Problemas comunes de las 9000 Series ASR con los Spanning Tree Protocol

Contenido

Introducción

Este documento describe los problemas comunes encontrados cuando usted integra sus redes actuales del Spanning-tree de la capa 2 (L2) en el Switches del ® del Cisco IOS con las 9000 Series del router de los servicios de la agregación de Cisco (ASR) que funcionan con el Cisco IOS XR.

Inconsistencia del puerto problemático VLAN ID (PVID)

Switches del Cisco IOS que se ejecuta por el árbol de expansión de VLAN más los puertos del switch del bloque (PVST+) cuando reciben un (BPDU) de la Unidad de bridge protocol data con un PVID insconsistent. Este problema ocurre cuando un dispositivo entre el Switches cambia o traduce las etiquetas del IEEE 802.1Q en el PVST+ BPDU.

Cuando un ASR 9000 proporciona el Punto a punto L2VPN o el servicio de múltiples puntos entre el Switches que ejecuta el PVST+ y reescribe las etiquetas del VLA N, estos mensajes de Syslog pudieron visualizar en los switches basado en Cisco IOS:

```
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent
peer vlan id 10 on GigabitEthernet0/10 VLAN20.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet0/10
on VLAN20. Inconsistent local vlan.
```

Este problema es debido a la etiqueta PVID que se incluye con el PVST+ BPDU. Esta etiqueta se

diseña para detectar el misconfigurations y evitar los loopes accidentales. Pero, en este escenario, hace cada extremo ser bloqueada y no permitir que el tráfico pase.

Aquí tiene un ejemplo:

Aquí está la configuración para la configuración de las 9000 Series ASR (a9k1):

```
2vpn
bridge group bg1
bridge-domain bd1
interface TenGigE0/0/0/0.10
!
interface TenGigE0/0/0/1.20

interface TenGigE0/0/0/0.10 l2transport
encapsulation dot1q 10
rewrite ingress tag pop 1 symmetric

interface TenGigE0/0/0/1.20 l2transport
encapsulation dot1q 20
rewrite ingress tag pop 1 symmetric
```

Solución

Para prevenir este problema, usted puede bloquear el PVST+ BPDU. Esta acción inhabilita el Spanning-tree, y puede dar lugar a los loopes si las conexiones redundantes están disponibles entre el Switches.

> Precaución: Tenga cuidado cuando usted bloquea los BPDU y inhabilita con eficacia el Spanning-tree.

Filtro BPDU en el Switches

Los BPDU se bloquean con la característica del filtro BPDU en el Switches. El filtro BPDU bloquea los BPDU en las ambas direcciones, que inhabilita con eficacia el Spanning-tree en el puerto. El filtro BPDU previene el BPDU entrante y saliente. Si usted habilita el BPDU que filtra en una interfaz, es lo mismo como si usted inhabilite el Spanning-tree en él, que puede dar lugar a los Spanning-Tree Loop.

En switch1 y switch2, filtros del permiso BPDU con este comando:

```
interface TenGigabitEthernet1/2
spanning-tree bpdufilter enable
```

Bloque PVST+ BPDU en ASR 9000

Se evita este problema si usted configura el ASR9000 para caer el PVST+ BPDU. Esto se hace con una lista de acceso de los servicios Ethernet L2 para negar los paquetes destinados a la dirección MAC PVST+ BPDU.

El PVST+ BPDU para el NON-VLA N 1 VLA N (extranjero) se envía a la dirección MAC PVST+

(también llamada la dirección MAC compartida del [SSTP] del Spanning Tree Protocol, 0100.0ccc.cccd), y se marca con etiqueta con una etiqueta correspondiente del VLA N del IEEE 802.1Q.

