

H3C MSR 系列路由器 配置举例一本通(命令行)

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

前言

本手册介绍了产品综合配置举例和典型配置举例。

前言部分包含如下内容：

- [读者对象](#)
- [特别申明](#)
- [本书约定](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

特别申明

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，请以设备实际情况为准。

本文中的内容为通用性技术信息，某些信息可能不适用于您所购买的产品。

本书约定

1. 命令行格式约定






格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项中选择一个或者不选。
{ x y ... }*	表示从多个选项中至少选取一个。
[x y ...]*	表示从多个选项中选择一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
<>	带尖括号“<>”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。





3. 各类标志





本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。

	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

H3C MSR 系列路由器

作为 TFTP client 升级版本配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	1
3.4 配置注意事项.....	1
3.5 配置步骤.....	2
3.5.1 Host 的配置.....	2
3.5.2 Router 的配置.....	2
3.6 验证配置.....	3
3.7 配置文件.....	5
4 相关资料.....	5

1 简介

本文档介绍使用 TFTP 方式升级集中式路由器软件版本的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 TFTP 的特性。

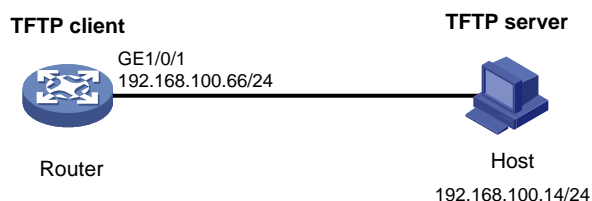
3 配置举例

3.1 组网需求

如[图 1](#)所示，Host 连接 Router 的 GigabitEthernet1/0/1 接口，Router 作为 TFTP 客户端，Host 作为 TFTP 服务器。

现要求：通过 TFTP 方式为 Router 升级软件版本。

图1 配置组网图



3.2 配置思路

为了使路由器在重启后使用新版本软件，需要指定下次启动时所用的主用启动文件为升级后的软件版本。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 当设备剩余的存储空间不够，请使用 `delete /unreserved file-url` 命令删除部分暂时不用的文件后再执行升级软件操作。

- 软件升级时需要重启设备，建议使用 **save** 命令保存设备的当前配置。

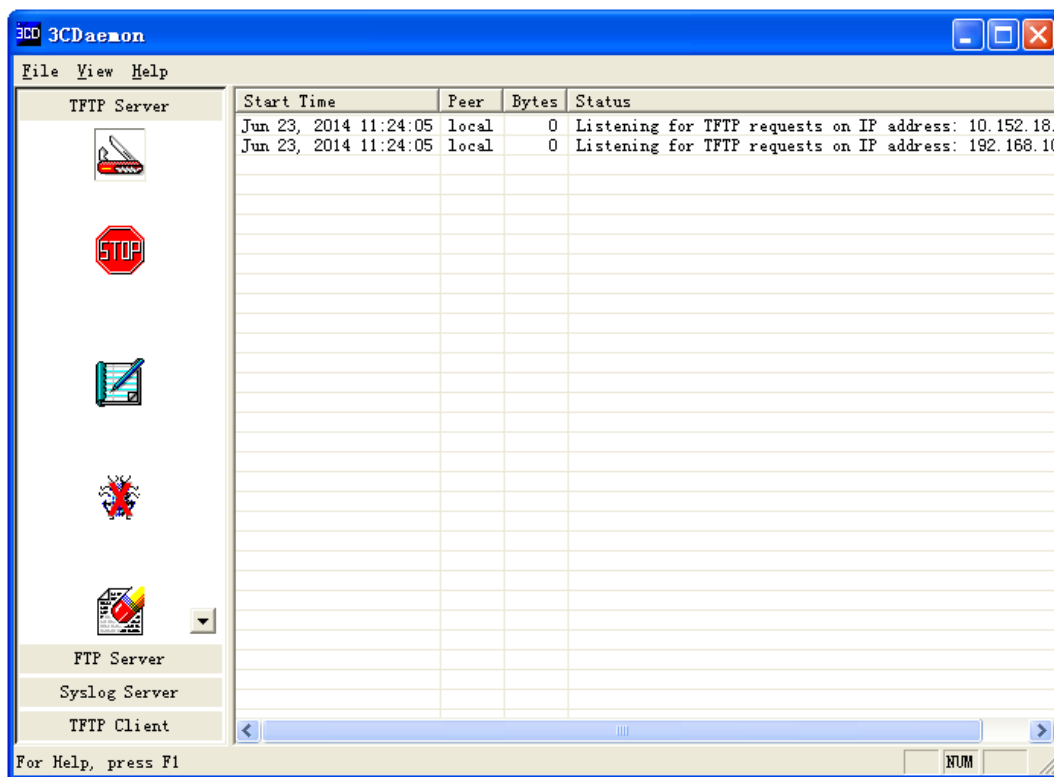
3.5 配置步骤

3.5.1 Host 的配置

配置 Host 的 IP 地址为 192.168.100.14/24，使得与 Router 路由可达，具体配置方法略。

启动 Host 上的 TFTP 服务器（以 3CDaemon 软件为例），设置 TFTP 服务器下载路径等参数，并开启服务。

图2 配置 TFTP 服务器



3.5.2 Router 的配置

配置 Router 接口 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.100.66 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
[Router] quit
```

在 Router ping TFTP 服务器地址，能够 ping 通。

```
<Router> ping 192.168.100.14
PING 192.168.100.14: 56 data bytes, press CTRL_C to break
Reply from 192.168.100.14: bytes=56 Sequence=0 ttl=128 time=2 ms
Reply from 192.168.100.14: bytes=56 Sequence=1 ttl=128 time=1 ms
```



```
Reply from 192.168.100.14: bytes=56 Sequence=2 ttl=128 time=1 ms
Reply from 192.168.100.14: bytes=56 Sequence=3 ttl=128 time=1 ms
Reply from 192.168.100.14: bytes=56 Sequence=4 ttl=128 time=1 ms
```

```
--- 192.168.100.14 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/2 ms
```

将 TFTP 服务器上的 **msr36.ipe** 文件下载到路由器上，以缺省文件名 **msr36.ipe** 保存。

```
<Router> tftp 192.168.100.14 get msr36.ipe
 % Total      % Received % Xferd  Average Speed   Time    Time     Time  Current
                               Dload  Upload  Total   Spent    Left   Speed
100 58.7M  100 58.7M    0     0 1193k      0  0:00:50  0:00:50  --:--:-- 1127k
```

指定 Router 下次启动时所用的主用启动文件为 **msr36.ipe**。

```
<Router> boot-loader file cfa0:/msr36.ipe main
Verifying the IPE file and the images....Done.
H3C MSR36-40 images in IPE:
  msr36-cmw710-boot-r0106.bin
  msr36-cmw710-system-r0106.bin
  msr36-cmw710-security-r0106.bin
  msr36-cmw710-voice-r0106.bin
  msr36-cmw710-data-r0106.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to the device.
Decompressing file msr36-cmw710-boot-r0106.bin to
cfa0:/msr36-cmw710-boot-r0106.bin.....Done.
Decompressing file msr36-cmw710-system-r0106.bin to
cfa0:/msr36-cmw710-system-r0106.bin.....Done.
Decompressing file msr36-cmw710-security-r0106.bin to
cfa0:/msr36-cmw710-security-r0106.bin...Done.
Decompressing file msr36-cmw710-voice-r0106.bin to
cfa0:/msr36-cmw710-voice-r0106.bin...Done.
Decompressing file msr36-cmw710-data-r0106.bin to
cfa0:/msr36-cmw710-data-r0106.bin...Done.
The images that have passed all examinations will be used as the main startup software images at the next reboot on the device.
```

指定 Router 的备用主控板下次启动时所用的备用启动文件为 **msr36-old.ipe**。

```
<Router> boot-loader file cfa0:/msr36-old.ipe backup
This command will set the backup startup software images. Continue? [Y/N]:y
The images that have passed all examinations will be used as the backup startup software images at the next reboot.
```

重启设备。

```
<Router> reboot
```

3.6 验证配置

设备重启后，使用 **display version** 命令查看设备版本信息。

```

<Router> display version
H3C Comware Software, Version 7.1.049, Release 0106
Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C MSR36-40 uptime is 0 weeks, 0 days, 0 hours, 2 minutes
Last reboot reason : User reboot
Boot image: cfa0:/msr36-cmw710-boot-r0106.bin
Boot image version: 7.1.049P04, Release 0106
  Compiled Feb 08 2014 17:43:51
System image: cfa0:/msr36-cmw710-system-r0106.bin
System image version: 7.1.049, Release 0106
  Compiled Feb 08 2014 17:43:51
Feature image(s) list:
  cfa0:/msr36-cmw710-security-r0106.bin, version: 7.1.049
    Compiled Feb 08 2014 17:44:41
  cfa0:/msr36-cmw710-voice-r0106.bin, version: 7.1.049
    Compiled Feb 08 2014 17:44:42
  cfa0:/msr36-cmw710-data-r0106.bin, version: 7.1.049
    Compiled Feb 08 2014 17:44:44

CPU ID: 0x2
2G bytes DDR3 SDRAM Memory
8M bytes Flash Memory
PCB          Version: 2.0
CPLD         Version: 2.0
Basic   BootWare Version: 1.20
Extended BootWare Version: 1.20
[SLOT 0]AUX          (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]GE1/0/1      (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]GE1/0/2      (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]GE1/0/3      (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]CELLULAR0/0  (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]CELLULAR0/1  (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 2]SIC-4FSW     (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 6]HMIM-4GEE    (Hardware)2.0, (Driver)1.0, (CPLD)0.0
[SLOT 8]HMIM-2SAE    (Hardware)3.0, (Driver)1.0, (CPLD)4.0

```

显示本次启动和下次启动所采用的启动软件包的名称。

```

<Router> display boot-loader
Software images on the device:
Current software images:
  cfa0:/msr36-cmw710-boot-r0106.bin
  cfa0:/msr36-cmw710-system-r0106.bin
  cfa0:/msr36-cmw710-security-r0106.bin
  cfa0:/msr36-cmw710-voice-r0106.bin
  cfa0:/msr36-cmw710-data-r0106.bin
Main startup software images:
  cfa0:/msr36-cmw710-boot-r0106.bin
  cfa0:/msr36-cmw710-system-r0106.bin
  cfa0:/msr36-cmw710-security-r0106.bin

```

```
cfa0:/msr36-cmw710-voice-r0106.bin
cfa0:/msr36-cmw710-data-r0106.bin
Backup startup software images:
cfa0:/msr36-cmw710-boot-r000703.bin
cfa0:/msr36-cmw710-system-r000703.bin
cfa0:/msr36-cmw710-security-r000703.bin
cfa0:/msr36-cmw710-voice-r000703.bin
cfa0:/msr36-cmw710-data-r000703.bin
```

3.7 配置文件

```
#
interface gigabitethernet1/0/1
 port link-mode route
 ip address 192.168.100.66 255.255.255.0
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“基础配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“基础配置命令参考”

H3C MSR 系列路由器

作为 FTP client 升级软件版本配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	1
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.5.1 Host 的配置.....	2
3.5.2 Router 的配置.....	3
3.6 验证配置.....	5
3.7 配置文件.....	7
4 相关资料.....	7

1 简介

本文档介绍使用 FTP 方式升级分布式路由器软件版本的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 FTP 的特性。

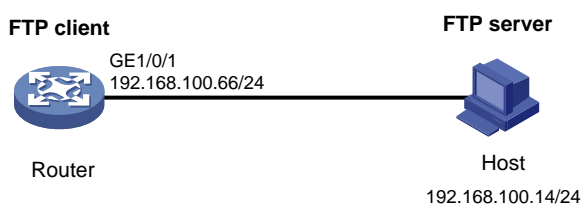
3 配置举例

3.1 组网需求

如图 1 所示，主机 Host 连接 Router 的 GigabitEthernet1/0/1 接口，Router 作为 FTP 客户端，Host 作为 FTP 服务器。现要求：

- 通过 FTP 方式为 Router 升级软件版本，将存储在 FTP 服务器上的文件 msr56.ipe 下载到 FTP 客户端。
- 配置 FTP 客户端登录 FTP 服务器的用户名为 123456，密码为 123456。

图1 配置组网图



3.2 配置思路

- 为了使设备的主用主控板和备用主控板都能够升级版本，在使用 FTP 方式将软件版本 get 到主用主控板后，需要将软件版本复制到备用主控板的根目录下，主用主控板和备用主控板都进行升级。
- 为了使路由器在重启后使用新软件版本，需要指定下次启动时所用的主用启动文件为升级后的软件版本。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 当设备剩余的内存空间不够，请使用 `delete /unreserved file-url` 命令删除部分暂时不用的文件后再执行升级软件操作。
- 确保主机和 Router 的 FTP 用户名、密码及文件名等参数保持一致。

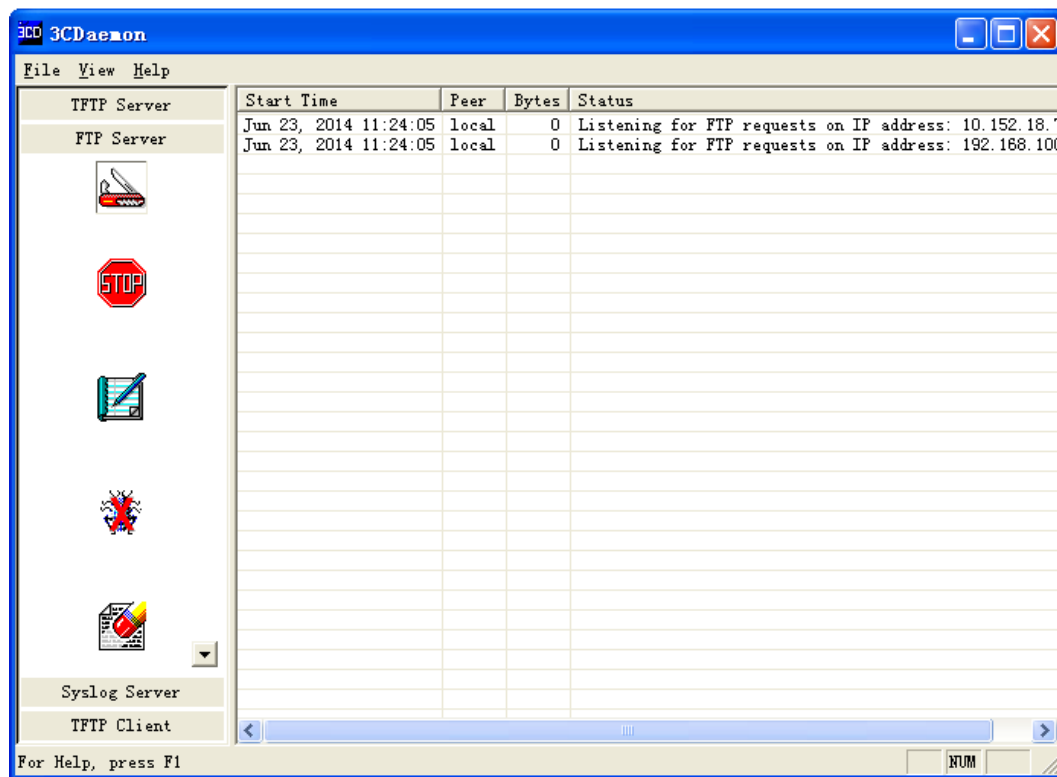
3.5 配置步骤

3.5.1 Host 的配置

配置 Host 的 IP 地址为 192.168.100.14/24，使得与 Router 路由可达，具体配置方法略。

启动 Host 上的 FTP 服务器（以 3CDaemon 软件为例）。

图2 配置 FTP 服务器



配置 FTP 服务器参数。



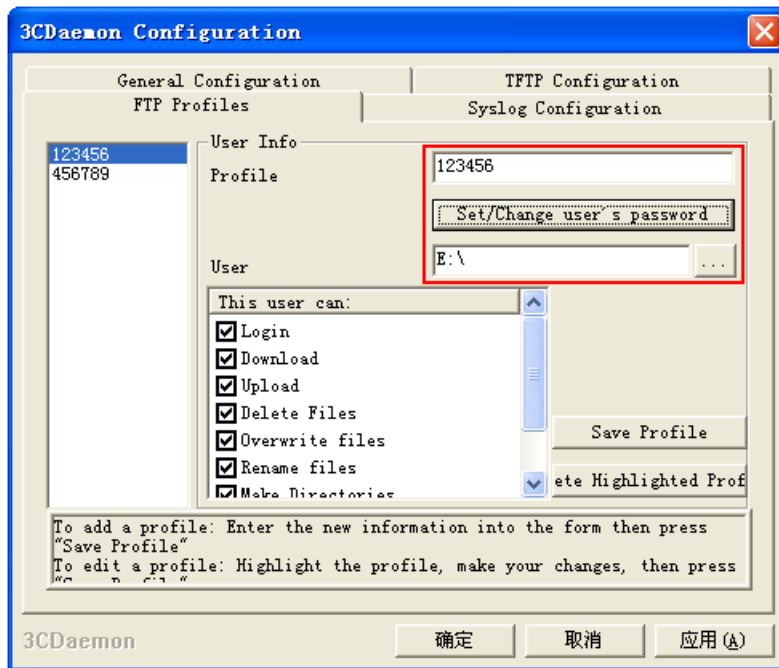
- 单击  按钮；
- 配置 FTP 用户名为 123456；
- 单击 “Set/Change user's password” 按钮，配置 FTP 密码为 123456；
- 单击 ，设置 FTP 服务器下载路径；
- 单击 “确定” 并保存。

