

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](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Qué es una conexión troncal.](#)

[Características básicas del enlace troncal 802.1q](#)

[Mecanismo de etiquetado](#)

[Consideración de árbol de expansión](#)

[Implementación de Cisco](#)

[Links troncales del 802.1Q de la configuración](#)

[Requisitos de hardware y software](#)

[Modos de DTP](#)

[Ejemplo paso a paso](#)

[Errores comunes](#)

[Distintas VLAN nativas](#)

[Dominios VTP diferentes](#)

[Error durante una tentativa de borrar los VLAN de alcances extendidos de un puerto troncal](#)

[Modo de concentración de enlaces incompatible con el tipo de encapsulado](#)

[Comandos usados en el documento](#)

[Resumen de Comandos](#)

[Información Relacionada](#)

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.](#)

prerrequisitos

Requisitos

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 Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Qué es una conexión troncal.

En terminología de Cisco, un trunk es un enlace punto a punto que lleva varios VLA N. El propósito de un trunk es salvar los puertos al establecer las relaciones entre dos dispositivos que implementen los VLA N, típicamente dos Switches. En este diagrama, hay dos VLA N que usted quiere tener disponible en dos Switches, Sa y Sb. El primer método sencillo a implementar es establecer dos vínculos físicos entre los dispositivos. Los vínculos físicos cada uno llevan el tráfico para un VLA N:



Por supuesto, esta solución no puede ampliarse. Si usted quiere agregar un tercer VLA N, usted debe sacrificar dos puertos adicionales. Este diseño es también ineficaz en términos de carga a compartir; el tráfico en algunos VLA N puede no alinear un link dedicado. Un trunk lía los links virtuales sobre un vínculo físico, pues este diagrama muestra:



Aquí, el único link físico entre los dos switches puede trasladar el tráfico para cualquier VLAN. Para alcanzar esto, cada trama enviada en el link es marcada con etiqueta por el Sa de modo que el Sb conozca el VLA N al cual pertenece. Diversos esquemas de Tagging existen. El mas comunes para los segmentos Ethernet son:

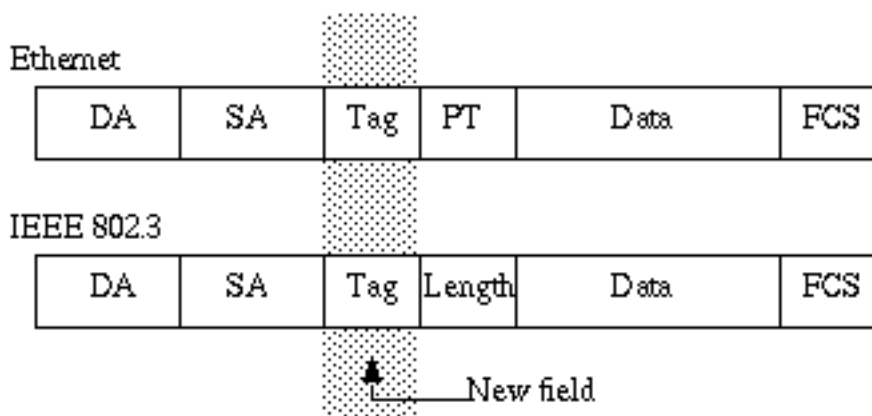
- Inter-Switch Link (ISL) (el protocolo ISL propietario original de Cisco)
- 802.1Q (la norma IEEE en la cual este documento se enfoca)

