VERSION 1.1

SEPTEMBER , 2021

[PRAKTIKUM JARINGAN KOMPUTER]

-MODUL 1 -

KONSEP SWITCH, VLANS, DAN INTER-VLAN ROUTING

DISUSUN OLEH:

- FACHRY FATHURAHMAN.
- WIEN DEWANI

DIAUDIT OLEH:

- DENAR REGATA AKBI, S.KOM, M.KOM

PRESENTED BY: TIM LAB-IT

UNIVERSITAS MUHAMMADIYAH MALANG

[JARINGAN KOMPUTER]

PERSIAPAN MATERI

- Konsep Switch
- VLans
- Inter-VLan Routing

TUJUAN

- Mahasiswa mampu memahami dan mengimplementasi konsep Switching
- Mahasiswa mampu memahami dan mengimplementasi VLan
- Mahasiswa mampu memahami dan mengimplementasi Inter-VLan Routing

TARGET MODUL

- Menjelaskan bagaimana Frame diteruskan pada Switch Network
- Membandingkan Collision Domain dengan Broadcast Domain
- Menjelaskan tujuan VLan pada Switch Network
- Menjelaskan bagaimana Switch meneruskan Frame berdasarkan konfigurasi VLans pada Multi-Switch
- Melakukan Konfigurasi Port Switch pada VLan berdasarkan kebutuhan
- Melakukan Konfigurasi Port Trunk pada Switch Lan
- Melakukan Konfigurasi Protokol Trunking Dinamis (Configure Dynamic Trunking Protocol)
- Menjelaskan opsi untuk Konfigurasi inter-VLan routing.
- Melakukan Konfigurasi Router-On-A-Stick inter-VLan routing.
- Melakukan Konfigurasi inter-VLan routing menggunakan Layer 3 Switch
- Troubleshooting masalah umum Konfigurasi inter-VLan

PERSIAPAN SOFTWARE/APLIKASI

- Komputer/Latop
- Sistem operasi Windows/ Linux/ Mac OS
- Simulator Packet Tracer

MATERI POKOK

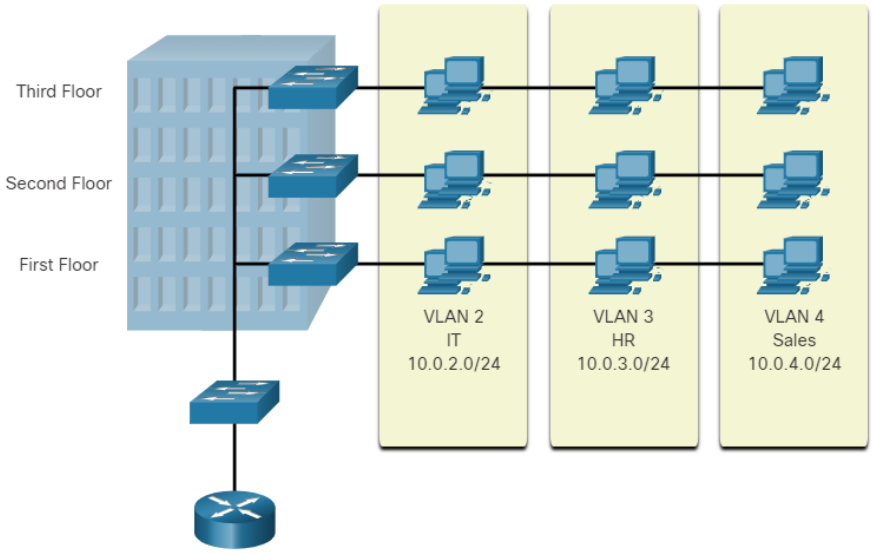
1. Switch

Switch merupakan suatu pengalih jaringan atau sebuah alat yang digunakan untuk menjalankan penghubung yang tidak terlihat penghubung penyekat (segmentation) dari banyak jaringan dengan mengalihkan dengan melihat alamat MAC. Switch pada jaringan bisa digunakan untuk menghubungkan komputer atau penghalang terdapat dalam sebuah area yang terbatas, Switch juga dapat bekerja di lapisan data yang terhubung (data link). Cara kerja dari Switch ini mirip pada jembatan (bridge), namun Switch memiliki beberapa port yang menjadikan sering disebut juga dengan multi port bridge (jembatan pancaporta).

2. VLAN

Virtual Local Area Network atau VLAN adalah sekumpulan perangkat yang ada di satu atau lebih jaringan LAN dan dikonfigurasikan oleh perangkat lunak sehingga dapat berkomunikasi antara satu dengan lainnya seolah-olah berada di saluran yang sama.

VLAN sendiri sebenarnya merupakan sebuah jaringan yang berada di dalam Local Area Network (LAN) sehingga dalam satu jaringan LAN bisa terdiri atas lebih dari satu jaringan VLAN.



Seperti yang ditunjukkan pada gambar, VLAN dalam jaringan yang diaktifkan memungkinkan pengguna di berbagai departemen (yaitu, TI, SDM, dan Penjualan) untuk terhubung ke jaringan yang sama terlepas dari sakelar fisik yang digunakan atau lokasi di LAN kampus.

VLAN memungkinkan administrator untuk membagi jaringan berdasarkan faktor-faktor seperti fungsi, tim, atau aplikasi, tanpa memperhatikan lokasi fisik pengguna atau perangkat.

