# MSR 系列路由器用 L2TP+IPsec+PPPoE 实现总部和多分支通信配置举例

# 目 录

# 1 简介

本文档介绍 MSR 系列路由器用 L2TP+IPsec+PPPoE 实现总部与多分支通信的典型配置举例。

# 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

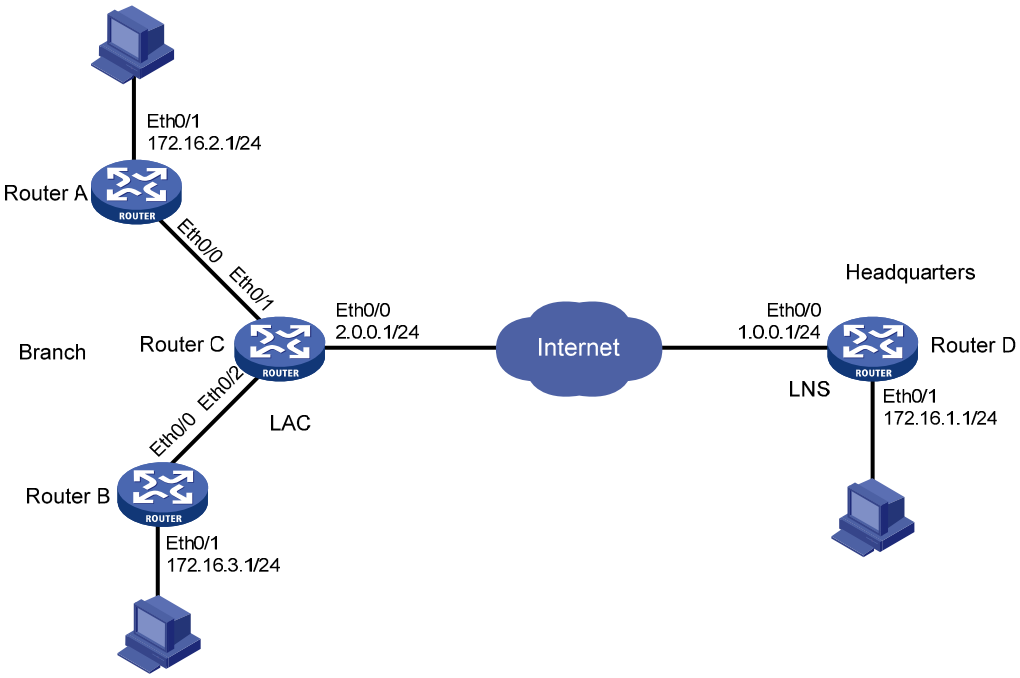
本文档假设您已了解 L2TP、IPsec 和 PPPoE 特性。

# 3 配置举例

## 3.1 组网需求

如 图 1 所示，Router A和Router B是某企业分支网关，Router C为L2TP的LAC，Router D为L2TP的LNS，要求：分支通过PPPoE拨上LAC，并触发LAC和LNS建立L2TP隧道，实现分支和总部的内网可以互访。

图1 MSR 系列路由器用 L2TP+IPsec+PPPoE 实现一总部、多分支式通信配置组网图



## 3.2 配置思路

当拨号成功以后，总部网关 LNS 会给分支网关 client 分配一个 IP 地址，总部 LNS 只会有分支网关的路由，而不会有分支内网的路由，要实现总部内网和分支内网间的通信要在总部配置一条目的地址为分支内网的静态路由，下一条指向分支网关，但是分支网关的 IP 地址是总部 LNS 这边的地址池里面动态分配的，所以下一条无法定义为具体的 IP 地址，只能定义为虚模板。不过这是一总部多分支的组网，所有的 L2TP 连接都是用的同一虚模板，所以无法满足用同一个下一跳地址实现和多个分支的通信。在这种情况下只能在 L2TP 上复用 IPsec 来实现路由功能，在 LNS 的虚接口 virtual-template 上下发 IPsec 策略，不同目的地址的数据流会触发不同的 ACL 来和不同的 IPsec 对等体通信，这样就可以实现一对多的精确路由了。

