Implementando Seguridad VLAN

Capítulo 3

3.1 Segmentación VLAN

3.2 Implementación de VLAN

3.3 Seguridad y Diseño de VLAN

3.4 Resumen

Capítulo 3: Objetivos

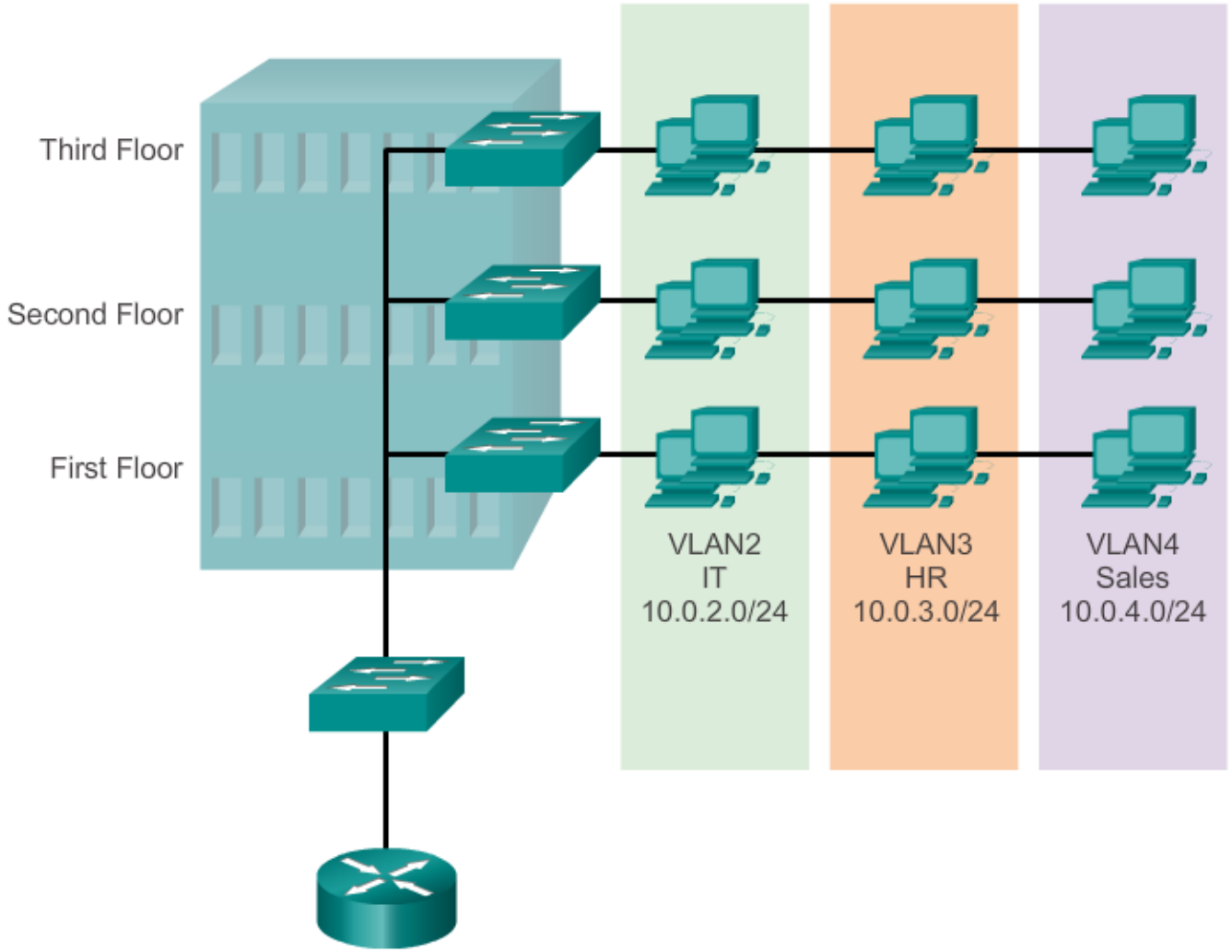
- Explicar el propósito de las VLAN en las redes conmutadas.
- Analizar cómo un switch reenvía tramas basado en configuración de VLAN en ambientes multi-conmutados.
- Configurar un puerto de switch para ser asignado a una VLAN basado en requerimientos.
- Configurar un puerto troncal en un switch LAN.
- Configurar Dynamic Trunk Protocol (DTP).
- Solucionar problemas de configuración de VLAN y troncales en una red conmutada.
- Configurar características de seguridad para mitigar ataques en un entorno segmentado por VLAN.
- Explicar las mejores prácticas de seguridad en un entorno segmentado por VLAN.

Definiciones de VLAN

- VLAN (LAN virtual) es una partición lógica de una red de capa 2.
- Múltiples particiones pueden ser creadas, permitiendo que múltiples VLANs co-existan.
- Cada VLAN es un dominio de broadcast, usualmente con su propia IP de red.
- Las VLANS están mutuamente aisladas y los paquetes solamente pueden pasar entre ellas a través de un router.
- Las particiones de red de capa 2, se lleva dentro de un dispositivo de capa 2, usualmente un switch.
- Los hosts agrupados dentro de una VLAN no son consientes de la existencia de la VLAN.