Características básicas del enlace troncal 802.1q

Mecanismo de etiquetado

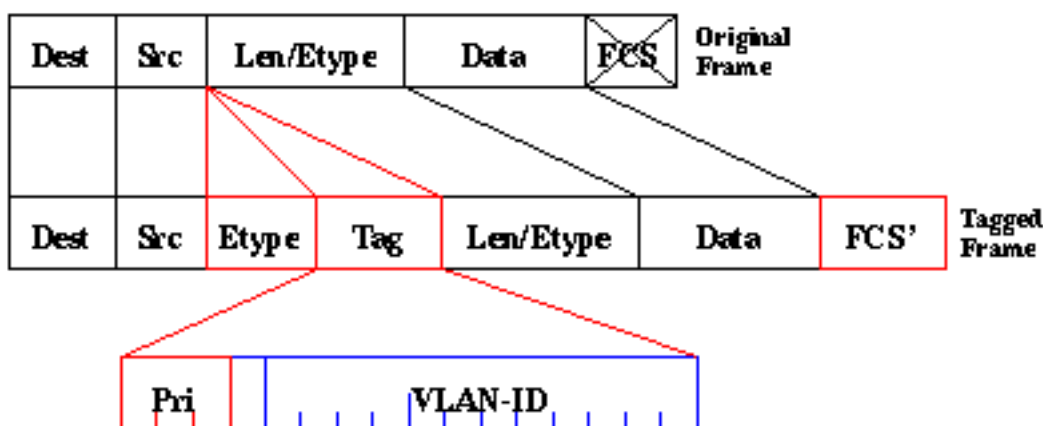
802.1Q usa un mecanismo de etiquetado interno. Interno significa que una etiqueta está insertada dentro de la trama:

Note: Con el ISL, la trama se encapsula en lugar de otro.



Note: En un tronco 802.1q, un VLAN no se marca con etiqueta. Esta VLAN, denominada VLAN nativa, debe configurarse de la misma forma en ambos lados del tronco. De esta manera, usted puede deducir a qué VLAN pertenece una trama cuando usted recibe una trama sin la etiqueta.

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

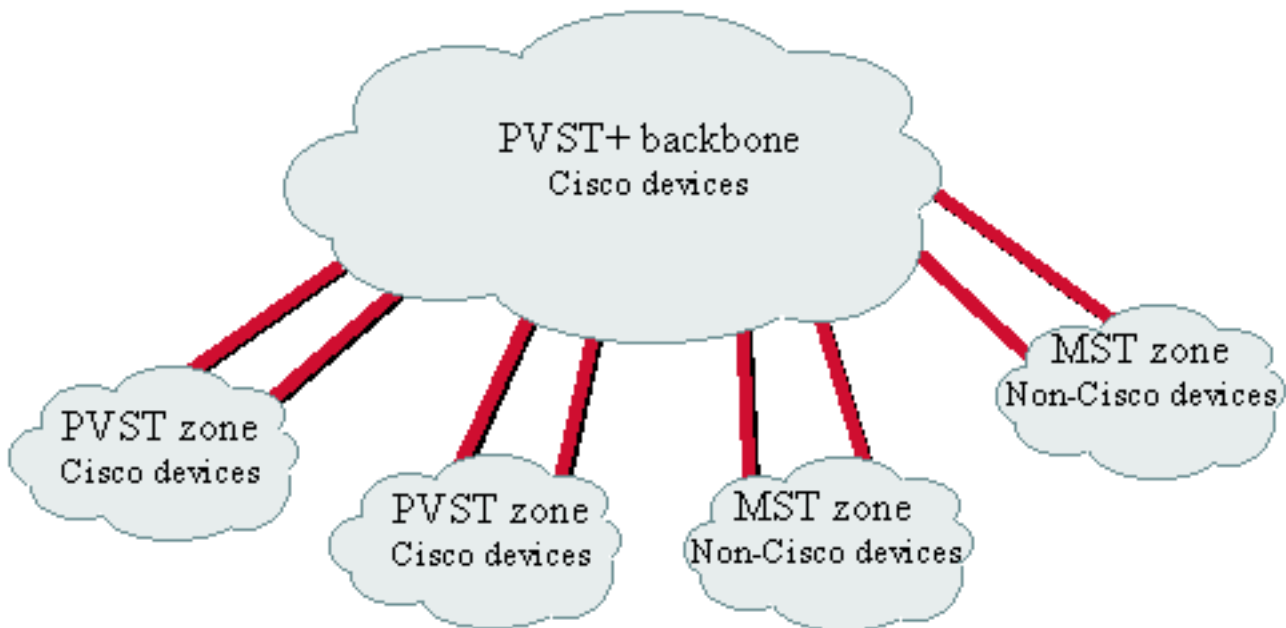


El campo del Ethertype que identifica la trama del 802.1Q es 0x8100. Además del 12-bit VLAN-ID, 3 bits son reservados para el etiquetado de prioridad del IEEE 802.1P.

