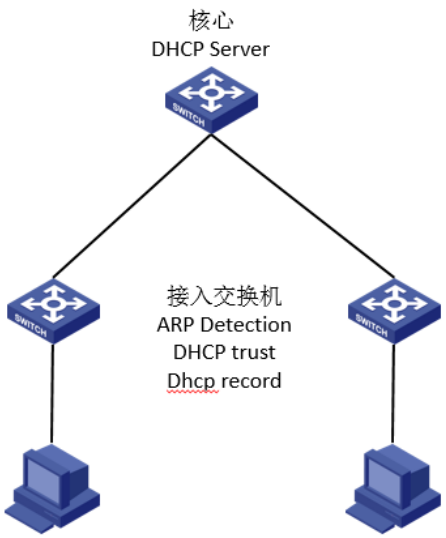
交换机开启arp detection之后不能上网

ARP攻击防御 DHCP/DHCP Relay DHCP Snooping 窦祖尧 2019-06-16 发表

组网及说明

现场核心交换机作为dhcp服务器连接两台接入交换机（1/0/1），接入交换机上开启dhcp中继功能和arp detection功能，使下面的终端只能使用动态分配的地址才能上网。



问题描述

现场工程师发现设备可以动态获取到地址，但是不能上网（学习不到arp）

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
1.1.1.1	4ce9-e48a-d343	3000	GE1/0/1	741	D
1.1.1.2	4ce9-e48a-d4e3	3000	GE1/0/1	741	D

把vlan下面的arpdetection功能删除之后终端可以正常上网（可以学习到arp）

```
[accesssw-1]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
1.1.1.1         4ce9-e48a-d343 3000       GE1/0/1                  889   D
1.1.1.3         4ce9-e48a-d61b 3000       GE1/0/1                  890   D
10.23.3.194     507b-9d1c-017b 251        GE1/0/47                 1194  D
[accesssw-1]ping 10.23.3.194
Ping 10.23.3.194 (10.23.3.194): 56 data bytes, press CTRL_C to break
56 bytes from 10.23.3.194: icmp_seq=0 ttl=64 time=1.509 ms
56 bytes from 10.23.3.194: icmp_seq=1 ttl=64 time=1.205 ms
56 bytes from 10.23.3.194: icmp_seq=2 ttl=64 time=1.201 ms

--- Ping statistics for 10.23.3.194 ---
3 packet(s) transmitted, 3 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.201/1.305/1.509/0.144 ms
%Jan  1 23:16:45:565 2013 accesssw-1 PING/6/PING_STATISTICS: Ping statistics for
 10.23.3.194: 3 packet(s) transmitted, 3 packet(s) received, 0.0% packet loss, r
ound-trip min/avg/max/std-dev = 1.201/1.305/1.509/0.144 ms.
```

过程分析

根据现场情况进行分析，设备故障点应该是在arp detection上面，所以使用命令：

display dhcp snooping binding命令用来显示DHCP Snooping表项信息。

【命令】

display dhcp snooping binding [**ip** *ip-address* [**vlan** *vlan-id*]] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

ip *ip-address*：显示指定IP地址对应的DHCP Snooping表项信息。

vlan *vlan-id*：显示指定VLAN内的DHCP Snooping表项信息。

verbose:显示DHCP Snooping表项的详细信息。如果未指定本参数，则显示DHCP Snooping表项的概

要信息。
【使用指导】
如果未指定**ip** *ip-address*和**vlan** *vlan-id*参数，则显示所有的DHCP Snooping表项信息。

但是发现两个接入设备的dhcp snooping表项都为空，那么问题出现的原因就是因为没有dhcp snooping表项，导致开启arp detection的功能之后接入交换机无法学习到终端的arp表项导致终端无法与网关通信。
后续检查设备配置后发现：

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3000
 arp detection trust
 dhcp snooping trust
 dhcp snooping binding record
#
vlan 250
 name vlan250-2
 arp detection enable
#
vlan 251
 name vlan251-2
 arp detection enable
#
```

dhcp snooping binding record

【视图】
二层以太网接口视图/二层聚合接口视图
VSI视图
VLAN视图
【缺省用户角色】
network-admin
【使用指导】
用户可在DHCP Snooping设备直接与客户端连接的端口上开启DHCP Snooping表项记录功能。

设备开启dhcp snooping binding record的端口1/0/1为连接核心交换机的上行口，但是实际上这个命令是要配置在连接客户端的端口，这样才能生成dhcp snooping表项，生成dhcp snooping表项之后终端才能正常上网。

解决方法

在连接客户端的接口开启dhcp snooping binding record