图3 配置 FTP 服务器参数



3.5.2 Router 的配置

配置 Router 接口 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.100.66 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
[Router] quit
```

在 Router 上 ping FTP 服务器地址，能够 ping 通。

```
<Router> ping 192.168.100.14
PING 192.168.100.14: 56 data bytes, press CTRL_C to break
  Reply from 192.168.100.14: bytes=56 Sequence=0 ttl=128 time=2 ms
  Reply from 192.168.100.14: bytes=56 Sequence=1 ttl=128 time=1 ms
  Reply from 192.168.100.14: bytes=56 Sequence=2 ttl=128 time=1 ms
  Reply from 192.168.100.14: bytes=56 Sequence=3 ttl=128 time=1 ms
  Reply from 192.168.100.14: bytes=56 Sequence=4 ttl=128 time=1 ms

--- 192.168.100.14 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/2 ms
```

以用户名 123456、密码 123456 登录 FTP 服务器。

```
<Router> ftp 192.168.100.14
Connected to 192.168.100.14 (192.168.100.14).
220 3Com 3C Daemon FTP Server Version 2.0
```



```

User (192.168.100.14:(none)): 123456
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
# 将文件 msr56.ipe 从 FTP 服务器下载到 Router 的主用主控板。
ftp> get msr56.ipe
227 Entering passive mode (192,168,100,14,8,86)
125 Using existing data connection
226 Closing data connection; File transfer successful.
70445056 bytes received in 53.6 seconds (1.25 Mbyte/s)
ftp> quit
# 将 Router 主用主控板的文件 msr56.ipe 拷贝到备用主控板的根目录下
<Router> copy cfa0:/msr56.ipe slot1#cfa0:/msr56.ipe
Copy cfa0:/msr56.ipe to slot1#cfa0:/msr56.ipe[Y/N]:y
Copying file cfa0:/msr56.ipe to slot1#cfa0:/msr56.ipe.
..... Done.
# 指定 Router 的主用主控板下次启动时所用的主用启动文件为 msr56.ipe。
<Router> boot-loader file cfa0:/msr56.ipe slot 0 main
Verifying the IPE file and the images.....Done.
H3C MSR56-60 images in IPE:
  msr56-cmw710-boot-r0106.bin
  msr56-cmw710-system-r0106.bin
  msr56-cmw710-security-r0106.bin
  msr56-cmw710-voice-r0106.bin
  msr56-cmw710-data-r0106.bin
This command will set the main startup software images. Continue? [Y/N]:Y
Add images to slot 0.
Decompressing file msr56-cmw710-boot-r0106.bin to
cfa0:/msr56-cmw710-boot-r0106.bin.....Done.
Decompressing file msr56-cmw710-system-r0106.bin to
cfa0:/msr56-cmw710-system-r0106.bin.....Done.
Decompressing file msr56-cmw710-security-r0106.bin to
cfa0:/msr56-cmw710-security-r0106.bin...Done.
Decompressing file msr56-cmw710-voice-r0106.bin to
cfa0:/msr56-cmw710-voice-r0106.bin...Done.
Decompressing file msr56-cmw710-data-r0106.bin to
cfa0:/msr56-cmw710-data-r0106.bin...Done.
The images that have passed all examinations will be used as the main startup software images
at the next reboot on slot 0.
# 指定 Router 的主用主控板下次启动时所用的备用启动文件为 msr56-old.ipe。
<Router> boot-loader file slot1#cfa0:/msr56-old.ipe slot 0 backup
This command will set the backup startup software images. Continue? [Y/N]:y
The images that have passed all examinations will be used as the backup startup
software images at the next reboot on slot 0.
# 指定 Router 的备用主控板下次启动时所用的主用启动文件为 msr56.ipe。
<Router> boot-loader file slot1#cfa0:/msr56.ipe slot 1 main

```

```

Verifying the IPE file and the images.....Done.
H3C MSR56-60 images in IPE:
  msr56-cmw710-boot-r0106.bin
  msr56-cmw710-system-r0106.bin
  msr56-cmw710-security-r0106.bin
  msr56-cmw710-voice-r0106.bin
  msr56-cmw710-data-r0106.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
Decompressing file msr56-cmw710-boot-r0106.bin to
slot1#cfa0:/msr56-cmw710-boot-r0106.bin.....Done.
Decompressing file msr56-cmw710-system-r0106.bin to
slot1#cfa0:/msr56-cmw710-system-r0106.bin.....
..Done.
Decompressing file msr56-cmw710-security-r0106.bin to
slot1#cfa0:/msr56-cmw710-security-r0106.bin...Done.
Decompressing file msr56-cmw710-voice-r0106.bin to
slot1#cfa0:/msr56-cmw710-voice-r0106.bin...Done.
Decompressing file msr56-cmw710-data-r0106.bin to
slot1#cfa0:/msr56-cmw710-data-r0106.bin...Done.
The images that have passed all examinations will be used as the main startup software images
at the next reboot on slot 1.
# 指定 Router 的备用主控板下次启动时所用的备用启动文件为 msr56-old.ipe。
<Router> boot-loader file slot1#cfa0:/msr56-old.ipe slot 1 backup
This command will set the backup startup software images. Continue? [Y/N]:y
The images that have passed all examinations will be used as the backup startup
software images at the next reboot on slot 1.
# 重启设备。
<Router> reboot

```

3.6 验证配置

```

# 设备重启后，使用 display version 命令查看设备版本信息。
<Router> display version
H3C Comware Software, Version 7.1.049, Release 0106
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C MSR56-60 uptime is 0 weeks, 0 days, 0 hours, 3 minutes
Last reboot reason : User reboot
Boot image: cfa0:/msr56-cmw710-boot-r0106.bin
Boot image version: 7.1.049P03, Release 0106
  Compiled Jan 15 2014 19:27:12
System image: cfa0:/msr56-cmw710-system-r0106.bin
System image version: 7.1.049, Release 0106
  Compiled Jan 15 2014 19:27:12
Feature image(s) list:
  cfa0:/msr56-cmw710-security-r0106.bin, version: 7.1.049
    Compiled Jan 15 2014 19:28:36
  cfa0:/msr56-cmw710-voice-r0106.bin, version: 7.1.049
    Compiled Jan 15 2014 19:28:37

```

```
cfa0:/msr56-cmw710-data-r0106.bin, version: 7.1.049
Compiled Jan 15 2014 19:28:39
```

.....略.....

显示设备主用主控板本次启动和下次启动所采用的启动软件包的名称。

```
<Router> display boot-loader slot 0
Software images on slot 0:
Current software images:
cfa0:/msr56-cmw710-boot-r0106.bin
cfa0:/msr56-cmw710-system-r0106.bin
cfa0:/msr56-cmw710-security-r0106.bin
cfa0:/msr56-cmw710-voice-r0106.bin
cfa0:/msr56-cmw710-data-r0106.bin
Main startup software images:
cfa0:/msr56-cmw710-boot-r0106.bin
cfa0:/msr56-cmw710-system-r0106.bin
cfa0:/msr56-cmw710-security-r0106.bin
cfa0:/msr56-cmw710-voice-r0106.bin
cfa0:/msr56-cmw710-data-r0106.bin
Backup startup software images:
cfa0:/msr56-cmw710-boot-r000703.bin
cfa0:/msr56-cmw710-system-r000703.bin
cfa0:/msr56-cmw710-security-r000703.bin
cfa0:/msr56-cmw710-voice-r000703.bin
cfa0:/msr56-cmw710-data-r000703.bin
```

显示设备备用主控板本次启动和下次启动所采用的启动软件包的名称。

```
<Router> display boot-loader slot 1
Software images on slot 1:
Current software images:
cfa0:/msr56-cmw710-boot-r0106.bin
cfa0:/msr56-cmw710-system-r0106.bin
cfa0:/msr56-cmw710-security-r0106.bin
cfa0:/msr56-cmw710-voice-r0106.bin
cfa0:/msr56-cmw710-data-r0106.bin
Main startup software images:
cfa0:/msr56-cmw710-boot-r0106.bin
cfa0:/msr56-cmw710-system-r0106.bin
cfa0:/msr56-cmw710-security-r0106.bin
cfa0:/msr56-cmw710-voice-r0106.bin
cfa0:/msr56-cmw710-data-r0106.bin
Backup startup software images:
cfa0:/msr56-cmw710-boot-r000703.bin
cfa0:/msr56-cmw710-system-r000703.bin
cfa0:/msr56-cmw710-security-r000703.bin
cfa0:/msr56-cmw710-voice-r000703.bin
cfa0:/msr56-cmw710-data-r000703.bin
```

3.7 配置文件

```
#  
interface gigabitethernet1/0/1  
  port link-mode route  
  ip address 192.168.100.66 255.255.255.0  
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“基础配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“基础配置命令参考”

H3C MSR 系列路由器

作为 FTP server 升级软件版本配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	2
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.5.1 Router 上配置 FTP 服务器.....	2
3.5.2 Host 的配置.....	2
3.5.3 Router 上配置启动文件.....	3
3.6 验证配置.....	4
3.7 配置文件.....	6
4 相关资料.....	6

1 简介

本文档介绍使用 FTP 方式升级分布式路由器软件版本的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 FTP 的特性。

3 配置举例

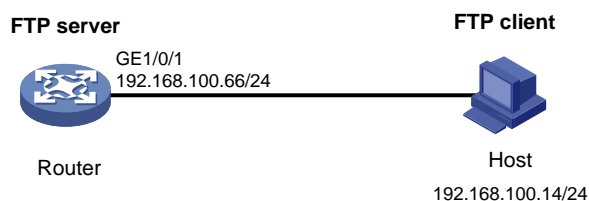
3.1 组网需求

如[图 1](#)所示，主机 Host 连接 Router 的 GigabitEthernet1/0/1 接口，Router 作为 FTP 服务器，Host 作为 FTP 客户端。

现要求：

- 通过 FTP 方式为 Router 升级软件版本，将存储在 FTP 客户端上的文件 msr56.ipe 上传到 FTP 服务器。
- 配置 FTP 客户端登录 FTP 服务器的用户名为 abc，密码为 123456。

图1 配置组网图



3.2 配置思路

- 为了使设备的主用主控板和备用主控板都能够升级版本，在使用 FTP 方式将软件版本 put 到主用主控板后，需要将软件版本复制到备用主控板的根目录下，主用主控板和备用主控板都进行升级。
- 为了使路由器在重启后使用新软件版本，需要指定下次启动时所用的主用启动文件为升级后的软件版本。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 当设备剩余的内存空间不够，请使用 `delete /unreserved file-url` 命令删除部分暂时不用的文件后再执行升级软件操作。
- 确保主机和 Router 的 FTP 用户名、密码及文件名等参数保持一致。
- 在 Router 和主机之间进行 FTP 传输，需要选择 `binary` 方式传输文件。

3.5 配置步骤

3.5.1 Router 上配置 FTP 服务器

配置 Router 接口 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.100.66 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
```

在 Router 上添加一个 FTP 用户 `abc`，并设置其认证密码为 `123456`。

```
[Router] local-user abc
[Router-luser-abc] password simple 123456
```

配置用户角色为 `network-admin`。

```
[Router-luser-abc] authorization-attribute user-role network-admin
```

为保证 FTP 用户仅使用授权的用户角色 `network-admin`，删除缺省用户角色 `network-operator`。

```
[Router-luser-abc] undo authorization-attribute user-role network-operator
```

配置服务类型为 `FTP`。

```
[Router-luser-abc] service-type ftp
[Router-luser-abc] quit
```

启动 Router 的 FTP 服务功能。

```
[Router] ftp server enable
[Router] quit
```

3.5.2 Host 的配置

配置主机 Host 的 IP 地址为 `192.168.100.14/24`，使得到 Router 路由可达，具体配置方法略。

从 FTP client 登录 FTP server，本例以 Windows 命令提示符界面为例。

```
C:\Documents and Settings\Administrator> ftp 192.168.100.66
Connected to 192.168.100.66.
220 FTP service ready.
```

以用户名 `abc`、密码 `123456` 登录 FTP 服务器。

```
User (192.168.100.66:(none)): abc
331 Password required for abc.
Password:
```



```

230 User logged in.
# 使用 lcd 命令，将 FTP 客户端本地的工作路径切换到软件版本所在的目录下。
ftp> lcd E:\
Local directory now E:\
# 将传输模式设置为 binary 方式。
ftp> binary
200 TYPE is now 8-bit binary
# 将本地 msr56.ipe 文件上传到 FTP 服务器上，缺省以文件名 msr56.ipe 保存。
ftp> put msr56.ipe
200 PORT command successful
150 Connecting to port 2903
226 File successfully transferred
ftp: 发送 70445056 字节，用时 1.05Seconds 67282.77Kbytes/sec.
# 使用 ls 命令查看 FTP 服务器上是否有文件。
ftp> ls msr56.ipe
200 PORT command successful
150 Connecting to port 3391
msr56.ipe
226 1 matches total
ftp: 收到 24 字节，用时 0.00Seconds 24000.00Kbytes/sec.
# 终止与 FTP 服务器的连接，并退回到用户视图。
ftp> bye

```

3.5.3 Router 上配置启动文件

```

# 将 Router 主用主控板的文件 msr56.ipe 拷贝到备用主控板的根目录下。
<Router> copy cfa0:/msr56.ipe slot1#cfa0:/msr56.ipe
Copy cfa0:/msr56.ipe to slot1#cfa0:/msr56.ipe[Y/N]:y
Copying file cfa0:/msr56.ipe to slot1#cfa0:/msr56.ipe.
..... Done.
# 指定 Router 的主用主控板下次启动时所用的主用启动文件为 msr56.ipe。
<Router> boot-loader file cfa0:/msr56.ipe slot 0 main
Verifying the IPE file and the images.....Done.
H3C MSR56-60 images in IPE:
  msr56-cmw710-boot-r0106.bin
  msr56-cmw710-system-r0106.bin
  msr56-cmw710-security-r0106.bin
  msr56-cmw710-voice-r0106.bin
  msr56-cmw710-data-r0106.bin
This command will set the main startup software images. Continue? [Y/N]:Y
Add images to slot 0.
Decompressing file msr56-cmw710-boot-r0106.bin to
cfa0:/msr56-cmw710-boot-r0106.bin.....Done.
Decompressing file msr56-cmw710-system-r0106.bin to
cfa0:/msr56-cmw710-system-r0106.bin.....Done.
Decompressing file msr56-cmw710-security-r0106.bin to
cfa0:/msr56-cmw710-security-r0106.bin...Done.

```

```
Decompressing file msr56-cmw710-voice-r0106.bin to
cfa0:/msr56-cmw710-voice-r0106.bin...Done.
Decompressing file msr56-cmw710-data-r0106.bin to
cfa0:/msr56-cmw710-data-r0106.bin...Done.
The images that have passed all examinations will be used as the main startup software images
at the next reboot on slot 0.
```

指定 Router 的主用主控板下次启动时所用的备用启动文件为 **msr56-old.ipe**。

```
<Router> boot-loader file slot1#cfa0:/msr56-old.ipe slot 0 backup
This command will set the backup startup software images. Continue? [Y/N]:y
The images that have passed all examinations will be used as the backup startup
software images at the next reboot on slot 0.
```

指定 Router 的备用主控板下次启动时所用的主用启动文件为 **msr56.ipe**。

```
<Router> boot-loader file slot1#cfa0:/msr56.ipe slot 1 main
Verifying the IPE file and the images.....Done.
```

```
H3C MSR56-60 images in IPE:
  msr56-cmw710-boot-r0106.bin
  msr56-cmw710-system-r0106.bin
  msr56-cmw710-security-r0106.bin
  msr56-cmw710-voice-r0106.bin
  msr56-cmw710-data-r0106.bin
```

