Telefónica

# HOSTED IP

## Redes de Area Virtual
## VLAN

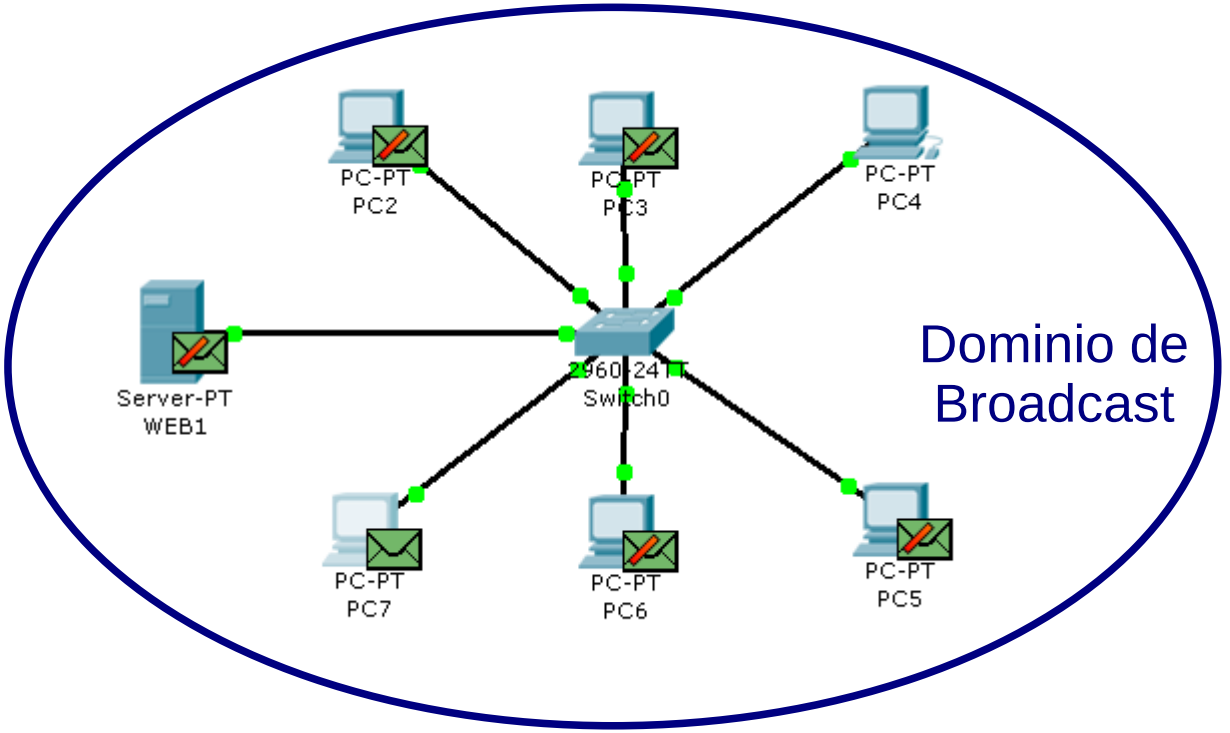
# Redes Virtuales

## Introducción

# Redes Virtuales. VLAN

## Introducción

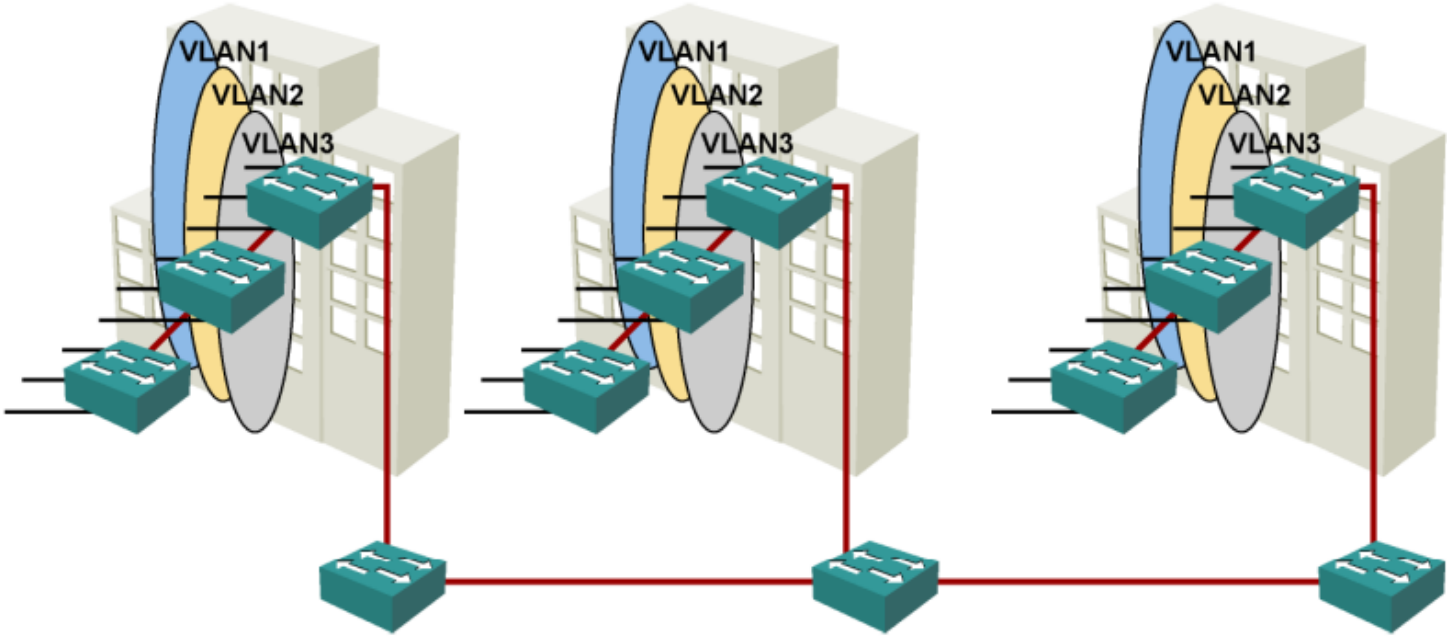
Una red constituida sobre dispositivos de nivel 2, es una red plana, solo existe un dominio de difusión



# Redes Virtuales. VLAN

## Introducción

Una VLAN, es una separación virtual dentro de un switch, que proporciona una LAN lógica, diferente e independiente




VLAN1 192.168.1.0

VLAN2 192.168.2.0

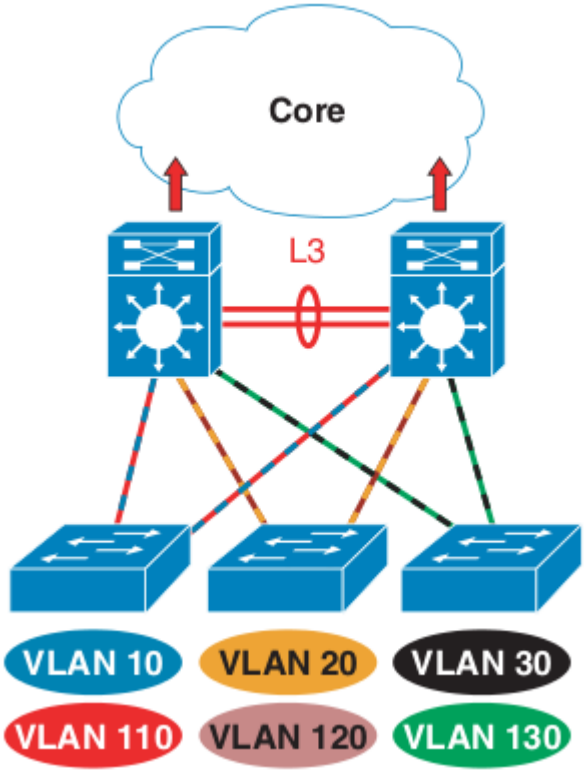
VLAN3 192.168.3.0

# Redes Virtuales. VLAN

## Introducción

### Cuando se diseña una red con VLAN

- Se recomienda asignar una subred a cada VLAN
- No permitir que las VLAN se propagen más allá de la capa de distribución (el tráfico de broadcast debe estar alejado del core)
- En las redes donde el modelo de tráfico cumpla la regla 80/20, se debe asignar una VLAN por sede



# Redes Virtuales. VLAN

## Introducción

Las VLAN están pensadas para la capa de acceso y proveen

- Seguridad, los grupos con datos sensibles, se separan del resto de la red
- Segmentación, se reduce el número de hosts en un dominio de broadcast
- Permiten agrupar a usuarios de un mismo dominio de broadcast con independencia de su ubicación física en la red

