

VERSI 2.0
AGUSTUS 2025



PRAKTIKUM JARINGAN KOMPUTER

**MODUL 2 MATERI PRAKTIKUM - KONSEP SWITCH, VLANS, DAN
INTER-VLAN ROUTING**

DISUSUN OLEH:

Ir. Mahar Faiqurahman, S.Kom., M.T.

Taufiq Ramadhan

Sutrisno Adit Pratama

TIM LABORATORIUM INFORMATIKA
UNIVERSITAS MUHAMMADIYAH MALANG

PENDAHULUAN

TUJUAN

1. Mahasiswa mampu memahami dan mengimplementasi konsep Switching.
2. Mahasiswa mampu memahami dan mengimplementasi Vlan.
3. Mahasiswa mampu memahami dan mengimplementasi Inter-Vlan Routing.

TARGET MODUL

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

PERSIAPAN MATERI

1. Konsep Switch
2. Vlans
3. Inter-Vlans Routing

PERSIAPAN SOFTWARE DAN HARDWARE

1. Komputer/Laptop
2. Sistem operasi Windows/ Linux/ MacOS
3. Simulator Packet Tracer - https://bit.ly/jarkom_2025_umm

KEYWORDS

Konsep Switch, Vlans, Inter-Vlans Routing



DAFTAR ISI

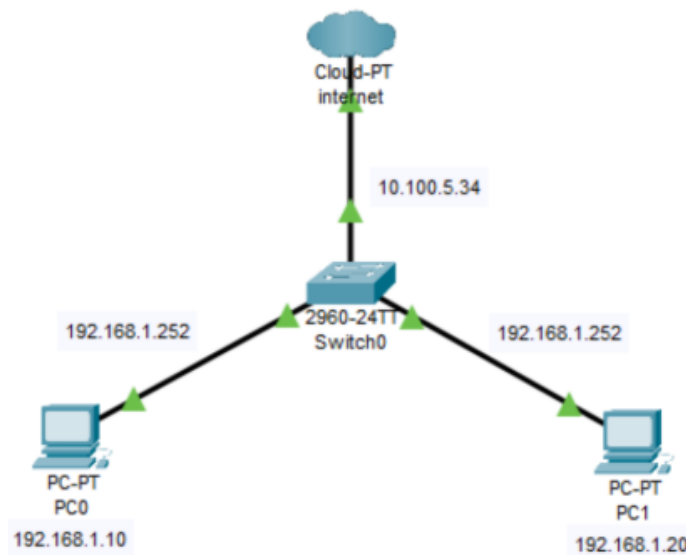
PENDAHULUAN.....	2
TUJUAN.....	2
TARGET MODUL.....	2
PERSIAPAN MATERI.....	2
PERSIAPAN SOFTWARE DAN HARDWARE.....	2
KEYWORDS.....	2
DAFTAR ISI.....	3
Materi Pokok.....	4
SWITCH.....	4
VLANS.....	4
Cara Kerja VLAN.....	5
Perintah Pembuatan Vlan.....	5
Perintah Penetapan Port VLAN.....	6
Perintah Untuk Informasi VLAN.....	6
Data dan Voice VLAN.....	7
Perbedaan Utama Data VLAN dan Voice VLAN.....	7
VLAN TRUNKS.....	7
INTER-VLAN ROUTING.....	8
CODELAB 1.....	9
Konfigurasi VLAN.....	9
Addressing Table.....	9
Tujuan.....	9
Latar Belakang.....	9
Bagian 1: Melihat default dari konfigurasi VLAN yang tersedia.....	9
Bagian 2: Konfigurasi VLAN.....	10
Bagian 3: Menetapkan VLAN ke Port.....	11
CODELAB 2.....	15
MASALAH.....	15
SOLUSI.....	15
Addressing Table.....	15
Latar Belakang.....	16
Instruksi.....	16
Bagian 1: Verifikasi VLANS.....	16
Bagian 2: Mengkonfigurasi Trunk.....	16
RUBRIK PENILAIAN.....	17



Materi Pokok

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 segmentasi banyak jaringan dengan forwarding berdasarkan alamat MAC).