```
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
```

```
Decompressing file msr56-cmw710-boot-r0106.bin to
slot1#cfa0:/msr56-cmw710-boot-r0106.bin.....Done.
Decompressing file msr56-cmw710-system-r0106.bin to
slot1#cfa0:/msr56-cmw710-system-r0106.bin.....
..Done.
Decompressing file msr56-cmw710-security-r0106.bin to
slot1#cfa0:/msr56-cmw710-security-r0106.bin...Done.
Decompressing file msr56-cmw710-voice-r0106.bin to
slot1#cfa0:/msr56-cmw710-voice-r0106.bin...Done.
Decompressing file msr56-cmw710-data-r0106.bin to
slot1#cfa0:/msr56-cmw710-data-r0106.bin...Done.
The images that have passed all examinations will be used as the main startup software images
at the next reboot on slot 1.
```

指定 Router 的备用主控板下次启动时所用的备用启动文件为 **msr56-old.ipe**。

```
<Router> boot-loader file slot1#cfa0:/msr56-old.ipe slot 1 backup
This command will set the backup startup software images. Continue? [Y/N]:y
The images that have passed all examinations will be used as the backup startup
software images at the next reboot on slot 1.
```

重启设备。

```
<Router> reboot
```

3.6 验证配置

设备重启后，使用 **display version** 命令查看设备版本信息。

```
<Router> display version
```

```
H3C Comware Software, Version 7.1.049, Release 0106
```

```
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
```

```
H3C MSR56-60 uptime is 0 weeks, 0 days, 0 hours, 3 minutes
Last reboot reason : User reboot
Boot image: cfa0:/msr56-cmw710-boot-r0106.bin
Boot image version: 7.1.049P03, Release 0106
  Compiled Jan 15 2014 19:27:12
System image: cfa0:/msr56-cmw710-system-r0106.bin
System image version: 7.1.049, Release 0106
  Compiled Jan 15 2014 19:27:12
Feature image(s) list:
  cfa0:/msr56-cmw710-security-r0106.bin, version: 7.1.049
    Compiled Jan 15 2014 19:28:36
  cfa0:/msr56-cmw710-voice-r0106.bin, version: 7.1.049
    Compiled Jan 15 2014 19:28:37
  cfa0:/msr56-cmw710-data-r0106.bin, version: 7.1.049
    Compiled Jan 15 2014 19:28:39
```

……略……

显示设备主用主控板本次启动和下次启动所采用的启动软件包的名称。

```
<Router> display boot-loader slot 0
Software images on slot 0:
Current software images:
  cfa0:/msr56-cmw710-boot-r0106.bin
  cfa0:/msr56-cmw710-system-r0106.bin
  cfa0:/msr56-cmw710-security-r0106.bin
  cfa0:/msr56-cmw710-voice-r0106.bin
  cfa0:/msr56-cmw710-data-r0106.bin
Main startup software images:
  cfa0:/msr56-cmw710-boot-r0106.bin
  cfa0:/msr56-cmw710-system-r0106.bin
  cfa0:/msr56-cmw710-security-r0106.bin
  cfa0:/msr56-cmw710-voice-r0106.bin
  cfa0:/msr56-cmw710-data-r0106.bin
Backup startup software images:
  cfa0:/msr56-cmw710-boot-r000703.bin
  cfa0:/msr56-cmw710-system-r000703.bin
  cfa0:/msr56-cmw710-security-r000703.bin
  cfa0:/msr56-cmw710-voice-r000703.bin
  cfa0:/msr56-cmw710-data-r000703.bin
```

显示设备备用主控板本次启动和下次启动所采用的启动软件包的名称。

```
<Router> display boot-loader slot 1
Software images on slot 1:
Current software images:
  cfa0:/msr56-cmw710-boot-r0106.bin
  cfa0:/msr56-cmw710-system-r0106.bin
  cfa0:/msr56-cmw710-security-r0106.bin
  cfa0:/msr56-cmw710-voice-r0106.bin
  cfa0:/msr56-cmw710-data-r0106.bin
Main startup software images:
```

```
cfa0:/msr56-cmw710-boot-r0106.bin
cfa0:/msr56-cmw710-system-r0106.bin
cfa0:/msr56-cmw710-security-r0106.bin
cfa0:/msr56-cmw710-voice-r0106.bin
cfa0:/msr56-cmw710-data-r0106.bin
Backup startup software images:
cfa0:/msr56-cmw710-boot-r000703.bin
cfa0:/msr56-cmw710-system-r000703.bin
cfa0:/msr56-cmw710-security-r000703.bin
cfa0:/msr56-cmw710-voice-r000703.bin
cfa0:/msr56-cmw710-data-r000703.bin
```

3.7 配置文件

```
#
interface gigabitethernet1/0/1
  port link-mode route
  ip address 192.168.100.66 255.255.255.0
#
local-user abc class manage
  password hash $h$6$YmVbbwFL/vviWcQu$+CuTbYCehNZtZo5RCXiadpYbXYWa2omt5TUtEh3UPCg
3fZjxYcP5WzbuE2GoowVi2YA/BK+mnSZJZqi5jRDuCG==
  service-type ftp
  authorization-attribute user-role network-admin
#
  ftp server enable
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“基础配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“基础配置命令参考”

H3C MSR 系列路由器

采用 Boot ROM TFTP 方式升级软件配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	1
3.3 配置注意事项.....	1
3.4 配置步骤.....	2
3.4.1 Host 的配置.....	2
3.4.2 Router 的配置.....	4
3.5 验证配置.....	7
3.6 配置文件.....	8
4 相关资料.....	8

1 简介

本文档介绍使用 Boot ROM 菜单升级软件版本的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

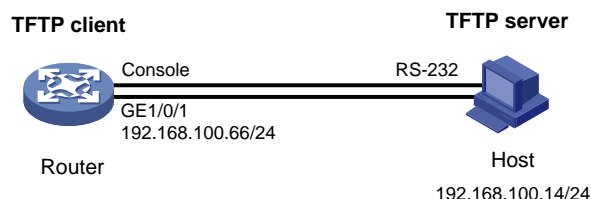
本文档假设您已了解 Boot ROM 菜单升级软件的特性。

3 配置举例

3.1 组网需求

如[图 1](#)所示，用户主机 Host 连接 Router 的 GigabitEthernet1/0/1 接口，同时 Host 通过串口线连接 Router 的 Console 口。现要求：采用 TFTP 方式，通过与主机直连的以太网接口，使用 Boot ROM 菜单升级路由器软件版本，版本文件为 msr36N.ipe。

图1 配置组网图



3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.3 配置注意事项

- 确保在主机上开启 TFTP 服务器功能。
- 当设备剩余的存储空间不够，请使用 `delete /unreserved file-url` 命令删除部分暂时不用的文件后，再执行升级软件操作。

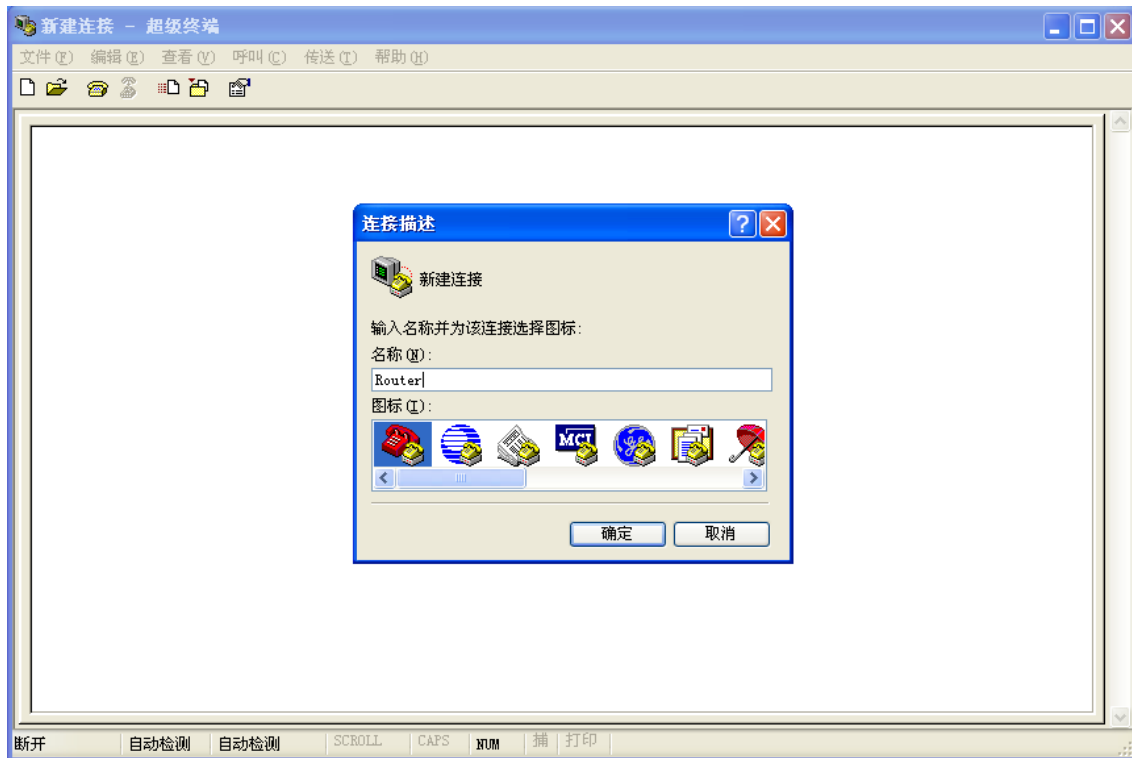
3.4 配置步骤

3.4.1 Host 的配置

配置主机 Host 的 IP 地址为 192.168.100.14/24，使得到 Router 路由可达，具体配置步骤略。

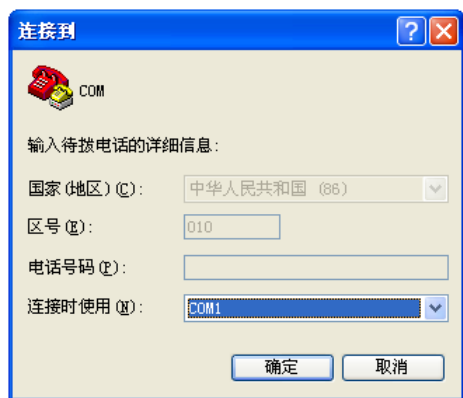
打开超级终端，创建一个新建连接 Router。

图2 新建连接



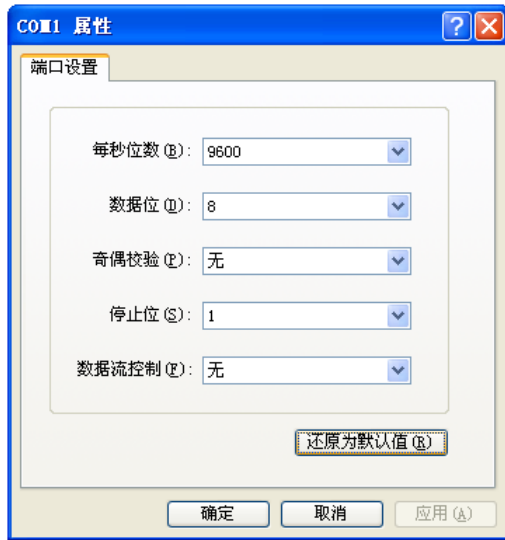
选择连接时使用的“COM1”，单击<确定>。

图3 连接到对话框



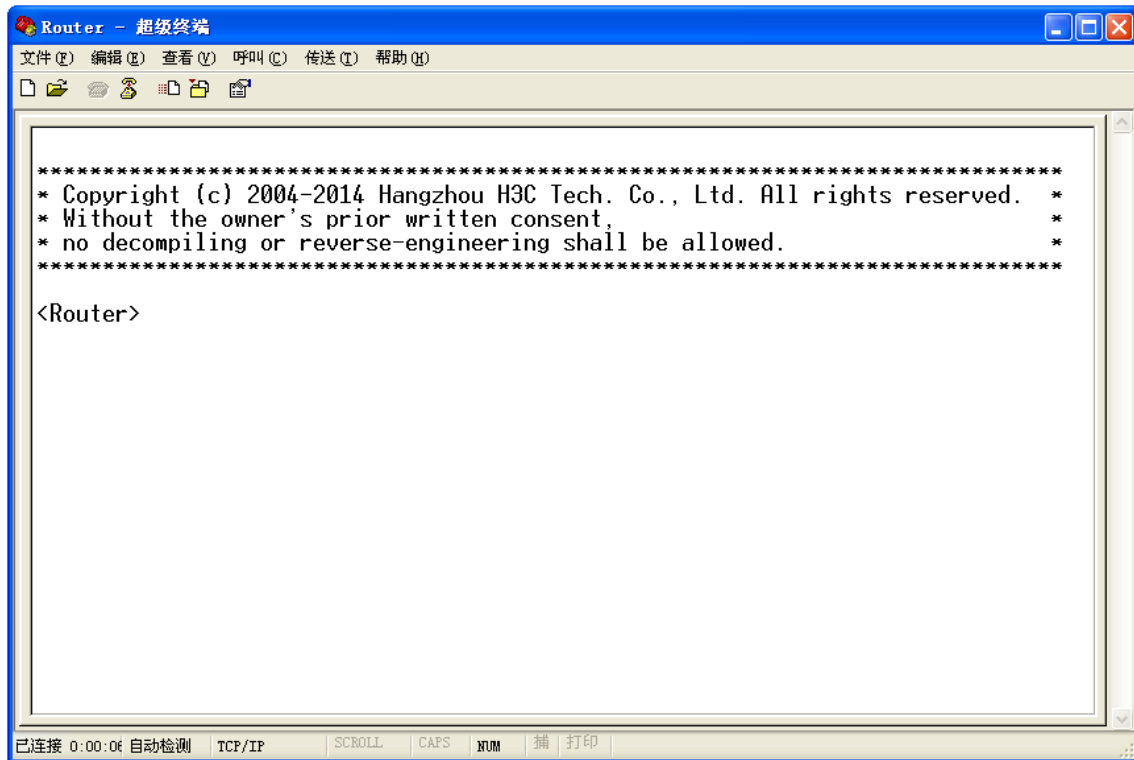
选择“还原为默认值”，单击<确定>。

图4 配置属性值



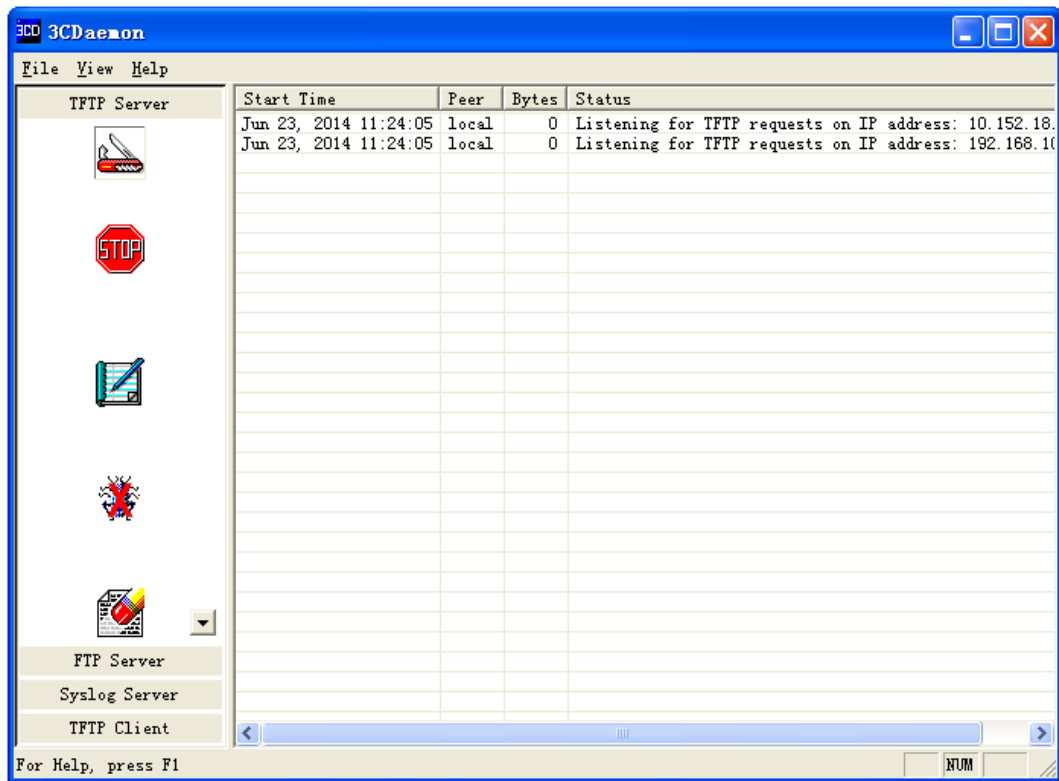
显示登录成功。

图5 登录设备



启动 Host 上的 TFTP 服务器（以 3C Daemon 软件为例），设置 TFTP 服务器下载路径等参数，并开启服务。

图6 配置 TFTP 服务器



3.4.2 Router 的配置

路由器上加电重启的过程中，在配置终端的屏幕上将显示：

```

System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start heavy memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing....Done.

*****
*
*           H3C MSR36-40 BootWare, Version 1.20
*
*****
Copyright (c) 2004-2014 Hangzhou H3C Technologies Co., Ltd.

Compiled Date       : Jun 21 2013
CPU ID              : 0x3
Memory Type         : DDR3 SDRAM
Memory Size         : 2048MB
BootWare Size       : 1024KB
Flash Size          : 8MB
cfa0 Size           : 247MB
    
```

CPLD Version : 2.0
PCB Version : 2.0

BootWare Validating...

