Conexión troncal entre los switches de las series Catalyst 4500/4000, 5500/5000 y 6500/6000 que usan encapsulación 802.1Q con el software del sistema CatOS de Cisco

Contenido

Introducción

Este documento presenta el concepto de trunking entre dos switches de Ethernet y se centra en la norma de trunking IEEE 802.1Q. Después de una breve descripción del mecanismo del trunking 802.1Q, el documento describe la implementación en los switches Catalyst 4500/4000, 5500/5000, and 6500/6000 Series. Se proporciona un ejemplo completo, junto con algunos errores comunes relacionados con la configuración de trunking 802.1Q con el uso del software del sistema Catalyst OS (CatOS). Para obtener ejemplos de trunking 802.1Q con el software del sistema Cisco IOS®, consulte Configuración del Trunking 802.1Q entre un Catalyst 3550/3560/3750 y Switches Catalyst que Ejecutan Cisco IOS Software.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

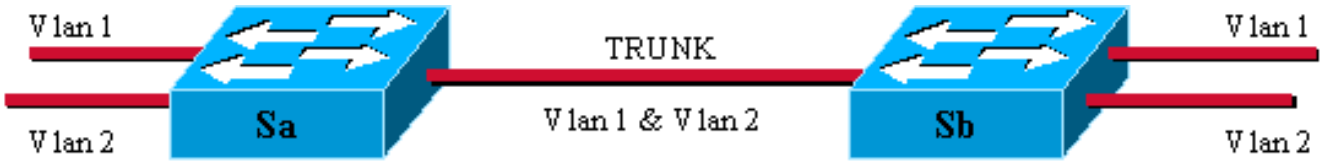
Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Qué es una conexión troncal.

En la terminología de Cisco, un trunk es un link punto a punto que transporta varias VLAN. El propósito de un trunk es guardar los puertos cuando se crea un link entre dos dispositivos que implementan VLAN, por lo general dos switches. En este diagrama, hay dos VLAN que desea tener disponibles en dos switches, Sa y Sb. El primer método fácil de implementar es crear dos links físicos entre los dispositivos. Los links físicos llevan el tráfico para una VLAN:

Por supuesto, esta solución no puede ampliarse. Si desea agregar una tercera VLAN, debe sacrificar dos puertos adicionales. Este diseño también es ineficiente en términos de distribución de carga; es posible que el tráfico en algunas VLAN no justifique un link dedicado. Un tronco agrupa links virtuales sobre un link físico, como muestra este diagrama:



Aquí, el único link físico entre los dos switches puede trasladar el tráfico para cualquier VLAN. Para lograr esto, cada trama enviada en el link es etiquetada por Sa de modo que Sb conozca la VLAN a la que pertenece. Existen diferentes esquemas de etiquetado. Los segmentos Ethernet más comunes son:

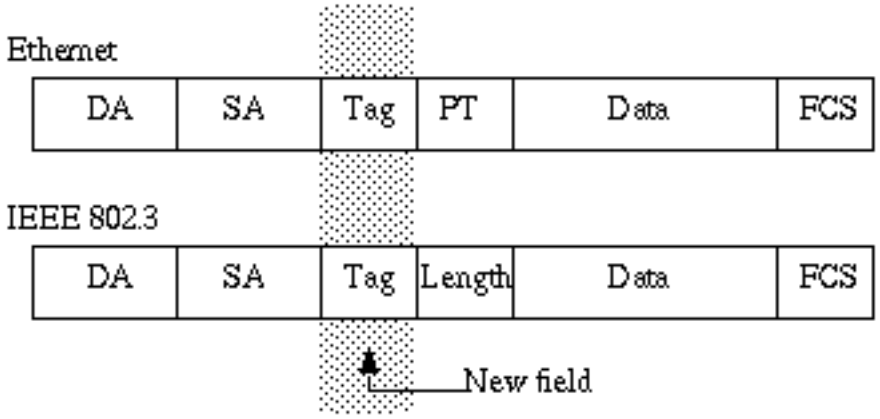
- Inter-Switch Link (ISL) (el protocolo ISL propietario original de Cisco)
- 802.1Q (el estándar IEEE en el que se centra este documento)

