LIST	141
<b>NAT</b>	<b>144</b>
STATIC NAT	144
DYNAMIC NAT	147
<b>GRE TUNNEL</b>	<b>151</b>
<b>DHCP</b>	<b>153</b>
PROSES DHCP	154
LAB DHCP SERVER	155
LAB DHCP RELAY	156
LAB DHCP SNOOPING	158
LAB DYNAMIC ARP INSPECTION (DAI)	160
<b>FHRP</b>	<b>164</b>
HSRP	166
VRRP	169
GLBP	172

## **NETWORKING TECHNOLOGIES** **177**

---

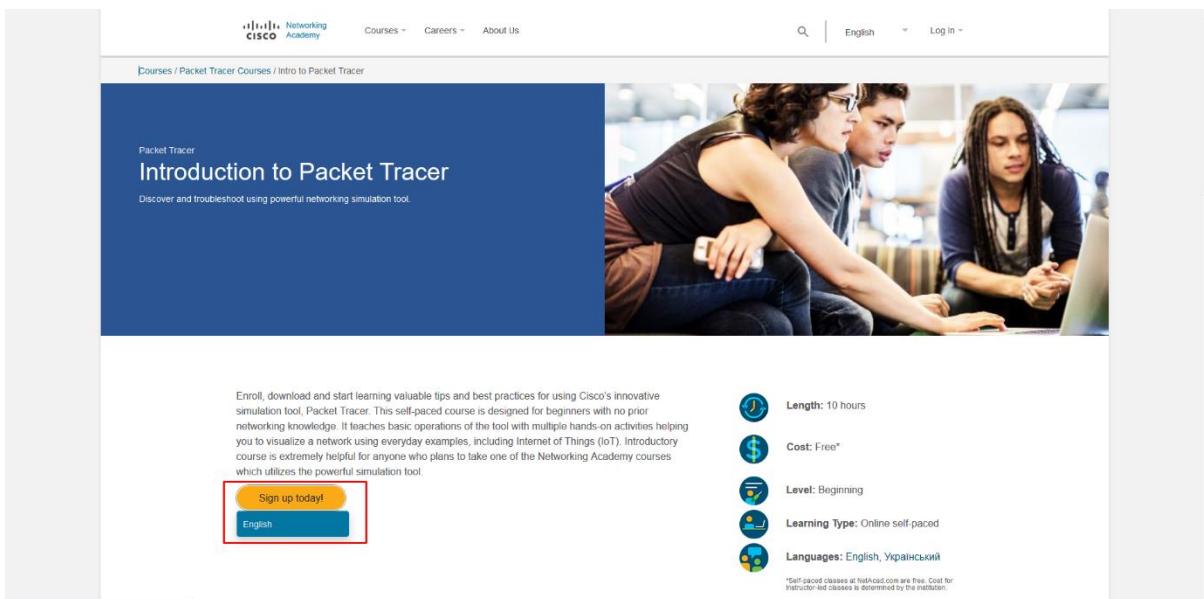
<b>WIRELESS</b>	<b>179</b>
RADIO FREQUENCY	179
FREQUENCY	179
FREQUENCY BAND	179
2,4GHz vs 5,8GHz	180
SSID	180
WIRELESS AUTHENTICATION	180
WIRELESS ENCRYPTION	180
<b>NETWORK AUTOMATION</b>	<b>181</b>
<b>VIRTUALIZATION</b>	<b>182</b>
<b>CLOUD COMPUTING</b>	<b>184</b>
SDN	185
<b><u>DAFTAR PUSTAKA</u></b>	<b><u>188</u></b>
<b><u>TENTANG PENULIS</u></b>	<b><u>190</u></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 CCNA Enterprise kali ini, maka disarankan untuk menggunakan perlengkapan berikut, agar kita bisa lebih memahami.

## 1. Cisco Packet Tracer.

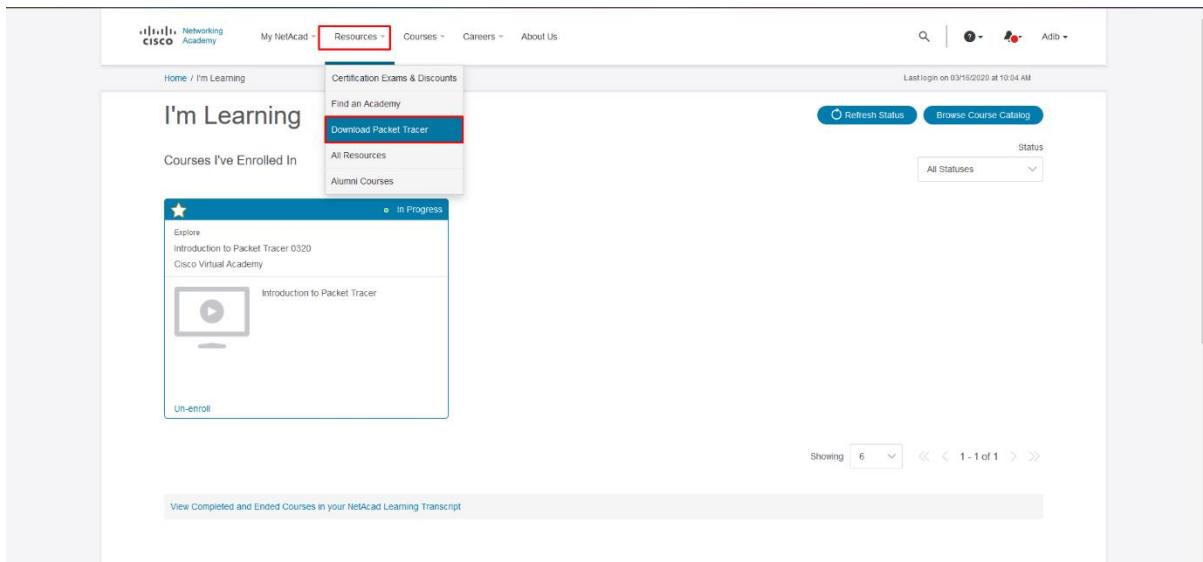
- Pertama-tama, kita daftar netacad terlebih dahulu, agar kita bisa menggunakan dan mengunduh CPT
- Klik <https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer>
- Lalu klik ‘Sign up Today!’ dan klik ‘English’ untuk bahasa inggris.



Gambar 0. 1 Pendaftaran NetAcad

- Selanjutnya kita isi formulir dan verifikasi e-mail.

- Jika kita sudah masuk ke homepage NetAcad.



Gambar 0. 2 Homepage NetAcad

## Download

Choose the OS you are using and download the relevant files. Read the [FAQ](#). View [Tutorials](#).

Packet Tracer requires authentication with your login and password when you first use it and for each new OS login session. (1)

### Considering to upgrade?

For CCNA 7, Packet Tracer 7.3.0 is the minimal version that supports CCNA 7.

For CCNA 6 (and older versions), we recommend instructors and students stay with Packet Tracer 7.2.2.

If you are learning/teaching both CCNA 6 and 7, please use Packet Tracer 7.3.0.

When using Packet Tracer 7.3.0 for CCNA 6, there is a small possibility you may encounter a warning message.

If so, you may disregard the message. It is simply a warning that scripts in this file need to be updated for Packet Tracer 7.3.0 compatibility.

### Windows Desktop Version 7.3.0 English

[64 Bit Download](#)

[32 Bit Download](#)

### Linux Desktop Version 7.3.0 English

[64 Bit Download](#)

### macOS Version 7.3.0 English

[Download](#)

### Mobile

iOS Version 3.0 English



Download on the  
App Store

Android Version 3.0 English



Gambar 0. 3 Unduh Packet Tracer

- 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-**

CHAPTER 1

# Network Fundamental

IS A  
BEGINNING

# **NETWORK FUNDAMENTAL**

## **CONTENT:**

**OSI & TCP/IP LAYER**

**TCP & UDP**

**IPV4**

**NETWORK PROTOCOL**

**NETWORK COMPONENT**

**NETWORK TOPOLOGY ARCHITECTURE**

**PHYSICAL INTERFACE & CABLE TYPE**

**CISCO ROUTER & SWITCH**

**BROADCAST DOMAIN & COLLISION DOMAIN**

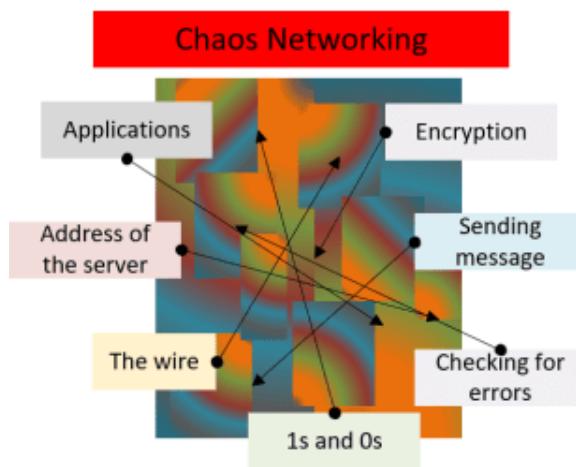
**INITIAL CONFIGURATION**

**REMOTE ACCESS**

# OSI & TCP/IP LAYER

## Sejarah

Tahukah kamu, bahwa jika ketika kita akan berselancar di 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

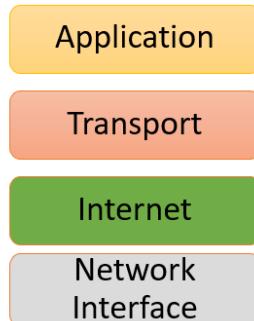
Gambar 1 . 1 Illustrasi Chaos Networking

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

TCP/IP terdiri dari 4 layer:



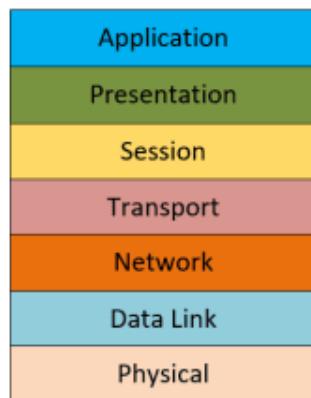
1. Network Interface
2. Internet
3. Transport
4. Application

Gambar 1 . 2 Model TCP/IP

## 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:



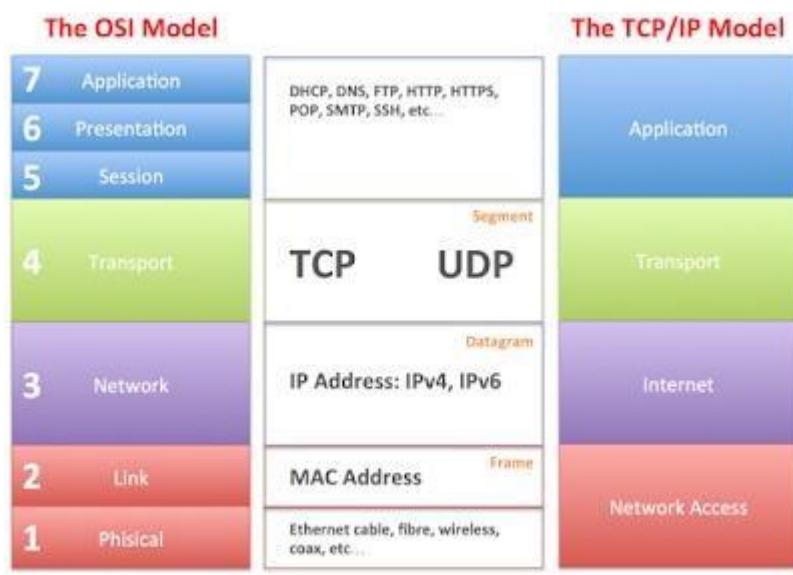
1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation

Gambar 1 . 3 Model OSI Layer

## 7. Application

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

Perbedaannya 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



Gambar 1 . 4 Perbandingan TCP/IP dan OSI

gunakan 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 biner (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	Pengalaman
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 Pengalaman*

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.

Perangkat	Layer	Konektivitas	Pengiriman Data	Memory
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 memperbaiknya, bisa dengan mengirim ulang data yang corrupt atau dengan mengirim semua data dari awal.

### Perbandingan TCP dan UDP

Berikut tabel perbandingan TCP dan UDP

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
-------------------------------------	------------------------------

TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP header size is 20 bytes.	UDP Header size is 8 bytes.
TCP is heavy-weight.	UDP is lightweight.
TCP is used by HTTP, HTTPS, FTP, SMTP and Telnet	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

Tabel 3 . 3 Perbandingan TCP dan UDP

**Mudahnya, jika kita analogikan dalam jaringan:**

**TCP:** Misalkan kita sebagai klien, mengirimkan 10 paket kepada server, jika waktu dijalan 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 dijalannya 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.

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

# IPV4

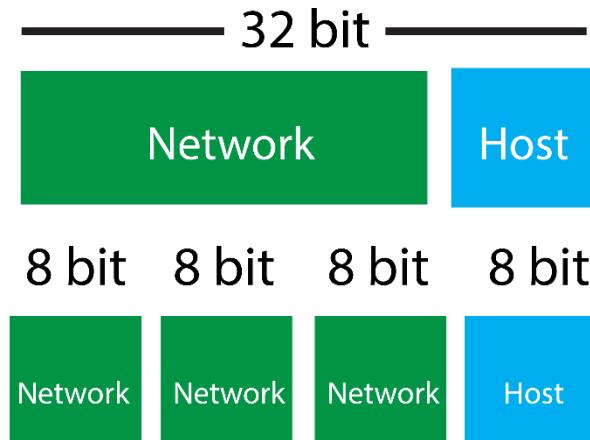
Secara dasar, dalam sebuah jaringan kita pasti membutuhkan sebuah alamat atau address agar semuanya bisa saling berkomunikasi atau terhubung. Atau bisa disebut juga, kita membutuhkan destinasi/tujuan kemana packet-packet yang kita kirimkan akan sampai. Hal seperti itu pasti membutuhkan yang namanya *Sender/Pengirim* 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):

- Beroperasi pada Layer Network di OSI Model.
- Connectionless protocol: IP tidak meng-setup sebuah koneksi, sehingga untuk mengirim data kita memerlukan “transport” layer dan menggunakan TCP dan UDP.
- 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:

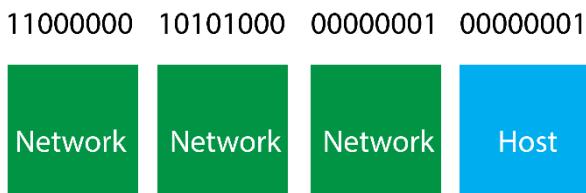
## Penulisan IPv4

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

Dan 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 ke kanan. 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.

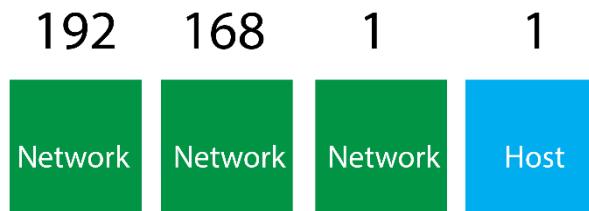
128	64	32	16	8	4	2	1
1	0	1	0	1	0	0	0

Tabel 3 . 4 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
0	0	0	0	0	0	0	1

Tabel 3 . 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.

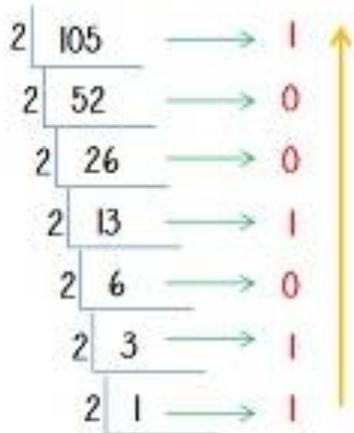
Misalkan mengonversi decimal 105, berapakah binernya?

### 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

## Konversi Bilangan Desimal ke Bilangan Biner



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
0	0	0	0	0	0	0	0

Tabel 3 . 6 Konversi decimal ke binary

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

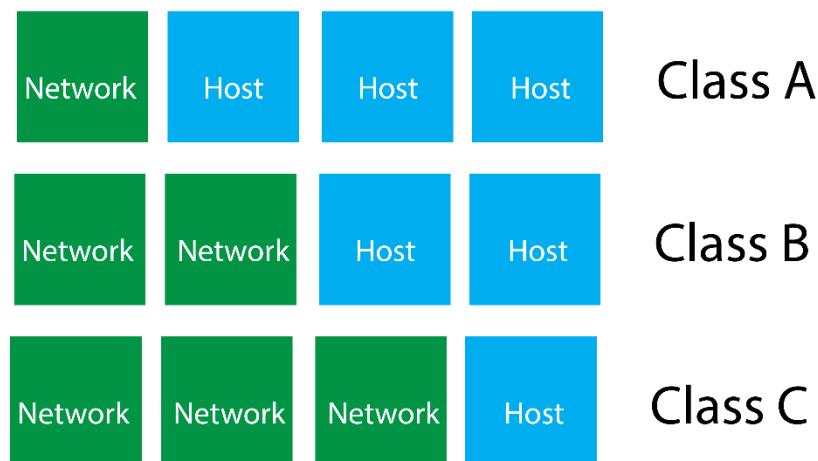
128	64	32	16	8	4	2	1
0	1	0	0	1	0	1	1

Tabel 3 . 7 Konversi decimal ke binary

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 memberitahu kita, ID dari Network yang kita gunakan. Bagian Host adalah angka unik yang berbeda di setiap perangkat yang mengidentifikasikan 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		
/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		
/9	255.128.0.0	8,388,608	0.127.255.255		
/8	255.0.0.0	16,777,216	0.255.255.255		
/7	254.0.0.0	33,554,432	1.255.255.255		
/6	252.0.0.0	67,108,864	3.255.255.255		
/5	248.0.0.0	134,217,728	7.255.255.255		
/4	240.0.0.0	268,435,456	15.255.255.255		
/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

# 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:

Protokol	Port Number	Fungsi
Hypertext Transfer Protocol (HTTP)	TCP 80	HTTP adalah dasar dari komunikasi data untuk World Wide Web. Hiperteks adalah teks terstruktur yang menggunakan hyperlink antara node yang mengandung teks.
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	TCP 443	HTTPS merupakan hasil pengembangan dari HTTP, yakni dengan menambahkan fitur keamanan tambahan. Komunikasi browser ke server dan server ke server akan dienkripsi, sehingga data user yang dikirimkan akan lebih aman.
File Transfer Protocol (FTP)	TCP 20/21	FTP digunakan untuk transfer File di jaringan public maupun di jaringan lokal.
Trivial File Transfer Protocol (TFTP)	UDP 69	TFTP memiliki fungsionalitas dasar dari protokol File Transfer Protocol (FTP). Namun TFTP tidak memiliki fitur autentikasi yang dimiliki FTP, dan menggunakan UDP untuk pengiriman paketnya.

Telnet	TCP 23	Kegunaan utama dari telnet adalah untuk remote sebuah devices, kekurangan utama dari telnet adalah tidak menggunakan secure connection, sehingga traffic datanya bisa di baca oleh orang lain.
Secured Shell (SSH)	TCP 22	Alternatif telnet, yang digunakan untuk remote device dan menawarkan fitur enkripsi sesi komunikasi, sehingga traffic datanya tidak akan bisa dilihat oleh orang lain.
Simple Network Management Protocol (SNMP)	UDP 161/162	Fungsi utama dari protocol ini ialah untuk monitoring network devices. Namun selain monitoring, kita juga bisa mengkonfigurasi network devices menggunakan protokol SNMP.
Domain Name System (DNS)	UDP 53	DNS digunakan untuk menerjemahkan dari Domain name ke IP Address.
Dynamic Host Configuration Protocol (DHCP)	UDP 67	Dynamic Host Configuration Protocol (DHCP) merupakan service yang memungkinkan perangkat dapat mendistribusikan/assign IP Address secara otomatis pada host dalam sebuah jaringan.

Tabel 3 . 9 Contoh Network Protocol

## NETWORK COMPONENTS

Sebelum kita dapat berselancar di 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 Component

Dibawah ini, contoh beberapa komponen jaringan:

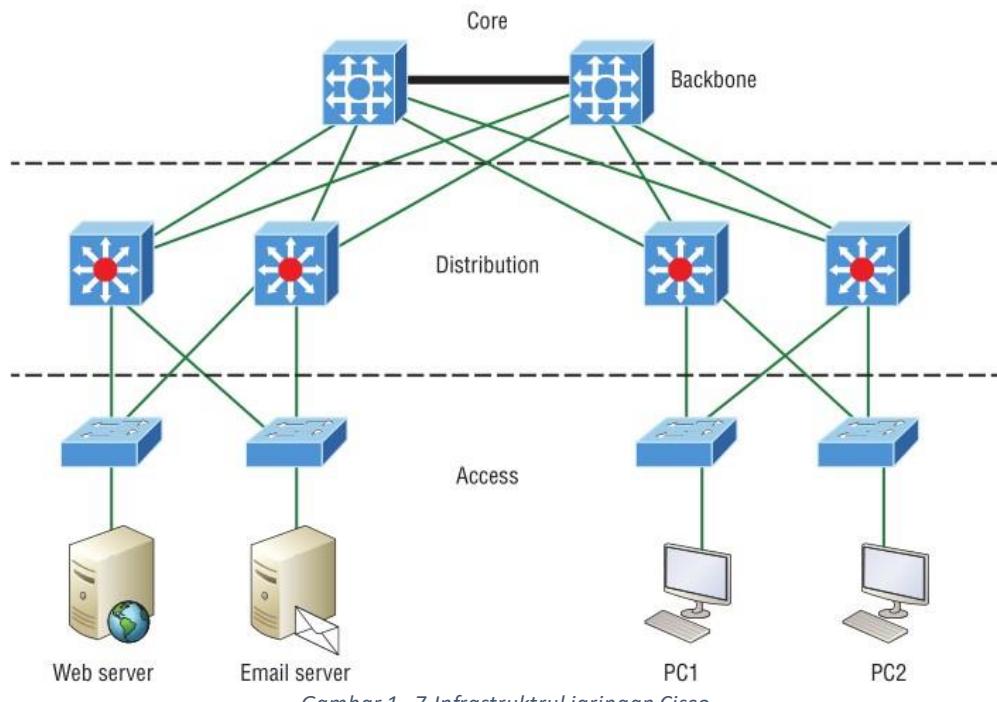
Network Component	Description
<b>Router</b>	Router termasuk kedalam perangkat WAN. Router sendiri merupakan perangkat Layer 3 – Network, yang bekerja berdasarkan IP Address. Data unit di perangkat router adalah Packet. Fungsi utamanya adalah untuk menghubungkan jaringan-jaringan yang berbeda. Dan juga sebagai penghubung antara jaringan LAN dan WAN.
<b>L2 &amp; L3 Switches</b>	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.  Pada Switch Managable terdapat fitur yang dinamakan VLAN, fitur ini berfungsi untuk memecah 1 broadcast domain, menjadi beberapa broadcast domain, sehingga memungkinkan didalam 1 Switch memiliki beberapa jaringan yang berbeda.  Tetapi jika kita ingin menghubungkan jaringan-jaringan tersebut kita tetap membutuhkan Router.  Tipe Switch terbagi menjadi 2, ada Switch Layer 2 & Switch Layer 3. Di Switch Layer 3 kita bisa langsung menghubungkan jaringan-jaringan VLAN yang berbeda tanpa harus menggunakan Router / Inter-Vlan Routing.
<b>Next-Generation Firewall &amp; IPS</b>	Next-Generation Firewall atau yang biasa disebut NGFW, adalah sebuah perangkat Firewall yang berfungsi untuk mencegah ancaman / serangan yang akan masuk ke jaringan enterprise kita. NGFW memiliki sistem keamanan yang lebih baik jika dibandingkan dengan Firewall Tradisional. Tidak seperti Firewall Tradisional / Stateful Firewall yang hanya bisa mengizinkan atau memblokir trafik berdasarkan state, protokol, port, dll.

	<p>Langkah-langkah pencegahan tidak akan pernah 100% efektif. Firewall kita juga harus memiliki kemampuan canggih untuk mendeteksi ancaman / serangan. Maka dari itu NGFW memiliki fitur-fitur yang canggih seperti IPS (Intrusion Prevention System) yang dapat mendeteksi ancaman dan memperketat pertahanan jaringan enterprise kita.</p>
<b>Access-point</b>	<p>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.</p> <p>Access Point juga dilengkapi dengan enkripsi keamanan untuk komunikasinya, generasi pertamanya dinamakan WEP, dimana enkripsi tersebut mudah untuk dibobol. Sedangkan generasi kedua dan ketiga dinamakan WPA &amp; WPA2 yang mana sistem enkripsi ini sudah termasuk aman, dan susah untuk dibobol oleh hacker.</p>
<b>Controller (Cisco DNA Center &amp; WLC)</b>	<p>Controllers merupakan sebuah perangkat yang digunakan untuk mensentralisasi pengelolaan Access Point, sehingga kita lebih mudah dalam mengatur berbagai macam konfigurasi dan keperluan Access Point yang kita miliki. Contoh perangkatnya seperti WLC atau Wireless LAN Controller.</p>
<b>Endpoint</b>	<p>Endpoint adalah perangkat elektrotik yang terhubung ke sebuah jaringan dan memiliki kemampuan untuk membuat, menerima, dan mentransmisikan informasi lewat jaringan tersebut. Contohnya seperti PC, Laptop, Handphone, IP Phone, Printer, dll.</p>
<b>Server</b>	<p>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.</p>

Tabel 3 . 10 Network Component

# NETWORK TOPOLOGY ARCHITECTURE

Dikarenakan jaringan komputer bisa sangat amat sangat amat sangat rumit, dengan berbagai macam protokol dan beragam teknologi. Cisco telah mengembangkan model hierarki berlapis untuk merancang infrastruktur jaringan yang handal. Model tiga lapis ini membantu kita untuk merancang, menerapkan, dan memelihara jaringan yang dapat ditingkatkan, handal, dan hemat biaya. Setiap lapisan memiliki fitur dan fungsi sendiri, yang mengurangi kompleksitas jaringan.



- ❖ **Akses** - mengontrol akses pengguna dan workgroup ke sumber daya di jaringan. Lapisan ini biasanya menggabungkan switch Layer 2 dan access point yang menyediakan koneksi antara workstation dan server. Kita dapat mengelola kontrol akses dan kebijakan, membuat collision domain yang terpisah, dan menerapkan keamanan port di lapisan ini.
- ❖ **Distribusi** - berfungsi sebagai titik komunikasi antara lapisan access dan core. Fungsi utamanya adalah menyediakan akses routing, filtering, dan WAN access untuk menentukan bagaimana paket dapat mengakses lapisan core. Lapisan ini

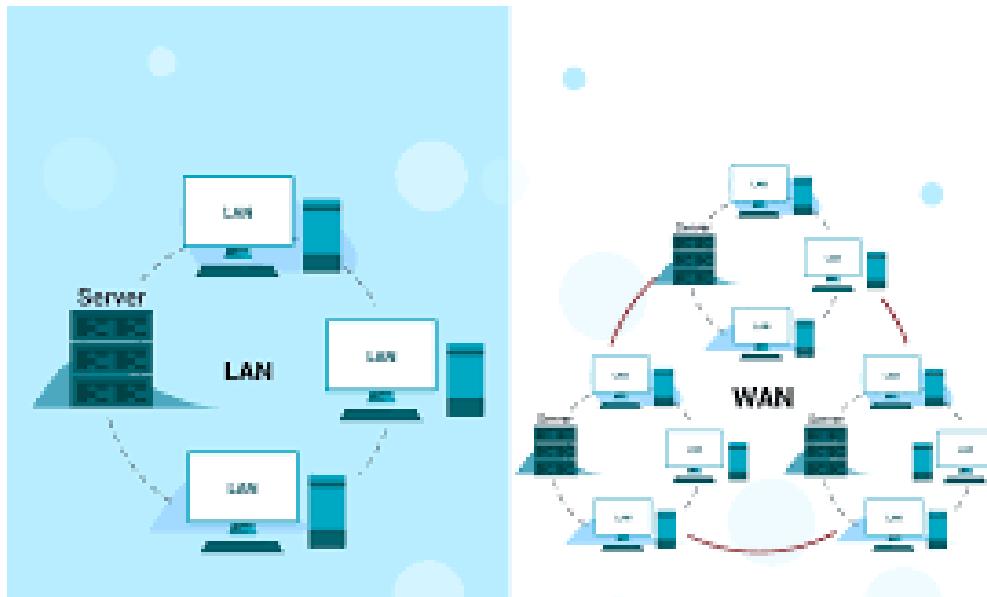
menentukan cara tercepat bahwa permintaan layanan jaringan diakses - misalnya, bagaimana permintaan file diteruskan ke server - dan, jika perlu, meneruskan permintaan ke lapisan inti. Lapisan ini biasanya terdiri dari router dan switch multilayer.

- ❖ **Core** - disebut juga sebagai backbone jaringan, lapisan ini bertanggung jawab untuk mengirim jenis trafik yang besar dengan sangat cepat. Lapisan core menyediakan interkoneksi antara perangkat lapisan distribution biasanya terdiri dari perangkat berkecepatan tinggi, seperti router high end dan switch dengan redundant link

Infrastruktur Jaringan dapat sangat bervariasi dalam hal:

- Area yang tercakup
- Jumlah user yang terkoneksi
- Service yang digunakan
- Area of responsibility

## Infrastruktur Jaringan



Gambar 1 . 8 Illustrasi LAN dan WAN

Dalam implementasinya, infrastruktur jaringan dibagi menjadi 2:

- **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.

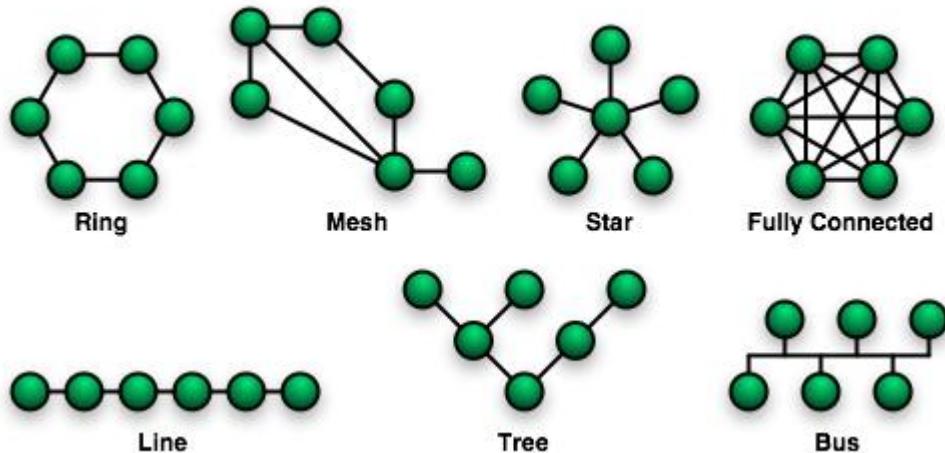
- **WAN (Wide Area Network)**- Merupakan jaringan skala besar yang terdiri dari kumpulan LAN yang saling terhubung satu sama lain. Contohnya Internet.

Adapun beberapa istilah jaringan lain yang berkaitan:

- **WLAN (Wireless Local Area Network)**- Merupakan jaringan skala kecil, sama seperti LAN. Namun dalam konektivitasnya menggunakan jaringan *wireless* (tanpa kabel).
- **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,



Gambar 1 . 9 Macam-macam topologi jaringan

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 Line/Linear**

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.