# Redes Virtuales. VLAN

## Introducción

Cuando se asigna una VLAN, se le asigna un número ID y un nombre

```
Switch#sh vlan brief

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
                                                Gig1/1, Gig1/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

# Redes Virtuales. VLAN

## Introducción

El número de VLAN, comprende:

- Rango normal, se identifica mediante un identificativo comprendido entre 1 y 1005
- Rango extendido, se identifican mediante un ID comprendido entre 1006 y 4094, admiten menos características de las de rango normal

# Redes Virtuales. VLAN

## Introducción

### El proceso de creación de VLAN

- Creación de la VLAN
- Asignación de VLAN a los puertos de interfaz necesarios

```
Switch#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Gig1/1, Gig1/2
10   VENTAS                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

# Redes Virtuales. VLAN

## Introducción

### El proceso de creación y asignación de VLAN

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name VENTAS
Switch(config-vlan)#end

Switch(config)#interface fastethernet range 0/1-5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#end
```

# Redes Virtuales

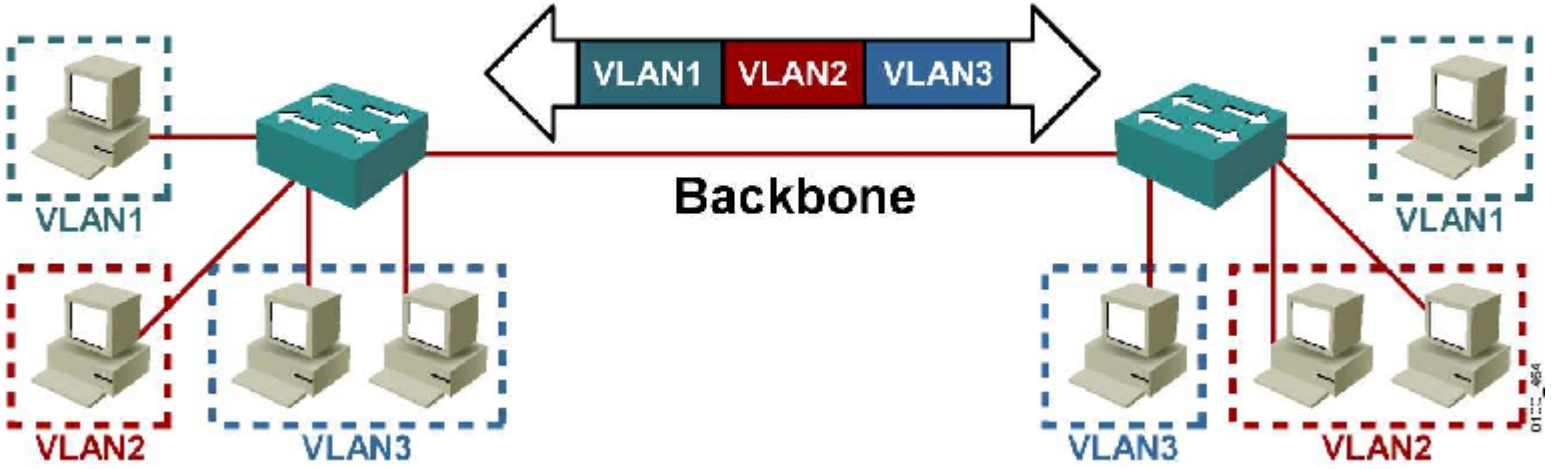
## Enlaces troncales

# Redes Virtuales. VLAN

## Enlaces troncales

La transferencia de tráfico unicast y broadcast, se limita a los dispositivos presentes en esa VLAN

En casos de usuarios de la misma VLAN ubicados en diferentes conmutadores, se utilizan enlaces troncales para su comunicación



# Redes Virtuales. VLAN

## Enlaces troncales

A medida que las tramas salen por el trunk, son etiquetadas para indicar a que VLAN pertenecen, en destino, se retiran esas etiquetas para ser entregadas al puerto correspondendiente

Existen dos posibilidades de etiquetado

- ISL (Inter Switch Link Protocol), propietario de Cisco. Esta en deshuso
- IEEE 802.1q

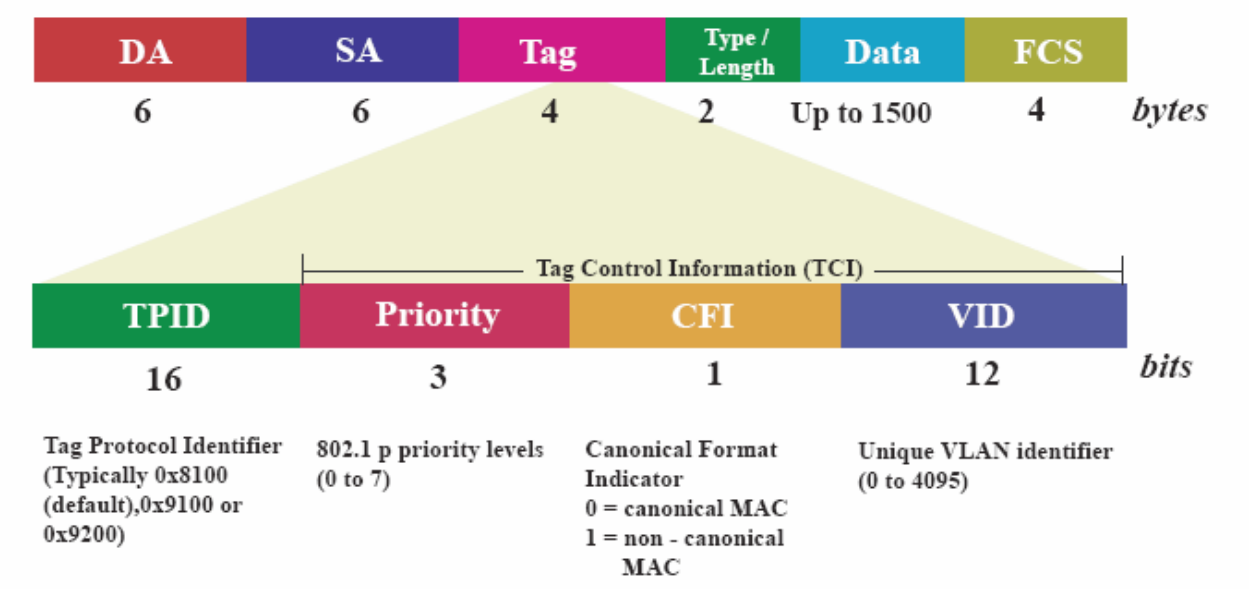
En una conexión troncal, ambos extremos deben estar de acuerdo sobre el protocolo a usar

# Redes Virtuales. VLAN

## Enlaces troncales

IEEE 802.1q es el estándar, introduce el concepto de VLAN Nativa.

Modifica la trama ethernet, añadiendo un campo de 4 bytes despues de la dirección ethernet origen

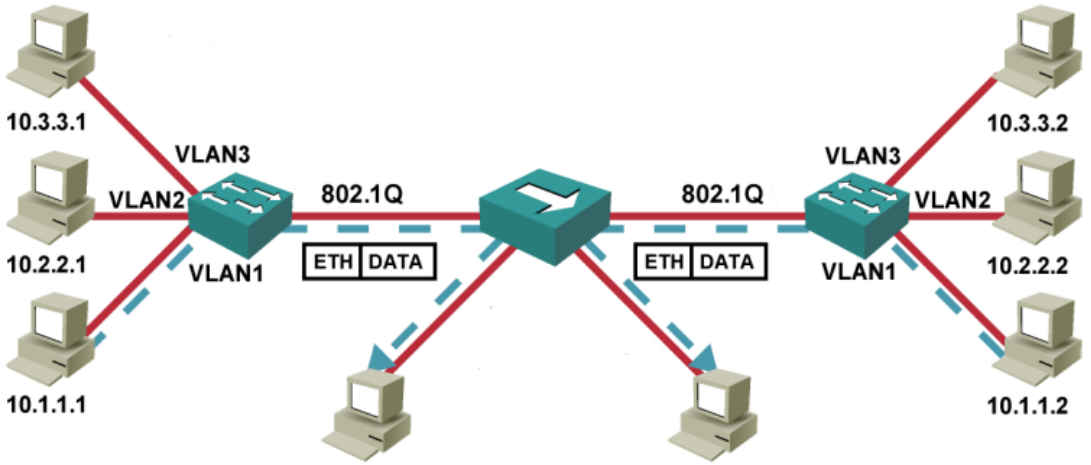


# Redes Virtuales. VLAN

## Enlaces troncales

El tráfico de control enviado en la VLAN nativa, debe estar sin etiquetar, si un puerto troncal 802.1q recibe una trama etiquetada en la VLAN nativa, descarta la trama

Cuando un trunk, recibe tramas sin etiquetar, envía esas tramas a la VLAN nativa



# Redes Virtuales. VLAN

## Enlaces troncales

La configuración de un trunk, implica determinar que puerto va a ser troncal, que protocolo va a usar y si el puerto va a negociar y como