Press Ctrl+B to access EXTENDED-BOOTWARE MENU...

当出现“Press Ctrl+B to enter extended boot menu...”时，键入<Ctrl+B>，系统提示：

Password recovery capability is enabled.

Note: The current operating device is cfa0

Enter < Storage Device Operation > to select device.

=====**<EXTENDED-BOOTWARE MENU>**=====

```
|<1> Boot System |
|<2> Enter Serial SubMenu |
|<3> Enter Ethernet SubMenu |
|<4> File Control |
|<5> Restore to Factory Default Configuration |
|<6> Skip Current System Configuration |
|<7> BootWare Operation Menu |
|<8> Skip Authentication for Console Login |
|<9> Storage Device Operation |
|<0> Reboot |
```

=====
Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format File System

在 **BootWare** 菜单下键入<3>，进入以太网口子菜单，系统显示如下：

Enter your choice(0-9): 3

=====**<Enter Ethernet SubMenu>**=====

```
|Note:the operating device is cfa0 |
|<1> Download Image Program To SDRAM And Run |
|<2> Update Main Image File |
|<3> Update Backup Image File |
|<4> Download Files(*.*) |
|<5> Modify Ethernet Parameter |
|<0> Exit To Main Menu |
|<Ensure The Parameter Be Modified Before Downloading!> |
```

在以太网口子菜单下键入<5>就可以进入以太网口配置菜单：

Enter your choice(0-5): 5

=====**<ETHERNET PARAMETER SET>**=====

```
|Note:      '.' = Clear field. |
|           '-' = Go to previous field. |
|           Ctrl+D = Quit. |
```

=====
Protocol (FTP or TFTP) :ftp tftp

Load File Name :MSR36-CMW710-E0006.IPE

:msr36N.ipe
Target File Name :MSR36-CMW710-E0006.IPE
 :msr36N.ipe
Server IP Address :192.168.1.100 192.168.100.14
Local IP Address :192.168.1.101 192.168.100.66
Subnet Mask :0.0.0.0 255.255.255.0
Gateway IP Address :0.0.0.0

按下 Enter 键，进入如下界面：

```
=====<Enter Ethernet SubMenu>=====
|Note:the operating device is cfa0          |
|<1> Download Image Program To SDRAM And Run  |
|<2> Update Main Image File                  |
|<3> Update Backup Image File                 |
|<4> Download Files(*.*)                      |
|<5> Modify Ethernet Parameter               |
|<0> Exit To Main Menu                       |
|<Ensure The Parameter Be Modified Before Downloading!> |
=====
```

在以太网口配置子菜单下，键入<2>为升级主启动文件：

Enter your choice(0-5): 2
Loading.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....Done.
33553920 bytes downloaded!

```
=====<Enter Ethernet SubMenu>=====
|Note:the operating device is cfa0          |
|<1> Download Image Program To SDRAM And Run  |
|<2> Update Main Image File                  |
|<3> Update Backup Image File                 |
|<4> Download Files(*.*)                      |
|<5> Modify Ethernet Parameter               |
|<0> Exit To Main Menu                       |
|<Ensure The Parameter Be Modified Before Downloading!> |
=====
```

键入<0>，返回 BootWare 主菜单：

Enter your choice(0-5): 0

```
=====<EXTENDED-BOOTWARE MENU>=====
|<1> Boot System                             |
|<2> Enter Serial SubMenu                    |
|<3> Enter Ethernet SubMenu                  |
```

```

|<4> File Control |
|<5> Restore to Factory Default Configuration |
|<6> Skip Current System Configuration |
|<7> BootWare Operation Menu |
|<8> Skip Authentication for Console Login |
|<9> Storage Device Operation |
|<0> Reboot |
=====
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
# 键入<1>, 进入引导系统:
Enter your choice(0-9): 1
Loading the main image files...
Loading file cfa0:/msr36-cmw710-system-r0106.bin.....
.....Done.
Loading file cfa0:/msr36-cmw710-voice-r0106.bin.....Done.
Loading file cfa0:/msr36-cmw710-data-r0106.bin.....Done.
Loading file cfa0:/msr36-cmw710-boot-r0106.bin.....Done.

Image file cfa0:/msr36-cmw710-boot-r0106.bin is self-decompressing.....
.....Done.
System image is starting...
Line aux0 is available.

Press ENTER to get started.
# 键入 Enter 键, 进入到用户视图。
<Router>

```

3.5 验证配置

设备重启后, 使用 **display version** 命令查看设备版本信息。

```

<Router> display version
H3C Comware Software, Version 7.1.049, Release 0106
Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C MSR36-40 uptime is 0 weeks, 0 days, 0 hours, 2 minutes
Last reboot reason : User reboot
Boot image: cfa0:/msr36-cmw710-boot-r0106.bin
Boot image version: 7.1.049P04, Release 0106
  Compiled Feb 08 2014 17:43:51
System image: cfa0:/msr36-cmw710-system-r0106.bin
System image version: 7.1.049, Release 0106
  Compiled Feb 08 2014 17:43:51
Feature image(s) list:
  cfa0:/msr36-cmw710-security-r0106.bin, version: 7.1.049
    Compiled Feb 08 2014 17:44:41
  cfa0:/msr36-cmw710-voice-r0106.bin, version: 7.1.049
    Compiled Feb 08 2014 17:44:42
  cfa0:/msr36-cmw710-data-r0106.bin, version: 7.1.049

```

Compiled Feb 08 2014 17:44:44

```
CPU ID: 0x2
2G bytes DDR3 SDRAM Memory
8M bytes Flash Memory
PCB          Version: 2.0
CPLD         Version: 2.0
Basic   BootWare Version: 1.20
Extended BootWare Version: 1.20
[SLOT 0]AUX          (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]GE1/0/1     (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]GE1/0/2     (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]GE1/0/3     (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]CELLULAR0/0 (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 0]CELLULAR0/1 (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 2]SIC-4FSW    (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[SLOT 6]HMIM-4GEE   (Hardware)2.0, (Driver)1.0, (CPLD)0.0
[SLOT 8]HMIM-2SAE   (Hardware)3.0, (Driver)1.0, (CPLD)4.0
```

使用 **display boot-loader** 命令显示本次启动和下次启动所采用的启动软件包的名称。

```
<Router> display boot-loader
Software images on the device:
Current software images:
cfa0:/msr36-cmw710-boot-r0106.bin
cfa0:/msr36-cmw710-system-r0106.bin
cfa0:/msr36-cmw710-voice-r0106.bin
cfa0:/msr36-cmw710-data-r0106.bin
Main startup software images:
cfa0:/msr36-cmw710-boot-r0106.bin
cfa0:/msr36-cmw710-system-r0106.bin
cfa0:/msr36-cmw710-voice-r0106.bin
cfa0:/msr36-cmw710-data-r0106.bin
Backup startup software images:
cfa0:/msr36-cmw710-boot-r000701.bin
cfa0:/msr36-cmw710-system-r000701.bin
cfa0:/msr36-cmw710-security-r000701.bin
cfa0:/msr36-cmw710-voice-r000701.bin
cfa0:/msr36-cmw710-data-r000701.bin
```

3.6 配置文件

无

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“基础配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“基础配置命令参考”

H3C MSR 系列路由器

内网用户通过 NAT 地址访问地址重叠的外网配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置步骤.....	2
3.5 验证配置.....	3
3.6 配置文件.....	4
4 相关资料.....	5

1 简介

本文档介绍 MSR 系列路由器内网用户通过 NAT 地址访问地址重叠的外网典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

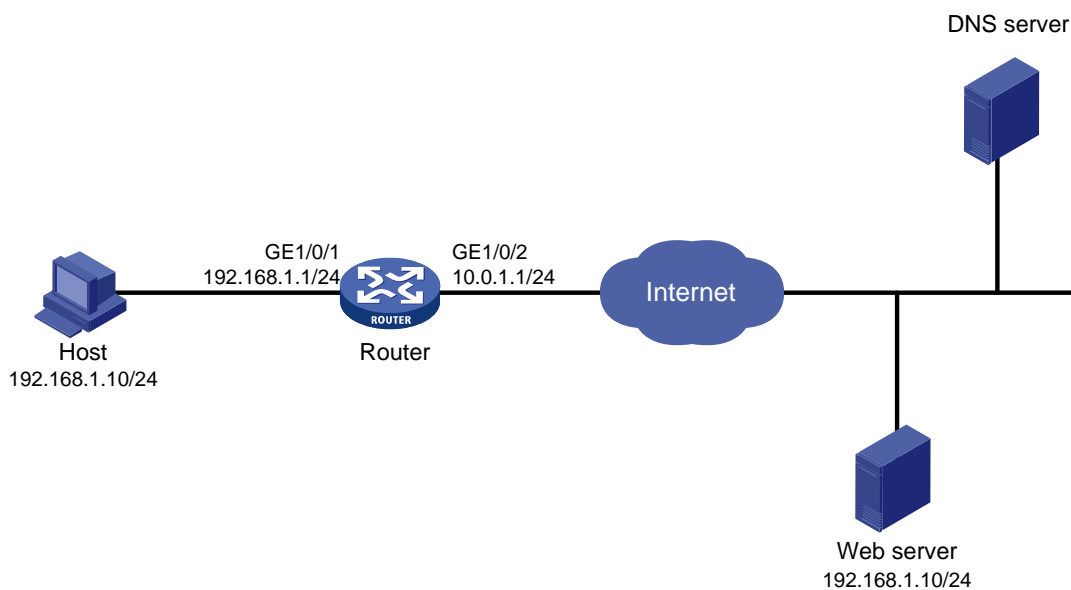
本文档假设您已了解 NAT 特性。

3 配置举例

3.1 组网需求

如图 1 所示，Router 作为某公司内网访问外网的网关，内网网段与外网 Web server 所在网段地址重叠。该公司拥有 202.38.1.2 和 202.38.1.3 两个公网地址。现要求 Host 可以通过域名访问外网的 Web server。

图1 内网用户通过 NAT 地址访问地址重叠的外网典型配置组网图



3.2 配置思路

- 由于外网 DNS 服务器回复给内网主机的 Web 服务器地址与内网主机地址重叠，因此 NAT 设备需要将 Web 服务器地址转换为动态分配的一个 NAT 地址。动态地址分配可以通过入方向动态地址转换实现，地址转换需要通过 DNS ALG 功能实现。
- 由于内网主机的地址与外网 Web 服务器的真实地址重叠，因此也需要为内网主机动态分配一个的 NAT 地址，可以通过出方向动态地址转换实现。
- 外网 Web 服务器对应的 NAT 地址在 NAT 设备上没有路由，因此需要手工添加静态路由。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置步骤

配置路由器各接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.1.1 24
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.0.1.1 24
[Router-GigabitEthernet1/0/2] quit
```

开启 DNS 协议的 ALG 功能。

```
[Router] nat alg dns
```

配置 ACL 2000，仅允许对 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

创建地址组 1。

```
[Router] nat address-group 1
```

添加地址组成员 202.38.1.2。

```
[Router-nat-address-group-1] address 202.38.1.2 202.38.1.2
[Router-nat-address-group-1] quit
```

创建地址组 2。

```
[Router] nat address-group 2
```

添加地址组成员 202.38.1.3。

```
[Router-nat-address-group-2] address 202.38.1.3 202.38.1.3
[Router-nat-address-group-2] quit
```

在接口 GigabitEthernet1/0/2 上配置入方向动态地址转换，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的外网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] nat inbound 2000 address-group 1 no-pat reversible
```

在接口 GigabitEthernet1/0/2 上配置出方向动态地址转换，允许使用地址组 2 中的地址对内网访问外网的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Router-GigabitEthernet1/0/2] nat outbound 2000 address-group 2
[Router-GigabitEthernet1/0/2] quit
```

配置静态路由，目的地址为外网服务器 NAT 地址 202.38.1.2，出接口为 GigabitEthernet1/2，下一跳地址为 10.0.1.1。

```
[Router] ip route-static 202.38.1.2 32 gigabitethernet 1/0/2 10.0.1.1
```

3.5 验证配置

以上配置完成后，Host 能够通过域名访问 Web server。在路由器上通过 **display nat all** 命令显示 NAT 配置信息。

```
[Router] display nat all
```

```
NAT address group information:
```

```
There are 2 NAT address groups.
```

```
Address group 1:
```

```
Address information:
```

Start address	End address
202.38.1.2	202.38.1.2

```
Address group 2:
```

```
Address information:
```

Start address	End address
202.38.1.3	202.38.1.3

```
NAT inbound information:
```

```
There are 1 NAT inbound rules.
```

```
Interface: GigabitEthernet1/0/2
```

ACL: 2000	Address group: 1	Add route: N
NO-PAT: Y	Reversible: Y	

```
NAT outbound information:
```

```
There are 1 NAT outbound rules.
```

```
Interface: GigabitEthernet1/0/2
```

ACL: 2000	Address group: 2	Port-preserved: N
NO-PAT: N	Reversible: N	

```
NAT logging:
```

Log enable	: Disabled
Flow-begin	: Disabled
Flow-end	: Disabled
Flow-active	: Disabled
Port-block-assign	: Disabled
Port-block-withdraw	: Disabled
Alarm	: Disabled

```
NAT mapping behavior:
```

```
Mapping mode: Address and Port-Dependent
ACL          : ---
```

NAT ALG:

```
DNS          : Enabled
FTP          : Enabled
H323        : Enabled
ICMP-ERROR  : Enabled
ILS         : Enabled
MGCP        : Enabled
NBT         : Enabled
PPTP        : Enabled
RSH         : Enabled
RTSP        : Enabled
SCCP        : Enabled
SIP         : Enabled
SQLNET      : Enabled
TFTP        : Enabled
XDMCP       : Enabled
```

通过 **display nat session verbose** 命令显示 NAT 会话的详细信息，可以看到 Host 访问 Web server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.10/1694
  Destination IP/port: 202.38.1.2/8080
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 192.168.1.10/8080
  Destination IP/port: 202.38.1.3/1025
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2013-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet1/0/1
Interface(out): GigabitEthernet1/0/2
Initiator->Responder:          7 packets          308 bytes
Responder->Initiator:         5 packets          312 bytes

Total sessions found: 1
```

