Resolviendo problemas el VLAN Trunk Protocol (VTP)

Contenido

Introducción

Este documento proporciona información sobre cómo resolver problemas de VLAN Trunk Protocol (VTP).

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Comprensión de VTP

Refiérase a Cómo Comprender VLAN Trunk Protocol (VTP) para obtener más información sobre VTP.

Configuración VTP

Consulte Configuración del VLAN Trunk Protocol (VTP) para obtener más información sobre la configuración del VTP.

Solución de problemas y advertencias sobre VTP

Esta sección discute algunas situaciones de Troubleshooting comunes para el VTP.

Incapaz de ver los detalles del VLA N en la salida del comando show run

Los cambios de configuración en CatOS se escriben al NVRAM inmediatamente después que se realiza un cambio. En cambio, el Cisco IOS ® Software no salva los cambios de configuración al NVRAM a menos que usted publique el **comando copy running-config startup-config**. El vtp client y los sistemas del servidor requieren las actualizaciones VTP de otros servidores VTP ser guardados inmediatamente en el NVRAM sin la intervención del usuario. Los requisitos de la actualización VTP son cumplidos por la operación predeterminada de CatOS, pero el modelo de la actualización del Cisco IOS requiere una operación de actualización alternativa.

Para esta alteración, una base de datos de VLAN fue introducida en el Cisco IOS Software como un método para salvar inmediatamente las actualizaciones VTP para los clientes y servidores VTP. En algunas versiones de software, esta base de datos de VLAN está bajo la forma de archivo distinto en el NVRAM, llamado el archivo del vlan.dat. Usted puede ver la información VTP/VLAN que se salva en el archivo del vlan.dat para el vtp client o el servidor VTP si usted publica el comando show vtp status.

El Switches del servidor VTP/de modo cliente no salva la configuración entera VTP/VLAN al archivo de la configuración de inicialización en el NVRAM cuando usted publica el **comando copy running-config startup-config** en estos sistemas. Guarda la configuración en el archivo del vlan.dat. Esto no se aplica a los sistemas que se ejecutan como VTP transparente. Los sistemas transparentes VTP salvan la configuración entera VTP/VLAN al archivo de la configuración de inicialización en el NVRAM cuando usted publica el **comando startup-config de los copyrunning-config**. Por ejemplo, si usted borra el archivo del vlan.dat después de que la configuración del VTP en el servidor o el modo cliente y recarga el Switch, reajusta la configuración VTP a las configuraciones predeterminadas. Sin embargo, si usted configura el VTP en el modo transparente, borre el vlan.dat y recargue el Switch. Esto conserva la configuración VTP.

Éste es un ejemplo de una configuración del VTP predeterminado:

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD3 0x78 0x41 0xC8 0x35 0x56 0x89 0x97
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Usted puede configurar los VLA N del iIntervalo normal (2 a 1000) cuando el Switch está en el servidor VTP o el modo transparente. Sin embargo, usted puede configurar solamente los VLAN de alcances extendidos (1025 a 4094) en los switches transparentes VTP.

- Para visualizar todas las configuraciones de VLAN, el VLAN ID, nombre, y así sucesivamente, que se salvan en el Archivo binario, usted debe publicar el **comando show vlan**.
- Usted puede visualizar la información VTP, el modo, dominio, y así sucesivamente, con el uso del **comando show vtp status**.
- La información de VLAN y la información VTP no se visualizan en el **comando show running-config** hecho salir cuando el Switch está en el servidor VTP/el modo cliente. Éste es comportamiento normal del Switch.`Router#show run | include vlan`
  `vlan internal allocation policy ascendingRouter#show run | include vtp`
- El Switches que es en la visualización del modo transparente VTP el VLA N y las configuraciones VTP en el **comando show running-config** hizo salir porque esta información también se salva en el archivo de texto de la configuración.`Router#show run | include vlan`

```
vlan internal allocation policy ascending
vlan 1
 tb-vlan1 1002
 tb-vlan2 1003
vlan 20-21,50-51
vlan 1002
 tb-vlan1 1
 tb-vlan2 1003
vlan 1003
 tb-vlan1 1
 tb-vlan2 1002
vlan 1004
vlan 1005
Router#show run | include vtp
vtp domain cisco
```

```
vtp mode transparent
```

Nota: Los VLAN de alcances extendidos no son soportados por 3500XL. El 2900XL y el 3500XL pueden utilizar solamente los VLA N en el rango de 1 a 1001, y no soportan los VLAN de alcances extendidos. Si usted actualiza el software del Switch, no trae una mejora para soportar la configuración de los VLAN de alcances extendidos.

Los switches de Catalyst no intercambian la información VTP

El VTP permite que el Switches haga publicidad de la información de VLAN entre otros miembros del mismo dominio VTP. El VTP permite una vista coherente de la red de switch a través de todo el Switches. Hay varias razones por las que la información de VLAN puede no poder ser intercambiado.

Verifique estos elementos si el Switches que ejecuta el fall VTP para intercambiar la información de VLAN:

- Pasos de la información VTP solamente a través de un puerto troncal. Aseegurese que todos los puertos que interconectan el Switches están configurados como trunks y son realmente enlace.Aseegurese que si los EtherChanneles se crean entre dos Switches, sólo los EtherChanneles de la capa 2 propagan la información de VLAN.
- Aseegurese que los VLA N son activos en todos los dispositivos.
- Uno del Switches debe ser el servidor VTP en un dominio VTP. Todos los cambios de VLAN se deben hacer en este Switch para hacerlo propagar a los clientes VTP.
- El Domain Name VTP debe hacer juego y es con diferenciación entre mayúsculas y minúsculas. CISCO y Cisco son dos diversos Domain Name.
- Aseegurese que no se fija ninguna contraseña entre el servidor y el cliente. Si se fija cualquier contraseña, aseegurese que la contraseña es lo mismo en los ambos lados.
- Cada Switch en el dominio VTP debe utilizar la misma versión de VTP. El VTP V1 y el VTP V2 no son compatibles en el Switches en el mismo dominio VTP. No habilite VTP V2 a menos que cada Switch en el dominio VTP soporte el V2.**Nota:** El VTP V2 se inhabilita por abandono en el Switches VTP V2-capable. Cuando usted habilita VTP V2 en un Switch, cada Switch VTP V2-capable en el dominio VTP habilita el V2. Usted puede configurar solamente la versión en el Switches en el servidor VTP o el modo transparente.
- Switches que actúa en los avisos VTP del descenso del modo transparente si no están en el mismo dominio VTP.
- Los VLAN de alcances extendidos no se propagan. Por lo tanto, usted debe configurar los VLAN de alcances extendidos manualmente en cada dispositivo de red.**Nota:** En el futuro, el Switches del Cisco IOS Software del Catalyst 6500 soporta la versión de VTP 3. Esta versión puede transmitir los VLAN de alcances extendidos. Hasta ahora, la versión de VTP 3 se soporta solamente en CatOS. Refiera a la *comprensión cómo la versión de VTP 3 trabaja la* sección de configurar el VTP para más información sobre la versión de VTP 3.
- Los valores del Security Association Identifier (SAID) deben ser únicos. DICHO es un utilizador configurable, el identificador de VLAN 4-byte. El DICHO identifica el tráfico que pertenece a un VLAN determinado. DIJO también determina a qué VLA N se conmuta cada paquete. El valor SAID es 100,000 más el número VLAN. Éstos son dos ejemplos:El DICHO para el VLA N 8 es 100008.El DICHO para el VLA N 4050 es 104050.
- Las actualizaciones de un servidor VTP no consiguen actualizadas en un cliente si el cliente tiene ya un número de revisión VTP mayor. También, el cliente no permite que estas actualizaciones fluyan a sus clientes VTP descendentes si el cliente tiene un número de

