

A thick black L-shaped frame is positioned on the left and bottom edges of the slide, framing the central text.

# VIRTUAL LANS / VLANs

Configuración de puertos en modo Acceso y Trunk

# Índice

- Teoría de las VLANs
- Configuración de puertos en modo Acceso
- PRÁCTICA: Configuración de puertos en modo Acceso
- Configuración de puertos en modo Trunk
- PRÁCTICA: Configuración de puertos en modo Trunk

# TEORÍA DE LAS VLANS



# Introducción

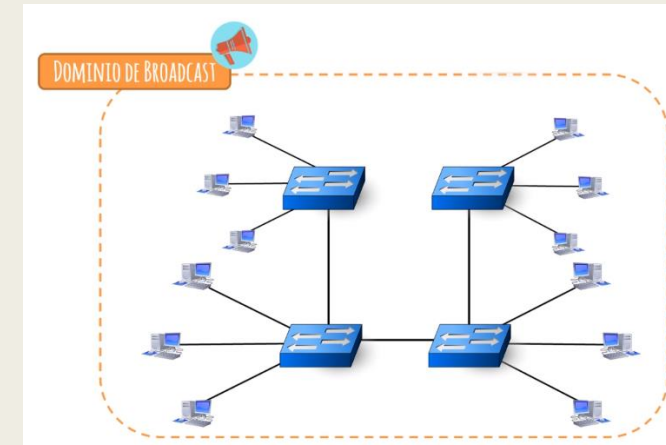
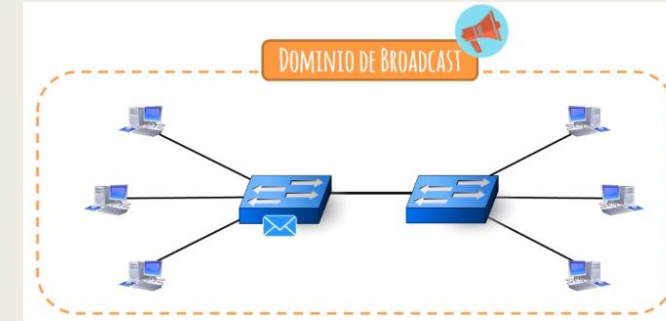
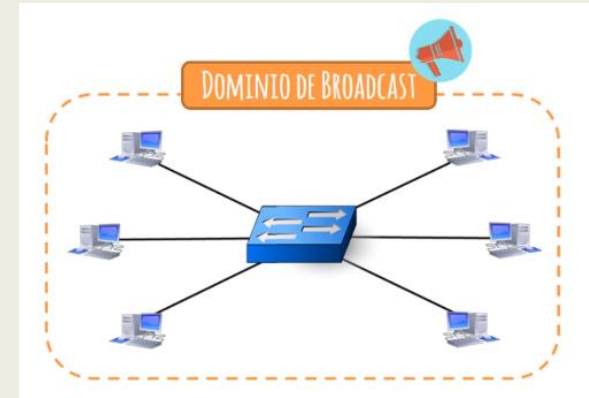
- En esta unidad vamos a tratar el tema de las Virtual LANs
- O lo que es lo mismo, VLANs
- Esta es una tecnología que aplica a equipos de capa 2 (Switch)



- Antes de comenzar con la teoría de las VLANs, necesitamos ver algo:
  - *El dominio de broadcast*

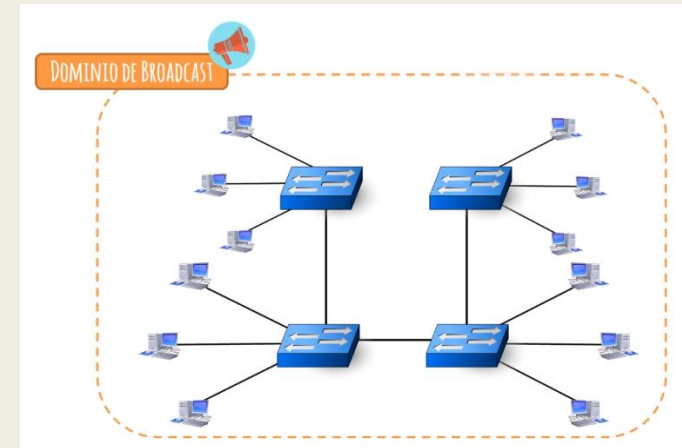
# Dominio de broadcast

- El **dominio de broadcast** hace referencia a todos los equipos que son susceptibles de recibir una trama de tipo broadcast cuando esta sea enviada.
- Si conectamos varios equipos a un switch (primera imagen), y uno de ellos envía una trama de broadcast, al llegar al switch, se reenviaría por todas las interfaces excepto por la que ha recibido la trama.
  - *El dominio de broadcast abarcaría todos los equipos de la red, incluido el que envió la trama.*
- Si conectamos otro switch y aumentamos la cantidad de equipos, seguimos teniendo un solo dominio de broadcast, pero es mayor.
- Si seguimos aumentando la red con más switches, continuamos teniendo un solo dominio de broadcast, pero es mucho mayor.



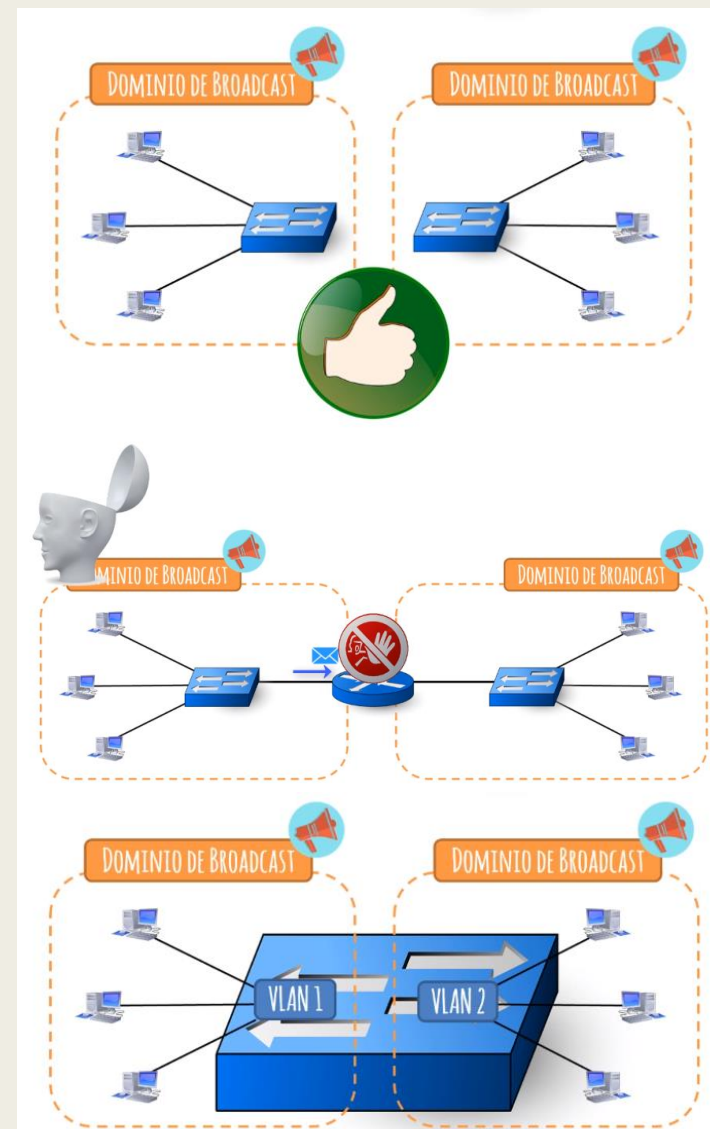
# Problemática de 1 solo dominio de broadcast

- Si contamos con un solo dominio de broadcast, pero tenemos una red muy grande, por ejemplo, de 500 equipos...
- Cada vez que un equipo haga una petición de tipo broadcast (como ARP, que es muy común), le llegaría a los 499 equipos, donde 498 no van a responder y no les interesa ese tráfico.
- Cuanto más grande sea el dominio de broadcast, más tráfico se va a generar, y menos eficiente será la red.
- ¿Qué solución puede haber a esta problemática?

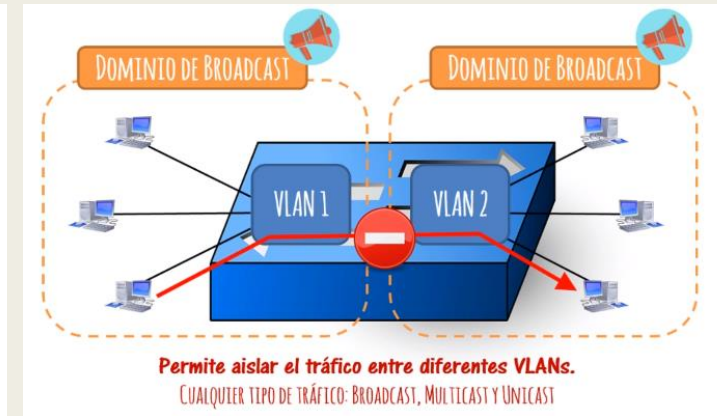
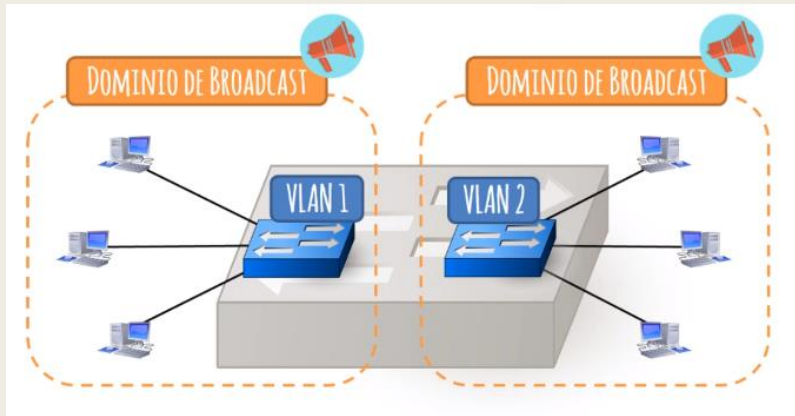
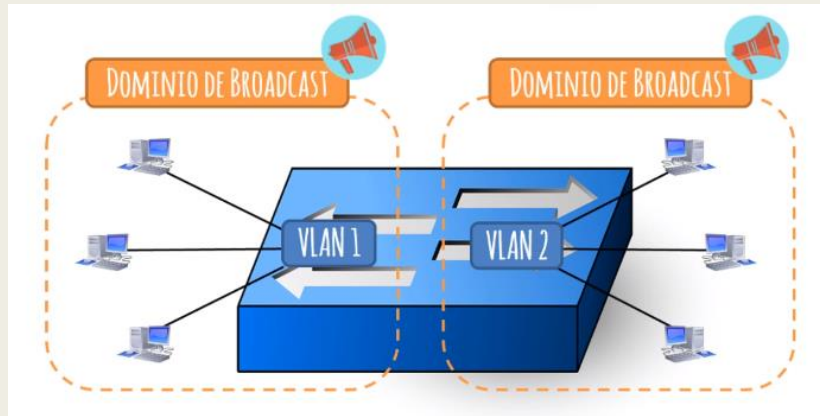


# Segmentar dominios de broadcast

- Si segmentamos los dominios de broadcast (pasar de uno a varios), mejoraríamos el rendimiento de la red.
- Podemos llegar a la norma de a más dominios de broadcast, será mejor para la red, porque:
  - *Al ser más pequeños, habrá menos tráfico innecesario.*
  - *Y por lo tanto el rendimiento será mayor.*
- Una forma de segmentar los dominios que vemos en la imagen es utilizar switches de forma exclusiva para cada dominio y sin que estos estén conectados entre sí.
- También podemos colocar routers en medio de los switches, ya que los routers sí segmentan los dominios de colisión, a diferencia de los switches.
- Y también podemos usar VLANs para segmentar la red



# ¿En qué consisten las VLANs?



- Con las VLAN podemos definir con un único switch, diferentes LAN virtuales (virtual LANs)
- Teniendo varias VLAN, asociamos los puertos del switch a una VLAN u otra en función de nuestras necesidades.
- Por ejemplo, en la imagen de ejemplo, los equipos conectados a los puertos de la izquierda del Switch están conectados a la VLAN 1, y los de la derecha a la VLAN 2.
  - Aunque todos ellos están conectados al mismo switch, están aislados unos de otros (están segmentados) y no es posible comunicar un PC de VLAN1 con uno de VLAN2.
  - A nivel operativo es como si tuviéramos dos switches no conectados entre sí.



