

第6章 安全VPN故障排除

ISSUE 3.0



课程目标


学习完本课程，您应该能够：

- 掌握**GRE**故障排除方法
- 掌握**L2TP**故障排除方法
- 掌握**IPSec VPN**故障排除方法
- 掌握安全**VPN**综合组网故障排除方法





目录

- **GRE故障排除**
 - **L2TP故障排除**
 - **IPSec VPN故障排除**
 - **安全VPN综合组网故障排除**
- 

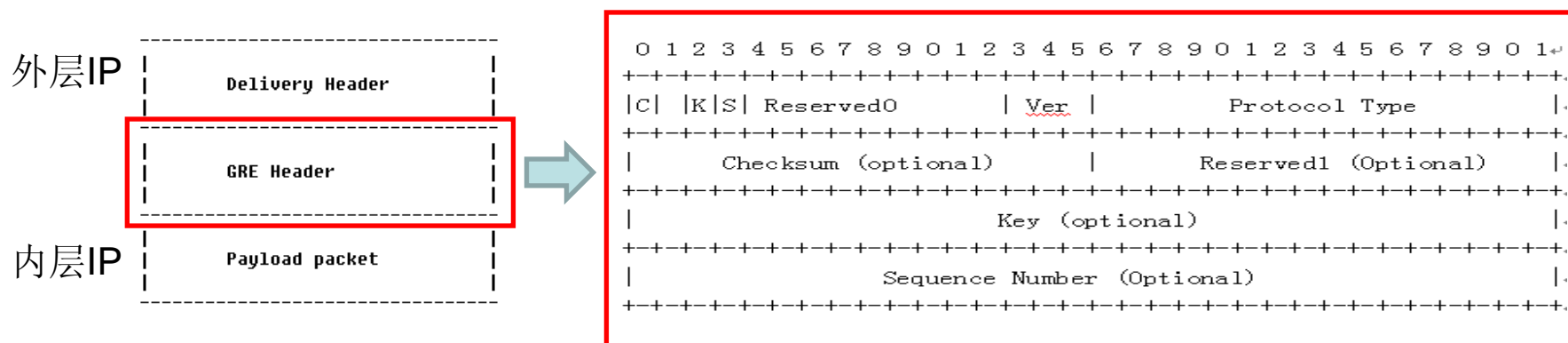
● GRE协议

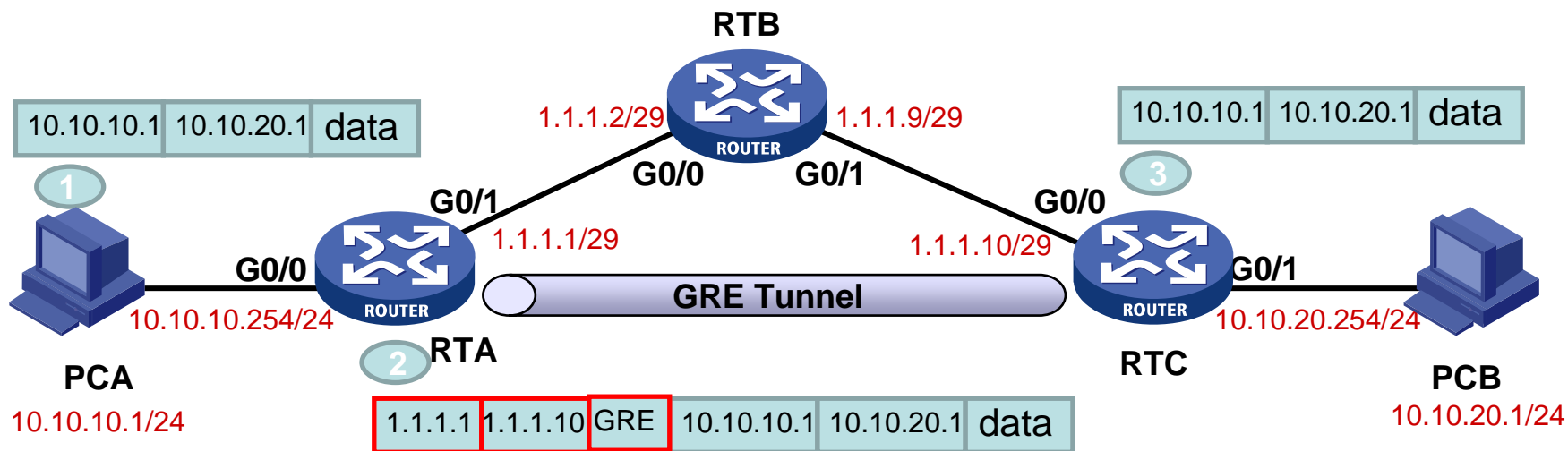
→ 最简单的一种三层隧道技术。

→ 以IP作为传输协议，在IP协议之上承载其他网络层协议，包括IP、IPX等。

→ GRE IP协议号为47。

● GRE封装格式如下所示：





● PCA访问PCB报文转发过程

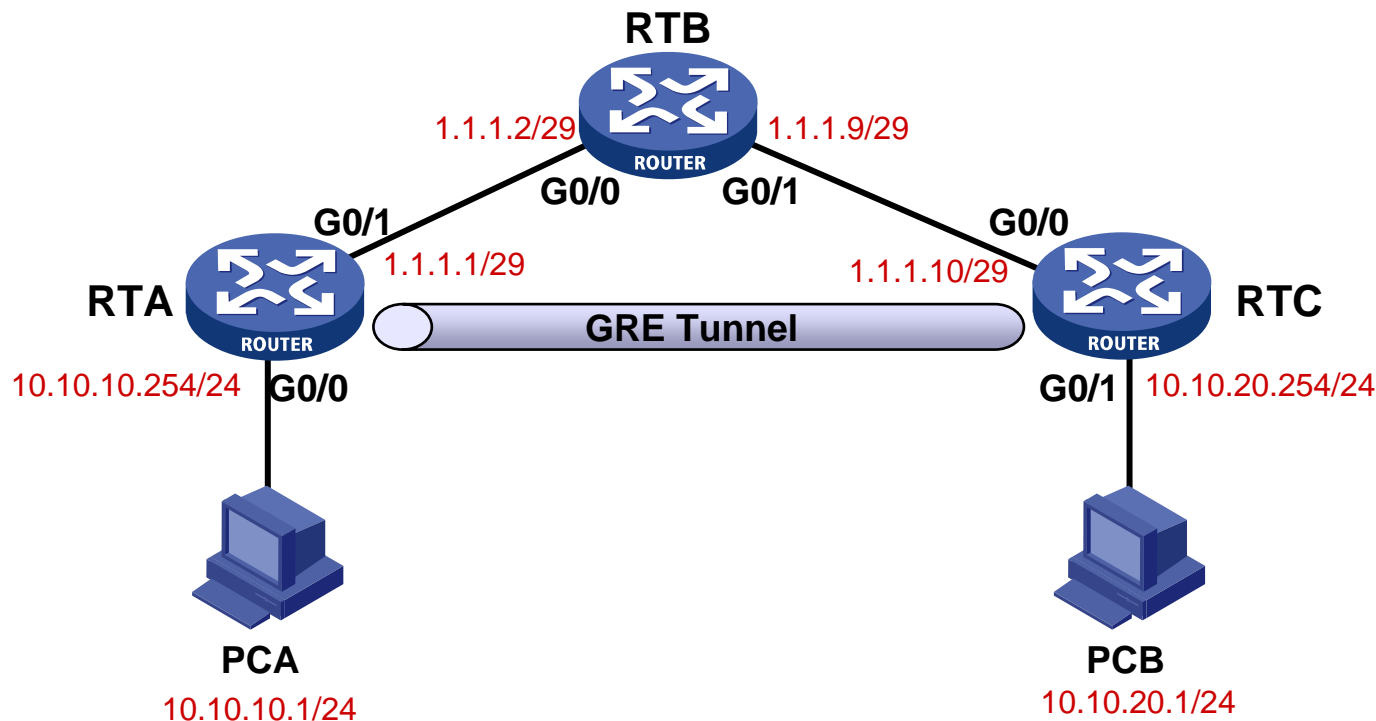
- PCA访问PCB，报文源IP为10.10.10.1，目的IP为10.10.20.1。
- RTA收到报文后，查找本地路由表，出接口为GRE Tunnel，加上GRE外层封装，外层源IP为1.1.1.1，外层目的IP为1.1.1.10，原始IP报文作为载荷。
- RTC收到GRE报文后，去除GRE外层封装，查找本地路由表，将原始IP报文转发给PCB。PCB收到IP报文，PCA单向访问PCB成功。

