Badji Mokhtar University Annaba

Electronics Department

Master 1: Networks and Telecommunication

Module: IP Routing

Chapter 2: VLAN (2)

November 13, 2018 Annaba, Algeria

VLANs

VLANs (Virtual LANs) are logical grouping of devices in the same broadcast domain.

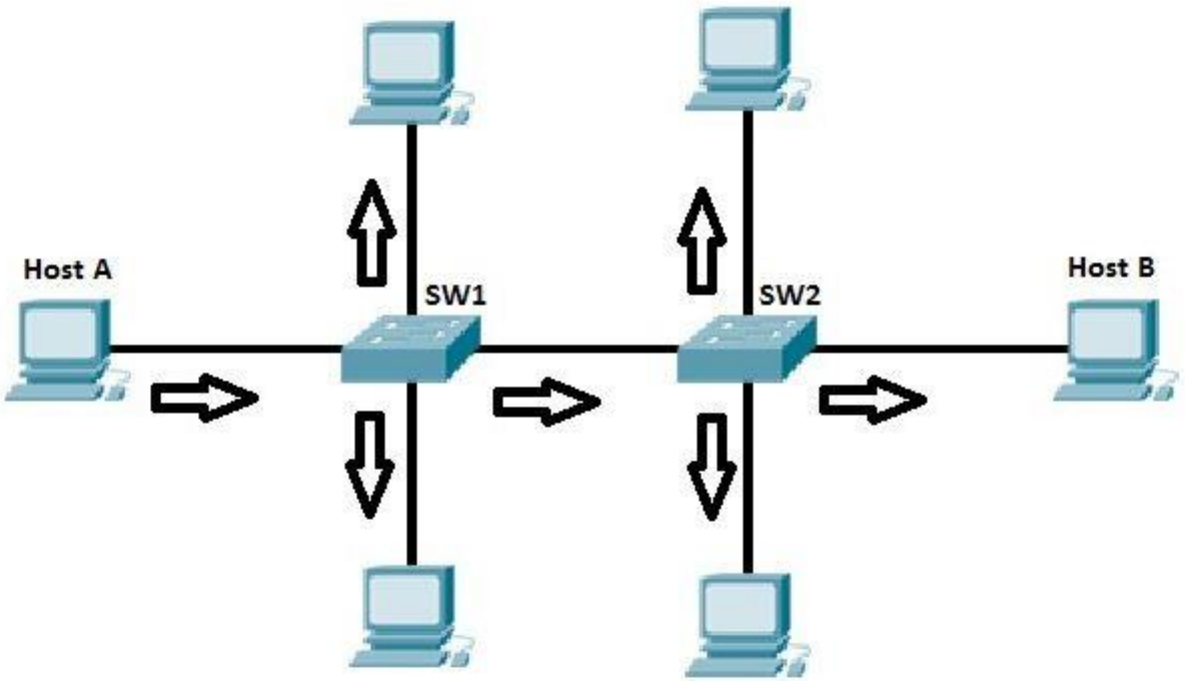
VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another.

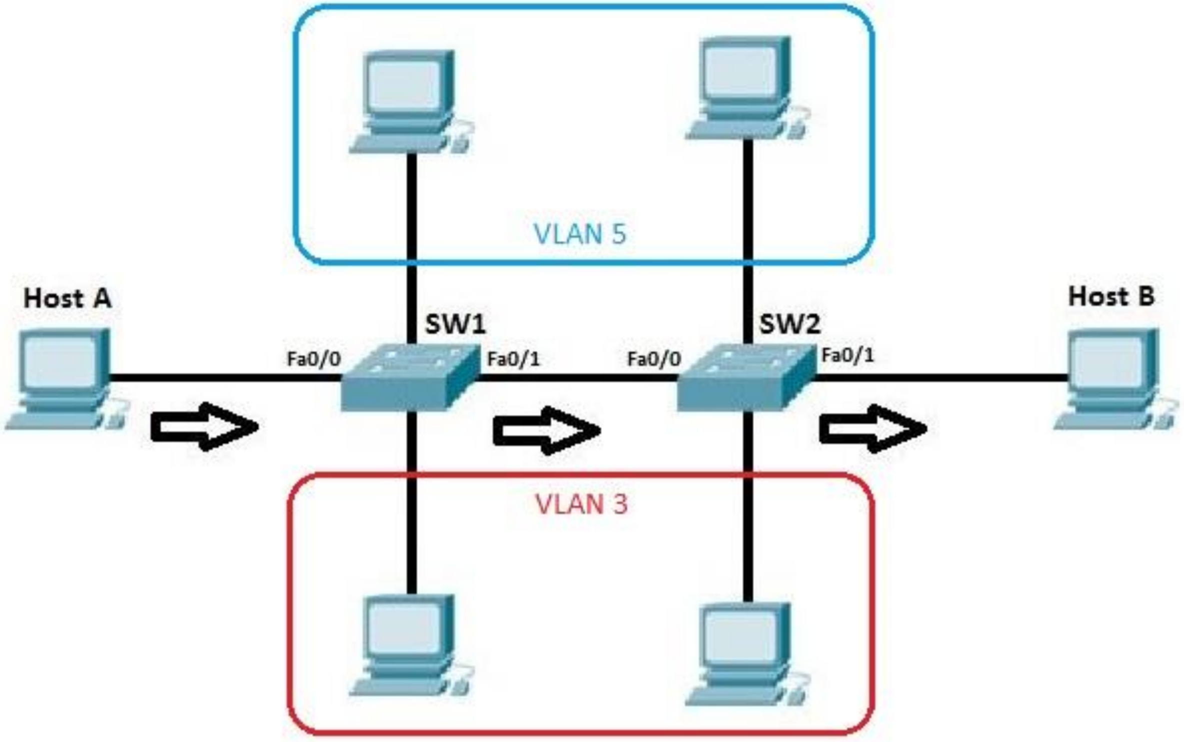
VLANs can be spread across multiple switches, with each VLAN being treated as its own subnet or broadcast domain. This means that frames broadcasted onto the network will be switched only between the ports within the same VLAN.

