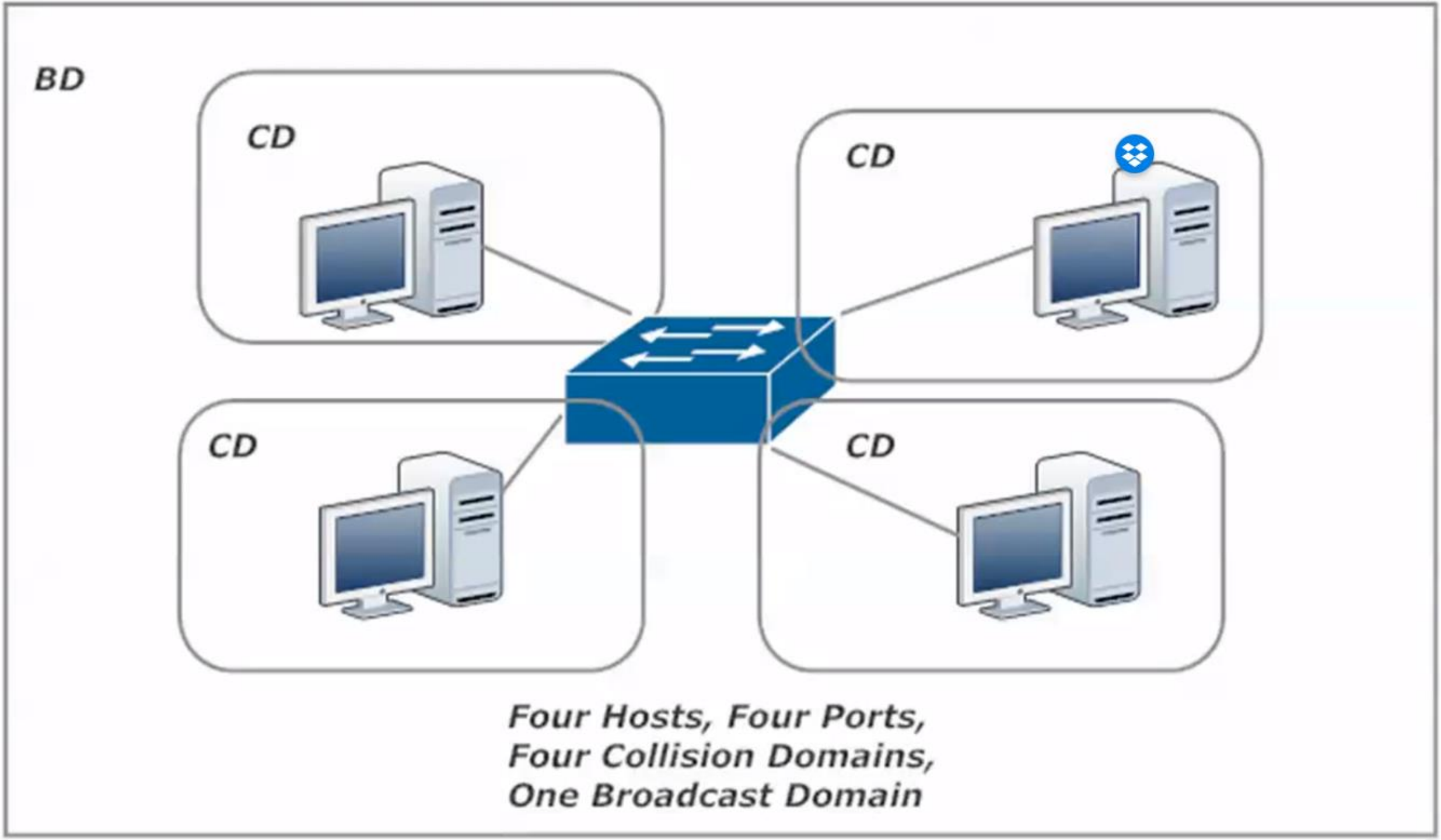
VLANs

Redes II

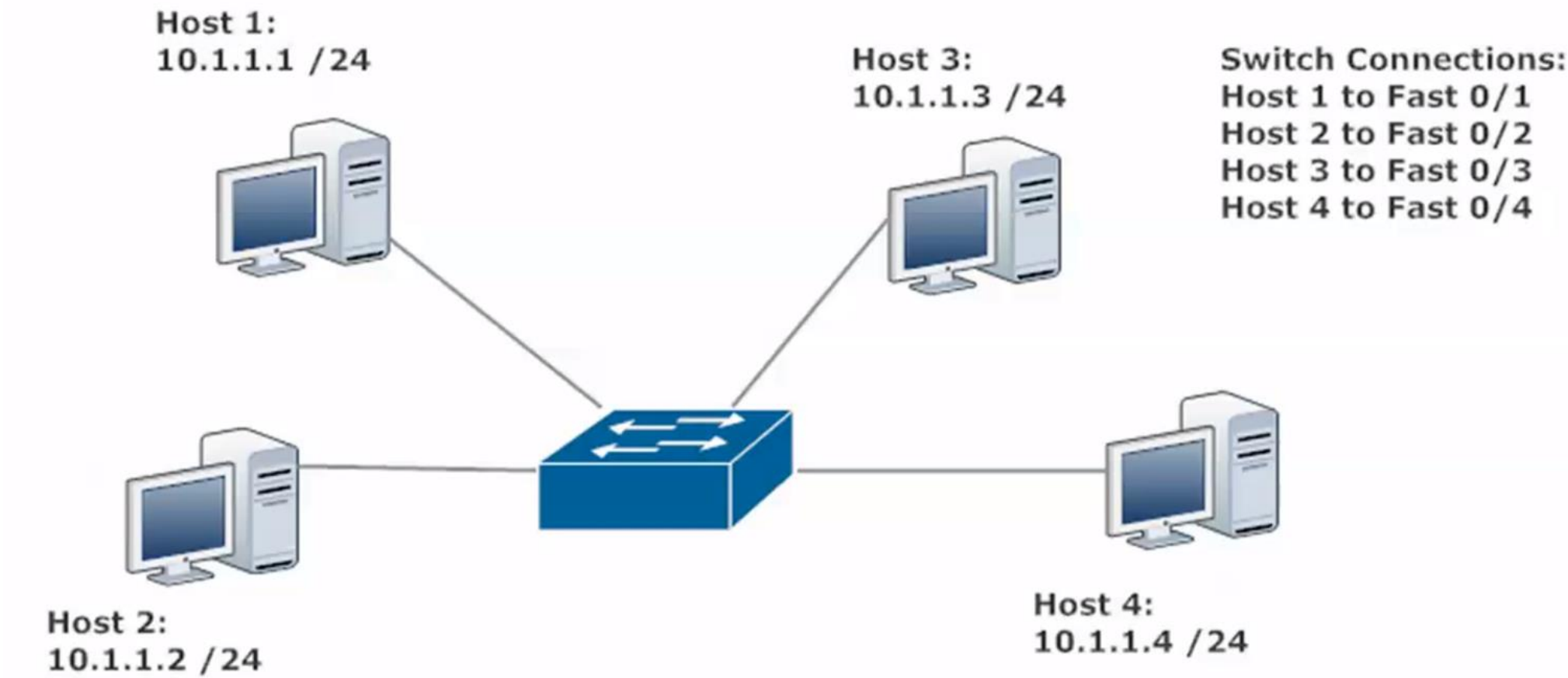

BD
CD
CD
CD
CD
Four Hosts, Four Ports,
Four Collision Domains,
One Broadcast Domain

Razones para usar una Virtual LAN:

- VLANs ayudan a agrupar hosts por departamento, autorizaciones de seguridad y casi cualquier criterio más allá que la ubicación física.
- VLANs permiten incrementar la seguridad “escondiendo” estos grupos de hosts de los demás hosts en una red.
- VLANs ayudan a prevenir la degradación del performance de la red limitando el alcance de los broadcasts de red, lo cual previene también las tormentas de broadcast.