revisión más alto que el que el servidor VTP envíe.

El switch de Catalyst cambia automáticamente al modo VTP del cliente a transparente

Algunos switches de configuración fija de la capa de Catalyst 2 y de la capa 3 cambian al modo VTP automáticamente del cliente a transparente con este mensaje de error:

```
%SW_VLAN-6-VTP_MODE_CHANGE: VLAN manager changing device mode from
CLIENT to TRANSPARENT.
```

Cualquiera de estas dos razones puede causar el cambio de modo VTP automático en este Switches:

- **Más funcionamiento de los VLA N en el Spanning Tree Protocol (STP) que el Switch puede soportar.**Los switches de configuración fija de la capa de Catalyst 2 y de la capa 3 soportan un diverso número máximo de casos del STP con el uso del Per-VLAN Spanning Tree + (PVST+). Por ejemplo, el Catalyst 2940 soporta cuatro casos del STP en el modo PVST+, mientras que el Catalyst 3750 soporta los casos 128 del STP en el modo PVST+. Si más que el número máximo de VLAN se define en el VTP, los VLA N que permanecen actúan con el STP inhabilitado.Si el número de casos del STP que es ya funcionando es mayor que el número máximo, usted puede inhabilitar el STP en uno de los VLA N y habilitarlo en el VLA N donde usted quisiera que el STP se ejecutara. No publique el **ningún** comando global configuration **vlan VLAN-***identificación del atravesar*-**árbol** para inhabilitar el STP en un VLA N específico. Entonces, publique el comando global configuration **vlan VLAN-***identificación del atravesar*-**árbol** para habilitar el STP en el VLA N deseado.**Nota:** El Switches que todavía no ejecuta el STP para remitirlo a las Unidades (BPDU) esas recibe. De esta manera, el otro Switches en el VLA N que tiene un caso del funcionamiento STP puede romper los loopes. Por lo tanto, el STP debe funcionar con encendido bastante el Switches para romper todos los loopes en la red. Por ejemplo, por lo menos un Switch en cada loop en el VLA N debe ejecutar el STP. Usted no necesita ejecutar el STP en todo el Switches en el VLA N. Sin embargo, si usted ejecuta el STP solamente en un conjunto mínimo de Switches, un cambio a la red puede introducir un loop en la red y puede dar lugar a una tormenta de broadcast.**Soluciones alternativas:**Reduzca el número de VLA N que se configuren a un número que el Switch soporte.Configure el IEEE 802.1S STP múltiple (MSTP) en el Switch para asociar los VLAN múltiples a un solo caso STP.Utilice el Switches y/o las imágenes ([EI] aumentado de la imagen) que soportan un mayor número de VLA N.
- **El Switch recibe más VLA N de un switch conectado que el Switch puede soportar.**Un cambio de modo VTP automático también puede ocurrir si el Switch recibe un mensaje de la base de datos de la configuración de VLAN que contenga más que un determinado número de VLA N. Esto sucede normalmente en los switches de configuración fija de la capa de Catalyst 2 y de la capa 3 cuando están conectados con un dominio VTP que tenga más VLA N que se soportan localmente.**Soluciones alternativas:**Configure la lista de VLAN permitida en el puerto troncal del switch conectado para restringir el número de VLA N que se pasen al Switch del cliente.Habilite la poda en el Switch del servidor VTP.Utilice el Switches y/o las imágenes (E-I) que soportan un mayor número de VLA N.

Tráfico de datos bloqueado entre los dominios VTP

Se requiere a veces para conectar con el Switches que pertenece a dos diversos dominios VTP. Por ejemplo, hay dos Switches llamado Switch1 y Switch2. El Switch1 pertenece al dominio VTP cisco1 y al Switch2 pertenece al dominio VTP cisco2. Cuando usted configura el trunk entre este dos Switches con la negociación del tronco dinámico (DTP), la negociación de tronco falla y el trunk entre el Switches no forma, porque el DTP envía el Domain Name VTP en un paquete DTP. Debido a esto, el tráfico de datos no pasa entre el Switches.

```
Switch1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : cisco1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled

Switch2#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 42
VTP Operating Mode              : Server
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled


Switch1#show interface fastethernet 1/0/23 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa1/0/23    auto         802.1q         not-trunking  1

Port      Vlans allowed on trunk
Fa1/0/23    1

Port        Vlans allowed and active in management domain
Fa1/0/23    1

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/23    1
```

Es posible que usted puede también ver este mensaje de error.

