

Network for Intermediate

Daftar Isi:

1. Arsitektur Wide Area Network (WAN)
2. Pengenalan Subnetting dan VLSM
3. Inter Vlan Routing
4. Konfigurasi Protokol EIGRP
5. Konfigurasi Protokol OSPF
6. Konfigurasi NAT, ACL dan DHCP
7. Konfigurasi Protokol BGP
8. Studi Kasus

BAB 1

Arsitektur Wide Area Network (WAN)

Objektif :

1. Mahasiswa dapat memahami Konsep Jaringan WAN
2. Mahasiswa dapat mengenal Protokol-protokol WAN

1.1. Pendahuluan

Jaringan Komputer adalah sebuah sistem yang terdiri atas komputer, perangkat lunak dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Tujuan dari jaringan komputer adalah :

- Membagi sumber daya: contohnya berbagi pemakaian printer, CPU, memory, dan harddisk.
- Komunikasi: contohnya e-mail/surat elektronik, instans messaging, dan chatting.
- Akses informasi

Masing-masing komputer memiliki sebuah kartu jaringan atau port komunikasi lainnya, yang kemudian dihubungkan dengan kabel maupun nirkabel sebagai medium transmisi, dan ada perangkat lunak jaringan sehingga membentuk suatu jaringan komputer.

Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan, seperti contohnya Hub, Bridge, Switch, dan Router sebagai peralatan interkoneksinya.

1.2. Arsitektur Wide Area Network (WAN)

WAN (Wide Area Network) merupakan sistem jaringan yang menghubungkan antara jaringan Local Area Network (LAN) dengan jaringan luar atau WAN yang tidak dibatasi oleh daerah geografis. Pada Sistem WAN anda dapat mengakses file/data milik orang lain pada tempat lain yang cukup jauh. Untuk memenuhi hal tersebut dibutuhkan suatu alat untuk dapat menyalurkan paket data ke jaringan publik, dapat berupa Switch, Router maupun peralatan lain yang dapat dipergunakan untuk komunikasi data.

Jaringan WAN memiliki beberapa kelebihan seperti :

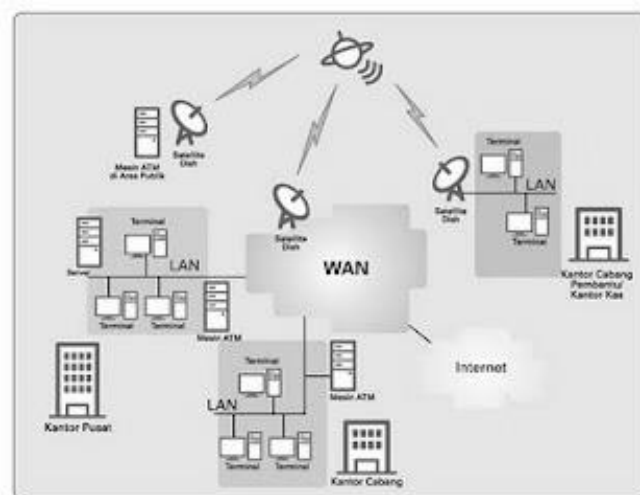
- Memiliki sistem jaringan yang sangat luas sehingga dapat berkomunikasi dengan berbagai negara, dan benua.
- Apabila terhubung dengan jaringan Internet, maka dapat melakukan transfer file dengan cepat seperti menggunakan fasilitas Email.

- Berbagi informasi melalui area yang lebih besar, dan lain – lain.

Selain memiliki kelebihan jaringan WAN tentunya juga memiliki beberapa kelemahan seperti :

- Dalam hal konfigurasi atau pengaturan jaringan WAN lebih rumit dan sulit jika dibandingkan dengan jaringan LAN dan alat – alat yang dibutuhkan sangat mahal.
- Memerlukan firewall yang baik untuk membatasi pengguna luar yang masuk sehingga dapat mengganggu jaringan.

Jaringan WAN memiliki arsitektur yang cukup berbeda dengan jaringan LAN, dimana jaringan WAN bertujuan untuk menghubungkan beberapa jaringan LAN agar dapat saling berkomunikasi dalam jarak yang cukup jauh dengan memanfaatkan jasa dari pihak ketiga atau Internet Service Provider. Berikut adalah salah satu contoh arsitektur jaringan WAN :



Arsitektur Jaringan WAN

Arsitektur WAN dari gambar diatas menunjukkan bahwa terdapat beberapa buah jaringan LAN pada masing – masing kantor cabang dan kantor pusat yang terhubung dengan pihak ketiga atau internet service provider sehingga

masing – masing LAN dapat saling berkomunikasi. Pada gambar tersebut kantor pusat berdiri sebagai server dan kantor cabang sebagai client sehingga kantor pusat dapat berbagi resource terhadap kantor cabang serta dapat memperoleh informasi – informasi yang terdapat pada kantor cabang.

1.3. Protocol WAN

Protokol jaringan adalah aturan-aturan atau tatacara yang digunakan dalam melaksanakan pertukaran data dalam sebuah jaringan. Protokol mengurus segala hal dalam komunikasi data, mulai dari kemungkinan perbedaan format data yang dipertukarkan hingga ke masalah koneksi dalam jaringan. Dalam suatu jaringan komputer, terjadi sebuah proses komunikasi antar entity atau perangkat yang berlainan sistemnya. Entity atau perangkat ini adalah segala sesuatu yang mampu menerima dan mengirim. Untuk berkomunikasi mengirim dan menerima antara dua entity dibutuhkan saling-pengertian di antara kedua belah pihak. Pengertian inilah yang dikatakan sebagai protokol. Jadi protokol adalah himpunan aturan-aturan main yang mengatur komunikasi data. Ada beberapa jenis koneksi pada jaringan WAN, diantaranya :

- **Leased Line**

Leased line yang juga disebut sebagai koneksi *Point to Point* atau *Dedicated*. Pada koneksi ini tidak membutuhkan proses *call setup* untuk memulai pengiriman paket/data. Mekanisme pengiriman paket dilakukan secara *Synchronous serial*.

- **Circuit Switching**

Koneksi ini terlebih dulu membuat *call setup* agar memulai pengiriman paket, sebagai contoh **PSTN** dan **ISDN** merupakan protocol WAN yang menerapkan koneksi Circuit Switching pada jaringan publik atau lebih dikenal sebagai Internet. Untuk mekanisme koneksi dilakukan secara *Asynchronous serial*.

- **Packet Switching**

Untuk koneksi Packet Switching kita dapat membagi bandwidth pada setiap pemakai sehingga koneksi akan lebih stabil dan dapat me-manage

bandwidth sesuai dengan jumlah pemakai. Packet Switching merupakan pengembangan dari koneksi Leased Line dan mekanisme koneksinya secara *Synchronous Serial*.

Selain itu, saat ini juga terdapat beberapa protocol WAN untuk menyediakan mekanisme komunikasi pengiriman data melalui jaringan WAN atau jaringan publik yaitu :

- **Protocol HDLC (High Level Data Link Control),**

Merupakan suatu protocol WAN yang bekerja pada data link layer dimana HDLC protocol untuk menetapkan metode enkapsulasi packet data pada *synchronous Serial*. HDLC keluaran ISO memiliki kelemahan yakni masih bersifat Singel protocol yang berarti hanya untuk komunikasi pada satu protocol, sedangkan untuk HDLC keluaran CISCO multiprotocol, dimana dapat melakukan komunikasi data dengan banyak protocol (misal IP, IPX) dan protocol yang terdapat pada layer tiga secara simultan.

- **Point to Point Protocol (PPP)**

Protocol pada data link yang dapat digunakan untuk komunikasi *Asynchronous Serial* maupun *Synchronous Serial*. PPP dapat melakukan autentikasi dan bersifat multiprotocol. Protocol ini merupakan pengembangan dari protocol SLIP (Serial Line Inteface Protocol) yaitu suatu protokol standar yang menggunakan protocol TCP/IP.

- **X.25 Protocol**

Merupakan protokol standar yang mendefinisikan hubungan antara sebuah terminal dengan jaringan Packet Switching. Untuk protokol ini dibuat untuk komunikasi data secara analog yang berarti proses pengiriman data harus mengikuti algoritma – algoritma yang ada pada Protocol X.25. Protokol ini melakukan suatu koneksi dengan membuat suatu *Circuit Virtual* dimana suatu jalur khusus pada jaringan publik yang dipakai untuk komunikasi data antar protokol X.25

- **Frame Relay**

Protokol Frame Relay untuk pengiriman data pada jaringan publik. Sama halnya dengan protokol X.25, Frame Relay juga memakai Circuit Virtual sebagai jalur komunikasi data khusus akan tetapi frame Relay masih lebih baik dari X.25 dengan berbagai kelengkapan yang ada pada Protokol Frame Relay. Encapsulasi packet pada Frame Relay menggunakan identitas koneksi yang disebut sebagai DLCI (*Data Link Connection Identifier*) yang mana pembuatan jalur Virtual Circuit akan ditandai dengan DLCI untuk koneksi antara komputer pelanggan dengan Switch atau router sebagai node Frame relay.

- **ISDN (Integrated Services Digital Network)**

Suatu layanan digital yang berjalan melalui jaringan telepon. ISDN juga protokol komunikasi data yang dapat membawa packet data baik dalam bentuk text, gambar, suara, video secara simultan. Protocol ISDN beroperasi pada bagian physical, data link, dan network.

1.4. Routing Protocol

Routing protocol adalah suatu aturan yang mempertukarkan informasi routing yang akan membentuk sebuah tabel routing sehingga pengalamatan pada paket data yang akan dikirim menjadi lebih jelas dan routing protocol mencari rute tersingkat untuk mengirimkan paket data menuju alamat yang dituju. Routing protocol dibagi menjadi 2, antara lain :

A. Interior Gateway Protocol

Interior Gateway Protocol biasanya digunakan pada jaringan yang bernama **Autonomous System**, yaitu sebuah jaringan yang berada hanya dalam satu kendali teknik yang terdiri dari beberapa subnetwork dan gateway yang saling berhubungan satu sama lain. Interior gateway diimplementasikan melalui protokol :

- **RIP**

RIP (Routing Information Protocol) termasuk dalam Distance vector protocol. Proses routing pada RIP ini, protocol memetakan daftar jarak

tempuh dari sumber melalui tiap-tiap network berdasarkan jumlah hop, yakni jumlah router yang harusalui oleh paket-paket untuk mencapai address tujuan. Jadi RIP ini akan menentukan jalur aliran data berdasarkan jarak terpendek. RIP dibatasi hanya sampai 15 hop. Broadcast di-update dalam setiap 30 detik untuk semua RIP router guna menjaga integritas. RIP cocok diimplementasikan untuk jaringan kecil.

- **OSPF**

OSPF (Open Shortest Path First) termasuk dalam Link state protocol. Dengan menggunakan routing OSPF maka router dan protocol dapat menentukan jalur transmisi data sendiri berdasarkan bandwidth. Setiap router memetakan map sederhana dari keseluruhan jaringan. Update-update dilakukan via multicast, dan dikirim. Jika terjadi perubahan konfigurasi. OSPF cocok untuk jaringan besar.

- **EIGRP**

EIGRP (Enhanced Interior Gateway Routing Protocol) adalah routing protocol yang hanya diadopsi oleh router cisco atau sering disebut sebagai proprietary protocol pada Cisco. Dimana EIGRP ini hanya bisa digunakan sesama router Cisco saja.

EIGRP sering disebut juga hybrid-distance-vector routing protocol, karena EIGRP ini terdapat dua tipe routing protocol yang digunakan, yaitu: distance vector dan link state.

- **IS-IS**

Intermediate System-to-Intermediate System (IS-IS) adalah protokol yang besar digunakan oleh perangkat jaringan untuk menentukan cara terbaik untuk datagram dipromosikan dari sisi ke sisi paket switched jaringan dan proses ini disebut routing. Menengah sistem-ke-intermediate sistem (IS-IS) membedakan antara tingkat-tingkat seperti tingkat 1 dan tingkat 2. Protokol routing dapat diubah tanpa perlu menghubungi wilayah intra routing protocol.

B. Exterior Gateway Protocol

Pada dasarnya internet terdiri dari beberapa Autonomous System yang saling berhubungan satu sama lain. Dan untuk menghubungkan Autonomous System dengan Autonomous System yang lainnya, maka Autonomous System menggunakan exterior routing protocol sebagai pertukaran informasi routingnya. Implementasi exterior gateway protocol melalui :

- **Border Gateway Protocol (BGP)**

Border Gateway Protocol (BGP) merupakan salah satu jenis routing protokol yang digunakan untuk koneksi antar Autonomous System (AS), dan salah satu jenis routing protokol yang banyak digunakan di ISP besar ataupun perbankan. BGP termasuk dalam kategori routing protokol jenis Exterior Gateway Protokol (EGP).

Dengan adanya EGP, router dapat melakukan pertukaran rute dari dan ke luar jaringan lokal Autonomous System (AS). BGP mempunyai skalabilitas yang tinggi karena dapat melayani pertukaran routing pada beberapa organisasi besar. Oleh karena itu BGP dikenal dengan routing protokol yang sangat rumit dan kompleks.

BAB 2

Pengenalan Subnetting & VLSM

Objektif :

1. Mahasiswa dapat memahami Alamat IP
2. Mahasiswa dapat memahami Pembagian Alamat IP
3. Mahasiswa dapat memahami Perhitungan Subnetting
4. Mahasiswa dapat memahami Variable Length Subnet Mask (VLSM)

2.1. IP Address

Pengertian

IP address digunakan sebagai alamat dalam hubungan antar host di internet sehingga merupakan sebuah sistem komunikasi yang universal, karena merupakan metode pengalamatan yang telah diterima di seluruh dunia. Dengan menentukan IP address berarti kita telah memberikan identitas yang universal bagi setiap interadce komputer. Jika suatu komputer memiliki lebih dari satu interface (misalkan menggunakan dua ethernet) maka kita harus memberi dua IP address untuk komputer tersebut masing-masing untuk setiap interfacenya.

Format Penulisan IP Address

IP address terdiri dari bilangan biner 32 bit yang dipisahkan oleh tanda titik setiap 8 bitnya. Tiap 8 bit ini disebut sebagai oktet. Bentuk IP address dapat ditulis sebagai berikut :

xxxxxxxx.xxxxxxxxxx.xxxxxxxxxx.xxxxxxxxxx

Jadi IP address ini mempunyai range dari 00000000.00000000.00000000.00000000 sampai 11111111.11111111.11111111.11111111. Notasi IP address dengan bilangan biner seperti ini susah untuk digunakan, sehingga sering ditulis dalam 4 bilangan desimal yang masing-masing dipisahkan oleh 4 buah titik yang lebih dikenal dengan “notasi desimal bertitik”. Setiap bilangan desimal merupakan nilai dari satu oktet IP address. Contoh hubungan suatu IP address dalam format biner dan desimal :

Desimal	167	205	206	100
Biner	10100111	11001101	11001110	01100100

Format IP Address

Dikenal dua cara pembagian IP Address, yakni: classfull dan classless addressing.

- **Classfull Addressing**

Classfull merupakan metode pembagian IP address berdasarkan kelas, dimana IP address (yang berjumlah sekitar 4 milyar)

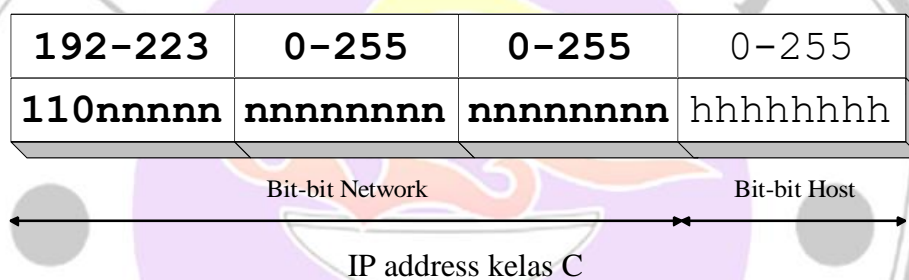
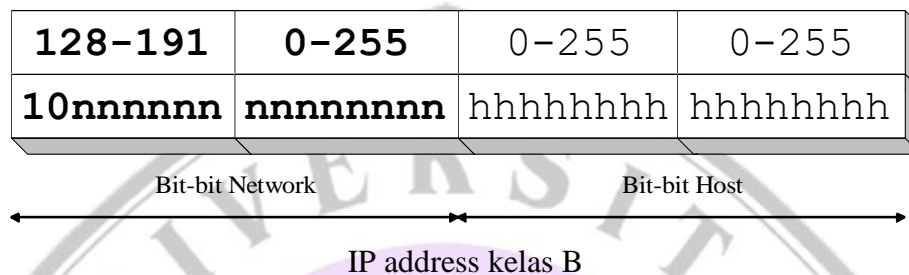
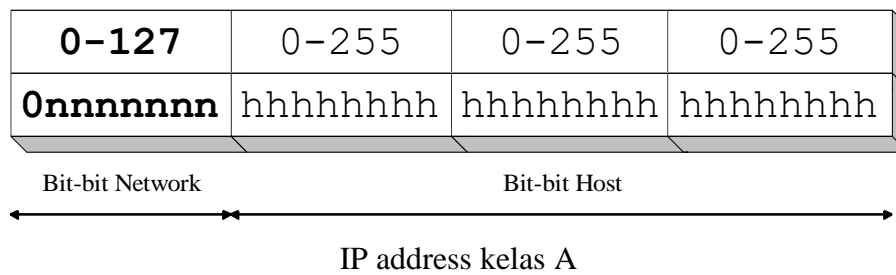
- **Classless Addressing**

Metode **classless addressing** (pengalamatan tanpa kelas) saat ini mulai banyak diterapkan, yakni dengan pengalokasian IP Address dalam notasi Classless Inter Domain Routing (**CIDR**). Istilah lain yang digunakan untuk menyebut bagian IP address yang menunjuk suatu jaringan secara lebih spesifik, disebut juga dengan **Network Prefix**.