Note: La inserción de una etiqueta en una trama que tenga ya el tamaño máximo de los Ethernetes crea trama de 1522 bytes que se puede considerar un "Baby Giant" por el equipo de recepción. El comité de IEEE 802.3 está ampliando el tamaño de trama estándar máximo para abordar este problema.

Consideración de árbol de expansión

El estándar del 802.1Q es más que apenas un mecanismo de Tagging. También define una instancia del árbol de expansión única que se ejecute en el VLAN nativo para todos los VLAN en la red. Una tan mono red del Spanning-tree (MST) falta una cierta flexibilidad con respecto a una red del Por VLAN Spanning Tree (PVST) que funcione con un caso del Spanning Tree Protocol (STP) por el VLAN. Cisco desarrolló el PVST+ para permitir el funcionar con de varios casos STP (incluso sobre una red del 802.1Q) usando un mecanismo de tunelización. Aunque fuera del alcance de este documento, pueda ser descrito abreviadamente como utilizar un dispositivo de Cisco para conectar una zona MST (típicamente la red 802.1Q-based de otro vendedor) con una zona PVST (típicamente una red ISL-basada Cisco). No hay configuración específica a ingresar para alcanzar esto. Idealmente, un entorno mezclado debe parecer este diagrama:



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, números VLAN del soporte de los dispositivos de Cisco solamente hasta 1005. Esta restricción, introducida para hacer juego el número de VLAN que estén disponibles con el ISL, es permitida por el estándar del 802.1Q. Cisco implementó un VLAN que asociaba la característica en CatOS 5.1 para simplificar la Interoperabilidad con los dispositivos del otro vendedor, pero es raramente necesario.

Note: Refiera a [configurar los VLAN](#) para la información sobre la característica de la asignación del VLAN.

Cisco también adaptó su protocolo dinámico ISL (DISL) y lo transformó en un protocolo de concentración de enlaces dinámico (DTP). El DISL puede negociar la conexión troncal de 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. Esto es una característica interesante pues algunos dispositivos de Cisco soportan solamente el ISL o el 802.1Q, mientras que algunos

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. Tal configuración es raramente necesaria pero es todavía posible con la incapacidad de la negociación DTP.

[Links troncales del 802.1Q de la configuración](#)

[Requisitos de hardware y software](#)

Desde un punto de vista del software, la primera aparición de la encapsulación del 802.1Q estaba con el software CatOS 4.1. En esta versión, la configuración de conexión de troncal tuvo que ser cifrada difícilmente; El DTP apareció solamente con CatOS 4.2. Vea la sección de los [modos DTP de](#) este documento.