VLANs

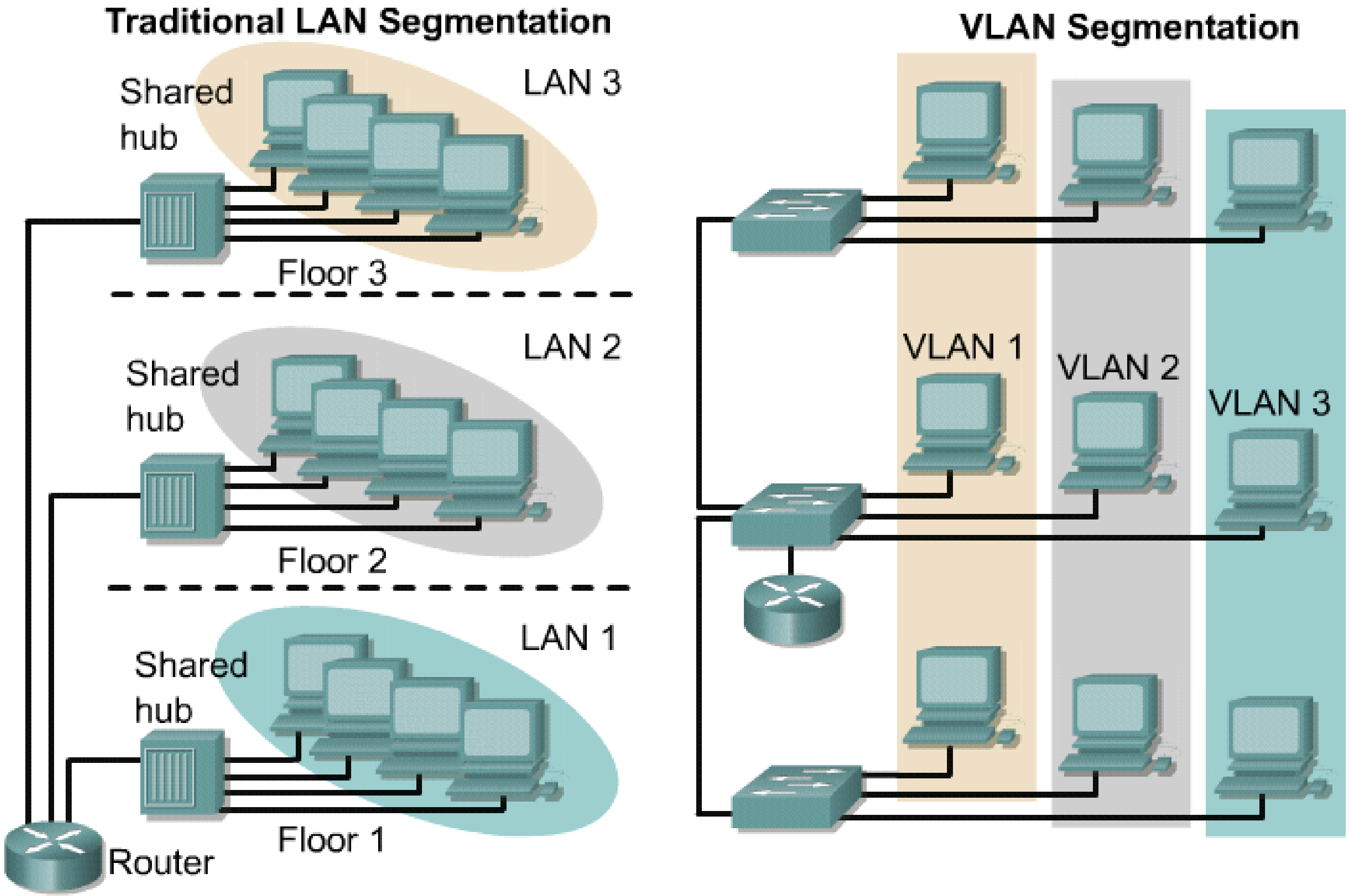
- VLANs increase the number of broadcast domains while decreasing their size.
- VLANs reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood.
- Keeping hosts that hold sensitive data on a separate VLAN to improve security.
- Creating more flexible network designs that group users by department instead of by physical location.
- Network changes are achieved with ease by just configuring a port into the appropriate VLAN.

VLANs


Host A
SW1
SW2
Host B


VLAN 5
Host A
Fa0/0
SW1
Fa0/1
Fa0/0
SW2
Fa0/1
Host B
VLAN 3

VLANs


Traditional LAN Segmentation
Shared hub
LAN 3
Floor 3
Shared hub
LAN 2
Floor 2
Shared hub
LAN 1
Floor 1
Router
VLAN Segmentation
VLAN 1
VLAN 2
VLAN 3

Access & trunk ports

Each port on a switch can be configured as either an access or a trunk port.

