Nexus 7000排除地址解析协议(ARP)风暴故障，无带内捕获

目录

简介

本文档介绍如何排除ARP风暴故障，而不带内ARP流量。

背景

ARP风暴是您在数据中心环境中看到的常见拒绝服务(DoS)攻击。

处理ARP数据包的常见交换机逻辑是：

- 具有广播目标媒体访问控制(MAC)的ARP数据包
- 具有单播目的MAC的ARP数据包，属于交换机

如果交换机虚拟接口(SVI)在接收VLAN中处于启用状态，则将通过软件中的ARP过程进行处理。

根据此逻辑，如果有一台或多台恶意主机在Vlan中继续发送ARP请求，其中交换机是该Vlan的网关。ARP请求将在软件中处理，因此交换机会被淹没。在某些较旧的思科交换机型号和版本中，您会看到ARP进程占用CPU的高级，并且系统太忙，无法处理其他控制平面流量。跟踪此类攻击的常见方法是运行带内捕获以识别ARP风暴的源MAC。

在Nexus 7000充当汇聚网关的数据中心中，Nexus 7000系列交换机上的CoPP可以降低这种影响。您仍可以在Nexus 7000上运行带内捕获Ethanalyzer故障排除指南，以识别ARP风暴的源MAC，因为控制平面策略(CoPP)只是一个缓慢但不会导致ARP风暴涌入CPU的强盗。

如果：

- SVI关闭
- 没有过多的ARP数据包被发送到CPU
- 由于ARP进程，没有高CPU

但交换机仍会看到与ARP相关的问题，例如直连主机的ARP不完整。是否可能由ARP风暴引起？

在Nexus 7000上，答案是肯定的。

根本原因

在nexus 7000线卡设计中，为了支持CoPP中的ARP数据包处理，ARP请求将驱动特殊逻辑接口(LIF)，然后在转发引擎(FE)中受CoPP的速率限制。 无论您是否为Vlan提供SVI，都会发生这种情况

。

因此，尽管FE做出的最终转发决定是不向带内CPU发送ARP请求（如果VLAN没有SVI），CoPP计数器仍会更新。它导致CoPP饱和，ARP请求过多，并丢弃合法ARP请求/应答。在此场景中，您不会看到任何过多的带内ARP数据包，但仍受到ARP风暴的影响。

我们已针对此CoPP第一天行为提交了增强的Bug CSCub47533。

解决方案

在此场景中，可以有几个选项来确定ARP风暴的源。一个有效的选择是：

- 首先确定ARP风暴来自哪个模块

```
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
...
```

- 第二步使用ELAM程序捕获到模块的所有ARP数据包。你可能需要做几次。但是，如果发生风暴，捕获违反的ARP数据包的机率比估计的ARP数据包要好得多。从ELAM捕获中确定源MAC和Vlan。