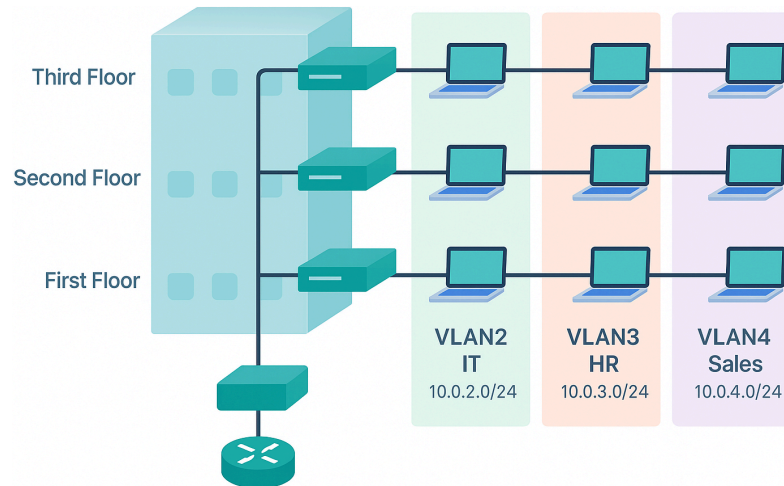


Cara kerja switch ialah dengan cara menerima paket data pada suatu port lalu akan melihat MAC (Media Access Control) tujuannya dan juga membangun sebuah koneksi logika dengan port yang sudah terhubung dengan node ataupun perangkat tujuan, sehingga selain port yang dituju tidak bisa menerima paket data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

VLANS

Virtual Local Area Network atau VLAN adalah sekumpulan perangkat yang ada di satu atau lebih jaringan LAN dan dikonfigurasi 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, HR, dan Sales) 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 switch hanya dapat ditetapkan ke satu VLAN (kecuali untuk port yang terhubung ke telepon IP atau ke switch 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 switch dan memberinya nama. Penamaan setiap VLAN dianggap sebagai praktik terbaik dalam konfigurasi switch.

Task	IOS Command
Masuk ke mode konfigurasi global.	Switch# configure terminal



Buat VLAN dengan nomor ID yang valid.	Switch(config)# vlan vlan-id
Menentukan nama unik untuk mengidentifikasi VLAN.	Switch(config-vlan)# name vlan-name
Kembali ke mode privileged EXEC.	Switch(config-vlan)# end

Perintah Penetapan Port VLAN

Tabel menampilkan sintaks untuk menentukan port menjadi port akses dan menentukannya 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
Masuk ke mode global configuration.	Switch# configure terminal
Masuk ke mode interface configuration.	Switch(config)# interface interface-id
Atur port ke access mode.	Switch(config-if)# switchport mode access
Tetapkan port ke sebuah VLAN.	Switch(config-if)# switchport access vlan vlan-id
Kembali ke mode privileged EXEC.	Switch(config-if)# end

Catatan : Gunakan perintah **interface range** untuk secara bersamaan mengkonfigurasi beberapa antarmuka.

Perintah Untuk Informasi VLAN

Tabel di bawah ini menjelaskan opsi perintah show vlan :

Task	Command Option
------	----------------



Menampilkan VLAN name, status, dan port yang dimilikinya (satu VLAN per baris).	brief
Menampilkan informasi tentang VLAN ID tertentu. Untuk <i>vlan-id</i> , rentangnya adalah 1 sampai 4094.	id vlan-id
Menampilkan informasi tentang VLAN name tertentu. <i>vlan-name</i> berupa string ASCII dari 1 sampai 32 karakter.	name vlan-name
Menampilkan ringkasan informasi VLAN.	summary

Data dan Voice VLAN

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

Perbedaan Utama Data VLAN dan Voice VLAN

Fitur	VLAN Data	VLAN Suara (Voice VLAN)
Fungsi Utama	Menangani lalu lintas data umum (web, email, file)	Menangani lalu lintas VoIP (panggilan suara) secara khusus
Sensitivitas Terhadap Delay	Rendah	Sangat Tinggi
Prioritas Jaringan (QoS)	Normal	Tinggi
Contoh Perangkat	PC, Laptop, Server, Printer	IP Phone, Softphone, IP PBX

VLAN TRUNKS

VLAN Trunk adalah tautan Layer 2 antara dua switch yang membawa lalu lintas untuk semua VLAN (kecuali daftar VLAN yang diizinkan dibatasi secara manual atau dinamis). Untuk



mengaktifkan tautan trunk, konfigurasi port interkoneksi dengan set perintah konfigurasi antarmuka yang ditunjukkan pada tabel dibawah ini.

