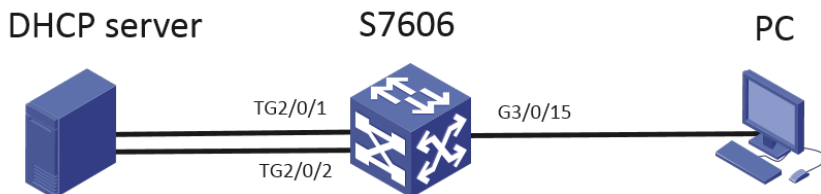


某局点S7606无法透传dhcp offer报文

二层转发 DHCP/DHCP Relay 陆世叶 2020-02-26 发表

组网及说明



S7606做二层转发，下行挂的终端PC去dhcp server获取IP地址

问题描述

现场反馈部分终端无法获取地址，在我司交换机S7606上下行口镜像抓包对比发现是S7606将丢弃。设备收到server回复的offer报文没有从下行口发给终端

过程分析

镜像上行TG2/0/1、TG2/0/2和下行G3/0/15有discover和offer

No.	Time	Source	Destination	Protocol	Length	Info
987	180.231742	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xd5750b73
988	180.232507	10.9.255.254	10.9.15.28	DHCP	389	DHCP Offer - Transaction ID 0xd5750b73
1176	154.235978	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xd5750b73
1177	154.237985	10.9.255.254	10.9.15.28	DHCP	389	DHCP Offer - Transaction ID 0xd5750b73
1269	156.171948	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xd5750b73
1270	156.172543	10.9.255.254	10.9.15.28	DHCP	389	DHCP Offer - Transaction ID 0xd5750b73
1411	160.208121	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xd5750b73
1412	160.208779	10.9.255.254	10.9.15.28	DHCP	389	DHCP Offer - Transaction ID 0xd5750b73
615	161.072773	49.4.38.388	172.16.169.67	TCP	128	80 + 40792 [FIN, ACK] Seq=1 Win=5792 Len=0 TSval=3474316934 TSecr=29751264
479	161.072777	172.16.169.67	49.4.38.388	TCP	136	136 [TCP out of order] Seq=0 Win=5792 Len=0 MSS=1394 SACK_PERM=1 TSval=3474318196 TSecr=29751264
1179	154.205428	49.4.38.388	172.16.169.67	TCP	136	80 + 40790 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1394 SACK_PERM=1 TSval=3474318196 TSecr=29751264
1180	154.205472	49.4.38.388	172.16.169.67	TCP	136	136 [TCP out of order] Seq=0 Ack=1 Win=5792 Len=0 MSS=1394 SACK_PERM=1 TSval=3474318196 TSecr=29751264
1215	155.000011	49.4.38.388	172.16.169.67	TCP	136	80 + 40792 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1394 SACK_PERM=1 TSval=3474318296 TSecr=29751264
1217	155.000054	49.4.38.388	172.16.169.67	TCP	136	136 [TCP out of order] Seq=0 Ack=1 Win=5792 Len=0 MSS=1394 SACK_PERM=1 TSval=3474318296 TSecr=29751264

镜像下行G3/0/15，只有discover

No.	Time	Source	Destination	Protocol	Length	Info
33	6.802741	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xebe494ea
34	6.803201	10.9.255.254	10.9.15.28	ICMP	60	Echo (ping) request id=0x0b12, seq=1/256, ttl=64 (no response found!)
38	7.340826	10.9.255.254	10.9.15.28	ICMP	60	Echo (ping) request id=0x0b12, seq=1/256, ttl=64 (no response found!)
40	7.789653	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xebe494ea
46	10.032072	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xebe494ea
52	13.794457	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xebe494ea
75	21.967961	0.0.0.0	255.255.255.255	DHCP	358	DHCP Discover - Transaction ID 0xebe494ea

可以判断设备将报文丢弃

查看上行口的offer报文，发现其源MAC为0，而能获取到地址的终端收到的offer报文其源MAC为网关MAC

No.	Time	Source	Destination	Protocol	Length	Info
133	2019-10-29 11:37:55.958088	10.9.255.254	10.9.14.52	DHCP	389	DHCP Offer - Transaction ID 0x57179c23
314	2019-10-29 11:37:59.945758	10.9.255.254	10.9.14.52	DHCP	389	DHCP Offer - Transaction ID 0x57179c23
637	2019-10-29 11:38:08.139830	10.9.255.254	10.9.14.52	DHCP	389	DHCP Offer - Transaction ID 0x57179c23
1076	2019-10-29 11:38:16.381031	10.9.255.254	10.9.14.52	DHCP	389	DHCP Offer - Transaction ID 0x57179c23
1459	2019-10-29 11:38:24.744840	10.9.255.254	10.9.14.52	DHCP	389	DHCP Offer - Transaction ID 0x57179c23
1869	2019-10-29 11:38:32.787045	10.9.255.254	10.9.14.52	DHCP	389	DHCP Offer - Transaction ID 0x57179c23

Frame 133: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits) on interface 0

- Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: Apple_c5:a6:f3 (f8:38:80:c5:a6:f3)
- Destination: Apple_c5:a6:f3 (f8:38:80:c5:a6:f3)
- Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 10.9.255.254, Dst: 10.9.14.52
- User Datagram Protocol, Src Port: 67, Dst Port: 68
- Dynamic Host Configuration Protocol (Offer)
 - Message type: Boot Reply (2)
 - Hardware type: Ethernet (0x01)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0x57179c23
 - Seconds elapsed: 0
 - Bootp flags: 0x0000 (Unicast)
 - Client IP address: 0.0.0.0
 - Your (client) IP address: 10.9.14.52
 - Next server IP address: 0.0.0.0
 - Relay agent IP address: 0.0.0.0
 - Client MAC address: Apple_c5:a6:f3 (f8:38:80:c5:a6:f3)
 - Client hardware address padding: 00000000000000000000
 - Server host name not given
 - Boot file name not given

但我司交换机对于源MAC为0的报文是丢弃的，认为其异常报文，不会正常转发

Pri 12, Group 2,usedEntries 39,mode Double, physlice 2/3/
=====

acl type	usedEntries[39]
[92]STM_DENYALL	1
[7]RX IPv4 Super High	2
[8]RX IPv4 High	5
[9]RX IPv4 Middle High	4
[10]RX IPv4 Middle	26
[64]Zero-Mac-Deny	1

=====

[H3C-probe]debug qacl show sl 2 chi 0 verbose 0 acl-type 64

=====
Acl-Type Zero-Mac-Deny, Stage IFP, Pipe 0, OuterPort, Installed, Active
Prio Mjr/Sub 524/2, Group 2 [2], Slice/Idx 6/50, Entry 31, Double: 10290/11314
Rule Match -----
Ports: 0x0000000000000001fffffffffe; 0x200000000001ffffffffffff
Source mac: 0000-0000-0000, FFFF-FFFF-FFFF
Actions -----
Deny
[H3C-probe]

Marvel的交换机目前实现也是一样，都是丢弃

解决方法

友商DHCP server版本问题。

注：有时候华为交换机能正常转发的问题，客户会要规避方法，以前老版本（V5）可以通过MQC实现，其优先级比Zero-Mac-Deny高，可以匹配放行。目前没有好的规避方法，关闭源MAC检测也没用：undo mac-address static source-check enable。