Características básicas del enlace troncal 802.1q

Mecanismo de etiquetado

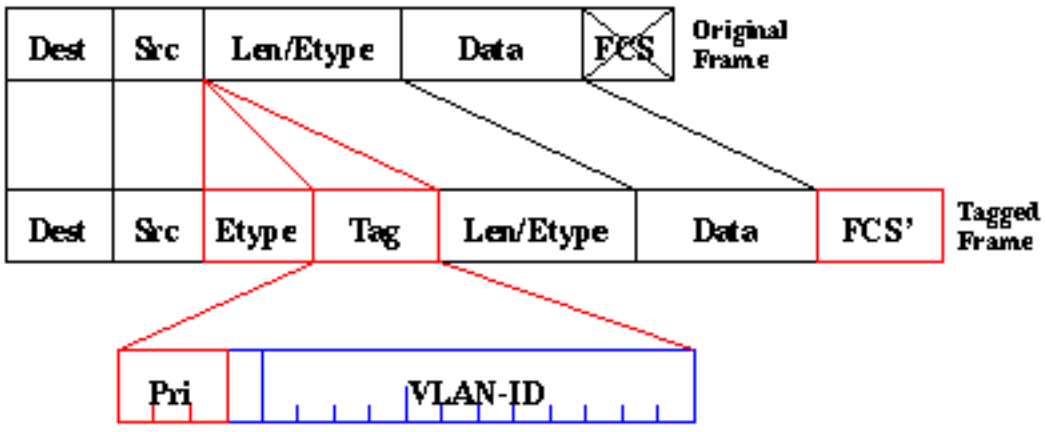
802.1Q usa un mecanismo de etiquetado interno. Interno significa que se inserta una etiqueta dentro del marco:

Nota: Con ISL, la trama se encapsula en su lugar.



Nota: En un tronco 802.1Q, una VLAN NO está etiquetada. Esta VLAN, denominada VLAN nativa, debe configurarse de la misma forma en ambos lados del tronco. De esta manera, puede deducir a qué VLAN pertenece una trama cuando recibe una trama sin etiqueta.

El mecanismo de etiquetado implica una modificación del marco; el dispositivo de enlace troncal inserta una etiqueta de 4 bytes y vuelve a calcular la secuencia de verificación de tramas (FCS):

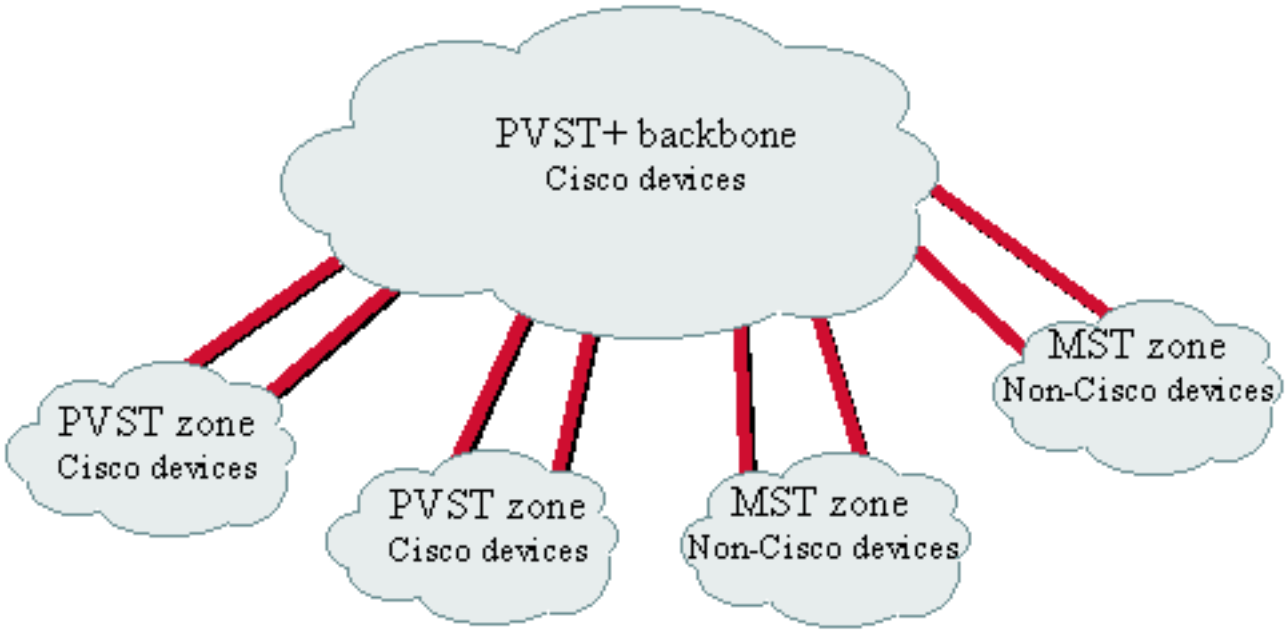


El campo EtherType que identifica la trama 802.1Q es 0x8100. Además del VLAN-ID de 12 bits, se reservan 3 bits para el etiquetado de prioridad IEEE 802.1p.

Nota: Al insertar una etiqueta en una trama que ya tiene el tamaño máximo de Ethernet, se crea una trama de 1522 bytes que el equipo receptor puede considerar un "baby gigante". El comité IEEE 802.3 está ampliando el tamaño máximo de trama estándar para abordar este problema.

