VERSION 1

JULI , 2022

[PRAKTIKUM JARINGAN KOMPUTER]

KONSEP SWITCH, VLANS, DAN INTER-VLAN ROUTING – MODUL 2

TIM PENYUSUN :

MAHAR FAIQURAHMAN, S.KOM, M.T

ALIF SYIFA ARSYILA

ARIEL BAGUS AR – RASYIID

PRESENTED BY: LAB - INFORMATIKA

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

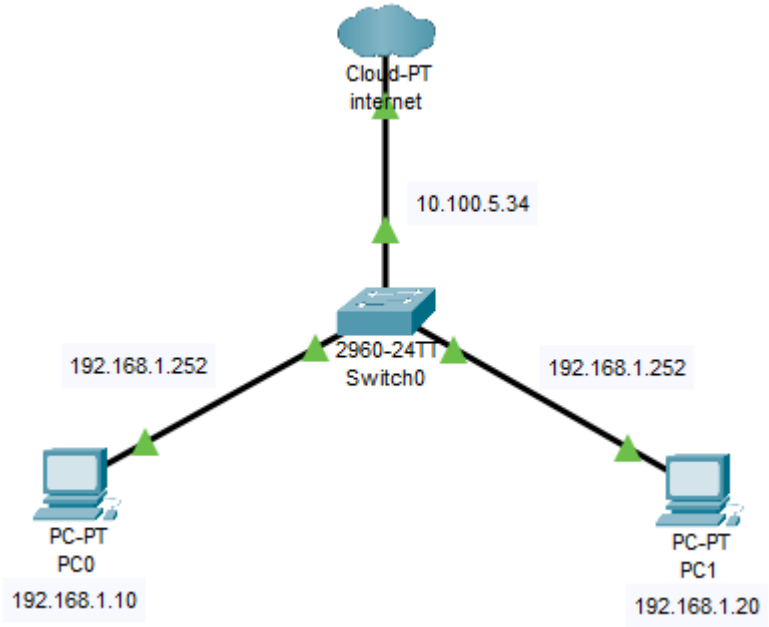
- Komputer/Latop
- Sistem operasi Windows/ Linux/ Mac OS
- Simulator Packet Tracer

MATERI POKOK

1. SWITCH

Switch adalah sebuah perangkat jaringan pada komputer yang memungkinkan untuk menghubungkan perangkat pada sebuah jaringan komputer dengan menggunakan pertukaran paket untuk menerima, memproses, dan mengirimkan data dari satu perangkat ke perangkat lainnya ataupun sebaliknya.

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). Switch melakukan *bridging* transparan (penghubung segementasi banyak jaringan dengan forwarding berdasarkan alamat MAC).