Broadcast storm

- Ocurre cuando una red está sobrecargada por multicast continuo o tráfico de broadcast. Cuando diferentes hosts están enviando o realizando broadcast de data sobre un enlace de red, y los otros dispositivos de dicha red re-envían de vuelta dicha data como respuesta. El switch está tan ocupado atendiendo el tráfico de broadcast que no puede mantener las funciones básicas de switching (como envío de tramas!) de una manera eficiente.


Host 1:
10.1.1.1 /24
Host 3:
10.1.1.3 /24
Switch Connections:
Host 1 to Fast 0/1
Host 2 to Fast 0/2
Host 3 to Fast 0/3
Host 4 to Fast 0/4
Host 2:
10.1.1.2 /24
Host 4:
10.1.1.4 /24

Asignar un puerto a una VLAN

En este ejemplo se asignará el puerto FastEthernet 0/1 del switch Switch1 a la VLAN 24. Si no existiese la VLAN previamente, al ejecutar la asignación del puerto se creará la VLAN.

- Switch1#conf t
- Switch1(conf)#interface fa0/2
- Switch1(conf-if)#switchport access vlan 24

Crear una VLAN

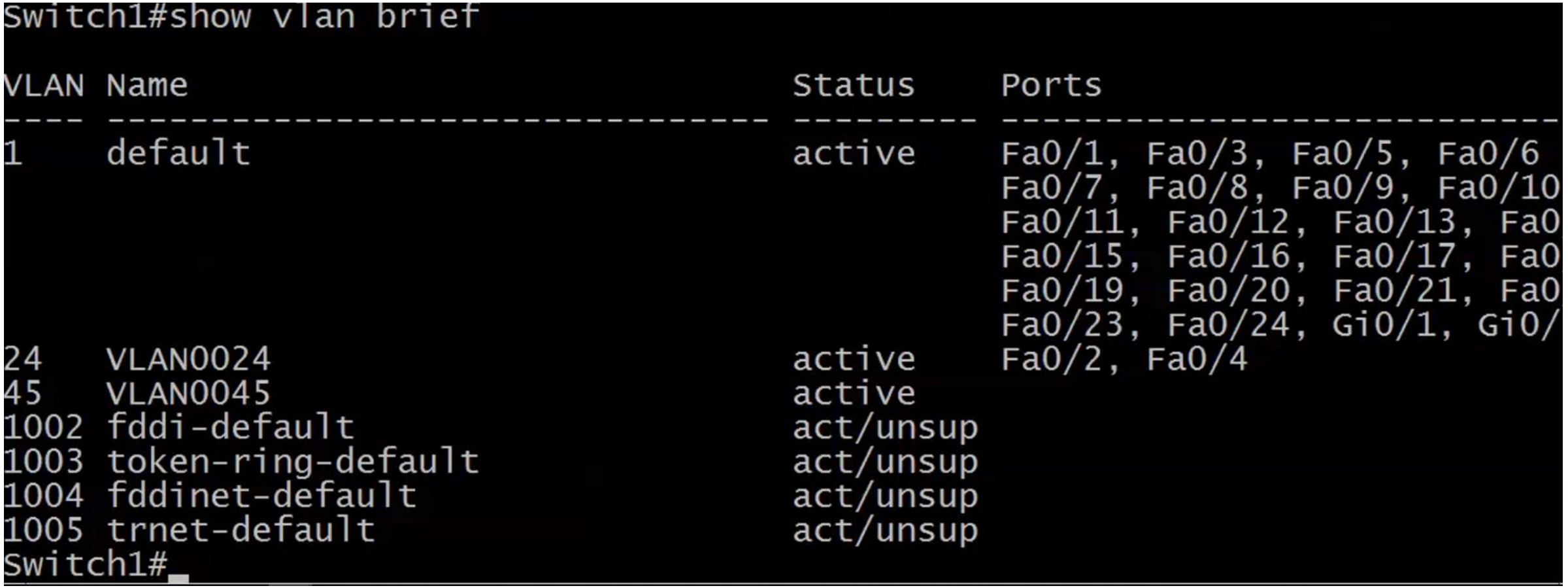
En este ejemplo se creará la VLAN 24 en el switch SW1.

