

Modul Prapraktikum IF2230 Jaringan Komputer

1 - Perkenalan CPT, Frame Switching, LAN, VLAN, Subnetting

Dipersiapkan oleh:

妹ラボラトリー

(Asisten Laboratorium Sistem Terdistribusi)

Sister; **L**ab²²

START

Minggu, 9 Maret 2024, 21.00 WIB

END

Minggu, 16 Maret 2024, 23.59 WIB

Daftar Revisi

Belum ada revisi.

Latar Belakang

Praktikum pada mata kuliah ini baru diadakan di beberapa tahun kebelakang. Tujuan daripada praktikum ini adalah agar lulusan IF2230 mempunyai pengetahuan tentang jaringan komputer yang tidak hanya terbatas pada *theory* yang dipelajari di kelas, tetapi juga *practice* yang dilakukan di industri. **Maka, praktikum ini tidak selalu mengimplementasikan atau mengacu kepada materi-materi yang diajarkan di kelas, tetapi tetap berkaitan** (tidak seperti, misalnya IF2240 Basis Data yang praktikumnya *apple to apple* dengan materi kuliah).

Kemudian tugas prapraktikum ini ditujukan untuk mempersiapkan peserta untuk praktikum kuliah ini. Dengan menyelesaikan tugas ini, Anda diharapkan memiliki persiapan dan pengetahuan dasar terhadap materi yang dibutuhkan.

Berikut topik-topik yang menjadi lingkup modul ini:

- Perkenalan Cisco Packet Tracer
- Frame Switching
- LAN dan Subnetting
- VLAN

Peraturan

Kerjakan tugas ini dengan mengikuti peraturan-peraturan berikut.

1. Prapraktikum ini menjadi syarat untuk praktikum yang akan diadakan terkait modul ini. **Tidak mengumpulkan tugas/modul ini akan menyebabkan nilai praktikum 0.**
2. Kumpulkan tugas Anda sesuai dengan arahan pengumpulan yang terdapat pada bagian [Pengerjaan dan Deliverables](#). Kami berhak mengurangi nilai Anda jika pengumpulan yang Anda lakukan tidak sesuai arahan pengumpulan tersebut.
3. Seperti biasa, Anda **diperbolehkan** menggunakan sumber-sumber eksternal, termasuk internet, *large language model* seperti ChatGPT, serta meminta bantuan teman. Namun, sebelum meminta bantuan teman, Anda sangat **dianjurkan** untuk mencoba mengerjakan sendiri terlebih dahulu.

4. Anda tetap **dilarang** menyalin pekerjaan orang lain secara langsung, apalagi melakukan pengumpulan pekerjaan orang lain. Tolong bertanggung jawab atas pekerjaan Anda sendiri.
5. Anda **sangat dilarang** melakukan kecurangan atau tindakan apapun yang merugikan peserta IF2230 lain.
6. Terdapat beberapa *task* pada prapraktikum ini yang meminta Anda untuk melampirkan *screenshot*. **Semua *screenshot* harus dapat dibaca dengan jelas dan kami berhak mengurangi nilai Anda jika *screenshot* Anda tidak bisa dibaca.**
7. Praktikan yang mengumpulkan lewat dari tenggat waktu akan dikurangi nilai praktikumnya dengan proporsi yang sesuai tingkat keterlambatan (bukan dihitung sebagai tidak mengumpulkan).

Pengerjaan dan Deliverables

Kerjakan dan kumpulkan tugas ini dengan mengikuti semua ketentuan berikut.

1. Buatlah salinan dari dokumen ini dengan **File -> Make a copy**, kemudian kerjakan tugas-tugas ini pada salinan dokumen Anda.
2. Ikuti arahan dan instruksi yang diberikan pada setiap bagian untuk menyelesaikan prapraktikum ini. Bagian-bagian yang perlu dikerjakan terdapat pada tabel-tabel dengan *header* kuning. Isilah jawaban Anda pada bagian dengan label **<Jawab>**.
3. Tolong kerjakan dengan rapi. Anda bisa (tetapi tidak harus) mengikuti *guidelines* berikut.
 - Gunakan font Open Sans dengan ukuran 11 (konfigurasi yang sama dengan dokumen ini).
 - ***Justify*** seluruh jawaban Anda yang berupa paragraf (*shortcut*: **Ctrl+Shift+J**)
 - Gunakan fitur ***Add space after list item*** dan fitur ***Add space after paragraph*** jika Anda ingin menambahkan ruang antar-*item* atau antarparagraf. Jangan gunakan ***newline*** atau ***enter***.
4. Diperbolehkan mengerjakan dalam Bahasa Indonesia maupun Bahasa Inggris.
5. Simpan tugas Anda dengan format ini: **IF2230_PraPrak[X]_<NIM>.pdf** (contoh: IF2230_PraPrak1_13522022.pdf)

6. Kumpulan tugas Anda melalui [form ini](#).
7. Tenggat waktu untuk tugas prapraktikum ini adalah Minggu, 16 Maret 2025, pukul 23.59 WIB.
8. Jika ada pertanyaan terkait pengerjaan maupun praktikum, tanyakan pada sheets QnA: <https://bit.ly/QnA-IF2230-2425>.
9. ***Heads-up*** bahwa pada praktikum, di samping kemampuan, pemahaman kalian juga akan diuji dengan **soal teori**. Oleh karena itu, pahamiilah semua materi prapraktikum dengan baik.

Modul Prapraktikum

Perkenalan Cisco Packet Tracer

Cisco Packet Tracer adalah kakas simulasi jaringan komputer yang dikembangkan oleh Cisco. Kakas ini digunakan terutama untuk tujuan pembelajaran dan tidak menyimulasikan jaringan atau perangkat seperti *virtual machine*. Kakas ini khusus menyediakan perangkat-perangkat keras jaringan Cisco.

Tugas 1

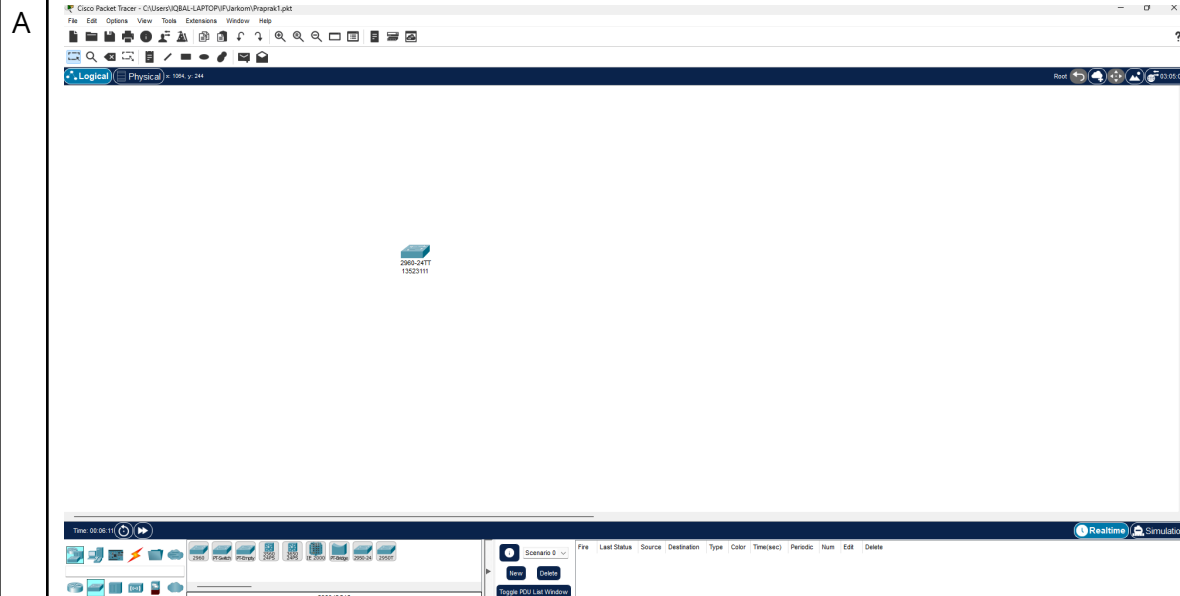
Q Unduh Cisco Packet Tracer menggunakan link ini.

