Comunicaciones de Datos

VLAN

Prof. Ing. Miguel Solinas

Agenda

1. Segmentación con VLAN
2. Implementación de VLAN
3. Seguridad y diseño de redes VLAN
4. Resumen

¿ Qué debería saber sobre VLAN ?

- Explicar la finalidad de las VLAN en una red conmutada.
- Analizar cómo un switch reenvía tramas según la configuración de VLAN en un entorno conmutado múltiple.
- Configurar un puerto de switch que se asigna a una VLAN según los requisitos.
- Configurar un puerto de enlace troncal en un switch LAN.
- Saber que existe un protocolo de enlace troncal dinámico (DTP).
- Solucionar problemas de configuración de VLAN y de enlaces troncales en una red conmutada.
- Configurar las características de seguridad para mitigar los ataques en un entorno segmentado por VLAN.
- Explicar las prácticas recomendadas de seguridad para un entorno segmentado por VLAN.

Algunas definiciones

La VLAN (LAN virtual) es una partición lógica de una red de capa 2.

Se pueden crear varias particiones para que coexistan varias VLAN.

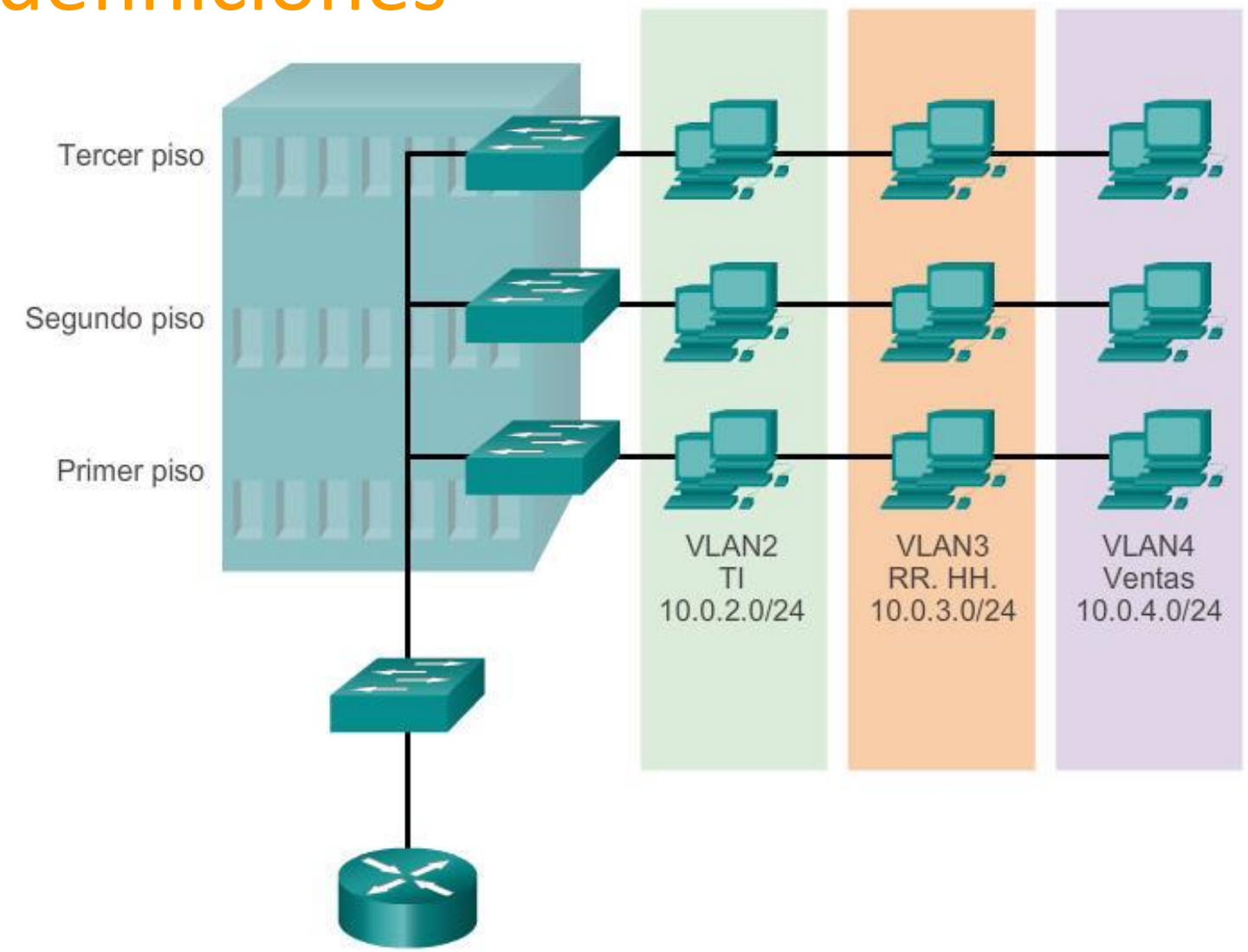
Cada VLAN es un dominio de difusión, que generalmente posee su propia red IP.

Las VLAN se aíslan mutuamente y los paquetes pueden pasar entre ellas solo mediante un router.

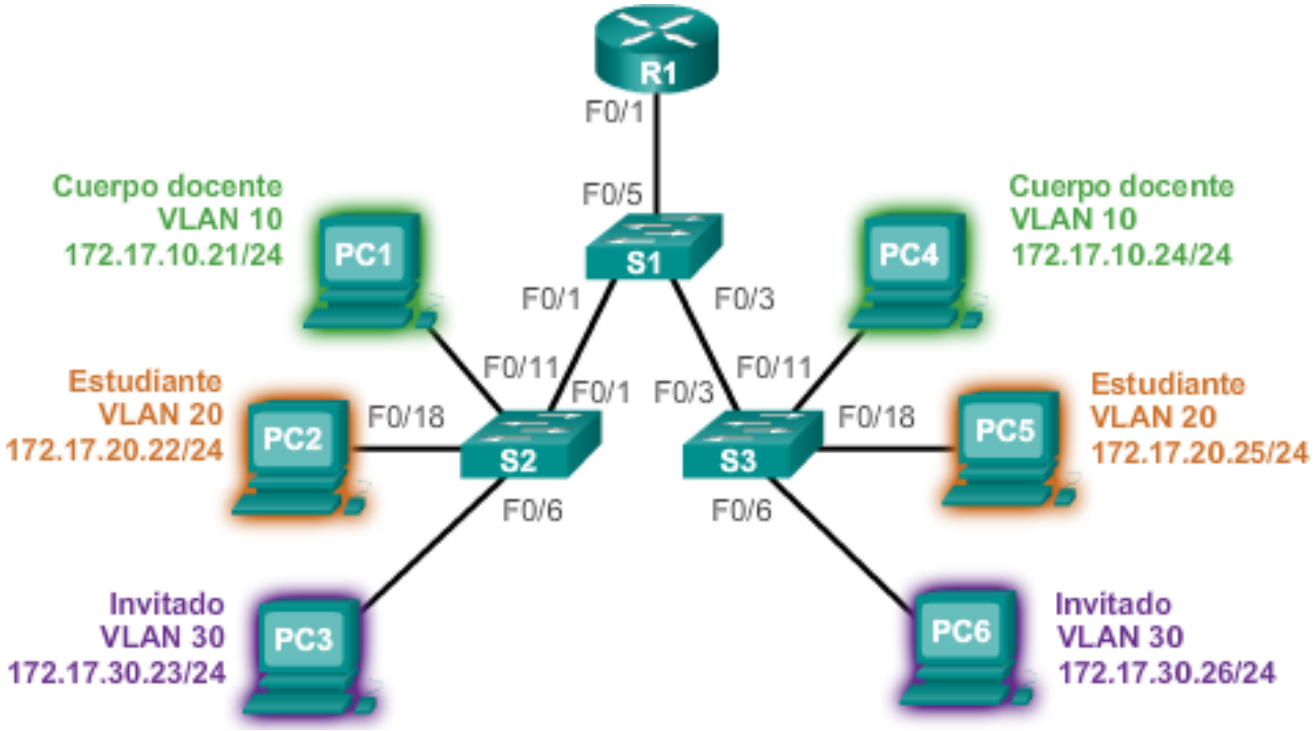
La partición de la red de capa 2 se lleva a cabo dentro de un dispositivo de capa 2 (por lo general, un switch).

