Implementando seguridad en VLAN

RAUL BAREÑO GUTIERREZ

Cisco | Networking Academy®
Mind Wide Open™

Objetivos

- Explicar el propósito de las VLAN en una red conmutada.
- Analizar el envió de las tramas basadas en la configuración de las VLAN en un entorno multi conmutado.
- Configurar el puerto del switch a asignar a una VLAN.
- Configure el puerto troncal en el switch LAN.
- Configurar el Protocolo Troncal dinámico (DTP).
- Solución de problemas y configuraciones de VLAN y troncales en una red conmutada.
- Configurar las características de seguridad para mitigar los ataques en el entorno de VLAN segmentado.

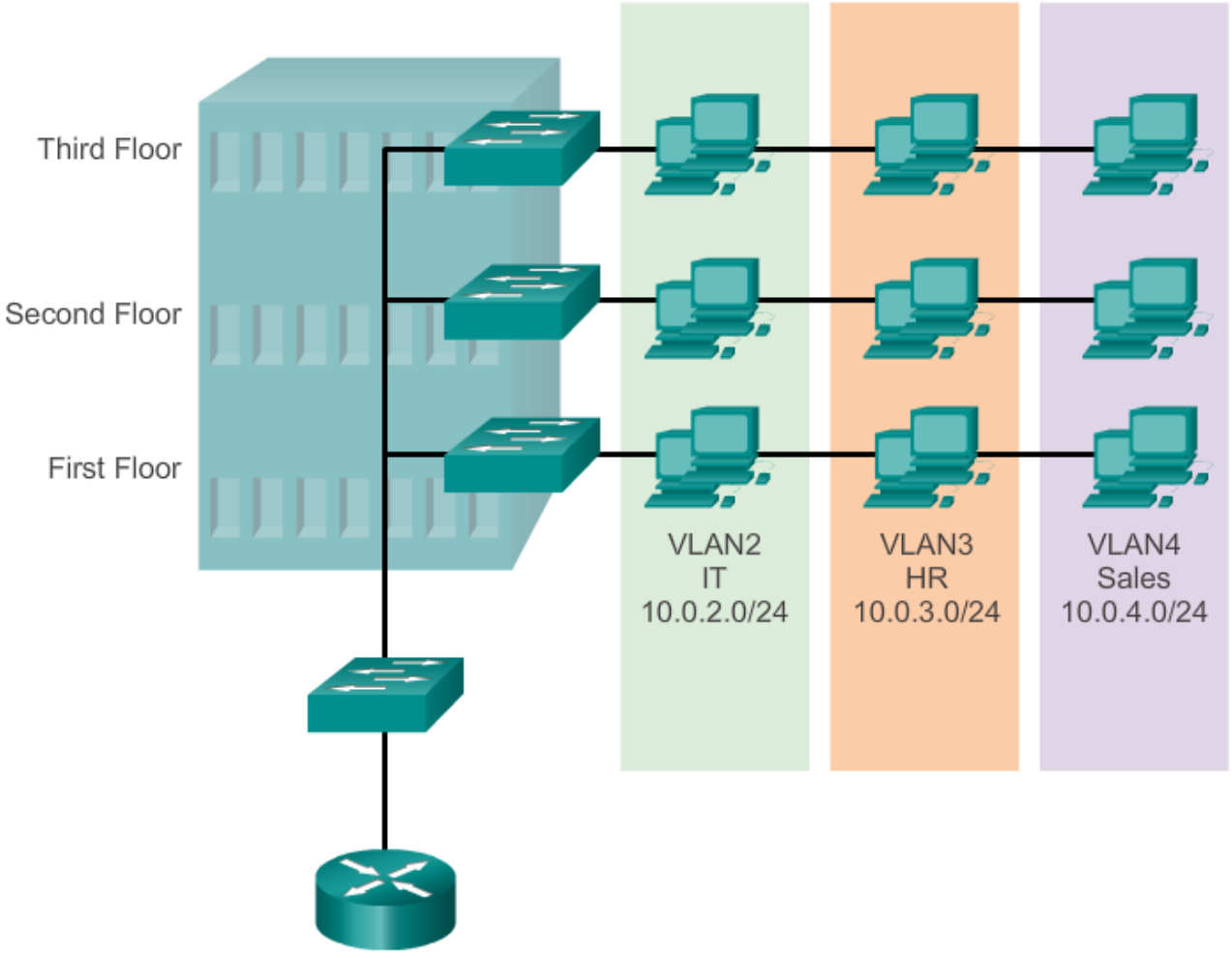
Definiciones de VLAN

- VLAN (Virtual LAN) es una partición lógica de una red de capa 2.

