Catalyst交换机DAI告警

目录

技术领域

LAN

硬件平台

Catalyst交换机

软件版本

所有

问题描述

Catalyst交换机上启用DHCP Snooping以及DAI（Dynamic ARP Inspection）功能，目的是防止出现DHCP假冒以及ARP欺骗攻击。其中，DAI功能的实现需要借助DHCP Snooping建立的IP与MAC地址的绑定表。

启用该功能后，发现交换机的某些端口每天不定时的发出大量ARP检测告警，告警发生时，相关联的PC无法访问网络，需要通过重新插拔网线来恢复。

故障诊断步骤

首先DAI功能是基于DHCP snooping建立的binding表项为依据来进行ARP报文的合法性的， DHCP snooping功能通过在DHCP snooping untrust接口的DHCP消息获得该接口下客户端的MAC、IP address、VLAN和Port四个参数建立唯一的binding表，每个MAC地址只能绑定唯一的IP地址。

例：

```
Cat4507#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ---------------
-----
00:21:97:13:C5:8B   82.0.255.99      619391      dhcp-snooping   425
GigabitEthernet3/17
00:10:DC:72:8B:90   82.0.255.81      1312129     dhcp-snooping   425
GigabitEthernet3/19
```

当交换机在使能DAI的VLAN端口收到ARP报文时，会检查其源IP及MAC地址，如果地址与binding表项一致，则允许通过并转发，如果和DHCP binding表项不统一，则认为是非法ARP报文并丢弃，同时系统打印告警日志。

在问题发生时，发生以下ARP检测告警信息：

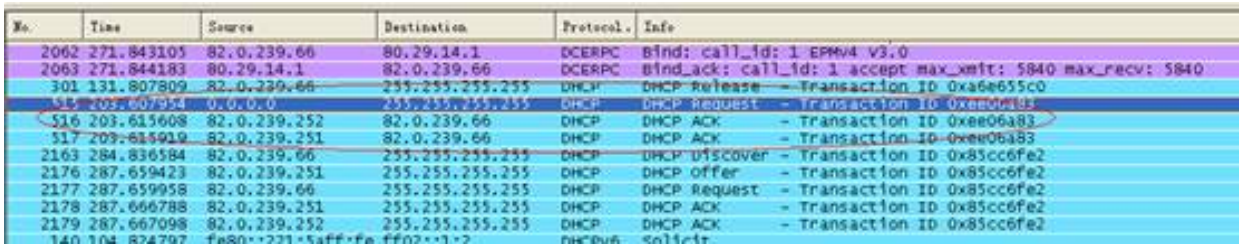
```
Jan 29 08:53:14.049 BJT: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on
Gi3/26,
vlan 425.([000a.e4c1.b8b7/82.0.255.163/0000.0000.0000/82.0.255.254/08:53:13 BJT Fri
Jan 29 2010])
```

这条告警信息的含义是，

交换机收在G3/26端口收到了一个ARP request报文，源IP及MAC地址分别为000a.e4c1.b8b7/82.0.255.163，需要请求IP地址为82.l0.255.254的MAC地址。交换机将该报文的源IP和MAC与本地的DHCP snooping binding表进行匹配检查，发现源MAC和IP与表项中信息不一致，认为是非法ARP请求报文，丢弃了该ARP请求包并打印了日志。

接着，对发生告警的交换机端口进行镜像抓包，发现以下现象：

1. 客户端开机后，通过DHCP协议正常获取了IP地址，此时可以正常访问网络，交换机上也建立了正确的DHCP snooping 绑定表项，没有DAI告警日志。此时，客户PC获得了IP地址为82.0.239.66。