Tugas	IOS Command
Masuk ke mode global configuration.	Switch# configure terminal
Masuk ke mode interface configuration.	Switch(config)# interface interface-id
Atur port ke permanent trunking mode.	Switch(config-if)# switchport mode trunk
Set native VLAN ke selain VLAN 1.	Switch(config-if)# switchport trunk native vlan vlan-id
Tentukan daftar VLAN yang diizinkan pada trunk link.	Switch(config-if)# switchport trunk allowed vlan vlan-list
Kembali ke mode privileged EXEC.	Switch(config-if)# end

INTER-VLAN ROUTING

Inter VLAN routing merupakan proses mem-forward lalu lintas dari satu jaringan VLAN ke VLAN lain atau dengan kata lain menghubungkan 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 virtual interfaces (SVIs).**
Merupakan cara yang paling efektif dan efisien untuk skala jaringan menengah keatas.



CODELAB 1

Tugas yang dilakukan yaitu mengerjakan aktivitas “Vlan Configuration” menggunakan packet tracer yang sudah disediakan di tautan berikut ini:

https://bit.ly/modul-2_jarkom_2025_umm

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

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

Tujuan

Bagian 1: Memverifikasi konfigurasi VLAN bawaan

Bagian 2: Mengkonfigurasi VLAN

Bagian 3: Menetapkan VLAN ke Port

Latar Belakang

VLAN sangat membantu dalam pengelolaan grup-grup logis , memungkinkan anggota dari sebuah grup untuk dengan mudah dipindahkan, diubah, atau ditambahkan. Aktivitas ini berfokus pada pembuatan dan penamaan VLAN, serta penetapan access port ke VLAN tertentu.

Bagian 1: Melihat default dari konfigurasi VLAN yang tersedia.

Langkah 1: Tampilkan VLAN saat ini

Ketikkan **show vlan brief** untuk menampilkan semua VLAN yang dikonfigurasi. Secara default, semua interface ditetapkan ke VLAN 1.(SWITCH S1)



```

CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up







S1>en
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

```

Langkah 2: Memverifikasi konektivitas antar PC pada jaringan yang sama
 Pastikan setiap PC dapat melakukan ping ke PC lain yang berbagi subnet dan 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

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC1	PC4	ICMP		0.000	N	0
	Successful	PC2	PC5	ICMP		0.000	N	1
	Successful	PC3	PC6	ICMP		0.000	N	2

Jika melakukan ping ke host lain yang tidak sesuai vlan nya maka akan gagal karena berbeda vlan bisa dilihat pada gambar berikut

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	N
	Failed	PC1	PC6	ICMP		0.000	N	

Pertanyaan: Apa manfaat yang dapat diberikan VLAN ke jaringan?

Bagian 2: Konfigurasi VLAN.

- 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

```

S1>en
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)#

```

- Buat dan beri nama VLAN pada S2 dan S3 dengan perintah yang sama dari langkah sebelumnya untuk membuat dan memberi nama VLAN yang sama pada S2 dan S3.
- Verifikasi semua konfigurasi dengan mengetikkan **show vlan brief** pada S1, S2, dan S3, hingga terlihat bahwa VLAN yang kita buat sudah terkonfigurasi.

```

S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/5, Fa0/9, Fa0/13, Fa0/17, Fa0/21, Gig0/1
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#

```

Bagian 3: Menetapkan VLAN ke Port

Langkah 1: Tetapkan VLAN ke port aktif di (S2 dan S3).

- 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>en
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#interface f0/6
S2(config-if)#switchport mode access
S2(config-if)#switch 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 padalink fisik yang sama. Secara default, interface trunk dapat membawa traffic untuk semua VLAN (dalam artian jika kita memiliki beberapa VLAN, agar dapat tersambung traffiknya menggunakan mode trunk ini sebagai bridging.

b. Konfigurasi S3 sebagai port akses dan tetapkan VLAN, mengikuti langkah-langkah yang sama seperti sebelumnya.

Langkah 2: Konfigurasi VOICE VLAN ke FastEthernet 0/11 di S3.

Seperti yang ditunjukkan pada topologi, interface FastEthernet 0/11 pada S3 terhubung ke sebuah Cisco IP Phone dan PC4. IP phone tersebut memiliki switch tiga-port 10/100 yang terintegrasi. Satu port pada telepon diberi label Switch dan terhubung ke F0/4. Port lainnya diberi label PC dan terhubung ke PC4. IP phone tersebut juga memiliki port internal yang terhubung ke fungsi-fungsi telepon IP.