```
Switch#configure terminal
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#no shutdown
```

# Redes Virtuales. VLAN

## Enlaces troncales

Opcionalmente, se pueden limitar las VLAN permitidas en el enlace troncal

```
Switch(config-if)#switchport trunk allowed vlan 10
Switch(config-if)#switchport trunk allowed vlan add 20
Switch(config-if)#switchport trunk allowed vlan except 15
Switch(config-if)#switchport trunk allowed vlan remove 20
```

# Redes Virtuales. VLAN

## Enlaces troncales

Podemos cambiar la VLAN nativa

```
Switch#configure terminal
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#end
```

# Redes Virtuales. VLAN

## Enlaces troncales

Para verificar el estado de los enlaces troncales

```
Switch#show interface trunk
```

```
SW1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/24      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      none
SW1#
```

# Redes Virtuales. VLAN

## Enlaces troncales. Protocolo DTP

DTP es un protocolo propietario de Cisco que se utiliza entre switches directamente conectados y que negocia de manera automática, la creación de enlaces troncales, así como el tipo de encapsupación. DTP define la manera en la que el puerto negocia con su par

- **Activado**, se envian notificaciones al puerto remoto indicando que se encuentra activado
- **Dinámico automático**, indica que puede establecer enlaces troncales, pero no solicita el paso al estado troncal
- **Conveniente**, el puerto indica que puede pasar al estado troncal y solicita el pase
- **Desactivado**, no envía solicitudes ni estado al puerto remoto

# Redes Virtuales. VLAN

## Enlaces troncales. Protocolo DTP

| | Dynamic Auto | Dynamic Desirable | Trunk | Access |
|---|---|---|---|---|
| Dynamic Auto | Access | Trunk | Trunk | Access |
| Dynamic Desirable | Trunk | Trunk | Trunk | Access |
| Trunk | Trunk | Trunk | Trunk | Not recommended |
| Access | Access | Access | Not recommended | Access |

# Redes Virtuales. VLAN

## Enlaces troncales. Protocolo DTP

### Problemas comúnes

- Falta de concordancia en la VLAN nativa, cuando se configura un enlace con diferentes VLAN nativas
- Falta de concordancia en el enlace troncal, en un puerto aparece como activo y en el otro como inactivo
- VLAN admitidas en el enlace troncal, o se envía tráfico no apropiado o no se envía el tráfico esperado

# Redes Virtuales

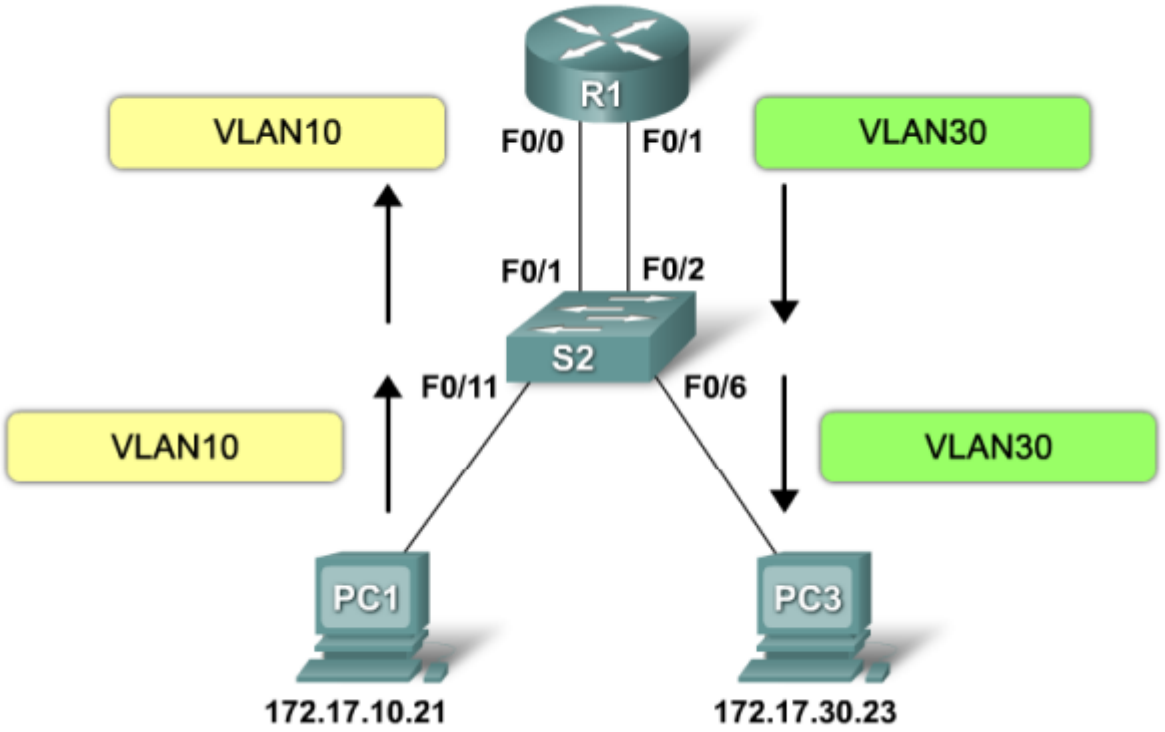
## Enrutamiento entre VLAN

# Redes Virtuales. VLAN

## Enrutamiento entre VLAN

Routing interVLAN, es el proceso de reenviar tráfico desde una VLAN  a otra

Routing tradicional



# Redes Virtuales. VLAN

## Enrutamiento entre VLAN

Cada interfaz del switch se configurará en una VLAN determinada.

El router, tendrá configurada una VLAN en cada interfaz

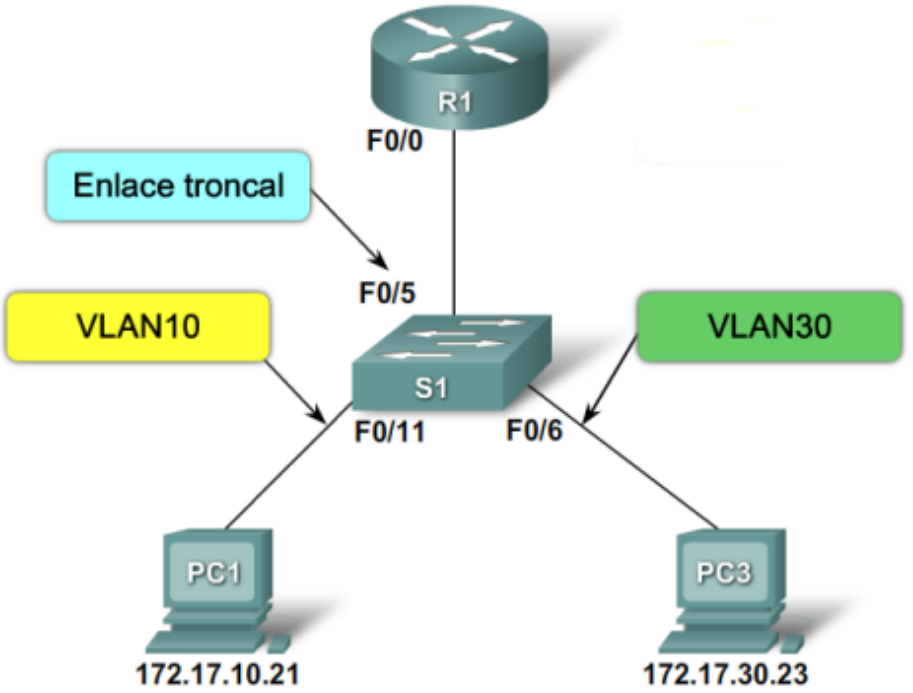
```
SW(config)#interface FastEthernet0/1
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 100

Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.100.1 255.255.255.0
Router(config-if)#no shutdown
```

# Redes Virtuales. VLAN

## Enrutamiento entre VLAN

Routing interVLAN, es el proceso de reenviar tráfico desde una VLAN  a otra

Router on a stick



# Redes Virtuales. VLAN

## Enrutamiento entre VLAN

Se configurará un trunk con las VLAN a enrutar

En el router hay que configurar tantas subinterfaces como VLAN queramos enrutar

```
SW(config)#interface FastEthernet0/1
SW(config-if)#switchport mode trunk
SW(config-if)#switchport trunk allowed vlan

Router(config)#interface FastEthernet0/0.100
Router(config-subif)#encapsulation dot1q 100
Router(config-subif)#ip address A.B.C.D M.M.M.M
Router(config-if)#no shutdown
```

# Redes Virtuales. VLAN

## Enrutamiento entre VLAN

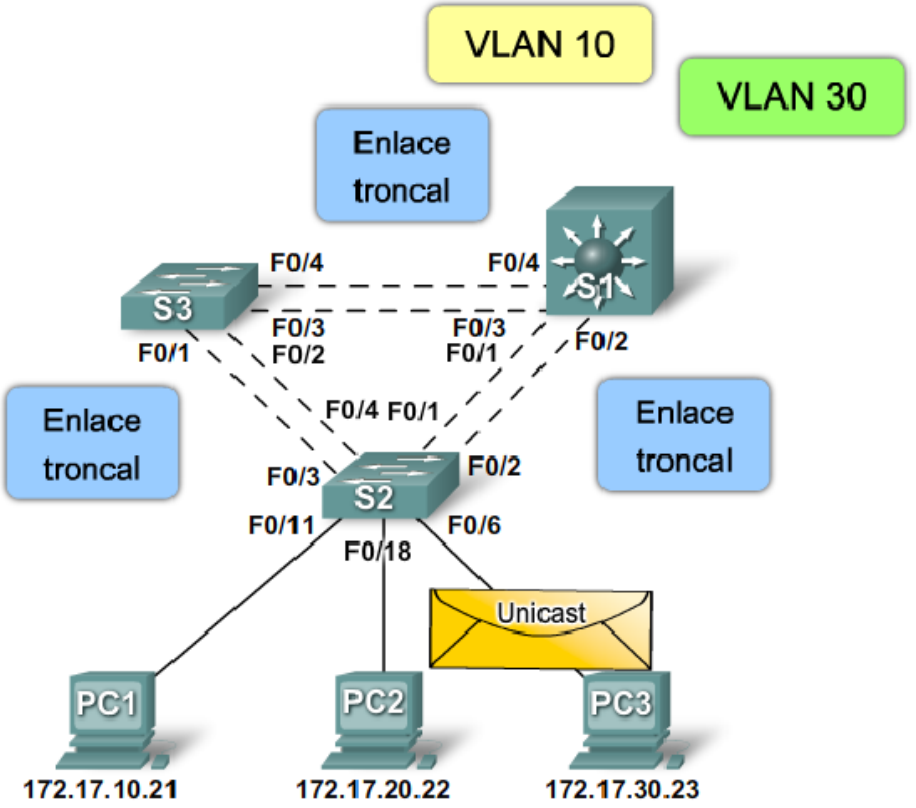
| **Interfaz física** | **Subinterfaz** |
|---|---|
| Una interfaz física por VLAN | Una interfaz física para muchas VLAN |
| No existe contención de ancho de banda | Contención del ancho de banda |
| Puerto de switch en modo acceso | Enlace troncal en el puerto del switch |
| Mas coste por solución | Menos costoso |
| Configuración de la conexión más compleja | Configuración de la conexión menos compleja |

# Redes Virtuales. VLAN

## Enrutamiento entre VLAN

Routing interVLAN, es el proceso de reenviar tráfico desde una VLAN  a otra

Switch Multicapa



# Redes Virtuales. VLAN

## Enrutamiento entre VLAN

Se configurará un trunk en el switch con las VLAN a enrutar

En el switch multicapa, se habilitará el proceso de routing y se asignará direccionamiento IP a las VLAN correspondientes

```
SW(config)#interface FastEthernet0/1
SW(config-if)#switchport mode trunk
SW(config-if)#switchport trunk allowed vlan

SW(config)#ip routing
SW(config)#interface vlan 1000
SW(config-subif)#ip address A.B.C.D M.M.M.M
```

# Redes Virtuales. VLAN

## Enrutamiento entre VLAN

### Errores típicos

- Conectar la interfaz física del router en un puerto equivocado del switch
- Configurar la VLAN incorrecta en el subinterfaz creado

### Comandos de verificación