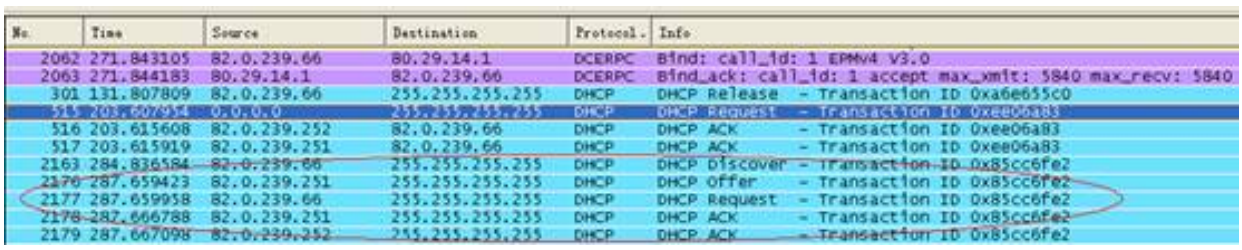


No.	Time	Source	Destination	Protocol	Info
2062	271.843105	82.0.239.66	80.29.14.1	DCERPC	Bind: call_id: 1 EPMv4 v3.0
2063	271.844183	80.29.14.1	82.0.239.66	DCERPC	Bind_ack: call_id: 1 accept max_xmit: 5840 max_recv: 5840
301	131.807809	82.0.239.66	255.255.255.255	DHCP	DHCP Release - Transaction ID 0xa6e655c0
515	203.607954	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xee06a83
516	203.615608	82.0.239.252	82.0.239.66	DHCP	DHCP ACK - Transaction ID 0xee06a83
517	203.615919	82.0.239.251	82.0.239.66	DHCP	DHCP ACK - Transaction ID 0xee06a83
2163	284.836584	82.0.239.66	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x85cc6fe2
2176	287.659423	82.0.239.251	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0x85cc6fe2
2177	287.659958	82.0.239.66	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x85cc6fe2
2178	287.666788	82.0.239.251	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x85cc6fe2
2179	287.667098	82.0.239.252	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x85cc6fe2
140	104.824797	fe80::221:5aff:fe	ff02::1:2	DHCPv6	Solicit

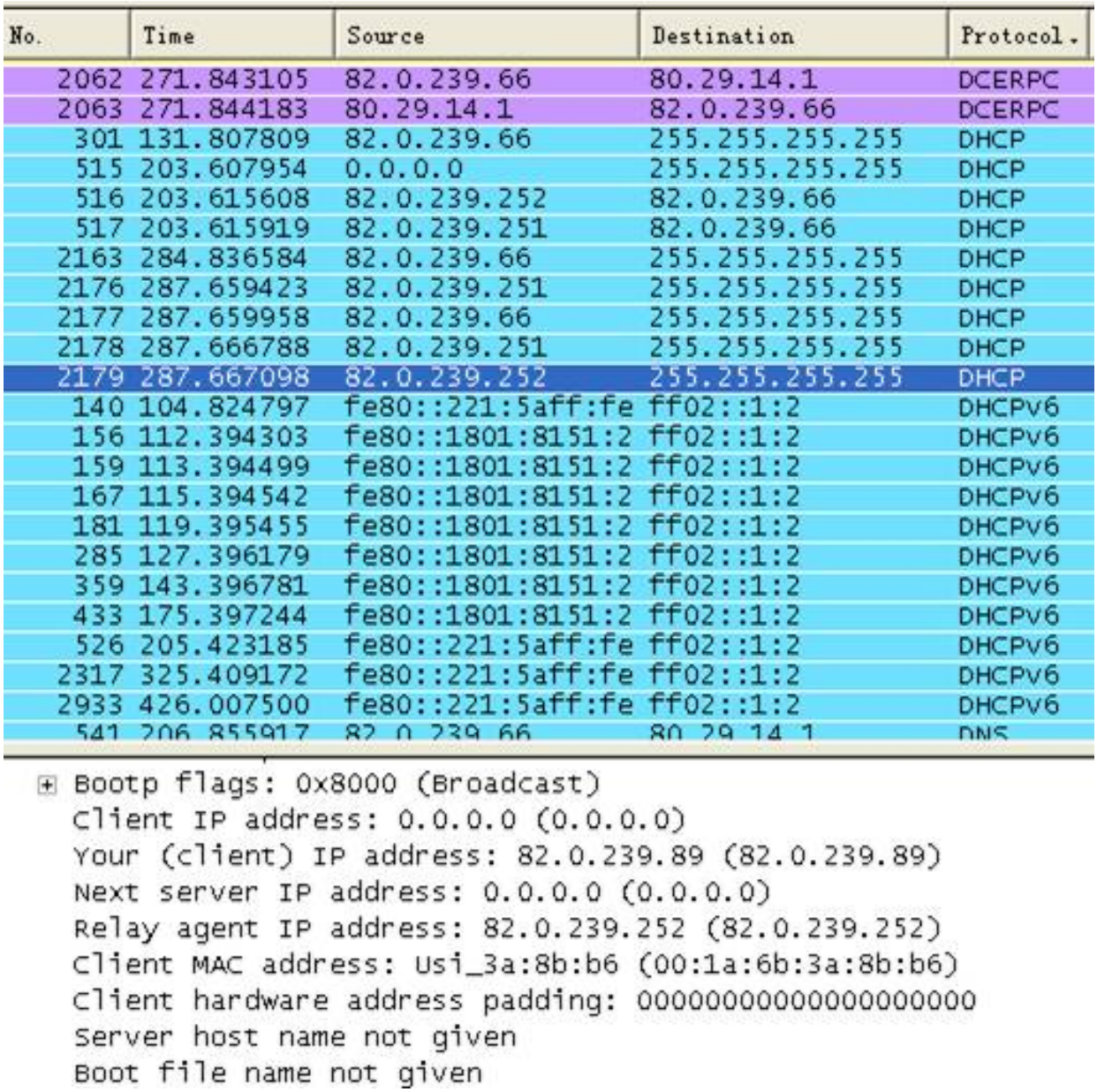
同时在交换机上也可以看到绑定表项的正确建立：

```
Cat4507#show ip dhcp snooping binding interface gigabitEthernet 4/3
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ---------------
-----
00:1A:6B:3A:8B:B6   82.0.239.66      2591916     dhcp-snooping   424
GigabitEthernet4/3
```