## 3.3 使用版本

本举例是在 Release 2317 版本上进行配置和验证的。

## 3.4 配置注意事项

- 配置 client 的时候，要配置一条默认路由，下一跳指向 LNS 虚模板的地址。
- 配置 LNS 的安全策略的时候，使用模板，不用配置 ACL。
- 分别在分支网关的拨号口和总部网关（LNS）的虚模板接口上下发安全策略。

## 3.5 配置步骤

### 3.5.1 Router A的配置

# 配置接口 Ethernet0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface ethernet 0/1
[RouterA-Ethernet0/1] ip address 172.16.2.1 255.255.255.0
[RouterA-Ethernet0/1] quit
```

# 配置拨号接口 Dialer0，地址协商获得。

```
[RouterA] dialer-rule 1 ip permit
[RouterA] interface dialer 0
[RouterA-Dialer0] link-protocol ppp
[RouterA-Dialer0] ppp chap user client1@lac
[RouterA-Dialer0] ppp chap password simple 123
[RouterA-Dialer0] ip address ppp-negotiate
[RouterA-Dialer0] dialer user pppoe
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] dialer bundle 1
[RouterA-Dialer0] quit
```

# 在接口 Ethernet0/0 上配置 PPPOE 会话。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] pppoe-client dial-bundle-number 1
[RouterA-Ethernet0/0] quit
```

# 配置默认路由指向 Router D。

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 100.0.0.1
```

# 创建 ACL，定义触发 IPsec 的数据流。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule 0 permit ip source 172.16.2.0 0.0.0.255
[RouterA-acl-adv-3000] quit
```

# 配置 IKE 对等体。

```
[RouterA] ike peer peer
[RouterA-ike-peer-peer] exchange-mode aggressive
[RouterA-ike-peer-peer] pre-shared-key 123
[RouterA-ike-peer-peer] id-type name
[RouterA-ike-peer-peer] remote-name center
[RouterA-ike-peer-peer] remote-address 100.0.0.1
[RouterA-ike-peer-peer] quit
```

# 采用安全提议的缺省配置。

```
[RouterA] ipsec proposal def
```

# 配置 ESP 协议采用 md5 认证算法。

```
[RouterA-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterA-ipsec-transform-set-def] quit
```

# 创建 IPsec 安全策略 policy，其协商方式为 isakmp。

```
[RouterA] ipsec policy policy 1 isakmp
[RouterA-ipsec-policy-isakmp-policy-1] security acl 3000
[RouterA-ipsec-policy-isakmp-policy-1] ike-peer peer
[RouterA-ipsec-policy-isakmp-policy-1] proposal def
[RouterA-ipsec-policy-isakmp-policy-1] quit
```

# 在拨号接口下应用安全策略。

```
[RouterA] interface dialer 0
[RouterA-Dialer0] ipsec policy policy
[RouterA-Dialer0] quit
```

### 3.5.2 Router B的配置

# 配置接口 Ethernet0/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface ethernet 0/1
[RouterB-Ethernet0/1] ip address 172.16.3.1 255.255.255.0
[RouterB-Ethernet0/1] quit
```

# 配置拨号接口 Dialer0，地址协商获得。

```
[RouterB] interface dialer 0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ppp chap user client2@lac
[RouterB-Dialer0] ppp chap password simple 123
[RouterB-Dialer0] ip address ppp-negotiate
[RouterB-Dialer0] dialer user pppoe
[RouterB-Dialer0] dialer-group 1
```