Consideración de árbol de expansión

El estándar 802.1Q es más que un simple mecanismo de etiquetado. También define una instancia única de spanning tree que se ejecuta en la VLAN nativa para todas las VLAN en la red. Esta red de árbol de extensión único (MST) carece de cierta flexibilidad en comparación con una red de árbol de extensión por VLAN (PVST) que ejecuta una instancia del protocolo de árbol de extensión (STP) por VLAN. Cisco desarrolló PVST+ para permitir la ejecución de varias instancias de STP (incluso en una red 802.1Q) mediante un mecanismo de tunelización. Aunque va más allá del alcance de este documento, se puede describir brevemente como el uso de un dispositivo Cisco para conectar una zona MST (normalmente la red basada en 802.1Q de otro proveedor) a una zona PVST (normalmente una red basada en Cisco ISL). No hay una configuración específica que ingresar para lograr esto. Idealmente, un entorno mixto debería tener el siguiente aspecto:



No direct trunk can be established between a MST and PVST zone.
There has to be a PVST+ zone in between.

Implementación de Cisco

En la implementación actual, los dispositivos de Cisco admiten sólo números de VLAN hasta 1005. Esta restricción, introducida para coincidir con el número de VLAN disponibles con ISL, está permitida por el estándar 802.1Q. Cisco implementó una función de mapeo de VLAN en CatOS 5.1 para simplificar la interoperabilidad con otros dispositivos proveedores, pero rara vez es necesaria.

Nota: Consulte Configuración de VLAN para obtener información sobre la función de mapping de VLAN.

Cisco también adaptó su protocolo dinámico ISL (DISL) y lo transformó en un protocolo de concentración de enlaces dinámico (DTP). DISL puede negociar enlaces troncales ISL en un link entre dos dispositivos; Además, DTP puede negociar el tipo de encapsulado de conexión de troncal (802.1Q o ISL) que también se utilizará. Se trata de una función interesante, ya que

algunos dispositivos de Cisco solo admiten ISL o 802.1Q, mientras que otros pueden ejecutar ambos.

En la implementación de Cisco, un tronco es un link punto a punto, aunque es posible utilizar la encapsulación 802.1Q en un segmento de Ethernet compartido por más de dos dispositivos. Esta configuración rara vez es necesaria, pero todavía es posible con la inhabilitación de la negociación DTP.

Configuración de troncales 802.1Q

Requisitos de hardware y software

Desde el punto de vista del software, la primera aparición de la encapsulación 802.1Q fue con el software CatOS 4.1. En esta versión, la configuración de trunking tuvo que ser codificada; DTP solo apareció con CatOS 4.2. Vea la sección Modos DTP de este documento.

No todos los puertos Catalyst admiten encapsulación 802.1Q. Actualmente, mientras que los switches Catalyst 4500/4000 sólo admiten 802.1Q, los puertos de las series Catalyst 6500/6000 pueden utilizar la encapsulación 802.1Q o ISL. Según el módulo, los puertos compatibles con troncales Catalyst 5500/5000 pueden utilizar encapsulación 802.1Q, encapsulación ISL o ambos. La mejor manera de verificar esto es usar el comando **show port capabilities**. La capacidad de conexión de troncal se establece en forma explícita:

```
Sa> (enable) show port capabilities 1/1
Model                     WS-X5530
Port                      1/1
Type                      1000BaseSX
Speed                     1000
Duplex                    full
Trunk encap type          802.1Q,ISL
Trunk mode                on,off,desirable,auto,nonegotiate
Channel                   no
Broadcast suppression     percentage(0-100)
Flow control              receive-(off,on,desired),send-(off,on,desired)
Security                  no
Membership                static
Fast start                yes
Rewrite                   no
```

Modos de DTP

Cuando configura un puerto para el trunking, puede establecer dos parámetros: el modo de conexión troncal y el tipo de encapsulación (si dicho puerto es compatible con DTP).

- El modo troncal define la forma en que el puerto negociará la configuración de un tronco con el puerto del par. A continuación se muestra una lista de los ajustes posibles:Tenga cuidado ya que ciertos modos (encendido, no negociación, apagado) especifican expresamente en qué estado finalizará el puerto. Una configuración incorrecta puede conducir a un estado peligroso e incoherente en el que un lado se conecta mediante trunking y el otro no.Un puerto en encendido, automático o deseable envía tramas DTP en forma regular. Un puerto de enlace troncal en *auto* o *desirable* regresa a no trunking si no recibe una actualización de DTP de su vecino en el término de 5 minutos.**Nota:** Si ejecuta el software CatOS 4.1, debe

inhabilitar cualquier forma de negociación usando el modo ***apagado*** o ***no negociación*** cuando configure el enlace troncal 802.1Q.
- El tipo de encapsulación le permite especificar al usuario si debe utilizarse 802.1Q o ISL cuando se configura el tronco. Por supuesto, el parámetro sólo es relevante si el módulo que utiliza puede utilizar ambos. El parámetro puede tener tres valores distintos:

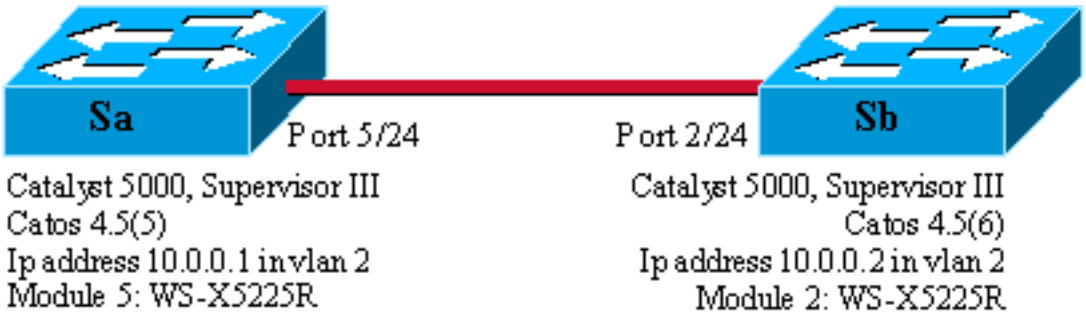
Refiérase a la sección *Resultados de Posibles Configuraciones de Troncal Fast Ethernet y Gigabit Ethernet de* Configuración de Trunks VLAN en Puertos Fast Ethernet y Gigabit Ethernet para obtener una lista de todas las configuraciones posibles resultantes.

Nota: No se llevará a cabo ninguna negociación entre dos switches en diferentes dominios de protocolo de troncal de VLAN (VTP). Consulte Configuración de VTP.

Ejemplo paso a paso

Diagrama de la red

Este ejemplo se basa en una configuración de laboratorio muy sencilla que implica dos switches Catalyst 5500/5000 que se vinculan a través de puertos con capacidad troncal. Para interconectar dos switches, se necesita un cable de cruce.



Configuración mínima de un troncal 802.1Q con pruebas de conectividad

Complete estos pasos:

1. Verifique que los estados de los puertos estén activos pero no de trunking.Conecte un terminal a la consola de los switches. Consulte el documento Conexión de un Terminal al Puerto de la Consola en los Catalyst Switches si fuera necesario. Primero, verifique el estado del puerto involucrado en la configuración. Utilice el comando **show port 5/24** en Sa (**show port 2/24** en Sb) y verifique que el estado esté conectado:

```
Sa> (enable) show port 5/24
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 5/24                    connected  1          normal a-full a-100 10/100BaseTX
!--- Output suppressed.
```

   Tiene el valor predeterminado para ese tipo de puerto. Se produjo al negociar el dúplex completo de 100 MB y se asigna a la VLAN 1. Ejecute el comando **show trunk 5/24** para ver claramente que el puerto no está realizando la conexión troncal y tiene una negociación de encapsulación y auto de modo predeterminado.

```
Sa> (enable) show trunk 5/24
Port      Mode         Encapsulation  Status        Native vlan
```

```
--------  -----------  -------------  ------------  -----------
 5/24     auto         negotiate      not-trunking  1
!--- Output suppressed.
```

2. Establezca una dirección IP en las interfaces de administración sc0.Utilice el comando **set interface sc0 10.0.0.1** en el switch Sa y el comando **set interface sc0 10.0.0.2** en el switch Sb para asignar una dirección IP a los dos switches. El comando **show interface** confirma que la interfaz de administración ahora está configurada correctamente en la VLAN 1 predeterminada:

```
Sa> (enable) set interface sc0 10.0.0.1
Interface sc0 IP address set.

Sa> (enable) show interface
sl0: flags=51<,POINTOPOINT,RUNNING>
        slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
        vlan 1 inet 10.0.0.1 netmask 255.0.0.0 broadcast 10.255.255.255
Sa> (enable)
```

   Si tiene el resultado de un comando **show interface** de su dispositivo Cisco, puede utilizar Output Interpreter (sólo clientes registrados) para mostrar posibles problemas y soluciones.

3. Verifique la conectividad entre Sa y Sb.Ejecute el comando **ping 10.0.0.2** del switch Sa para probar que el switch Sb ahora se puede alcanzar:

```
Sa> (enable) ping 10.0.0.2
10.0.0.2 is alive
Sa> (enable)
```

4. Configure el mismo dominio VTP en ambos switches.Ahora asigne el mismo dominio VTP a ambos switches. Como vio, tener el mismo dominio VTP es obligatorio para utilizar la negociación DTP. Ejecute el comando **set vtp domain cisco en ambos switches para configurarlos con el nombre de dominio "cisco":**

```
Sa> (enable) set vtp domain cisco
VTP domain cisco modified
Sa> (enable)
```

5. Cree una VLAN 2 en cada switch.Ejecute el comando **set vlan 2** en ambos switches para crear la VLAN 2. Si los switches ya estaban enlazados por un trunk, sólo tendría que ejecutar el comando en un switch y el otro switch lo aprendería automáticamente a través de VTP. Como todavía no tiene un trunk, no hay comunicación VTP entre Sa y Sb:

```
Sa> (enable) set vlan 2
Vlan 2 configuration successful
Sa> (enable)
```