# 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 :

- ➔ **10Base-T (IEEE 802.3)** - 10 Mbps dengan kabel cat 3 UTP. Jangkauan hingga 100 meter.
- ➔ **100Base-TX (IEEE 802.3u)** - dikenal juga sebagai Fast Ethernet, menggunakan kabel cat 5, 5E, atau cat 6 dengan jangkauan 100 meter.
- ➔ **100Base-FX (IEEE 802.3u)** - versi Fast Ethernet yang menggunakan kabel fiber optic dengan jangkauan hingga 412 meter.
- ➔ **100Base-CX (80002.3z)** - menggunakan kabel twisted-pair dengan jangkauan 25 meter.
- ➔ **100Base-T (IEEE 802.3ab)** - Gigabit Ethernet yang menggunakan Kabel cat 5 UTP dengan jangkauan 100 meter.
- ➔ **100Base-SX (IEEE 802.3z)** - 1 Gigabit Ethernet yang berjalan menggunakan multimode kabel fiberoptic.

- **100Base-LX (IEEE 802.3z)** - 1 Gigabit Ethernet yang berjalan single-mode kabel fiber optic.
- **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:

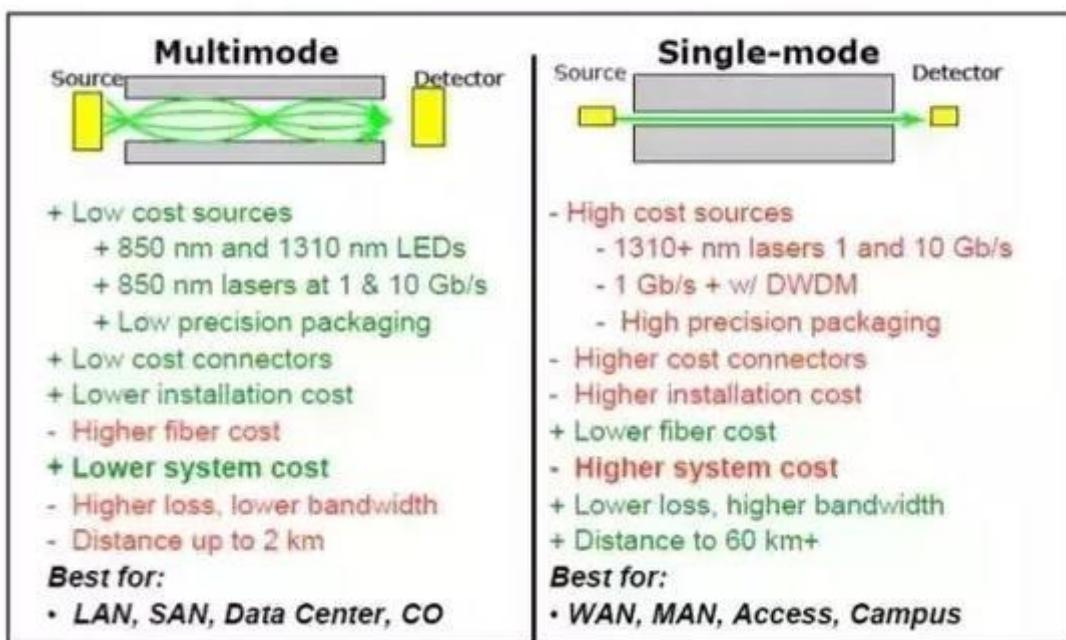
1. Jangkauan lebih jauh
2. Bandwidth lebih besar
3. Bebas gangguan interferensi gelombang elektromagnetik.

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

Kabel Fiber Optic biasanya dibagi menjadi 2 jenis.

1. Multimode
2. Singlemode

## Multi-mode v/s Single mode



Gambar 1 . 10 Mode Fiber Optic

### 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

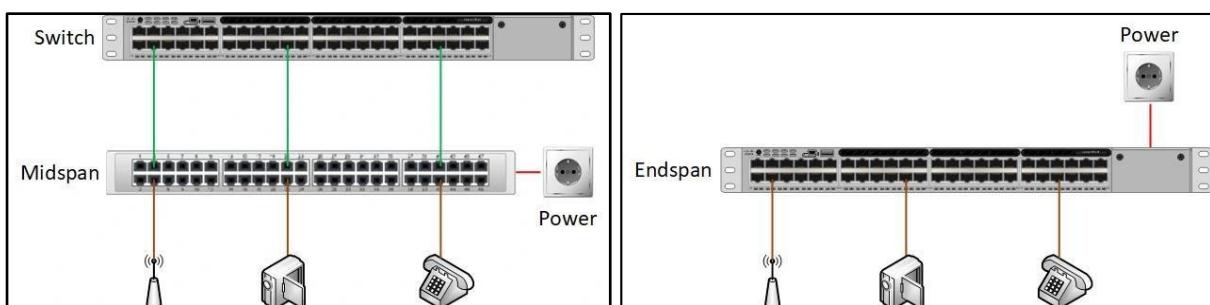
- IP cameras
- Wireless access points
- IoT devices
- Small routers and switches

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 (PoEout).

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



Gambar 1 . 11 Endspan dan 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.

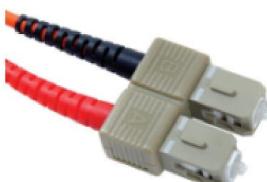
## PHYSICAL TERMINATIONS

packetlife.net

### Optical Terminations



ST (Straight Tip)



SC (Subscriber Connector)



LC (Local Connector)



MT-RJ

### Wireless Antennas



RP-TNC



RP-SMA



RJ-45



RJ-11



RJ-21 (25-pair)



DE-9 (Female)



DB-25 (Male)



DB-60 (Male)



1000Base-SX/LX



1000Base-T



Cisco GigaStack



1000Base-SX/LX SFP



1000Base-T SFP



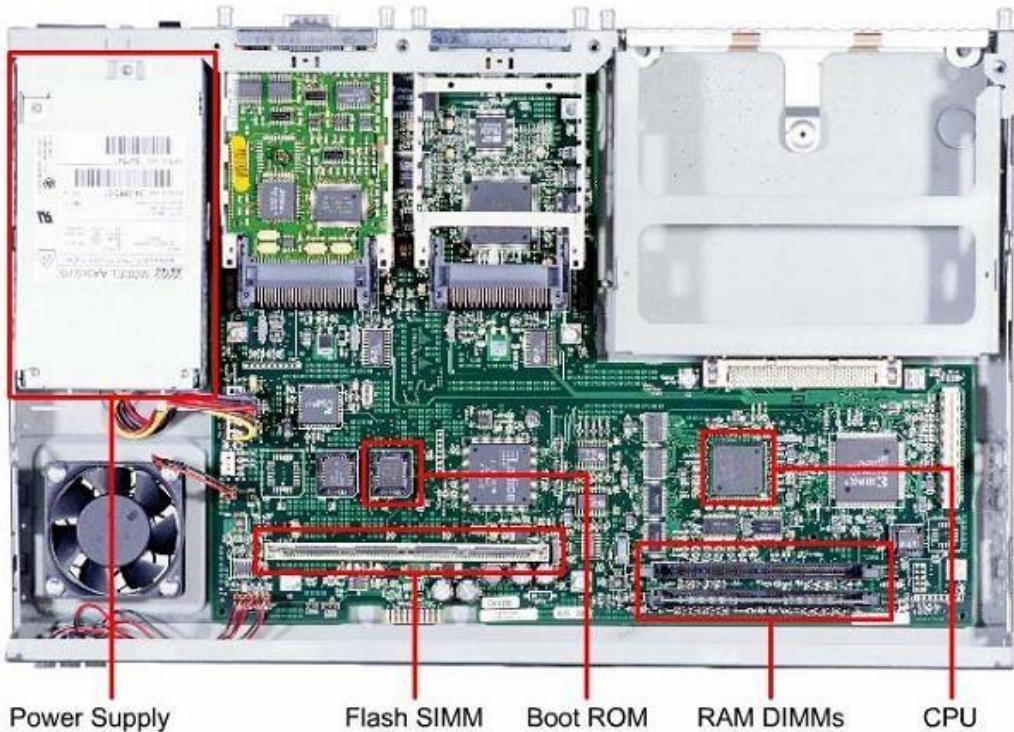
X2 (10Gig)

by Jeremy Stretch

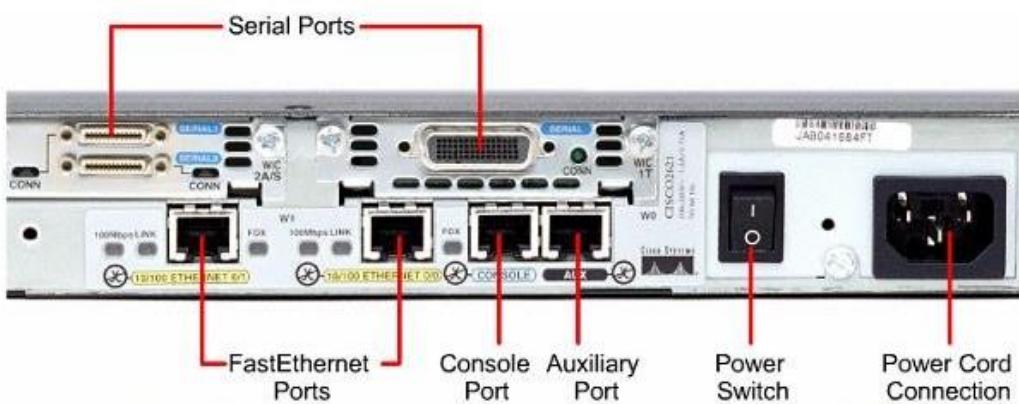
v1.1

# CISCO ROUTER & 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:**

- **CPU**

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

- **RAM**

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

- **NVRAM**

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

- **FLASH**

Flash merupakan tempat penyimpanan Os dari routernya yaitu Cisco IOS.

## **Perbedaan Hub, Switch dan Router**

### **A. Hub**

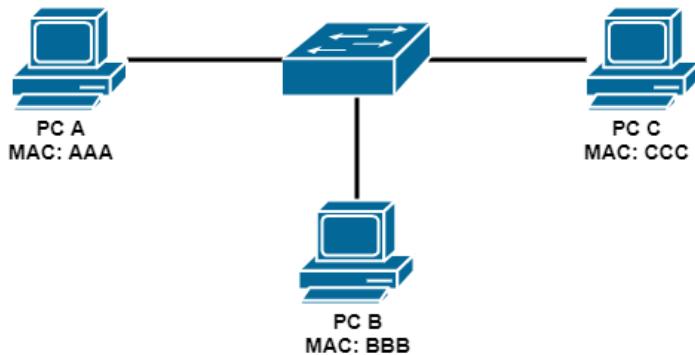
Hub tidak lebih dari physical repeater yang bekerja pada layer 1 dan tidak punya intelijensi. Cara kerja hub adalah dengan menerima sinyal electric dari satu interface dan mengirimkannya ke semua interface kecuali ke source interface, butuh atau tidak butuh.

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:



Gambar 1 . 14 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.

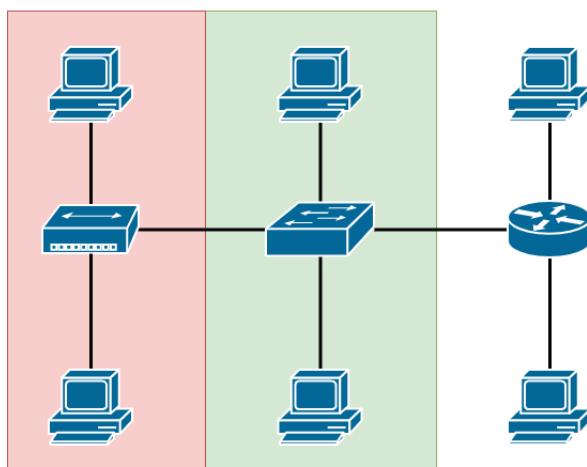
Catatan: Switch melakukan broadcast hanya ketika ada packet data yang destination MAC addressnya tidak terdapat pada tabel MAC address switch.

### 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

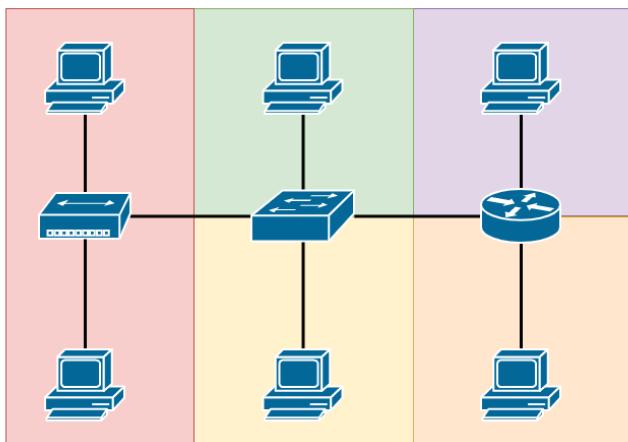
## Broadcast Domain



Gambar 1 . 15 Braodcast 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



Gambar 1 . 16 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

# INITIAL CONFIGURATION

## CLI Mode

```
router> router> ?  
router> enable  
ketika tanda ‘>’ ini pada posisi user mode
```

```
router# router# ?  
router# disable  
Ketika tanda ‘#’ ini adalah pada posisi privilege mode
```

```
router>  
router> enable  
router#conf t  
router(config)# ?
```

Ketika muncul ‘router(config)#’ ini pada posisi global config mode. Dari global config mode, jika ingin kembali ke privilege mode, kita tinggal menekan ‘ctrl+z’ atau end.

## Perintah SHOW

Perintah ‘show’ ini digunakan untuk melakukan verifikasi

```
router#show ?  
router#sh version  
router#sh flash  
router#sh start  
router#sh 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#sh run  
Building configuration...  
  
Current configuration : 852 bytes  
!  
version 12.4  
service timestamps debug datetime msec  
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
```

Perintah selanjutnya adalah **#show ip interface brief**

Interface	IP-Address	OK?	Method	Status
FastEthernet0/0	unassigned	YES	NVRAM	administratively down
FastEthernet0/1	unassigned	YES	NVRAM	administratively down

Status port yang akan kita temui akan ada 4:

- administratively down down : artinya status portnya dimatikan
  - down down : ada masalah L1 (Layer 1) -
  - up down : ada masalah L2 (Layer 2)

- up up : Layer 1 dan Layer 2 oke

## 5 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
```

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.

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 Bosque!! 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 Bosque!!  
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.

### Tips CLI

- Untuk menghapus satu kata (CTRL+W)
- Untuk kembali ke awal kata (CTRL+A)
- Untuk menuju ke akhir kata (CTRL+E)
- Untuk menghapus satu baris dari arah marker (CTRL+X)
- Untuk exit satu level keatas (CTRL+C)
- Untuk exit ke mode privilege (CTRL+Z)

# REMOTE ACCESS

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 konfig adalah line vty. Berikut ini adalah cara mengkonfigurasinya

## Remote Telnet

```
SEMARANG#conf t
SEMARANG(config)#line vty 0 4
SEMARANG(config-line)#login local
SEMARANG(config-line)#username cisco secret cisco
SEMARANG(config)#enable secret cisco
```

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.

Nah, kalau kita ingin tiap orang yang meremote memiliki authentikasi yang berbeda2, konfigurasinya sebagai berikut.

```
SEMARANG#conf t
SEMARANG(config)#line vty 0
SEMARANG(config-line)#no login

SEMARANG(config-line)#line vty 1
SEMARANG(config-line)#login local
SEMARANG(config-line)#privilege level 15
```

```
SEMARANG(config-line)#line vty 2
SEMARANG(config-line)#password 12345
SEMARANG(config-line)#login

SEMARANG(config-line)#line vty 3 4
SEMARANG(config-line)#password 6789
SEMARANG(config-line)#login

SEMARANG(config-line)#username abc password def
SEMARANG(config)#enable secret cisco
```

Konfigurasi di atas artinya, orang ke-1 yang melakukan remote, dia tidak akan login/langsung masuk. Orang ke-2 akan menggunakan username dan password, tapi akan langsung masuk ke privilege mode. Orang ke-3 akan login menggunakan password 12345. Orang ke-4 dan ke-5 akan login menggunakan password 6789.

## Remote SSH

Kalau hanya mengkonfigurasi dengan cara di atas, maka hanya protocol telnet saja yang bisa digunakan. Agar SSH bisa dipakai, tambahkan command berikut

```
SEMARANG(config)#line vty 0 4
SEMARANG(config-line)#transport input ssh
```

Namun, dengan command tersebut, justru telnet tidak bisa lewat, biar keduanya bisa lewat, command yang digunakan adalah :

```
SEMARANG(config)#line vty 0 4
SEMARANG(config-line)#transport input all
```

Ingat, untuk melakukan remote syaratnya router/switch **harus memiliki IP Address** yang reachable dari host.

```
SEMARANG(config)#ip domain-name idn.id
SEMARANG(config)#crypto key generate rsa
% You already have RSA keys defined named SEMARANG.idn.id.
```

```
Choose the size of the key modulus in the range of 360 to 4096 for
your General Purpose Keys. Choosing a key modulus greater than 512
may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

SEMARANG(config)#line vty 0 4
SEMARANG(config-line)#transport input all
SEMARANG(config-line)#login local
SEMARANG(config-line)#exit
SEMARANG(config) # username cisco password cisco
```

Catatan: Modulus RSA: Semakin Besar Enskripsi Semakin Susah Untuk Connect Via SSH. Jadi Harus Di ‘Transport Input SSH’ Tengah-Tengah: 1024

Perintah lain untuk konfigurasi SSH tanpa domain name:

```
R2(config) #crypto key generate rsa general-keys label R2 modulus 1024
The name for the keys will be: R2

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config) #
*Mar 1 00:01:55.935: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Untuk melakukan testing di packet tracer, masukan perintah “**ssh -I<username><ipaddress>**”.

## Perbedaan Telnet dan SSH

Telnet: Paketnya tidak terenkripsi, rentan pecurian data

SSH: Paketnya terenkripsi, aman dari pencurian data

## Catatan:

---

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

---

-Imam Syafi'i-

# Switching Session

CHAPTER 2

CCNA

ENTERPRISE

# **SWITCHING**

# **SESSION**

## **CONTENT:**

**VLAN (VIRTUAL LAN)**

**TRUNK**

**NATIVE VLAN**

**INTERVLAN ROUTING (ROUTER ON STICK)**

**PORT SECURITY**

**STP (SPANNING TREE PROTOCOL)**

**SPANNING TREE PORTFAST**

**ETHERCHANNEL**

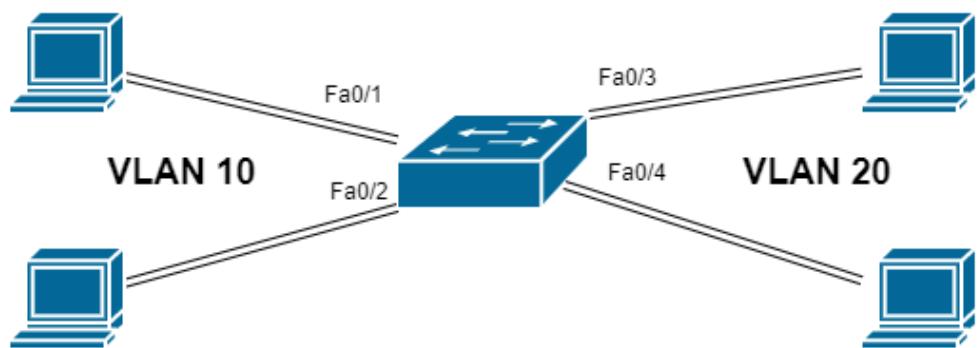
**NEIGHBOR DISCOVERY**

# 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 segmen/bagian yang dimana tiap segmen ini tidak dapat saling berkomunikasi padahal sudah satu network.

Hal ini dikarenakan VLAN tadi, yang memecah networknya. Dan VLAN ini, berjalan/hanya bisa dikonfigurasi di switch yang bekerja dilayer 2 yaitu data link. Karena switch sendiri, merupakan perangkat yang bisa menghubungkan satu jaringan saja.

Apabila kita menggunakan switch unmanaged, switch-switch harga 100 ribuan, maka semua portnya hanya bisa digunakan untuk dikoneksikan ke PC yang networknya sama. Nah pada switch managed, 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.



Gambar 2 . 1 Lab VLAN

Dengan adanya VLAN ini, maka kita bisa memisahkan atau mengelompokkan user sesuai kebutuhannya masing-masing. Misal kita bisa membuat VLAN Dosen, VLAN

Mahasiswa, VLAN Karyawan, VLAN Server, VLAN Lab, VLAN public dll. Bisa juga berdasarkan lantai, misal vlan 1 untuk semua network di lantai 1, vlan 2 untuk semua user di lantai 2 dst nya.

## MEMBUAT VLAN PADA SWITCH

```
Switch#configure terminal  
Switch(config) #vlan 10  
Switch(config-vlan)#name Kelas  
Switch(config) #vlan 20  
Switch(config-vlan)#name Kantor
```

## MASUKKAN VLAN KE PORTNYA

```
Switch(config) #int f0/1  
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan 10  
Switch(config) #int f0/2  
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan 10  
Switch(config) #int f0/3  
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan 20  
Switch(config) #int f0/4  
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan 20
```

Jika sudah, kita verifikasi/cek terlebih dahulu dengan perintah *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 verifikasi terlebih dahulu.

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
10	Kelas	active	Fa0/1, Fa0/2
20	Kantor	active	Fa0/3, Fa0/4
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Koneksikan PC ke Switch port f0/1-4 dengan menggunakan kabel straight. Kemudian setting PC dengan IP 10.10.10.10/24 dan 10.10.10.11/24 untuk PC VLAN 10 dan IP 10.10.10.13/24 dan 20.20.20.14/24 untuk pc vlan 20.

Pengetesannya lakukan ping ke PC lain baik dalam vlan yang sama maupun vlan yang berbeda.

Setelah melakukan tes ping, pada switch tampilkan mac address tabelnya

Switch#show mac-address-table			
Mac Address Table			
Vlan	Mac Address	Type	Ports
---	-----	-----	-----
10	0030.a3d3.8c27	DYNAMIC	Fa0/1
10	0090.2b28.0093	DYNAMIC	Fa0/2
20	0001.4350.7080	DYNAMIC	Fa0/4
20	0060.3e41.3a8d	DYNAMIC	Fa0/3

Berdasarkan Lab diatas, dapat kita simpulkan. Saat kita melakukan test ping antar PC yang berada di vlan yang sama, alhasil dapat berkomunikasi. Namun, jika berbeda vlan, hasilnya akan *timeout*, karena sudah berbeda vlan-nya.

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

by Jeremy Stretch

v2.0

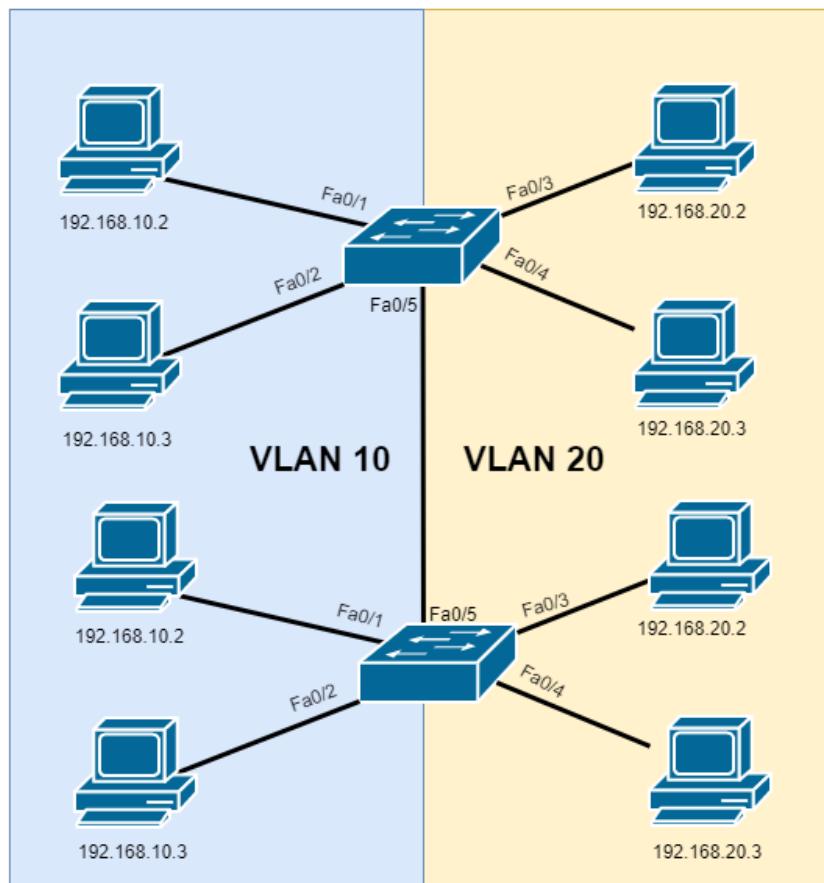
# TRUNK

Bagaimana caranya jika kita ingin menghubungkan 2 buah pc 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 enkapsulasi trunk yang hanya dikhususkan untuk switch cisco.
2. dot1q (Open Standard)- Protokol encapsulasi trunk standar yang bisa digunakan disemua jenis dan merek switch.



Gambar 2 . 2 Lab Trunk

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

```
Sw1(config)#int fa0/10
Sw1(config-if)#switchport trunk encapsulation dot1q -> 1
Sw1(config-if)#switchport mode trunk -> 2
```

1. Pada switch cisco support trunk dot1q (open standard) dan ISL (cisco proprietary)
2. Untuk switch seri tertentu (contoh: 2950&2960) hanya support dot1q. Jadi kalau pakai seri switch 2950 atau 2960 untuk konfigurasi trunknya hanya perlu command berikut :

```
Sw_contoh(config)#int fa0/10
Sw_contoh(config-if)#switchport mode trunk
```

Untuk mengecek apakah trunk yang kita konfigurasikan sudah berjalan atau belum, ketikkan command *show interface trunk*

```
SW1#sh int trunk
Port      Mode          Encapsulation  Status       Native
vlan Fa0/10    on           802.1q        trunking
               1
Port      Vlans allowed on trunk
Fa0/10   1-1005

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

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

```
SW2#sh int trunk
Port      Mode          Encapsulation  Status       Native vlan
Fa0/10    on           802.1q        trunking
               1
Port      Vlans allowed on trunk
Fa0/10   1-1005

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

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

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

## Allowed Trunk

Filtering VLAN saat menggunakan Trunk seringkali harus dilakukan oleh Network Engineer. 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 diatas kita akan mencoba untuk filtering VLAN 20 agar tidak dilewatkan ke Switch atas.

Caranya dengan masuk ke interface trunk, alu memilih VLAN mana yang akan di perbolehkan atau VLAN mana yang akan di filter.

```
SW2(config-if)#switchport trunk allowed vlan ?
WORD      VLAN IDs of the allowed VLANs when this port is in trunking mode
add       add VLANs to the current list
all       all VLANs
except    all VLANs except the following
none     no VLANs
remove   remove VLANs from the current list
SW2(config-if)#switchport trunk allowed vlan 1,10
```

Pada perintah sebelumnya dapat dilihat bahwa opsi yang tersedia untuk allowed VLAN cukup bervariasi.

Namun untuk kebutuhan kita saat ini, command yang digunakan cukup allow VLAN 1 dan 10 saja.

Untuk verifikasi, masukan perintah show interface trunk

```
SW2#show interface trunk
Port      Mode      Encapsulation      Status      Native vlan
Fa0/10    on        802.1q            trunking    1

Port      Vlans allowed on trunk
Fa0/10    1,10

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

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

# NATIVE VLAN

Native VLAN merupakan sebuah tipe/terminologi dalam vlan yang dikhususkan untuk mendukung hub, atau switch yang ketinggalan jaman. Istilah Native VLAN hanya akan ditemui jika kita menggunakan sebuah interface Trunk 802.1Q.

Fungsi dari Native Vlan ini sendiri, yaitu untuk menghubungkan antara hub maupun switch yang tidak mendukung protocol enkapsulasi dot1q pada interface nya. Jadi, ketika kita ingin melakukan trunk kepada hub/switch tersebut, kita gunakan native vlan.

Secara default, Native VLAN yang digunakan adalah VLAN 1. Biasanya banyak yang bingung perbedaan antara VLAN 1 (default) dengan Native VLAN. Namun sebenarnya Native VLAN dan Default VLAN merupakan 2 hal yang sangat berbeda. Karena seperti yang sudah disebutkan diatas, Native VLAN hanya akan ditemui di interface Trunk namun berbeda dengan Default VLAN yang sudah ada di setiap Switch.

Kita bisa lihat Native Vlan dengan mengetikkan command *show interface trunk*.

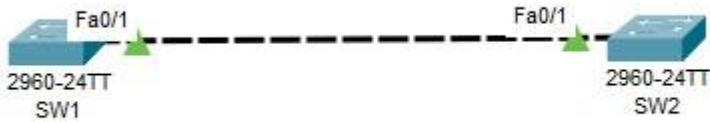
```
SW2#show interface trunk
Port      Mode      Encapsulation          Status           Native vlan
Fa0/10    on        802.1q                  trunking        1

Port      Vlans allowed on trunk
Fa0/10    1-1005

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

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

Dalam sebuah link trunk juga sangat dianjurkan untuk merubah settingan default VLAN menjadi VLAN lain selain VLAN 1. Dan untuk Lab kali ini, kita akan mencoba untuk merubah settingan Native VLAN dengan VLAN lain. Topology yang akan kita gunakan sangat simple, cukup gunakan 2 switch seperti ini dan konfigurasikan trunk antar switch.



```
SW(config) #vlan 99
SW(config-vlan)#name native
SW(config) #int fa0/1
SW(config-if)#switchport mode trunk
SW(config-if)#switchport trunk native vlan 99
```

Terapkan command diatas, ke setiap switch agar tidak terjadi Native VLAN Mismatch.

Untuk verifikasi kita bisa menggunakan perintah show interface trunk.

```
SW1#show int tr
Port      Mode       Encapsulation  Status          Native vlan
Fa0/1    on        802.1q        trunking          99

Port      Vlans allowed on trunk
Fa0/1    1-1005

Port      Vlans allowed and active in management
domain   Fa0/1      1,99

Port      Vlans in spanning tree forwarding state
pruned  Fa0/1      1

SW1#
```

```
SW2#show interface trunk
Port      Mode       Encapsulation  Status          Native Vlan
Fa0/1    on        802.1q        trunking          99

Port      Vlans allowed on trunk
Fa0/1    1-1005

Port      Vlans allowed and active in management
domain   Fa0/1      1,99

Port      Vlans in spanning tree forwarding state and not
pruned  Fa0/1      1,99

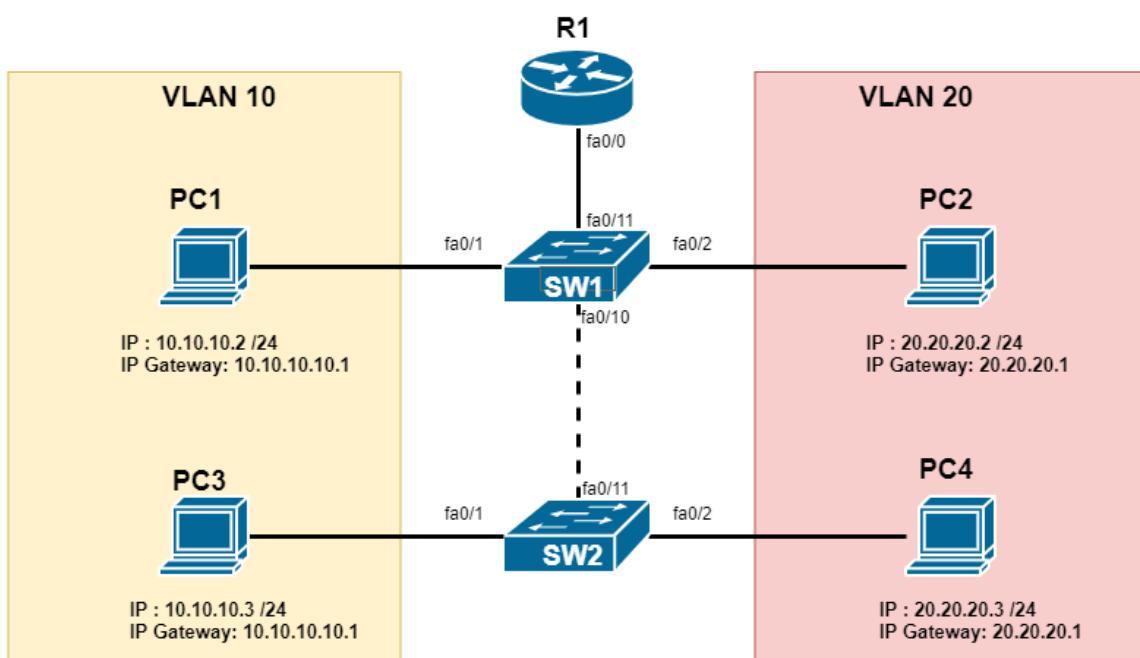
SW2#
```

# INTERVLAN

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. Kasus seperti ini biasa disebut dengan nama Intervlan Routing.

