免费ARP实现IPv4地址冲突检测原理分析

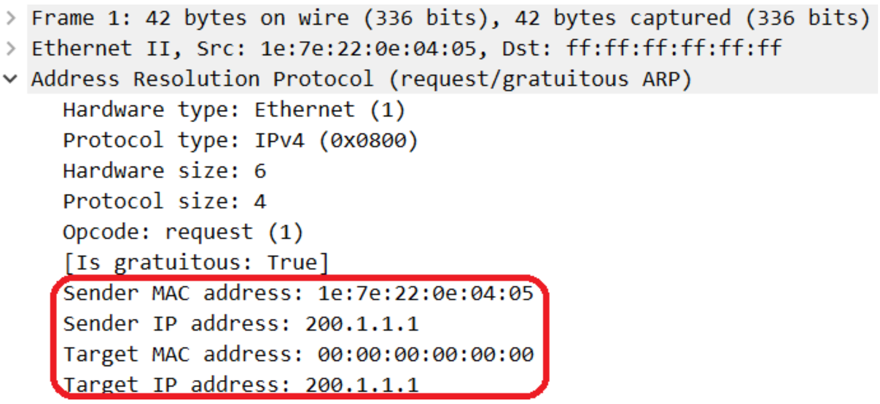
冯哲　2018-04-02 发表

当网络中存在IP地址冲突时，会引发网络路由振荡、网络业务或者流量中断等故障，这些故障会对用户的业务造成很大的影响。为了尽量避免由于错误组网或者用户错误配置造成IP地址冲突的情况发生，用户往往希望设备能够通过一种简单的手段，自主检测网络中是否存在IP地址冲突，及时提示用户冲突的根源，以帮助用户尽快消除冲突配置，切实减少对业务的影响。

本文主要对免费ARP实现IPv4地址冲突检测的原理进行简单介绍，并通过测试抓包对PC终端（Windows 10系统）以及H3C网络设备（Comware V7平台交换机/路由器/防火墙）实现情况做进一步阐述。

免费ARP原理

Gratuitous ARP，被翻译为“免费ARP”，也被称为“无故ARP”。相比“免费”这个翻译，“无故”这个更易理解：“在没有人问自己的情况下，无缘无故自问自答”，即免费ARP是设备发送的一个发送端IP地址和目标IP地址都是本设备IP地址的ARP request/reply报文：



```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 1e:7e:22:0e:04:05, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: 1e:7e:22:0e:04:05
    Sender IP address: 200.1.1.1
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 200.1.1.1
```

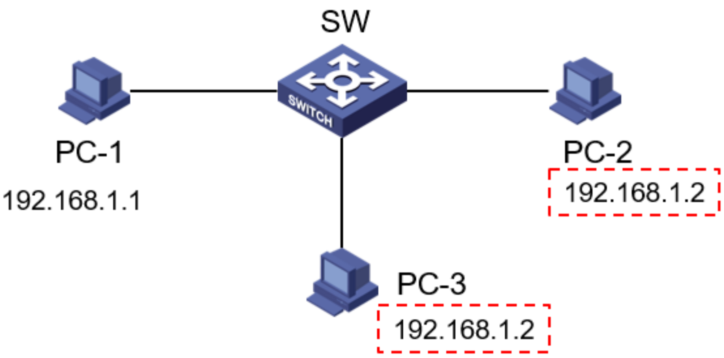
设备通过对外发送免费ARP报文来实现以下功能：

1、设备的硬件地址可能发生了变化（比如修改了MAC地址，或者换了网卡）。ARP request可以让LAN(或者VLAN)中所有设备更新ARP request发送者的IP和MAC的映射关系。

2、确定当前网络中是否有其他设备的IP和自己的IP是一样的。如果这个ARP request发出后，没有收到ARP reply，说明LAN（或者VLAN）中没有设备和自己IP地址一样。如果收到了ARP reply，说明当前LAN（或者VLAN）有设备使用了和本机一样的IP；这个时候系统通常会提醒用户IP地址冲突，并且会周期性的广播发送免费ARP应答报文，直到冲突解除。

故将免费ARP用于检测局域网内的IP地址冲突，能够在一定程度上能够给用户和网络运维人员提供帮助。

但免费ARP检测IP地址冲突也会带来一些网络问题。如下图所示，局域网内有PC-1、PC-2和PC-3三台设备，PC-1的地址为192.168.1.1，PC-2和PC-3的地址均为192.168.1.2。