Nota: Alguno del Switches no muestra este mensaje de error.

```
Switch1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : cisco1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled

Switch2#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
```

```
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 42
VTP Operating Mode              : Server
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled


Switch1#show interface fastethernet 1/0/23 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa1/0/23    auto         802.1q         not-trunking  1

Port      Vlans allowed on trunk
Fa1/0/23    1

Port        Vlans allowed and active in management domain
Fa1/0/23    1

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/23    1
```

La solución para este problema es forzar manualmente el enlace en lugar de otro para confiar en el DTP. Configure los puertos troncales entre el Switches con el **comando switchport mode trunk**.

```
Switch1(config)#interface fastethernet 1/0/23
switch1(config-if)#switchport mode trunk

Switch2(config)#interface fastethernet 3/3
switch2(config-if)#switchport mode trunk


switch1#show interface fastethernet 1/0/23 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa1/0/23    on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa1/0/23    1-4094

Port        Vlans allowed and active in management domain
Fa1/0/23    1-5

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/23    1-5
```

Cambios del switch CatOS al modo transparente VTP, VTP-4-UNSUPPORTEDCFGRCVD:

Un cambio reciente en CatOS incorporó una función protectora que hace un switch CatOS entrar el modo transparente VTP para prevenir la posibilidad de un Switch reajustado debido a un tiempo de espera de vigilancia. Este cambio se documenta en este bug Cisco ID:

- CSCdu32627 (clientes registrados solamente)
- CSCdv77448 (clientes registrados solamente)

¿Cómo determino si mi Switch pudo ser afectado?

El tiempo de espera de vigilancia puede ocurrir si se cumplen estas dos condiciones:

- La VLAN Token Ring (1003) se traduce a VLAN 1.
- Usted realiza un cambio en el VLAN1.

Publique el **comando show vlan** en el Catalyst para observar la traducción de VLAN Token Ring. Esto es un ejemplo del **comando show vlan** hecho salir:

```
Switch1(config)#interface fastethernet 1/0/23
switch1(config-if)#switchport mode trunk

Switch2(config)#interface fastethernet 3/3
switch2(config-if)#switchport mode trunk


switch1#show interface fastethernet 1/0/23 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa1/0/23    on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa1/0/23    1-4094

Port        Vlans allowed and active in management domain
Fa1/0/23    1-5

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/23    1-5
```

¿Cómo la versión CatOS 6.3(3) protege mi Switch contra un tiempo de espera de vigilancia?

Hay una función protectora para prevenir un tiempo de espera de vigilancia en esta versión CatOS. El Switches del switch de Catalyst del servidor VTP o del cliente al modo transparente VTP.

¿Cómo determino si mi Switch ha ido al modo transparente VTP para proteger contra un tiempo de espera de vigilancia?

Su Switch ha ido al modo transparente VTP si el nivel de registro para el VTP se aumenta a 4.

```
Console> (enable) set logging level vtp 4 default
```

Usted ve este mensaje cuando ocurre el intercambio:

```
Console> (enable) set logging level vtp 4 default
```

¿Cuáles son los efectos negativos cuando el Switch va al modo transparente VTP?

- Si está activado el recorte, los troncales se desactivan.
- Si van los trunks abajo y no hay otros puertos en ese VLA N, la interfaz VLAN en el (MSFC) de la placa de la característica de switch multicapa instalada va abajo.

Si ocurren estos efectos, y este Switch está en la base de su red, su red puede ser negativamente afectada.

¿De dónde proviene la configuración VTP no admitida?

Cualquier Switch basado en software del Cisco IOS, tal como el Switches en esta lista, puede suministrar la configuración VTP no admitida:

- Un Catalyst 2900/3500XL
- Un Catalyst 6500 del Cisco IOS Software
- Un Catalyst basado en software 4000 del Cisco IOS

Estos Productos traducen el VLA N 1003 al VLAN1 por abandono.

¿Cuál es la solución?

La solución en los switches basados en CatOS permite al Switches para manejar esta información traducida correctamente. La solución para el Switches basado en software del Cisco IOS es quitar esta traducción predeterminada y hacer juego el comportamiento de los switches basados en CatOS. Éstas son las versiones corregidas integradas que están actualmente disponibles:

Catalyst Switch	Versiones revisadas
Switches CatOS	5.5(14) y posterior 6.3(6) y posterior 7.2(2) y posterior
Catalyst 4000 (Supervisor Engine III)	No afectado
Catalyst 6500 (Cisco IOS Software del Supervisor Engine)	Cisco IOS Software Release 12.1(8a)EX y Posterior
Catalyst 2900 y 3500XL	Cisco IOS Software Release 12.0(5)WC3 y Posterior

Si usted no puede actualizar a las imágenes que tienen estos arreglos integrados, usted puede modificar la configuración en el Switches basado en software del Cisco IOS. Utilice este procedimiento si el Switch es servidor VTP:

```
goss#vlan data

goss(vlan)#no vlan 1 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default

goss(vlan)#no vlan 1003 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default

goss(vlan)#apply

APPLY completed.

goss(vlan)#exit

APPLY completed.
Exiting....
```

El VLA N 1002 puede ser traducido, pero usted puede también quitarlo si usted incluye esto en su configuración:

```
goss(vlan)#no vlan 1002 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
```

```
Resetting translation bridge VLAN 2 to default
```

¿Hace cuándo exactamente mi cambio del Switch al modo transparente VTP?

Una cierta confusión existe sobre cuando ocurre este intercambio al modo transparente VTP. Los escenarios en esta sección proporcionan los ejemplos de cuando el intercambio puede suceder.

- **Ejemplo 1**Éstas son las Condiciones iniciales:El Catalyst 6500 y el Catalyst 3500XL son servidores VTP con el mismo número de revisión de la configuración VTP.Ambos servidores poseen el mismo nombre de dominio VTP y la misma contraseña VTP, si la contraseña se configura.El Catalyst 3500XL tiene el VLAN Token Ring traducido.Usted enciende los servidores mientras que son disconnected.Si usted conecta este dos Switches, el Catalyst 6500 va al modo transparente VTP. Por supuesto, esto también sucede si Cisco 3500XL tiene un número de revisión más alto de la configuración VTP que el número de revisión de la configuración del Catalyst 6500. Por otra parte, si ocurre el Switch al modo transparente VTP cuando usted conecta físicamente el dos Switches, usted puede razonablemente asumir que ocurriría el cambio también si usted inició el Catalyst 6500 por primera vez mientras que el Switch fue conectado ya.
- **Ejemplo 2**Éstas son las Condiciones iniciales:El Catalyst 6500 es un servidor VTP.El Catalyst 3500XL es un vtp client.El Catalyst 3500XL tiene un número de revisión más alto de la configuración VTP que el número de revisión de la configuración del Catalyst 6500.Ambos switches tienen el mismo dominio VTP y la misma contraseña VTP, si se configura la contraseña.El Catalyst 3500XL tiene el VLAN Token Ring traducido.Usted enciende los servidores mientras que son disconnected.Si usted conecta este dos Switches, el Catalyst 6500 va al modo transparente VTP. En este escenario, si el Catalyst 3500XL tiene un número de revisión de configuración menor que el número de revisión de la configuración del Catalyst 6500, el Catalyst 6500 no conmuta al modo transparente VTP. Si el Catalyst 3500XL tiene el número de revisión de la misma configuración, el Catalyst 6500 no va al modo transparente VTP. Sin embargo, la traducción está todavía presente en el Catalyst 3500XL.