Esta lista de control de acceso (ACL) se puede utilizar para bloquear el PVST+ BPDU:

```
ethernet-services access-list l2acl
10 deny any host 0100.0ccc.cccd
 20 permit any any
```

Aplique el ACL a la interfaz configurada como l2transport:

```
interface TenGigE0/0/0/0.10 l2transport
encapsulation dot1q 10
rewrite ingress tag pop 1 symmetric
ethernet-services access-group l2acl ingress

interface TenGigE0/0/0/1.20 l2transport
encapsulation dot1q 20
rewrite ingress tag pop 1 symmetric
ethernet-services access-group l2acl ingress
```

Problema - Flap de los puertos del switch entre el bloqueo y el envío cuando usted utiliza los tipos múltiples de los Spanning Tree Protocol (STP) con un ASR 9000

El ASR9000 no hace el Spanning-tree por abandono como la mayoría del Switches del Cisco IOS. En el modelo del circuito virtual de los Ethernetes (EVC), un BPDU es simplemente otro paquete de multidifusión L2. Un problema frecuente encontrado es inconsistencias del Spanning-tree debido a los tipos múltiples de STP que se ejecuten a través de un dominio de Bridge ASR 9000. Esto aparece en algunas maneras diferentes.

Considere esta topología simple:

Asuma los funcionamientos switch1 Múltiples Árboles de expansión (MST) y switch2 los funcionamientos PVST+. Si a9k1 no funciona con ninguna forma de Spanning-tree, después switch1 ve esto como puerto del límite. El Switch1 recurre al modo PVST para los VLA N no en el caso 0 (CST0) del Common Spanning Tree. Si éste es el diseño deseado, usted debe ser familiar con la interacción MST y PVST según lo descrito en comprensión del White Paper del protocolo multiple spanning-tree (802.1s).

Ahora asuma que usted ejecuta el MST en switch1 y en la interfaz a9k1 que va a switch1, pero usted todavía ejecuta el PVST+ en switch2. El PVST+ BPDU pasa a través del dominio de Bridge y llega switch1. El Switch1 entonces ve MST BPDU de a9k1 y el PVST+ BPDU de switch2, que hace el Spanning-tree en el puerto switch1 ir constantemente del bloqueo al bloqueo y a los resultados en la pérdida de tráfico.

El Switch1 señala estos Syslog:

```
%SPANTREE-SP-2-PVSTSIM_FAIL: Superior PVST BPDU received on VLAN 2 port Gi2/13,
claiming root 2:000b.45b7.1100. Invoking root guard to block the port
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/13
on MST1.
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/13
on MST0.
```

```
%SPANTREE-SP-2-PVSTSIM_FAIL: Superior PVST BPDU received on VLAN 2 port Gi2/13,
claiming root 2:000b.45b7.1100. Invoking root guard to block the port
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/13
on MST1.
```

La salida del **comando show spanning-tree interface** muestra que la salida cambia constantemente en el dispositivo Cisco IOS switch1:

```
show spanning-tree interface gig 2/13
Mst Instance Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- -------
MST0 Desg BKN*20000 128.269 P2p Bound(PVST) *ROOT_Inc
MST1 Desg BKN*20000 128.269 P2p Bound(PVST) *ROOT_Inc
MST2 Desg BKN*20000 128.269 P2p Bound(PVST) *ROOT_Inc

show spanning-tree interface gig 2/13
Mst Instance Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ---------
MST0 Desg FWD 20000 128.269 P2p
MST1 Desg FWD 20000 128.269 P2p
MST2 Desg FWD 20000 128.269 P2p
```

Solución

Hay tres opciones a considerar para prevenir este problema.

- Configure el MST en switch2, y habilite el MST en las interfaces a9k1 a switch1 y a switch2.
- Utilice una lista de acceso de los servicios Ethernet en a9k1 para caer el PVST+ BPDU en el ingreso de switch2 o en la salida a switch1.
- Ejecútese por el gateway de acceso del árbol de expansión de VLAN (PVSTAG) en la interfaz a9k1 hacia switch2. Esto hace el a9k1 consumir el PVST+ BPDU de switch2.