No todos los puertos Catalyst soportan la encapsulación del 802.1Q. Actualmente, mientras que el Switches del Catalyst 4500/4000 soporta solamente el 802.1Q, los puertos de la serie del Catalyst 6500/6000 pueden utilizar el 802.1Q o la encapsulación ISL. Dependiendo del módulo, los puertos de la capacidad troncal del Catalyst 5500/5000 pueden utilizar la encapsulación, la encapsulación ISL, o ambas del 802.1Q. La mejor manera de marcar esto hacia fuera es utilizar el [comando show port capabilities](#). La capacidad de conexión de troncal se expone explícitamente:

```
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 usted configura un puerto para el enlace, usted puede fijar 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. Aquí está una lista de las configuraciones posibles: Tenga cuidado ya que ciertos modos (encendido, no negociación, apagado) especifican expresamente en qué estado finalizará el puerto. Una mala configuración puede llevar a un peligroso, estado incoherente en cuál el lado es enlace y no es el otro lado. Un puerto en encendido, automático o deseable envía tramas DTP en forma regular. Un puerto de troncal en *auto* o *deseable* vuelve a nontrunking si no recibe una actualización DTP de su vecino en el plazo de 5 minutos. **Note:** Si usted funciona con el software CatOS 4.1, usted debe inhabilitar cualquier

forma de negociación usando *apagado* o el *modo de no negociación* cuando usted configura el enlace del 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 es solamente relevante si el módulo que usted utiliza puede utilizar ambos. El parámetro puede tener tres valores distintos:

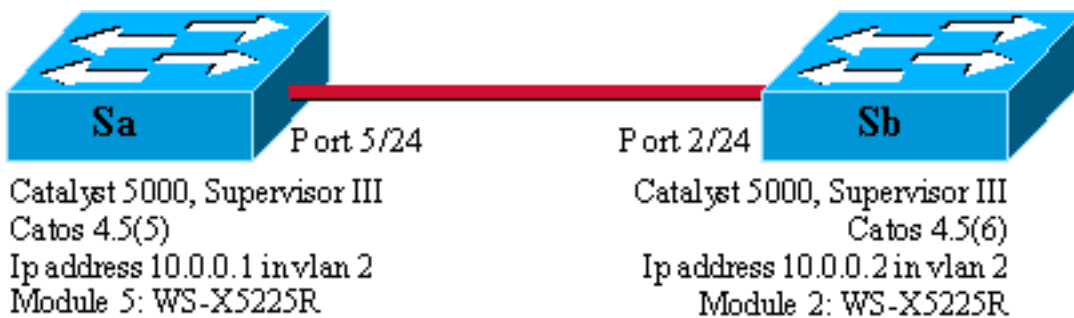
Refiera a los [resultados de la sección posible de los fast ethernet y de configuraciones del tronco de Gigabit Ethernet de configurar los troncales VLAN en los fast ethernet y los puertos Gigabit Ethernet](#) para una lista de todas las configuraciones resultantes posibles.

Note: Ninguna negociación ocurrirá entre dos Switches en diversos dominios del VLAN Trunk Protocol (VTP). Refiera a [configurar el VTP](#).

Ejemplo paso a paso

Diagrama de la red

Este ejemplo se basa en una configuración de laboratorio muy simple que implique dos Switches del Catalyst 5500/5000 que se conecte junto vía los puertos de la capacidad troncal. [Para interconectar dos switches, se necesita un cable de cruce.](#)



Configuración mínima de un tronco 802.1q con las pruebas de conectividad

Complete estos pasos:

1. Marque que los estatuses de los puertos son para arriba pero no enlace. Conecte un terminal a la consola de los switches. Refiera al documento [que conecta una terminal con el puerto de la consola en los switches de Catalyst](#) en caso necesario. Primero, marque el estatus del puerto que está implicado en la configuración. Utilice el [comando show port 5/24](#) en Sa ([puerto 2/24 de la demostración](#) en el Sb) y marque que el estatus está 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.
```

Usted tiene el valor predeterminado para eso bueno del puerto. Vino al negociar 100-MB por completo - el duplex, y él se asigna al VLA N 1. problemas el **comando show trunk 5/24** para ver claramente que el puerto no es enlace y hace que un auto y una encapsulación del modo predeterminado negocien.

```
Sa> (enable) show trunk 5/24
```

Port	Mode	Encapsulation	Status	Native vlan
5/24	auto	negotiate	not-trunking	1

!--- Output suppressed.

- Fije una dirección IP en las interfaces de administración del sc0. Utilice el comando de [10.0.0.1 del sc0 de la interfaz del conjunto](#) en Switch Sa y el comando de [10.0.0.2 del sc0 de la interfaz del conjunto](#) en el Sb del Switch para asignar una dirección IP al dos Switches. El [comando show interface](#) confirma que la interfaz de administración ahora está fijada correctamente en el VLAN predeterminado 1:

```
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 usted tiene la salida de un **comando show interface** de su dispositivo de Cisco, usted puede utilizar el [Output Interpreter \(clientes registrados solamente\)](#) para visualizar los problemas potenciales y los arreglos.

- Conectividad del control entre el Sa y el Sb. Publique el comando de [10.0.0.2 del ping](#) Switch Sa para probar que el Sb del Switch puede ahora ser alcanzado:

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

- Configure el mismo dominio VTP en ambo Switches. Ahora asigne el mismo dominio VTP a ambo Switches. Como usted vio, tener el mismo dominio VTP es obligatorio para utilizar la negociación DTP. Publique el [comando set vtp domain cisco](#) en ambo Switches para configurarlo con el Domain Name "Cisco":

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

- Cree una VLAN 2 en cada switch. Publique el [comando set vlan 2](#) en ambo Switches para crear el VLAN2. Si el Switches fuera conectado ya por un trunk, usted necesitaría solamente publicar el comando en un Switch, y el otro Switch lo aprendería automáticamente vía el VTP. Pues usted no tiene un trunk todavía, no hay comunicación VTP entre el Sa y el Sb:

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

- Cambie las interfaces de administración al VLAN2. Usted ahora se traslada la interfaz de administración de ambo Switches al VLA N 2. de esta manera, usted muestra que no hay comunicación entre el Sa y el Sb antes de que se establezca un trunk. Publique el [comando set interface sc0 2](#) en cada Switch para mover la interfaz del sc0 en el problema del VLA N 2. el [comando show interface](#) para marcar que el comando es eficaz:

```
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)
```

- Verifique si se cortó la conectividad entre los dos switches. Ahora el [ping 10.0.0.2 al Sb](#) falla del Sa, que prueba que no hay Conectividad en el VLAN2 entre el 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 que usted comience a configurar un trunk, usted puede marcar con el [comando show port capabilities](#) que ambos puertos pueden implementar el enlace del 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. Usted vio en el paso 1 que ambos puertos estaban en el modo de concentración de links definido en automático predeterminado, tipo de encapsulación negocia. 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. Con la consideración de la configuración predeterminada: Usted apenas necesita cambiar al modo tronco a deseable en un lado para traer el trunk para arriba. Esto es porque un puerto en el desirable mode notifica a su vecino que quiere ir enlace. Mientras que el telecontrol (en el modo automático) va al enlace si está indicado a, esto es bastante para traer el trunk para arriba. Si usted configura el dot1q de la encapsulación en una subinterfaz, ésta significa que ese VLA N no se puede utilizar otra vez en el sistema desde internamente, los 6500 o los 7600 afecta un aparato el VLA N y después hace esa subinterfaz al único miembro de él. No es tan posible tener un VLA N y después intentar utilizarlo en una subinterfaz o vice versa. Para reparar que el problema, en vez de las subinterfaces, crea los puertos troncales y que la manera el VLA N se puede considerar en todas las interfaces. Si se requieren las subinterfaces, después los VLA N agregados en las subinterfaces no se pueden utilizar en otros puertos. Usted también necesita especificar qué encapsulación usted quiere utilizar. Esto es porque ambos puertos son ISL capaz, y esta encapsulación se elige primero cuando son los ambos extremos adentro negocian el modo. La sintaxis del comando es la siguiente: **fije el /port del módulo troncal [en | desactivado | deseable | Auto | nonegocie] el [vlan_range] [isl | dot1q | negocie]**. Publique el [comando set trunk 5/24 dot1q desirable](#) en 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 trunk esté para arriba. El registro de la consola del comando anterior muestra claramente que el puerto se movió al enlace, solamente usted puede también publicar el [comando show trunk 5/24](#) en el Sa y el [comando show trunk 2/24](#) en el Sb para marcar. 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, la encapsulación es dot1q en el Sa mientras que es n-dot1q en el Sb. Éste es mostrar que el Sb negoció su encapsulación al dot1q. Si usted no especificara una encapsulación en el Sa, ambos puertos habrían terminado para arriba 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 usted tiene la salida de un comando **show trunk** de su dispositivo de Cisco, usted puede utilizar el [Output Interpreter \(clientes registrados solamente\)](#) para visualizar los problemas potenciales y los arreglos.

11. Conectividad del control. Usted puede marcar que el VLAN2 ahora está pasando a través de su trunk simplemente haciendo ping el Sb del Sa:

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

Fije el VLAN nativo

Complete estos pasos:

1. Publique el comando **set vlan**. Utilizan al [comando set vlan 2 5/24](#) de asignar un puerto a un VLA N específico. En el caso de un puerto de troncal, cambia el VLAN nativo al VLA N 2. por supuesto, usted necesita hacer lo mismo en el Sb con el [VLAN 2 2/24 del conjunto](#):

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

```
Sa> (enable)
```

Antes de que usted cambie el VLAN nativo en el Sb, ahora hay una inconsistencia entre la configuración Sa y del Sb. Los dos extremos del trunk no tienen la misma configuración de VLAN nativa. Aquí, algunos mensajes de advertencia se visualizan en la consola del Sb. **Note:** El Switch que señala la inconsistencia puede variar, de que depende cuál es el Root Bridge para los VLA N 1 y 2.

