Configuração manual de CTS com falha de propagação de SGT nos troncos da camada 2 do Catalyst 9500X

Contents

Problema

Ao habilitar a configuração manual de CTS com propagação de SGT nas interfaces de tronco de Camada 2 entre os switches de acesso Catalyst C9300L e os switches de núcleo Catalyst C9500X-60L4D, a conectividade é perdida dentro de alguns segundos, mesmo que um segundo uplink permaneça ativo e intocado. O switch de acesso se torna inalcançável a partir das estações de gerenciamento e o desligamento do uplink configurado pelo CTS imediatamente restaura a conectividade.

Os sintomas específicos observados incluem:

- O switch de acesso pára de receber BPDUs nas VLANs afetadas depois que o manual do CTS com propagate sgt é habilitado
- O switch de acesso declara-se raiz STP em ambos os uplinks, formando um loop de Camada 2
- Alto número de quedas de protocolo desconhecidas na interface do switch de acesso (~1,3M de quedas)
- A autorização de CTS é bem-sucedida com o SGT 9999 de mesmo nível instalado e nenhuma falha de CTS, MKA ou MACsec
- O IP de gerenciamento do switch de acesso C9300 se torna inalcançável a partir das estações de gerenciamento centrais
- O problema ocorre especificamente quando o tráfego marcado pelo CMD atravessa o caminho da Camada 2 envolvendo o C9500X

Ambiente

- Switches centrais Catalyst C9500X-60L4D executando o Cisco IOS
- Switches de acesso Catalyst C9300L executando várias versões do Cisco IOS (17.12.4, 17.15.4, 17.15.5)
- Uplinks de tronco de Camada 2 com topologia de spanning tree
- Configuração manual CTS com SGT 9999 estático e propagação habilitada para SGT
- Switches de acesso dual-homed conectados a dois switches centrais
- Configuração da VLAN 50 de gerenciamento

Resolução

Esse problema é causado por uma limitação de hardware específica para as plataformas Catalyst 9500X e Catalyst 9600X. A resolução envolve o entendimento da limitação da plataforma e a implementação de alternativas de projeto apropriadas.

Confirmação de limitação de plataforma

O departamento de engenharia confirmou que a plataforma Catalyst 9500X tem uma limitação de hardware documentada em que ela não adiciona nem remove o cabeçalho Cisco MetaData (CMD) para tráfego transposto de Camada 2. Isto significa:

- O tráfego que chega com CMD sai com CMD
- Tráfego que chega sem CMD sai sem CMD
- A plataforma suporta marcação em linha SGT somente para tráfego roteado (Camada 3)

Resultados do teste direcional

O teste de validação confirmou o comportamento direcional.

Teste 1 - Manual CTS sem propagação em ambos os lados

```
interface
 cts manual
  policy static sgt 9999
  no propagate sgt
Result: PASS - Connection remains stable
```

Teste 2A - Propagação ativada apenas no C9500X

```
! C9500X Core:
interface
 cts manual
  policy static sgt 9999 trusted
  propagate sgt

! C9300L Access:
interface
 cts manual
  policy static sgt 9999 trusted
  no propagate sgt
Result: PASS - Connection remains stable
```

Ensaio 2B: Propagação Habilitada somente no C9300L

```
! C9300L Access:
interface
 cts manual
  policy static sgt 9999 trusted
  propagate sgt

! C9500X Core:
interface
 cts manual
  policy static sgt 9999 trusted
  no propagate sgt
Result: FAIL - Connection breaks after a few seconds
```

Alternativa de design recomendada

Como o manual CTS com propagação SGT não funciona de forma confiável em troncos de Camada 2 para a plataforma C9500X, a solução recomendada é migrar uplinks para interfaces de Camada 3 com marcação em linha SGT.

Configuração do C9500X:

```
interface <interface-id>
 no switchport
 ip address <ip-address> <subnet-mask>
 mtu 9216
 cts role-based enforcement
 cts role-based sgt-map <subnet> sgt 9999
```

Configuração do C9300L:

```
interface <interface-id>
 no switchport
 ip address <ip-address> <subnet-mask>
 mtu 9216
 cts role-based enforcement
 cts role-based sgt-map <subnet> sgt 9999
```

Causa

O problema é causado por uma limitação de hardware específica para as plataformas Catalyst 9500X e Catalyst 9600X baseadas no Silicon One. Essas plataformas não suportam a remoção do cabeçalho do Cisco MetaData (CMD) para o tráfego transposto da Camada 2. Quando o C9300L envia tráfego de Camada 2 com cabeçalhos CMD por propagação SGT, o hardware do C9500X não pode remover o cabeçalho CMD antes de encaminhar pacotes para endpoints não TrustSec, causando problemas de conectividade.

Essa limitação está documentada no Guia de configuração de marcação em linha Cisco Catalyst 9500 SGT e é um comportamento de hardware pretendido em vez de um defeito de software. A restrição diz: "Independentemente da configuração manual cts na interface de saída, o dispositivo não adiciona nem remove o cabeçalho Cisco MetaData (CMD) para o tráfego de Camada 2."

Outras plataformas Catalyst 9000, incluindo a série Catalyst 9550, não têm essa limitação, pois usam arquiteturas de hardware diferentes.

Conteúdo relacionado

- Guia de configuração de marcação em linha Cisco Catalyst 9500 SGT
- ID de bug Cisco CSCwo92798
- Suporte técnico e downloads da Cisco

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.