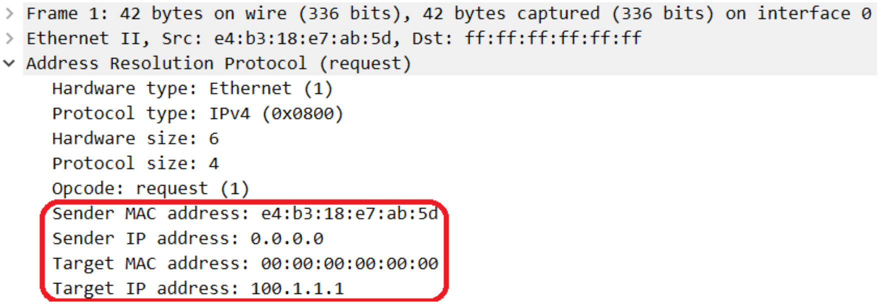
按照免费ARP的实现机制，上面的PC-2和PC-3检测到彼此的IP地址冲突后，会一直不停地对外发送免费ARP；与此同时，同一局域网的其他主机例如PC-1则会根据这两个免费ARP信息不断的修改本地ARP表，192.168.1.2一会映射到MAC-2，一会映射到MAC-3，直到一方修改了地址；免费ARP这种机制会对整个局域网中的设备造成持续的影响，不利于局域网的稳定性。因此RFC也提出了新的地址冲突检测机制。

地址冲突检测ACD（Address Conflict Detection）原理

针对局域网地址冲突问题以及免费ARP解决方案的缺陷，RFC 5227提出了一个新的机制：ACD（Address Conflict Detection）。ACD定义了ARP probe和ARP announcement两种ARP包（都是ARP request，只是填充内容不太一样）

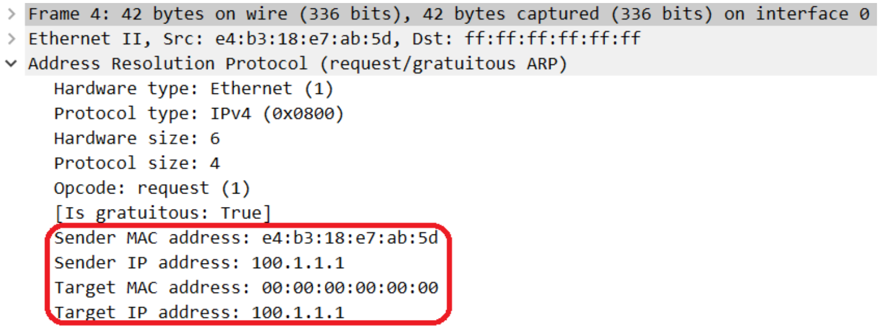
ARP probe：用于检测IP地址冲突，发送端IP填充为0，填充为0是为了避免对其他设备的ARP cache造

成污染（ARP probe报文不会使局域网中的其他设备刷新ARP映射关系，若已经有设备正在使用目标IP地址了，其通信不会受影响），目标IP是候选IP地址（即本设备想要使用的IP地址）。从“自己问自己”的角度看，ARP probe也算是免费ARP。



```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: e4:b3:18:e7:ab:5d, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: e4:b3:18:e7:ab:5d
    Sender IP address: 0.0.0.0
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 100.1.1.1
```

ARP announcement：用于“昭示天下”（LAN/VLAN）本设备要使用某个IP地址了，它其实就是一个免费ARP request，即发送端IP地址和目标IP地址都是本设备IP地址的ARP request报文。它会让LAN(VLAN)中所有主机都更新自己的ARP映射关系，将IP地址映射到发送者的MAC地址。



```
> Frame 4: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: e4:b3:18:e7:ab:5d, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: e4:b3:18:e7:ab:5d
    Sender IP address: 100.1.1.1
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 100.1.1.1
```

ACD检测流程

1、网卡/端口启动时（或者从睡眠状态恢复，或者链接建立时）会发送一个ARP probe。（为了避免多个网卡/端口同时启动同时发ARP probe造成拥塞，有一个拥塞避免策略，不会立刻发送ARP probe，会等待一个随机时间再发送，单个网卡的多个probe也不会连续发送，会有间隔时间）。

2、发送设备可能收到ARP reply或者ARP probe，如果收到了ARP reply，说明候选IP地址已经有设备在用了。如果收到了一个目标IP地址为候选IP的ARP probe，说明另外一个设备也同时想要使用该候选IP地址。这两种情况下，两个设备都会提醒用户出现了IP地址冲突。然后进行地址冲突处理。

3、 如果上述两种ARP包都没有收到，说明候选IP地址可用。设备发送一个ARP announcement，告诉其他设备这个候选IP已被使用了，这个免费ARP request报文会让LAN（VLAN）中其他设备更新ARP表项。