- SW1#conf t
- SW1(conf)#vlan 24
- SW1(conf-vlan)#^Z
- SW1#

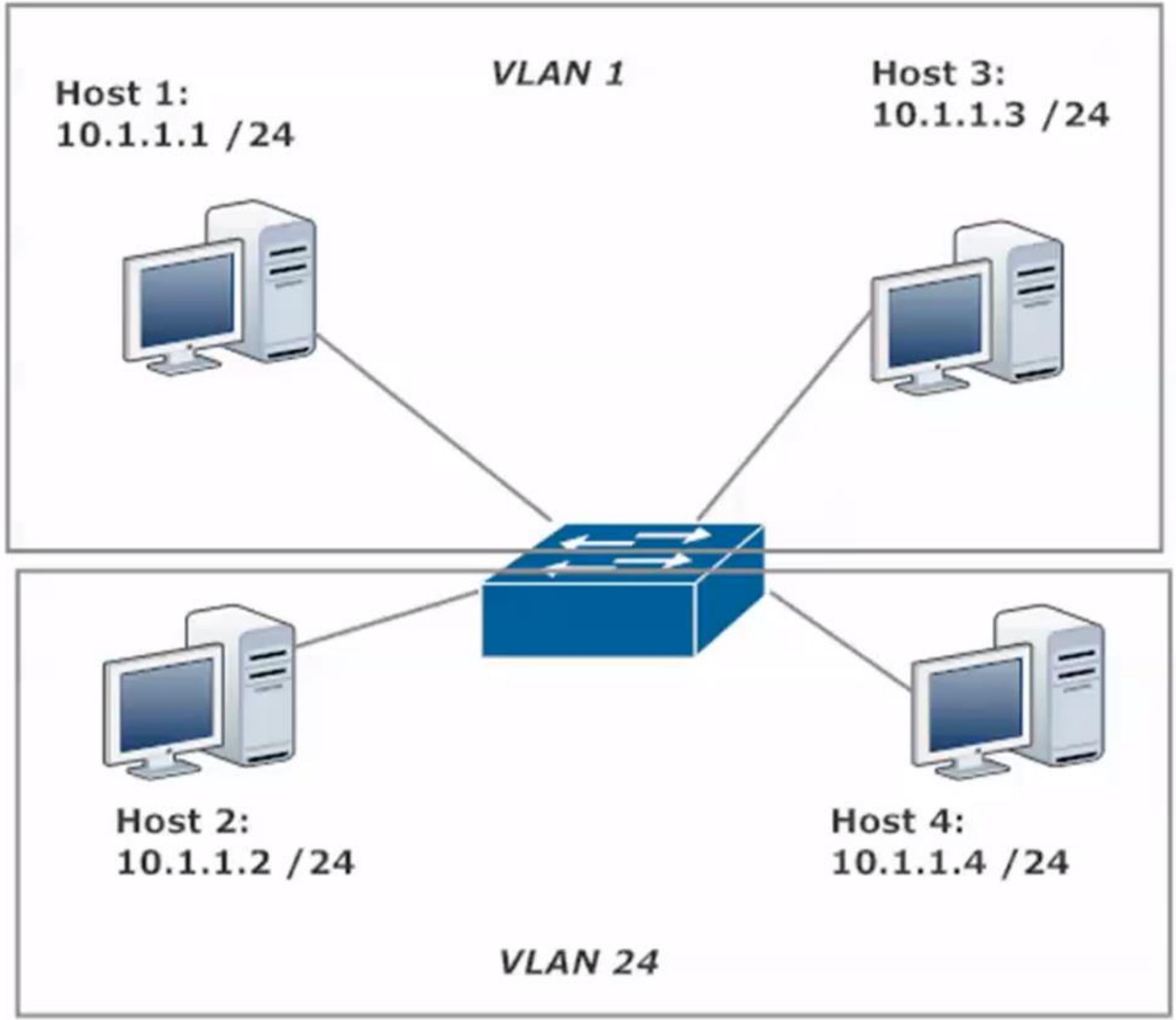
Al ejecutar lo anterior se creará la vlan 24 sin dirección IP asignada.

Mostrar VLANs creadas en un switch

- Switch1#show vlan brief



```
Switch1#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/3, Fa0/5, Fa0/6
                                                   Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                   Fa0/11, Fa0/12, Fa0/13, Fa0
                                                   Fa0/15, Fa0/16, Fa0/17, Fa0
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0
                                                   Fa0/23, Fa0/24, Gi0/1, Gi0/
24   VLAN0024                            active    Fa0/2, Fa0/4
45   VLAN0045                            active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup
Switch1#
```



Switch Connections:
Host 1 to Fast 0/1
Host 2 to Fast 0/2
Host 3 to Fast 0/3
Host 4 to Fast 0/4

Vlan.dat

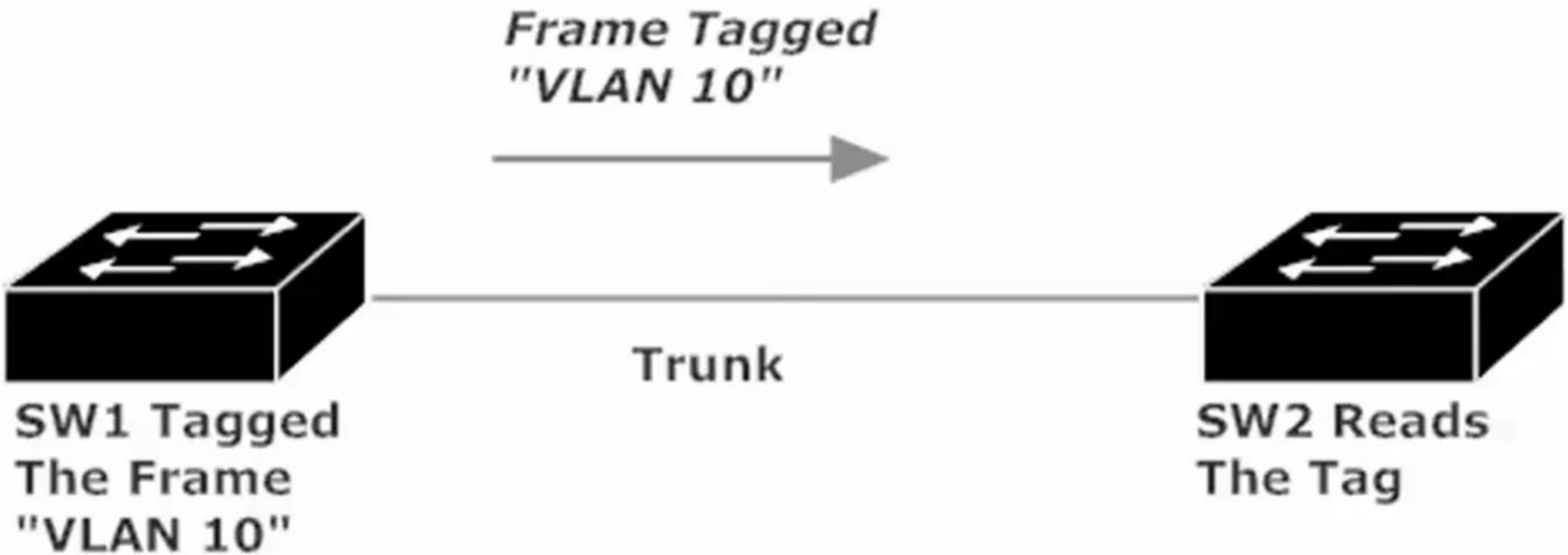
- La configuración de las VLANs de un equipo Cisco es almacenada en el archivo vlan.dat, el cual se encuentra en la Memoria No-volátil.

Trunking switches (y las VLANs que los aman)

- Trunking es el proceso de crear una conexión lógica entre dos switches conectados físicamente, permitiendo que la tramas fluyan entre ambos.

- Un tag (etiqueta) indicando la VLAN de destino se coloca en la trama del switch que transmite. El switch receptor usa este “frame tagging” para ver cuál VLAN debe recibir dicha trama.

- Esto permite que los miembros de la misma VLAN se comuniquen mientras están conectados a diferentes switches.


Frame Tagged
"VLAN 10"
Trunk
SW1 Tagged
The Frame
"VLAN 10"
SW2 Reads
The Tag

ISL (Inter Switch Link)

- Protocolo propiedad de Cisco que mantiene información sobre VLANs en el tráfico entre routers y switches.
- Es el método de encapsulación de Cisco para las VLAN que compite con el protocolo libre (no propietario) de IEEE 802.1Q.
- Encapsula la trama completa antes de enviarla a través del trunk, resultando en mayor sobrecarga que el protocolo de trunk IEEE 802.1q
- Cisco lo ha dejado de incluir en equipos recientes.
- No reconoce el concepto native VLAN.