2.2. Pembagian Kelas IP Address

Jumlah IP address yang tersedia secara teoritis adalah $255 \times 255 \times 255 \times 255$ atau sekitar 4 milyar lebih yang harus dibagikan ke seluruh pengguna jaringan internet di seluruh dunia. Pembagian kelas-kelas ini ditujukan untuk mempermudah alokasi IP Address, baik untuk host/jaringan tertentu atau untuk keperluan tertentu.

IP Address dapat dipisahkan menjadi 2 bagian, yakni bagian network (net ID) dan bagian host (host ID). Net ID berperan dalam identifikasi suatu network dari network yang lain, sedangkan host ID berperan untuk identifikasi host dalam suatu network. Jadi, seluruh host yang tersambung dalam jaringan yang sama memiliki net ID yang sama. Sebagian dari bit-bit bagian awal dari IP Address merupakan network bit/network number, sedangkan sisanya untuk host. Garis pemisah antara bagian network dan host tidak tetap, bergantung kepada kelas network. IP address dibagi ke dalam lima kelas, yaitu kelas A, kelas B, kelas C, kelas D dan kelas E. IP kelas A, B dan C dapat dilukiskan pada gambar berikut ini:



2.3. Address Khusus

Selain address yang dipergunakan untuk pengenalan host, ada beberapa jenis address yang digunakan untuk keperluan khusus dan tidak boleh digunakan untuk pengenalan host. Address tersebut adalah:

- Network Address.** Address ini digunakan untuk mengenali suatu network pada jaringan Internet.
- Broadcast Address.** Address ini digunakan untuk mengirim/menerima informasi yang harus diketahui oleh seluruh host yang ada pada suatu network.
- Multicast Address.** Diperlukan suatu mode khusus jika suatu host ingin berkomunikasi dengan beberapa host sekaligus (host group), dengan hanya mengirimkan satu datagram saja. Namun berbeda dengan mode broadcast, hanya host-host yang tergabung dalam suatu group saja yang akan

menerima datagram ini, sedangkan host lain tidak akan terpengaruh. Oleh karena itu, dikenalkan konsep multicast. Pada konsep ini, setiap group yang menjalankan aplikasi bersama mendapatkan satu multicast address. Struktur kelas multicast address dapat dilihat pada gambar berikut :

224-239	0-255	0-255	0-255
1110xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Struktur IP Address Kelas Multicast Address

Untuk keperluan multicast, sejumlah IP Address dialokasikan sebagai multicast address. Jika struktur IP Address mengikuti bentuk 1110xxxx.xxxxxxxxx.xxxxxxxxx.xxxxxxxxx (bentuk desimal 224.0.0.0 sampai 239.255.255.255), maka IP Address merupakan multicast address.

2.4. Aturan Dasar Pemilihan network ID dan host ID

Berikut adalah aturan-aturan dasar dalam menentukan network ID dan host ID yang digunakan :

- Network ID tidak boleh sama dengan 127
Network ID 127 secara default digunakan sebagai alamat loopback yakni IP address yang digunakan oleh suatu komputer untuk menunjuk dirinya sendiri.
- Network ID dan host ID tidak boleh sama dengan 255
Network ID atau host ID 255 akan diartikan sebagai alamat broadcast. ID ini merupakan alamat yang mewakili seluruh jaringan.
- Network ID dan host ID tidak boleh sama dengan 0
IP address dengan host ID 0 diartikan sebagai alamat network. Alamat network digunakan untuk menunjuk suatu jaringan bukan suatu host.
- Host ID harus unik dalam suatu network.
Dalam suatu network tidak boleh ada dua host yang memiliki host ID yang sama.

2.5. Alokasi IP Address di Jaringan

Teknik subnet merupakan cara yang biasa digunakan untuk mengalokasikan sejumlah alamat IP di sebuah jaringan (LAN atau WAN). Teknik subnet menjadi penting bila kita mempunyai alokasi IP yang terbatas misalnya hanya ada 200 IP untuk 200 komputer yang akan di distribusikan ke beberapa LAN.

Untuk memberikan gambaran, misalkan kita mempunyai alokasi alamat IP dari 192.168.1/24 untuk 254 host, maka parameter yang digunakan untuk alokasi tersebut adalah:

255.255.255.0	– subnet mask LAN
192.168.1.0	– netwok address LAN.
192.168.1.1 s/d 192.168.1.254	– IP yang digunakan host LAN
192.168.1.255	– broadcast address LAN
192.168.1.25	– contoh IP salah satu workstation di LAN.

Perhatikan bahwa,

- Alamat IP pertama 192.168.1.0 tidak digunakan untuk workstation, tapi untuk menginformasikan bahwa LAN tersebut menggunakan alamat 192.168.1.0. Istilah nya alamat IP 192.168.1.0 disebut network address.
- Alamat IP terakhir 192.168.1.255 juga tidak digunakan untuk workstation, karena digunakan untuk alamat broadcast. Alamat broadcast digunakan untuk memberikan informasi ke seluruh workstation yang berada di network 192.168.1.0 tersebut. Contoh informasi broadcast adalah informasi routing menggunakan Routing Information Protocol (RIP).
- Subnetmask LAN 255.255.255.0, dalam bahasa yang sederhana dapat diterjemahkan bahwa setiap bit “1” menunjukkan posisi network address, sedang setiap bit “0” menunjukkan posisi host address.

Konsep network address dan host address menjadi penting sekali berkaitan erat dengan subnet mask. Perhatikan dari contoh di atas maka alamat yang digunakan adalah :

192.168.1.0 network address

11000000.10101000.00000000.00000000

192.168.1.1 host ke 1

11000000.10101000.00000000.00000001

192.168.1.2 host ke 2

11000000.10101000.00000000.00000010

192.168.1.3 host ke 3

11000000.10101000.00000000.00000011

.....

192.168.1.254 host ke 254

11000000.10101000.00000000.11111110

192.168.1.255 broadcast address

11000000.10101000.00000000.11111111

Perhatikan bahwa angka 192.168.1 tidak pernah berubah sama sekali. Hal ini menyebabkan network address yang digunakan 192.168.1.0. Jika diperhatikan maka 192.168.1 terdiri dari 24 bit yang konstan tidak berubah, dan hanya 8 bit terakhir (bit hostID) yang berubah. Tidak heran kalau netmask yang digunakan adalah binary 11111111.11111111.11111111.00000000 (desimal = 255.255.255.0).

Walaupun alamat IP workstation tetap, tetapi netmask yang digunakan dimasing-masing router akan berubah-ubah bergantung pada posisi router dalam jaringan.

2.6. Subnet

Jumlah IP Address Versi 4 sangat terbatas, apalagi jika harus memberikan alamat semua host di Internet. Oleh karena itu, perlu dilakukan efisiensi dalam

penggunaan IP Address tersebut supaya dapat mengalami semaksimal mungkin host yang ada dalam satu jaringan.

Konsep subnetting dari IP Address merupakan teknik yang umum digunakan di Internet untuk mengefisienkan alokasi IP Address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP Address.

Subnetting merupakan proses memecah satu kelas IP Address menjadi beberapa subnet dengan jumlah host yang lebih sedikit, dan untuk menentukan batas network ID dalam suatu subnet, digunakan subnet mask.

Seperti yang telah dijelaskan pada bab sebelumnya, bahwa selain menggunakan metode classfull untuk pembagian IP address, kita juga dapat menggunakan metodeclassless addressing (pengalamatan tanpa klas), menggunakan notasi penulisan singkat dengan prefix.

Berikut ini daftar subnetting yang bisa dihapal dan diterapkan untuk membuat subnet.

Tabel Subnetting

Bit HostMasked	CIDR	Subnet	Net Mask	Host per Network
0	/8	1 network	255.0.0.0	16777214
1	/9	2	255.128.0.0	8388606
2	/10	4	255.192.0.0	4194302
3	/11	8	255.224.0.0	2097150
4	/12	16	255.240.0.0	1048574
5	/13	32	255.248.0.0	524286
6	/14	64	255.252.0.0	262142
7	/15	128	255.254.0.0	131070
8	/16	256	255.255.0.0	65534
9	/17	512	255.255.128.0	32766
10	/18	1024	255.255.192.0	16382
11	/19	2048	255.255.224.0	8910
12	/20	4096	255.255.240.0	4094
13	/21	8912	255.255.248.0	2046

Bit HostMasked	CIDR	Subnet	Net Mask	Host per Network
14	/22	16384	255.255.252.0	1022
15	/23	32768	255.255.254.0	510
16	/24	65536	255.255.255.0	254
17	/25	131072	255.255.255.128	126
18	/26	262144	255.255.255.192	62
19	/27	524288	255.255.255.224	30
20	/28	1048576	225.255.255.240	14
21	/29	2097152	255.255.255.248	6
22	/30	4194304	255.255.255.252	2 host
23	/31	invalid	255.255.255.254	invalid

Disamping menghafal tabel-tabel diatas, dapat juga mempelajari cara menghitung dengan mempergunakan rumus :

$$\text{Jumlah Host per Network} = 2^n - 2$$

Dimana n adalah jumlah bit tersisa yang belum diselubungi, misal Network Prefix /10, maka bit tersisa (n) adalah $32 - 10 = 22$

$$2^{22} - 2 = 4194302$$

Sedangkan untuk mencari :

$$\text{Jumlah Subnet} = 2^N$$

Dimana N adalah jumlah bit yang dipergunakan (diselubungi) atau $N = \text{Network Prefix} - 8$

Seperti contoh, bila network prefix /10, maka $N = 10 - 8 = 2 \rightarrow 2^2 = 4$

Untuk menyusun tabel Subnetting diatas, sebenarnya tidak terlalu sulit, anda bisa lebih detail memperhatikan bahwa, nilai jumlah host per network ternyata tersusun terbalik dengan jumlah subnet, Host/network dapat dengan gampang anda susun dengan rumus lain, seperti: $X \times 2 + 2 = X_n$

X = jumlah host sebelumnya, dan

X_n = jumlah host

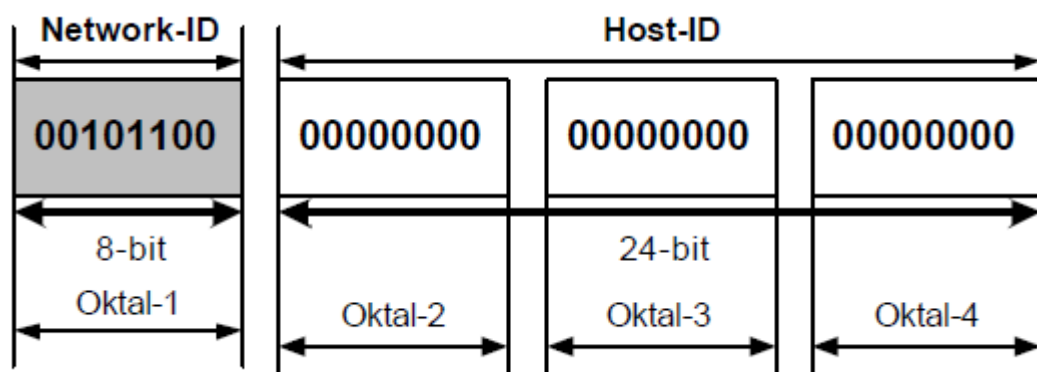
Perhatikan: $2 \times 2 + 2 = 6$, $6 \times 2 + 2 = 14$, $14 \times 2 + 2 = 30$ dst.

Subnet: $1 \times 2 = 2$, $2 \times 2 = 4$, $4 \times 2 = 8$, $8 \times 2 = 16$, dst.

Contoh perhitungan Subnetting :

Spesifikasi IP Address Kelas A:

IP Address = 44.132.1.20/8
 Subnet Mask = 255.0.0.0
 Network-ID = 44
 Host-ID = 132.1.20
 Network address = 44.0.0.0
 Broadcast address = 44.255.255.255
 Jumlah Host = $(256)^3 - 2$



Subnet Jaringan 44.0.0.0 menjadi 5 Subnetwork.

Langkah-1:

Hitung berapa bit yang dibutuhkan untuk menghasilkan 5 subnetwork ditambah 2 subnetwork (Subnetwork All-Zeros dan All-Ones).

$$7 = (2^? - 1) = (2^3 - 1) \Rightarrow 3 \text{ bit} : 111 = 7$$

Langkah-2:

- Geser garis pemisah antara bagian Network -ID dan bagian Host-ID sebanyak 3 bit.
- 8-bit pertama pada Network -ID merupakan bit Network -ID Natural dan tidak dapat diubah.
- 3-bit berikutnya pada Network -ID merupakan bit Host-ID dan dapat diubah dengan kombinasi nilai antara 0 dan 1 untuk membentuk subnetwork address yang baru.

00101100.	000	00000.00000000.00000000
00101100.	001	00000.00000000.00000000
00101100.	010	00000.00000000.00000000
00101100.	011	00000.00000000.00000000
00101100.	100	00000.00000000.00000000
00101100.	101	00000.00000000.00000000
00101100.	110	00000.00000000.00000000
00101100.	111	00000.00000000.00000000

Keterangan:

Block : Subnetwork Address yang tidak dapat digunakan. (All-Ones dan All-Zeros)

Block : Subnetwork Address yang dapat digunakan.

Langkah-3:

Ubah nilai binary menjadi nilai Decimal untuk semua network Address:

Binary	Decimal	Net.Address
0010100.00100000.00000000.00000000	= 44.32.0.0/11	Subnet-1
0010100.01000000.00000000.00000000	= 44.64.0.0/11	Subnet-2
0010100.01100000.00000000.00000000	= 44.96.0.0/11	Subnet-3
0010100.10000000.00000000.00000000	= 44.128.0.0/11	Subnet-4
0010100.10100000.00000000.00000000	= 44.160.0.0/11	Subnet-5
0010100.11000000.00000000.00000000	= 44.192.0.0/11	Subnet-6

Subnet ke-6 tidak diambil karena hanya dibutuhkan 5 Subnetwork Address.

Angka 11 pada bagian akhir merupakan jumlah bit Network -ID (8-bit Natural ditambah 3-bit hasil pergeseran sama dengan 11-bit).

Langkah-4:

Tentukan Subnet Mask (SM) untuk seluruh Subnetwork Address tersebut. Aturan menentukan Subnet Mask:

- Seluruh bit Network-ID dikonfigurasi menjadi bernilai 1.
- Seluruh bit Host-ID dikonfigurasi menjadi bernilai 0.

Binary		Decimal
11111111. 111	00000.00000000.00000000	= 255.224.0.0
11-bit Network-ID	21-bit Host-ID	

Langkah-5:

Ambil subnetwork ke-1 sebagai model subnetwork yang akan diuraikan:

Subnetwork ke-1: 44.32.0.0/11

Network Address : 44.32.0.0 (IP Address Pertama)

Subnet Mask : 255.224.0.0

Broadcast Address : 44.63.255.255 (IP Address Terakhir)

Range IP Address Host : 44.32.0.1 s.d 44.63.255.254

Jumlah Host : $[(2)^5 \times (256)^2] - 2$ Host

Catatan:

All-Zeros : Bit Network -ID yang seluruhnya bernilai = 0

All-Ones : Bit Network-ID yang seluruhnya bernilai = 1

Subnetwork Address All-Zeros dan All-Ones tidak dapat digunakan sebagai subnetwork pada jaringan LAN.

Penentuan Subnetwork dengan membatasi jumlah host tiap subnetwork, dapat dilakukandengan mengeser garis pemisah dari bit terakhir (bit ke-32).

Misal:

Jaringan Kelas A = 44.0.0.0/8

Subnetwork yang dibutuhkan adalah 5 Subnetwork dengan jumlah host untuk tiap subnetwork maksimum = 100 host.

Cara perhitungan:

Jumlah Host = $100 + 2 \Rightarrow$ Nilai 2 untuk Network dan Broadcast Address.

Bit yang dibutuhkan untuk Host : $102 \leq 2^x \Rightarrow x = 7\text{-bit}$

Bit Host yang digunakan untuk bit Network -ID:

(Bit Total = 32, bit Network-ID Natural = 8, bit-Host-ID = 7)

$(32 - 8) - 7 = 17$

Total bit Network -ID = $17 + 8 = 25\text{-bit}$

Binary		Decimal
11111111. 11111111.11111111.1		00000000
		= 255.224.0.0
25-bit Network-ID		7-bit Host-ID

No	Subnetmask (Binary)	Decimal	Tingkat
1	11111111.11111111.00000000.00000000	= 255.255.0.0	16 bit
2	11111111.11111111.11111111.00000000	= 255.255.255.0	24 bit
3	11111111.11111111.11111111.10000000	= 255.255.255.128	25 bit
4	11111111.11111111.11111111.11000000	= 255.255.255.192	26 bit
5	11111111.11111111.11111111.11100000	= 255.255.255.224	27 bit

Beberapa Contoh Subnetwork

2.7. Pengertian VLSM

VLSM atau Variable Length Subnet Mask adalah pengembangan mekanisme subnetting, dimana dalam VLSM dilakukan peningkatan dari kelemahan subnetting klasik, yang mana subnetting klasik, subnetting zeroes, dan subnetting ones tidak bisa digunakan. Jika proses subnetting yang menghasilkan beberapa sub jaringan dengan jumlah host yang sama telah dilakukan, maka ada kemungkinan di dalam segmen-segmen jaringan tersebut memiliki alamat-alamat yang tidak digunakan atau membutuhkan lebih banyak alamat. Untuk memaksimalkan penggunaan ruangan alamat yang tetap, subnetting diaplikasikan secara rekursif untuk membentuk beberapa sub jaringan dengan ukuran yang bervariasi yang diturunkan dari network identifier yang sama. Teknik subnetting ini disebut dengan Variable Length Subnetting. Sub jaringan dibuat dengan menggunakan teknik ini disebut variable Length Subnet Mask.

Cara Kerja VLSM

Dengan menggunakan Variable Length Subnetting, teknik subnetting dapat dilakukan secara rekursif maksudnya network identifier yang sebelumnya telah disubnetkan kembali. Bit-bit network identifier tersebut harus bersifat tetap dan subnetting dilakukan dengan mengambil sisa dari bit-bit host dan teknik ini pun membutuhkan routing yang baru (routing yang mendukung : RIPv2, OSPF, BPGv4).