¿Cuál es el modo más rápido de recuperarse después de que yo aviso la traducción en mi red?

Incluso si usted corrige la información del VLAN Token Ring en un Switch, tal como el Switch que funcionó incorrectamente, la información puede propagar en su red. Usted puede utilizar el **comando show vlan** para determinar si ocurrió éste. Por lo tanto, el modo más rápido de recuperarse es realizar estos pasos:

1. Tome el Cisco IOS Switch basado en software, tal como un Catalyst XL que esté conectado con la red, y cambie el Switch a un servidor VTP.
2. Quite los VLA N traducidos.
3. Después de que usted aplique el cambio en el Switch, vuelva a conectar el Switch a la red.El cambio se debe propagar al resto de servidores VTP y de clientes.Usted puede utilizar el **comando show vlan** para verificar que la traducción está entrada en la red. En este momento, usted debe poder cambiar el 6.3(3) Switch afectado de CatOS de nuevo a un servidor VTP.**Nota:** El Catalyst XL switches no soporta tantos VLA N como el soporte del Catalyst 6500s. Asegúrese de que todos los VLA N en el Catalyst 6500 existan en el Catalyst XL switch antes de que usted los vuelva a conectar. Por ejemplo, usted no quiere conectar un Catalyst 3548XL con 254 VLA N y un número de revisión más alto de la configuración VTP con un Catalyst 6500 que tenga 500 VLA N configurados.

Cómo un switch recientemente introducido puede provocar problemas en la red

Este problema ocurre cuando usted tiene un dominio conmutado grande que sea todo en el mismo dominio VTP, y usted quiere agregar un Switch en la red.

Se utilizó este switch anteriormente en laboratorio y se ingresó un buen nombre de dominio VTP. El Switch fue configurado como vtp client y conectado con el resto de la red. Entonces, usted trajo el link ISL hasta el resto de la red. En apenas algunos segundos, la red completa estaba abajo. ¿Cómo esto sucedió?

El número de revisión de la configuración del Switch que usted insertó era más alto que el número de revisión de la configuración del dominio VTP. Por lo tanto, su cambio recientemente introducido, con casi ningunos VLAN configurados, borró todos los VLA N a través del dominio VTP.

Esto ocurre si el Switch es un vtp client o servidor VTP. Un vtp client puede borrar la información de VLAN en un servidor VTP. Usted puede decir que esto ha ocurrido cuando muchos de los puertos en su red entran el estado inactivo pero continúa siendo asignada a un VLA N inexistente.

Solución

Vuelva a configurar rápidamente todas las VLAN en uno de los servidores VTP.

Qué a recordar

Aseegurese siempre que el número de revisión de la configuración de todos el Switches que usted inserta en el dominio VTP es más bajo que el número de revisión de la configuración del Switches que está ya en el dominio VTP.

Si usted tiene la salida de un **comando show tech-support de** su dispositivo de Cisco, usted puede utilizar el Output Interpreter (clientes registrados solamente) para visualizar los problemas potenciales y los arreglos.

Ejemplo:

Complete estos pasos para ver un ejemplo de este problema:

1. Publique estos comandos para ver que el clic tiene 7 VLA N (1, 2,3, y los valores por defecto), clic es el servidor VTP en el dominio nombrado prueba, y el puerto 2/3 está en el VLAN3:`clic (enable)` **`show vlan`**

```
1993 May 25 05:09:50 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1 lan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- -----------------------
1    default                          active    65      2/2,2/4-50
2    VLAN0002                         active    70
3    VLAN0003                         active    71      2/3
1002 fddi-default                     active    66
1003 token-ring-default               active    69
1004 fddinet-default                  active    67
1005 trnet-default                    active    68      68
```

```
clic (enable) show vtp domain
```

```
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- -------------- -------------
7          1023            0              disabled

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

clic (enable) show port 2/3

Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/3                     connected 3          normal   10  half 10/100BaseTX
```

2. Conecte el bing, que es un Switch del laboratorio en qué VLA N 4, 5, y 6 fueron creados.**Nota:** El número de revisión de la configuración es 3 en este Switch.`bing (enable)` **`show vlan`**

```
VLAN Name                           Status    IfIndex Mod/Ports, Vlans
---- ------------------------------ --------- ------- ------------------------
1    default                        active    4       2/1-48
                                                      3/1-6
4    VLAN0004                       active    63
5    VLAN0005                       active    64
6    VLAN0006                       active    65
1002 fddi-default                   active    5
1003 token-ring-default             active    8
1004 fddinet-default                active    6
1005 trnet-default                  active    7
```

3. Coloque el bing en el mismo dominio VTP (prueba).`bing (enable)` **`show vtp domain`**

```
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- -------------- -------------
8          1023            3              disabled

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

4. Configure el trunk entre el dos Switches para integrar el bing en la red.Bing borró el VLA N del clic, y ahora el clic tiene VLA N 4, 5, y 6. Sin embargo, el clic tiene no más VLA N 2 y 3, y el puerto 2/3 está inactivo.`clic (enable)` **`show vtp domain`**

```
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- -------------- -------------
8          1023            3              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
10.200.8.38     disabled disabled 2-1000
clic (enable)
```

```
clic (enable) show vlan

VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- -----------------------
1    default                          active    65      2/2,2/4-50
4    VLAN0004                         active    72
5    VLAN0005                         active    73
6    VLAN0006                         active    74
1002 fddi-default                     active    66
1003 token-ring-default               active    69
1004 fddinet-default                  active    67
1005 trnet-default                    active    68      68

clic (enable) show port 2/3

Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/3                     inactive   3          normal   auto  auto 10/100BaseTX
```

El Switch recientemente agregado no consigue los VLA N del servidor VTP

Aseegurese que el Switch nuevamente agregado tiene un número de revisión de la configuración que sea menos que el número de revisión actual del dominio. Vea cómo un switch insertado puede causar los problemas de red y reajustar recientemente las secciones del número de revisión de la configuración para más información.

El nuevo Switch no pudo recibir inmediatamente la lista de VLAN configurados del servidor VTP. Para superar esto, haga ninguno de estos modificaciones a la base de datos de VLAN:

- Crear cualquier VLAN.
- Remover cualquier VLAN.
- Modifique las propiedades de cualquier VLA N actual.

Haga las modificaciones a la base de datos de VLAN en cualquier servidor VTP del mismo dominio.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name 50thVLAN
Switch(config-vlan)#end
Switch#
```

Una vez que se completa la modificación, el Switch nuevamente agregado recibe la información de VLAN del servidor VTP.