# ¿Por qué se utilizan VLANs?

- Coste. Evita comprar nuevos switches y routers para aislar el tráfico.
  - *El escenario de la imagen de la derecha, sin VLAN, sería equivalente a utilizar 2 Switches y 1 Router.*
  - *A medida que se escala la red, el coste que nos ahorramos es cada vez mayor.*
- Para limitar el número de equipos que reciben los Broadcast.
- Para limitar el número de equipos que reciben Flooding.
  - *Reduce el uso de la CPU de los equipos.*
    - Equipos de red.
    - Equipos finales.
- Incrementamos la seguridad dado que cada VLAN está aislada
- Permiten agrupar los equipos de forma lógica y no física. →

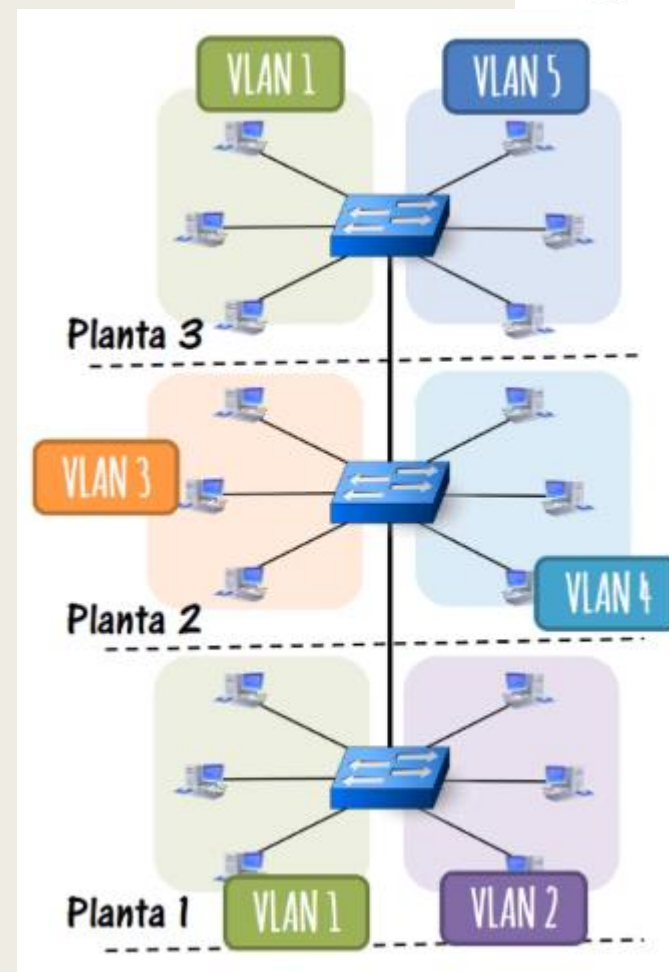


De forma lógica implica que podamos agrupar los equipos sin importar dónde están ubicados físicamente

# Agrupación de forma lógica y no física



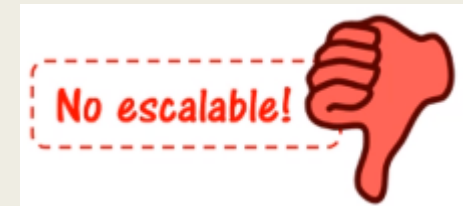
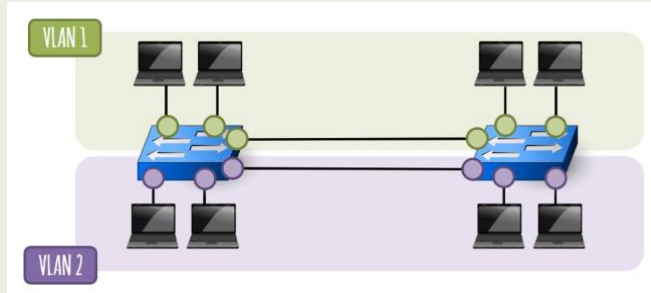
- Supongamos que tenemos un edificio de 3 plantas.
- En cada planta tenemos un switch, y cada switch segmenta la red en diferentes VLANs:
  - *Planta 1: VLAN1 y VLAN2*
  - *Planta 2: VLAN3 y VLAN4*
  - *Planta 3: VLAN1 y VLAN5*
- Vemos que la VLAN1 está tanto en la planta 1 como en la planta 3.
- Cuando esto sucede se suele hablar de VLAN extendida (a lo largo de la red, es decir, a lo largo de varios switches).
- ¿Cómo es esto posible si ni siquiera es el mismo switch? ¿Cómo se puede lograr? **De dos formas** (siguiente diapositiva)



# Compartir VLAN entre Switches. Método 1

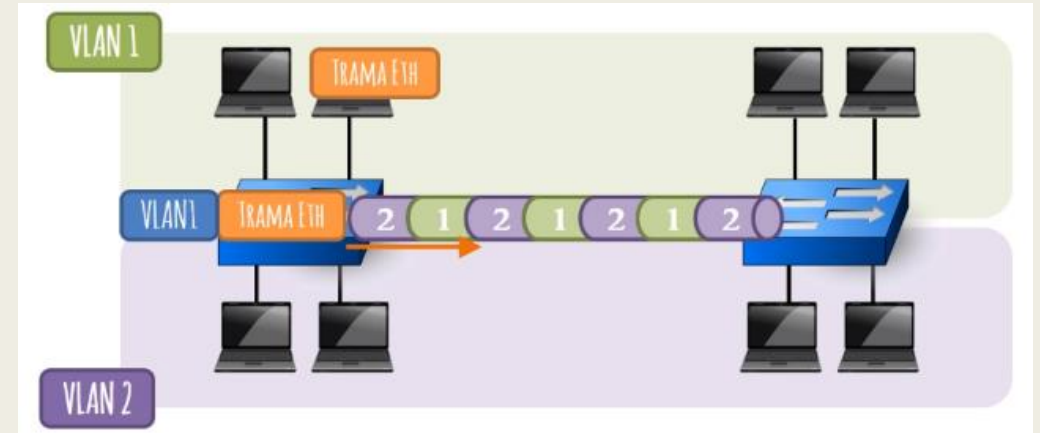
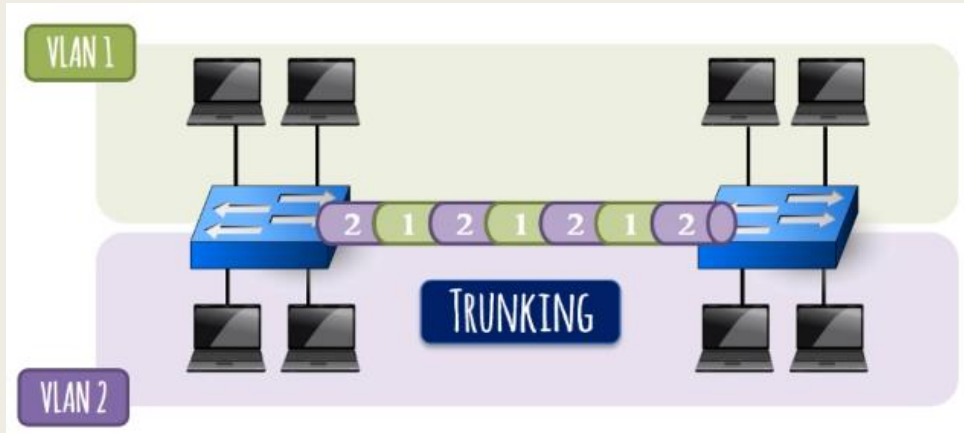
*Creamos un enlace entre switches por cada VLAN que queramos extender.*

- Una forma de realizar esta comunicación de VLAN entre varios switches sería la siguiente:



- Lo que vemos en la imagen es que se utiliza un puerto exclusivo para comunicar un switch con otro para esa VLAN.
  - *Es decir, para comunicar la VLAN1 del SW1 con la VLAN1 en el SW2, se conecta un cable conectado en los puertos de VLAN1 de ambos.*
- Esta opción es posible, pero a nivel de diseño no es buena, porque no es escalable.
  - *Si tenemos 2 VLAN, desperdiciamos dos puertos de cada switch para comunicar las VLAN, si tuviéramos 10 VLAN, desperdiciaríamos 10 puertos.*
- Además añade complejidad a la red y requiere de mayor inversión de dinero (más cable)

# Compartir VLAN entre Switches. Método 2



- La forma adecuada de realizar la comunicación entre VLANs que se encuentran entre varios switches es mediante **enlaces de tipo TRUNK**

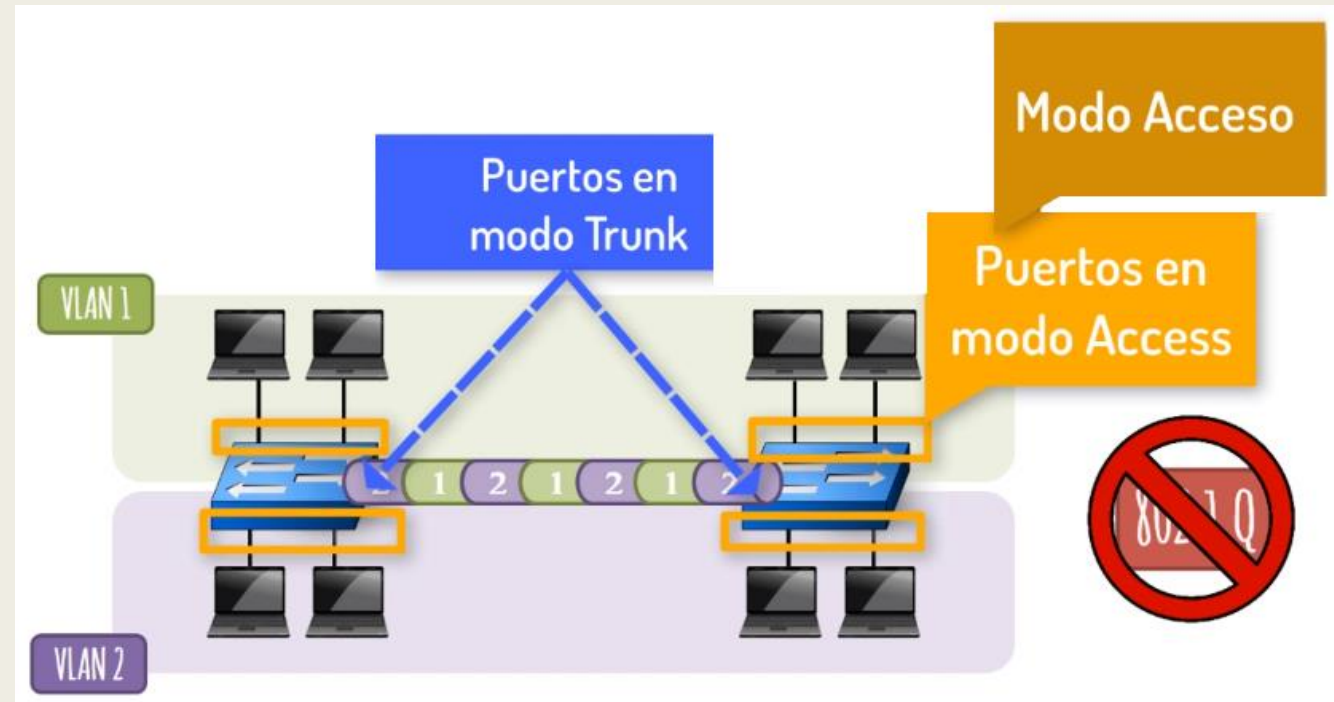
*Creamos un único enlace entre switches que transporte todas las VLANs que queramos*

*Añadimos una pequeña cabecera en la trama Ethernet para diferenciar las tramas de cada VLAN*

- Todas las VLAN compartirán un único enlace para la comunicación con diferentes switches.
- El protocolo que define el trunking es el 802.1 Q (o dot1Q).
- En español, el trunking suele llamarse **enlace troncal**.

