Troubleshooting de Loops de Capa 2

Contenido

Introducción

Prerequisites

Componentes Utilizados

Comandos usados

Teoría de Troubleshooting

Aplicación

Prevención

Introducción

Este documento describe información para ayudar a identificar el origen de los loops de Capa 2 y proporciona salvaguardas para prevenirlos en el futuro.

Prerequisites

Se recomienda que tenga conocimiento de los conceptos de STP.

Componentes Utilizados

Este documento no se limita a una versión específica de software o de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Comandos usados

- show interfaces | include is up|input rate
- show cdp neighbors <interface>
- show spanning-tree
- show logging

Teoría de Troubleshooting

Independientemente de la topología, del punto de partida (el switch al que se conectó por primera vez), el enfoque para realizar el seguimiento del origen del problema es el mismo.

Utilice el comando show interface proporcionado anteriormente. Nos centramos en la interfaz o interfaces con altas velocidades de entrada.

Las altas tasas de salida son un síntoma, no una causa.

A medida que se identifican las interfaces de alta velocidad de entrada, utilice el vecino CDP para verificar los links para los switches conectados. Si encuentra un puerto host, intente apagar el puerto para resolver el problema.

Cuando se trata de switches interconectados de link dual, utilice los comandos del árbol de expansión para confirmar los estados de bloqueo y reenvío. Esto ayuda a identificar un puerto/switch que no funciona correctamente.

Notificaciones de cambio de topología (TCN): ignórelas mientras trabaja en bucles.

Los switches más antiguos no tienen COPP o no pueden manejar el procesamiento de BPDU, lo que da lugar a TCN aleatorios.

Si encuentra el puerto que cree que es el problema - apáguelo y espere al menos 30 segundos. Si esto no resuelve el problema, continúe y no "cierre" la interfaz todavía.

Aplicación

```
DistroSwitch#show interfaces | include is up|input rate
GigabitEthernet1/0/1 is up, line protocol is up
 5 minute input rate 1482600 bits/sec, 2739 packets/sec
GigabitEthernet1/0/2 is up, line protocol is up
 5 minute input rate 291658000 bits/sec, 366176 packets/sec <------------
TenGigabitEthernet1/1/1 is up, line protocol is up
 5 minute input rate 1339000 bits/sec, 2614 packets/sec
```

```
DistroSwitch#show cdp neighbors gigabitEthernet 1/0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
 D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID Local Intrfce Holdtme Capability Platform Port ID
access Gig 1/0/2 158 S I C9300-48P Gig 2/0/2 <-----------------
```

<#root>

DistroSwitch#show logging

```
*May 3 18:33:45.885: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port G
*May 3 18:33:58.841: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
```

```
*May 3 18:34:13.842: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port G
*May 3 18:34:28.839: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
*May 3 18:34:43.840: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
*May 3 18:34:58.839: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
```

```
access#show spanning-tree vlan 1
Spanning tree instance(s) for vlan 1 does not exist.
```

Prevención

Prácticas recomendadas de STP

Protección BPDU: deshabilita las interfaces si obtienen protección BPDU en lugar de reenviarla

Root Guard (Protección de raíz) - Típicamente para la Distro orientada al Acceso - Usted nunca verá una BPDU superior o una BPDU inferior en la interfaz donde se aplica esto.

Protección contra loops - Generalmente para todos los switches globalmente - Si un switch recibe una BPDU en una interfaz, realiza un seguimiento de esa interfaz para verificar si sigue recibiendo las BPDU cada

