CISCO™

CCNA 200-301

Lesson 9

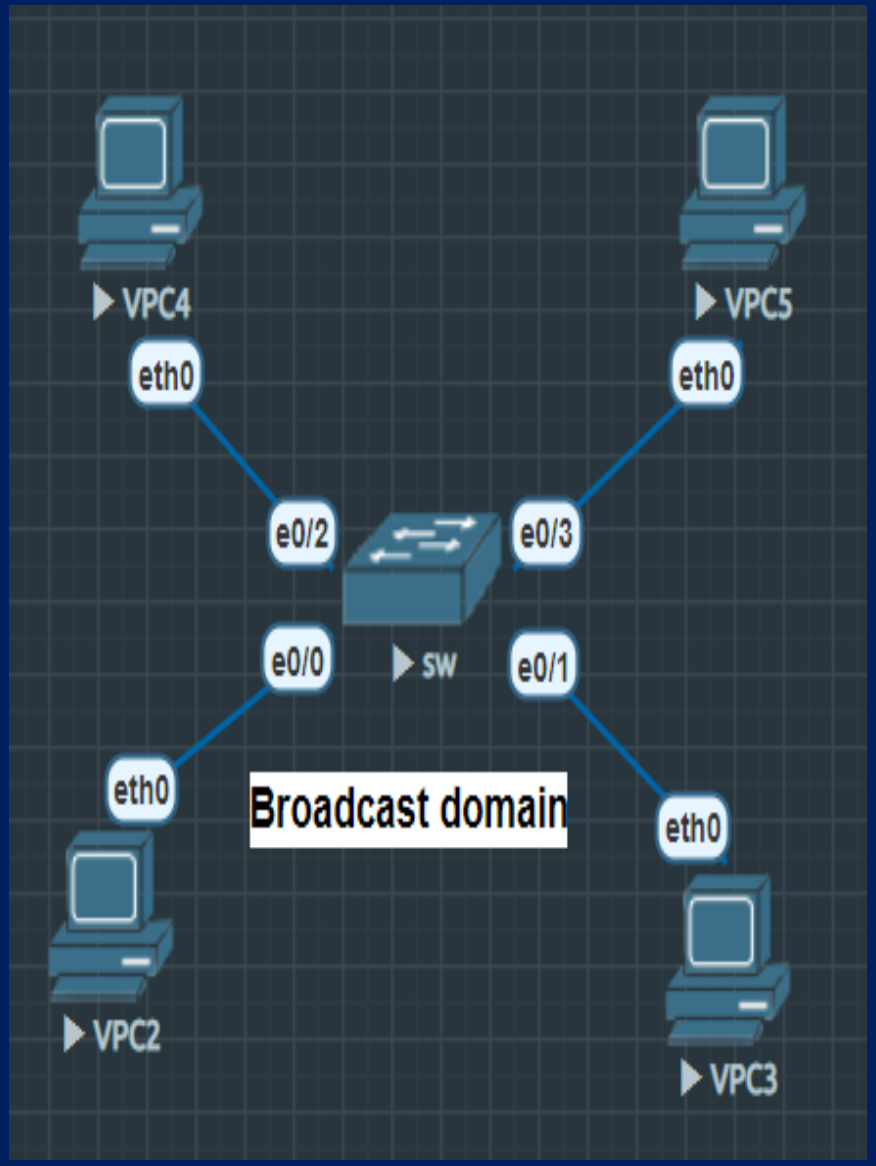
- Broadcast domain
- VLAN Definition
- VLAN Configuration
- VLAN tagging concept
- VLAN Trunking Protocols
- VLAN Trunking Configuration
- Switchport Operation modes

Broadcast domain

Firstly, we need to understand broadcast domain. In LAN concept, all switchports are assigned to VLAN 1 by default. it is called default VLAN. That is why, all devices connected to switch ports are in the same LAN and it is said all devices is in the same broadcast domain. This is the default switch setting. When the switch gets frame from its any connected ports, it will flood the frame to all its ports except receiving port.

If we want create second broadcast domain DO we need second switch ?

there is another technology ? VLAN…



VLAN (Virtual Local Area Network)

Using VLAN we create multiple broadcast domain. As a result, we divide a broadcast domain into small broadcast domains. Each VLAN is one broadcast domain.

