

Lab Guide & Module

Cisco Certified Network Associate 200-301 V.1.1



1. Virtual LAN

Virtual Local Area Network (VLAN) adalah teknologi yang memungkinkan segmentasi jaringan fisik menjadi beberapa jaringan logis. Dengan menggunakan VLAN, kita dapat meningkatkan keamanan dan efisiensi jaringan dengan memisahkan lalu lintas antar departemen atau kelompok kerja dalam organisasi.

Apabila kita menggunakan switch unmanagable, maka semua portnya hanya bisa digunakan untuk dikoneksikan ke PC yang networknya sama. Nah pada switch managable, kita bisa membuat pada sebuah switch untuk digunakan network yang berbeda. Setiap network memiliki LAN sendiri, sehingga pada sebuah switch seolah-olah terdapat beberapa LAN.

Yang perlu diingat pada penggunaan VLAN:

- Normal VLAN ID (1-1005) saved to flash:/vlan.dat
- Extended VLAN ID (1006-4094) saved to running-config
- Default VLAN ID = VLAN 1

1.1 VLAN Mode Access

Introduction:

VLAN mode Access umumnya dikonfigurasi ke arah host-device (PC, Laptop, Server, dll). By default, semua port yang ada di switch akan berada pada mode access VLAN 1. Oleh karena itu jika kita ingin membuat beberapa VLAN, kita perlu mengalokasikan beberapa port ke VLAN yang berbeda.

Port switch yang dikonfigurasi mode access, hanya akan melewatkan untagged frame (Frame Original) dan tidak akan melewatkan tagged frame (Modified Frame).

Dalam Lab kali ini, kita akan mencoba membuat VLAN untuk memisahkan broadcast domain VLAN 10 dan VLAN 20. Setelah melakukan konfigurasi VLAN, PC0 dapat berkomunikasi dengan PC1. Namun PC0 tidak dapat berkomunikasi dengan PC2, karena PC2 berada di VLAN yang berbeda.

Buat topologi berikut di Cisco Packet Tracer sesuai dengan tipe perangkat, lalu konfigurasi IP address PC sesuai dengan skenario.

Gunakan Gateway 192.168.10.1 untuk PC di VLAN 10

Gunakan Gateway 192.168.20.1 untuk PC di VLAN 20

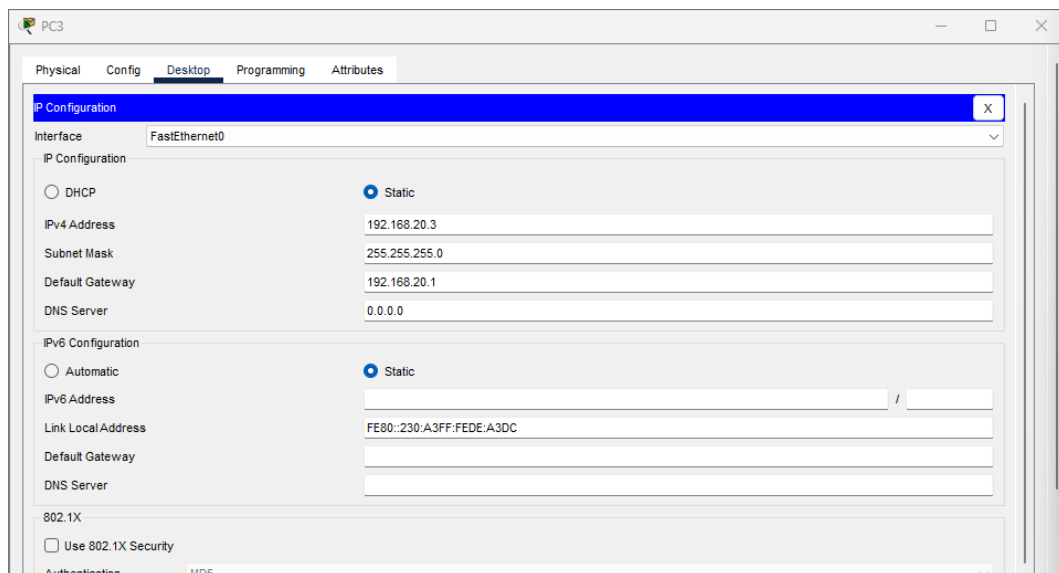
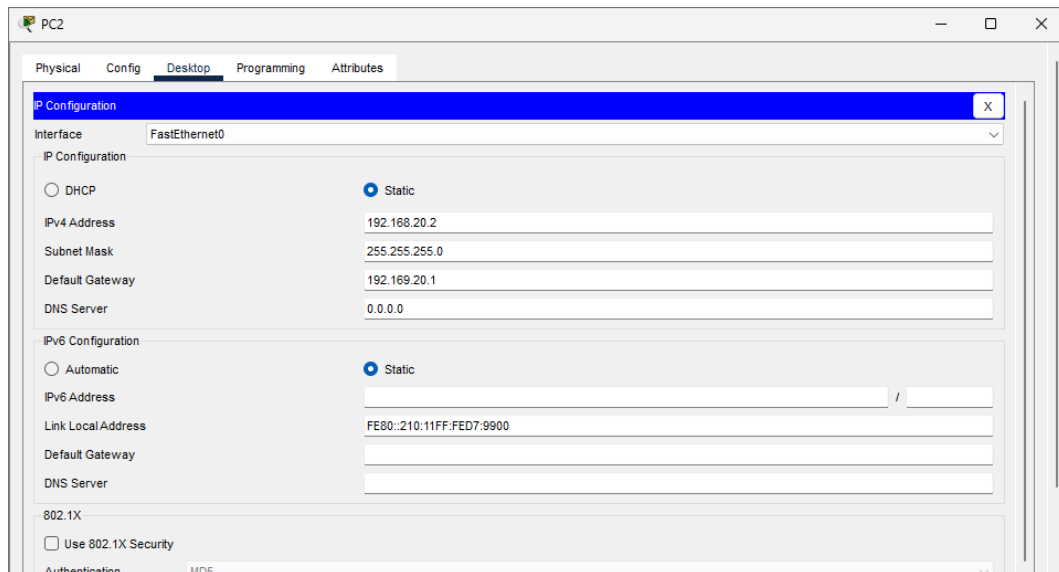
IP Addressing pada PC0, PC1, PC2, dan PC3.