Problema - Los puertos de árbol de expansión bloquearon debido a la detección de un uno mismo-loop

Cuando un Switch recibe un Spanning-tree BPDU que envió encendido la misma interfaz, bloquea ese VLA N debido a un uno mismo-loop. Éste es un problema común que ocurre cuando un Switch con un puerto troncal está conectado con un 9000 Router ASR que proporcione el L2 los servicios de múltiples puntos, y el ASR 9000 no reescribe las etiquetas del VLA N en las interfaces l2transport en el mismo dominio de Bridge.

Considere la misma topología simple mostrada previamente. Pero ahora, por una razón del diseño en el a9k1, los VLAN múltiples que vienen de la misma interfaz de tronco del Switch se combinan juntos en un dominio de Bridge.

Aquí está la configuración a9k1:

```
l2vpn
bridge group bg1
bridge-domain bd1
interface GigabitEthernet0/1/0/31.2
!
interface GigabitEthernet0/1/0/31.3
!
```

```
interface GigabitEthernet0/1/0/31.4
!
interface GigabitEthernet0/1/0/32.2
!
interface GigabitEthernet0/1/0/32.3
!
interface GigabitEthernet0/1/0/32.4

interface GigabitEthernet0/1/0/31.2 l2transport
encapsulation dot1q 2
!
interface GigabitEthernet0/1/0/31.3 l2transport
encapsulation dot1q 3
!
interface GigabitEthernet0/1/0/31.4 l2transport
encapsulation dot1q 4
```

Esto interliga los VLA N 2 a 4 juntos en un dominio de Bridge en el a9k1.

El modelo ASR 9000 EVC no reescribe ninguna etiquetas ni hace estallar por abandono. El PVST+ BPDU para el **VLAN2** viene adentro en el **carruaje 0/1/0/31.2 de la** interfaz y se remite se retira en el **carruaje 0/1/0/31.3** y el **carruaje 0/1/0/31.4**. Puesto que la configuración no es una reescritura de la acción del estallido del ingreso, el BPDU vuelve sin cambiar. El Switch considera esto como consigue su propio BPDU detrás, y los bloques ese VLA N debido a un uno mismo-loop.

El comando show spanning-tree interface muestra el VLA N bloqueado:

```
6504-A#show spanning-tree interface gig 2/13


Vlan Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- --------
VLAN0002 Desg BLK 4 128.269 self-looped P2p
VLAN0003 Desg BLK 4 128.269 self-looped P2p
VLAN0004 Desg BLK 4 128.269 self-looped P2p
```

Solución

Este problema se elimina con el uso del comando **estricto del salida-filtro de los Ethernetes** en las interfaces ASR 9000 l2transport.

Esto no es un diseño recomendado. Sin embargo, si éste es verdad el diseño deseado, después usted puede utilizar esta solución para evitar que el Switch reciba el BPDU que devolvió en la misma interfaz.

Usted puede utilizar el comando **estricto del salida-filtro de los Ethernetes** en las interfaces a9k1 l2transport o global. Aquí está el ejemplo de él bajo interfaz:

```
interface GigabitEthernet0/1/0/31.2 l2transport
encapsulation dot1q 2
ethernet egress-filter strict
!
interface GigabitEthernet0/1/0/31.3 l2transport
encapsulation dot1q 3
ethernet egress-filter strict
!
interface GigabitEthernet0/1/0/31.4 l2transport
encapsulation dot1q 4
```

`ethernet egress-filter strict`

Los Ethernetes estrictos de la salida de los permisos **estrictos del** comando del salida-**filtro de los Ethernetes** fluyen la punta (EFP) que filtra en la interfaz. Solamente los paquetes que pasan el filtro EFP del ingreso en la interfaz se transmiten fuera de esta interfaz. Otros paquetes se caen en el filtro de la salida. Esto significa que si el paquete que las salidas no hacen juego la escritura de la etiqueta del **dot1q de la** encapsulación configuró en la interfaz, después no se envía.

Información Relacionada

- Implementar el protocolo multiple spanning-tree
- Resolver problemas el Spanning-tree PVID- y las Tipo-inconsistencias
- Introducción al Protocolo Rapid Spanning Tree Protocol [protocolo de árbol de expansión rápida] (802.1s)
- Soporte Técnico y Documentación - Cisco Systems