Syarat Menggunakan VLSM

Perhitungan IP Address dengan menggunakan metode VLSM adalah metode yang berbeda dengan memberikan suatu network address lebih dari satu subnetmask. Dalam penerapan IP Address menggunakan metode VLSM agar tetap dapat berkomunikasi kedalam jaringan internet, sebaiknya pengelolaan network memenuhi syarat :

1. Routing Protocol yang digunakan harus mampu membawa informasi mengenai notasi prefix untuk setiap rute broadcastnya.
2. Semua perangkat router yang digunakan dalam jaringan harus mendukung metode VLSM yang menggunakan algoritma penerus packet informasi.

Contoh Menghitung VLSM

Studi Kasus :

Dalam suatu perusahaan terdiri dari 5 lantai. Lantai 1 membutuhkan 120 Host, Lantai 2 membutuhkan 225 Host, Lantai 3 membutuhkan 50 Host, Lantai 4 dan 5 masing-masing membutuhkan 10 Host. IP : 192.160.2.0/23

Langkah-langkah untuk memecahkan studi kasus diatas yaitu :

1. Mulailah menghitung dari yang membutuhkan host paling banyak sampai yang membutuhkan host paling sedikit.
2. Lihatlah tabel subnetting (halaman 21) sebagai acuan untuk melihat prefix berapa yang cocok untuk host yang dibutuhkan. Ingatlah kita harus mencari yang sama atau lebih dari host yang dibutuhkan, jangan sampai kurang.
3. Setelah menentukan prefix yang tepat barulah kita, menentukan Network Address, IP Host, Subnetmask dan Broadcast Address secara berurutan.
4. Yang harus diingat adalah Network Address selalu angka genap pada oktet terakhir, sedangkan Broadcast Address selalu angka ganjil.

I. Lantai 2 (225 Host)

Disini dibutuhkan 225 Host yang akan terhubung ke internet, untuk mendapatkan 225 Host atau lebih perhatikan tabel diatas. Karena yang dibutuhkan 10 Host maka cari hasil Host per Network 225 => 225 Host. Dari tabel diatas didapatkan prefixnya /24 yaitu $2^8 - 2 = 254$ Host, kenapa mesti dikurang 2? Karena untuk Network dan Broadcastnya.

Network Address : 192.160.2.0/24

IP Host : 192.160.2.1 – 192.160.2.254

Broadcast Address : 192.168.2.255

Subnet Mask : 255.255.255.0

Bit Host Masked	Prefix	Host ke 2^n	Net Mask	Host per Network
0	/8	2^{24}	255.0.0.0	16777214
1	/9	2^{23}	255.128.0.0	8388606
2	/10	2^{22}	255.192.0.0	4194302
3	/11	2^{21}	255.224.0.0	2097150
4	/12	2^{20}	255.240.0.0	1048574
5	/13	2^{19}	255.248.0.0	524286
6	/14	2^{18}	255.252.0.0	262142
7	/15	2^{17}	255.254.0.0	131070
8	/16	2^{16}	255.255.0.0	65534
9	/17	2^{15}	255.255.128.0	32766
10	/18	2^{14}	255.255.192.0	16382
11	/19	2^{13}	255.255.224.0	8910
12	/20	2^{12}	255.255.240.0	4094
13	/21	2^{11}	255.255.248.0	2046
14	/22	2^{10}	255.255.252.0	1022
15	/23	2^9	255.255.254.0	510

16	/24	2^8	255.255.255.0	254
17	/25	2^7	255.255.255.128	126
18	/26	2^6	255.255.255.192	62
19	/27	2^5	255.255.255.224	30
20	/28	2^4	225.255.255.240	14
21	/29	2^3	255.255.255.248	6
22	/30	2^2	255.255.255.252	2 host
23	/31	2^1	255.255.255.254	Invalid

II. Lantai 1 (120 Host)

Disini dibutuhkan 120 Host yang akan terhubung ke internet, untuk mendapatkan 120 Host atau lebih perhatikan tabel diatas. Karena yang dibutuhkan 120 Host maka cari hasil Host per Network 120 => 120 Host. Dari tabel diatas didapatkan prefixnya /25 yaitu $2^7 - 2 = 126$ Host.

Network Address : 192.160.3.0/25

IP Host : 192.160.3.1 – 192.160.3.126

Broadcast Address : 192.160.3.127

Subnet Mask : 255.255.255.128

III. Lantai 3 (50 Host)

Disini dibutuhkan 50 Host yang akan terhubung ke internet, untuk mendapatkan 50 Host atau lebih perhatikan tabel diatas. Karena yang dibutuhkan 50 Host maka cari hasil Host per Network 50 => 50 Host. Dari tabel diatas didapatkan prefixnya /26 yaitu $2^6 - 2 = 62$ Host.

Network Address : 192.160.3.128/25

IP Host : 192.160.3.129 – 192.160.3.190

Broadcast Address : 192.160.3.191

Subnet Mask : 255.255.255.192

IV. Lantai 4 dan 5 (10 Host)

Disini dibutuhkan 10 Host yang akan terhubung ke internet, untuk mendapatkan 10 Host atau lebih perhatikan tabel diatas. Karena yang dibutuhkan 10 Host maka cari hasil Host per Network 10 => 10Host. Dari tabel diatas didapatkan prefixnya /28 yaitu $2^4 - 2 = 14$ Host.

Lantai 4 :

Network Address : 192.160.3.192/28
IP Host : 192.160.3.193 – 192.160.3.206
Broadcast Address : 192.160.3.207
Subnet Mask : 255.255.255.240

Lantai 5 :

Network Address ; 192.160.3.208/28
IP Host : 192.160.3.209 – 192.160.3.222
Broadcast Address : 192.160.3.223
Subnet Mask : 255.255.255.240

BAB 3

Inter Vlan Routing

3.1 Objektif :

1. Mahasiswa dapat memahami Operasi Inter Vlan Routing
2. Mahasiswa dapat memahami Router-on-a-Stick Inter Vlan Routing
3. Mahasiswa dapat memahami Inter Vlan Routing menggunakan switch layer 3
4. Mahasiswa dapat memahami Troubleshoot Inter Vlan Routing

3.2 VLAN

VLAN digunakan untuk melakukan segmentasi jaringan Layer 2 yang dialihkan karena berbagai alasan. Host dalam satu VLAN tidak dapat berkomunikasi dengan host di VLAN lain kecuali ada router atau switch Layer 3 yang menyediakan layanan routing. Routing Inter VLAN adalah proses penerusan lalu lintas jaringan dari satu VLAN ke VLAN lain.

Ada tiga opsi routing Inter VLAN:

1. Perutean Inter-VLAN routing

Ini adalah solusi lama. Tidak dapat diskalakan dengan baik.

2. Router-on-a-Stick

Ini adalah solusi yang dapat diterima untuk jaringan berukuran kecil hingga sedang.

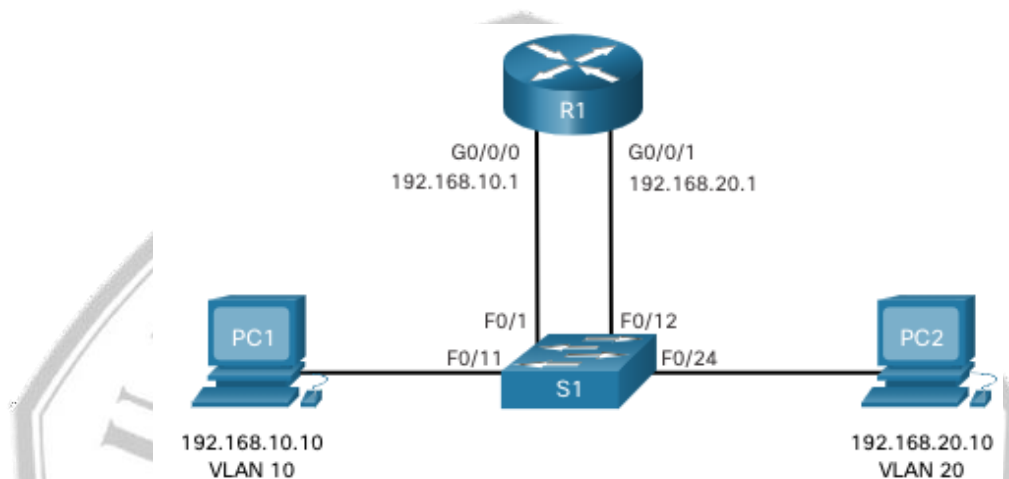
3. Switch Layer 3 yang menggunakan antarmuka virtual (SVI) yang dialihkan

Ini adalah solusi yang paling dapat diskalakan untuk organisasi menengah hingga besar.

3.2.1 Perutean Inter VLAN routing

1. Solusi perutean Inter VLAN pertama mengandalkan penggunaan router dengan beberapa antarmuka Ethernet. Setiap antarmuka router dihubungkan ke port switch di VLAN yang berbeda. Antarmuka router berfungsi sebagai gateway default ke host lokal pada subnet VLAN.
2. Perutean Inter VLAN lama yang menggunakan antarmuka fisik berfungsi, tetapi memiliki keterbatasan yang signifikan. Perutean ini tidak dapat diskalakan secara wajar karena router memiliki jumlah antarmuka fisik yang terbatas.

Catatan: Metode perutean Inter VLAN pada Gambar 3.1 tidak lagi diterapkan dalam jaringan yang dialihkan dan disertakan hanya untuk tujuan penjelasan



Gambar 3. 1 Contoh Topologi Inter Vlan

3.2.2 Router-on-a-Stick Inter-VLAN Routing

Metode perutean Inter VLAN ‘router-on-a-stick’ mengatasi keterbatasan metode perutean Inter VLAN lama. Metode ini hanya memerlukan satu antarmuka Ethernet fisik untuk merutekan lalu lintas antara beberapa VLAN pada suatu jaringan.

1. Antarmuka Ethernet router Cisco IOS dikonfigurasi sebagai jalur 802.1Q dan terhubung ke port jalur pada switch Layer 2. Secara khusus, antarmuka router dikonfigurasi menggunakan subinterface untuk mengidentifikasi VLAN yang dapat dirutekan.
2. Subinterface yang dikonfigurasi adalah antarmuka virtual berbasis perangkat lunak. Masing-masing dikaitkan dengan satu antarmuka Ethernet fisik. Subinterface dikonfigurasi dalam perangkat lunak pada router. Setiap subinterface dikonfigurasi secara independen dengan alamat IP dan penugasan VLAN.

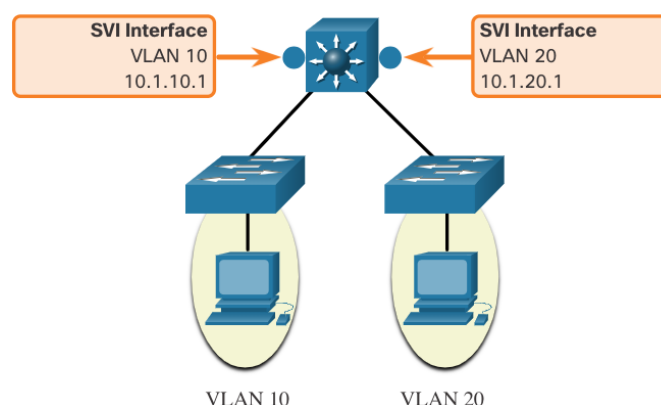
3. Ketika lalu lintas yang diberi tag VLAN memasuki antarmuka router, lalu lintas tersebut diteruskan ke subinterface VLAN. Setelah keputusan perutean dibuat berdasarkan alamat jaringan IP tujuan, router menentukan antarmuka keluar untuk lalu lintas tersebut. Jika antarmuka keluar dikonfigurasi sebagai subinterface 802.1q, bingkai data diberi tag VLAN dengan VLAN baru dan dikirim kembali melalui antarmuka fisik.

Catatan: Metode perutean Inter VLAN router-on-a-stick tidak dapat diskalakan melebihi 50 VLAN.

3.2.3 Perutean Inter VLAN pada Switch Layer 3

Metode modern untuk melakukan perutean Inter VLAN adalah dengan menggunakan switch Layer 3 dan antarmuka virtual yang diaktifkan (SVI). SVI adalah antarmuka virtual yang dikonfigurasi pada switch Layer 3, seperti yang ditunjukkan pada Gambar 3.2.

Catatan: Switch Layer 3 juga disebut switch multilayer karena beroperasi pada Layer 2 dan Layer 3. Namun, dalam kursus ini kami menggunakan istilah switch Layer 3.



Gambar 3. 2 Contoh Inter Vlan pada Switch Layer 3

SVI Inter VLAN dibuat dengan cara yang sama seperti antarmuka VLAN manajemen dikonfigurasi. SVI dibuat untuk VLAN yang ada di switch. Meskipun virtual, SVI menjalankan fungsi yang sama untuk VLAN seperti yang dilakukan antarmuka router. Secara khusus, SVI menyediakan pemrosesan Layer 3 untuk paket yang dikirim ke atau dari semua port switch yang terkait dengan VLAN tersebut.

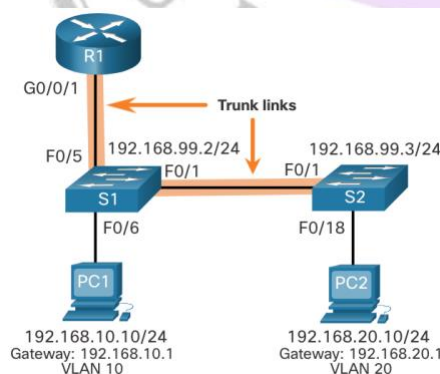
Berikut ini adalah keuntungan menggunakan switch Layer 3 untuk perutean Inter VLAN:

1. Switch Layer 3 jauh lebih cepat daripada router-on-a-stick karena semuanya dialihkan dan dirutekan melalui perangkat keras.
2. Tidak diperlukan tautan eksternal dari switch ke router untuk perutean.
3. Switch Layer 3 tidak terbatas pada satu tautan karena Layer 2 EtherChannel dapat digunakan sebagai tautan trunk antara switch untuk meningkatkan bandwidth.
4. Latensi jauh lebih rendah karena data tidak perlu meninggalkan switch untuk dirutekan ke jaringan lain.
5. Switch Layer 3 lebih umum digunakan di LAN kampus daripada router.
6. Satu-satunya kerugiannya adalah switch Layer 3 lebih mahal.

3.3 Router-on-a-Stick Inter VLAN Routing

3.3.1 Scenario Router-on-a-Stick

1. Pada Gambar 3.3, antarmuka R1 GigabitEthernet 0/0/1 terhubung ke port S1 FastEthernet 0/5. Port S1 FastEthernet 0/1 terhubung ke port S2 FastEthernet 0/1. Ini adalah tautan trunk yang diperlukan untuk meneruskan lalu lintas di dalam dan di antara VLAN.
2. Untuk merutekan di antara VLAN, antarmuka R1 GigabitEthernet 0/0/1 secara logis dibagi menjadi tiga subinterface, seperti yang ditunjukkan dalam tabel. Tabel tersebut juga menunjukkan tiga VLAN yang akan dikonfigurasi pada sakelar.
3. Asumsikan bahwa R1, S1, dan S2 memiliki konfigurasi dasar awal. Saat ini, PC1 dan PC2 tidak dapat saling melakukan ping karena berada di jaringan terpisah. Hanya S1 dan S2 yang dapat saling melakukan ping, tetapi keduanya tidak dapat dijangkau oleh PC1 atau PC2 karena keduanya juga berada di jaringan yang berbeda.
4. Agar perangkat dapat saling ping, switch wajib atau harus dikonfigurasi dengan VLAN dan trunking, dan router harus dikonfigurasi untuk melakukan operasi perutean Inter VLAN routing.



