

GRE VPN



前言

通用路由封装协议GRE（Generic Routing Encapsulation）提供了一种协议的报文封装在另一种协议报文中的机制，是一种隧道封装技术。GRE可以封装组播数据，并可以和IPSec结合使用，从而保证语音、视频等组播业务的安全。

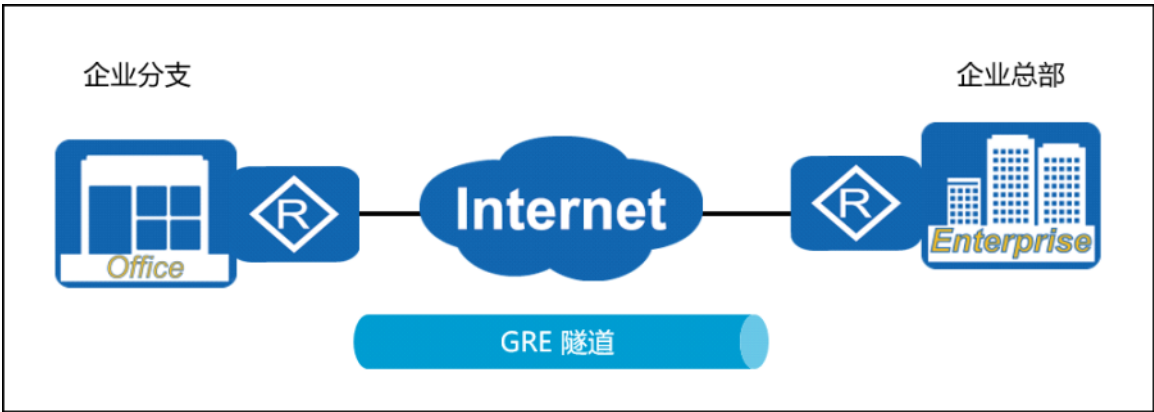
GRE: Generic Routing Encapsulation，通用路由封装

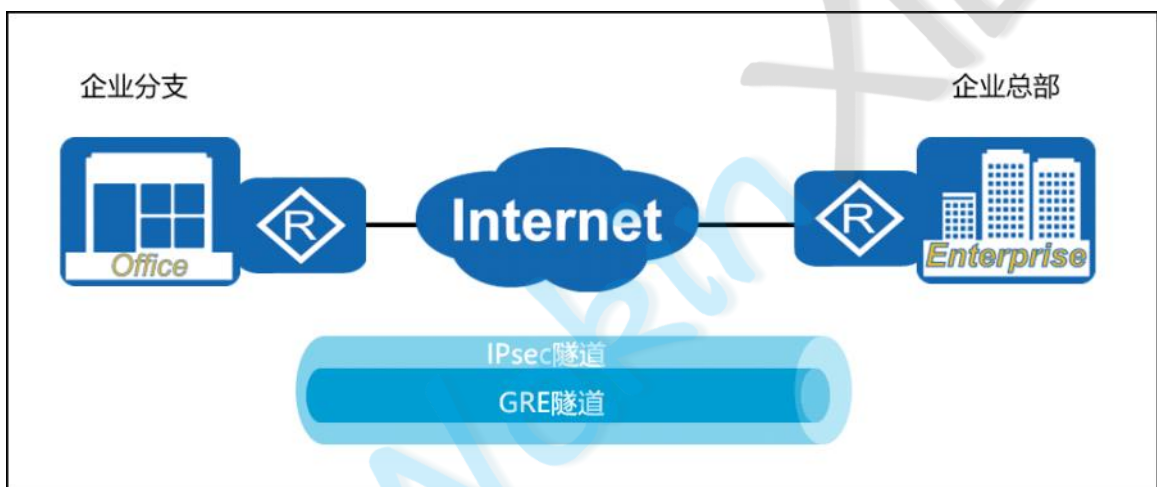
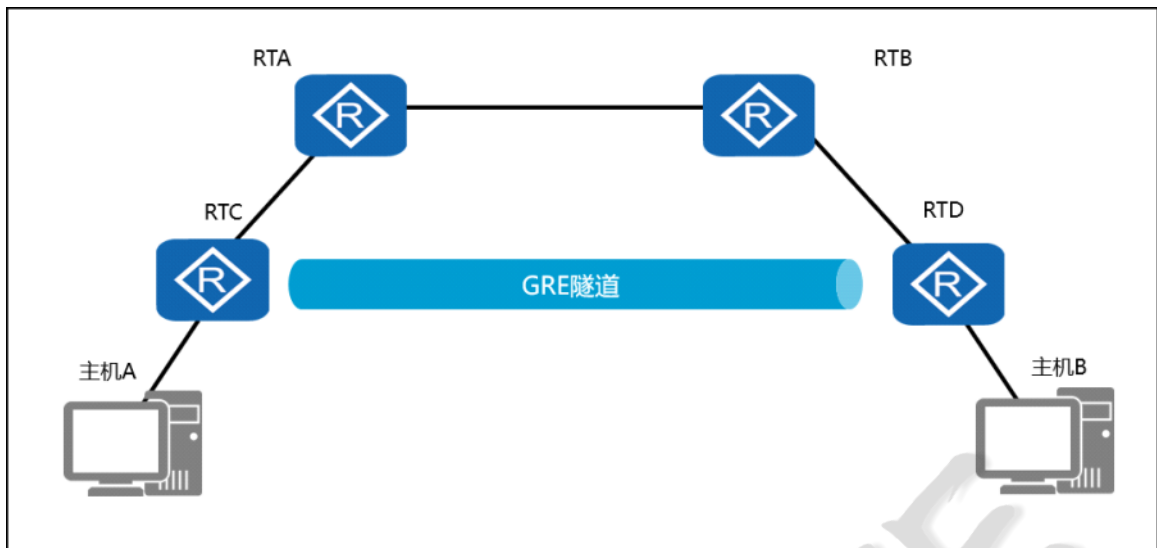
- 一种三层VPN封装技术
- 在任意一种网络协议上传送任意一种其它网络协议的封装方法
- 解决了跨越异种网络的报文传输问题，异种报文传输的通道称为**Tunnel**（隧道）