Reajuste el número de revisión de la configuración

Usted puede reajustar fácilmente el número de revisión de la configuración por cualquiera de los dos procedimientos proporcionados en esta sección.

Reajuste la revisión de la configuración usando el Domain Name

Complete estos pasos para reajustar el número de revisión de la configuración con el cambio del Domain Name:

1. Publique este comando para ver que la configuración está vacía:`clic (enable)` **`show vtp domain`**

```
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
                               1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- -------------- -------------
5          1023            0              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

2. Configure el Domain Name, que es **prueba** en este ejemplo, y cree dos VLA N.El número de revisión de la configuración va hasta 2:`clic (enable)` **`set vtp domain test`**

```
VTP domain test modified

clic (enable) set vlan 2

Vlan 2 configuration successful

clic (enable) set vlan 3

Vlan 3 configuration successful

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- -------------- -------------
7          1023            2              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

3. Cambie el nombre de dominio de “prueba” a “cisco”.El número de revisión de la configuración está de nuevo a 0, y todos los VLA N están todavía presentes:`clic (enable)` **`set vtp domain cisco`**

```
VTP domain cisco modified

clic (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
---------- --------------- -------------- -------------
7          1023            0              disabled

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

4. Cambie el Domain Name VTP de Cisco de nuevo a la prueba.La revisión de la configuración

es 0. No hay riesgo que cualquier cosa puede ser borrada, y todos los VLAN configurados permanecen previamente:`clic (enable) **set vtp domain test**`

```
VTP domain test modified

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- -------------- -------------
7          1023            0              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

Reajuste la revisión de la configuración usando el modo VTP

Complete estos pasos para reajustar el número de revisión de la configuración con el cambio del modo VTP:

1. Publique este comando para ver que la configuración está vacía:`clic (enable) **show vtp domain**`

```
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
                               1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- -------------- -------------
5          1023            0              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

2. Configure el Domain Name, que es **prueba** en este ejemplo, y cree dos VLA N.El número de revisión de la configuración va hasta 2:`clic (enable) **set vtp domain test**`

```
VTP domain test modified

clic (enable) set vlan 2

Vlan 2 configuration successful

clic (enable) set vlan 3

Vlan 3 configuration successful

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
```

```
---------- ---------------- -------------- -------------
7          1023             2              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

3. Cambie al modo VTP del servidor a transparente.El número de revisión de la configuración está de nuevo a 0, y todos los VLA N están todavía presentes:`clic (enable)` **`set vtp mode transparent`**

```
VTP domain test modified

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           transparent -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- -------------- -------------
7          1023             0              disabled

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

4. Cambie al modo VTP de transparente al servidor o al cliente.La revisión de la configuración es 0. No hay riesgo que cualquier cosa puede ser borrada, y todos los VLAN configurados permanecen previamente:`clic (enable)` **`set vtp mode server`**

```
VTP domain test modified

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- -------------- -------------
7          1023             0              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

Todo vira inactivo hacia el lado de babor después del ciclo del poder

Los puertos del switch se mueven al estado inactivo cuando son los miembros de VLAN que no existen en la base de datos de VLAN. Un problema frecuente es que todos los puertos se mueven a este estado inactivo después de un ciclo del poder. Generalmente, usted ve esto cuando el Switch se configura como vtp client con el puerto de link troncal ascendente en un VLA N con excepción del VLAN1. Porque el Switch está en el modo del vtp client, cuando las restauraciones del Switch, él pierden su base de datos de VLAN y causan el puerto de link ascendente y cualquier otro puerto que no fueran los miembros de VLAN 1 a entrar el modo inactivo.

Complete estos pasos para solucionar este problema:

1. Cambie temporalmente al modo VTP a transparente.`switch (enable)` **`set vtp mode transparent`**

   ```
   VTP domain austinlab modified
   switch (enable)
   ```
2. Agregue el VLA N al cual el puerto de link ascendente se asigna a la base de datos de VLAN.**Nota:** Este ejemplo asume que el VLAN3 es el VLA N que se asigna al puerto de link ascendente.`switch (enable)` **`set vlan 3`**

   ```
   VTP advertisements transmitting temporarily stopped,
   and will resume after the command finishes.
   Vlan 3 configuration successful
   switch (enable)
   ```
3. Cambie al modo VTP de nuevo al cliente después de que el puerto de link ascendente comience a remitir.`switch (enable)` **`set vtp mode client`**

   `VTP domain austinlab modified`Después de que usted complete estos pasos, el VTP debe re-poblar la base de datos de VLAN del servidor VTP. La repoblación mueve todos los puertos que eran los miembros de VLAN de que el servidor VTP hizo publicidad nuevamente dentro del estado activo.

Trunk abajo, que causa los problemas del VTP

Recuerde que los paquetes VTP están llevados en el VLAN1, pero solamente en los trunks (ISL, dot1q, o LAN Emulation [LANE]).

Si usted realiza los cambios de VLAN durante una época cuando usted tiene un trunk abajo o en que la conectividad lane es abajo entre dos partes de su red, usted puede perder su configuración de VLAN. Cuando la conectividad del troncal se restaura, ambos lados de la red se vuelven a sincronizar. Por lo tanto, el Switch con el número de revisión de la configuración más alto borra la configuración de VLAN del switch de revisión de la configuración más bajo.

VTP y STP (puerto de árbol de expansión lógico)

Cuando usted tiene un dominio VTP grande, usted también tiene un dominio STP grande. La VLAN 1 se debe expandir a través de todo el dominio VTP. Por lo tanto, se ejecuta un STP único para esa VLAN en todo el dominio.