Setiap VLAN dianggap sebagai jaringan logis terpisah. Perangkat dalam VLAN bertindak seolah-olah berada di jaringan independennya sendiri, meskipun perangkat tersebut berbagi infrastruktur yang sama dengan VLAN lain. Port switch apa pun bisa menjadi milik VLAN.

Menggunakan VLAN, administrator jaringan dapat mengimplementasikan akses dan kebijakan keamanan sesuai dengan pengelompokan pengguna tertentu. Setiap port sakelar hanya dapat ditetapkan ke satu VLAN (kecuali untuk port yang terhubung ke telepon IP atau ke sakelar lain).

Konfigurasi VLAN

1. Perintah Pembuatan VLAN

Saat mengkonfigurasi VLAN rentang normal, detail konfigurasi disimpan dalam memori flash pada sakelar dalam file bernama vlan.dat. Memori flash tetap dan tidak memerlukan perintah copy running-config startup-config. Namun, karena detail lainnya sering dikonfigurasi pada sakelar Cisco pada saat yang sama saat VLAN dibuat, praktik yang baik untuk menyimpan perubahan konfigurasi yang sedang berjalan ke konfigurasi startup.

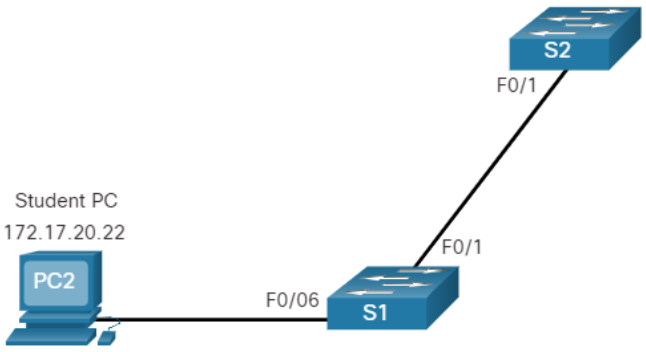
Tabel menampilkan sintaks perintah Cisco IOS yang digunakan untuk menambahkan VLAN ke sakelar dan memberinya nama. Penamaan setiap VLAN dianggap sebagai praktik terbaik dalam konfigurasi sakelar.

Task	IOS Command
Enter global configuration mode.	`Switch# configure terminal`
Create a VLAN with a valid ID number.	`Switch(config)# vlan vlan-id`
Specify a unique name to identify the VLAN.	`Switch(config-vlan)# name vlan-name`
Return to the privileged EXEC mode.	`Switch(config-vlan)# end`

2. Contoh Pembuatan VLAN

Secara topologi, komputer pelajar (PC2) belum dikaitkan dengan VLAN, tetapi memiliki alamat IP 172.17.20.22, yang termasuk dalam VLAN 20.

PC mahasiswa, host PC2, di alamat 172.17.20.22 terhubung ke switch S1 di port F0 / 6 yang terhubung melalui port F0 / 1 ke switch S2 di port F0 / 1



Contoh menunjukkan bagaimana VLAN mahasiswa (VLAN 20) dikonfigurasi pada sakelar S1.

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

Catatan: Selain memasukkan ID VLAN tunggal, serangkaian ID VLAN dapat dimasukkan dengan dipisahkan koma, atau berbagai ID VLAN yang dipisahkan dengan tanda hubung menggunakan perintah vlan vlan-id. Misalnya, memasukkan perintah konfigurasi global vlan 100,102,105-107 akan membuat VLAN 100, 102, 105, 106, dan 107.

3. Perintah Penugasan Port VLAN

Setelah membuat VLAN, langkah selanjutnya adalah menetapkan port ke VLAN.

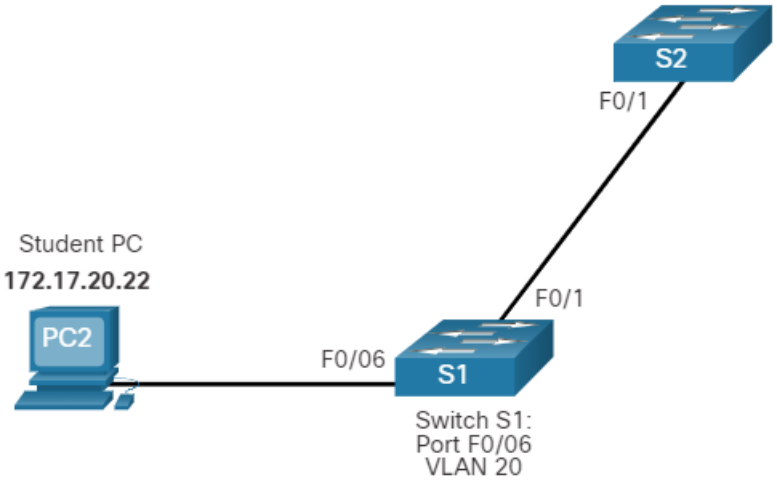
Tabel menampilkan sintaks untuk menentukan port menjadi port akses dan menetapkannya ke VLAN. Perintah akses mode switchport bersifat opsional, tetapi sangat disarankan sebagai praktik keamanan terbaik. Dengan perintah ini, antarmuka berubah menjadi mode akses ketat. Mode akses menunjukkan bahwa port tersebut dimiliki oleh satu VLAN dan tidak akan dinegosiasikan untuk menjadi link trunk.