```
SW# sh mac-sddress-table
SW# sh arp
SW# sh ip route
SW# sh ip cef
SW# sh adjacency
SW# sh interfaces vlan vlan_id
SW# sh interfaces
```

# Redes Virtuales

## Spanning Tree Protocol

# Redes Virtuales. VLAN

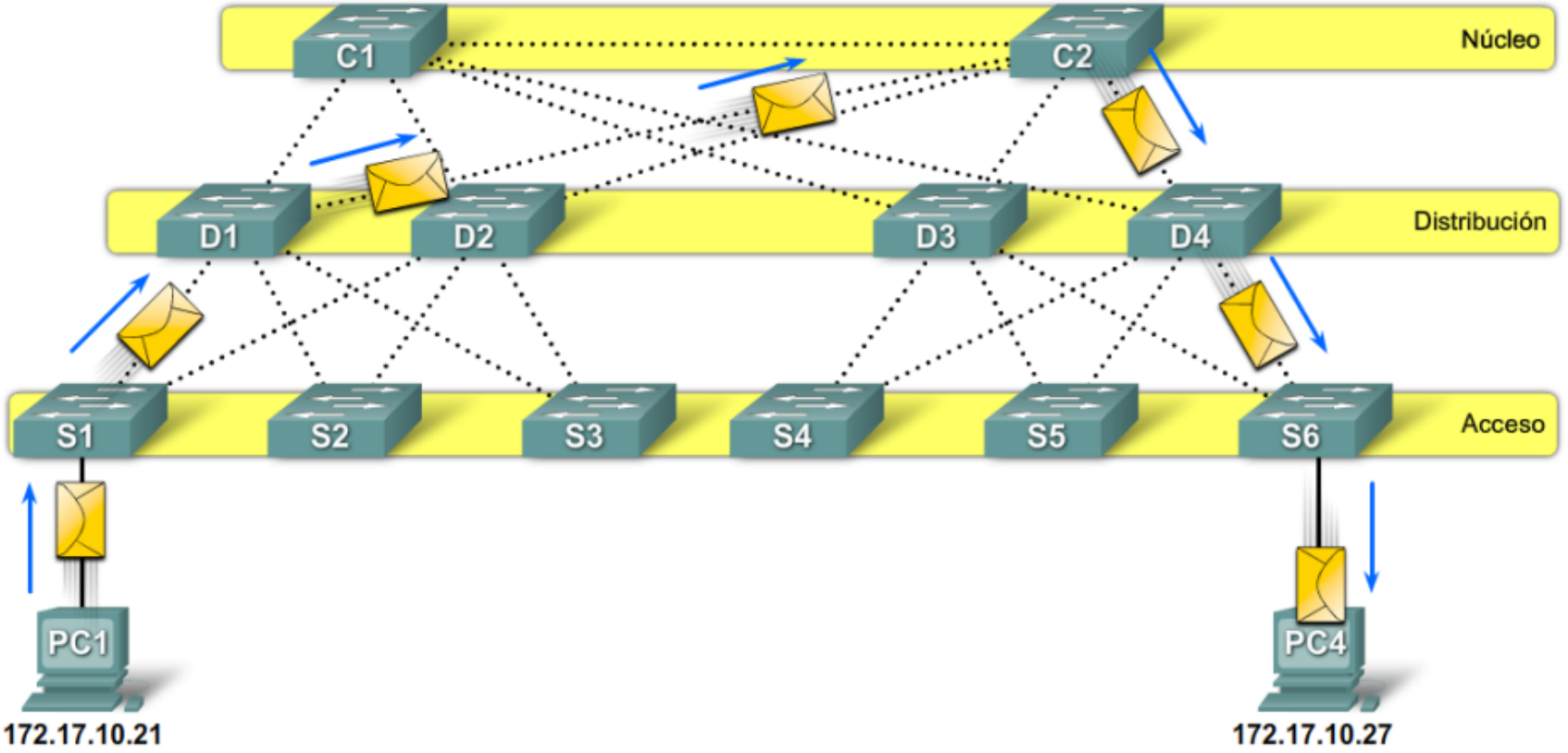
## Spanning Tree Protocol

### Redundancia

- La redundancia es la solución para lograr la disponibilidad necesaria en la infraestructura de red
- La redundancia de capa 2, mejora la disponibilidad de la red, implementando rutas de red alternas mediante el agregado de equipos y cables
- En un diseño jerarquico, la redundancia se logra en las capas de distribución y núcleo a través de hardware adicional y rutas alternativas a dicho hardware
- La redundancia, cuenta con algunas complicaciones a tener en cuenta

# Redes Virtuales. VLAN

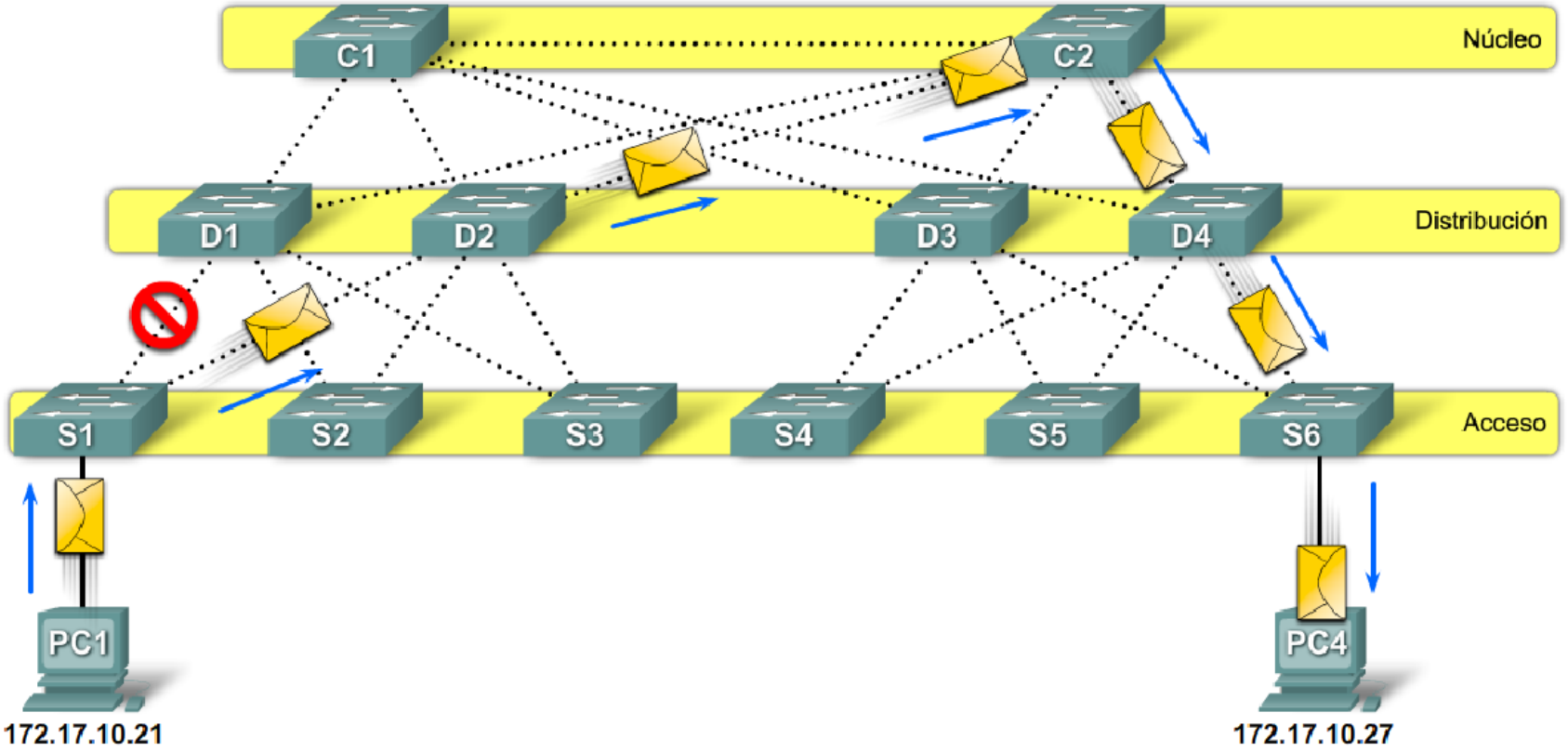
## Spanning Tree Protocol



# Redes Virtuales. VLAN

## Spanning Tree Protocol

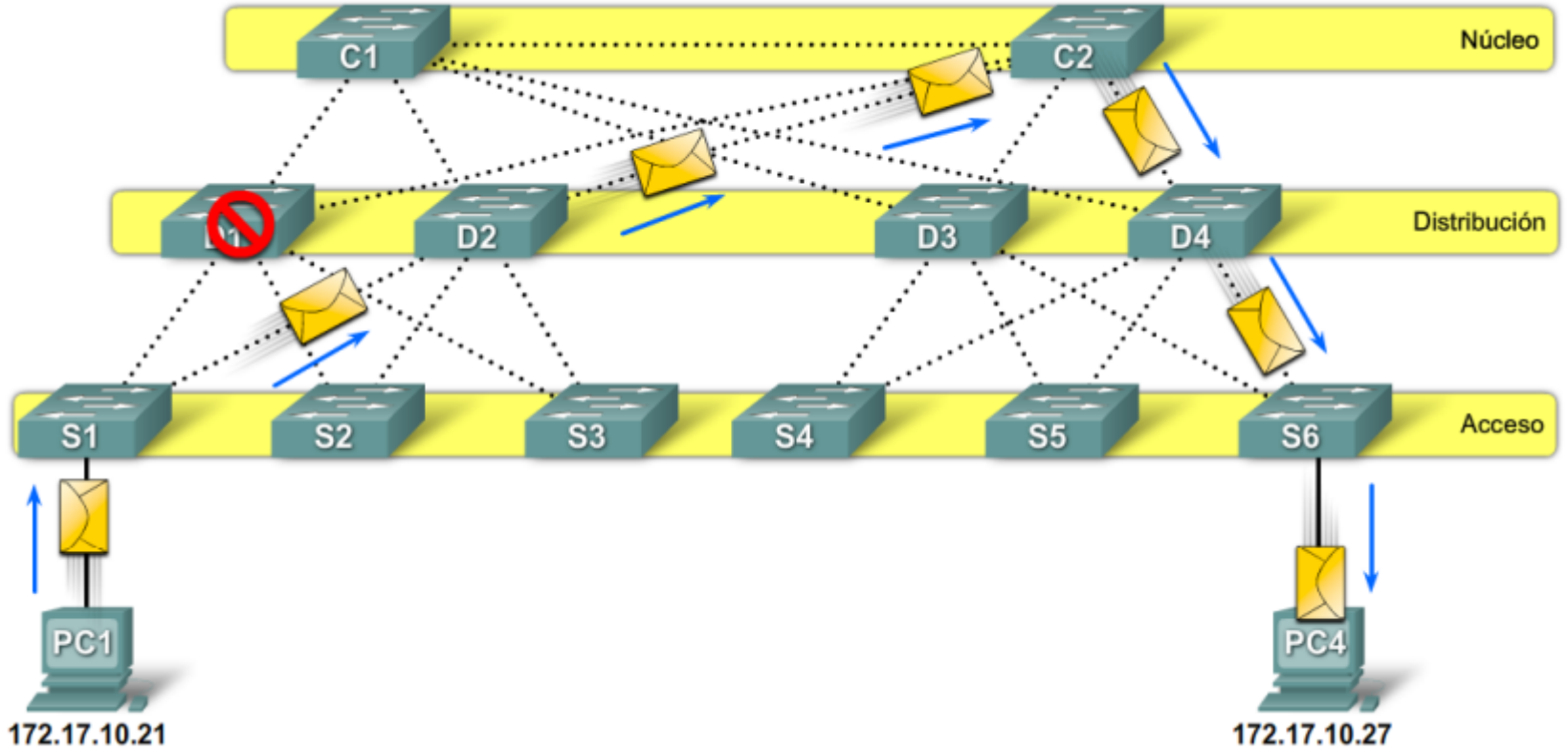
### Fallo de un enlace



# Redes Virtuales. VLAN

## Spanning Tree Protocol

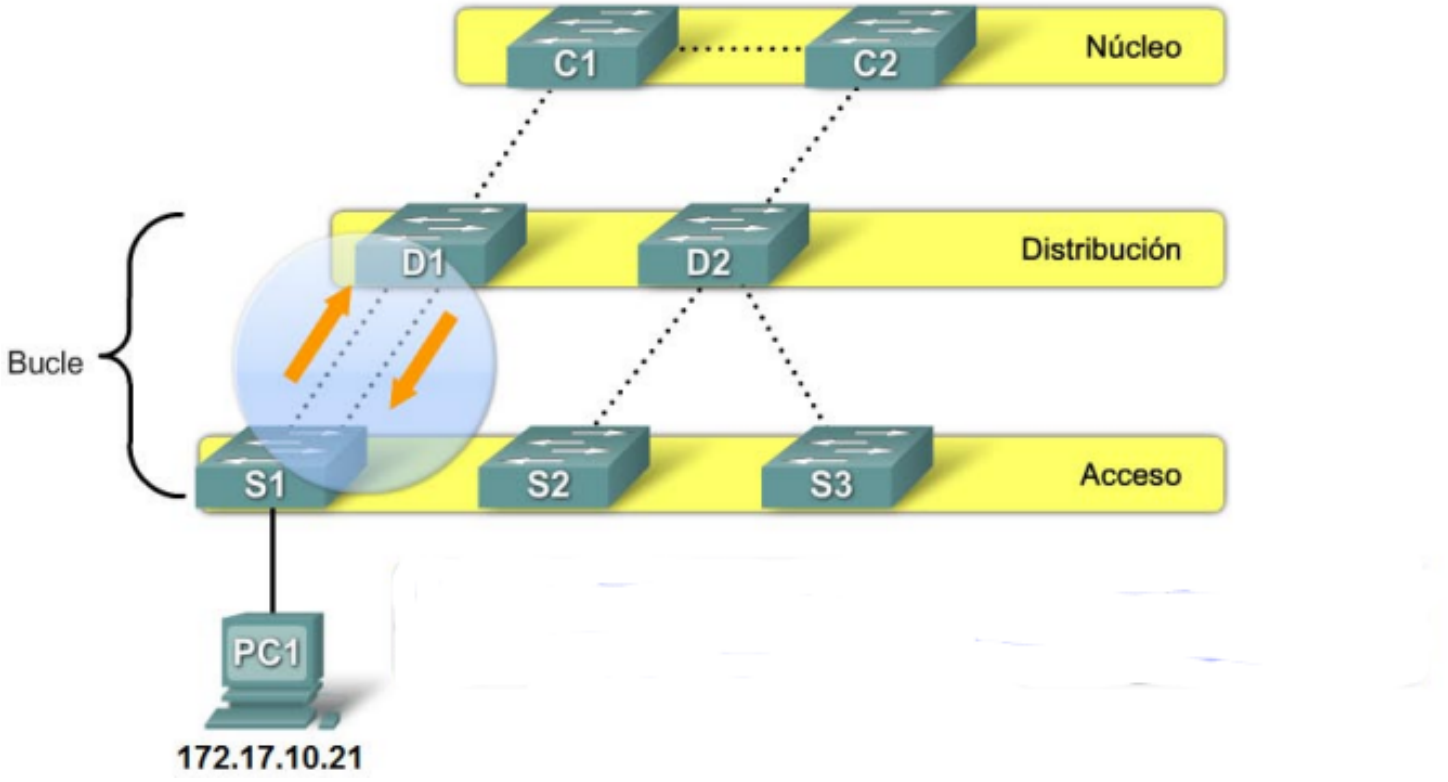
### Fallo de un dispositivo



# Redes Virtuales. VLAN

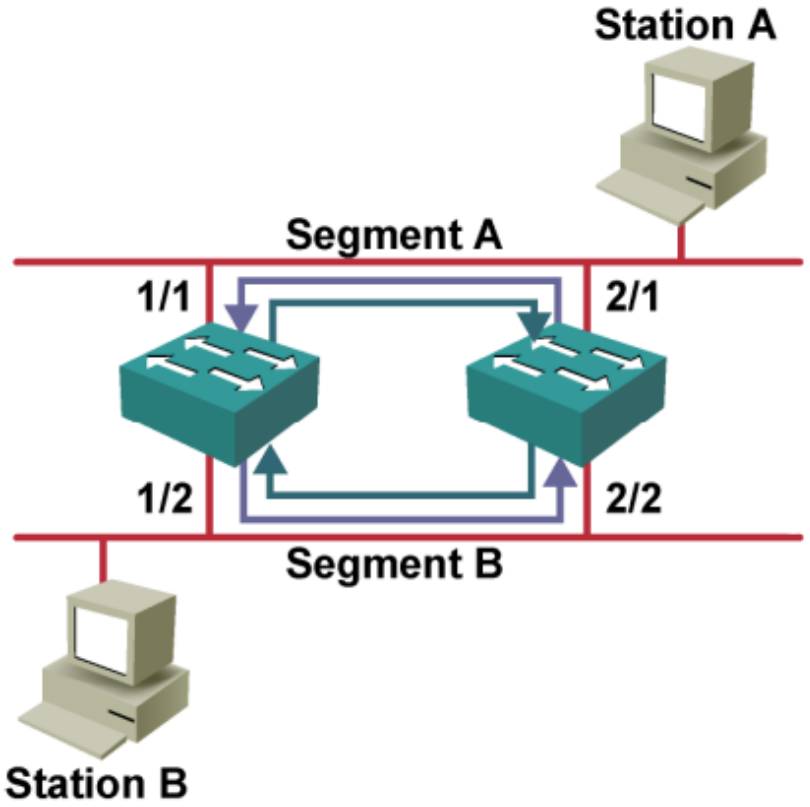
## Spanning Tree Protocol

### Bucles en el armario de cableado



# Redes Virtuales. VLAN

## Spanning Tree Protocol




### Bucles en el armario de cableado

- Los bucles siempre ocurrirán cuando exista un camino redundante entre varios switches
- El segmento B recibe una trama duplicado y provoca inconsistencias en las tablas CAM de ambos switches
- Ningún switch se da cuenta de la existencia del otro, por lo que se envían tramas constantemente

# Redes Virtuales. VLAN

## Spanning Tree Protocol

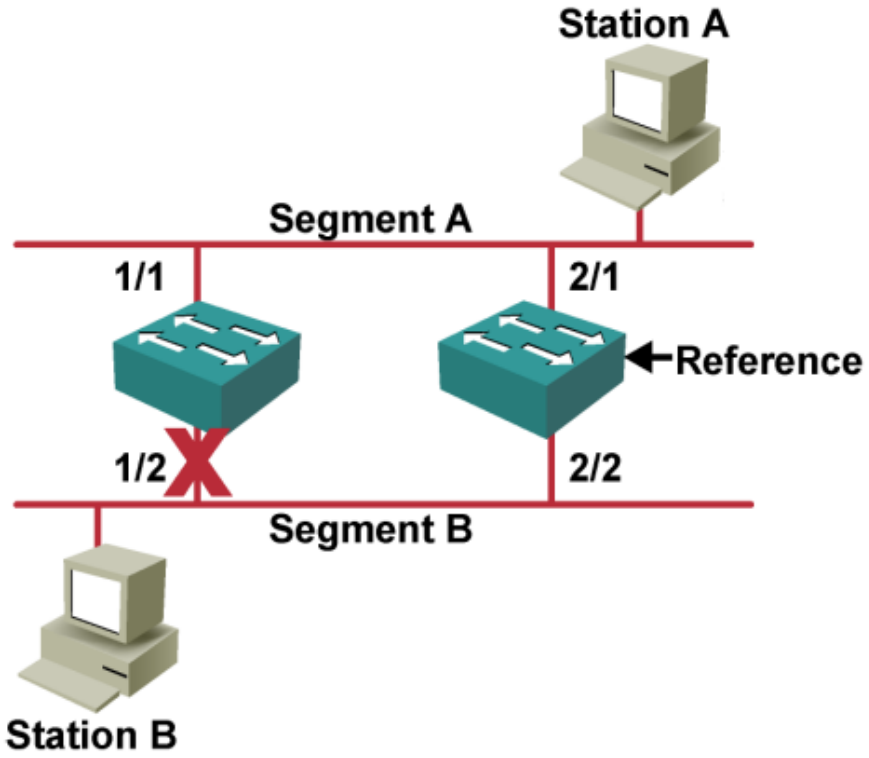
Con redundancia, podemos encontrar problemas como

- Inestabilidad de direcciones ethernet, al alcanzar una misma dirección por puertos distintos
- Tormenta de broadcast

El STP, es un protocolo de nivel 2, utilizado para evitar bucles en la capa de acceso, definido en el estándar 802.1d

# Redes Virtuales. VLAN

## Spanning Tree Protocol




- STP elige un punto de referencia en la red, calcula todos los caminos redundantes y selecciona uno para el envío de tráfico, bloqueando el resto
- Crea un solo camino entre dos puntos de la LAN
- Utiliza STA (Spanning Tree Algorithm)
- En caso de fallo, vuelve a ejecutar el proceso

# Redes Virtuales. VLAN

## Spanning Tree Protocol

El STA, designa un único switch como puente raíz (**RB**) y lo utiliza como punto de partida para todos los cálculos de rutas

El **RB**, se escoge a través de un proceso de selección, se intercamban ptramas **BPDU** y el switch que podea el menor **BID** (Bridge ID), será el puente raíz