Subinterface	VLAN	IP Address
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

Gambar 3. 3 Contoh Skenario Router-on-Stick dan Tabel Pengalamatannya

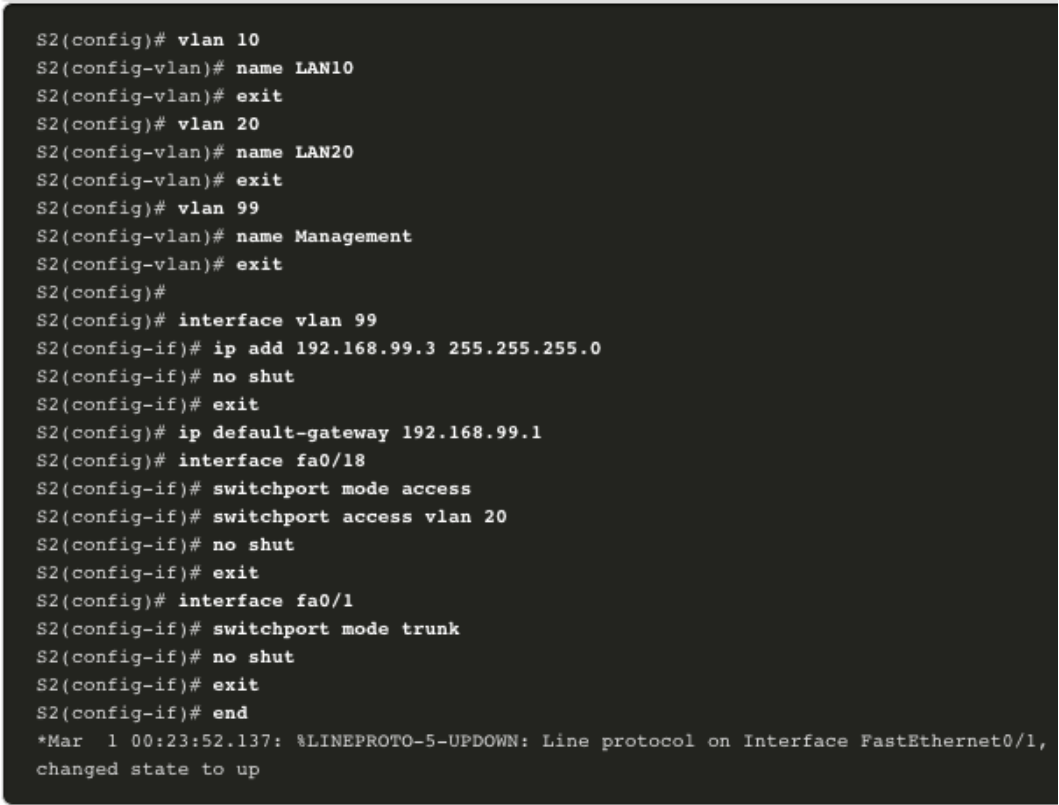
3.3.2 Konfigurasi VLAN Switch1 dan Trunking

Selesaikan langkah-langkah berikut untuk mengonfigurasi S1 dengan VLAN dan trunking:

1. Buat dan beri nama VLAN.
2. Buat antarmuka manajemen.
3. Konfigurasi port akses.
4. Konfigurasi port trunking.

3.3.3 Konfigurasi VLAN Switch2 dan Trunking

Gambar 3.4 merupakan contoh Konfigurasi untuk Switch.



```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
*Mar 1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

Gambar 3. 4 Contoh Konfigurasi Vlan pada Switch

3.3.4 Router1 Subinterface Configuration

Metode router-on-a-stick mengharuskan Anda membuat subinterface untuk setiap VLAN yang akan dirutekan. Subinterface dibuat menggunakan perintah mode konfigurasi global interface interface_id subinterface_id. Sintaks subinterface adalah antarmuka fisik yang diikuti oleh titik dan nomor subinterface. Meskipun tidak diwajibkan, biasanya nomor subinterface dicocokkan dengan nomor VLAN.

Setiap subinterface kemudian dikonfigurasi dengan dua perintah berikut:

1. **encapsulation dot1q** vlan_id [native]

Perintah ini mengonfigurasi subinterface untuk merespons lalu lintas yang dienkapsulasi 802.1Q dari vlan-id yang ditentukan. Opsi kata kunci native hanya ditambahkan untuk menyetel VLAN native ke sesuatu selain VLAN 1.

2. **ip address** ip-address subnet-mask

Perintah ini mengonfigurasi alamat IPv4 dari subinterface. Alamat ini biasanya berfungsi sebagai gateway default untuk VLAN yang teridentifikasi.

Ulangi proses untuk setiap VLAN yang akan dirutekan. Setiap subinterface router harus diberi alamat IP pada subnet unik agar perutean dapat terjadi. Setelah semua subinterface dibuat, aktifkan antarmuka fisik menggunakan perintah konfigurasi antarmuka no shutdown. Jika antarmuka fisik dinonaktifkan, semua subinterface dinonaktifkan.

Dalam konfigurasi, subinterface Router1 G0/0/1 dikonfigurasi untuk VLAN 10, 20, dan 99. Gambar 3.5 merupakan contoh konfigurasi subinterface pada Router.

```
R1(config)# interface G0/0/1.10
R1(config-subif)# Description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# Description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# Description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# Description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
R1#
```

Gambar 3. 5 Contoh Konfigurasi Subinterface pada Router

3.3.5 Verifikasi Konektivitas Antara PC1 dan PC2

Konfigurasi router-on-a-stick selesai setelah switch trunk dan subinterface router telah dikonfigurasi. Konfigurasi dapat diverifikasi dari host, router, dan switch. Dari host, verifikasi konektivitas ke host di VLAN lain menggunakan perintah ping. Sebaiknya verifikasi terlebih dahulu konfigurasi IP host saat ini menggunakan perintah ipconfig Windows host. Selanjutnya, gunakan ping untuk memverifikasi konektivitas dengan PC2 dan S1, seperti yang ditunjukkan pada Gambar 3.6. Output ping berhasil mengonfirmasi bahwa perutean Inter VLAN beroperasi.

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```

Gambar 3. 6 Contoh Verifikasi Konektifitas pada PC

3.3.6 Verifikasi Perutean Inter VLAN Router-on-a-Stick

Selain menggunakan ping antar perangkat, perintah show berikut dapat digunakan untuk memverifikasi dan memecahkan masalah konfigurasi router-on-a-stick.

- show ip route
- show ip interface brief
- show interfaces
- show interfaces trunk

Dalam Packet Tracer akan menyelesaikan tujuan berikut:

- Bagian 1: Menambahkan VLAN ke Switch
- Bagian 2: Mengonfigurasi Subinterface
- Bagian 3: Menguji konektivitas dengan Inter-VLAN Routing

3.4 Perutean Inter VLAN menggunakan Switch Layer 3

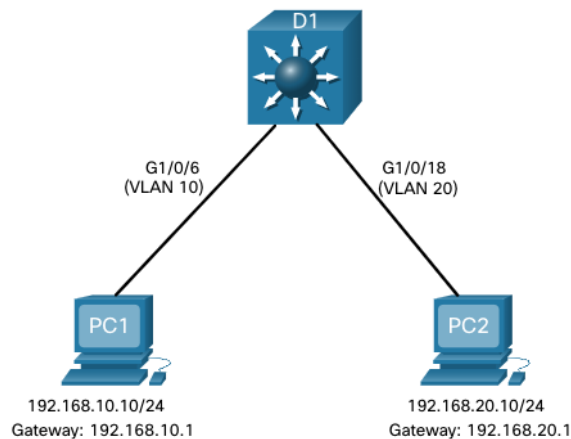
Perutean Inter VLAN menggunakan metode router-on-a-stick mudah diterapkan untuk organisasi kecil hingga menengah. Namun, perusahaan besar memerlukan metode yang lebih cepat dan lebih terukur untuk menyediakan perutean Inter VLAN. LAN kampus perusahaan menggunakan switch Layer 3 untuk menyediakan perutean Inter VLAN. Switch Layer 3 menggunakan peralihan berbasis perangkat keras untuk mencapai kecepatan pemrosesan paket yang lebih tinggi daripada router. Switch Layer 3 juga umumnya diterapkan di lemari kabel lapisan distribusi perusahaan.

Kemampuan switch Layer 3 mencakup kemampuan untuk melakukan hal berikut:

1. Merutekan dari satu VLAN ke VLAN lain menggunakan beberapa antarmuka virtual yang dialihkan (SVI).
2. Mengonversi port switch Layer 2 ke antarmuka Layer 3 (yaitu, port yang dirutekan). Port yang dirutekan mirip dengan antarmuka fisik pada router Cisco IOS.
3. Untuk menyediakan perutean Inter VLAN, switch Layer 3 menggunakan SVI. SVI dikonfigurasi menggunakan perintah `interface vlan vlan-id` yang sama yang digunakan untuk membuat SVI manajemen pada switch Layer 2. SVI Layer 3 harus dibuat untuk setiap VLAN yang dapat dirutekan.

3.4.2 Skenario Switch Layer 3

Pada Gambar 3.7, switch Layer 3, D1, terhubung ke dua host pada VLAN yang berbeda. PC1 berada di VLAN 10 dan PC2 berada di VLAN 20, seperti yang ditunjukkan. Switch Layer 3 akan menyediakan layanan routing Inter VLAN ke dua host.



Gambar 3. 7 Contoh Skenario Switch Layer 3

3.4.3 Konfigurasi Switch Layer 3

Selesaikan langkah-langkah berikut untuk mengonfigurasi S1 dengan VLAN dan trunking:

- Langkah 1 => Buat VLAN. Dalam contoh ini, VLAN 10 dan 20 digunakan.
- Langkah 2 => Buat antarmuka VLAN SVI. Alamat IP yang dikonfigurasi akan berfungsi sebagai gateway default untuk host di VLAN masing-masing.
- Langkah 3 => Konfigurasi port akses. Tetapkan port yang sesuai ke VLAN yang diperlukan.
- Langkah 4 => Aktifkan perutean IP. Keluarkan perintah konfigurasi global ip routing untuk memungkinkan lalu lintas dipertukarkan antara VLAN 10 dan 20. Perintah ini harus dikonfigurasi untuk mengaktifkan perutean antar-VAN pada sakelar Layer 3 untuk IPv4.

3.4.4 Verifikasi Perutean Inter VLAN Switch Layer 3

Perutean Inter VLAN menggunakan sakelar Layer 3 lebih mudah dikonfigurasi daripada metode router-on-a-stick. Setelah konfigurasi selesai, konfigurasi dapat diverifikasi dengan menguji konektivitas antara host.

- Dari host, verifikasi konektivitas ke host di VLAN lain menggunakan perintah **ping**. Sebaiknya verifikasi terlebih dahulu konfigurasi IP host saat ini menggunakan perintah **ipconfig** Windows host.
- Selanjutnya, verifikasi konektivitas dengan PC2 menggunakan perintah **ping** Windows host. Output **ping** yang berhasil mengonfirmasi bahwa perutean Inter VLAN sedang beroperasi.

Jika VLAN dapat dijangkau oleh perangkat Layer 3 lainnya, maka VLAN tersebut harus diiklankan menggunakan perutean statis atau dinamis. Untuk mengaktifkan perutean pada sakelar Layer 3, port yang dirutekan harus dikonfigurasi. Port yang dirutekan dibuat pada sakelar Layer 3 dengan menonaktifkan fitur switchport pada port Layer 2 yang terhubung ke perangkat Layer 3 lainnya. Secara khusus, mengonfigurasi perintah konfigurasi antarmuka no switchport pada port Layer 2 akan mengubahnya menjadi antarmuka Layer 3. Kemudian antarmuka tersebut dapat dikonfigurasi dengan konfigurasi IPv4 untuk terhubung ke router atau sakelar Layer 3 lainnya.

3.5 Troubleshoot Inter VLAN Routing

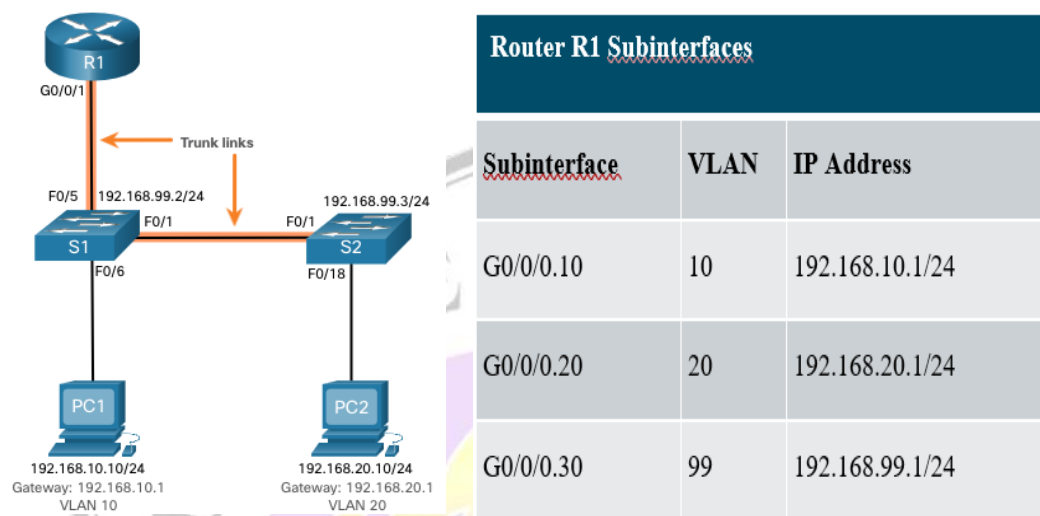
3.5.1 Masalah Umum Inter VLAN

Ada sejumlah alasan mengapa konfigurasi antar-VLAN mungkin tidak berfungsi. Semuanya terkait dengan masalah konektivitas. Pertama, periksa lapisan fisik untuk mengatasi masalah apa pun saat kabel mungkin tersambung ke port yang salah. Jika koneksinya benar, gunakan daftar dalam tabel untuk alasan umum lainnya mengapa konektivitas Inter VLAN mungkin gagal.

Jenis Masalah	Problem Solving	Verifikasi
VLAN yang hilang	<ul style="list-style-type: none"> - Buat (atau buat ulang) VLAN jika belum ada. - Pastikan port host ditetapkan ke VLAN yang benar. 	<ul style="list-style-type: none"> - show vlan [brief] - show interfaces switchport - ping
Masalah Port Trunk Switch	<ul style="list-style-type: none"> - Pastikan trunk dikonfigurasi dengan benar. - Pastikan port adalah port trunk dan diaktifkan. 	<ul style="list-style-type: none"> - show interface trunk - show running-config
Masalah Port Akses Switch	<ul style="list-style-type: none"> - Tetapkan VLAN yang benar ke port akses. - Pastikan port tersebut adalah port akses dan diaktifkan. - Host dikonfigurasi secara salah di subnet yang salah. 	<ul style="list-style-type: none"> - show interfaces switchport - show running-config interface - ipconfig
Masalah Konfigurasi Router	<ul style="list-style-type: none"> - Alamat IPv4 subinterface router dikonfigurasi secara salah. - Subinterface router ditetapkan ke ID VLAN 	<ul style="list-style-type: none"> - show ip interface brief - show interfaces

3.5.2 Skenario Troubleshoot Inter VLAN Routing

Contoh beberapa masalah perutean Inter VLAN ini sekarang akan dibahas lebih rinci. Topologi pada Gambar 3.8 merupakan Skenario Problem di Inter Vlan.



Gambar 3. 8 Contoh Skenario Problem di Inter Vlan

3.5.3 VLAN Hilang

Masalah konektivitas Inter VLAN dapat disebabkan oleh VLAN yang hilang. VLAN tersebut dapat hilang jika tidak dibuat, tidak sengaja terhapus, atau tidak diizinkan pada tautan trunk. Saat VLAN dihapus, port apa pun yang ditetapkan ke VLAN tersebut menjadi tidak aktif. Port tersebut tetap terkait dengan VLAN (dan karenanya tidak aktif) hingga Anda menentukannya ke VLAN baru atau membuat ulang VLAN yang hilang. Membuat ulang VLAN yang hilang akan secara otomatis menetapkan ulang host ke VLAN tersebut.

Gunakan perintah **show interface interface-id switchport** untuk memverifikasi keanggotaan VLAN port. Gambar 3.9 merupakan konfigurasi untuk mencari vlan yang hilang.

```
S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

Gambar 3. 9 Contoh Konfigurasi Mencari Vlan Hilang

3.5.4 Masalah Port Trunk Switch

Masalah lain untuk perutean Inter VLAN mencakup port switch yang dikonfigurasi secara salah. Dalam solusi Inter VLAN lama, hal ini dapat disebabkan saat port router penghubung tidak ditetapkan ke VLAN yang benar. Namun, dengan solusi router-on-a-stick, penyebab paling umum adalah port trunk yang dikonfigurasi secara salah.

- Pastikan port yang menghubungkan ke router dikonfigurasi dengan benar sebagai tautan trunk menggunakan perintah show interface trunk. Gambar 3.10 merupakan contoh konfigurasi untuk melihat interface trunk sebagai upaya mengetahui masalah port trunk switch.
- Jika port tersebut tidak ada dalam output, periksa konfigurasi port dengan perintah show running-config interface X untuk melihat bagaimana port tersebut dikonfigurasi.

```
S1# show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1
Port      Vlans allowed on trunk
Fa0/1     1-4094
Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,99
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,99
S1#
```

Gambar 3. 10 Contoh Konfigurasi Mengatasi Masalah Port Trunk Switch

3.5.5 Masalah Port Akses Switch

Jika ada dugaan masalah dengan konfigurasi port akses switch, gunakan perintah verifikasi untuk memeriksa konfigurasi dan mengidentifikasi masalah. Indikator umum masalah ini adalah PC memiliki konfigurasi alamat yang benar (Alamat IP, Subnet Mask, Gateway Default), tetapi tidak dapat melakukan ping ke gateway default-nya.