- **检查GRE Tunnel参数配置是否正确**
 - 查看GRE Tunnel的源、目的IP是否配置正确。
- **检查GRE Tunnel外层IP可达性**
 - 使用ping检测GRE Tunnel外层源、目的IP的可达性。
- **检查GRE Tunnel两端KEY是否一致**
 - 如果启用了GRE KEY，GRE Tunnel两端KEY必须一致。
- **检查GRE Tunnel两端设备路由表**
 - 配置静态路由，或者动态路由，指向GRE Tunnel。
- **检查GRE Tunnel的MTU值**
 - 检查GRE Tunnel的MTU大小，是否支持1500字节的数据包。

● **display interface tunnel** [*number*]

→display interface tunnel命令用来显示Tunnel接口的状态。

```
[RTA]display interface Tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1476
Internet Address is 10.10.12.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID not set.
Tunnel source 1.1.1.1, destination 1.1.1.10
Tunnel keep-alive disable
Tunnel protocol/transport GRE/IP
```



● 故障现象

→ RTA、RTC之间GRE隧道状态正常，但PCA和PCB之间时通时断。

●RTA上的配置:

```
interface LoopBack0
ip address 2.2.2.1 255.255.255.255
#
interface Tunnel0
ip address 10.10.12.1 255.255.255.0
source 2.2.2.1
destination 2.2.2.2
#
ospf 1
area 0.0.0.0
network 10.10.0.0 0.0.255.255
network 2.2.2.1 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

●RTC上的配置:

```
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
interface Tunnel0
ip address 10.10.12.2 255.255.255.0
source 2.2.2.2
destination 2.2.2.1
#
ospf 1
area 0.0.0.0
network 10.10.0.0 0.0.255.255
network 2.2.2.2 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.9
```

● 排障过程

- 查看GRE隧道状态，隧道两端状态正常，没有配置GRE key；
- 查看OSPF邻居状态，OSPF邻居时有时无
- 启用debug ospf event，发现OSPF在full和down之间震荡。
- RTA上发现2.2.2.2/32路由时有时无
- 检查GRE和OSPF配置，发现loopback0为GRE Tunnel的源地址，同时又启用OSPF，导致OSPF邻居震荡。

● 原因分析

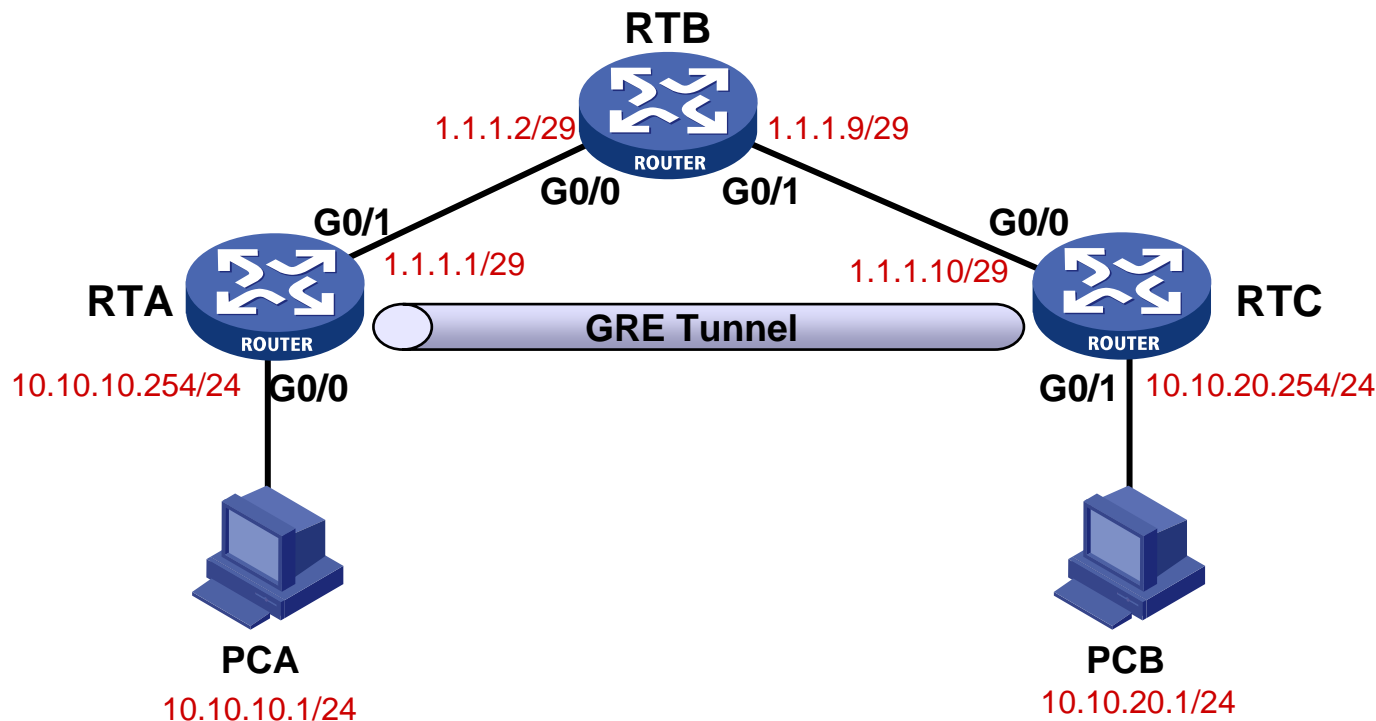
- OSPF邻居建立之前，报文外层IP匹配缺省路由，能够被GRE隧道转发，PC间能够正常连通；
- OSPF邻居建立之后，路由器通过OSPF学到对端loopback的32位路由，根据最长匹配原则，报文外层IP匹配OSPF学到的32位路由，致使GRE封装出错；
- OSPF邻居变为down后，路由又切换至缺省路由，PC间再次连通，如此周而复始，网络一直处于震荡之中。

● 解决方案

- 在OSPF中取消导入loopback路由，就可以消除网络震荡。
- 或者使用物理接口IP作为GRE Tunnel的源IP 地址。

● 建议和总结

- GRE Tunnel承载在IP路由之上，由IP路由提供GRE Tunnel外层IP的连通性，如果在GRE Tunnel上运行动态路由协议，必须确保GRE Tunnel学到的路由不会与物理接口学到的路由相互影响，否则可能出现报文外层IP匹配GRE隧道学到的路由，导致路由黑洞，报文无法正常转发。



- **PCA**可以ping通**PCB**，但是**PCA**通过**WEB**方式访问**PCB**，无法正常显示页面。

●RTA上的配置:

```
interface Tunnel0
ip address 10.10.12.1 255.255.255.0
source 1.1.1.1
destination 1.1.1.10
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
ip route-static 10.10.20.0 255.255.255.0
    Tunnel0
```

●RTC上的配置:

```
interface Tunnel0
ip address 10.10.12.2 255.255.255.0
source 1.1.1.10
destination 1.1.1.1
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.9
ip route-static 10.10.10.0 255.255.255.0
    Tunnel0
```

● 排障过程

- 在RTA、RTC上分别查看GRE隧道状态，隧道两端状态正常；
- 从PCA可以ping通PCB，证明PCA、PCB之间路由正常；
- 因为PCA能够ping通PCB，但无法访问HTTP，所以怀疑GRE MTU问题。在PCA上用ping -f命令来发送DF置位的ICMP报文测试，发现如果ICMP包大于1448字节时，PCA无法 ping 通PCB；ICMP包小于等于1448字节时，PCA 可以ping通PCB。
- 至此原因找到了。是GRE隧道的MTU问题。

- 解决方案

- 修改GRE隧道MTU为1500。从PCA可以ping通PCB，从PCA采用HTTP方式访问PCB，页面能够正常显示。

- 建议和总结

- GRE Tunnel封装开销包括外层IP头和GRE头，共24字节，因此GRE Tunnel的缺省MTU为 $1500 - 24 = 1476$ ，GRE Tunnel转发1500字节的IP载荷时，需要进行分段，如果IP载荷设置了DF位，将导致转发失败，解决的办法为修改GRE Tunnel的MTU为1500，或者修改TCP MSS值为1436。



目录

- GRE故障排除

- **L2TP故障排除**

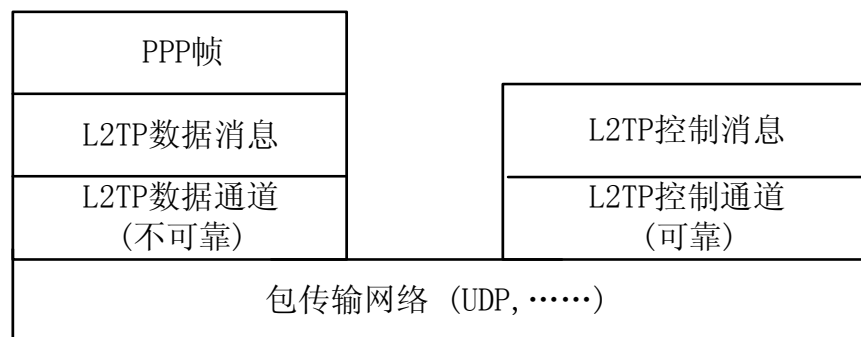
- IPSec VPN故障排除

- 安全VPN综合组网故障排除



● L2TP协议

- 是一种二层隧道技术，用于构建VPDN网络。
- L2TP模型由Client、LAC、LNS构成，Client、LAC之间为PPP链路，如PSTN拨号、PPPoE等，LAC、LNS之间为IP网络，通过IP路由互通。
- L2TP采用UDP封装，对应的UDP端口号为1701，L2TP的协议栈如下所示。



- **display l2tp tunnel**

→ 显示当前的L2TP隧道的信息。

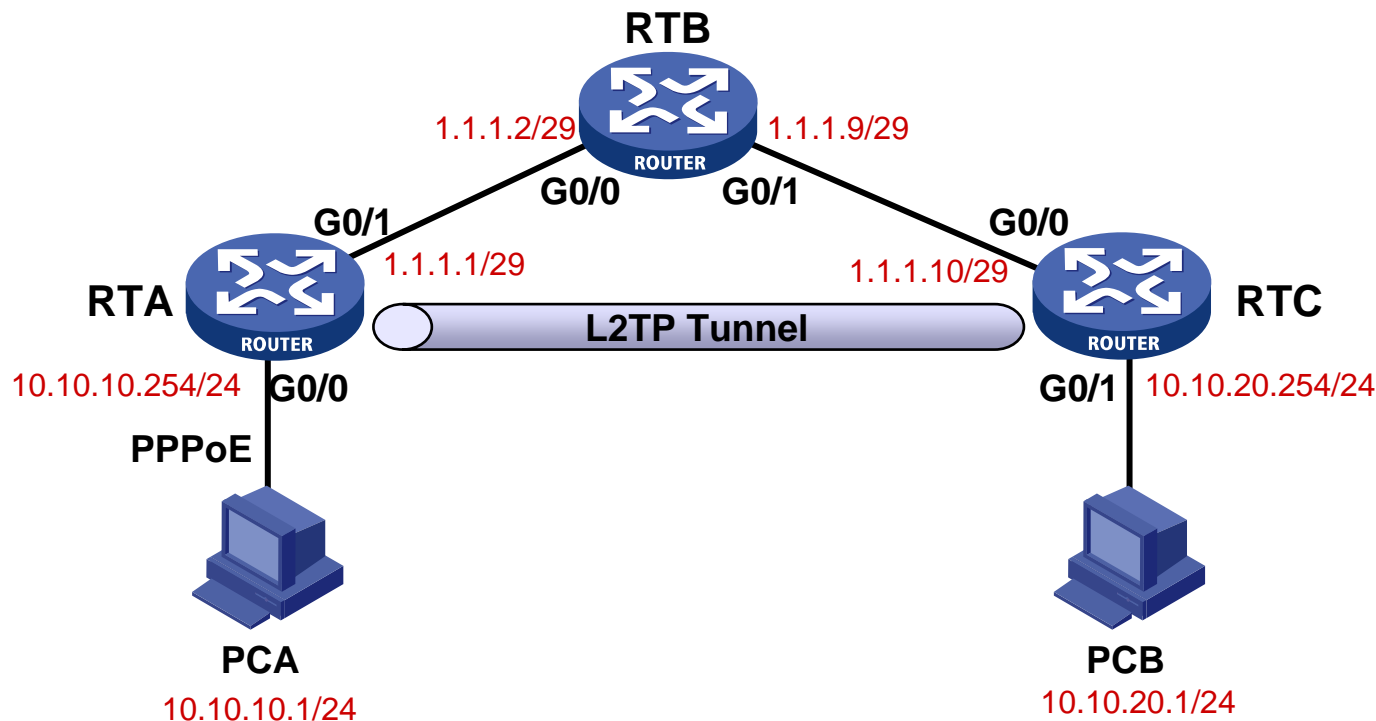
- **display l2tp session**

→ 显示当前的L2TP会话的信息。

- **debugging l2tp**

→ 打开L2TP调试信息开关，undo debugging l2tp命令用来关闭L2TP调试信息开关。

- **检查LAC与LNS是否连通**
 - 从LAC端使用ping命令测试与LNS端的连通性。
- **检查L2TP两端tunnel password是否一致**
 - 缺省情况下，L2TP启用隧道验证，LAC、LNS必须配置相同tunnel password才能通过验证，建立L2TP隧道。
- **检查LNS地址池配置是否正确**
 - 在配置了用户验证的情况下，必须在domain视图下配置地址池，否则将导致LNS无法给Client分配IP地址。
- **检查隧道对端name是否正确**
 - 在LNS端，除了l2tp-group 1，其他l2tp-group需要明确指定LAC端的name。
- **其他疑难L2TP问题**
 - 开启L2TP的Debugging开关，通过调试信息分析问题原因。



- 故障现象

→ PCA通过PPPoE成功拨入RTA，但是RTA、RTC无法建立L2TP Tunnel。

●RTA上的配置：

```
l2tp enable
#
local-user vpdnuser
password simple 123
service-type ppp
#
l2tp-group 1
tunnel name LAC
start l2tp ip 1.1.1.10 fullusername
vpdnuser
#
interface Virtual-Template1
ppp authentication-mode chap
ppp chap user vpdnuser
#
interface GigabitEthernet0/0
port link-mode route
pppoe-server bind Virtual-Template 1
```

●RTC上的配置：

```
l2tp enable
#
local-user vpdnuser
password simple 123
service-type ppp
#
domain system
ip pool 1 10.10.12.11 10.10.12.20
#
l2tp-group 1
allow l2tp virtual-template 1
tunnel name LNS
#
interface Virtual-Template1
ppp authentication-mode chap
remote address pool 1
ip address 10.10.12.254 255.255.255.0
```

● 排障过程

- 在RTA上ping RTC，没有丢包，说明LAC、LNS之间IP可达
- 在RTA上查看L2TP Tunnel状态，没有建立任何L2TP Tunnel。
- 在RTC上开启debugging l2tp命令并观察输出信息。发现RTC可以收到RTA发送的challenge，并清除l2tp tunnel状态。

```
*Dec 5 10:44:10:200 2008 RTC L2TP/7/L2TDBG: L2TP_CONTROL: Put AVP  
Challenge :26 48 17 03 B3 BC 07 08 FE 0F 1F E6 7F 8F D1 35
```

```
*Dec 5 10:44:10:351 2008 RTC L2TP/7/L2TDBG: L2TP_EVENT: Got a challenge in  
SCCRQ
```

