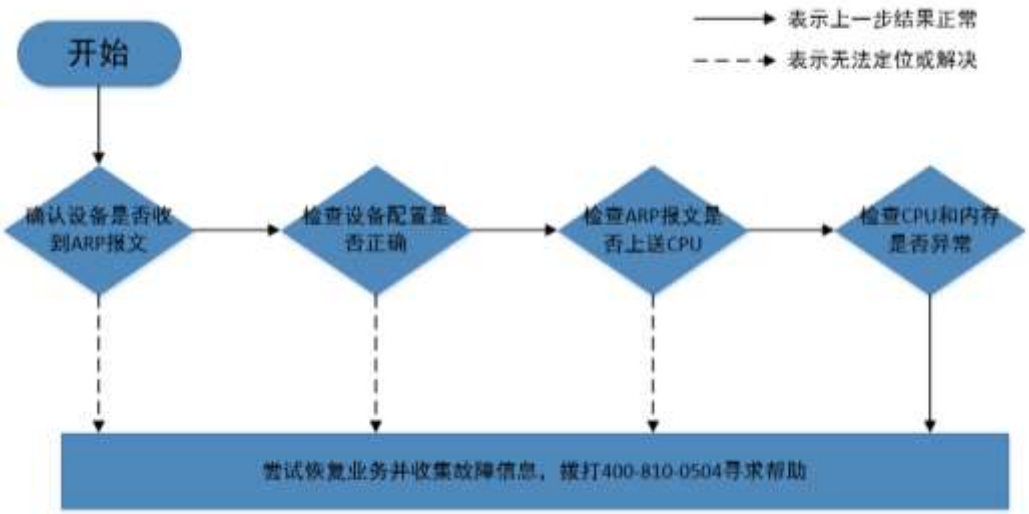
V7 交换机无法学习 ARP 问题排查云图



一、 开始

交换机对于三层报文转发需要学习到对应 IP 地址的 ARP 表项，ARP 会将 IP 地址解析为以太网 MAC 地址。在网络中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址），由于 IP 数据报必须封装成帧才能通过物理网络发送，因此还需要知道对方的物理地址，所以设备上需要存在一个从 IP 地址到物理地址的映射关系，即 ARP 表项。如果交换机无法学习到对应 ARP 表项，会导致三层数据转发异常，需进一步排查定位。

具体排查步骤如下：

步骤 1：确认设备接口是否收到对应 ARP 报文

步骤 2：检查设备配置是否正确

步骤 3：检查 ARP 报文是否上送 CPU

步骤 4：检查 CPU 和内存是否异常

步骤 5：尝试恢复业务并收集故障信息，拨打 4008100504 寻求帮助

二、 流程图相关操作说明

1、 确认设备接口是否收到对应 ARP 报文

交换机设备上 display arp 没有对应 IP 地址的 ARP 表项，首先需要确认对应的 ARP 报文

在对应接口是否有收到。可以通过流量统计或者镜像抓包的方式判断。

具体 ARP 报文流量统计可以参考如下配置方式：

针对 ARP 报文的流统需要注意的是，必须创建一个 MAC ACL，指定类型编号为 0806 的 ARP 报文、根据报文的源目MAC 进行匹配。假设需统计广播 ARP 请求报文，需要创建一个 MAC ACL 匹配 0806 类型、源 MAC 为 0001-0001-0001 的报文。

```
Step 1：定义 MAC ACL 匹配一个方向的 ARP 流量（ARP Request 为例）
ACL Mac 4000
 Rule 5 permit type 0806 ffff source-mac 0001-0001-0001 ffff-ffff-ffff

Step 2:定义类匹配 ACL 和计数动作
Traffic classifier classifier_1
If-match acl 4000
Traffic behavior behavior_1
Accounting packet

Step 3:定义 QOS 关联类和动作
Qos policy policy_1
Classifier classifier_1 behavior behavior_1

Step 4:应用 QOS 策略到对应接口的对应方向
Interface  Ten-GigabitEthernet 1/0/1
Qos apply policy policy_1 inbound

Step 5：查看流量统计计数
Display qos policy interface Ten-GigabitEthernet 1/0/1 inbound
```

