Configurazione manuale CTS con propagazione SGT non riuscita sui trunk Catalyst 9500X Layer 2

Sommario

Problema

Quando si abilita la configurazione manuale CTS con propagazione SGT sulle interfacce trunk di layer 2 tra gli switch di accesso Catalyst C9300L e gli switch core Catalyst C9500X-60L4D, la connettività viene persa in pochi secondi anche se un secondo uplink rimane attivo e non viene toccato. Lo switch di accesso non è più raggiungibile dalle stazioni di gestione e la chiusura dell'uplink configurato con CTS ripristina immediatamente la connettività.

I sintomi specifici osservati includono:

- Lo switch di accesso non riceve più BPDU sulle VLAN interessate dopo l'abilitazione del manuale CTS con segmento di propagazione
- Lo switch di accesso dichiara se stesso come radice STP su entrambi gli uplink, formando un loop di layer 2
- Numero elevato di cadute di protocollo sconosciute sull'interfaccia dello switch di accesso (~1,3 MB di cadute)
- Autorizzazione CTS riuscita con peer SGT 9999 installato e nessun errore CTS, MKA o MACsec
- L'IP di gestione dello switch di accesso C9300 non è più raggiungibile dalle stazioni di gestione centrali
- Questo problema si verifica in modo specifico quando il traffico con tag CMD attraversa il percorso di layer 2 che interessa il C9500X

Ambiente

- Switch core Catalyst C9500X-60L4D con Cisco IOS
- Switch di accesso Catalyst C9300L con diverse versioni di Cisco IOS (17.12.4, 17.15.4, 17.15.5)
- Uplink di trunk di livello 2 con topologia Spanning Tree
- CTS Configurazione manuale con SGT 9999 statico e propagazione abilitata per SGT
- Switch ad accesso dual-homed collegati a due switch core
- Configurazione della VLAN 50 di gestione

Risoluzione

Questo problema è causato da una limitazione hardware specifica delle piattaforme Catalyst 9500X e Catalyst 9600X. La risoluzione prevede la comprensione dei limiti della piattaforma e l'implementazione di alternative di progettazione appropriate.

Conferma limitazione piattaforma

Il personale tecnico ha confermato che la piattaforma Catalyst 9500X ha una limitazione hardware documentata per cui non aggiunge né rimuove l'intestazione Cisco MetaData (CMD) per il traffico con bridging di layer 2. Ciò significa che:

- Il traffico in arrivo con CMD parte con CMD
- Il traffico in arrivo senza CMD parte senza CMD
- La piattaforma supporta il tagging in linea SGT solo per il traffico indirizzato (livello 3)

Risultati dei test direzionali

Il comportamento direzionale è stato confermato dai test di convalida.

Test 1 - Manuale CTS senza propagazione su entrambi i lati

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

Test 2A - Propagazione abilitata solo su 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
```

Test 2B: Propagazione abilitata solo su 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
```

Design consigliato

Poiché il manuale CTS con propagazione SGT non funziona in modo affidabile sui trunk di layer 2 per la piattaforma C9500X, la soluzione consigliata è la migrazione degli uplink alle interfacce di layer 3 con tagging in linea SGT.

Configurazione 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
```

Configurazione 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

Il problema è causato da una limitazione hardware specifica delle piattaforme Catalyst 9500X e Catalyst 9600X basate su Silicon One. Queste piattaforme non supportano la rimozione dell'intestazione Cisco MetaData (CMD) per il traffico con bridging di layer 2. Quando il C9300L invia traffico di layer 2 con intestazioni CMD tramite propagazione SGT, l'hardware C9500X non può rimuovere l'intestazione CMD prima di inoltrare i pacchetti agli endpoint non TrustSec, causando problemi di connettività.

Questa limitazione è documentata nella guida alla configurazione dei tag in linea di Cisco Catalyst 9500 SGT ed è un comportamento hardware previsto piuttosto che un difetto software. La restrizione prevede quanto segue: "A prescindere dalla configurazione manuale CTS sull'interfaccia in uscita, il dispositivo non aggiunge né rimuove l'intestazione Cisco MetaData (CMD) per il traffico di layer 2."

Altre piattaforme Catalyst 9000, inclusa la serie Catalyst 9550, non hanno questo limite in quanto utilizzano architetture hardware diverse.

Contenuto correlato

- Guida alla configurazione di Cisco Catalyst 9500 SGT Inline Tagging
- ID bug Cisco CSCwo92798
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).