Identificar e Solucionar Problemas de Loops de Camada 2

Contents

Introdução

Este documento descreve informações para ajudar a identificar a origem dos loops de Camada 2 e fornece proteções para evitá-los no futuro.

Pré-requisitos

É recomendável que você tenha conhecimento dos conceitos do STP.

Componentes Utilizados

Este documento não é restrito a versões de software ou hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Comandos utilizados

- show interfaces | include is up|taxa de entrada
- show cdp neighbors <interface>
- show spanning-tree
- show logging

Teoria de Troubleshooting

Não importa a topologia, não importa o ponto de partida (o switch ao qual você está conectado primeiro), a abordagem para rastrear a origem do problema é a mesma.

Use o comando show interface fornecido anteriormente. Estamos nos concentrando na interface ou nas interfaces com altas taxas de entrada.

Altas taxas de saída são um sintoma, não uma causa.

À medida que as interfaces High Input Rate são identificadas, use o CDP neighbor para verificar os links para switches conectados. Se você encontrar uma porta de host, tente desligar a porta para resolver o problema.

Quando você chegar aos switches interconectados de link duplo, use os comandos Spanning Tree para confirmar os estados blocking e forwarding. Isso ajuda a identificar uma porta/switch com defeito.

Topology Change Notifications (TCN) - Ignore-as ao trabalhar em loops.

Os switches mais antigos não têm COPP ou não podem lidar com o processamento de BPDU, o que resulta em TCNs aleatórios.

Se você encontrar a porta que acredita ser o problema - desligue-a e aguarde pelo menos 30 segundos. Se isso não resolver o problema, continue e não "feche" a interface ainda.

Aplicativo

```
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.
```

Prevenção

Práticas recomendadas de STP

BPDU Guard - desabilita as interfaces se elas obtiverem o BPDU guard em vez de encaminhá-lo

Protetor de Raiz - Normalmente para Distro voltado para o Acesso - Você nunca verá um BPDU superior ou inferior na interface onde isso é aplicado.

Proteção de loop - Geralmente para todos os switches globalmente - Se um switch receber uma BPDU em uma interface, ele rastreará essa interface para verificar se continua recebendo as BPDUs a cada

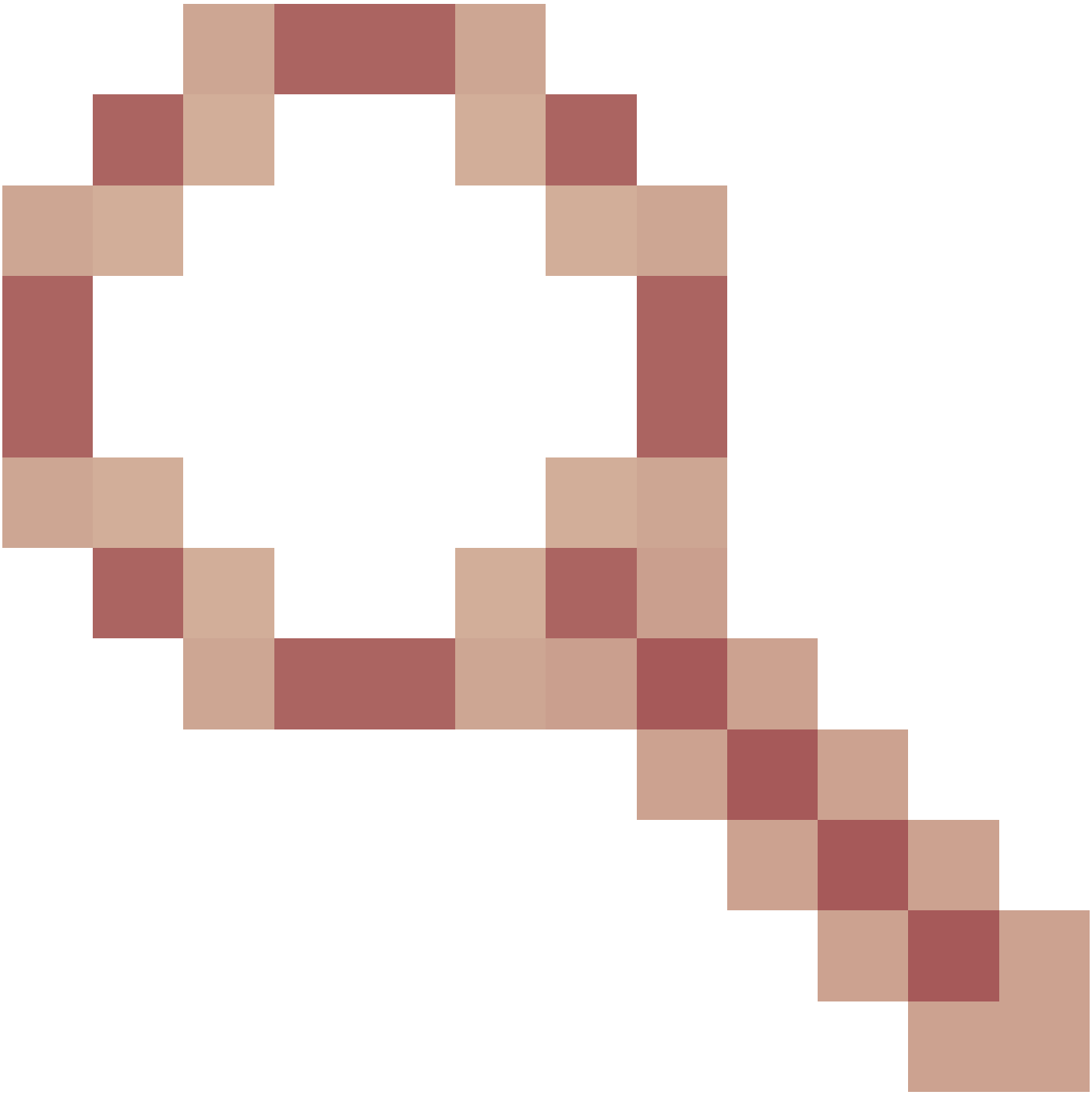
2 segundos depois disso. Caso contrário, ele fica inconsistente em loop.

Filtro de BPDU - Desativa o STP. BPDUs não enviados nem processados no recebimento. Comum com provedores de serviços, não necessariamente redes corporativas

NÃO RECOMENDE TODOS OS RECURSOS DO STP - por exemplo, bpdufilter supera bpduguard

UDLD Agressivo

Controle de Tempestade de Mensagens - definido como 1%, não maior nem menor - Cisco bug IDCSCvt85758



CoPP e QoS para cenários específicos são úteis, mas não comuns.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.