

知

S7510E 设备DHCP snooping+ip verify功能实现异常

DHCP/DHCP Relay

DHCP Snooping

IP Source Guar

包过滤

姚智祥 2021-12-14 发表

组网及说明

无

问题描述

现场设备当前是DHCP Snooping与dhcp relay均配置在该设备上，需求是使用ip verify source ip-address + dhcp snooping表项记录功能实现对接入用户进行合法性检查，防止用户配置静态IP接入网络。但是反馈当前终端能够正常获取地址，ip source binding 和dhcp snooping binding表项也都已生成，但是现场发现通过在终端配置一个不在ip source binding表项中的地址测试时，发现也是可以正常接入的，现象表现为IP Source Guard没有生效。

过程分析

DHCP snooping是二层特性，dhcp snooping设备收到dhcp request报文，会在vlan里面广播给dhcp server设备，因此源目的端口要求都在同一个vlan内。DHCP relay是三层特性，DHCP relay设备收到dhcp request报文，会单播转发给dhcp server。本身是两种特性功能，根据现场的配置，dhcp server连接的是0/0/1和1/0/1口，去dhcp server走的是三层转发，因此现场不应该配置DHCP snooping功能。

```
interface GigabitEthernet0/0/1
port link-mode bridge
description "connect ZHOA_YQ_S1"
port access vlan 1031
undo stp enable
dhcp snooping trust
#
interface GigabitEthernet1/0/1
port link-mode bridge
description "connect ZHOA_YQ_S2"
port access vlan 1032
undo stp enable
dhcp snooping trust
```

建议现场删除dhcp snooping配置。全局增加“dhcp relay client-information record”命令

现场配置的包过滤acl中，permit了icmp报文和ip报文

```
acl number 3200 name antivirus#oa
rule 5 permit icmp
rule 5000 permit ip
```

配置ip Source Guard功能后，会下发2条acl：PortBind Bind（permit）和PortBind Default（deny）规则：

#本地测试环境：

```
[H3C-probe]debug qacl show slot 6 c 0 verbose 0 acl-type 32
```

=====

```
Acl-Type PortBind Bind, Stage IFP, Pipe 0, NoExpand, Installed, Active
Prio Mjr/Sub 514/31, Group 4 [4], Slice/Idx 11/0, Entry 221, Single: 2816
```

Rule Match -----

```
Ports: 0x0003fffffffffe; 0x3cc7fffffffffff
Outer Vlan: 0x64, 0xfff
Source IP: 100.0.0.2, 255.255.255.255
IP Type: Any IPv4 packet
```

Actions -----

```
Permit
Red Permit
Yel Permit
```

```
[H3C-probe]debug qacl show slot 6 c 0 verbose 0 acl-type 31
```

=====

```
Acl-Type PortBind Default, Stage IFP, Pipe 0, Global, Installed, Active
Prio Mjr/Sub 514/29, Group 4 [4], Slice/Idx 11/1, Entry 220, Single: 2817
```

Rule Match -----

```
Ports: 0x0003fffffffffe; 0x3cc7fffffffffff
Outer Vlan: 0x64, 0xfff
IP Type: Any IPv4 packet
```

Actions -----

```
Deny
```

ip Source Guard下发的acl规则是在IFP中，包过滤的规则也是在IFP中，且包过滤的优先级比ip Source Guard的高；如果进来的流量优先匹配了包过滤的，就无法再匹配ip Source Guard的PortBind Default规则了。

本地测试：

```
#
acl number 3000
rule 0 permit icmp
```

```
rule 5 permit ip
```

```
#
```

解决方法

配置现场删除的情况下，终端配置指定增加dhcp relay可以ping通（无法ping通ip Source Guard的PortBind Default规则）
E3C-Vlan-interface177下去掉包过滤的配置；或者acl 3200下去掉“rule 0 permit icmp”和“rule 5 p
E3C-Vlan-interface100]di this

```
#
```

```
interface Vlan-interface100
```

```
ip address 100.0.0.1 255.255.255.0
```

```
packet-filter 3000 inbound
```

```
dhcp select relay
```

```
dhcp relay server-address 101.0.0.1
```

```
ip verify source ip-address
```

```
#
```

```
return
```

```
<129>ping 100.0.0.3
```

```
Ping 100.0.0.3 (100.0.0.3): 56 data bytes, press CTRL+C to break
```

```
56 bytes from 100.0.0.3: icmp_seq=0 ttl=127 time=2.649 ms
```

```
56 bytes from 100.0.0.3: icmp_seq=1 ttl=127 time=1.391 ms
```

```
56 bytes from 100.0.0.3: icmp_seq=2 ttl=127 time=1.225 ms
```

```
56 bytes from 100.0.0.3: icmp_seq=3 ttl=127 time=1.172 ms
```

```
56 bytes from 100.0.0.3: icmp_seq=4 ttl=127 time=1.215 ms
```

```
--- Ping statistics for 100.0.0.3 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 1.172/1.530/
```

去掉包过滤配置后，可正常命中ip Source Guard的PortBind Default规则，无法ping通

```
[H3C-Vlan-interface100]undo packet-filter 3000 in
```

```
[H3C-Vlan-interface100]di this
```

```
#
```

```
interface Vlan-interface100
```

```
ip address 100.0.0.1 255.255.255.0
```

```
dhcp select relay
```

```
dhcp relay server-address 101.0.0.1
```

```
ip verify source ip-address
```

```
#
```

```
return
```

```
<129>ping 100.0.0.3
```

```
Ping 100.0.0.3 (100.0.0.3): 56 data bytes, press CTRL+C to break
```

```
Request time out
```

```
Request time out
```

```
Request time out
```

```
Request time out
```

```
Request time out
```

```
--- Ping statistics for 100.0.0.3 ---
```

```
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