```
Sb> (enable) 2000 Dec 07 16:31:24 %SPANTRREE-2-RX_1QPVIDERR: Rcvd
pvid_inc BPDU on 1Q port 2/24 vlan 1.
2000 Dec 07 16:31:24 %SPANTRREE-2-TX_BLKPORTPVID: Block 2/24 on xmtting
vlan 2 for inc peer vlan.
2000 Dec 07 16:31:24 %SPANTRREE-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 %SPANTRREE-2-PORTUNBLK: Unblock
previously inc port 2/24 on vlan 1.
2000 Dec 07 16:31:48 %SPANTRREE-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 marque simplemente el resultado de estos comandos en su trunk 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 los VLA N que se permiten en el trunk](#)

Complete estos pasos:

1. Cree VLAN adicionales. Cuando crea un nuevo tronco, éste transporta de manera predeterminada todas las VLAN de la red. Usted verá cómo restringir la lista de VLA N permitidos en un trunk. Primero, usted debe crear dos VLA N adicionales (3 y 4). Usted puede publicar el [comando set vlan 3](#) y el [comando set vlan 4](#) en el Sa, por ejemplo, para crear los VLA N adicionales. Usted necesita solamente ingresar el comando en un Switch; El VTP propaga esta información al otro Switch. **Note:** Esta parte de la configuración es absolutamente lo mismo si el 802.1Q o la encapsulación ISL está utilizado.

```
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 permite que usted quite un o vario VLA N de un trunk dado. Aquí, los cuatro VLA N que usted creó fueron definidos en su trunk. Quite el VLAN2 y el VLAN3 con el uso del [comando clear trunk 5/24 2-3](#) en el Sa y el [comando clear trunk 2/24 2-3](#) en el Sb. Usted puede marcar el resultado del **comando clear** con el uso del [comando show trunk 5/24](#). Solamente los VLA N 1 y 4 ahora cruzan el trunk entre el Sa y el Sb. Un ping entre el Sa y el 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 un VLA N detrás 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

```

El VLAN2 ahora está fluyendo otra vez en el trunk. Un ping del Sa al Sb es posible.

Errores comunes

Distintas VLAN nativas

Esto es un Error de configuración frecuente. El VLAN nativo que se configura en cada extremo de un tronco 802.1q debe ser lo mismo. Recuerde que un Switch que recibe una trama nontagged la asigna al VLAN nativo del trunk. Si un extremo se configura para el VLAN nativo 1 y el otro al VLAN nativo 2, una trama que se envía en el VLAN1 en un lado se recibe en el VLAN2 en el otro. Esto da lugar a la fusión del VLAN1 y 2. No hay razón que usted querría eso, y puede implicar algunos problemas de conectividad en su red.

Un dispositivo de Cisco le advierte generalmente de una discrepancia de VLAN nativa. Vea que el paso 1 de la sección [fijó el VLAN nativo](#) para los mensajes del tipo de error que usted consigue en la consola en este caso. Marque siempre que el VLAN nativo es lo mismo en la configuración del tronco de su Switches.

Dominios VTP diferentes

Cuando usted crea un trunk entre dos Switches y usted utiliza la negociación DTP, compruebe con minuciosidad que el dominio VTP que se configura en ambo Switches es lo mismo. La negociación no ocurre entre dos Switches que esté en diversos dominios VTP. El ejemplo en esta sección toma la configuración de conexión de troncal de trabajo que se describe arriba.

Note: Incluso si dos Switches está en diversos dominios VTP, usted puede hacer que este Switches comunica con uno a si usted agrega los VLA N manualmente en cada Switch. Aunque haya una discordancia del dominio VTP, la comunicación de VLAN trabaja muy bien. Sin embargo, las actualizaciones VTP no se propagan a través de este link en ese VLA N porque los dominios son diferentes.