- Gunakan perintah **show vlan brief**, **show interface X switchport** atau **show running-config interface X** untuk memverifikasi penugasan VLAN antarmuka. Gambar 3.11 merupakan contoh konfigurasi untuk melihat interface switchport sebagai upaya mengetahui masalah port akses switch.

```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Gambar 3. 11 Contoh Konfigurasi Mengatasi Masalah Port Akses Switch

3.5.6 Masalah Konfigurasi Router

Masalah konfigurasi router-on-a-stick biasanya terkait dengan kesalahan konfigurasi subinterface.

- Verifikasi status subinterface menggunakan perintah `show ip interface brief`.
- Verifikasi VLAN mana yang digunakan setiap subinterface. Untuk melakukannya, perintah `show interfaces` berguna tetapi menghasilkan banyak output tambahan yang tidak diperlukan. Output perintah dapat dikurangi menggunakan filter perintah IOS. Dalam contoh ini yang ditunjukkan pada Gambar 3.12, menggunakan kata kunci `include` untuk mengidentifikasi bahwa hanya baris yang berisi huruf “Gig” atau “802.1Q”

```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID 1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID 100.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID 20.
GigabitEthernet0/0/1.99 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID 99.
R1#
```

Gambar 3. 12 Contoh Konfigurasi Mengatasi Masalah Konfigurasi Router

BAB 4

Konfigurasi Protokol EIGRP

Objektif :

1. Mahasiswa dapat memahami Dynamic Routing
2. Mahasiswa dapat memahami Protokol EIGRP
3. Mahasiswa dapat melakukan Konfigurasi EIGRP pada Router Cisco

4.1. Pengertian Routing

Routing adalah proses pengiriman data dari satu host dalam satu network ke host dalam network yang lain melalui suatu router. Agar router dapat mengetahui bagaimana meneruskan paket ke alamat yang dituju dengan menggunakan jalur terbaik, router menggunakan peta atau routing table. Routing Table adalah tabel yang memuat seluruh informasi IP Address dari interfaces router yang lain, sehingga router yang satu dengan router lainnya bisa berkomunikasi. Routing Table hanya memberikan informasi sedang routing algorithm yang menganalisa dan mengatur routing table. Intinya, router hanya tahu cara menghubungkan network atau subnet yang terhubung langsung dengan router tersebut.

4.2. Dynamic Routing Protocol

Pada jaringan besar yang menggunakan banyak router, dynamic routing merupakan metode yang paling umum digunakan. Karena jika menggunakan metode static routing, maka harus mengkonfigurasi semua router secara manual dan ini tidak mungkin untuk seorang network administrator. Dengan menggunakan metode static routing dibutuhkan banyak konfigurasi, sedangkan pada dynamic routing dapat mengkonfigurasi seminimal mungkin. Jadi sangat dimungkinkan metode dynamic routing untuk mengembangkan bagaimana router berkomunikasi dengan protocol yang digunakan. Dynamic IP routing adalah cara yang digunakan untuk melepaskan kewajiban mengisi masukan masukan ke routing table secara manual.

Routing protocol mengatur router-router sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi routing yang dapat mengubah isi routing table, tergantung keadaan jaringannya. Dengan cara ini, router-router mengetahui keadaan jaringan yang terakhir dan mampu meneruskan datagram ke arah yang benar. Remote network dapat dikategorikan di routing table dengan menggunakan dynamic routing protocol.

Dynamic routing protocol contohnya sebagai berikut:

a) Network Discovery

Memelihara dan meng-update tabel routing-automatic network discovery. Network discovery adalah kemampuan routing protocol untuk membagi informasi tentang jaringan dengan router lainnya dengan menggunakan routing protocol yang sama daripada mengkonfigurasi router secara static, dynamic routing dapat secara otomatis membaca jaringan dari router-router lainnya. Pemilihan jalur terbaik pada setiap jaringan terdapat pada routing table dengan menggunakan dynamic routing.

b) Maintaining Routing Tables

Setelah mengenal jaringannya, dynamic routing akan selalu meng-update dan menentukan jalur-jalurnya pada routing table. Dynamic routing tidak hanya membuat jalur terbaik ke jaringan yang berbeda, routing dinamik juga akan menentukan jalur baru yang baik jika tujuannya tidak tersedia (jika topologinya berubah), untuk ini, dynamic routing mempunyai keuntungan lebih dari static routing. Router yang menggunakan dynamic routing akan secara otomatis membagi informasi routing-nya kepada router yang lain dan menyesuaikan dengan topologi yang berubah tanpa pengaturan dari seorang network administrator.

c) IP Routing Protocols

Ada beberapa dynamic routing untuk IP. dibawah ini adalah dynamic routing yang sering digunakan, yaitu:

- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP)
- Open Short Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

4.3. Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) adalah sebuah protocol proprietary (milik) Cisco yang bekerja pada Router Cisco dan pada processor-processor route internal, yang terdapat pada switch layer core dan switch layer distributor Cisco. EIGRP adalah sebuah protocol distance-vector

yang classless dan yang sudah ditingkatkan (enhanced), yang memberikan keunggulan yang nyata dibandingkan protocol proprietary Cisco lainnya, yaitu Interior Gateway Routing Protocol (IGRP). Inilah pada dasarnya mengapa disebut Enhanced IGRP.

Seperti IGRP, EIGRP menggunakan konsep dari sebuah autonomous system untuk menggambarkan kumpulan dari router-router yang contiguous (berentetan,sebelah-menyebelah)yang menjalankan routing protocol yang sama dan berbagiinformasi routing. Tetapi tidak seperti IGRP, EIGRP memasukan subnet mask ke dalamupdate route-nya. Advertisement (pengumuman) dari informasi subnet memungkinkan penggunaan VLSM dan melakukan summarization (perangkuman) ketika merancang sebuah network.

EIGRP kadang-kadang disebut sebagai routing protocol hybrid karenamempunyai karakteristik-karakteristik baik dari protocol distance-vector maupun dari protocol link-state. Sebagai contoh, EIGRP tidak mengirimkan paket-paket link-state seperti dilakukan OSPF melainkan mengirimkan update distance-vector yangtradisional yang berisi informasi tentang network-network ditambah dengan cost (biaya) untuk mencapai mereka dari prespektif router yang melakukan pengumuman tersebut. Sebuah EIGRP memiliki karakteristik-karakteristik link-state, yaitu mensinkronisasikan routing table antara router-router tetangga pada saat dimulai startup (dijalankan), dan kemudian mengirimkan update-update yang spesifik hanya jika topologi network berubah. Ini membuat EIGRP sesuai untuk network-network yang sangat besar. EIGRP mempunyai sebuah jumlah hop maksimum.

Fitur-fitur EIGRP

Ada sejumlah fitur yang kuat dan membuat EIGRP jauh lebih baik dibandingkan IGRP dan protocol-protocol lainnya. Yang utamanya adalah sebagai berikut:

- 1) Mendukung IP, IPX, dan AppleTalk melalui modul-modul yang bersifat protocol-dependent (bergantung pada protocol).

- 2) Pencarian neighbor discovery (network tetangga) yang dilakukan dengan efisien.
- 3) Komunikasi melalui Reliable Transport Protocol (RTP).
- 4) Pemilihan jalur terbaik melalui Diffusing Update Algorithm (DUAL).

4.4. Modul Protocol Dependent

Satu dari Fitur paling menarik EIGRP adalah menyediakan dukungan routing untuk berbagai protokol layer network seperti IP, IPX dan AppleTalk. Satu-satunya routing protocol lain yang hampir menyamai EIGRP dan mendukung banyak protokol layer network adalah Intermediate System to Intermediate System (IS-IS) tetapi protokol ini hanya mendukung IP dan Connectionless Network Service (CLNS). EIGRP mendukung protokol-protokol layer Network yang berbeda melalui penggunaan modul-modul yang disebut Protocol-Dependent Modules (PDM). Setiap PDM dari EIGRP akan memelihara serangkaian tabel yang terpisah yang mengandung informasi routing yang berlaku untuk sebuah protokol yang spesifik. Ini artinya akan ada table-tabel IP/EIGRP, table-tabel IPX/EIGRP, dan table-tabel AppleTalk/EIGRP.

4.5. Neighbor Discovery

Sebelum router-router EIGRP bersedia untuk melakukan pertukaran route-route satu dengan yang lain, mereka harus menjadi tetangga-tetangga. Ada tiga kondisi yang harus dipenuhi untuk menetapkan apakah sebuah router menjadi tetangga atau tidak (Neighborship establishment):

- a) Menerima Hello atau Acknowledgement (ACK).
- b) Nomor-nomor Autonomous System (AS) cocok.
- c) Metric-metric yang identik (Nilai K).

Protocol link-state cenderung menggunakan pesan Hello untuk menetapkan neighborship karena protokol link-state dalam keadaan normal tidak mengirimkan update-update route keluar, dan karena itu harus ada semacam mekanisme untuk membantu router-router tetangga tersebut untuk menyadari ketika sebuah router

baru bergabung atau router lama pergi atau telah mati. Untuk memelihara hubungan neighborship tersebut, router-router EIGRP harus terus menerima pesan-pesan Hello dari router-router tetangga mereka.

Satu-satunya saat ketika EIGRP mengumumkan routing table-nya secara lengkap adalah ketika menemukan sebuah tetangga baru dan membentuk sebuah adjacency (hubungan atau kedekatan) dengan tetangga baru tersebut melalui pertukaran paket-paket Hello. Ketika ini terjadi, kedua router yang bertetangga tersebut akan mengumumkan routing table mereka secara lengkap kepada yang lain. Setelah masing-masing mempelajari route-route milik tetangganya, sejak saat itu hanya perubahan-perubahan pada routing table yang akan dikirimkan ke tetangganya.

Ketika router-router EIGRP menerima update-update milik tetangga mereka, router-router EIGRP menyimpannya dalam sebuah tabel topologi lokal. Tabel ini berisi semua route yang diketahui dari semua router tetangga yang dikenal, dan bekerja sebagai sumber dari mana route-route yang terbaik akan dipilih dan ditempatkan ke dalam routing table.

Istilah-istilah yang perlu diketahui:

- a) **Feasible Distance** ini adalah metric terbaik dari semua path yang menuju ke sebuah network remote, termasuk metric ke router tetangga yang mengumumkan network remote tersebut. Ini adalah route yang akan anda temukan di routing table, karena dianggap jalur terbaik. Metric dari sebuah feasible distance adalah metric yang dilaporkan oleh tetangga (disebut reported distance) ditambah metric ke router tetangga yang melaporkan route tersebut.
- b) **Reported Distance** ini adalah metric dari sebuah network remote seperti dilaporkan oleh sebuah router tetangga.
- c) **Feasible Successor** adalah sebuah jalur yang memiliki reported distance yang lebih kecil daripada feasible distance dan dianggap sebagai sebuah route backup. EIGRP akan menyimpan sampai enam buah feasible successor di tabel topologi. Hanya satu feasible successor dengan metric terbaik yang akan ditempatkan di routing

table. Dengan menggunakan feasible distance, dan memiliki beberapa feasible successor di table topologi sebagai link backup, network dapat melakukan converge (mengumpulkan routing table dari route lain) dengan cepat, dan update-update ke router tetangga manapun merupakan satu-satunya lalu lintas data yang dikirimkan dari EIGRP.

4.6. Reliable Transport Protocol (RTP)

EIGRP menggunakan sebuah protocol propriety, yang disebut Reliable Transport Protocol (RTP), untuk mengelola komunikasi dari pesan-pesan di antara router-router yang menggunakan EIGRP. Dan seperti yang terlihat dari namanya, reliabilitas adalah perhatian utama dari protocol ini. Cisco telah merancang sebuah mekanisme yang memanfaatkan multicast dan unicast untuk mengirimkan update secara cepat, dan untuk melacak penerimaan data.

Router menyimpan setiap informasi yang mereka kirimkan dengan memberikan sebuah nomor urut pada setiap paket. Dengan teknik ini, adalah mungkin bagi router untuk mendeteksi datangnya informasi yang sudah lama, informasi yang redundant, atau yang tidak urut (out-of-sequence). Kemampuan melakukan hal-hal ini adalah sangat penting karena EIGRP merupakan sebuah protokol yang diam (quiet). EIGRP bergantung pada kemampuannya melakukan sinkronisasi database-database routing pada saat mulai bekerja (startup) dan kemudian memelihara konsistensi database-nya terhadap waktu dengan cara meng-komunikasikan hanya perubahan-perubahannya saja.

Jadi, hilangnya paket-paket secara permanen, atau paket yang dieksekusi dengan tidak urut, dapat mengakibatkan rusaknya database routing tersebut.

4.7. Diffusing Update Algorithm (DUAL)

EIGRP menggunakan sebuah algoritma yang disebut Diffusing Update Algorithm (DUAL) untuk memilih dan memelihara jalur terbaik dari setiap network remote. Algoritma ini memungkinkan hal-hal berikut:

- a) Penentuan route backup jika tersedia
- b) Dukungan terhadap Variable Length Subnet Mask (VLSM)

- c) Recovery untuk route dinamis
- d) Mengirimkan keluar permintaan untuk sebuah route alternatif jika tidak ada route yang dapat ditemukan.

DUAL memberikan EIGRP waktu convergence route yang mungkin tercepat diantara semua Protokol. Kunci kecepatan convergence EIGRP ada dua:

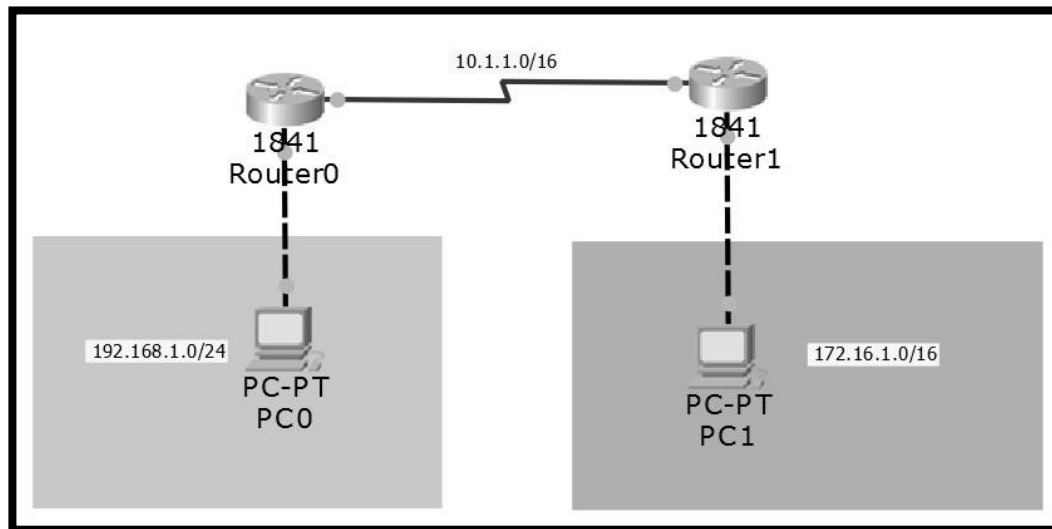
- a) Router-router EIGRP memelihara sebuah copy dari route-route milik semua tetangganya, yang mereka gunakan untuk menghitung cost mereka sendiri ke setiap network remote. Jika jalur terbaik mati atau putus, router-router EIGRP hanya akan memeriksa isi dari tabel topologinya untuk memilih route pengganti yang terbaik.
- b) Jika tidak ada alternatif yang baik di tabel topologi lokal, router-router EIGRP akan dengan cepat menanyakan kepada tetangga mereka untuk membantu mencarikannya. Mengandalkan router-router lain dan memanfaatkan informasi yang mereka sediakan, merupakan alasan karakter diffusing (membaur) dari DUAL.

Seluruh ide dari protocol Hello adalah untuk memungkinkan deteksi yang cepat dari tetangga baru atau tetangga yang mati. RTP melakukan tugas ini dengan menyediakan sebuah mekanisme yang dapat diandalkan untuk mengirimkan dan mengurutkan pesan-pesan. Dibangun diatas pondasi yang solid ini, DUAL bertanggung jawab untuk memilih dan memelihara informasi tentang jalur-jalur terbaik.

4.8. Konfigurasi EIGRP

EIGRP dapat dikonfigurasi dengan memasuki mode router configuration, dan harus menentukan nomor khusus yang disebut dengan Autonomous System Number (ASN) yang digunakan untuk keperluan pertukaran informasi antar router (neighbor relationship dan exchange routes).

Di bawah ini adalah contoh topologi yang akan digunakan untuk melakukan routing EIGRP.



Pada konfigurasi ini ditentukan ASN-nya adalah 1. Perintahnya sebagai berikut:

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-router)#network 192.168.1.0 0.0.0.255
R1(config-router)#network 10.1.1.0 0.0.255.255
```

Pada konfigurasi EIGRP, masukkan network yang ingin dikenal oleh router tetangga, yaitu 192.168.1.0 dengan subnet mask 255.255.255.0. Untuk konfigurasi EIGRP masukkan wildcard mask, seperti contoh di atas yaitu 0.0.0.255, kebalikan dari subnet mask.

BAB 5

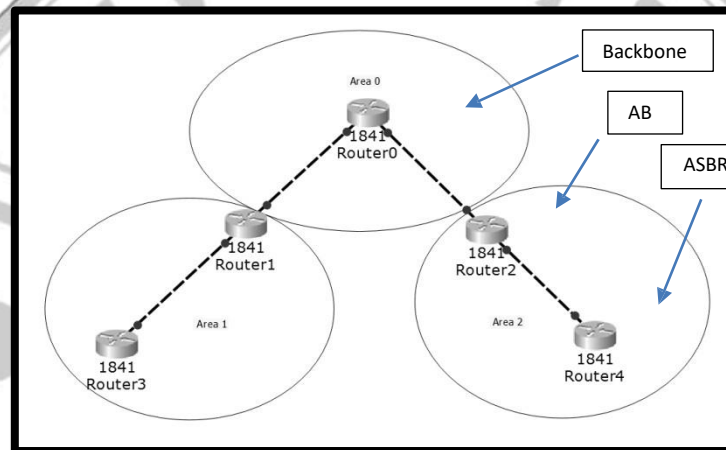
Konfigurasi Protokol OSPF

Objektif :

1. Mahasiswa dapat memahami Protokol OSPF
2. Mahasiswa dapat melakukan konfigurasi OSPF pada Router Cisco

5.1. Pengertian Open Shortest Path First (OSPF)

OSPF merupakan routing protocol berbasis link state, termasuk dalam Interior Gateway Protocol (IGP). Menggunakan Algoritma Dijkstra untuk menentukan jalur tercepat dan terbaik pada jaringan (shortest path first). Pertama, sebuah pohon jalur terpendek (shortest path tree) akan di bangun, dan kemudian routing table akan diisi dengan jalur-jalur terbaik yang dihasilkan dari pohon tersebut. OSPF melakukan coverage dengan cepat dan OSPF mendukung multiple route dengan biaya (cost) yang sama, ke tujuan yang sama. Setelah antar router bertukar informasi maka akan terbentuk database link state pada masing-masing router.



Gambar di atas menunjukkan sebuah rancangan yang sederhana yang khas OSPF. Perhatikan bahwa setiap router terhubung ke backbone yang disebut area 0, atau area backbone. OSPF harus memiliki sebuah area 0, dan semua router harus terhubung ke area ini jika memungkinkan, tetapi router-router yang menghubungkan area-area lain ke backbone di dalam sebuah Autonomous System disebut Area Border Routers (ABRs). Meskipun demikian paling sedikit satu interface harus berada di area 0.

OSPF bekerja didalam sebuah Autonomous System, tetapi juga menghubungkan banyak Autonomous System bersama. Router yang menghubungkan beberapa AS bersama disebut sebuah Autonomous System Border Router (ASBR).

