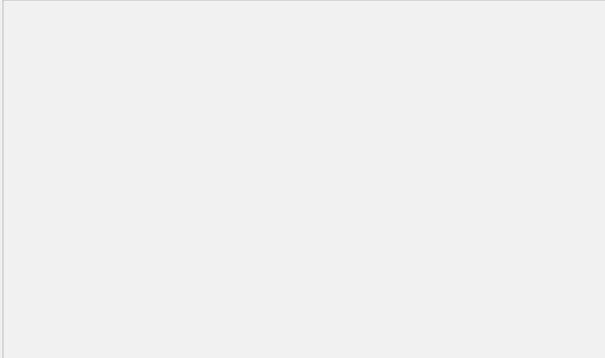


SR66SR66-X系列路由器ARP异常导致直连不通 问题经验案例

一、组网：



二、问题描述：

客户网络中有两台SR6608路由器，下联交换机，某天客户发现，其中有一台SR6608设备间接性不能访问，SR6608-1与SR6608-2 OSPF邻居DOWN，两设备直连不通。设备CPU及内存利用率正常。

三、过程分析：

故障发生后，收集了设备的诊断信息以及logfile文件，查看诊断信息发现SR6608-2路由器下连接口G3/1/0入方向有大量异常等广播报文：

```
GigabitEthernet3/1/0 current state: UP
Line protocol current state: UP
Description: AHYC-EX8208-2
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e2de-b040
IPv6 Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e2de-b040
Media type is twisted pair, loopback not set, promiscuous mode not set
1000M, Full, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Output queue : (Urgent queuing : Size/Length/Discards) 0/100/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards) 0/1024/0
Last clearing of counters: Never
  Last 300 seconds input rate 79676680.00 bytes/sec, 637413440 bits/sec, 1171713
.12 packets/sec
  Last 300 seconds output rate 45.33 bytes/sec, 360 bits/sec, 0.66 packets/sec
Input: 9800983650 packets, 666468478676 bytes, 3293422820 no buffers
  9800868552 broadcasts, 115098 multicasts, 0 pauses
    0 errors, 0 runts, 0 giants
    0 crc, 0 align errors, 0 overruns
    0 dribbles, 0 drops
Output:5644 packets, 383792 bytes
  5644 broadcasts, 0 multicasts, 0 pauses
    0 errors, 0 underruns, 0 collisions
    0 deferred, 0 lost carriers
```

查看设备Slot 3 VCPU信息，发现VCPU 20有大量的报文溢出：

```
=====
=====display dfwd-queue slot 3=====
=====
Distribute Flow VCPU information:
VCPU 1: Total Tokens = 2048   Used Tokens = 0
VCPU 2: Total Tokens = 2048   Used Tokens = 1023
```

Forwarding VCPU information:

VCPU 4: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 5: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 6: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 7: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 8: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 9: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 10: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 11: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 12: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 13: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 14: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 15: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 16: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 17: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 18: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 19: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 20: TotalPkts = 1022	Overflows(no buffers) = 3316792199
VCPU 21: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 22: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 23: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 24: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 25: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 26: TotalPkts = 0	Overflows(no buffers) = 0
VCPU 27: TotalPkts = 0	Overflows(no buffers) = 0

再通过logfile查看当天设备的异常信息，发现自凌晨三点左右，从G3/1/0接口收到大量的ARP异常报文，从而导致VCPU20利用率较高：

```
%@126133%Sep 14 03:27:29:092 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; arp:
warning(25893 pps)
%@126134%Sep 14 03:27:29:092 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; arp:p
eak(25893 pps)
%@126135%Sep 14 03:28:29:089 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; arp:r
ecover(1 pps)
%@126136%Sep 14 03:29:29:087 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; arp:
warning(152689 pps)
%@126137%Sep 14 03:29:29:087 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; arp:p
eak(152689 pps)
%@126138%Sep 14 03:29:29:087 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; Gig
abitEthernet3/1/0 broadcast input rate warning : 346253 pps
%@126139%Sep 14 03:29:29:087 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; Giga
bitEthernet3/1/0 broadcast input rate peak : 346253 pps
%@126140%Sep 14 03:29:33:893 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; VCP
U 20 Warning(66%)
%@126141%Sep 14 03:29:33:893 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; VCP
U 20 Peak(66%)
%@126142%Sep 14 03:29:59:085 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; Giga
bitEthernet3/1/0 broadcast input rate peak : 901066 pps
%@126143%Sep 14 03:30:29:084 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; arp:r
ecover(0 pps)
%@126144%Sep 14 03:30:29:084 2014 AH_SR66_02 DMON/7/MSG: -Slot=3; Giga
bitEthernet3/1/0 broadcast input rate peak : 1345190 pps
```

综上所述，9月14日凌晨开始SR6608-2从G3/1/0接口收到大量的ARP广播报文，导致VCPU 20利用率较高，从而挤掉了正常的ARP报文，设备学习不到对端设备的MAC地址，导致转发不通。Shutdown G3/1/0接口后，通信恢复正常。

三、 解决方法：

建议排查G3/1/0接口下的ARP攻击报文源头，并配置ARP攻击防范。