```
*Dec 5 10:44:10:462 2008 RTC L2TP/7/L2TDBG: L2TP_EVENT: Cleared Tunnel  
remote ID:1, local ID:1.
```

- 检查RTA、RTC两端L2TP配置，发现没有给隧道配置相应的password。

- 解决方案

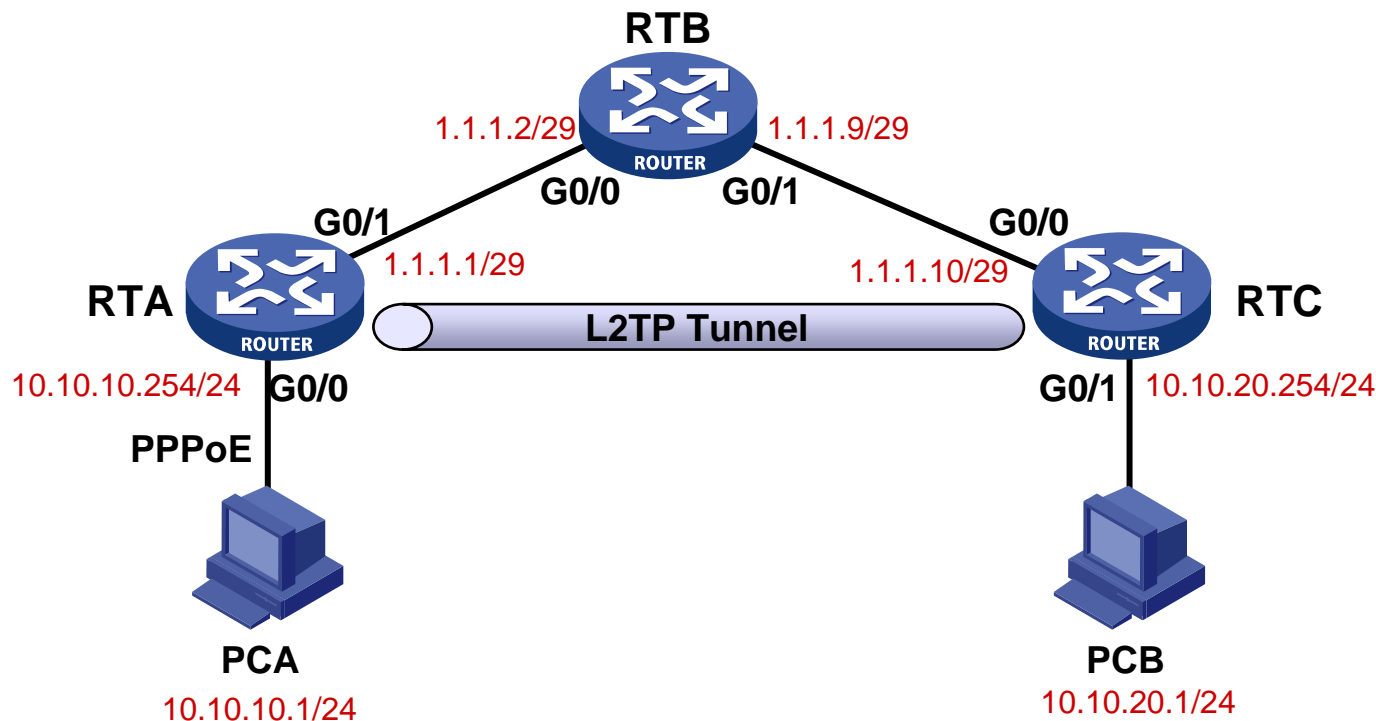
→ 在RTA、RTC配置相同的tunnel password后，问题得以解决。

```
RTA
l2tp-group 1
tunnel password simple
123
```

```
RTB
l2tp-group 1
tunnel password simple
123
```

- 建议与总结

- L2TP Tunnel缺省启用密码验证，如果Tunnel两端不配置密码，或者密码不一致，将导致Tunnel验证失败，无法正确建立L2TP Tunnel。
- 在隧道无法建立的情况下，通过查看debugging l2tp命令的输出信息，可以更快的发现隧道无法建立的原因



● 故障现象

→ PCA通过PPPoE成功拨入RTA，但是PCA不能从RTC上获取IP地址。

●RTA上的配置:

```
l2tp enable
#
local-user vpdnuser
password simple 123
service-type ppp
#
l2tp-group 1
tunnel password simple 123
tunnel name LAC
start l2tp ip 1.1.1.10 fullusername
vpdnuser
#
interface Virtual-Template1
ppp authentication-mode chap
ppp chap user vpdnuser
#
interface GigabitEthernet0/0
port link-mode route
pppoe-server bind Virtual-Template 1
```

●RTC上的配置:

```
l2tp enable
#
ip pool 1 10.10.12.11 10.10.12.20
#
local-user vpdnuser
password simple 123
service-type ppp
#
l2tp-group 1
allow l2tp virtual-template 1
tunnel password simple 123
tunnel name LNS
#
interface Virtual-Template1
ppp authentication-mode chap
remote address pool 1
ip address 10.10.12.254 255.255.255.0
```

● 排障过程

- 在RTA上ping RTC，没有丢包，说明LAC、LNS之间IP可达；
- 在RTA上查看L2TP Tunnel状态，状态正常；
- 在RTC上开启debugging ppp ipcp查看IPCP过程。

***Feb 20 13:54:04:312 2009 RTC PPP/7/debug2:**

PPP Event:

Virtual-Template1:0 IPCP RCR-(Receive Config Bad Request) Event state reqsent

***Feb 20 13:54:04:312 2009 RTC PPP/7/debug2:**

PPP Packet:

Virtual-Template1:0 Output IPCP(8021) Pkt, Len 14

State reqsent, code ConfRej(04), id 0, len 10

IP Address(3), len 6, val 00000000

- 从输出信息中发现，IPCP协商未能通过，所以客户端无法从LNS获取IP地址。
- 检查L2TP相关配置，发现地址池配置在全局视图下。至此原因找到了，因为配置错误，使LNS端无地址可分配给客户端。

- 解决方案


- 在RTC上地址池配置从全局视图改为域视图后，PCA可以正常获取IP地址，问题解决。

- 建议与总结

- 在LNS为LAC分配IP地址的过程中，如果LNS 没有配置认证，系统将使用全局地址池给用户分配IP 地址，如果LNS启用了认证，系统将使用域视图下的地址池给用户分配IP 地址。
 - 因此在配置了用户验证的情况下，必须在domain视图下配置地址池，否则将导致LNS无法给Client分配IP地址。

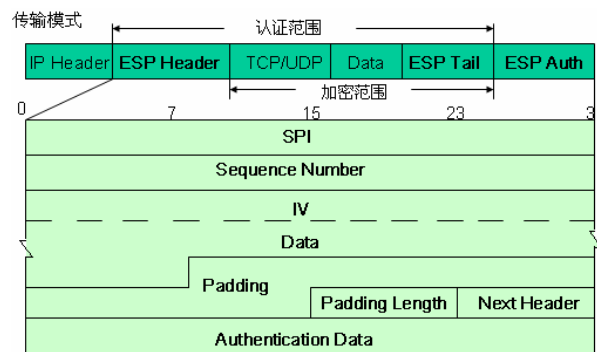
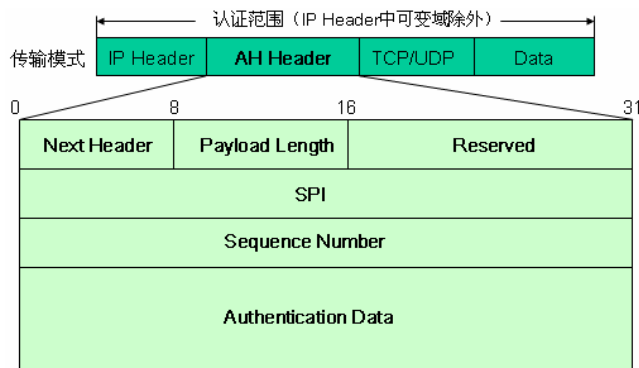


目录

- GRE故障排除
 - L2TP故障排除
 - IPSec VPN故障排除
 - 安全VPN综合组网故障排除
- 

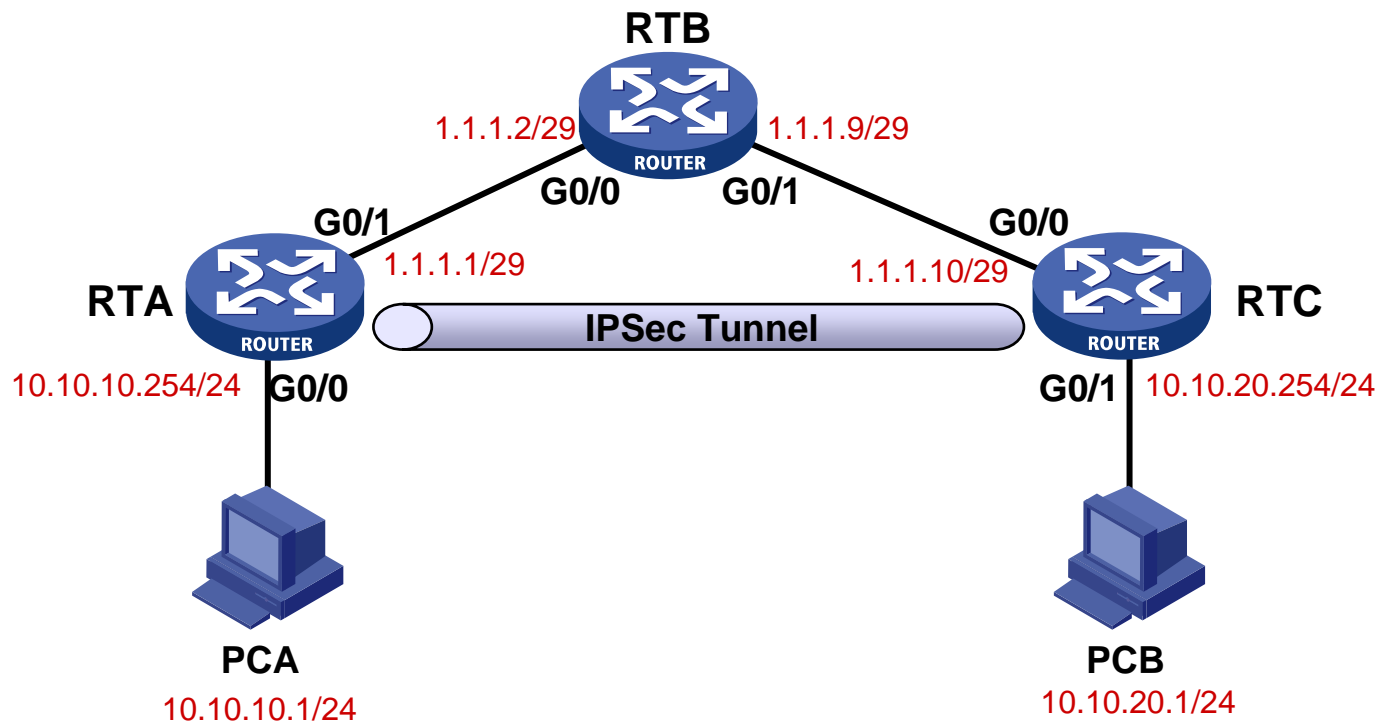
● IKE和IPSec协议

- IKE是一种动态协商IPSec SA的协议，建立在ISAKMP定义的框架之上，能够简化IPSec的使用和管理。
- IPSec是一种保障IP数据安全传输的协议。
- IPSec介于网络层和传输层之间，能够为上层协议提供安全服务，包括数据的完整性、真实性、机密性以及防重放。
- IPSec封装格式包括AH和ESP两种，报文格式如下所示。



- **display ike sa**
 - 显示由IKE建立的安全隧道。
- **display ipsec sa**
 - 显示IPSec安全联盟的具体信息。
- **debugging ike**
 - 打开IKE调试开关
 - 命令undo debugging ike用来关闭IKE调试开关。
- **debugging ipsec**
 - 打开IPSec调试开关
 - 命令undo debugging ipsec用来关闭IPSec调试开关。

- **检查IPSec隧道公网地址是否可达**
 - 从IPSec隧道一侧ping对端公网地址，检查公网地址可达性。
- **检查Security ACL配置是否正确**
 - IPSec要求通讯双方的Security ACL互为镜像，如果不符合镜像原则，会导致IPSec SA协商失败。
- **检查Security ACL模式是否一致**
 - IPSec隧道两端Security ACL 模式必须一致，IPSec隧道才能连通。
- **检查IPSec隧道两端安全提议是否一致**
 - IPSec通讯双方的隧道封装模式、封装格式、加密算法、验证算法等，都应该一致
- **检查预共享密钥是否相同**
 - IPSec隧道两端预共享密码必须完全相同，否则会导致IKE载荷不能识别，无法通过阶段一协商。
- **IPSec MTU问题**
 - IPSec封装后的报文比原始IP报文大约多40字节，如果接口的MTU为1500，所能承载的原始IP报文长度应该 ≤ 1460 。



● 故障现象

→ RTA、RTC之间无法建立IPSec Tunnel。

●RTA上的配置:

```
ike local-name spoke
#
acl number 3001
 rule 0 permit ip destination 10.10.20.0
    0.0.0.255
#
ike peer hub
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name hub
 remote-address 1.1.1.10
#
ipsec proposal prop
#
ipsec policy policy 10 isakmp
 security acl 3001
 ike-peer hub
 proposal prop
```

●RTC上的配置:

```
ike local-name hub
#
acl number 3001
 rule 0 permit ip destination 10.10.10.0
    0.0.0.255
#
ike peer spoke
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name spoke
 remote-address 1.1.1.1
#
ipsec proposal prop
#
ipsec policy policy 10 isakmp
 security acl 3001
 ike-peer spoke
 proposal prop
```

● 排障过程

- 在RTA上ping RTC，没有丢包，说明IPSec隧道公网地址可达；
- 在RTA上查看IKE SA，发现Phase 1正常，说明 IKE协商正常，但Phase 2 不正常，说明IPSec协商有问题；
- 开启debug ike all查找原因

```
*Feb 20 15:05:54:750 2009 RTA IKE/7/DEBUG: PROTO: ISAKMP
*Feb 20 15:05:54:750 2009 RTA IKE/7/DEBUG: SPI_SZ: 0
*Feb 20 15:05:54:765 2009 RTA IKE/7/DEBUG: MSG_TYPE:
INVALID_ID_INFORMATION
```

- 从输出信息中发现，不合法ID导致Phase 2协商失败；
- 检查RTA、RTC两端IPSec相关配置。发现Security ACL没有互为镜像

- 解决方案

→ 将RTA、RTC上的Security ACL修改为完全镜像后，IPSec协商通过。

RTA

acl number 3001

rule 0 permit ip source 10.10.10.0 0.0.0.255 destination 10.10.20.0 0.0.0.255

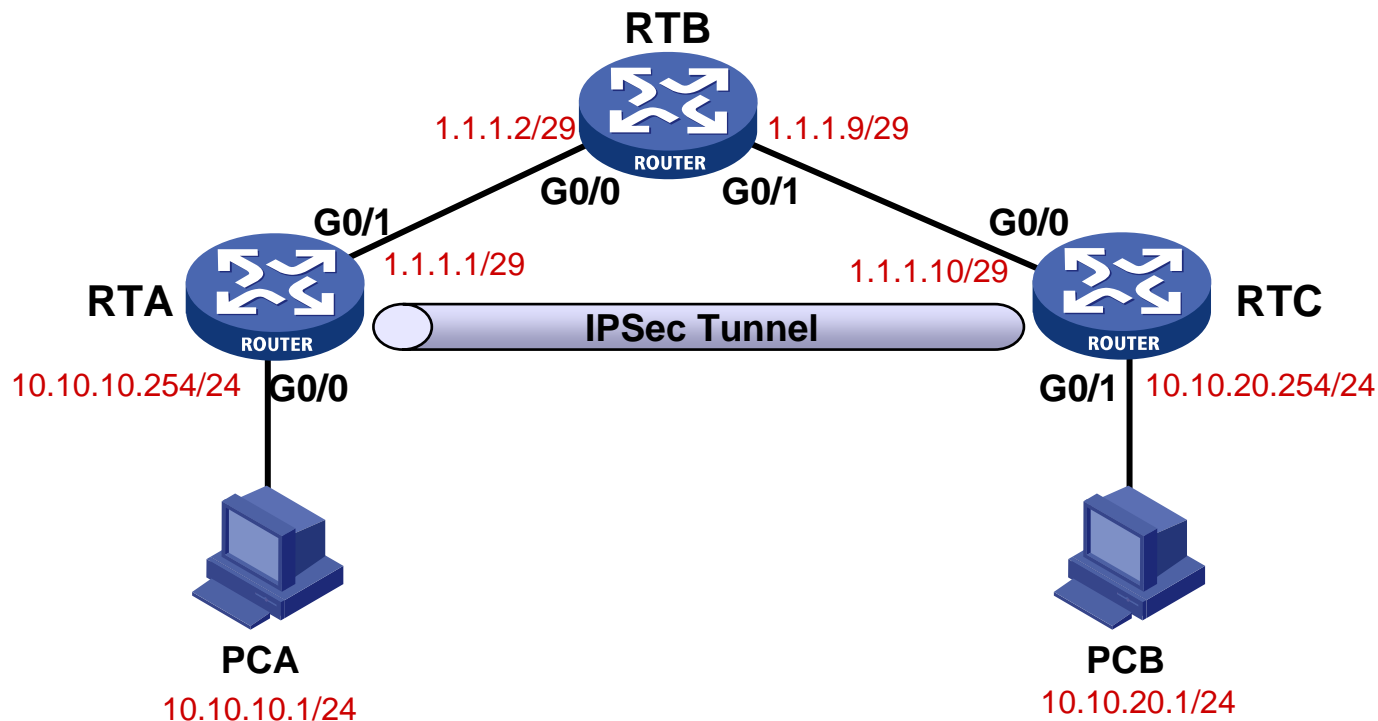
RTC

acl number 3001

rule 0 permit ip source 10.10.20.0 0.0.0.255 destination 10.10.10.0 0.0.0.255

- 建议与总结

→ IPSec Tunnel两端的Security ACL必须互为镜像，即两端Security ACL的源和目的互反，否则会导致隧道无法正确建立。



● 故障现象

→ RTA、RTC之间的IPSec隧道开始时运行正常。某天突然中断。

●RTA上的配置:

```
ike local-name spoke
#
acl number 3001
 rule 0 permit ip source 10.10.10.0
   0.0.0.255 destination 10.10.20.0
   0.0.0.255
#
ike peer hub
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name hub
 remote-address 1.1.1.10
#
ipsec proposal prop
#
ipsec policy policy 10 isakmp
 security acl 3001
 ike-peer hub
 proposal prop
```

●RTC上的配置:

```
ike local-name hub
#
ike peer spoke
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name spoke
#
ipsec proposal prop
#
ipsec policy-template temp 10
 ike-peer spoke
 proposal prop
#
ipsec policy policy 10 isakmp template
 temp
```

● 排障过程

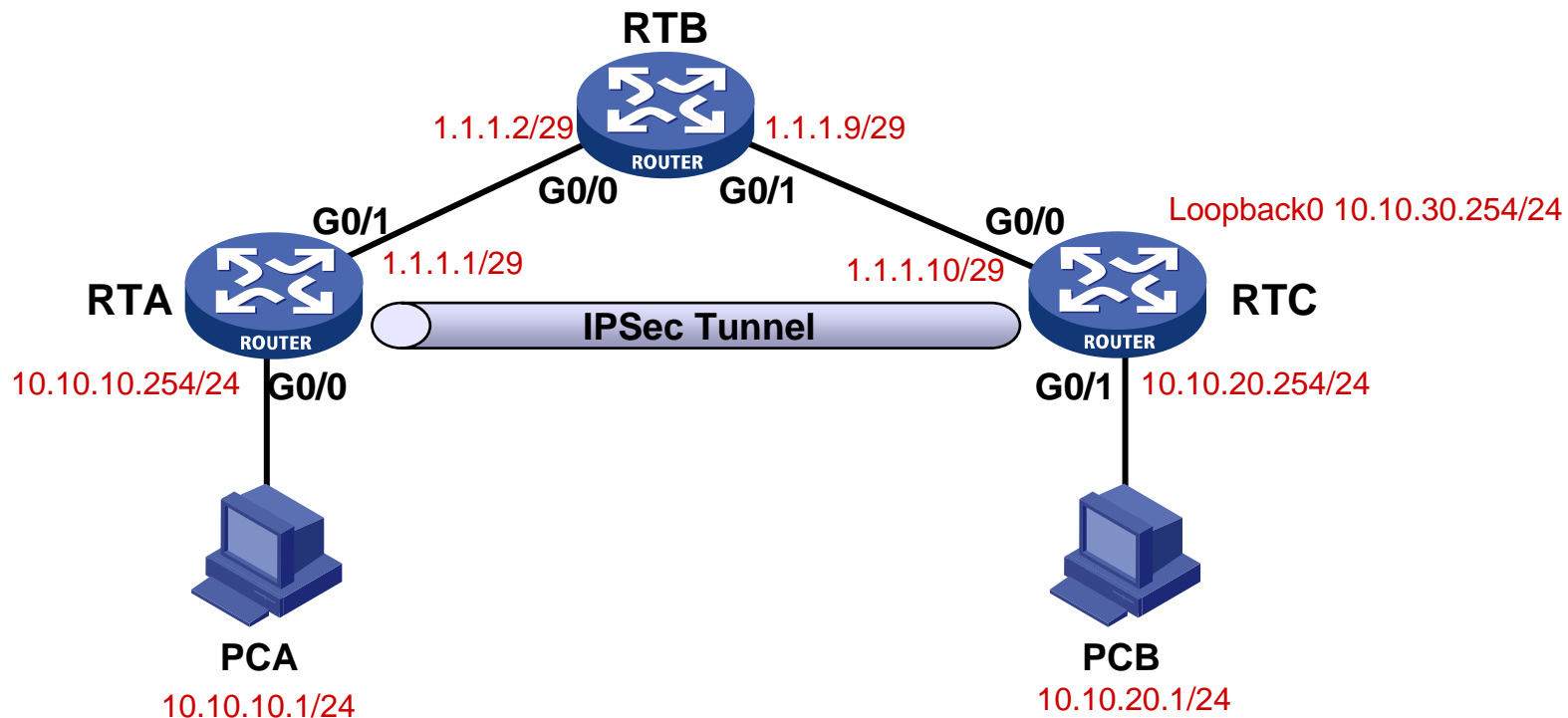
- 在RTA上ping RTC，没有丢包，说明IPSec隧道外层IP地址可达；
- 在RTA上从用户网段10.10.10.254 ping RTC上用户网段地址10.10.20.254，不能ping通。说明IPSec隧道有问题。
- 查看RTA、RTC两端IKE SA状态，发现在RTA上，阶段一连接不存在，只有阶段二连接；而在RTC上，两个阶段都不存在。
- 故障的原因找到。是因为一端有IPSec SA，而另一端没有。RTA使用已有的IPSec SA对数据进行封装，但对端RTC没有IPSec SA，无法解封装。

- 解决方案

- 在RTA上执行reset ipsec sa命令，使RTA、RTC重新协商，IPSec隧道建立正常，问题得以解决。

- 建议与总结

- IPSec与IKE紧密结合，又有相对的独立性。正确的复位IPSec连接的顺序为：先重置IPSec SA，然后重置IKE SA。如果先重置IKE SA。这种情况下，除非没有IPSec SA的一端主动发起到对端的访问，触发重新建立IKE连接；或者手工删除已有的IPSec SA，才能正确建立IPSec隧道。



● 故障现象

→ RTA可以访问RTC上的10.10.20.254，不能访问RTC上的10.10.30.254。

●RTA上的配置:

```
ike local-name spoke
#
acl number 3001
 rule 0 permit ip source 10.10.10.0 0.0.0.255
   destination 10.10.20.0 0.0.0.255
 rule 1 permit ip source 10.10.10.0 0.0.0.255
   destination 10.10.30.0 0.0.0.255
#
ike peer hub
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name hub
 remote-address 1.1.1.10
#
ipsec proposal prop
#
ipsec policy policy 10 isakmp
 security acl 3001 aggregation
 ike-peer hub
 proposal prop
```

●RTC上的配置:

```
ike local-name hub
#
acl number 3001
 rule 0 permit ip source 10.10.20.0 0.0.0.255
   destination 10.10.10.0 0.0.0.255
 rule 1 permit ip source 10.10.30.0 0.0.0.255
   destination 10.10.10.0 0.0.0.255
#
ike peer spoke
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name spoke
 remote-address 1.1.1.1
#
ipsec proposal prop
#
ipsec policy policy 10 isakmp
 security acl 3001
 ike-peer hub
 proposal prop
```

● 排障过程

- 在RTA上以源地址10.10.10.254发送IMCP报文。可以ping通10.10.20.254，但是不能ping通10.10.30.254；
- 在RTA上ping RTC，没有丢包，说明IPSec隧道外层IP地址可达；
- 在RTA、RTC上查看IKE SA，IKE协商正常，IPSec协商也正常；
- 分别在RTA、RTC上查看IPSec SA，在RTC上只有10.10.20.0/24到10.10.10.0/24的IPSec SA，没有10.10.30.0/24到10.10.10.0/24的IPSec SA；
- 检查RTA、RTC两端IPSec相关配置，发现RTA使用聚合方式的Security ACL，RTC使用非聚合方式的Security ACL，导致两者协商出来的IPSec SA不一致。

- 解决方案

→ 将RTA改为非聚合方式后，问题得以解决。

