VLAN 인스턴스 제한으로 인한 네트워크 중단 이해

목차

소개

이 문서에서는 로우엔드 레거시 Catalyst 스위치의 VLAN 인스턴스 제한과 그 방지로 인한 잠재적인 네트워크 중단에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 기본 스위칭 개념에 대한 지식과 함께 Cisco Catalyst 스위치의 STP(Spanning Tree Protocol) 및 기능에 대한 이해를 가질 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 주로 로우엔드 레거시 디바이스인 Cisco Catalyst 스위치를 기반으로 하며, 특정 소프트웨어 또는 하드웨어 버전에 제한되지 않고 모든 버전에 적용할 수 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

네트워크 인프라의 안정성은 조직 운영에 매우 중요하며, 네트워킹 하드웨어의 제약 조건을 관리하는 것이 지속적인 안정성을 보장하는 데 핵심적입니다. 기존의 많은 네트워크 환경에서 대표적인 로우엔드 레거시 Catalyst 스위치는 VLAN 인스턴스 제한과 같은 심각한 문제로 이어질 수 있는 한

계에 직면하는 경우가 많습니다. 이 제한은 스위치에서 동시에 지원할 수 있는 STP 인스턴스 수와 관련이 있습니다. 조직이 이러한 스위치의 VLAN 인스턴스 제한에 도달하면 추가 VLAN에 대해 STP를 활성화할 수 없으므로 네트워크 루프 및 잠재적 중단의 위험이 있습니다.

VLAN 인스턴스 제한 이해

루프 방지를 위해 STP가 필요한 스위치의 각 VLAN은 별도의 인스턴스로 계산됩니다. 로우엔드 및 레거시 스위치는 처리할 수 있는 동시 STP 인스턴스의 수에 엄격한 제한을 두고 있습니다. 최대치에 도달하면 STP 보호 장치 없이 추가 VLAN이 작동하므로 네트워크가 루프 위험에 노출되어 브로드캐스트 스톰과 광범위한 중단이 발생할 수 있습니다.

Cisco Catalyst 3850 스위치가 지원하는 것보다 많은 VLAN을 사용하여 작동하는 예를 들면 다음과 같습니다.

<#root>

Switch#show run | i span

```
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

no spanning-tree vlan 43,125,402,404,406,409,412,414-415,418-420,422-424,426 < ----- STP disabled on the

no spanning-tree vlan 427,430

spanning-tree vlan 1-1005 priority 40960

스위치는 지원되는 최대 스패닝 트리 인스턴스 수로 작동하고 있습니다.

<#root>

Switch#show spannig-tree summary totals

```
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
```

128 vlans < -----

```
           29         0        0       1481       1510
```

Switch#show spanning-tree instances

MAX STP instances supported is 128 < -----

VLAN 인스턴스 제한 초과 위험

스위치에서 VLAN 인스턴스 제한을 초과해도 즉시 중단되지는 않습니다. 그 대신, 네트워크 재구성 시 또는 새 연결이 실수로 루프를 생성하는 경우 예기치 않게 발생할 수 있는 잠재적인 위험이 발생합니다. 이러한 루프를 탐지하고 차단하는 STP가 없으면 하나의 잘못된 단계로 인해 심각한 네트워크 중단이 발생할 수 있습니다.

일반적인 증상

1. MAC - 플랩:

```
%MAC_MOVE-SW1-4-NOTIF: Host xxxx.xxxx.xxxx in vlan <> is flapping between port (1) and port (2)
%MAC_MOVE-SW1-4-NOTIF: Host yyyy.yyyy.yyyy in vlan <> is flapping between port port (1) and port (2)
%MAC_MOVE-SW1-4-NOTIF: Host zzzz.zzzz.zzzz in vlan <> is flapping between port (1) and port (2)
```

2. 토폴로지 변경 통지

<#root>

```
VLAN0999 is executing the rstp compatible Spanning Tree protocol
  Number of topology
```

changes 72413

```
 last change occurred
```

0o:00:05 ago

from TenGigabitEthernet1/1/1

```
VLAN0608 is executing the rstp compatible Spanning Tree protocol
  Number of topology
```

changes 1106

```
 last change occurred
```

00:07:53 ago

from TenGigabitEthernet1/1/1

```
VLAN0301 is executing the rstp compatible Spanning Tree protocol
  Number of topology
```

changes 25824

```
 last change occurred
```

00:03:13 ago

```
          from Port-channel21
```

3. 인터럽트/ARP 입력/STP 프로세스로 인한 높은 CPU 사용률

```
<#root>

CPU utilization for

five seconds: 99%/5%;

 one minute: 98%; five minutes: 97%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process

  11   48417100   4048595      11957  28.47% 27.55% 27.15%   0 ARP Input < ----- High CPU due to ARP Inp


 130    2296685   1887488       1216  21.19% 20.49% 20.01%   0 Spanning Tree
 205   12387701   1054338      11749   8.91%  9.02%  9.10%   0 Hulc LED Process
  88    3036802    283172      10723   6.71%  6.98%  6.85%   0 IP Input
  44     867032    754781       1148   4.27%  4.45%  4.35%   0 Interrupts
```

예방 및 완화 기법

네트워크 관리자는 로우엔드 레거시 Catalyst 스위치의 VLAN 인스턴스 제한과 관련된 위험을 완화하기 위해 다음과 같은 여러 전략을 사용할 수 있습니다.

1. VLAN 통합: 가능한 경우 네트워크 트래픽을 결합 또는 재구성하여 STP를 사용하는 VLAN 수를 줄입니다.
2. MSTP 구현: PVST+ 또는 Rapid-PVST+에서 MSTP(Multiple Spanning Tree Protocol)로 이동하여 VLAN을 더 적은 수의 STP 인스턴스로 그룹화합니다.
3. STP 참여 최적화: 루프 위험이 낮은 VLAN 또는 대체 루프 방지 메커니즘이 있는 네트워크 세그먼트에서 STP를 비활성화합니다.
4. 네트워크 인프라 업그레이드: 구형 로우엔드 스위치를 더 많은 수의 STP 인스턴스를 지원할 수 있는 최신 하드웨어로 교체하십시오.
5. 네트워크 재설계: 트래픽 흐름을 최적화하고, 필요한 VLAN 수를 줄이며, 기존 하드웨어의 기능에 더 잘 부합하도록 네트워크 설계를 재평가합니다.

결론

로우엔드 레거시 스위치의 VLAN 인스턴스 제한에 도달하는 것은 해결되지 않을 경우 네트워크 중단을 초래할 수 있는 시한폭탄입니다. 하드웨어 업그레이드 및 전략적 네트워크 설계 조정을 비롯한 사전 대응적 네트워크 관리는 이러한 위험을 완화하고 노후화된 기술에 직면한 네트워크 인프라의 복원력을 보장하기 위해 필수적입니다.

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.