Task	IOS Command
Enter global configuration mode.	`Switch# configure terminal`
Enter interface configuration mode.	`Switch(config)# interface` *interface-id*
Set the port to access mode.	`Switch(config-if)# switchport mode access`
Assign the port to a VLAN.	`Switch(config-if)# switchport access vlan` *vlan-id*
Return to the privileged EXEC mode.	`Switch(config-if)# end`

Catatan: Gunakan perintah rentang antarmuka untuk secara bersamaan mengkonfigurasi beberapa antarmuka.

4. Contoh Penetapan Port VLAN

Pada gambar, port F0 / 6 pada sakelar S1 dikonfigurasi sebagai port akses dan ditetapkan ke VLAN 20. Perangkat apa pun yang terhubung ke port itu akan dikaitkan dengan VLAN 20. Oleh karena itu, dalam contoh kami, PC2 ada di VLAN 20.



Contoh menunjukkan konfigurasi S1 untuk menetapkan F0 / 6 ke VLAN 20.

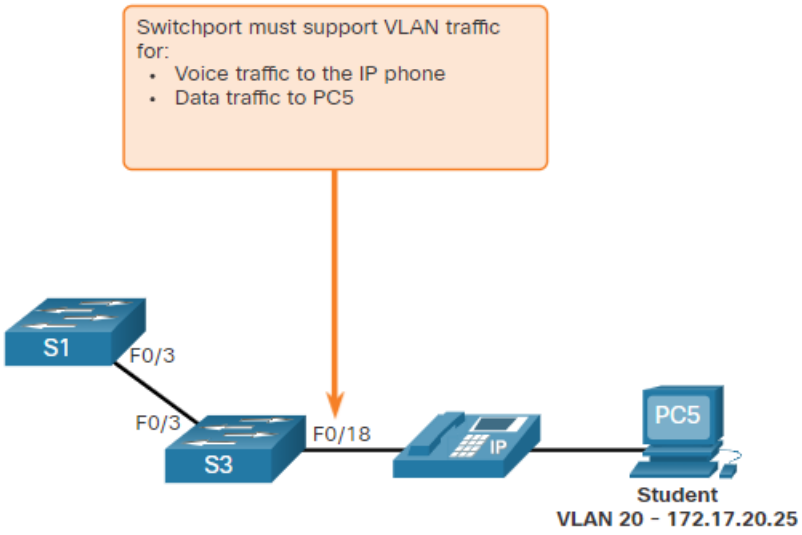
```
S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
```

VLAN dikonfigurasi pada port switch dan bukan pada perangkat akhir. PC2 dikonfigurasi dengan alamat IPv4 dan subnet mask yang dikaitkan dengan VLAN, yang dikonfigurasi pada port switch. Dalam contoh ini, ini adalah VLAN 20. Ketika VLAN 20 dikonfigurasi pada sakelar lain, administrator jaringan harus mengkonfigurasi komputer siswa lain agar berada di subnet yang sama dengan PC2 (172.17.20.0/24).

5. VLAN Data dan Suara

Port akses hanya dapat dimiliki oleh satu data VLAN pada satu waktu. Namun, port juga dapat dikaitkan ke VLAN suara. Misalnya, port yang terhubung ke telepon IP dan perangkat akhir akan dikaitkan dengan dua VLAN: satu untuk suara dan satu untuk data.

Perhatikan topologi pada gambar. PC5 terhubung ke telepon IP Cisco, yang pada gilirannya terhubung ke antarmuka FastEthernet 0/18 di S3. Untuk mengimplementasikan konfigurasi ini, VLAN data dan VLAN suara dibuat.



Host PC5 ada di Student VLAN 20 di alamat 172.17.20.25. PC5 terhubung ke telepon IP yang terhubung ke saklar S3 di port F0 / 18. Kotak teks dengan panah menunjuk ke port ini berbunyi: switchport harus mendukung lalu lintas VLAN untuk lalu lintas suara ke telepon IP dan lalu lintas data ke PC5. S3 dihubungkan melalui port F0 / 3 untuk beralih S1 di port F0 / 3.

6. Verifikasi Informasi VLAN

Setelah VLAN dikonfigurasi, konfigurasi VLAN dapat divalidasi menggunakan perintah acara Cisco IOS. Perintah show vlan menampilkan daftar semua VLAN yang dikonfigurasi. Perintah show vlan juga dapat digunakan dengan opsi. Sintaks lengkapnya adalah show vlan [singkat | id vlan-id | nama vlan-nama | ringkasan].

Tabel menjelaskan opsi perintah show vlan.

Task	Command Option
Display VLAN name, status, and its ports one VLAN per line.	`brief`
Display information about the identified VLAN ID number. For *vlan-id*, the range is 1 to 4094.	`id` *`vlan-id`*
Display information about the identified VLAN name. The *vlan-name* is an ASCII string from 1 to 32 characters.	`name` *`vlan-name`*
Display VLAN summary information.	`summary`

Perintah show vlan summary menampilkan jumlah semua VLAN yang dikonfigurasi.

```
S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0
```