```
RTA
ipsec policy policy 10 isakmp
security acl 3001
```

- 建议与总结

→ 在V5版本中，IPSec Policy缺省使用非聚合方式的Security ACL；而V3版本只支持聚合方式的Security Acl。因此，如果两端设备版本不同，一端为V5、一端为V3，则需要在两端都使用聚合模式。

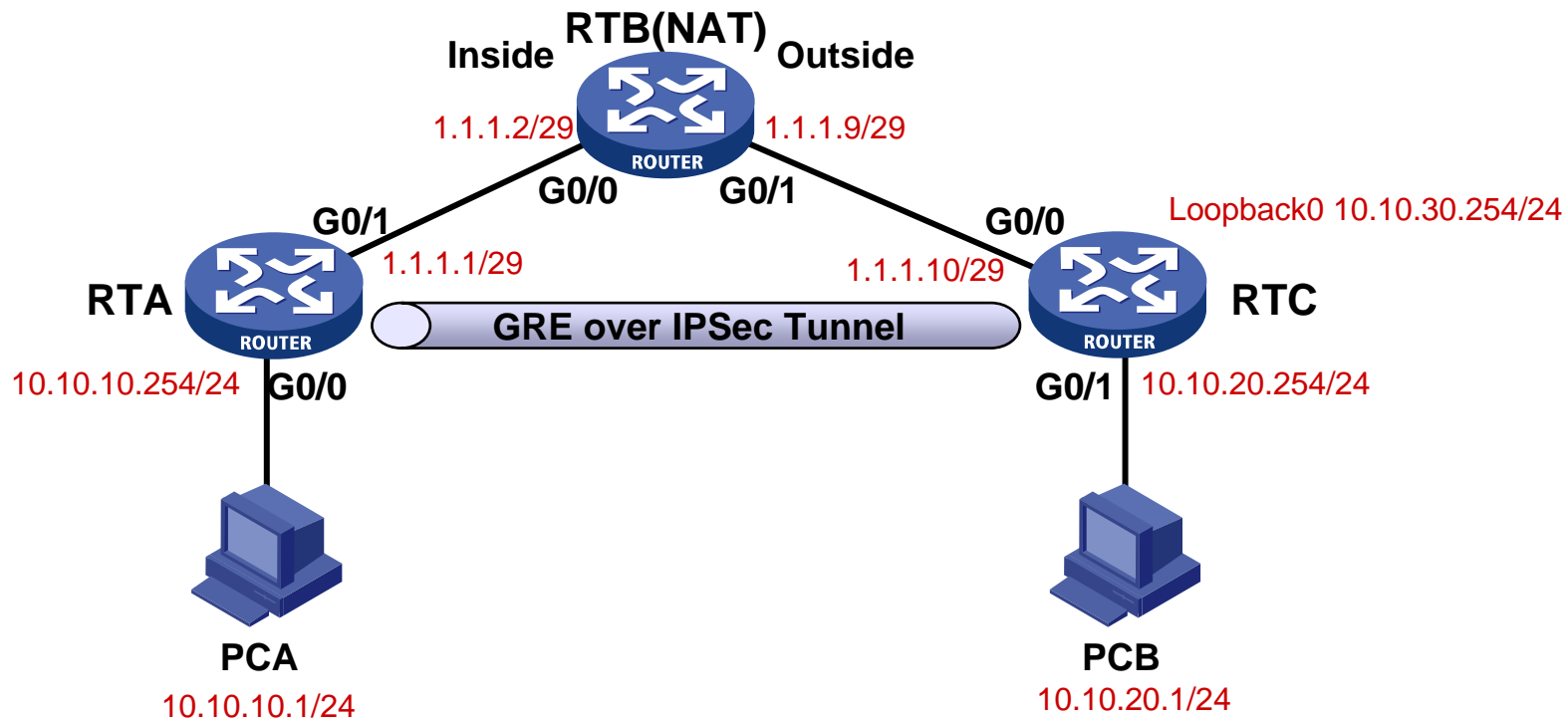


目录

- GRE故障排除
 - L2TP故障排除
 - IPSec VPN故障排除
 - 安全VPN综合组网故障排除
- 

● VPN综合组网应用

- **GRE over IPSec**。通过GRE over IPsec封装，可以在IPSec站点之间运行动态路由协议，又保证数据的机密性，一举二得。
- **L2TP over IPSec**。通过L2TP over IPsec封装，既保证了数据的安全性，又能借助于L2TP的认证功能、动态IP分配等特性，实现用户的远程IPSec拨入。
- **IPSec NAT穿越**。启用NAT Traversal特性后，在IKE协商时，通过NAT-T能力检测发现NAT设备，采用UDP格式封装IPSec报文，实现IPSec的NAT穿越。为了保持NAT设备上IPSec会话表项激活，IKE需要定时发送NAT Keepalive报文。
- **IPSec高可靠性组网**。在IPSec大型组网中，多个分支接入单个中心，由于中心单链路、设备单点故障等问题，很容易造成全网中断，为了提高整网的可靠性，中心应该采用双链路、双设备的高可靠性组网。



● 故障现象

- RTA、RTC之间IKE协商成功，双方都学习到正确的IPSec SA，但是PCA无法ping通PCB。

●RTA上的配置：

```
ike local-name spoke
#
acl number 3001
 rule 0 permit gre
#
ike peer hub
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name hub
 remote-address 1.1.1.10
 nat traversal
#
ipsec proposal prop
 encapsulation-mode transport
#
ipsec policy policy 10 isakmp
 security acl 3001
 ike-peer hub
 proposal prop
```

●RTC上的配置：

```
ike local-name hub
#
ike peer spoke
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name spoke
 nat traversal
#
ipsec proposal prop
 encapsulation-mode transport
#
ipsec policy-template temp 10
 ike-peer spoke
 proposal prop
#
ipsec policy policy 10 isakmp template
 temp
```

● 排障过程

- 在RTA上ping RTC，没有丢包，说明IPSec隧道外层IP地址可达；
- 在RTA上ping RTC的GRE隧道互连地址，不能ping通，说明IPSec隧道连通性有问题；
- 在RTA、RTC上查看IKE SA，IKE协商正常，IPSec协商也正常；
- 在RTA上用debug ipsec packet，发现系统提示IPSec丢弃报文，并提示报文在传输模式下不受保护。

PING 10.10.13.3: 56 data bytes, press CTRL_C to break

***Dec 16 11:40:49:542 2008 RTA IPSEC/7/DBG:IPSec drop packet! this packet can't be protect in transport mode.**

- 解决方案

→ 在RTA、RTC上将IPSec封装模式改为隧道模式后，问题得以解决。

RTA

```
ipsec proposal prop  
encapsulation-mode tunnel
```

RTC

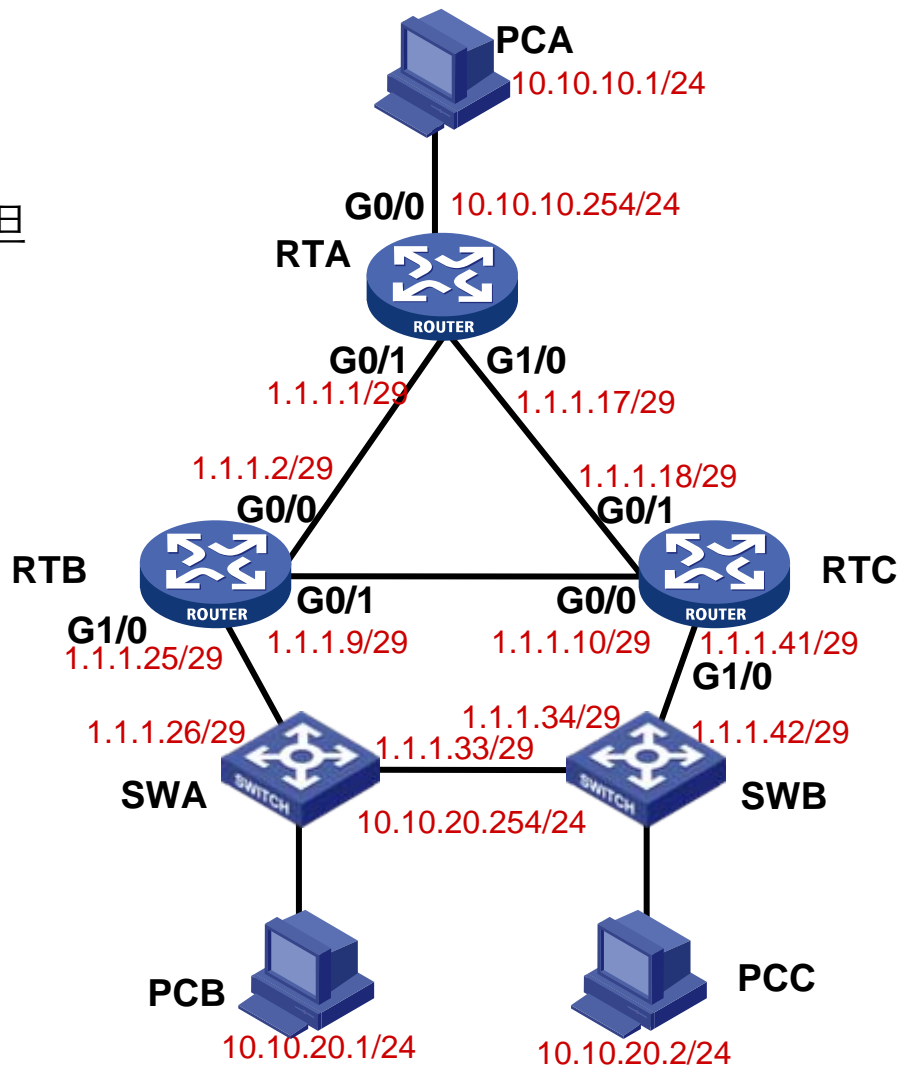
```
ipsec proposal prop  
encapsulation-mode tunnel
```

- 建议和总结

→ IPSec的NAT穿越只支持隧道模式，不支持传输模式，如果使用传输模式将导致IPSec封装失败，IPSec通信中断。

● 故障现象

→ PCA能够与PCB正常通信，但是不能与PCC正常通信。



●RTA上的配置：