3.6 配置文件

```
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 192.168.1.1 255.255.255.0
```

```
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 10.0.1.1 255.255.255.0
  nat inbound 2000 address-group 1 no-pat reversible
  nat outbound 2000 address-group 2
#
  ip route-static 202.38.1.2 32 GigabitEthernet1/0/2 10.0.1.1
#
acl number 2000
  rule 0 permit source 192.168.1.0 0.0.0.255
#
nat address-group 1
  address 202.38.1.2 202.38.1.2
#
nat address-group 2
  address 202.38.1.3 202.38.1.3
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”

H3C MSR 系列路由器

内网用户通过 NAT 地址访问内网服务器配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置步骤.....	2
3.5 验证配置.....	2
3.6 配置文件.....	4
4 相关资料.....	4

1 简介

本文档介绍 MSR 系列路由器内网用户通过 NAT 地址访问内网服务器典型配置。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 NAT 特性。

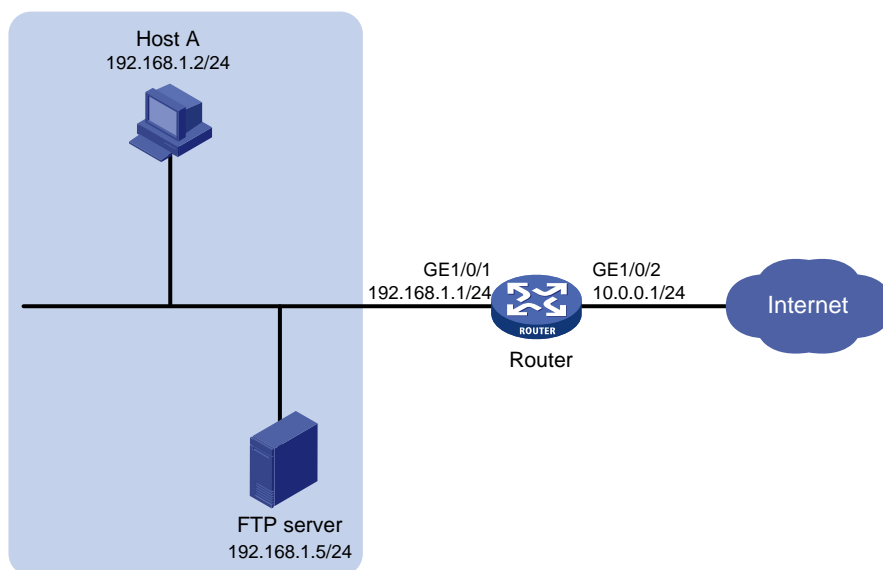
3 配置举例

3.1 组网需求

如[图 1](#)所示，Host A 和 FTP 服务器同在一个局域网内，Router 作为该局域网的网关，具体要求如下：

- 外网主机可以通过 Router 访问内网 FTP 服务器；
- 内网主机在访问 FTP 服务器时，需要通过外网地址访问，从而有效的避免服务器受到来自内部网络的攻击。

图1 内网用户通过外网地址访问内网服务器



3.2 配置思路

- 通过定义 ACL 规则，并将其与 NAT 配置关联，实现只对内网匹配指定的 ACL 规则的报文进行地址转换。
- 为使外网主机可以通过外网地址访问内网 FTP 服务器，需要在外网侧接口配置 NAT 内部服务器功能。
- 为使内网主机通过外网地址访问内网 FTP 服务器，需要在内网侧接口使能 NAT hairpin 功能。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置步骤

配置 Router 的内网接口 GigabitEthernet1/0/1 和外网接口 GigabitEthernet1/0/2 的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.1.1 24
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.0.0.1 24
[Router-GigabitEthernet1/0/2] quit
```

配置 ACL 2000，允许对内部网络中 192.168.1.0/24 网段的报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

在接口 GigabitEthernet1/0/2 上配置 NAT 内部服务器，允许外网主机使用地址 10.0.0.1 访问内网 FTP 服务器，同时使得内网主机访问内网 FTP 服务器的报文可以进行目的地址转换。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] nat server protocol tcp global 10.0.0.1 inside 192.168.1.5 ftp
```

在接口 GigabitEthernet1/0/2 上配置 Easy IP 方式的出方向动态地址转换，使得内网主机访问内网 FTP 服务器的报文可以使用接口 GigabitEthernet1/0/2 的 IP 地址进行源地址转换。

```
[Router-GigabitEthernet1/0/2] nat outbound 2000
[Router-GigabitEthernet1/0/2] quit
```

在接口 GigabitEthernet1/0/1 上使能 NAT hairpin 功能。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] nat hairpin enable
[Router-GigabitEthernet1/0/1] quit
```

3.5 验证配置

以上配置完成后，内网主机和外网主机均能够通过外网地址访问内网 FTP Server。通过 **display nat all** 命令查看所有 NAT 的配置信息，可以看到 GigabitEthernet1/0/1 接口上使能了 NAT hairpin 功能。

```
[Router] display nat all
```

NAT outbound information:

There are 1 NAT outbound rules.

Interface: GigabitEthernet1/0/2

ACL: 2000 Address group: --- Port-preserved: N

NO-PAT: N Reversible: N

NAT internal server information:

There are 1 internal servers.

Interface: GigabitEthernet1/0/2

Protocol: 6(TCP)

Global IP/port: 10.0.0.1/21

Local IP/port: 192.168.1.5/21

NAT logging:

Log enable : Disabled

Flow-begin : Disabled

Flow-end : Disabled

Flow-active : Disabled

Port-block-assign : Disabled

Port-block-withdraw : Disabled

Alarm : Disabled

NAT hairpinning:

There are 1 interfaces enabled with NAT hairpinning.

Interface: GigabitEthernet1/0/1

NAT mapping behavior:

Mapping mode: Address and Port-Dependent

ACL : ---

NAT ALG:

DNS : Enabled

FTP : Enabled

H323 : Enabled

ICMP-ERROR : Enabled

ILS : Enabled

MGCP : Enabled

NBT : Enabled

PPTP : Enabled

RSH : Enabled

RTSP : Enabled

SCCP : Enabled

SIP : Enabled

SQLNET : Enabled

TFTP : Enabled

XDMCP : Enabled

通过 **display nat session verbose** 命令查看 NAT 会话的详细信息，可以看到 Host A 访问 FTP server 时生成 NAT 会话信息。

[Router] display nat session verbose

```
Initiator:
  Source      IP/port: 192.168.1.2/1694
  Destination IP/port: 10.0.0.1/21
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 192.168.1.5/21
  Destination IP/port: 10.0.0.1/1025
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2013-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet1/0/1
Interface(out): GigabitEthernet1/0/2
Initiator->Responder:          7 packets          308 bytes
Responder->Initiator:         5 packets          312 bytes

Total sessions found: 1
```

3.6 配置文件

```
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 192.168.1.1 255.255.255.0
  nat hairpin enable
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 10.0.0.1 255.255.255.0
  nat outbound 2000
  nat server protocol tcp global 10.0.0.1 21 inside 192.168.1.5 21
#
acl number 2000
  rule 0 permit source 192.168.1.0 0.0.0.255
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”

H3C MSR 系列路由器

内部服务器负载分担配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.6 验证配置.....	3
3.7 配置文件.....	5
4 相关资料.....	6

1 简介

本文介绍 NAT 内部服务器负载分担典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 NAT 特性。

3 配置举例

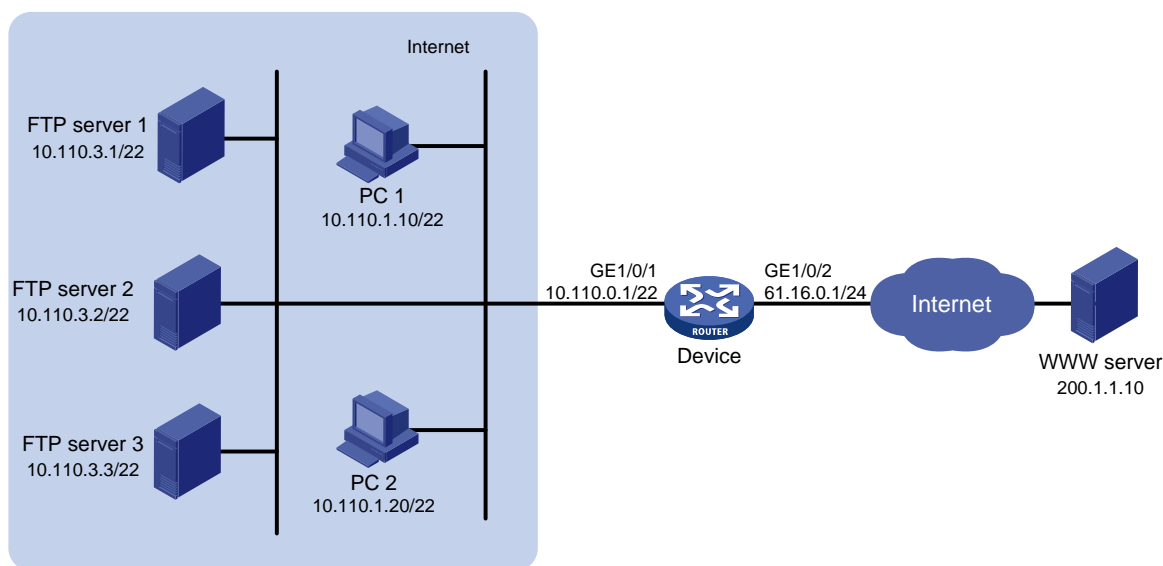
3.1 组网需求

如图 1 所示，某公司内网地址是 10.110.0.0/22，向运营商申请的公网地址是 61.16.0.1~61.16.0.3。公司内网用户使用 10.110.0.0~10.110.2.255 地址段内 IP 地址；公司内网目前共有 3 台 FTP 服务器可以同时提供服务，服务器使用 10.110.3.1~10.110.3.3 的 IP 地址。

要求实现如下功能：

- 内网用户经过地址转换后使用 61.16.0.2~61.16.0.3 公网地址访问 Internet；
- 外网主机和内网主机都可以通过 61.16.0.1 访问内网中的 FTP 服务器；
- 3 台 FTP 服务器提供服务时进行负载分担，但不允许主动访问外网。

图1 负载分担内部服务器配置组网图



3.2 配置思路

- 为了实现 10.110.0.0~10.110.2.255 可以转换成 61.16.0.2~61.16.0.3 公网地址访问 Internet, 需要定义 ACL 规则, 实现只对内网匹配指定的 ACL 规则的报文在 Device 的 GigabitEthernet1/0/2 出方向上进行动态地址转换。
- 为了保证 3 台 FTP 服务器同时提供服务, 需要配置 NAT 内部服务器组, 并采用负载分担方式。
- 为了实现内网用户也可以使用 61.16.0.1 地址访问 FTP 服务器, 需要在 Device 的 GigabitEthernet1/0/1 上使能 NAT hairpin 功能。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

如果配置了 hairpin 功能, 那么配置 `nat server/nat outbound/nat hairpin` 的接口都要在同一个接口板上。

3.5 配置步骤

(1) 配置接口 IP 地址

配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.110.0.1 255.255.252.0
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ip address 61.16.0.1 255.255.255.0
[Device-GigabitEthernet1/0/2] quit
```

(2) 配置内网用户访问外网

配置地址组 0, 包含两个外网地址 61.16.0.2 和 61.16.0.3。

```
[Device] nat address-group 0
[Device-nat-address-group-0] address 61.16.0.2 61.16.0.3
[Device-nat-address-group-0] quit
```

配置 ACL 2000, 仅允许对内部网络中 10.110.0.0~10.110.2.255 网段的用户报文进行地址转换。

```
[Device] acl number 2000
[Device-acl-basic-2000] rule permit source 10.110.0.0 0.0.1.255
[Device-acl-basic-2000] rule permit source 10.110.2.0 0.0.0.255
[Device-acl-basic-2000] quit
```

在接口 GigabitEthernet1/0/2 上配置出方向动态地址转换, 允许使用地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换, 并在转换过程中使用端口信息。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat outbound 2000 address-group 0
[Device-GigabitEthernet1/0/2] quit
```

(3) 配置 FTP 服务器同时提供服务

配置内部服务器组 0 及其成员 10.110.3.1、10.110.3.2 和 10.110.3.3。

```
[Device] nat server-group 0
[Device-nat-server-group-0] inside ip 10.110.3.1 port 21
[Device-nat-server-group-0] inside ip 10.110.3.2 port 21
[Device-nat-server-group-0] inside ip 10.110.3.3 port 21
[Device-nat-server-group-0] quit
```

在接口 GigabitEthernet1/0/2 上配置负载分担内部服务器，引用内部服务器组 0，该组内的主机共同提供 FTP 服务。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] nat server protocol tcp global 61.16.0.1 ftp inside
server-group 0
[Device-GigabitEthernet1/0/2] quit
```

在接口 GigabitEthernet1/0/1 上使能 NAT hairpin 功能。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] nat hairpin enable
[Device-GigabitEthernet1/0/1] quit
```

3.6 验证配置

当 PC 1 访问 WWW server 时，可以看到生成的 NAT 会话信息。

```
[Device] display nat session verbose
Initiator:
  Source      IP/port: 10.110.1.10/1024
  Destination IP/port: 200.1.1.10/80
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)
Responder:
  Source      IP/port: 200.1.1.10/80
  Destination IP/port: 61.16.0.2/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)
State: UDP_READY
Application: HTTP
Start time: 2014-07-08 13:30:47  TTL: 60s
Interface(in) : GigabitEthernet1/0/1
Interface(out): GigabitEthernet1/0/2
Initiator->Responder:      21946552 packets 2414120720 bytes
Responder->Initiator:      650389 packets  71542790 bytes
```

Total sessions found: 1

当有两个外网用户 (61.16.0.10、61.16.0.11) 同时请求 FTP 服务时，可以查看到建立了 2 条 NAT 会话，并且 FTP server 1 和 FTP server 2 分别为这两个用户提供 FTP 服务。

```
[Device] display nat session verbose
Initiator:
```



```

Source      IP/port: 61.16.0.11/1024
Destination IP/port: 61.16.0.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: TCP(6)
Responder:
Source      IP/port: 10.110.3.1/21
Destination IP/port: 61.16.0.11/1024
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-07-08 14:11:41  TTL: 3600s
Interface(in) : GigabitEthernet1/0/2
Interface(out): GigabitEthernet1/0/1
Initiator->Responder:      598098 packets    65790780 bytes
Responder->Initiator:      0 packets      0 bytes

```

```

Initiator:
Source      IP/port: 61.16.0.10/1024
Destination IP/port: 61.16.0.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: TCP(6)
Responder:
Source      IP/port: 10.110.3.2/21
Destination IP/port: 61.16.0.10/1024
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-07-08 14:12:00  TTL: 3600s
Interface(in) : GigabitEthernet1/0/2
Interface(out): GigabitEthernet1/0/1
Initiator->Responder:      74783 packets    8226130 bytes
Responder->Initiator:      0 packets      0 bytes

```

Total sessions found: 2

当 PC 1 通过 61.16.0.1 地址访问 FTP 服务器时，可以查看到建立的 NAT 会话。

```
[Device] display nat session verbose
```

```

Initiator:
Source      IP/port: 10.110.1.10/1024
Destination IP/port: 61.16.0.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: TCP(6)

```

```
Responder:
  Source      IP/port: 10.110.3.1/21
  Destination IP/port: 61.16.0.2/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-07-08 14:24:15  TTL: 3600s
Interface(in) : GigabitEthernet1/0/1
Interface(out): GigabitEthernet1/0/1
Initiator->Responder:      209716 packets   23068760 bytes
Responder->Initiator:      0 packets      0 bytes

Total sessions found: 1
```

3.7 配置文件

```
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 10.110.0.1 255.255.252.0
  nat hairpin enable
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 61.16.0.1 255.255.255.0
  nat outbound 2000 address-group 0
  nat server protocol tcp global 61.16.0.1 21 inside server-group 0
#
acl number 2000
  rule 0 permit source 10.110.0.0 0.0.1.255
  rule 5 permit source 10.110.2.0 0.0.0.255
#
acl number 2001
  rule 0 permit source 10.110.0.0 0.0.1.255
  rule 5 permit source 10.110.2.0 0.0.0.255
#
nat address-group 0
  address 61.16.0.2 61.16.0.3
#
nat server-group 0
  inside ip 10.110.3.1 port 21
  inside ip 10.110.3.2 port 21
  inside ip 10.110.3.3 port 21
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”

H3C MSR 系列路由器

NAT DNS mapping 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	2
3.4 配置步骤.....	2
3.5 验证配置.....	2
3.6 配置文件.....	3
4 相关资料.....	3

1 简介

本文档介绍 MSR 系列路由器 NAT DNS mapping 典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

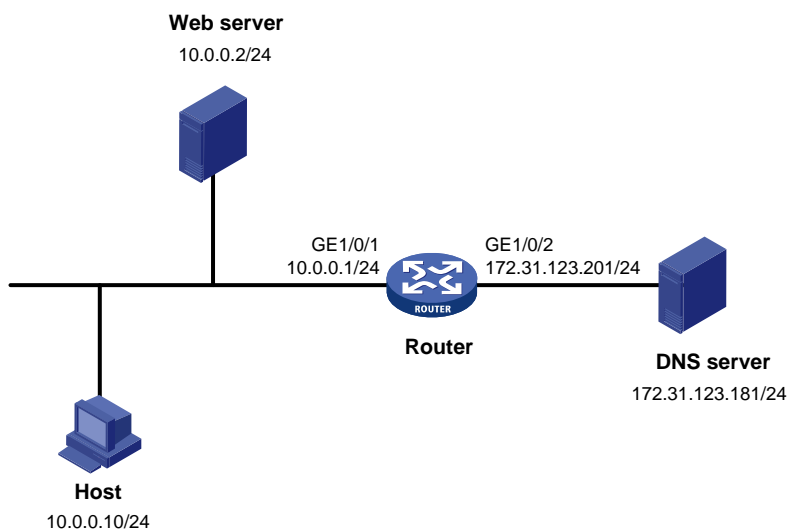
本文档假设您已了解 NAT 特性。

3 配置举例

3.1 组网需求

如 [图 1](#) 所示，私网对外提供 Web 服务，网段为 10.0.0.0/24。该私网具有 172.31.123.201~172.31.123.203 三个公网 IP 地址。另外内网用户的 DNS 服务器在公网中，IP 地址为 172.31.123.181。现要求：内网主机和外网主机均可以通过域名访问内网服务器。