Una vez elegido el puente raíz, se calcula la ruta más corta hacia el puente raíz, para ello, se consideran los costos de la ruta y el puerto

# Redes Virtuales. VLAN

## Spanning Tree Protocol

### El BID contiene

- Prioridad de puerto, valor que puede personalizarse y puede influir sobre la elección del switch raíz,  está comprendido entre 1 y 65536 y el valor por defecto es 32768
- ID del sistema extendido, contiene el valor de la VLAN con la que está asociada la BPDU
- Dirección ethernet, si no se modifica la prioridad por defecto, la menor dirección ethernet, será la elegida para el switch root
- La prioridad inicial del switch, será la suma de la prioridad de puerto y la VLAN inicial (32768 + 1)

# Redes Virtuales. VLAN

## Spanning Tree Protocol

### Las mejores rutas al puente raíz

- La determinación de ruta, se determina mediante la suma de los costos individuales de los puertos que atraviesan hasta el puente raíz
- Los costos de los puertos, se determinan pr la velocidad a la que funcionan los mismos

| Velocidad | Costo |
|---|---|
| 10 Mb/s | 100 |
| 100 Mb/s | 19 |
| 1 Gb/s | 4 |
| 10 Gb/s | 2 |

# Redes Virtuales. VLAN

## Spanning Tree Protocol

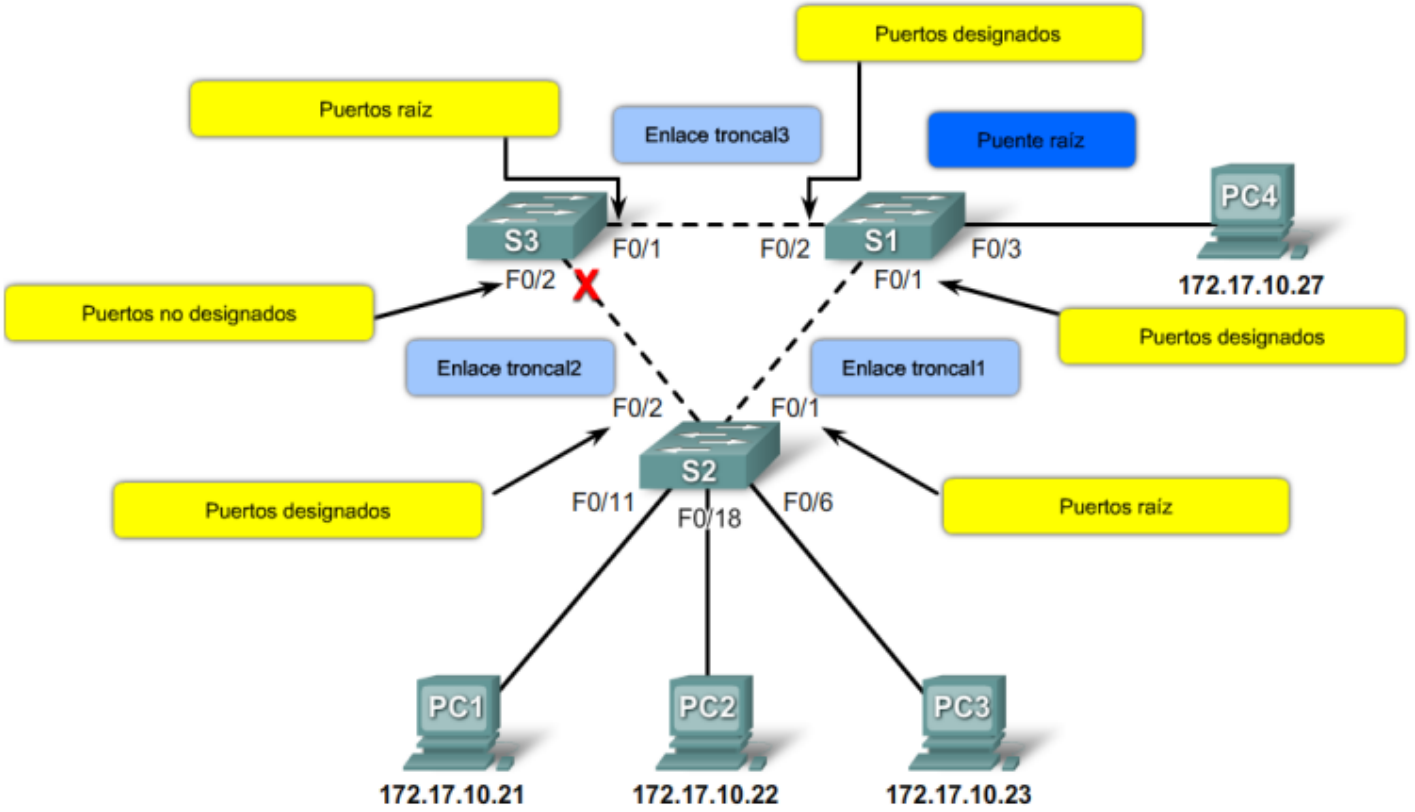
### Funciones de los puertos

- **Puerto raíz (RP)**, existe en los switches no raíz y es el puerto del switch con mejor camino hacia el switch raíz
- **Puerto designado (DP)**, en el switch raíz, todos los puertos son designados, para el resto, es el que envía y recibe tráfico, solo se permite un puerto designado por segmento
- **Puerto no designado**, es el puerto del switch que queda bloqueado, estos, son los que evitan la generación de bucles
- **Puerto deshabilitado**, es aquel que está administrativamente desconectado y no participa del proceso STA

# Redes Virtuales. VLAN

## Spanning Tree Protocol

Las funciones de los puertos, describen su relación en la red con el puente raíz



# Redes Virtuales. VLAN

## Spanning Tree Protocol

### Elección del switch raíz

- Inicialmente, cada switch se considera raíz y el ID raíz, coincide con el BID local
- Todos los switches de un dominio de broadcast participan en el proceso de elección, al iniciarse, envían tramas BPDU con el BID y el ID raíz cada 2 segundos
- Si el ID raíz de la BPDU recibida es menor que el ID local, este switch, actualiza actualiza su ID raíz con la identificación del switch adyacente, indicando quien es el switch raíz en las siguientes BPDU
- STP, determina un switch como raíz, todos los interfaces del switch, están en estado de envío.