Perintah berguna lainnya adalah show interfaces interface-id switchport dan perintah show interfaces vlan vlan-id. Misalnya, perintah show interface fa0 / 18 switchport dapat digunakan untuk mengonfirmasi bahwa port FastEthernet 0/18 telah ditetapkan dengan benar ke data dan VLAN suara.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
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: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 150
Administrative private-vlan host-association: none
(Output omitted)
```

9. Ubah Keanggotaan Port VLAN

Jika port akses sakelar telah salah ditetapkan ke VLAN, cukup masukkan kembali perintah konfigurasi antarmuka vlan vlan-id akses switchport dengan ID VLAN yang benar. Misalnya, anggap Fa0 / 18 salah dikonfigurasi menjadi VLAN 1 default, bukan VLAN 20. Untuk mengubah port ke VLAN 20, cukup masukkan akses switchport vlan 20. Untuk mengubah keanggotaan port kembali ke VLAN 1 default, gunakan perintah mode konfigurasi antarmuka vlan tanpa akses switchport seperti yang ditunjukkan.

Dalam output misalnya, Fa0 / 18 dikonfigurasi menjadi default VLAN 1 seperti yang dikonfirmasi oleh perintah show vlan brief.

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
S1# show vlan brief
VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gi0/1, Gi0/2
20   student              active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

Perhatikan bahwa VLAN 20 masih aktif, meskipun tidak ada port yang ditetapkan untuk itu.

Tampilan antarmuka f0 / 18 output switchport juga dapat digunakan untuk memverifikasi bahwa akses VLAN untuk antarmuka F0 / 18 telah diatur ulang ke VLAN 1 seperti yang ditunjukkan pada output.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

10. Hapus VLAN

Perintah mode konfigurasi global no vlan vlan-id digunakan untuk menghapus VLAN dari file switch vlan.dat.

Perhatian: Sebelum menghapus VLAN, tetapkan ulang semua port anggota ke VLAN yang berbeda terlebih dahulu. Setiap port yang tidak dipindahkan ke VLAN aktif tidak dapat berkomunikasi dengan host lain setelah VLAN dihapus dan sampai mereka ditetapkan ke VLAN aktif.

Seluruh file vlan.dat dapat dihapus menggunakan perintah mode EXEC delete flash: vlan.dat privileged. Versi perintah yang disingkat (hapus vlan.dat) dapat digunakan jika file vlan.dat belum dipindahkan dari lokasi defaultnya. Setelah mengeluarkan perintah ini dan memuat ulang sakelar, VLAN yang dikonfigurasi sebelumnya tidak lagi ada. Ini secara efektif menempatkan sakelar ke kondisi default pabrik terkait dengan konfigurasi VLAN.

3. VLAN Trunks

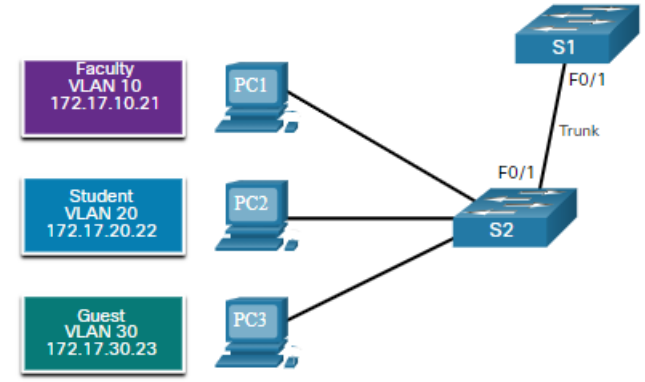
- Trunk Configuration

VLAN Trunk adalah tautan Layer 2 antara dua sakelar yang membawa lalu lintas untuk semua VLAN (kecuali daftar VLAN yang diizinkan dibatasi secara manual atau dinamis). Untuk mengaktifkan tautan trunk, konfigurasikan port interkoneksi dengan set perintah konfigurasi antarmuka yang ditunjukkan pada tabel.

Task	IOS Command
Enter global configuration mode.	`Switch# configure terminal`
Enter interface configuration mode.	`Switch(config)# interface interface-id`
Set the port to permanent trunking mode.	`Switch(config-if)# switchport mode trunk`
Sets the native VLAN to something other than VLAN 1.	`Switch(config-if)# switchport trunk native vlan vlan-id`
Specify the list of VLANs to be allowed on the trunk link.	`Switch(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`Switch(config-if)# end`

- Contoh Trunk Configuration

Pada gambar, VLAN 10, 20, dan 30 mendukung komputer Fakultas, Mahasiswa, dan Tamu (PC1, PC2, dan PC3). Port F0 / 1 pada sakelar S1 dikonfigurasi sebagai port trunk dan meneruskan lalu lintas untuk VLAN 10, 20, dan 30. VLAN 99 dikonfigurasi sebagai VLAN asli.



The subnets associated with each VLAN are:

- VLAN 10 – Faculty/Staff – 172.17.10.0/24
- VLAN 20 – Students – 172.17.20.0/24
- VLAN 30 – Guests – 172.17.30.0/24
- VLAN 99 – Native – 172.17.99.0/24

Contoh tersebut menunjukkan konfigurasi port F0 / 1 pada sakelar S1 sebagai port trunk. VLAN asli diubah menjadi VLAN 99 dan daftar VLAN yang diizinkan dibatasi hingga 10, 20, 30, dan 99.

```
S1(config)# interface fastEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Catatan: Konfigurasi ini mengasumsikan penggunaan sakelar Cisco Catalyst 2960 yang secara otomatis menggunakan enkapsulasi 802.1Q pada tautan trunk. Sakelar lain mungkin memerlukan konfigurasi enkapsulasi manual. Selalu konfigurasikan kedua ujung tautan trunk

dengan VLAN asli yang sama. Jika konfigurasi trunk 802.1Q tidak sama di kedua ujungnya, Cisco IOS Software melaporkan kesalahan....