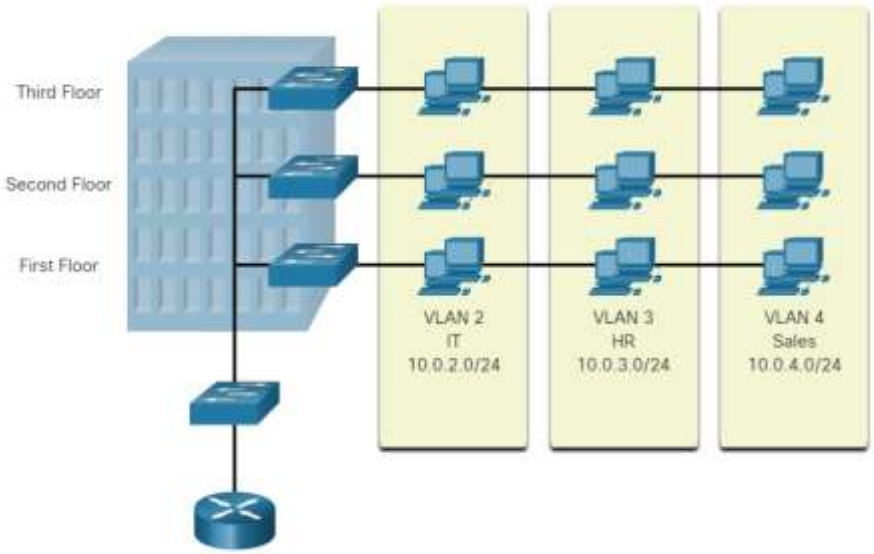


Cara kerja switch ialah dengan cara menerima paket data pada suatu port lalu akan melihat MAC (Media Access Control) tujuannya dan juga membangun sebuah koneksi logika dengan port yang sudah terhubung dengan node ataupun perangkat tujuan, sehingga selain port yang dituju tidak bisa menerima paket data yang dikirimkan dan akan mengurangi terjadinya tabrakan data atau disebut juga dengan collision. Setiap perangkat yang terhubung ke port tertentu, MAC addsernya dan akan dicatat di MAC address table yang nantinya akan disimpan pada memori chache switch, itulah bagaimana switch bekerja.

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 di atas, 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)

- **CARA KERJA VLAN**

Secara umum, cara kerja VLAN yakni menghubungkan semua perangkat komputer dalam lebih dari satu jaringan Local Area Network. Jaringan VLAN menyediakan akses data ke semua client komputer yang terhubung ke switch dan diberi ID yang sama. Server VLAN pada dasarnya membuat domain broadcastnya sendiri, memisahkan jaringan fisik menjadi beberapa jaringan logis. Di atas kertas, lalu lintas komunikasi VLAN diatur oleh server, kemudian switch memastikan bahwa data pergi dan diakses ke proses selanjutnya seperti LAN pada umumnya.

➢ PERINTAH PEMBUATAN VLAN

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`

➢ PERINTAH PENUGASAN PORT 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.

➢ PERINTAH INFORMASI VLAN

Tabel di bawah ini 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`

3. VLAN Data dan Suara

VLAN data memiliki fungsi utama untuk mengatur lalu lintas data yang terjadi dalam sebuah jaringan VLAN. Sedangkan VLAN suara Secara garis besar adalah jaringan yang sudah mendukung layanan VoIP dan sudah dirancang khusus untuk menunjang kebutuhan komunikasi berbasis suara.

4. VLAN Trunks

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 table dibawah ini.

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`

5. 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.

AKTIVITAS MANDIRI

Agar mempermudah pemahaman terhadap konsep Switch, VLAN, dan Inter-VLAN , silahkan kerjakan task percobaan dibawah ini. Packet tracer dapat di unduh melalui link berikut :

https://bit.ly/jarkom2022UMM

Note : Di mohon untuk menunjukkan hasil percobaan ini kepada asisten ketika kegiatan praktikum berlangsung. Semangat ☺

KONFIGURASI VLAN

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

Langkah 1 : Lihat default dari konfigurasi VLAN yang tersedia.

a. Ketikkan **show vlan brief** untuk menampilkan semua VLAN yang dikonfigurasi. Secara default, semua interface ditetapkan ke VLAN 1.

```
S1>enable
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
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

b. Periksa dan pastikan apakah setiap PC dapat melakukan ping ke PC lain yang berbagi subnet yang sama pada jaringan yang sama.

- PC 1 dapat melakukan ping ke PC 4

- PC 2 dapat melakukan ping ke PC 5
- PC 3 dapat melakukan ping ke PC 6

Langkah 2 : Konfigurasi VLAN.

a. Buat dan beri nama VLAN pada S1 sesuai dengan ketentuan di bawah :

- VLAN 10: Faculty/Staff
- VLAN 20: Students
- VLAN 30: Guest(Default)
- VLAN 99: Management&Native
- VLAN 150: VOICE

Note : Nama peka terhadap huruf besar dan kecil

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name Faculty/Staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name Students
S1(config-vlan)#vlan 30
S1(config-vlan)#name Guest(Default)
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#vlan 150
S1(config-vlan)#name VOICE
S1(config-vlan)#
```

b. Buat dan beri nama VLAN pada S2 dan S3 dengan perintah yang sama dari langkah sebelmnya untuk membuat dan memberi nama VLAN yang sama pada S2 dan S3.