## Router on Stick

Berikut contoh topologinya:



Gambar 2 . 3 Lab Intervlan 1

Apabila kita menghubungkan switch ke router dimana ada beberapa VLAN yang perlu dilewatkan diantaranya, maka pada switch diset Trunk. Namun bila pada switch hanya terdapat 1 vlan saja maka cukup diset access. Kali ini karena kita ingin melewakan beberapa vlan yakni vlan 10 dan 20, maka di sisi switch diset trunk. Gunakan kabel straight untuk menghubungkan switch ke router.

Langkah – langkah konfigurasi :

## Membuat vlan di SW1 & SW2

```
SW1#conf t  
SW1(config)#vlan 10  
SW1(config)#vlan 20
```

```
SW2#conf t  
SW2(config)#vlan 10  
SW2(config)#vlan 20
```

## Meng-assign port ke vlan

```
SW1(config)#int f0/1  
SW1(config-if)#switchport access vlan 10 SW1(config)#int f0/2  
SW1(config-if)#switchport access vlan 20
```

```
SW2(config)#int f0/1  
SW2(config-if)#switchport access vlan 10  
SW2(config)#int f0/2  
SW2(config-if)#switchport access vlan 20
```

## Konfigurasi trunk di port antar SW1,SW2 dan ke Router

```
SW1(config)#int f0/10  
SW1(config-if)#switchport mode trunk  
SW1(config)#int f0/11  
SW1(config-if)#switchport mode trunk  
  
SW2(config)#int f0/11  
SW2(config-if)#switchport mode trunk
```

Disini kita akan mengfungsikan router sebagai gateway untuk vlan 10 dan vlan 20. Agar router bisa digunakan untuk gateway vlan , maka kita konfigurasi sub-interface. Berikut contohnya :

```
router# sh ip int brief  
Interface IP-Address OK? Method Status  
Protocol  
FastEthernet0/0 unassigned YES NVRAM administratively  
down down  
FastEthernet0/1 unassigned YES NVRAM administratively  
down down
```

kita lihat , diatas interface fisiknya adalah fastEthernet0/0. kita ingin membuat sub interface yang difungsikan sebagai gateway untuk vlan 10 dan 20.

```
ROUTER(config)#int Fa0/0  
ROUTER(config-if)#no shut  
ROUTER(config)#int Fa0/0.10 >> SUB INTERFACE  
ROUTER(config-subif)#encapsulation dot1q 10  
ROUTER(config-subif)#ip addr 10.10.10.1 255.255.255.0  
ROUTER(config)#int Fa0/0.20  
ROUTER(config-subif)#encapsulation dot1q 20
```

```
ROUTER(config-subif) #ip addr 20.20.20.1 255.255.255.0
```

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.

#### Pastikan konfigurasi router sudah benar dengan verifikasi :

Router#sh ip int br	Interface	IP-Address	OK?	Method	Status	Protocol
	FastEthernet0/0	unassigned	YES	unset	up	up
	FastEthernet0/0.10	10.10.10.1	YES	manual	up	up
	FastEthernet0/0.20	20.20.20.1	YES	manual	up	up

Jika ingin verifikasi lebih detail : #show run

Pada router kita membuat subinterface 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 vlannya.

#### Fa0/0 = main interface **fa0/0.10** dan **f0/0.20** = subinterface

Tipe encapsulation yang digunakan adalah dot1q (802.1q), pilihan lainnya adalah ISL(cisco Proprietary). Namun demikian tidak semua router dan switch support ISL, sehingga enkapsulasi dot1q lebih banyak digunakan. Pada switch tanpa kita mendefinisikan tipe enkapsulasinya, maka yang digunakan oleh switch adalah dot1q secara default.

Pengetesannya, lakukan tes ping ke ip gatewanya terlebih dahulu, bila mendapatkan reply, selanjutnya lakukan ping ke pc lain yang berbeda vlan. Setelah semua pc diping satu persatu, pada router akan muncul tampilan berikut ketika kita mengetikkan show arp

```
Router#show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.10.10.2	2		0090.2B28.0093	ARPA
FastEthernet0/0.10					
Internet	10.10.10.3	1		0030.A3D3.8C27	ARPA
FastEthernet0/0.10					
Internet	10.10.10.4	0		00D0.D39D.5A73	ARPA
FastEthernet0/0.10					
Internet	20.20.20.2	0		0001.4350.7080	ARPA
FastEthernet0/0.20					
Internet	20.20.20.3	0	0060.3E41.3A8D	ARPA	
FastEthernet0/0.20	Internet	20.20.20.4		2	000A.4134.4E8A
ARPA	FastEthernet0/0.20				

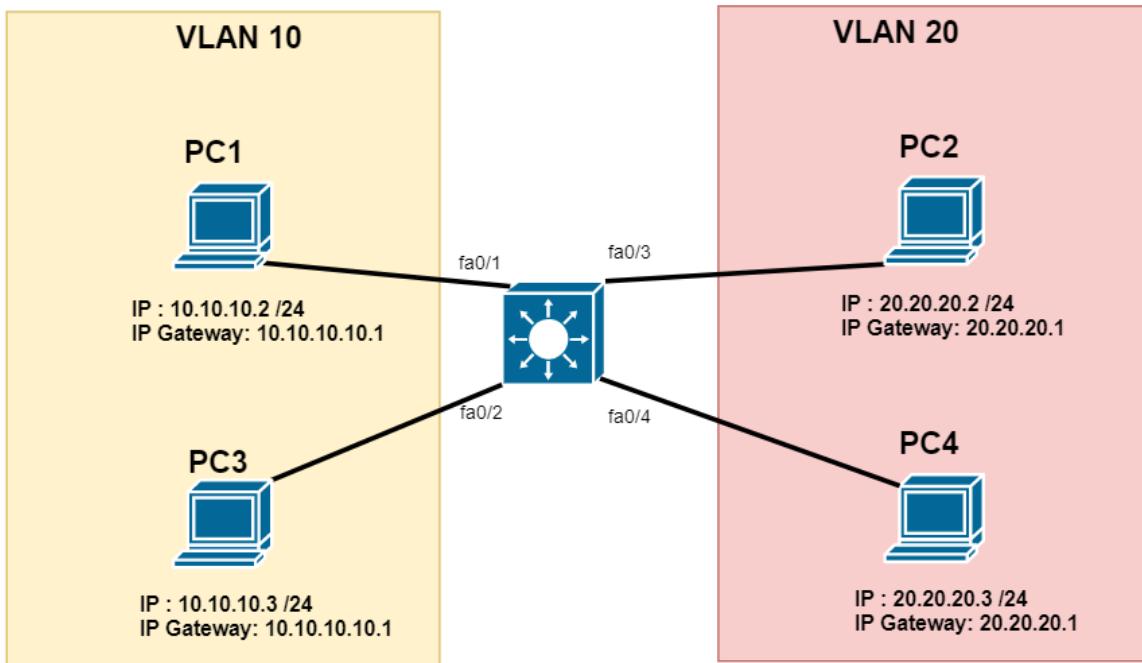
Sebagai tambahan, kita bisa membuat vlan management utk telnet ke switch.

```
SW1(config)#vlan 30
SW1(config-vlan)#name MANAGEMENT
SW1(config-vlan)#int vlan 30
SW1(config-if)#ip address 30.30.30.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#ip default-gateway 30.30.30.30
SW1(config)#line vty 0 4
SW1(config-line)#password cisco
SW1(config-line)#login
SW1(config-line)#enable secret cisco
```

Tambahkan konfigurasi di sisi Router.

```
ROUTER(config)#int Fa0/0.30
ROUTER(config-if)#encapsulation dot1q 30
ROUTER(config-if)#ip addr 30.30.30.30 255.255.255.0
```

## Multilayer Switch (MLS)



Gambar 2 . 4 Lab MLS

Buat vlan 10 dan 20 terlebih dahulu

```
switch(config) #vlan 10  
switch(config) #vlan 20
```

Assign VLAN 10 dan 20 ke port interface switch

```
switch(config) #int fa0/1  
Switch(config-if)#switchport mode access  
switch(config-if)#switchport access vlan 10  
switch(config) #int fa0/2  
Switch(config-if)#switchport mode access  
switch(config-if)#switchport access vlan 10  
switch(config) #int fa0/3  
Switch(config-if)#switchport mode access  
switch(config-if)#switchport access vlan 20  
switch(config) #int fa0/4  
Switch(config-if)#switchport mode access  
switch(config-if)#switchport access vlan 20
```

Konfigurasikan IP Address Interface VLAN

```
switch(config) #int vlan 10  
switch(config-if)#ip address 10.10.10.1 255.255.255.0  
switch(config) #int vlan 20  
switch(config-if)#ip address 20.20.20.1 255.255.255.0
```

Aktifkan ip routing agar bisa meroutingkan antar vlan yang berbeda.

```
switch(config) #ip routing
```

Konfigurasikan IP Address pada setiap PC di Vlan10 dengan IP 10.10.10.2/24 & 10.10.10.3/24 dengan IP gateway 10.10.10.1. PC pada Vlan20 dan IP 20.20.20.2/24 & 20.20.20.3/24 dengan IP Gateway 20.20.20.1 Pengetesannya, lakukan tes ping ke ip gatewanya terlebih dahulu, bila mendapatkan reply, selanjutnya lakukan ping ke pc lain yang berbeda vlan.

```
Switch#show ip int br
Interface          IP-Address      OK? Method Status           Protocol
FastEthernet0/1    unassigned     YES unset  up               up
FastEthernet0/2    unassigned     YES unset  up               up
FastEthernet0/3    unassigned     YES unset  up               up
FastEthernet0/4    unassigned     YES unset  up               up
FastEthernet0/5    unassigned     YES unset  down             down
FastEthernet0/6    unassigned     YES unset  down             down
FastEthernet0/7    unassigned     YES unset  down             down
FastEthernet0/8    unassigned     YES unset  down             down
FastEthernet0/9    unassigned     YES unset  down             down
FastEthernet0/10   unassigned     YES unset  down             down
FastEthernet0/11   unassigned     YES unset  down             down
FastEthernet0/12   unassigned     YES unset  down             down
GigabitEthernet0/1 unassigned     YES unset  down             down
GigabitEthernet0/2 unassigned     YES unset  down             down
Vlan1              unassigned     YES unset  administratively down down
Vlan10             10.10.10.1    YES manual up              up
Vlan20             20.20.20.1    YES manual up              up
Switch#
```

Setelah semua pc diping satu persatu, tampilkan mac address tabelnya

```
Switch#show mac address-table
Mac Address Table
-----
Vlan   Mac Address        Type      Ports
---  -----
 10   0060.5c4c.4bb9  DYNAMIC   Fa0/1
 10   0060.7082.1b9d  DYNAMIC   Fa0/2
 20   0002.1762.2eb3  DYNAMIC   Fa0/4
 20   000c.cf4b.3ae9  DYNAMIC   Fa0/3
```

Tampilkan informasi arp nya

```
Switch#show arp
Protocol  Address          Age (min)  Hardware Addr  Type  Interface
Internet  10.10.10.1      -          00D0.BCA2.C9E6  ARPA  Vlan10
Internet  10.10.10.2      9          0060.5C4C.4BB9  ARPA  Vlan10
Internet  10.10.10.3      0          0060.7082.1B9D  ARPA  Vlan10
Internet  20.20.20.1      -          00D0.BCA2.C9E6  ARPA  Vlan20
Internet  20.20.20.2      0          000C.CF4B.3AE9  ARPA  Vlan20
Internet  20.20.20.3      9          0002.1762.2EB3  ARPA  Vlan20
```

# NEIGHBOR DISCOVERY

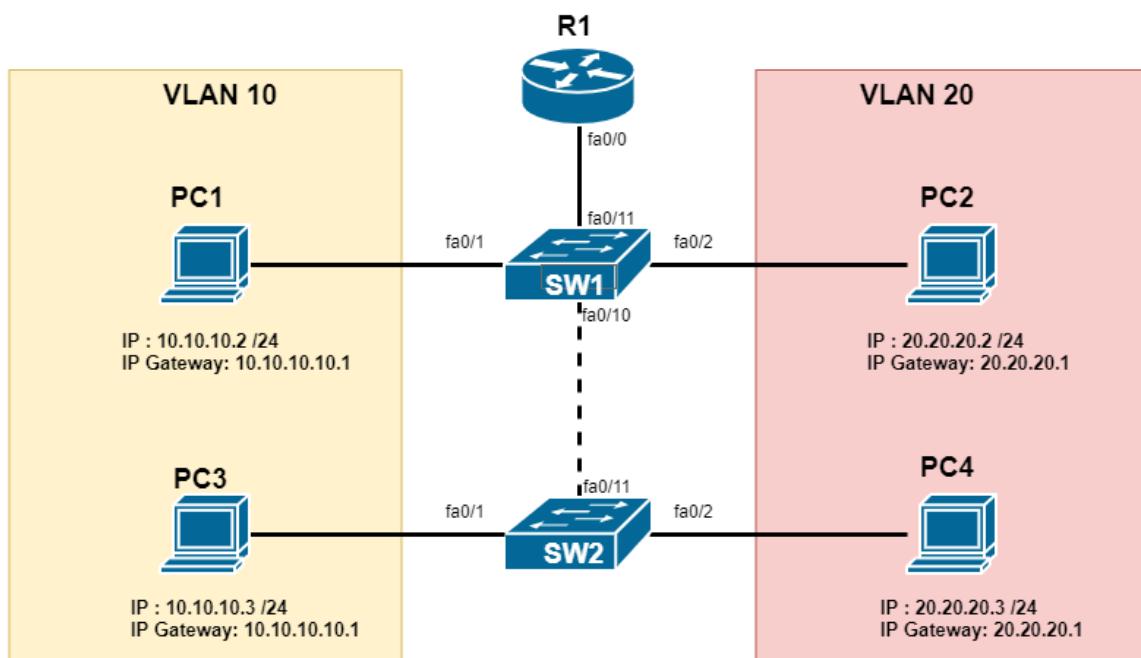
Saat kita berada dilapangan, pada saat kita me-remote sebuah perangkat, kadangkala kita bingung. Dengan perangkat apakah yang terhubung dengan perangkat yang kita remote ini. Maka dari itu, untuk mengetahui kemanakah perangkatnya terhubung kita gunakan protocol *Neighbor Discovery*.

Protokol ini berjalan di layer 2. Terdapat 2 macam Neighbor Discovery pada Cisco:

1. CDP (Cisco Discovery Protocol)
2. LLDP (Link Layer Discovery Protocol)

Fungsi dari kedua protocol ini sama persis, namun secara default pada perangkat cisco hanya running CDP saja.

Untuk Lab CDP & LLDP kita akan menggunakan topologi dari LAB sebelumnya.



Gambar 2 . 5 Lab Neigbor Discovery

Untuk konfigurasinya, cukup ketikkan command di setiap perangkat jaringan:

## LLDP

```
SW1(config)# lldp run  
SW2(config)# lldp run  
R1(config)# lldp run
```

## CDP

```
SW1(config)# cdp run  
SW2(config)# cdp run  
R1(config)# cdp run
```

Jika kedua command neighbor discovery sudah kita ketikkan, maka kita dapat melihat isi neighbor discovery tersebut dengan mengetikkan command:

## CDP

Dari Router

```
R1#show cdp neighbor  
Capability Codes: R - Router, T - Trans Bridge, B - Source Route  
Bridge  
                                S - Switch, H - Host, I - IGMP, r - Repeater, P -  
Phone  
Device ID      Local Intrfce     Holdtme   Capability  Platform    Port  
ID SW1          Fas 0/0           176        S          2960  
Fas 0/11  
R1#
```

Dari Switch

```
SW1#show cdp neighbor  
Capability Codes: R - Router, T - Trans Bridge, B - Source Route  
Bridge  
                                S - Switch, H - Host, I - IGMP, r - Repeater, P -  
Phone  
Device ID      Local Intrfce     Holdtme   Capability  Platform    Port  
ID  
R1             Fas 0/11          141        R          C1841      Fas  
0/0  
R1             Fas 0/11          141        R          C1841      Fas  
0/0.10  
R1             Fas 0/11          141        R          C1841      Fas  
0/0.20  
SW2             Fas 0/10          141        S          2960      Fas  
0/10
```

## LLDP

Dari Router

```
R1#show lldp neighbor  
Capability codes:  
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device  
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

Device ID Switch	Local Intf Fa	Hold-time 120	Capability B	Port ID Fa0/11
Total entries displayed: 1				

### Dari Switch

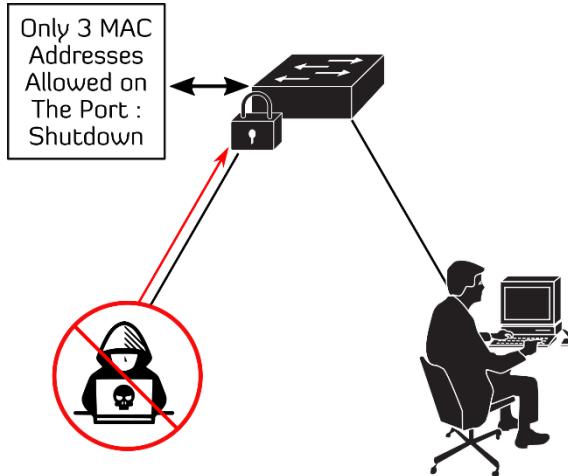
```
SW1#show lldp neighbor
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID          Local Intf      Hold-time  Capability      Port ID
R1                Fa0/11        120          R            Fa
Total entries displayed: 1
```

Jika kita ingin melihat lebih lengkap lagi mengenai neighbor discovery, ketikkan command berikut:

```
SW1#show cdp neighbor detail
SW1#show lldp neighbor detail
```

Secara fungsi dan keunggulan, jauh lebih baik CDP daripada LLDP. Karena informasi yang diberikan oleh CDP lebih lengkap daripada LLDP, namun CDP hanya dapat dikonfigurasikan pada perangkat jaringan merk Cisco saja, sementara untuk semua vendor, alias *open standart*, lebih baik menggunakan LLDP.

## PORT SECURITY



Gambar 2 . 6 Illustrasi 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 menantisipasi, kita dapat menggunakan Port Security.

Langkah-langkah konfigurasi Port Security:

- Pertama-tama, kita aktifkan terlebih dahulu command port security pada port yang ingin kita amankan.

```
Switch (config) #int fa0/1
Switch (config-if)#switchport mode access
Switch (config-if)#switchport 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.

```
Switch (config) #switchport port security mac address ?
Switch (config-if)#switchport port-security mac-address ?
H.H.H      48 bit mac address
sticky     Configure dynamic secure addresses as sticky
```

- Selanjutnya kita pilih violation untuk portnya. Terdapat 3 violation:
  - **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)

```
Switch (config-if)#switchport port security violation shutdown
```

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. Namun kita bisa merubah nilai maximal mac Address yang dapat di simpan di interface tersebut. (MAX = 132 Mac Address)

```
Switch(config)#int fa0/1
Switch(config-if)#switchport port-security maximum ? <1-132> Maximum
addresses
Switch(config-if)#switchport port-security maximum 2
```

Jika kita ingin mengembalikan status port yang ada di state **err-disable** maka kita bisa melakukan perintah berikut:

```
Switch(config)#int fa0/1
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
```

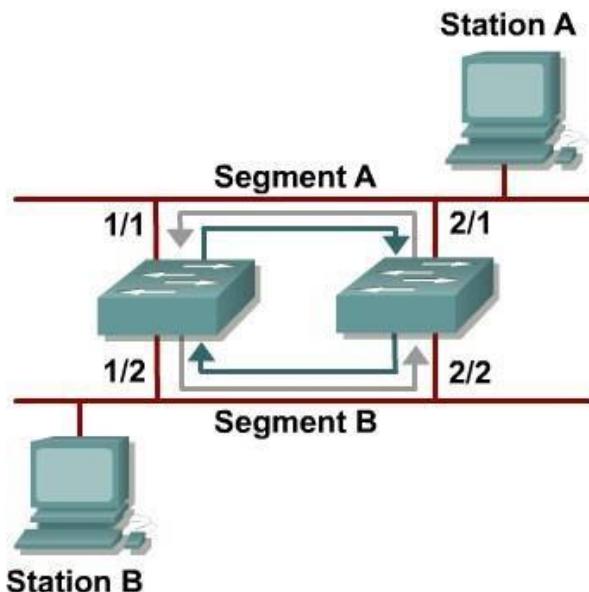
Namun jika dirasa langkah tersebut merepotkan, kita bisa mengembalikan status port secara otomatis dengan menggunakan perintah:

```
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#errdisable recovery interval 30
```

Dengan memasukan perintah diatas, maka setiap 30 detik port akan restore ke keadaan semula, sehingga tidak perlu merepotkan admin. Defaultnya recovery interval dari errdisable sendiri ialah 5 menit.

# SPANNING TREE PROTOCOL

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



Gambar 2 . 7 Illustrasi STP

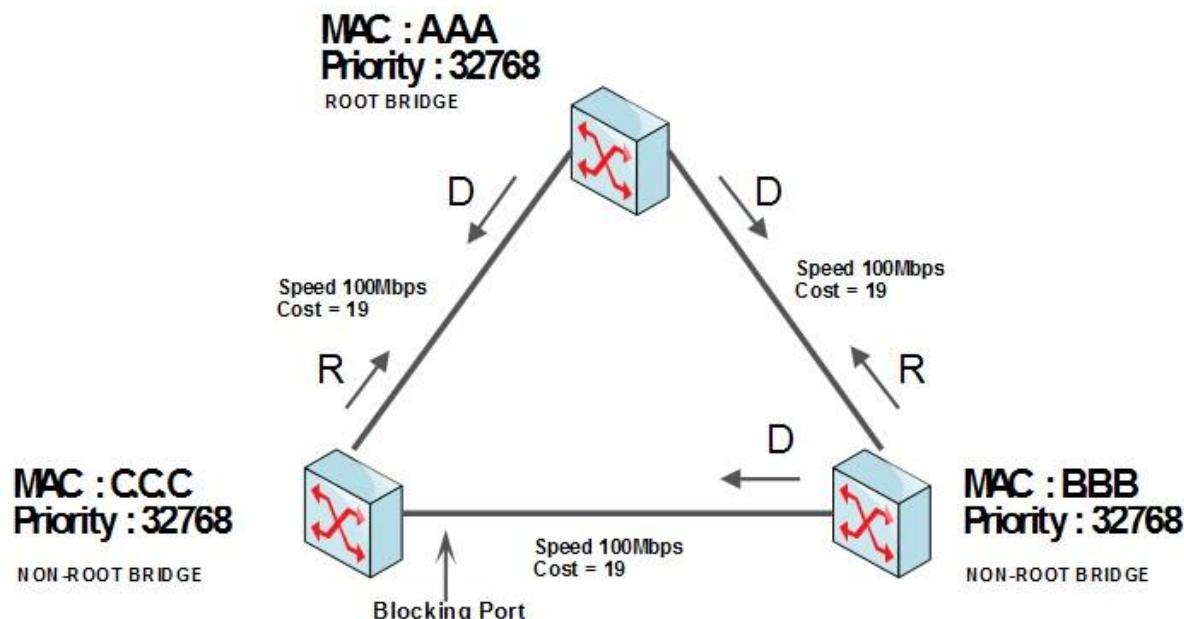
Misalkan pada switch kiri mau mengirim sebuah data yang tidak ada destinasinya pada tabel mac addressnya, sehingga switchnya akan membroadcast ke semua port hingga sampailah ke switch kanan. Sementara di switch kanan juga sama, dia juga tidak tahu destinasinya kemana sehingga dibroadcast ulang dan sampai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



Gambar 2 . 8 Lab 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:**

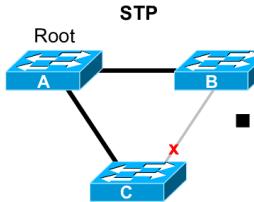
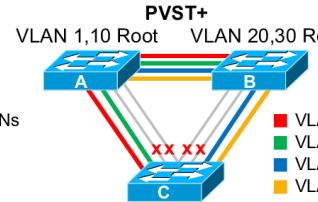
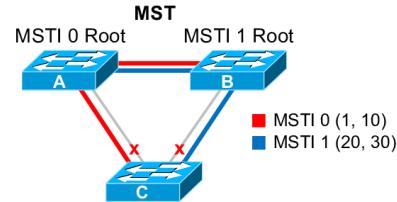
Ethernet: 100

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 802.1s, 802.1Q-2003
<b>Instances</b>	1	Per VLAN	Per VLAN	1	Per VLAN Configurable
<b>Trunking</b>	N/A	ISL	802.1Q, ISL	N/A	802.1Q, ISL 802.1Q, ISL
Spanning Tree Instance Comparison					
<b>STP</b>		<b>PVST+</b>		<b>MST</b>	
	All VLANs	VLAN 1,10 Root VLAN 20,30 Root	VLAN 1 VLAN 10 VLAN 20 VLAN 30	MSTI 0 Root MSTI 1 Root	MSTI 0 (1, 10) MSTI 1 (20, 30)
BPDU Format		Spanning Tree Specifications			Link Costs
Field	Bits	802.1s	802.1Q-2003	802.1Q-2005	Bandwidth Cost
Protocol ID	16	802.1D-1998	802.1Q-1998	802.1D-2004	4 Mbps 250
Version	8			802.1w	10 Mbps 100
BPDU Type	8				16 Mbps 62
Flags	8				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			RPVST+	1 Gbps 4
Message Age	16				10 Gbps 2
Max Age	16				20+ Gbps 1
Hello Time	16				
Forward Delay	16				
Default Timers		IEEE 802.1D-1998 · Deprecated legacy STP standard			Port States
Hello	2s	IEEE 802.1w · Introduced RSTP			Legacy ST Rapid ST
Forward Delay	15s	IEEE 802.1D-2004 · Replaced legacy STP with RSTP			Disabled
Max Age	20s	IEEE 802.1s · Introduced MST			Blocking Discarding
		IEEE 802.1Q-2003 · Added MST to 802.1Q			Listening
		IEEE 802.1Q-2005 · Most recent 802.1Q revision			Learning Learning
		PVST · Per-VLAN implementation of legacy STP			Forwarding Forwarding
		PVST+ · Added 802.1Q trunking to PVST			
		RPVST+ · Per-VLAN implementation of RSTP			
Spanning Tree Operation					
<b>1 Determine root bridge</b>	The bridge advertising the lowest bridge ID becomes the root bridge	Port Roles			
<b>2 Select root port</b>	Each bridge selects its primary port facing the root	Legacy ST Rapid ST			Root Root
<b>3 Select designated ports</b>	One designated port is selected per segment	Designated Designated			Designated Designated
<b>4 Block ports with loops</b>	All non-root and non-designated ports are blocked	Blocking Alternate			Alternate
		Blocking Backup			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 bpduguard enable spanning-tree bpdufilter enable</pre>	<table border="1"> <thead> <tr> <th>4</th> <th>12</th> <th>48</th> </tr> <tr> <th>Pri</th> <th>Sys ID Ext</th> <th>MAC Address</th> </tr> </thead> </table>	4	12	48	Pri	Sys ID Ext	MAC Address
4	12	48					
Pri	Sys ID Ext	MAC Address					
	<b>Priority</b> 4-bit bridge priority (configurable from 0 to 61440 in increments of 4096)						
	<b>System ID Extension</b> 12-bit value taken from VLAN number (IEEE 802.1t)						
	<b>MAC Address</b> 48-bit unique identifier						
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 BPDUs 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	Optional PVST+ Enhancements						
	<b>PortFast</b> Enables immediate transition into the forwarding state (designates edge ports under MST)						
	<b>UplinkFast</b> Enables switches to maintain backup paths to root						
	<b>BackboneFast</b> Enables immediate expiration of the Max Age timer in the event of an indirect link failure						
Spanning Tree Protection	RSTP Link Types						
	<b>Root Guard</b> Prevents a port from becoming the root port						
	<b>BPDU Guard</b> Error-disables a port if a BPDU is received						
	<b>Loop Guard</b> Prevents a blocked port from transitioning to listening after the Max Age timer has expired						
	<b>BPDU Filter</b> Blocks BPDUs on an interface (disables STP)						
Point-to-Point	Point-to-Point						
	<b>Point-to-Point</b> Connects to exactly one other bridge (full duplex)						
Shared	Shared						
	<b>Shared</b> Potentially connects to multiple bridges (half duplex)						
Edge	Edge						
	<b>Edge</b> Connects to a single host; designated by PortFast						
Troubleshooting	Troubleshooting						
	<code>show spanning-tree [summary   detail   root]</code>						
	<code>show spanning-tree [interface   vlan]</code>						
	<code>show spanning-tree mst [...]</code>						

by Jeremy Stretch

v3.0

# SPANNING TREE PORTFAST

Bila kita colokkan kabel ke switch maka biasanya butuh waktu agak lama portnya dari oranye menjadi hijau.

Total waktu yang dibutuhkan adalah 30 detik.

```
Blocking -----> Listening -----> Learning ----->
Forwarding
  (Max Age;optional)      (Forward Delay)      (Forward Delay)
    20 S                  15 S                  15 S
```

```
SW1(config)# interface range fastethernet0/1 - 2
SW1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
```

Dengan memasukan perintah tersebut, 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 30 detik. Portfast, tidak dapat sejalan 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.

Selain dengan perintah diatas, kita juga bisa memasukan perintah **spanning-tree portfast default**.