- Verifikasi Trunk Configuration

Output sakelar menampilkan konfigurasi port sakelar F0 / 1 pada sakelar S1. Konfigurasi diverifikasi dengan perintah show interfaces interface-ID switchport.

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

Area teratas yang disorot menunjukkan bahwa port F0 / 1 memiliki mode administratif yang disetel ke trunk. Port dalam mode trunking. Area yang disorot berikutnya memverifikasi bahwa VLAN asli adalah VLAN 99. Lebih jauh ke bawah dalam output, area yang disorot di bawah menunjukkan bahwa VLAN 10, 20, 30, dan 99 diaktifkan di trunk.

Catatan: Perintah lain yang berguna untuk antarmuka trunk veryfing adalah perintah show interface trunk.

- Setel Ulang Trunk ke Status Default

Gunakan vlan no switchport trunk yang diizinkan dan perintah vlan native no switchport trunk untuk menghapus VLAN yang diizinkan dan menyetel ulang VLAN asli dari trunk. Saat direset ke status default, trunk mengizinkan semua VLAN dan menggunakan VLAN 1 sebagai VLAN asli. Contoh ini menunjukkan perintah yang digunakan untuk mengatur ulang semua karakteristik trunking dari antarmuka trunking ke pengaturan default.

```
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
```

```
The show interfaces f0/1 switchport command reveals that the trunk has been reconfigured to a default
state.
```

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

Output sampel ini menunjukkan perintah yang digunakan untuk menghapus fitur trunk dari port sakelar F0 / 1 pada sakelar S1. Perintah show interfaces f0 / 1 switchport mengungkapkan bahwa antarmuka F0 / 1 sekarang dalam mode akses statis.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
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
(output omitted)
```

4. Inter VLan Routing

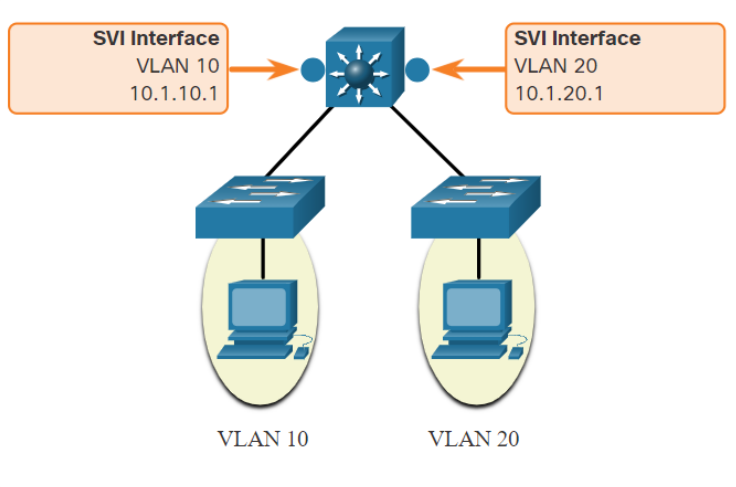
Inter VLAN routing merupakan proses mem-forward lalu lintas dari satu jaringan VLAN ke VLAN lain atau dengan kata lain mengubungkan host-host yang berada pada VLAN yang berbeda. Terdapat 3 opsi Inter-VLAN Routing, yaitu:

- **Legacy Inter-VLAN Routing**.

- Merupakan cara lama yang kurang efisien karena setiap VLAN harus terhubung ke satu interface pada Router.
- **Router-On-a-Stick**
  Ini adalah solusi alternatif untuk skala jaringan yang kecil hingga menengah.
- **Layer 3 switch using switched vitual interfaces (SVIs)**.
  Merupakan cara yang paling efektif dan efisien untuk skala jaringan menengah keatas.

Inter –VLAN Routing pada Layer 3 Switch

Metode modern dari inter-VLAN adalah penggunaan layer 3 switch dan Switched Virtual Interface (SVI). Sebuah SVI adalah antarmuka virtual yang dikonfigurasi pada layer 3 seperti gambar di bawah ini :



SVI Inter-VLAN terbentuk dengan cara yang sama dengan managemen pembentukan VLAN. SVI terbentu untuk VLAN yang ada di switch. Meskipun bersifat virtual, perfoman SVI memiliki fungsi yang sama untuk VLAN sebagai anatarmuka router. Secara spesifik, ia menyediakan pemrosesan paket di layer 3 yang akan dikirim ke atau sari port sqitch yang terhubung dengan VLAN.

Kemampuan switch Layer 3 mencakup kemampuan untuk melakukan hal berikut:

a. Routing dari satu VLAN ke VLAN lainnya menggunakan beberapa antarmuka virtual (SVIs) yang dialihkan.

b. Mengonversi switchport Layer 2 ke antarmuka Layer 3 (yaitu, port yang dirutekan).Port rute mirip dengan antarmuka fisik pada router IOS Cisco

Untuk menyediakan perutean antar-VLAN, sakelar Layer 3 menggunakan SVIs.SVIs dikonfigurasi menggunakan perintah vlan vlan-id antarmuka yang sama yang digunakan untuk membuat SVI manajemen pada sakelar Layer 2.Lapisan 3 SVI harus dibuat untuk setiap VLAN yang dapat di-routable.

Jika VLAN dapat dijangkau oleh perangkat Layer 3 lainnya, maka mereka harus diiklankan menggunakan perutean statis atau dinamis.Untuk mengaktifkan perutean pada switch Layer 3, port yang dirutekan harus dikonfigurasi.Port rute 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 switchport pada port Layer 2 mengubahnya menjadi

antarmuka Layer 3.Kemudian antarmuka dapat dikonfigurasi dengan konfigurasi IPv4 untuk terhubung ke router atau switch Layer 3 lainnya.

TUGAS

Tugas yang dilakukan yaitu mengerjakan Activity Lab Packet Tracer - Configure Layer 3 Switching and Inter-VLAN Routing. Download file Packet Tracer pada link di bawah ini :

https://bit.ly/Modul1_JaringanKomputer_2021

Konfigurasi harus dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. Petunjuk pengerjaan praktikum juga dapat dilihat pada perintah dibawah. Setelah selesai melakukan konfigurasi pada File Packet Tracer, simpan hasil konfigurasi tersebut, kemudian ganti nama file Packet Tracer tersebut mengikuti format Tugas-nama-nim.pka. Tugas dikumpulkan di infotech.umm.ac.id pada bagian attachment **sebelum** berlangsungnya kegiatan praktikum.

Packet Tracer - Configure Layer 3 Switching and Inter-VLAN Routing

1. ADDRESSING TABLE

Device	Interface	IP Address / Prefix
MLS	VLAN 10	192.168.10.254 /24
		2001:db8:acad:10::1/64
	VLAN 20	192.168.20.254 /24
		2001:db8:acad:20::1/64
	VLAN 30	192.168.30.254/24
		2001:db8:acad:30::1/64
	VLAN 99	192.168.99.254/24
	G0/2	209.165.200.225
		2001:db8:acad:a::1/64
PC0	NIC	192.168.10.1
PC1	NIC	192.168.20.1
PC2	NIC	192.168.30.1
PC3	NIC	192.168.10.2/24
		2001:db8:acad:10::2/64
PC4	NIC	192.168.20.2/24
		2001:db8:acad:20::2/64

PC5	NIC	192.168.30.2
		2001:db8:acad:10::2/64
S1	VLAN 99	192.168.99.1
S2	VLAN 99	192.168.99.2
S3	VLAN 99	192.168.99.3

2. OBJECTIVES

Part 1: Configure Layer 3 Switching

Part 2: Configure Inter-VLAN Routing

Part 3: Configure IPv6 Inter-VLAN Routing

3. BACKGROUND / SCENARIO

A multilayer switch like the Cisco Catalyst 3650 is capable of both Layer 2 switching and Layer 3 routing. One of the advantages of using a multilayer switch is this dual functionality. A benefit for a small to medium-sized company would be the ability to purchase a single multilayer switch instead of separate switching and routing network devices. Capabilities of a multilayer switch include the ability to route from one VLAN to another using multiple switched virtual interfaces (SVIs), as well as the ability to convert a Layer 2 switchport to a Layer 3 interface.

4. INSTRUCTIONS

1. CONFIGURE LAYER 3 SWITCHING

In Part 1, you will configure the GigabitEthernet 0/2 port on switch MLS as a routed port and verify that you can ping another Layer 3 address.

a. On MLS, configure G0/2 as a routed port and assign an IP address according to the Addressing Table.