- Sa en el modo de concentración links deseable, dot1q de la encapsulación
- El Sb en el modo de concentración de links definido en automático, encapsulación negocia
- El mismo VLAN nativo, y los mismos VLA N permitidos en cada lado

La única diferencia es que usted asigna el dominio VTP “c” en el Sa y el dominio VTP “Cisco” en el 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)

Usted puede ver que no subió el trunk. Cuando usted ve esa clase de problema, marque el dominio VTP que se configura en el Switches. Publique 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 ponga Switch Sa en el dominio VTP “Cisco” con el uso del [comando set vtp domain cisco](#) Después de algunos segundos, el trunk se negocia y sube otra vez:

```
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 usted quiere guardar diversos dominios VTP pero todavía crear un trunk entre dos Switches, usted debe hard code trunking en cada lado del trunk (con el uso de nonegotiate/on).

[Error durante una tentativa de borrar los VLAN de alcances extendidos de un puerto troncal](#)

Cuando usted intenta borrar los VLAN de alcances extendidos de un puerto troncal con el uso del [comando clear trunk](#), este error se muestra a veces en la consola del Switch:

```
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
```

Note: El alcance extendido del término incluye cualquier VLA N a partir de 1025 a 4094. El alcance extendido del valor por defecto del término incluye todos los VLA N a partir de 1025 a 4094. Si usted intenta borrar cualquier VLA N en el rango a partir de 1025 a 4094, el VLA N se convierte en *alcance extendido no valor por defecto*. El número máximo de trunks que pasen el *alcance extendido no valor por defecto* es 64. Esto incluye inactivo y los troncales activos.

Este error y la limitación de 64 trunks vienen del bloque del NVRAM que se utiliza para salvar las configuraciones no predeterminadas para los VLAN de alcances extendidos. Si usted publica el [comando show trunk extended-range](#), usted puede ver todos los trunks que se configuran con los alcances extendidos del nondefault. Por abandono, la configuración completa se salva en el

NVRAM. El NVRAM tiene diversos “bloques” para guardar las configuraciones no predeterminadas. Los bloques se ponen en diversas categorías, tales como global o módulo. El bloque que lleva a cabo la configuración no predeterminada para los alcances extendidos tiene una limitación de 64 trunks.

Hay dos soluciones alternativas para reducir el número de trunks del alcance extendido del nondefault. El primer método es fijar los puertos troncales inactivos/inusitados a un valor por defecto no prohibido para los VLA N. Utilice el [comando set trunk mod/port 1025-4094](#). Entonces el **comando clear trunk mod/port 1025-4094** debe trabajar para los VLA N extendidos. La segunda medida elusiva es cambiar al modo de configuración del binario (valor por defecto) al Modo de texto. Utilice el [comando set config mode text](#) para cambiar al modo de configuración al Modo de texto. El Modo de texto utiliza típicamente menos NVRAM o espacio de memoria Flash que las aplicaciones del modo de la configuración binaria.

Note: Al actuar en el modo de configuración del archivo de texto, la mayoría de los ajustes de usuario no se guardan inmediatamente al NVRAM; los cambios de configuración se escriben solamente al DRAM. Usted debe publicar el [comando write memory](#) para salvar la configuración en el almacenamiento permanente. Utilice el **comando set config mode text auto-save** para salvar la configuración de texto en el NVRAM automáticamente.

Modo de concentración de enlaces incompatible con el tipo de encapsulado

Éste es un problema frecuente que comenzó a ser planteado al [Soporte técnico de Cisco](#) cuando los primeros módulos que podían soportar el 802.1Q y el ISL enviados. Utilizaron a la gente a la configuración de un trunk con el uso del **comando set trunk module/port on** o del **comando set trunk module/port nonegotiate**. El problema es que, por abandono, fijan al tipo de encapsulación para negociar. A los modos de concentración de links deseables soporta al tipo de encapsulación de la negociación solamente el auto o. Encendido y nonegotiate los tipos de encapsulación no realizan ningunas negociaciones entre el Switches y deben ser fijados difícilmente a la encapsulación ISL o del 802.1Q cuando los configuran. Aquí está un registro de qué 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 usted no negocia con el telecontrol, cómo usted conocería qué clase de encapsulación (802.1Q o ISL) de utilizar para traer para arriba el trunk? Hay dos posibilidades:

- Utilice el desirable mode. En este caso, usted negocia al modo de encapsulación con el telecontrol:

```
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 usted quiere 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](#)
- [fije el dominio del vtp](#)
- [show interface](#)
- [show port](#)
- [show port capabilities](#)
- [show trunk](#)
- [show vtp domain](#)

Información Relacionada

- [Configurando la conexión troncal de ISL en el Catalyst 5500/5000 y 6500/6000 de los switches de la familia](#)
- [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](#)