如果设备入方向 ARP 流统没有计数，需要检查下对应终端是否有发送 ARP 报文，在沿途设备下流统下看 ARP 报文是否转发过程中被丢弃还是故障设备端口丢弃了报文，检查故障设备的相应端口物理状态和链路状态是否正常、STP 状态是否为 forward 状态等。

2、 检查设备配置是否正确

ARP 报文流统看到已经进入设备后，下一步需要检查设备上的配置，例如接口放通的 vlan 和 ARP 报文的 vlan tag 是否一致，或者有在接口或者全局下配置学习动态 ARP 表项的最大数目 **arp max-learning-number** *max-number*，如果设备或者端口下学习到的 ARP 表项

超过了配置的最大条目后将不再学习动态 ARP 表项。

同时，部分非常规组网下设备配置的 ARP 攻击防御也可能导致设备无法学习 ARP，例如配置了源 MAC 地址固定的 ARP 攻击检测功能 **arp source-mac filter**，在 5 秒内如果收到同一源 MAC 地址的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中，当设置的检查模式为过滤模式，会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉。

3、检查 ARP 报文是否上送 CPU

设备正常收到 ARP 报文需要上送 CPU 进行报文解析和表项学习，可以通过 Debugging arp packet 命令打开 ARP 模块的调试开关，将上送的报文打印出来，为避免打印的报文过多可以命令后加 ACL 过滤或者指定某个端口的 ARP 报文打印。通过回显信息看到 ARP 报文的发送端 Mac 地址、IP 地址，请求的目的 Mac 和目的 IP。

```
<S6800>debugging arp packet interface ?
  FortyGigE            FortyGigE interface
  Route-Aggregation    Route-Aggregation interface
  Ten-GigabitEthernet  Ten-GigabitEthernet interface
  Vlan-interface       VLAN interface
  Vsi-interface        Vsi interface

<S6800>debugging arp packet acl ?
  INTEGER<2000-2999>  Basic ACL number
  INTEGER<3000-3999>  Advanced ACL number
  INTEGER<4000-4999>  Layer 2 ACL number

<S6800-2011>terminal debugging
<S6800-2011>terminal monitor

*Apr 26 18:02:53:677 2011 S6800 ARP/7/ARP_RCV: Received an ARP message, operation:
1, sender MAC: c4ca-d9b9-bba4, sender IP: 192.168.89.254, target MAC: 0000-0000-
0000, target IP: 192.168.89.31
```

（1）如果 Debugging arp packet 没有对应 ARP 报文的回显，需要通过 probe 视图下命令 debug rxtx softcar show+对应框号槽位号查看 ARP 是否上送太多超过 softcar 限速值而被丢弃。设备为了防止过量报文上送冲击 CPU，对于上送 CPU 的报文设置了每秒报文限速，如下举例所示 Type 列为报文类型，RcvPps 列为当前每秒收到的报文数，Rcv_All 列为收到的报文

总数，DisPkt_All 列为丢弃报文总数，Pps 列即为每秒报文限速。

```
[S6800]probe
[S6800-probe]debug rxtx softcar show  slot   1

ID  Type               RcvPps Rcv_All    DisPkt_All Pps  Dyn Swi Hash ACLmax
0   ROOT               0      139688     0          1000 S   On  SMAC 0
1   ISIS               0      0          0          1000 D   On  SMAC 8
2   ESIS               0      0          0          300  S   On  SMAC 8
3   CLNP               0      0          0          300  S   On  SMAC 8
4   VRRP               0      167740     0          1000 S   On  SMAC 8
5   UNKNOWN_IPV4MC     0      0          0          300  S   On  SMAC 8
……
29  ARP                0      1275494    3849       1000 S   On  SMAC 8
30  ARP_REPLY          0      2340       0          1000 S   On  SMAC 8
31  DHCP_CLIENT        0      0          0          300  S   On  SMAC 8
32  DHCP_SERVER        0      0          0          300  S   On  SMAC 8
33  DHCP_RELAY_CLIENT  0      0          0          300  S   On  SMAC 8
```