Descripción de VLANs

Definiciones de VLAN



Beneficios de las VLANs

- Seguridad
- Reducción de costos
- Mejor rendimiento
- Reduce el tamaño de los dominios de broadcast
- Mejora la eficiencia del personal de TI
- Protección y administración de aplicaciones más simple

Tipos de VLANs

- VLAN de datos
- VLAN por defecto
- VLAN Nativa
- VLAN de Administración

Tipos de VLANs

VLAN 1

```
Switch# show 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
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

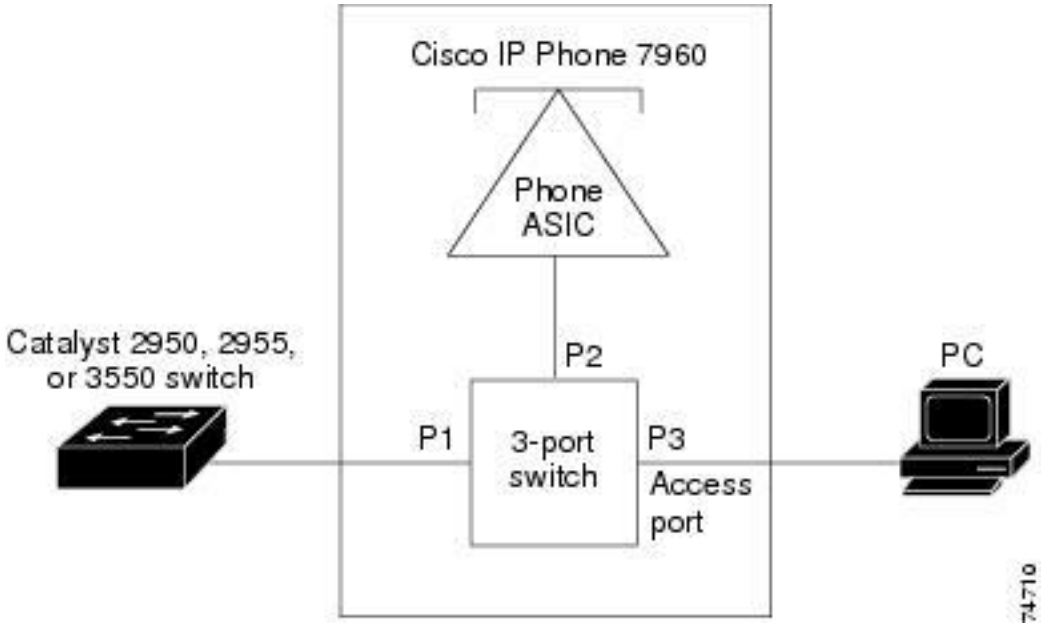
- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

VLANs de Voz

- El tráfico de VoIP es sensible al tiempo y requiere:
  - Ancho de banda asegurado para asegurar calidad de servicio
  - Prioridad de transmisión sobre otros tipos de tráfico de red
  - Habilidad de ser ruteado alrededor de áreas congestionadas en la red
  - Retardo de menos de 150 ms a través de la red
- La característica de VLAN de voz permite a los puertos de acceso llevar tráfico voz IP desde un teléfono IP.
- El switch se puede conectar a un teléfono IP Cisco 7960 y llevar tráfico de voz IP.
- Debido a que la calidad del sonido de una llamada por teléfono IP se puede deteriorar si los datos se envían de forma desigual, el switch debe soportar calidad de servicio (QoS).

VLANs Voz