```
SW1(config)# spanning-tree portfast default
```

Perintah tersebut akan mengaktifkan portfast disetiap port yang menggunakan mode access. Jadi tidak perlu konfigurasi ke setiap interface untuk set portfast.

# 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.

Syarat wajib terbentuknya Etherchannel, yaitu:

- Duplex sama.
- Speed sama.
- Switchport mode harus sama di kedua sisi.
- Native VLAN harus sama.

Terdapat 3 jenis Etherchannel:

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

Open Standard IEEE 802.1AD Etherchannel, terdapat 2 mode:

- **Active**: Protokol LACP yang mengajak untuk menjadi etherchannel
- **Passive**: Protokol LACP yang menunggu untuk menjadi etherchannel

- **PAGP (Port Aggregation Protocol)**

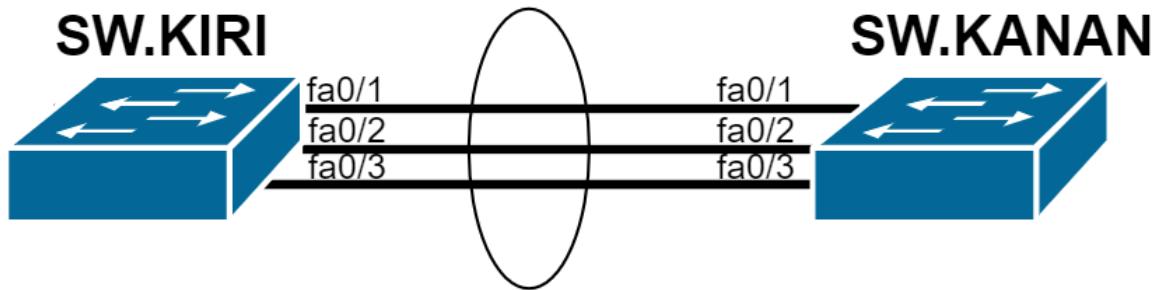
Cisco Proprietary, hanya bekerja pada sesama switch Cisco, terdapat 2 mode:

- **Desirable**: Protokol PAGP yang mengajak untuk menjadi etherchannel
  - **Auto**: Protokol PAGP yang menunggu untuk diajak etherchannel
- **Layer 3 Etherchannel**

Protokol Etherchannel yang hanya dapat dilakukan di MLS, atau layer 3, hanya terdapat 1 mode:

- **ON**: Protokol Etherchannel layer 3 yang mengajak untuk menjadi etherchannel.

Berikut lab Etherchannel:



Gambar 2 . 9 Lab Etherchannel

Kita konfigurasikan Etherchannel layer 2 (LACP)

```
SW.KIRI(config)#int range fa0/1 - 3
SW.KIRI(config-if-range)#channel-group 1 mode active
SW.KIRI(config-if-range)#int port-channel 1
SW.KIRI(config-if)#switchport mode trunk
```

```
SW.KANAN(config)#int range fa0/1 - 3
SW.KANAN(config-if-range)#channel-group 1 mode active
SW.KANAN(config-if-range)#int port-channel 1
SW.KANAN(config-if)#switchport mode trunk
```

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 secara keseluruhan

- Ketik *show etherchannel summary* untuk melihat etherchannel yang berjalan
- Ketik *show interface port-channel 1* melihat isi port gabungan dari etherchannel

```

SW.KIRI#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 1 etherchannel aktif, protokolnya LACP dan menggunakan 3 port.

```

SW.KIRI#show interface port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0011.218e.9d81 (bia 0011.218e.9d81)
  MTU 1500 bytes, BW 300000 Kbit, DLY 1000 usec, reliability 255/255,
  txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set Full-
  duplex, 100Mb/s
  input flow-control is off, output flow-control is off
Members in this channel: Fa0/1 Fa0/2 Fa0/3

```

Perlu diketahui *Port Channel*, merupakan interface buatan yang terbentuk secara otomatis ketika kita membuat etherchannel. Port channel ini berisi beberapa interface yang dibundel.

Sementara itu, berikut konfigurasi etherchannel L2 PAGP

```

SW.KIRI(config)#int range fa0/1 - 3
SW.KIRI(config-if-range)#channel-group 1 mode desirable
SW.KIRI(config-if-range)#int port-channel 1
SW.KIRI(config-if)#switchport mode trunk

```

```

SW.KANAN(config)#int range fa0/1 - 3
SW.KANAN(config-if-range)#channel-group 1 mode desirable
SW.KANAN(config-if-range)#int port-channel 1
SW.KANAN(config-if)#switchport mode trunk

```

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 3

```

SW.KIRI(config)#int range fa0/1 - 3
SW.KIRI(config-if-range)#channel-group 1 mode on
SW.KIRI(config-if-range)#no switchport
SW.KIRI(config)#int port-channel 1

```

```
SW.KIRI(config-if)#ip addr 10.10.10.1 255.255.255.0
```

```
SW.KANAN(config)#int range fa0/1 - 3
SW.KANAN(config-if-range)#channel-group 1 mode on
SW.KANAN(config-if-range)#no switchport
SW.KANAN(config-if-range)#int port-channel 1
SW.KANAN(config-if)#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.

## Catatan:

---

**“ALLAH AKAN MENGANGKAT DERAJAT ORANG-ORANG YANG BERIMAN DAN ORANG-ORANG YANG BERILMU DI ANTARA KAMU SEKALIAN.”**

---

**-Q. S Al-Mujadilah: 11-**



# **IPV6**

## **CONTENT:**

**IPV6 INTRODUCTION**

**IPV6 ADDRESS NOTATION**

**IPV6 CONVERSION**

**IPV6 COMPRESSION**

**IPV6 ADDRESS TYPE**

**IPV6 ADDRESS CONFIGURATION**

# 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

Tabel 3 . 12 Tabel contoh IPv6

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 CONVERSION

## Konversi Desimal ke Binary

Pada IPv6, satu fieldsnya terdiri dari 16 bit bilangan hexadecimal.

Misalkan hexadesimal 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 3 . 13 Konversi Binary

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

Tabel 3 . 14 Konveri Binary

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

Tabel 3 . 15 Konversi Binary

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, capek??

## 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

Tabel 3 . 16 Konversi Binary

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.

Setelah mengetahui caranya, kerjakanlah beberapa latihan berikut!

1. Konversikan IPv6 berikut menjadi binary:
  - 2100:1FDD:0000:24EF:F9A1:0000:71FA:4123
  - 0001:23FA:7ADF:4301:00FF:11DA:560A:0000
2. Konversikan Binary IPv6 menjadi Hexadesimal:
  - 1010 0110 1101 1111:0011 1101 0011 1001:0101 1110 0111 0000
  - 0101 1111 1001 0110:1100 0111 0001 0100 1100 1000 0000 1011
  -

## 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:E7:0000:0000:0000: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:F2C1:00E7:0:0:0:0D71:34FE**

### 3. Mengganti angka 0000 yang berturut-turut menjadi “::” (double colon).

Misalkan ada IPv6: **2001:0000:0000:2F4D:5AC2:DE12:0000:0000**

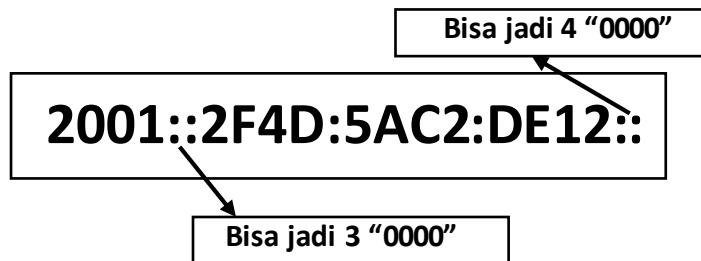
Kita dapat *compress* menjadi: **2001::2F4D:5AC2:DE12:0000:0000**

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.



Gambar 3 . 1 Illustrasi Compression IPv6

Namun jika hanya ada satu *double colon* router pasti dengan mudah dapat mengenalinya.



Gambar 3 . 2 Illustrasi Compression IPv6

Setelah belajar *Compress* IPv6 mari kita coba mengerjakan latihannya!

Kompres beberapa IPv6 address berikut:

**2001:0db8:0ab0:0d00:0000:0000:0000:0c01**

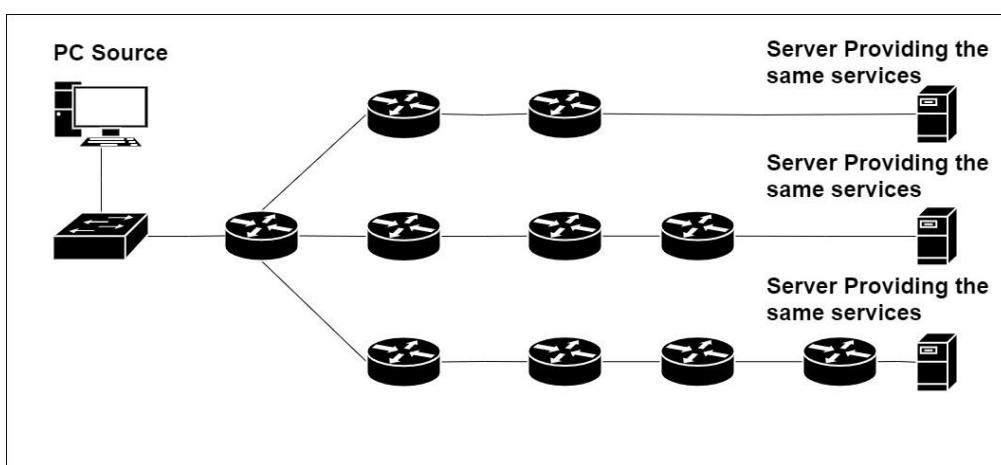
**2001:0db8:0000:4c05:0000:0000:05ad:0bb1**

**2001:0db8:0000:0000:1234:0000:0000:da61**

# 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.



*Gambar 3 . 3 Illustrasi Anycast IPv6*

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 atas, ini dikarenakan PC akan diarahkan ke serverterdekat.

## 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:

Tipe	Fungsi
<b>Link-local Address</b>	+ hanya digunakan antar tetangga pada tautan yang sama (konfigurasi alamat otomatis, penemuan tetangga, penemuan router, dan oleh banyak protokol routing). Ini hanya valid pada subnet saat ini. + selalu dikonfigurasi secara otomatis. + router tidak meneruskan paket dengan alamat tautan-lokal + dialokasikan dengan awalan FE80 :: / 64 + sama seperti 169.254.x.x dalam IPv4 (alamat APIPA), ditugaskan ketika server DHCP tidak tersedia dan tidak ada alamat statis yang ditugaskan + biasanya dibuat secara dinamis menggunakan awalan tautan-lokal FE80 :: / 10 dan pengenal antarmuka 64-bit (berdasarkan alamat MAC 48-bit)
<b>Unique-local Address</b>	+ digunakan antara node yang berkomunikasi dengan node lain di situs yang sama + memungkinkan perangkat di organisasi yang sama, atau situs, untuk bertukar data + dimulai dengan FC00 :: / 7 (untuk digunakan dalam jaringan pribadi). Mereka analog dengan kelas alamat pribadi IPv4. + Mungkin Anda akan terkejut tetapi alamat Situs-lokal tidak lagi didukung

	(usang) oleh RFC 3879 jadi mungkin Anda tidak akan melihatnya di masa depan
<b>Global Unicast Address</b>	<ul style="list-style-type: none"> <li>+ paket unicast yang dikirim melalui Internet publik (setara dengan alamat IPv4 publik)</li> <li>+ unik secara global di seluruh Internet</li> <li>+ dimulai dengan awalan 2000 :: / 3 (ini berarti alamat apa saja yang dimulai dengan 2 atau 3). Tetapi di masa depan alamat unicast global mungkin tidak memiliki batasan ini.</li> </ul>

## IPV6 EUI-64

EUI-64 merupakan sebuah cara pengalamatan pada sebuah jaringan dengan menggunakan MAC Address sebagai IPv6. Namun MAC address hanya memiliki 48 bit, sementara yang kita butuhkan yaitu 64 bit sebagai Interface ID.

Caranya adalah sebagai berikut:

### 1. Kita pecah MAC address menjadi dua:

MAC address ini terdiri dari dua bagian, **24 bit IOU** dan **24 bit NIC**. Misalkan ada MAC address **80:C1:6E:59:2E:43**, kita pecah menjadi 2 bagian.

80	C1	6E	59	2E	43
<b>OUI (Organizationally Unique Identifier)</b>			<b>NIC (Network Interface Card)</b>		

Tabel 3 . 17 Illustrasi EUI-64

### 2. Kita tambahkan hexadecimal “FFEE” pada tengah-tengah MAC address:

80	C1	6E	FF	EE	59	2E	43
OUI			NIC				

Tabel 3 . 18 Illustrasi EUI-64

### 3. Kita rubah bit ketujuh (7) pada 8 bit pertama ke angka “1”:

80	C1	6E	FF	EE	59	2E	43
OUI			NIC				

Tabel 3 . 19 Illustrasi EUI-64

Kita rubah 8 bit pertama, yaitu pada angka 8 dan 0. Caranya dengan menggunakan tabel konversi decimal ke biner IPv6.

4 binary pertama:

1	0	0	0
8	4	2	1

Tabel 3 . 20 Konversi Desimal ke Binary

4 binary berikutnya:

0	0	1	0
8	4	2	1

Tabel 3 . 21 Konversi Desimal ke Binary

Jika pada bit ketujuh tidak kita rubah menjadi “1” maka menandakan bahwa alamat tersebut merupakan universal. Sedangkan dalam EUI-64, kita harus merubahnya agar menandakan bahwa alamat tersebut telah di administrasi secara lokal.

Maka menjadi:

82	C1	6E	FF	EE	59	2E	43
OUI						NIC	

Tabel 3 . 22 Illustrasi EUI-64

Maka hasil dari Interface ID dengan menggunakan EUI-64 ialah:

**82C1:6EFF:EE59:2E43**

# IPV6 ADDRESS CONFIGURATION

Melanjutkan bahasan EUI-64 tadi, mari kita konfigurasikan interface dengan menggunakan metode EUI dan cara biasa.

## Dengan menggunakan metode EUI-64:

```
R1(config)#int fa0/0
R1(config-if)#ipv6 add 2001:ABCD:1111::/64 eui-64
```

## Dengan menggunakan cara biasa:

```
R1(config)#int fa0/1
R1(config-if)#ipv6 add 2001:ABCD:2222::1/64
```

Fitur routing pada IPv6 secara default tidak aktif, maka jika ingin mengaktifkan fitur routing IPv6, kita harus mengaktifkan perintah berikut:

```
R1(config)#ipv6 unicast-routing
```

Selanjutnya mari kita lakukan verifikasi dengan menggunakan perintah show

```
R1#show ipv6 interface brief
FastEthernet0/0          [up/up]
  FE80::2E0:F9FF:FEA3:A401
  2001:ABCD:1111:0:2E0:F9FF:FEA3:A401
FastEthernet0/1          [administratively down/down]
  FE80::2E0:F9FF:FEA3:A402
  2001:ABCD:2222::1
Vlan1                  [administratively down/down]      unassigned
```

Dari gambar show interface tersebut bisa kita simpulkan beberapa hal:

1. Fitur EUI-64 secara default sudah digunakan penerapannya pada interface link-local.
2. Perhitungan Interface ID yang dilakukan pada materi sebelumnya sudah tepat.
3. Dalam satu interface bisa kita konfigurasikan beberapa IP address.

# IPv6

packetlife.net

Protocol Header				Address Notation				
Ver	Traffic Class	Flow Label		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>				
Payload Length	Next Header	Hop Limit	Address Formats					
Source Address						Global unicast		
Destination Address						Global Prefix      Subnet      Interface ID 48                16                64		
<b>Version</b> (4 bits) · Always set to 6						Link-local unicast		
<b>Traffic Class</b> (8 bits) · A DSCP value for QoS						FE80::/64      Interface ID 64                64		
<b>Flow Label</b> (20 bits) · Identifies unique flows (optional)						Multicast		
<b>Payload Length</b> (16 bits) · Length of the payload in bytes						FF Flags Scope      Group ID 8 4 4                112		
<b>Next Header</b> (8 bits) · Header or protocol which follows						EUI-64 Formation		
<b>Hop Limit</b> (8 bits) · Similar to IPv4's time to live field						MAC      EUI-64 00 0a 27 5c 88 19      02 0a 27 ff fe 5c 88 19		
<b>Source Address</b> (128 bits) · Source IP address						· Insert 0xffffe between the two halves of the MAC		
<b>Destination Address</b> (128 bits) · Destination IP address						· Flip the seventh bit (universal/local flag) to 1		
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				Extension Headers				
1 Interface-local	5 Site-local	<b>Hop-by-hop Options (0)</b>		Carries additional information which must be examined by every router in the path				
2 Link-local	8 Org-local	<b>Routing (43)</b>		Provides source routing functionality				
4 Admin-local	E Global	<b>Fragment (44)</b>		Included when a packet has been fragmented by its source				
Special-Use Ranges								
<b>::/0</b>	Default route	<b>Encapsulating Security Payload (50)</b>		Provides payload encryption (IPsec)				
<b>::/128</b>	Unspecified	<b>Authentication Header (51)</b>		Provides packet authentication (IPsec)				
<b>::1/128</b>	Loopback	<b>Destination Options (60)</b>		Carries additional information which pertains only to the recipient				
<b>::/96</b>	IPv4-compatible*	<b>Transition Mechanisms</b>						
<b>::FFFF:0:0/96</b>	IPv4-mapped	<b>Dual Stack</b>		Transporting IPv4 and IPv6 across an infrastructure simultaneously				
<b>2001::/32</b>	Teredo	<b>Tunneling</b>		IPv6 traffic is encapsulated into IPv4 using IPv6-in-IP, UDP (Teredo), or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)				
<b>2001:DB8::/32</b>	Documentation	<b>Translation</b>		Stateless IP/ICMP Translation (SIIT) translates IP header fields, NAT Protocol Translation (NAT-PT) maps between IPv6 and IPv4 addresses				
<b>2002::/16</b>	6to4							
<b>FC00::/7</b>	Unique local							
<b>FE80::/10</b>	Link-local unicast							
<b>FEC0::/10</b>	Site-local unicast*							
<b>FF00::/8</b>	Multicast							
* Deprecated								

by Jeremy Stretch

v2.0

## Catatan:

---

**“TUNTUTLAH ILMU. DI SAAT KAMU MISKIN, IA AKAN  
MENJADI HARTAMU. DI SAAT KAMU KAYA, IA AKAN  
MENJADI PERHIASANMU.”**

---

**-Luqman al-Hakim-**

CHAPTER 4

# Routing Session

CCNA

ENTERPRISE

# **ROUTING SESSION**

## **CONTENT:**

**ROUTING INTRODUCTION**

**ROUTING FUNDAMENTAL**

**STATIC ROUTE**

**DYNAMIC ROUTE OSPF**

# 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 detil

# 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.

Contoh routing table:

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

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/2] via 23.23.23.3, 00:02:39, FastEthernet0/1
        4.0.0.0/32 is subnetted, 1 subnets
R        4.4.4.4 [120/2] via 23.23.23.3, 00:00:27, FastEthernet0/1
        12.0.0.0/24 is subnetted, 1 subnets
C        12.12.12.0 is directly connected, FastEthernet0/0
SMRG#
```

Pada routing table diatas, router telah menjangkau/mengenali network:

- 2.2.2.2/32 directly connected
- 3.3.3.3/32 OSPF
- 4.4.4.4/32 RIP
- 12.12.12.0/24 directly connected

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?

## 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).

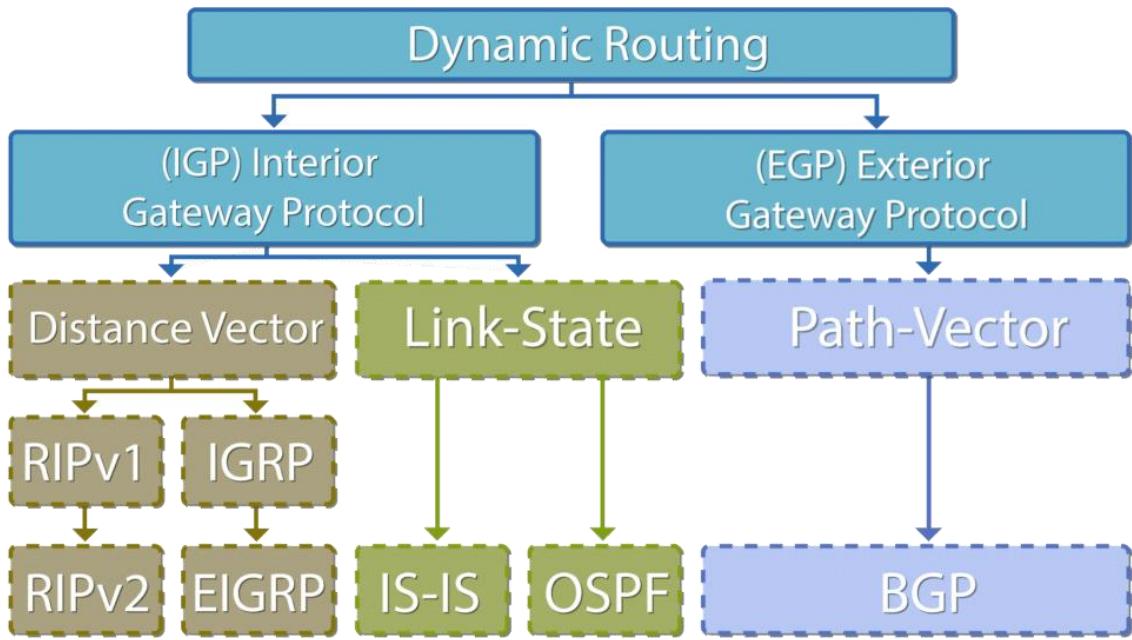
### 3. Round Robin

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 digunakan oleh Router untuk saling bertukar informasi Routing, pertukaran inrformasi 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.



Gambar 4 . 1 Protokol Dynamic Route

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 koneksi其实nya pada sebuah jaringan, dia akan memilih jalur routing dengan loncatan/*hop count* tersendik 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 koneksi其实nya 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)

Sedang 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 daftar dari *Administrative Distance*:

Route Source	Default Distance Value
<b>Connected interface</b>	0
<b>Static route</b>	1
<b>Enhanced Interior Gateway Routing Protocol (EIGRP) summary route</b>	5
<b>External Border Gateway Protocol (BGP)</b>	20
<b>Internal EIGRP</b>	90
<b>IGRP</b>	100
<b>Open Shortest Path First (OSPF)</b>	110
<b>Intermediate System-to-Intermediate System (IS-IS)</b>	115
<b>Routing Information Protocol (RIP)</b>	120
<b>Exterior Gateway Protocol (EGP)</b>	140
<b>On Demand Routing (ODR)</b>	160
<b>External EIGRP</b>	170
<b>Internal BGP</b>	200

Tabel 4 . 1 Daftar Administrative Distance

## Metric

Metrik 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 di jadikan 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 Eror atau kegagalan dalam link tersebut. Nilai reliability tertinggi akan menjadi Best Path.

Sebelum memasuki materi static routing, mari kita pahami cara memberikan IP Address pada sebuah interface.

## Setting IP ADDRESS Interface FAST ETHERNET

Check nama interface dulu dengan perintah #show ip int brief

Interface Protocol	IP-Address	OK?	Method	Status
FastEthernet0/0 down down	unassigned	YES	NVRAM	administratively
FastEthernet0/1 down down	unassigned	YES	NVRAM	administratively

Jika ingin memberikan ip address di interface FastEthernet0/0 maka dilakukan konfigurasi seperti berikut :

```
router(config) # int fa0/0
router(config-if) # description ### LINK KE INTERNAL ####
router(config-if) # ip addr 10.10.10.1 255.255.255.0
router(config-if) # no shutdown
```

untuk verifikasi apakah ip nya sudah dikonfigurasi atau belum :

```
router#sh ip int brief
```

Interface	IP-Address	OK?	Method	Status
Protocol				

```

FastEthernet0/0           10.10.10.1      YES NVRAM  administratively down
down
FastEthernet0/1           unassigned       YES NVRAM  administratively
down down

```

```

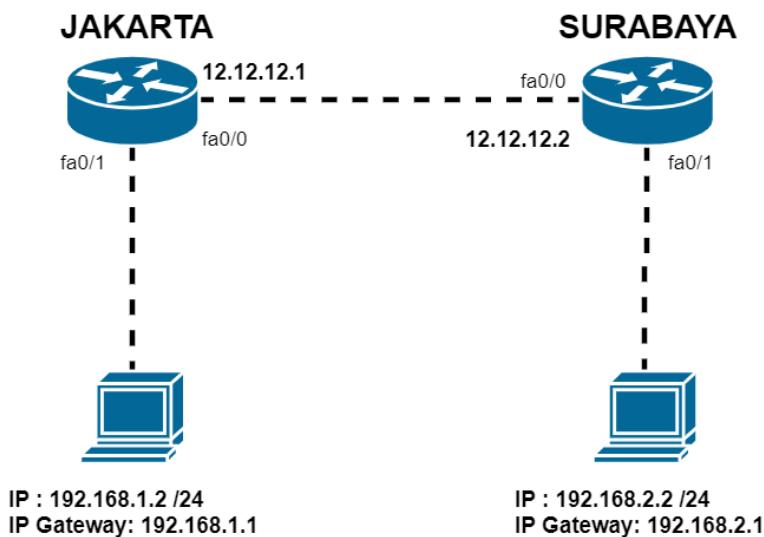
router#sh run
-----
! interface
FastEthernet0/0
 ip address 10.10.10.1 255.255.255.0
description ### LINK KE INTERNAL ###
-----
```

## STATIC ROUTING

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.

### Lab-1



Gambar 4 . 2 Lab Static Route 1

Berikut lab pertama pada static routing:

Kita akan menghubungkan Router JAKARTA dan Router SURABAYA agar klien/PC dapat berkomunikasi.

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

### **Router JAKARTA:**

```
Router>en
Router#conf t
Router(config) #hostname JAKARTA
JAKARTA(config)#int f0/0
JAKARTA(config-if)#ip addr 12.12.12.1 255.255.255.252
JAKARTA(config-if)#no shutdown
JAKARTA(config-if)#int f0/1
JAKARTA(config-if)#ip addr 192.168.1.1 255.255.255.0
JAKARTA(config-if)#no shutdown
```

### **Router SURABAYA**

```
Router>en
Router#conf t
Router(config) #hostname SURABAYA
SURABAYA(config)#int f0/0
SURABAYA(config-if)#ip addr 12.12.12.2 255.255.255.252
SURABAYA(config-if)#no shutdown
SURABAYA(config-if)#int f0/1
SURABAYA(config-if)#ip addr 192.168.2.1 255.255.255.0
SURABAYA(config-if)#no shutdown
```

Jika keduanya sudah, selanjutnya kita konfigurasikan Static Route-nya.

Berikut confignya:

```
Router(config) # ip route A.B.C.D (destination network/host) A.B.C.D
(subnet mask) A.B.C.D (Next Hop/IP Tetangga )
```

Cara lain untuk menentukan next hop selain menggunakan IP address ialah dengan menggunakan nama Port.

Misalkan : ethernet0, E0, S0/0, Fa 0/1 dan lain lain.

```
Router(config) # ip route A.B.C.D (destination network/host) A.B.C.D
(subnet mask) S 0/0 (Next Hop/IP Tetangga)
```

Pada Router JAKARTA, kita konfigurasikan routing ke network 192.168.2.0 yaitu network PC pada Router SURABAYA.

Sementara pada Router SURABAYA, kita konfigurasikan routing ke network 192.168.1.0 yaitu network PC pada router JAKARTA.

### **Router JAKARTA:**

```
JAKARTA(config)#ip route 192.168.2.0 255.255.255.0 12.12.12.2
```

### **Router SURABAYA:**

```
SURABAYA(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
```

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

### Show ip route JAKARTA

```
JAKARTA#show ip route
12.0.0.0/30 is subnetted, 1 subnets
C      12.12.12.0 is directly connected, FastEthernet0/0
C      192.168.1.0/24 is directly connected, FastEthernet0/1
S      192.168.2.0/24 [1/0] via 12.12.12.2
```

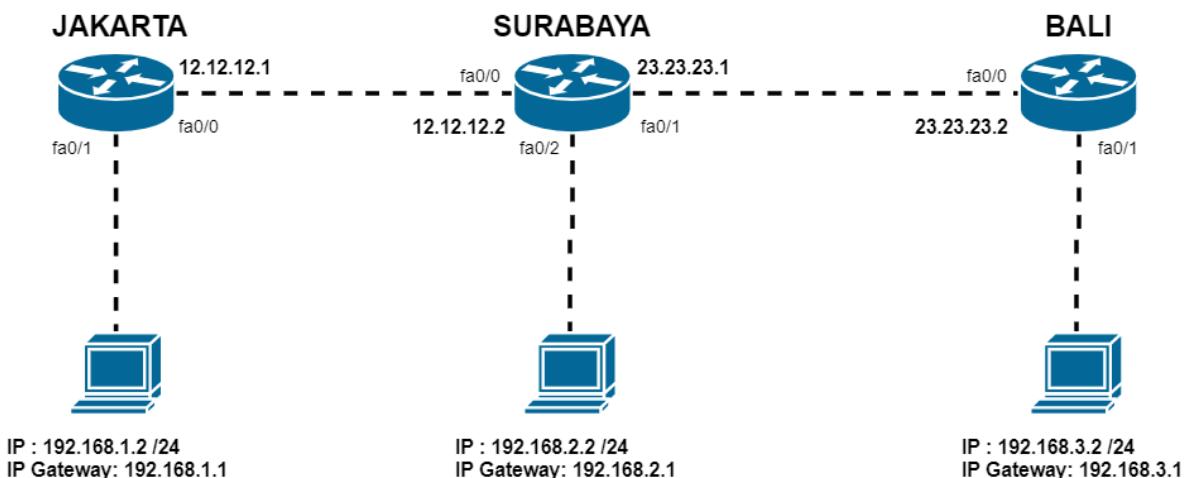
### Show ip route SURABAYA

```
SURABAYA#show ip route
12.0.0.0/30 is subnetted, 1 subnets
C      12.12.12.0 is directly connected, FastEthernet0/0
S      192.168.1.0/24 [1/0] via 12.12.12.1
C      192.168.2.0/24 is directly connected, FastEthernet0/1
```

Untuk Routing static, ditandai dengan **S** dan Administravite Distancenya **1**

Untuk pengetesan, coba lakukan PC JAKARTA dan PC SURABAYA, pastikan reply.

## Lab-2



Gambar 4 . 3 Lab Static Route 2

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.