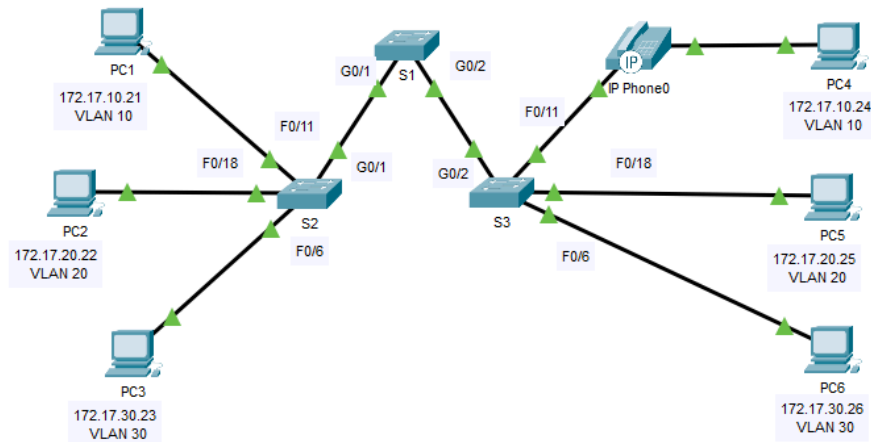
Interface F0/11 pada S3 harus dikonfigurasi untuk mendukung lalu lintas pengguna ke PC4 menggunakan VLAN 10 dan lalu lintas suara (voice) ke IP phone menggunakan VLAN 150. Interface tersebut juga harus mengaktifkan QoS dan memercayai nilai Class of Service (CoS) yang ditetapkan oleh IP phone. Lalu lintas suara IP memerlukan jumlah throughput minimum untuk mendukung kualitas komunikasi suara yang dapat diterima. Perintah ini membantu switchport untuk menyediakan jumlah throughput minimum tersebut.

Gunakan perintah seperti di bawah ini :

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface f0/11
S3(config-if)#mls qos trust cos
S3(config-if)#switchport voice vlan 150
S3(config-if)#
```

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





Langkah 3: Verifikasi hilangnya konektivitas.

- Gunakan perintah `show vlan brief` untuk memastikan apakah langkah sebelumnya sudah terkonfigurasi.

SWITCH 2 (S2)