```
[RouterB-Dialer0] dialer bundle 1
[RouterB-Dialer0] quit
```
# 在接口 Ethernet0/0 上配置 PPPoE 会话。
```
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] pppoe-client dial-bundle-number 1
[RouterB-Ethernet0/0] quit
```
# 配置默认路由指向 Router D。
```
[RouterB] ip route-static 0.0.0.0 0.0.0.0 100.0.0.1
```
# 创建 ACL，定义触发 IPsec 的数据流。
```
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule 0 permit ip source 172.16.3.0 0.0.0.255
[RouterB-acl-adv-3000] quit
```
# 配置 IKE 对等体。
```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] exchange-mode aggressive
[RouterB-ike-peer-peer] pre-shared-key 123
[RouterB-ike-peer-peer] id-type name
[RouterB-ike-peer-peer] remote-name center
[RouterB-ike-peer-peer] remote-address 100.0.0.1
[RouterB-ike-peer-peer] quit
```
# 采用安全提议的缺省配置。
```
[RouterB] ipsec proposal def
```
# 配置 ESP 协议采用 md5 认证算法。
```
[RouterB-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterB-ipsec-transform-set-def] quit
```
# 创建 IPsec 安全策略 policy，其协商方式为 isakmp。
```
[RouterB] ipsec policy policy 1 isakmp
[RouterB-ipsec-policy-isakmp-policy-1] security acl 3000
[RouterB-ipsec-policy-isakmp-policy-1] ike-peer peer
[RouterB-ipsec-policy-isakmp-policy-1] proposal def
[RouterB-ipsec-policy-isakmp-policy-1] quit
```
# 在拨号接口下应用安全策略。
```
[RouterB] interface dialer 0
[RouterB-Dialer0] ipsec policy policy
[RouterB-Dialer0] quit
```

### 3.5.3 Router C的配置

# 启用 L2TP 服务。
```
<RouterC> system-view
[RouterC] l2tp enable
```
# 采用 ISP 域的缺省配置。
```
[RouterC] domain lac
```
# 设置一个 L2TP 组，不启用隧道验证。
```
[RouterC] l2tp-group 1
```

```
[RouterC-l2tp1] undo tunnel authentication
```
# 指定 LNS 的地址及发起 L2TP 隧道连接的域名。
```
[RouterC-l2tp1] start l2tp ip 1.0.0.1 domain lac
[RouterC-l2tp1] quit
```
# 创建本地用户，配置用户名、密码及服务类型。
```
[RouterC] local-user client1
[RouterC-luser-client1] password simple 123
[RouterC-luser-client1] service-type ppp
[RouterC-luser-client1] quit
[RouterC] local-user client2
[RouterC-luser-client2] password simple 123
[RouterC-luser-client2] service-type ppp
[RouterC-luser-client2] quit
```
# 配置接口 Ethernet0/0 的 IP 地址。
```
[RouterC] interface ethernet 0/0
[RouterC-Ethernet0/0] ip address 2.0.0.1 255.255.255.0
[RouterC-Ethernet0/0] quit
```
# 配置虚拟模板接口 Virtual-Template0。
```
[RouterC] interface Virtual-Template0
[RouterC-Virtual-Template0] ppp authentication-mode chap domain lac
[RouterC-Virtual-Template0] quit
```
# 在接口下将 PPPoE 服务器与 Virtual-Template0 绑定。
```
[RouterC] interface ethernet 0/1
[RouterC-Ethernet0/1] pppoe-server bind virtual-template 0
[RouterC-Ethernet0/1] quit
```

### 3.5.4 Router D的配置

# 配置接口 Ethernet0/0 的 IP 地址。
```
<RouterD> system-view
[RouterD] interface ethernet 0/0
[RouterD-Ethernet0/0] ip address 1.0.0.1 255.255.255.0
[RouterD-Ethernet0/0] quit
```
# 配置接口 Ethernet0/1 的 IP 地址。
```
[RouterD] interface ethernet 0/1
[RouterC-Ethernet0/1] ip address 172.16.1.1 255.255.255.0
[RouterC-Ethernet0/1] quit
```
# 启用 L2TP 服务。
```
[RouterD] l2tp enable
```
# 采用 ISP 域的缺省配置。
```
[RouterD] domain lac
```
#在域内配置 IP 地址池，用于分配给 client。
```
[RouterD-isp-lac] ip pool 1 100.0.0.2 100.0.0.255
[RouterD-isp-lac] quit
```
# 设置一个 L2TP 组，不启用隧道验证。