IEEE 802.1q (“dot1q”)

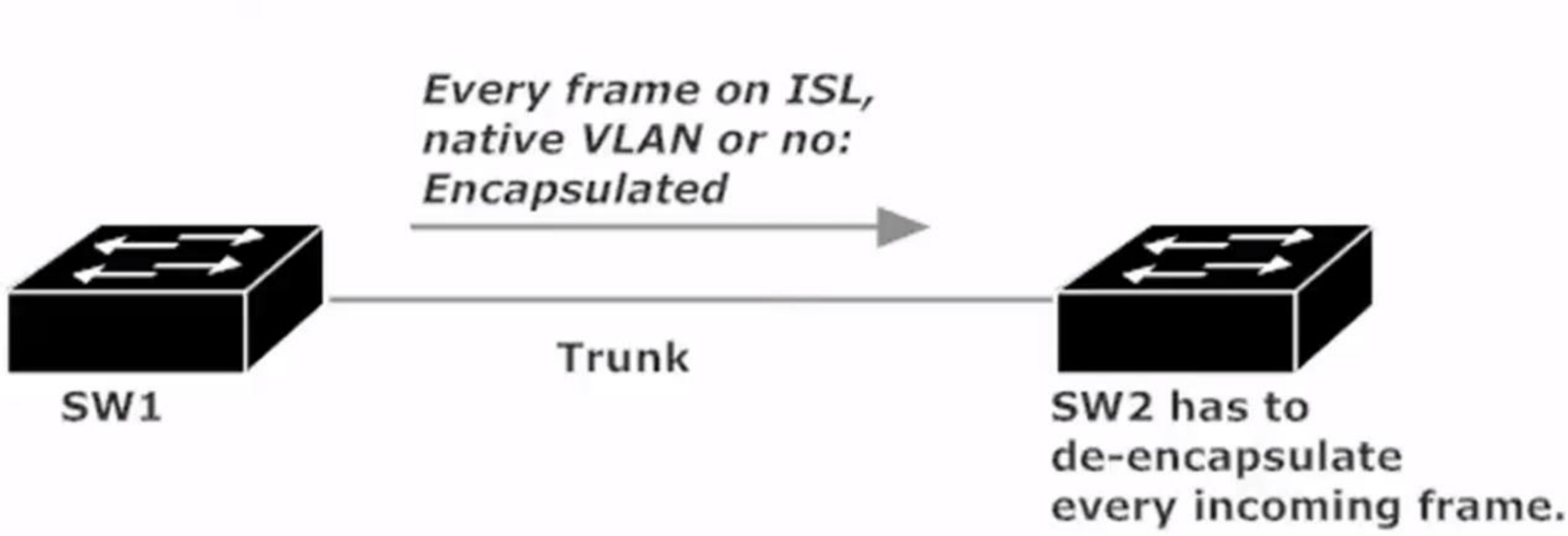
- Es el estándar de la industria para el protocolo de trunking, puede ser usado por equipos Cisco y No-Cisco.
- No encapsula la trama
- Inserta un valor de 4 bytes en el Ethernet header indicando el VLAN ID.
- Reconoce el concepto native VLAN.

¿Qué es native VLAN?

- La native VLAN es simplemente la VLAN default, y está VLAN la conocemos como VLAN 1 por defecto en los switches Cisco.

Dot1q reconoce la native VLAN, y no coloca el valor de 4 bytes en el header de Ethernet si la trama tiene como destino la native VLAN. Cuando un switch remoto recibe una trama sin tag (untagged frame), sabe que la trama tiene como destino la native VLAN, y esta trama se envía a todos los puertos pertenecientes a dicha VLAN.

En el caso de ISL, no conoce a la native VLAN y no le importa, solo encapsula cada una de las tramas antes de enviarlas a través del trunk, native VLAN o no.


Every frame on ISL,
native VLAN or no:
Encapsulated
Trunk
SW1
SW2 has to
de-encapsulate
every incoming frame.

Access Ports (puertos en modo acceso)

- Un puerto de un switch Cisco tiene que ser un puerto de acceso (access port) o un puerto trunk (trunk port), pero no puede ser ambos.

- Los access ports pertenecen a una, y solo una VLAN. Se puede ver la pertenencia (VLAN membership) para todos los puertos en modo acceso con los comandos “show vlan” y “show vlan brief”.

Trunk ports

- Los puertos Trunk pertenecen a todas las VLANs.
- Se puede verificar que puertos del switch están en modo Trunk con el comando “show interface trunk”.
- Los puertos trunk no aparecen al correr los comandos “show vlan” y “show vlan brief”.

Port modes

- Existen tres modos en los que una interfaz (puerto) de un switch puede ser configurada:

1. Access: convierte el puerto a modo acceso, el cual pertenecerá a una y solo una VLAN. Esta opción apaga el trunking en dicho puerto
2. Trunk: esta opción habilita el trunking en el puerto.
3. Dynamic: permite que el puerto haga la negociación del trunking dinámicamente. Ref: http://www.omnisecu.com/cisco-certified-network-associate-ccna/difference-between-dtp-dynamic-desirable-and-dynamic-auto-modes.php

Port modes

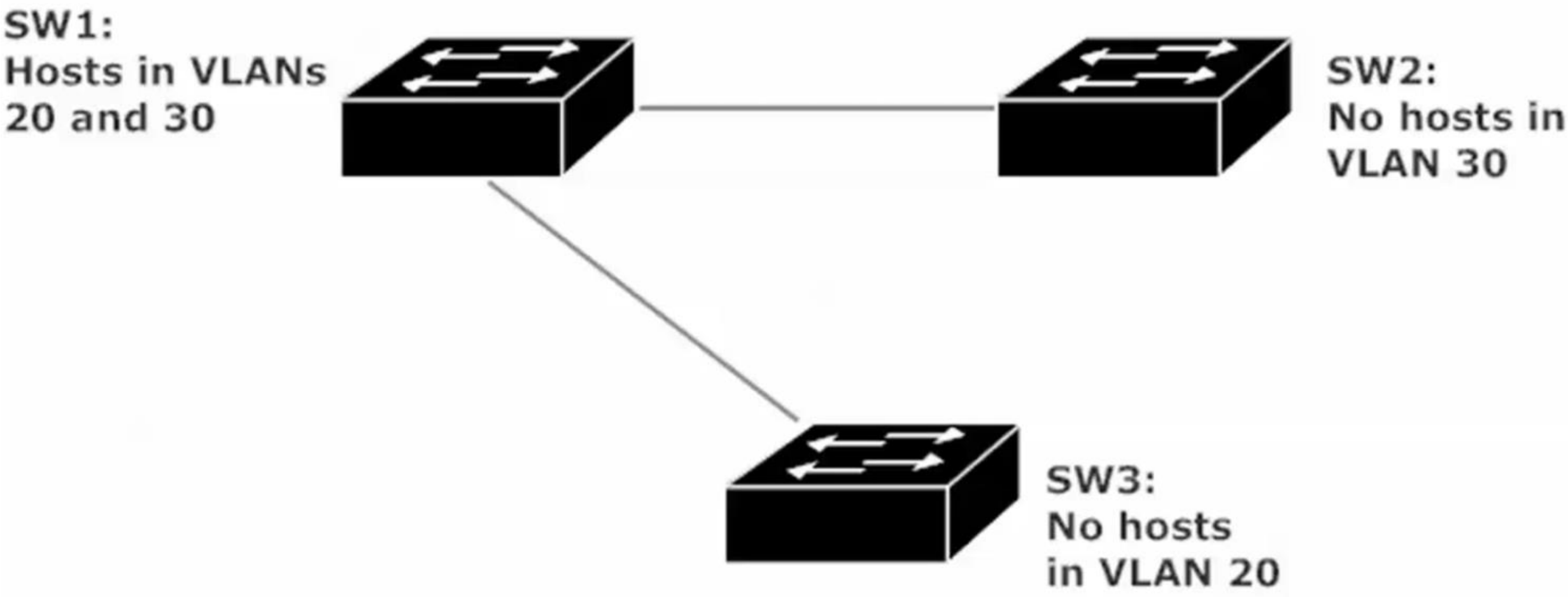
```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int fast 0/2
SW1(config-if)#switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate access or trunk mode
  trunk    Set trunking mode to TRUNK unconditionally

SW1(config-if)#switchport mode dynamic ?
  auto       Set trunking mode dynamic negotiation parameter to AUTO
  desirable  Set trunking mode dynamic negotiation parameter to DESIRABLE
```