- Particiones múltiples pueden ser creadas, lo que permite múltiples VLANs coexistir.
- Cada VLAN es un dominio de broadcast, por lo general con su propia red IP.

- Las VLAN son mutuamente aisladas y sólo pueden pasar las tramas a través del router entre ellas.

Definiciones de VLAN



Ventajas de las VLAN

- Seguridad
- Reducción de costos
- Mejor rendimiento.
- Reducen los dominios de broadcast.
- Mejora de la eficiencia del personal de IT.
- Simplificación de los proyectos y la gestión de aplicaciones.

Tipos de VLAN

- VLAN de datos.
- VLAN predeterminada.
- VLAN Nativa.
- VLAN de Gestión o admin

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.

VLAN Voice

- El Tráfico de VoIP es sensible al tiempo y requiere:
- Buen ancho de banda mínimo para la calidad de voz.
- Prioridad de transmisión con otros tipos de tráfico de red
- Retardo de menos de 150 ms a través de la red

- Su función es permitir a los puertos de acceso transportar tráfico de voz IP desde un teléfono IP.

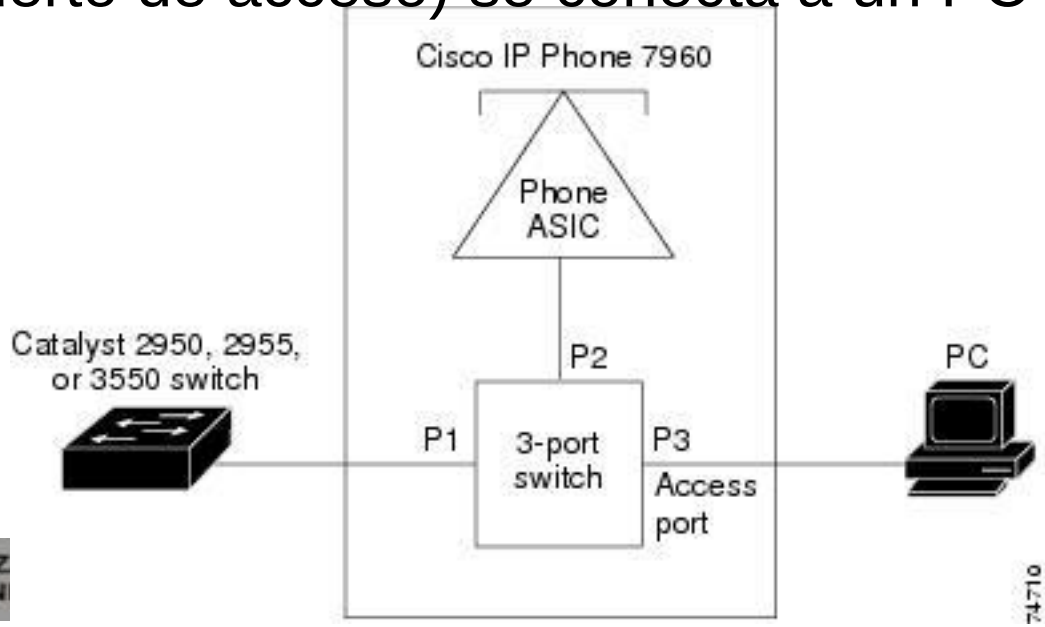
- Aplicar calidad de servicio (QoS)

VLAN Voice

- El telefono IP contiene un switch de tres puertos 10/100 integrado:

El puerto 1 se conecta al switch
El Puerto 2 es una interfaz interna que lleva el tráfico telefónico IP

El Puerto 3 (puerto de acceso) se conecta a un PC u otro dispositivo.



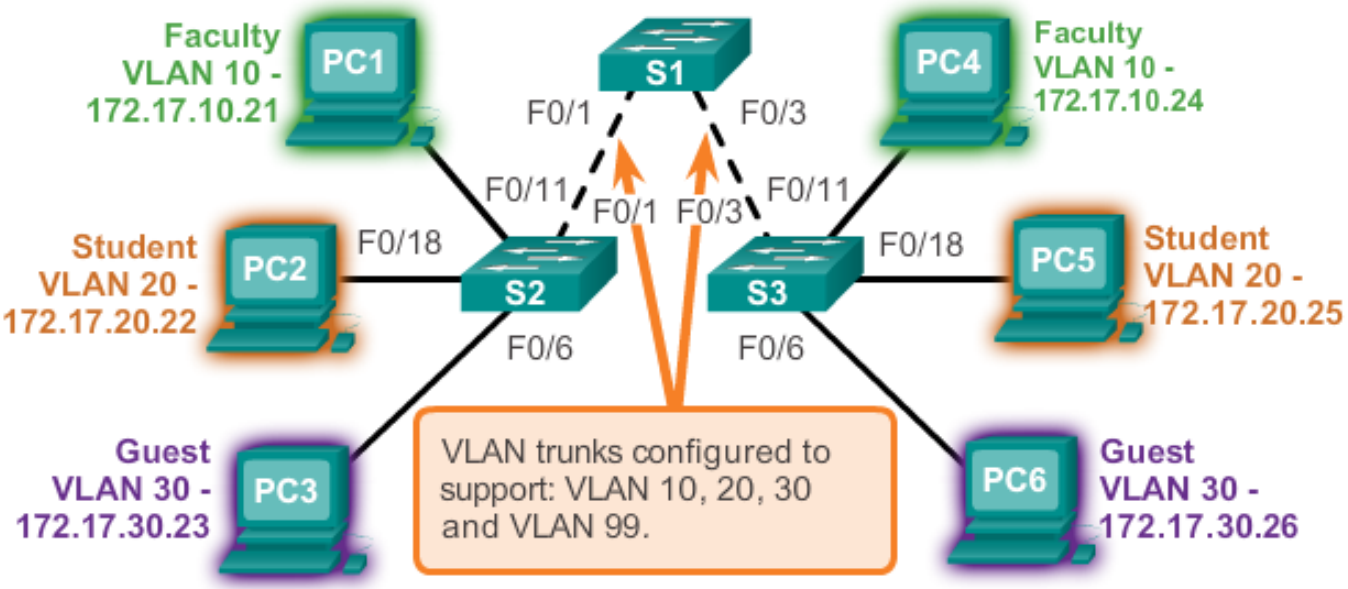
VLANs en un entorno multi-Switched? VLAN y troncales.

- Una puerto troncal lleva más de una VLAN.
- Se establecen entre switches; aunque físicamente estén conectados a diferentes switches.
- Un puerto troncal no está asociado a ninguna VLAN. Tampoco los puertos troncales utilizados para establecerse el enlace troncal.
- Cisco IOS soporta IEEE 802.1q, el protocolo troncal mas popular de las VLAN.

Troncales de VLAN o puertos

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.



El control de los dominios de broadcast con VLAN

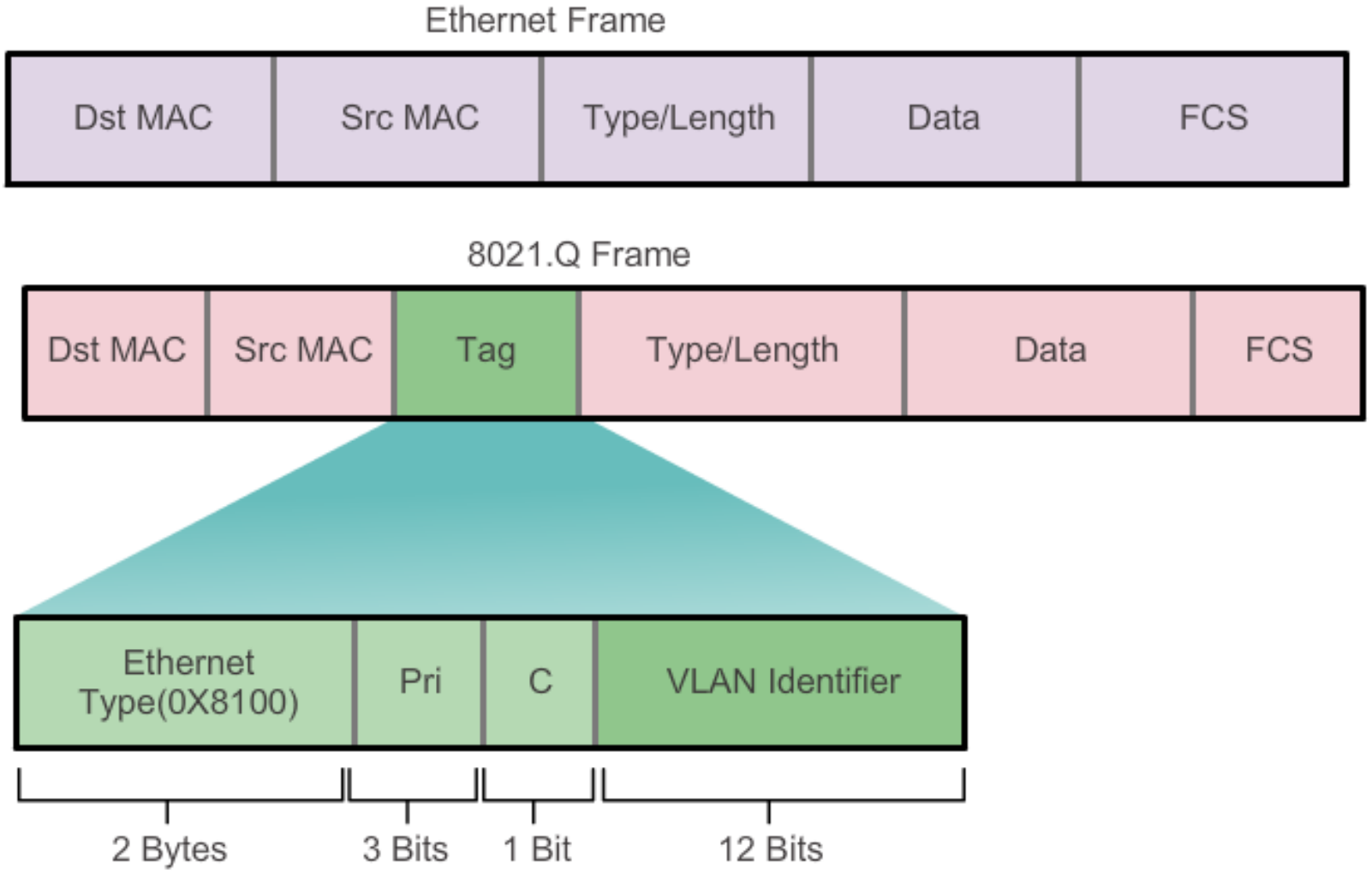
- Las VLAN se pueden usar para limitar el alcance de las tramas de broadcast.
- Una VLAN es un dominio de broadcast propio.

- La trama de broadcast enviada por un dispositivo en una VLAN específica se reenvía sólo dentro de esa VLAN.
- Las Tramas unicast y de broadcast se reenvían entre los originarios en sus VLAN.

Etiquetado de tramas Ethernet para la identificación de las VLAN

- Se utiliza para transmitir múltiples tramas de VLAN a través del enlace troncal
- Los switch etiquetan las tramas para identificar la VLAN a que pertenecen. El protocolo de etiquetado, con IEEE 802.1q.
- Los switch agregarán etiquetas de VLAN a las tramas antes enviar a los enlaces troncales y deben quitar las etiquetas antes de reenviar tramas a través de puertos no troncales.
- Una vez etiquetadas, las tramas pueden pasar por cualquier switch a través de los enlaces troncales y seguir hasta la VLAN correcta hacia su destino.

Etiquetado de tramas Ethernet para la identificación de las VLAN



VLAN nativas y etiquetado 802.1Q

- La trama que pertenece a la VLAN nativa no será etiquetada.
- La trama que se recibe sin etiquetar permanecerá sin etiquetar; y se coloca el numero de la VLAN nativa cuando deba ser enviada por el enlace troncal.
- Si no hay puertos asociados a los enlaces troncales y a las VLAN nativas, la trama sin etiqueta será descartada.

- En los switch la VLAN nativa es la VLAN 1 por defecto

Rangos de VLAN en Switches Catalyst

- Los switch 2960 y 3560 soportan cerca de 4000 VLANs. Se dividen en 2 categorías:
- **VLANs rango normal:** Del 1 a 1005
- Las configuraciones se guardan en vlan.dat (en la flash)
- VTP sólo puede aprender y almacenar las VLAN de rango normal.
- **VLAN de rango extendido:** Del 1006 a 4096
- Las configuraciones se guardan en el running config (en la NVRAM)
- VTP no aprende las VLAN de rango extendido

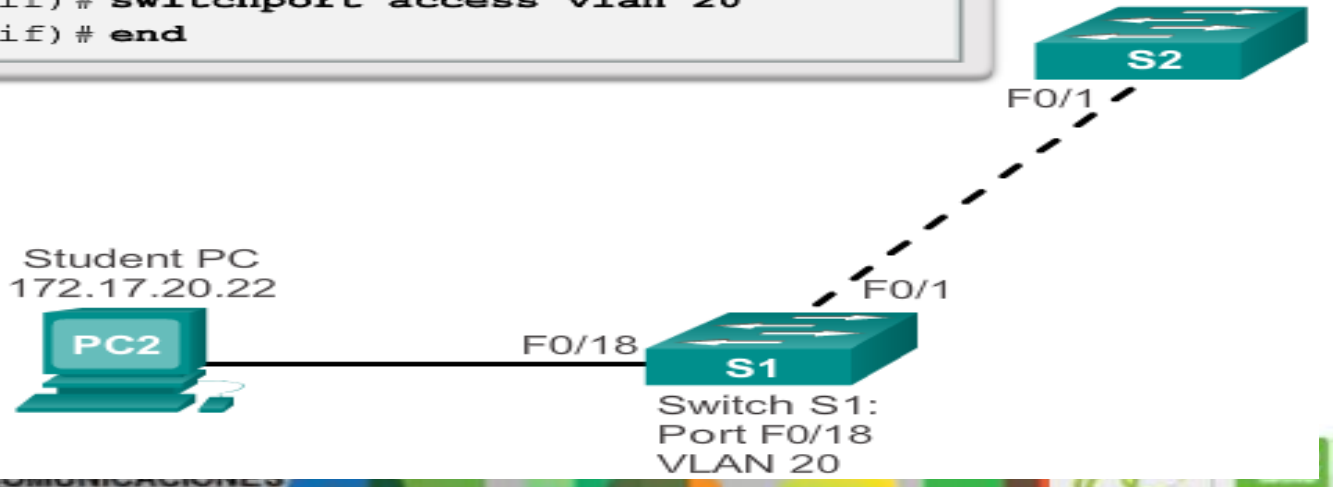
Creación de una VLAN

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`

Asignación de puertos a las VLAN

Cisco Switch IOS Commands	
Enter global configuration mode.	S1 # **configure terminal**
Enter interface configuration mode for the SVI.	S1(config) # **interface** *interface_id*
Configure the management interface IP address.	S1(config) # **ip address 172.17.99.11**
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**

```
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
```



Membresía Cambio de puertos de 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#
```

Membresía Cambio de puertos de 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#
```

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#
```

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#
```

```
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
```

Configuración de enlaces troncales 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
```

Verificando la configuración del enlace 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>
```

Introducción a la DTP

- Los puertos de switch se configuran manualmente para ser troncales.
- Pueden negociar ser troncal con un punto conectado.
- El Protocolo de enlace troncal dinámico (DTP) es un protocolo para gestionar la negociación troncal.
- DTP de Cisco está activado por defecto en 2960 y 3560.
- Si el puerto del vecino está configurado en un modo de troncal que soporte DTP, administra la negociación.
- La configuración por defecto DTP para los switch es auto dinámico (dynamic auto).

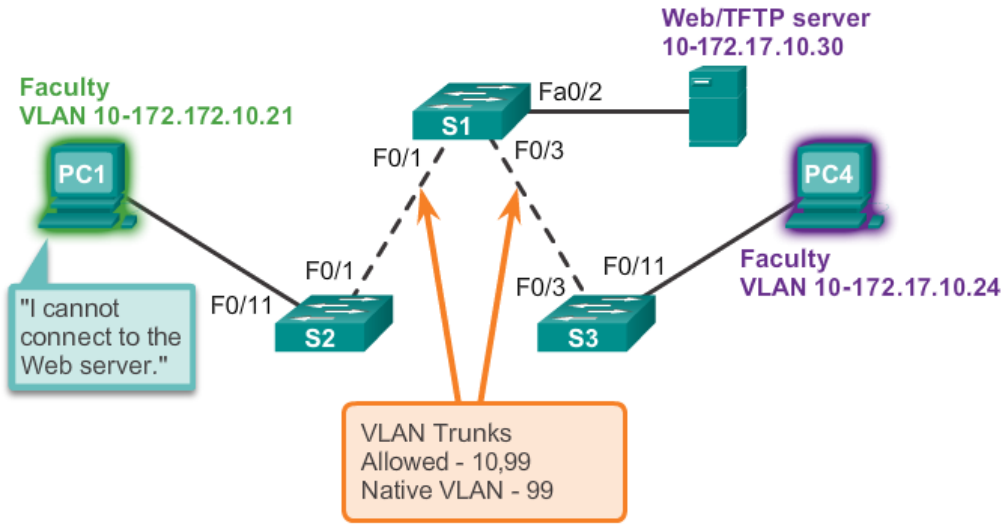
Modos de negociación de las interfaces

- **Switchport mode auto dinámico (dynamic auto)**
- **Switchport mode deseable dinámico (dynamic desiderable).**
- **Modo switchport 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**

Resolviendo problemas de direccionamiento de las VLAN

- Es muy común asociar la VLAN con la red IP.
- Entre diferentes redes IP sólo se comunican por el router, todos los PC dentro de una VLAN deben formar parte de la red con el mismo rango de IP.
- En la figura, PC1 no puede comunicarse con el servidor debido a que tiene una dirección IP errónea.



Problemas comunes con los troncales

- Se asocian con configuraciones incorrectas.
- El tipo más común de los errores de configuración son:

1. Desajuste en la VLAN nativa
2. Desajuste en el modo troncal
3. Las VLAN permitidas en los troncales

- Si se detecta un problema en el enlace troncal, las mejores guías de práctica recomiendan solucionar los problemas en el orden indicado anteriormente.

Diferencias en el modo de enlace troncal

- Si un puerto se configura como troncal y es incompatible con el puerto troncal del vecino, el enlace troncal no se forma entre los dos switch.

- Compruebe el estado de los puertos troncales en el switch usando el comando show interfaces trunk.

- Para solucionar el problema, configure las interfaces con los modos apropiados troncales.

Lista incorrecta de VLAN

- Para que las VLAN puedan pasar por el enlace troncal antes las tramas deben tomar el numero de la VLAN.

- Utilice el comando **switchport trunk allowed vlan** para especificar cuáles VLAN están permitidos en el enlace troncal.

- Para garantizar las VLAN correctas permitidas en el enlace troncal, se utiliza el comando **show interfaces trunk.**

Ataque de suplantación del switch

- El ataque de suplantación de VLAN es uno ellos.
- La configuración predeterminada es automática dinámica.
- Si configura un PC para que actúe como un switch y formar un enlace troncal, se obtiene acceso a cualquier VLAN en la red.
- El atacante está en condiciones de acceder a otras VLAN, esto se llama **un salto de ataque de VLAN.**
- Para prevenir el ataque básico de suplantación de switch, **apague el enlace troncal en todos los puertos, excepto aquellos que Específicamente requieren trunking.**

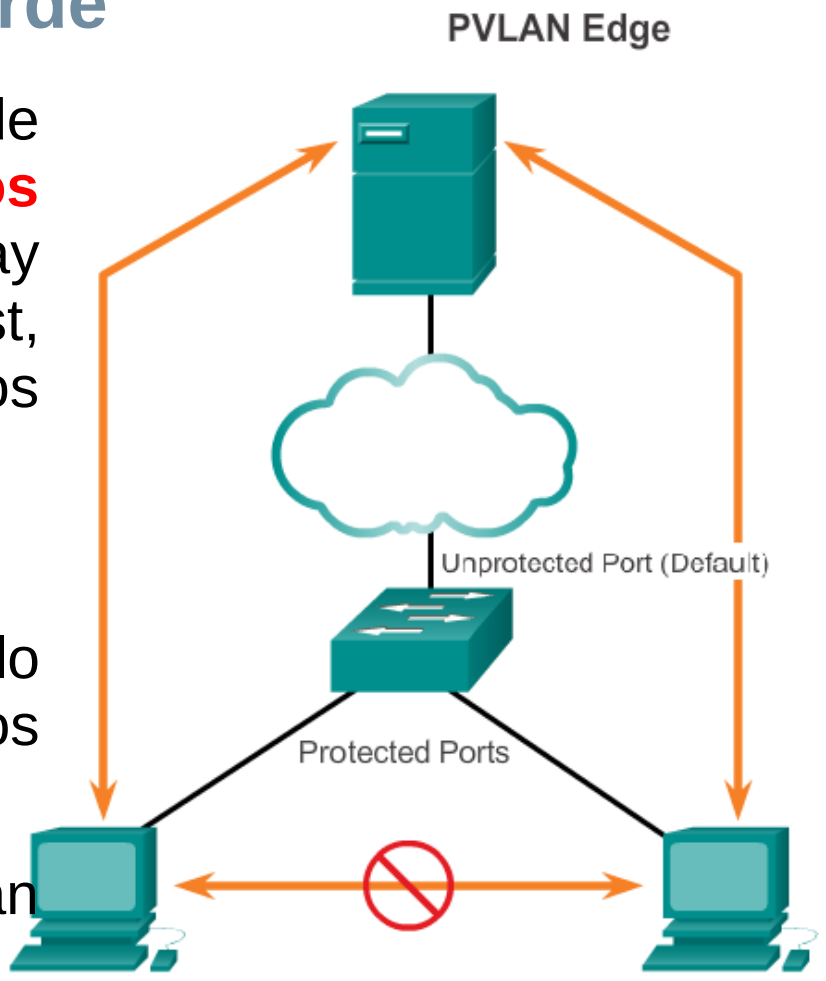
Ataque de doble etiquetado

- Los switch. encapsulan etiquetas 802.1Q.
- Permite a un atacante incrustar un segundo ataque, en el encabezado de la trama.
- Después de la eliminación del encabezado en la cabecera 802.1Q, el switch envía la trama a la VLAN especificada en la cabecera 802.1Q no autorizada.

- La mejor manera de mitigar los ataques de doble etiquetado **es asegurar que la VLAN nativa de los puertos troncales sea diferente a la VLAN de los puertos de usuario**

PVLAN de borde

- La VLAN Privada de borde (PVLAN), conocida como **puertos protegidos,** Asegura que no hay intercambio de tráfico unicast, broadcast o multicast entre los puertos protegidos en el switch.
- operan localmente.
- Un puerto protegido sólo intercambia tráfico con los puertos no protegidos.
- Estos puertos no intercambian tráfico con otro puerto protegido



Guia de base para el Diseño de las VLAN

- Mueva todos los puertos de la VLAN 1 y asígnelos a una VLAN de poco uso.
- Deshabilite todos los puertos del switch no utilizados.
- Separe la Gestión, del tráfico de datos de usuario.
- Cambie la VLAN de administración a una VLAN que no sea VLAN1. haga lo mismo con la VLAN nativa.
- Asegúrese que sólo los dispositivos en la VLAN de administración se pueden conectar a los switches.
- El switch sólo debe aceptar conexiones SSH.
- Deshabilitar la negociación automática en los puertos troncales.
- No utilizar los modos auto o deseable en los puertos del switch

Resumen

- El protocolo IEEE 802.1Q etiquetado de tramas y cómo se permite la diferenciación entre las tramas Ethernet asociados con distintas VLANs que atraviesan los enlaces troncales comunes.

- Examina la configuración, verificación y solución de problemas de las VLAN y los troncales utilizando el IOS y la seguridad básica explorando las consideraciones de diseño en el contexto de las VLAN.

Cisco | Networking Academy®
Mind Wide Open™

MUCHAS GRACIAS

CONSTRUIMOS FUTURO