#### **Router JAKARTA:**

```
Router>en
Router#conf t
Router(config) #hostname JAKARTA
JAKARTA(config)#int f0/0
JAKARTA(config-if)#ip addr 12.12.12.1 255.255.255.252
JAKARTA(config-if)#no shutdown
JAKARTA(config-if)#int f0/1
JAKARTA(config-if)#ip addr 192.168.1.1 255.255.255.0
JAKARTA(config-if)#no shutdown
```

#### **Router SURABAYA**

```
Router>en
Router#conf t
Router(config) #hostname SURABAYA
SURABAYA(config)#int f0/0
SURABAYA(config-if)#ip addr 12.12.12.2 255.255.255.252
SURABAYA(config-if)#no shutdown
SURABAYA(config)#int f0/1
SURABAYA(config-if)#ip addr 23.23.23.1 255.255.255.252
SURABAYA(config-if)#no shutdown
SURABAYA(config-if)#int f0/2
SURABAYA(config-if)#ip addr 192.168.2.1 255.255.255.0
SURABAYA(config-if)#no shutdown
```

#### **Router BALI**

```
Router>en
Router#conf t
Router(config) #hostname BALI
BALI(config) #
BALI(config)#int f0/0
BALI(config-if)#ip addr 23.23.23.2 255.255.255.252
BALI(config-if)#no shutdown
BALI(config-if)#int f0/1
BALI(config-if)#ip addr 192.168.3.1 255.255.255.0
BALI(config-if)#no shutdown
```

Selanjutnya kita konfigurasikan static routing pada tiap router

#### **Router JAKARTA:**

```
JAKARTA(config)#ip route 23.23.23.0 255.255.255.252 12.12.12.2
JAKARTA(config)#ip route 192.168.2.0 255.255.255.0 12.12.12.2
JAKARTA(config)#ip route 192.168.3.0 255.255.255.0 12.12.12.2
```

#### **Router SURABAYA:**

```
SURABAYA(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
SURABAYA(config)#ip route 192.168.3.0 255.255.255.0 12.12.12.1
```

## Router BALI

```
BALI(config)#ip route 12.12.12.0 255.255.255.252 23.23.23.1
BALI(config)#ip route 192.168.2.0 255.255.255.0 23.23.23.1
BALI(config)#ip route 192.168.1.0 255.255.255.0 23.23.23.1
```

Kemudian kita liat hasilnya, ketikkan **show ip route**

## Show ip route JAKARTA

```
JAKARTA#sh ip route
 12.0.0.0/30 is subnetted, 1 subnets
 C      12.12.12.0 is directly connected, FastEthernet0/0
 23.0.0.0/30 is subnetted, 1 subnets
 S        23.23.23.0 [1/0] via 12.12.12.2
 C      192.168.1.0/24 is directly connected, FastEthernet0/1
 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
```

## Show ip route SURABAYA

```
SURABAYA#show ip route
 12.0.0.0/30 is subnetted, 1 subnets
 C      12.12.12.0 is directly connected, FastEthernet0/0
 23.0.0.0/30 is subnetted, 1 subnets
 C        23.23.23.0 is directly connected, FastEthernet0/1
 S        192.168.1.0/24 [1/0] via 12.12.12.1
 C      192.168.2.0/24 is directly connected, FastEthernet0/2
 S        192.168.3.0/24 [1/0] via 23.23.23.2
```

## Show ip route BALI

```
BALI#show ip route
 12.0.0.0/30 is subnetted, 1 subnets
 S        12.12.12.0 [1/0] via 23.23.23.1
 23.0.0.0/30 is subnetted, 1 subnets
 C        23.23.23.0 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
 C        192.168.3.0/24 is directly connected, FastEthernet0/1
```

Kemudian untuk pengetesan, coba ping antar PC pada masing-masing router, pastikan reply

## Floating Static Route

Ada kalanya kita harus mengganti administrative distance sebuah static routing, salah satu kegunaannya ialah untuk menjadi backup dari dynamic routing. Untuk konfigurasinya cukup mudah, kita akan menggunakan Router JAKARTA dan mengubah AD menjadi 120.

```
JAKARTA(config)#ip route 23.23.23.0 255.255.255.0 12.12.12.0 120
JAKARTA(config)#do show ip route | b Gateway
Gateway of last resort is not set

      12.0.0.0/24 is subnetted, 1 subnets
C          12.12.12.0 is directly connected, FastEthernet0/0
      23.0.0.0/24 is subnetted, 1 subnets
S          23.23.23.0 [120/0] via 12.12.12.0

JAKARTA(config)#

```

## Default Static Route

Default route biasa kita gunakan untuk mengkoneksikan router di rumah kita (edge router) ke internet. Kita bisa menggunakan IP penyedia internet (ISP) sebagai IP next-hop. Contoh konfigurasinya seperti berikut:

```
JAKARTA(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.2
JAKARTA(config)#do show ip route | b Gateway
Gateway of last resort is 12.12.12.2 to network 0.0.0.0
      12.0.0.0/24 is subnetted, 1 subnets
C          12.12.12.0 is directly connected, FastEthernet0/0
      23.0.0.0/24 is subnetted, 1 subnets
S          23.23.23.0 [5/0] via 12.12.12.0
S*        0.0.0.0/0 [1/0] via 12.12.12.2

JAKARTA(config)#

```

Konfigurasinya sekilas sama persis seperti konfigurasi static route biasa, namun network destinationnya ialah **0.0.0.0/0** yang mana jika kita coba subnetting hasilnya ialah semua IPv4 address yang tersedia!

Namun walau begitu, default route memiliki prefix yang sangat tidak spesifik **/0**.

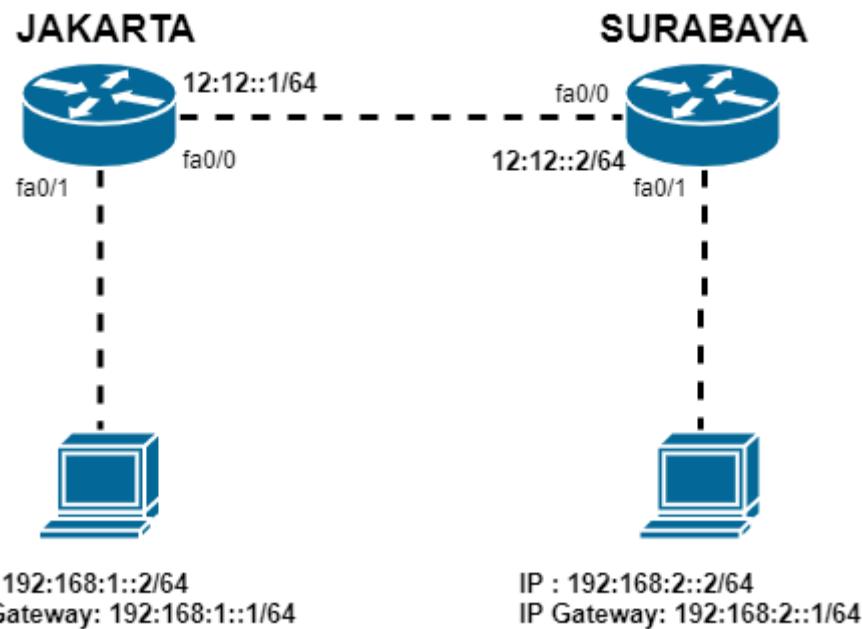
Maka dari itu router akan menggunakan default route sebagai opsi terakhir saja.

## Static Route IPv6

Setelah di bab sebelumnya kita membahas tentang IPv6, maka kali ini kita akan membahas static route dari IPv6 ini.

### Lab-1

Labnya kita ambil dari lab IPv4 barusan:



Gambar 4 . 4 Lab Static Route v6 1

Pertama kita masukkan IPv6 ke tiap interface terlebih dahulu.

#### Router JAKARTA

```
JAKARTA>en
JAKARTA#conf t
JAKARTA(config)#ipv6 unicast-routing
JAKARTA(config)#int f0/0
JAKARTA(config-if)#ipv6 addr 12:12::1/64
JAKARTA(config-if)#int f0/1
JAKARTA(config-if)#ipv6 addr 192:168:1::1/64
```

#### Router SURABAYA

```
SURABAYA>en
SURABAYA#conf t
SURABAYA(config)#
SURABAYA(config)#ipv6 unicast-routing
```

```
SURABAYA(config)#int f0/0
SURABAYA(config-if)#ipv6 addr 12:12::2/64
SURABAYA(config-if)#int f0/1
SURABAYA(config-if)#ipv6 addr 192:168:2::1/64
```

Secara default, IPv6 tidak bisa langsung digunakan untuk routing, maka dari itu kita harus menggunakan command *ipv6 unicast-routing* agar IPv6 dapat melakukan route.

Selanjutnya kita lakukan route antar router

### Router JAKARTA

```
JAKARTA(config)#ipv6 route 192:168:2::/64 12:12::2
```

### Router SURABAYA

```
SURABAYA(config)#ipv6 route 192:168:1::/64 12:12::1
```

Jika ingin melihat hasilnya, kita pastikan dengan command *show ipv6 route*.

### Show ipv6 route JAKARTA

```
JAKARTA#show ipv6 route

C      12:12::/64 [0/0]
          via ::, FastEthernet0/0
L      12:12::1/128 [0/0]
          via ::, FastEthernet0/0
C      192:0:168::/64 [0/0]
          via ::, FastEthernet0/0
L      192:0:168::1/128 [0/0]
          via ::, FastEthernet0/0
C      192:168::/64 [0/0]
          via ::, FastEthernet0/0
L      192:168::1/128 [0/0]
          via ::, FastEthernet0/0
C      192:168:1::/64 [0/0]
          via ::, FastEthernet0/1
L      192:168:1::1/128 [0/0]
          via ::, FastEthernet0/1
S      192:168:2::/64 [1/0]
          via 12:12::2
L      FF00::/8 [0/0]
          via ::, Null0
```

### Show ipv6 route SURABAYA

```
SURABAYA#show ipv6 route
C      12:12::/64 [0/0]
          via ::, FastEthernet0/0
L      12:12::2/128 [0/0]
```

```

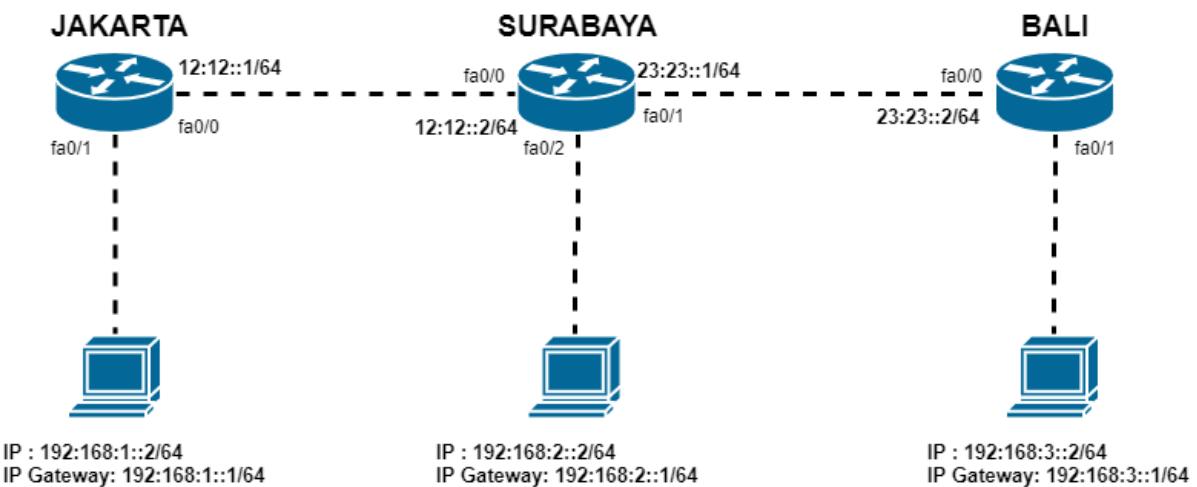
        via ::, FastEthernet0/0
S  192:168:1::/64 [1/0]
        via 12:12::1
C  192:168:2::/64 [0/0]
        via ::, FastEthernet0/1
L  192:168:2::1/128 [0/0]
        via ::, FastEthernet0/1
L  FF00::/8 [0/0]
        via ::, Null0

```

Static route ditandai dengan flag ‘S’. Dengan ini, maka antar kedua PC di tiap router dapat berkomunikasi lewat IPv6, coba lakukan test ping, pastikan mendapat reply.

## Lab-2

Pada lab kedua ini, kita hanya akan menambahkan satu PC dan satu router.



Gambar 4 . 5 Lab Static Route V6 2

Seperti biasa kita konfigurasikan terlebih dahulu IP pada interfacenya.

### Router JAKARTA

```

JAKARTA>en
JAKARTA#conf t
JAKARTA(config)#ipv6 unicast-routing
JAKARTA(config)#int f0/0
JAKARTA(config-if)#ipv6 addr 12:12::1/64
JAKARTA(config-if)#int f0/1
JAKARTA(config-if)#ipv6 addr 192:168:1::1/64

```

## Router SURABAYA

```
SURABAYA>en
SURABAYA#conf t
SURABAYA(config)#
SURABAYA(config)#ipv6 unicast-routing
SURABAYA(config)#int f0/0
SURABAYA(config-if)#ipv6 addr 12:12::2/64
SURABAYA(config-if)#int f0/1
SURABAYA(config-if)#ipv6 addr 23:23::1/64
SURABAYA(config-if)#int f0/2
SURABAYA(config-if)#ipv6 addr 192:168:2::1/64
```

## Router BALI

```
BALI>en
BALI#conf
BALI(config)#
BALI(config)#ipv6 unicast-routing
BALI(config)#int f0/0
BALI(config-if)#ipv6 addr 23:23::2/64
BALI(config-if)#int f0/1
BALI(config-if)#ipv6 addr 192:168:3::1/64
```

Selanjutnya kita konfigurasikan static routenya

## Router JAKARTA

```
JAKARTA(config)#ipv6 route 23:23::/64 12:12::2
JAKARTA(config)#ipv6 route 192:168:2::/64 12:12::2
JAKARTA(config)#ipv6 route 192:168:3::/64 12:12::2
```

## Router SURABAYA

```
SURABAYA(config)#ipv6 route 192:168:1::/64 12:12::1
SURABAYA(config)#ipv6 route 192:168:3::/64 23:23::2
```

## Router BALI

```
BALI(config)#ipv6 route 12:12::/64 23:23::1
BALI(config)#ipv6 route 192:168:2::/64 23:23::1
BALI(config)#ipv6 route 192:168:1::/64 23:23::1
```

Jika ingin melihat hasilnya, kita pastikan dengan command *show ipv6 route*.

## Show ipv6 route JAKARTA

```
JAKARTA#show ipv6 route
C 12:12::/64 [0/0]
```

```
        via ::, FastEthernet0/0
L 12:12::1/128 [0/0]
    via ::, FastEthernet0/0
S 23:23::/64 [1/0]
    via 12:12::2
C 192:0:168::/64 [0/0]
    via ::, FastEthernet0/0
L 192:0:168::1/128 [0/0]
    via ::, FastEthernet0/0
C 192:168::/64 [0/0]
    via ::, FastEthernet0/0
L 192:168::1/128 [0/0]
    via ::, FastEthernet0/0
C 192:168:1::/64 [0/0]
    via ::, FastEthernet0/1
L 192:168:1::1/128 [0/0]
    via ::, FastEthernet0/1
S 192:168:2::/64 [1/0]
    via 12:12::2
S 192:168:3::/64 [1/0]
    via 12:12::2
L FF00::/8 [0/0]
    via ::, Null0
```

### Show ipv6 route SURABAYA

```
SURABAYA#show ipv6 route
C 12:12::/64 [0/0]
    via ::, FastEthernet0/0
L 12:12::2/128 [0/0]
    via ::, FastEthernet0/0
C 23:23::/64 [0/0]
    via ::, FastEthernet0/1
L 23:23::1/128 [0/0]
    via ::, FastEthernet0/1
S 192:168:1::/64 [1/0]
    via 12:12::1
C 192:168:2::/64 [0/0]
    via ::, FastEthernet0/2
L 192:168:2::1/128 [0/0]
    via ::, FastEthernet0/2
S 192:168:3::/64 [1/0]
    via 23:23::2
L FF00::/8 [0/0]
    via ::, Null0
```

### Show ipv6 route BALI

```
BALI#show ipv6 route
S 12:12::/64 [1/0]
    via 23:23::1
C 23:23::/64 [0/0]
    via ::, FastEthernet0/0
L 23:23::2/128 [0/0]
```

```
      via ::, FastEthernet0/0
S  192.168.1.1/64 [1/0]
      via 23.23.1
S  192.168.2.1/64 [1/0]
      via 23.23.1
C  192.168.3.1/64 [0/0]
      via ::, FastEthernet0/1
L  192.168.3.1/128 [0/0]
      via ::, FastEthernet0/1
L  FF00::/8 [0/0]
      via ::, Null0
```

Dengan begini semua PC sudah saling terhubung dan dapat berkomunikasi, untuk pengetesan, coba ping antar PC pastikan reply.

## DYNAMIC ROUTE OSPF

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 untuk membuat OSPF di desain secara hierarchical:

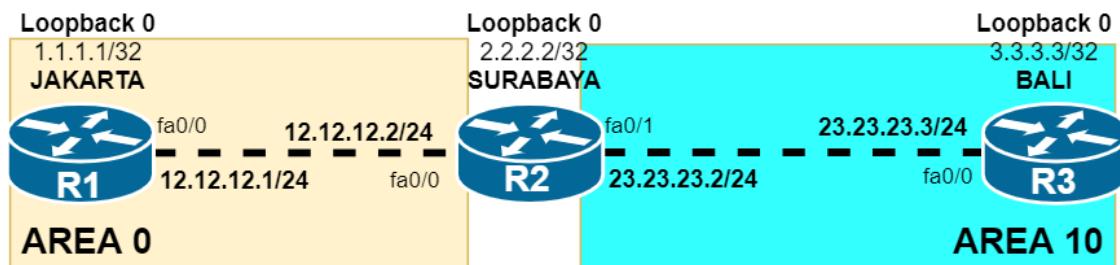
- Menurunkan routing overhead

- Mempercepat convergence
- membatasi network yang tidak stabil agar tidak menyebar ke area yang laen.

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.

## Lab OSPF



Gambar 4 . 6 Lab OSPF

Pertama konfigurasikan IP Address sesuai dengan topologi diatas. Lalu konfigurasikan OSPF di masing-masing Router seperti berikut:

### Setting Router Jakarta

```
JAKARTA(config)#router ospf 10
JAKARTA(config-router)#network 12.12.12.0 0.0.0.255 area 0
JAKARTA(config-router)#network 1.1.1.1 0.0.0.0 area 0
```

### Setting Router Semarang

```
SEMARANG(config)#router ospf 10
SEMARANG(config-router)#network 12.12.12.0 0.0.0.255 area 0
SEMARANG(config-router)#network 23.23.23.0 0.0.0.255 area 10
SEMARANG(config-router)#network 2.2.2.2 0.0.0.0 area 10
```

### Setting Router Surabaya

```
SURABAYA(config)#router ospf 10
SURABAYA(config-router)#network 23.23.23.0 0.0.0.255 area 10
SURABAYA(config-router)#network 3.3.3.3 0.0.0.0 area 10
```

Pada OSPF, **digunakan wildcard mask**, wildcard mask merupakan kebalikan dari subnet mask, cara mendapat wildcard mask adalah: **subnet mask-255.255.255.255**

## Verifikasi

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

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
O    1.1.1.1 [110/2] via 12.12.12.1, 00:02:41, FastEthernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
C    2.2.2.2 is directly connected, Loopback0
      3.0.0.0/32 is subnetted, 1 subnets
O    3.3.3.3 [110/2] via 23.23.23.3, 00:02:11, FastEthernet0/1
      12.0.0.0/24 is subnetted, 1 subnets
C    12.12.12.0 is directly connected, FastEthernet0/0
23.0.0.0/24 is subnetted, 1 subnets
C    23.23.23.0 is directly connected, FastEthernet0/1
```

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

```
SEMARANG#sh ip ospf neighbor
Neighbor ID      Pri   State            Dead Time     Address
Interface
1.1.1.1          1     FULL/BDR        00:00:37      12.12.12.1
FastEthernet0/0
3.3.3.3          1     FULL/BDR        00:00:32      23.23.23.3
FastEthernet0/1
```

```
Jakarta#sh ip ospf database
OSPF Router with ID (1.1.1.1) (Process ID 10)
Router Link States (Area 0)

Link ID          ADV Router      Age       Seq#      Checksum Link count
1.1.1.1          1.1.1.1        1288      0x80000006 0x00feff 3
2.2.2.2          2.2.2.2        1286      0x80000007 0x00feff 2
                                         Summary Net Link States (Area 0)
Link ID          ADV Router      Age       Seq#      Checksum
2.2.2.2          2.2.2.2        1272      0x80000005 0x00fa02
3.3.3.3          2.2.2.2        1203      0x80000006 0x00fa02
```

```

Jakarta#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32
ms Jakarta#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 62/62/63
ms

```

Hasil ping sukses, maka bisa dipastikan bahwa konfigurasi yang dilakukan sudah berhasil!

## Cara Kerja OSPF

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

### OSPF Packet Type

Dalam pembentukan jaringan, OSPF menggunakan beberapa packet multicast khusus:

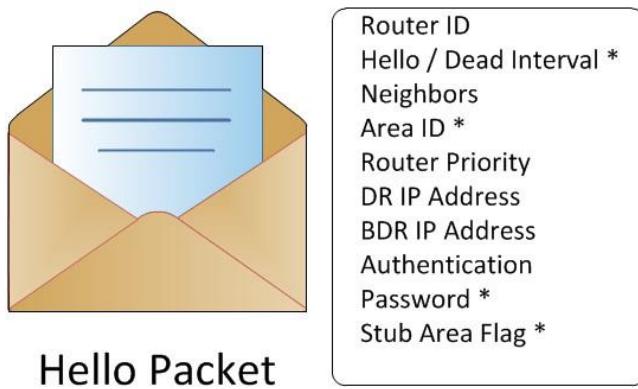
- **Hello:** sebagai *neighbor discovery* saat protokol berjalan dan sebagai penjaga stabilitas agar jaringan OSPF berjalan dengan baik.
- **DBD:** digunakan untuk mengecek LSDB jika ada dua router yang sama. **DBD merupakan ringkasan dari LSDB**
- **LSR:** untuk meminta Link-State records yang spesifik
- **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 diambil jalur-jalur terbaik sehingga menghasilkan suatu database yang dinamakan LSDB

Pada OSPF terdapat 7 keadaan sebelum akhirnya bisa menjadi *neighbor*

- **Down:** Tidak terdapat OSPF *neighbor* saat itu.
- **Init:** Hello Packet diterima.

- **Two-way:** Terdapat router-id pada hello packet
- **Exstart:** Pembentukan role pada OSPF (DR, BDR)
- **Exchange:** Database Description Packet (DBD) telah dikirim secara multicast kesemua router OSPF
- **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.



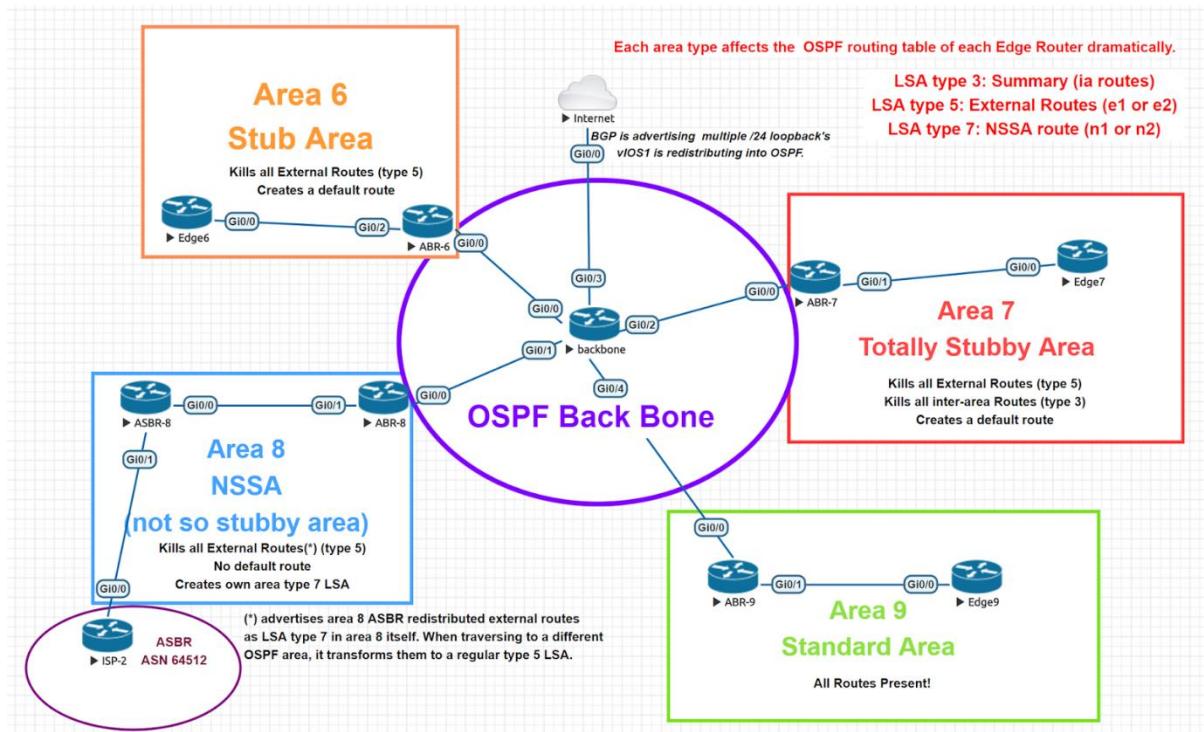
Nantinya setiap hello packet akan membawa informasi seperti pada ilustrasi disamping. Banyak informasi yang dibawa oleh hello packet ini, tapi yang bisa kita highlight untuk saat ini ialah Router ID, Hello/Dead Interval, Area ID.

**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 tertinggih 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

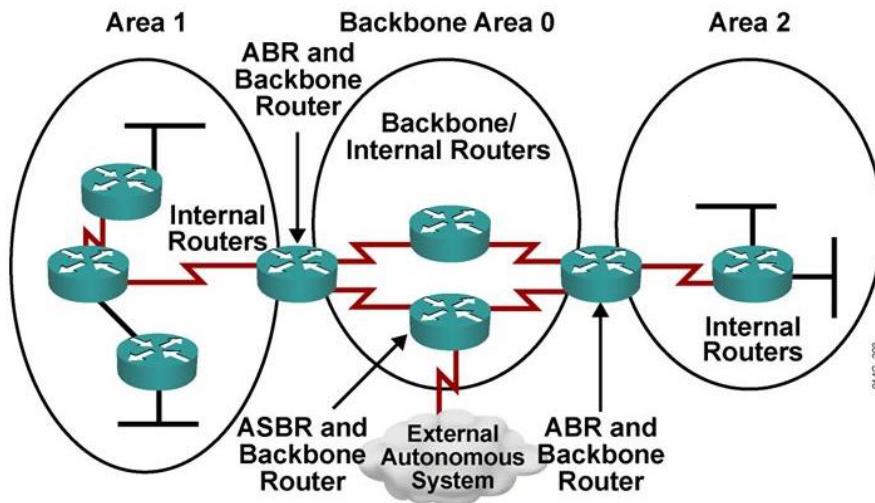


Gambar 4 . 8 Illustrasi area OSPF

Pada OSPF, koneksi 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 dari 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



Gambar 4 . 9 Illustrasi router OSPF

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 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.

Seperti pada topologi yang sudah kita lihat tadi

```
SEMARANG#sh ip ospf neighbor
Neighbor ID      Pri   State            Dead Time     Address
Interface
1.1.1.1          1     FULL/BDR        00:00:37      12.12.12.1
FastEthernet0/0
3.3.3.3          1     FULL/BDR        00:00:32      23.23.23.3
FastEthernet0/1
```

Pada router SEMARANG, kita bisa lihat bahwa state nya adalah menjadi BDR yang artinya menjadi backup dari DR bila terjadi suatu masalah.

# OSPF • PART 1

packetlife.net

Protocol Header				Attributes			
8	16	24	32	Type Link-State			
Version	Type	Length		Algorithm Dijkstra			
	Router ID			Metric Cost (Bandwidth)			
	Area ID			AD 110			
Checksum	Instance ID	Reserved		Standard RFC 2328, 2740			
	Data			Protocols IP			
				Transport IP/89			
				Authentication Plaintext, MD5			
				AllSPF Address 224.0.0.5			
				AllDR Address 224.0.0.6			
Link State Advertisements				Metric Formula			
<b>Router Link (Type 1)</b> Lists neighboring routers and the cost to each; flooded within an area				$\text{cost} = \frac{100,000 \text{ Kbps}^*}{\text{link speed}}$			
<b>Network Link (Type 2)</b> Generated by a DR; lists all routers on an adjacent segment; flooded within an area				* modifiable with ospf auto-cost reference-bandwidth			
<b>Network Summary (Type 3)</b> Generated by an ABR and advertised among areas							
<b>ASBR Summary (Type 4)</b> Injected by an ABR into the backbone to advertise the presence of an ASBR within an area							
<b>External Link (Type 5)</b> Generated by an ASBR and flooded throughout the AS to advertise a route external to OSPF							
<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							
Router Types		Area Types					
<b>Internal Router</b> All interfaces reside within the same area		<b>Standard Area</b> Default OSPF area type					
<b>Backbone Router</b> A router with an interface in area 0 (the backbone)		<b>Stub Area</b> External link (type 5) LSAs are replaced with a default route					
<b>Area Border Router (ABR)</b> Connects two or more areas		<b>Totally Stubby Area</b> Type 3, 4, and 5 LSAs are replaced with a default route					
<b>AS Boundary Router (ASBR)</b> Connects to additional routing domains; typically located in the backbone		<b>Not So Stubby Area (NSSA)</b> A stub area containing an ASBR; type 5 LSAs are converted to type 7 within the area					
External Route Types							
<b>E1</b> · Cost to the advertising ASBR plus the external cost of the route							
<b>E2 (Default)</b> · Cost of the route as seen by the ASBR							
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 [...]						
Virtual Links							
· Tunnel formed to join two areas across an intermediate							
· Both end routers must share a common area							
· At least one end must reside in area 0							
· Cannot traverse stub areas							

by Jeremy Stretch

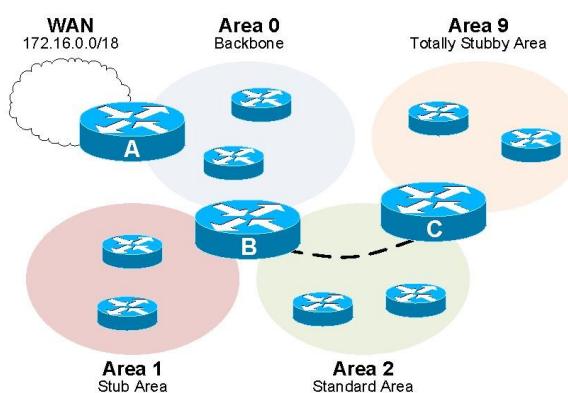
v2.1

# 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

## Configuration Example