ACD地址冲突处理

当检测到IP地址冲突后，RFC5527提供了三种可选的解决机制：

1、直接放弃使用该IP地址；

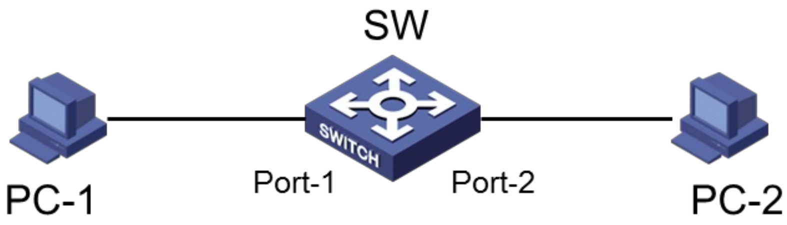
2、发送一个ARP announcement来进行IP地址“守卫”，如果冲突仍然继续存在，放弃使用这个IP；

3、无视冲突，继续使用这个IP。

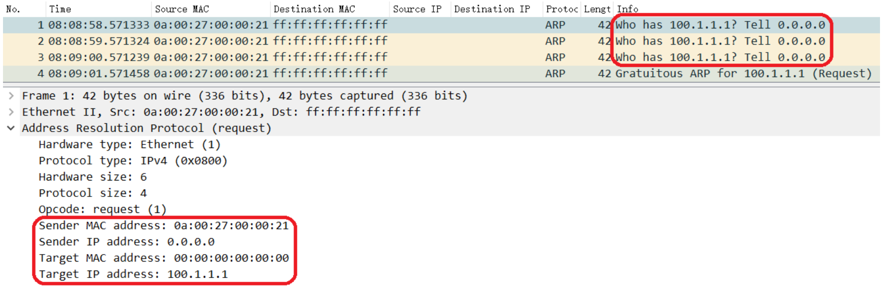
至此，我们简单了解了免费ARP检测地址冲突的原理，下面将通过实验，直观地了解下免费ARP如何实现IP地址冲突检测。

Windows系统主机的地址冲突检测实现情况

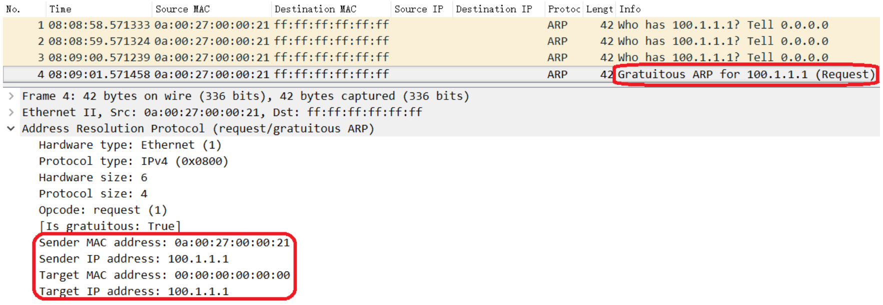
通过实验抓包，结合上文对地址冲突检测原理的说明，我们对Windows系统主机的地址冲突检测机制做进一步阐述，如下图组网，PC-1与PC-2均连接至SW上，且两台PC机属于同一VLAN，初始时两台PC机均未配置IP地址：



1、PC-1安装了Windows 10操作系统，手工给PC-1配置IP地址100.1.1.1/24，然后再SW的Port-1接口上镜像抓包，通过Wireshark可以观察到如下ARP报文：



```
No.    Time            Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
     1 08:08:58.571333 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 100.1.1.1? Tell 0.0.0.0
     2 08:08:59.571324 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 100.1.1.1? Tell 0.0.0.0
     3 08:09:00.571239 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 100.1.1.1? Tell 0.0.0.0
     4 08:09:01.571458 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request)

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 0a:00:27:00:00:21, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 0a:00:27:00:00:21
    Sender IP address: 0.0.0.0
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 100.1.1.1
```

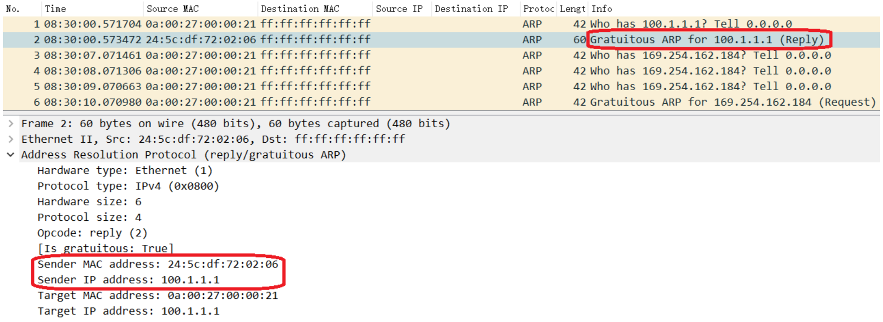


```
No.    Time            Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
     1 08:08:58.571333 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 100.1.1.1? Tell 0.0.0.0
     2 08:08:59.571324 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 100.1.1.1? Tell 0.0.0.0
     3 08:09:00.571239 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 100.1.1.1? Tell 0.0.0.0
     4 08:09:01.571458 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request)

> Frame 4: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 0a:00:27:00:00:21, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: 0a:00:27:00:00:21
    Sender IP address: 100.1.1.1
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 100.1.1.1
```