- Los teléfonos IP Cisco 7960 IP contienen tres puertos de switch integrados de 10/100:
  - Port 1 conecta al switch.
  - Port 2 es una interfaz interna de 10/100 que lleva el tráfico.
  - Port 3 (puertos acceso) conecta a un PC u otro dispositivo.



VLAN Trunks

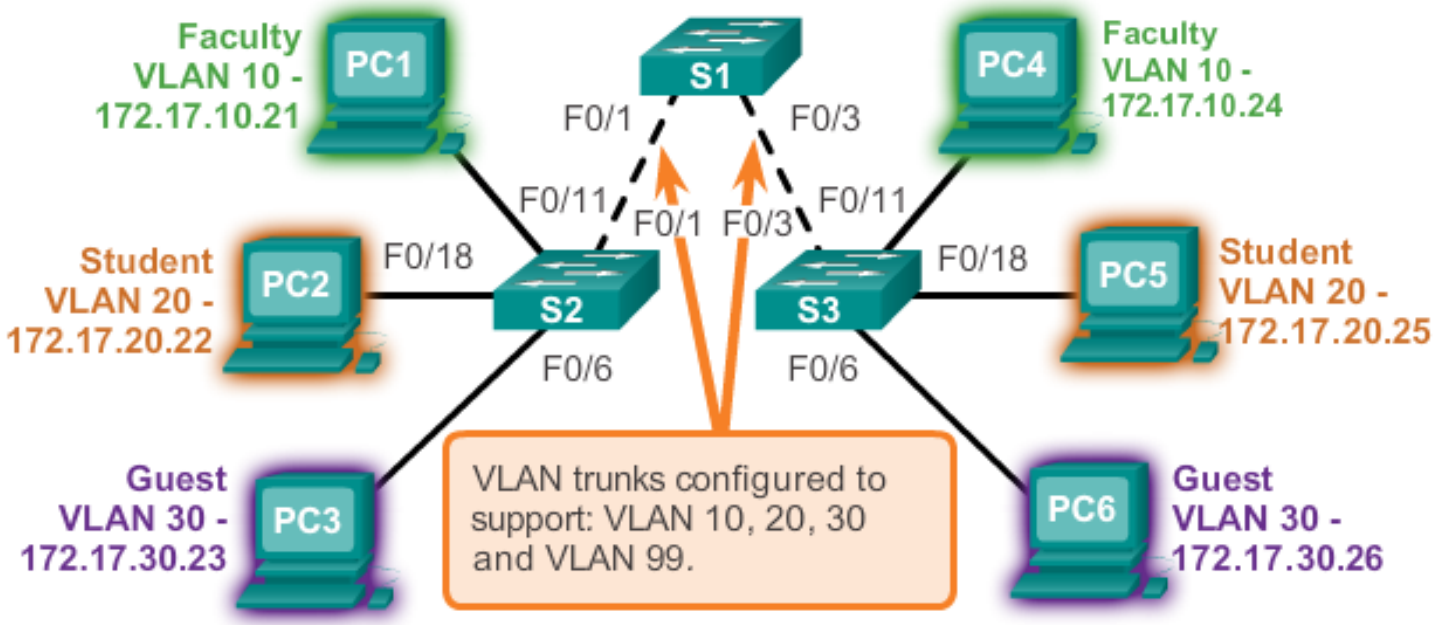
- Un troncal VLAN lleva más de una VLAN.
- Usualmente establecido entre switch para que dispositivos de la misma VLAN se puedan comunicar, aún si están conectados a diferentes switches.
- Un troncal VLAN no se asocia a ninguna VLAN. Tampoco se usa el puerto troncal para establecer el enlace troncal.
- Cisco IOS soporta IEEE802.1q, un popular protocolo de VLAN trunk.

VLANs en un entorno multi-conmutado

VLAN Trunks

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.



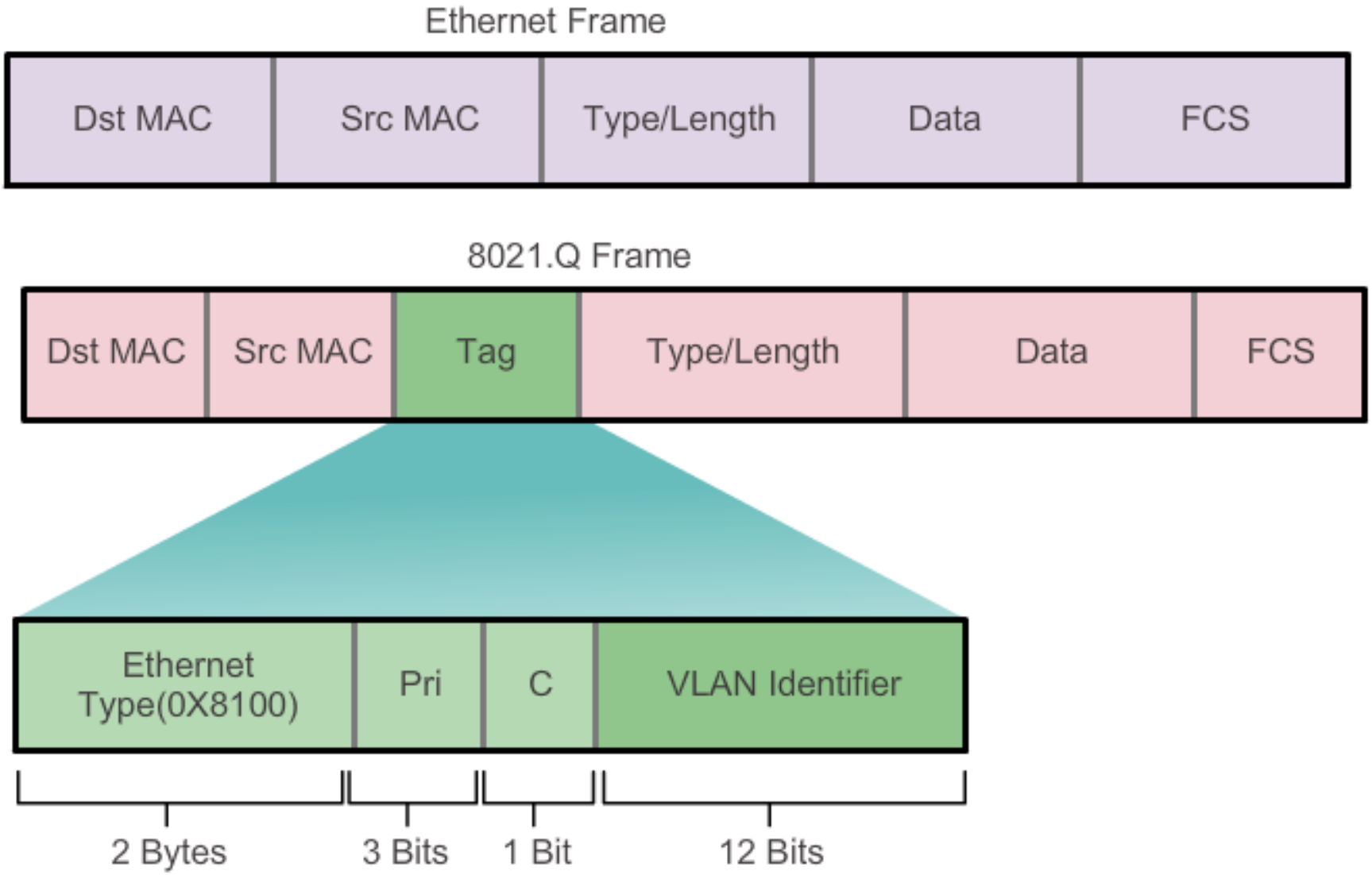
Controlando dominios de Broadcast con VLANs

- Las VLANs pueden ser usadas para limitar el alcance de las tramas de broadcast.
- Una VLAN es un dominio de broadcast por si misma.
- Por lo tanto, una trama broadcast enviada por un dispositivo en una VLAN específica es reenviada solamente dentro de esa VLAN.
- Esto ayuda a controlar el alcance de las tramas de broadcast y su impacto en la red.
- Tramas unicast y multicast son reenviadas también dentro de la VLAN originaria.

Etiquetado de tramas Ethernet para la identificación de VLAN