[Resource Hub: Get Packet Tracer, Virtual Machines, and More \(netacad.com\)](https://www.netacad.com/resources/cisco-packet-tracer)

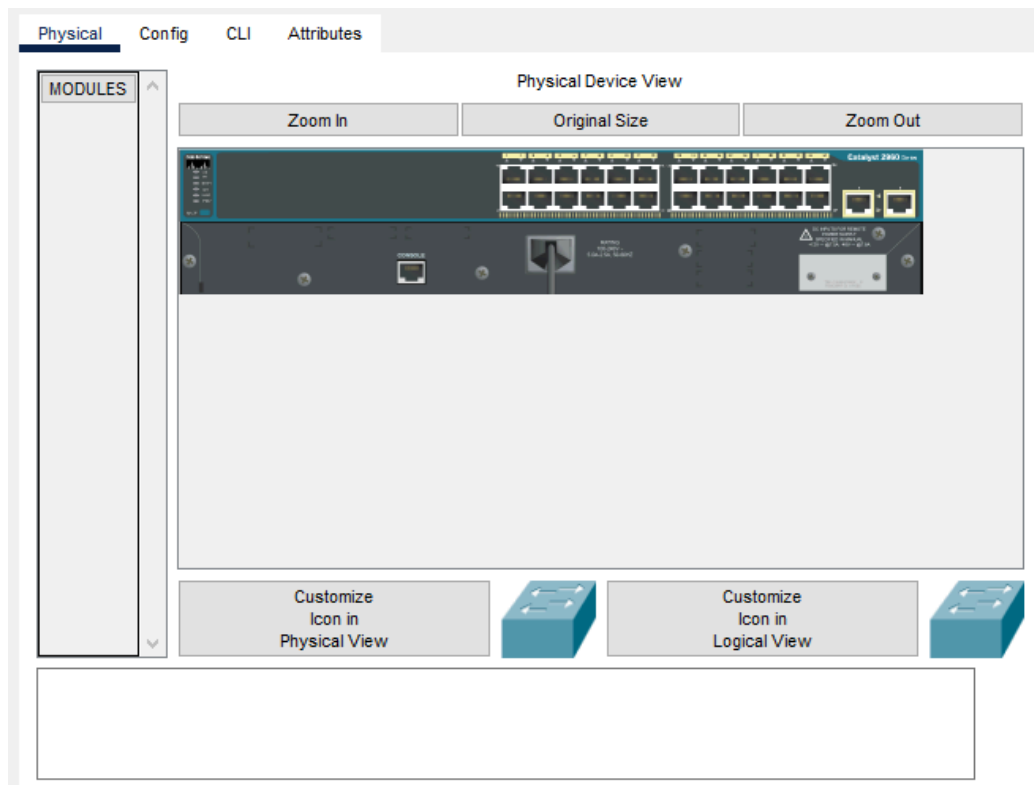
Login dengan email Anda (akun apa saja, ITB atau pribadi) dan ikuti instruksi hingga Anda dapat mengakses antarmuka Cisco Packet Tracer. Tambahkan perangkat *switch* 2960 dan ganti *display name switch* tersebut menjadi NIM Anda.

Tugas:

Screenshot dan lampirkan hasilnya di bawah!

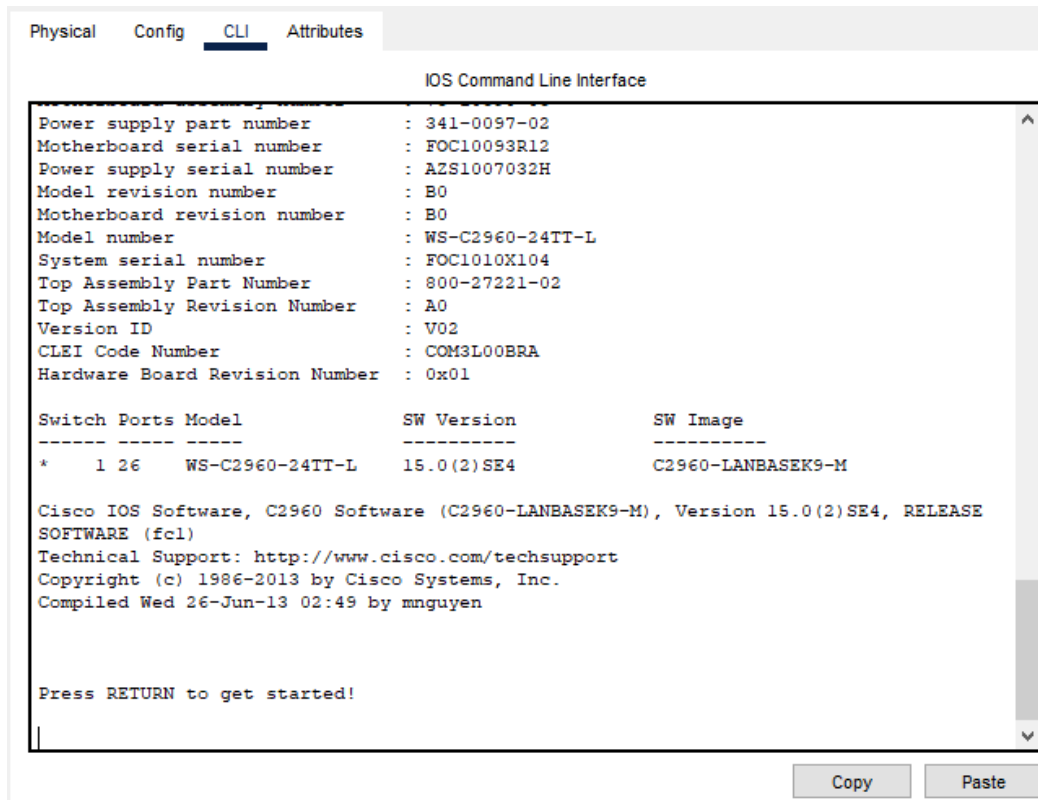


Cisco Packet Tracer menyediakan simulasi perangkat keras pada perangkat-perangkat yang Anda tambahkan. Ini memungkinkan Anda menambah/mengurangi modul-modul pada perangkat tersebut. Antarmuka ini dapat diakses dengan *double click* pada perangkat, dan memilih bagian **Physical** pada menu bagian atas.



Gambar 1. Antarmuka Konfigurasi Perangkat Keras

Router dan switch dikonfigurasi pada lokasinya secara langsung melalui *serial port* yang diakses menggunakan *rollover cable*, umumnya menggunakan perangkat lunak seperti [PuTTY](#) atau [SecureCRT](#). Namun, Cisco Packet Tracer menyederhanakan proses ini dengan menyediakan CLI (Command Line Interface) pada antarmuka yang sama dengan antarmuka perangkat keras dengan memilih **CLI** pada menu bagian atas.



Gambar 2. Antarmuka CLI

Apa itu *rollover cable*? *rollover cable* adalah salah satu konfigurasi [RJ45](#) dengan jenis kabel [UTP \(Unshielded Twisted Pair\)](#). Kabel-kabel dihubungkan dengan urutan *rolling*: 1-to-8, 2-to-7, 3-to-6, dan seterusnya hingga 8-to-1. Terdapat konfigurasi kabel lain seperti *Straight-through* dan *Crossover*. Naumn, kabel-kabel ini sudah jarang digunakan sejak munculnya [Auto MDI-X](#).

Terdapat beberapa mode konfigurasi pada CLI perangkat-perangkat Cisco. Saat pertama kali terhubung, pengguna mengakses dengan mode **User EXEC**. Mode ini ditandai dengan simbol **>** sebagai pemisah antara *hostname* (nama perangkat) dan terminal aktif. Untuk menampilkan petunjuk-petunjuk terkait *command* CLI, pengguna dapat mengetikkan simbol **?**, untuk menampilkan daftar *command* yang ada atau menunjukkan *completion* berdasarkan *state* dari CLI. **Fitur ini sangat berguna, Anda menjadi tidak harus menghafal sintaks secara mutlak sehingga sangat disarankan untuk digunakan.**

```

Router>?
Exec commands:
<1-99>      Session number to resume
connect     Open a terminal connection
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
logout      Exit from the EXEC
ping        Send echo messages
resume      Resume an active network connection
show        Show running system information
ssh         Open a secure shell client connection
telnet      Open a telnet connection
terminal    Set terminal line parameters
traceroute  Trace route to destination
Router>

```

Gambar 3. Command pada Mode User EXEC

Pada daftar *command* di atas, hanya sedikit konfigurasi perangkat yang dapat dilakukan pada mode ini. Untuk melakukan konfigurasi pada perangkat, pengguna harus terlebih dahulu memasuki mode **privileged EXEC** dengan *command* `enable`. Mode *privileged EXEC* ditandai dengan simbol `#` sebagai pemisah antara *hostname* dan terminal aktif.

```

Router>en
Router#?
Exec commands:
<1-99>      Session number to resume
auto        Exec level Automation
clear       Reset functions
clock       Manage the system clock
configure   Enter configuration mode
connect     Open a terminal connection
copy        Copy from one file to another
debug       Debugging functions (see also 'undebug')
delete      Delete a file
dir         List files on a filesystem
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
erase       Erase a filesystem
exit        Exit from the EXEC
logout      Exit from the EXEC
mkdir       Create new directory
more        Display the contents of a file
no          Disable debugging informations
ping        Send echo messages
reload      Halt and perform a cold restart
resume      Resume an active network connection
rmdir       Remove existing directory
send        Send a message to other tty lines
setup       Run the SETUP command facility
show        Show running system information
ssh         Open a secure shell client connection
telnet      Open a telnet connection
terminal    Set terminal line parameters
traceroute  Trace route to destination
undebg      Disable debugging functions (see also 'debug')
vlan        Configure VLAN parameters
write       Write running configuration to memory, network, or terminal
Router#

```

Gambar 4. Command pada Mode Privileged EXEC

Pada gambar di atas, mengetikkan **en** memiliki efek seperti mengetikkan **enable** secara lengkap. Cisco CLI dapat mengeksekusi singkatan *command* ketika hanya ada satu *command* yang diawali dengan singkatan tersebut. Pada contoh di atas, tidak terdapat *command* lain yang diawali dengan **en** pada mode *User EXEC*.

Terdapat banyak *command* yang dapat dijalankan pada mode *Privileged EXEC*, tetapi konfigurasi tertentu diakses dengan mengaktifkan mode konfigurasi spesifik. Konfigurasi umum perangkat dapat dilakukan pada mode *Global Configuration* yang diakses dengan *command* **configure terminal** pada mode Privileged EXEC. Mode *Global Configuration* ditandai dengan '(config)#' sebagai pemisah antara *hostname* dan terminal aktif.

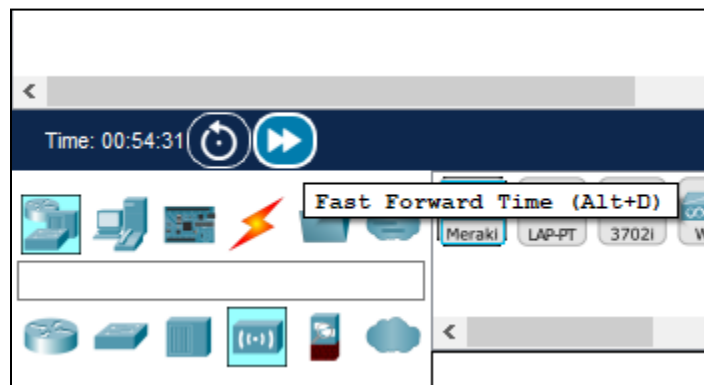
```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#?
Configure commands:
aaa                Authentication, Authorization and Accounting.
access-list        Add an access list entry
banner             Define a login banner
bba-group          Configure BBA Group
boot              Modify system boot parameters
cdp               Global CDP configuration subcommands
class-map          Configure Class Map
clock             Configure time-of-day clock
config-register    Define the configuration register
crypto            Encryption module
default           Set a command to its defaults
dial-peer         Dial Map (Peer) configuration commands
do               To run exec commands in config mode
dot11            IEEE 802.11 config commands
enable            Modify enable password parameters
end              Exit from configure mode
ephone           define ethernet phone
ephone-dn         Configure ephone phone lines (Directory Numbers)
exit             Exit from configure mode
flow             Global Flow configuration subcommands
hostname         Set system's network name
interface        Select an interface to configure
ip              Global IP configuration subcommands
ipv6            Global IPv6 configuration commands
key             Key management
line            Configure a terminal line
lldp           Global LLDP configuration subcommands
logging         Modify message logging facilities
login          Enable secure login checking
mac-address-table Configure the MAC address table
no             Negate a command or set its defaults
ntp            Configure NTP
parameter-map  parameter map
parser         Configure parser
policy-map     Configure QoS Policy Map
port-channel   EtherChannel configuration
priority-list  Build a priority list
privilege      Command privilege parameters
queue-list     Build a custom queue list
router         Enable a routing process
secure         Secure image and configuration archival commands
security       Infra Security CLIs
service        Modify use of network based services
snmp-server    Modify SNMP engine parameters
spanning-tree  Spanning Tree Subsystem
tacacs-server  Modify TACACS query parameters
telephony-service Configure Cisco Unified Communications Manager Express
username       Establish User Name Authentication
vpdn           Virtual Private Dialup Network
vpdn-group     VPDN group configuration
zone           FW with zoning
zone-pair      Zone pair command
Router(config)#
```

Gambar 5. Daftar Command pada Global Configuration Mode

Terdapat beberapa mode konfigurasi lain, beberapa di antaranya adalah mode *line configuration*, mode *interface configuration*, dan mode *multi-interface configuration*. Sebagian mode-mode tersebut akan digunakan pada aktivitas lab ke depannya. Anda dapat mengakses penjelasan lebih lengkap terkait CLI pada [Cisco IOS official CLI reference book](#).

Catatan: Ketika Anda memasukkan *command* yang tidak dikenali oleh Cisco CLI, CLI akan melakukan *DNS lookup* (DNS akan dipelajari di kelas kedepannya), dan mengakibatkan pengguna harus menunggu cukup lama. Tentunya Anda tidak mau menunggu DNS lookup selesai setiap kali salah memasukkan *command*. Untuk mengatasi hal ini, terdapat beberapa hal yang dapat Anda lakukan:

- Batalkan *command* dengan menggunakan **Ctrl+Shift+6**
- Jika Anda ingin menonaktifkan DNS lookup pada perangkat, aktifkan mode *Global Configuration* (telah dibahas di bagian sebelumnya) dan gunakan *command* `no ip domain-lookup`
- Anda juga bisa menggunakan fitur *fast-forward time* untuk mempercepat *DNS lookup* (tombolnya terletak di kiri bawah). Perhatikan bahwa fitur ini juga bisa digunakan untuk hal lain, misalnya mempercepat proses ARP atau PING (dibahas pada [tugas 3](#)).



Untuk mengulangi (karena poin ini sangat penting): kami **sangat menyarankan** Anda untuk menggunakan "?" setiap kali Anda menggunakan *command* baru untuk mendapatkan intuisi dan pengertian lebih terkait sintaks CLI dari sekarang.

Tugas 2	
Q	Konfigurasi switch yang telah Anda tambahkan pada Tugas 1 : <ul style="list-style-type: none">- Set <i>hostname</i> menjadi nama belakang Anda- Set unencrypted password untuk menghubungkan perangkat- Set unencrypted password untuk mengakses mode <i>privileged EXEC</i>

	<ul style="list-style-type: none"> - Encrypt the password to enter privileged mode using MD5 algorithm - Save konfigurasi <p>Tugas:</p> <p>Lampirkan <i>screenshot-screenshot</i> berikut pada kolom jawaban di bawah!</p> <ol style="list-style-type: none"> 1. Prompt <i>password</i> saat menghubungkan CLI 2. Prompt <i>password</i> saat memasuki mode <i>privileged EXEC</i> 3. Konfigurasi perangkat sebelum dan sesudah password dienkripsi 4. <i>Startup-config</i> sebelum dan sesudah <i>saving</i> (cukup <i>highlight</i> sebagian perubahan)
A	<ol style="list-style-type: none"> 1. <pre> User Access Verification Password: haidar> </pre> 2. <pre> haidar>en Password: haidar# </pre> 3. Sebelum <pre> no service password-encryption ! hostname haidar ! enable password useradmin ! ! . </pre> <p>Sesudah</p> <pre> no service password-encryption ! hostname haidar ! enable secret 5 \$1\$mERr\$16PHnFa52zAllM4wZFzo10 enable password useradmin </pre> 4. Sebelum

```
Using 1080 bytes
!  
version 15.0  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Haidar  
!  
!
```

```
line con 0  
!  
line vty 0 4  
login  
line vty 5 15  
login  
!  
!  
!  
!
```

Sesudah

```
Using 1182 bytes  
!  
version 15.0  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname haidar  
!  
enable secret 5 $1$mERr$16PHnFa52zA1lM4wZFzo10  
enable password useradmin  
!
```

```
line con 0  
password useradmin  
login  
!  
line vty 0 4  
login  
line vty 5 15  
login  
!  
!  
!  
!  
end
```

Frame Switching

Sebuah frame adalah [PDU \(Protocol Data Unit\)](#) pada *layer* ke-2 [OSI Model](#), *data link layer*. *Data link layer* menyediakan *transfer* data antar-*node* yang terhubung secara langsung. Selain itu, *layer* ini mendeteksi dan bisa saja mengoreksi *error* yang muncul pada *physical layer* dan mendefinisikan protokol untuk memulai dan menutup koneksi antara dua perangkat yang terhubung secara fisik. *Layer* ini juga menyediakan protokol untuk mengatur *flow* antar-*node*.

OSI model				
Layer		Protocol data unit (PDU)	Function ^[26]	
Host layers	7	Application	Data	High-level protocols such as for resource sharing or remote file access, e.g. HTTP .
	6	Presentation		Translation of data between a networking service and an application; including character encoding , data compression and encryption/decryption
	5	Session		Managing communication sessions , i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation , acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing , routing and traffic control
	2	Data link	Frame	Transmission of data frames between two nodes connected by a physical layer
	1	Physical	Bit, Symbol	Transmission and reception of raw bit streams over a physical medium

Gambar 6. Tabel OSI Model

Switch bekerja pada *layer* ini dengan mencatat *identifier* perangkat yang bernama [MAC \(Media Access Control\)](#) dan memetakan *identifier* tersebut dengan antarmuka *port* yang terhubung pada *MAC Table*. Meskipun demikian, alamat yang digunakan pada antarmuka jaringan komputer tidak menggunakan *MAC address* melainkan [IP address](#), karena *MAC address* ditujukan sebagai *identifier* dari *network interface controller* dan tidak ditujukan sebagai alamat untuk *routing* komunikasi antar-*node*. [ARP \(Address Resolution Protocol\)](#) digunakan untuk menentukan *MAC address* dari *IP address*, karena transmisi antar-*node* menggunakan *MAC address*.

[Ping](#) adalah kakas jaringan komputer yang digunakan untuk memeriksa keterjangkauan perangkat dalam jaringan melalui *internet protocol* dengan menggunakan [ICMP](#). Kakas ini akan sangat sering digunakan dalam aktivitas-aktivitas lab ke depannya. Untuk memahami

frame switching, kita dapat menggunakan *ping* sebagai contoh. *Ping* biasa dijalankan dengan perintah berikut.

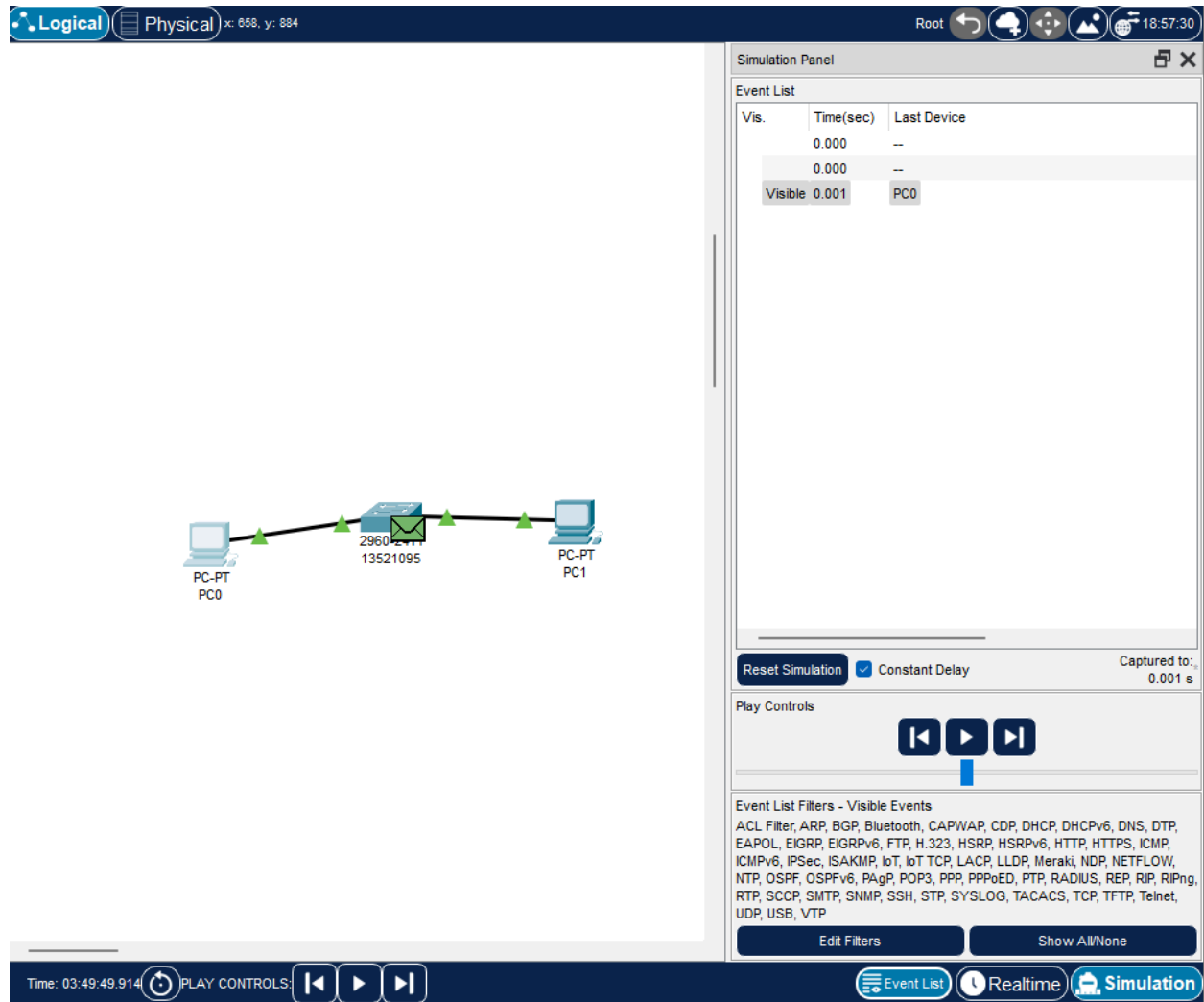
```
ping <IP_Address>
```

Misalkan terdapat dua komputer yang terhubung dengan satu sama lain melalui *switch* yang baru dinyalakan dengan *MAC address table* yang kosong, PC0 terhubung dengan *IP address* 192.168.1.1 dan *subnet mask* 255.255.255.0 serta PC1 terhubung dengan *IP address* 192.168.1.2 dan *subnet mask* 255.255.255.0, *ping* akan dijalankan dengan langkah-langkah berikut.

Step	Explanation
<i>ARP Request</i> PC0 ke Switch	PC0 hanya memiliki informasi <i>IP address</i> PC1, jadi PC0 mengirimkan <i>ARP request</i> dengan tujuan <i>MAC address</i> ffff:ffff:ffff pada frame header .
<i>ARP Request Flooding</i> Switch ke semua PC kecuali PC0	Karena switch memiliki <i>MAC address table</i> yang kosong, tidak ada informasi mengenai tujuan paket tersebut sehingga switch mengirimkan paket tersebut ke semua <i>port</i> kecuali <i>port</i> yang menerima paket tersebut (hal ini dinamakan <i>flooding</i>). Switch juga mencatat <i>MAC address</i> PC0 yang terdapat pada <i>frame header</i> yang diterimanya beserta <i>port</i> yang menerimanya.
<i>ARP Reply</i> PC1 ke Switch	PC1 mengenali <i>IP address</i> pada <i>ARP payload</i> dan membalas <i>request</i> tersebut ke switch.
<i>ARP Reply</i> Switch ke PC0	Switch telah mencatat <i>MAC address</i> PC0 dan meneruskan paket menuju <i>port</i> yang sesuai. Switch juga mencatat <i>MAC address</i> PC1 yang terdapat pada <i>frame header</i> beserta <i>port</i> yang sesuai.
<i>ICMP Echo Request</i> PC0 ke Switch	Setelah mengetahui <i>MAC address</i> PC1, PC0 mengirimkan paket ICMP.
<i>ICMP Echo Request</i> Switch ke PC1	Switch melakukan decapsulation paket ICMP hingga terdapat <i>MAC address</i> tujuan,

	mengkapsulasi ulang paket tersebut, dan meneruskan paket ICMP menuju <i>port</i> tujuannya.
<i>ICMP Echo Reply</i> PC1 ke Switch	PC1 membalas <i>request</i> ICMP PC0, mengonfirmasi <i>liveness</i> dan <i>reachability</i> PC1.
<i>ICMP Echo Reply</i> Switch ke PC0	Switch melakukan <i>decapsulation</i> paket ICMP hingga terdapat <i>MAC address</i> tujuan, mengkapsulasi ulang paket tersebut, dan meneruskan paket ICMP menuju <i>port</i> tujuannya.

Cisco Packet Tracer memiliki fitur untuk memperlambat aktivitas perangkat-perangkat. Fitur ini dapat digunakan untuk memvisualisasikan cara kerja *ping request* seperti yang telah dijelaskan di atas. Selain itu, Anda juga dapat melihat isi dari data komunikasi antar-*node* dengan mengeklik ikon surat atau melalui entri pada *event list*.



Gambar 7. Fitur Simulasi Cisco Packet Tracer

Tugas 3

Q Pada Cisco Packet Tracer, buatlah topologi *star* yang terdiri dari satu 2960 Switch yang terhubung pada 4 komputer.

Gunakan *display name* dan *IP address* pada setiap perangkat, urutan penomoran PC dibebaskan:

- Switch_<NIM>: -
- PC1_<NIM>: 192.168.1.1, subnet mask 255.255.255.0

- PC2_<NIM>: 192.168.1.2, subnet mask 255.255.255.0
- PC3_<NIM>: 192.168.1.3, subnet mask 255.255.255.0
- PC4_<NIM>: 192.168.1.4, subnet mask 255.255.255.0

Kemudian coba lakukan *ping* PC4 dari PC1 dan amati langkah-langkah yang terjadi seperti penjelasan di atas.

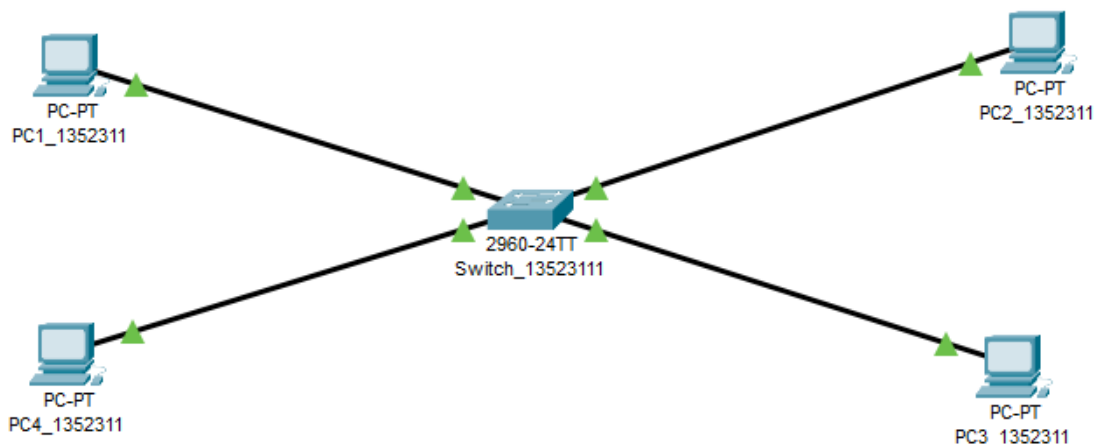
Tugas:

Lampirkan topologi dan langkah-langkah *ping* pada kolom di bawah (gunakan [fitur simulasi packet tracer](#)!). Selain itu, jelaskan apa yang terjadi pada setiap langkah pada *ping*.

Warning:

Penjelasan pada setiap langkah ping haruslah berdasarkan pemahaman individu, dilarang COPAS!

A



Langkah-langkah	Penjelasan
ARP Request [PC1 to Switch]	PC1 melakukan ARP Request sebab MAC Address PC4 belum terdaftar di PC1
Learning STP State [Switch]	Switch melakukan STP sebab MAC Address PC1 baru pertama kali ditemukan oleh Switch
ARP Request	PC1 kembali melakukan ARP Request

[PC1 to Switch]	sebab yang tadi timeout
ARP Request Flooding [Switch]	Switch mengirimkan paket ARP Request ke semua port yang terhubung kecuali PC1
ARP Reply [PC4 to Switch]	PC4 membalas ARP Request berupa MAC Addressnya sekaligus Switch menyimpan MAC Address dari PC4
ARP Reply [Switch to PC1]	Switch meneruskan ARP Reply PC4 kepada PC1
ICMP Echo Request [PC1 to Switch]	PC1 mengirimkan ICMP Echo Request dengan tujuan akhir MAC Address PC4
ICMP Echo Request [Switch to PC4]	Switch meneruskan paket ICMP Echo Request kepada PC4
ICMP Echo Reply [PC4 to Switch]	PC4 mengirimkan pesan balasan ICMP Echo Reply yang ditujukan kepada IP PC1
ICMP Echo Reply [Switch to PC1]	Switch meneruskan paket menuju port yang terhubung dengan PC1

LAN dan Subnetting

LAN adalah singkatan dari *Local Area Network*. Secara formal, LAN didefinisikan sebagai jaringan dengan satu [broadcast domain](#), yang merupakan area atau grup dari *nodes* yang menerima *broadcast* yang sama dari perangkat jaringan pada **data link layer**. Berdasarkan definisi tersebut, **perangkat dalam sebuah jaringan tidak dapat berkomunikasi dengan perangkat dalam jaringan lain tanpa [routing](#)**. Semua jaringan memiliki beberapa nomor-nomor penting, salah satu yang terutama adalah **network address** dan **subnet mask**.

Network address terdiri dari **IP address** yang digunakan perangkat-perangkat dan jaringan lain untuk mengidentifikasi sebuah jaringan. Namun, *IP address* tidak memberikan informasi yang cukup terkait "bagian" jaringan mana yang dirujuk oleh nomor tersebut,

sebuah informasi tambahan diperlukan untuk membedakan *network address* dari *device address*. Sumber informasi tambahan ini dikenal sebagai **subnet mask**. Sederhananya, **subnet mask** adalah nomor dengan panjang 32-bit (pada IPv4) yang memungkinkan perangkat untuk membedakan bagian dari *IP address* yang merupakan bagian dari jaringan, dan yang merupakan bagian dari perangkat dalam jaringan tersebut.

Sebagai contoh, sebuah komputer yang terhubung pada jaringan memiliki *IP address* 192.168.100.1, dan *subnet mask* 255.255.255.0. Untuk mempermudah penulisan, digunakan notasi *IP address* **192.168.100.1/24** yang disebut [*CIDR notation*](#). Untuk mendapatkan *network address* dari alamat tersebut, gunakan **operator AND** pada kedua nomor. Operasi tersebut menghasilkan 192.168.100.0. Semua alamat, **dan hanya** alamat dari 192.168.100.1 hingga 192.168.100.254 merupakan perangkat yang terhubung pada jaringan tersebut (bagaimana dengan 192.168.100.0/24 & 192.168.100.255/24?).

Terdapat nomor penting lain, yaitu **broadcast address**, yang dapat digunakan untuk mengirimkan pesan kepada semua perangkat lain dalam jaringan yang sama, yaitu pada *broadcast domain* yang sama. Nomor ini adalah alamat terakhir dalam jaringan. Pada contoh di atas, *broadcast address* jaringan tersebut adalah 192.168.100.255.

Tugas 4

Q Pada Cisco Packet Tracer, buat dua topologi *star*, masing-masing terdiri dari satu 2960 Switch yang terhubung ke tiga komputer.

Hint: gunakan ulang dengan meng-copy dan sesuaikan hasil dari tugas sebelumnya.

Untuk topologi pertama, gunakan *display name* dan *IP address* berikut untuk masing-masing perangkat. Urutan penomoran PC dibebaskan: (**IP address terakhir bukan salah ketik**)

- SwitchA_<NIM>: -
- PC1A_<NIM>: 192.168.1.1, subnet mask 255.255.255.0
- PC2A_<NIM>: 192.168.1.2, subnet mask 255.255.255.0
- PC3A_<NIM>: 192.168.2.3, subnet mask 255.255.255.0

Untuk topologi ke-dua, gunakan *display name* dan *IP address* berikut untuk masing-masing perangkat. Urutan penomoran PC dibebaskan: (**IP address terakhir bukan salah ketik**)

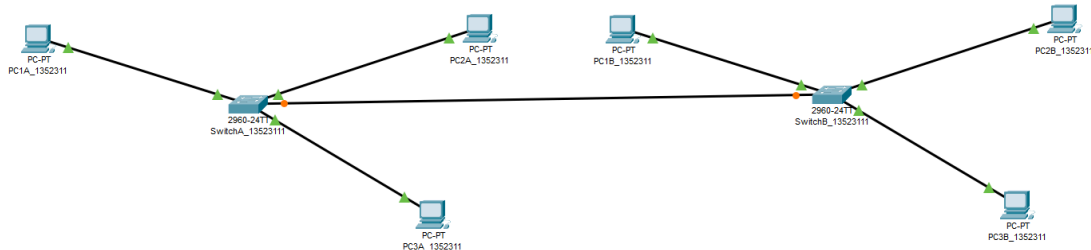
- SwitchB_<NIM>: -
- PC1B_<NIM>: 192.168.2.1, subnet mask 255.255.255.0
- PC2B_<NIM>: 192.168.2.2, subnet mask 255.255.255.0
- PC3B_<NIM>: 192.168.1.3, subnet mask 255.255.255.0

Kemudian, hubungkan SwitchA dan SwitchB pada *port* FastEthernet masing-masing.

Tugas:

lampirkan topologinya, kemudian coba ping semua PC dari PC1A dan PC1B. Apa yang terjadi? Lampirkan hasilnya dan jelaskan!