Al usar VTP y crear una nueva VLAN, la VLAN se distribuye por todo el dominio VTP. Luego se crea la VLAN en todos los switches en el dominio VTP. Todos los switches Cisco utilizan el PVST, así que significa que el Switches ejecuta un STP separado para cada VLA N. Esto agrega al carga de la CPU del Switch. Usted debe referir al número máximo de puertos lógicos (para el STP) que se soporten en el Switch para tener una idea del número de STP que usted pueda tener en cada Switch. El número de puertos lógicos es áspero el número de puertos que ejecuten el STP.

Nota: Un puerto troncal funciona con un caso del STP para cada VLAN activo en el trunk.

Usted puede realizar una rápida evaluación de este valor para su Switch con esta fórmula:

`switch (enable)` **`set vtp mode client`**

`VTP domain austinlab modified`

Este número, que es el número máximo de puertos lógicos para el STP, varía del Switch para conmutar y se documenta en los Release Note para cada producto. Por ejemplo, en un Catalyst 5000 con el Supervisor Engine 2, usted puede tener un máximo de 1500 casos STP. Cada vez que usted crea un nuevo VLA N con el VTP, el VLA N se propaga por abandono a todo el Switches y es posteriormente activo en todos los puertos. Usted puede ser que necesite podar los vlanes innecesaria del trunk para evitar la inflación del número de puertos lógicos.

Nota: Los vlanes innecesaria de la poda del trunk se pueden realizar con uno de dos métodos:

- **Recorte manual del vlan innecesaria en el trunk** — éste es el mejor método, y evita el uso de atravesar - árbol. En lugar, el método ejecuta el VLA N podado en los trunks. La sección del recorte VTP de este documento describe el recorte manual más lejos.
- **Recorte VTP** — Evite este método si la meta es reducir el número de casos STP. los VLA N VTP-podados en un trunk siguen siendo parte del atravesar - árbol. Por lo tanto, los VLA N VTP-podados no reducen el número de casos del puerto de árbol de expansión.

Recorte VTP

El recorte VTP aumenta el ancho de banda disponible. El recorte VTP restringe el tráfico saturado a esos links de troncal que el tráfico deba utilizar para acceder los dispositivos de red apropiados. Por abandono, se inhabilita el recorte VTP. La habilitación del recorte VTP en un servidor VTP habilita la poda para el dominio de administración entero. **El comando set vtp pruning enable** poda los VLA N automáticamente y para la inundación de trama no efectiva donde no están necesarias las tramas. Por abandono, los VLA N 2 a 1000 son poda elegible. El recorte VTP no poda el tráfico de los VLA N poda-inelegibles. El VLAN1 es siempre poda inelegible; el tráfico del VLAN1 no puede ser podado.

Nota: El distinto al manual VLAN Pruning, recorte automático no limita al diámetro del árbol de expansión.

Todos los dispositivos en el dominio de administración deben soportar el recorte VTP para que el recorte VTP sea eficaces. En los dispositivos que no soportan el recorte VTP, usted debe configurar manualmente los VLA N que se permiten en los trunks. Usted puede realizar el recorte manual del VLA N del trunk con el **comando clear trunk mod/port** y el **comando clear trunk vlan_list**. Por ejemplo, usted puede elegir permitir solamente, en cada trunk, un switch del núcleo a los VLA N que son realmente necesarios. Esto ayuda a reducir la carga en los CPU de todo el Switches (los switches del núcleo y los switches de acceso) y evita el uso del STP para esos VLA N que extiendan con toda la red. Esta poda limita los problemas de STP en el VLA N.

Aquí tiene un ejemplo:

- **Topología** — La topología es dos switches del núcleo que están conectados el uno al otro, cada uno con 80 conexiones de tronco a 80 diversos switches de acceso. Con este diseño, cada switch del núcleo tiene 81 trunks, y cada switch de acceso tiene dos links troncales ascendentes. Esto asume que los switches de acceso tienen, además de los dos dos o tres trunks del uplinks, que van a un Catalyst 1900. Éste es un total de cuatro a cinco trunks por el switch de acceso.
- **Plataforma** — Los switches del núcleo son Catalyst 6500s con el Supervisor Engine 1A y el Policy Feature Card 1 (PFC1) ese Software Release 5.5(7) del funcionamiento. Según los Release Note para el Software Release 5.x del Catalyst 6000/6500, esta plataforma no puede tener más de 4000 puertos lógicos STP.

- **Switches de acceso** — Los switches de acceso son cualquiera:Catalyst 5000 Switch con el Supervisor Engine 2, que no soportan más de 1500 puertos lógicos STPCatalyst 5000 Switch con el Supervisor Engine 1 y el 20 MB del DRAM, que no soportan más de 400 puertos lógicos STP
- **Número de VLA N** — Recuerde utilizar el VTP. UN VLA N en el servidor VTP se crea en todo el Switches en la red. Si usted tiene 100 VLA N, la base debe dirigir áspero 100 VLA N x 81 trunks = 8100 puertos lógicos, que está sobre el límite. El switch de acceso debe dirigir 100 VLA N x 5 trunks = 500 puertos lógicos. En este caso, los Catalyst en la base exceden el número soportado de puertos lógicos, y los switches de acceso con el Supervisor Engine 1 están también sobre el límite.
- **Solución** — Si usted asume que los solamente cuatro o cinco VLA N están necesitados realmente en cada switch de acceso, usted puede podar el resto de VLA N del trunk en la capa del núcleo. Por ejemplo, si solamente los VLA N 1, 10, 11, y 13 se necesitan en el trunk 3/1 eso va a ese switch de acceso, la configuración en la base es:`Praha> (enable) set trunk 1/1 des`

  ```
  Port(s) 1/1 trunk mode set to desirable.

  Praha> (enable) clear trunk 1/1 2-9,12,14-1005

  Removing Vlan(s) 2-9,12,14-1005 from allowed list.
  Port 1/1 allowed vlans modified to 1,10,11,13.

  Praha> (enable) clear trunk 1/1 2-9,12,14-1005
  ```

  Nota: Incluso si usted no excede el número de puertos lógicos permitidos, pode los VLA N de un trunk. La razón es que un STP loop en un VLA N amplía solamente donde se permite el VLA N y no pasa a través del campus entero. El broadcast en un VLA N no alcanza el Switch que no necesita el broadcast. En las versiones que son anteriores que el Software Release 5.4, usted no puede VLAN1 claro de los trunks. En versiones posteriores, usted puede borrar el VLAN1 con este comando:`Praha> (enable) clear trunk 1/1 1`

  ```
  Default vlan 1 cannot be cleared from module 1.
  ```

  El caso de la sección del VLAN1 de este documento discute las técnicas en cómo guardar el VLAN1 de atravesar el todo el campus.

