Problemas comunes de la serie ASR 9000 con los protocolos de árbol de extensión

Contenido

Introducción

Este documento describe los problemas comunes encontrados cuando integra sus redes actuales de Spanning Tree de Capa 2 (L2) en los switches Cisco IOS® con Cisco Aggregation Services Router (ASR) 9000 Series que ejecutan Cisco IOS XR.

Problema: incoherencia de ID de VLAN de puerto (PVID)

Los switches Cisco IOS que ejecutan Per VLAN Spanning Tree Plus (PVST+) bloquean los puertos del switch cuando reciben una Unidad de datos de protocolo de puente (BPDU) con un PVID inconsistente. Este problema ocurre cuando un dispositivo entre los switches cambia o traduce las etiquetas IEEE 802.1Q en las BPDU PVST+.

Cuando un ASR 9000 proporciona un servicio L2VPN punto a punto o multipunto entre switches que ejecutan PVST+ y vuelve a escribir las etiquetas VLAN, estos mensajes de syslog pueden mostrarse en los switches basados 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 se debe a la etiqueta PVID que se incluye con las BPDU PVST+. Esta etiqueta se

ha diseñado para detectar errores de configuración y evitar bucles accidentales. Pero, en este escenario, hace que cada extremo se bloquee y no permita el paso del tráfico.

Aquí tiene un ejemplo:

Esta es la configuración de la serie ASR 9000 (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 evitar este problema, puede bloquear las BPDU PVST+. Esta acción inhabilita el Spanning Tree, y puede dar lugar a loops si hay conexiones redundantes disponibles entre los switches.

> **Precaución**: tenga cuidado cuando bloquee las BPDU y desactive eficazmente el árbol de expansión.

Filtro BPDU en switches

Las BPDU se bloquean con la función de filtro BPDU en los switches. El filtro BPDU bloquea las BPDU en ambas direcciones, lo que inhabilita eficazmente el Spanning Tree en el puerto. El filtro BPDU evita BPDU entrante y saliente. Si habilita el filtrado BPDU en una interfaz, es igual que si inhabilita el Spanning Tree en ella, lo que puede dar lugar a loops de Spanning Tree.

En switch1 y switch2, habilite los filtros BPDU con este comando:

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

Bloqueo de PVST+ BPDU en ASR 9000

Este problema se evita si configura el ASR9000 para descartar las BPDU de PVST+. Esto se realiza con una lista de acceso de servicios Ethernet L2 para denegar los paquetes destinados a la dirección MAC de PVST+ BPDU.

Las PVST+ BPDU para la VLAN no VLAN 1 (no nativa) se envían a la dirección MAC PVST+ (también denominada dirección MAC de protocolo de árbol de extensión compartido [SSTP], 0100.0ccc.cccd) y se etiquetan con una etiqueta IEEE 802.1Q VLAN correspondiente.

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

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

Aplique la 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: los puertos del switch alternan entre el bloqueo y el reenvío cuando se utilizan varios tipos de protocolos de árbol de extensión (STP) a través de ASR 9000

El ASR9000 no hace Spanning Tree de forma predeterminada como la mayoría de los switches Cisco IOS. En el modelo de circuito virtual Ethernet (EVC), una BPDU es simplemente otro paquete multicast L2. Un problema común encontrado es la inconsistencia del Spanning Tree debido a los diversos tipos de STP que se ejecutan a través de un dominio de bridge ASR 9000. Esto aparece de varias maneras diferentes.

Considere esta topología sencilla:

Suponga que switch1 ejecuta árbol de extensión múltiple (MST) y switch2 ejecuta PVST+. Si a9k1 no ejecuta ninguna forma de Spanning Tree, el switch1 ve esto como un puerto de límite. El switch 1 vuelve al modo PVST para las VLAN que no están en la instancia 0 del árbol de expansión común (CST0). Si éste es el diseño deseado, debe estar familiarizado con la interacción de MST y PVST, como se describe en el informe técnico Introducción al protocolo de árbol de extensión múltiple (802.1s).