c. Verifikasi semua konfigurasi dengan mengetikkan **show vlan brief** pada S1, S2, dan S3, hingga terlihat bahwa VLAN yang kita buat sudah terkonfigurasi.

```
S1>enable
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
                                                Gig0/1, Gig0/2
10   Faculty/Staff                    active
20   Students                         active
30   Guest(Default)                   active
99   Management&Native                active
150  VOICE                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

Langkah 3 : Tetapkan VLAN ke port aktif di S2 dan S3.

a. Konfigurasi interface sebagai port akses dan tetapkan VLAN sebagai berikut:

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

```
S2(config-vlan)#exit
S2(config)#interface f0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#exit
S2(config)#interface f0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#
```

Note : Switch port digunakan untuk mengelola interface fisik dan protokol Layer 2 terkait dan tidak menangani routing ataupun bridging. Terdapat beberapa mode switchport diantaranya :

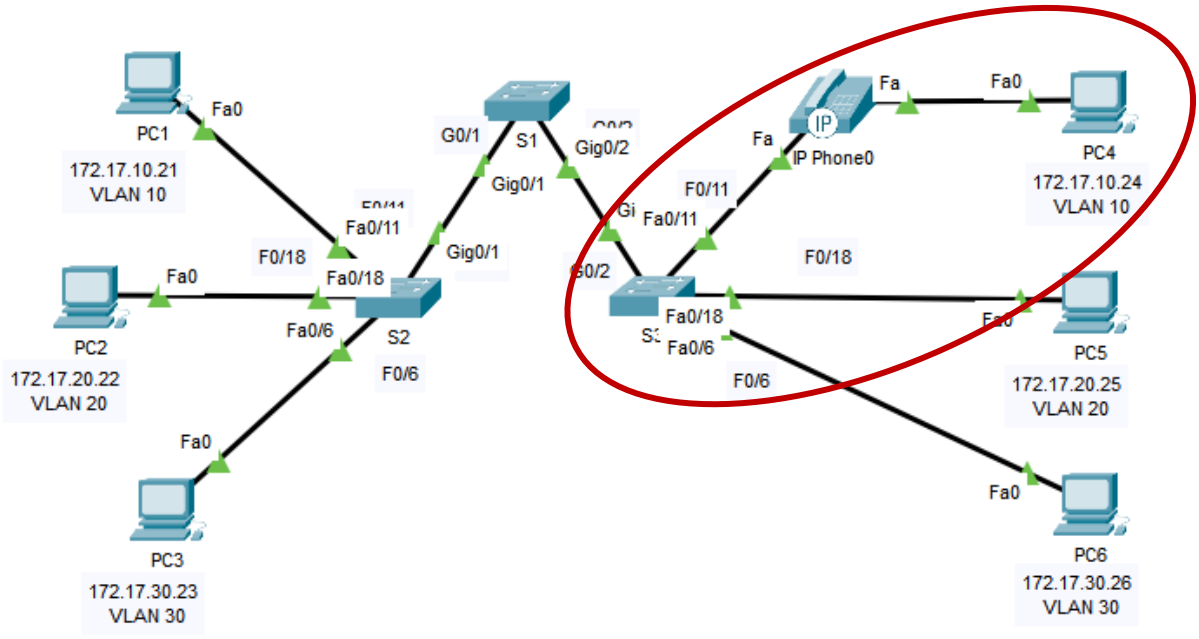
- Mode Access : akan memaksa port menjadi port akses sementara dan perangkat apa pun yang dicolokkan ke port ini hanya akan dapat berkomunikasi dengan perangkat lain yang berada di VLAN yang sama.