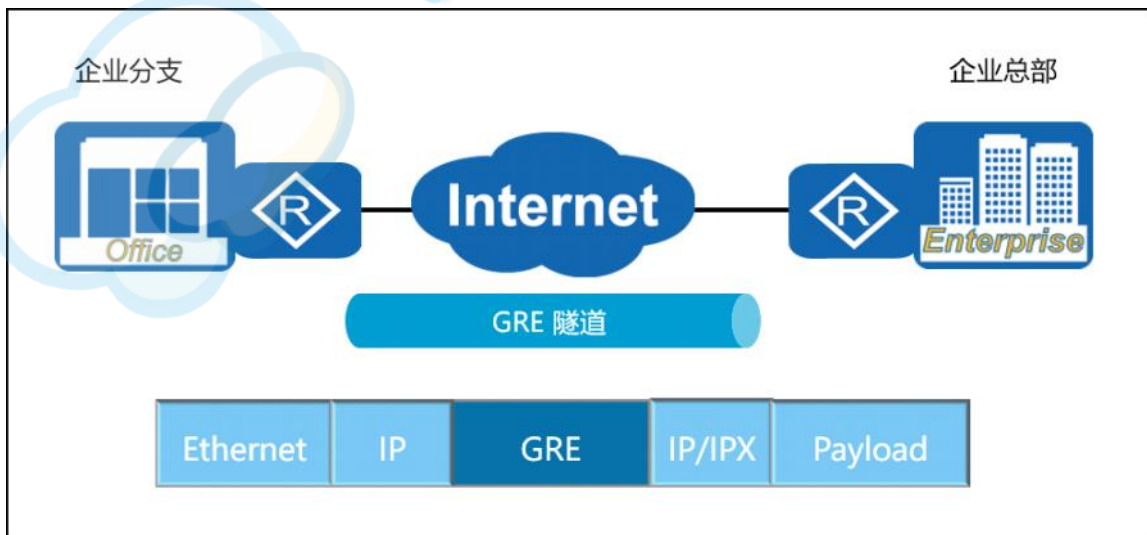
GRE优点	GRE缺点
建立隧道	点对点隧道
支持多种网络层协议	静态配置隧道参数
支持路由组播	布署复杂连接关系时代价巨大
配置简单，容易布署	缺乏安全性

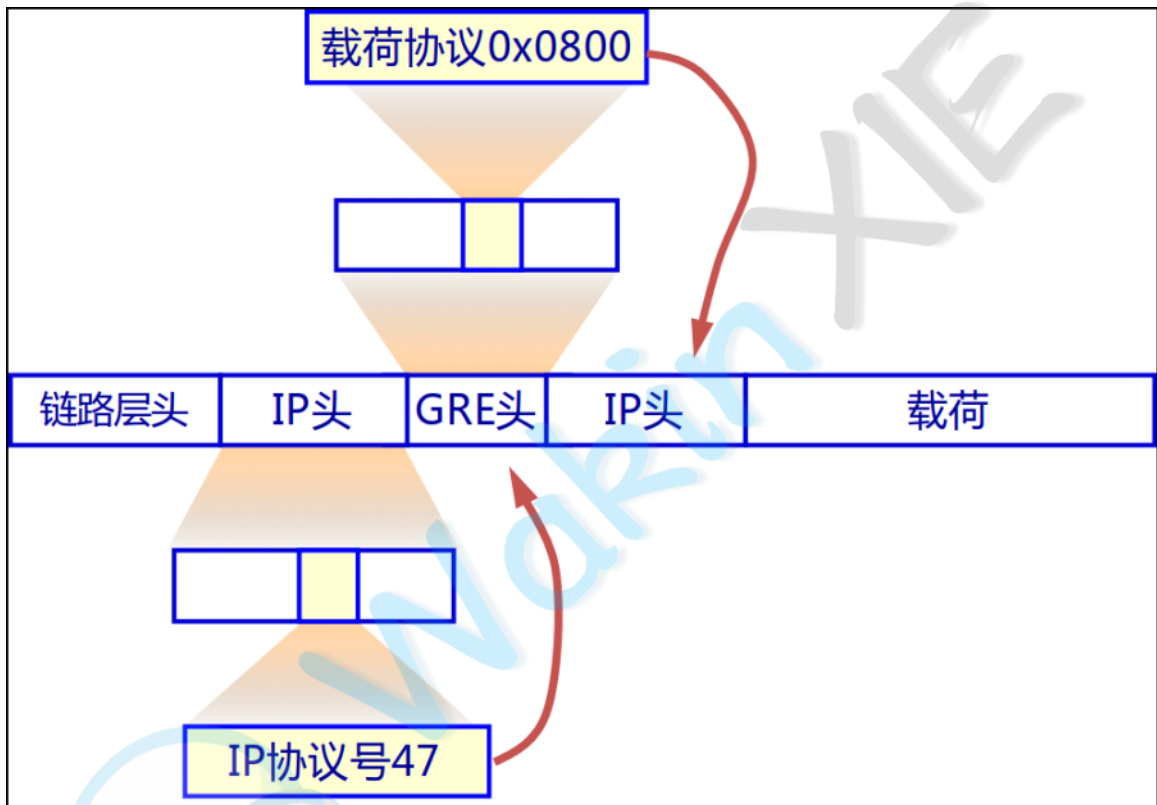
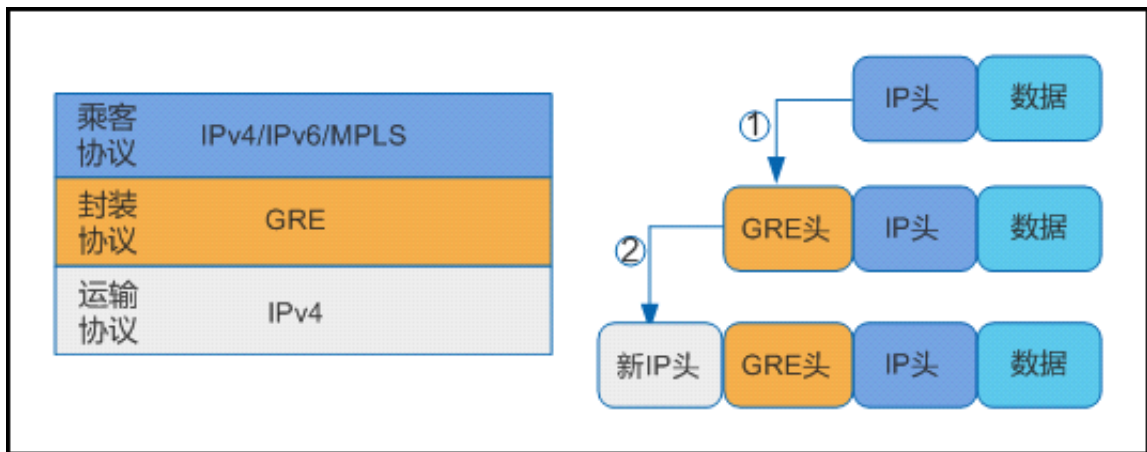
GRE核心功能：建立隧道，打通私网