Los VLA N no se podan

Si dos Switches, A y B, está conectado con un puerto de Switch A, que se configura como trunk, y está conectado con un teléfono del IP, después el VTP se une a los mensajes que pasan del Switch A al switch B. Por lo tanto, el switch B no puede podar el VLANS inusitado.

Este problema puede ser resuelto si usted configura el puerto conectado con el teléfono del IP como VLA N de la Voz del puerto de acceso.

```
Switch#interface FastEthernet0/1
switchport access vlan <vlan number>
switchport voice vlan <vlan number>
```

El caso de VLAN 1

Usted no puede aplicar el recorte VTP a los VLA N que necesitan existir por todas partes y que necesitan ser permitidos en todo el Switches en el campus, para poder llevar el VTP, el tráfico del protocolo cisco discovery [CDP], y el otro tráfico de control. Sin embargo, hay una manera de limitar el fragmento del VLAN1. La característica se llama neutralización del VLAN1 en el trunk. La

característica está disponible en el Switches de los Catalyst 4500/4000, 5500/5000, y 6500/6000 Series en la versión de software CatOS 5.4(x) y posterior. La característica permite que usted pode el VLAN1 de un trunk, como usted hace para cualquier otro VLA N. Esta poda no incluye todo el tráfico del protocolo de control que todavía se permite en el trunk (DTP, PAgP, CDP, VTP, y otros). Sin embargo, la poda bloquea todo el tráfico de usuarios en ese trunk. Con esta característica, usted puede guardar el VLA N de atravesar el campus entero. Los loopes STP se limitan en el fragmento, incluso en el VLAN1 de la configuración del VLA N 1. que se inhabilitará, pues usted configuraría otros VLA N que se borrarán del trunk:

```
Console> (enable) set trunk 2/1 desirable

Port(s)  2/1 trunk mode set to desirable.

Console> (enable) clear trunk 2/1 1

Removing Vlan(s) 1 from allowed list.
Port  2/1 allowed vlans modified to 2-1005.
```

El UDLD utiliza el VLAN nativo para hablar con el vecino. Así pues, en un puerto troncal, el VLAN nativo no se debe podar para que el UDLD trabaje correctamente.

Resuelva problemas los errores del número de revisión de la configuración VTP que se consideran en la salida del comando show vtp statistics

El VTP se diseña para un entorno administrativo en el cual la base de datos de VLAN para el dominio se cambie en solamente un Switch a cualquier momento. Asume que la nueva revisión propaga en el dominio antes de que se haga otra revisión. Si usted cambia la base de datos simultáneamente en dos diversos dispositivos en el dominio administrativo, usted puede hacer dos diferentes bases de datos ser generado con el mismo número de revisión. Estas bases de datos propagan y sobregraban la información existente hasta que se encuentren en un switch de Catalyst intermedio en la red. Este Switch no puede validar cualquier anuncio porque los paquetes tienen el mismo número de revisión pero un diverso valor MD5. Cuando el Switch detecta esta condición, el Switch incrementa `no del` contador de `errores de la revisión de los config`.

Nota: La salida del **comando show vtp statistics** en esta sección proporciona un ejemplo.

Si usted encuentra que la información de VLAN no está puesta al día en cierto Switch, o si usted encuentra otro, los problemas similares, publican el **comando show vtp statistics**. Determine si la cuenta de los paquetes VTP con los errores del número de revisión de la configuración está aumentando:

```
Console> (enable) show vtp statistics

VTP statistics:
summary advts received          4690
subset  advts received          7
request advts received          0
summary advts transmitted       4397
subset  advts transmitted       8
request advts transmitted       0
No of config revision errors    5
No of config digest errors      0
VTP pruning statistics:
Trunk     Join Transmitted  Join Received  Summary advts received from
                                           non-pruning-capable device
--------  --------------  -------------  --------------------------
```

```
 1/1      0               0              0
 1/2      0               0              0
Console> (enable)
```

Si usted observa un error de la revisión de la configuración, usted puede resolver este problema si usted cambia la base de datos de VLAN de cierta manera para crear una base de datos VTP con un número de revisión más alto que el número de revisión de las bases de datos competentes. Por ejemplo, en el Switch que actúa como el servidor VTP principal, agregue o borre un VLA N falso en el dominio administrativo. Esta revisión actualizada se propaga en el dominio y sobregraba la base de datos en todos los dispositivos. Cuando todos los dispositivos en el dominio hacen publicidad de una base de datos idéntica, el error aparece no más.

Errores de la publicación de la configuración VTP del Troubleshooting que se consideran en la salida del comando show vtp statistics

Direccionamientos de esta sección cómo resolver problemas los errores de la publicación de la configuración VTP que usted ve cuando usted publica el **comando show vtp statistics**. Aquí tiene un ejemplo:

```
Console> (enable) show vtp statistics

VTP statistics:
summary advts received          3240
subset  advts received          4
request advts received          0
summary advts transmitted       3190
subset  advts transmitted       5
request advts transmitted       0
No of config revision errors    0
No of config digest errors      2
VTP pruning statistics:
Trunk     Join Transmitted  Join Received  Summary advts received from
                                           non-pruning-capable device
--------  ---------------  -------------  --------------------------
 1/1      0                0              0
 1/2      0                0              0
Console> (enable)
```

Los fines generales de un valor MD5 son verificar la integridad de un paquete recibido y detectar cualquier cambio al paquete o a la corrupción del paquete durante para transitar. Cuando un Switch detecta un número de nueva revisión que sea diferente actualmente del valor almacenado, el Switch envía un mensaje request al servidor VTP y pide los subgrupos VTP. Un anuncio de subconjuntos contiene una lista de información VLAN. El Switch calcula el valor MD5 para los anuncios del subconjunto y compara el valor al valor MD5 del anuncio de resumen VTP. Si los dos valores son diferentes, el Switch aumenta `no del` contador de `errores de recopilación de configuración`.

Un motivo común para estos errores de compilación es que la contraseña de VTP no está configurada en forma consistente en todos los servidores VTP en el dominio VTP. A la hora de resolver estos errores, trátelos como problemas de configuración errónea o de corrupción de datos.

Cuando usted resuelve problemas este problema, asegúrese de que el contador de errores no sea histórico. El Menú de estadísticas cuenta los errores desde la restauración más reciente del dispositivo o la restauración de las estadísticas VTP.