A



PC1A RTO ketika ping PC3A, PC1B, PC2B. PC1B RTO ketika ping PC1A, PC2A, PC3B. Hal ini disebabkan kedua device berada pada subnet yang berbeda.

Subnet mask 255.255.255.0 atau /24 berarti sebuah subnet dapat memiliki 254 + 2 alamat IP yang dapat digunakan untuk perangkat yang termasuk ke dalam subnet tersebut ditandai dengan 8 bit terakhir dari IP Address.

Ketika 24 bit pertama IP Address sama maka kedua device dapat dipastikan berada dalam subnet yang sama dengan demikian ping dapat dilakukan, sedangkan apabila 24 bit pertama IP Address berbeda maka dapat dipastikan kedua device berada dalam subnet yang berbeda dengan demikian ping tidak dapat dilakukan.

Dengan memanfaatkan *isolation property* dari jaringan dan *subnet mask*, rentang *IP address* dapat dibagi menjadi jaringan-jaringan yang lebih kecil melalui **subnetting**. Sebagai contoh, dengan rentang *IP addresses* 192.168.100.0-192.168.100.255, dapat digunakan **subnet mask untuk membagi jaringan tersebut menjadi dua jaringan terpisah yang lebih kecil**, seperti *sub network* 192.168.100.0/25 dan 192.168.100.128/25.

Tugas 5

Q Seperti tugas sebelumnya, buat dua topologi *star*, masing-masing terdiri dari satu 2960 Switch yang terhubung ke tiga komputer. Hint: gunakan ulang dan sesuaikan hasil dari tugas sebelumnya.

Untuk topologi pertama, gunakan *display name* dan *IP address* berikut untuk masing-masing perangkat. Urutan penomoran PC dibebaskan: (**IP address terakhir bukan salah ketik**)

- SwitchA_<NIM>: -
- PC1A_<NIM>: 192.168.1.1, subnet mask 255.255.255.0
- PC2A_<NIM>: 192.168.1.2, subnet mask 255.255.255.0
- PC3A_<NIM>: 192.168.1.129, subnet mask 255.255.255.0

Untuk topologi ke-dua, gunakan *display name* dan *IP address* berikut untuk masing-masing perangkat. Urutan penomoran PC dibebaskan: (**IP address terakhir bukan salah ketik**)

- SwitchB_<NIM>: -
- PC1B_<NIM>: 192.168.1.3, subnet mask 255.255.255.0
- PC2B_<NIM>: 192.168.1.4, subnet mask 255.255.255.0
- PC3B_<NIM>: 192.168.1.130, subnet mask 255.255.255.0

- a. Kemudian, hubungkan SwitchA dan SwitchB pada *port* FastEthernet masing-masing.

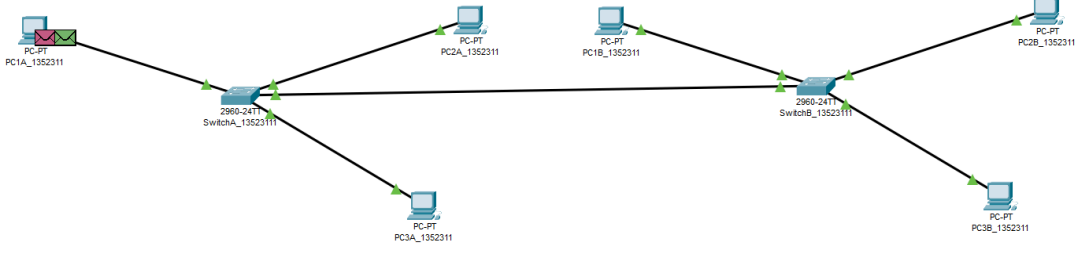
Tugas:

lampirkan topologinya, kemudian coba lakukan ping semua PC dari PC1A dan PC1B. Apa yang terjadi? Lampirkan hasilnya dan jelaskan!

- b. Kemudian, ganti *subnet mask* semua PC menjadi 255.255.255.128.

Tugas:

coba lakukan ping semua PC dari PC1A dan PC1B. Apa yang terjadi? Lampirkan hasilnya dan jelaskan!

	<p>c. Apakah ada perbedaan antara kondisi soal a dan b? Jika ya, mengapa hal tersebut dapat terjadi?</p> <p>Tugas: Berikan penjelasan secukupnya dan jelas mengenai perbedaan kondisi yang didapat dan alasannya!</p>
A	<p>a.</p>  <p>Baik PC1A ataupun PC1B berhasil melakukan ping untuk setiap PC lainnya. Hal tersebut karena seluruh PC A atau B masih berada dalam subnet yang sama</p> <p>Subnet mask 255.255.255.0 atau /24 memiliki range IP Address 254 + 2 yang ditinjau pada 8 bit terakhir.</p> <p>b. Kedua PC RTO ketika ping PC3A dan PC3B sebab kedua PC tersebut tidak berada dalam subnet yang sama dengan PC1A dan PC1B.</p> <p>Subnet mask 255.255.255.128 atau /25 memiliki range IP Address 126 + 2 yang ditinjau pada 7 bit terakhir.</p> <p>c. Ya terdapat perbedaan kondisi yakni subnet mask yang digunakan. 255.255.255.0 atau /24 memiliki range IP Address yang lebih besar ketimbang 255.255.255.128 atau /25 sehingga PC3A dan PC3B berada pada subnet yang sama dengan PC1A dan PC1B jika menggunakan subnet mask /24 namun berbeda subnet jika menggunakan subnet mask /25.</p>

VLAN

VLAN adalah singkatan dari *Virtual Local Area Network*, yang berfungsi persis seperti LAN. Dengan VLAN, pada satu infrastruktur perangkat keras jaringan yang sama, yang bisa saja terletak pada lokasi fisik yang sama dapat dibagi menjadi beberapa LAN yang terpisah secara *logical*. Hal ini dapat digunakan untuk menggabungkan perangkat-perangkat dengan

lokasi fisik berbeda-beda ke dalam sebuah jaringan tertentu tanpa harus membuat infrastruktur jaringan yang rumit (terdapat beberapa *use case* lain dari VLAN - silakan cari tahu).

VLAN dijalankan pada ***data link layer***, dan bekerja dengan memberi ***tag*** pada ***network frames***. Untuk membuat VLAN, dibutuhkan *managed switch* (seperti Cisco 2950 dan 2960). Manajemen *tag* dari *frame* dilakukan oleh switch, dan pengguna hanya perlu melakukan konfigurasi *grouping* port pada switch.

Tugas 6

Q Pada Cisco Packet Tracer, buat sebuah topologi *star*, masing-masing terdiri dari satu 2960 Switch yang terhubung ke empat komputer.

Hint: gunakan ulang dan sesuaikan hasil dari tugas sebelumnya (cek [Tugas 3](#)).

Gunakan *display name* dan *IP address* pada setiap perangkat, urutan penomoran PC dibebaskan:

- Switch_<NIM>: -
- PC1_<NIM>: 192.168.1.1, subnet mask 255.255.255.0
- PC2_<NIM>: 192.168.1.2, subnet mask 255.255.255.0
- PC3_<NIM>: 192.168.1.3, subnet mask 255.255.255.0
- PC4_<NIM>: 192.168.1.4, subnet mask 255.255.255.0

Kali ini, hubungkan PC pada *port* FastEthernet switch sesuai dengan nomornya masing-masing (misal PC1 menuju *port* FastEthernet0/1). **Ini hanya membantu mengurangi kebingungan pada langkah-langkah selanjutnya. Silakan gunakan *port* lain sesuka hati!**

Kemudian, kosongkan *MAC address table* pada **switch** menggunakan `clear mac-address-table`.

Untuk menampilkan *MAC address* saat ini, gunakan *command* `show mac-address-table`.