# ¿Cómo configuraremos el trunking?

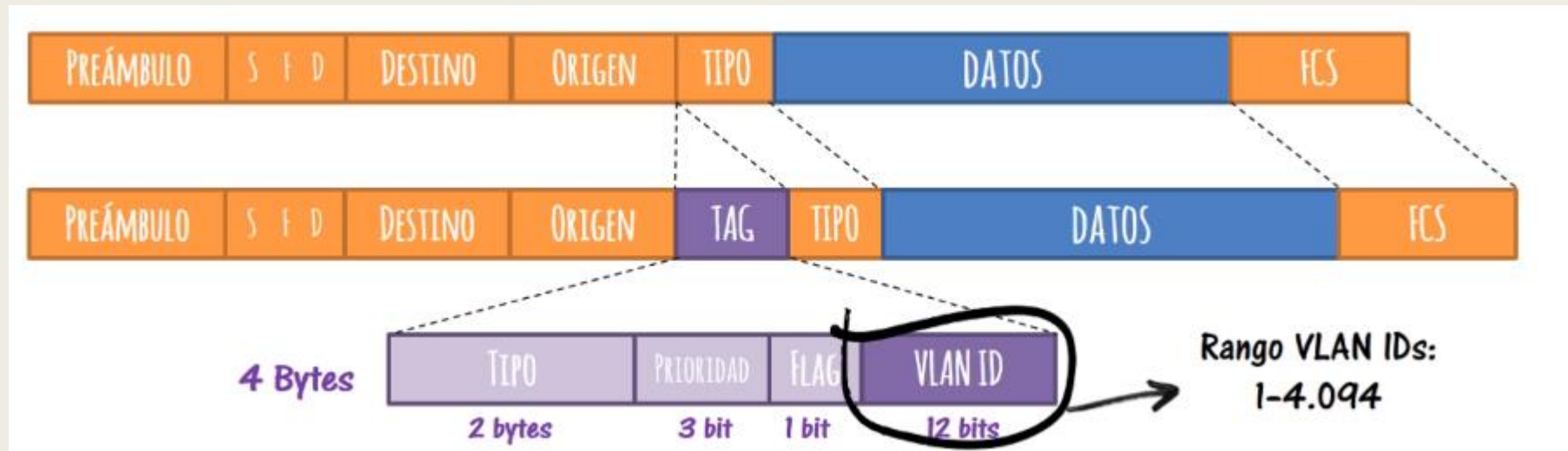
- A grandes rasgos, el puerto por el que circularán tramas de varias VLAN se configurará en modo TRUNK.
  - *Trabajan con 802.1 Q*
    - Porque necesitamos usar alguna cabecera para identificar la VLAN a la que pertenece la trama.
- Y los puertos por los que no circulan varias VLAN (normalmente los puertos que conectan con equipos), se configurarán en modo ACCESS (modo Acceso).
  - *No trabajan con 802.1 Q*



Puede darse algún caso en que un equipo final como un servidor sí tenga configurado un modo Trunk

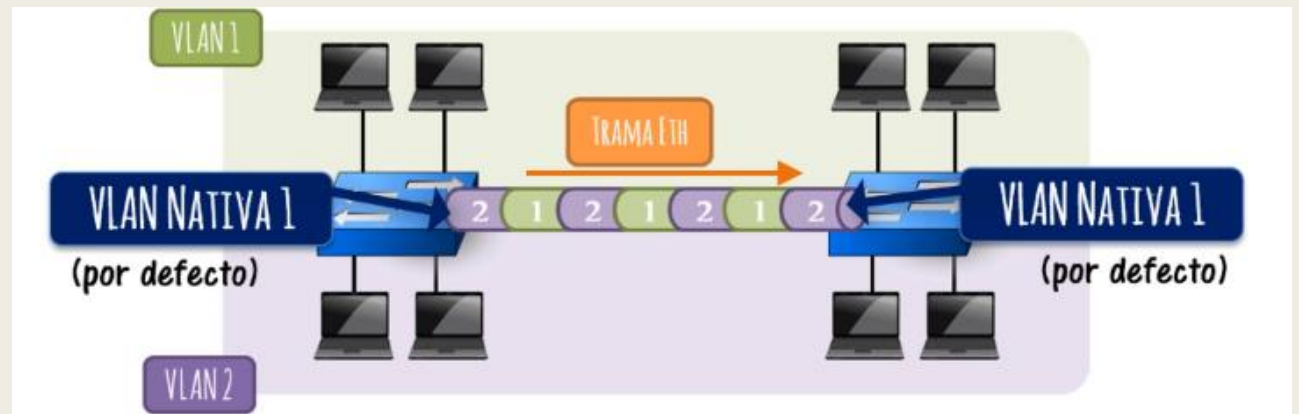
# ¿Cómo es la cabecera con 802.1 Q?

- En la cabecera de la trama Ethernet, se añade un campo TAG de 4 Bytes, donde dentro tendremos varios campos, donde el más importante es **VLAN ID**
  - *VLAN ID nos permitirá identificar a qué VLAN pertenece una trama*





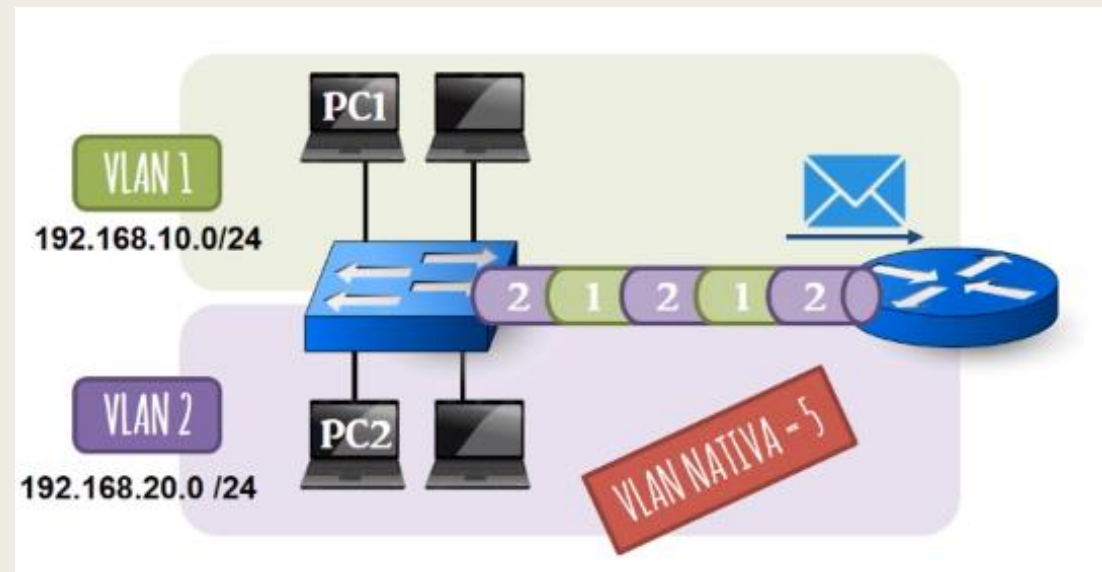
# VLAN Nativa



- Los enlaces troncales tendrán por defecto definida una VLAN Nativa.
- La VLAN nativa es la VLAN por defecto, por ejemplo, la 1. (y de serie, por defecto es la 1)
- ¿Qué implica esto?
  - *Que todo el tráfico que viaje por la VLAN nativa, no tendrá que añadir cabecera del protocolo 802.1Q*
  - *Es decir, el switch automáticamente determinará que cuando le llegue una trama por el enlace trunk y vea que no tiene cabecera del 802.1Q, será la VLAN Nativa (por defecto).*
- La VLAN Nativa debe configurarse la misma en ambos puertos extremos.
  - *¡Ojo! Si configuramos VLAN Nativas en cada extremo habrá cruces de tráfico = problemas → **Native VLAN Mismatch***
- **¡Ojo!** La VLAN Nativa se configura en cada puerto trunk, no es un valor global del switch.

# ¿Es posible la comunicación entre 2 VLAN?

- La comunicación directa NO ES POSIBLE.
  - *Esa es la función de las VLAN*
- Pero es posible comunicarlas mediante Routing.
- ¿A nivel 3 las VLAN tienen que formar parte de redes distintas?
  - *Sí, a nivel de diseño es importante asignar redes distintas a cada VLAN.*
- Si dos VLAN comparten el mismo direccionamiento, no sería correcto a nivel de diseño y podría ocasionar problemas.

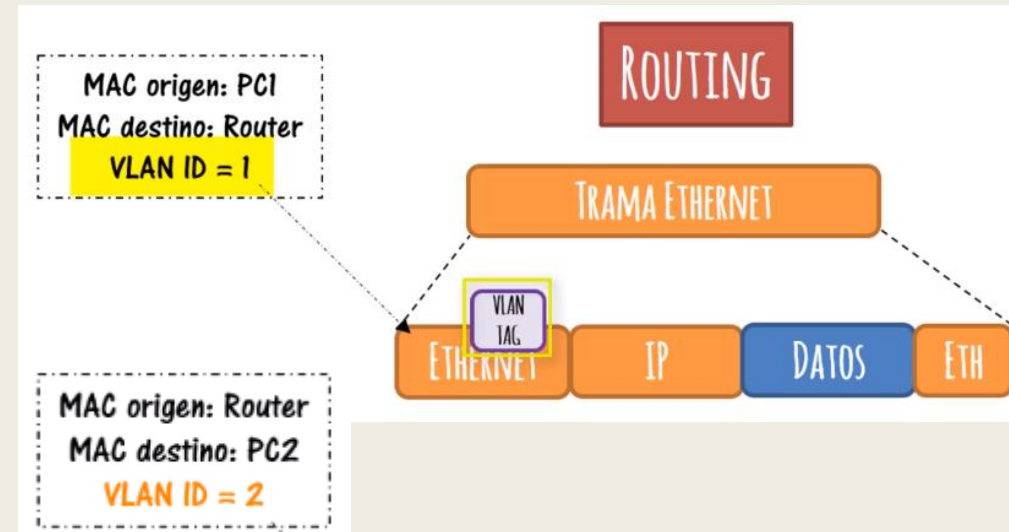
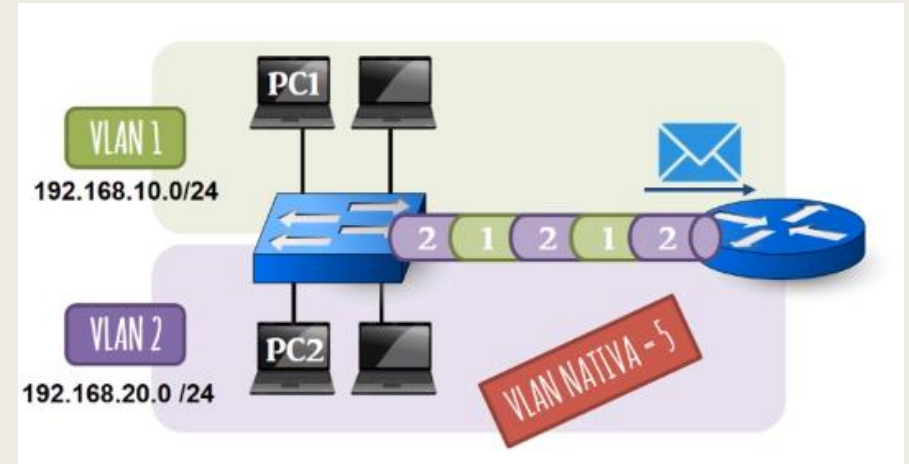