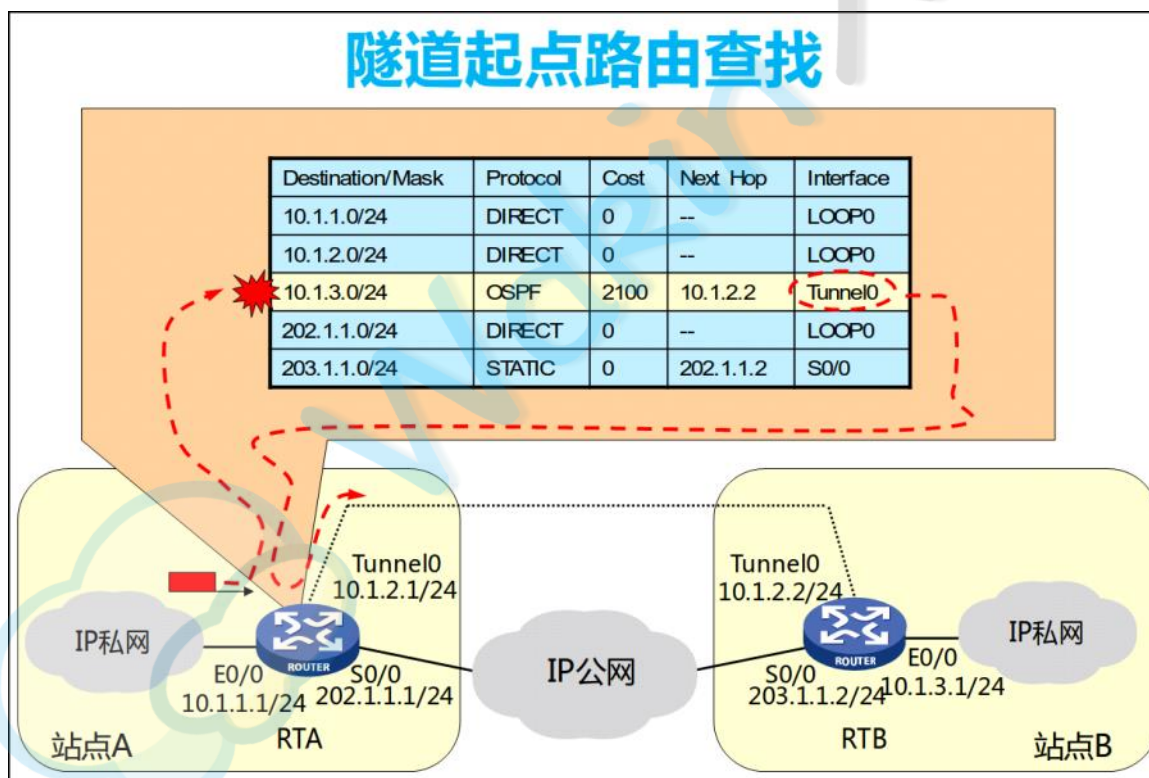
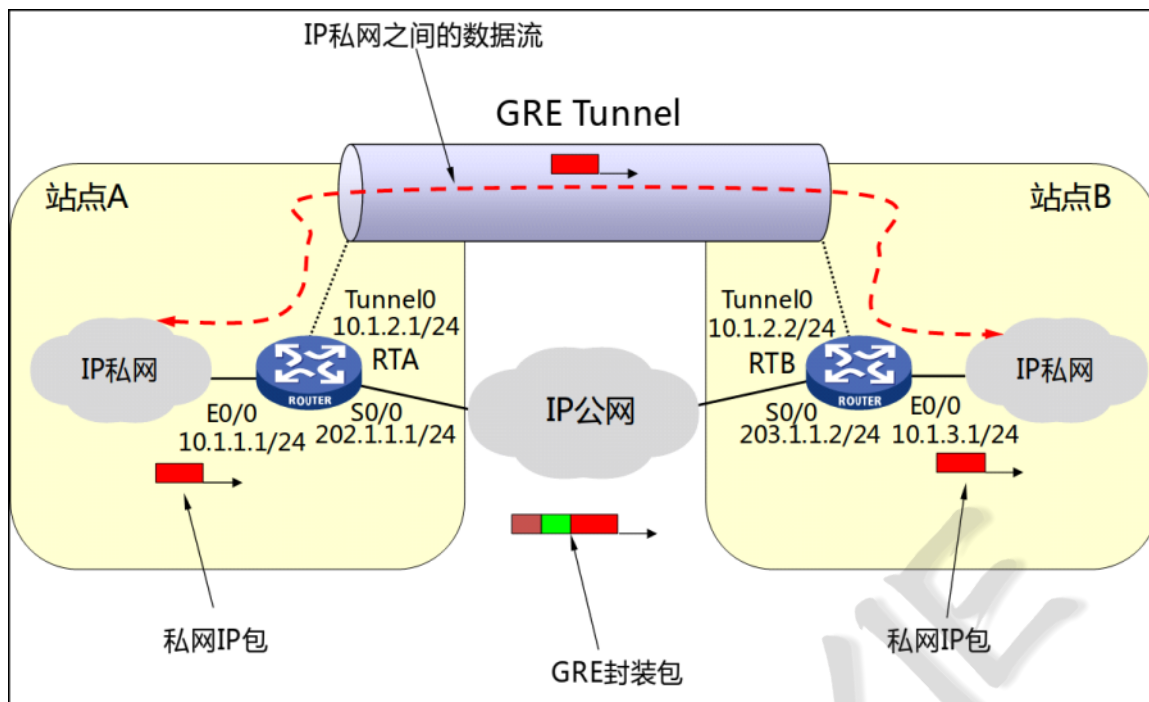
GRE封装：穿马甲





```
Internet Protocol Version 4, Src: 12.0.0.1 (12.0.0.1), Dst: 23.0.0.3 (23.0.0.3)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not-ECT))
  Total Length: 124
  Identification: 0x0005 (5)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: GRE (47)
  Header checksum: 0x984a [validation disabled]
  Source: 12.0.0.1 (12.0.0.1)
  Destination: 23.0.0.3 (23.0.0.3)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Generic Routing Encapsulation (IP)
  Flags and Version: 0x0000
  Protocol Type: IP (0x0800)
Internet Protocol Version 4, Src: 13.0.0.1 (13.0.0.1), Dst: 13.0.0.3 (13.0.0.3)
Internet Control Message Protocol
```