Los hosts que se agrupan dentro de una VLAN desconocen la existencia de esta.

Algunas definiciones



Beneficios de las redes VLAN



- Seguridad
- Reducción de costos
- Mejor rendimiento
- Reducción de dominios de difusión
- Mejora de la eficiencia del personal de TI
- Administración más simple de aplicaciones y proyectos

Tipos de VLAN

- VLAN de datos
- VLAN predeterminada
- VLAN nativa
- VLAN de administración

Tipos de VLAN: VLAN 1

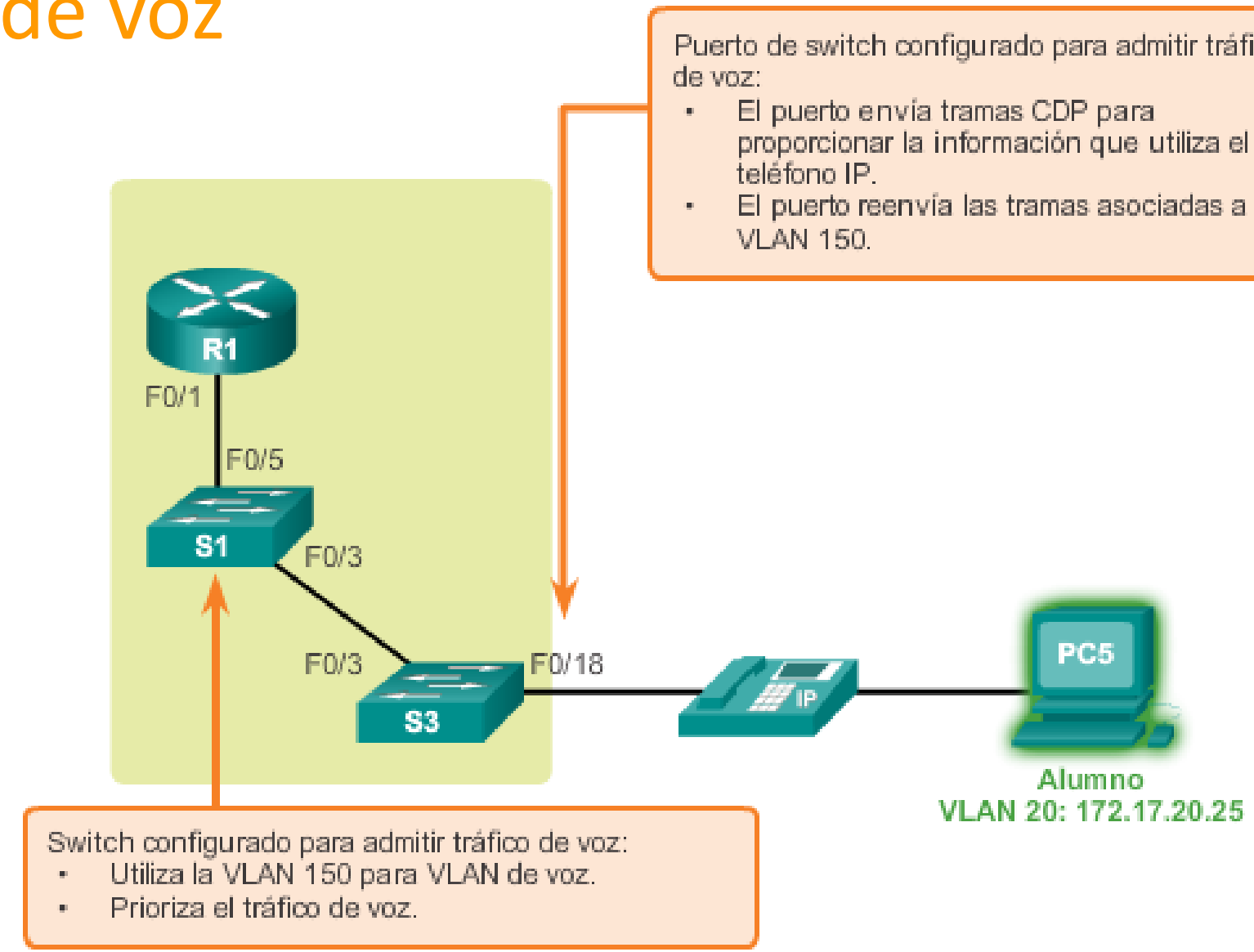
- De manera predeterminada, todos los puertos están asignados a la VLAN 1 para reenviar datos.
- De manera predeterminada, la VLAN nativa es la VLAN 1.
- De manera predeterminada, la VLAN de administración es la VLAN 1
- No se puede cambiar el nombre ni eliminar la VLAN 1

```
S1#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
10   Faculty                           active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
20   Students                          active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
30   Guests                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

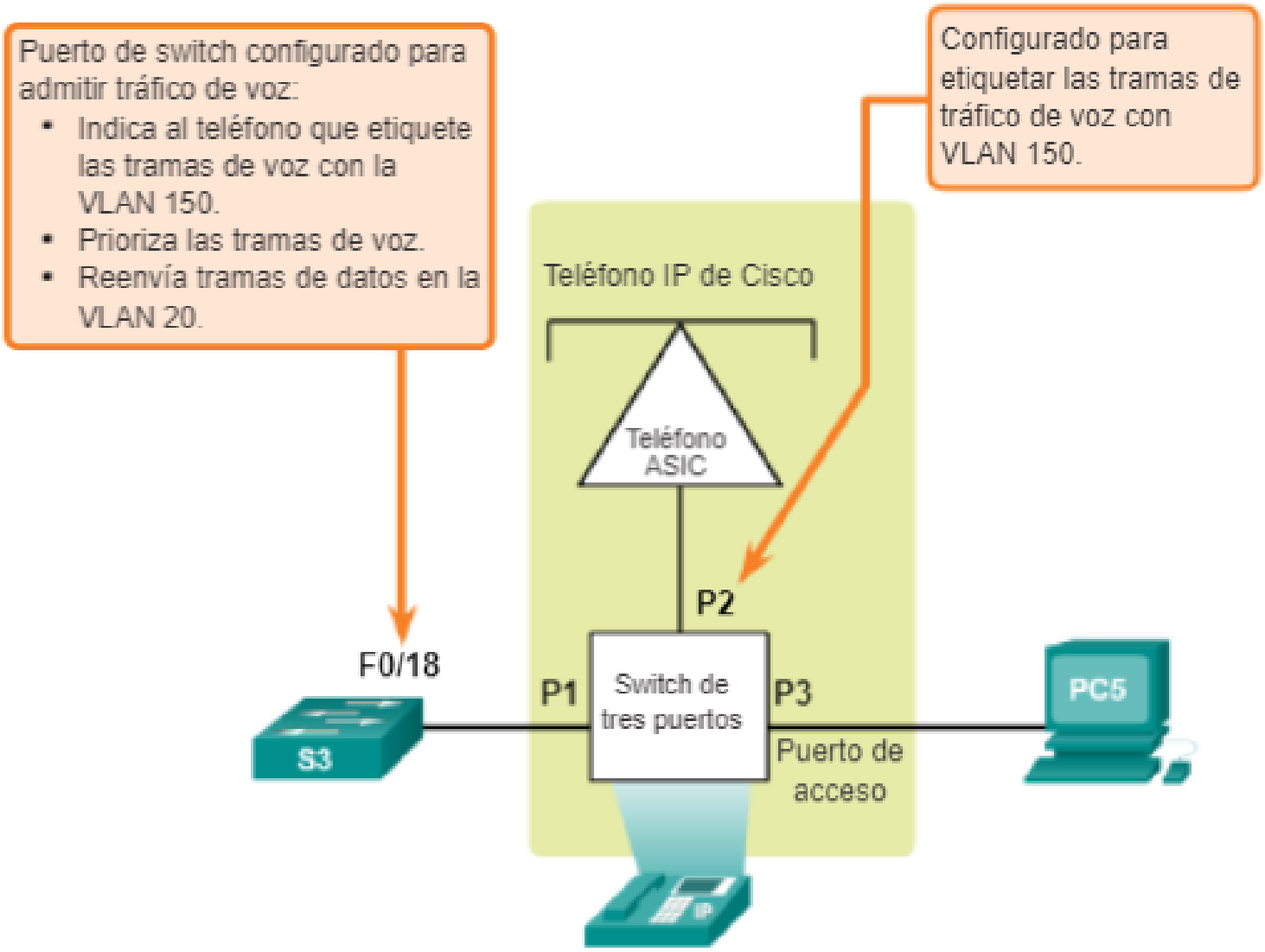
VLAN de voz

- El tráfico VoIP depende del factor tiempo y requiere lo siguiente:
  - Ancho de banda garantizado para asegurar la calidad de la voz
  - Prioridad de la transmisión sobre los tipos de tráfico de la red
  - Capacidad para ser enrutado en áreas congestionadas de la red
  - Demora inferior a 150 ms a través de la red
- La característica de la VLAN de voz permite que los puertos de acceso envíen el tráfico de voz IP desde un teléfono IP.
- El switch puede conectarse a un teléfono IP 7960 de Cisco y transportar el tráfico de voz IP.
- Dado que la calidad de sonido de una llamada desde un teléfono IP puede disminuir si la información no se envía de manera uniforme, el switch admite la calidad de servicio (QoS).