图1 MSR 系列路由器 NAT DNS mapping 典型配置组网图



3.2 配置思路

- 为了使内网服务器能够对外提供服务，需要配置 NAT 内部服务器将各服务器的内网 IP 地址和端口映射为一个外网地址和端口。

- 为了使内网主机能够通过域名访问内网服务器，需要通过地址转换访问外网的 DNS 服务器，并获取内网服务器的内网 IP 地址。由于 DNS 服务器向内网主机发送的响应报文中包含的是内网服务器的外网地址，因此 NAT 设备需要将 DNS 报文载荷内的外网地址转换为内网地址，这可以通过查找 DNS mapping 映射表配合 DNS ALG 功能实现。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置步骤

配置接口 IP 地址

```
<Router> system-view
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/1] ip address 172.31.123.201 24
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/0] ip address 10.0.0.1 24
[Router-GigabitEthernet1/0/0] quit
```

配置 NAT 内部服务器功能，允许外网主机使用地址 172.31.123.202 访问内网 Web 服务器。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/1] nat server protocol tcp global 172.31.123.202 inside 10.0.0.2
http
[Router-GigabitEthernet1/0/1] nat outbound
[Router-GigabitEthernet1/0/1] quit
```

配置 DNS mapping 表项：Web 服务器的域名 www.server.com 对应 IP 地址 172.31.123.202。

```
[Router] nat dns-map domain www.server.com protocol tcp ip 172.31.123.202 port http
[Router] quit
```

3.5 验证配置

配置完成后，内网主机和外网主机均可以通过域名访问内网服务器。通过查看如下显示信息，可以验证以上配置成功。

```
<Router> display nat all
NAT internal server information:
  There are 1 internal servers.
  Interface: GigabitEthernet1/0/1
  Protocol: 6(TCP)
  Global IP/port: 172.31.123.202/80
  Local IP/port: 10.0.0.2/80
```

```
NAT DNS mapping information:
  There are 1 NAT DNS mappings.
  Domain name: www.server.com
  Global IP : 172.31.123.202
  Global port: 80
  Protocol : TCP(6)
```

```

NAT logging:
  Log enable : Disabled
  Flow-begin : Disabled
  Flow-end   : Disabled
  Flow-active: Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL          : ---

NAT ALG:
  DNS          : Enabled
  FTP          : Enabled
  H323         : Enabled
  ICMP-ERROR   : Enabled
  RTSP         : Enabled
  SIP          : Enabled
  TFTP         : Enabled

```

3.6 配置文件

```

#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 172.31.123.201 255.255.255.0
  nat outbound
  nat server protocol tcp global 172.31.123.202 80 inside 10.0.0.2 80
#
nat dns-map domain www.server.com protocol tcp ip 172.31.123.202 port 80
#

```

4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“三层技术-IP 业务命令参考”

H3C MSR 系列路由器

定时执行任务配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	1
3.3 配置注意事项.....	1
3.4 配置步骤.....	2
3.5 验证配置.....	3
3.6 配置文件.....	5
4 相关资料.....	6

1 简介

本文档介绍使用定时执行任务功能的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

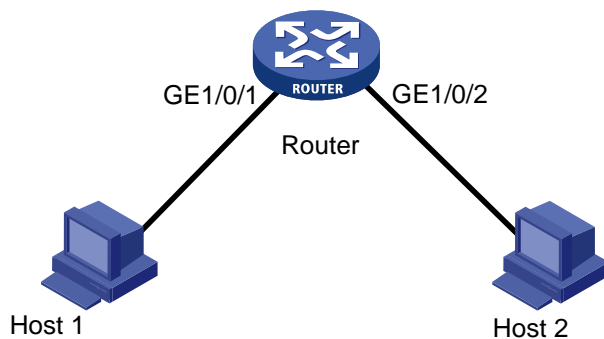
本文档假设您已了解定时执行任务功能特性。

3 配置举例

3.1 组网需求

如图 1 所示，路由器 Router 连接两台主机，现要求：对 Router 配置定时执行任务功能，使得在星期一到星期五的上午八点到下午十八点开启 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，其它时间关闭端口。

图1 配置组网图



3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.3 配置注意事项

- 通过 **command** 指定的命令行必须是设备上可成功执行的命令行；否则，命令行不能自动被执行。
- 通过 **command** 指定的命令行不能包括 **telnet**、**ftp**、**ssh2** 和 **monitor process** 命令。

- 在配置定时任务前，需查看系统时间是否正确。如果系统时间不正确的话，可以通过配置 NTP 功能或者 `clock` 命令进行修改，保证设备获得准确的时间。

3.4 配置步骤

(1) 配置关闭和开启接口的工作任务

创建名称为 `shutdown-GigabitEthernet1/0/1` 的工作任务并进入 Job 视图。

```
[Router] scheduler job shutdown-GigabitEthernet1/0/1
```

为 Job 分配命令，以进入系统视图。

```
[Router-job-shutdown-GigabitEthernet1/0/1] command 1 system-view
```

为 Job 分配命令，以进入 `GigabitEthernet1/0/1` 接口视图。

```
[Router-job-shutdown-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
```

为 Job 分配命令，以执行关闭 `GigabitEthernet1/0/1` 接口。

```
[Router-job-shutdown-GigabitEthernet1/0/1] command 3 shutdown
```

```
[Router-job-shutdown-GigabitEthernet1/0/1] quit
```

创建名称为 `shutdown-GigabitEthernet1/0/2` 的工作任务并进入 Job 视图。

```
[Router] scheduler job shutdown-GigabitEthernet1/0/2
```

为 Job 分配命令，以进入系统视图。

```
[Router-job-shutdown-GigabitEthernet1/0/2] command 1 system-view
```

为 Job 分配命令，以进入 `GigabitEthernet1/0/2` 接口视图。

```
[Router-job-shutdown-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2
```

为 Job 分配命令，以执行关闭 `GigabitEthernet1/0/2` 接口。

```
[Router-job-shutdown-GigabitEthernet1/0/2] command 3 shutdown
```

```
[Router-job-shutdown-GigabitEthernet1/0/2] quit
```

创建名称为 `start-GigabitEthernet1/0/1` 的工作任务并进入 Job 视图。

```
[Router] scheduler job start-GigabitEthernet1/0/1
```

为 Job 分配命令，以进入系统视图。

```
[Router-job-start-GigabitEthernet1/0/1] command 1 system-view
```

为 Job 分配命令，以进入 `GigabitEthernet1/0/1` 接口视图。

```
[Router-job-start-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
```

为 Job 分配命令，以执行开启 `GigabitEthernet1/0/1` 接口。

```
[Router-job-start-GigabitEthernet1/0/1] command 3 undo shutdown
```

```
[Router-job-start-GigabitEthernet1/0/1] quit
```

创建名称为 `start-GigabitEthernet1/0/2` 的工作任务并进入 Job 视图。

```
[Router] scheduler job start-GigabitEthernet1/0/2
```

为 Job 分配命令，以进入系统视图。

```
[Router-job-start-GigabitEthernet1/0/2] command 1 system-view
```

为 Job 分配命令，以进入 `GigabitEthernet1/0/2` 接口视图。

```
[Router-job-start-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2
```

为 Job 分配命令，以执行开启 `GigabitEthernet1/0/2` 接口。

```
[Router-job-start-GigabitEthernet1/0/2] command 3 undo shutdown
```

```
[Router-job-start-GigabitEthernet1/0/2] quit
```

(2) 配置定时执行任务

```

# 创建名为 connect-host1/host2 的 Schedule，并进入 Schedule 视图。
[Router] scheduler schedule connect-host1/host2
# 为 Schedule 分配名为 start-GigabitEthernet1/0/1 的 job。
[Router-schedule-connect-host1/host2] job start-GigabitEthernet1/0/1
# 为 Schedule 分配名为 start-GigabitEthernet1/0/2 的 job。
[Router-schedule-connect-host1/host2] job start-GigabitEthernet1/0/2
# 为 Schedule 配置循环执行的时间，在星期一到星期五的上午 8 点开启 GigabitEthernet1/0/1
和 GigabitEthernet1/0/2 接口。
[Router-schedule-connect-host1/host2] time repeating at 08:00 week-day Mon Tue Wed Thu
Fri
[Router-schedule-connect-host1/host2] quit
# 创建名为 unconnect-host1/host2 的 Schedule，并进入 Schedule 视图。
[Router] scheduler schedule unconnect-host1/host2
# 为 Schedule 分配名为 shutdown-GigabitEthernet1/0/1 的 job。
[Router-schedule-unconnect-host1/host2] job shutdown-GigabitEthernet1/0/1
# 为 Schedule 分配名为 shutdown-GigabitEthernet1/0/2 的 job。
[Router-schedule-unconnect-host1/host2] job shutdown-GigabitEthernet1/0/2
# 为 Schedule 配置循环执行的时间，在星期一到星期五的下午 18 点关闭
GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 接口。
[Router-schedule-unconnect-host1/host2] time repeating at 18:00 week-day Mon Tue Wed
Thu Fri
[Router-schedule-unconnect-host1/host2] quit

```

3.5 验证配置

使用 **display scheduler job** 命令显示 Job 的配置信息。

```

<Router> display scheduler job
Job name: shutdown-GigabitEthernet1/0/1
  system-view
  interface gigabitethernet1/0/1
  shutdown

Job name: shutdown-GigabitEthernet1/0/2
  system-view
  interface gigabitethernet1/0/2
  shutdown

Job name: start-GigabitEthernet1/0/1
  system-view
  interface gigabitethernet1/0/1
  undo shutdown

Job name: start-GigabitEthernet1/0/2
  system-view
  interface gigabitethernet1/0/2
  undo shutdown

```

使用 **display scheduler schedule** 命令显示定时任务的运行信息。

```
<Router> display scheduler schedule
Schedule name      : connect-host1/host2
Schedule type      : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time         : Thu Nov 14 08:00:00 2013
Last execution time : Yet to be executed

-----

Job name                Last execution status
start-GigabitEthernet1/0/1  -NA-
start-GigabitEthernet1/0/2  -NA-

Schedule name      : unconnect-host1/host2
Schedule type      : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time         : Wed Nov 13 18:00:00 2013
Last execution time : Yet to be executed

-----

Job name                Last execution status
shutdown-GigabitEthernet1/0/1  -NA-
shutdown-GigabitEthernet1/0/2  -NA-
```

在上午 7:59 时，使用 **display ip interface brief** 命令查看三层接口状态。

```
[Router] display ip interface brief
*down: administratively down
(s): spoofing (l): loopback

Interface                Physical Protocol IP Address      Description
Ana3/0                   down      down    --              --
Aux0                      up        down    --              --
GE0/0                    up        up      192.168.100.67 --
GE1/0/1                  *down    down    --              --
GE1/0/2                  *down    down    --              --
```

当到上午 8:00 时候，设备有如下日志信息显示。

```
%Apr 22 08:00:10:245 2014 Router IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/1 changed to up.
%Apr 22 08:00:10:245 2014 Router IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/1 changed to up.
%Apr 22 08:00:10:250 2014 Router IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to up.
%Apr 22 08:00:10:250 2014 Router IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/2 changed to up.
```

在上午 8:00 时，使用 **display ip interface brief** 命令查看三层接口状态。

```
[Router] display ip interface brief
*down: administratively down
(s): spoofing (l): loopback

Interface                Physical Protocol IP Address      Description
Ana3/0                   down      down    --              --
Aux0                      up        down    --              --
GE0/0                    up        up      192.168.100.67 --
GE1/0/1                  up        up      --              --
GE1/0/2                  up        up      --              --
```

当到下午 18:00 时候, 设备有如下日志信息显示。

```
%Apr 22 18:00:06:250 2014 Router IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/1 changed to down.
```

```
%Apr 22 18:00:06:250 2014 Router IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/1 changed to down.
```

```
%Apr 22 18:00:06:256 2014 Router IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to down.
```

```
%Apr 22 18:00:06:256 2014 Router IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/2 changed to down.
```

在下午 18:00 时, 使用 **display ip interface brief** 命令查看三层接口状态。

```
[Router] display ip interface brief
```

```
*down: administratively down
```

```
(s): spoofing (l): loopback
```

Interface	Physical	Protocol	IP Address	Description
Ana3/0	down	down	--	--
Aux0	up	down	--	--
GE0/0	up	up	192.168.100.67	--
GE1/0/1	*down	down	--	--
GE1/0/2	*down	down	--	--

3.6 配置文件

```
#
scheduler job shutdown-GigabitEthernet1/0/1
  command 1 system-view
  command 2 interface gigabitethernet1/0/1
  command 3 shutdown
#
scheduler job shutdown-GigabitEthernet1/0/2
  command 1 system-view
  command 2 interface gigabitethernet1/0/2
  command 3 shutdown
#
scheduler job start-GigabitEthernet1/0/1
  command 1 system-view
  command 2 interface gigabitethernet1/0/1
  command 3 undo shutdown
#
scheduler job start-GigabitEthernet1/0/2
  command 1 system-view
  command 2 interface gigabitethernet1/0/2
  command 3 undo shutdown
#
scheduler schedule connect-host1/host2
  job start-GigabitEthernet1/0/1
  job start-GigabitEthernet1/0/2
  time repeating at 08:00 week-day Mon Tue Wed Thu Fri
#
scheduler schedule unconnect-host1/host2
```

```
job shutdown-GigabitEthernet1/0/1
job shutdown-GigabitEthernet1/0/2
time repeating at 18:00 week-day Mon Tue Wed Thu Fri
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“基础配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“基础配置命令参考”

H3C MSR 系列路由器

RBAC 配置举例

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置用户具有特定特性中读写类型命令的执行权限举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	1
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.6 验证配置.....	3
3.7 配置文件.....	5
4 Telnet 用户的 RADIUS 用户角色授权配置举例.....	5
4.1 组网需求.....	5
4.2 配置思路.....	6
4.3 使用版本.....	6
4.4 配置注意事项.....	6
4.5 配置步骤.....	6
4.5.1 设备配置.....	6
4.5.2 RADIUS 服务器配置.....	8
4.6 验证配置.....	10
4.7 配置文件.....	12
5 配置用户在某些 VPN 中具有特定特性的执行权限举例.....	13
5.1 组网需求.....	13
5.2 配置思路.....	13
5.3 使用版本.....	13
5.4 配置注意事项.....	13
5.5 配置步骤.....	14
5.5.1 设备配置.....	14
5.5.2 RADIUS 服务器配置.....	15
5.6 验证配置.....	17
5.7 配置文件.....	18
6 创建新用户角色并授权更改用户权限举例.....	19
6.1 组网需求.....	19

6.2 配置思路	20
6.3 使用版本	20
6.4 配置注意事项	20
6.5 配置步骤	20
6.6 验证配置	23
6.6.1 配置更改用户权限前的验证	23
6.6.2 配置更改用户权限后的验证	24
6.7 配置文件	25
7 配置用户具有切换用户角色权限举例	26
7.1 组网需求	26
7.2 配置思路	26
7.3 使用版本	26
7.4 配置注意事项	27
7.5 配置步骤	27
7.6 验证配置	28
7.7 配置文件	31
8 配置具有流量控制执行权限举例	32
8.1 组网需求	32
8.2 配置思路	33
8.3 使用版本	33
8.4 配置注意事项	33
8.5 配置步骤	34
8.5.1 设备配置	34
8.5.2 RADIUS 服务器配置	35
8.6 验证配置	38
8.7 配置文件	41
9 相关资料	42

1 简介

本文介绍了通过 RBAC 对登录设备的用户权限进行控制的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 RBAC 的特性。

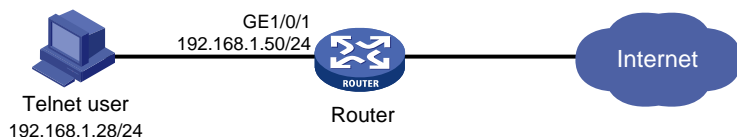
3 配置用户具有特定特性中读写类型命令的执行权限举例

3.1 组网需求

如[图 1](#)所示，为了加强用户登录的安全性，采用本地 AAA 认证对登录设备的 Telnet 用户进行认证。使得 Telnet 用户具有如下权限：

- 允许执行特性 ospf 相关的所有读写类型命令。
- 允许执行特性 filesystem 相关的所有读写类型命令。

图1 特定特性中读写类型命令的执行权限配置组网图



3.2 配置思路

- 为了使 Telnet 用户能够具备以上权限，需要创建 Telnet 本地用户和用户角色 role1，并对 Telnet 用户授予用户角色 role1。
- 通过配置用户角色规则，限定 Telnet 用户可以执行特性特性 ospf 和 filesystem 相关的读写类型命令。
- 为了确保 Telnet 用户仅使用授权的用户角色 role1，需要删除用户具有的缺省用户角色。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 一个 ISP 域被配置为缺省的 ISP 域后将不能够被删除，必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域，然后才可以被删除。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。