- Mode trunk : Sebuah port trunk dapat membawa traffic dalam satu atau lebih VLAN pada link fisik yang sama. Secara default, interface trunk dapat membawa traffic untuk semua VLAN (dalam artian jika kita memiliki beberapa VLAN, agar dapat tersambung trafficnya ya menggunakan mode trunk ini sebagai bridging.

b. Lakukan langkah yang sama seperti langkah sebelumnya pada S3 untuk mengkonfigurasi interface sebagai port akses dan tetapkan VLAN sesuai dengan langkah sebelumnya.

c. Konfigurasi VOICE VLAN ke FastEthernet 0/11 di S3. Gunakan perintah seperti di bawah ini :

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

Mengapa kita perlu melakukan langkah ini (langkan 3.c) ???



Jika kita perhatikan pada topologi di atas, antarmuka S3 FastEthernet 0/11 terhubung ke Cisco IP Phone dan PC4 (ada dia diantara kita :v [ada telepon di antara S3 dan PC 4]). Satu port di telepon diberi label Switch dan terhubung ke F0/4. Port lain di telepon diberi label PC dan terhubung ke PC4. Hal ini memungkinkan lalu lintas terhambat, sehingga kita perlu melakukan konfigurasi untuk mendukung lalu lintas pengguna ke PC4 menggunakan VLAN 10 dan lalu lintas suara ke telepon IP menggunakan VLAN 150. Maka dari itu langkah ini membantu switchport untuk menyediakan jumlah throughput minimum untuk mendukung kualitas komunikasi suara yang dapat diterima. Paham yak ? :v semoga paham ☺

Langkah 4 : Verifikasi hilangnya konektivitas.

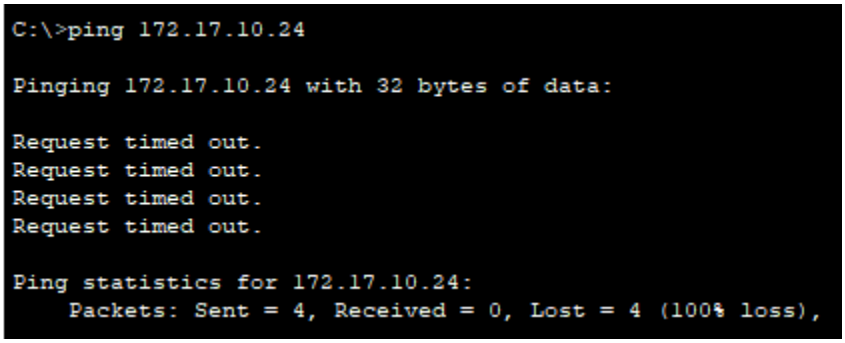
a. Gunakan perintah **show vlan brief** untuk memastikan apakah langkah sebelumnya sudah terkonfigurasi.