如果当前收到的 ARP 报文超限速，可以检查下组网中是否有环路引起的广播风暴，是否有 Mac 漂移。同时，也有可能是由 ARP 攻击导致的，可以通过 Debugging arp packet 观察 ARP 报文是否有异常。常见的 ARP 攻击有 SIP/SMAC 固定、DIP 变化的 ARP 扫描攻击，排查对应源 Mac 设备、开启 ARP 源抑制功能 **arp source-suppression enable** 或者源 MAC 固定 ARP 攻击检测功能 **arp source-mac { filter | monitor }**，注意源 MAC 固定 ARP 攻击检测功能还会将源/目的 MAC 地址为该 MAC 地址的数据报文也过滤掉。对于 SMAC 变化的 ARP 攻击，则无法定位到具体的用户，一般情况下只能根据报文入端口信息确定攻击源所在端口，沿着攻击源所在端口逐级排查，或者在端口配置 **arp rate-limit** 对 ARP 报文进行速率限制，确保一个端口受到攻击不会影响该其他端口的用户正常使用网络。另外，ARP 攻击源也可能构造 SMAC 与 ARP 报文源 Mac 不一致的地址扫描攻击报文，由于以太网源地址是网卡驱动程序产生的，比较难以构造，通常攻击报文（病毒报文）的以太网源地址都是固定的，而发送端以太网地址是变化的，网络中存在该类型的 ARP 报文攻击可以通过开启 ARP 源 MAC 一致性检查功能 **arp valid-check enable**，防御以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同的 ARP 攻击。

（2）ARP 队列拥塞也可能导致 Debugging arp packet 没有对应 ARP 报文的回显，在诊断中 queue info 下可以查看对应单板的 ARP 当前队列深度，如果当前队列已经占满，一般是由于环路导致的 Mac 和 ARP 漂移，可以 display mac-address mac-move 查看是否有实时的漂移产生。（probe 视图下，view /proc/kque | inc ARP_PKT 加对应框号和槽位号也可以查看）

```
  ==============queue info on slot 2===============
kque_debug: 1
ontrail: ID  name    depth/cursize/max/drops (magic)
……
0: c000000241bc8e00  ARPSNP_PKT    4096/0/0/0 (0x4b515545)
0: c000000241bc8f00  ARP_VSISUP_PKT    4096/0/0/0 (0x4b515545)
0: c000000241bc9000  ARP_EVENT    8192/0/1/0 (0x4b515545)
0: c000000241bc9100  ARP_FREQEVENT    8192/0/0/0 (0x4b515545)
0: c000000241bc9200  ARP_MACNOTIFYEVENT    1/0/0/0 (0x4b515545)
0: c000000083fc9500  ARP_PKT    65536/1/737/0 (0x4b515545)
```

（3）如果 ARP 队列也没有拥塞，需要检查 ARP 报文本身是否异常，可以镜像抓包查看对应的 ARP 报文是否格式异常，或者尝试 Debugging Ethernet packet 加对应过滤条件进行过滤，观察是否 Ethernet 层是否有上送，避免因源 Mac 检查不通过导致报文被丢弃等问题。常见问题例如部分设备会丢弃源 Mac 为组播 Mac 的报文、部分设备收到源 Mac 为设备本身 Mac 的报文需要关闭静态源 Mac 检查 undo mac-address static source-check enable 等。

```
<H3C>debugging ethernet packet ?
  acl        Display information for packets identified by the ACL
  interface  Specify an interface
  <cr>
<H3C>terminal debugging
<H3C>terminal monitor
```

4、检查 CPU 和内存是否异常

如果设备 CPU 或者内存异常也会导致无法学习 ARP，但一般也会对路由协议等其他方面造成影响，设备数据转发有明显异常。这种情况下一般会伴随日志告警，需 display logbuffer 查看，同时可以通过以下命令查看设备 CPU 及内存使用率。

```
[6800]display  cpu
Slot 1 CPU 0 CPU usage:
       1% in last 5 seconds
       1% in last 1 minute
      16% in last 5 minutes
[6800]display memory
Memory statistics are measured in KB:
Slot CPU        Total      Used      Free  Buffers    Caches FreeRatio
   1   0      2024320   1507072    517248     2512    317344     26.2%
```

5、 尝试恢复业务并收集故障信息

故障时如果业务需要紧急恢复，可以通过 **arp static** *ip-address mac-address* 加出接口的方式绑定静态 ARP 表项进行规避，或者将业务迁移。条件允许的情况下可以按照云图步骤进行检查，仍无法定位或解决的情况下可以收集相关设备的诊断信息、日志信息、诊断日志、详细组网及问题现象，然后拨打 400-810-0504 热线寻求帮助。