PC-1配置好地址后，发送了三个探测100.1.1.1地址的ARP probe报文（三个报文间隔1s），因均未收到网络中其他设备对该探测报文的ARP reply，故此时PC机确认100.1.1.1地址可用，向网络中发布了ARP announcement报文宣告对100.1.1.1地址的使用。

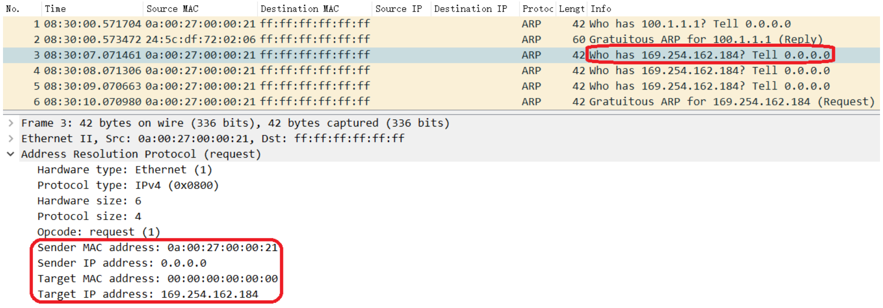
由此可以看出Windows系统ACD的实现与RFC5227中所规定的流程一致，下面继续观察当地址冲突时，Windows系统对地址冲突的处理机制。

2、将上述网络恢复初始状态后，先给PC-2手工配置地址100.1.1.1/24，然后再给PC-1手工配置地址100.1.1.1/24，同时在SW上的Port-1镜像抓包，通过Wireshark观察有如下ARP交互：

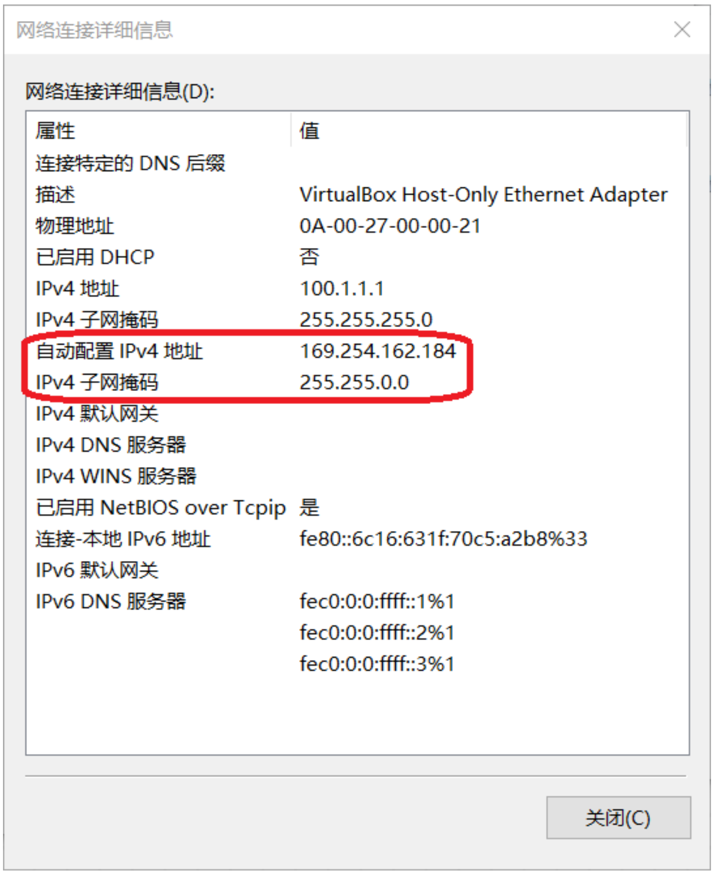


```
No.    Time            Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
     1 08:30:00.571704 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 100.1.1.1? Tell 0.0.0.0
     2 08:30:00.573472 24:5c:df:72:02:06 ff:ff:ff:ff:ff:ff                            ARP      60 Gratuitous ARP for 100.1.1.1 (Reply)
     3 08:30:07.071461 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 169.254.162.184? Tell 0.0.0.0
     4 08:30:08.071306 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 169.254.162.184? Tell 0.0.0.0
     5 08:30:09.070663 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 169.254.162.184? Tell 0.0.0.0
     6 08:30:10.070980 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 169.254.162.184 (Request)

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: 24:5c:df:72:02:06, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: 24:5c:df:72:02:06
    Sender IP address: 100.1.1.1
    Target MAC address: 0a:00:27:00:00:21
    Target IP address: 100.1.1.1
```