```
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
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S2#
```

b. Verifikasi konektivitas antar PC :

- PC 1 dapat melakukan ping ke PC 4
- PC 2 dapat melakukan ping ke PC 5
- PC 3 dapat melakukan ping ke PC 6



Sebelumnya, PC yang berbagi jaringan yang sama dapat melakukan ping satu sama lain dengan sukses. Setelah langkah-langkah di atas di laksanakan maka akan terjadi RTO ketika kita melakukan pengecekan konektivitas kembali. Kenapa ?? karena antara S2 dan S1 dengan S1 dan S3 berada dalam mode akses (sudah tau kan mode akses yang sudah saya terangkan di atas). Jadi , ping gagal karena port antara switch ada di VLAN 1 dan PC1 dan PC4 ada di VLAN 10.

Lalu bagaimana cara mengatasi ini ?? Solusinya adalah menjadikan tautan tersebut menjadi trunking. Kemudian bagaimana cara kita membuat tautan trunk ??

Nah hal itu yang akan menjadi PR kalian di bagian TUGAS setelah percobaan ini. OK ?? selamat mencobaaaa ☺

PRE-PRAKTIKUM

Tugas yang dilakukan yaitu mengerjakan aktivitas konfigurasi trunk menggunakan paket tracer yang sudah di sediakan di tautan berikut ini :

https://bit.ly/jarkom2022UMM

Konfigurasi harus dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. 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**.

Kemudian buatlah laporan tertulis sebagai bukti pemahaman kalian terhadap pekerjaan yang kalian kerjakan. Laporan ini akan di cek, apabila ada kesamaan kata-kata dan penjelasan, maka akan dilakukan pengurangan nilai (menghindari CTRL+C dan CTRL+V). Format laporan **Tugas-nama-nim.pdf**.

Tugas dikumpulkan di infotech.umm.ac.id pada bagian attachment **sebelum** berlangsungnya kegiatan praktikum.

CONFIGURE TRUNK

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

OBJECTIVES

Part 1: Verify VLANs

Part 2: Configure Trunks

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.

INSTRUCTIONS

PART 1: VERIFY VLANS

STEP 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**.

STEP 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.

PART 2: CONFIGURE TRUNKS

STEP 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.

Question:

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

STEP 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.

Question:

Which active VLANs are allowed to cross the trunk?

Type your answers here.

STEP 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.

STEP 4: VERIFY CONFIGURATIONS ON S2 AND S3.

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

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

Question:

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

PRAKTIKUM

Download file Packet Tracer pada link di bawah ini :

https://bit.ly/jarkom2022UMM

Praktikum dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. Petunjuk pengerjaan praktikum juga dapat dilihat pada perintah dibawah. Praktikum akan dilaksanakan secara **live configuration**, yang akan dilakukan secara **real time** pada saat jam praktikum dilaksanakan. Jadi tolong dipersiapkan dan dipelajari dengan sungguh-sungguh agar tidak menghambat kelancaran jalannya praktikum. Terimakasih

IMPLEMENTS VLANS AND TRUNKING

ADDRESSING TABLE

Device	Interface	IP Address	Subnet Mask	Switchport	VLAN
PC1	NIC	192.168.10.10	255.255.255.0	SWB F0/1	VLAN 10
PC2	NIC	192.168.20.20	255.255.255.0	SWB F0/2	VLAN 20
PC3	NIC	192.168.30.30	255.255.255.0	SWB F0/3	VLAN 30
PC4	NIC	192.168.10.11	255.255.255.0	SWC F0/1	VLAN 10
PC5	NIC	192.168.20.21	255.255.255.0	SWC F0/2	VLAN 20
PC6	NIC	192.168.30.31	255.255.255.0	SWC F0/3	VLAN 30
PC7	NIC	192.168.10.12	255.255.255.0	SWC F0/4	VLAN 10 VLAN 40 (Voice)
SWA	SVI	192.168.99.252	255.255.255.0	N/A	VLAN 99
SWB	SVI	192.168.99.253	255.255.255.0	N/A	VLAN 99
SWC	SVI	192.168.99.254	255.255.255.0	N/A	VLAN 99

OBJECTIVES

Part 1: Configure VLANs

Part 2: Assign Ports to VLANs

Part 3: Configure Static Trunking

Part 4: Configure Dynamic Trunking

BACKGROUND

You are working in a company that is getting ready to deploy a set of new 2960 switches in a branch office. You are working in the lab to test out the VLAN and trunking configurations that are planned. Configure and test the VLANs and trunks.

INSTRUCTIONS

PART 1: CONFIGURE VLANS

Configure VLANs on all three switches. Refer to the VLAN Table. Note that the VLAN names must match the values in the table exactly.

VLAN Table

VLAN Number	VLAN Name
10	Admin
20	Accounts
30	HR
40	Voice
99	Management
100	Native

PART 2: ASSIGN PORTS TO VLANS

STEP 1: ASSIGN ACCESS PORTS TO VLANS

On SWB and SWC, assign ports to the VLANs. Refer to the Addressing Table.

STEP 2: CONFIGURE THE VOICE VLAN PORT

Configure the appropriate port on switch SWC for voice VLAN functionality.

STEP 3: CONFIGURE THE VIRTUAL MANAGEMENT INTERFACES

a. Create the virtual management interfaces, on all three switches.

b. Address the virtual management interfaces according to the Addressing Table.

c. The switches should not be able to ping each other.

PART 3: CONFIGURE STATIC TRUNKING

a. Configure the link between SWA and SWB as a static trunk. Disable dynamic trunking on this port.

b. Disable DTP on the switch port on both ends of the trunk link.

c. Configure the trunk with the native VLAN and eliminate native VLAN conflicts if any.

PART 4: CONFIGURE DYNAMIC TRUNKING

a. Assume that the trunk port on SWC is set to the default DTP mode for 2960 switches. Configure G0/2 on SWA so that it successfully negotiates trunking with SWC.

b. Configure the trunk with the native VLAN and eliminate native VLAN conflicts if any.

RUBRIK PENILAIAN

Pemahaman Materi	10%
Pre-praktikum	20%
Praktikum	70%