- An access port is a port that can be assigned to a single VLAN.

This type of interface is configured on switch ports that are connected to devices with a normal network card, for example a host on a network.

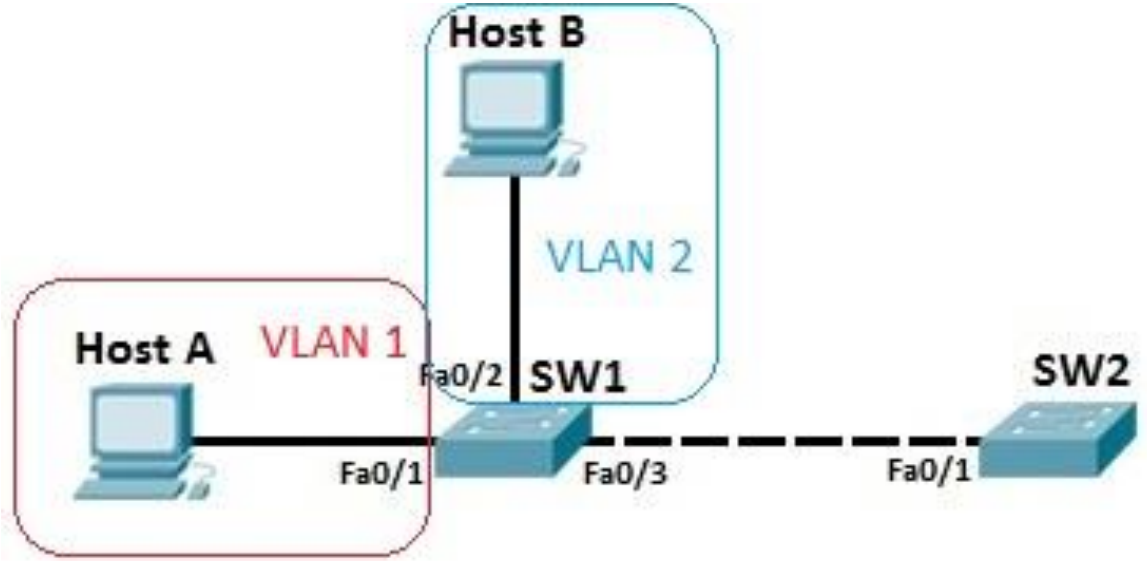
- A trunk interface is an interface that is connected to another switch. This type of interface can carry traffic of multiple VLANs.

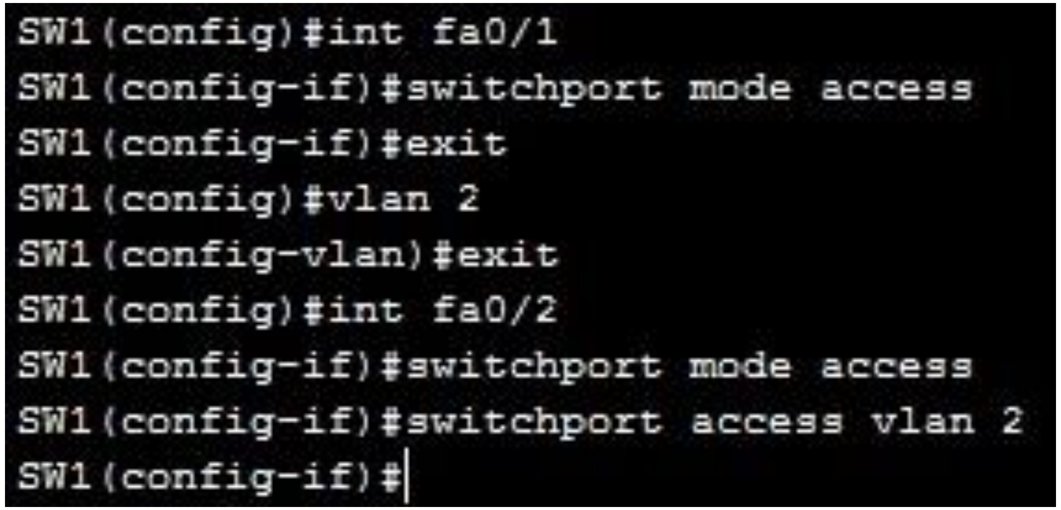
Configuring access & trunk ports

- To configure an interface to be an access interface, the ***switchport mode access*** interface command is used. This type of interface can be assigned only to a single VLAN.

- To configure a trunk interface, the ***switchport mode trunk*** interface command is used. This type of interface can carry traffic of multiple VLANs.

Configuring access & trunk ports



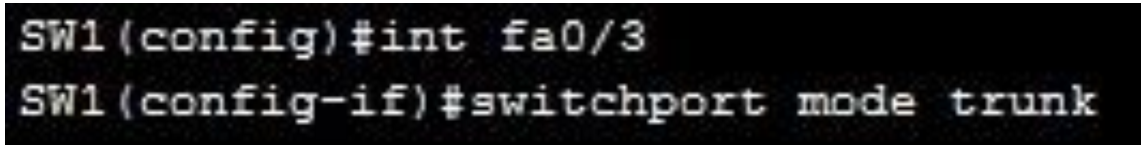


```
SW1(config)#int fa0/1
SW1(config-if)#switchport mode access
SW1(config-if)#exit
SW1(config)#vlan 2
SW1(config-vlan)#exit
SW1(config)#int fa0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#
```