GRE VPN转发过程详解:



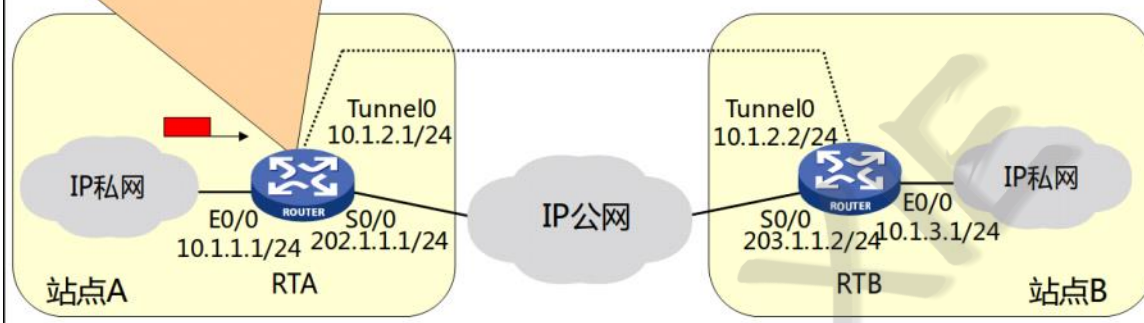
加封装

RTA Tunnel0接口参数：

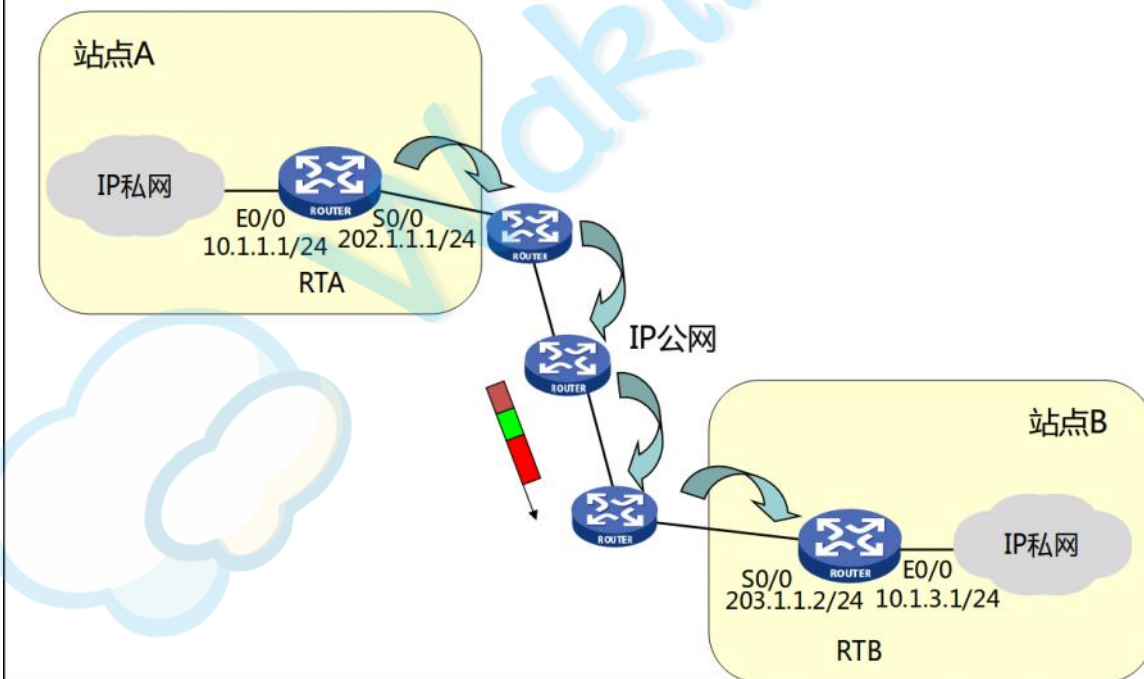
- GRE封装
- 源接口S0/0，地址202.1.1.1
- 目标地址203.1.1.2