- a. Setelah mengosongkan *MAC address table*, tampilkan *MAC address table* saat ini
Tugas:

	<p>Tampilkan <i>MAC address table</i> dan jelaskan apa yang terjadi pada kolom di bawah ini.</p> <p>b. Kemudian, lakukan <i>ping</i> setiap PC dari PC1, kemudian tampilkan <i>MAC address table</i>.</p> <p>Tugas:</p> <p>Tampilkan <i>MAC address table</i> dan jelaskan apa yang terjadi pada kolom di bawah ini.</p>																																
A	<p>a.</p> <pre>Switch#show mac-address-table Mac Address Table -----</pre> <table><thead><tr><th>Vlan</th><th>Mac Address</th><th>Type</th><th>Ports</th></tr><tr><th>----</th><th>-----</th><th>-----</th><th>----</th></tr></thead><tbody></tbody></table> <p>Apabila dilakukan pengosongan MAC Address Table, maka switch tidak memiliki data mengenai mapping ports dengan MAC Address yang terhubung.</p> <p>b.</p> <pre>Switch#show mac-address-table Mac Address Table -----</pre> <table><thead><tr><th>Vlan</th><th>Mac Address</th><th>Type</th><th>Ports</th></tr><tr><th>----</th><th>-----</th><th>-----</th><th>----</th></tr></thead><tbody><tr><td>1</td><td>0001.64a8.269e</td><td>DYNAMIC</td><td>Fa0/2</td></tr><tr><td>1</td><td>0006.2a13.17db</td><td>DYNAMIC</td><td>Fa0/1</td></tr><tr><td>1</td><td>0090.2194.5398</td><td>DYNAMIC</td><td>Fa0/3</td></tr><tr><td>1</td><td>00d0.d35c.d295</td><td>DYNAMIC</td><td>Fa0/4</td></tr></tbody></table> <p>Switch membangun MAC Address Table yang baru secara dinamis dengan memeriksa MAC Address dari tiap frame yang masuk dari tiap ports.</p>	Vlan	Mac Address	Type	Ports	----	-----	-----	----	Vlan	Mac Address	Type	Ports	----	-----	-----	----	1	0001.64a8.269e	DYNAMIC	Fa0/2	1	0006.2a13.17db	DYNAMIC	Fa0/1	1	0090.2194.5398	DYNAMIC	Fa0/3	1	00d0.d35c.d295	DYNAMIC	Fa0/4
Vlan	Mac Address	Type	Ports																														
----	-----	-----	----																														
Vlan	Mac Address	Type	Ports																														
----	-----	-----	----																														
1	0001.64a8.269e	DYNAMIC	Fa0/2																														
1	0006.2a13.17db	DYNAMIC	Fa0/1																														
1	0090.2194.5398	DYNAMIC	Fa0/3																														
1	00d0.d35c.d295	DYNAMIC	Fa0/4																														
Q	<p>Setelah menyiapkan topologi perangkat keras, saatnya mengonfigurasi VLAN. Konfigurasi VLAN untuk memisahkan PC1 & PC2 ke dalam satu VLAN, dan PC3 & PC4 ke dalam VLAN lain.</p> <p>Lakukan ini dengan mengonfigurasi <i>interface (port)</i> yang akan dikelompokkan ke dalam VLAN.</p> <p>Hint: akses mode <i>interface configuration</i> menggunakan</p>																																

	<p>interface range ... dan gunakan konfigurasi switchport</p> <p>a. Tampilkan konfigurasi VLAN!</p> <p>Tugas:</p> <p>Tampilkan <i>screenshot</i> yang jelas dari konfigurasi VLAN!</p> <p>Hint:</p> <p>tampilkan konfigurasi VLAN menggunakan <code>show VLAN</code></p> <p>b. Lakukan <i>ping</i> ke semua PC dari PC1, kemudian lakukan hal yang sama dari PC4.</p> <p>Tugas:</p> <p>Apa yang terjadi? Jelaskan pada kolom jawaban di bawah. Kemudian, tampilkan <i>MAC address table</i> dari switch!</p>
A	a.

```

VLAN Name                Status    Ports
-----
1    default                active    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   VLAN0010                active    Fa0/1, Fa0/2
20   VLAN0020                active    Fa0/3, Fa0/4
1002 fddi-default            active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet     100001    1500   -       -       -       -   -         0       0
10   enet     100010    1500   -       -       -       -   -         0       0
20   enet     100020    1500   -       -       -       -   -         0       0
1002 fddi     101002    1500   -       -       -       -   -         0       0
1003 tr      101003    1500   -       -       -       -   -         0       0
1004 fdnet   101004    1500   -       -       -       ieee -         0       0
1005 trnet   101005    1500   -       -       -       ibm  -         0       0

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----

Remote SPAN VLANs
-----

Primary Secondary Type            Ports
-----
Switch#

```

b.

```

Mac Address Table
-----
Vlan  Mac Address      Type      Ports
----  -
10    0001.64a8.269e   DYNAMIC   Fa0/2
10    0006.2a13.17db   DYNAMIC   Fa0/1
20    0090.2194.5398   DYNAMIC   Fa0/3
20    00d0.d35c.d295   DYNAMIC   Fa0/4

```

PC1 RTO untuk PC3 dan PC4, PC4 RTO untuk PC1 dan PC2. Hal tersebut dapat terjadi sebab kedua device berada pada VLAN yang berbeda sehingga seolah-olah mereka terlihat berada pada 2 jaringan berbeda. Dengan begitu ping yang dilakukan pasti akan gagal.

Terkadang, infrastruktur sebuah jaringan terdiri dari berbagai *host* yang terhubung pada sebuah infrastruktur jaringan, dan sebuah *switch* tidak mampu menangani jumlah port

yang dibutuhkan untuk menghubungkan perangkat-perangkat yang ada. Untuk mengatasi ini, dapat digunakan *bridge* (yang tidak akan digunakan untuk kegiatan *lab*), *backbone* switch (yang merupakan switch yang digunakan untuk menghubungkan switch-switch lain) yang menghubungkan *edge* switch, atau menghubungkan switch-switch yang ada (contohnya *ring topology*).

Karena tag VLAN diletakkan pada **frames**, kita dapat melakukan ini dengan mengonfigurasi grup LAN pada switch yang memungkinkan PDU dengan tag tersebut agar dapat melalui *interface* yang tepat (belum tentu *port* karena akan diperkenalkan *trunk*)

Tugas 7

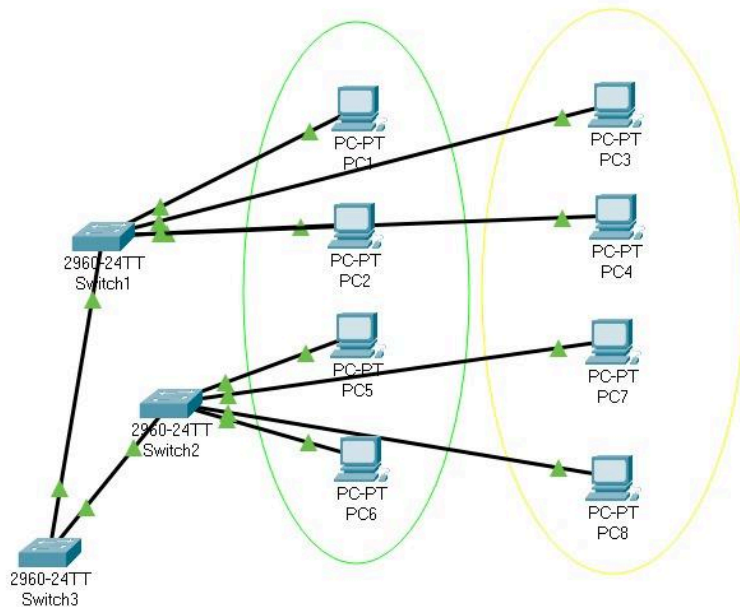
Q Pada Cisco Packet Tracer, buat dua topologi *star*, masing-masing terdiri dari satu 2960 Switch yang terhubung ke empat komputer. (seperti pada [Tugas 6](#)), kemudian hubungkan kedua switch dengan 2960 Switch lain.

Kali ini, gunakan *display name* dan *IP address* berikut pada setiap perangkat, urutan penomoran PC dibebaskan:

- Switch1_<NIM>: -
- PC1_<NIM>: 192.168.1.1, subnet mask 255.255.255.0
- PC2_<NIM>: 192.168.1.2, subnet mask 255.255.255.0
- PC3_<NIM>: 192.168.1.3, subnet mask 255.255.255.0
- PC4_<NIM>: 192.168.1.4, subnet mask 255.255.255.0

- Switch2_<NIM>: -
- PC5_<NIM>: 192.168.1.5, subnet mask 255.255.255.0
- PC6_<NIM>: 192.168.1.6, subnet mask 255.255.255.0
- PC7_<NIM>: 192.168.1.7, subnet mask 255.255.255.0
- PC8_<NIM>: 192.168.1.8, subnet mask 255.255.255.0

- Switch3_<NIM>: -



Sama seperti tugas sebelumnya, hubungkan PC1-4 menuju *port* FastEthernet Switch1 (PC1 menuju *port* FastEthernet0/1). Kemudian lakukan hal yang serupa pada PC5-8 di Switch2 (PC5 to *port* FastEthernet0/1, dan seterusnya) **Seperti pada tugas sebelumnya, penggunaan port dibebaskan**. Setelah menghubungkan PCs pada masing-masing switchnya, hubungkan kedua switch yang menghubungkan PC-PC ke Switch3,

Setelah menyiapkan topologi perangkat keras, saatnya mengonfigurasi VLAN. Konfigurasi VLAN untuk memisahkan PC1, PC2, PC5, & PC6 ke dalam satu VLAN, dan PC3, PC4, PC7, & PC8 ke dalam VLAN lain. Silakan lakukan konfigurasi pada switch manapun yang Anda perlukan.