Configuring access & trunk ports

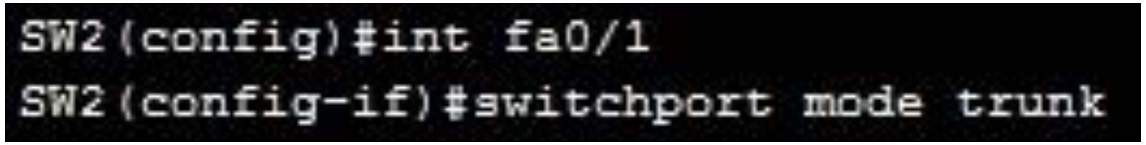
Because the link between SW1 and SW2 needs to carry traffic of multiple VLANs, it needs to be configured as a trunk interface. This is done by using the following commands on both SW1 and SW2:

On SW1:



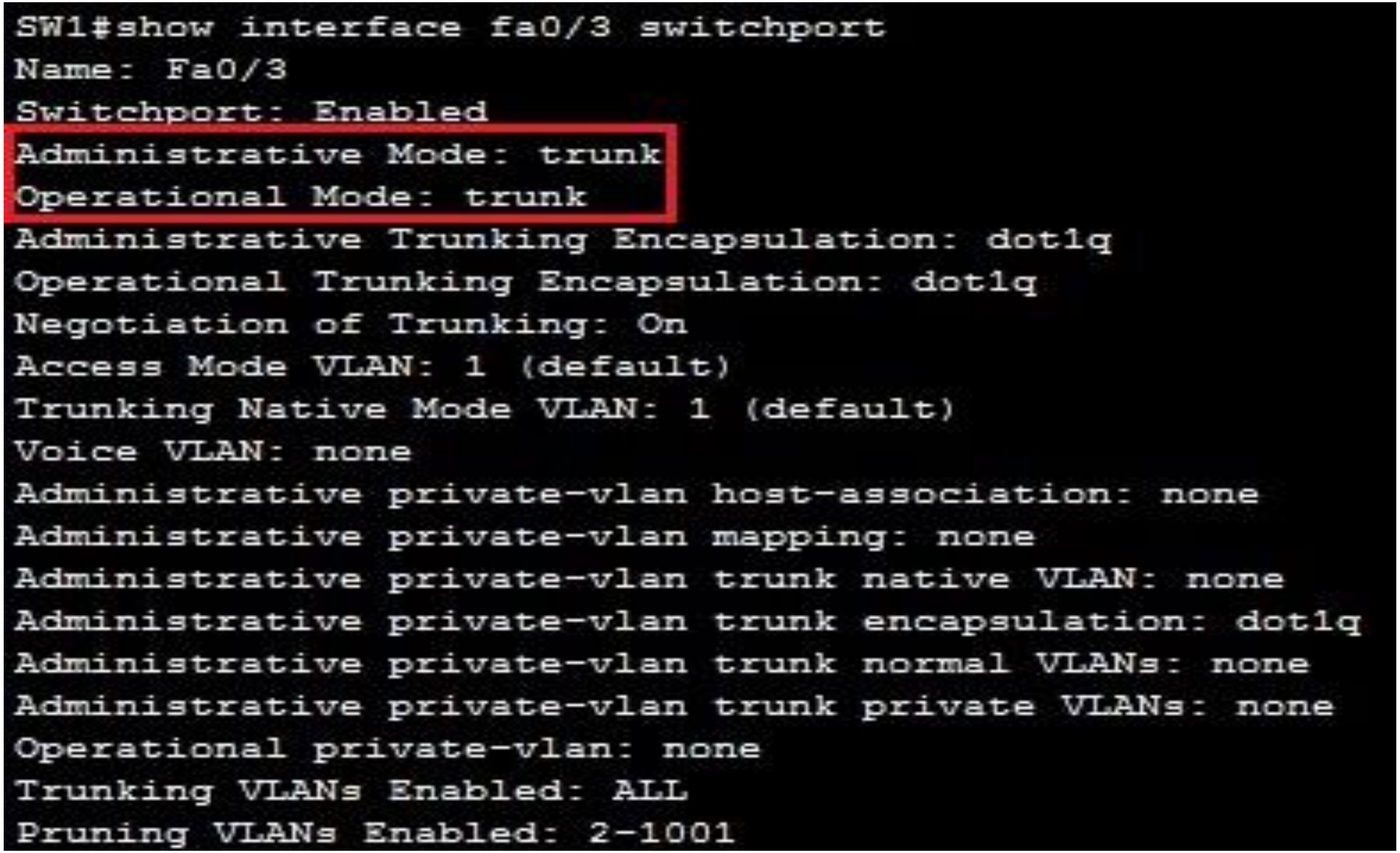
```
SW1(config)#int fa0/3
SW1(config-if)#switchport mode trunk
```