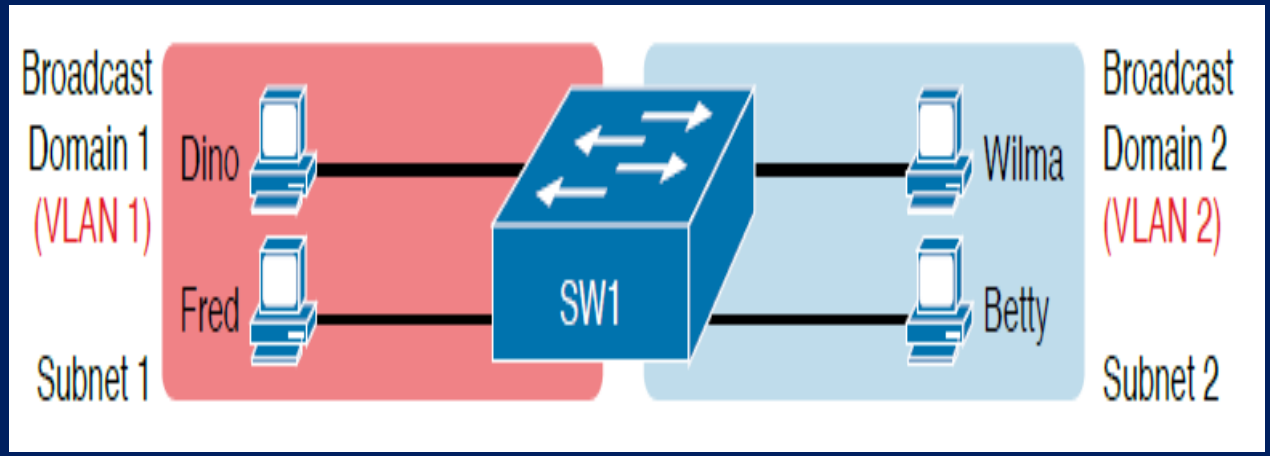
In the image, we have one switch and four computers. Two of them are in broadcast domain 1 (VLAN 1), the other two are in another broadcast domain (VLAN 2).

Each VLAN has its own subnets.

For ex:

VLAN 1: 192.168.1.0/24

VLAN 2: 192.168.2.0/24



VLAN cont.

Most common reasons for choosing to create smaller broadcast domains (VLANs):

- To reduce CPU overhead on each device, improving host performance, by reducing the number of devices that receive each broadcast frame.
- To reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood (broadcasts, multicasts, and unknown unicasts)
- To improve security for hosts through the application of different security policies per VLAN
- To create more flexible designs that group users by department, or by groups that work together, instead of by physical location
- To solve problems more quickly, because the failure domain for many problems is the same set of devices as those in the same broadcast domain
- To reduce the workload for the Spanning Tree Protocol (STP) by limiting a VLAN to a single access switch

VLAN Configuration

According to the topology we configure switchports.

PC2 and PC4 are in the VLAN 10.

PC3 and PC5 are in the VLAN 20.