Incapaz de cambiar al modo VTP de un Switch del servidor/transparente

Si el Switch es un independiente (es decir, no conectado con la red), y usted quiera configurar al modo VTP como el cliente, después de la reinicialización, el Switch sube como un servidor VTP o un VTP transparente, dependiente sobre el modo VTP del Switch antes de que fuera configurado como el vtp client. El Switch no se permite que sea configurado como vtp client cuando no hay servidor VTP cerca.

Hellos OSPF bloqueado en un dominio VTP

El hellos del Open Shortest Path First (OSPF) puede conseguir bloqueado y la adyacencia puede ser caída si un Switch en el dominio VTP se cambia del servidor o del modo cliente al modo transparente. Este problema puede ocurrir si el recorte VTP se habilita en el dominio.

Utilice ninguno de estos opciones para resolver el problema:

- Código duro los vecinos OSPF.
- Recorte VTP de la neutralización en el dominio.
- Invierta al modo VTP del Switch al servidor o al cliente.

SW_VLAN-4-VTP_USER_NOTIFICATION

Esta sección habla de las variantes comúnmente de ocurrencia de este mensaje de error:

```
Console> (enable) show vtp statistics

VTP statistics:
summary advts received          3240
subset  advts received          4
request advts received          0
summary advts transmitted       3190
subset  advts transmitted       5
request advts transmitted       0
No of config revision errors    0
No of config digest errors      2
VTP pruning statistics:
Trunk     Join Transmitted  Join Received  Summary advts received from
                                           non-pruning-capable device
--------  ---------------  -------------  --------------------------
 1/1      0                0              0
 1/2      0                0              0
Console> (enable)
```

%SW_VLAN-4-VTP_USER_NOTIFICATION: Notificación de usuario del protocolo VTP: El dispositivo de la versión 1 detectado en el [int] después del período de gracia ha terminado

Por abandono, la versión del VLAN Trunking Protocol (VTP) en los switches Cisco es versión 2 y es compatible con la versión 1. Este mensaje es apenas una notificación que indica que hay un Switch conectado en el puerto Gig0/10 que funciona con la versión de VTP 1. Todo continúa trabajando muy bien, a menos que usted ejecute el IPX, y no hay nada dañino para el Switch.

Para resolver este problema, cambie la versión de VTP con estos comandos.

Para el Switches del Cisco IOS, utilice estos comandos:

```
Switch#vlan database
Switch(vlan)#vtp v2-mode
```

Para los switches CatOS, utilice este comando:

```
Console> (enable) set vtp version 2 enable
```

%SW_VLAN-SP-4-VTP_USER_NOTIFICATION: Notificación de usuario del protocolo VTP: Discordancía de la suma de comprobación de la publicación MD5 en el recibo del resumen igual de la revisión en el trunk: [int]

Para conocer más la causa y resolver el problema, vea los errores de la publicación de la configuración VTP del Troubleshooting que se consideran en la sección de resultados del comando show vtp statistics.

%SW_VLAN-4-VTP_USER_NOTIFICATION: Notificación de usuario del protocolo VTP: Error detectado en el número de revisión VTP para el índice del dominio VTP [dec]

Para conocer más la causa y resolver el problema, vea los errores del número de revisión de la configuración VTP del Troubleshooting que se consideran en la sección de resultados del comando show vtp statistics.

Escoja el switchport trunk que permitió el comando vlan aparece como comandos múltiples en la salida del comando show running-config

Cuando el número de VLA N permitidos extiende más allá de algunos caracteres, que es el ancho del terminal predeterminado, el **comando show running-config** envuelve la línea y agrega el **switchport trunk no prohibido el comando add vlan a la** línea. Ésta es la manera que el Cisco IOS maneja las listas largas en el **switchport trunk no prohibido el comando vlan**.

```
Switch#configure terminal
Switch(config)#int fa3/30
Switch(config-if)#switchport trunk allowed vlan 14, 105, 110, 115, 120, 125, 130-132,
140, 150, 155, 200, 210, 220, 222, 230, 232, 240, 301-309, 840, 860-862, 870, 880,
881, 884-886, 889, 896, 898, 411, 412, 413, 421
!--- The previous command should be in a single line. It has been wrapped into three lines for
proper formatting.
```

La salida de los ejecutar-**config de la demostración** parece similar a esto:

```
Switch#show running-config | begin 3/30
interface FastEthernet3/30
 switchport
 switchport trunk allowed vlan 14,105,110,115,120,125,130-132,140,150,155,200
 switchport trunk allowed vlan add 210,220,222,230,232,240,301-309,411-413,421
 switchport trunk allowed vlan add 840,860-862,870,880,881,884-886,889,896,898
!
!--- rest of output elided
```

Usted puede también notar que la lista de VLAN ha sido orden en el orden ascendente y visualizada en la salida.

Quite el VLAN1 de la lista permitida así que usted puede inhabilitar el VLAN1 en cualquier puerto troncal del VLAN individual para reducir el riesgo de Spanning-Tree Loop o de tormentas. Cuando usted quita el VLAN1 de un puerto troncal, la interfaz continúa enviando y recibiendo el tráfico de administración, por ejemplo, el Cisco Discovery Protocol (CDP), el Port Aggregation Protocol (PAgP), el protocolo link aggregation control (LACP), el Dynamic Trunking Protocol (DTP), y el VLAN Trunking Protocol (VTP) en el VLAN1.

La ninguna forma del **comando vlan permitido** reajusta la lista a la lista predeterminada, que

permite todos los VLA N.

Uso interno del VLA N

Todos los paquetes enviados al CONDE se deben prefijar por un VLAN ID, porque ése es el formato de paquetes que el CONDE espera. Los puertos ruteados no tienen un VLAN ID visible puesto que uno no se configura explícitamente, así que el Switch pide prestado un VLA N del pool de 4096 que tenga. Usted puede dar instrucciones el Catalyst 6500 Series Switch para comenzar a pedir prestados los VLA N del top, y desciende a partir del 4096, o de la parte inferior, y asciende a partir del 1006, con el uso el comando **vlan de la política de asignación del** modo de configuración global.

```
Switch(config)#vlan internal allocation policy {ascending | descending}
```

Así es comportamiento normal para que el VLA N interno sea utilizado con ruteado o la interfaz de WAN.

Información Relacionada

- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems