某局点S6800-54QF开启ARP主动确认功能时上行防火墙vrrp主备切换断网一分钟问题

ARP 张文宁 2020-02-28 发表

组网及说明

如下图所示，两台启明FW起了vrrp主备，与S6800三层互联，S6800上写了缺省路由指向vrrp组的虚地址实现S6800下面终端访问外网的路径备份。

问题描述

现场发现当防火墙主备倒换的时候，S6800下面终端访问外网的业务会中断一分钟，问题必现，故障时候在S6800上ping启明防火墙实地址，发现ping不通，对比查看故障和恢复后S6800的ARP表项发现主备倒换后的1分钟内S6800没有及时更新ARP的出接口和mac（他们主备切换虚ip的mac也会变化），所以不通。现场查看设备存在以下不熟悉的配置，怀疑导致设备无法更新arp，删除后再主备倒换发现arp立刻更新了，要求这边给出命令的解释和故障分析报告：

Arp active-ack enable

Arp source-suppression enable

Arp source-suppression limit 100

过程分析

查看上述命令，后面两条命令只是arp的抑制，防止收到网络中有主机向设备发送大量目标IP地址不能解析的IP报文的恶意攻击，而现场只是防火墙侧主备倒换，理论上和这两条命令无关。

问题锁定到第一条命令Arp active-ack enable，ARP主动确认功能：

1.7.1 ARP主动确认功能简介

ARP的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。

配置ARP主动确认功能后，设备在新建或更新ARP表项前需进行主动确认，防止产生错误的ARP表项。

配置严格模式后，新建ARP表项前，ARP主动确认功能会执行更严格的检查：

·收到目标IP地址为自己的ARP请求报文时，设备会发送ARP应答报文，但不建立ARP表项；

·收到ARP应答报文时，需要确认本设备是否对该报文中的源IP地址发起过ARP解析：若发起过解析，解析成功后则设备启动主动确认功能，主动确认流程成功完成后，设备可以建立该表项；若未发起过解析，则设备丢弃该报文。

1.7.2 开启ARP主动确认功能

表1-9 开启ARP主动确认功能

配置步骤	命令	说明
进入系统视图	system-view	-
开启ARP主动确认功能	arp active-ack [strict] enable	缺省情况下，ARP主动确认功能处于关闭状态

因为现场没有收集反馈任何信息，因此只能采用相同版本进行本地模拟复现，结果并未复现，测试如下：

S125-X-----S6800

原本S6800能正常学习到S125-X的arp报文，此时老化时间是1191：

<2064-6800>dis arp

Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid

IP address MAC address VLAN/VSI Interface/Link ID Aging Type

120.1.1.2 74ea-c830-5001 1 XGE1/0/31 1191 D

在S125-X上直接shutdown int vlan 1然后修改mac为74ea-c830-5102：

[125X]int vlan 1

[125X-Vlan-interface1]shut

[125X-Vlan-interface1]%Sep 12 11:07:57:146 2019 125X IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the interface Vlan-interface1 changed to down.
%Sep 12 11:07:57:146 2019 125X IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the interface Vlan-interface1 changed to down.
[125X-Vlan-interface1]mac-address 74ea-c830-5102
[125X-Vlan-interface1]undo shut
[125X-Vlan-interface1]%Sep 12 11:09:48:000 2019 125X IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the interface Vlan-interface1 changed to up.
%Sep 12 11:09:48:001 2019 125X IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the interface Vlan-interface1 changed to up.

然后在S6800上可以看到过程：
<2064-6800>
*Sep 12 03:12:27:223 2019 2064-6800 ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 74ea-c830-5102, sender IP: 120.1.1.2, target MAC: 0000-0000-0000, target IP: 120.1.1.2 ----------收到免费arp 1（网卡起来会发两次免费arp）
*Sep 12 03:12:27:223 2019 2064-6800 ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender MAC: 9ce8-9572-8330, sender IP: 120.1.1.1, target MAC: 74ea-c830-5001, target IP: 120.1.1.2 ----------不信这个arp的表项发生了变化，先发出个老mac的arp 请求报文
*Sep 12 03:12:27:227 2019 2064-6800 ARP/7/ARP_RCV: Received an ARP message, operation: 2, sender MAC: 74ea-c830-5102, sender IP: 120.1.1.2, target MAC: 9ce8-9572-8330, target IP: 120.1.1.1 ----------收到了这个ip就是新mac的应答。
*Sep 12 03:12:31:432 2019 2064-6800 ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 74ea-c830-5102, sender IP: 120.1.1.2, target MAC: 0000-0000-0000, target IP: 120.1.1.2 ----------收到免费arp 2（网卡起来会发两次免费arp）
*Sep 12 03:12:31:860 2019 2064-6800 ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender MAC: 9ce8-9572-8330, sender IP: 120.1.1.1, target MAC: 74ea-c830-5102, target IP: 120.1.1.2
----------再去请求这个ip对应新mac的arp请求报文。
*Sep 12 03:12:31:862 2019 2064-6800 ARP/7/ARP_RCV: Received an ARP message, operation: 2, sender MAC: 74ea-c830-5102, sender IP: 120.1.1.2, target MAC: 9ce8-9572-8330, target IP: 120.1.1.1 ----------得到应答。 主动确认过程结束。 更新arp表项。