Sw(config)#vlan 10 ➡ creation VLAN 10

Sw(config-vlan)#name subnet 10

Sw(config)#vlan 20 ➡ creation VLAN 20

Sw(config-vlan)#name subnet 20

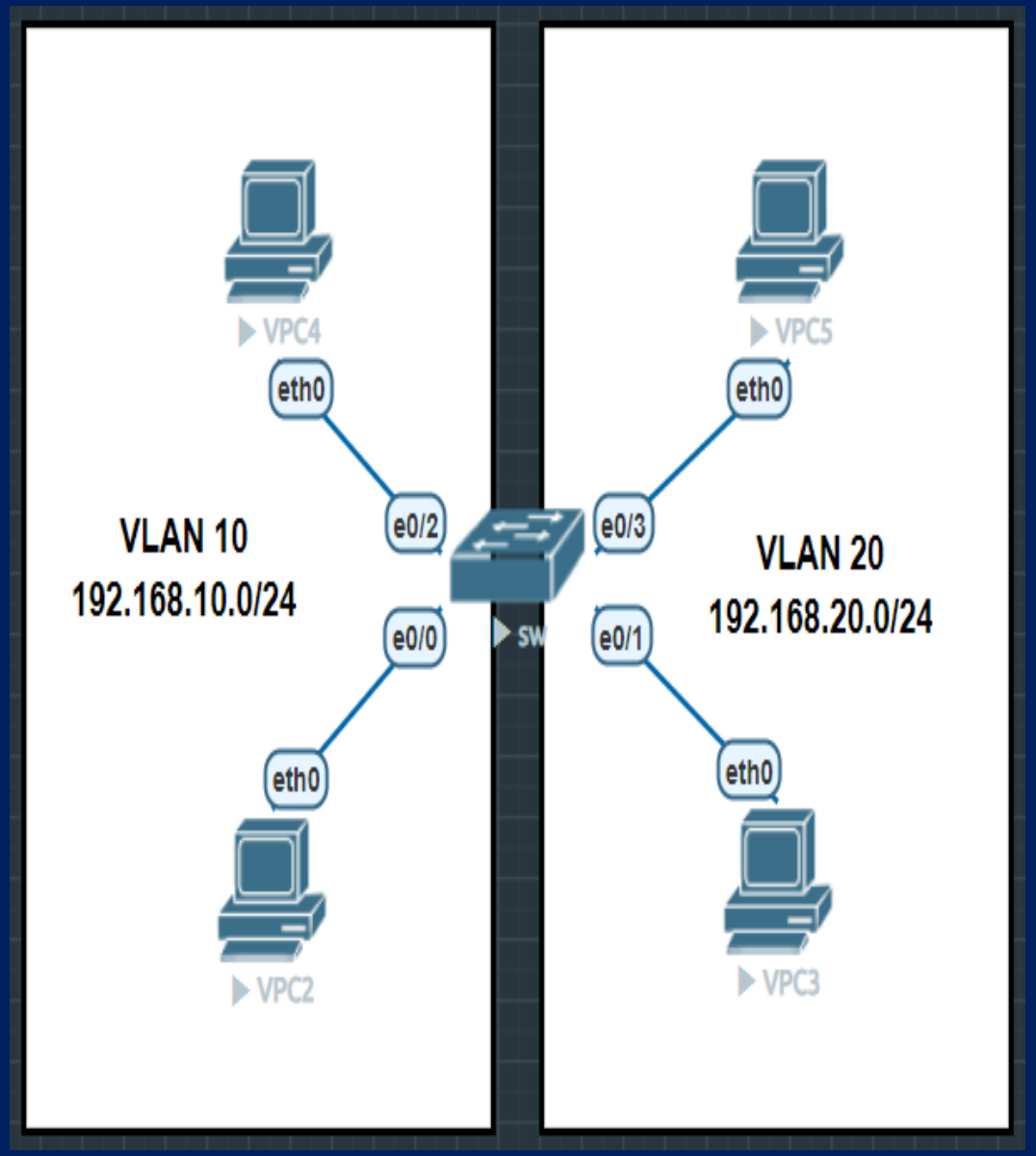
Sw(conf)#interface eth0/2

Sw(conf-if)#switchport access vlan 10

Sw(conf-if)#switchport mode access

Sw(conf-if)#end

Sw#



VLAN Configuration

PC2 and PC4 are in the VLAN 10.

PC3 and PC5 are in the VLAN 20.

```
Sw(conf)#interface eth0/0
Sw(conf-if)#switchport access vlan 10
Sw(conf-if)#switchport mode access
Sw(conf-if)#end
```

```
Sw(conf)#interface eth0/1
Sw(conf-if)#switchport access vlan 10
Sw(conf-if)#switchport mode access
Sw(conf-if)#end
```

```
Sw(conf)#interface eth0/3
Sw(conf-if)#switchport access vlan 10
Sw(conf-if)#switchport mode access
Sw(conf-if)#end
```

switchport mode access – is an optional command. By default, Catalyst switchports mode are access mode.

