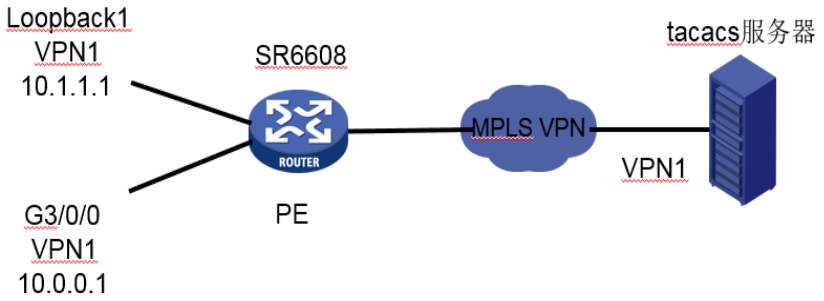
某局点SR6608 telnet结合hwtacacs认证失败问题

MPLS L3VPN Tacacs Telnet 袁野 2019-08-29 发表

组网及说明

如下图所示，SR6608是telnet服务器，通过MPLS VPN网络结合远端vpn的一台tacacs服务器做认证。



问题描述

设备在最近运行中发现结合tacacs认证的用户均无法telnet到设备，在tacacs服务器上做认证的其他设备没有问题，出现问题时设备上查看服务器状态block，服务器到这台设备之间通过SNMP读取mib节点、获取设备日志等功能、连通性测试始终没有问题。设备上直接对telnet用户使用本地认证也正常。

过程分析

通过问题描述中反馈的信息得出该问题排查的方向为设备侧到tacacs服务器侧的报文交互。排查步骤如下：

1、由于之前使用正常，运行中出现问题，需要先了解下设备和服务器侧是否存在配置或者网络变动的情况。在本问题中，和客户沟通了解到并无相关 的变动。

2、收集网络中正常设备和出现问题设备的配置、debug、抓包等信息作对比看看区别在什么地方。在本问题中，经过对比配置并未发现明显的区别，

在debug tacacs信息对比中发现异常时设备在发送tacacs认证请求后收到了errorcode=104的报文，随后关闭了连接。

*Aug 19 09:54:15:605 2019 H3CSR6608 TACACS/7/send_packet: -MDC=1;

version: 0xc0 type: AUTHEN_REQUEST seq_no: 1 flag: ENCRYPTED_FLAG

session-id: 0x43d3e4ad

length of payload: 35

action: LOGIN priv_lvl: 0 authen_type: ASCII service: LOGIN

user_len: 4 port_len: 4 rem_len: 9 data_len: 10

user: ***

port: vty1

rem_addr: ***

data: ******

*Aug 19 09:54:15:614 2019 H3CSR6608 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Reply Socket Fd received EPOLLIN event.

*Aug 19 09:54:15:614 2019 H3CSR6608 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Received packet, length=-1, **errorCode=104.**

*Aug 19 09:54:15:615 2019 H3CSR6608 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Reply Socket Fd received EPOLLIN event.

*Aug 19 09:54:15:615 2019 H3CSR6608 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Received socket close event.

*Aug 19 09:54:15:615 2019 H3CSR6608 TACACS/7/ERROR: -MDC=1; PAM_TACACS: Failed to get available server.

3、根据经验errorcode=104可能为与服务器之间的共享秘钥key不匹配，确认秘钥并重新配置后发现还是一样现象。由于该报文是由服务器侧回复，协调服务器侧进一步确认错误代码含义，但服务器侧答复并未收到设备发来的认证报文。这一说法与设备debug信息矛盾，因此需要在服务器侧抓包确认。
4、通过在服务器侧抓包，按照客户提供的设备侧IP地址并未过滤到交互报文，这一现象与设备侧debug显示相矛盾。确认抓包无误后进一步查看抓包文件发现，设备与服务器侧交互时使用的IP地址并非客户提供的该vpn的loopback地址，而是设备上该vpn下的一个物理接口地址。查看该物理接口地址与服务器的交互报文与设备侧的debug过程吻合。由于服务器侧对认证ip地址做了限制，因此使用该物理接口ip地址向服务器认证是无法成功的。通过在系统视图下配置hwtacacs nas-ip vpn-instance手工指定设备的源ip为loopback口后，问题解决。经过了解，该物理接口ip地址为后来添加，因此客户之前使用正常，后来运行中出现问题。
5、那么在未指定源地址的情况下，为什么配置该接口ip后，设备的源地址会发生变化呢？这是由于在未指定源ip的情况下，设备默认是使用出接口ip地址作为源ip，而对于MPLS vpn场景来说，设备通过查询该vpn的FIB表，目的地址为服务器ip地址得到的出接口是一个MPLS标签值并不是一个具体的物理出接口，在这种情况下，设备会选择该VPN接口下ip地址最小的作为源IP，如拓扑图中所示，在VPN1中G3/0/0接口ip小于loopback1，因此优选G3/0/0接口ip地址为源地址。

至此，问题得到解决，原因也已确认。

解决方法

配置hwtacacs nas-ip X.X.X.X vpn-instance XXX 手工指定源ip及VPN后，问题解决。为避免类似问题发生，在这种场景下务必要手工指定源ip地址。