6. Cambie las interfaces de administración a VLAN 2.Ahora mueve la interfaz de administración de ambos switches a la VLAN 2. De esta manera, usted muestra que no hay comunicación entre Sa y Sb antes de que se establezca un trunk. Ejecute el comando **set interface sc0 2** en cada switch para mover la interfaz sc0 en la VLAN 2. Ejecute el comando **show interface** para verificar que el comando es efectivo:

```
Sa> (enable) set interface sc0 2
Interface sc0 vlan set.
Sa> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
        slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
        vlan 2 inet 10.0.0.1 netmask 255.0.0.0 broadcast 10.255.255.255
Sa> (enable)
```

7. Verifique si se cortó la conectividad entre los dos switches.Ahora el **ping 10.0.0.2** a Sb falla desde Sa, lo que prueba que no hay conectividad en VLAN 2 entre los switches:

```
Sa> (enable) ping 10.0.0.2
no answer from 10.0.0.2
Sa> (enable)
```

8. Verifique las funciones del puerto.Antes de comenzar a configurar un trunk, puede verificar con el comando show port capabilities que ambos puertos pueden implementar el trunking 802.1Q:

```
Sa> (enable) show port capabilities 5/24
Model                   WS-X5225R
Port                    5/24
Type                    10/100BaseTX
Speed                   auto,10,100
Duplex                  half,full
Trunk encap type        802.1Q,ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 5/23-24,5/21-24
Broadcast suppression   percentage(0-100)
Flow control            receive-(off,on),send-(off,on)
Security                yes
Membership              static,dynamic
Fast start              yes
Rewrite                 yes
Sa> (enable)
```

9. Configure la encapsulación de enlace troncal para que sea 802.1Q.Ahora se debe configurar la troncal en SA. En el Paso 1, observó que ambos puertos se encontraban en el modo de concentración de enlaces predeterminado automático, negociación de tipo de encapsulación. Una combinación automático-automático no hace que el enlace troncal aparezca. Esto es normal; cada lado desea convertirse en un troncal pero sólo lo harán si el remoto lo solicita. Teniendo en cuenta la configuración predeterminada:Solo tiene que cambiar el modo troncal a deseable en un lado para activar el tronco. Esto se debe a que un puerto en modo deseable notifica a su vecino que desea ir a la conexión troncal. Como el mando a distancia (en modo automático) va al enlace troncal si se le solicita, esto es suficiente para activar el tronco.Si configura el dot1q de encapsulación en una subinterfaz, esto significa que esa VLAN no se puede volver a utilizar en el sistema desde internamente, el 6500 o el 7600 asignan la VLAN y luego hacen que esa subinterfaz sea el único miembro de ella. Por lo tanto, no es posible tener una VLAN y luego intentar usarla en una subinterfaz o viceversa. Para solucionar ese problema, en lugar de subinterfaces, cree puertos trunk y de esa manera la VLAN se pueda ver en todas las interfaces. Si se requieren subinterfaces, las VLAN agregadas en las subinterfaces no se pueden utilizar en otros puertos.También debe especificar qué encapsulación desea utilizar. Esto se debe a que ambos puertos son compatibles con ISL y esta encapsulación se elige primero cuando ambos extremos están en modo de negociación.La sintaxis del comando es la siguiente: **set trunk** ***module/port*** **[on | desactivado | deseable | auto | nonegotiate] [vlan_range] [isl | dot1q | negociar]**. Ejecute el comando set trunk 5/24 dot1q desirable en el switch Sa:

```
Sa> (enable) set trunk 5/24 dot1q desirable
Port(s) 5/24 trunk mode set to desirable.
Port(s) 5/24 trunk type set to dot1q.
1997 May 07 17:32:01 %DTP-5-TRUNKPORTON:Port 5/24 has become dot1q trunk
1997 May 07 17:32:02 %PAGP-5-PORTFROMSTP:Port 5/24 left bridge port 5/24
1997 May 07 17:32:13 %PAGP-5-PORTTOSTP:Port 5/24 joined bridge port 5/24
```

10. Verifique que el tronco esté activo.El registro de la consola del comando anterior muestra claramente que el puerto se movió al trunking, pero también puede ejecutar el comando show trunk 5/24 en Sa y el comando show trunk 2/24 en Sb para verificar. Puede observar una diferencia sutil entre los dos resultados:El puerto en Sa se encuentra en el modo deseado, mientras que el puerto Sb se encuentra en el modo automático.Más interesante aún, la encapsulación es dot1q en Sa mientras que es **n-dot1q** en Sb. Esto es para mostrar que Sb negoció su encapsulación a dot1q. Si no especificó una encapsulación en Sa,

ambos puertos habrían terminado en la encapsulación n-isl:

```
Sa> (enable) show trunk 5/24
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 5/24     desirable    dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ------------------------------------------------------------
 5/24     1-1005

Port      Vlans allowed and active in management domain
--------  ------------------------------------------------------------
 5/24     1-2

Port      Vlans in spanning tree forwarding state and not pruned
--------  ------------------------------------------------------------
 5/24     1-2
Sa> (enable)
Sb> (enable) show trunk 2/24
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/24     auto         n-dot1q        trunking      1
!--- Output suppressed.
```

Si tiene el resultado de un comando **show trunk** de su dispositivo Cisco, puede utilizar Output Interpreter (sólo clientes registrados) para mostrar posibles problemas y soluciones.