Ahora asuma que ejecuta MST en el switch1 y en la interfaz a9k1 que va al switch1, pero aún ejecuta PVST+ en el switch2. Las BPDU PVST+ pasan a través del dominio de bridge y llegan al

switch1. El Switch1 luego ve las BPDU MST de a9k1 y las BPDU PVST+ del switch2, lo que hace que el Spanning Tree en el puerto del switch1 pase constantemente de bloquear a no bloquear y resulta en pérdida de tráfico.

El Switch1 informa estos syslogs:

```
%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.
```

El resultado del comando **show spanning-tree interface** muestra que el resultado 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 MST en el switch2 y habilite MST en las interfaces a9k1 para el switch1 y el switch2.
- Utilice una lista de acceso de servicios Ethernet en a9k1 para descartar las BPDU PVST+ en el ingreso desde el switch2 o en el egreso al switch1.
- Ejecute Per VLAN Spanning Tree Access Gateway (PVSTAG) en la interfaz a9k1 hacia el switch2. Esto hace que a9k1 consuma las PVST+ BPDUs del switch2.

Problema: puertos del árbol de extensión bloqueados debido a la detección de un bucle automático

Cuando un switch recibe una BPDU de Spanning Tree que envió en la misma interfaz, bloquea esa VLAN debido a un auto-loop. Este es un problema común que ocurre cuando un switch con un puerto trunk se conecta a un router ASR 9000 que proporciona servicios multipunto L2, y ASR 9000 no reescribe las etiquetas VLAN en las interfaces de transporte L2 en el mismo dominio de bridge.

Considere la misma topología simple mostrada anteriormente. Pero ahora, por una razón de diseño en el a9k1, varias VLAN que provienen de la misma interfaz troncal del switch se fusionan en un dominio de bridge.

Esta es la configuración de 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 une las VLAN 2 a 4 en un dominio de bridge en el a9k1.

El modelo ASR 9000 EVC no vuelve a escribir ninguna etiqueta ni mensaje emergente de forma predeterminada. La PVST+ BPDU para **VLAN2** entra en la interfaz **gig 0/1/0/31.2** y se reenvía de vuelta en **gig 0/1/0/31.3** y **gig 0/1/0/31.4**. Dado que la configuración no es una reescritura de la acción pop de ingreso, la BPDU regresa sin cambios. El switch ve esto cuando recupera su propia BPDU y bloquea esa VLAN debido a un loop automático.

El comando **show spanning-tree interface** muestra la VLAN bloqueada:

```
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 mediante el uso del comando **ethernet egress-filter strict** en las interfaces de transporte ASR 9000 l2.

Este no es un diseño recomendado. Sin embargo, si este es realmente el diseño deseado, puede utilizar esta solución para evitar que el switch reciba la BPDU que envió de vuelta en la misma interfaz.

Puede utilizar el comando **ethernet egress-filter strict** en las interfaces l2transport a9k1 o globalmente. Aquí está el ejemplo de esto bajo la 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
```

El comando **ethernet egress-filter strict** habilita el filtrado de punto de flujo Ethernet (EFP) de salida estricto en la interfaz. Sólo los paquetes que pasan el filtro EFP de ingreso en la interfaz se transmiten fuera de esta interfaz. Los demás paquetes se descartan en el filtro de salida. Esto significa que si el paquete que egresa no coincide con la etiqueta encapsulation **dot1q** configurada en la interfaz, entonces no se envía.

Información Relacionada

- Implementación de protocolo de árbol de extensión múltiple
- Solución de problemas de inconsistencias de tipo y de PVID de árbol de expansión
- Introducción al Protocolo Rapid Spanning Tree Protocol [protocolo de árbol de expansión rápida] (802.1s)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).