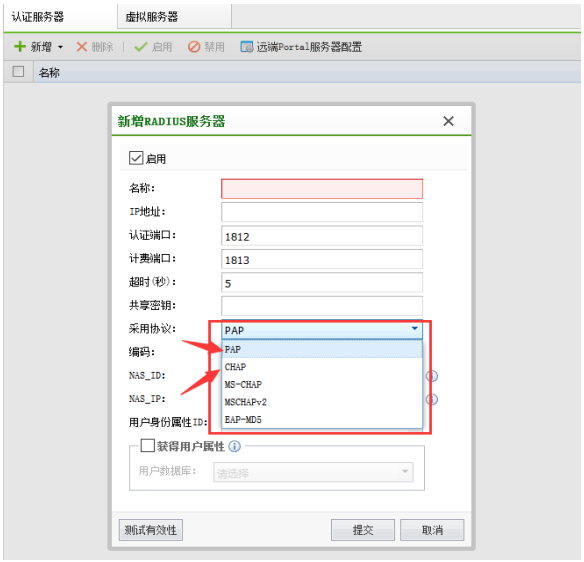
PAP 认证，CHAP 认证

1、背景

在我们配置控制外部服务器时 ,经常看到采用协议或者身份验证等参数添加 ,该参数中最常见的是 PAP，CHAP 认证。在对接一些第三方平台的时候，如果不清楚网络情况或者遗漏可能会导致对接失败。



2、解决的问题

对接 radius 时，可利用该原理进行定位对接过程中失败的原因。

3、PAP 认证，CHAP 认证解析

PAP 认证-------- password authentication protocol 密码认证（明文）

一：原理：被认证端直接发送用户名和密码，并且是明文发送的，如果认证成功则接口 up,从此不需要再认证，即使密码删除，除非把接口 down 了才需要重认证。PAP 支持双向认证，即两段都需要配置 PAP 认证并且发送对端数据库里面有的用户名和密码。

二：PAP 实验测试配置（此处用思科模拟器）:

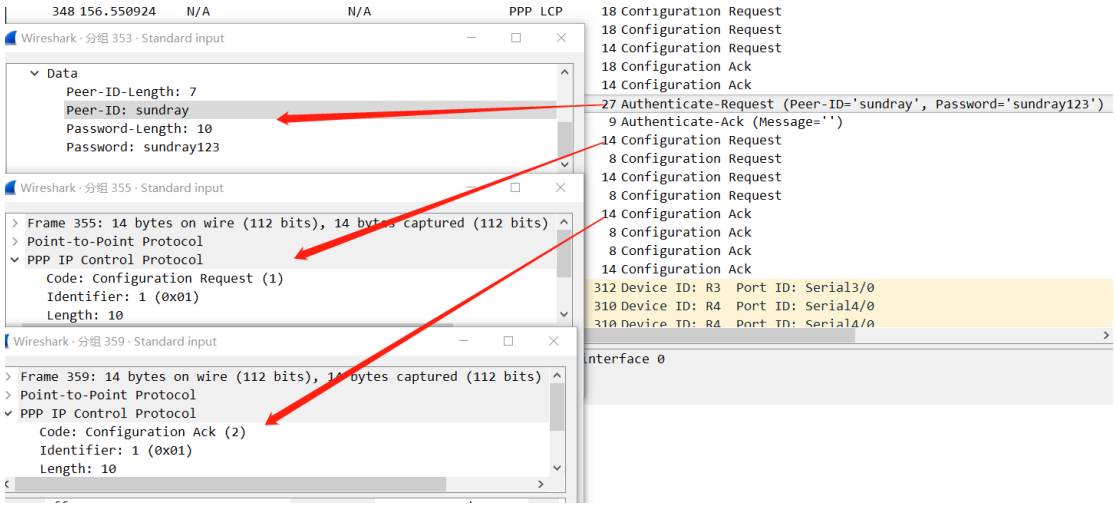
R3（config-if)ppp authentication pap ----服务端开启认证

R3（config）username sundray password sundray123 ---定义本地的数据库条目

R4（config-if)ppp pap sent-username sundray password sundray123 ----客户端主动发送用户名和密码

三：抓包查看字段

被认证端每两秒发送一个认证的请求（code 等于 1），如果服务器端认证成功则回复一个 ACK（code 等于 2），如果认证失败则回复 NAK（code 等于 3）