```
ike local-name spoke
#
acl number 3001
 rule 0 permit ip source 10.10.10.0 0.0.0.255
   destination 10.10.20.0 0.0.0.255
#
ike peer hub1
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name hub1
 remote-address 1.1.1.2
#
ike peer hub2
 exchange-mode aggressive
 pre-shared-key simple 123
 id-type name
 remote-name hub2
 remote-address 1.1.1.18
#
ipsec proposal prop
```

```
ipsec policy policy 10 isakmp
 security acl 3001
 ike-peer hub1 hub2
 proposal prop
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
ip route-static 0.0.0.0 0.0.0.0 1.1.1.18
 preference 200
```

●RTB上的配置:

```
ike local-name hub1
#
ike peer spoke
  exchange-mode aggressive
  pre-shared-key simple 123
  id-type name
  remote-name spoke
#
ipsec proposal prop
#
ipsec policy-template temp 10
  ike-peer spoke
  proposal prop
#
ipsec policy policy 10 isakmp template temp
#
ospf 1
  default-route-advertise cost 10
  area 0.0.0.0
    network 1.1.1.0 0.0.0.255
ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

●RTC上的配置:

```
ike local-name hub2
#
ike peer spoke
  exchange-mode aggressive
  pre-shared-key simple 123
  id-type name
  remote-name spoke
#
ipsec proposal prop
#
ipsec policy-template temp 10
  ike-peer spoke
  proposal prop
#
ipsec policy policy 10 isakmp template temp
#
ospf 1
  default-route-advertise cost 100
  area 0.0.0.0
    network 1.1.1.0 0.0.0.255
ip route-static 0.0.0.0 0.0.0.0 1.1.1.17
```

● 排障过程

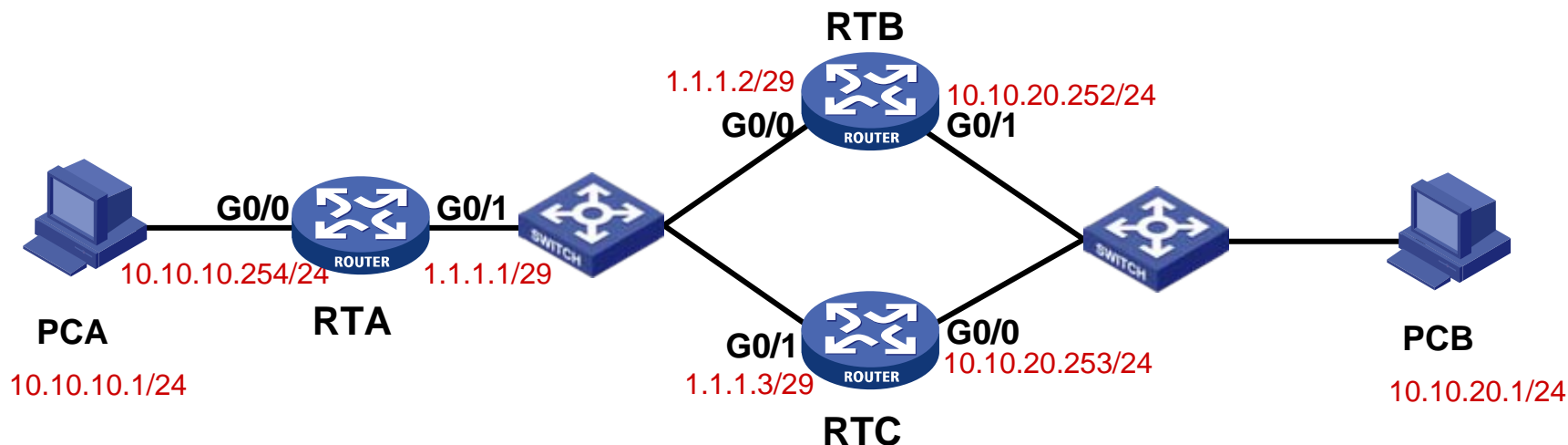
- 在RTA上ping RTB、RTC，没有丢包，说明IPSec隧道外层IP地址可达；
- 在PCA上ping PCB，能够ping通；在PCA上ping PCC，不能ping通；
- 在RTA、RTB上查看IKE SA，IKE协商正常，IPSec协商也正常；
- 在SWB上查看路由表，发现缺省路由形成等价路由，下一跳分别指向SWA、RTC；
- 发现问题原因：经过SWA的数据包被转发给RTB。由于RTB、RTA之间建立了IPSec隧道，所以数据可以被转发到RTA；而经过RTC的数据包直接匹配RTC本地配置的缺省路由，由于RTC没有与RTA建立IPSec隧道，导致所有经过RTC的数据包被丢弃。

- 解决方案

- 通过调整RTC上缺省路由优先级，可以解决等价路由造成IPSec隧道局部访问不通的问题。

- 建议和总结

- IPSec隧道要求来回路径必须一致。存在等价路由的组网中，可能出现访问同一网段的不同主机时，有些主机能够连通，另外一些主机不能连通的奇怪现象。其根本原因是网络中存在等价路由，致使部分数据流的来回路径不一致，从而导致数据流被丢弃。遇到这种情况时，可以通过消除等价路由来解决。



● 故障现象

→ RTA上IKE协商成功，但是PCA不能与PCB正常通讯

●RTB上的配置：

```
interface GigabitEthernet0/0
port link-mode route
ip address 1.1.1.2 255.255.255.248
vrrp vrid 1 virtual-ip 1.1.1.4
vrrp vrid 1 priority 110
ipsec policy policy
#
interface GigabitEthernet0/1
port link-mode route
ip address 10.10.20.252 255.255.255.0
vrrp vrid 10 virtual-ip 10.10.20.254
```

●RTC上的配置：

```
interface GigabitEthernet0/0
port link-mode route
ip address 10.10.20.253 255.255.255.0
vrrp vrid 10 virtual-ip 10.10.20.254
vrrp vrid 10 priority 110
#
interface GigabitEthernet0/1
port link-mode route
ip address 1.1.1.3 255.255.255.248
vrrp vrid 1 virtual-ip 1.1.1.4
ipsec policy policy
```


● 排障过程

- 在PCA上ping PCB，不能ping通；
- 在RTA上ping RTB、RTC以及公网VRRP虚地址1.1.1.4，都没有丢包，说明IPSec隧道公网地址可达；
- 在RTA、RTC上查看IKE SA，IKE协商正常，IPSec协商也正常；
- 在RTB上查看VRRP状态，发现RTB内外网接口VRRP主备状态不一致；
- 问题原因发现了。由于内外网VRRP主备关系不一致，致使来回路径不一致，因此PCA无法ping通PCB。

● 解决方案

→ 调整内网的VRRP主备优先级，就可以解决这个问题。

RTB

```
interface GigabitEthernet0/1  
vrrp vrid 10 priority 110
```

RTC

```
interface GigabitEthernet0/1  
vrrp vrid 10 priority 100
```

● 建议与总结

→ 在IPSec高可靠性组网中，普遍使用VRRP方式实现中心IPSec接入设备的冗余。如果中心IPSec设备内外接口都启用VRRP，必须保证内外VRRP的主备关系一致，否则会出现来回路径不一致，导致IPSec通讯失败。

本章总结

- **GRE**相关知识与故障排除
- **L2TP**相关知识与故障排除
- **IPSec VPN**相关知识与故障排除
- **安全VPN**综合组网相关知识与故障排除

H3C

IToIP 解决方案专家

杭州华三通信技术有限公司

www.h3c.com