<2064-6800>dis arp
Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid
IP address MAC address VLAN/VSI Interface/Link ID Aging Type
120.1.1.2 74ea-c830-5102 1 XGE1/0/31 1199 D
<2064-6800>

因此从理论上和本地复现分析，我们应该能快速地主动确认并更新到arp表项的，从日志时间点可以看到主动确认时间在4秒内就完成了（接口stp状态不变的情况下）和现场长达1分钟没有更新到arp的情况不相符。

因此怀疑现象的主动确认过程应该是卡在某个阶段了，最后客户协调窗口时间进行复现，并收集debug arp packet如下，可以发现设备在02:00:16收到了启明FW切换时发送的免费ARP，但是却等了大概1分钟后的02:01:08才发起主动确认过程。因此问题锁定在为什么这么慢才发起主动确认过程。
[H3C]#*Jan 1 01:59:48:100 2011 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0010-f37d-ac88, sender IP: 10.197.254.173, target MAC: 0000-0000-0000, target IP: 10.197.254.173

[H3C]*Jan 1 02:00:16:961 2011 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0010-f37d-a940, sender IP: 10.197.254.173, target MAC: 0000-0000-0000, target IP: 10.197.254.173
*Jan 1 02:00:16:962 2011 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0010-f37d-a940, sender IP: 10.197.254.173, target MAC: 0000-0000-0000, target IP: 10.197.254.173
*Jan 1 02:00:17:151 2011 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0010-f37d-a940, sender IP: 10.197.254.173, target MAC: 0000-0000-0000, target IP: 10.197.254.173
*Jan 1 02:00:17:154 2011 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0010-f37d-a940, sender IP: 10.197.254.173, target MAC: 0000-0000-0000, target IP: 10.197.254.173

[H3C]*Jan 1 02:01:08:219 2011 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0010-f37d-a940, sender IP: 10.197.254.173, target MAC: 0000-0000-0000, target IP: 10.

197.254.173
*Jan 1 02:01:08:219 2011 H3C ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender MAC: 5098-b817-f3a0, sender IP: 10.197.254.169, target MAC: 0010-f37d-ac88, target IP: 10.197.254.173
*Jan 1 02:01:13:031 2011 H3C ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender MAC: 5098-b817-f3a0, sender IP: 10.197.254.169, target MAC: 0010-f37d-a940, target IP: 10.197.254.173
*Jan 1 02:01:13:033 2011 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 2, sender MAC: 0010-f37d-a940, sender IP: 10.197.254.173, target MAC: 5098-b817-f3a0, target IP: 10.197.254.169
*Jan 1 02:01:38:457 2011 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0010-f37d-a940, sender IP: 10.197.254.173, target MAC: 0000-0000-0000, target IP: 10.197.254.173

最后找到平台研发走读代码发现，ARP主动确认发起过程有个判断机制，如果一个arp是1分钟内学习或者更新的，不会立刻触发主动确认功能，而是会1分钟后才会切换，目的是避免受到反复变化的arp恶意攻击。

重新查看上述的debug可以看到，对端防火墙平时就在不停发送当前ip的 免费ARP（30秒一个）。 所以在 01:59:48 的时候 刚刚收到过旧MAC(ac88)的免费ARP。 所以这条就ARP的时间搓是 01:59:48，所以在02:00:48秒之前发来的新mac(a940)的免费ARP是不做处理的，
现场收到第一个新mac(a940)的ARP是在02:00:16， 还在1分钟之内，不更新。 所以直到02:01:08(a940)收到的这次新mac 的ARP才处理，才触发了主动探测。导致业务中断约1分钟。

定位结论：
1、 机制配合问题。交换机开启ARP主动确认功能后，收到免费arp不会立刻更新arp，会进行主动确认。而且针对新学习的arp（1分钟内）不会立刻触发主动确认过程。

解决方法

解决方法：
本侧关闭arp主动确认功能或者对端调大、关闭定时发送免费arp功能。