Terminologi OSPF

Berikut ini adalah istilah-istilah penting OSPF yang harus dipahami:

- a) **Link** adalah sebuah network atau sebuah interface router yang ditempatkan pada sebuah network. Ketika sebuah interface ditambahkan ke proses OSPF, maka interface tersebut dianggap oleh OSPF sebagai sebuah link. Link ini atau interface, akan memiliki informasi status yang berkaitan dengannya (status hidup atau mati) dan memiliki satu atau lebih alamat IP.
- b) **Router ID (RID)** adalah sebuah alamat IP yang digunakan untuk mengidentifikasi router. Cisco memilih menggunakan RID dengan menggunakan alamat IP tertinggi dari semua interface loopback yang dikonfigurasi. Jika tidak ada interface loopback yang terkonfigurasi dengan alamat-alamat IP, OSPF akan memilih alamat IP tertinggi dari semua interface-interface fisik yang aktif.
- c) **Neighbors** adalah dua atau lebih router yang memiliki sebuah interface pada sebuah network yang sama, seperti dua router yang terhubung pada sebuah link serial point-to-point.
- d) **Adjacency** atau kedekatan adalah sebuah hubungan antara dua buah router OSPF yang mengizinkan pertukaran langsung dari update-update route.
- e) **Neighborship Database** adalah daftar dari semua router OSPF, dimana paket hello dari router tersebut sudah terlihat. Berbagai detail, termasuk router ID dan statusnya, dipelihara pada setiap router didalam Neighborship Database.
- f) **Topology Database** mengandung informasi dari semua paket Link State Advertisement (LSA) yang telah diterima untuk sebuah area. Router menggunakan informasi dari Topology Database sebagai input kedalam Algoritma Dijkstra yang menghitung jalur terpendek ke semua network.
- g) **Link State Advertisement (LSA)** adalah paket data OSPF yang mengandung informasi link-state dan informasi routing yang dibagi

diantara router-router OSPF. Sebuah router OSPF akan bertukar paket-paket LSA hanya dengan router-router dimana router tersebut telah menetapkan adjacency.

- h) **OSPF areas** adalah pengelompokan dari network dan router yang contiguous (berentetan). Semua router di area yang sama berbagi sebuah Area ID yang sama. Karena sebuah router dapat menjadi sebuah anggota dari banyak area pada satu kesempatan, maka area ID diasosiasikan dengan interface tertentu di router. Ini akan mengizinkan beberapa interface untuk masuk ke area 1, sementara interface yang lain masuk ke area 0. Semua router di area yang sama memiliki tabel topologi yang sama. Ketika mengkonfigurasi OSPF, anda harus ingat bahwa harus ada area 0, dan biasanya ini di konfigurasi untuk router-router yang terhubung ke backbone dari network. Area juga memainkan sebuah peranan dalam menetapkan sebuah organisasi network yang hierarkis, sesuatu yang meningkatkan skalabilitas OSPF.

OSPF mungkin merupakan IGP yang paling banyak digunakan. Menggunakan metode MD5 untuk autentikasi antar router sebelum menerima Link State Advertisement (LSA). Dari awal OSPF sudah mendukung CIDR dan VLSM, berbeda dengan RIP. Bahkan untuk OSPFv3 sudah mendukung untuk IPv6. OSPF tidak menggunakan TCP atau UDP melainkan IP protocol 89.

OSPF memiliki 3 table di dalam router:

a) Routing Table

Routing table biasa juga disebut sebagai Forwarding database. Database ini berisi the lowest cost untuk mencapai router-router/network-network lainnya. Setiap router mempunyai Routing table yang berbeda-beda.

b) Adjacency database

Database ini berisi semua router tetangganya. Setiap router mempunyai Adjacency database yang berbeda-beda.

c) Topological database

Database ini berisi seluruh informasi tentang router yang berada dalam satu network-nya/areanya.

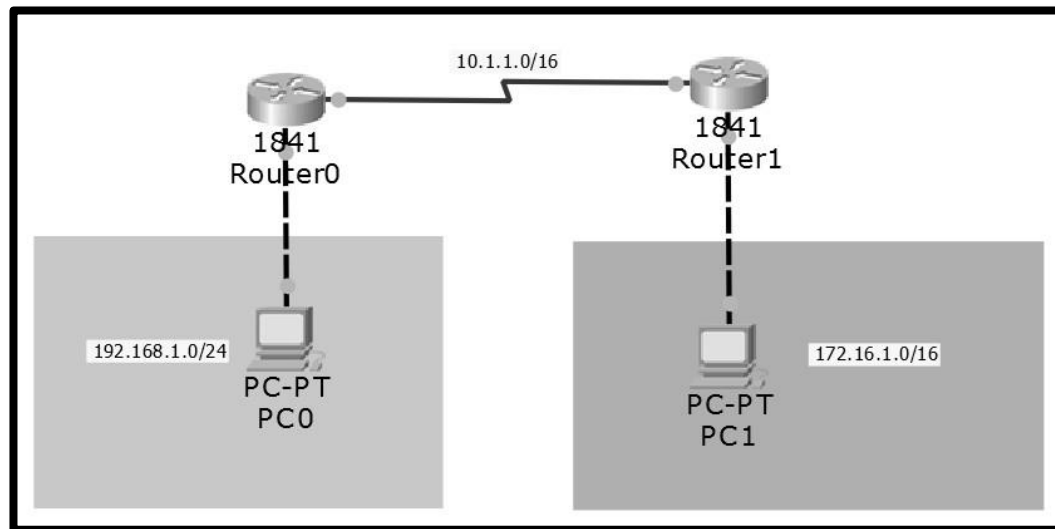
Keuntungan dari OSPF adalah:

- a) OSPF menggunakan pembagian jaringan berdasarkan konsep area-area
- b) Konsep jaringannya yang hirarki, sehingga membuat proses update informasinya lebih termanajemen dengan baik
- c) Adanya Convergence, dimana router akan menerima informasi dari router lain yang bertindak sebagai tetangganya, sehingga pada akhirnya seluruh informasi yang ada dalam sebuah jaringan dapat diketahui oleh semua router yang ada dalam jaringan
- d) Sistem update informasi routing yang cukup teratur
- e) OSPF menghemat penggunaan bandwidth jaringan
- f) OSPF menggunakan cost sebagai metric

5.2. Konfigurasi OSPF

Sama seperti konfigurasi EIGRP, konfigurasi OSPF dilakukan pada mode router configuration. Pada OSPF memasukkan Process-ID yang terdiri dari bilangan bulat positif dari 1 s.d. 65535. Process-ID ini bersifat lokal (bagi router masing-masing), pada sebuah area nilainya tidak perlu sama. Agar mudah untuk menghapalnya maka gunakan Process-ID yang sama. Sedangkan Area-ID adalah nomor area yang terkait dengan subnet. Lazimnya router-router yang satu subnet dikelompokkan dalam satu area. Area-ID terdiri dari angka bulat positif dari 0 s.d. 4294967295.

Di bawah ini adalah contoh topologi yang akan digunakan untuk melakukan routing OSPF.



```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.255.255 area 0
```

Sama seperti EIGRP, pada OSPF hanya memasukkan network yang terhubung pada router tersebut untuk mengenalkan pada router-router tetangga.

BAB 6

Konfigurasi NAT, ACL dan DHCP

Objektif :

1. Mahasiswa dapat memahami Konsep Dasar NAT
2. Mahasiswa dapat memahami Konsep Dasar DHCP
3. Mahasiswa dapat memahami Konsep Dasar ACL
4. Mahasiswa dapat memahami Konfigurasi NAT pada Router Cisco
5. Mahasiswa dapat memahami Konfigurasi DHCP pada Router Cisco
6. Mahasiswa dapat memahami Konfigurasi ACL pada Router Cisco

Konsep Dasar NAT (Network Address Translation)

NAT adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (Security), kemudahan serta fleksibilitas dalam administrasi jaringan.

NAT merupakan salah satu protokol dalam suatu sistem jaringan, NAT memungkinkan suatu jaringan dengan IP atau internet protokol yang bersifat privat IP belum teregistrasi di jaringan internet untuk mengakses jalur internet, hal ini berarti suatu alamat IP dapat mengakses internet dengan menggunakan IP Privat atau bukan menggunakan IP Public, NAT biasanya dibenamkan dalam sebuah router, NAT juga sering digunakan untuk menggabungkan atau menghubungkan dua jaringan yang berbeda, dan mentranslate atau menterjemahkan IP Privat dalam jaringan internal ke dalam jaringan yang legal network sehingga memiliki hak untuk melakukan akses data dalam sebuah jaringan. Tujuan NAT adalah mengurangi keterbatasan IPv4 dan menyembunyikan skema network internal.

Terminologi NAT

Berikut ini adalah istilah-istilah penting NAT :

- **Inside Local Address** : source address sebelum translasi (IP private)
- **Outside Local Address** : destination address sebelum translasi (IP private)
- **Inside Global Address** : inside host setelah translasi (IP public)
- **Outside Global Address** : outside destination host setelah translasi (IP public)

IP Private

Yaitu IP yang digunakan oleh organisasi secara internal dan tidak dapat dirutekan di Internet. Jadi selain dari range IP di bawah ini adalah IP Public.

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

Keuntungan NAT

Berikut ini adalah keuntungan menggunakan NAT :

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

Kerugian NAT

Berikut ini adalah kerugian menggunakan NAT :

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

Tipe NAT

Tipe NAT terdiri dari NAT Static, NAT Dynamic, dan PAT (Port Address Translation). Berikut ini adalah penjelasan mengenai :

a). NAT Static

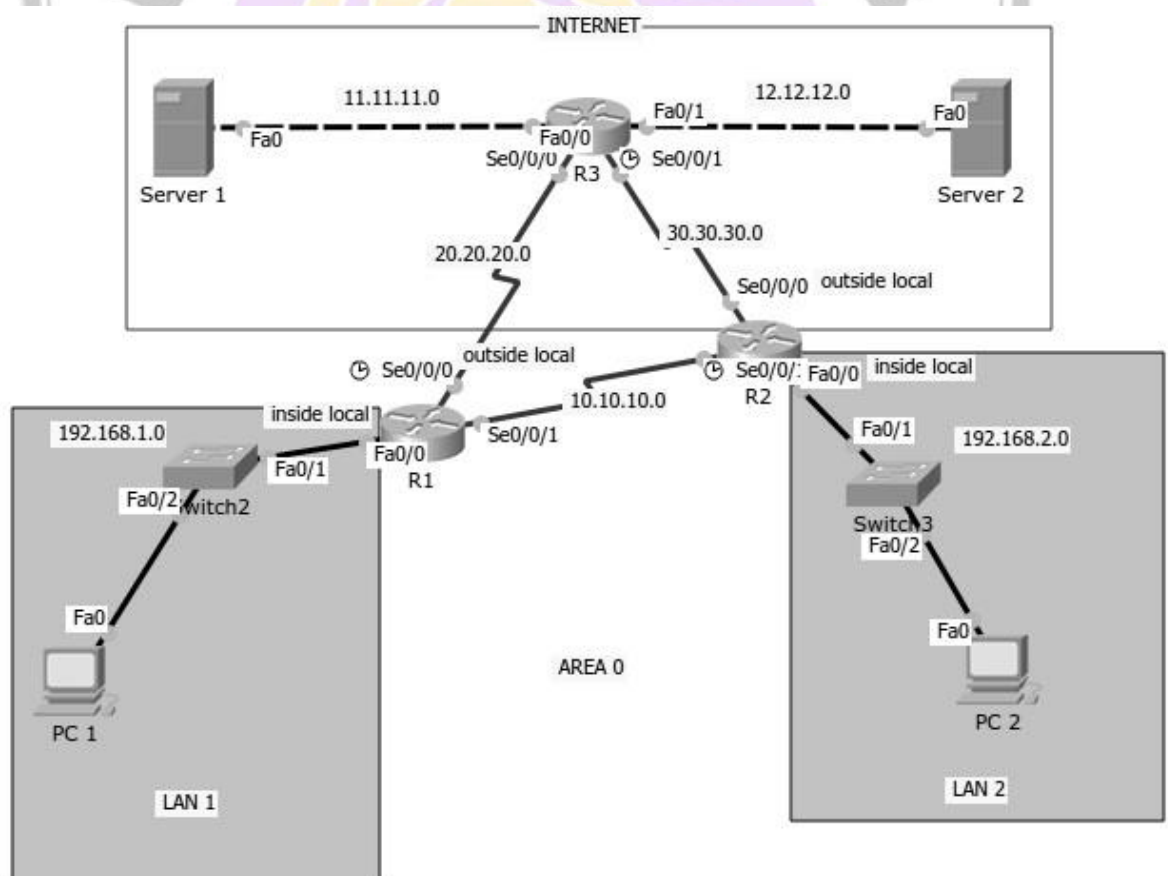
NAT Statis menggunakan table routing yang tetap, atau alokasi translasi alamat ip ditetapkan sesuai dengan alamat asal atau source ke alamat tujuan atau destination, sehingga tidak memungkinkan terjadinya pertukaran data dalam suatu alamat ip bila translasi alamat IPnya belum didaftarkan dalam table NAT. Berikut karakteristik NAT Static :

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

Konfigurasi

Contoh topologi :

Untuk mempraktikkan konsep NAT Static ini, kita asumsikan bahwa semua area jaringan (kecuali jaringan LAN 1 dan LAN 2) menggunakan routing OSPF. Jaringan LAN 1 dan LAN 2 tidak diadvertise oleh OSPF sehingga masuk Network Private, sehingga untuk mengakses Internet dibutuhkan NAT. Agar jaringan LAN 1 dan LAN 2 tidak diadvertise oleh OSPF berarti kita tidak perlu memasukkan jaringan LAN 1 dan LAN 2 pada perintah OSPF di R1 maupun R2.



Tabel Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	Se0/0/0	20.20.20.1	255.255.255.0	N/A
	Se0/0/1	10.10.10.1	255.255.255.0	N/A
R2	Fa0/0	192.168.2.1	255.255.255.0	N/A
	Se0/0/0	30.30.30.1	255.255.255.0	N/A
	Se0/0/1	10.10.10.2	255.255.255.0	N/A
R3	Fa0/0	11.11.11.1	255.255.255.0	N/A
	Fa0/1	12.12.12.1	255.255.255.0	N/A
	Se0/0/0	20.20.20.2	255.255.255.0	N/A
	Se0/0/1	30.30.30.2	255.255.255.0	N/A
Server 1	NIC	11.11.11.2	255.255.255.0	11.11.11.1
Server 1	NIC	12.12.12.2	255.255.255.0	12.12.12.1
PC 1	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC 2	NIC	192.168.2.2	255.255.255.0	129.168.2.1

Tampilan routing table R1

```

R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

```

```

Gateway of last resort is not set

```

```

      10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0/1
      11.0.0.0/24 is subnetted, 1 subnets
O       11.11.11.0 [110/65] via 20.20.20.2, 00:36:31, Serial0/0/0
      12.0.0.0/24 is subnetted, 1 subnets
O       12.12.12.0 [110/65] via 20.20.20.2, 00:36:31, Serial0/0/0
      20.0.0.0/24 is subnetted, 1 subnets
C       20.20.20.0 is directly connected, Serial0/0/0
      30.0.0.0/24 is subnetted, 1 subnets
O       30.30.30.0 [110/128] via 10.10.10.2, 00:36:21, Serial0/0/1
              [110/128] via 20.20.20.2, 00:36:21, Serial0/0/0
C       192.168.1.0/24 is directly connected, FastEthernet0/0

```

Tampilan routing table R2

```

R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0/1
    11.0.0.0/24 is subnetted, 1 subnets
O       11.11.11.0 [110/65] via 30.30.30.2, 00:44:27, Serial0/0/0
    12.0.0.0/24 is subnetted, 1 subnets
O       12.12.12.0 [110/65] via 30.30.30.2, 00:44:27, Serial0/0/0
    20.0.0.0/24 is subnetted, 1 subnets
O       20.20.20.0 [110/128] via 10.10.10.1, 00:44:27, Serial0/0/1
        [110/128] via 30.30.30.2, 00:44:27, Serial0/0/0
    30.0.0.0/24 is subnetted, 1 subnets
C       30.30.30.0 is directly connected, Serial0/0/0
C       192.168.2.0/24 is directly connected, FastEthernet0/0

```

Dari output kedua routing table di R1 dan R2, sudah tidak terlihat lagi route menuju masing-masing jaringan LAN 1 dan LAN 2.

Tabel NAT R1

Private IP	Public IP
192.168.1.2	20.20.20.20
192.168.1.3	20.20.20.30
192.168.1.4	20.20.20.40

Tabel NAT R2

Private IP	Public IP
192.168.2.2	30.30.30.20
192.168.2.3	30.30.30.30
192.168.2.4	30.30.30.40

Langkah sederhana Konfigurasi NAT Static:

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

Konfigurasi NAT Static di R1

Perintah untuk mengkonfigurasi NAT Static. Contoh IP Private 192.168.1.2 akan di NAT menjadi IP Public 20.20.20.20

```
R1(config)#interface f0/0
R1(config-if)#ip nat inside
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat inside source static 192.168.1.2 20.20.20.20
```

Konfigurasi NAT Static di R2

Perintah untuk mengkonfigurasi NAT Static. Contoh IP Private 192.168.2.2 akan di NAT menjadi IP Public 30.30.30.20

```
R2(config)#interface f0/0
R2(config-if)#ip nat inside
R2(config-if)#interface s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#ip nat inside source static 192.168.2.2 30.30.30.20
```

Verifikasi

Tes Ping dari PC 1 ke Server 1

```
PC1>ping 11.11.11.2
Pinging 11.11.11.2 with 32 bytes of data:
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Ping statistics for 11.11.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Tes Ping dari PC 2 ke Server 2

```

PC1>ping 12.12.12.2
Pinging 12.12.12.2 with 32 bytes of data:
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Ping statistics for 12.12.12.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Dari tampilan diatas dapat diketahui bahwa PC 1 dan PC 2 yang berada di Private Network dapat berkomunikasi dengan server yang berada di Internet.