Dynamic Trunking Protocol (DTP)

- Es un protocolo de trunking propietario de Cisco utilizado para negociar trunking en un enlace entre dos switches Cisco.
- También puede ser utilizado para negociar el tipo de encapsulamiento entre 802.1q o Cisco ISL (Inter-Switch Link)
- Si el puerto se coloca como “switchport nonegotiate”, se establecerá el trunk en el puerto pero las tramas del DTP no se enviarán a través de dicho trunk.

Filtrado de tráfico por VLAN

- Los puertos trunk son miembros de cada VLAN existente en el switch.
- En ocasiones, esta pertenencia universal de VLAN resulta en un envío de tráfico innecesario, lo que resulta en trabajo extra de nuestros switches y gasto de ancho de banda.

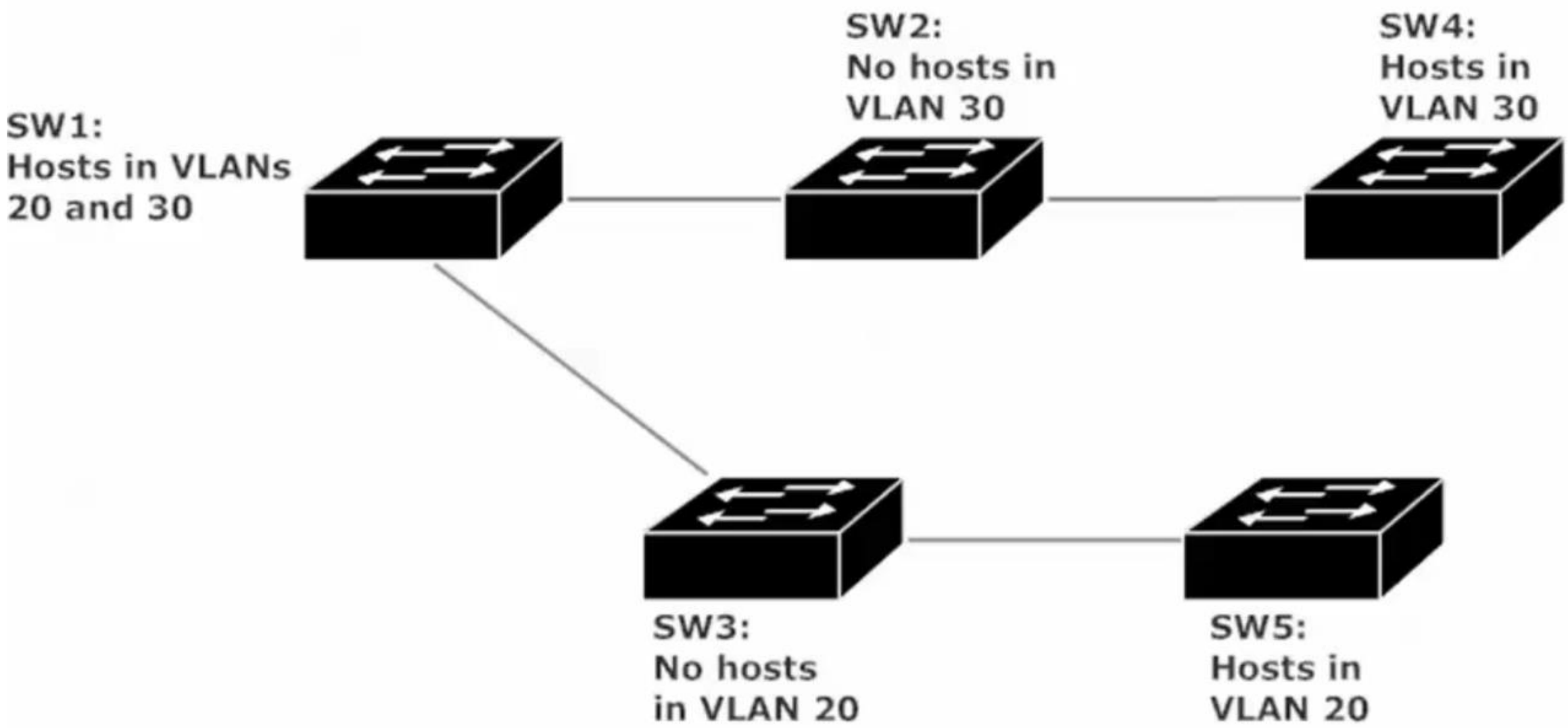

SW1:
Hosts in VLANs
20 and 30
SW2:
No hosts in
VLAN 30
SW3:
No hosts
in VLAN 20

- SW2 no tiene hosts en VLAN 30, por lo que no hay razón para que SW1 envíe tráfico de la VLAN 30 hacia SW2.

- SW3 no tiene hosts en VLAN 20, por lo que no hay razón para que SW1 envíe tráfico de la VLAN 20 hacia SW3.

