스위치드 캠퍼스 네트워크의 유니캐스트 플러딩

목차

소개

이 문서에서는 스위치드 네트워크에서 유니캐스트 패킷 플러딩의 가능한 원인과 영향에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

문제 정의

LAN 스위치는 포워딩 테이블(L2(Layer 2) 테이블, CAM(Content Addressable Memory) 테이블)을 사용하여 프레임의 VLAN 번호 및 대상 MAC 주소를 기반으로 특정 포트로 트래픽을 전송합니다.수신 VLAN에서 프레임의 대상 MAC 주소에 해당하는 항목이 없으면 (유니캐스트) 프레임이 해당 VLAN 내의 모든 포워딩 포트로 전송되어 플러딩이 발생합니다.

제한적 홍수는 일반적인 스위칭 프로세스의 일부입니다.그러나 지속적인 플러딩이 네트워크에 부정적인 영향을 미칠 수 있는 상황이 있습니다.이 문서에서는 플러딩으로 인해 발생할 수 있는 문제

및 특정 트래픽이 지속적으로 플러딩되는 가장 일반적인 이유에 대해 설명합니다.

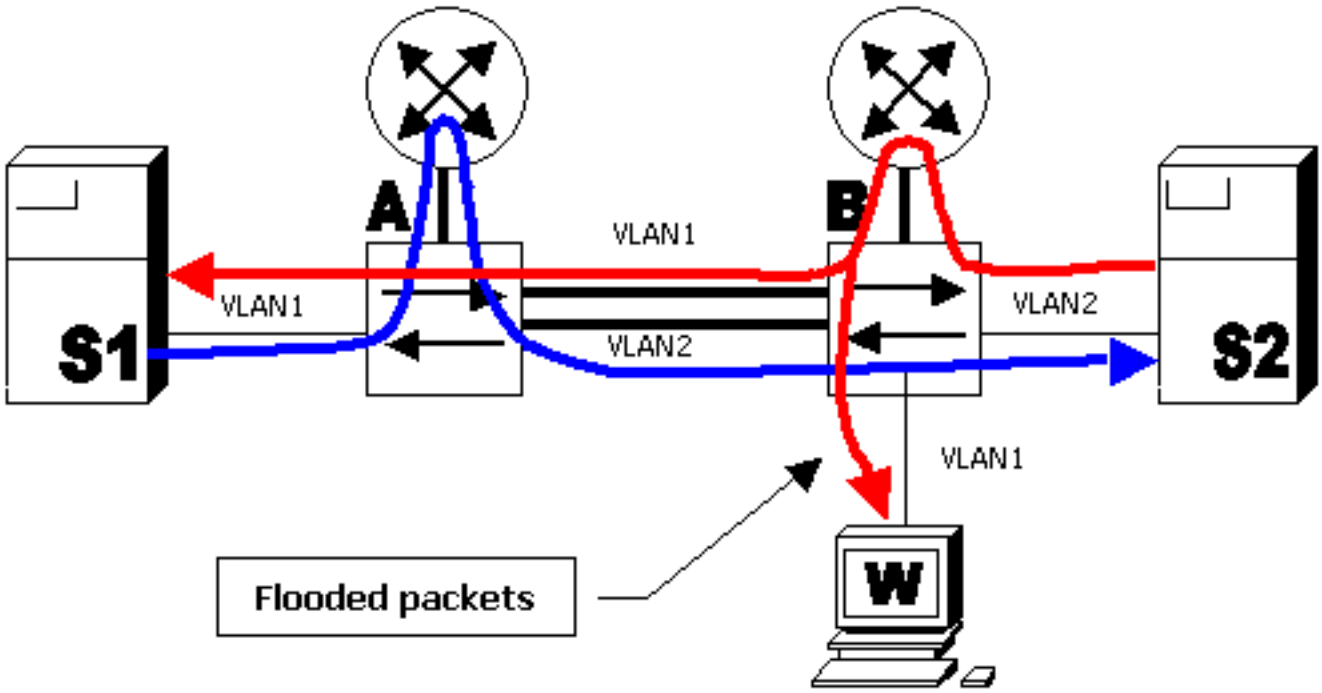
Catalyst 2900 XL, 3500 XL, 2940, 2950, 2970, 3550, 3750, 4500/4000, 5000 및 65000/6000 시리즈 스위치를 포함한 대부분의 최신 스위치는 L2 포워딩 테이블을 유지합니다.

홍수의 원인

패킷의 대상 MAC 주소가 스위치의 L2 포워딩 테이블에 없는 것이 플러딩의 원인입니다.이 경우 패킷은 VLAN의 모든 포워딩 포트(수신된 포트 제외)에서 플러딩됩니다. 아래 사례 연구는 대상 MAC 주소가 스위치에 알려지지 않은 가장 일반적인 이유를 보여줍니다.

원인 1:비대칭 라우팅

대량의 플러딩된 트래픽은 낮은 대역폭 링크를 포화, 네트워크 성능 문제를 야기하거나 이러한 낮은 대역폭 링크를 통해 연결된 장치에 대한 완전한 연결 중단을 초래할 수 있습니다.다음 다이어그램을 고려하십시오.



위 다이어그램에서 VLAN 1의 서버 S1은 VLAN 2의 서버 S2에 대한 백업(대량 데이터 전송)을 실행하고 있습니다. 서버 S1에는 라우터 A의 VLAN 1 인터페이스를 가리키는 기본 게이트웨이가 있습니다.서버 S2에는 라우터 B의 VLAN 2 인터페이스를 가리키는 기본 게이트웨이가 있습니다.S1에서 S2로의 패킷은 다음 경로를 따릅니다.

- S1—VLAN 1—스위치 A—라우터 A—VLAN 2—스위치 B—VLAN 2—S2(파란색 회선)

S2에서 S1까지의 패킷은 다음 경로를 따릅니다.

- S2—VLAN 2—스위치 B—라우터 B—라우터 B—VLAN 1—스위치 A—플러딩된 VLAN 1—S1(빨간색 라인)로 플러딩됨

이러한 방식으로 배치하면, 소스 MAC 주소가 라우터 B에 의해 재작성되고 패킷이 VLAN 1에만 도달하기 때문에 스위치 A는 VLAN 2의 S2 MAC 주소에서 오는 트래픽을 "볼 수 없습니다. 즉, 스위치 A가 S2 MAC 주소로 패킷을 전송해야 할 때마다 패킷이 VLAN 2로 플러딩됩니다. 스위치 B의 S1 MAC 주소에서도 동일한 상황이 발생합니다.

이러한 동작을 비대칭 라우팅이라고 합니다.패킷은 방향에 따라 다른 경로를 따릅니다.비대칭 라우팅은 홍수의 가장 일반적인 두 가지 원인 중 하나입니다.

유니캐스트 플러딩의 영향

위의 예로 돌아가면 S1과 S2 간의 데이터 전송 패킷이 대부분 스위치 A의 VLAN 2와 스위치 B의 VLAN 1로 플러딩됩니다. 즉, 스위치 B의 VLAN 1에 있는 모든 연결된 포트(이 예에서는 워크스테이션 W)는 S1과 S2 간의 모든 대화 패킷을 수신합니다. 서버 백업에 50Mbps의 대역폭이 사용된다고 가정합니다.이 트래픽 양은 10Mbps 링크를 포화 시킵니다.이로 인해 PC에 대한 완전한 연결이 중단되거나 속도가 크게 저하됩니다.

이 플러딩은 비대칭 라우팅 때문이며 서버 S1이 브로드캐스트 패킷(예: ARP(Address Resolution Protocol)을 전송할 때 중지될 수 있습니다. 스위치 A는 이 패킷을 VLAN 1로 플러딩하고 스위치 B는 S1의 MAC 주소를 수신하고 학습합니다. 스위치가 지속적으로 트래픽을 수신하지 않으므로 이 전달 항목은 결국 타임아웃되고 플러딩이 다시 시작됩니다.동일한 프로세스가 S2에 적용됩니다.

비대칭 라우팅으로 인한 플러딩을 제한하는 여러 가지 방법이 있습니다.자세한 내용은 다음 문서를 참조하십시오.

- Catalyst 2948G-L3 및 4908G-L3 스위치에서 브리지 그룹을 사용한 비대칭 라우팅
- 비대칭 라우팅 및 HSRP(HSRP를 실행하는 라우터를 사용하는 네트워크에서 유니캐스트 트래픽의 과도한 플러딩)

일반적으로 라우터의 ARP 시간 초과 및 스위치의 포워딩 테이블 에이징 시간을 서로 가깝게 설정하는 방식입니다.그러면 ARP 패킷이 브로드캐스트됩니다.재학습은 L2 포워딩 테이블 항목이 만료되기 전에 이루어져야 합니다.

이러한 문제가 발생할 수 있는 일반적인 시나리오는 HSRP(Hot Standby Router Protocol)와 로드 밸런싱하도록 구성된 중복 L3(Layer 3) 스위치(예: MSFC(Multilayer Switch Feature Card)가 있는 Catalyst 600)가 있는 경우입니다. 이 경우 짝수 VLAN에 대해 하나의 스위치가 활성화되고 다른 스위치는 홀수 VLAN에 대해 활성화됩니다.

원인 2:스패닝 트리 프로토콜 토폴로지 변경

플러딩으로 인해 발생하는 또 다른 일반적인 문제는 STP(Spanning-Tree Protocol) TCN(Topology Change Notification)입니다.TCN은 전달 토폴로지가 변경된 후 전달 테이블을 수정하도록 설계되었습니다.토폴로지가 변경되면 특정 포트를 통해 이전에 액세스할 수 있었던 일부 목적지가 서로 다른 포트를 통해 액세스할 수 있으므로 연결 중단을 방지하기 위해 이 작업이 필요합니다.TCN은 포워딩 테이블 에이징 시간을 단축하여 작동하며, 이 경우 주소가 재학습되지 않으면 에이징되고 플러딩이 발생합니다.

TCN은 전달 상태로 전환하거나 전달 상태에서 전환하는 포트에 의해 트리거됩니다.TCN 이후, 특정 목적지 MAC 주소가 오래되었더라도 주소가 다시 학습되므로 대부분의 경우 플러딩이 오래 발생하지 않아야 합니다.TCN이 짧은 간격으로 반복적으로 발생할 경우 문제가 발생할 수 있습니다.이 스위치는 지속적으로 포워딩 테이블을 빠르게 에이징하므로 플러딩이 거의 일정하게 유지됩니다.

일반적으로 TCN은 잘 구성된 네트워크에서 드문 경우입니다.스위치의 포트가 작동 또는 다운되면 포트의 STP 상태가 포워딩으로 또는 포워딩에서 변경되면 결국 TCN이 발생합니다.포트가 플래핑되면 반복 TCN과 플러딩이 발생합니다.

STP portfast 기능이 활성화된 포트는 전달 상태로 전환하거나 전달할 때 TCN을 발생시키지 않습니다.프린터, PC, 서버 등과 같은 모든 엔드 디바이스 포트에서 포트 컨피그레이션을 수행하면 TCN이 낮게 제한됩니다.TCN에 대한 자세한 내용은 이 문서를 참조하십시오.

- 스패닝 트리 프로토콜 토폴로지 변경 이해

참고: MSFC IOS에는 각 VLAN에 TCN이 있을 때 VLAN 인터페이스가 ARP 테이블을 다시 채우도록 트리거하는 최적화가 있습니다.ARP 브로드캐스트가 있을 것이므로 TCN의 경우 플러딩이 제한되며 호스트가 ARP에 응답할 때 호스트 MAC 주소가 다시 학습됩니다.

원인 3:포워딩 테이블 오버플로

또 다른 가능한 원인은 스위치 포워딩 테이블의 오버플로일 수 있습니다.이 경우, 새 주소를 알 수 없으며 해당 주소로 향하는 패킷은 포워딩 테이블에서 일부 공간을 사용할 수 있을 때까지 플러딩됩니다.그런 다음 새 주소를 학습합니다.대부분의 최신 스위치에는 대부분의 설계에서 MAC 주소를 수용할 수 있는 포워딩 테이블이 충분히 크기 때문에 이러한 작업은 가능하지만 드문 일입니다.

포워딩 테이블 소모는 한 호스트가 각각 다른 MAC 주소로 소싱된 프레임을 생성하기 시작하는 네트워크에 대한 공격으로 인해 발생할 수도 있습니다.이렇게 하면 모든 포워딩 테이블 리소스가 연결됩니다.포워딩 테이블이 포화 상태가 되면 새로운 학습이 이루어지지 않으므로 다른 트래픽이 플러딩됩니다.이러한 종류의 공격은 스위치 포워딩 테이블을 검토하여 탐지할 수 있습니다.대부분의 MAC 주소는 동일한 포트 또는 포트 그룹을 가리킵니다.이러한 공격은 포트 보안 기능을 사용하여 신뢰할 수 없는 포트에서 학습된 MAC 주소의 수를 제한함으로써 방지할 수 있습니다.

Cisco IOS® 또는 CatOS 소프트웨어를 실행하는 Catalyst 스위치에 대한 컨피그레이션 가이드에는 포트 보안 구성 또는 포트 기반 트래픽 제어 구성이라는 섹션이 있습니다.자세한 내용은 Cisco 스위치 제품 페이지의 스위치 기술 문서를 참조하십시오.

참고: 유니캐스트 플러딩이 "Restrict(제한)"의 조건으로 포트 보안용으로 구성된 스위치 포트에서 발생하는 경우 보안 위반이 트리거됩니다.

```
Router(config-if)#switchport port-security violation restrict
```

참고: 이러한 보안 위반이 발생하면 "restrict" 모드에 대해 구성된 영향 받는 포트는 알 수 없는 소스 주소가 있는 패킷을 삭제해야만 보안 MAC 주소 수가 최대값 아래로 떨어질 수 있습니다.이로 인해 SecurityViolation 카운터가 증가합니다.

참고: 이 동작 대신 스위치 포트가 "Shutdown" 상태로 전환되면 유니캐스트 플러딩에 대해 특정 스위치 포트가 비활성화되도록 `(config-if)#switchport` 구성해야 합니다.

과도한 플러딩을 탐지하는 방법

대부분의 스위치는 플러딩을 탐지하기 위해 특별한 명령을 구현하지 않습니다.Cisco IOS System 소프트웨어(기본) 버전 12.1(14)E 이상 또는 Cisco CatOS 시스템 소프트웨어 버전 7.5 이상을 실행하는 Catalyst 6500/600 Supervisor Engine 2 이상 시리즈 스위치는 '**유니캐스트 플러드 보호**' 기능을 구현합니다.간단히 말해, 이 기능을 사용하면 스위치가 VLAN당 유니캐스트 플러딩의 양을 모니터링하고 플러딩이 지정된 양을 초과할 경우 지정된 조치를 취할 수 있습니다.작업은 syslog, limit 또는 shutdown VLAN일 수 있습니다. syslog는 플러드 탐지에 가장 유용합니다.플러딩이 구성된 속도를 초과하고 구성된 작업이 syslog인 경우 다음과 유사한 메시지가 인쇄됩니다.

```
%UNICAST_FLOOD-4-DETECTED: Host 0000.0000.2100 on vlan 1 is flooding
to an unknown unicast destination at a rate greater than/equal to 1 Kfps
```

표시된 MAC 주소는 이 스위치에서 패킷이 플러딩되는 소스 MAC입니다.스위치가 플러딩되는 대상 MAC 주소를 알아야 하는 경우가 많습니다(대상 MAC 주소를 확인하여 스위치가 포워딩되기 때문).

Cisco IOS(Native) 버전 12.1(20)E for Catalyst 6500/6000 supervisor engine 2 및 on은 플러딩이 발생하는 MAC 주소를 표시하는 기능을 구현합니다.

```
cat6000#sh mac-address-table unicast-flood
Unicast Flood Protection status: enabled

Configuration:
 vlan      Kfps         action       timeout
------+----------+----------------+----------
   55          1             alert      none

Mac filters:
 No.   vlan   souce mac addr.           installed on           time left (mm:ss)
-----+------+----------------+-----------------------------+------------------

Flood details:
 Vlan   souce mac addr.              destination mac addr.
------+---------------+-------------------------------------------------
   55   0000.2222.0000    0000.1111.0029, 0000.1111.0040, 0000.1111.0063
                          0000.1111.0018, 0000.1111.0090, 0000.1111.0046
                          0000.1111.006d
```

그런 다음 MAC 주소 0000.2222.0000이 대상 MAC 주소 섹션에 나열된 MAC 주소로 트래픽을 전송해야 하는지 확인하기 위해 추가 조사를 수행할 수 있습니다.트래픽이 합법적인 경우 목적지 MAC 주소가 스위치에 알려지지 않은 이유를 설정해야 합니다.

슬로우 또는 중단 시 워크스테이션에서 보이는 패킷의 추적을 캡처하여 플러딩이 발생하는지 감지할 수 있습니다.일반적으로 워크스테이션과 관련이 없는 유니캐스트 패킷은 포트에서 반복적으로 볼 수 없습니다.만약 이것이 일어난다면, 홍수가 발생하고 있을 가능성이 있습니다.패킷 추적은 플러딩의 다양한 원인이 있을 때 다르게 보일 수 있습니다.

비대칭 라우팅을 사용하면 특정 MAC 주소에 대한 패킷이 있을 수 있으며, 이는 목적지 응답 후에도 플러딩을 멈추지 않습니다.TCN을 사용하면 플러딩에 여러 주소가 포함되지만, 결국 중지했다가 다시 시작해야 합니다.

L2 포워딩 테이블 오버플로의 경우 비대칭 라우팅과 동일한 종류의 플러딩을 볼 수 있습니다.차이점은 많은 양의 이상한 패킷이 있거나 다른 소스 MAC 주소를 가진 비정상적인 수량의 일반 패킷이 있을 가능성이 높다는 것입니다.

관련 정보

- 스위치 제품 지원
- LAN 스위칭 기술 지원
- Technical Support - Cisco Systems