The screenshot shows the configuration window for PC0. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is 'FastEthernet0'. The 'Static' radio button is selected. The fields are filled with: IPv4 Address: 192.168.10.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.10.1, and DNS Server: 0.0.0.0. The 'IPv6 Configuration' section has 'Static' selected, with IPv6 Address and Link Local Address fields empty. The '802.1X' section has 'Use 802.1X Security' unchecked. The 'Authentication' dropdown is set to 'MD5'.

| Field | Value |
|--|--------------------------|
| Interface | FastEthernet0 |
| IP Configuration | |
| <input type="radio"/> DHCP | |
| <input checked="" type="radio"/> Static | |
| IPv4 Address | 192.168.10.2 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.10.1 |
| DNS Server | 0.0.0.0 |
| IPv6 Configuration | |
| <input type="radio"/> Automatic | |
| <input checked="" type="radio"/> Static | |
| IPv6 Address | |
| Link Local Address | FE80::204:9AFF:FE67:88DE |
| Default Gateway | |
| DNS Server | |
| 802.1X | |
| <input type="checkbox"/> Use 802.1X Security | |
| Authentication | MD5 |

The screenshot shows the configuration window for PC1. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is 'FastEthernet0'. The 'Static' radio button is selected. The fields are filled with: IPv4 Address: 192.168.10.3, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.10.1, and DNS Server: 0.0.0.0. The 'IPv6 Configuration' section has 'Static' selected, with IPv6 Address and Link Local Address fields empty. The '802.1X' section has 'Use 802.1X Security' unchecked. The 'Authentication' dropdown is set to 'MD5'.

| Field | Value |
|--|--------------------------|
| Interface | FastEthernet0 |
| IP Configuration | |
| <input type="radio"/> DHCP | |
| <input checked="" type="radio"/> Static | |
| IPv4 Address | 192.168.10.3 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.10.1 |
| DNS Server | 0.0.0.0 |
| IPv6 Configuration | |
| <input type="radio"/> Automatic | |
| <input checked="" type="radio"/> Static | |
| IPv6 Address | |
| Link Local Address | FE80::201:63FF:FEB9:516A |
| Default Gateway | |
| DNS Server | |
| 802.1X | |
| <input type="checkbox"/> Use 802.1X Security | |
| Authentication | MD5 |



Langkah Pengerjaan:

Masuk ke mode Global Configuration, setup Hostname, lalu buatlah VLAN 10 dan VLAN 20

Switch0

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#hostname Switch0
```

```
Switch0(config)#vlan 10

Switch0(config-vlan)#name Sales

Switch0(config-vlan)#exit

Switch0(config)#vlan 20

Switch0(config-vlan)#name Engineering

Switch0(config-vlan)#exit
```

Konfigurasi port FastEthernet0/1 dan FastEthernet0/2 menjadi VLAN 10 lalu port FastEthernet0/3 dan FastEthernet0/4 ke VLAN 20:

