Manuelle CTS-Konfiguration mit SGT-Propagierung scheitert an Catalyst 9500X Layer-2-Trunks

Inhalt

Problem

Wenn die manuelle CTS-Konfiguration mit SGT-Propagierung an Layer-2-Trunk-Schnittstellen zwischen Catalyst C9300L Access Switches und Catalyst C9500X-60L4D Core Switches aktiviert wird, geht die Verbindung innerhalb weniger Sekunden verloren, obwohl ein zweiter Uplink aktiv und unberührt bleibt. Der Access Switch kann von den Managementkonsolen nicht mehr erreicht werden, und durch das Herunterfahren des CTS-konfigurierten Uplinks wird die Verbindung umgehend wiederhergestellt.

Zu den beobachteten spezifischen Symptomen gehören:

- Access Switch beendet den Empfang von BPDUs in betroffenen VLANs, nachdem das CTS-Handbuch mit Propagate Sgt aktiviert wurde
- Access Switch deklariert sich selbst als STP-Root auf beiden Uplinks und bildet eine Layer-2-Schleife
- Große Anzahl unbekannter Protokollverluste an der Access Switch-Schnittstelle (~1,3 Mio.)
- CTS-Autorisierung erfolgreich mit installiertem Peer-SGT 9999 und ohne CTS-, MKA- oder MACsec-Fehler
- Die Management-IP-Adresse des Access Switches C9300 ist für zentrale Verwaltungsstationen nicht mehr erreichbar.
- Das Problem tritt besonders auf, wenn CMD-markierter Datenverkehr den Layer-2-Pfad mit dem C9500X durchläuft

Umwelt

- Catalyst C9500X-60L4D Core-Switches mit Cisco IOS
- Catalyst C9300L Access Switches mit verschiedenen Cisco IOS-Versionen (17.12.4, 17.15.4, 17.15.5)
- Layer-2-Trunk-Uplinks mit Spanning Tree-Topologie
- CTS Manuelle Konfiguration mit statischem SGT 9999 und SGT-aktivierter Propagierung
- Dual-Homed Access Switches verbunden mit zwei Core Switches
- Konfiguration des Management-VLAN 50

Auflösung

Dieses Problem wird durch eine spezifische Hardwarebeschränkung für die Plattformen Catalyst 9500X und Catalyst 9600X verursacht. Die Lösung besteht darin, die Plattformbeschränkungen zu verstehen und geeignete Designalternativen zu implementieren.

Plattformbeschränkung - Bestätigung

Die Techniker bestätigten, dass die Catalyst 9500X-Plattform eine dokumentierte Hardwarebeschränkung aufweist, da der Cisco MetaData (CMD)-Header für Layer-2-Bridge-Datenverkehr weder hinzugefügt noch entfernt wird. Das bedeutet:

- Datenverkehr, der mit CMD eingeht, verlässt CMD
- Ohne CMD ankommender Datenverkehr verlässt ohne CMD
- Die Plattform unterstützt SGT-Inline-Tagging nur für gerouteten Datenverkehr (Layer 3).

Ergebnisse der Richtungsprüfung

Validierungstests bestätigten das Richtungsverhalten.

Test 1 - CTS-Handbuch ohne Propagierung auf beiden Seiten

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

Test 2A - Propagierung nur auf C9500X aktiviert

```
! 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: Propagierung nur auf C9300L aktiviert

```
! 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
```

Empfohlene Designalternative

Da das CTS-Handbuch mit SGT-Propagierung auf Layer-2-Trunks für die C9500X-Plattform nicht zuverlässig funktioniert, wird empfohlen, Uplinks zu Layer-3-Schnittstellen mit SGT-Inline-Tagging zu migrieren.

Konfiguration des 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
```

Konfiguration des 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
```

Ursache

Das Problem wird durch eine Hardwarebeschränkung verursacht, die speziell für die Plattformen Catalyst 9500X und Catalyst 9600X mit Silicon One gilt. Diese Plattformen unterstützen das Entfernen des Cisco MetaData (CMD)-Headers für Layer-2-Bridge-Datenverkehr nicht. Wenn der C9300L Layer-2-Datenverkehr mit CMD-Headern über SGT-Propagierung sendet, kann die C9500X-Hardware den CMD-Header nicht entfernen, bevor Pakete an Endpunkte weitergeleitet werden, die nicht TrustSec-konform sind, was zu Verbindungsproblemen führt.

Diese Einschränkung wird im Konfigurationsleitfaden für das Cisco Catalyst 9500 SGT Inline-Tagging dokumentiert. Es handelt sich hierbei nicht um einen Softwarefehler, sondern um ein beabsichtigtes Hardwareverhalten. Die Einschränkung besagt: "Unabhängig von der manuellen CTS-Konfiguration an der Ausgangsschnittstelle fügt das Gerät den Cisco MetaData (CMD)-Header für Layer-2-Datenverkehr weder hinzu noch entfernt es ihn."

Andere Catalyst 9000-Plattformen, darunter die Catalyst Serie 9550, unterliegen dieser Einschränkung nicht, da sie unterschiedliche Hardwarearchitekturen verwenden.

Verwandte Inhalte

- Konfigurationsleitfaden für Cisco Catalyst 9500 SGT Inline-Tagging
- Cisco Bug-ID CSCwo92798
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.