- El etiquetado de tramas es usado para transmitir apropiadamente tramas de múltiples VLAN a través de un enlace troncal.
- Los Switches etiquetarán las tramas la VLAN a la cual ellas pertenecen. Existen diferentes protocolos, siendo el **IEEE 802.1q** uno muy popular.
- Los protocolos definen la estructura del etiquetado agregado al encabezado de la trama.
- Los switches agregarán etiquetas de VLAN a las tramas antes de ponerlas en el enlace troncal y quita la etiqueta antes de reenviar la trama a través de puertos no troncales.
- Una vez etiquetada correctamente, las tramas pueden atravesar varios switches vía enlaces troncales y todavía ser reenviada dentro de la VLAN correcta al destino.

Etiquetado de tramas Ethernet para la identificación de VLAN

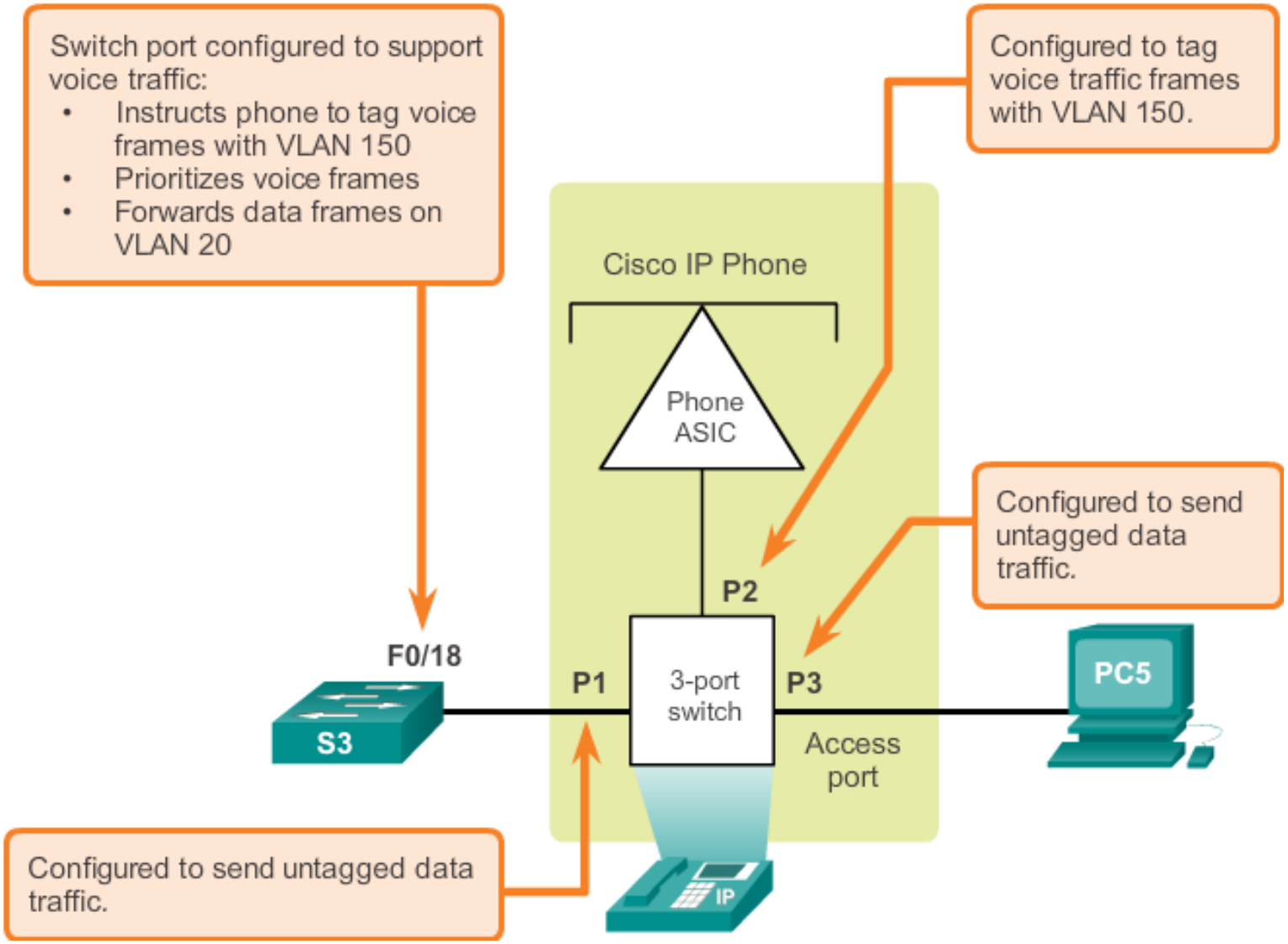


VLANs Nativas y etiquetado 802.1q

- Una trama que pertenece a la VLAN nativa no será etiquetada.
- Una trama que es recibida sin etiqueta permanecerá sin etiqueta y será puesta en la VLAN nativa cuando se reenvíe.
- Si no hay puertos asociados a la VLAN nativa y no hay otros puertos troncales, una trama no etiquetada será descartada.
- En switchs Cisco, La VLAN nativa es la VLAN 1 por defecto.

VLANs en un entorno multi-conmutado

Etiquetado de VLAN de Voz



Rangos de VLAN en Switchs Catalyst