PPP 帧头	PPP 协议域	代码	标识符	长度	数据
0x 7E FF 03	0xC023	1Byte	1Byte	2Byte	

代码域代表 PAP 包的类型。PAP 代码分配如下：

0x01 Authenticate-Request（认证请求）

0x02 Authenticate-Ack（认证应答）

0x03 Authenticate-Nak（认证无应答）

CHAP -----challenge handshake authentication protocol 挑战握手认证协议（密文）

一：原理

①服务端发起认证，服务器端产生一个随机的 challenge(随机的一个字符串)，然后把这个 challenge 和服务器的用户名一起发出去（用户名默认是设备名，如果接口有配置用户名则使用接口配置的用户名）

②客户端收到 challenge+用户名的数据，先查看本地的数据库有没有匹配该用户名的条目，如果有则使用本地的密码和 challenge 进行哈希得到一个哈希值 HASH1，然后将 HASH1 和用户名一起发出去（用户名默认是设备名，如果接口有配置用户名则使用接口的用户名），如果客户端的本地没有匹配收到的用户名的条目则会使用接口的配置的密码和 challenge 进行哈希得到哈希值。哈希值和用户名一起发出去

③服务器端收到客户端发来的 HASH1+客户端用户名，查看服务器端本地数据库看是否有匹配客户端用户名的条目，如果有则使用该条目对应的密码于 challenge 进行哈希得到哈希值 HASH2,对比如果 HASH1 等于 HASH2，则认证成功。

④如果 HASH1 不等于 HASH2 则认证失败（**在服务器最后验证的时候，接口配置的用户名和密码无效**）

二：CHAP 实验测试配置（此处用思科模拟器）

R3config-if)#ppp authentication chap ---要求对端进行 chap 认证

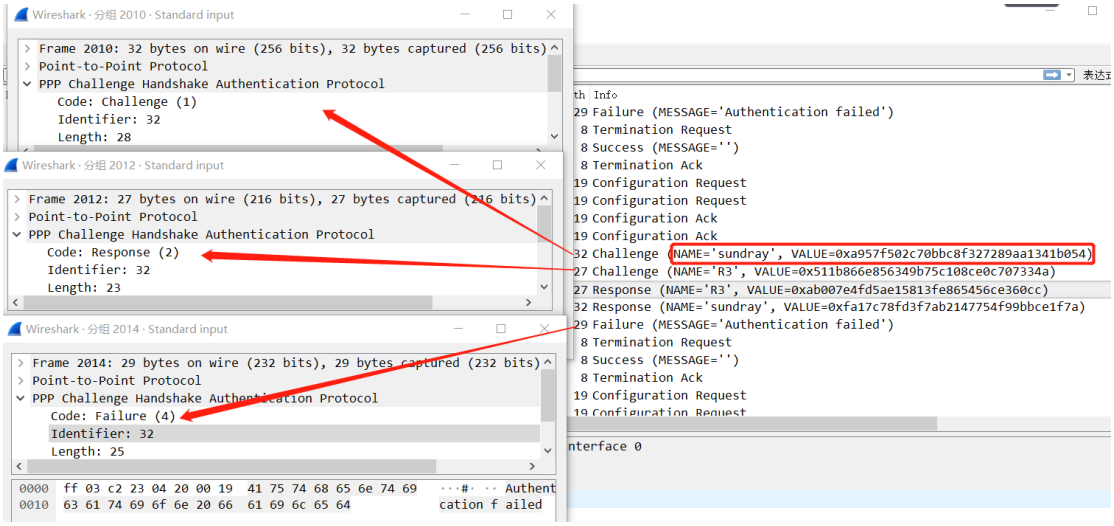
R4config-if)#ppp chap password cisco----接口下配置密码

R4config-if)#ppp chap hostname cisco----接口下配置接口名

三：抓包查看字段

CHAP 有四个报文，第一个 challenge,response,success,failure 对应的 code 分别是 1，2，3，4，如

果没有认证成功则每 2 秒持续的发送 challenge.



PPP 帧头	PPP 协议域	代码	标识符	长度	数据
7E FF 03	0xC223	1Byte	1Byte	2Byte	

代码字段指示CHAP 包的类型，分配如下：

1	挑战	Challenge
2	应答	Response
3	成功	Success
4	失败	Failure