源地址：202.1.1.1

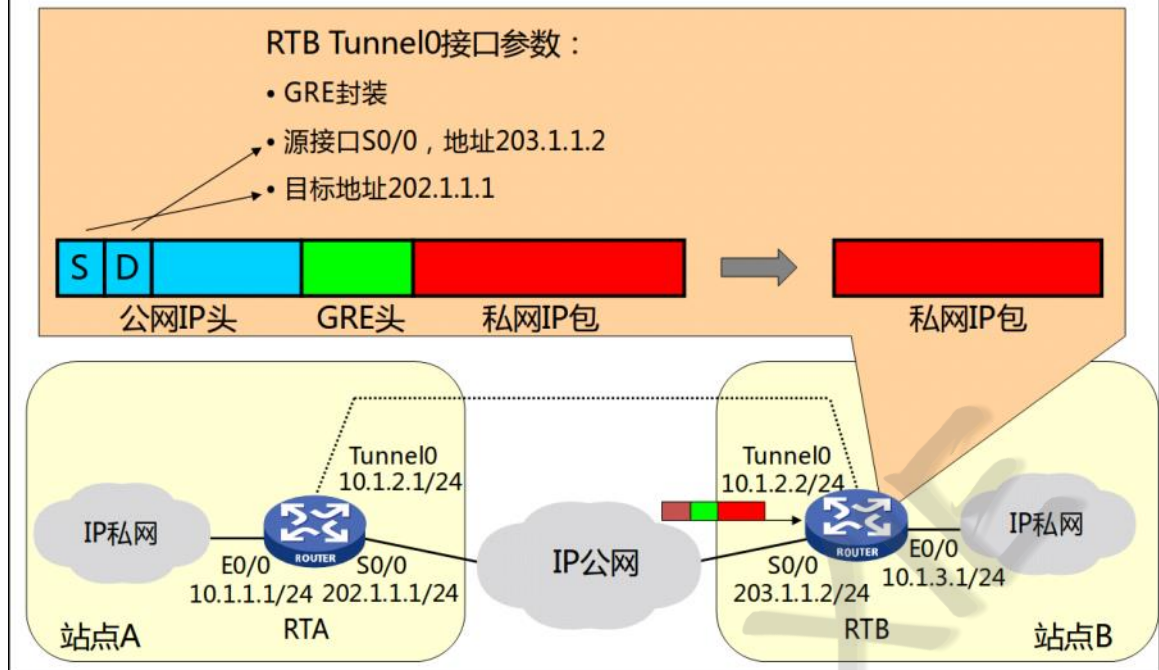
目的地址：203.1.1.2



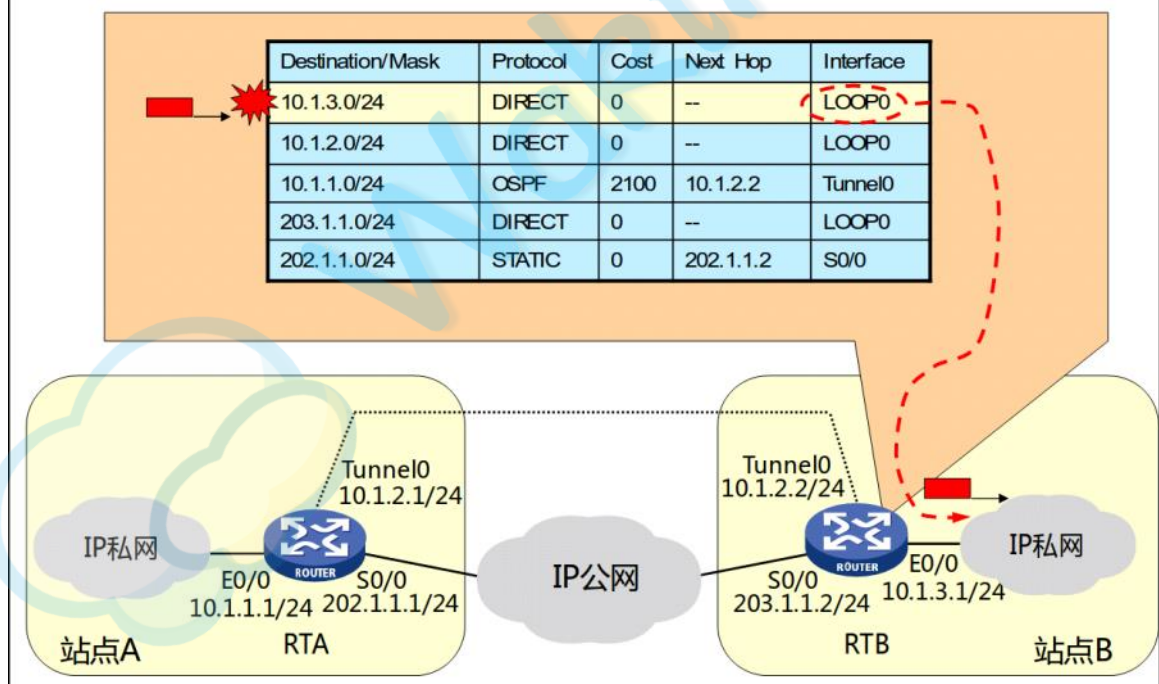
中途转发

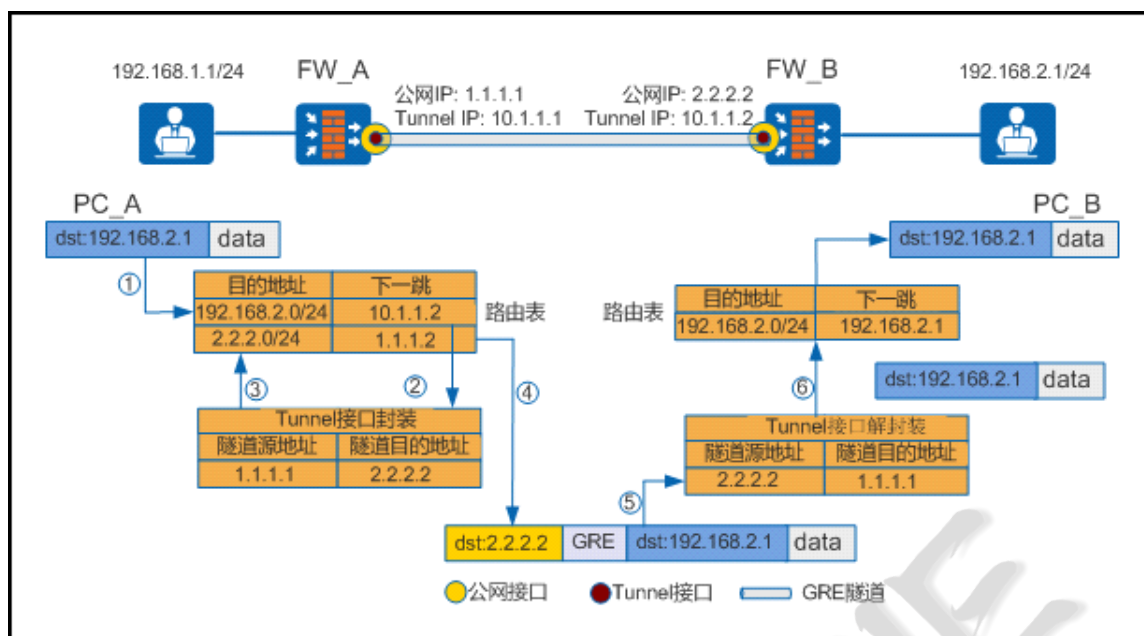


解封装



隧道终点路由查找

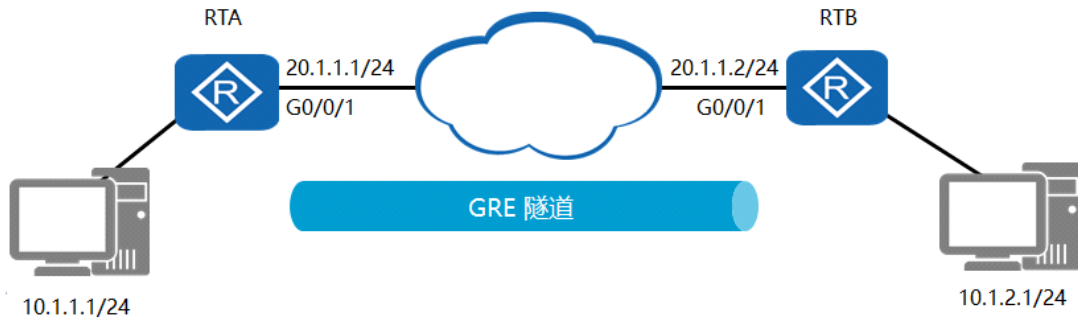




GRE VPN的配置:

命令	备注
<code>interface tunnel 0/0/1</code>	创建隧道口。
<code>tunnel-protocol gre</code>	指定协议。
<code>source 12.0.0.2</code>	指定隧道源。
<code>destination 13.0.0.3</code>	指定隧道目标。
配置IP地址、路由	注意下一跳、出站口、宣告口。
<code>display interface tunnel 0/0/1</code>	查看隧道口状态。
<code>keepalive period 5 retry-times 3</code>	开启Keepalive检测避免数据黑洞。

GRE配置



```
[RTA]interface Tunnel 0/0/1
[RTA-Tunnel0/0/1]tunnel-protocol gre
[RTA-Tunnel0/0/1]ip address 40.1.1.1 24
[RTA-Tunnel0/0/1]source 20.1.1.1
[RTA-Tunnel0/0/1]destination 20.1.1.2
[RTA-Tunnel0/0/1]quit
[RTA]ip route-static 10.1.2.0 24 Tunnel 0/0/1
```

配置验证

```
[RTA]display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2013-08-21 13:37:38
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port, The Maximum Transmit Unit is 1476
Internet Address is 40.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 20.1.1.1 (GigabitEthernet0/0/1), destination 20.1.1.2
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
.....
```