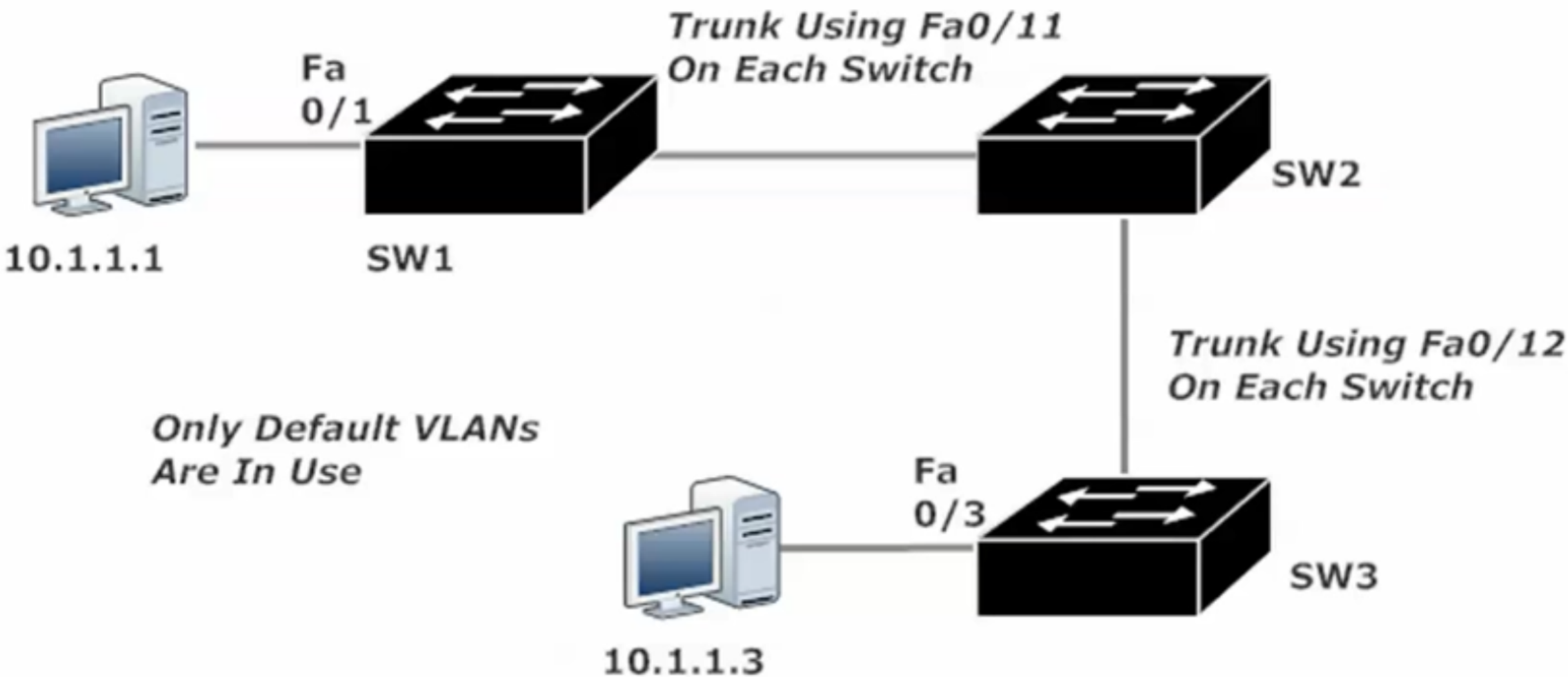
- Podemos denegar al tráfico la habilidad de cruzar el trunk por medio de filtrado de VLAN utilizando la instrucción “switchport trunk allowed vlan”.

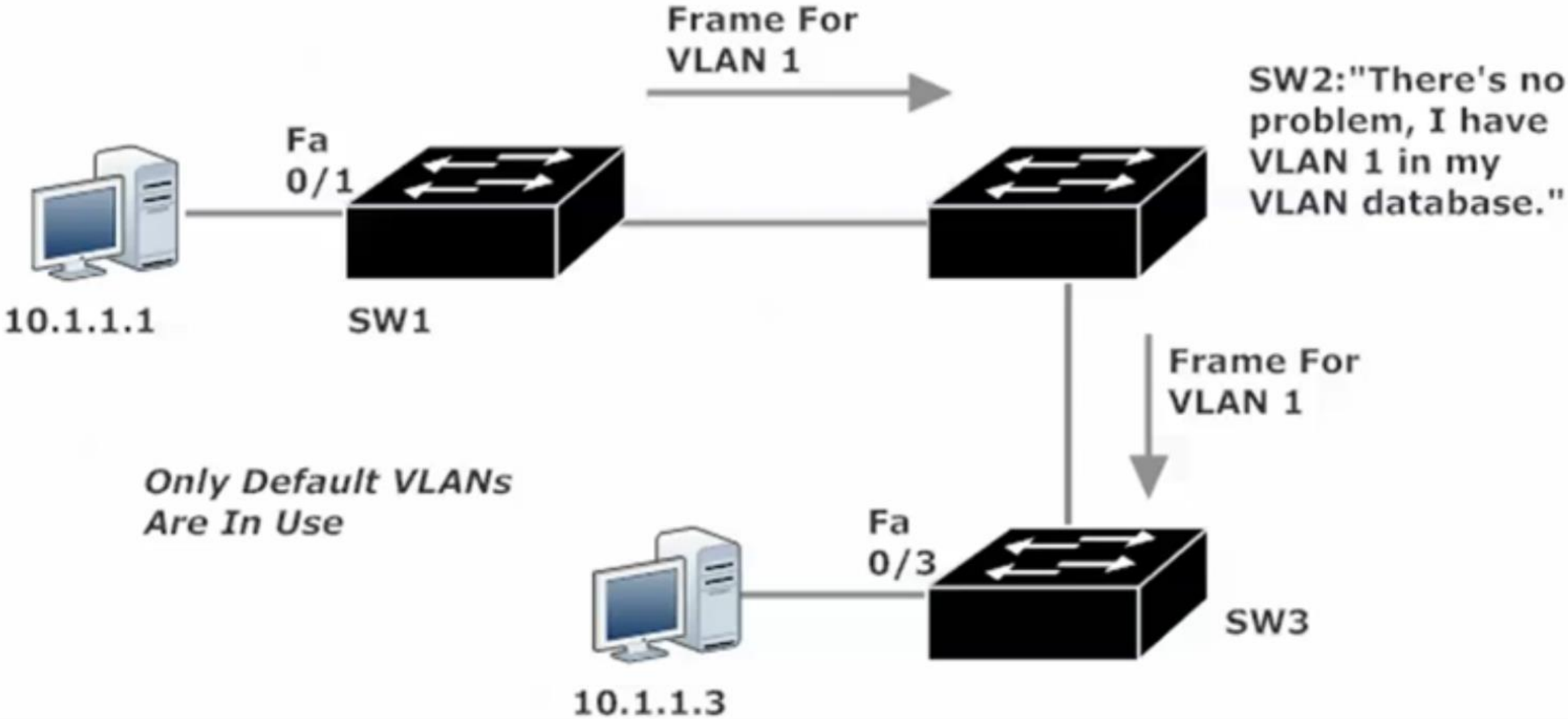
```
SW1(config-if)#switchport trunk allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list
```


SW1:
Hosts in VLANs
20 and 30
SW2:
No hosts in
VLAN 30
SW4:
Hosts in
VLAN 30
SW3:
No hosts
in VLAN 20
SW5:
Hosts in
VLAN 20