```
MLS(config)# interface g0/2
MLS(config-if)# no switchport
MLS(config-if)# ip address 209.165.200.225 255.255.255.252
```

b. Verify connectivity to **Cloud** by pinging 209.165.200.226.

```
MLS# ping 209.165.200.226


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

2. CONFIGURE INTER-VLAN ROUTING

1. ADD VLANS.

Add VLANs to MLS according to the table below. Packet Tracer scoring is case-sensitive, so type the names exactly as shown.

VLAN Number	VLAN Name
10	Staff
20	Student
30	Faculty

2. CONFIGURE SVI ON MLS.

Configure and activate the SVI interfaces for VLANs 10, 20, 30, and 99 according to the Addressing Table. The configuration for VLAN 10 is shown below as an example.

```
MLS(config)# interface vlan 10
MLS(config-if)# ip address 192.168.10.254 255.255.255.0
```

3. CONFIGURE TRUNKING ON MLS.

Trunk configuration differs slightly on a Layer 3 switch. On the Layer 3 switch, the trunking interface needs to be encapsulated with the dot1q protocol, however it is not necessary to specify VLAN numbers as it is when working with a router and subinterfaces.

a. On MLS, configure interface **g0/1**.

b. Make the interface a static trunk port.

```
MLS(config-if)# switchport mode trunk
```

c. Specify the native VLAN as 99.

```
MLS(config-if)# switchport trunk native vlan 99
```

d. Encapsulate the link with the dot1q protocol.

```
MLS(config-if)# switchport trunk encapsulation dot1q
```

Note: Packet Tracer may not score the trunk encapsulation.

4. CONFIGURE TRUNKING ON S1.

a. Configure interface **g0/1** of S1 as a static trunk.

b. Configure the native VLAN on the trunk.

5. ENABLE ROUTING.

a. Use the **show ip route** command. Are there any active routes?

b. Enter the **ip routing** command to enable routing in global configuration mode.