Los routers también soportan el trunking

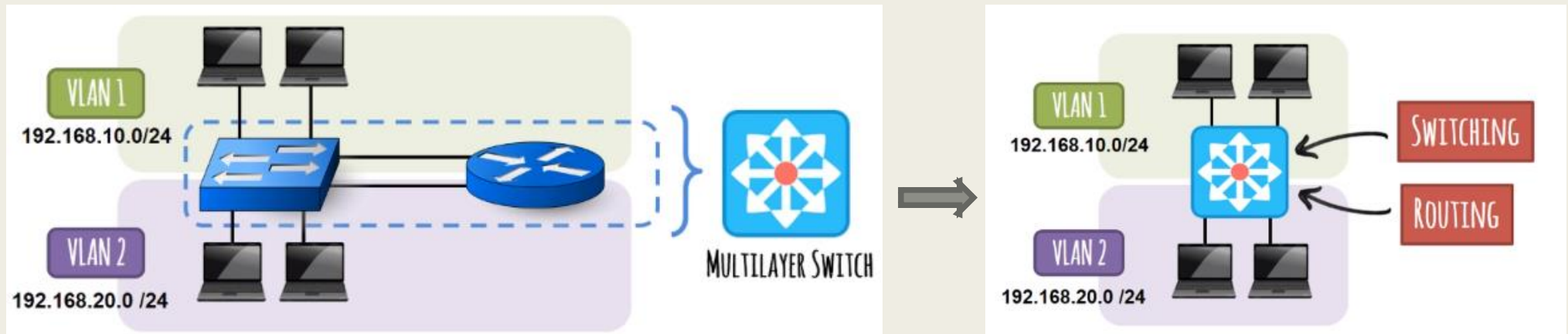


# Ejemplo de comunicación entre 2 VLAN diferentes

- Supongamos que el PC1 envía algo al PC2.
- El router, al recibir la trama del PC1 por el puerto en modo trunk, la analizará y comprobará que el TAG proviene de la VLAN 1.
- Posteriormente, para hacer el forwarding hacia el PC2, a nivel de capa 2, cambiará la trama indicando en el TAG que es para la VLAN 2.



# Switch Multicapa (Multilayer Switch)

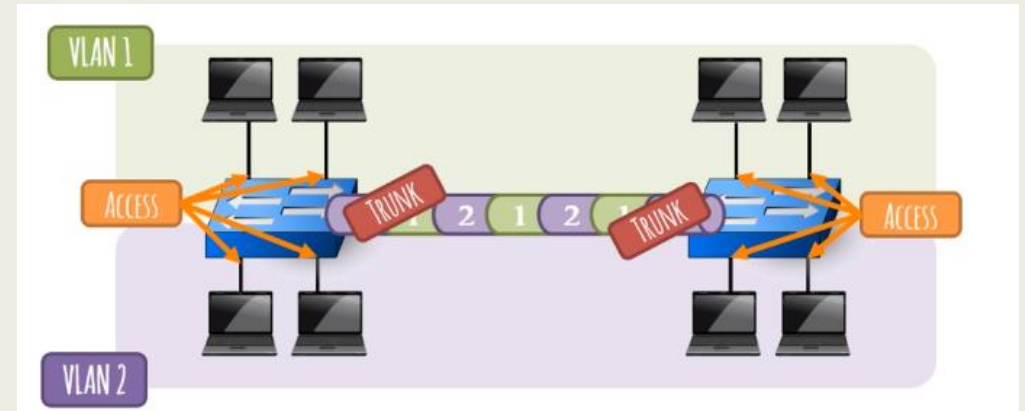


- Siguiendo con la dinámica de ahorrar equipos, existe un equipo de red llamado:
  - *Multilayer Switch o Switch Multicapa.*
- Este equipo realiza funciones de Switchin y funciones de Routing.
- Con lo que un mismo equipo permitiría segmentar las VLAN, e intercomunicarlas.
- Se trata de un equipo de capa 3, y la diferencia principal es que tiene muchos más puertos.
- Es capaz de realizar switching únicamente cuando no hay que enrutar, en cambio un router se realiza a hacer routing únicamente.

# CONFIGURACIÓN DE PUERTOS EN MODO ACCESO



# Recapitulando



- Hasta ahora hemos visto que las VLAN sirven para aislar el tráfico dentro de un mismo SWITCH.
- De modo que configurando varias VLAN conseguimos aislar la comunicación entre los equipos que no pertenecen a la misma VLAN.
- Para hacer esto, hemos visto que podemos configurar los puertos:
  - *En modo ACCESO. Enfocado principalmente a los equipos finales.*
  - *En modo TRUNK. Enfocado para unir dispositivos de red, como 2 switches, o 1 switch con 1 router.*
    - Y en estos enlaces troncales puede viajar tráfico de diferentes VLAN a la vez, sin tener que dedicar un enlace exclusivo para cada VLAN.
- Ahora vamos a ver cómo configurar esto en equipos reales. Empezaremos con la configuración de puertos en modo Acceso, y cómo crear las VLANs.

# Configuración Puertos ACCESS

- Para configurar los puertos en modo ACCESO necesitaremos seguir 3 pasos:
  1. Creación la VLAN a nivel global (crearla en el Switch)
  2. Definir el modo del puerto (opcional)
    - *En este caso será el modo Access o acceso*
  3. Asignar la VLAN al puerto que acabamos de configurar en modo Access

# Paso 1. Crear la VLAN a nivel global

- Para crear la VLAN, debemos acceder al modo de configuración global.
- Una vez dentro usaremos el comando:
  - `vlan número_de_vlan`
- Esto nos creará una VLAN, y automáticamente nos meterá dentro de su submodo de configuración.
  - *Opcionalmente, dentro de este modo podemos asignarle un nombre con el comando:*
    - `name nombre_vlan`
  - *Si no asignamos un nombre, por defecto se le asigna uno.*
- Podremos consultar las VLANs desde el modo privilegiado con el comando:
  - `show vlan`



```
Switch(config)#vlan 12
Switch(config-vlan)#exi
Switch(config)#exi
Switch#sh vlan
```

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
12	VLAN0012	active	Gig0/1, Gig0/2

Si tenemos una vlan de la oficina, podemos llamarla oficina, es mejor que simplemente VLAN0012

## Paso 2. Definir modo de puerto (opcional)

- Para definir el modo de acceso (o trunk) de un puerto, tendremos que acceder a su interfaz. Y dentro utilizar el comando `switchport mode access`

```
(CONFIG)# CONFIGURACIÓN GLOBAL  
interface FastEthernet 0/4  
(CONFIG-IF)# INTERFAZ  
switchport mode access
```

- Es opcional porque esto se podría configurar de modo automático mediante un protocolo DTP que veremos cómo funciona en esta presentación.
  - *DTP hará la negociación y establecerá el tipo de puerto según unos parámetros.*



Es muy recomendable configurar siempre las interfaces en modo “no-automático”.



+ SEGURIDAD



# Paso 3. Asignar VLAN a puerto

- Para asignar un puerto a una VLAN concreta, debemos acceder a dicha interfaz y usar el comando:
  - *switchport mode access* ← en caso de que no lo hayamos puesto ya
  - *switchport Access vlan numero\_de\_vlan*
- El resto de puertos estarán en la vlan por defecto

```
Switch(config)#interface FastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 12
Switch(config-if)#exi
Switch(config)#exi
Switch#sh vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, 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
12	VLAN0012	active	Fa0/4

(CONFIG)# CONFIGURACIÓN GLOBAL

interface FastEthernet 0/4

(CONFIG-IF)# INTERFAZ

switchport mode access

switchport access vlan numero\_de\_vlan

¡Ojo! La VLAN por defecto es diferente de la VLAN nativa.

VLAN nativa: Aquella que se define en un enlace troncal para la cual las tramas no serán etiquetadas, y en ese caso usará la VLAN por defecto del switch.

La VLAN por defecto será la que tengan asignados los puertos sin VLAN configurada.



# Modo rápido para configurar VLAN

- Existe la posibilidad de configurar de forma más rápida la VLAN, con solo un paso:
  - *Asignar la VLAN a un puerto*

```
(CONFIG)# CONFIGURACIÓN GLOBAL
interface FastEthernet 0/5
  (CONFIG-If)# INTERFAZ
  switchport access vlan numero_de_vlan
```

- *Esto nos crea la VLAN de forma automática*

```
Switch(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
```

# Comparativa de creación de modo rápido vs modo normal

- Si configuramos la VLAN de forma rápida, el modo administrativo es dynamic auto.
  - *Con dynamic auto se negociará qué modo utilizar, y ese resultado determinará si el puerto está en modo ACCESS o modo TRUNK*
- Si configuramos la VLAN de la forma “normal”, el modo administrativo es static
  - *Con static Access el modo siempre será ACCESS y no cambiará*

```
Switch#sh int fa 0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
```

(CONFIG)# CONFIGURACIÓN GLOBAL

interface FastEthernet 0/5

(CONFIG-IF)# INTERFAZ

switchport access vlan numero\_de\_vlan

MODULO RÁPIDO !!

```
Switch#sh int fa 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```

(CONFIG)# CONFIGURACIÓN GLOBAL

interface FastEthernet 0/4

(CONFIG-IF)# INTERFAZ

switchport mode access

switchport access vlan numero\_de\_vlan

En este ejemplo, en este modo, ambos están funcionando como static access.

Modo administrativo:  
Cómo se ha configurado.

Modo operacional:  
Cómo funciona finalmente.

# ¿Es posible configurar un conjunto de interfaces a la vez?

- Es posible, con el comando: **interface range**

- Ejemplo:

```
(CONFIG)# CONFIGURACIÓN GLOBAL  
interface range FastEthernet 0/1 - 6
```

```
{  
FastEthernet 0/1  
FastEthernet 0/2  
FastEthernet 0/3  
FastEthernet 0/4  
FastEthernet 0/5  
FastEthernet 0/6  
}
```

- Cuando escribimos el comando, veremos que el prompt tiene un -range:

```
(CONFIG-IF-RANGE)# RANGO-INTERFAZ  
description Puerto_de_acceso  
switchport mode access  
switchport access vlan 9
```

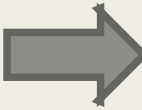
- Y los comandos que pongamos, se aplicarán a todas las interfaces.

# Ejemplo de configuración de varias interfaces

```
Switch#sh run
Building configuration...
```

```
Current configuration : 1203 bytes
```

```
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
```



```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL
Switch(config)#interface range fastethernet 0/1 - 6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 9
```

```
Switch#sh run
Building configuration...

Current configuration : 1731 bytes
!
interface FastEthernet0/1
description Puerto_de_acceso
switchport access vlan 9
switchport mode access
!
interface FastEthernet0/2
description Puerto_de_acceso
switchport access vlan 9
switchport mode access
!
interface FastEthernet0/3
description Puerto_de_acceso
switchport access vlan 9
switchport mode access
!
interface FastEthernet0/4
description Puerto_de_acceso
switchport access vlan 9
switchport mode access
!
interface FastEthernet0/5
description Puerto_de_acceso
switchport access vlan 9
switchport mode access
!
interface FastEthernet0/6
description Puerto_de_acceso
switchport access vlan 9
switchport mode access
!
```

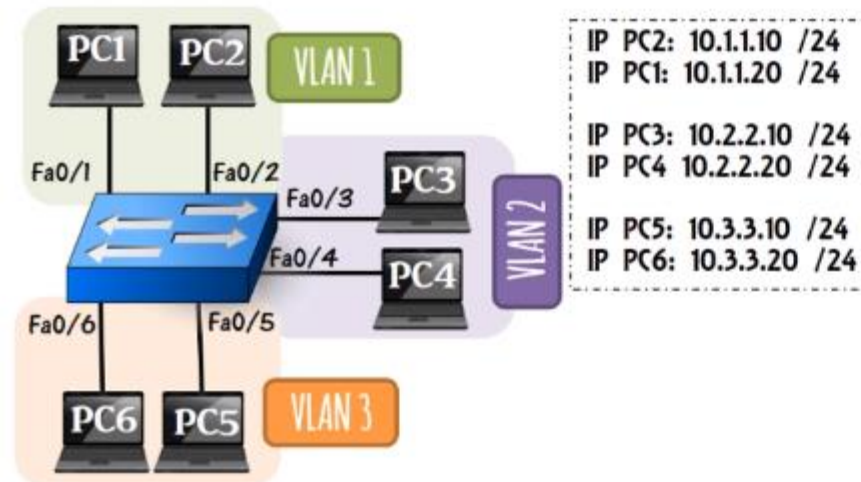
# PRÁCTICA: CONFIGURACIÓN DE PUERTOS EN MODO ACCESO





# Ejercicio Práctico

- Vamos a poner en práctica lo aprendido hasta ahora.
- En el aula virtual tenéis un archivo de packet tracer para poder trabajar.



