连结7000排除故障地址解析服务(ARP)风暴，不用带内捕获

目录

[简介](#)
[背景](#)
[根本原因](#)
[解决方案](#)

简介

本文描述如何排除故障ARP风暴，不用任何带内ARP流量。

背景

ARP风暴是您在数据中心环境会看到的一次普通的服务拒绝(DoS)攻击。

处理ARP数据包的普通的交换机逻辑是那：

- 有广播目的地媒体访问控制的(MAC) ARP数据包
- ARP数据包用单播目的地MAC，属于交换机

如果Switch Virtual Interface (SVI)是UP在接收的VLAN，将由ARP进程在软件方面处理。

由此逻辑，如果有一个或更多malicous主机在VLAN保留发送ARP请求，交换机是该VLAN网关。因此ARP请求在软件方面将处理引起被淹没的交换机。在某个更旧的Cisco交换机型号和版本中，您看到ARP进程采取CPU使用情况至高层次，并且系统太忙碌以至于不能处理其他控制层面流量。跟踪这样攻击的普通方法是运行带内捕获识别ARP风暴的源MAC。

在连结7000作为聚合网关的数据中心， CoPP减少这样影响在连结7000系列交换机。您可能仍然运行在连结7000故障排除指南的带内捕获Ethanalyzer识别ARP风暴的源MAC，因为控制平面策略(CoPP)是不elminating的匪盗减速，但是冲对CPU的ARP风暴。

此方案where:怎么样

- SVI发生故障
- 没有额外的ARP数据包是平底船对CPU
- 没有高CPU由于ARP进程

然而交换机仍然看到ARP相关问题，即直接连接的主机有不完整ARP。它可能是否是由ARP风暴造成的？

答案是在连结7000的是。

根本原因

在连结7000线路卡设计，支持在CoPP的ARP数据包进程， ARP请求在转发引擎(FE)方面将驱动一

个特殊逻辑接口(LIF)然后是CoPP限制的速率。这发生您有一SVI VLAN的没有问题。

因此，而FE做的最终转发决策是不发送ARP请求对带内CPU (在案件编号SVI VLAN)， CoPP计数器仍然更新。它导致CoPP饱和与额外的ARP请求和下降合法ARP请求/回复。在此方案中，您将看不到所有额外的带内ARP数据包，但是仍然影响受ARP风暴的。

为此CoPP天一行为有一增强版bug CSCub47533归档的我们。

解决方案

能有一些个选项识别ARP风暴来源在此方案的。一个有效选项是：

- 首先请识别哪个模块ARP风暴来自

```
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
...
```

- 获取所有ARP数据包的第二个使用伊拉姆步骤点击模块。您也许需要执行它几次。但是，如果有继续的风暴，您获取违反ARP数据包的机会比legetimate ARP数据包是好。识别源MAC和VLAN从伊拉姆捕获。