```
Switch0

Switch0(config)#interface fastethernet 0/1

Switch0(config-if)#switchport mode access

switch0(config-if)#switchport access vlan 10

Switch0(config-if)#exit

Switch0(config)#

Switch0(config)#int fa0/2

Switch0(config-if)#sw mode access

Switch0(config-if)#sw access vlan 10

Switch0(config-if)#exit

Switch0(config)#

Switch0(config)#int range fa0/3-4

Switch0(config-if-range)#sw mode access

Switch0(config-if-range)#sw access vlan 20
```

Verification:

Pengecekan alokasi VLAN per interface dengan perintah "show vlan brief".

Switch0

```
Switch0#show vlan brief
```

Lakukan pengetesan ping dari PC dengan VLAN yang sama. (Contoh: PC0 → PC1)

1.2 VLAN Mode Trunk

Introduction:

VLAN mode trunk biasa dikonfigurasi pada link point-to-point antar switch. Tidak hanya pada switch, trunking juga bisa dikoneksikan ke arah router. VLAN Trunk berfungsi sebagai saluran komunikasi VLAN antara switch-ke-switch.

Ketika sebuah frame dilewatkan pada koneksi trunk, maka akan dilakukan penandaan (tagging) VLAN. Oleh karena itu, port trunk biasa juga disebut tagging port karena adanya proses tagging yang dilakukan setiap kali melewati koneksi trunk.

Protocol yang biasa digunakan pada VLAN Trunk ialah 802.1Q (dot1q). Namun Cisco juga sempat membuat protocol InterSwitched Link (ISL) sebagai protocol trunk proprietary.

Masih melanjutkan lab sebelumnya, tambahkan Switch1 dan koneksikan ke Switch0 via port GigabitEthernet0/1. Tambahkan juga PC4 dan ServerVLAN10 sesuai dengan skema IP di topologi.

Pada Lab ini, kita akan menghubungkan perangkat di VLAN yang sama (misal: PC2 to PC4). Yang perlu diingat, pada lab ini kita masih belum bisa menghubungkan VLAN yang berbeda. Karena untuk menghubungkan VLAN yang berbeda kita perlu menggunakan perangkat Layer 3.

Langkah Pengerjaan:

Sebelum menambahkan konfigurasi Trunk, mari kita lakukan konfigurasi di Switch1

Switch1

```
Switch>enable
```

```
Switch#configure terminal
```

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

```
Switch(config)#hostname Switch1
```

```
Switch1(config)#
```

```
Switch1(config)#int fa0/1
```

```
Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 10

% Access VLAN does not exist. Creating vlan 10

Switch1(config-if)#exit

Switch1(config)#

Switch1(config)#int fa0/2

Switch1(config-if)#switchport mode access

Switch1(config-if)#switchport access vlan 20

% Access VLAN does not exist. Creating vlan 20

Switch1(config-if)#end

Switch1#
```

Tambahkan konfigurasi Trunk di Switch0

```
Switch0

Switch0(config)#int range g0/1-2

Switch0(config-if-range)#switchport mode trunk.

Switch0(config-if-range)#exit
```

Verification:

```
Switch0

Switch0#show interface trunk
```


1.3 InterVLAN (Router on Stick)

Introduction:

Pada topologi sebelumnya, kedua VLAN yang berada pada network yang berbeda masih belum dapat saling berkomunikasi. Untuk itu kita memerlukan perangkat Layer 3 yakni berupa Switch Multilayer ataupun sebuah Router agar kedua VLAN dapat saling berkomunikasi. Lab kali ini kita akan menggunakan sebuah router.

Penggunaan Router on Stick cocok diterapkan jika dalam jaringan yang dimiliki tidak terdapat multilayer switch. Konfigurasi utama dalam yang perlu dilakukan dalam penerepan InterVLAN routing ialah konfigurasi encapsulation dot1q <vlan-id> yang diaktifkan disetiap sub-interface. Jadi pastikan konfigurasi tersebut tidak terlewat dalam setiap konfigurasi InterVLAN routing pada perangkat Router.

Masih melanjutkan topologi sebelumnya, kita tambahkan sebuah router series 2911 yang dihubungkan ke Switch0 port G0/2.

Dengan mengaktifkan Sub-Interface di Router), maka router memiliki 2 Directly Connected Network sehingga bisa menghubungkan VLAN 10 dan VLAN 20. Jika kita ingin menambahkan VLAN, maka kita perlu membuat Sub-Interface tambahan sehingga Directly Connected Network akan bertambah di tabel routing perangkat Router.

Langkah Pengerjaan:

Tambahkan Sub-Interface masing-masing VLAN, aktifkan fitur dot1q dan tambahkan IP address di masing-masing Sub-Interface.

Router0

```
Router>enable

Router#config t

Enter configuration commands, one per line. End with CHTL/2.