Pasos

1. Verificar que Fa0/1 y Fa0/2 ya se encuentran en VLAN1 y operando en modo acceso.
2. Verificar la conectividad a nivel IP (ping) entre PC1 y PC2 .
3. Generar Broadcast y ver que sucede (ping 10.1.1.255 desde el PC1 en modo Simulación)
4. Configurar los puertos Fa0/3 y Fa0/4 en la VLAN2 en modo acceso utilizando "interface range ...".
5. Probar la conectividad a nivel IP (ping) entre PC3 y PC4. Mirar en que VLAN y modo se encuentran.
6. Configurar los puertos Fa0/5 y Fa0/6 en la VLAN3 (modo de configuración rápido).
7. Verificar que hay conectividad a nivel IP entre PC5 y PC6. Mirar en que VLAN y modo se encuentran.
8. Ver la asignación de puertos a VLANs.
9. Generar Broadcast y ver que las VLANs estan aisladas entre ellas.

## 1. Verificar que Fa0/1 y Fa0/2 ya se encuentran en VLAN1 y operando en modo acceso.

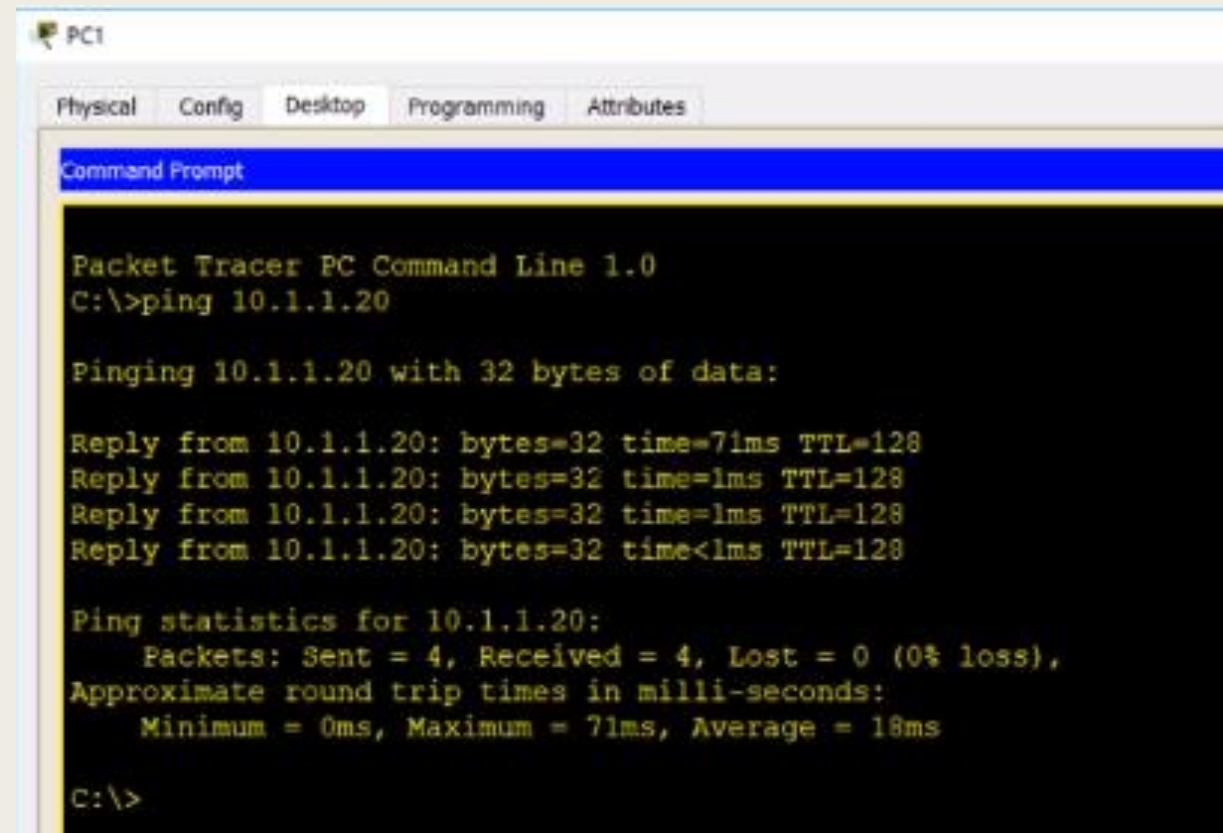
```
Switch#show interfaces fa 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

```
Switch#show interfaces fa 0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

- Podemos apreciar que por defecto todos los puertos se encuentran en la VLAN por defecto (default) y es la 1.

## 2. Verificar la conectividad a nivel IP (ping) entre PC1 y PC2 .

- Funciona. Tiene lógica, se encuentran en la misma VLAN y ya tienen asignadas las IPs.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.20

Pinging 10.1.1.20 with 32 bytes of data:

Reply from 10.1.1.20: bytes=32 time=71ms TTL=128
Reply from 10.1.1.20: bytes=32 time=1ms TTL=128
Reply from 10.1.1.20: bytes=32 time=1ms TTL=128
Reply from 10.1.1.20: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 71ms, Average = 18ms

C:\>
```



### 3. Generar Broadcast y ver que sucede (ping 10.1.1.255 desde el PC1 en modo Simulacion)

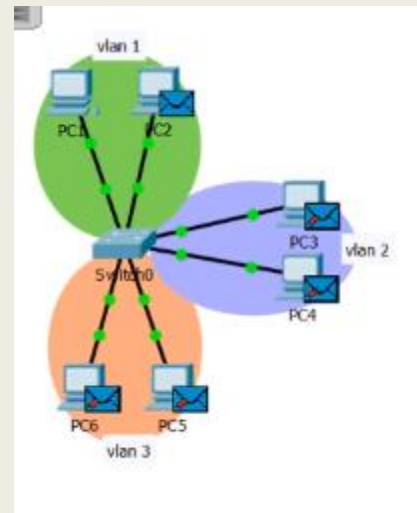
```
PC1
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.20

Pinging 10.1.1.20 with 32 bytes of data:
Reply from 10.1.1.20: bytes=32 time=7ms TTL=64
Reply from 10.1.1.20: bytes=32 time=1ms TTL=64
Reply from 10.1.1.20: bytes=32 time=1ms TTL=64
Reply from 10.1.1.20: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.1.20:
    Packets: Sent = 4, Received = 4,
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 71ms, Average = 19ms

C:\>ping 10.1.1.255
```



- Al hacer el ping en modo broadcast, vemos que el paquete se envía a todos los equipos excepto por el que lo ha enviado.
- Es lo normal dado que están todos en la misma red y VLAN.

#### 4. Configurar los puertos Fa0/3 y Fa0/4 en la VLAN2 en modo acceso utilizando “interface range ...”.

- \*Hemos añadido un name a VLAN 2 para identificarla mejor.
- Si usamos “show vlan brief” nos muestra las vlan pero de forma más breve.

```
Switch#sh vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, 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
2 VLAN_AZUL	active	Fa0/3, Fa0/4

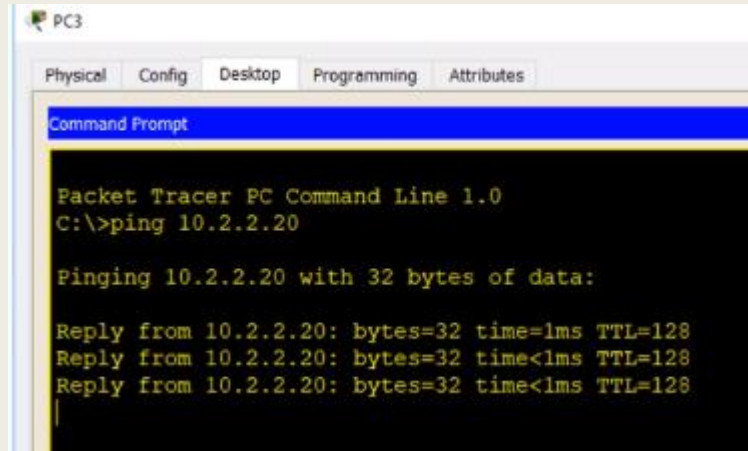
```
Switch(config)#interface range fastEthernet 0/3-4
Switch(config-if-range)#switchport mode
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport mode access
```

```
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN_AZUL
```

```
Switch(config)#interface range fastEthernet 0/3-4
Switch(config-if-range)#switchport mode
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan
Switch(config-if-range)#switchport access vlan 2
```

## 5. Probar la conectividad a nivel IP (ping) entre PC3 y PC4. Mirar en que VLAN y modo se encuentran.

- El ping funciona



The screenshot shows the 'PC3' window with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Command Prompt' tab is active, displaying the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.2.2.20

Pinging 10.2.2.20 with 32 bytes of data:

Reply from 10.2.2.20: bytes=32 time=1ms TTL=128
Reply from 10.2.2.20: bytes=32 time<1ms TTL=128
Reply from 10.2.2.20: bytes=32 time<1ms TTL=128
|
```

- Se encuentran en modo static access (y ambos en la VLAN 2)

```
Switch#show interfaces fastEthernet 0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (VLAN_AZUL)
```

```
Switch#show interfaces fastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (VLAN_AZUL)
```

## 6. Configurar los puertos Fa0/5 y Fa0/6 en la VLAN3 (modo de configuración rápido).

- Para variar, en este caso se ha accedido individualmente a cada interfaz, pero se podría haber accedido a las dos a la vez con el range

```
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
```

```
Switch(config)#interface fastEthernet 0/6
Switch(config-if)#
Switch(config-if)#switchport access vlan 3
```

```
Switch#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, 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
2	VLAN AZUL	active	Fa0/3, Fa0/4
3	VLAN0003	active	Fa0/5, Fa0/6

## 7. Verificar que hay conectividad a nivel IP entre PC5 y PC6. Mirar en que VLAN y modo se encuentran.

- Hay conectividad

```
C:\>ping 10.3.3.20

Pinging 10.3.3.20 with 32 bytes of data:

Reply from 10.3.3.20: bytes=32 time=1ms TTL=128
Reply from 10.3.3.20: bytes=32 time<1ms TTL=128
Reply from 10.3.3.20: bytes=32 time<1ms TTL=128
```

- Para variar a la hora de consultar las VLAN podemos escribir:
  - *show interfaces switchport* (muestra la misma info pero para todos los puertos)

```
Name: Fa0/5
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 3 (VLAN0003)
Trunking Native Mode VLAN: 1 (default)
```

```
Name: Fa0/6
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 3 (VLAN0003)
Trunking Native Mode VLAN: 1 (default)
```



## 8. Ver la asignación de puertos a VLANs.

- show vlan (o show vlan brief)

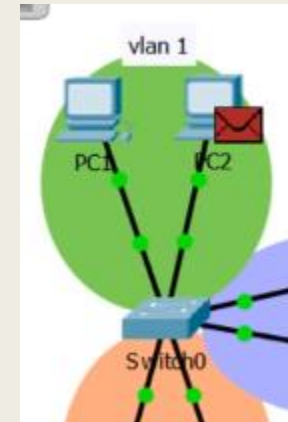
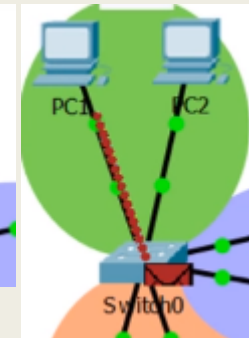
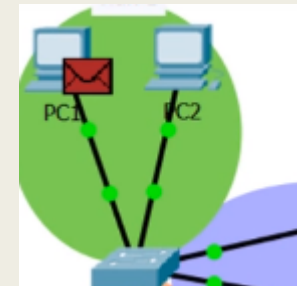
```
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, 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
2	VLAN_AZUL	active	Fa0/3, Fa0/4
3	VLAN0003	active	Fa0/5, Fa0/6

## 9. Generar Broadcast y ver que las VLANs estan aisladas entre ellas.

- Vemos que ahora el ping solo se envía por la VLAN en la que está el PC1.