```

Router A
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

```

```

Router B
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

```

```

Router C
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

```

by Jeremy Stretch

v2.1

## Catatan:

---

**“ILMU ITU BAGAIKAN HEWAN BURUAN, SEBALIKNYA  
PENA MERUPAKAN PENGIKATNYA. MAKA IKATLAH  
HEWAN BURUAN TERSEBUT DENGAN TALI YANG  
KOKOH.”**

---

-**Imam Syafi'i-**

CHAPTER 5

# Network Management

CCNA ENTERPRISE

The title is rendered in a hand-drawn, sketchy style. The word "Network" is written in large, blue, cursive letters, tilted slightly upwards and to the right. Below it, the word "Management" is written in yellow, cursive letters, also tilted similarly. A yellow banner is positioned above "Network", containing the text "CHAPTER 5" in blue. To the left of "Network", the acronym "CCNA" is written in yellow. To the right of "Management", the words "ENTERPRISE" are written in blue. All text is surrounded by hand-drawn lines and strokes in blue and yellow, giving it a dynamic, artistic feel.

# **NETWORK MANAGEMENT**

## **CONTENT:**

**QUALITY OF SERVICE (QOS)**

**ACCESS LIST (ACL)**

**NETWORK ADDRESS TRANSLATION (NAT)**

**GENERIC ROUTING ENCAPSULATION (GRE) TUNNEL**

**DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)**

**FIRST HOP REDUNDANCY PROTOCOL (FHRP)**

# QoS

QoS merupakan singkatan dari **Quality of Service** atau dalam Bahasa Indonesia diartikan sebagai **Kualitas Layanan**.

QoS digunakan untuk menjaga layanan jaringan tetap pada batas minimalnya, contohnya, ketika banyak klien yang menggunakan layanan jaringan yang menyebabkan traffic penuh dan menyebabkan penurunan pada kualitas layanan jaringan.

Dalam QoS terdapat beberapa istilah pada QoS:

**Bandwidth:** kapasitas dari sebuah link yang diukur dengan satuan bits per second.

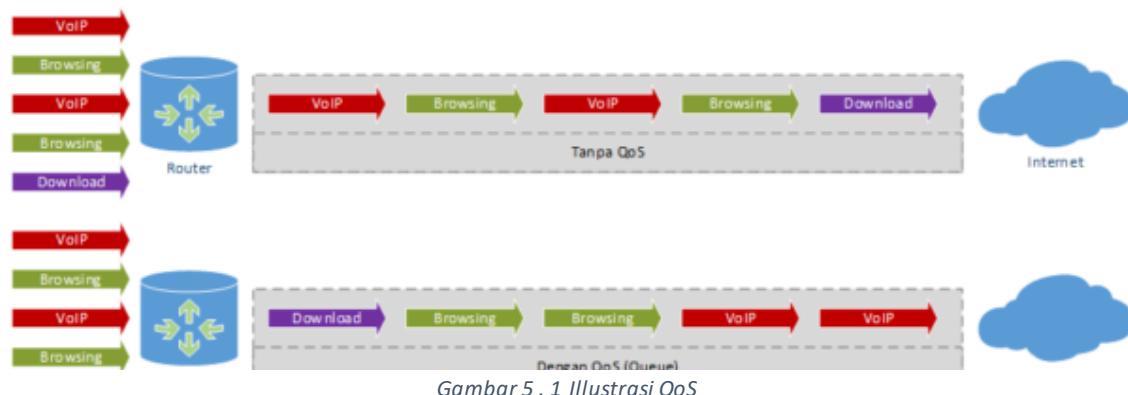
**Delay or Latency:** Seberapa lama sebuah paket sampai dari pengirim sampai ke penerima. Semakin besar delay, semakin lambat network tersebut. Delay biasa diukur dengan satuan milliseconds (ms).

**Jitter:** mengukur variasi delay antar paket. Sebagai contoh, jika sebuah paket membutuhkan delay 50ms untuk sampai ketujuan lalu paket selanjutnya membutuhkan delay 40ms maka jitter dari case tsb 10ms.

**Loss:** Ketika paket dikirim ke tujuan, paket bisa saja tidak sampai.

## Fungsi QoS

Ketika tanpa menggunakan QoS, sebuah traffic akan secara acak memenuhi/menggunakan bandwidth yang tersedia. Akibatnya, beberapa aplikasi yang



membutuhkan data lebih cepat tidak terpenuhi dengan semestinya. Pada kasus traffic VoIP, akan terjadi delay yang lumayan lama yang dapat menyebabkan terganggunya komunikasi antara dua orang yang menggunakan layanan tersebut.

Dengan menggunakan QoS, sebuah traffic akan disusun berdasarkan skala prioritas dalam sebuah sistem antrian atau biasa disebut Queue. dengan adanya sistem prioritas, traffic yang mempunyai prioritas lebih tinggi akan diproses oleh router terlebih dahulu, dibandingkan traffic dengan prioritas yang lebih kecil. Pada kasus traffic VoIP misalnya, traffic tersebut akan diproses terlebih dahulu oleh router agar proses komunikasi dapat tetap nyaman antara kedua orang yang menggunakan layanan tersebut. Selain itu dengan menggunakan QoS, sebuah traffic dapat dibatasi penggunaan bandwidth-nya.

Terdapat beberapa alat pada QoS:

Jenis Tools	Fungsi
<b>Classification</b>	Mengidentifikasi traffic menjadi beberapa bagian (voice, video dan data) agar bandwidth dapat dibagi berdasarkan klasifikasi tadi dan tidak menimbulkan pemborosan bandwidth akibat pemakainnya yang tidak tertata.
<b>Mark</b>	Menandai packet pada layer 2 (CoS) dan kemudian ketiga sampai dilayer 3(ToS) akan diidentifikasi packetnya, apakah boleh lanjut, apakah harus dibuang.
<b>Shaping</b>	Merubah kecepatan bandwidth pada suatu interface, misalkan pada satu interface, bandwidthnya 100mbps, kita rubah,

	dengan cara mengecilkannya hingga hanya menjadi 10mbps.
<b>Policing</b>	Dengan membuat aturan (policy) pada router. Dimana jika terdapat transfer yang melibih limit yang sudah dibuat, maka packet tersebut akan dibuang semua.

Tabel 5 . 1 Tools QoS

## QoS Variant

Dalam QoS terdapat banyak cara, berikut beberapa contoh QoS:

- **First-in, first-out (FIFO):** FIFO entails no concept of priority or classes of traffic.  
With FIFO, transmission of packets out the interface occurs in the order the packets arrive, which means no QoS
- **Priority Queuing (PQ):** schedules traffic such that the higher-priority queues “always” get serviced first
- **Custom Queuing (CQ):** provide specific traffic guaranteed bandwidth at a potential congestion point, assuring the traffic a fixed portion of available bandwidth and leaving the remaining bandwidth to other.
- **Weighted fair queueing (WFQ):** offers dynamic, fair queueing that divides bandwidth across queues of traffic based on weights. Low Traffic senders get priority over high traffic senders.

# ACCESS LIST

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**:

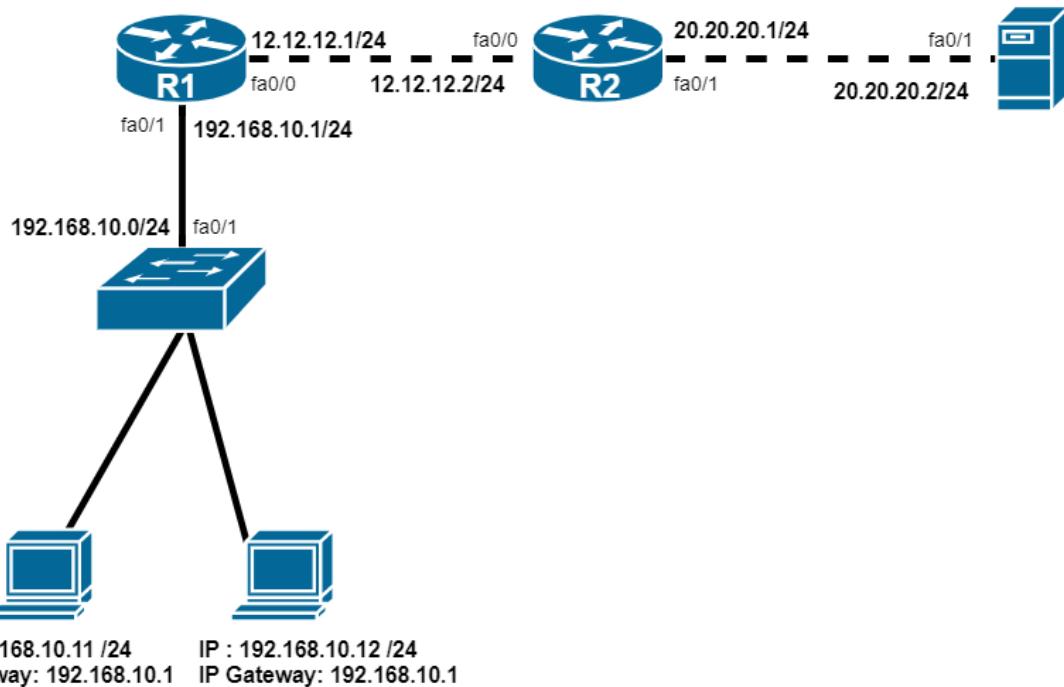
Standard Access List	Extended Access List
Nomer ACL antara 1-99	Nomer ACL antara 100-199
Bisa memblokir network, host dan subnet.	Bisa membolehkan/melarang network, host, subnet, service dan protocol.
Semua service diblokir	Bisa memilih service mana yang mau diblokir
Dikonfigurasikan sedekat mungkin 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> .

Tabel 5 . 2 Perbandingan Access List

## 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.

Selanjutnya kita akan Lab Standard Access List, berikut topologinya:



Gambar 5 . 2 Lab Standard Access List

Pada lab ini kita akan memblokir akses PC terhadap web server menggunakan Standard Access List.

Berikut step-step dalam membuat labnya:

1. Buat topologi
2. Setting IP Address agar sesuai

#### Pada R1

```
R1(config) #int fa0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#int fa0/0
R1(config-if)#ip add 12.12.12.1 255.255.255.0
R1(config-if)#no shutdown
```

#### Pada R2

```
R2(config) #int fa0/1
R2(config-if)#ip add 20.20.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#int fa0/0
R2(config-if)#ip add 12.12.12.2 255.255.255.0
R2(config-if)#no shutdown
```

3. Gunakan routing agar antar network dapat berkomunikasi

#### Pada R1

```
R1(config)#ip route 20.20.20.0 255.255.255.0 12.12.12.2
```

#### Pada R2

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

Pastikan antara PC dan Server dapat berkomunikasi

4. Kita set Access List nya di R2 (terdekat dengan sumber)

```
R2(config)#access-list 1 deny 192.168.10.0 0.0.0.255  
R2(config)#access-list 1 permit any
```

- Kita gunakan Standard Access List nomer 1
- Konfigurasikan deny 'menolak' network 192.168.10.0 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

```
R2(config)#int fa0/1  
R2(config-if)#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.

Untuk pengetesan, coba ping dari PC menuju server.

Ping dari PC

```
PC>ping 20.20.20.2
```

Lalu cek di router pada access list, terdapat 4 packet yang di block.

```
R2#show access-lists  
Standard IP access list 1  
    deny 192.168.10.0 0.0.0.255 (4 match(es))  
    permit any
```

Kemudian tes ping lagi, namun dari router R1 dengan source selain IP 192.168.10.0/24 dengan jumlah packet default yakni 5.

```
R1#ping
Protocol <ip>: 20.20.20.2
Target IP address: 20.20.20.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.2, timeout is 2
seconds: Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/10 ms
```

Kemudian kita cek di router R2, maka terdapat 5 packet yang di permit.

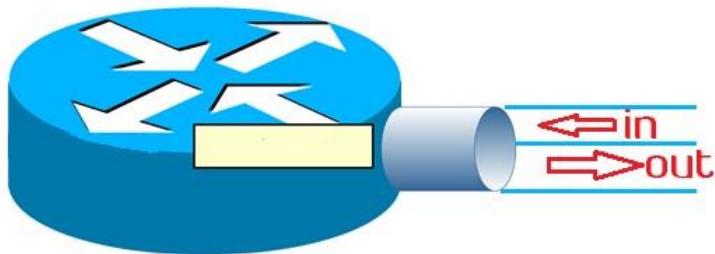
```
R2#sh ip access-lists
Standard IP access list 1
    deny 192.168.10.0 0.0.0.255 (4 match(es))
    permit any (5 match(es))
```

Kita tes ping lagi di R1 namun menggunakan source IP 192.168.10.0/24 dan packet berjumlah 11

```
R1#ping
Protocol [ip]:
Target IP address: 20.20.20.2
Repeat count [5]: 11
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.10.10.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 11, 100-byte ICMP Echos to 20.20.20.2, timeout is 2
seconds: Packet sent with a source address of 10.10.10.1
!!!!!!!
Success rate is 0 percent (0/11)
```

Kemudian, kita cek lagi di ACL R2, terlihat bahwa packet yang terdeny bertambah

```
R2#sh access-lists  
Standard IP access list 1  
    deny 192.168.10.0 0.0.0.255 (15 match(es))  
    permit any (5 match(es))
```



Gambar 5 . 3 Illustrasi access-group

Sekarang, kita akan akan **filtering terhadap satu host saja**, jadi salah satu host bisa mengakses sementara yang satu lagi tidak bisa.

### Konfigurasi ACL

```
R2(config)#access-list 2 deny 192.168.10.11 0.0.0.0  
R2(config)#access-list 2 permit any  
R2(config)#int fa0/1  
R2(config-if)#ip access-group 2 out
```

Setelah kita pasang access-group pada interface, maka secara otomatis access-group yang sebelumnya kita konfigurasikan access-group 1 akan hilang. Karena pada interface hanya dapat dipasang satu access-group. Jadi hanya satu access list yang dapat dipasang pada satu interface.

Untuk pengetesan:

Untuk pengetesan, lakukan ping dari pc 192.168.10.11 ke IP server

```
PC>ping 20.20.20.2
```

Cek ACL di router R2

```
R2#sh access-lists  
Standard IP access list 1  
    deny 192.168.10.0 0.0.0.255 (15match(es))  
    permit any (5 match(es))  
Standard IP access list 2  
    deny host 192.168.10.11 (4 match(es))  
    permit any
```

Lakukan ping dari pc 192.168.10.12/24

```
PC>ping 20.20.20.2
```

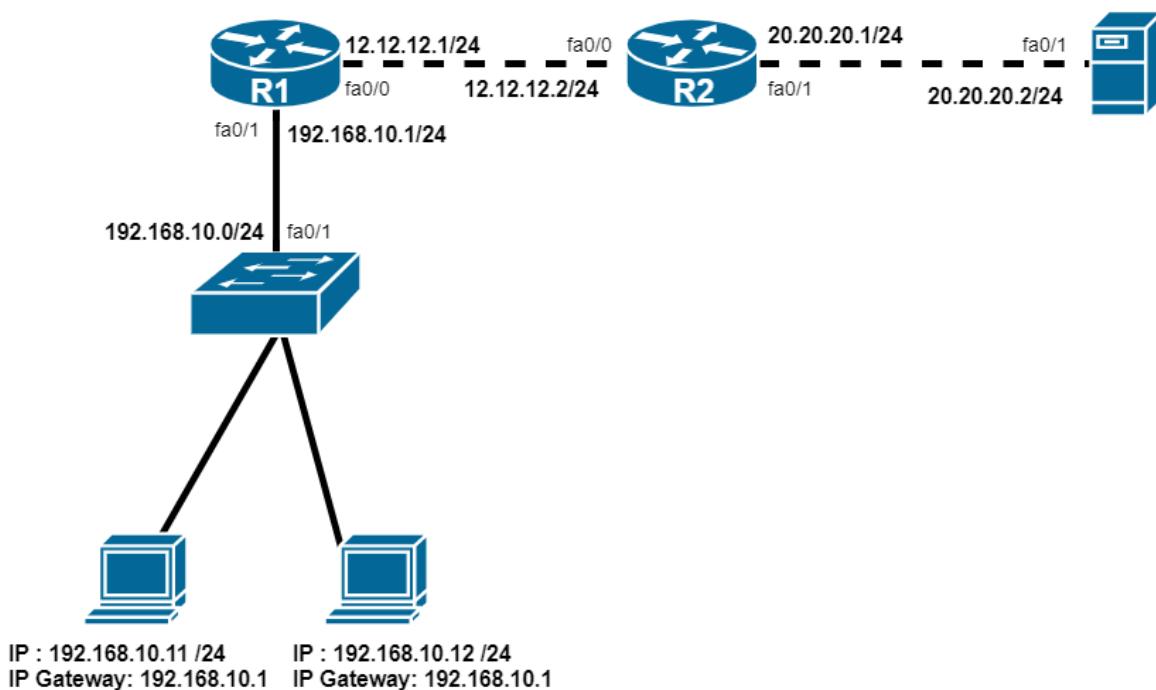
Cek ACL nya kembali, maka akan terdapat packet permit.

```
R2#sh access-lists
Standard IP access list 1
    deny 192.168.10.0 0.0.0.255 (15
match(es))      permit any (5 match(es))
Standard IP access list 2
    deny host 192.168.10.11 (4 match(es))
permit any (4 match(es))
```

## 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.

Labnya sama seperti Standard Access List`



Gambar 5 . 4 Lab Extended Access List

Pada Lab ini kita akan memblokir akses host terhadap web (TCP port 80) pada server.

### Langkah Konfigurasi:

Kita hapus konfigurasi Standard ACL yang sebelumnya berjalan

```
R2 (config) #no access-list 1
R2 (config) #no access-list 2
```

Selanjutnya kita konfigurasikan extended ACLnya

```
R1(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255 host  
20.20.20.2 eq 80  
R1(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*.

Selanjutnya kita masukkan konfigurasi Extended Access list tersebut kedalam interface

```
R1(config)#int fa0/0  
R1(config-if)#ip access-group 100 in
```

Untuk pengetesan, apabila kita mencoba ping ke server dari PC maka hasilnya reply, namun jika kita mencoba mengakses web, maka hasilnya gagal.

```
PC>ping 20.20.20.2
```

Selanjutnya kita cek Access Listnya

```
R1#sh access-lists  
Extended IP access list 100  
deny tcp 10.10.10.0 0.0.0.255 host 20.20.20.2 eq www (12 match(es))  
permit ip any any (4 match(es))
```

Maka akan terlihat, packet ping tadi akan masuk ke *permit* packet, dan saat kita mencoba web, maka akan masuk ke *deny* packet.

# 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			
<b>1-99</b>	IP standard	<b>any</b> Any address			
<b>1300-1999</b>	IP standard	<b>host</b> <address> A single address			
<b>100-199</b>	IP extended	<b>&lt;network&gt;</b> <mask> Any address matched by the wildcard mask			
<b>2000-2699</b>	IP extended				
<b>200-299</b>	Protocol	IP Options			
<b>300-399</b>	DECnet	<b>dscp</b> <DSCP> Match the specified IP DSCP			
<b>400-499</b>	XNS	<b>fragments</b> Check non-initial fragments			
<b>500-599</b>	Extended XNS	<b>option</b> <option> Match the specified IP option			
<b>600-699</b>	Appletalk	<b>precedence</b> {0-7} Match the specified IP precedence			
<b>700-799</b>	Ethernet MAC	<b>ttl</b> <count> Match the specified IP time to live (TTL)			
<b>800-899</b>	IPX standard	TCP/UDP Port Definitions			
<b>900-999</b>	IPX extended	<b>eq</b> <port> Equal to	<b>neq</b> <port> Not equal to		
<b>1000-1099</b>	IPX SAP	<b>lt</b> <port> Less than	<b>gt</b> <port> Greater than		
<b>1100-1199</b>	MAC extended	<b>range</b> <port> <port> Matches a range of port numbers			
<b>1200-1299</b>	IPX summary	Miscellaneous Options			
		<b>reflect</b> <name> Create a reflexive ACL entry			
		<b>time-range</b> <name> Enable rule only during the given time range			
Applying ACLs to Restrict Traffic					
<pre>interface FastEthernet0/0 ip access-group {&lt;number&gt;   &lt;name&gt;} {in   out}</pre>					
Troubleshooting					
<pre>show access-lists [&lt;number&gt;   &lt;name&gt;] show ip access-lists [&lt;number&gt;   &lt;name&gt;] show ip access-lists interface &lt;interface&gt; show ip access-lists dynamic show ip interface [&lt;interface&gt;] show time-range [&lt;name&gt;]</pre>					

by Jeremy Stretch

v2.0

# NAT

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.

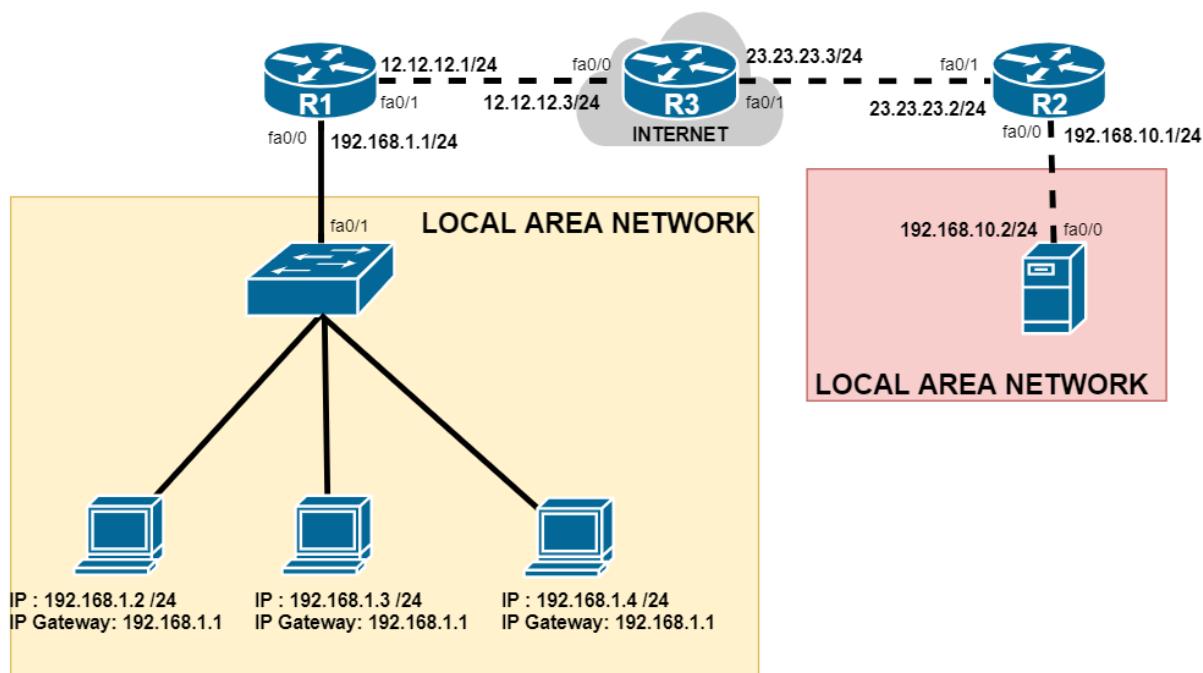
Kita akan bahas lebih lanjut mengenai NAT:

## Static NAT

Seperti yang sudah dijelaskan diatas, Static NAT adalah NAT yang kita harus konfigurasi secara manual.

Lab Static NAT terdapat di halaman selanjutnya.

Pada Lab ini R3 berperan sebagai Internet atau semua router yang ada didunia, yang diwakili dengan /0



Gambar 5 . 5 Lab Static NAT

#### Langkah konfigurasi Static NAT:

Konfigurasikan IP Address seperti dengan topologi

#### Setting R1:

```
R1(config)#int f0/0
R1(config-if)#ip addr 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int f0/1
R1(config-if)#ip addr 12.12.12.1 255.255.255.0
R1(config-if)#no shut
```

#### Setting R2

```
R2(config)#int f0/0
R2(config-if)#ip addr 192.168.10.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int f0/1
R2(config-if)#ip addr 23.23.23.2 255.255.255.0
R2(config-if)#no shut
```

#### Setting R3

```
R3(config)#int f0/0
R3(config-if)#ip addr 12.12.12.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int f0/1
R3(config-if)#ip ad 23.23.23.3 255.255.255.0
R3(config-if)#no shut
```

Selanjutnya konfigurasikan Default route pada R1 dan R2

### Default route R1

```
R1(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.3
```

### Default Route R2

```
R2(config)#ip route 0.0.0.0 0.0.0.0 23.23.23.3
```

### Show ip route

```
R2#show ip route | b Gateway
Gateway of last resort is 23.23.23.3 to network 0.0.0.0
  23.0.0.0/24 is subnetted, 1 subnets
C       23.23.23.0 is directly connected, FastEthernet0/1
C       192.168.10.0/24 is directly connected, FastEthernet0/0
S*     0.0.0.0/0 [1/0] via 23.23.23.3
```

```
R2#
```

Kemudian, kita konfigurasikan Static NAT

```
R2(config)#ip nat inside source static tcp 192.168.10.2 80 23.23.23.2 80
R2(config)#int f0/0
R2(config-if)#ip nat inside
R2(config-if)#int f0/1 R2(config-if)#ip nat outside
```

- **Ip nat inside** bermaksud untuk konfigurasi NAT kedalam/ke area local
- **source** itu kliennya
- **static** itu cara terjemahannya (NAT) selain *static* ada juga cara *dynamic*
- **tcp** adalah protocol yang akan digunakan dalam NAT, selain TCP bisa UDP dll
- **192.168.10.2** IP privatnya
- **80** artinya port 80, berarti TCP port 80. Klien ingin menggunakan TCP port 80 sebagai NAT
- **23.23.23.2** IP publicnya
- **80** artinya port 80, berarti TCP port 80. Berarti ketika klien mengakses web (HTTP) maka dia akan dikenali sebagai 23.23.23.3 karena NAT nya hanya untuk protocol TCP 80
- **Ip nat inside** berarti interface tersebut mengarah ke source/ke klien
- **Ip nat outside** berarti interface tersebut mengarah ke luar/IP public

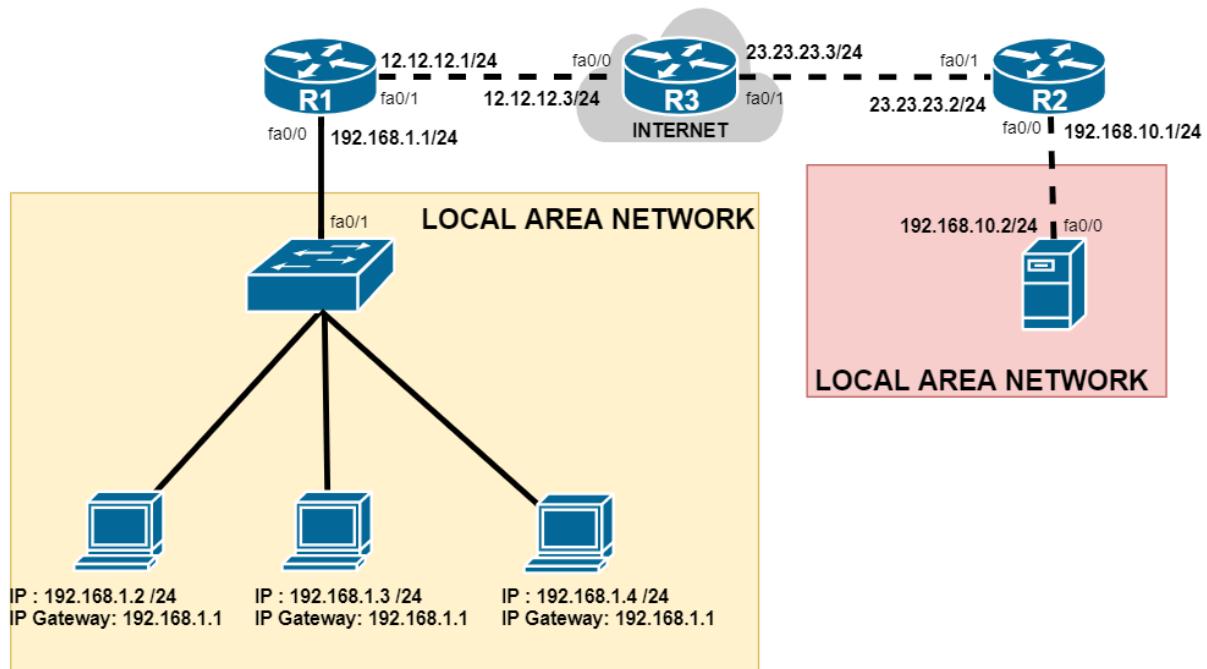
Selanjutnya kita akan lanjut mengonfigurasi Dynamic NAT nya

## Dynamic NAT

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.

Dengan topologi masih sama



Gambar 5 . 6 Topologi Dynamic NAT

Kita akan konfigurasikan Dynamic NAT Overload nya pada R1:

```
R1(config) #access-list 1 permit 192.168.1.0 0.0.0.255  
R1(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 Dynamic NAT, 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*.

Dan jangan lupa masukkan interface NAT nya

```
R1(config)#int f0/0
R1(config-if)#ip nat inside
R1(config-if)#int f0/1
R1(config-if)#ip nat outside
R1(config-if)#

```

## Pengetesan

Jalankan debug ip nat di sisi router R1

```
R1# debug ip nat
```

Dari sisi PC user local, Ping ke IP Public Server di internet

```
Packet Tracer PC Command Line 1.0
C:\>ping 23.23.23.2

Pinging 23.23.23.2 with 32 bytes of data:

Reply from 23.23.23.2: bytes=32 time<1ms TTL=253
Reply from 23.23.23.2: bytes=32 time<1ms TTL=253
```

Cek debug di sisi router R1

```
NAT: s=192.168.1.2->12.12.12.1, d=23.23.23.2 [1]
NAT*: s=23.23.23.2, d=12.12.12.1->192.168.1.2 [22]
NAT: s=192.168.1.2->12.12.12.1, d=23.23.23.2 [2]
NAT*: s=23.23.23.2, d=12.12.12.1->192.168.1.2 [23]
```

Cek akses HTTP dari PC 192.168.1.3/24 ke IP Public Web server.



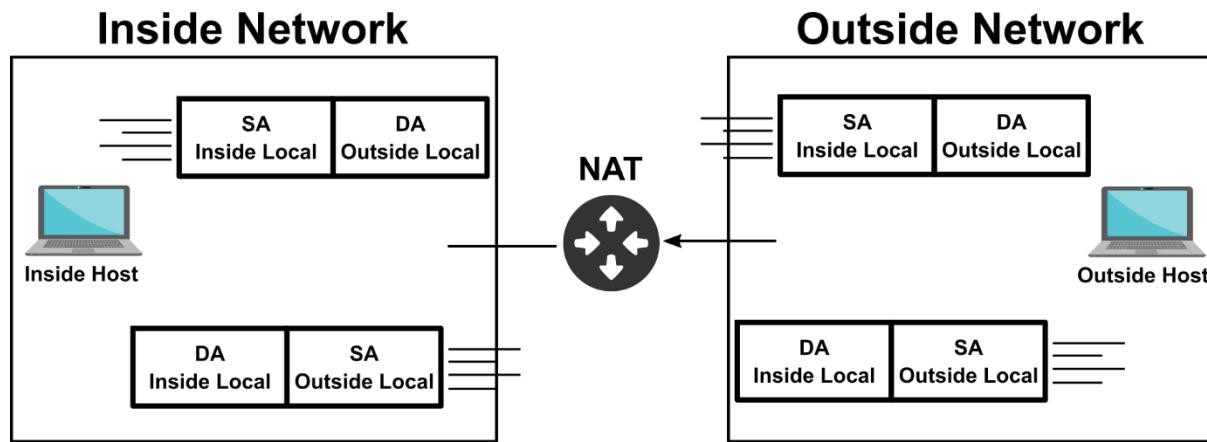
Gambar 5 . 7 Web Server Cisco Packet Tracer

Kita cek hasil NAT dengan command *show ip nat translation*

#### show ip nat translation R1

```
R1#show ip nat translation
Pro Inside global      Inside local        Outside local       Outside global
tcp 12.12.12.1:1025   192.168.1.3:1025   23.23.23.2:80    23.23.23.2:80
tcp 12.12.12.1:1026   192.168.1.3:1026   23.23.23.2:80    23.23.23.2:80
```

Dengan begini, ketika jaringan lokal dari network PC (192.168.1.0) dapat mengakses web server dengan menggunakan IP public 12.12.12.1.



Gambar 5 . 8 Illustrasi NAT

Berdasarkan Illustrasi diatas, maka jaringan lokal dalam (inside network) dapat berkomunikasi dengan jaringan lokal lain (outside network) lewat internet.

