CTS Manual Configuration with SGT Propagation Fails on Catalyst 9500X Layer 2 Trunks

Contents

Issue

When enabling CTS Manual configuration with SGT propagation on Layer 2 trunk interfaces between Catalyst C9300L access switches and Catalyst C9500X-60L4D core switches, connectivity is lost within a few seconds even though a second uplink remains active and untouched. The access switch becomes unreachable from management stations, and shutting down the CTS-configured uplink immediately restores connectivity.

Specific symptoms observed include:

- Access switch stops receiving BPDUs on affected VLANs after CTS manual with propagate sgt is enabled
- Access switch declares itself STP root on both uplinks, forming a Layer 2 loop
- High number of unknown protocol drops on the access switch interface (~1.3M drops)
- CTS authorization succeeds with peer SGT 9999 installed and no CTS, MKA, or MACsec failures
- Management IP of the C9300 access switch becomes unreachable from central management stations
- Issue occurs specifically when CMD-tagged traffic traverses the Layer 2 path involving the C9500X

Environment

- Catalyst C9500X-60L4D core switches running Cisco IOS
- Catalyst C9300L access switches running various Cisco IOS versions (17.12.4, 17.15.4, 17.15.5)
- Layer 2 trunk uplinks with spanning tree topology
- CTS Manual configuration with static SGT 9999 and propagate SGT-enabled
- Dual-homed access switches connected to two core switches
- Management VLAN 50 configuration

Resolution

This issue is caused by a hardware limitation specific to the Catalyst 9500X and Catalyst 9600X platforms. The resolution involves understanding the platform limitation and implementing appropriate design alternatives.

Platform Limitation Confirmation

Engineering confirmed that the Catalyst 9500X platform has a documented hardware limitation where it neither adds nor removes the Cisco MetaData (CMD) header for Layer 2 bridged traffic. This means:

- Traffic arriving with CMD leaves with CMD
- Traffic arriving without CMD leaves without CMD
- The platform supports SGT inline tagging only for routed (Layer 3) traffic

Directional Testing Results

Validation testing confirmed the directional behavior.

Test 1 - CTS Manual without Propagation on Both Sides

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

Test 2A - Propagation Enabled only on 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 Enabled only on 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
```

Recommended Design Alternative

Since CTS manual with SGT propagation does not work reliably on Layer 2 trunks for the C9500X platform, the recommended solution is to migrate uplinks to Layer 3 interfaces with SGT inline tagging.

C9500X configuration:

```
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
```

C9300L configuration:

```
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
```

Cause

The issue is caused by a hardware limitation specific to Silicon One-based Catalyst 9500X and Catalyst 9600X platforms. These platforms do not support removal of the Cisco MetaData (CMD) header for Layer 2 bridged traffic. When the C9300L sends Layer 2 traffic with CMD headers via SGT propagation, the C9500X hardware cannot remove the CMD header before forwarding packets to non-TrustSec endpoints, causing connectivity issues.

This limitation is documented in the Cisco Catalyst 9500 SGT Inline Tagging Configuration Guide and is an intended hardware behavior rather than a software defect. The restriction states: "Irrespective of the cts manual configuration on the egress interface, the device neither adds nor removes the Cisco MetaData (CMD) header for Layer 2 traffic."

Other Catalyst 9000 platforms, including the Catalyst 9550 Series, do not have this limitation as they use different hardware architectures.

Related Content

- Cisco Catalyst 9500 SGT Inline Tagging Configuration Guide
- Cisco bug ID CSCwo92798
- Cisco Technical Support & Downloads