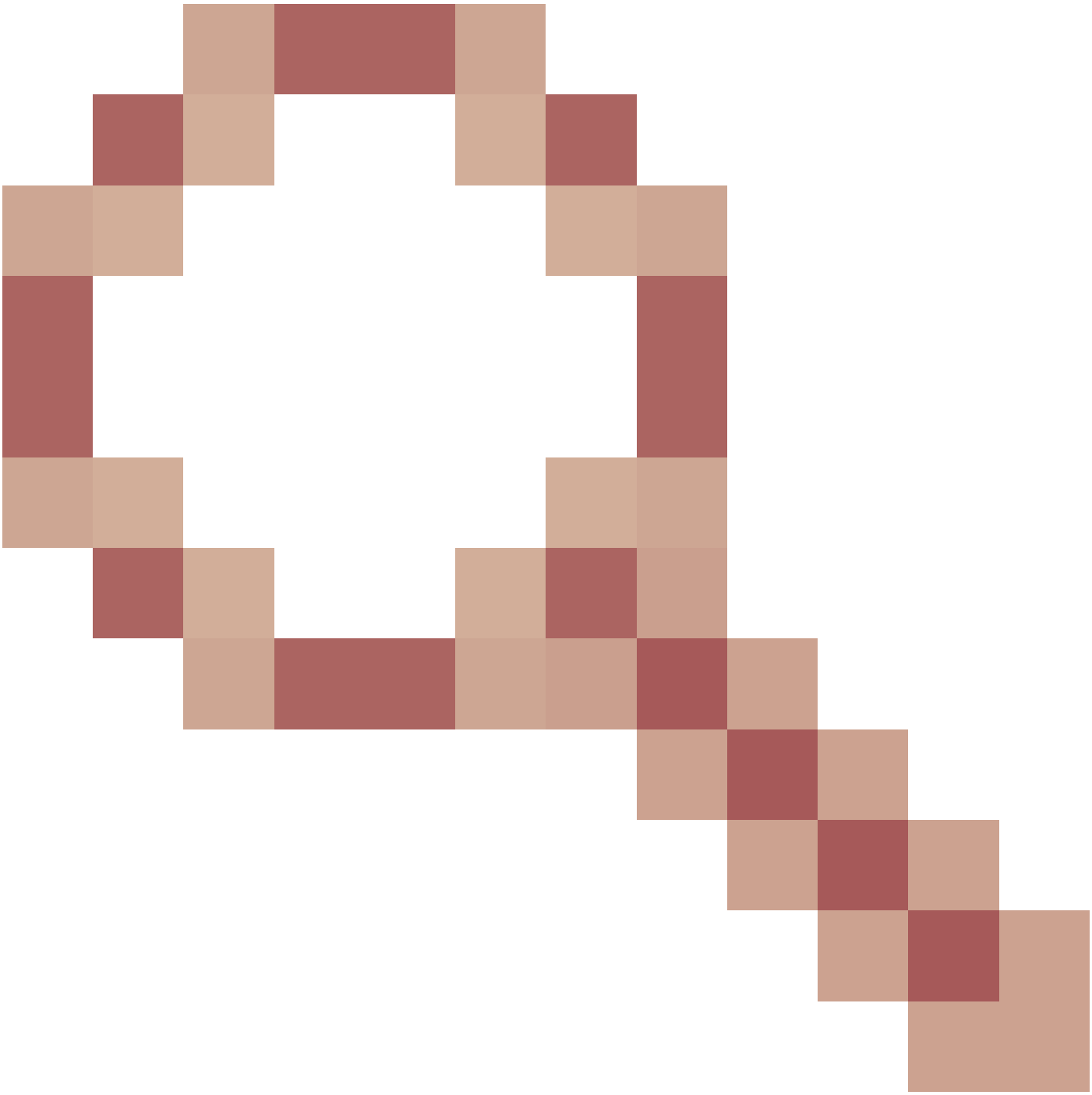
2 segundos después de eso. Si no, se vuelve incoherente con el loop.

Filtro BPDU - Inhabilita STP. BPDU no enviadas ni procesadas tras la recepción. Común con proveedores de servicios, no necesariamente redes empresariales

NO RECOMIENDE TODAS LAS CARACTERÍSTICAS DE STP - por ejemplo bpdufilter supera a bpduguard

UDLD agresivo

Control de tormentas: establecido en un 1% no superior ni inferior. Error de Cisco IDCSCvt85758



CoPP y QoS para escenarios específicos son útiles pero no comunes.

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).