11. Compruebe la conectividad.Puede verificar que la VLAN 2 está atravesando su tronco simplemente haciendo ping a Sb desde Sa:

```
Sa> (enable) ping 10.0.0.2
10.0.0.2 is alive
Sa> (enable)
```

Configure la VLAN nativa

Complete estos pasos:

1. Ejecute el comando **set vlan**.El comando set vlan 2 5/24 se utiliza para asignar un puerto a una VLAN específica. En el caso de un puerto de enlace troncal, cambia la VLAN nativa a VLAN 2. Por supuesto, hay que hacer lo mismo en Sb con set vlan 2 2/24 :

```
Sa> (enable) set vlan 2 5/24
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ----------------------
2     5/24

Sa> (enable)
```

Antes de cambiar la VLAN nativa en Sb, ahora hay una inconsistencia entre la configuración Sa y Sb. Los dos extremos del tronco no tienen la misma configuración de VLAN nativa. Aquí, se muestran algunos mensajes de advertencia en la consola Sb.**Nota:** El switch que informa de la inconsistencia puede variar, lo que depende de cuál es el root bridge para las VLAN 1 y 2.

```
Sb> (enable) 2000 Dec 07 16:31:24 %SPANTREE-2-RX_1QPVIDERR: Rcved
pvid_inc BPDU on 1Q port 2/24 vlan 1.
2000 Dec 07 16:31:24 %SPANTREE-2-TX_BLKPORTPVID: Block 2/24 on xmtting
vlan 2 for inc peer vlan.
2000 Dec 07 16:31:24 %SPANTREE-2-RX_BLKPORTPVID: Block 2/24 on rcving
vlan 1 for inc peer vlan 2.
```

```
Sb> (enable)
Sb> (enable) set vlan 2 2/24
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ----------------------
2     2/24
Sb> (enable) 2000 Dec 07 16:31:46 %SPANTREE-2-PORTUNBLK: Unblock
previously inc port 2/24 on vlan 1.
2000 Dec 07 16:31:48 %SPANTREE-2-PORTUNBLK: Unblock previously inc
port 2/24 on vlan 2.
```

La discordancia de VLAN nativa se corrigió y ahora todo vuelve a la normalidad.

2. Compruebe el resultado.Ahora simplemente verifique el resultado de estos comandos en su tronco con el uso del comando show trunk 5/24:

```
Sa> (enable) show trunk 5/24
 Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 5/24     desirable    dot1q          trunking      2

<
```

Especifique las VLAN permitidas en el tronco

Complete estos pasos:

1. Cree VLAN adicionales.Cuando crea un nuevo tronco, éste transporta de manera predeterminada todas las VLAN de la red. Verá cómo restringir la lista de VLAN permitidas en un trunk. Primero, debe crear dos VLAN adicionales (3 y 4). Puede ejecutar el comando set vlan 3 y el comando set vlan 4 en Sa, por ejemplo, para crear las VLAN adicionales. Sólo necesita ingresar el comando en un switch; VTP propaga esta información al otro switch.**Nota:** Esta parte de la configuración es absolutamente la misma si se utiliza la encapsulación 802.1Q o ISL.

```
Sa> (enable) set vlan 3
Vlan 3 configuration successful
Sa> (enable) set vlan 4
Vlan 4 configuration successful
```

2. Eliminar las VLAN del tronco.El comando **clear trunk** *module/port vlan-list* le permite quitar una o varias VLAN de un trunk dado. Aquí, las cuatro VLAN que creó se definieron en su tronco. Quite VLAN 2 y VLAN 3 con el uso del comando clear trunk 5/24 2-3 en Sa y el comando clear trunk 2/24 2-3 en Sb. Puede verificar el resultado del comando **clear** con el comando show trunk 5/24 . Sólo las VLAN 1 y 4 ahora cruzan el tronco entre Sa y Sb. Un ping entre Sa y Sb ahora falla:

```
Sa> (enable) clear trunk 5/24 2-3
Removing Vlan(s) 2-3 from allowed list.
Port 5/24 allowed vlans modified to 1,4-1005.
Sa> (enable) show trunk 5/24
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 5/24     desirable    dot1q          trunking      2

Port      Vlans allowed on trunk
--------  ----------------------------------------------------------
 5/24     1,4-1005

Port      Vlans allowed and active in management domain
--------  ----------------------------------------------------------
 5/24     1,4
```

```
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------
 5/24     1,4
```

3. Reactivación de una VLAN.Para agregar una VLAN nuevamente en un trunk, utilice el comando set trunk *module/port vlan-list*.

```
Sa> (enable) set trunk 5/24 2
Adding vlans 2 to allowed list.
Port(s) 5/24 allowed vlans modified to 1-2,4-1005.
Sa> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 5/24     desirable    dot1q          trunking      2

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------
 5/24     1-2,4-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------
 5/24     1-2,4

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------
 5/24     1-2,4
```

La VLAN 2 fluye ahora de nuevo en el tronco. Es posible realizar un ping de Sa a Sb.