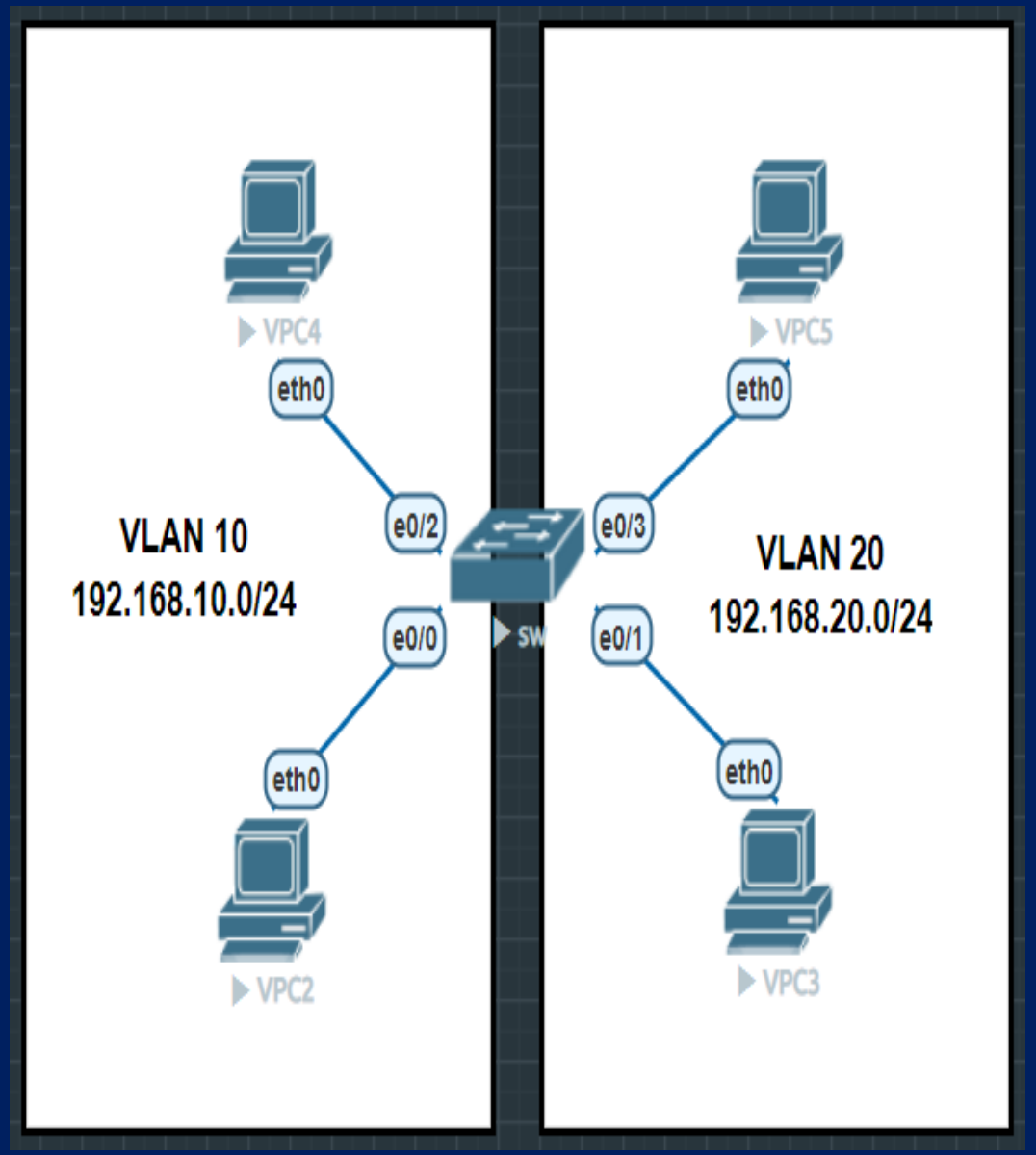
Verification commands:

