Nexus 7000 Troubleshoot ARP(Address Resolution Protocol) Storm Without Inband Capture

목차

소개

이 문서에서는 인밴드 ARP 트래픽 없이 ARP 스톰을 해결하는 방법에 대해 설명합니다.

배경

ARP 폭풍은 데이터 센터 환경에서 흔히 볼 수 있는 DoS(denial-of-service) 공격입니다.

ARP 패킷을 처리하는 일반적인 스위치 로직은 다음과 같습니다.

- 브로드캐스트 대상 MAC(Media Access Control)이 포함된 ARP 패킷
- 스위치에 속하는 유니캐스트 목적지 MAC가 있는 ARP 패킷

SVI(Switch Virtual Interface)가 수신 VLAN에 있는 경우 소프트웨어에서 ARP 프로세스에 의해 처리됩니다.

이 논리로, 하나 이상의 악성 호스트가 VLAN에서 ARP 요청을 계속 보내는 경우, 여기서 스위치는 해당 VLAN의 게이트웨이입니다.ARP 요청은 소프트웨어에서 처리되므로 스위치가 과중한 상태가 됩니다.일부 이전 Cisco 스위치 모델 및 버전에서는 ARP 프로세스가 CPU 사용량을 최고 수준으로 올리고 시스템이 너무 사용량이 많아 다른 컨트롤 플레인 트래픽을 처리할 수 없음을 확인할 수 있습니다.이러한 공격을 추적하는 일반적인 방법은 인밴드 캡처를 실행하여 ARP 스톰의 소스 MAC을 식별하는 것입니다.

Nexus 7000이 어그리게이션 게이트웨이 역할을 하는 데이터 센터에서는 이러한 영향을 Nexus 7000 Series 스위치의 CoPP로 줄일 수 있습니다.CoPP(Control Plane Policing)는 속도를 늦추지만 ARP 스톰이 CPU로 돌진하는 것을 막지 않으므로 Nexus 7000 Troubleshooting Guide에서 인밴드 캡처 Ethanalyzer를 실행하여 ARP 스톰의 소스 MAC를 식별할 수 있습니다.

다음과 같은 경우 이 시나리오는 어떻습니까?

- SVI가 다운되었습니다.
- CPU에 대한 과도한 ARP 패킷이 적용되지 않음
- ARP 프로세스로 인해 높은 CPU 없음

그러나 스위치에는 ARP 관련 문제가 계속 표시됩니다. 예를 들어 직접 연결된 호스트에 불완전한 ARP가 있습니다.ARP 폭풍에 의한 것일 수 있습니까?

Nexus 7000에서 그렇습니다.

근본 원인

Nexus 7000 라인 카드 설계에서 CoPP의 ARP 패킷 프로세스를 지원하기 위해 ARP 요청은 LIF(Special Logical Interface)를 구동한 다음 FE(Forwarding Engine)의 CoPP로 속도를 제한합니다. 이는 VLAN에 대한 SVI가 있는지 여부에 관계없이 발생합니다.

따라서 FE에서 최종 포워딩 결정을 내릴 때 인밴드 CPU에 ARP 요청을 보내지 않는 반면(VLAN에 대해 SVI가 지원되지 않는 경우) CoPP 카운터는 계속 업데이트됩니다.이로 인해 CoPP에 과도한 ARP 요청 및 합법적인 ARP 요청/회신이 포화 상태가 됩니다.이 시나리오에서는 과도한 인밴드 ARP 패킷은 표시되지 않지만 ARP 폭풍의 영향을 받습니다.

이 CoPP Day 1 동작에 대한 향상된 버그 CSCub47533이 있습니다.

솔루션

이 시나리오에서는 ARP 스톰의 소스를 식별하는 몇 가지 옵션이 있을 수 있습니다.한 가지 효과적인 옵션은 다음과 같습니다.

- 먼저 ARP 스톰이 발생하는 모듈을 확인합니다.

```
N7K# sh policy-map interface control-plane class copp-system-p-class-normal
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match exception ip multicast directly-connected-sources
match exception ipv6 multicast directly-connected-sources
match protocol arp
set cos 1
police cir 680 kbps bc 250 ms
conform action: transmit
violate action: drop
 module 3:
conformed 4820928 bytes,
5-min offered rate 0 bytes/sec
peak rate 104 bytes/sec at Thu Aug 25 08:12:12 2016
 violated 9730978848 bytes,
       5-min violate rate 6983650 bytes/sec
       peak rate 7632238 bytes/sec at Thu Aug 25 00:43:33 2016
module 4:
conformed 4379136 bytes,
5-min offered rate 0 bytes/sec
peak rate 38 bytes/sec at Wed Aug 24 07:12:09 2016
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
...
```

- 두 번째는 ELAM Procedure를 사용하여 모듈을 적중하는 모든 ARP 패킷을 캡처합니다.여러 번 하셔야 할 것 같습니다하지만 폭풍이 진행 중인 경우, ARP 패킷을 캡처할 경우 합법적인 ARP 패킷보다 훨씬 더 좋습니다.ELAM 캡처에서 소스 MAC 및 VLAN을 식별합니다.