- Los Switch Catalyst serie 2960 y 3560 soportan sobre 4,000 VLANs.
- Estas VLANs están divididas en 2 categorías:
- Rango de **VLANs normales**
  - Números de VLAN desde **1 a 1005**.
  - Configuraciones almacenadas en el archivo vlan.dat (en la flash).
  - VTP pueden aprender y almacenar solamente rango de VLANs normales.
- Rango de **VLANs extendidas**
  - Números de VLAN desde **1006 a 4096**.
  - Configuraciones almacenadas en el running-config (en la NVRAM).
  - VTP no aprende VLANs extendidas.

Asignación de VLAN

Creando una VLAN

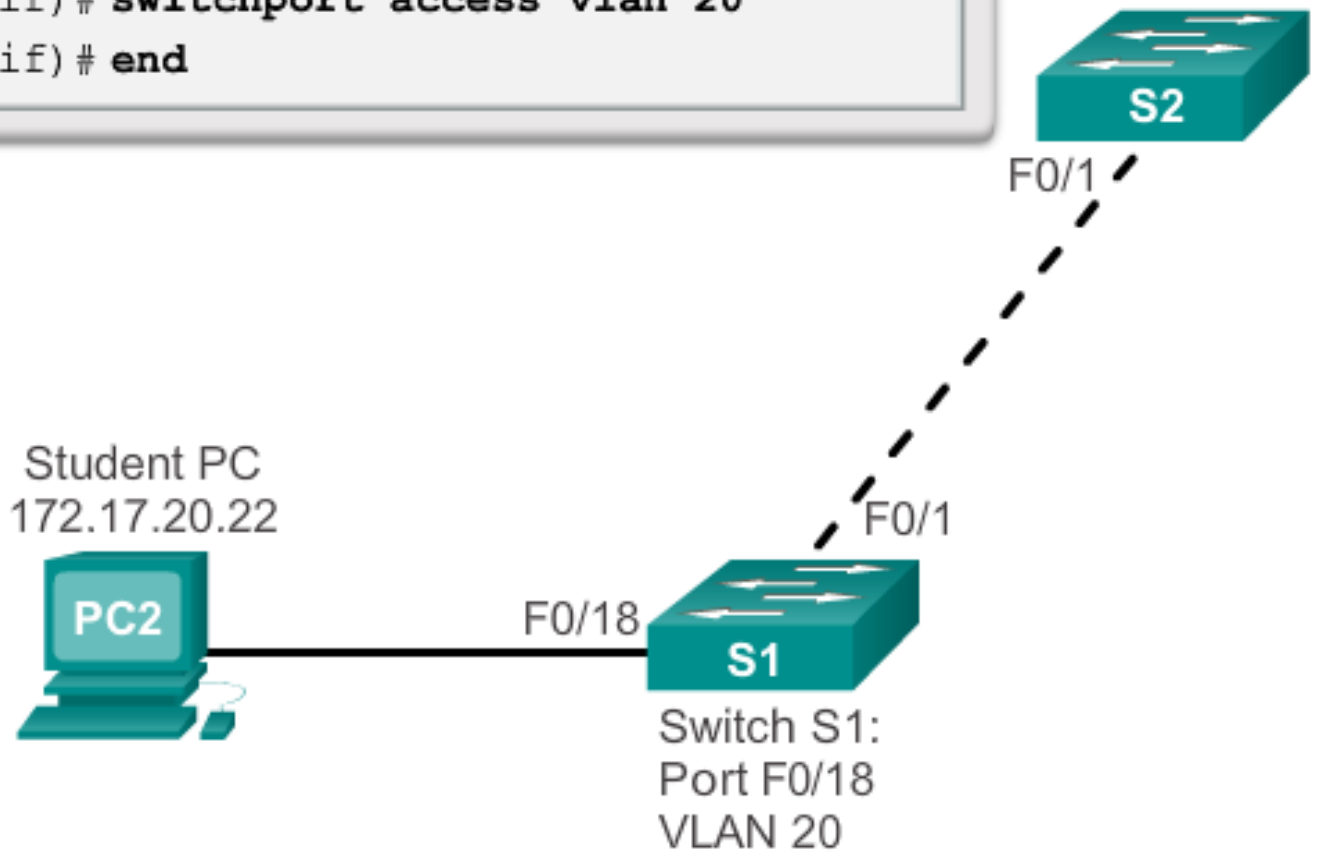
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan_id`
Specify a unique name to identify the VLAN.	`S1(config)# name vlan_name`
Return to the privileged EXEC mode.	`S1(config)# end`

Asignando Puertos a VLANs

Cisco Switch IOS Commands	
Enter global configuration mode.	S1 # **configure terminal**
Enter interface configuration mode	S1(config) # **interface** *interface_id*
Set the port to access mode.	S1(config-if) # **switchport mode access**
Assign the port to a VLAN.	S1(config-if) # **switchport access vlan** *vlan_id*
Return to the privileged EXEC mode.	S1(config-if) # **end**

Asignando Puertos a VLANs

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



Asignación de VLAN

Cambiando pertenencia de puerto a VLAN