VLAN de voz


Puerto de switch configurado para admitir tráfico de voz:
• El puerto envía tramas CDP para proporcionar la información que utiliza el teléfono IP.
• El puerto reenvía las tramas asociadas a la VLAN 150.
R1
F0/1
F0/5
S1
F0/3
F0/3
F0/18
S3
IP
PC5
Alumno
VLAN 20: 172.17.20.25
Switch configurado para admitir tráfico de voz:
• Utiliza la VLAN 150 para VLAN de voz.
• Prioriza el tráfico de voz.

VLAN de voz


Puerto de switch configurado para admitir tráfico de voz:
• Indica al teléfono que etiquete las tramas de voz con la VLAN 150.
• Prioriza las tramas de voz.
• Reenvía tramas de datos en la VLAN 20.
Configurado para etiquetar las tramas de tráfico de voz con VLAN 150.
Teléfono IP de Cisco
Teléfono ASIC
P2
F0/18
P1
Switch de tres puertos
P3
Puerto de acceso
S3
PC5

Enlaces troncales de VLAN

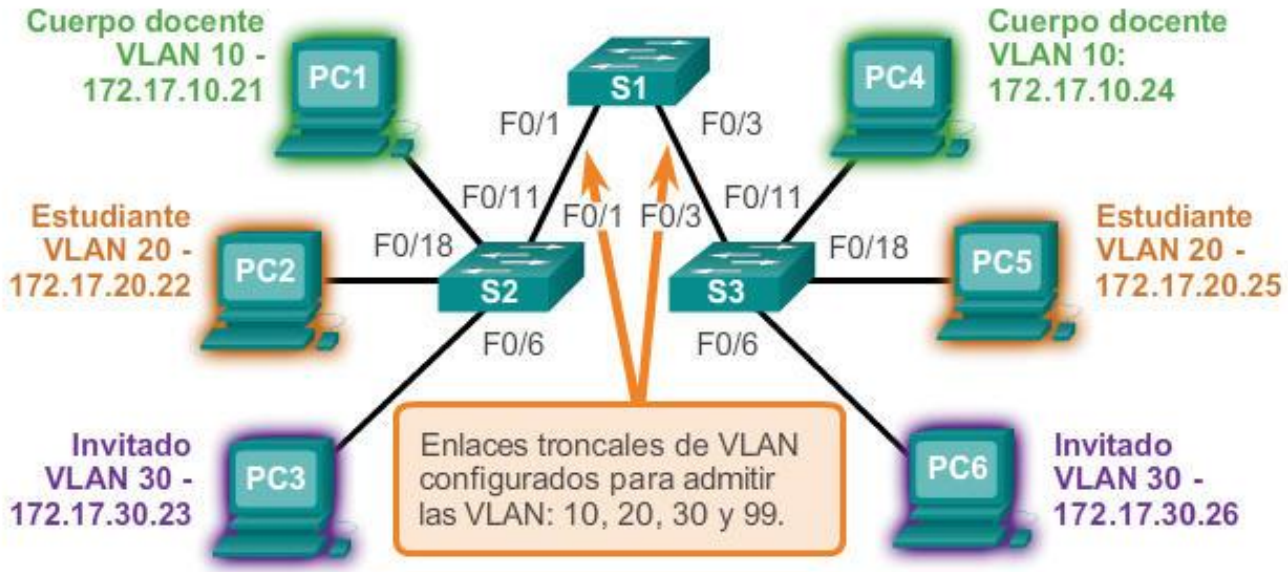
- Un enlace troncal de VLAN transporta más de una VLAN.
- Generalmente, se establece entre los switches para que los dispositivos de una misma VLAN se puedan comunicar incluso si están conectados físicamente a switches diferentes.
- Un enlace troncal de VLAN no está relacionado con ninguna VLAN. Tampoco lo están los puertos de enlace troncal que se utilizan para establecer el enlace troncal.
- IOS de Cisco admite IEEE802.1q, un protocolo de enlace troncal de VLAN conocido.

Redes VLAN en un entorno conmutado múltiple

Enlaces troncales de VLAN

VLAN 10 de cuerpo docente/personal: 172.17.10.0/24
VLAN 20 de estudiantes: 172.17.20.0/24
VLAN 30 de invitados: 172.17.30.0/24
VLAN 99 de administración y nativa: 172.17.99.0/24

Las interfaces F0/1 a 5 son interfaces de enlace troncal 802.1Q con una VLAN nativa 99.
Las interfaces F0/11 a 17 están en la VLAN 10.
Las interfaces F0/18 a 24 están en la VLAN 20.
Las interfaces F0/6 a 10 están en la VLAN 30.



Redes VLAN en un entorno conmutado múltiple

Control de dominios de difusión con VLAN

- Las VLAN se pueden utilizar para limitar el alcance de las tramas de difusión.
- Una VLAN es un dominio de difusión propio.
- Por lo tanto, una trama de difusión que envía un dispositivo en una VLAN específica se reenvía solamente dentro de esa VLAN.
- Esto ayuda a controlar el alcance de las tramas de difusión y su impacto en la red.
- Las tramas de unidifusión y multidifusión también se reenvían dentro de la VLAN de origen.

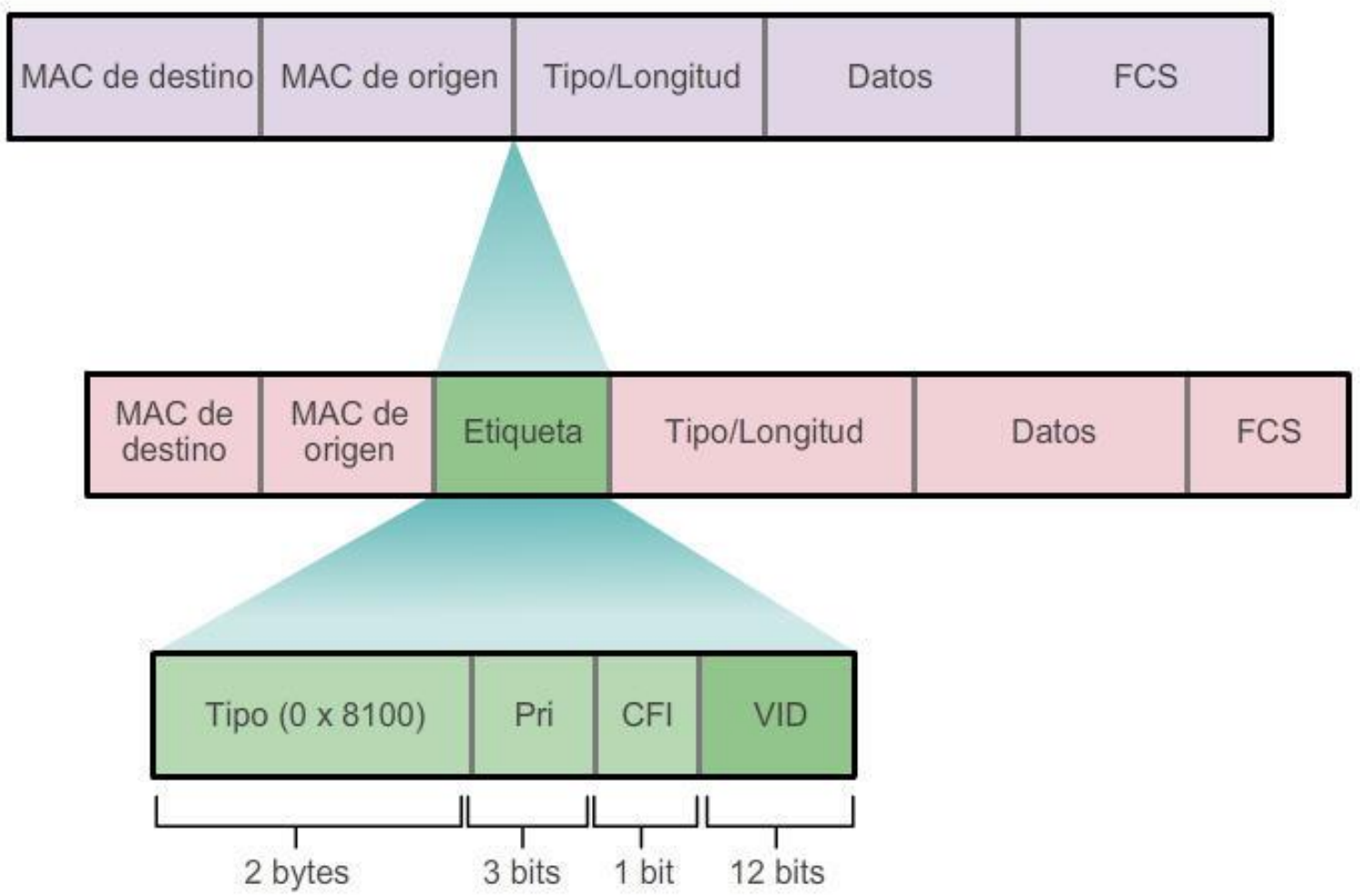
Redes VLAN en un entorno conmutado múltiple

Etiquetado de tramas Ethernet para la identificación de VLAN

- El etiquetado de tramas se utiliza para transmitir correctamente las tramas de varias VLAN a través de un enlace troncal.
- Los switches etiquetan las tramas para identificar la VLAN a la que pertenecen. Existen diferentes protocolos de etiquetado. IEEE 802.1q es uno muy popular.
- El protocolo define la estructura del encabezado de etiquetado que se agrega a la trama.
- Los switches agregan etiquetas VLAN a las tramas antes de colocarlas en los enlaces troncales y quitan las etiquetas antes de reenviar las tramas a través de los puertos de enlace no troncal.
- Una vez que están etiquetadas correctamente, las tramas pueden atravesar cualquier cantidad de switches mediante los enlaces troncales y aun así se pueden reenviar dentro de la VLAN correcta en el destino.

Redes VLAN en un entorno conmutado múltiple

Etiquetado de tramas Ethernet para la identificación de VLAN



Redes VLAN en un entorno conmutado múltiple

VLAN nativas y etiquetado de 802.1q

- Las tramas que pertenecen a la VLAN nativa no se etiquetan.
- Una trama que se recibe sin etiqueta seguirá sin etiqueta y se colocará en la VLAN nativa cuando se reenvíe.
- Una trama sin etiqueta se descarta si no hay puertos asociados a la VLAN nativa y si no hay otros enlaces troncales.
- En los switches Cisco, la VLAN nativa es la VLAN 1 de manera predeterminada.

Asignación de VLAN

Rangos de VLAN en los switches Catalyst

- Los switches de las series Catalyst 2960 y 3560 admiten más de 4000 VLAN.
- Estas VLAN se dividen en dos categorías:
- VLAN de rango normal
  - Números de VLAN de 1 a 1005.
  - La configuración se almacena en el archivo vlan.dat (en la memoria flash).
  - VTP solo puede descubrir y almacenar las VLAN de rango normal.
- VLAN de rango extendido
  - Números de VLAN de 1006 a 4096.
  - La configuración se almacena en la configuración en ejecución (en la NVRAM).
  - VTP no descubre las VLAN de rango extendido.

Asignación de VLAN

Creación de una VLAN

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	`S1# configure terminal`
Cree una VLAN con un número de ID válido.	`S1(config)#vlan` *id-vlan*
Especifique un nombre único para identificar la VLAN.	`S1(config-vlan)#name` *nombre-vlan*
Vuelva al modo EXEC privilegiado.	`S1(config-vlan)# end`

Asignación de VLAN

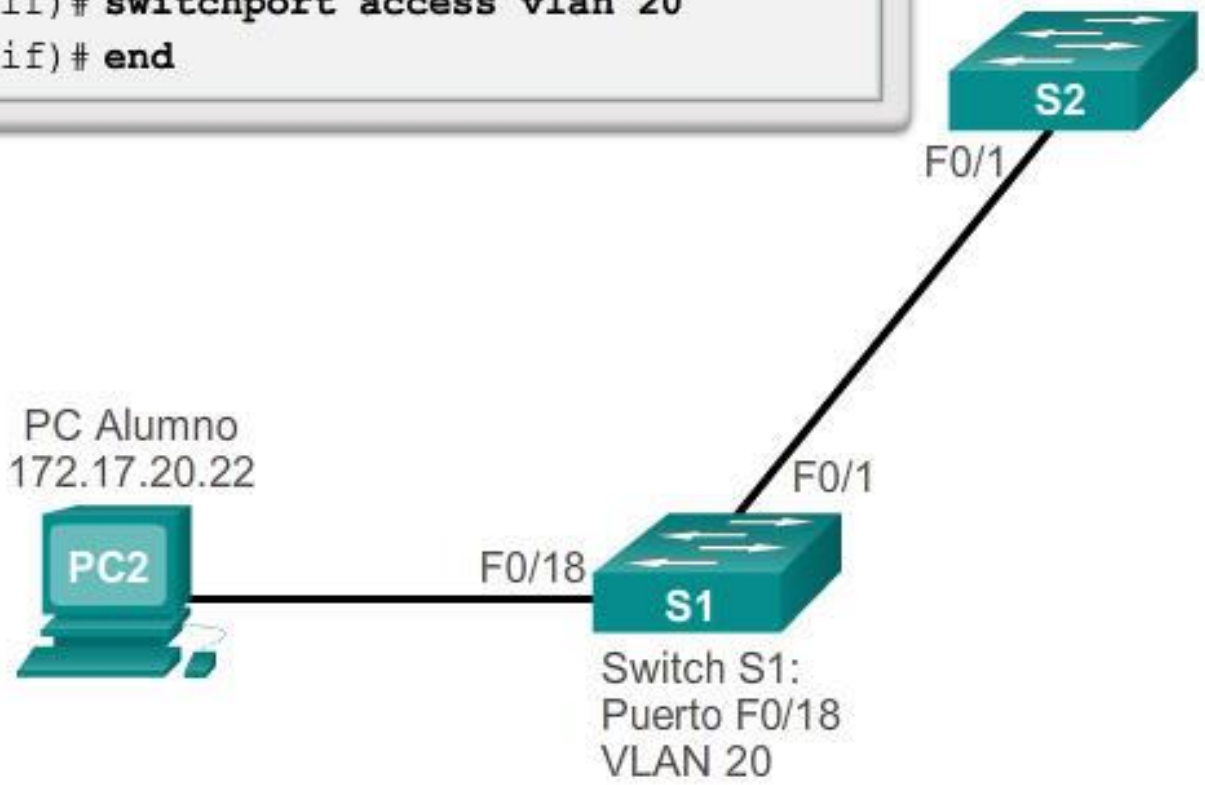
Asignación de puertos a las redes VLAN

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese al modo de configuración de interfaz para la SVI.	`S1(config)# interface` *id_interfaz*
Establezca el puerto en modo de acceso.	`S1(config-if)# switchport mode access`
Asigne el puerto a una VLAN.	`S1(config-if)# switchport access vlan` *id_vlan*
Vuelva al modo EXEC privilegiado.	`S1(config-if)# end`

Asignación de VLAN

Asignación de puertos a las redes VLAN

```
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

Cambio de pertenencia de puertos de una 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

Cambio de pertenencia de puertos de una 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

Eliminación de VLAN

```
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

Verificación de información de VLAN

```
S1# show vlan name Students

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
20   Students                          active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16

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

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

Configuración de enlaces troncales IEEE 802.1Q

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	S1# **configure terminal**
Ingrese al modo de configuración de interfaz para la SVI.	S1(config)# **interface** *id_interfaz*
Haga que el enlace sea un enlace troncal.	S1(config-if)# **switchport mode trunk**
Especifique una VLAN nativa para enlaces troncales 802.1Q sin etiquetar.	S1(config-if)# **switchport trunk native vlan** *id_vlan*
Especifique la lista de VLAN que se permitirán en el enlace troncal.	S1(config-if)# **switchport trunk allowed vlan** *lista-vlan*
Vuelva al modo EXEC privilegiado.	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
```

Asignación de VLAN

Restablecimiento

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>
```

Asignación de VLAN

Restablecimiento

Restablecimiento del puerto al modo de acceso

```
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
<resultado omitido>
```

Asignación de VLAN

Verificación

Verificación de la configuración de enlace troncal

```
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
<resultado omitido>
```

Protocolos de enlace troncal dinámico

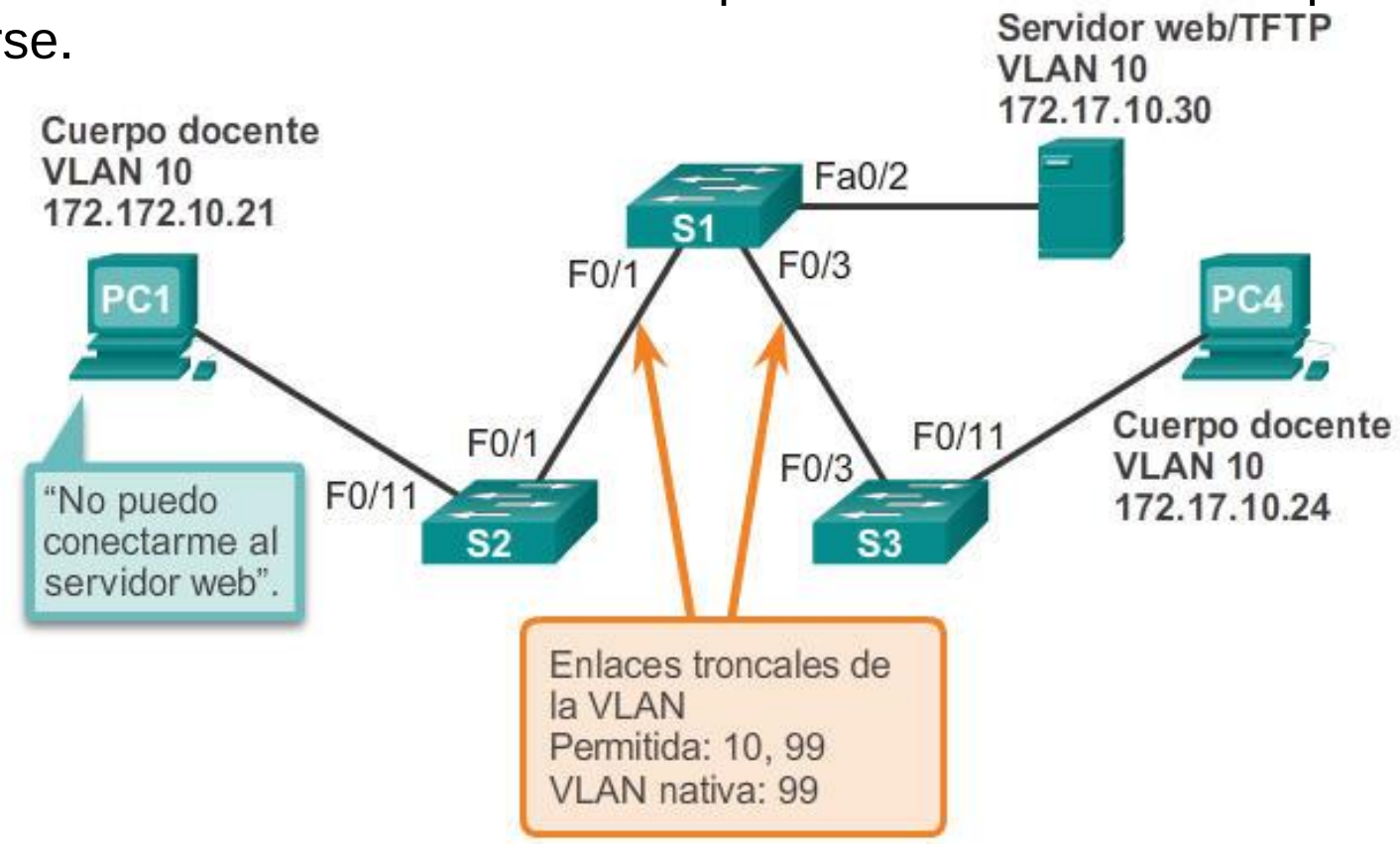
Protocolo DTP

- Los puertos de switch se pueden configurar manualmente para formar enlaces troncales.
- Los puertos de switch también se pueden configurar para negociar y para establecer un enlace troncal con un peer conectado.
- El protocolo de enlace troncal dinámico (DTP) administra la negociación de enlaces troncales.
- DTP es un protocolo exclusivo de Cisco que se habilita de manera predeterminada en los switches Cisco Catalyst 2960 y Catalyst 3560.
- DTP administra la negociación del enlace troncal si el puerto en el switch vecino se configura en un modo de enlace troncal que admite DTP.
- La configuración predeterminada de DTP para los switches Cisco Catalyst 2960 y 3560 es dynamic auto (dinámico automático).

Resolución de problemas de VLAN y enlaces troncales

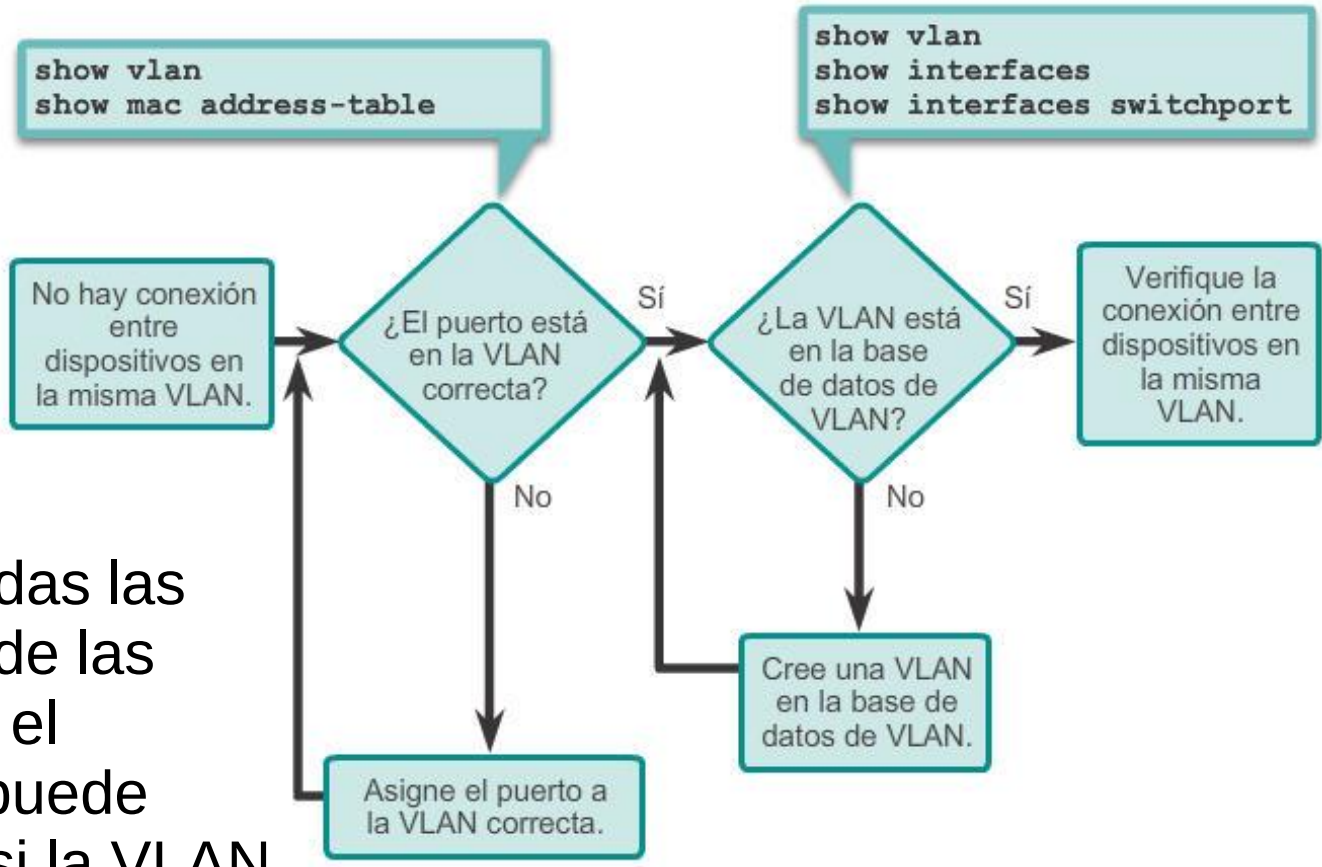
Problemas de direccionamiento de VLAN

- Es una práctica común asociar una VLAN a una red IP.
- Diferentes redes IP solo se comunican mediante un router, todos los dispositivos dentro de una VLAN deben formar parte de la misma red IP para poder comunicarse.