Sw#show vlan brief

Sw#show running configuration

Sw#show vlan id 10

Packet Tracer Practice



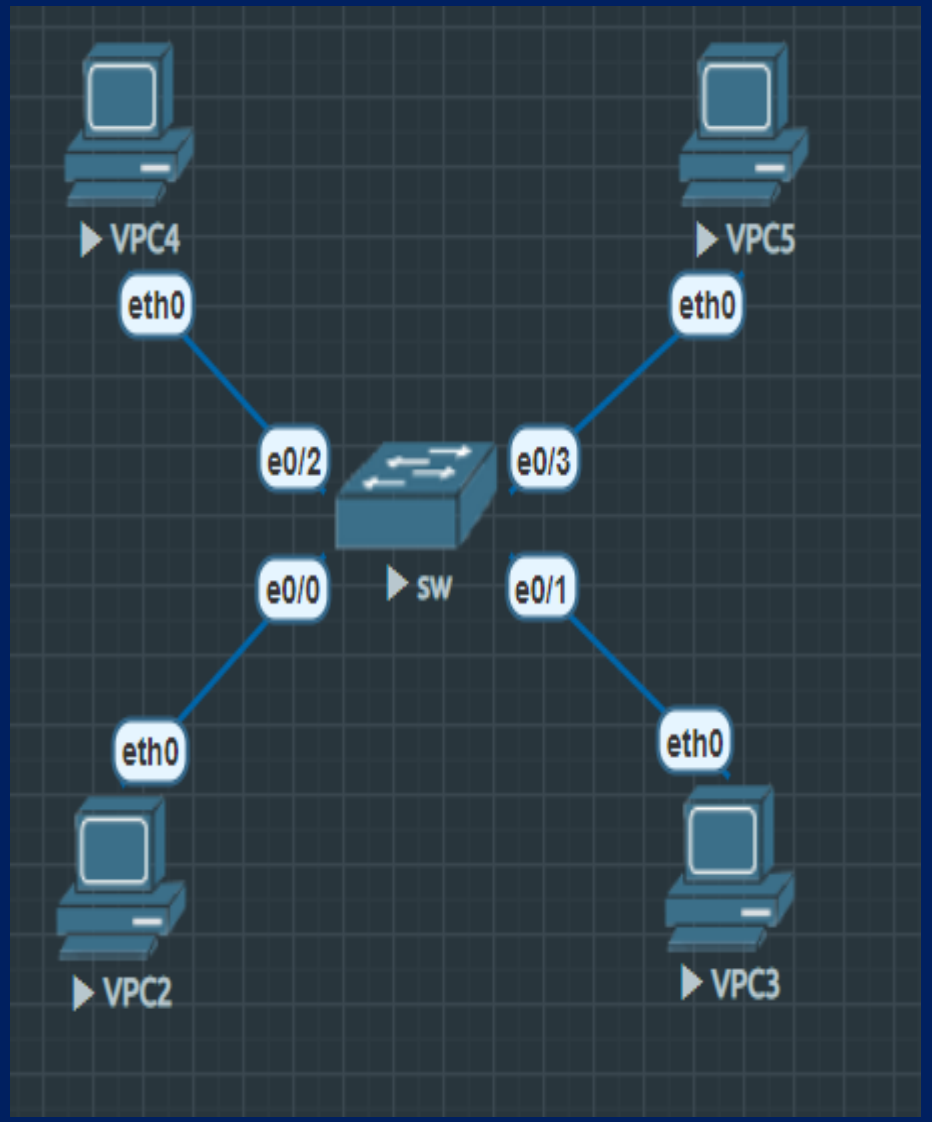
Catalyst switch default VLAN database

Sw#show vlan brief

```
Sw#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Sw#
```

- Reserved VLANs: 0 & 4095
- VLAN 1: default vlan; cannot be deleted; can be used
- VLAN 2-1001: ethernet VLANs; can be used
- VLAN 1002-1005: FDDI & TokenRing VLANs. cannot be deleted
- Extended VLANs: 1006-4094: ethernet VLANs only



VLANs in multiswitch topology

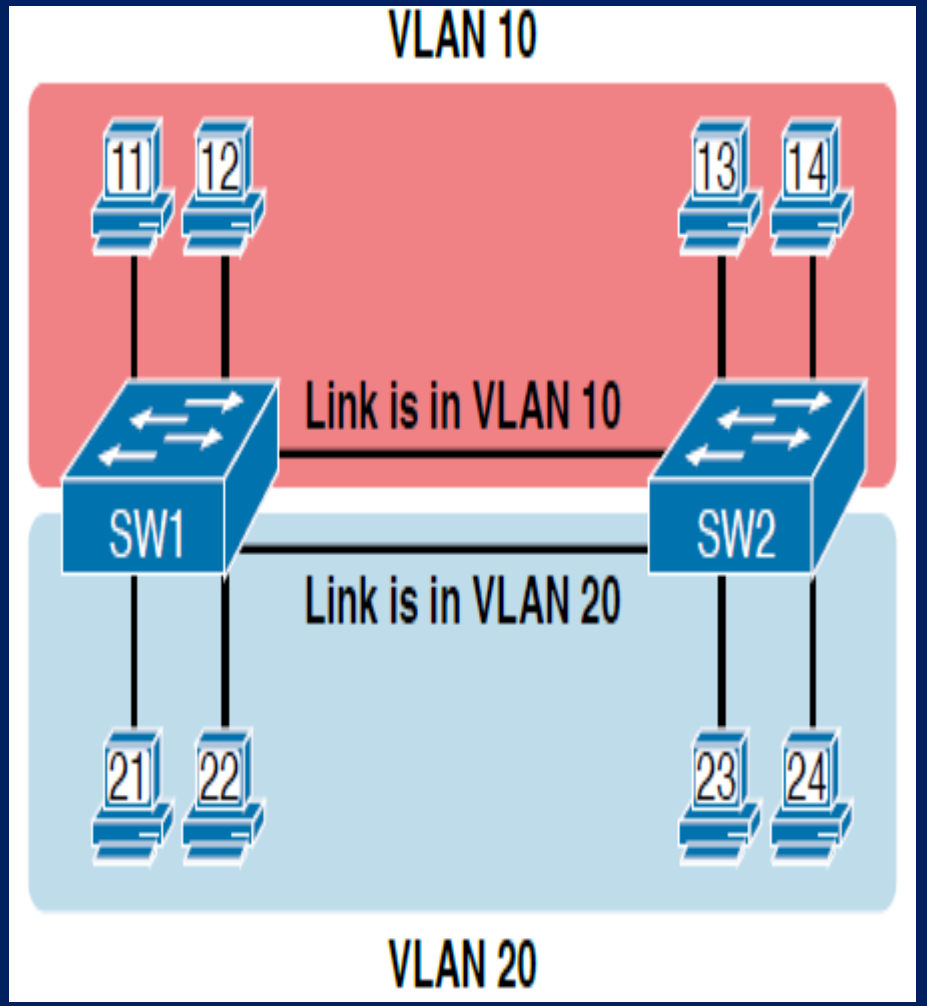
Let’s suppose we have topology with two switches and eight computers.