# NETWORK ADDRESS TRANSLATION

packetlife.net

Example Topology		Address Classification										
		<b>Inside Local</b>	An actual address assigned to an inside host									
FastEthernet0 10.0.0.1/16 NAT Inside		<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>		<b>Location</b>	<table border="1"> <tr> <th></th> <th>Local</th> <th>Global</th> </tr> <tr> <td>Inside</td> <td>Inside Local</td> <td>Inside Global</td> </tr> <tr> <td>Outside</td> <td>Outside Local</td> <td>Outside Global</td> </tr> </table>		Local	Global	Inside	Inside Local	Inside Global	Outside	Outside Local	Outside Global
	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)		Special NAT Pool Types										
<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>Rotary</b>	Used for load balancing									
		<b>Match-Host</b>	Preserves the host portion of the address after translation									
Inside Destination Translation		Troubleshooting										
<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>		<pre>show ip nat translations [verbose] show ip nat statistics clear ip nat translations</pre>	<pre>ip nat translation tcp-timeout &lt;seconds&gt; ip nat translation udp-timeout &lt;seconds&gt; ip nat translation max-entries &lt;number&gt;</pre>									

by Jeremy Stretch

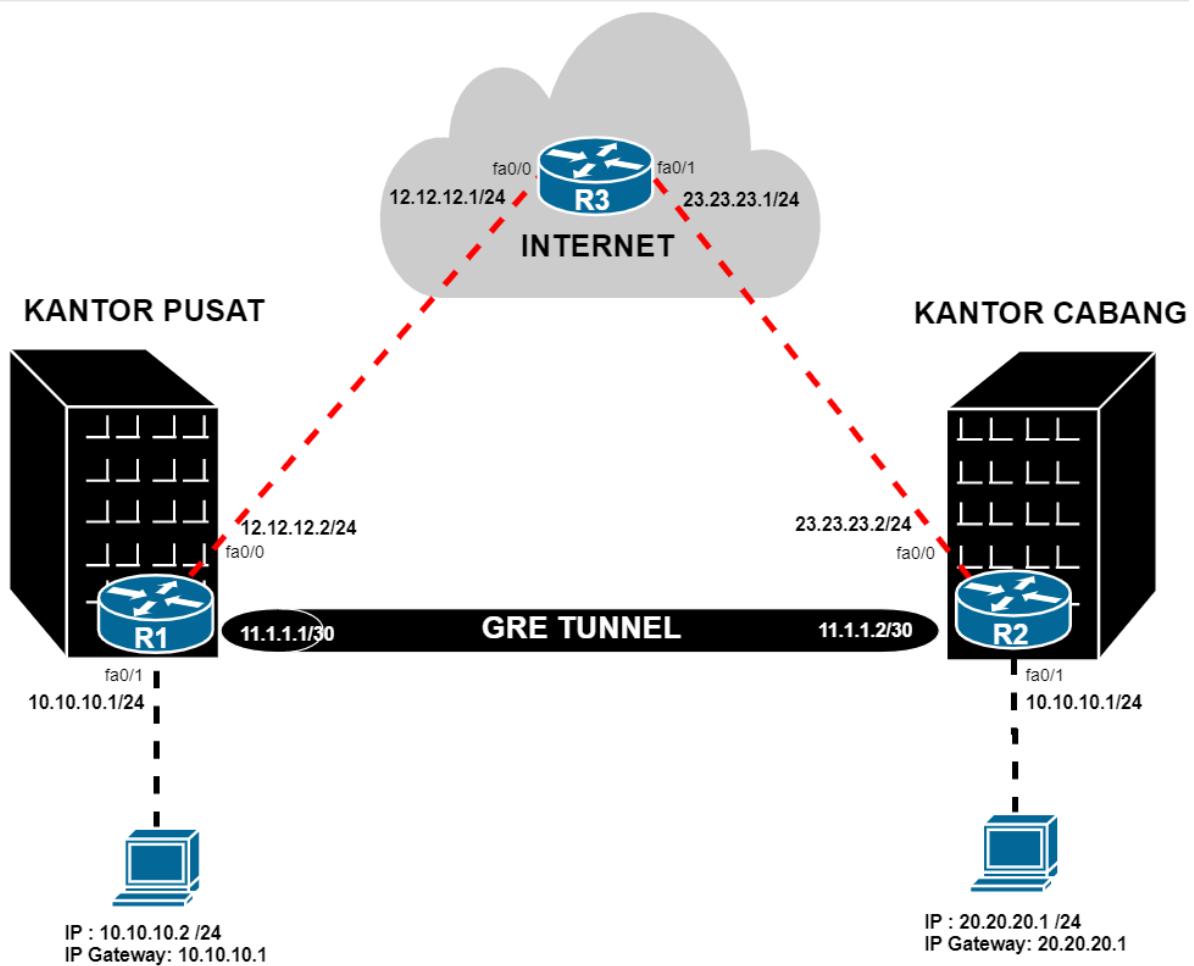
v1.0

# GRE TUNNEL

Dalam sebuah keperluan, biasanya sebuah instansi/perusahaan membutuhkan suatu koneksi yang sifatnya private kesemua cabangnya yang terpisah dan letaknya berjauhan. Oleh karena itu, digunakanlah sebuah VPN (*Virtual Private Network*) agar komunikasi antar cabang tersebut aman. VPN ini dilewaskan 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.

Pada Cisco sendiri sudah terdapat tunnel milik *proprietary Cisco* yaitu GRE tunnel.

Berikut Lab GRE Tunnel:



Gambar 5 . 9 Lab GRE Tunnel

Di lab ini R3 berperan sebagai internet yang menghubungkan R1 dan R2

**KITA SETTING IP ADDRESS SESUAI TOPOLOGY**

```
R1(config)# int fa0/0
R1(config-if)# ip addr 12.12.12.2 255.255.255.0
R1(config-if)# no shutdown
```

```
R1(config)# int fa0/1
R1(config-if)# ip addr 10.10.10.1 255.255.255.0
R1(config-if)# no shutdown
```

```
R2(config)# int fa0/0
R2(config-if)# ip addr 23.23.23.2 255.255.255.0
R2(config-if)# no shutdown
```

```
R2(config)# int fa0/1
R2(config-if)# ip addr 20.20.20.1 255.255.255.0
R2(config-if)# no shutdown
```

```
R3(config)# int fa0/0
R3(config-if)# ip addr 12.12.12.1 255.255.255.0
R3(config-if)# no shutdown
```

```
R3(config)# int fa0/1
R3(config-if)# ip addr 23.23.23.1 255.255.255.0
R3(config-if)# no shutdown
```

Pastikan kedua router cabang bisa saling komunikasi dengan IP Public nya , setting default route di R1 dan R2

```
R1(config)# ip route 0.0.0.0 0.0.0.0 12.12.12.1
```

```
R2(config)# ip route 0.0.0.0 0.0.0.0 23.23.23.1
```

```
R1#ping 23.23.23.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.23.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
Router#
```

## KONFIGURASI GRE TUNNEL

```
R1(config)#int tunnel 0
R1(config-if)#tunnel source fa0/0
R1(config-if)#tunnel destination 23.23.23.2      -> IP PUBLIC LAWAN
R1(config-if)#ip address 11.1.1.1 255.255.255.252
```

```
R2(config)#int tunnel 0
R2(config-if)#tunnel source fa0/0
R2(config-if)#tunnel destination 12.12.12.2      -> IP PUBLIC LAWAN
```

```
R2(config-if)#ip address 11.1.1.2 255.255.255.252
```

### TEST PING KEDUA INTERFACE TUNNEL

```
R1# ping 11.1.1.2
```

### STATIC ROUTE KE MASING MASING JARINGAN LOCAL

Agar jaringan local bisa saling komunikasi maka buatkan static route ke jaringan local antar cabang

```
R1(config)# ip route 20.20.20.0 255.255.255.0 11.1.1.2
```

```
R2(config)# ip route 10.10.10.0 255.255.255.0 11.1.1.1
```

```
R1#sh ip int brief
Interface          IP-Address OK? Method      Status     Protocol
FastEthernet0/0   12.12.12.2  YES manual    up         up
FastEthernet0/1   10.10.10.1  YES manual    up         up
Tunnel0          11.1.1.1 YES manual  up        up
Vlan1            unassigned YES unset    administratively down down
R1#
```

# DHCP

DHCP merupakan singkatan dari **Dynamic Host Configuration Protocol**. adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan.

### Fungsi DHCP

Fungsinya adalah untuk mempermudah pendapatkan IP Address pada suatu jaringan. Misalnya jika pada suatu jaringan tidak dipasang DHCP Server, maka pengalaman 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:

#### DHCP Server

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

#### DHCP Client

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

### 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

### IP Least Discover

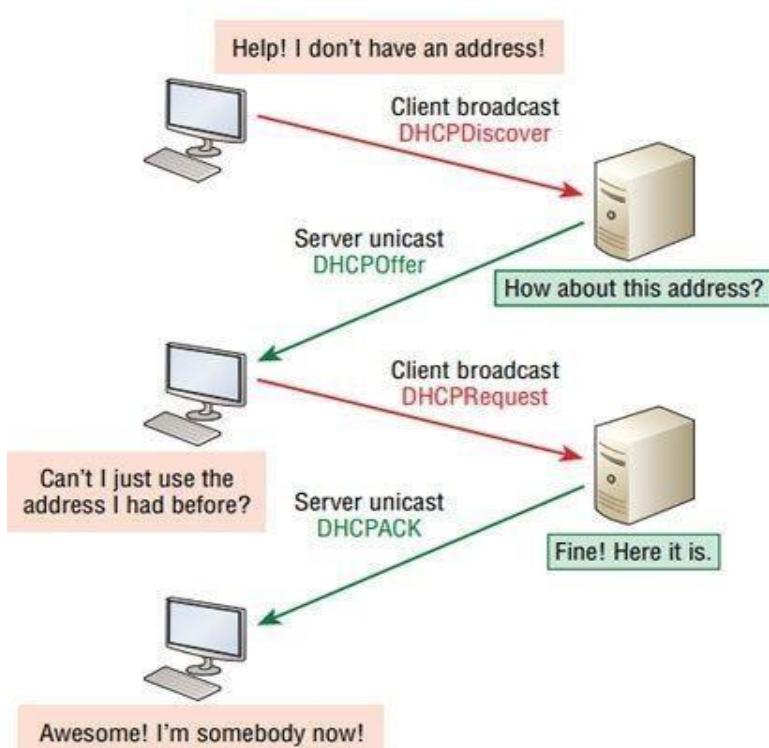
Komputer client meminta alamat IP ke server

### IP Least Offer

DHCP server yang memiliki list alamat IP memberikan penawaran kepada komputer client

### IP Lease Request

Komputer client memilih/menyeleksi penawaran yang pertama kali diberikan DHCP, kemudian melakukan broadcast dengan mengirim pesan bahwa komputer client menyetujui penawaran tersebut



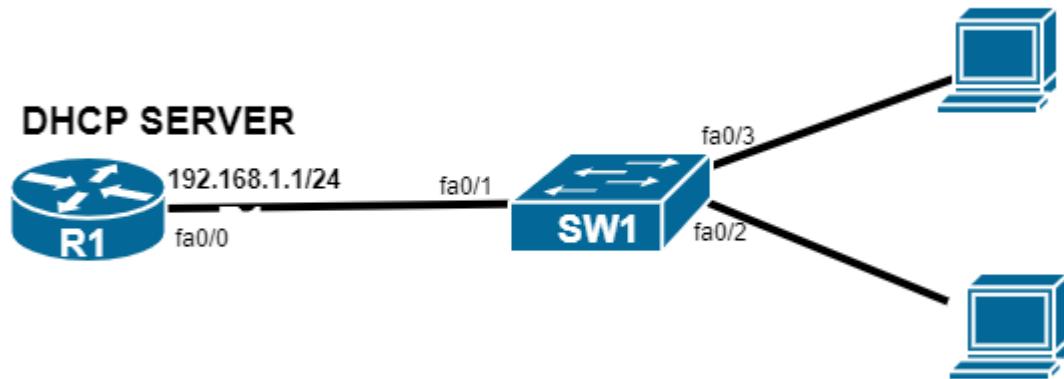
Gambar 5 . 10 Proses DHCP

### IP Lease Acknowledge

Pada tahap ini DHCP server menerima pesan tersebut dan mulai mengirim suatu paket acknowledge (DHCPACK) kepada client.

Paket tersebut berisi berapa lama komputer client bisa menggunakan alamat IP tersebut (yang diberikan DHCP server) beserta konfigurasi lainnya. Dan komputer client pun dapat terhubung ke jaringan.

## Lab DHCP Server



Gambar 5 . 11 Lab DHCP Server

Kita akan konfigurasikan R1 menjadi DHCP Server

Langkah pertama, konfigurasikan interface Fa0/1 dengan IP address 192.168.1.1/24

```
Router(config) #interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

Tambahkan konfigurasi DHCP Server berikut.

```
Router(config) #ip dhcp pool client-1
Router(dhcp-config) #network 192.168.1.0 255.255.255.0
Router(dhcp-config) #dns-server 1.1.1.1
Router(dhcp-config) #default-router 192.168.1.1
Router(dhcp-config) #exit
```

- **ip dhcp** command dari DHCP
- **pool (nama pool)** contoh pool client-1
- **network 192.168.1.0** network yang diberikan ke klien
- **dns-server 1.1.1.1** DNS server yang akan diberikan oleh server
- **default-router 192.168.1.1** gateway yang akan diberikan server

Jika terdapat IP yang tidak akan dialokasikan oleh DHCP Server, maka gunakan exclude-address

```
Router(config) #ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Dengan konfigurasi diatas, maka PC akan mendapatkan IP mulai dari 192.168.1.11.

Selanjutnya rubah settingan IP pada PC menjadi dynamic dengan klik pilihan “Obtain an IP Address Automatically” dan selanjutnya buka command prompt dan ketikkan ipconfig, pastikan sudah mendapatkan alokasi IP addressnya.

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

```
Router#show ip dhcp binding
IP address          Client-ID/           Lease expiration      Type
                  Hardware address
192.168.1.11        0003.E4AE.9DB6      --
Automatic 192.168.1.12    000B.BE9C.66A6      --
Automatic Router#
```

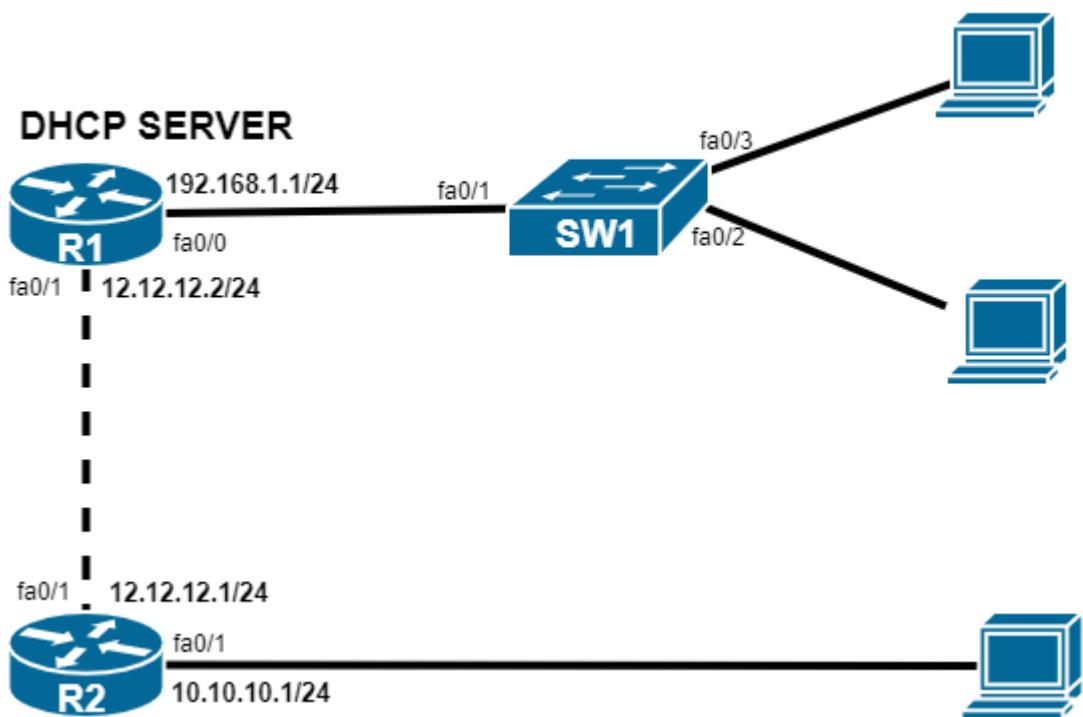
Jika pada switch ingin dijadikan sebuah dhcp-client, maka kita bisa setting interface VLAN 1 agar mendapat IP dari Router.

```
SW1(config)#int vlan 1
SW1(config-if)#ip address dhcp
SW1(config-if)#no shutdown
SW1(config-if)#
%DHCP-6-ADDRESS_ASSIGN: Interface Vlan1 assigned DHCP address
192.168.1.13, mask
255.255.255.0, hostname SW1
```

Hanya saja, jika switch menjadi DHCP server, maka hanya satu jaringan saja yang bisa digunakan, karena dasarnya switch bekerja dilayer 2 bukan dilayer 3.

## Lab DHCP Relay

Seperti pada keterangan diatas fungsi dari DHCP Relay adalah meneruskan DHCP Server, berikut adalah labnya:



Gambar 5 . 12 Lab DHCP Relay

### KONFIGURASI IP ADDRESS TIAP ROUTER

```
R-DHCP-SERVER(config)#interface FastEthernet0/1
R-DHCP-SERVER(config-if)#no shutdown
R-DHCP-SERVER(config-if)#ip address 12.12.12.2 255.255.255.252
```

```
R-DHCP-RELAY(config)#interface FastEthernet0/0
R-DHCP-RELAY(config-if)#ip address 10.10.10.1 255.255.255.0
R-DHCP-RELAY(config-if)#no shutdown
R-DHCP-RELAY(config)#interface FastEthernet0/1
R-DHCP-RELAY(config-if)#ip address 12.12.12.1 255.255.255.252
R-DHCP-RELAY(config-if)#no shutdown
```

### Buat DHCP Server khusus untuk PC2 pada R-DHCP-SERVER

```
R-DHCP-SERVER(config)#ip dhcp pool pc2
R-DHCP-SERVER(dhcp-config)#network 10.10.10.0 255.255.255.0
R-DHCP-SERVER(dhcp-config)#dns-server 1.1.1.1
R-DHCP-SERVER(dhcp-config)#default-router 10.10.10.1
R-DHCP-SERVER(config)#ip dhcp excluded-address 10.10.10.1
```

### Selanjutnya mari kita konfigurasikan DHCP relay pada R-TETANGGA

```
R-DHCP-RELAY(config)#int fa0/0
R-DHCP-RELAY(config-if)#ip helper-address 12.12.12.2
```

Dengan begini, ketika PC yang berada di R-DHCP-RELAY meminta DHCP, maka R-DHCP-SERVER lah yang akan memberikan DHCP. Sementara itu R-DHCP-RELAY, berfungsi untuk menjembatani R-DHCP-SERVER agar dapat memberikan DHCP ke PC yang berada di R-DHCP-RELAY.

Selanjutnya tes hasil konfigurasi dengan request IP DHCP dari PC2, pastikan PC tersebut mendapat IP yang sesuai.

## Lab DHCP Snooping

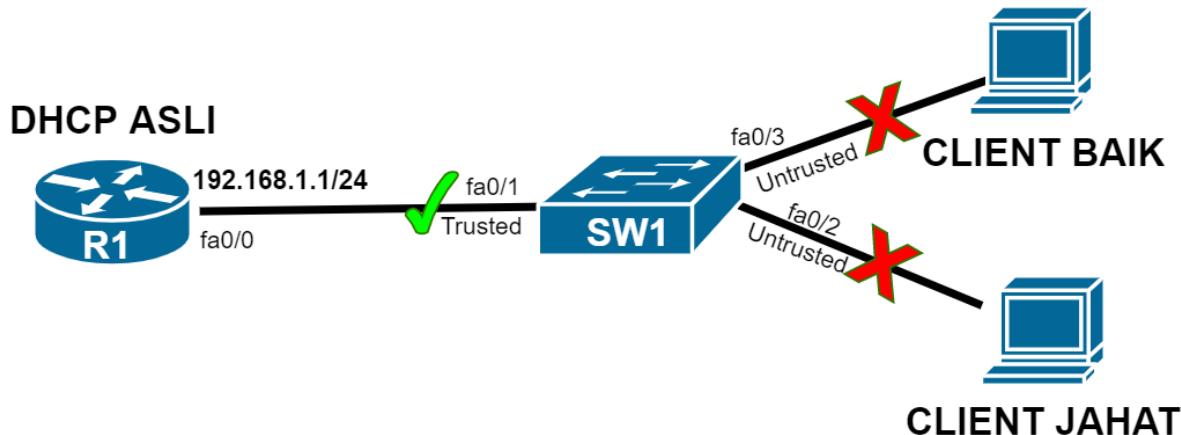
Pada DHCP, sebuah server bertanggung jawab untuk memberikan IP secara otomatis kepada client. Namun, apa yang terjadi jika pada sebuah jaringan, terdapat sebuah DHCP server palsu yang sehingga, ketika client mencoba request, justru mendapatkan IP palsu. Hal ini merupakan **DHCP Spoofing**, sebuah cara untuk meretas jaringan yang dimana, si *attacker* berpura-pura menjadi DHCP Server agar mendapat IP address korban dan memberikan gateway dan bahkan DNS palsu dan akhirnya biasanya digunakan untuk meretas korban.

**DHCP Snooping** pada Cisco, ditujukan untuk mencegah terjadinya serangan ini. Pada jaringan local, biasanya DHCP Snooping dijalankan pada switch. Cara kerjanya, pada switch membagi jenis portnya menjadi 2 **trusted** dan **untrusted**.

- **Trusted**, berarti diperboleh adanya traffic DHCP pada portnya.
- **Untrusted**, berarti tidak diperbolehkan adanya traffic DHCP pada portnya.

Secara default, ketika kita pertama kali mengaktifkan DHCP Snooping, portnya untrusted

Berikut Lab DHCP Snooping:



Gambar 5 . 13 Lab DHCP Snooping

## KONFIGURASI DHCP SNOOPING PADA SWITCH

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#no ip dhcp snooping information option
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
```

- **ip dhcp snooping** untuk meng-enable fitur DHCP Snooping.
- **ip dhcp snooping vlan 1** untuk menggunakan DHCP Snooping di Vlan yang lebih spesifik.
- **no ip dhcp infotmation option** untuk menghilangkan *option-82* pada Snooping.
- **ip dhcp snooping trust** untuk set interface menjadi **Trust**.

Lakukan request DHCP client pada sisi client. Pastikan mendapatkan IP dari DHCP server yang asli.

## CEK DENGAN SHOW IP DHCP SNOOPING PADA SWITCH

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is
disabled circuit-id default
format: vlan-mod-port
remote-id: aabb.cc00.0100 (MAC)
Option 82 on untrusted port is
not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
```

Interface	Trusted	Allow option	Rate limit (pps)
FastEthernet0/0	yes	yes	unlimited
Custom circuit-ids:			

Setiap klien DHCP yang ada di port untrusted akan disimpan informasinya di dalam DHCP Snooping Binding.

Untuk digunakan oleh fitur Dynamic Arp Inspection (DAI).

```

Switch#show ip dhcp snooping binding
MacAddress          IPAddress          Lease(sec)    Type           VLAN
Interface
-----
00:50:79:66:68:00  192.168.1.4       86220        dhcp-snooping  1
Ethernet0/1
Total number of bindings: 1

Switch#

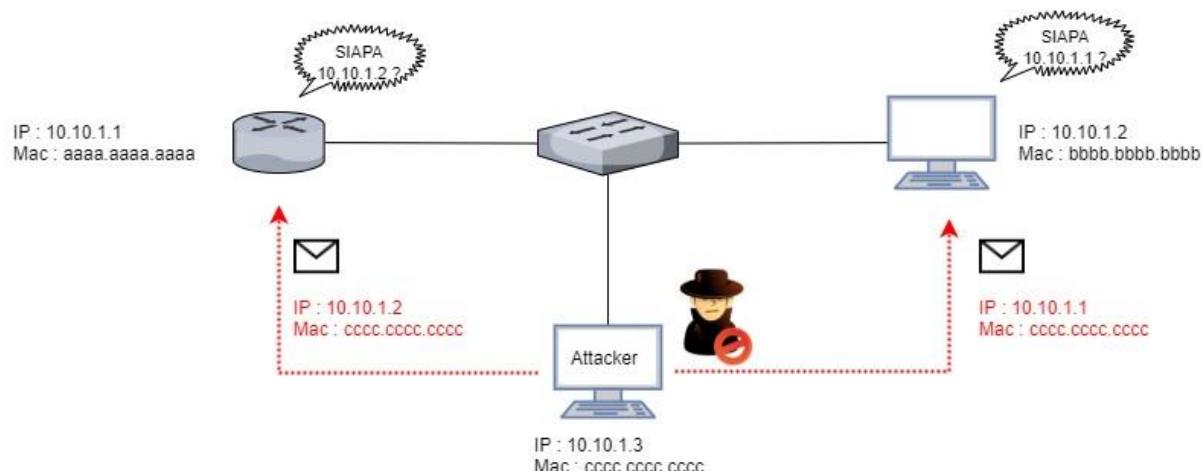
```

Jika **Client Jahat** mencoba membuat DHCP server, maka packetnya akan di-drop dikarenakan portnya adalah **untrusted** sehingga ketika PC request DHCP akan mendapat IP dari server yang sebenarnya.

## Lab Dynamic ARP Inspection (DAI)

**ARP (Address Resolution Protocol)** adalah sebuah cara untuk mengetahui MAC address melalui IP address, misalkan ada pengirim dan penerima. Sebelum si pengirim dapat mengirimkan, dia harus mengetahui MAC address si penerima terlebih dahulu, agar tidak salah kirim alias si pengirim harus membutuhkan MAC addressnya untuk proses enkapsulasi data. Maka digunakan ARP untuk mengetahui MAC address dari penerima.

Namun Tahukah kamu, bahwa seseorang bisa saja memanipulasi ARP. Ini dikenal dengan *ARP spoofing attack*. *Attacker* menyebarkan informasi palsu dengan memanipulasi IP Address yang sama dengan korban namun dengan informasi MAC address yang salah. Sehingga paket akan dikirim kan kepada attacker.



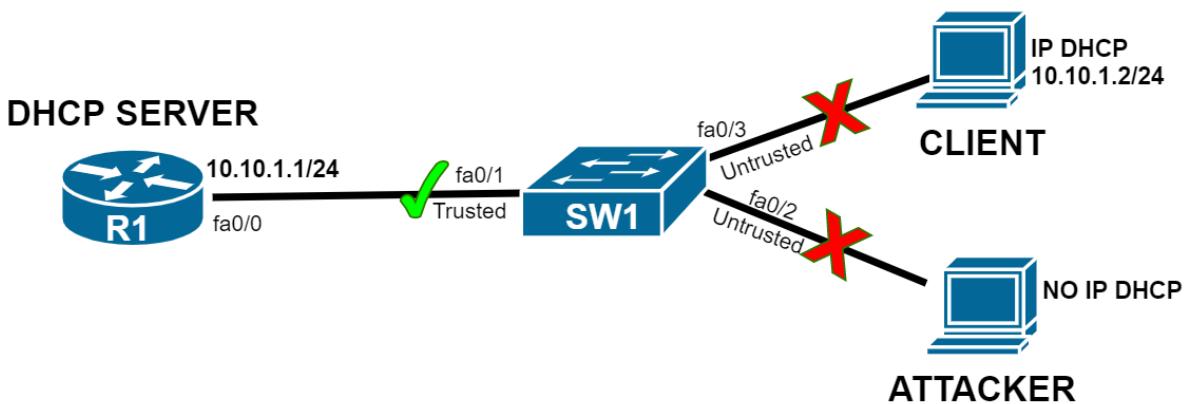
Gambar 5 . 14 Illustrasi ARP Spoofing

**Dynamic ARP Inspection**, hampir sama seperti DHCP Snooping, dengan adanya **Trusted & Untrusted port**.

- **Trusted port**, biasanya di set untuk port yang mengarah ke gateway karena potensinya kecil
- **Untrusted port**, biasanya di set untuk port yang mengarah ke host, karena potensinya sangat besar. Maka Dynamic Arp Inspection akan memeriksa setiap paket pada port ini, untuk menghindari ARP Spoofing.

Secara default, ketika kita pertama kali mengaktifkan DAI, portnya untrusted

Berikut LAB DAI:



Gambar 5 . 15 Lab Dynamic ARP Inspection

#### KONFIGURASI DAI DI SWITCH

```
SW1(config)#int f0/1
SW1(config-if)#ip arp inspection trust
SW1(config-if)#exit
SW1(config)#ip arp inspection vlan 1
SW1(config)#
```

- **ip arp inspection trust** untuk set interface ke **Trust**.
- **ip arp inspection vlan 1** untuk menggunakan DAI di Vlan yang lebih spesifik.

#### CEK DENGAN SHOW IP ARP INSPECTION INTERFACE

```
SW1#show ip arp inspection interfaces
Interface      Trust State    Rate(pps)    Burst Interval
-----  -----
Fa0/1          Trusted       15           1
Fa0/2          Untrusted     15           1
Fa0/3          Untrusted     15           1
Fa0/4          Untrusted     15           1
```

Coba berikan IP address pada PC client secara static, kemudian gateway

```
Client> ip 10.10.1.2/24
Checking for duplicate address...
PC1 : 10.10.1.2 255.255.255.0
Client> ping 10.10.1.1
host (10.10.1.1) not reachable
```

Secara default, semua traffic akan di blok oleh DAI, kecuali traffic DHCP. Karena DAI akan menggunakan database Dhcp snooping untuk mencatat IP dan Mac-Address yang Valid. Perhatikan log yang muncul pada Switch.

```
Switch(config)#
*Jan  8 16:19:19.852: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Req) on
Gi0/1, vlan
1.([0050.7966.6804/10.10.1.2/ffff.ffff.ffff/10.10.1.2/16:19:19 UTC Wed
Jan 8 2020])
*Jan  8 16:19:20.854: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Req) on
Gi0/1, vlan
1.([0050.7966.6804/10.10.1.2/ffff.ffff.ffff/10.10.1.2/16:19:20 UTC Wed
Jan 8 2020])
*Jan  8 16:19:21.891: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Req) on
Gi0/1, vlan
1.([0050.7966.6804/10.10.1.2/ffff.ffff.ffff/10.10.1.2/16:19:21 UTC
Wed Jan 8 2020])
```

Sehingga ketika kita menggunakan IP static, maka ip kita tidak akan ada di database dhcp snooping, akibatnya traffic akan di drop. Ingat, DAI menggunakan database dhcp snooping untuk mengetahui ip dan mac address klien.

Sekarang coba rubah IP PC ke DHCP dan ping gateway.

```
Client> ip dhcp
DORA IP 10.10.1.2/24 GW 10.10.1.1
```

Maka IP dan mac address akan dicatat dalam database DHCP snooping binding.