Menghubungkan switch dengan switch lain dapat dilakukan dengan menghubungkan beberapa kabel untuk setiap grup VLAN, atau menggunakan [trunking](#). Trunking ini akan sangat membantu pada aktivitas lab-lab berikutnya sehingga **Anda diwajibkan** untuk mencoba.

Lakukan ini dengan mengonfigurasi *interface (port)* yang akan dikelompokkan ke dalam VLAN.

	<p>Hint: akses mode <i>interface configuration</i> menggunakan interface [range] ... dan gunakan konfigurasi switchport</p> <p>a. Tampilkan konfigurasi VLAN! (tampilkan juga konfigurasi trunking) Tugas: Tampilkan berupa <i>screenshot</i> yang jelas</p> <p>Hint: tampilkan konfigurasi VLAN menggunakan <code>show VLAN</code> tampilkan konfigurasi trunking menggunakan <code>show interfaces trunk</code></p> <p>b. Lakukan <i>ping</i> ke semua PC dari PC1, kemudian lakukan hal yang sama dari PC8. Tugas: Apa yang terjadi? Jelaskan pada kolom jawaban di bawah. Kemudian, tampilkan <i>MAC address table</i> dari semua switch!</p>
A	a. Switch1_13523111

```
Switch1_13523111#sh vl
```

VLAN Name	Status	Ports
1 default	active	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 VLAN0010	active	Fa0/1, Fa0/2
20 VLAN0020	active	Fa0/3, Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Transl	Trans2
1	enet	100001	1500	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	ibm	-	0	0

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Transl	Trans2
-----------	------	-----	--------	--------	----------	-----	----------	--------	--------

Remote SPAN VLANs

Primary	Secondary	Type	Ports
---------	-----------	------	-------

```
Switch1_13523111#sh int tr
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/5	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/5	10,20

Port	Vlans allowed and active in management domain
Fa0/5	10,20

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/5	10,20

Switch2_13523111

```
Switch2_13523111#sh vl
```

VLAN Name	Status	Ports
1 default	active	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 VLAN0010	active	Fa0/1, Fa0/2
20 VLAN0020	active	Fa0/3, Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
------	------	------	-----	--------	--------	----------	-----	----------	--------	--------

Remote SPAN VLANs

Primary	Secondary	Type	Ports
---------	-----------	------	-------

```
Switch2_13523111#sh int tr
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/5	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/5	10,20

Port	Vlans allowed and active in management domain
Fa0/5	10,20

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/5	10,20

Switch3_13523111

```
Switch3_13523111#sh vlan
```

VLAN Name	Status	Ports
1 default	active	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 VLAN0010	active	
20 VLAN0020	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	0	0
1005	trnet	101005	1500	-	-	-	ibm	0	0

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
-----------	------	-----	--------	--------	----------	-----	----------	--------	--------

Remote SPAN VLANs

Primary	Secondary	Type	Ports
---------	-----------	------	-------

```
Switch3_13523111#sh int tr
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	10,20
Fa0/2	10,20

Port	Vlans allowed and active in management domain
Fa0/1	10,20
Fa0/2	10,20

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	10,20
Fa0/2	10,20

b. **Switch1_13523111**


```
Switch1_13523111#sh mac-
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	000c.cf71.ba01	DYNAMIC	Fa0/5
10	0001.42c3.327d	DYNAMIC	Fa0/5
10	0001.96bb.5389	DYNAMIC	Fa0/1
10	000d.bde4.106e	DYNAMIC	Fa0/5
10	00e0.f9aa.9830	DYNAMIC	Fa0/2
20	0006.2ab0.5d05	DYNAMIC	Fa0/5
20	0060.47e2.b854	DYNAMIC	Fa0/3
20	00d0.97bd.d1c7	DYNAMIC	Fa0/4

Switch2_13523111

```
Switch2_13523111#sh mac-
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	000c.cf71.ba02	DYNAMIC	Fa0/5
10	0001.42c3.327d	DYNAMIC	Fa0/1
10	0001.96bb.5389	DYNAMIC	Fa0/5
10	000c.cf71.ba02	DYNAMIC	Fa0/5
10	000d.bde4.106e	DYNAMIC	Fa0/2
20	0006.2ab0.5d05	DYNAMIC	Fa0/4
20	000c.cf71.ba02	DYNAMIC	Fa0/5
20	0060.47e2.b854	DYNAMIC	Fa0/5
20	0090.2194.28ce	DYNAMIC	Fa0/3
20	00d0.97bd.d1c7	DYNAMIC	Fa0/5

Switch3_13523111

```
Switch3_13523111#sh mac-
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	0001.634a.4505	DYNAMIC	Fa0/2
1	0040.0b52.3005	DYNAMIC	Fa0/1
10	0001.42c3.327d	DYNAMIC	Fa0/2
10	0001.96bb.5389	DYNAMIC	Fa0/1
10	000d.bde4.106e	DYNAMIC	Fa0/2
10	0040.0b52.3005	DYNAMIC	Fa0/1
20	0006.2ab0.5d05	DYNAMIC	Fa0/2
20	0040.0b52.3005	DYNAMIC	Fa0/1
20	0060.47e2.b854	DYNAMIC	Fa0/1
20	00d0.97bd.d1c7	DYNAMIC	Fa0/1

Ketika dilakukan ping, apabila kedua device berada dalam VLAN yang berbeda

maka ping akan gagal sebab secara logika mereka seolah-olah berada dalam dua jaringan yang berbeda. Namun device yang terhubung dalam Switch yang berbeda tetapi masih dalam VLAN yang sama apabila dilakukan ping akan berhasil.

Kedua router terhubung dengan sebuah router tambahan dimana setiap router dihubungkan dengan hanya 1 kabel. Hal ini dimungkinkan dengan trunking dimana sebuah port bisa menjadi anggota dari beberapa VLAN sehingga paket-paket yang ditujukan untuk device yang terhubung dengan switch tidak terbatas untuk 1 VLAN saja.

TIPS

1. **Sering-seringlah save pekerjaan Anda.** Cisco Packet Tracer bukan *software* yang mangkus sehingga rentan *not responding* dan *crash* (terutama jika menggunakan fitur *fast-forward* yang kadang *lemotnya minta ampun*) yang bisa mengakibatkan pekerjaan Anda hilang.
2. **TOLONG sering-seringlah save pekerjaan Anda.** Tips ini ditulis dua kali karena di praktikum semester yang lalu, ada kejadian Cisco Packet Tracer milik *[REDACTED]* nge-*crash* di praktikum pertama dan 30 menit terbuang sia-sia. Jangan melakukan kesalahan yang sama.
3. Jangan lupa gunakan fitur tanda tanya. Fitur ini memang sepenting itu sampai sudah di-*mention* untuk yang ketiga kalinya agar tidak terlewat.
4. PING tidak selalu berhasil di *packet* pertama **jika topologinya cukup rumit/besar**. Jika Anda ingin memastikan apakah sebuah PING berhasil/gagal, Anda bisa menunggu hingga PING selesai sepenuhnya (Anda juga bisa menggunakan fitur simulasi untuk melacak apakah *packet* hilang atau tidak). Catatan, ini mungkin belum terjadi pada modul pertama karena topologinya masih cukup kecil.
5. Banyak tutorial video di internet yang menunjukkan sekaligus menjelaskan dengan baik tentang berbagai *task* pada modul-modul prapraktikum. Tolong carilah sumber informasi dengan baik, alih-alih hanya menjadikan LLM sebagai referensi utama.
6. Estimasi waktu pengerjaan tugas ini adalah **±6 jam** (diambil dari testimoni mahasiswa IF22 non-*imba* yang mengerjakan **tanpa bantuan teman**). Silakan gunakan itu sebagai tolak ukur Anda dalam mengatur waktu pengerjaan.
7. Pada sebuah *device*, selain menu CLI dan *Physical*, perhatikan bahwa ada menu **config**. Anda bisa menggunakan menu tersebut untuk melakukan beberapa konfigurasi yang dibutuhkan dalam tugas ini untuk mempercepat waktu pengerjaan Anda.

Referensi

Cisco. (n.d.). *Cisco Networking Academy*. <https://www.netacad.com>

Lammle, T. (2020). *CCNA certification study guide: Exam 200-301*. Sybex.

On routers, switches, and packets ~ <https://www.youtube.com/watch?v=zhIMLRNY5-4>

On VLANs and Trunks ~ <https://www.youtube.com/watch?v=WIRh6S8SojI>