```
C:\>  
C:\>ping 10.1.1.255
```



# Extra. Cambiar la VLAN de PC4 a VLAN3 y probar conectividad

```
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#swi
Switch(config-if)#switchport a
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 3
```

```
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 3 (VLAN0003)
```

```
Ping statistics for 10.2.2.20:
Packets: Sent = 4, Received = 0, Drop = 4
Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Lo estamos lanzando desde el PC3

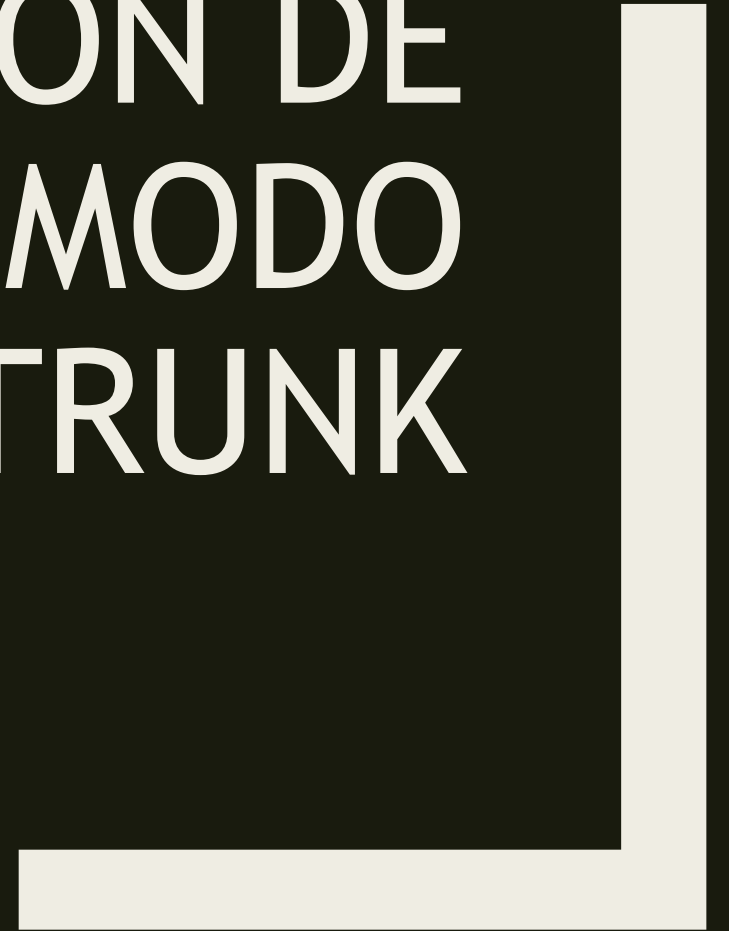
```
C:\>
C:\>
C:\>ping 10.2.2.20
```

```
Pinging 10.2.2.20 with 32 bytes of data:
Request timed out.
```

El ping ahora no llega a su destino

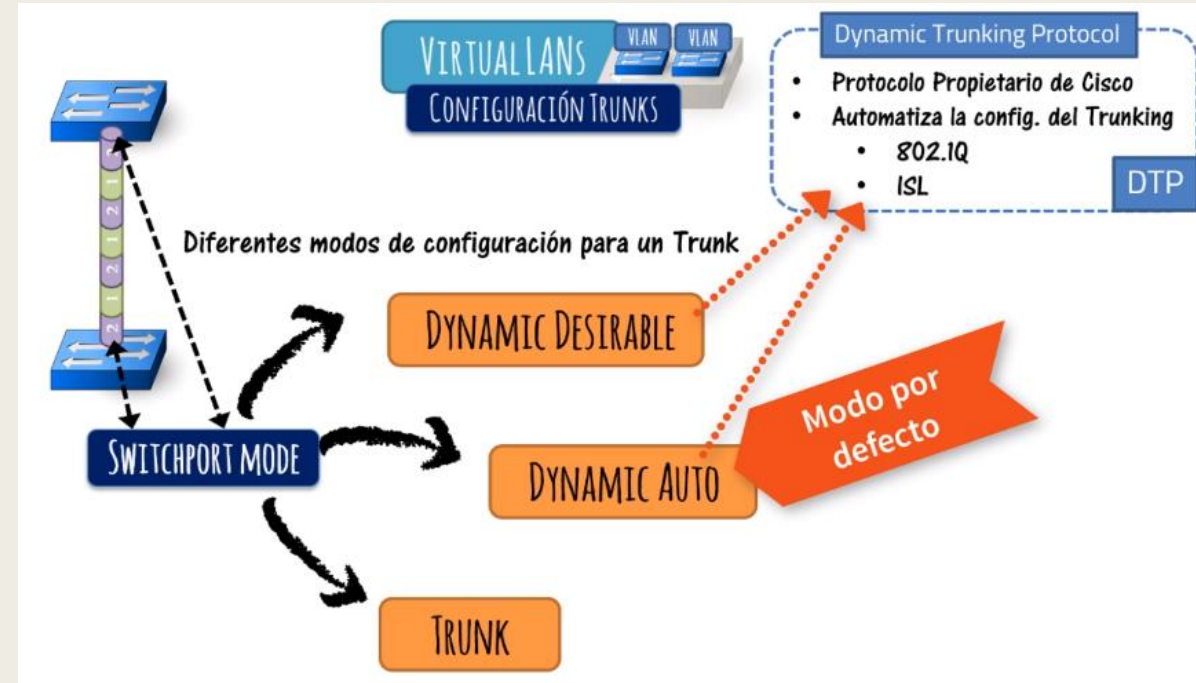


# CONFIGURACIÓN DE PUERTOS EN MODO TRUNK



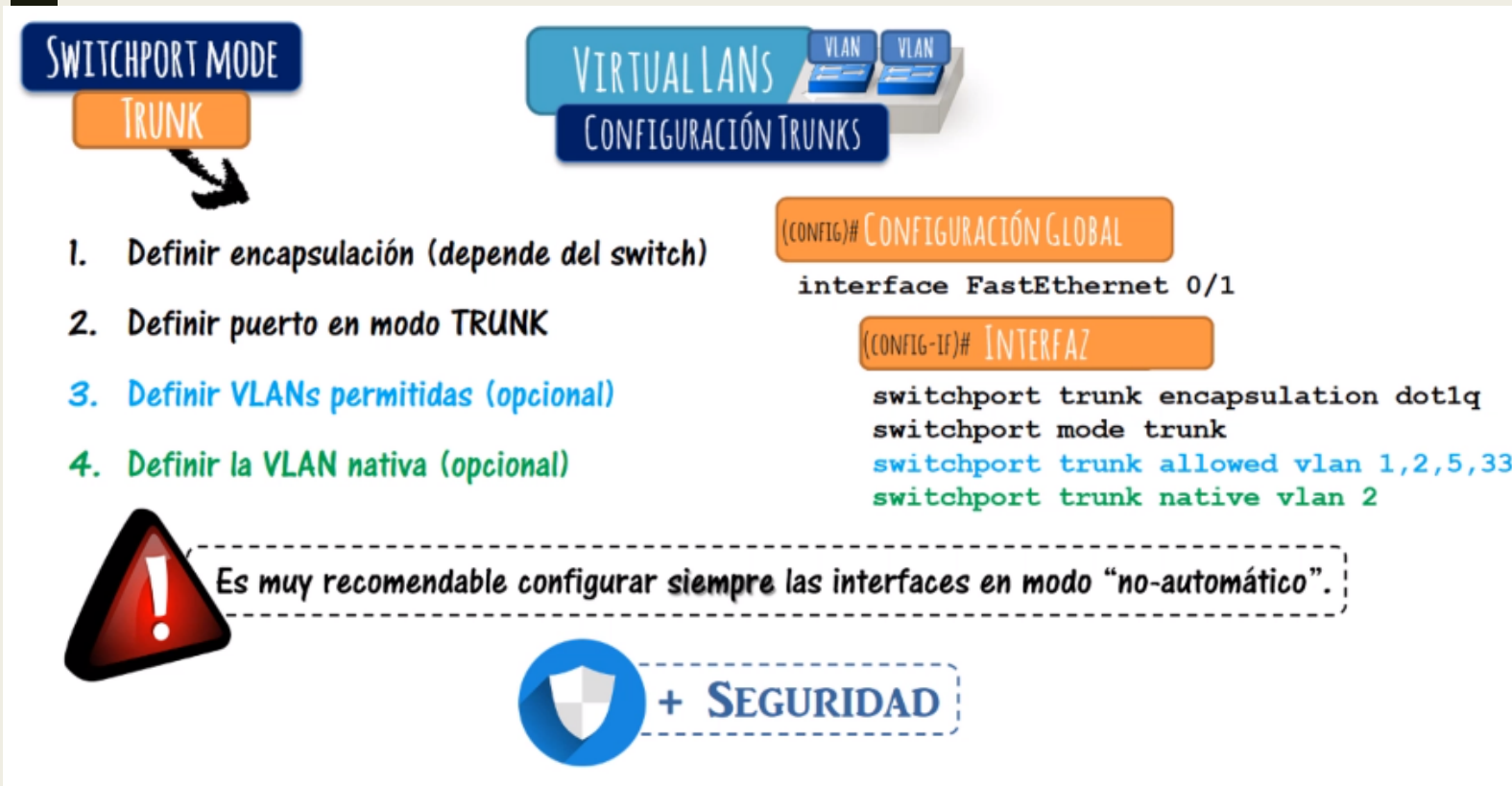
# Introducción

- Ahora vamos a ver la configuración de los puertos en modo trunk
- Aquí es un poco más complejo, porque para la configuración tendremos más opciones:
  - *Dynamic desirable*
  - *Dynamic auto*
  - *Trunk*
- Para la configuración dinámica, se llevará a cabo mediante el protocolo DTP, del que es propietario CISCO.
- La automatización con DTP se puede realizar mediante el protocolo 802.1Q o mediante ISL (de CISCO también)



ISL no lo veremos ya que está en desuso.  
Hay switches que no soportan ya ISL

# Configuración TRUNK



- A tener en cuenta:
  - 1. solo será necesario si el switch soporta dot1q e ISL.
    - Si solo soporta dot1q no es necesario.
  - 3. No es necesario si queremos que puedan circular por ese puerto todas las vlan.
  - 3. Y las vlan las podemos indicar con rango también
  - 4. No es necesario si no queremos cambiar la vlan nativa y queremos que se use la vlan por defecto.

# DTP (Dynamic Trunking Protocol)

- Vamos a ver cómo funciona DTP, que es:

Es una forma de automatizar la configuración de los puertos troncales

- Esta opción no es recomendable.
  - *Nos permite ahorrar algo de tiempo, pero tiene muchas desventajas que no podemos asumir en una red productiva.*
- La negociación del DTP será diferente en función del modo administrativo que tenga configurado:

FUNCIONAMIENTO		
MODO ADMINISTRATIVO	Dynamic Auto	De forma pasiva, se mantiene a la espera de recibir mensajes de negociación, para que dado el caso, responda y negocie la utilización del puerto como Trunk.
	Dynamic Desirable	Inicia de forma activa la negociación, enviando y respondiendo a los mensajes de negociación para determinar si el puerto puede funcionar como Trunk.
	Trunk	Funciona siempre como puerto Trunk.
	Access	Funciona siempre como puerto de acceso.

Si está en modo Dynamic auto, espera a que el otro extremo le hable.


# DTP - Combinaciones de modos administrativos en ambos extremos

Dos extremos dynamic auto esperarán y nunca obtendrán respuesta del otro. (= ACCESS)

- Dependiendo de la configuración que tengan los puertos en cada extremo en su modo administrativo, su modo operativo será diferente.