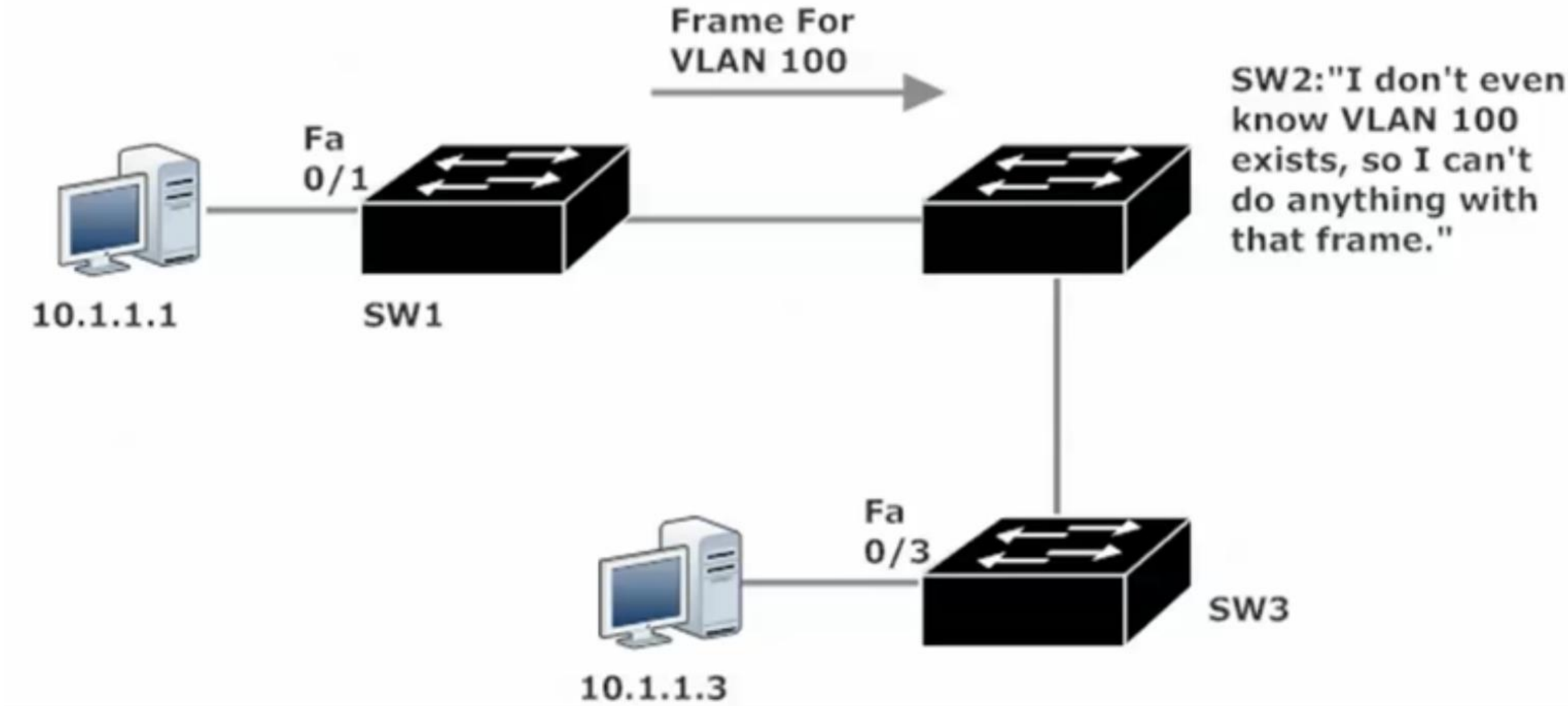
The VLAN Trunking Protocol (VTP)

- Generalmente deseamos que todos los switches de nuestra red conozcan todas las VLANs existentes en dicha red, incluso cuando no exista ningún puerto asociado de un switch el alguna de dichas VLANs.


Trunk Using Fa0/11
On Each Switch
Fa
0/1
SW2
10.1.1.1
SW1
Trunk Using Fa0/12
On Each Switch
Only Default VLANs
Are In Use
Fa
0/3
SW3
10.1.1.3


Frame For
VLAN 1
SW2:"There's no
problem, I have
VLAN 1 in my
VLAN database."
Fa
0/1
10.1.1.1
SW1
Frame For
VLAN 1
Only Default VLANs
Are In Use
Fa
0/3
SW3
10.1.1.3

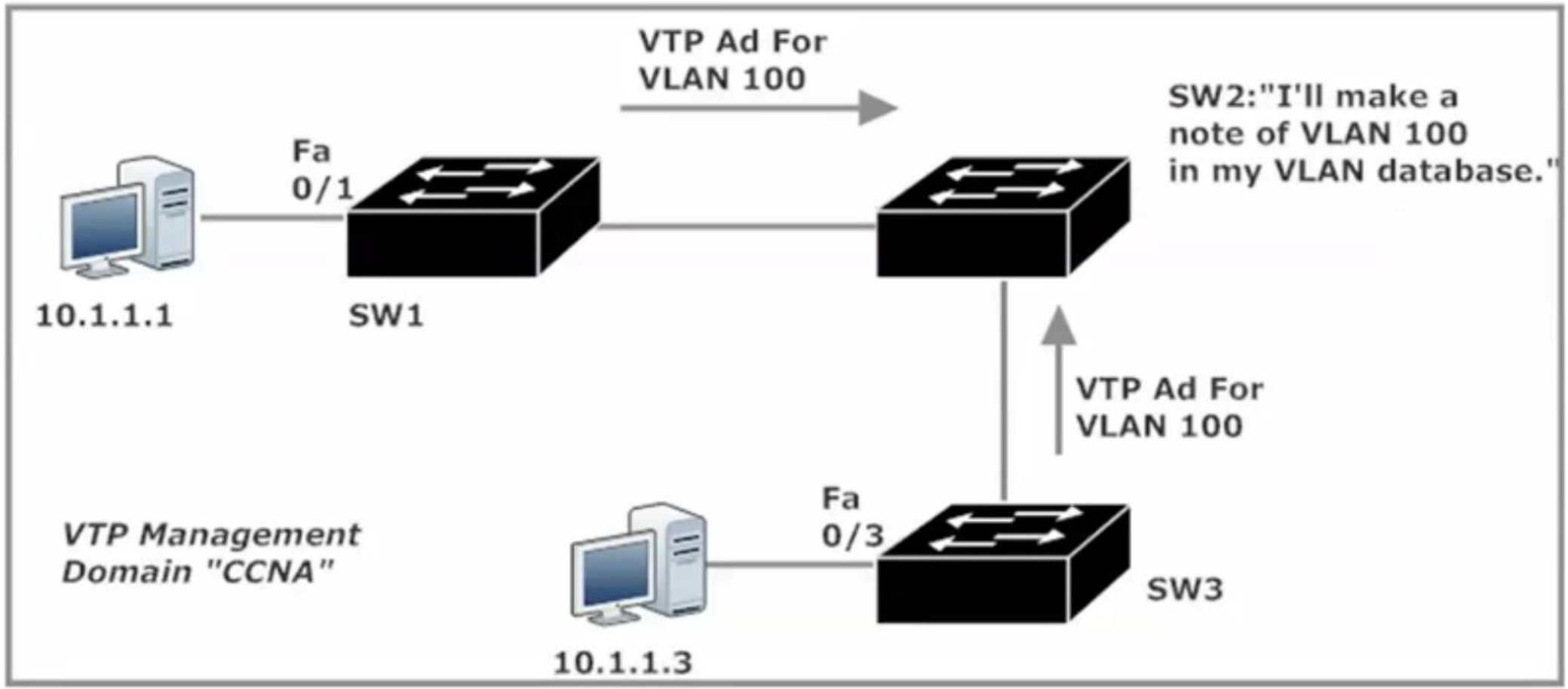
- Cambiamos la Interfaz Fa0/11 del SW1 a VLAN 100


Frame For
VLAN 100
SW2:"I don't even know VLAN 100 exists, so I can't do anything with that frame."
Fa
0/1
10.1.1.1
SW1
Fa
0/3
SW3
10.1.1.3

Posibles soluciones

- Crear manualmente la VLAN 100 en SW2
- ¿Qué pasaría si tuviéramos que editar 300 switches?

