Échec de la configuration manuelle CTS avec propagation SGT sur les agrégations de couche 2 Catalyst 9500X

Table des matières

Problème

Lors de l'activation de la configuration manuelle CTS avec propagation SGT sur les interfaces d'agrégation de couche 2 entre les commutateurs d'accès Catalyst C9300L et les commutateurs principaux Catalyst C9500X-60L4D, la connectivité est perdue en quelques secondes, même si une seconde liaison ascendante reste active et intacte. Le commutateur d'accès devient inaccessible à partir des stations de gestion et l'arrêt de la liaison ascendante configurée par CTS restaure immédiatement la connectivité.

Les symptômes spécifiques observés sont les suivants :

- Le commutateur d'accès arrête de recevoir des BPDU sur les VLAN affectés après l'activation du manuel CTS avec propate sgt
- Le commutateur d'accès se déclare racine STP sur les deux liaisons ascendantes, formant une boucle de couche 2
- Nombre élevé de suppressions de protocoles inconnus sur l'interface du commutateur d'accès (~1,3 million)
- L'autorisation CTS réussit avec l'homologue SGT 9999 installé et aucune défaillance CTS, MKA ou MACsec
- L'adresse IP de gestion du commutateur d'accès C9300 devient inaccessible à partir des stations de gestion centrales
- Le problème se produit spécifiquement lorsque le trafic étiqueté CMD traverse le chemin de couche 2 impliquant le C9500X

Environnement

- Commutateurs principaux Catalyst C9500X-60L4D exécutant Cisco IOS
- Commutateurs d'accès Catalyst C9300L exécutant diverses versions de Cisco IOS (17.12.4, 17.15.4, 17.15.5)
- Liaisons ascendantes d’agrégation de couche 2 avec topologie Spanning Tree
- Configuration manuelle CTS avec SGT 9999 statique et propagation activée par SGT
- Commutateurs d'accès à double résidence connectés à deux commutateurs principaux
- Configuration du VLAN 50 de gestion

Résolution

Ce problème est dû à une limitation matérielle spécifique aux plates-formes Catalyst 9500X et Catalyst 9600X. La résolution implique de comprendre les limites de la plate-forme et de mettre en oeuvre des alternatives de conception appropriées.

Confirmation de limitation de plateforme

L'équipe technique a confirmé que la plate-forme Catalyst 9500X présente une limitation matérielle documentée qui n'ajoute ni ne supprime l'en-tête Cisco MetaData (CMD) pour le trafic ponté de couche 2. Cela signifie :

- Le trafic arrivant avec CMD part avec CMD
- Trafic arrivant sans CMD quitte sans CMD
- La plate-forme prend en charge l'étiquetage en ligne SGT uniquement pour le trafic routé (couche 3)

Résultats des tests directionnels

Les tests de validation ont confirmé le comportement directionnel.

Test 1 - Manuel CTS sans propagation des deux côtés

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

Test 2A - Propagation activée uniquement sur 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 : Propagation activée uniquement sur 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
```

Alternative de conception recommandée

Étant donné que le manuel CTS avec propagation SGT ne fonctionne pas de manière fiable sur les agrégations de couche 2 pour la plate-forme C9500X, la solution recommandée est de migrer les liaisons ascendantes vers les interfaces de couche 3 avec étiquetage en ligne SGT.

Configuration 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
```

Configuration 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
```

Motif

Le problème est causé par une limitation matérielle spécifique aux plates-formes Catalyst 9500X et Catalyst 9600X basées sur Silicon One. Ces plates-formes ne prennent pas en charge la suppression de l'en-tête Cisco MetaData (CMD) pour le trafic ponté de couche 2. Lorsque le C9300L envoie du trafic de couche 2 avec des en-têtes CMD via la propagation SGT, le matériel C9500X ne peut pas supprimer l'en-tête CMD avant de transférer les paquets vers des points d'extrémité non-TrustSec, ce qui entraîne des problèmes de connectivité.

Cette limitation est documentée dans le Guide de configuration de l'étiquetage en ligne des balises SGT de Cisco Catalyst 9500 et constitue un comportement matériel prévu plutôt qu'un défaut logiciel. La restriction stipule : « Quelle que soit la configuration manuelle de cts sur l'interface de sortie, le périphérique n'ajoute ni ne supprime l'en-tête Cisco MetaData (CMD) pour le trafic de couche 2. »

Les autres plates-formes Catalyst 9000, y compris la gamme Catalyst 9550, n'ont pas cette limitation car elles utilisent des architectures matérielles différentes.

Autres informations utiles

- Guide de configuration du balisage en ligne Cisco Catalyst 9500 SGT
- ID de bogue Cisco CSCwo92798
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.