		FUNCIONAMIENTO	
MODOS ADMINISTRATIVOS	Dynamic Auto	Si está en modo Dynamic auto, espera a que el otro extremo hable para configurarse o no como trunk.	
	Dynamic Desirable	Si está en modo Dynamic desirable, toma la iniciativa a la hora de negociar si el puerto funcionará como trunk.	
	Trunk	Funciona siempre como puerto Trunk.	
	Access	Funciona siempre como puerto de acceso.	

- Error de configuración: Un extremo modo Access y el otro modo Trunk.

		MODOS ADMINISTRATIVOS			
MODOS ADMINISTRATIVOS		Dynamic Auto	Dynamic Desirable	Trunk	Access
	Dynamic Auto	Access	Trunk	Trunk	Access
	Dynamic Desirable	Trunk	Trunk	Trunk	Access
	Trunk	Trunk	Trunk	Trunk	-----
	Access	Access	Access	-----	Access



# Resumen comandos show

Muestra información detallada a nivel de VLAN de TODAS las interfaces

```
show interfaces switchport
```

Muestra información detallada a nivel de VLAN de la interfaz indicada

```
show interfaces Fa0/1 switchport
```

Muestra información detallada a nivel de VLAN de la interfaz indicada

```
show interfaces trunk
```

**show vlan** Muestra las VLANs creadas y los puertos asignados a cada VLAN.

```
sw2#sh vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, 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
2	VLAN0002	active	Fa0/2
100	gestion	active	Fa0/9
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0

```
show vlan id n°_de_vlan
```

```
show vlan brief
```



# PRÁCTICA: CONFIGURACIÓN DE PUERTOS EN MODO TRUNK



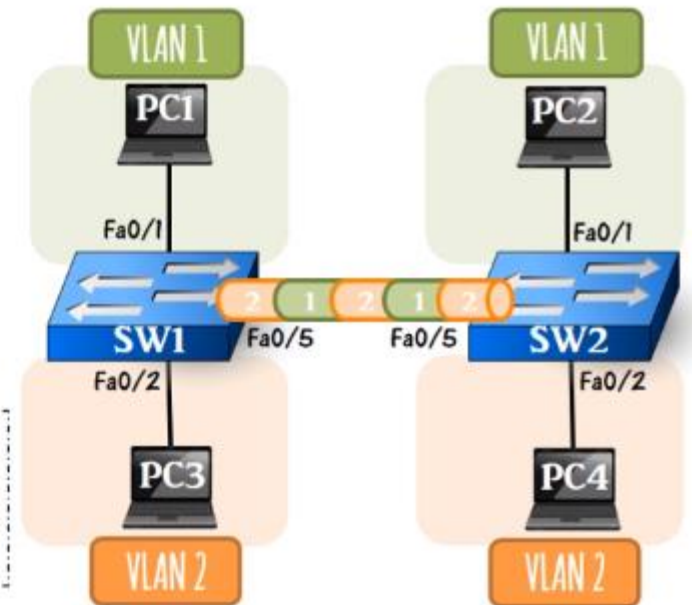
# Ejercicio práctico

- En esta práctica vamos a configurar tanto modos trunk como modos de acceso.
- En el aula virtual tenéis colgado el archivo base para poder hacer este ejercicio.

1. Crear VLANs. Configurar puertos en modo acceso con las VLANs correspondientes.
2. Ver qué VLANs existen en cada switch y los puertos asignados.
3. Comprobar conectividad entre PC1 y PC2. Y entre PC3 y PC4. Funciona? Porque?
4. Verificar el modo switchport operacional y administrativo en Fa0/5 de SW1 y SW2, así como la native VLAN.
5. Cambiar el modo switchport administrativo en Fa0/5 del SW1 a dynamic desirable
6. Verificar el modo switchport operacional en Fa0/5 de SW1 y SW2.
7. Comprobar conectividad entre PC1 y PC2. Y entre PC3 y PC4.
8. Mostrar la información sobre todas las interfaces Trunk.
9. Cambiar el modo Administrativo de los puertos Fa0/5 a Trunk.
10. Comprobar conectividad entre PC1 y PC2. Y entre PC3 y PC4.



IP PC1: 10.1.1.1 /24  
IP PC2: 10.1.1.2 /24  
  
IP PC3: 10.2.2.1 /24  
IP PC4: 10.2.2.2 /24



## 1. Crear VLANs. Configurar puertos en modo acceso con las VLANs correspondientes.

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vlan 2
```

```
SW1(config)#interface fastEthernet 0/2
SW1(config-if)#swi
SW1(config-if)#switchport mode
SW1(config-if)#switchport mode acc
SW1(config-if)#switchport mode access
SW1(config-if)#swi
SW1(config-if)#switchport acc
SW1(config-if)#switchport access vlan 2
```

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#swi
SW1(config-if)#switchport mo
SW1(config-if)#switchport mode acc
SW1(config-if)#switchport mode access
```

```
SW2#configure t
SW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#vlan 2
```

```
SW2(config)#interface fastEthernet 0/1
SW2(config-if)#swi
SW2(config-if)#switchport mod
SW2(config-if)#switchport mode acc
SW2(config-if)#switchport mode access
SW2(config-if)#exi
SW2(config)#interface fastEthernet 0/2
SW2(config-if)#switchport mode access
SW2(config-if)#
SW2(config-if)#swi
SW2(config-if)#switchport acc
SW2(config-if)#switchport access vlan
SW2(config-if)#switchport access vlan 2
```

## 2. Ver qué VLANs existen en cada switch y los puertos asignados.

- Hacemos el show vlan brief en ambos switches y podemos ver toda la información

```
SW1#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, 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
2	VLAN0002	active	Fa0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SW1#
```

### 3. Comprobar conectividad entre PC1 y PC2. Y entre PC3 y PC4. Funciona? Porque?

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

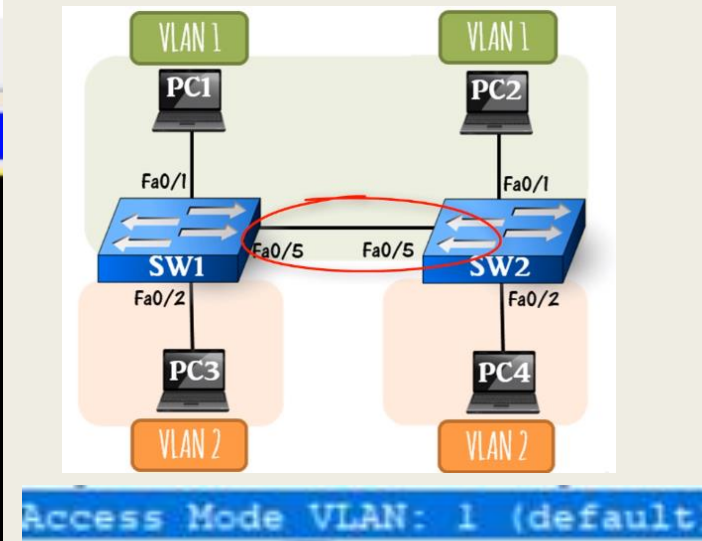
Reply from 10.1.1.2: bytes=32 time=17ms TTL=128
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128
Reply from 10.1.1.2: bytes=32 time=2ms TTL=128
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.2:
```

```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
```



- El PC1 tiene conectividad con el PC2 pero el PC3 no tiene conectividad con el PC4
- ¿A qué se debe? A la configuración de los modos administrativos (ambos en dynamic auto), que hacen que la relación entre ambos sea ACCESS (con VLAN 1 por defecto).
- El esquema de red equivalente que tenemos es el que se muestra en la imagen de la derecha (la VLAN2 está aislada).



4. Verificar el modo switchport operacional y administrativo en Fa0/5 de SW1 y SW2, así como la native VLAN.

```
SW1#show interfaces fastEthernet 0/5 sw
SW1#show interfaces fastEthernet 0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: native
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
```



## 5. Cambiar el modo switchport administrativo en Fa0/5 del SW1 a dynamic desirable

- Al cambiar el modo switchport administrativo a dynamic desirable pasaremos a tener TRUNK en modo operativo.



```
SW1(config-if)#switchport mode dynamic desirable
```

## 6. Verificar el modo switchport operacional en Fa0/5 de SW1 y SW2.

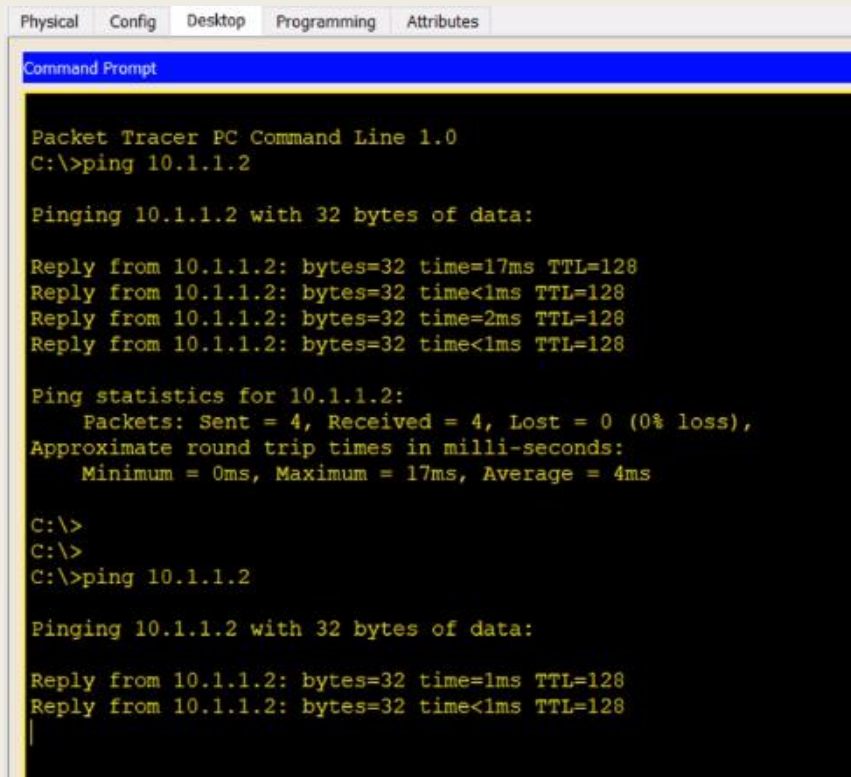
- Ojo, ahora mismo, este enlace troncal permitirá TODAS las VLANs

```
SW1#  
SW1#show interfaces fastEthernet 0/5 switchport  
Name: Fa0/5  
Switchport: Enabled  
Administrative Mode: dynamic desirable  
Operational Mode: trunk  
Administrative Trunking Encapsulation:  
Operational Trunking Encapsulation: dot1q  
Negotiation of Trunking: On  
Access Mode VLAN: 1 (default)
```

```
SW2#show interfaces fastEthernet 0/5 swi  
SW2#show interfaces fastEthernet 0/5 switchport  
Name: Fa0/5  
Switchport: Enabled  
Administrative Mode: dynamic auto  
Operational Mode: trunk  
Administrative Trunking Encapsulation:
```