On SW2:



```
SW2(config)#int fa0/1
SW2(config-if)#switchport mode trunk
```

Configuring access & trunk ports



```
SW1#show interface fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

Frame tagging

To identify the VLAN a packet is belonging to, switches use tagging to assign a numerical value to each frame in a network with multiple VLANs. This is done to ensure that switches know out which ports to forward frames.

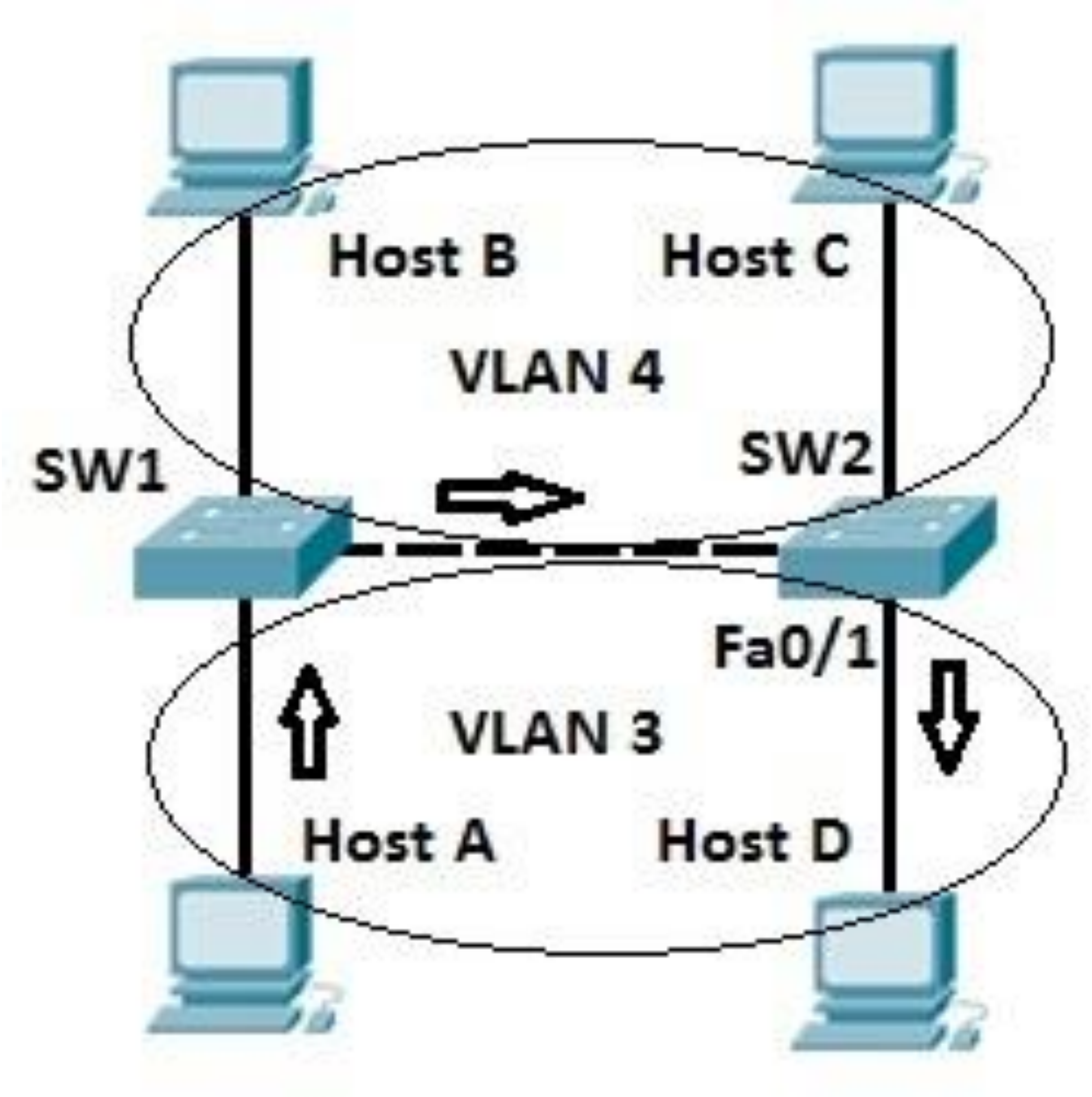
Frame tagging

- There are two VLANs in the toplogy pictured above, namely VLAN 3 and VLAN 4.

- Host A sends a broadcast packet to switch SW1. Switch SW1 receives the packet, tags the packet with the VLAN ID of 3 and sends it to SW2.

- SW2 receives the packet, looks up at the VLAN ID, and forwards the packet only out the port Fa0/1, since only that port is in VLAN 3.

- Host B and host C will not receive the packet because they are in different VLAN than host A

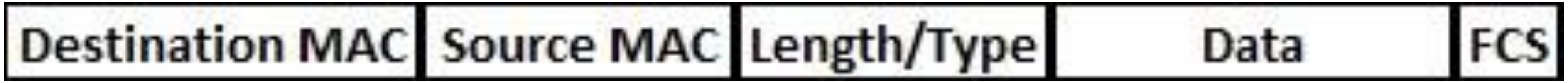


IEEE 802.1Q

IEEE 802.1Q is one of the VLAN tagging protocols supported by Cisco switches. This standard was created by the Institute of Electrical and Electronics Engineers (IEEE), so it an open standard and can be used on non-Cisco switches.

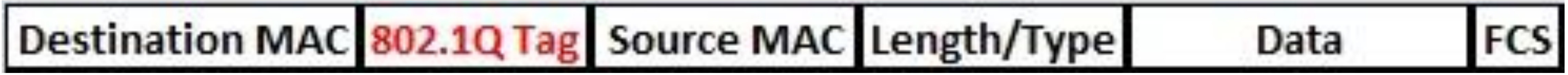
To identify to which VLAN a frame belongs to, a field is inserted into the frame’s header.

Original frame:



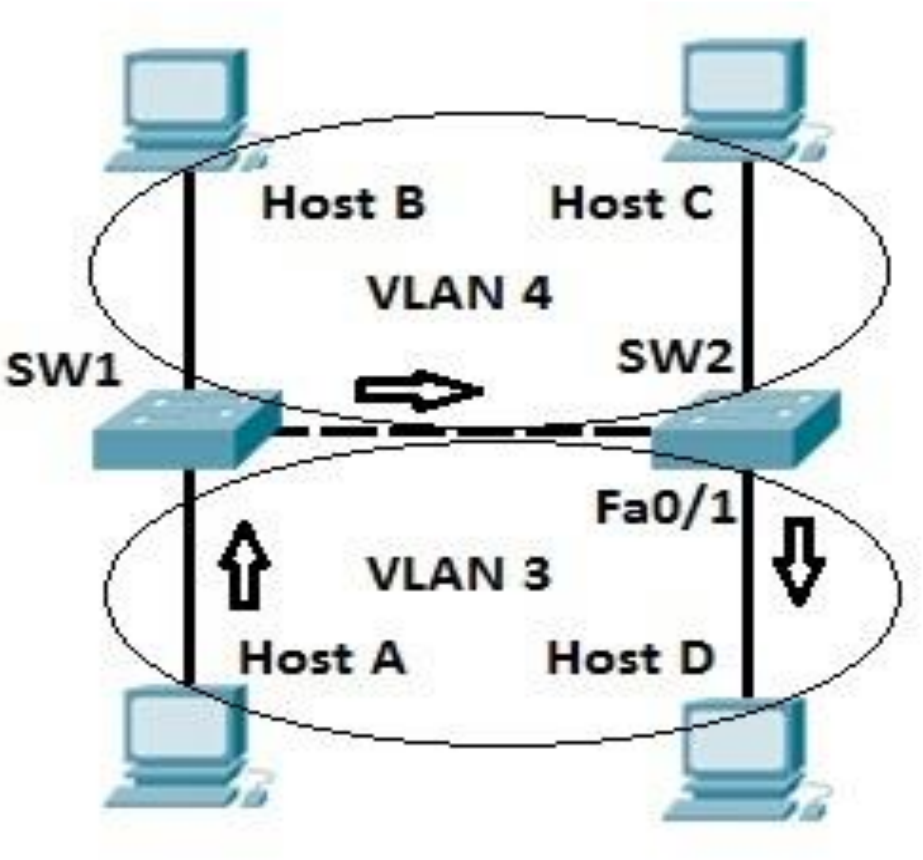
Destination MAC	Source MAC	Length/Type	Data	FCS

802.1Q frame:



Destination MAC	802.1Q Tag	Source MAC	Length/Type	Data	FCS

IEEE 802.1Q



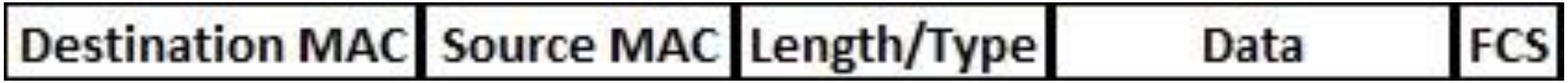
On the segment between two switches, a process called VLAN trunking is used. Let’s say that host A sends a broadcast frame. SW1 “tags” the frame by inserting the VLAN ID in the header of the frame before sending the frame to SW2. SW2 receives the frame and knows that the frame belongs to VLAN 3, so it sends the frame only to host D, since that host is in VLAN 3.

Inter-Switch Link (ISL)