Tampilan NAT table di R1

```

R1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 20.20.20.20:13      192.168.1.2:13    11.11.11.2:13      11.11.11.2:13
icmp 20.20.20.20:14      192.168.1.2:14    12.12.12.2:14      12.12.12.2:14
--- 20.20.20.20          192.168.1.2       ---                ---
--- 20.20.20.2           192.168.1.2       ---                ---

```

Tampilan NAT table di R1

```

R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 30.30.30.20:31      192.168.2.2:31    11.11.11.2:31      11.11.11.2:31
icmp 30.30.30.20:32      192.168.2.2:32    12.12.12.2:32      12.12.12.2:32
--- 30.30.30.20          192.168.2.2       ---                ---

```

b). NAT Dynamic

Konsep Dasar

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

Konfigurasi

Contoh topologi :

Topologi yang digunakan pada konfigurasi ini sama dengan topologi yang digunakan pada NAT static.

Pool NAT R1

Private IP (ACL 1)	Public IP (POOL R1)
192.168.1.0 /24	20.20.20.10 - 20.20.20.20

Pool NAT R2

Private IP (ACL 1)	Public IP (POOL R2)
192.168.2.0 /24	30.30.30.10 – 30.30.30.20

Langkah sederhana setting NAT Dynamic:

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

Setting NAT Dynamic di R1

Perintah untuk mensetting NAT Dynamic

```
R1(config)#interface f0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#
R1(config)#ip nat pool POOLR1 20.20.20.10 20.20.20.20 netmask 255.255.255.0
R1(config)#
R1(config)#ip nat inside source list 1 pool POOLR1
```

Setting NAT Dynamic di R2

Perintah untuk mensetting NAT Dynamic

```
R2(config)#interface f0/0
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#interface s0/0/1
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#exit
R2(config)#
R2(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R2(config)#
R2(config)#ip nat pool POOLR2 30.30.30.10 30.30.30.20 netmask 255.255.255.0
R2(config)#
R2(config)#ip nat inside source list 1 pool POOLR2
```

Verifikasi

Tes Ping dari PC 1 ke Server 1

```
PC1>ping 11.11.11.2
Pinging 11.11.11.2 with 32 bytes of data:
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Ping statistics for 11.11.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Tes Ping dari PC 2 ke Server 2

```
PC1>ping 12.12.12.2
Pinging 12.12.12.2 with 32 bytes of data:
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Ping statistics for 12.12.12.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Dari tampilan diatas dapat diketahui bahwa PC 1 dan PC 2 yang berada di Private Network dapat berkomunikasi dengan server yang berada di Internet.

Tampilan NAT table di R1

```
R1#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 20.20.20.10:7        192.168.1.2:7    11.11.11.2:7      11.11.11.2:7
icmp 20.20.20.10:8        192.168.1.2:8    12.12.12.2:8      12.12.12.2:8
```


Tampilan NAT table di R2

```
R2#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 30.30.30.10:24     192.168.2.2:24   11.11.11.2:24     11.11.11.2:24
icmp 30.30.30.10:25     192.168.2.2:25   12.12.12.2:25     12.12.12.2:25
```

Dari tampilan NAT tabel di R1 dapat dilihat proses translasi dari host 192.168.1.2 menjadi 20.20.20.10 dengan tujuan host 11.11.11.2 dan 12.12.12.2. Dan R2 dari host 192.168.2.2 menjadi 30.30.30.10 dengan tujuan host 11.11.11.2 dan 12.12.12.2.

c). NAT Dynamic Overload (PAT)

Konsep Dasar

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

Konfigurasi

Contoh topologi :

Topologi yang digunakan pada konfigurasi ini sama dengan topologi yang digunakan pada NAT static.

Pool NAT R1

Private IP (ACL 1)	Public IP (POOL R1)
192.168.1.0 /24	20.20.20.10

Pool NAT R2

Private IP (ACL 1)	Public IP (POOL R2)
192.168.2.0 /24	30.30.30.10

Langkah sederhana setting NAT Dynamic PAT:

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

Setting NAT Dynamic PAT di R1

Perintah untuk mensetting NAT Dynamic PAT.

```
R1(config)#interface f0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#
R1(config)#ip nat pool POOLR1 20.20.20.10 20.20.20.10 netmask 255.255.255.0
R1(config)#
R1(config)#ip nat inside source list 1 pool POOLR1 overload
```

Setting NAT Dynamic PAT di R2

Perintah untuk mensetting NAT Dynamic PAT.

```
R2(config)#interface f0/0
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#interface s0/0/1
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#exit
R2(config)#
R2(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R2(config)#
R2(config)#ip nat pool POOLR2 30.30.30.10 30.30.30.10 netmask 255.255.255.0
R2(config)#
R2(config)#ip nat inside source list 1 pool POOLR2 overload
```

Verifikasi

Tes Ping dari PC 1 ke Server 1

```
PC1>ping 11.11.11.2
Pinging 11.11.11.2 with 32 bytes of data:
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Reply from 11.11.11.2: bytes=32 time=1ms TTL=254
Reply from 11.11.11.2: bytes=32 time=0ms TTL=254
Ping statistics for 11.11.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Tes Ping dari PC 2 ke Server 2

```
PC1>ping 12.12.12.2
Pinging 12.12.12.2 with 32 bytes of data:
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Reply from 12.12.12.2: bytes=32 time=1ms TTL=254
Reply from 12.12.12.2: bytes=32 time=0ms TTL=254
Ping statistics for 12.12.12.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Dari tampilan diatas dapat diketahui bahwa PC 1 dan PC 2 yang berada di Private Network dapat berkomunikasi dengan server yang berada di Internet.

Tampilan NAT table di R1

```
R1#show ip nat translations
Pro Inside global      Inside local           Outside local          Outside global
icmp 20.20.20.10:10     192.168.1.2:10        11.11.11.2:10         11.11.11.2:10
icmp 20.20.20.10:11     192.168.1.2:11        12.12.12.2:11         12.12.12.2:11
icmp 20.20.20.10:12     192.168.1.2:12        11.11.11.1:12         11.11.11.1:12
```

Tampilan NAT table di R1

```
R2#show ip nat translations
Pro Inside global      Inside local           Outside local          Outside global
icmp 30.30.30.10:28     192.168.2.2:28        11.11.11.2:28         11.11.11.2:28
icmp 30.30.30.10:29     192.168.2.2:29        12.12.12.2:29         12.12.12.2:29
icmp 30.30.30.10:30     192.168.2.2:30        11.11.11.1:30         11.11.11.1:30
```

Dari tampilan NAT tabel di R1 dapat dilihat proses translasi dari host 192.168.1.2 menjadi 20.20.20.10 dengan tujuan host 11.11.11.2 dan 12.12.12.2. Dengan menggunakan single-IP address Public, maka yang membedakan tiap sessionnya yaitu port. Dan begitu pun dengan tampilan NAT table di R2.

Konsep Dasar DHCP (Dynamic Host Configuration Protocol)

DHCP adalah protokol berdasarkan arsitektur client/server yang diaplikasikan untuk mempermudah pengalokasian IP Address pada suatu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP diharuskan secara manual memberikan IP Address kepada semua komputer. Jika DHCP terpasang pada jaringan lokal, maka semua komputer yang terhubung ke jaringan akan memperoleh IP Address secara otomatis dari DHCP server. Selain IP Address banyak parameter jaringan yang dapat diberikan oleh DHCP, misalnya default gateway dan DNS server.

Proses pertukaran data antara DHCP Server dan DHCP klien



Konfigurasi

Contoh Topologi :

Topologi yang digunakan pada konfigurasi ini sama dengan topologi yang digunakan pada NAT static.

Login console ke R1 dan R2 untuk mempraktikkan konfigurasi DHCP

Untuk mensetting DHCP di R1, berikut ini perintah yang digunakan :

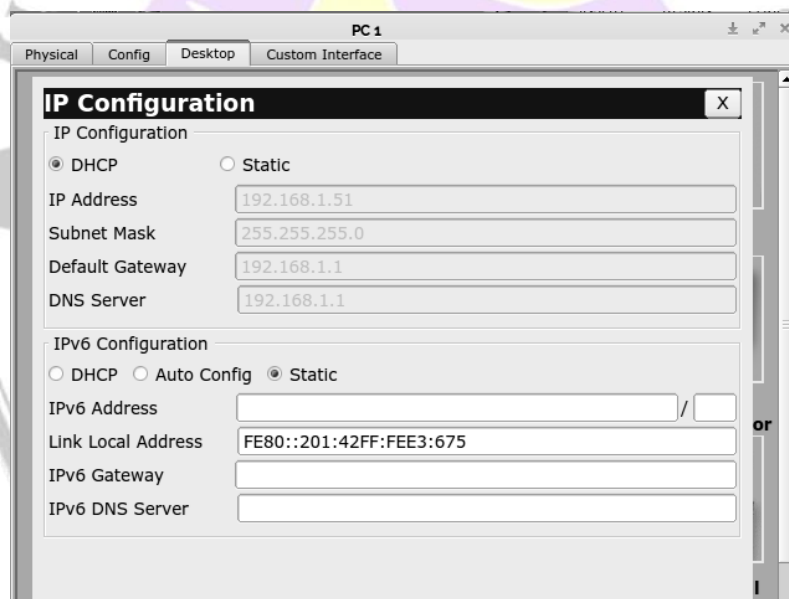
```
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.50
R1(config)#ip dhcp pool Pool_R1
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#dns-server 192.168.1.1
```

Keterangan:

- excluded-address : untuk menentukan IP yang tidak boleh di lease oleh DHCP, biasanya berupa IP static untuk server / printer
- pool : tentukan nama pool DHCP, misal untuk network 192.168.1.0 namanya Pool_R1
- network : menentukan network DHCP
- default-router : menentukan default gateway untuk klien
- dns-server : menentukan dns server untuk klien

Verifikasi

Klik **PC 1** -> Pilih **Desktop** -> Pilih **IP Configuration** -> Pilih **DHCP**



Keamanan Menggunakan ACL

Dalam dunia jaringan cukup banyak *threats* (potensi serangan). Berbagai *threats* yang mengancam network security seperti contoh nya *viruses, worms, trojan horses, spyware, adware, hacker attacks, DoS*, dan masih banyak lainnya.

Pada bab ini akan membahas tentang keamanan jaringan dengan menggunakan Cisco Access List (ACL). Cisco ACL merupakan sebuah metode yang digunakan untuk menyeleksi paket-paket yang keluar masuk *network*. Ada beberapa tipe ACL, yaitu :

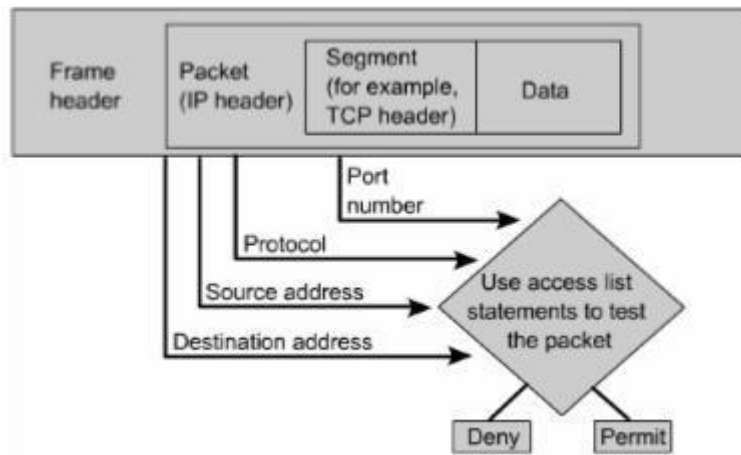
- Standard IP
- Extended IP
- IPX
- AppleTalk

Pada materi ini kita akan membahas ACL jenis *Standard* dan *Extended IP*.

Penjelasan Cisco Access List (ACL)

Untuk mem-filter trafik jaringan, ACL menentukan jika paket itu dilewatkan atau diblok pada interface router. Router ACL membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor port.

ACL harus didefinisikan berdasarkan protokol, arah atau port. Untuk mengontrol aliran trafik pada interface, ACL harus didefinisikan setiap protokol pada interface. ACL kontrol trafik pada satu arah dalam interface. Dua ACL terpisah harus dibuat untuk mengontrol trafik inbound dan outbound. Setiap interface boleh memiliki banyak protokol dan arah yang sudah didefinisikan. Jika router mempunyai dua interface diberi IP, AppleTalk dan IPX, maka dibutuhkan 12 ACL. Minimal harus ada satu ACL setiap interface.



Cisco ACL memeriksa paket pada header upper-layer



One list per interface, per direction, and per protocol

Grup access list dalam Router

Berikut ini adalah fungsi dari ACL:

- Membatasi trafik jaringan dan meningkatkan unjuk kerja jaringan. Misalnya, ACL memblokir trafik video, sehingga dapat menurunkan beban jaringan dan meningkatkan unjuk kerja jaringan.
- Mengatur aliran trafik. ACL mampu memblokir update routing. Jika update tidak dibutuhkan karena kondisi jaringan, maka bandwidth dapat dihemat.
- Mampu memberikan dasar keamanan untuk akses ke jaringan. Misalnya, host A tidak diijinkan akses ke jaringan HRD dan host B diijinkan.
- Memutuskan jenis trafik mana yang akan dilewatkan atau diblok melalui interface router. Misalnya, trafik email dilayani, trafik telnet diblok.
- Mengontrol daerah-daerah dimana klien dapat mengakses jaringan.

- Memilih host-hots yang diijinkan atau diblok akses ke segmen jaringan. Misal, ACL mengijinkan atau memblok FTP atau HTTP.

Penerapan access list itu sendiri terbagi menjadi dua macam, antara lain:

- Standard Access List - yang akan melakukan penyeleksian paket berdasarkan alamat IP pengirim paket.
- Extended Access List - yang akan menyeleksi sebuah paket berdasarkan alat IP pengirim dan penerima, protokol, dan jenis port paket yang dikirim.

Ketika ACL dikonfigurasi pada sebuah router, maka ACL harus memiliki sebuah nomor identifikasi unik yang diberikan kepadanya. Nomor ini menandakan jenis access list yang dibuat dan harus berada pada range tertentu dari nomor yang valid untuk jenis daftar tersebut.

Jenis Access List	Range Nomor Pengenal
IP Standard	1-99
IP Extended	100-199
IPX Standard	800-899
IPX Extended	900-999
Apple Talk	600-699
IPX SAP Filter	1000-1099

Fungsi dari wildcard mask

Wildcard mask panjangnya 32-bit yang dibagi menjadi empat octet. Wildcard mask adalah pasangan IP address. Angka 1 dan 0 pada mask digunakan untuk mengidentifikasikan bit-bit IP address. Wildcard mask mewakili proses yang cocok dengan ACL mask-bit. Wildcard mask tidak ada hubungannya dengan subnet mask. Wildcard mask dan subnet mask dibedakan oleh dua hal. Subnet mask menggunakan biner 1 dan 0 untuk mengidentifikasi jaringan, subnet

dan host. Wildcard mask menggunakan biner 1 atau 0 untuk memfilter IP address individual atau grup untuk diijinkan atau ditolak akses. Persamaannya hanya satu dua-duanya sama-sama 32-bit.

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255

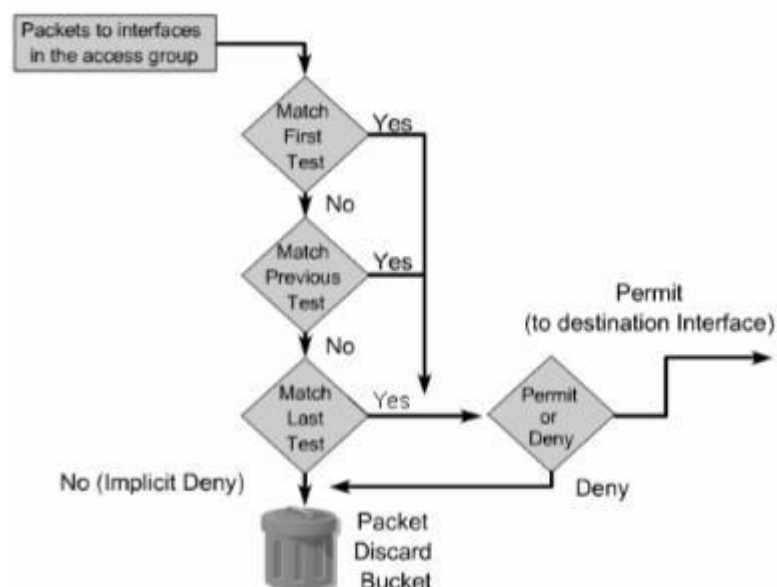
Can be written as:
Router(config)#access-list 1 permit any

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0

Can be written as:
Router(config)#access-list 1 permit host 172.30.16.29
```

Ada dua kata kunci di sini yaitu any dan host. Any berarti mengganti 0.0.0.0 untuk IP address dan 255.255.255.255 untuk wildcard mask. Host berarti mengganti 0.0.0.0 untuk mask. Mask ini membutuhkan semua bit dari alamat ACL dan alamat paket yang cocok. Opsi ini akan cocok hanya untuk satu alamat saja.

Cara kerja Cisco Access List



Keputusan dibuat berdasarkan pernyataan/statement cocok dalam daftar akses dan kemudian menerima atau menolak sesuai apa yang didefinisikan di

daftar pernyataan. Perintah dalam pernyataan ACL adalah sangat penting, kalau ditemukan pernyataan yang cocok dengan daftar akses, maka router akan melakukan perintah menerima atau menolak akses.

Pada saat frame masuk ke interface, router memeriksa apakah alamat layer 2 cocok atau apakah frame broadcast. Jika alamat frame diterima, maka informasi frame ditandai dan router memeriksa ACL pada interface inbound. Jika ada ACL, paket diperiksa lagi sesuai dengan daftar akses. Jika paket cocok dengan pernyataan, paket akan diterima atau ditolak. Jika paket diterima di interface, ia akan diperiksa sesuai dengan table routing untuk menentukan interface tujuan dan di-switch ke interface itu. Selanjutnya router memeriksa apakah interface tujuan mempunyai ACL. Jika ya, paket diperiksa sesuai dengan daftar akses. Jika paket cocok dengan daftar akses, ia akan diterima atau ditolak. Tapi jika tidak ada ACL paket diterima dan paket dienkapsulasi di layer 2 dan di-forward keluar interface device berikutnya.

Konfigurasi Cisco Access List(ACL)

ACL terbagi dua jenis :

Standard ACL :

Diletakkan dekat dengan destination, nomor yang dipakai biasanya 1-99, tidak dapat memilih port atau traffic yang diatur, semua kena. Perintahnya :