MLS(config)# **ip routing**

c. Use the **show ip route** command to verify routing is enabled.

```
MLS# 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

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.99.0/24 is directly connected, Vlan99
     209.165.200.0/30 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, GigabitEthernet0/2
```

6. VERIFY END-TO-END CONNECTIVITY.

a. From PC0, ping PC3 or MLS to verify connectivity within VLAN 10.

b. From PC1, ping PC4 or MLS to verify connectivity within VLAN 20.

c. From PC2, ping PC5 or MLS to verify connectivity within VLAN 30.

d. From S1, ping S2, S3, or MLS to verify connectivity with VLAN 99.

e. To verify inter-VLAN routing, ping devices outside the sender's VLAN.

f. From any device, ping this address inside **Cloud**, 209.165.200.226.

The Layer 3 switch is now routing between VLANs and providing routed connectivity to the cloud.

3. CONFIGURE IPV6 INTER-VLAN ROUTING

Layer 3 switches also route between IPv6 networks.

1. ENABLE IPV6 ROUTING.

Enter the **ipv6 unicast-routing** command to enable IPv6 routing in global configuration mode.

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

2. CONFIGURE SVI FOR IPV6 ON MLS.

Configure IPv6 addressing on SVI for VLANs 10, 20, and 30 according to the Addressing Table. The configuration for VLAN 10 is shown below.

```
MLS(config)# interface vlan 10
MLS(config-if)# ipv6 address 2001:db8:acad:10::1/64
```

3. CONFIGURE G0/2 WITH IPV6 ON MLS.

a. Configure IPv6 addressing on G0/2.

```
MLS(config)# interface G0/2
MLS(config-if)# ipv6 address 2001:db8:acad:a::1/64
```

b. Use the **show ipv6 route** command to verify IPv6 connected networks.

MLS# **show ipv6 route**

```
IPv6 Routing Table - 10 entries
```

```
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
     via 2001:DB8:ACAD:A::2, GigabitEthernet0/2
C   2001:DB8:ACAD:A::/64 [0/0]
     via ::, GigabitEthernet0/2
L   2001:DB8:ACAD:A::1/128 [0/0]
     via ::, GigabitEthernet0/2
C   2001:DB8:ACAD:10::/64 [0/0]
     via ::, Vlan10
L   2001:DB8:ACAD:10::1/128 [0/0]
     via ::, Vlan10
C   2001:DB8:ACAD:20::/64 [0/0]
     via ::, Vlan20
L   2001:DB8:ACAD:20::1/128 [0/0]
     via ::, Vlan20
C   2001:DB8:ACAD:30::/64 [0/0]
     via ::, Vlan30
L   2001:DB8:ACAD:30::1/128 [0/0]
     via ::, Vlan30
L   FF00::/8 [0/0]
     via ::, Null0
```

4. VERIFY IPV6 CONNECTIVITY.

Devices PC3, PC4, and PC5 have been configured with IPv6 addresses. Verify IPv6 inter-VLAN routing and connectivity to **Cloud**.

a. From PC3, ping MLS to verify connectivity within VLAN 10.

b. From PC4, ping MLS to verify connectivity within VLAN 20.

c. From PC5, ping MLS to verify connectivity within VLAN 30.

d. To verify inter-VLAN routing, ping between devices PC3, PC4, and PC5.

e. From PC3 ping the address inside **Cloud**, 2001:db8:acad:a::2.

PRAKTIKUM

Download file Packet Tracer pada link di bawah ini :

https://bit.ly/Modul1_JaringanKomputer_2021

Praktikum dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. Petunjuk pengerjaan praktikum juga dapat dilihat pada perintah dibawah. Pengerjaan praktikum diselesaikan sebelum berlangsungnya kegiatan praktikum. Ketika jam praktikum berlangsung praktikan menyiapkan hasil pengerjaanya yang kemudian di demokan ke asisten.

PRAKTIKUM 1

Packet Tracer - VLAN Configuration

Addressing Table

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

1. OBJECTIVES

   Part 1: Verify the Default VLAN Configuration

   Part 2: Configure VLANs

   Part 3: Assign VLANs to Ports

BACKGROUND

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

1. VIEW THE DEFAULT VLAN CONFIGURATION

1. DISPLAY THE CURRENT VLANS.

On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.

2. VERIFY CONNECTIVITY BETWEEN PCS ON THE SAME NETWORK.

Notice that each PC can ping the other PC that shares the same subnet.

- PC1 can ping PC4
- PC2 can ping PC5
- PC3 can ping PC6

Pings to hosts on other networks fail.

What benefits can VLANs provide to the network?

2. CONFIGURE VLANS

1. CREATE AND NAME VLANS ON S1.

a. Create the following VLANs. Names are case-sensitive and must match the requirement exactly:

- VLAN 10: Faculty/Staff

```
S1#(config)# vlan 10
S1#(config-vlan)# name Faculty/Staff
```

b. Create the remaining VLANS.

- VLAN 20: Students
- VLAN 30: Guest(Default)
- VLAN 99: Management&Native
- VLAN 150: VOICE

2. VERIFY THE VLAN CONFIGURATION.

Which command will only display the VLAN name, status, and associated ports on a switch?

3. CREATE THE VLANS ON S2 AND S3.

Use the same commands from Step 1 to create and name the same VLANs on S2 and S3.