3.5 配置步骤

(1) 配置接口

为接口 GigabitEthernet1/0/1 配置 IP 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 192.168.1.50 24
[Sysname-GigabitEthernet1/0/1] quit
```

(2) 配置 Telnet 用户登录设备的认证方式

开启设备的 Telnet 服务器功能。

```
[Sysname] telnet server enable
```

在编号为 0~63 的 VTY 用户线下，配置 Telnet 用户登录采用 AAA 认证方式。

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

(3) 配置 ISP 域 bbb 的 AAA 方法

创建 ISP 域 bbb，为 login 用户配置的 AAA 方法为本地认证、本地授权。

```
[Sysname] domain bbb
[Sysname-isp-bbb] authentication login local
[Sysname-isp-bbb] authorization login local
[Sysname-isp-bbb] quit
```

(4) 配置设备管理类本地用户 telnetuser 的密码和服务类型。

创建设备管理类本地用户 telnetuser。

```
[Sysname] local-user telnetuser class manage
```

配置用户的密码是明文的 123456TESTplat&!。

```
[Sysname-luser-manage-telnetuser] password simple 123456TESTplat&!
```

指定用户的服务类型是 Telnet。

```
[Sysname-luser-manage-telnetuser] service-type telnet
[Sysname-luser-manage-telnetuser] quit
```

(5) 创建用户角色 role1，并配置用户角色规则

创建用户角色 role1，进入用户角色视图。

```
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行特性 ospf 中所有读写类型的命令。

```
[Sysname-role-role1] rule 1 permit read write feature ospf
```

配置用户角色规则 2，允许用户执行特性 **filesystem** 中所有读写类型的命令。

```
[Sysname-role-role1] rule 2 permit read write feature filesystem
[Sysname-role-role1] quit
```

(6) 为本地用户配置授权用户角色

进入设备管理类本地用户 **telnetuser** 视图。

```
[Sysname] local-user telnetuser class manage
```

指定用户 **telnetuser** 的授权角色为 **role1**。

```
[Sysname-luser-manage-telnetuser] authorization-attribute user-role role1
```

为保证用户仅使用授权的用户角色 **role1**，删除用户 **telnetuser** 具有的缺省用户角色 **network-operator**。

```
[Sysname-luser-manage-telnetuser] undo authorization-attribute user-role
network-operator
```

```
[Sysname-luser-manage-telnetuser] quit
```

3.6 验证配置

(1) 查看用户角色信息

通过 **display role** 命令查看显示用户角色 **role1** 的信息。

```
<Sysname> display role name role1
```

```
Role: role1
```

```
Description:
```

```
VLAN policy: permit (default)
```

```
Interface policy: permit (default)
```

```
VPN instance policy: permit (default)
```

```
Security zone policy: permit (default)
```

```
-----
Rule      Perm   Type  Scope      Entity
-----
```

```
1         permit RW-  feature    ospf
```

```
2         permit RW-  feature    filesystem
```

```
R:Read W:Write X:Execute
```

(2) 用户登录设备

用户向设备发起 **Telnet** 连接，在 **Telnet** 客户端按照提示输入用户名 **telnetuser@bbb** 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50
```

```
*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****
```

```
login: telnetuser@bbb
```

```
Password:
```

```
<Sysname>
```

(3) 验证用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- 可执行特性 **ospf** 中所有写类型的命令。（以配置 **OSPF** 为例）

```
[Sysname] ospf 1
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
```

- 可执行特性 **ospf** 相关的读类型命令。

```
[Sysname] show ospf
```

```
OSPF Process 1 with Router ID 192.168.1.50
OSPF Protocol Information
```

```
RouterID: 192.168.1.50   Router type:
Route tag: 0
Multi-VPN-Instance is not enabled
Ext-community type: Domain ID 0x5, Route Type 0x306, Router ID 0x107
Domain ID: 0.0.0.0
Opaque capable
ISPF is enabled
SPF-schedule-interval: 5 50 200
LSA generation interval: 5 50 200
LSA arrival interval: 1000
Transmit pacing: Interval: 20 Count: 3
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route preference: 10
ASE route preference: 150
SPF calculation count: 0
RFC 1583 compatible
Fast-reroute: Remote-lfa Disabled
  Maximum-cost: 4294967295
Node-Protecting Preference: 40
Lowest-cost Preference: 20
Graceful restart interval: 120
SNMP trap rate limit interval: 10 Count: 7
Area count: 0   NSSA area count: 0
ExChange/Loading neighbors: 0
MPLS segment routing: Disabled
  Segment routing adjacency   : Disabled
  Effective SRGB               : 16000 24000
  Segment routing local block  : 15000 15999
Segment routing tunnel count: 0
```

- 可执行特性 **filesystem** 相关的所有读写类型命令。（以配置设备发送 **FTP** 报文的源 IP 地址为 **192.168.0.60** 为例）

```
[Sysname-a] ftp client source ip 192.168.0.60
[Sysname-a] quit
```

- 不能执行特性 **filesystem** 相关的执行类型命令。（以进入 **FTP** 视图为例）

```
<Sysname-a> ftp
Permission denied.
```

通过显示信息可以确认配置生效。

3.7 配置文件

```
#
telnet server enable
#
interface GigabitEthernet1/0/1
ip address 192.168.1.50 24
#
line vty 0 63
authentication-mode scheme
user-role network-operator
#
domain bbb
authentication login local
authorization login local
#
role name role1
rule 1 permit read write feature ospf
rule 2 permit read write feature filesystem
#
local-user telnetuser class manage
password hash $h$6$kZwlrKFsAY4lhgUz$+teVly8gmKN4Mr00VWgXQTB8ai94gKHLrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6AlupH2jbmRoTcfDzZ9Gmw==
service-type telnet
authorization-attribute user-role role1
#
```

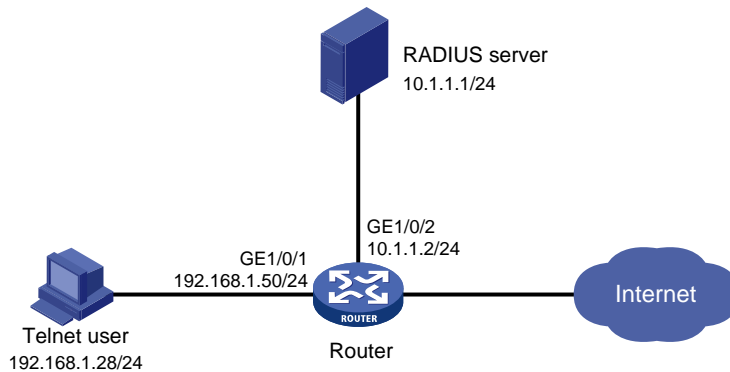
4 Telnet 用户的 RADIUS 用户角色授权配置举例

4.1 组网需求

如图 2 所示，Telnet 用户主机与设备相连，设备与一台 RADIUS 服务器相连，要实现 RADIUS 服务器对登录设备的 Telnet 用户进行认证和授权，使得 Telnet 用户具有如下用户权限：

- 允许用户执行 ISP 视图下的所有命令；
- 允许用户执行 ARP 和 RADIUS 特性中读和写类型的命令；
- 允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令，并只具有操作 VLAN 10~VLAN 20 的权限；
- 允许用户执行进入接口视图以及接口视图下的相关命令，并具有操作接口 GigabitEthernet6/1~GigabitEthernet6/3 的权限。

图2 Telnet 用户 RADIUS 认证/授权配置组网图



4.2 配置思路

- 为了使 Telnet 用户可以执行 ARP 和 RADIUS 特性的读写类型命令，可创建特性组 `feature-group1`，配置包含 ARP 和 RADIUS 特性。
- 为了授权 Telnet 用户可以执行所要求权限的命令，需要配置对应的用户角色规则和资源控制策略。
- 为了使 Telnet 用户能够具备以上权限，需要在 RADIUS 服务器上对 Telnet 用户授权用户角色 `role1`。

4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.4 配置注意事项

- 一个 ISP 域被配置为缺省的 ISP 域后将不能够被删除，必须首先使用命令 `undo domain default enable` 将其修改为非缺省 ISP 域，然后才可以被删除。
- 由于 RADIUS 服务器的授权信息是随认证应答报文发给 RADIUS 客户端的，所以必须保证认证和授权方法相同。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。

4.5 配置步骤

4.5.1 设备配置

(1) 配置接口和路由

配置接口 `GigabitEthernet1/0/1` 的 IP 地址，Telnet 用户将通过该地址连接设备。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 192.168.1.50 255.255.255.0
[Sysname-GigabitEthernet1/0/1] quit
# 配置接口 GigabitEthernet1/0/2 的 IP 地址，设备将通过该地址与服务器通信。
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ip address 10.1.1.2 255.255.255.0
[Sysname-GigabitEthernet1/0/2] quit
# 配置缺省路由，使得 Telnet 用户到 RADIUS 服务器路由可达。
[Sysname] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

(2) 配置 Telnet 用户登录设备的认证方式

```
# 开启设备的 Telnet 服务器功能。
[Sysname] telnet server enable
# 配置 Telnet 用户登录采用 AAA 认证方式。
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

(3) 配置 RADIUS 方案和认证服务器

```
# 创建 RADIUS 方案 rad。
[Sysname] radius scheme rad
# 配置主认证/授权服务器的 IP 地址为 10.1.1.1，主计费服务器的 IP 地址为 10.1.1.1。
[Sysname-radius-rad] primary authentication 10.1.1.1
[Sysname-radius-rad] primary accounting 10.1.1.1
# 配置与认证/授权服务器、主计费服务器交互报文时的共享密钥为明文 aabbcc。
[Sysname-radius-rad] key authentication simple aabbcc
[Sysname-radius-rad] key accounting simple aabbcc
[Sysname-radius-rad] quit
```

(4) 配置 ISP 域 bbb 的 AAA 方法

```
# 创建 ISP 域 bbb，为 login 用户配置的 AAA 认证方法为 RADIUS 认证、RADIUS 授权、RADIUS 计费。
[Sysname] domain bbb
[Sysname-isp-bbb] authentication login radius-scheme rad
[Sysname-isp-bbb] authorization login radius-scheme rad
[Sysname-isp-bbb] accounting login radius-scheme rad
[Sysname-isp-bbb] quit
```

(5) 配置特性组

```
# 创建特性组 fgroup1。
[Sysname] role feature-group name fgroup1
# 配置特性组 fgroup1 中包含特性 ARP 和 RADIUS。
[Sysname-featuregrp-fgroup1] feature arp
[Sysname-featuregrp-fgroup1] feature radius
[Sysname-featuregrp-fgroup1] quit
```

(6) 在设备上创建用户角色 role1，并配置用户角色规则和资源控制策略

```
# 创建用户角色 role1。
[Sysname] role name role1
```

```

# 配置用户角色规则 1，允许用户执行 ISP 视图下的所有命令。
[Sysname-role-role1] rule 1 permit command system-view ; domain *
# 配置用户角色规则 2，允许用户执行特性组 fgroup1 中所有特性的读和写类型的命令。
[Sysname-role-role1] rule 2 permit read write feature-group fgroup1
# 配置用户角色规则 3，允许用户执行创建 VLAN 的命令。
[Sysname-role-role1] rule 3 permit command system-view ; vlan *
# 配置用户角色规则 4，允许用户执行进入接口视图以及接口视图下的相关命令。
[Sysname-role-role1] rule 4 permit command system-view ; interface *
# 进入 VLAN 策略视图，允许用户具有操作 VLAN 10~VLAN 20 的权限。
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 10 to 20
[Sysname-role-role1-vlanpolicy] quit
# 进入接口策略视图，允许用户具有操作接口 GigabitEthernet6/1~GigabitEthernet6/3 的权限。
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 6/1 to gigabitethernet 6/3
[Sysname-role-role1-ifpolicy] quit
[Sysname-role-role1] quit

```

4.5.2 RADIUS 服务器配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 RADIUS 服务器的基本配置。

增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置认证及计费的端口号分别为“1812”和“1813”；
- 设置与 AC 交互报文时使用的认证、计费共享密钥和确认共享密钥为“aabbcc”；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 ? 帮助

接入配置

认证端口 *	<input type="text" value="1812"/>	计费端口 *	<input type="text" value="1813"/>
组网方式	<input type="text" value="不启用混合组网"/>	业务类型	<input type="text" value="设备管理业务"/>
接入设备类型	<input type="text" value="H3C(General)"/>	接入设备分组	<input type="text" value="无"/>
共享密钥 *	<input type="text" value="*****"/>	确认共享密钥 *	<input type="text" value="*****"/>
业务分组	<input type="text" value="未分组"/>		

设备列表

设备名称	设备IP地址	设备型号	备注	删除
	10.1.1.2			<input type="button" value="删除"/>

共有1条记录。

增加设备管理用户。

选择“用户”页签，单击导航树中的[接入用户管理/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 创建用户名，这里输入“telnetuser@bbb”，并配置密码和确认密码；
- 选择服务类型为“Telnet”；
- 添加用户角色名“role1”；
- 添加所管理设备的IP地址，IP地址范围为“10.1.1.0~10.1.1.10”；
- 单击<确定>按钮完成操作。

图4 增加设备管理用户

用户 > 设备管理用户 > 增加设备管理用户 ? 帮助

增加设备管理用户

设备管理用户基本信息

帐号名 * ?

用户密码 *

密码确认 *

服务类型

EXEC权限级别 ?

角色名

提示

注意：输入绑定的多个角色名时，每行只能写一个角色名，且角色名占用字节数与角色名个数（出现多个相同角色名时被视为一个角色名）总和不超过234。例如，假定输入10个角色，则角色占用字节数应不超过224个。

绑定的用户IP地址列表

起始IP地址	结束IP地址	删除
未找到符合条件的记录。		

所管理设备IP地址列表

起始IP地址	结束IP地址	删除
10.1.1.0	10.1.1.10	

4.6 验证配置

(1) 查看用户角色和特性组信息

通过 **display role** 命令查看用户角色 **role1** 的信息。

```
<Sysname> display role name role1
Role: role1
Description:
VLAN policy: deny
Permitted VLANs: 10 to 20
Interface policy: deny
Permitted interfaces: GigabitEthernet6/1 to GigabitEthernet6/3
VPN instance policy: permit (default)
Security zone policy: permit (default)
```

```
-----
Rule   Perm  Type  Scope      Entity
-----
```

```

1      permit      command      system-view ; domain *
2      permit RW-  feature-group fgroup1
3      permit      command      system-view ; vlan *
4      permit      command      system-view ; interface *
R:Read W:Write X:Execute

```

(2) 用户登录设备

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 `telnetuser@bbb` 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50
```

```

*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

```

```

login: telnetuser@bbb
Password:
<Sysname>

```

(3) 验证用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- 可执行 **ISP** 视图下所有的命令。

```

<Sysname> system-view
[Sysname] domain abc
[Sysname-isp-abc] authentication login radius-scheme abc
[Sysname-isp-abc] quit

```

- 可执行 **RADIUS** 特性中读和写类型的命令。（ARP 特性同，此处不再举例）

```

[Sysname] radius scheme rad
[Sysname-radius-rad] primary authentication 2.2.2.2
[Sysname-radius-rad] display radius scheme rad

```

- 可操作 **VLAN 10~VLAN 20**。（以创建 VLAN 10、VLAN 30 为例）

```

[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] vlan 30
Permission denied.

```

- 可操作接口 **GigabitEthernet6/1~GigabitEthernet6/3**。（以接口 GigabitEthernet6/1 为例）

```

[Sysname] interface gigabitethernet 6/1
[Sysname-GigabitEthernet6/1] ip address 1.1.1.1 24
[Sysname-GigabitEthernet6/1] quit

```

- 不能操作其它接口。（以进入 GigabitEthernet6/0 接口视图为例）

```

[Sysname] interface gigabitethernet 6/0
Permission denied.

```

通过显示信息可以确认配置生效。

4.7 配置文件