## 7. Comprobar conectividad entre PC1 y PC2. Y entre PC3 y PC4.

- Ahora funciona la conectividad en ambos casos.



```
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

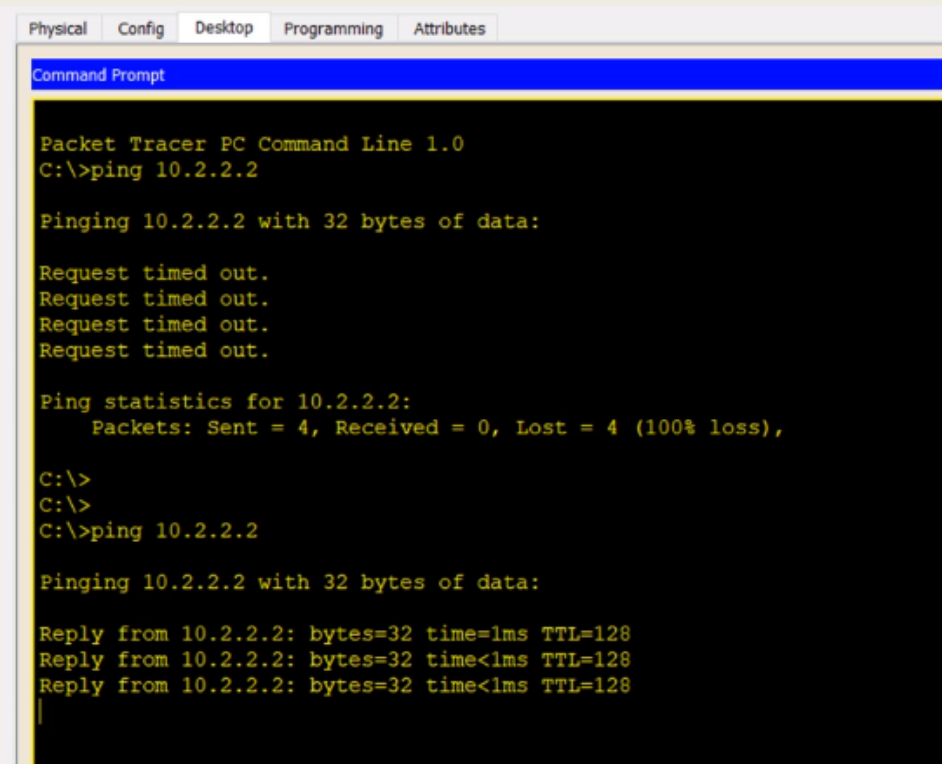
Reply from 10.1.1.2: bytes=32 time=17ms TTL=128
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128
Reply from 10.1.1.2: bytes=32 time=2ms TTL=128
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 17ms, Average = 4ms

C:\>
C:\>
C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=1ms TTL=128
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128
|
```



```
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.2.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
C:\>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:

Reply from 10.2.2.2: bytes=32 time=1ms TTL=128
Reply from 10.2.2.2: bytes=32 time<1ms TTL=128
Reply from 10.2.2.2: bytes=32 time<1ms TTL=128
|
```

## 8. Mostrar la información sobre todas las interfaces Trunk.

- Podemos ver que estos switches SOLO soportan la encapsulación de 802.1q
  - *No soportan la encapsulación ISL de cisco que hemos comentado antes que estaba en desuso.*
- Por lo tanto, no podríamos ponerles el comando:

```
switchport trunk encapsulation dot1q
```

```
SW1#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/5     desirable n-802.1q       trunking      1

Port      Vlans allowed on trunk
Fa0/5     1-1005

Port      Vlans allowed and active in management domain
Fa0/5     1,2

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/5     1,2

SW1#
```

## 9. Cambiar el modo Administrativo de los puertos Fa0/5 a Trunk.

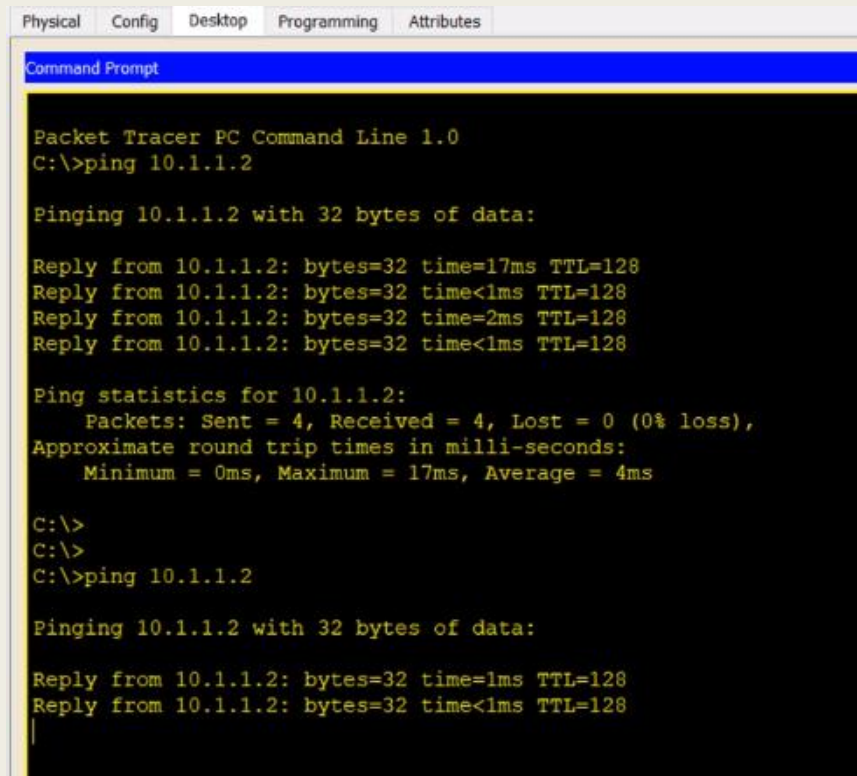
```
SW1(config)#interface fastEthernet 0/5
SW1(config-if)#sw
SW1(config-if)#switchport mo
SW1(config-if)#switchport mode tr
SW1(config-if)#switchport mode trunk
SW1(config-if)#swi
```

```
SW2(config)#int
SW2(config)#interface fa
SW2(config)#interface fastEthernet 0/5
SW2(config-if)#swi
SW2(config-if)#switchport mo
SW2(config-if)#switchport mode tru
SW2(config-if)#switchport mode trunk
SW2(config-if)#
```

```
SW1#show interfaces fastEthernet 0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation:
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

## 10. Comprobar conectividad entre PC1 y PC2. Y entre PC3 y PC4.

- Tenemos el mismo resultado que antes, funciona:



```
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

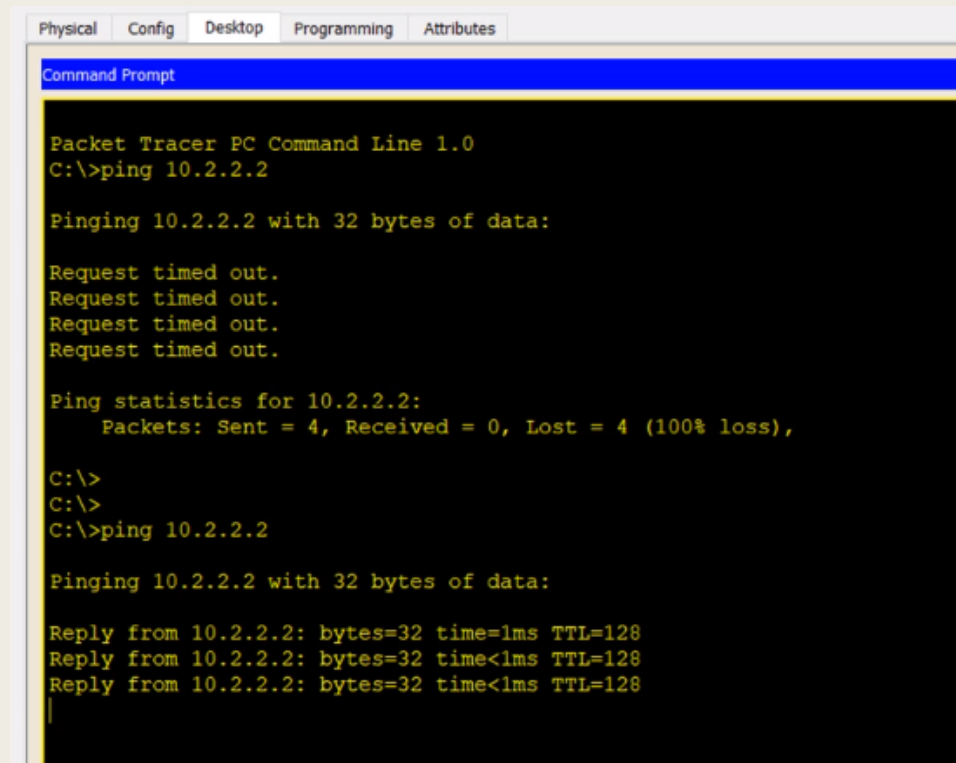
Reply from 10.1.1.2: bytes=32 time=17ms TTL=128
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128
Reply from 10.1.1.2: bytes=32 time=2ms TTL=128
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 4ms

C:\>
C:\>
C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=1ms TTL=128
Reply from 10.1.1.2: bytes=32 time<1ms TTL=128
|
```



```
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.2.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
C:\>ping 10.2.2.2

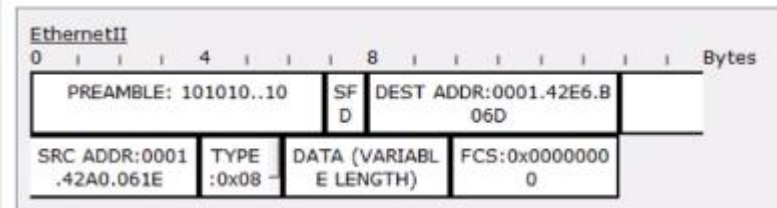
Pinging 10.2.2.2 with 32 bytes of data:

Reply from 10.2.2.2: bytes=32 time=1ms TTL=128
Reply from 10.2.2.2: bytes=32 time<1ms TTL=128
Reply from 10.2.2.2: bytes=32 time<1ms TTL=128
|
```

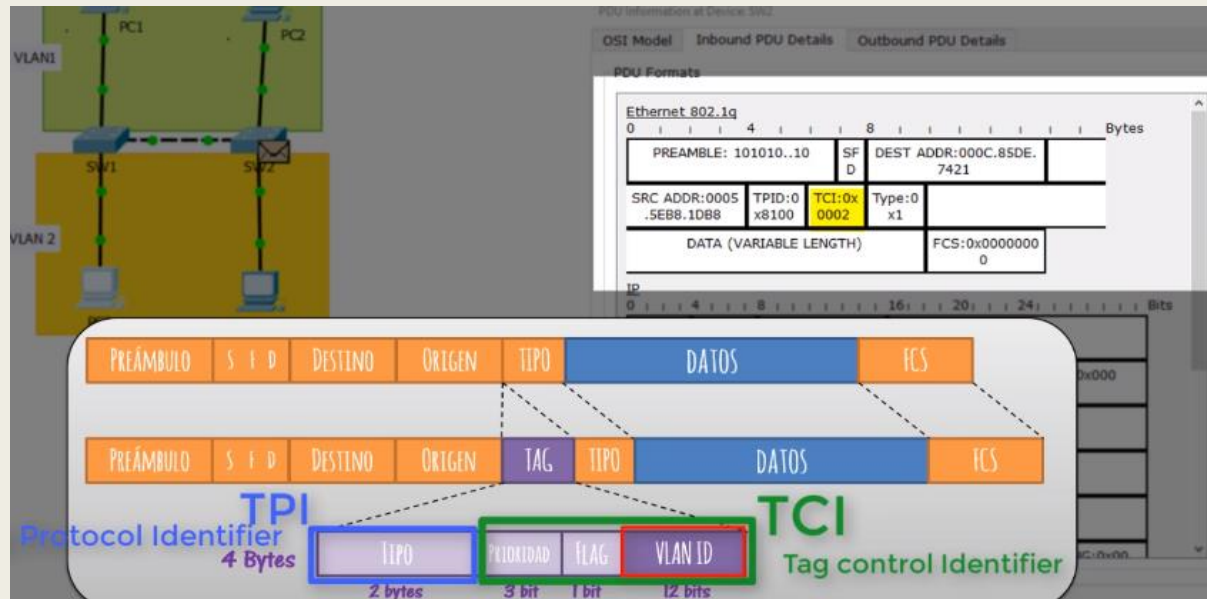


# Breve inciso: ¿Cómo viaja la trama cuando la VLAN Nativa es 1?

- Desde el PC1 al PC2 no se añade ninguna trama extra:



- Desde el PC3 al PC4 se añade la trama TCI:



¿Preguntas?

A thick black L-shaped frame is positioned around the text. It starts at the top left, goes right, then down, then right again, and finally down to the bottom right corner.

# VIRTUAL LANS / VLANs

Configuración de puertos en modo Acceso y Trunk