PC-1配置好地址后，同样发送了100.1.1.1地址的ARP probe报文，但因此时网络中PC-2已配置了地址100.1.1.1，故PC-2收到这个ARP probe后会给PC-1回应一个ARP reply，通知PC-1自己才是地址100.1.1.1的拥有者。



```
No.    Time            Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
     1 08:30:00.571704 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 100.1.1.1? Tell 0.0.0.0
     2 08:30:00.573472 24:5c:df:72:02:06 ff:ff:ff:ff:ff:ff                            ARP      60 Gratuitous ARP for 100.1.1.1 (Reply)
     3 08:30:07.071461 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 169.254.162.184? Tell 0.0.0.0
     4 08:30:08.071306 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 169.254.162.184? Tell 0.0.0.0
     5 08:30:09.070663 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Who has 169.254.162.184? Tell 0.0.0.0
     6 08:30:10.070980 0a:00:27:00:00:21 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 169.254.162.184 (Request)

> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 0a:00:27:00:00:21, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 0a:00:27:00:00:21
    Sender IP address: 0.0.0.0
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 169.254.162.184
```



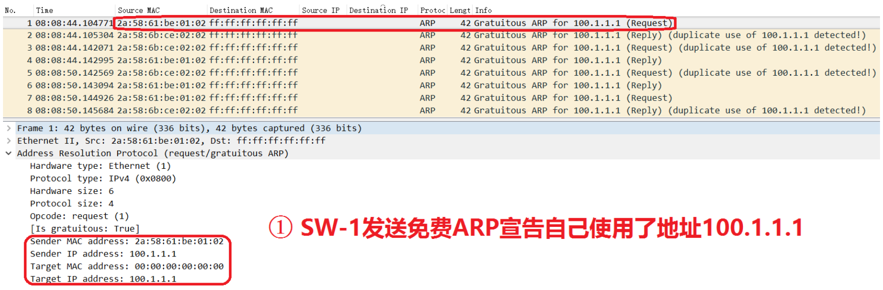
网络连接详细信息(D):

属性	值
连接特定的 DNS 后缀	
描述	VirtualBox Host-Only Ethernet Adapter
物理地址	0A-00-27-00-00-21
已启用 DHCP	否
IPv4 地址	100.1.1.1
IPv4 子网掩码	255.255.255.0
自动配置 IPv4 地址	169.254.162.184
IPv4 子网掩码	255.255.0.0
IPv4 默认网关	
IPv4 DNS 服务器	
IPv4 WINS 服务器	
已启用 NetBIOS over Tcpip	是
连接-本地 IPv6 地址	fe80::6c16:631f:70c5:a2b8%33
IPv6 默认网关	
IPv6 DNS 服务器	fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1

PC-1收到PC-2的ARP reply后，因在PC-1上该地址非DHCP动态获取，PC-1直接放弃使用地址100.1.1.1，用Microsoft的保留网段169.254.X.X/16自动生成了一个地址169.254.162.184，然后对这个地址再次重复前文所述的探测过程：三个ARP probe无回应后发送免费ARP宣告占用地址。
由此可以看出Windows系统ACD检测到地址冲突后，对地址冲突处理机制的实现与RFC5227中所提供的“机制一”一致，即：直接放弃对冲突地址的使用。

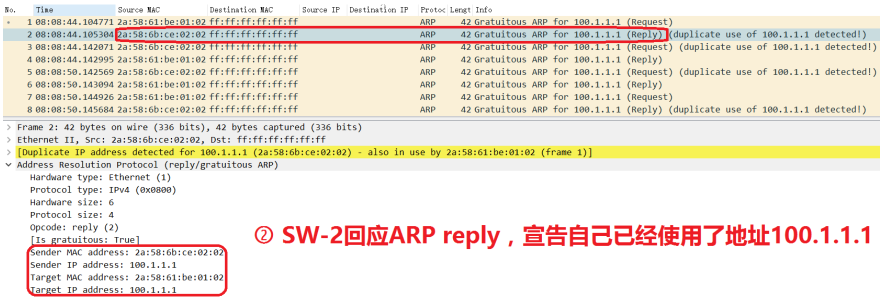
H3C交换机/路由器/防火墙的地址冲突检测实现情况

通过实验抓包，结合上文对地址冲突检测原理的说明，我们对H3C交换机/路由器/防火墙的地址冲突检测机制做进一步阐述，如下图组网，SW-1与SW-2互联，给SW-2的Port-2配置地址100.1.1.1，然后给SW-1的Port-1也配置地址100.1.1.1，在SW-1的Port-1上镜像抓包，通过Wireshark观察有如下ARP交互：



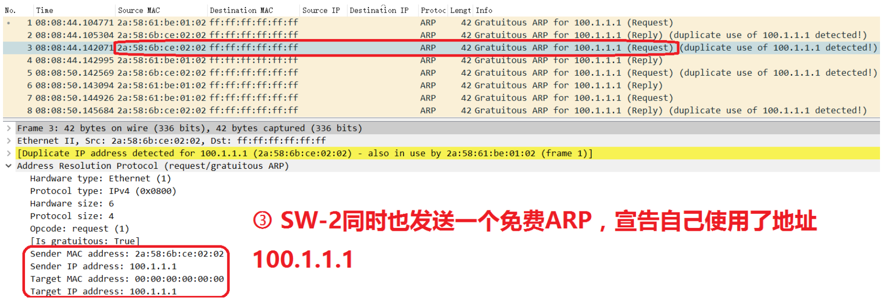
```
No.  Time             Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
   1 08:08:44.104771 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request)
   2 08:08:44.105304 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
   3 08:08:44.142071 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
   4 08:08:44.142995 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Reply)
   5 08:08:50.142569 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
   6 08:08:50.143094 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Reply)
   7 08:08:50.144926 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request)
   8 08:08:50.145684 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 2a:58:61:be:01:02, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: 2a:58:61:be:01:02
    Sender IP address: 100.1.1.1
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 100.1.1.1
```

① SW-1发送免费ARP宣告自己使用了地址100.1.1.1



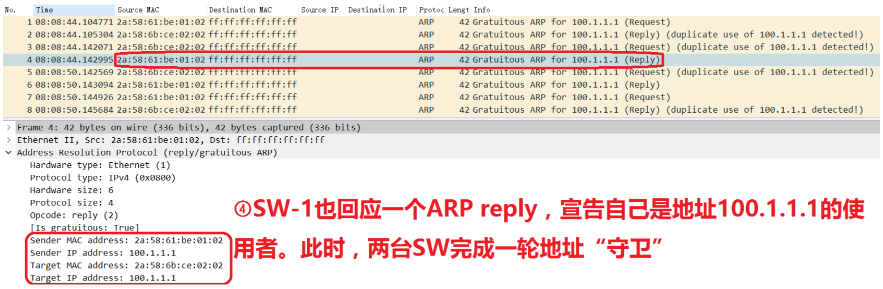
```
No.  Time             Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
   1 08:08:44.104771 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request)
   2 08:08:44.105304 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
   3 08:08:44.142071 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
   4 08:08:44.142995 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Reply)
   5 08:08:50.142569 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
   6 08:08:50.143094 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Reply)
   7 08:08:50.144926 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Request)
   8 08:08:50.145684 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP      42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)

> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 2a:58:6b:ce:02:02, Dst: ff:ff:ff:ff:ff:ff
> [Duplicate IP address detected for 100.1.1.1 (2a:58:6b:ce:02:02) - also in use by 2a:58:61:be:01:02 (frame 1)]
v Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: 2a:58:6b:ce:02:02
    Sender IP address: 100.1.1.1
    Target MAC address: 2a:58:61:be:01:02
    Target IP address: 100.1.1.1
```

② SW-2回应ARP reply，宣告自己已经使用了地址100.1.1.1



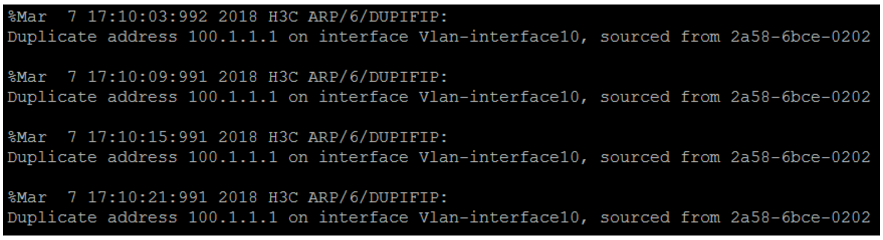
```
No.   Time            Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
    1 08:08:44.104771 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Request)
    2 08:08:44.105304 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
    3 08:08:44.142071 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
    4 08:08:44.142995 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply)
    5 08:08:50.142569 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
    6 08:08:50.143094 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply)
    7 08:08:50.144926 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Request)
    8 08:08:50.145684 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 2a:58:6b:ce:02:02, Dst: ff:ff:ff:ff:ff:ff
> [Duplicate IP address detected for 100.1.1.1 (2a:58:6b:ce:02:02) - also in use by 2a:58:61:be:01:02 (frame 1)]
v Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: 2a:58:6b:ce:02:02
    Sender IP address: 100.1.1.1
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 100.1.1.1
```

③ SW-2同时也发送一个免费ARP，宣告自己使用了地址100.1.1.1



```
No.   Time            Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
    1 08:08:44.104771 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Request)
    2 08:08:44.105304 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
    3 08:08:44.142071 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
    4 08:08:44.142995 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply)
    5 08:08:50.142569 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
    6 08:08:50.143094 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply)
    7 08:08:50.144926 2a:58:61:be:01:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Request)
    8 08:08:50.145684 2a:58:6b:ce:02:02 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
> Frame 4: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 2a:58:61:be:01:02, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: 2a:58:61:be:01:02
    Sender IP address: 100.1.1.1
    Target MAC address: 2a:58:6b:ce:02:02
    Target IP address: 100.1.1.1
```