2. 在客户PC获得IP地址后不久，又再次发出DHCP Discovery报文来向DHCP服务器申请IP地址。DHCP服务器响应了请求，分配了83.0.239.89给客户端。



No.	Time	Source	Destination	Protocol	Info
2062	271.843105	82.0.239.66	80.29.14.1	DCERPC	Bind: call_id: 1 EPMv4 v3.0
2063	271.844183	80.29.14.1	82.0.239.66	DCERPC	Bind_ack: call_id: 1 accept max_xmit: 5840 max_recv: 5840
301	131.807809	82.0.239.66	255.255.255.255	DHCP	DHCP Release - Transaction ID 0xa6e655c0
515	203.607954	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xee06a83
516	203.615608	82.0.239.252	82.0.239.66	DHCP	DHCP ACK - Transaction ID 0xee06a83
517	203.615919	82.0.239.251	82.0.239.66	DHCP	DHCP ACK - Transaction ID 0xee06a83
2163	284.836584	82.0.239.66	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x85cc6fe2
2176	287.659423	82.0.239.251	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0x85cc6fe2
2177	287.659958	82.0.239.66	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x85cc6fe2
2178	287.666788	82.0.239.251	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x85cc6fe2
2179	287.667098	82.0.239.252	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x85cc6fe2



No.	Time	Source	Destination	Protocol
2062	271.843105	82.0.239.66	80.29.14.1	DCERPC
2063	271.844183	80.29.14.1	82.0.239.66	DCERPC
301	131.807809	82.0.239.66	255.255.255.255	DHCP
515	203.607954	0.0.0.0	255.255.255.255	DHCP
516	203.615608	82.0.239.252	82.0.239.66	DHCP
517	203.615919	82.0.239.251	82.0.239.66	DHCP
2163	284.836584	82.0.239.66	255.255.255.255	DHCP
2176	287.659423	82.0.239.251	255.255.255.255	DHCP
2177	287.659958	82.0.239.66	255.255.255.255	DHCP
2178	287.666788	82.0.239.251	255.255.255.255	DHCP
2179	287.667098	82.0.239.252	255.255.255.255	DHCP
140	104.824797	fe80::221:5aff:fe	ff02::1:2	DHCPv6
156	112.394303	fe80::1801:8151:2	ff02::1:2	DHCPv6
159	113.394499	fe80::1801:8151:2	ff02::1:2	DHCPv6
167	115.394542	fe80::1801:8151:2	ff02::1:2	DHCPv6
181	119.395455	fe80::1801:8151:2	ff02::1:2	DHCPv6
285	127.396179	fe80::1801:8151:2	ff02::1:2	DHCPv6
359	143.396781	fe80::1801:8151:2	ff02::1:2	DHCPv6
433	175.397244	fe80::1801:8151:2	ff02::1:2	DHCPv6
526	205.423185	fe80::221:5aff:fe	ff02::1:2	DHCPv6
2317	325.409172	fe80::221:5aff:fe	ff02::1:2	DHCPv6
2933	426.007500	fe80::221:5aff:fe	ff02::1:2	DHCPv6
541	206.855917	82.0.239.66	80.29.14.1	DNS

```
⊞ Bootp flags: 0x8000 (Broadcast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 82.0.239.89 (82.0.239.89)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 82.0.239.252 (82.0.239.252)
  Client MAC address: Usi_3a:8b:b6 (00:1a:6b:3a:8b:b6)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
```

同一时间，交换机上的绑定表项也更新为新IP地址：

```
Cat4507#show ip dhcp snooping binding interface gigabitEthernet 4/3
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ---------------
-----
00:1A:6B:3A:8B:B6   82.0.239.89      2591999     dhcp-snooping   424
GigabitEthernet4/3
```

3. 新的绑定表项建立后，交换机开始出现大量ARP检测告警日志：

```
Mar 31 15:41:52.927 BJT: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on
Gi4/3, vlan
424.([001a.6b3a.8bb6/82.0.239.66/0000.0000.0000/82.0.239.254/15:41:52 BJT Wed
Mar 31 2010])
Mar 31 15:41:53.927 BJT: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on
Gi4/3, vlan
424.([001a.6b3a.8bb6/82.0.239.66/0000.0000.0000/82.0.239.254/15:41:53 BJT Wed
Mar 31 2010])
```

下一步计划

客户确认是Windows的RAS（Remote Access Service）服务发起了第二次DHCP申请。故建议客户或者取消PC机的RAS服务，抑或停止相应交换机接口下的DAI检测功能。