```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show 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
                                  Gi0/1, Gi0/2
20   student              active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Asignación de VLAN

Cambiando pertenencia de puerto a VLAN

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show 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, Fa0/12, Fa0/1
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/
                                     Gi0/2
20   student              active     Fa0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Asignación de VLAN

Borrando VLANs

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# 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, Fa0/12, Fa0/13
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                    Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Asignación de VLAN

Verificando Información de VLAN

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----------------- ------ ------ -------- ---- -------- ------
20  enet 100020 1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0

S1#
```

Asignación de VLAN

Verificando Información de VLAN

```
S1#show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configurando enlace troncal IEEE 802.1q

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI.	S1(config)# **interface** *interface_id*
Force the link to be a trunk link.	S1(config)# **switchport mode trunk**
Specify a native VLAN for untagged 802.1Q trunks.	S1(config-if)# **switchport trunk native vlan** *vlan_id*
Specify the list of VLANs to be allowed on the trunk link.	S1(config-if)# **switchport trunk allowed vlan** *vlan-list*
Return to the privileged EXEC mode.	S1(config-if)# **end**

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

Reseteando el troncal al estado por defecto

Resetting Trunk Link Example

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
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)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Reseteando el troncal al estado por defecto

Return Port to Access Mode

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
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: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

Asignación de VLAN

Verificando la Configuración Troncal

Verifying Trunk Configuration

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
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: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Dynamic Trunking Protocol

Introducción a DTP

- Los puertos de switch pueden ser manualmente configurados para formar troncales.
- Los puertos de switch también pueden ser configurados para negociar y establecer un enlace troncal con un par conectado.
- Dynamic Trunking Protocol (DTP) es un protocolo para administrar la negociación troncal.
- DTP es un protocolo propietario Cisco y **está habilitado** por defecto en los switch Cisco Catalyst 2960 y 3560.
- Si el puerto en el switch vecino está configurado en un modo troncal que soporta DTP, él administra la negociación.
- La configuración por defecto de DTP para los switches Cisco Catalyst 2960 y 3560 es **`dynamic auto`.**

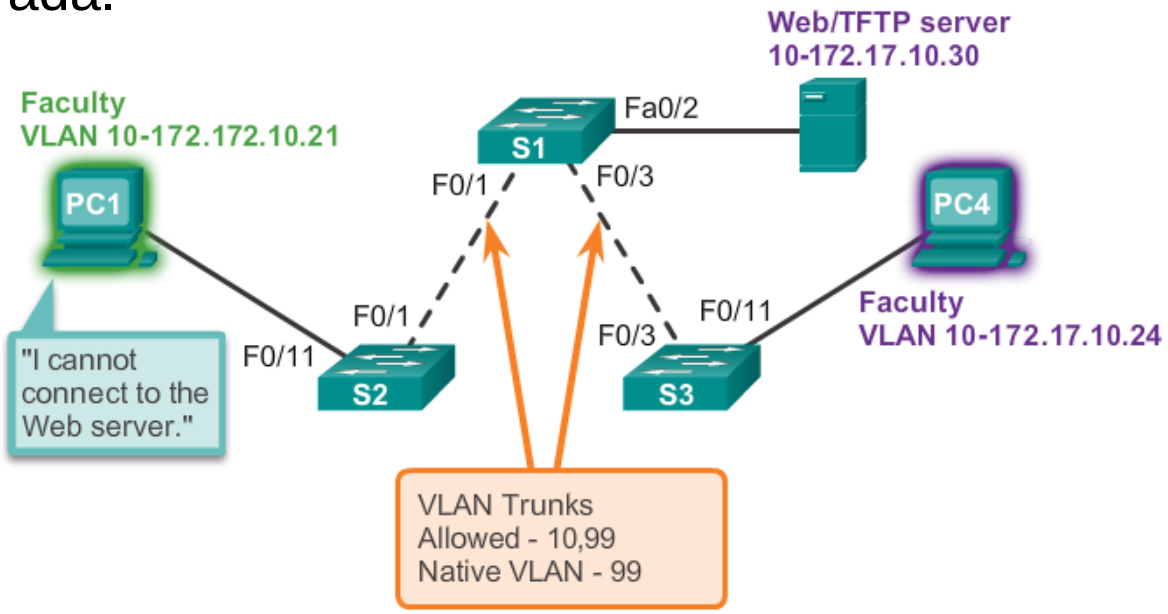
Modos de Negociación de Interfaz

- Cisco Catalyst 2960 y 3560 soportan los siguientes modos troncales:
  - switchport mode dynamic auto
  - switchport mode dynamic desirable
  - switchport mode trunk
  - switchport nonegotiate