④SW-1也回应一个ARP reply，宣告自己是地址100.1.1.1的使用者。此时，两台SW完成一轮地址“守卫”



```
%Mar  7 17:10:03:992 2018 H3C ARP/6/DUPIFIP:
Duplicate address 100.1.1.1 on interface Vlan-interface10, sourced from 2a58-6bce-0202

%Mar  7 17:10:09:991 2018 H3C ARP/6/DUPIFIP:
Duplicate address 100.1.1.1 on interface Vlan-interface10, sourced from 2a58-6bce-0202

%Mar  7 17:10:15:991 2018 H3C ARP/6/DUPIFIP:
Duplicate address 100.1.1.1 on interface Vlan-interface10, sourced from 2a58-6bce-0202

%Mar  7 17:10:21:991 2018 H3C ARP/6/DUPIFIP:
Duplicate address 100.1.1.1 on interface Vlan-interface10, sourced from 2a58-6bce-0202
```

SW-1配置地址100.1.1.1后，直接向网络中发送了一个免费ARP request，宣告自己使用了100.1.1.1这个地址，此时SW-2立即回应了一个ARP reply报文，宣告自己已经占用了地址100.1.1.1，与此同时SW-2也向网络中发送了一个免费ARP request，宣告自己使用了100.1.1.1，而SW-1也立即回应了一个ARP reply宣告自己是地址100.1.1.1的使用者，此时SW-1和SW-2完成了一轮对地址100.1.1.1的“守卫”，并分别通过日志向用户告警地址冲突，然后继续下一轮“守卫”，直至用户修改一端的地址消除冲突。通过抓包及告警日志可以看出两轮“守卫”的时间间隔是6秒。

使用H3C的路由器/防火墙重复上述实验，实验结果一致；由此可以看出，H3C的交换机/路由器/防火墙直接使用免费ARP进行地址冲突检测，而不是RFC 5227中新的ACD机制；H3C的设备在检测地址冲突后，不会放弃对冲突地址的使用，并且周期性发送免费ARP进行地址守卫，直至人工消除地址冲突，这种处理机制与RFC 5227中提供的“机制三”是一致的，这种方式在网络设备与终端设备对接时，有利于网络整体稳定性。

H3C设备地址冲突告警机制

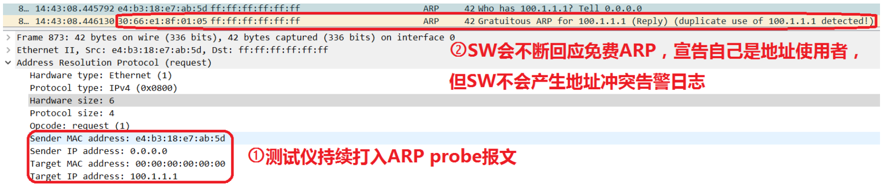
在上文中，我们对PC等终端设备、H3C网络设备地址冲突机制进行了实验及分析，在地址冲突检测过程中共涉及到3种ARP报文：ARP probe、ARP announcement以及ARP reply（发送者IP与标记IP一致），那么H3C设备对这三种ARP报文是如何处理的呢?

通过以下的实验进行分析：

一、设备“不开启源IP地址冲突提示功能”（默认情况）

如下拓扑所示，将SW与测试仪器互联的地址配置为100.1.1.1/24，然后用测试仪器向SW分别持续打入3种报文。

1、 打入ARP probe



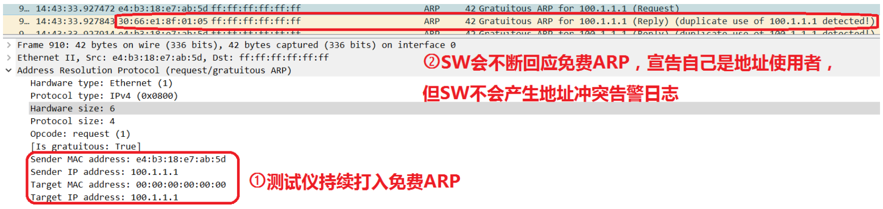
```
8… 14:43:08.445792 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                            ARP       42 Who has 100.1.1.1? Tell 0.0.0.0
8… 14:43:08.446130 30:66:e1:8f:01:05 ff:ff:ff:ff:ff:ff                            ARP       42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
> Frame 873: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: e4:b3:18:e7:ab:5d, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: e4:b3:18:e7:ab:5d
    Sender IP address: 0.0.0.0
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 100.1.1.1
```