# Redes Virtuales. VLAN

## Spanning Tree Protocol

### Elección del puerto raíz

- Cada uno de los demás switches que no son raíz, deben identificar su posición en la red en relación al switch raíz
- Se selecciona un puerto raíz en cada switch, apuntando al switch raíz, en función del coste de la ruta, el puerto que tenga mejor coste, será el puerto raíz y estará en estado de envío

# Redes Virtuales. VLAN

## Spanning Tree Protocol

### Elección del puerto designado

- Los switches, eligen solo un puerto designado para cada segmento, basandose en el menor coste hacia el switch raíz
- Cuando ujn switch, recibe un coste hacia el raíz por un puerto mayor al que tiene, asume el rol de puerto designado

# Redes Virtuales. VLAN

## Spanning Tree Protocol

Para facilitar el aprendizaje de spanning tree, cada puerto del switch, sufre una transición a través de 5 estados y 3 temporizadores

- **Bloqueo**, es un puerto no designado y no participa en el envío de tráfico, recibe tramas BPDU
- **Escuchar**, el puerto, envía y recibe tramas BPDU e informa a los switches adyacentes que se prepara para participar en STP
- **Aprender**, comienza a llenar la tabla de direcciones ethernet
- **Enviar**, se considera parte de la topología activa, envía y recibe tramas BPDU
- **Deshabilitado**, bloqueado por el administrador y no participa de STP

# Redes Virtuales. VLAN

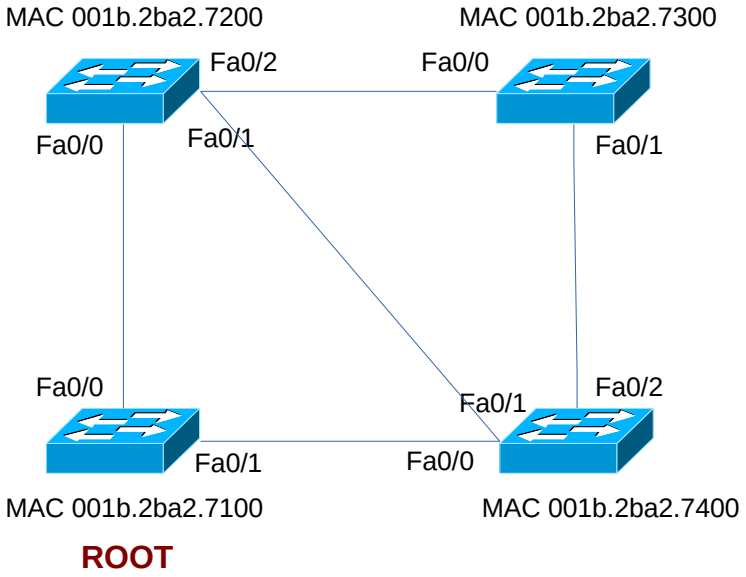
## Spanning Tree Protocol

| | Envía Frames | Aprende MAC | |
|---|---|---|---|
| Blocking (20s) | NO | NO | Estable |
| Listening (15s) | NO | NO | Transitorio |
| Learning (15s) | NO | SÍ | Transitorio |
| Forwarding | SÍ | SÍ | Estable |
| Disabled | NO | NO | Estable |

# Redes Virtuales. VLAN

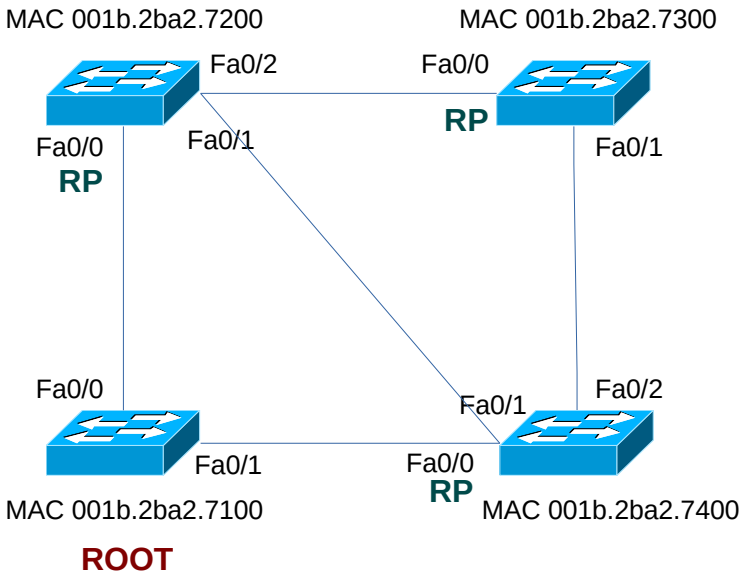
## Spanning Tree Protocol

- Elección del switch root



# Redes Virtuales. VLAN

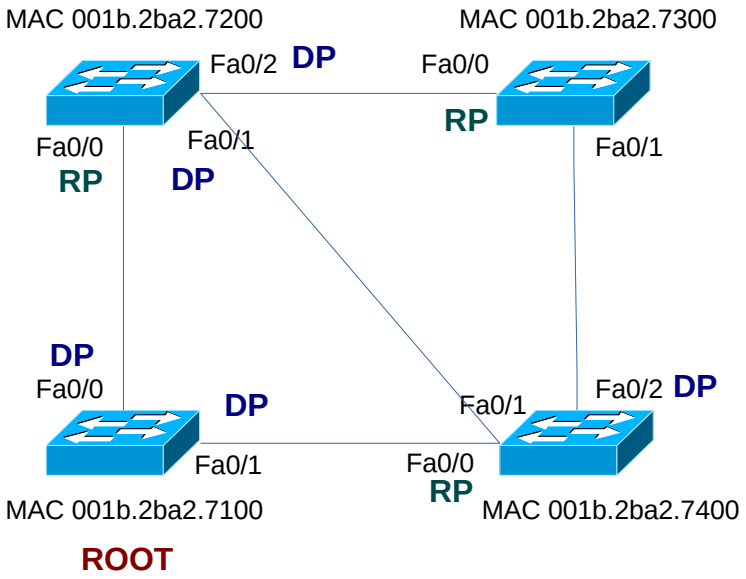
## Spanning Tree Protocol




- Elección del switch root (BID mas baja)
- Elección del root port (RP) para el resto del switch

# Redes Virtuales. VLAN

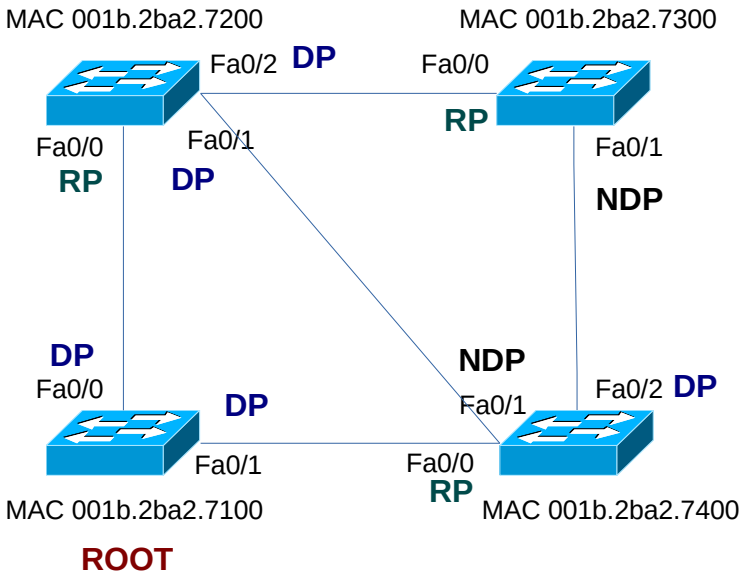
## Spanning Tree Protocol




- Elección del switch root (BID mas baja)
- Elección del root port (RP) para el resto del switch
- Elección del designated port (DP) para todos los switches que no son root

# Redes Virtuales. VLAN

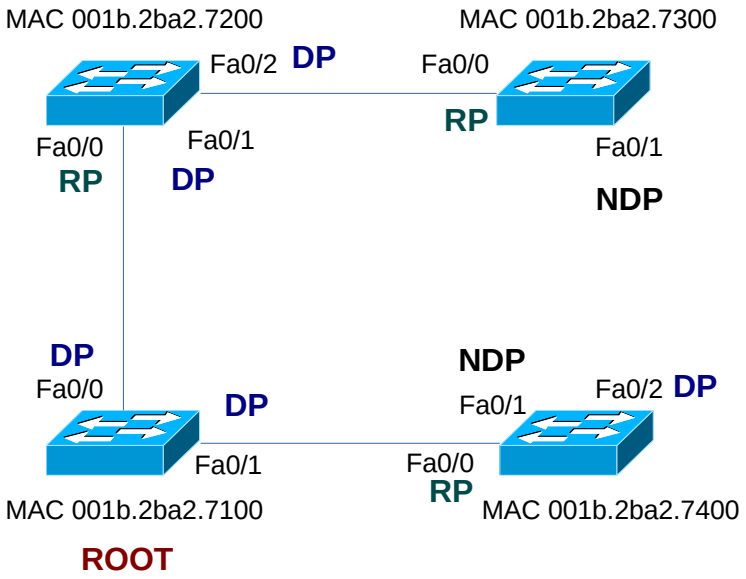
## Spanning Tree Protocol




- Elección del switch root (BID mas baja)
- Elección del root port (RP) para el resto del switch
- Elección del designated port (DP) para todos los switches que no son root
