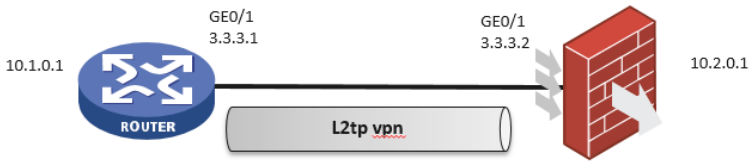
L2TP隧道建立后断掉，virtual-ppp接口频繁up，down，接口一直处于物理up协议down

L2TP VPN 郭尧 2021-01-18 发表

组网及说明



防火墙对接路由器建立L2TP，采用l2tp-auto-client

问题描述

隧道建立起来后会断，virtual-ppp接口频繁up、down，接口物理up协议一直down

如下：

display l2tp session

LocalSID RemoteSID LocalTID State

61147 24651 61422 Established

display l2tp session

LocalSID RemoteSID LocalTID State

61147 24651 61422 Established

%Jan 18 18:48:55:361 2021 H3C IFNET/3/PHY_UPDOWN: Physical state on the interface Virtual-PPP0 changed to down. 接口down

display l2tp session 会话中断

No session exists.

display l2tp session

display l2tp tunnel

LocalTID RemoteTID State Sessions RemoteAddress RemotePort RemoteName

61422 6883 Established 0 3.3.3.2 1701 SZKM1

接口频繁updown

%Jan 18 18:49:05:309 2021 H3C IFNET/3/PHY_UPDOWN: Physical state on the interface Virtual-PPP0 changed to up.

%Jan 18 18:49:08:400 2021 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the interface Virtual-PPP0 changed to up.

%Jan 18 18:49:08:401 2021 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the interface Virtual-PPP0 changed to down.

%Jan 18 18:49:45:223 2021 H3C IFNET/3/PHY_UPDOWN: Physical state on the interface Virtual-PPP0 changed to down.

%Jan 18 18:49:45:308 2021 H3C IFNET/3/PHY_UPDOWN: Physical state on the interface Virtual-PPP0 changed to up.

%Jan 18 18:49:48:401 2021 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the interface Virtual-PPP0 changed to up.

display interface brief 看vpp接口协议一直处于down

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) - spoofing

Interface	Link	Protocol	Primary IP	Description
GE0/0	DOWN	DOWN	--	
GE0/1	UP	UP	3.3.3.1	
GE0/2	DOWN	DOWN	--	
GE5/0	DOWN	DOWN	--	
GE5/1	DOWN	DOWN	--	
GE6/0	DOWN	DOWN	--	
GE6/1	DOWN	DOWN	--	
InLoop0	UP	UP(s)	--	
Loop0	UP	UP(s)	10.1.0.1	
NULL0	UP	UP(s)	--	
REG0	UP	--	--	
Ser1/0	DOWN	DOWN	--	
Ser2/0	DOWN	DOWN	--	
Ser3/0	DOWN	DOWN	--	
Ser4/0	DOWN	DOWN	--	
VPPP0	**UP**	**DOWN**	**--**	

过程分析

核对两端配置未见明显异常

路由器:

```
interface Virtual-PPP0
 ppp chap password cipher $c$3$iRZLP2//1p95mxWjEt6rftZamxSxJA==
 ppp chap user SZKM1
 ip address ppp-negotiate
 l2tp-auto-client l2tp-group 1
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 3.3.3.1 255.255.255.0
#
 ip route-static 10.1.0.0 16 Virtual-PPP0
#
l2tp-group 1 mode lac
 lns-ip 3.3.3.2
 tunnel name SZKM1
 tunnel password cipher $c$3$2xfIDkYmdokWerkxaIzkkWCnzeXfNA==
#
 l2tp enable
#
```

防火墙:

```
 # ip pool l2tp 10.210.248.2 10.210.249.254
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool l2tp
 ip address 10.210.248.1 255.255.254.0

interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 3.3.3.2 255.255.255.0
#
ip route-static 10.2.0.0 16 10.210.248.7
#
local-user SZKM1 class network
 password cipher $c$3$NR/RIx7XxJva6i0OV5NPcPgGt5XAUg==
 service-type ppp
 bind-attribute ip 10.210.248.7
 authorization-attribute user-role network-operator
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1 remote SZKM1
 tunnel name SZKM1
 tunnel password cipher $c$3$X+3ru37M6RecnjGKQM0WNx9Wd8QkXg==
#
 l2tp enable
#
```

收集防火墙debug

```
*Jan 18 19:00:40:944 2021 H3C PPP/7/AUTH_ERROR_0:
  PPP Error:
     BAS0(1ae3c5fa80000086) CHAP: Receive AAA reject message, authentication failed!
```

防火墙接收到拒绝接入AAA导致认证失败

```
*Jan 18 19:00:40:944 2021 H3C PPP/7/AUTH_ERROR_0:
  PPP Error:
```

BAS0(1ae3c5fa80000086) CHAP: Server authentication failed No. 1 !