配置验证

```
[RTA]display ip routing-table
```

Route Flags: R - relay, D - download to fib

Routing Tables: Public Destinations : 13 Routes : 14

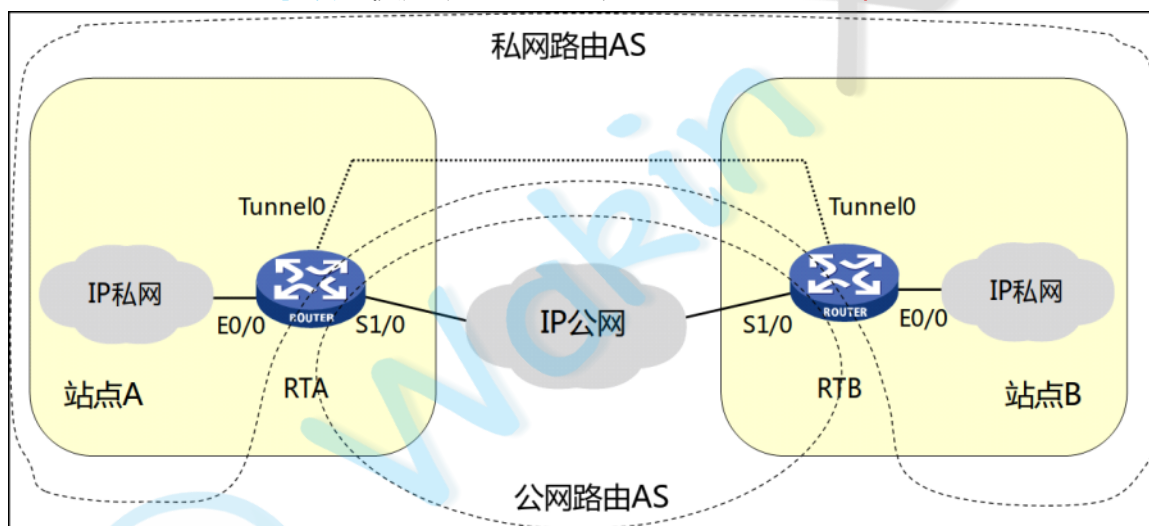
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
------------------	-------	-----	------	-------	---------	-----------

.....

10.1.2.0/24	Static	60	0	RD	40.1.1.2	Tunnel 0/0/1
-------------	--------	----	---	----	----------	--------------

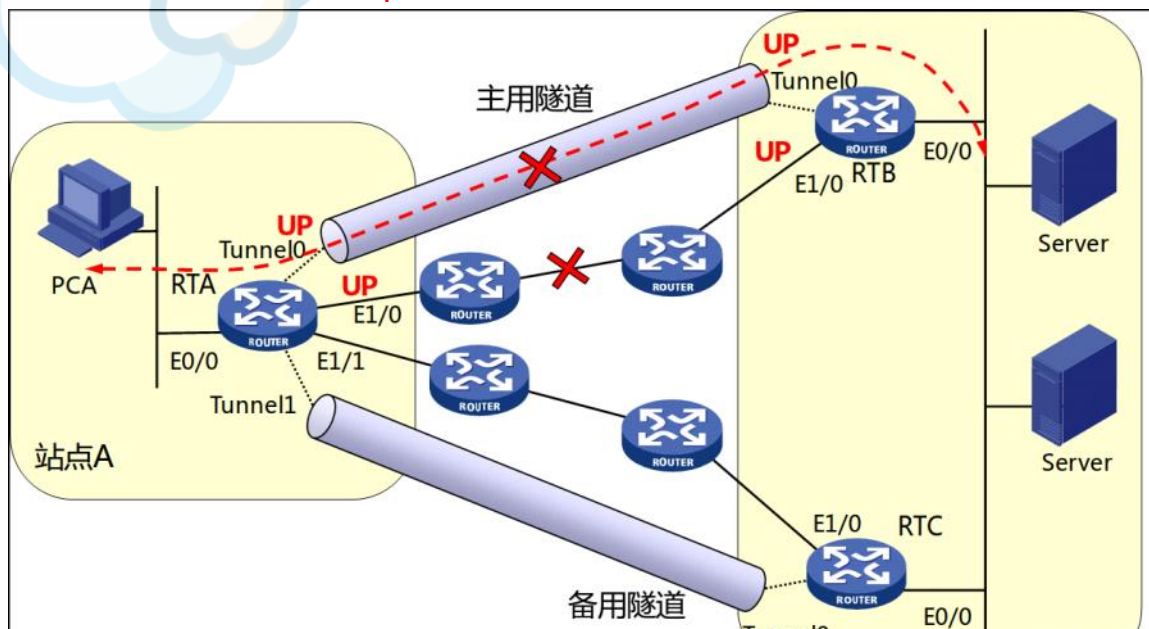
.....