Resolución de problemas de VLAN y enlaces troncales

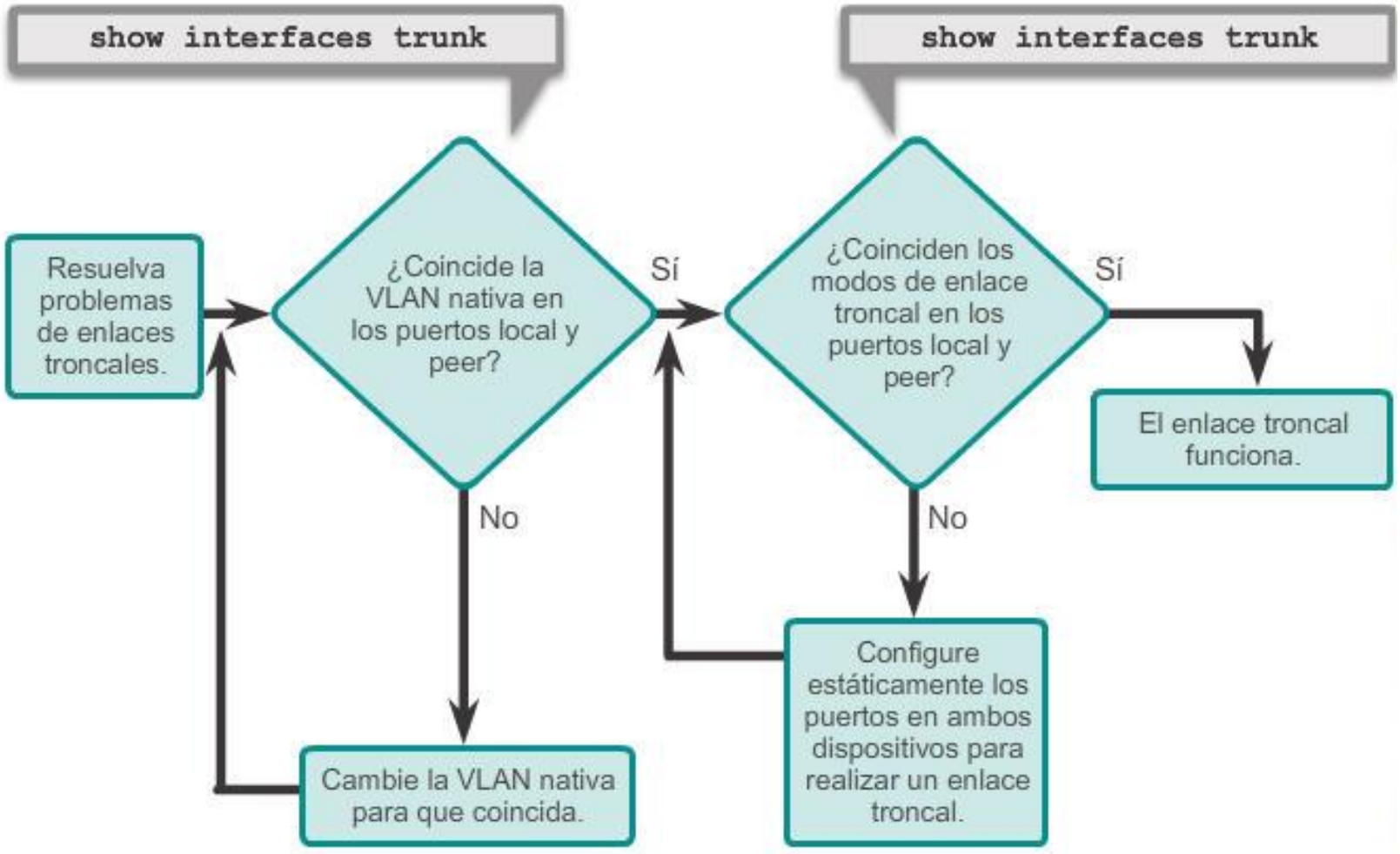
VLAN Faltantes



- Si se resolvieron todas las incompatibilidades de las direcciones IP pero el dispositivo aún no puede conectarse, revise si la VLAN existe en el switch.

Resolución de problemas de VLAN y enlaces troncales

Intr. a la resolución de problemas en enlaces troncales



Resolución de problemas de VLAN y enlaces troncales

Problemas comunes con enlaces troncales

- En general, los problemas de enlaces troncales se deben a una configuración incorrecta.
- Los tipos más comunes de errores de configuración de enlaces troncales son los siguientes:
  1. Falta de concordancia de la VLAN nativa
  2. Falta de concordancia del modo de enlace troncal
  3. VLAN permitidas en enlaces troncales
- Si se detecta un problema de enlace troncal, se recomienda, según las pautas de prácticas recomendadas, resolver los problemas en el orden anterior.

Resolución de problemas de VLAN y enlaces troncales

Incompatibilidad del modo de enlace troncal

- Cuando un puerto en un enlace troncal se configura con un modo de enlace troncal que no es compatible con el puerto de enlace troncal vecino, no se puede formar un enlace troncal entre los dos switches.
- Verifique el estado de los puertos enlace troncal de los switches con el comando **show interfaces trunk**.
- Para resolver el problema, configure las interfaces en los modos de enlace troncal apropiados.

	Dinámico automático	Dinámico deseado	Enlace troncal	Acceso
Dinámico automático	Acceso	Enlace troncal	Enlace troncal	Acceso
Dinámico deseado	Enlace troncal	Enlace troncal	Enlace troncal	Acceso
Enlace troncal	Enlace troncal	Enlace troncal	Enlace troncal	Conectividad limitada
Acceso	Acceso	Acceso	Conectividad limitada	Acceso

Resolución de problemas de VLAN y enlaces troncales

Lista de VLAN incorrectas

- Se deben permitir las VLAN en el enlace troncal para que se puedan transmitir las tramas a través del enlace.
- Utilice el comando **switchport trunk allowed vlan** para especificar las VLAN permitidas en el enlace troncal.
- Para asegurarse de que se permitan las VLAN apropiadas en un enlace troncal, utilice el comando **show interfaces trunk**.

Ataques a redes VLAN

Ataque de suplantación de identidad de switch

- Existen diferentes tipos de ataques a VLAN en las redes conmutadas modernas. El salto de VLAN es uno de ellos.
- La configuración predeterminada del puerto de switch es dynamic auto (dinámico automático).
- Al configurar un host para que funcione como switch y formar un enlace troncal, un atacante podría acceder a cualquier VLAN en la red.
- Debido a que el atacante ahora puede acceder a otras VLAN, esto se denomina “ataque con salto de VLAN”.
- Para evitar un ataque de suplantación de identidad de switch básico, desactive el enlace troncal en todos los puertos, excepto en los que requieren el enlace troncal específicamente.