②SW会不断回应免费ARP，宣告自己是地址使用者，但SW不会产生地址冲突告警日志

①测试仪持续打入ARP probe报文

可以观察到当SW持续收到地址100.1.1.1的ARP probe报文后，会不断以地址100.1.1.1的免费ARP进行回应，但不会产生地址冲突的告警日志。

2、 打入ARP announcement（免费ARP request）



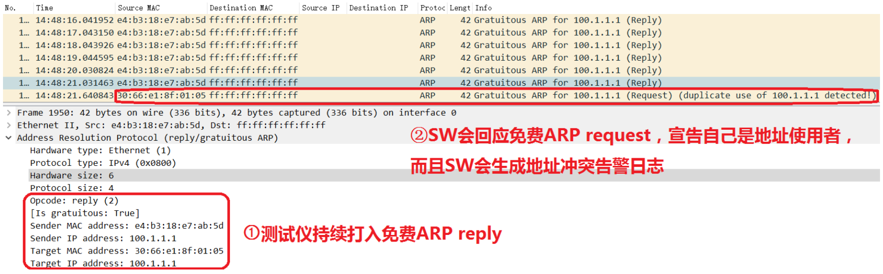
```
9… 14:43:33.927472 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Request)
9… 14:43:33.927843 30:66:e1:8f:01:05 ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
9… 14:43:33.927914 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Reply) (duplicate use of 100.1.1.1 detected!)
> Frame 910: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: e4:b3:18:e7:ab:5d, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: e4:b3:18:e7:ab:5d
    Sender IP address: 100.1.1.1
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 100.1.1.1
```

②SW会不断回应免费ARP，宣告自己是地址使用者，但SW不会产生地址冲突告警日志

①测试仪持续打入免费ARP

可以观察到当SW持续收到地址100.1.1.1的免费ARP request报文后，会不断以地址100.1.1.1的免费ARP进行回应，但不会产生地址冲突的告警日志。

3、打入ARP reply（发送者IP与标记IP均为100.1.1.1）



```
No.  Time              Source MAC        Destination MAC   Source IP  Destination IP  Protoc Lengt Info
1… 14:48:16.041952 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Reply)
1… 14:48:17.043150 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Reply)
1… 14:48:18.043926 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Reply)
1… 14:48:19.044595 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Reply)
1… 14:48:20.030824 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Reply)
1… 14:48:21.031463 e4:b3:18:e7:ab:5d ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Reply)
1… 14:48:21.640843 30:66:e1:8f:01:05 ff:ff:ff:ff:ff:ff                    ARP     42 Gratuitous ARP for 100.1.1.1 (Request) (duplicate use of 100.1.1.1 detected!)
> Frame 1950: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: e4:b3:18:e7:ab:5d, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: e4:b3:18:e7:ab:5d
    Sender IP address: 100.1.1.1
    Target MAC address: 30:66:e1:8f:01:05
    Target IP address: 100.1.1.1
```

②SW会回应免费ARP request，宣告自己是地址使用者，而且SW会生成地址冲突告警日志

①测试仪持续打入免费ARP reply

可以观察到当SW持续收到地址100.1.1.1的免费ARP reply报文后，每隔6s会回应一个免费ARP request报文，检测冲突是否消除，而且会生成地址冲突的告警日志。

二、设备“开启源IP地址冲突提示功能”

重复上述三个打流过程，此时设备收到地址100.1.1.1的三种免费ARP报文后，每隔6s都会回应一个免费ARP request报文，检测冲突是否消除，而且会生成地址的冲突的告警日志。

1、PC/服务器等终端设备通常采用RFC 5227中新的ACD检测流程，当检测到地址冲突后，其处理方式与RFC 5227中提供的“机制一”一致，即直接放弃对冲突地址的使用。在修改终端地址、新终端接入局域网等应用场景下，如果产生地址冲突，该方式最有利于网络的稳定性。

2、H3C网络设备直接采用免费ARP实现地址冲突检测，而非RFC 5227中新的ACD检测流程。当检测到地址冲突时，其处理方式与RFC 5227中提供的“机制三”一致，即继续占用冲突地址。在修改终端地址、新终端接入局域网等应用场景下，如果产生地址冲突，网络设备比终端设备更“强势”，终端设备更容易放弃对冲突地址的使用，这样有利于网络的整体稳定性。但在网络设备间地址冲突的情况下，该机制对整网稳定性会造成持续影响。

3、当H3C网络设备关闭源IP地址冲突提示功能时（默认情况），仅在收到免费ARP reply后，每隔6s会回应一个免费ARP request报文，检测冲突是否消除，而且会生成地址冲突的告警日志；当开启源IP地址冲突提示功能时，只要收到ARP报文的目标IP与本地地址一致，每隔6s会回应一个免费ARP request报文，检测冲突是否消除，而且会生成地址冲突的告警日志。