iMC portal 认证提示“向设备发送请求超时”导致认证失败的经验案例

Portal　李树兵　2016-11-27 发表

PORTAL是目前最常见一种认证方式，因为其简单方便，不需要任何客户端的这些优点而广泛使用，iMC EIA组件可以提供完整的PORTAL服务和RADIUS服务。在实际生产和配置过程中由于配置错误经常会出现认证不成功的现场，比如常见的页面提示为“向设备发送请求超时”，下面介绍一下由于配置错误导致出现认证不成功的情况以及解决方法。

页面报错如下图：

一般认证失败需要收集如下信息：组网情况、设备和iMC EIA的软件版本、设备的配置和iMC的配置截图、UAM以及PORTAL的调试级别的日志、设备上的debug portal all和debug radius all的信息、测试过程中认证客户端的IP地址、测试时间以及测试的用户名和密码信息。收集方法可以参考KMS案例库《业务软件日志收集宝典》，链接：http://kms.h3c.com/case/info.aspx?id=40196 。
此案例通过分析收集的PORTAL调试级别日志，看到报错信息显示在PORTAL服务器收到设备回应过来的ACK_INFO 报文之后显示“MD5检查失败”，而提示MD5检查失败的原因一般都是设备上配置的portal服务器的密钥和iMC上添加设备的时候输入的密钥不一致导致，还有一种情况就是iMC侧添加设备的时候portal协议的版本类型和设备的不一致。信息如下：
2016-11-23 17:09:37.568[Portal服务器][调试(0)][21][ProxyRequestHandler::run]172.17.118.8 ; ACK_INFO(10) ; 40 ; 172.17.255.2:2000 ; 报文处理成功(0)

Packet Type:ACK_INFO(10)
SerialNo:40
Address:10.4.0.121
Port:50908
RemoteIp:172.17.255.2
RemotePort:2000
Version:portal 2.0
Auth Type:CHAP
ErrorID:0
UserIP:172.17.118.8
UserPort:0
ReqID:0
Rsvd:0
attriNum:1

Port:slot=1;subslot=0;port=0;vlanid=550;

00000000h: 00 00 00 00 00 00 00 00　00 00 00 00 AC 11 FF 02 ;.....
00000010h: 07 D0 C3 B4 02 0A 00 00　00 28 00 00 AC 11 76 08 ;.....(....v.
00000020h: 00 00 00 01 08 25 73 6C　6F 74 3D 31 3B 73 75 62 ;.....%slot=1;sub

00000030h: 73 6C 6F 74 3D 30 3B 70 6F 72 74 3D 30 3B 76 6C ;slot=0;port=0;vl
00000040h: 61 6E 69 64 3D 35 35 30 3B ;anid=550;
2016-11-23 17:09:37.568[Portal服务器][调试(0)][185][RequestProcessor::run]Begin processRequest() method.
2016-11-23 17:09:37.568[Portal服务器][错误(0)][185][PacketAnalyser::analyzeAttribute]报文最后一个属性的类型为“61”，长度为“48”。
2016-11-23 17:09:37.568[Portal服务器][错误(0)][185][RequestProcessor::ackInfoEvent]userPrivateIp: 172.17.118.8 ; deviceIp: 172.17.255.2 ; expect authenticator is 00000000h: D4 44 47 48 E5 84 DE DF F8 18 14 BD 34 63 49 84 ;.DGH.....4cI.
but revieved authenticator is 00000000h: 08 25 73 6C 6F 74 3D 31 3B 73 75 62 73 6C 6F 74 ; .%slot=1;subslot

2016-11-23 17:09:37.568[Portal服务器][错误(0)][185][RequestProcessor::ackInfoEvent]userPrivateIp: 172.17.118.8 ; deviceIp: 172.17.255.2 ; MD5检查失败
2016-11-23 17:09:37.697[Portal服务器][调试(0)][23][TimerSendTask::stopProcess]用户“172.17.118.3”状态从“LOGIN_PORT_REQUEST_STATUS”变为“DEL_STATUS”
2016-11-23 17:09:37.697[Portal服务器][调试(0)][23][RequestProcessor::sendLoginRespToUser]errorCode = 124
2016-11-23 17:09:37.697[Portal服务器][错误(0)][23][TimerSendTask::stopProcess]device response time out, stop send packet to device success, device ip is 172.17.255.2，onlineUser
2016-11-23 17:09:37.697[Portal服务器][调试(0)][22][ProxyResponseClientHandler::run]172.17.118.3 ; CODE_PP_LOGIN_RESPONSE(101) ; 147 ; 10.4.0.121:52580 ; 向设备发送请求超时(124)

通过对比设备上配置的以及iMC上的配置，发现设备上配置的portal的协议类型为CMCC，但是iMC上增加这个设备的时候协议类型为PORTAL 2.0，协议不一致。将设备上的类型协议修改为portal之后就可以认证成功。

认证页面提示“向设备发送请求超时”的原因有如下几点：
1.iMC上增加portal设备的IP地址和设备上配置的发送portal报文的源IP地址不一致，V5和V7设备上默认以配置portal服务的接口的IP地址来发送，也可以配置portal nas-ip x.x.x.x 来进行指定。
2.iMC上增加设备时配置的密钥和设备上配置的密钥不一致。
3.两边配置的portal协议类型不一致。
4.设备上配置的portal重定向的url地址错误。