*Jan 18 19:00:40:944 2021 H3C PPP/7/CHAP_STATE_0:

PPP State Change:

BAS0(1ae3c5fa80000086) CHAP: WaitingAAA --> ServerFailed

*Jan 18 19:00:40:944 2021 H3C PPP/7/CHAP_PACKET_0:

PPP Packet:

BAS0(1ae3c5fa80000086) Output CHAP(c223) Pkt, Len 33

State ServerFailed, code FAILURE(04), id 1, Len 29

Message: Illegal user or password.

*Jan 18 19:00:40:944 2021 H3C PPP/7/CHAP_PACKET_0:

PPP Packet:

BAS0(1ae3c5fa80000086) Output CHAP(c223) Pkt, Len 28

State ServerFailed, code Challenge(01), id 2, Len 24

Value_Size: 16 Value: 05 0d 50 db d6 84 8f 61 54 e1 78 bf b2 ec 9d c1

Name: H3C

*Jan 18 19:00:40:945 2021 H3C PPP/7/CHAP_STATE_0:

PPP State Change:

BAS0(1ae3c5fa80000086) CHAP: ServerFailed --> SendChallenge

*Jan 18 19:04:45:312 2021 H3C PPP/7/CHAP_PACKET_0:

PPP Packet:

BAS0(1ae3c5fa80000086) Input CHAP(c223) Pkt, Len 33

State SendResponse, code FAILURE(04), id 1, Len 29

Message: Illegal user or password.

%Jan 18 19:04:45:313 2021 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the interface Virtual-PPP0 changed to down.

*Jan 18 19:04:45:312 2021 H3C PPP/7/CHAP_EVENT_0:

PPP Event:

VPPP0(85) CHAP Receive Failure Event

State SendResponse

*Jan 18 19:04:45:312 2021 H3C PPP/7/AUTH_ERROR_0:

PPP Error:

VPPP0(85) CHAP: Client authentication failed No. 1 !

*Jan 18 19:04:45:312 2021 H3C PPP/7/CHAP_STATE_0:

PPP State Change:

VPPP0(85) CHAP: SendResponse --> ClientFailed

检查两端chap的password密码配置，确认两端一致后，问题依然存在，用户名SZKM1两端确认最后一个字符是数字1而不是小写l

确认两端配置的用户名和密码都无误

到此，从debug信息可以看出，报错原因是用户或者密码导致的，根本还是配置问题

再次检查配置，发现防火的local-user配置如下：

local-user SZKM1 class network

password cipher c3$NR/RIx7XxJva6i0OV5NPcPgGt5XAUg==

service-type ppp

bind-attribute ip 10.210.248.7

authorization-attribute user-role network-operator

local-user下面配置了绑定属性 **bind-attribute ip 10.210.248.7，目的是为了该用户能够获取到指定的ip地址**

而该命令说明如下：

bind-attribute

bind-attribute命令用来设置用户的绑定属性。

undo bind-attribute命令用来删除指定的用户绑定属性。

【命令】

bind-attribute { call-number call-number [: subcall-number] | ip ip-address | location interface interface-type interface-number | mac mac-address | vlan vlan-id } *

undo bind-attribute { call-number | ip | location | mac | vlan } *

【缺省情况】

未设置用户的绑定属性。

【视图】

本地用户视图

【缺省用户角色】

解决方法

要在local-user下面指定用户授权获取的ip地址，使用authorization-attribute ip命令进行配置，更改配置后问题解决

authorization-attribute (Local user view/user group view)

authorization-attribute命令用来设置本地用户或用户组的授权属性，该属性在本地用户认证通过之后，由设备下发给用户。

undo authorization-attribute命令用来删除指定的授权属性，恢复用户具有的缺省访问权限。

【命令】

authorization-attribute { acl acl-number | callback-number callback-number | idle-cut minutes | ip ipv4-address | ipv6 ipv6-prefix | user-role role-name }*

undo authorization-attribute { acl | callback-number | idle-cut | ip | ipv6 | user-role } *

【缺省情况】

授权FTP/SFTP/SCP用户可以访问的目录为设备的根目录，但无访问权限。

由用户角色为network-admin或level-15的用户创建的本地用户被授权用户角色network-operator。

【视图】

本地用户视图

用户组视图

【缺省用户角色】

network-operator

【参数】

ip ipv4-address：指定本地用户的静态IP地址。本地用户认证成功后，将允许使用该IP地址。

network-admin

【参数】

call-number call-number：指定PPP用户认证的主叫号码。其中call-number为1～64个字符的字符串。