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress      Lease(sec)    Type        VLAN      Interface
00:50:79:66:68:04  10.10.1.2     86400        dhcp-snooping 1          Gi0/1
Total number of bindings: 1
```

```
Client> ping 10.10.1.1

84 bytes from 10.10.1.1 icmp_seq=1 ttl=255 time=10.181 ms
84 bytes from 10.10.1.1 icmp_seq=2 ttl=255 time=5.922 ms
84 bytes from 10.10.1.1 icmp_seq=3 ttl=255 time=8.632 ms
84 bytes from 10.10.1.1 icmp_seq=4 ttl=255 time=7.141 ms
```

Setelah menggunakan DHCP client, ternyata traffic bisa diteruskan oleh switch. Sementara ketika kita menggunakan IP static traffic kita di blok. Lihat statistic jumlah paket yang di forward dan di blok oleh switch.

Switch#sh ip arp inspection statistics					
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops	
1	4	10	10	0	
Vlan	DHCP Permits	ACL Permits	Probe Permits	Source MAC Failures	
1	3	0	0	0	
Vlan	Dest MAC Failures	IP Validation Failures	Invalid Protocol Data		
1	0	0	0	0	

## ARP ACCESS LIST

Dalam beberapa kasus, tidak semua IP address yang dipasang pada perangkat menggunakan IP DHCP, ada beberapa perangkat yang memang menggunakan IP Static seperti Access Point, PC yang dikhkusukan, juga server. Secara default, DAI akan mem-forward traffic jika IPnya masuk kedalam database DHCP Snooping, kita bisa menerapkan cara lain agar traffic dari IP Static dapat di-forward. Caranya dengan menggunakan **ARP ACCESS LIST**.

Pertama, kita kembalikan dulu IP PC menjadi Static dan pastikan hilang dari database DHCP Snooping

```
Client> ip 10.10.1.20/24
Checking for duplicate address...
PC1 : 10.10.1.20
```

Kemudian, kita buat ARP Access Listnya di switch

```
Switch(config) #arp access-list client-Static
Switch(config-arp-nacl)#permit host 10.10.1.20 mac host
00:50:79:66:68:04
Switch(config-arp-nacl)#exit
Switch(config) #ip arp inspection filter client-Static vlan 1
```

- **arp access-list (nama)** command dari ARP acces-list dan membuat nama untuk access-list tersebut
- **permit host 10.10.1.20 mac host 00:50:79:66:68:04** membolehkan IP Address 10.10.1.20 dan MAC address 00:50:79:66:68:04 pada ARP access-list

- ***ip arp inspection filter (nama) vlan 1*** memasukkan konfigurasi ARP access-list yang telah dibuat kedalam vlan yang lebih spesifik

Sekarang coba ping dari klien, seharusnya traffic tidak akan di drop.

```
VPCS> ping 10.10.1.1
84 bytes from 10.10.1.1 icmp_seq=1 ttl=255 time=7.666 ms
84 bytes from 10.10.1.1 icmp_seq=2 ttl=255 time=7.058 ms
84 bytes from 10.10.1.1 icmp_seq=3 ttl=255 time=6.145 ms
84 bytes from 10.10.1.1 icmp_seq=4 ttl=255 time=7.038 ms
```

Coba kita cek lagi di ***show ip arp inspection statistics***

Switch#sh ip arp inspection statistics				
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
----	-----	-----	-----	-----
1	8	10	0	
Vlan	DHCP Permits	ACL Permits	Probe Permits	Source MAC
Failures	-----	-----	-----	-----
----	-----	-----	-----	-----
1	3	4	0	0

Maka akan terdapat packet masuk pada bagian *ACL Permits* yang berarti traffic dari klien yang menggunakan IP Static tadi telah masuk.

Dynamic Arp Inspection menggunakan metode diatas untuk menghindari klien yang dengan sengaja merubah IP dan MACaddress nya secara Illegal. Hal tersebut adalah contoh sederhana dari ARP Spoofing.

## FHRP

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)
<b>Router role</b>		- 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.
<b>Scope</b>		Cisco proprietary	IEEE standard	Cisco proprietary
<b>Election</b>		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)
<b>Optimization features</b>	<b>Tracking</b>	yes	yes	yes
	<b>Preempt</b>	yes	yes	yes
	<b>Timer adjustments</b>	yes	yes	yes
<b>Traffic type</b>		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
<b>Timers</b>		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	
<b>Load-balancing functionality</b>		- 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.

Tabel 5 . 3 Perbandingan FHRP

Selanjutnya kita akan bahas lebih lanjut semua FHRP yang ada pada Cisco

## HSRP

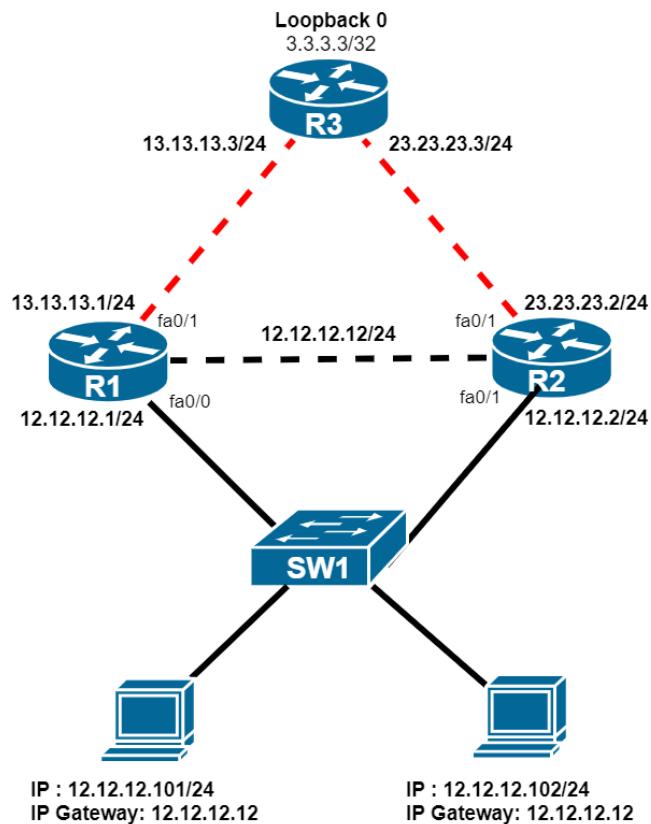
HSRP (Hot Standby Redudancy Protocol) merupakan protocol redundancy milik Cisco yang kini sudah menjadi multivendor. Menggunakan protokol UDP *port number 1985* serta menggunakan IP Multicast 224.0.0.2 dalam berkomunikasi.

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.

Berikut Lab HSRP:



Gambar 5 . 16 Lab HSRP

Di lab ini kita akan mencoba simulasi dimana terdapat 2 gateway yang menuju ke internet, kita set R2 sebagai jalur utama dan R1 jalur cadangan.

Berikut konfigurasinya:

### Konfigurasi R1

```
R1(config)#int fa0/0
R1(config-if)#ip address 12.12.12.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#int fa0/1
R1(config-if)#ip address 13.13.13.1 255.255.255.0
R1(config-if)#no shutdown
```

### Konfigurasi di R2

```
R2(config)#int fa0/0
R2(config-if)#ip address 12.12.12.2 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#int fa0/1
R2(config-if)#ip address 23.23.23.2 255.255.255.0
R2(config-if)#no shutdown
```

### Konfigurasi di R3 ( ISP )

```
R3(config)#int fa0/0
R3(config-if)#ip address 13.13.13.3 255.255.255.0
R3(config-if)#no shutdown

R3(config-if)#int fa0/1
R3(config-if)#ip address 23.23.23.3 255.255.255.0
R3(config-if)#no shutdown

R3(config-if)#int Loopback0
R3(config-if)#ip address 8.8.8.8 255.255.255.255
R3(config-if)#no shutdown
```

### SETTING DEFAULT ROUTE DI R1 dan R2

```
R1(config)#ip route 0.0.0.0 0.0.0.0 13.13.13.3
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 23.23.23.3
```

### SETTING NAT DI R1 dan R2

```
R1 & R2(config)#access-list 1 permit 12.12.12.0 0.0.0.255
R1 & R2(config)#ip nat inside source list 1 interface fa0/1 overload
R1 & R2(config)#int fa0/0
R1 & R2(config-if)#ip nat inside
R1 & R2(config-if)#int fa0/1
```

```
R1 & R2(config-if)#ip nat outside  
R1 & R2(config-if)#{
```

### PASTIKAN DARI R1 dan R2 bisa ping ke INTERNET ( 8.8.8.8)

```
R1#ping 8.8.8.8  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/14 ms
```

### 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**

```
R1(config)#int fa0/0  
R1(config-if)#standby 1 ip 12.12.12.12  
R1(config-if)#standby 1 preempt
```

```
R2(config)#int fa0/0  
R2(config-if)#standby 1 ip 12.12.12.12  
R2(config-if)#standby 1 preempt  
R2(config-if)#standby 1 priority 105
```

### KONFIGURASI DI PC

```
PC : 12.12.12.101/24 dan 12.12.12.102/24 , Gateway : 12.12.12.12
```

### PENGECEKAN

#### R1, R2: show standby brief

#### PC: ping 8.8.8.8

```
R1(config-if)#do sh stand br  
P indicates configured to preempt.  
|  
Interface   Grp   Pri P State   Active           Standby          Virtual IP  
Fa0/0       1      100 P Standby 12.12.12.2      local            12.12.12.12  
R1(config-if)#{
```

```
R2(config-if)#do sh stand br  
P indicates configured to preempt.  
|  
Interface   Grp   Pri P State   Active           Standby          Virtual IP  
Fa0/0       1      105 P Active   local            12.12.12.1      12.12.12.12
```

Shutdown interface fa0/0 pada R2, maka Fa0/1 R1 akan berubah dari standby ke active.

```
R2(config-if)#int f0/0
R2(config-if)#shutdown
*Mar 1 03:17:46.079: %LINK-5-CHANGED: Interface FastEthernet0/0,
changed state to administratively down
*Mar 1 03:17:47.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
R2(config-if)#

```

```
R1(config)#
*Mar 1 03:17:44.075: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 1 state
Standby -> Active
R1(config)#do sh standby brief
P indicates configured to preempt.
|
Interface   Grp   Pri P State      Active           Standby          Virtual IP
Fa0/0        1     100 P Active    local            unknown         12.12.12.12

```

Lalu apa yang akan terjadi jika Fa0/1 pada R2 mati?

Maka client tidak akan bisa akses jaringan internet, oleh karena itu kita bisa melakukan command **tracking** untuk memonitor route ke 0.0.0.0/0

```
R2(config)#track 1 ip route 0.0.0.0/0 reachability
R2(config)#int fa0/0
R2(config-if)#standby 1 track 1 decrement 20

```

Dengan menambahkan konfigurasi diatas, maka setiap kali default route pada R2 mati, maka priority dari R2 akan dikurangi 20 sehingga akan menjadikan R1 sebagai router Active.

## 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**.

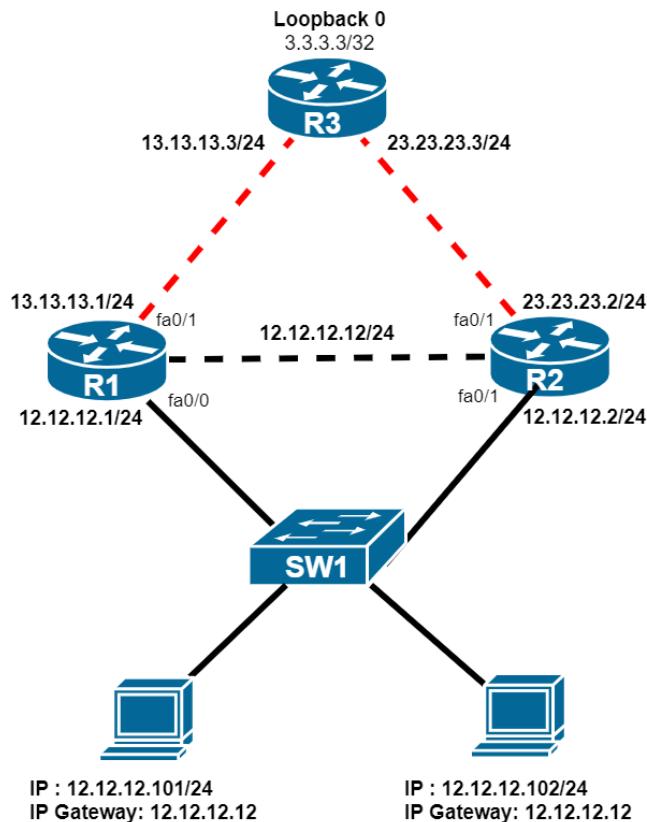
Sama seperti HSRP, VRRP juga terdapat 3 istilah yang artinya sama:

- **Master Router:** Router yang akan mengforward paket.

- **Backup Router:** Router yang akan backup jika Active Router mati.
- **VRRP Group:** Kumpulan Router anggota HSRP.

### Default priority VRRP:100

Lab VRRP sama seperti HSRP hanya saja konfigurasi HSRP dihapus.



Gambar 5 . 17 Lab VRRP

### HAPUS KONFIGURASI HSRP DARI LAB SEBELUMNYA

```

R1(config)#Int f0/0
R1(config-if)#no standby 1
R2(config)#Int f0/0
R2(config-if)#no standby 1
  
```

### KONFIGURASI VRRP DI R1

```

R1(config)#interface f0/0
R1(config-if)#vrrp 1 ip 12.12.12.12
R1(config-if)#vrrp 1 priority 110
  
```

### KONFIGURASI VRRP DI R2

```
R2 (config) #interface f0/0
R2 (config-if)#vrrp 1 ip 12.12.12.12
```

Dengan begini VRRP sudah aktif, dan kita set R1 sebagai jalur utama

## PENGECEKAN

### R1&R2: show vrrp brief

```
R1#show vrrp brief
Interface  Grp Pri Time  Own Pre State    Master addr      Group addr
Fa0/0      1   110 3570  Y  Master          12.12.12.1       12.12.12.12
R1#
```

```
R2#show vrrp brief
Interface  Grp Pri Time  Own Pre State    Master addr      Group addr
Fa1/0      1   100 3609  Y  Backup          12.12.12.1       12.12.12.12
R2#
```

Bisa kita lihat di Pre statenya, status dari R1 adalah sebagai **Master** sementara R2 sebagai **Backup**.

Kemudian kita set agar jalur dapat berpindah ke R2 jika R1 mati.

```
R1 (config) #track 1 ip route 0.0.0.0/0 reachability
R1 (config-if)#vrrp 1 track 1 decrement 20
```

Kemudian coba kita matikan R1 agar jalur berpindah ke R2

### SHUTDOWN INTERFACE F0/0 R1 (MASTER)

```
R1 (config) #int f0/0
R1 (config-if)#shutdown
*Mar  1 03:56:07.083: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Master ->
Init
*Mar  1 03:56:09.087: %LINK-5-CHANGED: Interface FastEthernet0/0,
changed state to administratively down
R1#show vrrp brief
Interface      Grp Pri Time  Own Pre State    Master addr      Group addr
Fa1/0         1   110 3570  Y  Init          0.0.0.0       12.12.12.12
```

```
*Mar  1 03:56:07.707: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Backup ->
Master
R2#show vrrp brief
Interface      Grp Pri Time  Own Pre State    Master addr      Group addr
Fa1/0         1   100 3609  Y  Master        12.12.12.2     12.12.12.12
```

Dengan begini, gateway akan pindah secara otomatis ketika R1 mati.

## 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*.

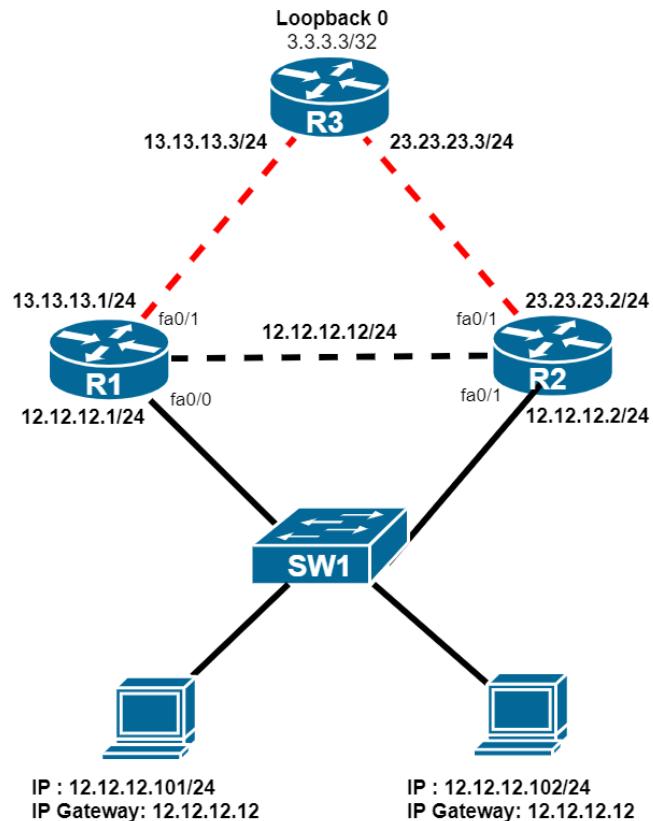
Default **Hello-timer** dari GLBP adalah **3 detik** dengan **hold time 10 detik**.

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.

### Default Priority GLBP:100

Labnya masih sama seperti sebelumnya



Gambar 5 . 18 Lab GLBP

## HAPUS KONFIGURASI VRRP DI R1 DAN R2

```
R1(config)#int f0/0
R1(config-if)#no vrrp 1
R2(config)#int f0/0
R2(config-if)#no vrrp 1
```

## KONFIGURASI DI R1

```
R1(config)#interface f0/0
R1(config-if)#glbp 1 ip 12.12.12.12
```

## KONFIGURASI DI R2

```
R2(config)#interface f0/0
R2(config-if)#glbp 1 ip 12.12.12.12
```

Dengan adanya konfigurasi diatas, maka GLBP secara otomatis aktif. Ketika ada client ingin mengirim sesuatu, maka gateway akan membagi bebannya di tiap gateway.

## PENGECEKAN

**R1&R2: show glbp brief**

**PC: traceroute ke 3.3.3.3 (internet)**

```
R1#sh glbp brief
Interface Grp Fwd Pri State Address Active router Standby router
Fa1/0    1   - 100 Active 12.12.12.12 local      12.12.12.2
Fa1/0    1   1   - Listen 0007.b400.0101 12.12.12.2  -
Fa1/0    1   2   - Active 0007.b400.0102 local      -
```

```
R2#sh glbp brief
Interface Grp Fwd Pri State Address Active router Standby router
Fa1/0    1   - 100 Standby 12.12.12.12 12.12.12.1 local
Fa1/0    1   1   - Active 0007.b400.0101 local      -
Fa1/0    1   2   - Listen 0007.b400.0102 12.12.12.1  -
```

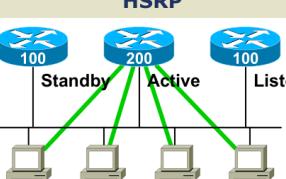
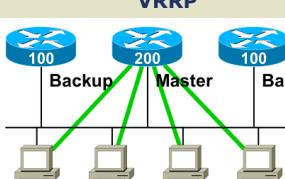
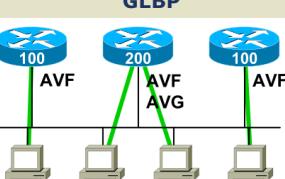
```
PC1#traceroute 3.3.3.3 Type escape sequence to abort.
Tracing the route to 3.3.3.3
1 12.12.12.2 40 msec 44 msec 20 msec
2 23.23.23.3 64 msec * 72 msec
```

```
PC2#traceroute 3.3.3.3 Type escape sequence to abort.
Tracing the route to 3.3.3.3
1 12.12.12.1 56 msec 28 msec 36 msec
2 13.13.13.3 64 msec * 88 msec
```

Berdasarkan hasil traceroute diatas, kedua jalur sudah aktif.

# 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		VRRP		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	
Round-Robin (default)		GLBP Load Balancing		
		The AVG answers host ARP requests for the virtual router with the next router in the cycle		
Host-Dependent		Host-Dependent		
		Round-robin cycling is used while a consistent AVF is maintained for each host		
Weighted		Weighted		
		Determines the proportionate share of hosts handled by each AVF		
Troubleshooting				
		show standby [brief]	show vrrp [brief]	
		show glbp [brief]	show track [brief]	

by Jeremy Stretch

v2.0

## Catatan:

---

**“BARANGSIAPA YANG MENEMPUH SUATU JALAN  
UNTUK MENUNTUT ILMU, MAKAN ALLAH AKAN  
MUDAHKAN BAGINYA JALAN KE SURGA.”**

---

-HR. Tirmidzi-

CHAPTER 6

# Networking Technologies

CCNA  
ENTERPRISE

The title is presented in a hand-drawn, sketchy style. The word "Networking" is written in teal cursive script, tilted diagonally upwards from left to right. Below it, the word "Technologies" is written in yellow cursive script, also tilted diagonally upwards. To the left of "Networking", the letters "CCNA" are written in yellow. To the right of "Technologies", the words "ENTERPRISE" are written in teal. A yellow banner at the top left contains the text "CHAPTER 6". The background features several yellow and teal hand-drawn lines and strokes that intersect and overlap, creating a dynamic, layered effect.

# **NETWORKING TECHNOLOGIES**

## **CONTENT:**

**WIRELESS**

**NETWORK AUTOMATION**

**VIRTUALIZATION**

**CLOUD**

**SOFTWARE DEFINED NETWORKING**

# 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:

1 Hz: 1 cycle	Turuan
1 Kilo-Hz: 1.000 cycle	
1 Mega-Hz: 1.000.000 cycle	
1 Giga-Hz: 1.000.000.000 cycle	

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 didunia 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 sistem

**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

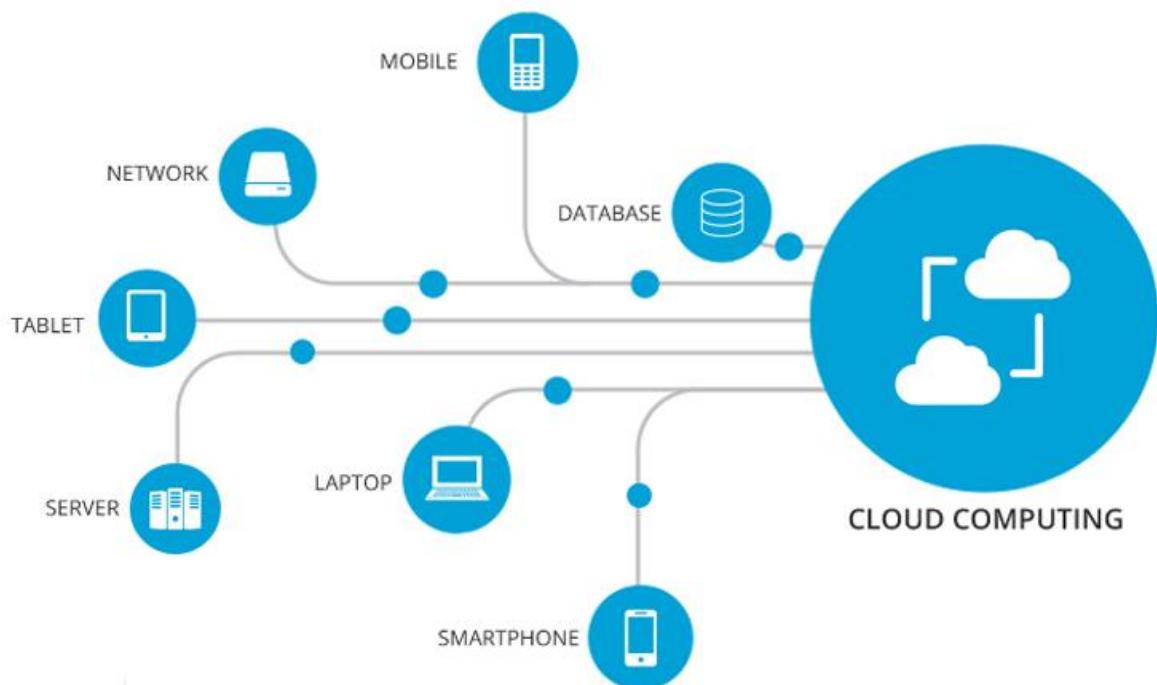
**3. Satu Pusat Serangan.**

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

# CLOUD COMPUTING

Cloud Computing merupakan istilah dari Cloud diartikan sebagai internet dan Computing diartikan sebagai komputer. Definisi dari Cloud Computing adalah sebuah proses pengolahan daya komputasi melalui jaringan internet yang memiliki fungsi agar dapat menjalankan program melalui komputer yang telah terkoneksi satu sama lain pada waktu yang sama.

Cloud Computing merupakan sebuah teknologi yang menjadikan internet sebagai pusat server untuk mengelola data dan juga aplikasi pengguna. Cloud Computing memudahkan penggunanya untuk menjalankan program tanpa harus menginstall aplikasi terlebih dahulu dan memudahkan pengguna untuk mengakses data dan informasi melalui internet.



Gambar 6 . 1 Illustrasi Cloud Computing

Beberapa keuntungan Cloud Computing:

## 1. Media Penyimpanan Terpusat pada Server

Teknologi Cloud Computing memudahkan pengguna untuk menyimpan data secara terpusat di satu server sesuai layanan yang sudah disediakan oleh Cloud Computing. Selain itu, dari segi infrastruktur pengguna tidak perlu lagi menyediakannya seperti data center, media penyimpanan, sudah tersedia secara virtual oleh Cloud Computing.

## **2. Keamanan Data**

Dalam penerapan teknologi Cloud Computing penyedia Cloud Computing telah menyediakan jaminan data sehingga data tidak mudah corrupt atau rusak , platform teknologi, jaminan ISO. Tentunya dengan Cloud Computing akan membuat data dan informasi Anda bisa lebih aman terjaga dibandingkan metode konvensional yang digunakan oleh kebanyakan orang saat ini.

## **3. Lebih Murah dan Tahan Lama**

Cloud Computing tidak memerlukan media penyimpanan storage pada hard disk eksternal karena sudah ada media penyimpanan terpusat pada server. Karena semua produk hardware atau fisik memiliki masa pemakaian dan setelah masa pemakaian tersebut biasanya akan terjadi beberapa kerusakan dan berfungsi tidak optimal dan sering terjadi error.

# **SDN**

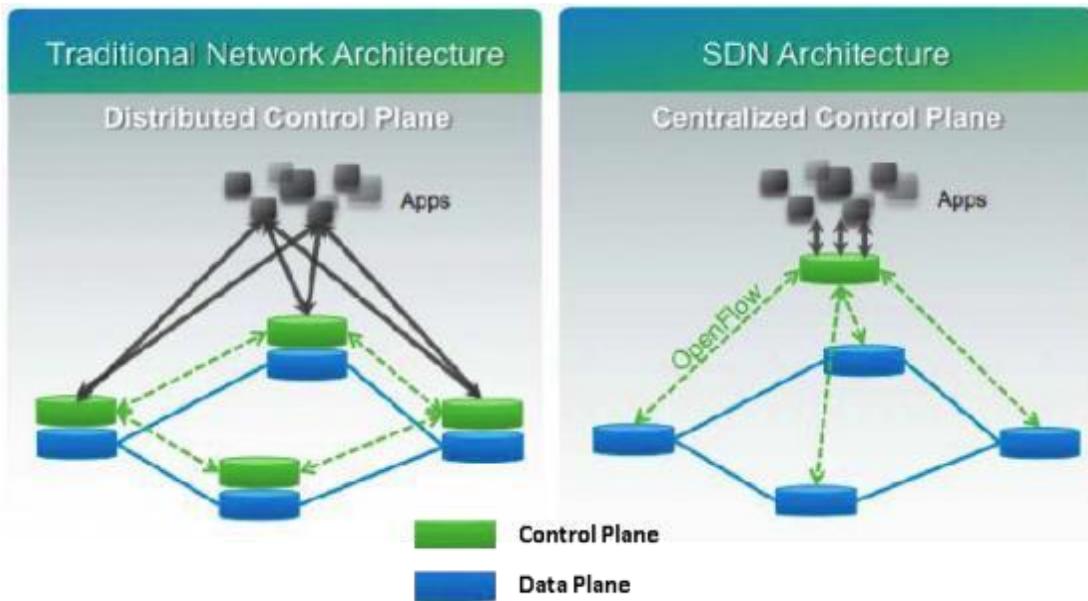
SDN atau ***Software Defined Networking***, merupakan teknologi baru di dunia networking. Teknologi ini hampir mirip seperti *Network Automation*, hanya saja konsepnya lebih bagus, penggunaannya lebih tertata dan fleksibel.

Konsep SDN ini berhubungan dengan perangkat jaringan karena SDN tidak jauh dari kata *Control Plane* dan *Data Plane* yang terdapat pada perangkat jaringan.

- *Control Plane* adalah bagian yang berfungsi untuk mengatur logika pada perangkat *networking* seperti *routing table*, pemetaan jaringan, dan sebagainya.
- *Data Plane* adalah bagian yang berfungsi untuk meneruskan paket-paket yang masuk ke suatu *port* pada perangkat *networking* menuju *port* keluar dengan berkonsultasi kepada *Control Plane*.

Jadi, konsep SDN adalah dengan memisahkan antara *Control Plane* dan *Data Plane*. Lokasi data plane berada di perangkat jaringan, sementara control plane-nya terpisah, berada di satu device yang bisa disebut sebagai *Controller*.

Hal ini berbeda dengan konsep Traditional Networking, yang dimana *Control Plane* dan *Data Plane* masih berada di perangkat jaringan.



Gambar 6 . 2 Perbedaan Arsitektur SDN dan Traditional Network

Berdasarkan gambar diatas, dapat disimpulkan. Jika kita ingin mengonfigurasi/meremote perangkat, tanpa adanya SDN kita harus meremote perangkat tersebut secara satu-persatu. Sementara jika menggunakan SDN, kita hanya perlu meremote ke satu device yang menjadi *controller* sehingga kita dapat melakukan remote device secara terpusat.

## Catatan:

# DAFTAR PUSTAKA

-Netmonk. 2020 *Apa Itu Network Automation?*

<https://netmonk.id/apa-itu-network-automation/>

-Ulum, Mas. 2012 *Apa Itu Virtualization?*

<https://blog.wowrack.co.id/2012/07/apa-itu-virtualization.html>

-Sugianto, Masim Vavai. 2011 *Keuntungan Teknologi Virtualisasi Cloud Computing*

<https://www.excellent.co.id/product-services/vmware/keuntungan-teknologi-virtualisasi-cloud-computing/>

-Pratama, Prima Nur. 2015 *Apa Itu Openflow Network Atau Software*

<http://kalengmadu.blogspot.com/2015/05/apa-itu-openflow-network-atau-software.html>

-Cisco. 2018 *Configuring VRRP*

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\\_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-vrrp.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-vrrp.html)

-Cisco. 2018 *Configuring GLBP*

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\\_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-glbp.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-glbp.html)

-Rahman, Miftah. 2014 *Wireless Fundamental*

<https://belajarcomputernetwork.com/2014/08/18/wireless-fundamentals/>

-Asfihan, Akbar. 2019 *QOS Adalah*

<https://adalah.co.id/qos/>

-Knowledge, Base. 20-- *OSPF Packet Types*

<https://sites.google.com/site/amitsciscozone/home/important-tips/ospf/ospf-packet-types>

**-Cisco. 20-- Cisco DHCP**

[https://www.cisco.com/en/US/docs/ios/12\\_4t/ip\\_addr/configuration/guide/htdhcpsv.html](https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpsv.html)

**-Danar. 2020 *Kata-Kata Motivasi Belajar Islam***

<https://www.cryptowi.com/kata-kata-motivasi-belajar-islam/>

# TENTANG PENULIS



Beliau bernama Muhammad Adib Aulia Nurkhafif, Lahir di Pekalongan 11 April 2004. Panggilannya Adib, ia tinggal di Desa Sijono, Kecamatan Warungasem, Kabupaten Batang, usianya masih enam belas 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.

Dan kini, diusianya yang masih dibilang muda, ia telah mendapatkan dua sertifikat internasional bergengsi yang pada masanya anak SMK jarang yang memiliki. Sekarang, ia masih duduk di bangku Sekolah SMK IDN dan masih kelas sepuluh.

Jika ingin bertanya atau ingin mengenal penulis lebih dalam, kalian bisa menghubunginya di:



Telepon:

+6281393195779



Email:

adibnk11@gmail.com



Instagram

adib\_nk



WhatsApp

+6282241033809



Facebook

Nur Khafif

