MAC地址认证失败后无法进行802.1x认证

802.1X MAC地址认证 端口安全 贾珊珊 2022-11-24 发表

组网及说明

设备： H3C S5130S-52S-EI

版本：Release 6343P08

问题描述

工程师反馈现场存在哑终端和PC，因此需要进行MAC地址认证和802.1X认证。但是配置后发现当终端MAC地址认证失败后无法进行802.1X认证。

过程分析

检查配置如下：

```
#
 interface GigabitEthernet1/0/1
  stp edged-port
  dot1x
  dot1x auth-fail vlan 380
  dot1x critical vlan 888
  mac-authentication
  mac-authentication timer auth-delay 180
  mac-authentication critical vlan 888
 #
```

解决方法

由于现场配置了critical vlan，导致设备认为该vlan的用户是由于认证服务器不可达导致的默认通过认证的用户，因此不会再进行802.1x认证。

可以通过如下命令让该vlan的用户重新进行认证：port-security mac-move permit

1.1.17 port-security mac-move permit

port-security mac-move permit命令用来开启允许MAC迁移功能。

undo port-security mac-move permit命令用来关闭允许MAC迁移功能。

【命令】

port-security mac-move permit

undo port-security mac-move permit

【缺省情况】

允许MAC迁移功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

允许MAC迁移功能是指，允许在线的802.1X用户或MAC地址认证用户迁移到设备的其它端口上或迁移到同一端口下的其它VLAN接入后可以重新认证上线。

迁移到其它端口上接入的功能对系统中的所有802.1X认证用户和MAC地址认证用户生效：

· MAC迁移功能处于关闭状态时，如果用户从某一端口上线成功，则该用户在未从当前端口下线的情况下无法在设备的其它端口上（无论该端口是否与当前端口属于同一VLAN）发起认证，也无法上线。

· MAC迁移功能处于开启状态时，如果用户从某一端口上线成功，则允许该在线用户在设备的其它端口上（无论该端口是否与当前端口属于同一VLAN）发起认证。如果该用户在后接入的端口上认证成功，则当前端口会将该用户立即进行下线处理（不论用户在当前端口上通过哪种方式进行认证），保证该用户仅在一个端口上处于上线状态。

迁移到同一端口下其它VLAN接入的功能只在用户报文携带VLAN Tag的情况下生效：

· MAC迁移功能处于关闭状态时，在用户报文携带VLAN Tag的情况下，如果用户从端口下的某个VLAN上线成功，则当该用户迁移到同一端口下的其它VLAN内发起认证时，用户认证失败。

· MAC迁移功能处于开启状态时，在用户报文携带VLAN Tag的情况下，如果用户从端口下的某个VLAN上线成功，则当该用户迁移到同一端口下的其它VLAN内发起认证时，用户认证成功，并且端口会对迁移前的在线用户立即进行下线处理，保证该用户仅在一个VLAN上处于上线状态。

如果用户进行MAC地址迁移前，服务器在线用户数已达到上限，则用户MAC地址迁移不成功。

对于迁移到同一端口下的其它VLAN内接入的用户，MAC地址认证的多VLAN模式优先级高于MAC迁移功能，即当通过mac-authentication host-mode multi-vlan命令开启端口的多VLAN模式后，用户无法迁移到同一端口下的其它VLAN内接入。