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

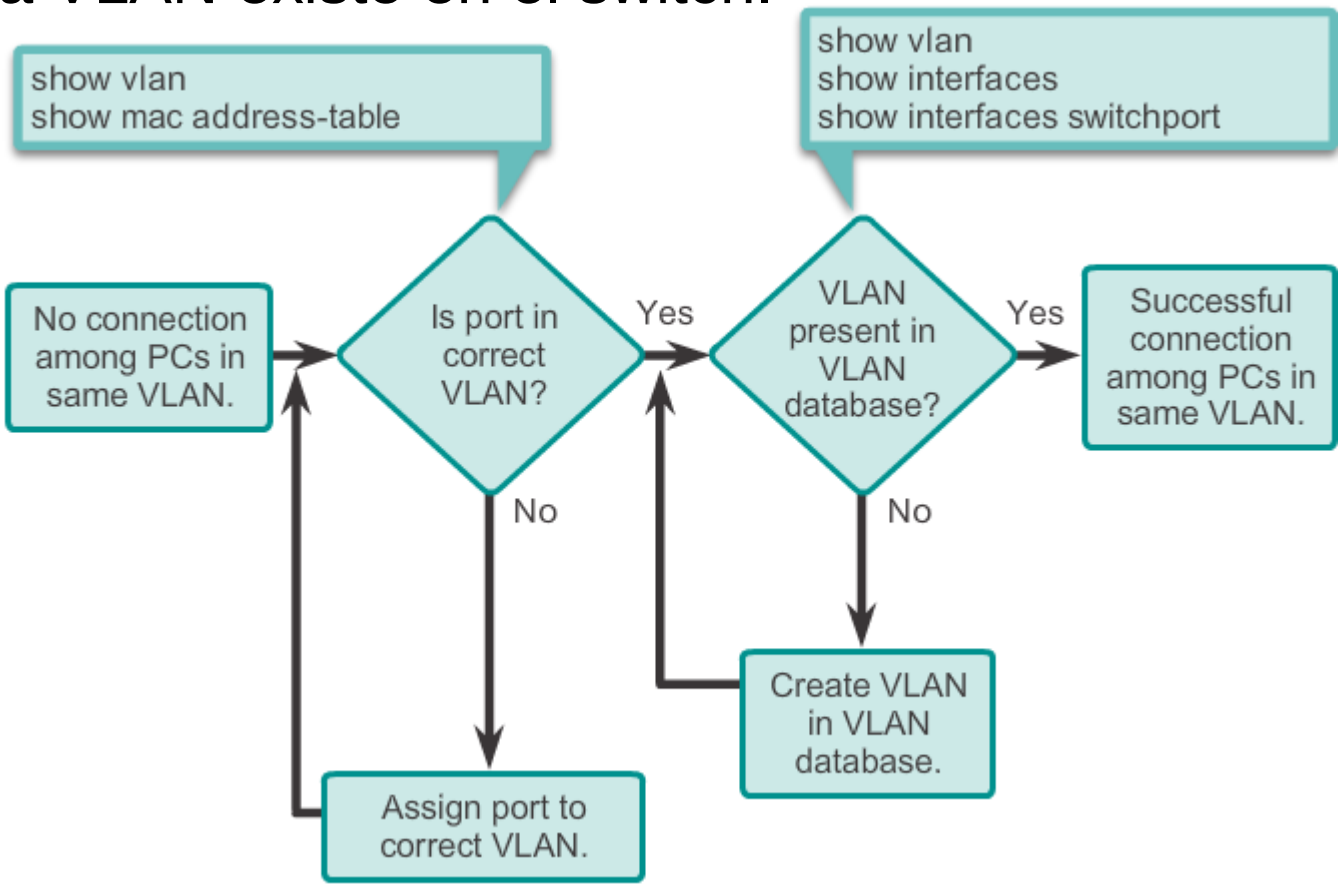
Abordando problemas con VLAN

- Es una práctica muy común asociar una VLAN con una red IP.
- Ya que diferentes rede IP sólo se pueden comunicar a través de un router, todos los dispositivos dentro de una VLAN deben ser parte de la misma red IP para comunicarse.
- En la imagen de abajo, el PC1 no puede comunicarse al servidor debido a que tiene una dirección IP errónea configurada.

