某局点BRAS设备配置l2tp-user radius-force命令之后用户认证失败的经验案例

认证 Radius L2TP VPN 叶靖 2022-04-30 发表

组网及说明

某客户局点购买了我司的SR8808-F作为BRAS设备配置L2TP服务，L2TP隧道采用NAS-Initiated模式。设备版本为：version 7.1.075, Release 7751P01

问题描述

现场配置完成正常的L2TP配置之后，可以正常进行认证。后续由于考虑到安全需求，想实现提供AAA远程认证方式对PPP用户进行身份验证，所以在LAC的用户所属的ISP域下配置了l2tp-user radius-force命令。正常情况下，配置了l2tp-user radius-force命令之后，仅当通过RADIUS服务器给用户授权了64号属性（Tunnel-Type），且隧道类型为L2TP时，LAC才认为该PPP用户为L2TP用户，进行后续的L2TP处理。但是现场配置了l2tp-user radius-force命令且确认radius服务器上下发了64号属性之后，用户无法认证成功，且一旦将l2tp-user radius-force命令删除之后，便可以正常认证。

过程分析

L2TP隧道采用NAS-Initiated模式时，LAC上的L2TP隧道属性可以通过RADIUS服务器来下发。此时，在LAC上只需开启L2TP服务，并配置采用AAA远程认证方式对PPP用户进行身份验证，无需进行其他L2TP配置。

当L2TP用户拨入LAC时，LAC作为RADIUS客户端将用户的身份信息发送给RADIUS服务器。RADIUS服务器对L2TP用户的身份进行验证。RADIUS服务器将验证结果返回给LAC，并将该用户对应的L2TP隧道属性下发给LAC。LAC根据下发的隧道属性，创建L2TP隧道和会话。

目前，RADIUS服务器可以为LAC下发的属性如下表：

表： RADIUS服务器为LAC下发的主要属性列表

属性编号	属性名称	描述
64	Tunnel-Type	隧道类型，目前只支持L2TP隧道类型
65	Tunnel-Medium-Type	隧道的传输媒介类型，目前只支持IPv4
66	Tunnel-Client-Endpoint	隧道源IP地址
67	Tunnel-Server-Endpoint	LNS的IP地址
69	Tunnel-Password	隧道验证密钥
81	Tunnel-Private-Group-Id	隧道的Group ID LAC将该值发送给LNS，以便LNS根据该值进行相应的处理
82	Tunnel-Assignment-Id	隧道的Assignment ID 用来标识会话承载在哪条隧道上，具有相同Tunnel-Assignment-ID、Tunnel-Server_Endpoint和Tunnel-Password的L2TP用户共用同一条L2TP隧道
83	Tunnel-Preference	隧道的优先级 用来标识LNS IP地址的优先级，数值越小，优先级越高
90	Tunnel-Client-Auth-Id	LAC端的隧道名称 用来标识本端隧道

想确认radius服务器是否正常下发了对应属性，可以通过 debugging radius packet命令进行查看。

现场通过debugging radius packet命令查看debug信息如下：

```
*Dec 12 09:36:11:971 2015 SR8804X-1 RADIUS/7/PACKET: -MDC=1-Slot=2;
 Received a RADIUS packet
 Server IP  : 172.31.1.192
 NAS-IP   : 172.31.1.65
 VPN instance : --(public)
 Server port  : 1812
 Type   : Authentication accept
 Length   : 38
 Packet ID  : 68
*Dec 12 09:36:11:971 2015 SR8804X-1 RADIUS/7/PACKET: -MDC=1-Slot=2;
 Tunnel-Type:0=L2TP
 Framed-Protocol=PPP
Framed-Compression=Van-Jacobson-TCP-IP
```

可以看到现场radius服务器是正常下发了64号属性Tunnel-Type，且Tunnel-Type属性值为L2TP ，但是现场依然无法正常认证成功。

后来经确认发现，当radius服务器下发64号属性tunnel type时，需要配合下发65号属性tunnel medium type = 1、67号属性Tunnel-Server-Endpoint = x.x.x.x（lns地址），即bras上配置了l2tp-user radius-force时，需要aaa同时下发64、65、67三个属性。

正确下发64/65/66号属性时debug信息如下：

```
*Dec 13 00:46:37:572 2015 SR8804X-1 RADIUS/7/PACKET: -MDC=1-Slot=2;
  Received a RADIUS packet
  Server IP    : 172.31.1.192
  NAS-IP     : 172.31.1.65
  VPN instance  : --(public)
  Server port   : 1812
  Type      : Authentication accept
  Length     : 55
  Packet ID    : 169
*Dec 13 00:46:37:572 2015 SR8804X-1 RADIUS/7/PACKET: -MDC=1-Slot=2;
```

Tunnel-Type:0=L2TP

Tunnel-Medium-Type:0=IPv4

Tunnel-Server-Endpoint:0="100.1.1.1"

Framed-Protocol=PPP

Framed-Compression=Van-Jacobson-TCP-IP

解决方法

当bras上配置了l2tp-user radius-force时，需要aaa同时下发64、65、67三个属性。其对应属性含义如下：

属性编号	属性名称	描述
64	Tunnel-Type	隧道类型，目前只支持L2TP隧道类型
65	Tunnel-Medium-Type	隧道的传输媒介类型，目前只支持IPv4
67	Tunnel-Server-Endpoint	LNS的IP地址

此外，现网版本R7951P01对该属性支持上可能有问题，如果需要用该功能，建议使用R7953P12。