La configuración manual de CTS con la propagación de SGT falla en los troncales de capa 2 de Catalyst 9500X

Contenido

Problema

Al habilitar la configuración manual de CTS con propagación de SGT en interfaces troncales de capa 2 entre switches de acceso Catalyst C9300L y switches de núcleo Catalyst C9500X-60L4D, la conectividad se pierde en unos pocos segundos aunque un segundo enlace ascendente permanezca activo y sin ser tocado. El switch de acceso se vuelve inalcanzable desde las estaciones de administración, y el cierre del link ascendente configurado por CTS restaura inmediatamente la conectividad.

Los síntomas específicos observados incluyen:

- El switch de acceso deja de recibir BPDU en las VLAN afectadas después de que el manual CTS con sgt de propagación esté habilitado
- El switch de acceso se declara root STP en ambos links ascendentes, formando un loop de Capa 2
- Gran número de caídas de protocolos desconocidos en la interfaz del switch de acceso (~1,3 millones de caídas)
- La autorización de CTS se realiza correctamente con el SGT 9999 instalado y sin errores de CTS, MKA o MACsec
- La IP de administración del switch de acceso C9300 se vuelve inalcanzable desde las estaciones de administración centrales
- Este problema se produce específicamente cuando el tráfico etiquetado CMD atraviesa la ruta de capa 2 que implica el C9500X

Entorno

- Switches de núcleo Catalyst C9500X-60L4D que ejecutan Cisco IOS
- Switches de acceso Catalyst C9300L que ejecutan varias versiones de Cisco IOS (17.12.4, 17.15.4, 17.15.5)
- Enlaces ascendentes de tronco de capa 2 con topología de árbol de extensión
- Configuración manual de CTS con SGT 9999 estático y propagación habilitado para SGT
- Switches de acceso de doble conexión conectados a dos switches de núcleo
- Configuración de VLAN 50 de administración

Resolución

Este problema se debe a una limitación de hardware específica de las plataformas Catalyst 9500X y Catalyst 9600X. La resolución implica entender la limitación de la plataforma e implementar alternativas de diseño apropiadas.

Confirmación de limitación de plataforma

El departamento de ingeniería confirmó que la plataforma Catalyst 9500X tiene una limitación de hardware documentada en la que no agrega ni elimina el encabezado Cisco MetaData (CMD) para el tráfico puenteado de capa 2. Esto significa:

- El tráfico que llega con CMD sale con CMD
- El tráfico que llega sin CMD sale sin CMD
- La plataforma admite el etiquetado en línea de SGT solo para el tráfico enrutado (capa 3)

Resultados de pruebas direccionales

Las pruebas de validación confirmaron el comportamiento direccional.

Prueba 1: manual CTS sin propagación en ambos lados

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

Prueba 2A: propagación habilitada solo en 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
```

Prueba 2B: Propagación habilitada solo en 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 diseño recomendada

Dado que el manual de CTS con propagación de SGT no funciona de forma fiable en los enlaces troncales de capa 2 para la plataforma C9500X, se recomienda migrar los enlaces ascendentes a las interfaces de capa 3 con etiquetado en línea de SGT.

Configuración de 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
```

Configuración de 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

El problema se debe a una limitación de hardware específica de las plataformas Catalyst 9500X y Catalyst 9600X basadas en Silicon One. Estas plataformas no admiten la eliminación del encabezado Cisco MetaData (CMD) para el tráfico puenteado de capa 2. Cuando el C9300L envía tráfico de capa 2 con encabezados CMD a través de la propagación de SGT, el hardware del C9500X no puede eliminar el encabezado CMD antes de reenviar paquetes a terminales que no sean TrustSec, lo que provoca problemas de conectividad.

Esta limitación se documenta en la Guía de configuración de etiquetado en línea de SGT de Cisco Catalyst 9500 y es un comportamiento de hardware intencionado en lugar de un defecto de software. La restricción establece: "Independientemente de la configuración manual de cts en la interfaz de salida, el dispositivo no agrega ni elimina el encabezado de Cisco MetaData (CMD) para el tráfico de capa 2".

Otras plataformas Catalyst 9000, incluida la serie Catalyst 9550, no tienen esta limitación, ya que utilizan arquitecturas de hardware diferentes.

Contenido relacionado

- Guía de configuración de Cisco Catalyst 9500 SGT Inline Tagging
- ID de bug de Cisco CSCwo92798
- Soporte técnico y descargas de Cisco

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).