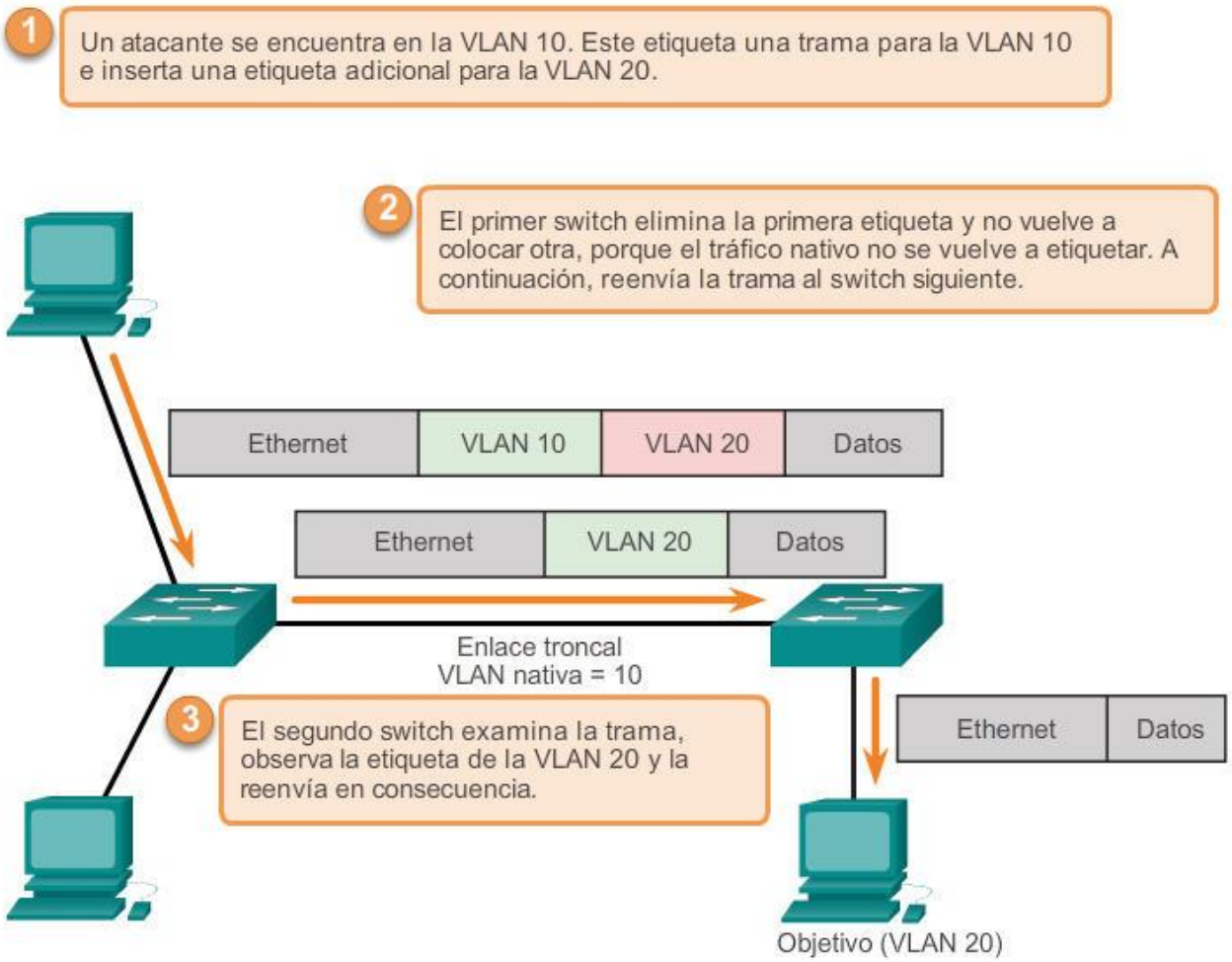
Ataques a redes VLAN

Ataque de etiquetado doble

- El ataque de etiquetado doble aprovecha la forma en que el hardware desencapsula las etiquetas 802.1Q en la mayoría de los switches.
- Muchos switches realizan solamente un nivel de desencapsulación 802.1Q, lo que permite que un atacante incorpore un segundo encabezado de ataque no autorizado en la trama.
- Después de quitar el primer encabezado 802.1Q legítimo, el switch reenvía la trama a la VLAN especificada en el encabezado 802.1Q no autorizado.
- El mejor método para mitigar los ataques de etiquetado doble es asegurar que la VLAN nativa de los puertos de enlace troncal sea distinta de la VLAN de cualquier puerto de usuario.

Ataques a redes VLAN

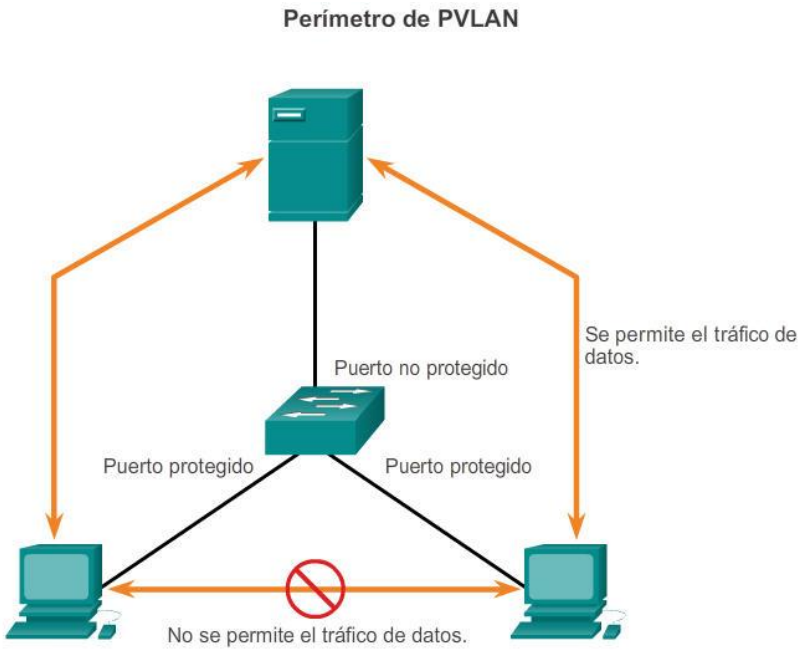
Ataque de etiquetado doble



Ataques a redes VLAN

Perímetro de PVLAN

- La característica de perímetro de VLAN privada (PVLAN), también conocida como “puertos protegidos”, asegura que no se intercambie tráfico de unidifusión, difusión o multidifusión entre los puertos protegidos del switch.
- Solo tiene importancia local.
- Un puerto protegido intercambia tráfico solamente con los puertos no protegidos.
- Un puerto protegido no intercambia tráfico con otro puerto protegido.



Prácticas recomendadas de diseño para las VLAN

Pautas de diseño

- Mueva todos los puertos de la VLAN1 y asígnelos a una VLAN que no se utilice.
- Desactive todos los puertos de switch sin utilizar.
- Separe el tráfico de administración y de datos de usuario.
- Cambie la VLAN de administración por una VLAN distinta de VLAN 1. Lo mismo aplica para la VLAN nativa.
- Asegúrese de que solo los dispositivos en la VLAN de administración se puedan conectar a los switches.
- El switch solo debe aceptar las conexiones SSH.
- Deshabilite la autonegociación en los puertos de enlace troncal.
- No utilice los modos de puerto de switch automático ni deseado.

Resumen

- En este capítulo, se presentaron las VLAN y sus tipos.
- También se analizó la conexión entre las VLAN y el dominio de difusión.
- Se abarca, además, el etiquetado de tramas IEEE 802.1Q y la manera en que este permite la diferenciación entre tramas de Ethernet asociadas a distintas VLAN mientras atraviesan enlaces troncales comunes.
- En este capítulo, también se analizó la configuración y la verificación de redes VLAN y de enlaces troncales, así como la resolución de problemas relacionados mediante la CL de IOS de Cisco, y se exploraron las consideraciones básicas de seguridad y de diseño en el contexto de las redes VLAN.

Bibliografía

1. “Redes de Computadores”, James F. Kurose, Keith W.Ross, Pearson Addison Wesley.-
2. “Multiple Access Protocols: Perfomance and Analysis”; Rom, M. Sidi; Springer-Verlang; New York 1990.-
3. “Cisco LAN Switching, CCIE Profesional Development”, Kennedy Clark, Kevin Hamilton.-
4. http://www.ethermanage.com/ethernet/ethernet.html


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
BÏYAN
SHUKRIA
TINGKI
YAQHANYELAY
TASHAKKUR ATU
SUKSAMA
EKHMET
MEHRBANI
GRAZIE
MAAKE
KOMAPSUMNIDA
JUSPAXAR
GOZAIMASHITA
EFCHARISTO
PALDIES
BOLZÏN
MERCI
SPASSIBO
SNACHALHUYA
NUHUN
CHALTU
WABEEJA
MAITEKA
YUSPAGARÁTAM
HUI
DHANYAADAAD
AHHA
ATTO
MERSI
SPASIBO
DENKAUJA
NENACHALHYA
UNALCHÉESH
GUI
HATUR
EKOJU
SIKOMO
MAKETAI
MINMONCHAR
SANCO
MERASTAWHY
GAEJTHO
LAH
TAVTAPUCH
MEDAWAGSE
AGUYJE
FAKAAUE
BAIKA