PC11, PC12, PC13, PC14 are in the VLAN 10.

PC21, PC22, PC23, PC24 are in the VLAN 20.

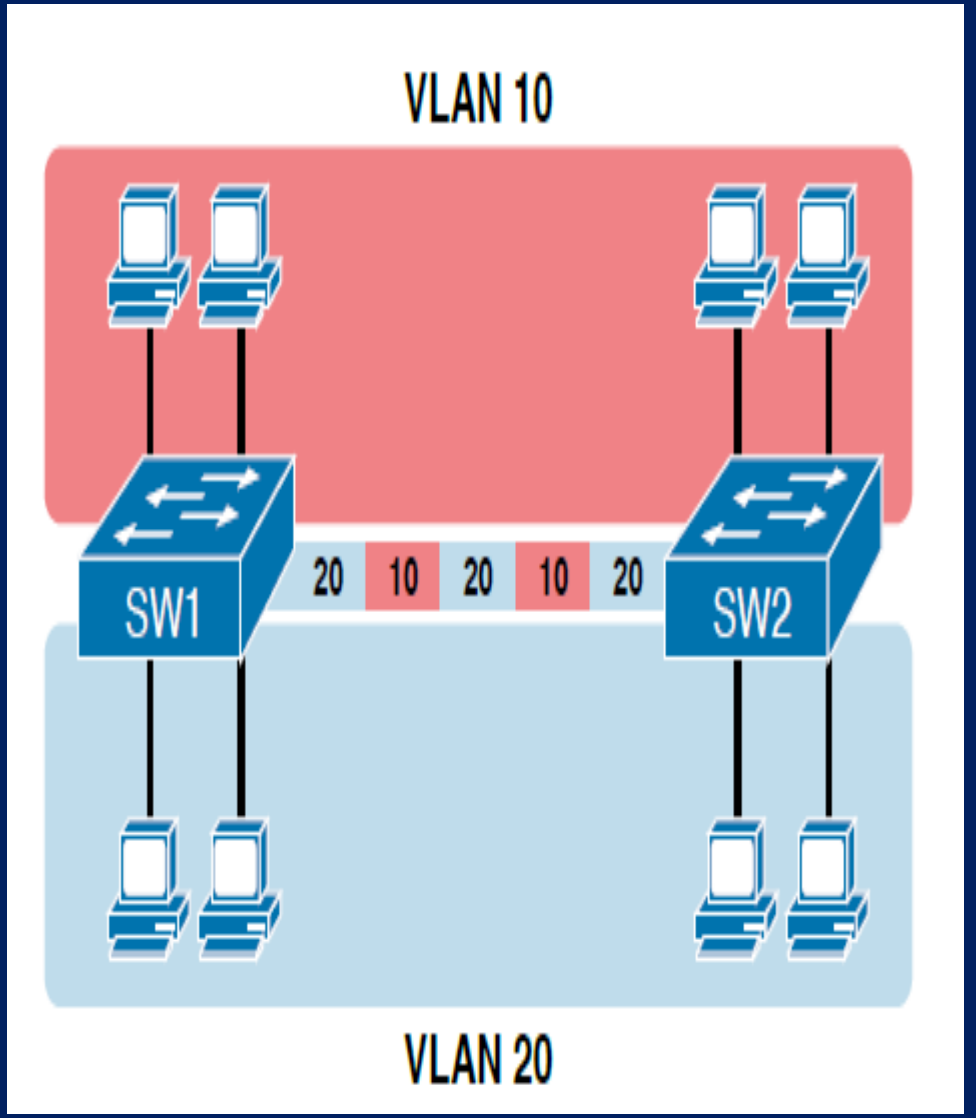
For communication of PCs in the same VLAN but different switches we need per VLAN per physical link between switches. It works but is not scalable. If we have more VLANs we need more physical links.

