Nexus 7000排除地址解析協定(ARP)風暴故障，無需帶內捕獲

目錄

簡介

本文說明如何在不使用任何帶內ARP流量的情況下對ARP風暴進行故障排除。

背景

ARP風暴是常見的資料中心環境中的拒絕服務(DoS)攻擊。

處理ARP資料包的常見交換機邏輯如下：

- 具有廣播目的地媒體存取控制(MAC)的ARP封包
- 帶有單播目標MAC的ARP資料包，屬於交換機

如果在接收Vlan中的交換機虛擬介面(SVI)處於開啟狀態，則軟體中的ARP進程將對其進行處理。

根據這一邏輯，如果有一個或多個惡意主機不斷在Vlan中傳送ARP請求，則其中交換機是該Vlan的網關。ARP請求將在軟體中處理，因此會導致交換機不堪重負。在一些較舊的Cisco交換機型號和版本中，您會看到ARP進程將CPU使用率提升到較高水準，而且系統太繁忙，無法處理其他控制平面流量。跟蹤此類攻擊的常見方法是運行帶內捕獲，以識別ARP風暴的源MAC。

在Nexus 7000充當匯聚網關的資料中心，Nexus 7000系列交換機上的CoPP降低了此類影響。您仍然可以在Nexus 7000故障排除指南上運行帶內捕獲Ethanalyzer以確定ARP風暴的源MAC，因為控制平面管制(CoPP)只是一種放慢速度，但無法消除湧向CPU的ARP風暴。

在以下情況下，該場景如何：

- SVI已關閉
- 沒有過多的ARP資料包被傳送到CPU
- 由於ARP進程沒有高CPU

但是，交換機仍會遇到與ARP相關的問題，例如直連主機的ARP不完整。是否可能由ARP風暴引起？

在Nexus 7000上，答案是肯定的。

根本原因

在nexus 7000線卡設計中，為了支援CoPP中的ARP資料包處理，ARP請求將驅動一個特殊的邏輯

介面(LIF)，然後受到轉發引擎(FE)中CoPP的速率限制。 無論您是否已為Vlan建立SVI，都會發生這種情況。

因此，雖然FE做出的最終轉發決策是不向帶內CPU傳送ARP請求（如果沒有VLAN的SVI），但CoPP計數器仍然會更新。這會導致CoPP充斥著過多的ARP請求和丟棄合法ARP請求/應答。在此案例中，您不會看到任何過多的帶內ARP資料包，但仍會受到ARP風暴的影響。

我們針對此CoPP第1天行為歸檔了增強型錯誤CSCub47533。

解決方案

在此案例中，可能有幾個選項用於確定ARP風暴的來源。一個有效的選項是：

- 首先識別ARP風暴來自哪個模組

```
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
...
```

- 然後使用ELAM過程捕獲到達模組的所有ARP資料包。您可能需要執行好幾次。但是如果風暴正在發生，您捕獲違規ARP資料包的機率要比獲取ARP資料包的機率高得多。從ELAM捕獲中識別源MAC和Vlan。