GRE VPN路由宣告注意事项: 使用动态路由协议宣告接口时千万**不能宣告公网接口**。

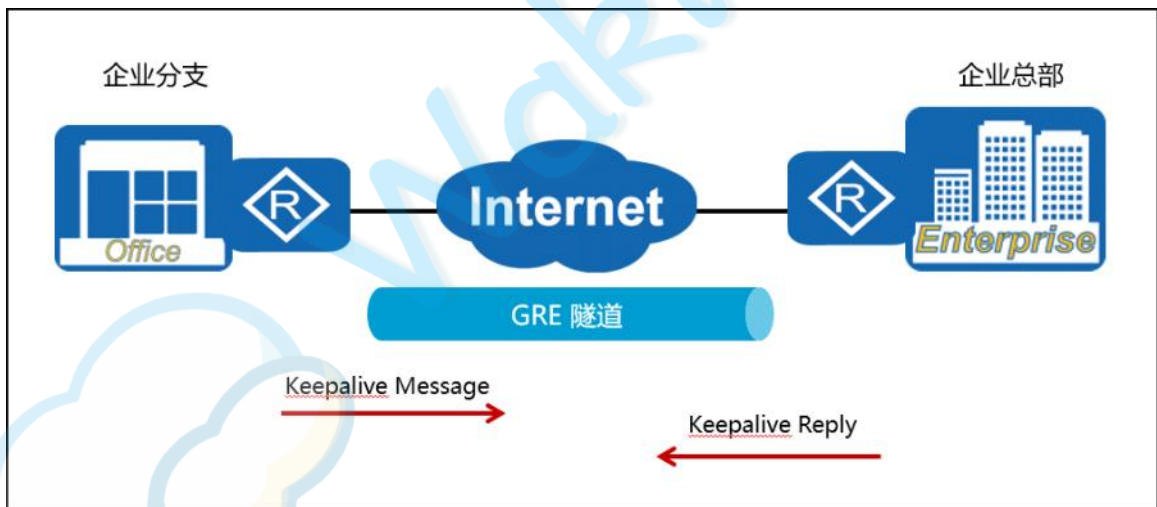
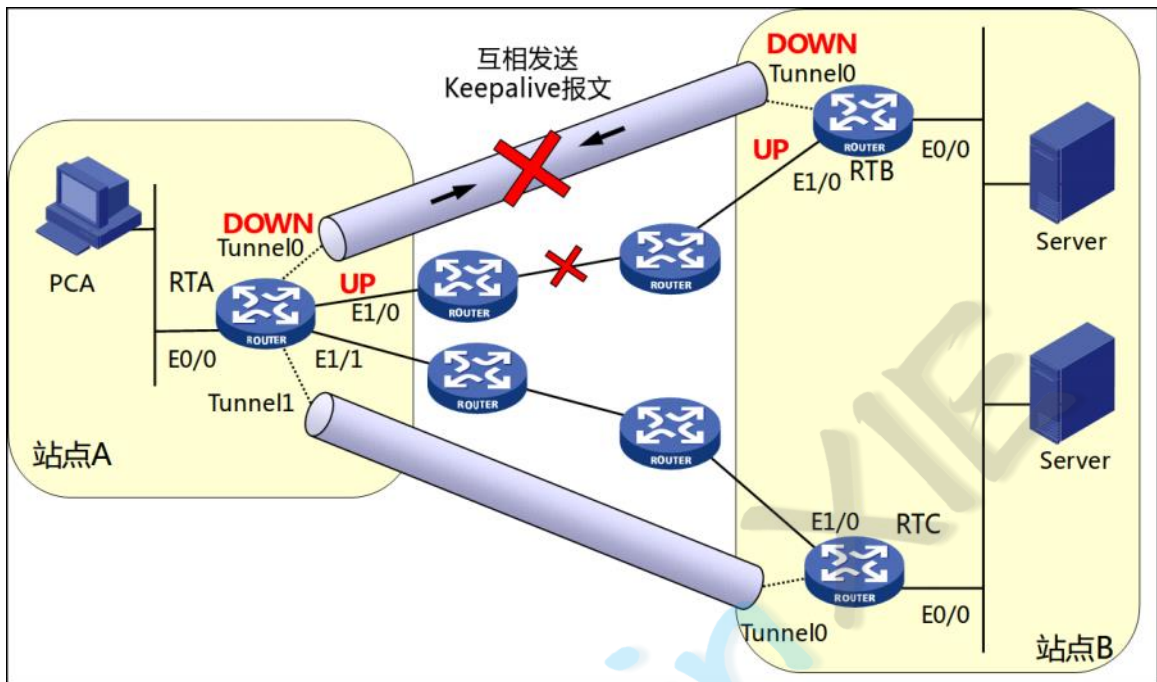


GRE VPN隧道口虚假状态问题: 只要有到达隧道目标的路由, 隧道口即可**激活**

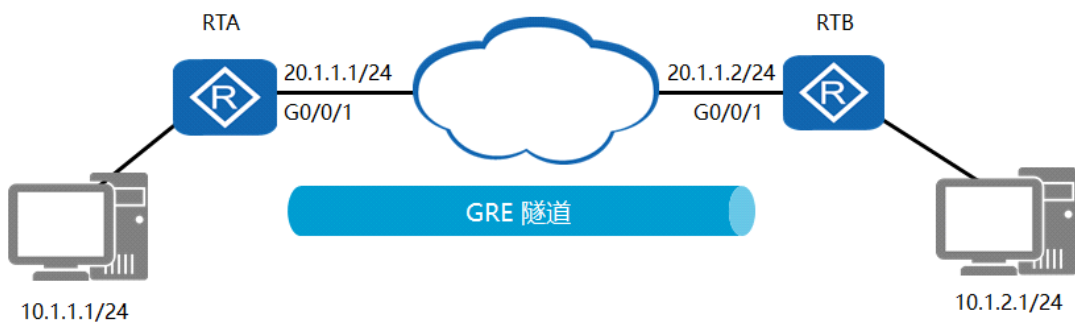
- 解决方法: 开启GRE的**Keepalive**, 用于检测隧道对端是否可达。



By Wakin 安徽肯耐博 禁止传播



配置Keepalive检测



```
[RTA]interface Tunnel 0/0/1
[RTA-Tunnel0/0/1]keepalive period 3
```

By Wakin 安徽肯耐博 禁止传播

```
[RTA]interface Tunnel 0/0/1
[RTA-Tunnel0/0/1]keepalive period 3
[RTA-Tunnel0/0/1]quit
```

配置验证

```
[RTA]display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port, The Maximum Transmit Unit is 1476
Internet Address is 40.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 20.1.1.1 (GigabitEthernet0/0/1), destination 20.1.1.2
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 3 retry-times 3
Checksumming of packets disabled
.....
```