```
[RouterD] l2tp-group 1
[RouterD-l2tp1] undo tunnel authentication
```
# 指定接收呼叫的虚拟模板接口。
```
[RouterD-l2tp1] allow l2tp Virtual-Template 0
[RouterD-l2tp1] quit
```
# 配置虚拟模板接口 Virtual-Template0。
```
[RouterD] interface Virtual-Template0
[RouterD-Virtual-Template0] ppp authentication-mode chap domain lac
```
# 指定对端地址为地址池中的地址。
```
[RouterD-Virtual-Template0] remote address pool 1
[RouterD-Virtual-Template0] ip address 100.0.0.1 255.255.255.0
[RouterD-Virtual-Template0] quit
```
# 设置用户名、密码及服务类型。
```
[RouterD] local-user client1
[RouterD-luser-client1] password simple 123
[RouterD-luser-client1] service-type ppp
[RouterD-luser-client1] quit
[RouterD] local-user client2
[RouterD-luser-client2] password simple 123
[RouterD-luser-client2] service-type ppp
[RouterD-luser-client2] quit
```
# 配置一条默认路由来实现和分支内网的互通。
```
[RouterD] ip route-static 0.0.0.0 0.0.0.0 Virtual-Template0
```
# 配置 IKE 对等体。
```
[RouterD] ike peer peer
[RouterD-ike-peer-peer] exchange-mode aggressive
[RouterD-ike-peer-peer] pre-shared-key 123
[RouterD-ike-peer-peer] id-type name
[RouterD-ike-peer-peer] remote-name client
[RouterD-ike-peer-peer] quit
```
# 采用安全提议的缺省配置。
```
[RouterD] ipsec proposal def
```
# 配置 ESP 协议采用 md5 认证算法。
```
[RouterD-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterD-ipsec-transform-set-def] quit
```
# 配置 IPsec 安全策略模板。
```
[RouterD] ipsec policy-template test 1
[RouterD-ipsec-policy-template-test-1] ike-peer peer
[RouterD-ipsec-policy-template-test-1] proposal def
[RouterD-ipsec-policy-template-test-1] quit
```
# 引用 IPsec 安全策略模板创建一条 IPsec 安全策略。
```
[RouterD] ipsec policy policy 1 isakmp template test
```
# 在虚拟模板接口下应用安全策略。
```
[RouterD] interface Virtual-Template0
```

```
[RouterD-Virtual-Template0] ipsec policy policy
[RouterD-Virtual-Template0] quit
```

## 3.6 验证配置

# 可以通过以下显示信息查看 pppoe-client 的拨号情况。以 Router A 为例：

```
<RouterA> display pppoe-client session packet
PPPoE Client Session:
  ID: 1                           Interface: Eth0/0
  InPackets: 125                  OutPackets: 124
  InBytes:   1300                 OutBytes:   1287
  InDrops:   0                    OutDrops:   0
```

# 可以通过以下显示信息查看 LAC 端的 pppoe-server 的拨号情况。

```
<RouterC> display pppoe-server session packet
Total PPPoE Session(s): 1

SID   Intf        InP      InO      InD   OutP     OutO     OutD
1     Eth0/1      176      1807     0     177      1820     0
```

# 可以通过以下显示查看 LAC 端的 L2TP 会话信息。

```
<RouterC> display l2tp session
 Total session = 1

 LocalSID  RemoteSID  LocalTID
  4163      27245      1
<RouterC> display l2tp tunnel
 Total tunnel = 1

 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         1.0.0.1          1701   1        LAC
```

# 可以通过以下显示查看 LNS 端的 L2TP 会话信息。

```
<RouterD> display l2tp session
 Total session = 1

 LocalSID  RemoteSID  LocalTID
  27245     4163       1
<RouterD> display l2tp tunnel
 Total tunnel = 1

 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         1.0.0.2          1701   1        PE1
```

# 可以通过如下信息看到 LNS 侧可以 ping 通分支内网。

```
<RouterD> ping 172.16.2.1
  PING 172.16.2.1: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.1: bytes=56 Sequence=0 ttl=255 time=5 ms
    Reply from 172.16.2.1: bytes=56 Sequence=1 ttl=255 time=4 ms
    Reply from 172.16.2.1: bytes=56 Sequence=2 ttl=255 time=4 ms
```

```
    Reply from 172.16.2.1: bytes=56 Sequence=3 ttl=255 time=5 ms
    Reply from 172.16.2.1: bytes=56 Sequence=4 ttl=255 time=5 ms

  --- 172.16.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/5 ms
```

# 可以在 Router A、Router B 和 Router D 上通过 display ike sa 和 display ipsec sa 查看 IPsec 建立情况。

## 3.7 配置文件

- Router A：

```
#
acl number 3000
 rule 0 permit ip source 172.16.2.0 0.0.0.255
#
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher $c$3$ABcQkUeBtve6rmSB0B0ej62294PnNg==
 id-type name
 remote-name center
 remote-address 100.0.0.1
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy policy 1 isakmp
 security acl 3000
 ike-peer peer
 transform-set def
#
interface Dialer0
 link-protocol ppp
 ppp chap user client1@lac
 ppp chap password cipher $c$3$oD09I72nb4O+rIS4MUZeDWnHcnOVrRBZ
 ip address ppp-negotiate
 dialer user pppoe
 dialer-group 1
 dialer bundle 1
 ipsec policy policy
#
interface Ethernet0/1
 port link-mode route
 ip address 172.16.2.1 255.255.255.0
```

```
#
interface Ethernet0/0
 port link-mode route
 pppoe-client dial-bundle-number 1
#
ip route-static 0.0.0.0 0.0.0.0 100.0.0.1
#
dialer-rule 1 ip permit
#
```

- Router B：

```
#
acl number 3000
 rule 0 permit ip source 172.16.3.0 0.0.0.255
#
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher $c$3$JVGo5rF3xFKO593n6VAFZgE1W7/8Lg==
 id-type name
 remote-name center
 remote-address 100.0.0.1
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy policy 1 isakmp
 security acl 3000
 ike-peer peer
 transform-set def
#
interface Dialer0
 link-protocol ppp
 ppp chap user client2@lac
 ppp chap password cipher $c$3$Zs7w3agJP+iRRBOJicxAdT3AAb4yWLbq
 ip address ppp-negotiate
 dialer user pppoe
 dialer-group 1
 dialer bundle 1
 ipsec policy policy
#
interface Ethernet0/1
 port link-mode route
 ip address 172.16.3.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
 pppoe-client dial-bundle-number 1
```

```
#
ip route-static 0.0.0.0 0.0.0.0 100.0.0.1
#
dialer-rule 1 ip permit
#
```

- Router C：

```
#
 l2tp enable
#
domain lac
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
local-user client1
 password cipher $c$3$8jQGCiqZMOmOQRpUmF/t+gqLoAsQ4Q==
 service-type ppp
local-user client2
 password cipher $c$3$Flsg/8txuG+/nqXjFIj0OwZzgbw6gg==
 service-type ppp
#
l2tp-group 1
 undo tunnel authentication
 start l2tp ip 1.0.0.1 domain lac
#
interface Ethernet0/0
 port link-mode route
 ip address 2.0.0.1 255.255.255.0
#
interface Ethernet0/1
 port link-mode route
 pppoe-server bind Virtual-Template 0
#
interface Virtual-Template0
 ppp authentication-mode chap domain lac
#
```

- Router D：

```
#
 l2tp enable
#
domain lac
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 1 100.0.0.2 100.0.0.255
#
```

```
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher $c$3$f188ftJE8sP8Lu4BXu+DJHn5r4chOw==
 id-type name
 remote-name client
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy-template test 1
 ike-peer peer
 transform-set def
#
ipsec policy policy 1 isakmp template test
#
local-user client1
 password cipher $c$3$y+FUsYxFVXcTi6eKsHzJZvkdlAdImg==
 service-type ppp
local-user client2
 password cipher $c$3$JEThVTG4MBHbr18/Wvx3/cC5/6ipCw==
 service-type ppp
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 0
#
interface Ethernet0/0
 port link-mode route
 ip address 1.0.0.1 255.255.255.0
#
interface Virtual-Template0
 ppp authentication-mode chap domain lac
 remote address pool 1
 ip address 100.0.0.1 255.255.255.0
 ipsec policy policy
#
ip route-static 0.0.0.0 0.0.0.0 Virtual-Template0
#
```

# 4 相关资料

- H3C MSR 系列路由器 命令参考(V5)-R2311
- H3C MSR 系列路由器 配置指导(V5)-R2311