```
Router(config)#access-list numberacl permit/deny sourcenetwork  
wildcardsourcenetwork
```

Terapkan pada interface :

```
Router(config)#interface interface number  
Router(config-if)#ip access-group numberacl in/out
```

Pada akhir setiap ACL statement, letakkan perintah :

```
Router(config)#access-list numberacl permit any
```


Perhatikan :

- Host dengan wildcard 0.0.0.0 dapat digantikan dengan kata-kata “host”,

Contoh :

IP tunggal

192.168.10.1 0.0.0.0

Dapat ditulis juga :

Host 192.168.10.1

- Seluruh network dengan pernyataan :

0.0.0.0 255.255.255.255

Dapat digantikan dengan kata :

any

Extended ACL :

Diletakkan dekat dengan source, nomor yang dipakai biasanya 100-199, dapat memilih protocol ataupun port yang diatur. Perintahnya :

```
Router(config)#access-list numberacl permit | deny protocol  
sourcenetwork wildcard sourcenetwork destinationnetwork  
wilcarddestinationnetwork eq | lt | gt | neq servicename/serviceport
```

Terapkan pada interface :

```
Router(config)#interface interface number  
Router(config-if)#ip access-group numberacl in/out
```

Pada akhir ACL statement, pasang perintah :

```
Router(config)#access-list numberacl permit ip any any
```

Perintah-perintah show :

- a) Melihat statement ACL :

```
Router(config)#show access-list
```

- b) Melihat arah inbound atau outbound ACL :

```
Router(config)#show ip interface
```

- c) Melihat ACL di running-config :

```
Router(config)#show run
```

Standard dari extended ACL yang di pelajari merupakan numbered ACL, ada pula named ACL yang terdiri dari standard dan extended ACL

Contoh :

- a) Named Standard ACL

```
Router(config)# ip access-list standard namedacl
```

```
Router(config-std-nacl)# permit | deny sourcenetw wildcardsource
```

```
Router(config)#interface interface numberint
```

```
Router(config)#ip access-group namedacl in/out
```

- b) Named Extended ACL

```
Router(config)# ip access-list extended namedacl
```

```
Router(config-ext-nacl)# permit | deny protocol sourcenetw
```

```
wildcardsourcenetw destinationnetw wildcarddestinationnetw eq | lt | gt |
```

```
neq protocol/port Router(config)#ip access-group nameacl in/out
```

Selain access-list, juga terdapat access-class yang diterapkan pada line vty atau telnet line.

BAB 7

Konfigurasi Protokol BGP

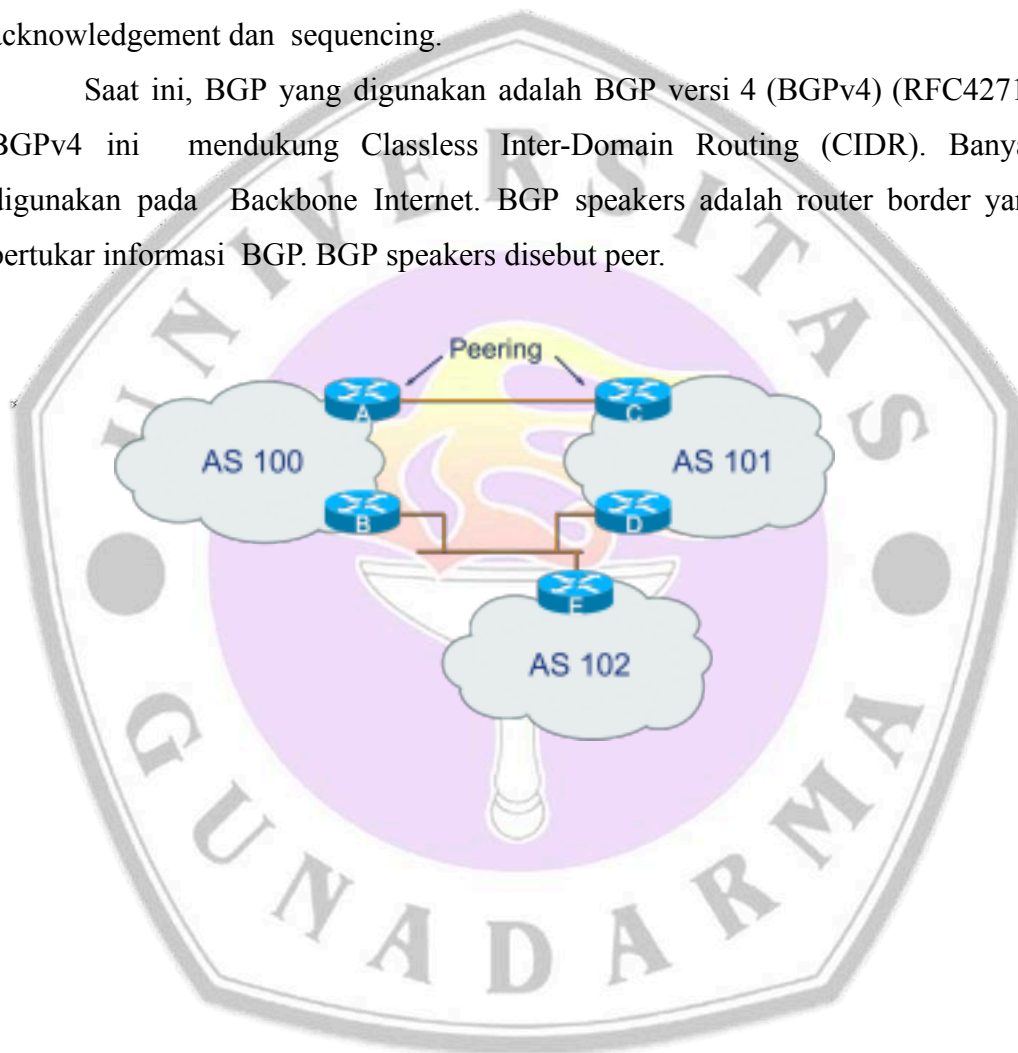
Objektif :

- Mahasiswa dapat memahami Konsep Dasar BGP
- Mahasiswa dapat Melakukan konfigurasi BGP pada Cisco Packet Tracer

Pengertian Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) merupakan routing protocol yang berfungsi untuk mempertukarkan informasi antar Autonomous System (AS) (RFC1105). BGP merupakan protocol routing yang memanfaatkan protokol TCP untuk pertukaran informasi antar router. Dengan protocol TCP ini BGP tidak perlu lagi menggunakan protocol lain untuk menangani fragmentasi, retransmisi, acknowledgement dan sequencing.

Saat ini, BGP yang digunakan adalah BGP versi 4 (BGPv4) (RFC4271). BGPv4 ini mendukung Classless Inter-Domain Routing (CIDR). Banyak digunakan pada Backbone Internet. BGP speakers adalah router border yang bertukar informasi BGP. BGP speakers disebut peer.



Konfigurasi BGP

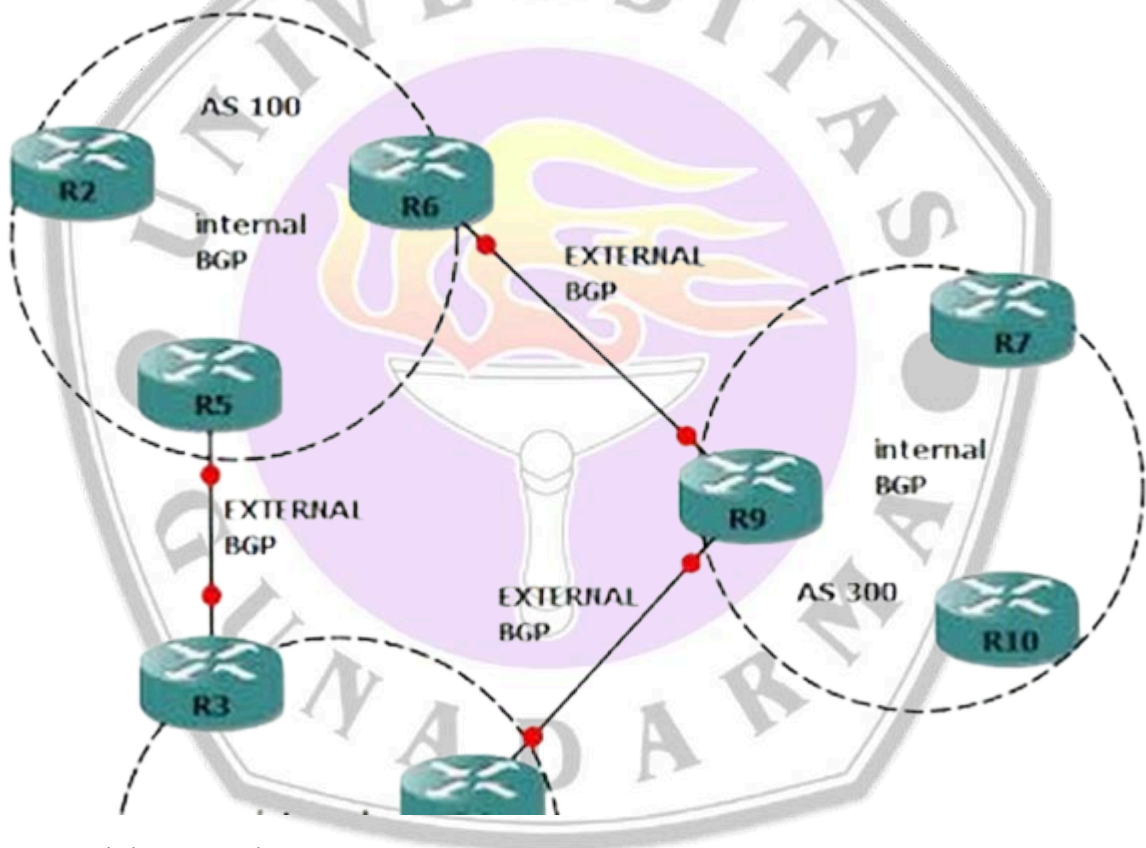
Langkah-langkah konfigurasinya adalah sebagai berikut:

1. **enable**
2. **configure terminal**
3. **router bgp** <autonomous-system-number>
4. **network** <network-number> **mask** <network-mask>
5. **neighbor** <ip-address> **remote-as** <autonomous-system-number>
6. **end**



Pengertian Autonomous System

Autonomous System (AS) adalah kumpulan dari jaringan dalam satu administrasi/kebijakan routing yang sama. Biasanya hal tersebut mengacu pada suatu institusi, contoh: Telkomsel, Indosat, atau XL. Gambar berikut



menunjukkan contoh AS

Contoh AS (Autonomous System)

Pengertian Autonomous System Number

Autonomous System Number (ASN) adalah nomor unik secara global yang digunakan untuk mengidentifikasi Autonomous System (AS) dan yang memungkinkan sebuah AS untuk bertukar informasi routing eksterior antar AS tetangga.

ASN terdiri dari 16-bit mulai dari 0 sampai 65535 (RFC1930). Namun demikian, seiring dengan perkembangan Internet, maka permintaan akan ASN juga meningkat. Akibatnya ASN yang 16-bit tadi, diperluas menjadi 32-bit (RFC4893). Tabel 2.1 di bawah ini memperlihatkan alokasi ASN yang ada.

Tabel 2.1. Alokasi ASN

Number	Bits	Description	Reference
0	16	Reserved	[RFC1930]
1 - 23455	16	Public ASN's	
23456	16	Reserved for AS Pool Transition	[RFC6793]
23457 - 64534	16	Public ASN's	
64000 - 64495	16	Reserved by IANA	
64496 - 64511	16	Reserved for use in	[RFC5398]
		documentation/sample code	
64512 - 65534	16	Reserved for Private Use	
65535	16	Reserved	
65536 - 65551	32	Reserved for use in documentation	[RFC4893]
		and sample code	[RFC5398]
65552 - 131071	32	Reserved	
131072 - 4199999999	32	Public 32-bit ASN's	
4200000000 -			
		32 Reserved for Private Use	[RFC6996]
4294967294			
4294967295	32	Reserved	

Dalam ASN dikenal juga istilah PUBLIC ASN dan PRIVATE ASN. Public ASN adalah ASN yang digunakan untuk koneksi antar jaringan di internet. Sedangkan Private ASN digunakan untuk keperluan internal dan tidak digunakan untuk koneksi ke internet. Alokasi Public ASN maupun Private ASN bisa dilihat pada tabel 2.1 di atas.

Pengertian Interior & Exterior BGP

iBGP adalah sesi BGP yang terjadi antara router-router dalam Autonomous System (AS) yang sama. iBGP digunakan untuk mendistribusikan informasi rute yang diterima dari eBGP atau sumber lain di dalam AS tersebut.

eBGP adalah sesi BGP yang terjadi antara router-router di AS yang berbeda. eBGP digunakan untuk bertukar informasi rute antar jaringan yang berbeda di internet. Gambar dibawah ini adalah contoh dari iBGP dan eBGP



BAB 8

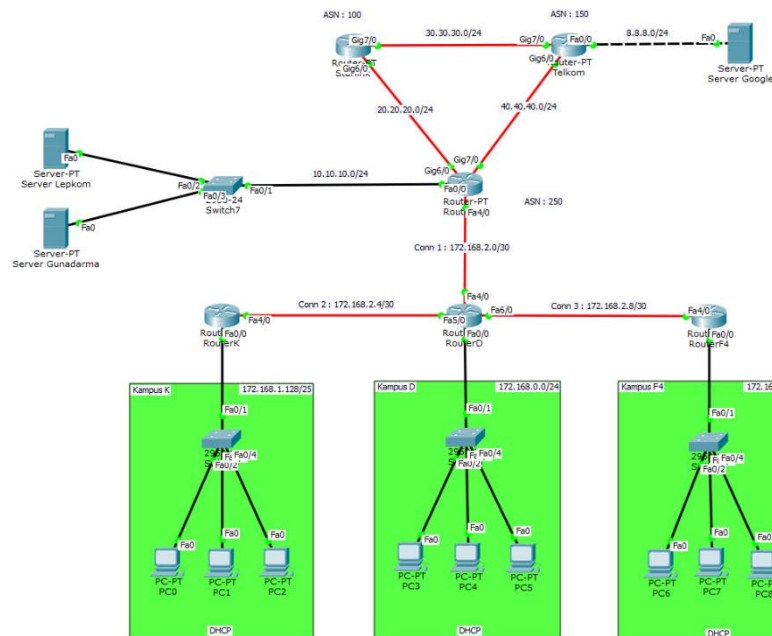
Studi Kasus

Objektif :

1. Mahasiswa dapat memahami Alamat IP & VLSM
2. Mahasiswa dapat melakukan konfigurasi DHCP pada Router Cisco
3. Mahasiswa dapat melakukan konfigurasi OSPF pada Router Cisco
4. Mahasiswa dapat melakukan konfigurasi BGP pada Router Cisco
5. Mahasiswa dapat melakukan konfigurasi ACL pada Router Cisco

Studi Kasus (VLSM, DHCP, OSPF, BGP, ACL)

Topologi :



Studi Kasus:

Universitas Gundarma, sebuah universitas besar dengan beberapa cabang kampus (Kampus K, Kampus D, dan Kampus F4). Masing-masing kampus terhubung melalui jaringan yang dirancang untuk mendukung akses ke server utama melalui router pusat, serta mendukung koneksi ke internet melalui dua penyedia layanan internet, yaitu ISP Starlink dan ISP Telkom.

Namun, terdapat beberapa tantangan yang perlu diselesaikan untuk mencapai jaringan yang optimal:

1. Pembagian Alamat IP yang efisien: Penggunaan VLSM untuk membagi subnet yang berbeda di setiap kampus dengan optimal tanpa pemborosan IP.
2. Otomatisasi Alamat IP di Setiap Kampus: Pengaturan DHCP agar setiap perangkat mendapatkan IP secara otomatis untuk memudahkan manajemen jaringan, terutama pada perangkat di area umum seperti perpustakaan dan laboratorium.

3. Konektivitas Antar Kampus dan Koneksi Internet Terpadu: Menggunakan OSPF sebagai routing untuk menghubungkan network antar kampus dan menjaga jalur komunikasi antar kampus tetap efisien, serta penggunaan BGP untuk mengatur jalur terbaik ke internet.

4. Keamanan dan Pengendalian Akses: Penerapan ACL agar hanya perangkat dan pengguna yang diperbolehkan yang bisa saling berkomunikasi, dan mencegah adanya komunikasi yang tidak diinginkan.

Anda ditugaskan untuk mengonfigurasi jaringan pada Universitas Gunadarma secara optimal dan sesuai dengan kebutuhan yang diminta. Berikut adalah ketentuan pada Studi Kasus 8:

1. PC di setiap kampus diberikan IP menggunakan metode DHCP.
2. Router UG, Router D, Router K dan Router F4 di routing menggunakan OSPF.
3. Router UG, ISP Telkom, dan ISP Starlink dirouting menggunakan BGP.
4. Kampus D tidak diperbolehkan untuk berkomunikasi dengan Kampus F4.
5. Seluruh Alamat IP baik Server, Router, dan PC (Kecuali PC Kampus F4) sudah dikonfigurasi.

Pada Activity 8 ini, praktikan diminta untuk mengerjakan serangkaian tugas sebagai berikut:

1. Menghitung VLSM dengan IP Base yang telah diberikan.
2. Melakukan konfigurasi protokol DHCP untuk Kampus F4.
3. Melakukan konfigurasi Routing OSPF untuk Router K, Router D, dan Router F4. (*OSPF Router UG sudah dikonfigurasi)
4. Melakukan konfigurasi routing BGP untuk Router UG dan ISP Telkom. (*BGP ISP Starlink sudah dikonfigurasi)
5. Mencegah komunikasi antara Kampus D dengan Kampus F4 menggunakan Standard Access List.