Catalyst 9500X Layer 2 Trunk에서 SGT 전파가 포함된 CTS 수동 컨피그레이션 실패

목차

문제

Catalyst C9300L 액세스 스위치와 Catalyst C9500X-60L4D 코어 스위치 간 레이어 2 트렁크 인터페이스에서 SGT 전파로 CTS 수동 구성을 활성화하면 두 번째 업링크가 활성 상태로 유지되지만 몇 초 내에 연결이 끊깁니다. 액세스 스위치가 관리 스테이션에서 연결할 수 없게 되고 CTS 구성 업링크를 종료하면 연결이 즉시 복원됩니다.

관찰된 특정 증상은 다음과 같습니다.

- CTS manual with propagate sgt가 활성화된 후 액세스 스위치가 영향을 받는 VLAN에서 BPDU 수신을 중지합니다.
- 액세스 스위치가 두 업링크 모두에서 자체 STP 루트를 선언하여 레이어 2 루프를 형성함
- 액세스 스위치 인터페이스에서 알 수 없는 프로토콜 삭제 수가 많음(~1.3M 삭제)
- 피어 SGT 9999가 설치되어 있고 CTS, MKA 또는 MACsec 오류가 없는 경우 CTS 권한 부여가 성공함
- 중앙 관리 스테이션에서 C9300 액세스 스위치의 관리 IP에 연결할 수 없음
- 특히 CMD 태그가 지정된 트래픽이 C9500X와 관련된 레이어 2 경로를 통과할 때 문제가 발생합니다

환경

- Cisco IOS를 실행하는 Catalyst C9500X-60L4D 코어 스위치
- 다양한 Cisco IOS 버전(17.12.4, 17.15.4, 17.15.5)을 실행하는 Catalyst C9300L 액세스 스위치

- 스패닝 트리 토폴로지를 사용하는 레이어 2 트렁크 업링크
- 정적 SGT 9999 및 전파 SGT가 활성화된 CTS 수동 구성
- 2개의 코어 스위치에 연결된 듀얼 홈 액세스 스위치
- 관리 VLAN 50 컨피그레이션

해결

이 문제는 Catalyst 9500X 및 Catalyst 9600X 플랫폼별 하드웨어 제한으로 인해 발생합니다. 해결에는 플랫폼의 제한 사항을 이해하고 적절한 설계 대안을 구현하는 것이 포함됩니다.

플랫폼 제한 확인

엔지니어링에서는 Catalyst 9500X 플랫폼에 레이어 2 브리지 트래픽에 대한 Cisco CMD(MetaData) 헤더를 추가하거나 제거하지 않는 문서화된 하드웨어 제한이 있음을 확인했습니다. 이는 다음을 의미합니다.

- CMD로 도착하는 트래픽은 CMD로 떠남
- CMD 없이 도착하는 트래픽은 CMD 없이 떠남
- 이 플랫폼은 라우팅된(레이어 3) 트래픽에 대해서만 SGT 인라인 태깅을 지원합니다

방향 테스트 결과

검증 테스트를 통해 방향 동작이 확인되었습니다.

테스트 1 - 양쪽에서 전파가 없는 CTS 수동

```
interface
 cts manual
```

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

테스트 2A - C9500X에서만 전파 활성화

```
! 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
```

테스트 2B: C9300L에서만 전파 활성화

```
! 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
```

권장 설계 대안

C9500X 플랫폼의 레이어 2 트렁크에서는 SGT 전파가 포함된 CTS 매뉴얼이 안정적으로 작동하지 않으므로, SGT 인라인 태깅이 포함된 레이어 3 인터페이스에 업링크를 마이그레이션하는 것이 좋습니다.

C9500X 구성:

```
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 구성:

```
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
```

원인

이 문제는 Silicon One 기반 Catalyst 9500X 및 Catalyst 9600X 플랫폼에 한정된 하드웨어 제한으로 인해 발생합니다. 이러한 플랫폼은 레이어 2 브리지 트래픽에 대한 CMD(Cisco MetaData) 헤더 제거를 지원하지 않습니다. C9300L이 SGT 전파를 통해 CMD 헤더가 포함된 레이어 2 트래픽을 전송할 경우, C9500X 하드웨어는 패킷을 비 TrustSec 엔드포인트로 전달하기 전에 CMD 헤더를 제거할 수 없으므로 연결 문제가 발생합니다.

이러한 제한은 Cisco Catalyst 9500 SGT Inline Tagging 컨피그레이션 가이드에 설명되어 있으며 소프트웨어 결함이 아닌 의도된 하드웨어 동작입니다. 제한 상태는 다음과 같습니다. "이그레스 인터페이스의 cts 수동 컨피그레이션과 상관없이 디바이스는 레이어 2 트래픽에 대한 Cisco CMD(MetaData) 헤더를 추가하거나 제거하지 않습니다."

Catalyst 9550 Series를 포함한 다른 Catalyst 9000 플랫폼은 서로 다른 하드웨어 아키텍처를 사용하므로 이러한 제한이 없습니다.

관련 콘텐츠

- Cisco Catalyst 9500 SGT 인라인 태깅 컨피그레이션 가이드
- Cisco 버그 ID CSCwo92798
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.