Another VLAN tagging protocol is Inter-Switch Link (ISL). This protocol is Cisco proprietary, which means that, unlike 802.1Q, it can be used only between Cisco switches. It is considered to be deprecated, and newer Cisco switches don't even support it.

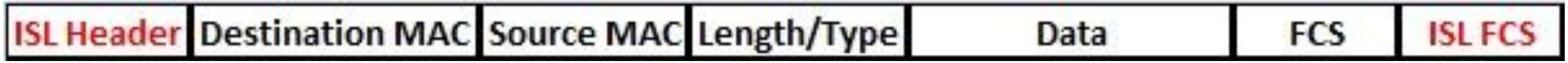
ISL works by encapsulating a frame in an ISL header and trailer. The encapsulated frame remains unchanged. The VLAN ID is included in the ISL header.

Original frame:



Destination MAC	Source MAC	Length/Type	Data	FCS

ISL frame:



ISL Header	Destination MAC	Source MAC	Length/Type	Data	FCS	ISL FCS

What is VTP?

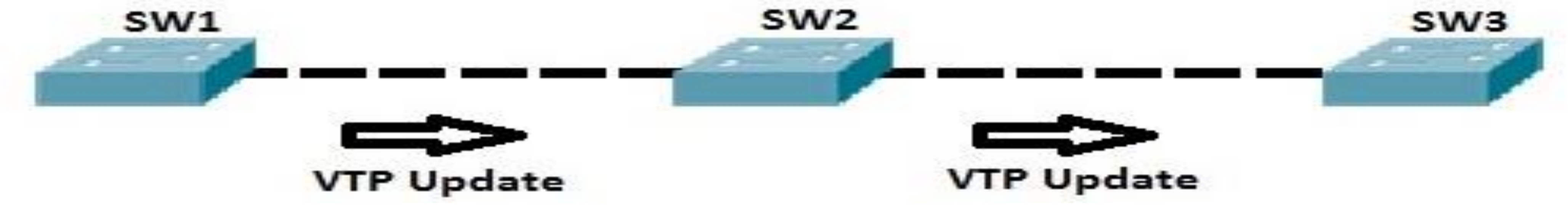
VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol used by Cisco switches to exchange VLAN information. With VTP, you can synchronize VLAN information (like VLAN ID or VLAN name) with switches inside the same VTP domain.

To better understand the true value of VTP, consider an example network with 100 switches. Without VTP, if you want to create a VLAN on each switch, you would have to manually enter VLAN configuration commands on each switch! VTP enables you to create the VLAN only on a single switch. That switch can then propagate information about that VLAN to each switch on a network and cause other switches to create that VLAN too.

Likewise, if you want to delete a VLAN, you only need to delete it on one switch, and the change is automatically propagated to every other switch inside the same VTP domain.

What is VTP?

The following network topology explains the concept more thoroughly.



On SW1, we have created a new VLAN. SW1 sends a VTP update to SW2, which in turn sends its VTP update to SW3. Now all three switches have the same VLAN created.

NOTE
VTP does not advertise information about which switch ports are assigned to which VLAN.

VTP modes

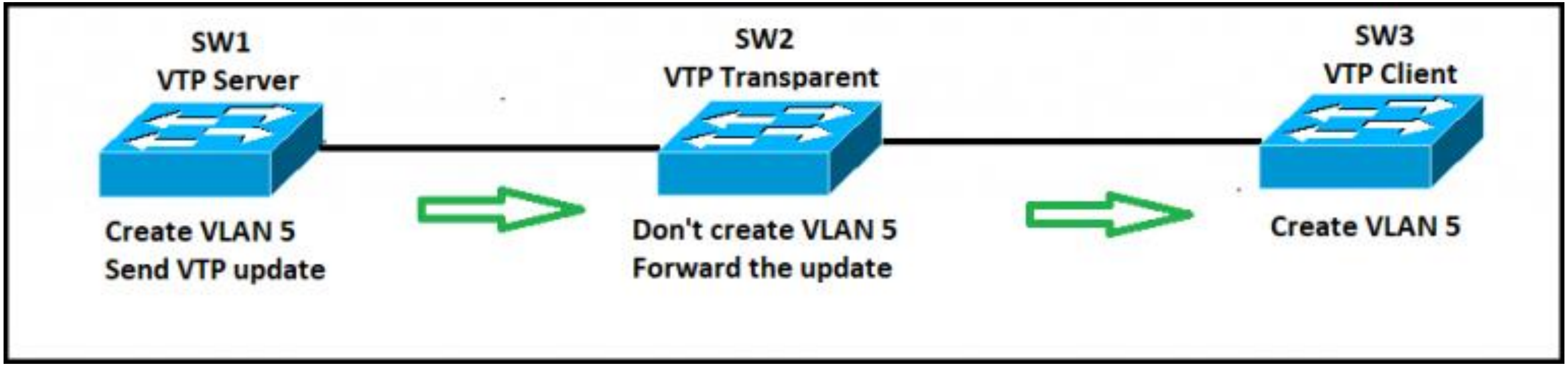
Each switch can use one of three different VTP modes:

•**VTP client mode** – a switch using this mode can’t change its VLAN configuration. That means that a VTP client switch can’t create or delete VLANs. Received VTP updates are processed and forwarded.

•**VTP server mode** – a switch using this mode can create and delete VLANs. A VTP server switch will propagate VLAN changes. This is the default mode for Cisco switches.

•**VTP transparent mode** – a switch using this mode doesn’t share its VLAN database, but it forwards received VTP advertisements. You can create and delete VLANs on a VTP transparent switch, but the changes are not sent to other switches.

VTP modes



We have a simple network of three switches. SW1 is configured as VTP server. After the VLAN 5 is created on SW1, this switch will notify the connected switch (SW2) about the created VLAN.

SW2 will receive the update but, since it uses the VTP transparent mode, it will not create this VLAN in its configuration. However, it will forward the VTP update to SW3.

Since SW3 is configured as VTP client, it will process the update and create VLAN 5.

VTP configuration

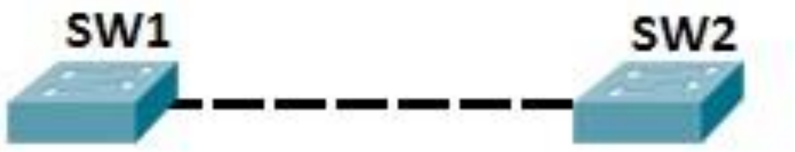
In a typical network, some switches are configured as VTP servers and other switches are configured as VTP clients. A VLAN created on a VTP server switch is automatically advertised to all switches inside the same VTP domain. A VTP domain is simply the collection of switches with the same VTP domain name configured.

To exchange VTP messages, five requirements must be met:

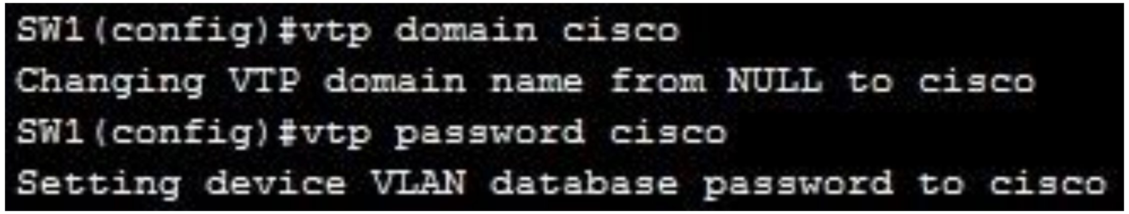
1. A switch has to be configured as either a VTP server or VTP client
2. The VTP domain name has to be the same on both switches
3. If present, the VTP domain password has to be the same
4. VTP versions have to match
5. The link between the switches has to be a trunk link

VTP configuration

Switches SW1 and SW2 are connected via trunk link. We will configure SW1 to serve as a VTP server and SW2 to serve as a VTP client.

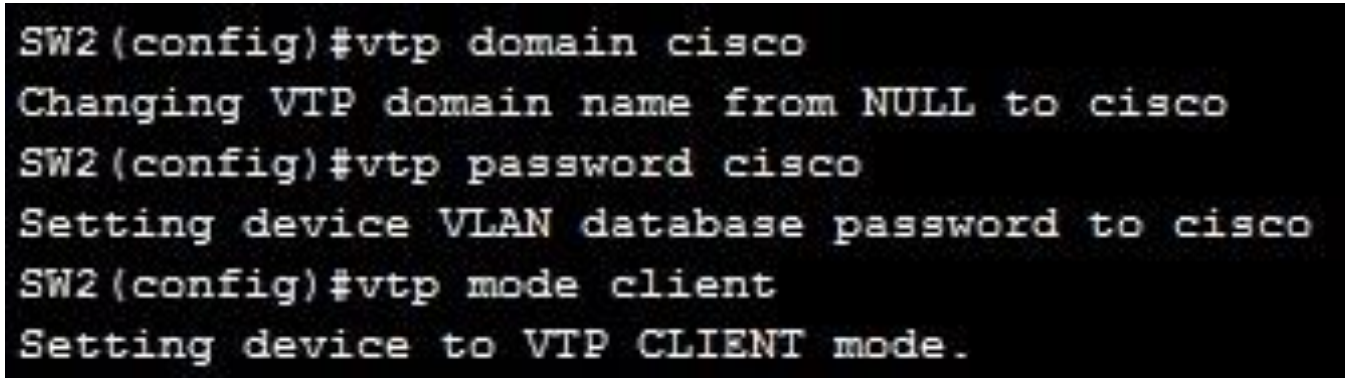


First, we configure SW1:



```
SW1(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
SW1(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Next, we configure SW2:

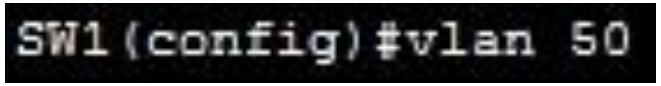


```
SW2(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
SW2(config)#vtp password cisco
Setting device VLAN database password to cisco
SW2(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

VTP configuration

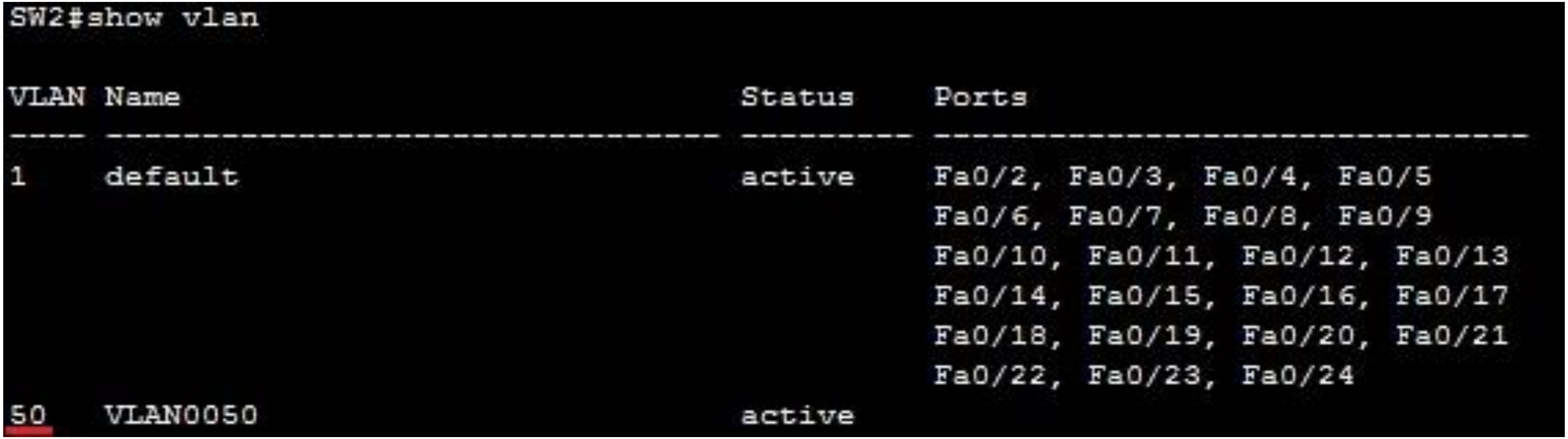
Now, we will create VLAN 50 on SW1. The information about this VLAN will automatically be propagated to SW2. SW2 should also create that VLAN.

On SW1, we will create the new VLAN:



```
SW1(config)#vlan 50
```

VTP forces SW2 to create the same VLAN:



```
SW2#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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
50   VLAN0050                         active
```

Thank you for your attention