4. VERIFY THE VLAN CONFIGURATION.

3. ASSIGN VLANS TO PORTS

1. ASSIGN VLANS TO THE ACTIVE PORTS ON S2.

a. Configure the interfaces as access ports and assign the VLANs as follows:

- VLAN 10: FastEthernet 0/11

S2(config)# **interface f0/11**
S2(config-if)# **switchport mode access**
S2(config-if)# **switchport access vlan 10**

b. Assign the remaining ports to the appropriate VLAN.

- VLAN 20: FastEthernet 0/18
- VLAN 30: FastEthernet 0/6

2. ASSIGN VLANS TO THE ACTIVE PORTS ON S3.

S3 uses the same VLAN access port assignments as S2. Configure the interfaces as access ports and assign the VLANs as follows:

- VLAN 10: FastEthernet 0/11
- VLAN 20: FastEthernet 0/18
- VLAN 30: FastEthernet 0/6

3. ASSIGN THE VOICE VLAN TO FASTETHERNET 0/11 ON S3.

As shown in the topology, the S3 FastEthernet 0/11 interface connects to a Cisco IP Phone and PC4. The IP phone contains an integrated three-port 10/100 switch. One port on the phone is labeled Switch and connects to F0/4. Another port on the phone is labeled PC and connects to PC4. The IP phone also has an internal port that connects to the IP phone functions.

The S3 F0/11 interface must be configured to support user traffic to PC4 using VLAN 10 and voice traffic to the IP phone using VLAN 150. The interface must also enable QoS and trust the Class of Service (CoS) values assigned by the IP phone. IP voice traffic requires a minimum amount of throughput to support acceptable voice communication quality. This command helps the switchport to provide this minimum amount of throughput.

```
S3(config)# interface f0/11
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
```

4. VERIFY LOSS OF CONNECTIVITY.

Previously, PCs that shared the same network could ping each other successfully.

Study the output of from the following command on **S2** and answer the following questions based on your knowledge of communication between VLANS. Pay close attention to the Gig0/1 port assignment.

```
S2# show vlan brief
VLAN Name                              Status    Ports
```

```
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   Faculty/Staff                    active    Fa0/11
20   Students                         active    Fa0/18
30   Guest(Default)                   active    Fa0/6
99   Management&Native                active
150  VOICE                            active
```

Try pinging between PC1 and PC4.

Although the access ports are assigned to the appropriate VLANs, were the pings successful? Explain.

What could be done to resolve this issue?

PRAKTIKUM 2

Packet Tracer - Configure Trunks

1. ADDRESSING TABLE

Device	Interface	IP Address	Subnet Mask	Switch Port	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S2 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S2 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S2 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S3 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S3 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S3 F0/6	30

2. OBJECTIVES

Part 1: Verify VLANs

Part 2: Configure Trunks

3. BACKGROUND

Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A

trunk port by default is a member of all VLANs. Therefore, it carries traffic for all VLANs. This activity focuses on creating trunk ports and assigning them to a native VLAN other than the default.

1. INSTRUCTIONS

1. VERIFY VLANS

1. DISPLAY THE CURRENT VLANS.

a. On **S1**, issue the command that will display all VLANs configured. There should be ten VLANs in total. Notice that all 26 access ports on the switch are assigned to VLAN 1.

b. On **S2** and **S3**, display and verify that all the VLANs are configured and assigned to the correct switch ports according to the **Addressing Table**.

2. VERIFY LOSS OF CONNECTIVITY BETWEEN PCS ON THE SAME NETWORK.

Ping between hosts on the same the VLAN on the different switches. Although **PC1** and **PC4** are on the same network, they cannot ping one another. This is because the ports connecting the switches are assigned to VLAN 1 by default. In order to provide connectivity between the PCs on the same network and VLAN, trunks must be configured.

2. CONFIGURE TRUNKS

1. CONFIGURE TRUNKING ON S1 AND USE VLAN 99 AS THE NATIVE VLAN.

a. Configure G0/1 and G0/2 interfaces on S1 for trunking.

```
S1(config)# interface range g0/1 - 2
S1(config-if)# switchport mode trunk
```

b. Configure VLAN 99 as the native VLAN for G0/1 and G0/2 interfaces on **S1**.

S1(config-if)# **switchport trunk native vlan 99**

The trunk port takes about a short time to become active due to Spanning Tree Protocol. Click **Fast Forward Time** to speed the process. After the ports become active, you will periodically receive the following syslog messages:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet0/2 (99), with S3 GigabitEthernet0/2 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet0/1 (99), with S2 GigabitEthernet0/1 (1).
```

You configured VLAN 99 as the native VLAN on S1. However, S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.

Although you have a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Explain.

2. VERIFY TRUNKING IS ENABLED ON S2 AND S3.

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3. You will learn more about DTP later in the course.

Which active VLANs are allowed to cross the trunk?

3. CORRECT THE NATIVE VLAN MISMATCH ON S2 AND S3.

a. Configure VLAN 99 as the native VLAN for the appropriate interfaces on S2 and S3.

b. Issue **show interface trunk** command to verify the correct native VLAN configuration.

4. VERIFY CONFIGURATIONS ON S2 AND S3.

. Issue the **show interface** *interface* **switchport** command to verify that the native VLAN is now 99.

a. Use the **show vlan** command to display information regarding configured VLANs.

Why is port G0/1 on S2 no longer assigned to VLAN 1?

DETAIL PENILAIAN TUGAS

Tugas	30%
Praktikum 1	30%
Praktikum 2	40%