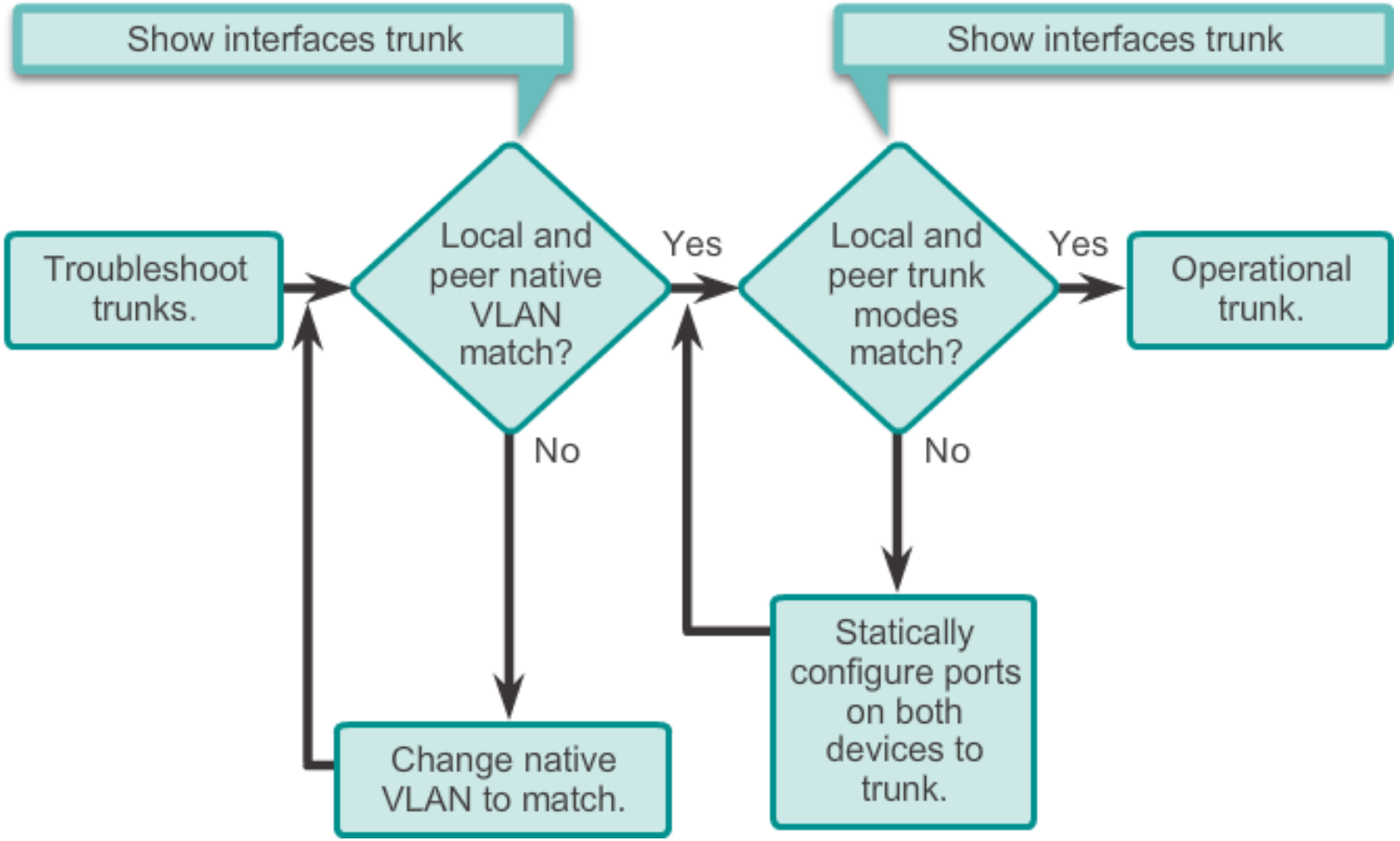


Missing VLANs

- Si todas las direcciones IP erróneas han sido resueltas pero los dispositivos aún no se pueden conectar, revisa si la VLAN existe en el switch.



Introducción a Troubleshooting de troncales



Problemas Comunes con Troncales

- Los problemas de troncales son usualmente asociados con configuraciones incorrectas.
- Los tipos más comunes de errores de configuración troncales son:
  1. Desajuste (mismatches) de VLAN Nativa
  2. Desajuste (mismatches) de modo Troncal
  3. VLANs permitidas (Allowed) en los troncales
- Si un problema es detectado, Las pautas de mejores prácticas recomendadas, se muestran en orden arriba.

Modos Mismatches (erróneos) de Troncales

- Si un puerto en un enlace troncal es configurado con un modo troncal que es incompatible con el puerto troncal del vecino, un enlace troncal falla de formarse entre los dos switches.
- Verifica el estado de los puertos troncales en los switches usando el comando **`show interfaces trunk.`**
- Para solucionar el problema, configura las interfaces con los modos troncales apropiados.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

Pauta de Diseño VLAN

- Mueve todos los puertos de la VLAN1 y asígnalos a una VLAN no usada.
- **`Shutdown`** todos los puertos del switch no usados.
- Separa el tráfico de administración del de datos.
- Cambia la VLAN de administración a otra VLAN que no sea la VLAN1. Lo mismo para la VLAN nativa.
- Asegúrate que sólo dispositivos en la VLAN de administración puedan conectarse a los switches.
- El switch debería aceptar sólo conexiones SSH.
- Deshabilita la autonegociación de puertos troncales.
- No uses modos auto o desirable en puertos del switch.