- Cuando colocamos los tres switches anteriores en el mismo dominio de VTP management (generalmente conocido como VTP domain), ellos intercambiaran información sobre las VLANs que ellos conocen y los tres tendrán una vista sincronizada de las VLANs de la red.
- Nuestros hosts en VLAN 100 pueden comunicarse entonces sin crear manualmente las VLAN necesarias en el SW2.

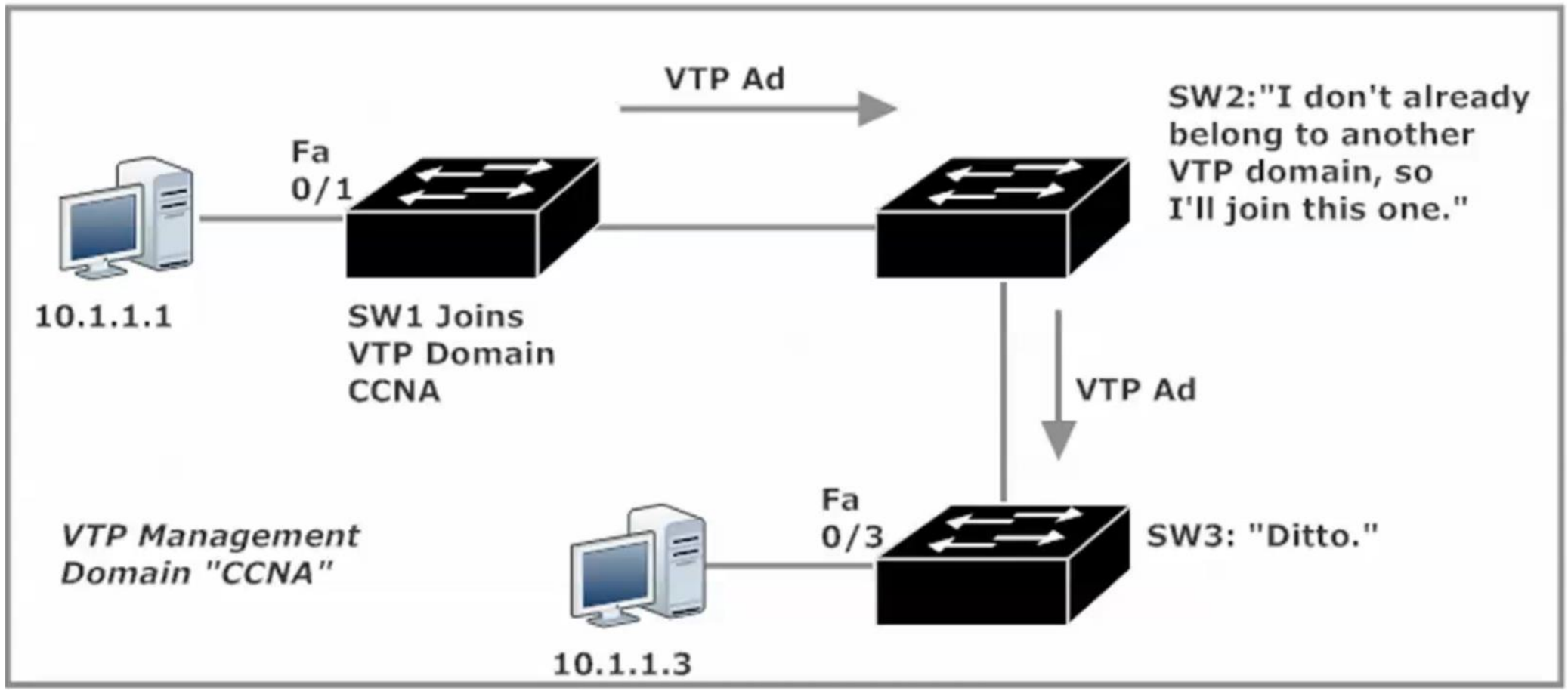

VTP Ad For
VLAN 100
SW2:"I'll make a
note of VLAN 100
in my VLAN database."
Fa
0/1
10.1.1.1
SW1
VTP Ad For
VLAN 100
Fa
0/3
SW3
VTP Management
Domain "CCNA"
10.1.1.3

Como crear un VTP Domain

- SW1(config)#vtp domain CCNA

Para revisar los settings del VTP Domain:

- SW1#show vtp status


VTP Ad
SW2:"I don't already belong to another VTP domain, so I'll join this one."
Fa 0/1
10.1.1.1
SW1 Joins VTP Domain CCNA
VTP Ad
Fa 0/3
SW3: "Ditto."
VTP Management Domain "CCNA"
10.1.1.3

The VTP Modes

- Server
- Client
- Transparent
- Off

VTP Server Mode

- Un switch puede crear, eliminar y modificar VLANs. Por “modificar” entenderemos “hacer cualquier cosa en el modo de configuración de la base de datos de VLANs”.
- Agregar puertos a una VLAN puede realizarse en modo servidor, cliente y transparente.
- Es necesario tener al menos un switch de un dominio VTP en modo servidor, o no podremos crear nuevas VLANs o eliminar las existentes.

Cambiar el modo vtp

- SW3(config)#vtp mode <opción>

```
SW3(config)#vtp mode ?
  client       Set the device to client mode.
  off          Set the device to off mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
```

VTP Client Mode:

- Los switches que corren en VTP client mode no pueden crear, modificar o eliminar VLANs. Los clientes escuchan los VTP advertisements y actualizan sus bases de datos apropiadamente cuando estos avisos llegan.

VTP Transparent Mode

- Los switches en este modo no participan completamente en el VTP domain. Switches en modo VTP transparente no sincronizan sus bases de datos de VTP con los demás switches en el mismo dominio. Ellos ni siquiera anuncian su propia información de VLAN. VLANs creadas en un switch en modo transparente no serán anunciadas para otros switches que hablen VTP en el dominio, lo que las convierte en VLANs localmente significativas únicamente (locally significant only).

VTP Transparent Mode

- Cuando un switch en modo transparente recibe anuncios de VTP (VTP advertisements), los ignorará pero los renviará a sus otros Trunks.

VTP Mode Off

- Desabilita el VTP en el switch, y el switch no enviará VTP advertisements.