802.1X+MAC认证接入后5s内进入guest vlan

802.1X MAC地址认证 王天吉 2024-08-29 发表

问题描述

交换机上配置了802.1X+MAC认证+guest vlan：

```
#
 dot1x
 dot1x authentication-method eap
 dot1x quiet-period
 dot1x timer quiet-period 10
 dot1x timer tx-period 5
#
 mac-authentication
 mac-authentication timer quiet 1
 mac-authentication user-name-format mac-address with-hyphen uppercase
#
interface GigabitEthernet1/0/2
 dot1x
 undo dot1x handshake
 dot1x mandatory-domain imc_dot1x
 undo dot1x multicast-trigger
 dot1x unicast-trigger
 dot1x timer reauth-period 60
 mac-authentication
 mac-authentication carry user-ip
 mac-authentication domain imc_dot1x
 mac-authentication timer auth-delay 10
 mac-authentication guest-vlan 450
 undo mac-authentication offline-detect enable
#
```

测试认证终端接入认证到进入guest vlan需要花30s以上，想要实现接入后进入guest vlan的时间在5s内。

过程分析

收集**debugging dot1x all、debugging mac-authentication all、debugging radius all**

从debug看整个流程都是正常的：

*Jul 3 02:08:19:982 2024 S5130 DOT1X/7/EVENT: Processing new mac event: UserMAC=****.****.****.****, VLANID=450, Interface=GigabitEthernet1/0/2.

====1x处理newmac;

*Jul 3 02:08:31:993 2024 S5130 MACA/7/EVENT: Processing MAC authentication delay: UserMAC=****.****.****.****, VLANID=450, Interface=GigabitEthernet1/0/2.

====1x 客户端2次没有应答，总共10秒左右超时，转mac-auth；macauth添加延迟表；

*Jul 3 02:08:42:402 2024 S5130 MACA/7/EVENT: Authentication delay timer expired: UserMAC=****.****.****.****, VLANID=450, Interface=GigabitEthernet1/0/2.

====在10秒后，开始触发macauth；

*Jul 3 02:08:42:403 2024 S5130 MACA/7/EVENT: Notified PortSec of new MAC processing result 3: UserMAC=****.****.****.****, VLANID=450, Interface=GigabitEthernet1/0/2.

====但认证直接结束，看配置有mac-authentication carry user-ip， 分析是由于驱动上报newmac的ip为0被拦住了

*Jul 3 02:08:44:628 2024 S5130 DOT1X/7/EVENT: Processing new mac event: UserMAC=****.****.****.****, VLANID=450, Interface=GigabitEthernet1/0/2.

====然后还是上面这个逻辑，1x收到newmac在重新处理，再转macauth, 等macauth延迟认证超时，再触发macauth，但这回真正触发了macauth，即new mac报的ip非0，然后认证失败加gvlan.

发现按照目前的配置是需要等待802.1X超时，进入MAC认证，MAC认证失败后才进入到guest vlan中。

查询配置发现可以配置802.1X的guest vlan，实现触发802.1X认证就进入guest vlan。

更改后实测在接入后的两秒内可以进入guest vlan：

%Jul 4 **06:22:41:807** 2024 S5130 IFNET/5/LINK_UPDOWN: Line protocol state on the interface Gig

abitEthernet1/0/2 changed to up.

*Jul 4 06:22:42:746 2024 S5130 DOT1X/7/EVENT: Processing new mac event: UserMAC=****.****.****.****, VLANID=450, Interface=GigabitEthernet1/0/2.

*Jul 4 **06:22:42:811** 2024 S5130 DOT1X/7/EVENT: Started the user aging timer in the guest VLAN: Length=1000(s), UserMAC=****.****.****.****, VLANID=450, Interface=GigabitEthernet1/0/2.

解决方法

更改配置为：

```
#
interface GigabitEthernet1/0/2
 dot1x
 undo dot1x handshake
 dot1x mandatory-domain imc_dot1x
 undo dot1x multicast-trigger
 dot1x unicast-trigger
 dot1x guest-vlan 450
 dot1x timer reauth-period 60
 mac-authentication
 mac-authentication domain imc_dot1x
 mac-authentication timer auth-delay 10
 mac-authentication guest-vlan 450
 mac-authentication guest-vlan auth-period 5
 undo mac-authentication offline-detect enable
#
```