Errores comunes

Distintas VLAN nativas

Este es un error de configuración frecuente. La VLAN nativa que se configura en cada extremo de un troncal 802.1Q debe ser la misma. Recuerde que un switch que recibe una trama no etiquetada la asigna a la VLAN nativa del tronco. Si un extremo se configura para VLAN 1 nativa y el otro para VLAN 2 nativa, una trama que se envía en VLAN 1 en un lado se recibe en VLAN 2 en el otro. Esto da como resultado la combinación de VLAN 1 y 2. No hay ninguna razón para desearlo, y puede implicar algunos problemas de conectividad en su red.

Un dispositivo Cisco normalmente le advierte de una discordancia VLAN nativa. Consulte el Paso 1 de la sección Establecer la VLAN nativa para ver el tipo de mensajes de error que recibe en la consola en este caso. Verifique siempre que la VLAN nativa sea la misma en la configuración troncal de sus switches.

Dominios VTP diferentes

Cuando cree un trunk entre dos switches y utilice la negociación DTP, verifique dos veces que el dominio VTP configurado en ambos switches sea el mismo. La negociación no tiene lugar entre dos switches que se encuentran en diferentes dominios VTP. El ejemplo de esta sección toma la configuración de trunking en funcionamiento que se describe anteriormente.

Nota: Incluso si dos switches están en diferentes dominios VTP, puede hacer que estos switches se comuniquen entre sí si agrega VLAN manualmente en cada switch. Aunque hay una discordancia de dominio VTP, la comunicación VLAN funciona bien. Sin embargo, las actualizaciones de VTP no se propagan a través de este link en esa VLAN porque los dominios son diferentes.

- Sa in trunking mode desirable, encapsulation dot1q
- Sb en modo de concentración de enlaces definido en automático, negocia la encapsulación
- La misma VLAN nativa y las mismas VLAN permitidas en cada lado

La única diferencia es que asigna el dominio VTP "c" en el dominio Sa y VTP "**cisco**" en Sb:

```
Sa> (enable) show trunk
No ports trunking.
Sa> (enable) show trunk 5/24
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 5/24     desirable    dot1q          not-trunking  1

Port      Vlans allowed on trunk
--------  ------------------------------------------------------------
 5/24     1-1005

Port      Vlans allowed and active in management domain
--------  ------------------------------------------------------------
 5/24     1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ------------------------------------------------------------
 5/24


Sb> (enable) show trunk
No ports trunking.
Sb> (enable) show trunk 2/24
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/24     auto         negotiate      not-trunking  1

Port      Vlans allowed on trunk
--------  ------------------------------------------------------------
 2/24     1-1005

Port      Vlans allowed and active in management domain
--------  ------------------------------------------------------------
 2/24     1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ------------------------------------------------------------
 2/24
Sb> (enable)
```

Pueden ver que el tronco no apareció. Cuando vea ese tipo de problema, verifique el dominio VTP configurado en los switches. Ejecute el comando [show vtp domain:]

```
Sa> (enable) show vtp domain
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
c                              1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
8          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
10.0.0.1        disabled disabled 2-1000
```

```
Sb> (enable) show vtp domain
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
cisco                          1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- -------------- -------------
8          1023            20             disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
10.0.0.1        disabled disabled 2-1000
```

Ahora coloque el switch Sa en el dominio VTP "cisco" con el uso del comando set vtp domain cisco. Después de unos segundos, el tronco se negocia y se activa de nuevo:

```
Sa> (enable) set vtp domain cisco
VTP domain cisco modified
Sa> (enable) 1997 May 13 13:59:22 %DTP-5-TRUNKPORTON:Port 5/24 has become dot1q trunk
1997 May 13 13:59:22 %PAGP-5-PORTFROMSTP:Port 5/24 left bridge port 5/24
1997 May 13 13:59:33 %PAGP-5-PORTTOSTP:Port 5/24 joined bridge port 5/24
```

Si desea mantener diferentes dominios VTP pero aun así crear un tronco entre dos switches, debe codificar el trunking en cada lado del tronco (con el uso de no negociación/encendido).

Error al intentar eliminar VLAN de rango extendido de un puerto troncal

Cuando intenta eliminar las VLAN de rango extendido de un puerto trunk con el uso del comando clear trunk, este error a veces se muestra en la consola del switch:

```
Failed to clear vlans in the extended range Maximum of 64 trunks can have
non-default extended range vlan configuration. Use the 'set trunk' command to restore
some existing entries to the default value.
```

Nota: El término *extended range* incluye cualquier VLAN entre 1025 y 4094. El término *rango extendido predeterminado* incluye todas las VLAN del 1025 al 4094. Si intenta borrar cualquier VLAN en el rango de 1025 a 4094, la VLAN se convierte en *rango extendido no predeterminado*. El número máximo de troncales que pasan *un rango extendido no predeterminado* es 64. Esto incluye los trunks inactivos y activos.

Este error y la limitación de 64 troncales provienen del bloque NVRAM que se utiliza para almacenar configuraciones no predeterminadas para VLAN de rango extendido. Si ejecuta el comando show trunk extended-range, puede ver todos los troncos configurados con rangos extendidos no predeterminados. De forma predeterminada, toda la configuración se almacena en NVRAM. NVRAM tiene diferentes "bloques" para guardar las configuraciones no predeterminadas. Los bloques se colocan en diferentes categorías, como global o module. El bloque que contiene la configuración no predeterminada para los rangos extendidos tiene una limitación de 64 troncales.

Hay dos soluciones alternativas para reducir el número de troncales de rango extendido no predeterminados. El primer método es configurar cualquiera de los puertos troncales no activos/no utilizados de nuevo en las VLAN predeterminadas permitidas. Utilice el comando set trunk *mod/port* 1025-4094 . A continuación, el comando **clear trunk** *mod/port* **1025-4094** debe funcionar para las VLAN extendidas. La segunda solución consiste en cambiar el modo de

configuración del modo binario (predeterminado) al modo de texto. Utilice el comando **set config mode text** para cambiar el modo de configuración al modo de texto. El modo de texto normalmente utiliza menos espacio de memoria NVRAM o Flash que el modo de configuración binaria.

Nota: Cuando funciona en el modo de configuración de archivos de texto, la mayoría de las configuraciones de usuario no se guardan inmediatamente en NVRAM; los cambios de configuración sólo se escriben en DRAM. Debe ejecutar el comando **write memory** para almacenar la configuración en el almacenamiento no volátil. Utilice el comando **set config mode text auto-save** para guardar automáticamente la configuración de texto en NVRAM.

Modo de concentración de enlaces incompatible con el tipo de encapsulado

Este es un problema común que comenzó a plantearse al Soporte Técnico de Cisco cuando se enviaron los primeros módulos que pudieron soportar tanto 802.1Q como ISL. Las personas fueron usadas para la configuración de un trunk con el comando **set trunk** *module/port* **on** o el comando **set trunk** module/port **nonegotiate**. El problema es que, de forma predeterminada, el tipo de encapsulación está configurado para negociar. El tipo de encapsulación negociada sólo es soportado por los modos de trunking automático o deseable. Los tipos de encapsulación on y nonegotiate no realizan ninguna negociación entre los switches y deben configurarse de forma rígida en ISL o encapsulación 802.1Q cuando se configuran. A continuación se muestra un registro de lo que sucede en el switch en este caso:

```
Sa> (enable) set trunk 5/24 on
Failed to set port 5/24 to trunk mode on.
Trunk mode 'on' not allowed with trunk encapsulation type 'negotiate'.
Sa> (enable) set trunk 5/24 nonegotiate
Failed to set port 5/24 to trunk mode nonegotiate.
Trunk mode 'nonegotiate' not allowed with trunk encapsulation type
'negotiate'.
Sa> (enable)
```

Esto tiene sentido porque si no negocia con el mando a distancia, ¿cómo sabría qué tipo de encapsulación (802.1Q o ISL) utilizar para activar el tronco? Hay dos posibilidades:

- Utilice el modo deseable. En este caso, negocia el modo de encapsulación con el mando a distancia:
  ```
  Sa> (enable) set trunk 5/24 desirable
  Port(s) 5/24 trunk mode set to desirable.
  Sa> (enable) 1997 May 09 17:49:19 %DTP-5-TRUNKPORTON:Port 5/24 has become
  isl trunk
  ```
- Especifique la encapsulación que desea utilizar:
  ```
  Sa> (enable) set trunk 5/24 isl on
  Port(s) 5/24 trunk mode set to on.
  Port(s) 5/24 trunk type set to isl.
  Sa> (enable) 1997 May 09 17:50:16 %DTP-5-TRUNKPORTON:Port 5/24 has become
  isl trunk
  ```

Comandos usados en el documento

Resumen de Comandos

- ping

- set interface
- set trunk
- set vlan
- set vtp domain
- show interface
- show port
- show port capabilities
- show trunk
- show vtp domain

Información Relacionada

- Configuración de Trunking ISL en Switches de la Familia Catalyst 5500/5000 y 6500/6000
- Configuración de troncales VLAN en Fast Ethernet y puertos Ethernet Gigabit
- Comprensión y configuración del protocolo de troncal VLAN
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems