

知 某局点dot1x认证用户认证成功后，过一段时间认证成功的终端会掉线

802.1X MAC地址认证 zhiliao_Eu03A 2018-11-28 发表

组网及说明

现场采用了dot1x结合mac认证的组合方案，用户通过dot1x进行认证，哑终端通过mac地址进行认证，接口下 dot1x跟 mac认证同时开启。

问题描述

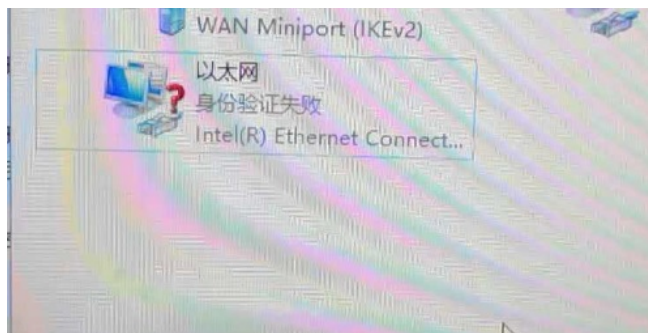
dot1x认证用户认证成功后，过一段时间日志会显示mac地址认证失败且认证成功的终端会掉线。

```
%Jan 11 21:39:07:516 2013 BJFD-F04-10.33.192.10 IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/11 is up.
%Jan 11 21:39:07:843 2013 BJFD-F04-10.33.192.10 DOT1X/6/DOT1X_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/11-MACAddr=d8cb-8a96-af42-VLANId=22-UserName=host/LJ-20180828NLVH.ljstaff.com; The user failed the 802.1X authentication.
%Jan 11 21:39:07:848 2013 BJFD-F04-10.33.192.10 MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/11-MACAddr=d8cb-8a96-af42-VLANId=22-UserName=d8cb8a96af42-UserNameFormat=MAC address; The user failed the MAC address authentication.
%Jan 11 21:40:11:873 2013 BJFD-F04-10.33.192.10 DOT1X/6/DOT1X_LOGIN_SUCC: -IfName=GigabitEthernet1/0/11-MACAddr=d8cb-8a96-af42-VLANId=22-UserName=liyuxuan003; The user passed 802.1X authentication and got online successfully.
%Jan 11 21:40:52:222 2013 BJFD-F04-10.33.192.10 DOT1X/6/DOT1X_LOGOFF: -IfName=GigabitEthernet1/0/11-MACAddr=d8cb-8a96-af42-VLANId=22-UserName=host/LJ-20180828NLVH.ljstaff.com-ErrCode=4; Session of the 802.1X user was terminated.
%Jan 11 21:40:52:226 2013 BJFD-F04-10.33.192.10 MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/11-MACAddr=d8cb-8a96-af42-VLANId=22-UserName=d8cb8a96af42-UserNameFormat=MAC address; The user failed the MAC address authentication.
```

过程分析

从日志信息中，可以发现dot1x认证成功后，过了一段时间会提示errcode=4（重认证失败），dot1x会话终止，此时认证的用户名已经发生了改变，之后用户进行mac地址认证失败，用户下线。从日志看，造成用户下线的主要原因是重认证的时候，用户信息发生了改变后导致的。但是进行重认证的原因没有找到，现场改成端口安全部署后，交换机上显示认证上来了，终端电脑显示验证失败，但是已经可以上网了。还是会出现掉线现象。

```
[BJSZ5G-F05-5F-N04-10.39.0.201-A]dis dot1x connection
Slot ID: 1
User MAC address: 8c16-4586-8636
Access interface: GigabitEthernet1/0/25
Username: huzeya001
Authentication domain: lj
Authentication method: EAP
Initial VLAN: 10
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization ACL ID: N/A
Authorization user profile: N/A
Termination action: N/A
Session timeout period: N/A
Online from: 2018/11/19 16:25:39
Online duration: 0h 1m 35s
Total 1 connections matched.
[BJSZ5G-F05-5F-N04-10.39.0.201-A] dis cu
```



此时开启端口，触发认证过程的日志信息显示如下：

```
%Jan 12 04:19:00:699 2013 BJFD-F04-10.33.192.10 IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/7 link status is up.
%Jan 12 04:19:00:702 2013 BJFD-F04-10.33.192.10 IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/7 is up.
%Jan 12 04:19:05:374 2013 BJFD-F04-10.33.192.10 DOT1X/6/DOT1X_LOGIN_SUCC: -IfName=GigabitEthernet1/0/7-MACAddr=1c1b-0d02-99dc-VLANId=22-UserName=lianjia'shilei03; The user pass
```

ed 802.1X authentication and got online successfully.

%Jan 12 04:36:28:548 2013 BJFD-F04-10.33.192.10 DOT1X/6/DOT1X_LOGOFF: -

IfName=GigabitEthernet1/0/7-MACAddr=1c1b-0d02-99dc-VLANId=22-UserName=lianjia\shilei03-**Err Code=9; Session of the 802.1X user was terminated.**

%Jan 12 04:36:34:574 2013 BJFD-F04-10.33.192.10 MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/7-MACAddr=1c1b-0d02-99dc-VLANId=22-UserName=1c1b0d0299dc-

UserNameFormat=MAC address; The user failed the MAC address authentication.

可以发现此时日志提示ErrCode=9握手失败，dot1x会话终止，那么触发重认证，用户下线的原因是和终端握手不成功导致的。

解决方法

检查了配置发现有如下定时器的配置

```
dot1x timer handshake-period 60
```

```
dot1x timer supp-timeout 10
```

```
dot1x timer tx-period 10
```

让现场将dot1x定时器删除，在接口下关闭握手功能后问题解决