- El resto de puertos, serán no designate ports (NDP), y serán los puertos en estado de blocking

# Redes Virtuales. VLAN

## Spanning Tree Protocol




- Elección del switch root (BID mas baja)
- Elección del root port (RP) para el resto del switch
- Elección del designated port (DP) para todos los switches que no son root
- El resto de puertos, serán no designate ports (NDP), y serán los puertos en estado de blocking

# Redes Virtuales. VLAN

## Spanning Tree Protocol

Cuando el puerto de un switch se configura como **portfast**, se establece como puerto de acceso y la transición del estado de bloqueo al de envio, es inmediata

- Evita los estados de Listening y Learning
- Solo hay que hacerlo en puertos de acceso

# Redes Virtuales. VLAN

## Spanning Tree Protocol

Si una interfaz portfast recibe una trama BPDU, si está activo **BPDU Guard**, STP pone el puerto en estado de bloqueo

- Evita lproblemas de seguridad en la LAN
- Usado para impedir que se conecten switches que puedan alterar el switch root

# Redes Virtuales

## Seguridad de puerto

# Redes Virtuales. VLAN

## Seguridad de puerto

En algunos entornos, la red debe estar asegurada para controlar que hosts deben tener acceso

Los switches, tienen una característica que controla las direcciones ethernet asignadas a cada puerto

Estas pueden ser configuradas explicitamente a de forma dinámica a través del tráfico entrante en ese puerto

```
SW1(config-if)#switchport port-security maximun 10
SW1(config-if)#switchport port-security mac-address 0000.0000.0000
```

# Redes Virtuales. VLAN

## Seguridad de puerto

Hay que definir como actúa una interfaz con seguridad de puerto activa, cuando ocurre un intento de violación.

- **Shutdown**, el puerto se pone en errdisable y tendrá que ser habilitado manualmente
- **Restrict**, el puerto permanece activo, pero los paquetes origen de la violación, son eliminados
- **Protect**, el puerto permanece activo, pero los paquetes origen de la violación, son eliminados y no que constancia de nada

# Redes Virtuales. VLAN

## Seguridad de puerto

### Ejemplo de configuración

```
SW1(config)#interface g0/1
SW1(config-if)#switchport access vlan 10
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security violation shutdown
SW1(config-if)#spanning-tree portfast
```

# Redes Virtuales. VLAN

## Seguridad de puerto

El estado del puerto puede verse y en el caso de que se cumpla la condición restrict o protect, se deberán borrar las direcciones ethernet que no son permitidas

```
SW1#show port-security interface fastethernet 0/1
SW1#clear port-security dynamic [address 0000.1111.2222 | interface f0/1]
```


Telefónica