```
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	

SWITCH 3 (S3)









```
S3#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	Fa0/11
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

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

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	E
	Failed	PC1	PC4	ICMP		0.000	N	0	
	Failed	PC2	PC5	ICMP		0.000	N	1	
	Failed	PC3	PC6	ICMP		0.000	N	2	

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

Lalu bagaimana cara mengatasi connection gagal tersebut ?

Solusinya adalah menjadikan port antar switch(s1 dan s2 ke s3) sebagai trunk port, bukan access port. Dengan begitu, port tersebut bisa membawa lalu lintas dari banyak VLAN sekaligus, termasuk VLAN 10 yang digunakan oleh PC1 dan PC4.

Hal itu yang akan menjadi tugas kalian melakukan konfigurasi trunking pada CODELAB-2 lalu melakukan verifikasi koneksi dengan mencoba ping antar PC di VLAN yang sama untuk memastikan semua perangkat dapat saling terhubung. Selain itu, pastikan port yang terhubung ke PC tetap sebagai access port agar perangkat akhir tetap berada di VLAN yang benar.



CODELAB 2

MASALAH

Port antar switch (S1 ↔ S3 dan S2 ↔ S3) saat ini masih dikonfigurasi sebagai access port, sehingga hanya mampu membawa satu VLAN saja. Hal ini menyebabkan PC1 dan PC4, yang berada di VLAN 10, tidak dapat saling berkomunikasi melalui S3, karena switch S3 tidak menerima frame dari VLAN 10. Kondisi ini mengakibatkan kegagalan koneksi jaringan dan membatasi kemampuan perangkat untuk berinteraksi sesuai segmentasi VLAN yang telah ditentukan. Masalah ini merupakan bagian penting dalam memahami bagaimana trunking VLAN bekerja dalam jaringan yang memiliki lebih dari satu VLAN.

SOLUSI

Solusi yang diterapkan adalah mengubah port antar switch menjadi trunk port. Dengan konfigurasi trunk, port dapat membawa frame dari berbagai VLAN secara bersamaan, termasuk VLAN 10 yang digunakan oleh PC1 dan PC4. Trunking memungkinkan switch untuk mengidentifikasi dan memisahkan traffic berdasarkan VLAN saat melewati port yang sama, sehingga perangkat di VLAN berbeda tetap dapat mengirim dan menerima data sesuai aturan VLAN masing-masing.

Kegiatan berikut merupakan aktivitas untuk konfigurasi Trunk. Gunakan file packet tracer yang sudah disediakan pada tautan berikut:

https://bit.ly/modul-2_jarkom_2025_umm

1. 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 praktikum-nama-nim.pka.
2. 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 COPAS).
Format laporan praktikum-nama-nim.pdf.
3. CODELAB dikumpulkan di infotech.umm.ac.id pada bagian attachment sebelum berlangsungnya kegiatan praktikum.

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

Latar Belakang

Trunk diperlukan untuk meneruskan informasi VLAN antar switch. Sebuah port pada switch bisa berupa access port atau trunk port. Access port membawa lalu lintas dari VLAN tertentu yang ditugaskan pada port tersebut. Trunk port secara default adalah anggota dari semua VLAN, sehingga dapat membawa lalu lintas untuk semua VLAN. Aktivitas ini berfokus pada pembuatan trunk port dan menetapkan native VLAN selain default.

Instruksi

Bagian 1: Verifikasi VLANS

Langkah 1: Tampilkan VLAN yang ada saat ini

- Pada S1, masukkan perintah untuk menampilkan semua VLAN yang dikonfigurasi. Seharusnya ada sepuluh VLAN secara total. Perhatikan bahwa semua 26 access port pada switch ditugaskan ke VLAN 1.
- Pada S2 dan S3, tampilkan dan verifikasi bahwa semua VLAN telah dikonfigurasi dan ditugaskan ke port switch yang benar sesuai dengan Addressing Table.

Langkah 2: Verifikasi hilangnya konektivitas antar PC di jaringan yang sama

Lakukan ping antar host pada VLAN yang sama di switch yang berbeda. Meskipun PC1 dan PC4 berada di jaringan yang sama, mereka tidak dapat saling ping. Hal ini karena port yang menghubungkan switch ditempatkan ke VLAN 1 secara default. Agar PC pada VLAN yang sama dapat saling berkomunikasi, trunk harus dikonfigurasi.

Bagian 2: Mengkonfigurasi Trunk

Langkah 1: Konfigurasi trunking pada S1 dan gunakan VLAN 99 sebagai native VLAN

- Konfigurasi interface G0/1 dan G0/2 pada S1 untuk trunking:

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

- Konfigurasi VLAN 99 sebagai native VLAN untuk interface G0/1 dan G0/2 pada S1:

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

Port trunk membutuhkan waktu singkat untuk menjadi aktif karena Spanning Tree Protocol. Klik *Fast Forward Time* untuk mempercepat proses. Setelah port menjadi aktif, kalian akan sesekali menerima pesan syslog berikut:




```
%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).
```

Kalian telah mengkonfigurasi VLAN 99 sebagai native VLAN di S1. Namun, S2 dan S3 masih menggunakan VLAN 1 sebagai native VLAN default, sebagaimana ditunjukkan oleh pesan syslog.

Pertanyaan:

Meskipun terdapat **native VLAN mismatch**, ping antar PC pada VLAN yang sama sekarang berhasil. Jelaskan!

Langkah 2: Verifikasi trunking di S2 dan S3

Pada S2 dan S3, ketikkan perintah `show interface trunk` untuk memastikan DTP berhasil menegosiasikan trunking dengan S1. Output juga menampilkan informasi mengenai interface trunk pada S2 dan S3.

Pertanyaan:

VLAN aktif mana saja yang diizinkan untuk melewati trunk?

Langkah 3: Perbaiki native VLAN mismatch pada S2 dan S3

- Konfigurasi VLAN 99 sebagai native VLAN pada interface yang sesuai di S2 dan S3.
- Untuk memverifikasi konfigurasi *native VLAN* yang benar, masukkan perintah `show interface trunk`.

Langkah 4: Verifikasi konfigurasi pada S2 dan S3

- Ketik perintah `show interface interface switchport` untuk memverifikasi bahwa native VLAN sekarang adalah 99.
- Gunakan perintah `show vlan` untuk menampilkan informasi mengenai VLAN yang dikonfigurasi.

Pertanyaan:

Mengapa port G0/1 pada S2 tidak lagi ditugaskan ke VLAN 1?

RUBRIK PENILAIAN

CODELAB 1	10%
CODELAB 2	10%
Pemahaman Materi	30%
Tugas Praktikum	50%