Router(config)#hostname Router0

Router0(config)#int g0/0.10

Router0(config-subif)#encapsulation dot1q 10
```

```
Router0(config-subif)#ip address 192.168.10.1 255.255.255.0

Router0(config-subif)#exit

Router0(config)#int g0/0.20

Router0(config-subif)#encapsulation dot1q 20

Router0(config-subif)#ip address 192.168.20.1 255.255.255.0

Router0(config-subif)#exit

Router0(config)#int g0/0

Router0(config-if)#no shutdown
```

Setelah interface fisik G0/0 yang terhubung ke Switch0 sudah aktif, maka table routing akan terisi informasi 2 rute network, yakni 192.168.10.0/24 dan 192.168.20.0/24

Router0

```
Router0#show ip route
```

Selanjutnya lakukan test ping dari PC0 VLAN10 ke PC2 VLAN20, lakukan test beberapa kali dan pastikan hasilnya reply. Jika percobaan ping pertama gagal, kemungkinan disebabkan karena proses resolve ARP yang belum selesai, maka dari itu coba test ping beberapa kali ke setiap host device yang ada.

1.4 InterVLAN (Multilayer Switch)

Introduction:

Penerapan InterVLAN Routing selanjutnya kita akan menggunakan Multilayer Switch untuk menghubungkan VLAN yang berbeda. Multilayer Switch merupakan perangkat switch yang memiliki kapabilitas fitur Layer 3, sehingga kita bisa menggunakan Multilayer Switch sebagai pengganti Router dalam menghubungkan network yang berbeda.

Buatlah file Cisco Packet Tracer Baru, lalu buatlah topologi dengan skema IP sesuai skenario.

Konfigurasi yang akan dilakukan kurang lebih masih sama seperti Lab VLAN sebelumnya, namun kali ini kita akan mengaktifkan Interface VLAN, Interface VLAN adalah interface virtual yang bisa digunakan pada switch Layer 2 / Layer 3 dan dapat diaktifkan jika terdapat port fisik yang aktif (mode access/trunk).

Perbedaan dari penggunaan switch Layer 2 dengan Switch Layer 3 berada pada perintah ip routing, dimana perintah tersebut berfungsi untuk mengaktifkan fitur Layer 3, sehingga multilayer switch dapat memiliki table routing yang dapat menghubungkan VLAN berbeda.

Langkah Pengerjaan:

Konfigurasikan VLAN, Interface VLAN dan aktifkan fitur Layer 3 di Multilayer Switch

MLS

```
Switch(config)#hostname MLS
MLS(config)#vlan 10
MLS(config-vlan)#vlan 20
MLS(config-vlan)#vlan 30
MLS(config-vlan)#exit
MLS(config)#
MLS(config)#int range fa0/1-2
MLS(config-if-range)#sw mode access
```

```
MLS(config-if-range)#sw access vlan 10

MLS(config-if-range)#exit

MLS(config)#

MLS(config)#int range fa0/3-4

MLS(config-if-range)#sw mode access

MLS(config-if-range)#sw access vlan 20

MLS(config-if-range)#exit

MLS(config)#

MLS(config)#int fa0/5

MLS(config-if)#sw mode access

MLS(config-if)#sw access vlan 30

MLS(config-if)#exit

MLS(config)#

MLS(config)#ip routing

MLS(config)#

MLS(config)#int vlan10

MLS(config-if)#ip address 192.168.10.1 255.255.255.0

MLS(config-if)#exit

MLS(config)#

MLS(config)#int vlan20

MLS(config-if)#ip address 192.168.20.1 255.255.255.0

MLS(config-if)#exit

MLS(config)#

MLS(config)#int vlan30

MLS(config-if)#ip address 192.168.30.1 255.255.255.0

MLS(config-if)#end
```

Verification:

Lakukan pengecekan VLAN dan Table Routing

MLS

```
MLS#show vlan brief
```

Selanjutnya lakukan test ping dari PC0 VLAN10 ke PC2 VLAN20, lakukan test beberapa kali dan pastikan hasilnya reply. Jika percobaan ping pertama gagal, kemungkinan disebabkan karena proses resolve ARP yang belum selesai, maka dari itu coba test ping beberapa kali ke setiap host device yang ada.