The solution for this problem is VLAN tagging.



VLAN Tagging Concepts

VLAN trunking creates one link between switches that supports as many VLANs as you need. As a VLAN trunk, the switches treat the link as if it were a part of all the VLANs. At the same time, the trunk keeps the VLAN traffic separate, so frames in VLAN 10 would not go to devices in VLAN 20, and vice versa, because each frame is identified by VLAN number as it crosses the trunk.



VLAN Tagging Concepts cont.

The use of trunking allows switches to forward frames from multiple VLANs over a single physical connection by adding a small header to the Ethernet frame. The image in the right defines the process.

PC11 in SW1, PC13 and PC14 in SW2 are in the VLAN 10.

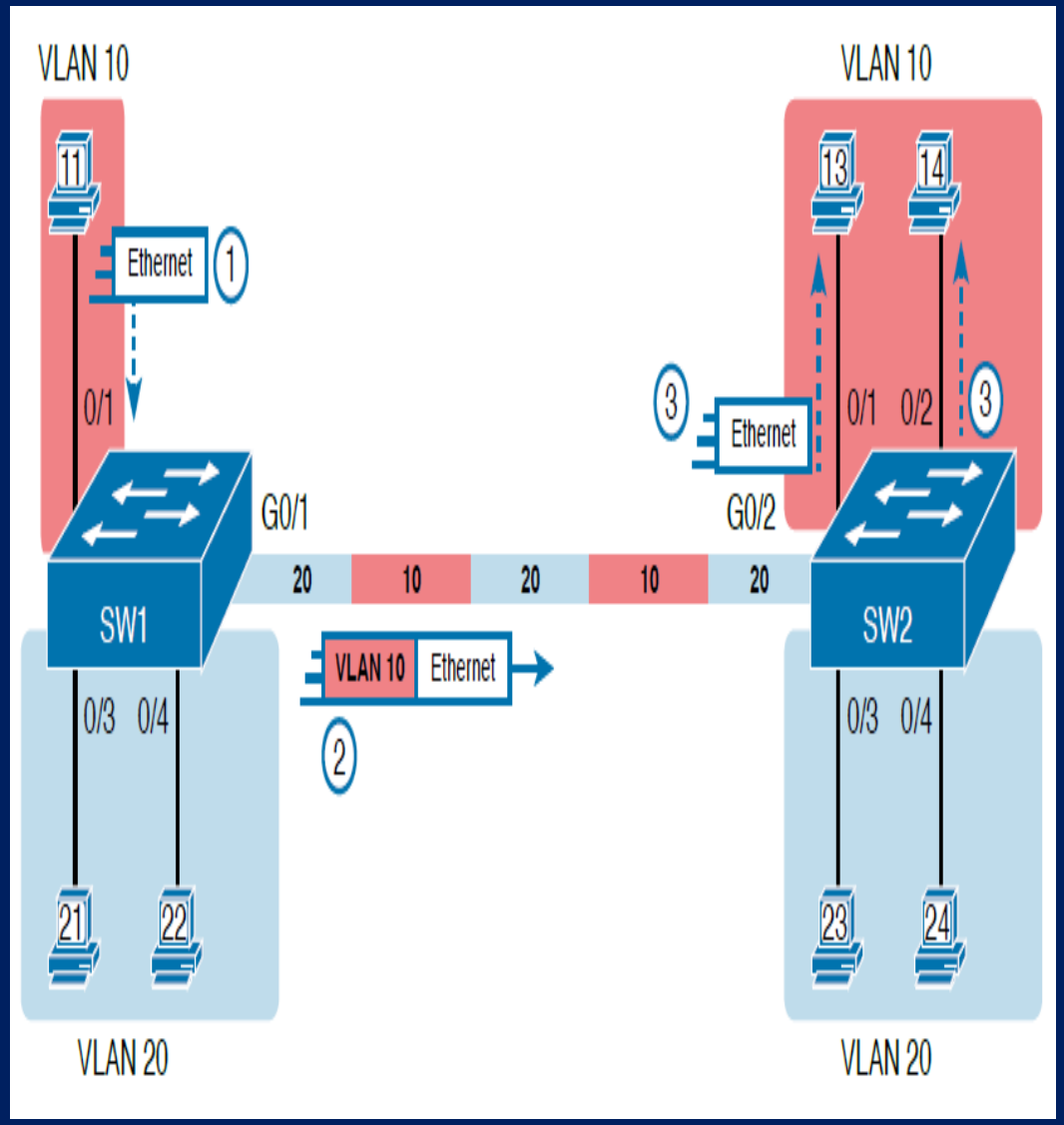
PC21,PC22 in SW1 and PC23, PC24 in SW2 are in VLAN 20.

G0/1 in SW1 and G0/2 in SW2 are trunk ports.

Step1: PC11 sends ethernet frame.

Step2: SW1 adds VLAN tag to the frame on its G0/1 interface and forwards frame to SW2.

Step3: SW2 looks VLAN tag and identifies to which port the frame will be flooded. In our case SW2 removes VLAN tag and will flood the frame to 0/1 and 0/2 interfaces.



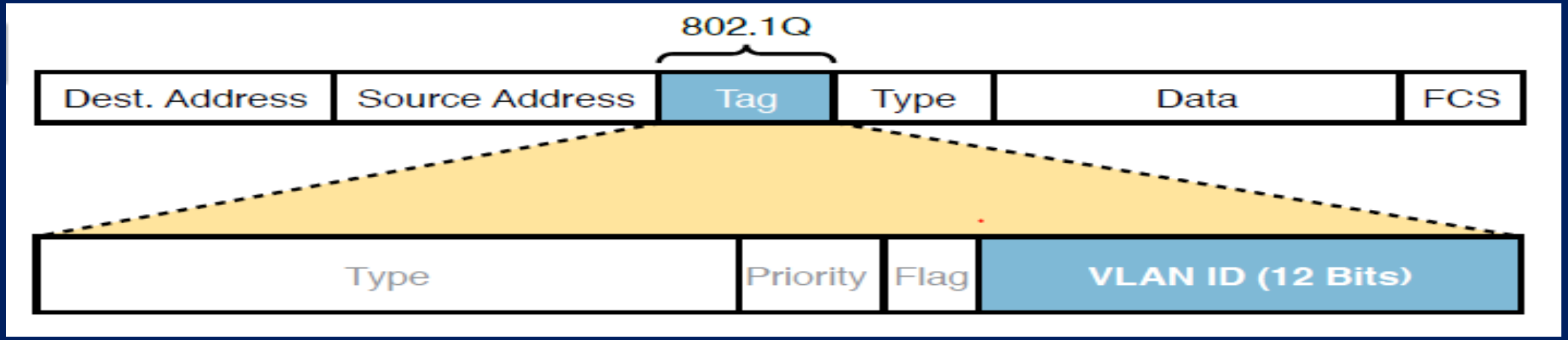
The 802.1Q and ISL VLAN Trunking Protocols

Cisco has supported two different trunking protocols over the years:

- ISL (Inter-Switch Link)
- 802.1Q

Cisco created the ISL years before 802.1Q, in part because the IEEE had not yet defined a VLAN trunking standard. Today, 802.1Q has become the more popular trunking protocol, with Cisco not even bothering to support ISL in many of its switch models today.

While both ISL and 802.1Q tag each frame with the VLAN ID, the details differ. 802.1Q inserts an extra 4-byte 802.1Q VLAN header into the original frame's Ethernet header.



802.1Q header = 32 Bit. VLAN ID = 12 Bits

VLAN Trunking Configuration

We can configure trunk port statically using the next command in the interface configuration mode.

Sw(conf-if)#switchport mode trunk

However, trunking configuration on Cisco switches includes many more options, including several options for dynamically negotiating various trunking settings. The configuration can either predefine different settings or tell the switch to negotiate the settings, as follows:

- **The type of trunking:** IEEE 802.1Q, ISL, or negotiate which one to use, on switches that support both types of trunking.
- **The administrative mode:** Whether to always trunk, always not trunk, or negotiate whether to trunk or not.

The negotiation is done by DTP (Dynamic Trunking Protocol)

Sw(conf-if)#switchport mode trunk command allows all VLANs to pass trunk port. If we give permission to special VLANs then we use the next command:

Sw(conf-if)#switchport trunk allow vlan 10,20,30

We can also change native VLAN. By default native VLAN is 1 (default VLAN).

Sw(config-if)#switchport trunk native vlan 10

Packet Tracer Practice …

Switchports Operational Modes

Command Option	Description
access	Always act as an access (nontrunk) port
trunk	Always act as a trunk port
dynamic desirable	Initiates negotiation messages and responds to negotiation messages to dynamically choose whether to start using trunking
dynamic auto	Passively waits to receive trunk negotiation messages, at which point the switch will respond and negotiate whether to use trunking

Packet Tracer Practice…

That is all for Lesson 9

The key is :

Learn

Repeat

Practice

You will be able to reach your goals.

GOOD LUCK !!!!!...