```
#
telnet server enable
#
interface GigabitEthernet1/0/1
ip address 192.168.1.50 24
#
interface GigabitEthernet1/0/2
ip address 10.1.1.2 24
#
line vty 0 63
authentication-mode scheme
user-role network-operator
#
ip route-static 0.0.0.0 0 10.1.1.1
#
radius scheme rad
primary authentication 10.1.1.1
primary accounting 10.1.1.1
key authentication cipher $c$3$JzDegvL0G5KZICJhzscTHLA4WasBVh0UOw==
key accounting cipher $c$3$CdejNYYxvjW0Y+Zydi4rZgBwjYb4h6LKmg==
#
domain bbb
authentication login radius-scheme rad
authorization login radius-scheme rad
accounting login radius-scheme rad
#
role feature-group name fgroup1
feature arp
feature radius
#
role name role1
rule 1 permit command system-view ; domain *
rule 2 permit read write feature-group fgroup1
rule 3 permit command system-view ; vlan *
rule 4 permit command system-view ; interface *
vlan policy deny
permit vlan 10 to 20
interface policy deny
permit interface GigabitEthernet6/1 to GigabitEthernet6/3
#
```

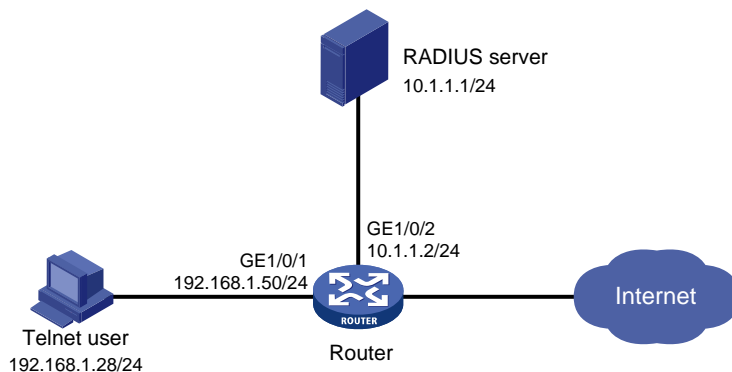
5 配置用户在某些 VPN 中具有特定特性的执行权限举例

5.1 组网需求

如图5所示,为了加强用户登录的安全性,采用 RADIUS 服务器对登录设备的 Telnet 用户进行认证、授权,使得 Telnet 用户有如下权限:

- 允许执行系统预定义特性组 L3 相关的所有命令。
- 允许执行所有以 **display** 开头的命令。
- 只允许对特定 VPN 实例 vpn1、vpn2 和 vpn3 进行操作。

图5 某些 VPN 中具有特定特性的执行权限配置组网图



5.2 配置思路

- 为了授权 Telnet 用户可以执行所要求权限的命令,需要创建用户角色 **role1** 并配置对应的用户角色规则和资源控制策略。
- 为了使 Telnet 用户能够具备以上权限,需要在 RADIUS 服务器上配置 Telnet 用户授权用户角色 **role1**。

5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

5.4 配置注意事项

- 一个 ISP 域被配置为缺省的 ISP 域后将不能够被删除,必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域,然后才可以被删除。
- 由于 RADIUS 服务器的授权信息是随认证应答报文发给 RADIUS 客户端的,所以必须保证认证和授权方法相同。
- 一个用户角色中允许创建多条规则,各规则以创建时指定的编号为唯一标识,被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突,则规则编号大的有效。例如,规则 1 允许执行命令 A,规则 2 允许执行命令 B,规则 3 禁止执行命令 A,则最终规则 2 和规则 3 生效,即禁止执行命令 A,允许执行命令 B。

5.5 配置步骤

5.5.1 设备配置

(1) 配置接口和路由

为接口 GigabitEthernet1/0/1 配置 IP 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 192.168.1.50 24
[Sysname-GigabitEthernet1/0/1] quit
```

为接口 GigabitEthernet1/0/2 置 IP 地址。

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ip address 10.1.1.2 24
[Sysname-GigabitEthernet1/0/2] quit
```

配置缺省路由，使得 Telnet 用户到 RADIUS 服务器路由可达。

```
[Sysname] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

(2) 配置 Telnet 用户登录设备的认证方式

开启设备的 Telnet 服务器功能。

```
[Sysname] telnet server enable
```

在编号为 0~63 的 VTY 用户线下，配置 Telnet 用户登录采用 AAA 认证方式。

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

(3) 配置 RADIUS 方案和认证服务器

创建 RADIUS 方案 rad。

```
[Sysname] radius scheme rad
```

配置主认证/授权服务器的 IP 地址为 10.1.1.1，主计费服务器的 IP 地址为 10.1.1.1。

```
[Sysname-radius-rad] primary authentication 10.1.1.1
[Sysname-radius-rad] primary accounting 10.1.1.1
```

配置与认证/授权服务器、主计费服务器交互报文时的共享密钥为明文 aabbcc。

```
[Sysname-radius-rad] key authentication simple aabbcc
[Sysname-radius-rad] key accounting simple aabbcc
[Sysname-radius-rad] quit
```

(4) 配置 ISP 域 bbb 的 AAA 方法

创建 ISP 域 bbb，为 login 用户配置的 AAA 认证方法为 RADIUS 认证、RADIUS 授权、RADIUS 计费。

```
[Sysname] domain bbb
[Sysname-isp-bbb] authentication login radius-scheme rad
[Sysname-isp-bbb] authorization login radius-scheme rad
[Sysname-isp-bbb] accounting login radius-scheme rad
[Sysname-isp-bbb] quit
```

(5) 在设备上创建用户角色 role1，并配置用户角色规则和资源控制策略

创建用户角色 role1，进入用户角色视图。

```
[Sysname] role name role1
```

```
# 配置用户角色规则 1，允许用户执行预定义特性组 L3 相关的所有命令。
[Sysname-role-role1] rule 1 permit execute read write feature-group L3
# 配置用户角色规则 2，允许用户执行所有以 display 开头的命令。
[Sysname-role-role1] rule 2 permit command display *
# 进入用户角色 VPN 策略视图，配置允许用户具有操作 VPN 实例 vpn1、vpn2 和 vpn3 的权限。
[Sysname-role-role1] vpn policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn1 vpn2 vpn3
[Sysname-role-role1-vpnpolicy] quit
[Sysname-role-role1] quit
```

5.5.2 RADIUS 服务器配置



下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 RADIUS 服务器的基本配置。

增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理>接入设备管理>接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置认证及计费的端口号分别为“1812”和“1813”；
- 设置与 AC 交互报文时使用的认证、计费共享密钥和确认共享密钥为“aabbcc”；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 ? 帮助

接入配置

认证端口 * <input type="text" value="1812"/>	计费端口 * <input type="text" value="1813"/>
组网方式 <input type="text" value="不启用混合组网"/>	业务类型 <input type="text" value="设备管理业务"/>
接入设备类型 <input type="text" value="H3C(General)"/>	接入设备分组 <input type="text" value="无"/>
共享密钥 * <input type="password" value="*****"/>	确认共享密钥 * <input type="password" value="*****"/>
业务分组 <input type="text" value="未分组"/>	

设备列表

设备名称	设备IP地址	设备型号	备注	删除
	10.1.1.2			

共有1条记录。

增加设备管理用户。

选择“用户”页签，单击导航树中的[接入用户管理/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 创建用户名，这里输入“telnetuser@bbb”，并配置密码和确认密码；
- 选择服务类型为“Telnet”；
- 添加用户角色名“role1”；
- 添加所管理设备的IP地址，IP地址范围为“10.1.1.0~10.1.1.10”；
- 单击<确定>按钮完成操作。

图7 增加设备管理用户

用户 > 设备管理用户 > 增加设备管理用户 ? 帮助

增加设备管理用户

设备管理用户基本信息

帐号名 * ?

用户密码 *

密码确认 *

服务类型

EXEC权限级别 ?

角色名

提示

注意：输入绑定的多个角色名时，每行只能写一个角色名，且角色名占用字节数与角色名个数（出现多个相同角色名时被视为一个角色名）总和不超过234。例如，假定输入10个角色，则角色占用字节数应不超过224个。

绑定的用户IP地址列表

起始IP地址	结束IP地址	删除
未找到符合条件的记录。		

所管理设备IP地址列表

起始IP地址	结束IP地址	删除
10.1.1.0	10.1.1.10	

5.6 验证配置

(1) 查看用户角色和特性组信息

通过 **display role** 命令查看用户角色 **role1** 的信息。

```
<Sysname> display role name role1
Role: role1
Description:
VLAN policy: permit (default)
Interface policy: permit (default)
VPN instance policy: deny
Permitted VPN instances: vpn1, vpn2, vpn3
Security zone policy: permit (default)
-----
Rule   Perm  Type  Scope      Entity
-----
1      permit RWX  feature-group L3
```

```
2      permit      command      display *
```

```
R:Read W:Write X:Execute
```

通过 **display role feature-group** 命令查看特性组 L3 中包括的特性信息，此处不详细介绍。

(2) 用户登录设备

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 `telnetuser@bbb` 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50
```

```
*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****
```

```
login: telnetuser@bbb
```

```
Password:
```

```
<Sysname>
```

(3) 验证用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- 可执行系统预定义特性组 L3 中的所有命令。（以创建 VPN 实例 `vpn1` 并配置其 RD 为 22:1 为例）

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 22:1
[Sysname-vpn-instance-vpn1] display this
#
ip vpn-instance vpn1
  route-distinguisher 22:1
#
return
[Sysname-vpn-instance-vpn1] quit
```

- 不能操作其它 VPN 实例。（以 VPN 实例 `vpn5` 为例）

```
[Sysname] ip vpn-instance vpn5
Permission denied.
```

通过显示信息可以确认配置生效。

5.7 配置文件

```
#
telnet server enable
#
interface GigabitEthernet1/0/1
  ip address 192.168.1.50 24
#
interface GigabitEthernet1/0/2
```

```

ip address 10.1.1.2 24
#
line vty 0 63
  authentication-mode scheme
  user-role network-operator
#
ip route-static 0.0.0.0 0 10.1.1.1
#
radius scheme rad
  primary authentication 10.1.1.1
  primary accounting 10.1.1.1
  key authentication cipher $c$3$JzDegvL0G5KZICJhzscTHLA4WasBVh0UOw==
  key accounting cipher $c$3$CdejNYYxvjW0Y+Zydi4rZgBwjYb4h6LKmg==
#
domain bbb
  authentication login radius-scheme rad
  authorization login radius-scheme rad
  accounting login radius-scheme rad
#
role name role1
  rule 1 permit read write execute feature-group L3
  rule 2 permit command display *
  vpn-instance policy deny
    permit vpn-instance vpn1
    permit vpn-instance vpn2
    permit vpn-instance vpn3
#

```

6 创建新用户角色并授权更改用户权限举例

6.1 组网需求

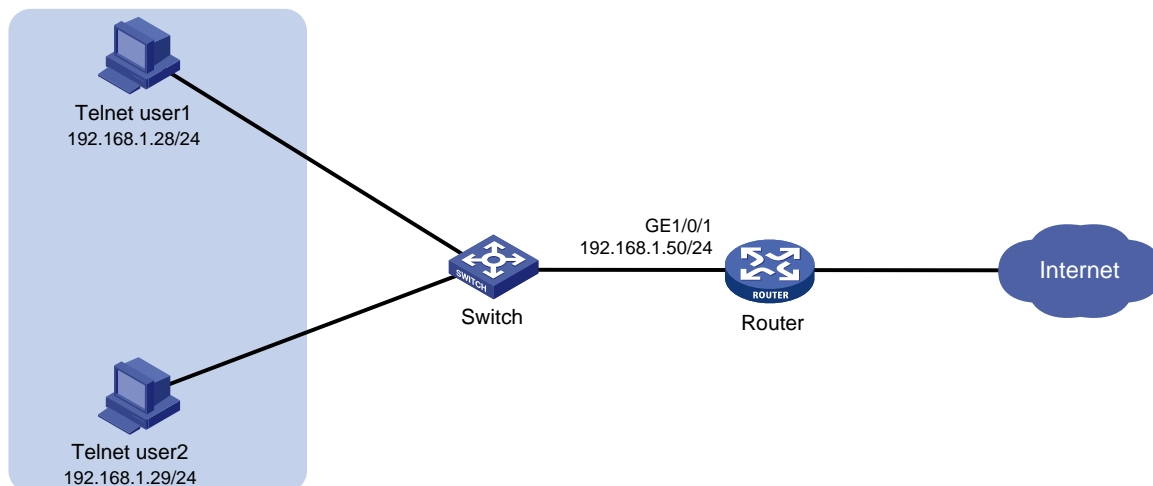
如图 8 所示，为了加强用户登录的安全性，采用本地 AAA 认证对登录设备的 Telnet 用户进行认证。Telnet 用户 telnetuser1 和 telnetuser2 通过 ISP 域 bbb 接入网络，成功登录设备后，均被赋予用户角色 role1，具有如下权限：

- 允许执行所有以 **display** 开头的命令。
- 允许执行创建 VLAN 的命令。
- 只允许对 VLAN 10~VLAN 15 进行操作。
- 只允许对特定接口 GigabitEthernet6/1 进行操作。

现要求为 Telnet 用户 telnetuser1 增加对设备的操作权限，具体需求如下：

- 允许对 VLAN 16~VLAN 20 进行操作。
- 允许对特定接口 GigabitEthernet6/2~GigabitEthernet6/3 进行操作。

图8 更改用户权限配置组网图



6.2 配置思路

- 为了使 Telnet 用户 telnetuser1 增加上述权限，并且不改变 Telnet 用户 telnetuser2 的权限，可以通过创建用户角色 role2，并对 Telnet 用户 telnetuser1 授予用户角色 role2。
- 为了增加 Telnet 用户 telnetuser1 可执行所要求权限的命令，需要配置用户角色规则和资源控制策略。

6.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

6.4 配置注意事项

- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。
- 用户可以同时被授权多个用户角色。拥有多个用户角色的用户可获得这些角色中被允许执行的功能以及被允许操作的资源的集合。
- 对当前在线用户授权新的用户角色，待该用户重新上线后才能生效。

6.5 配置步骤

(1) 配置接口

为接口 GigabitEthernet1/0/1 配置 IP 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 192.168.1.50 24
```

- ```
[Sysname-GigabitEthernet1/0/1] quit
```
- (2) 配置 Telnet 用户登录设备的认证方式
- # 开启设备的 Telnet 服务器功能。
- ```
[Sysname] telnet server enable
```
- # 在编号为 0~63 的 VTY 用户线下，配置 Telnet 用户登录采用 AAA 认证方式。
- ```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```
- (3) 配置 ISP 域 bbb 的 AAA 方法
- # 创建 ISP 域 bbb，为 login 用户配置的 AAA 方法为本地认证、本地授权。
- ```
[Sysname] domain bbb
[Sysname-isp-bbb] authentication login local
[Sysname-isp-bbb] authorization login local
[Sysname-isp-bbb] quit
```
- (4) 配置设备管理类本地用户 telnetuser1 和 telnetuser2 的密码和服务类型
- # 创建设备管理类本地用户 telnetuser1。
- ```
[Sysname] local-user telnetuser1 class manage
```
- # 配置用户的密码是明文的 123456TESTplat&!。
- ```
[Sysname-luser-manage-telnetuser1] password simple 123456TESTplat&!
```
- # 指定用户的服务类型是 Telnet。
- ```
[Sysname-luser-manage-telnetuser1] service-type telnet
[Sysname-luser-manage-telnetuser1] quit
```
- # 创建设备管理类本地用户 telnetuser2。
- ```
[Sysname] local-user telnetuser2 class manage
```
- # 配置用户的密码是明文的 123456TESTplat&!。
- ```
[Sysname-luser-manage-telnetuser2] password simple 123456TESTplat&!
```
- # 指定用户的服务类型是 Telnet。
- ```
[Sysname-luser-manage-telnetuser2] service-type telnet
[Sysname-luser-manage-telnetuser2] quit
```
- (5) 创建用户角色 role1，并配置用户角色规则
- # 创建用户角色 role1，进入用户角色视图。
- ```
[Sysname] role name role1
```
- # 配置用户角色规则 1，允许用户执行所有以 **display** 开头的命令。
- ```
[Sysname-role-role1] rule 1 permit command display *
```
- # 配置用户角色规则 2，允许执行进入 VLAN 视图命令。
- ```
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```
- # 配置用户角色规则 3，允许执行进入接口视图命令以及进入接口视图后的相关命令。
- ```
[Sysname-role-role1] rule 3 permit command system-view ; interface *
```
- # 进入用户角色 VLAN 策略视图，配置允许用户具有操作 VLAN 10~VLAN 15 的权限。
- ```
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 10 to 15
[Sysname-role-role1-vlanpolicy] quit
```
- # 进入用户角色接口策略视图，配置允许用户具有操作接口 GigabitEthernet6/1 的权限。



- ```
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 6/1
[Sysname-role-role1-ifpolicy] quit
[Sysname-role-role1] quit
```
- (6) 为本地用户 **telnetuser1** 和 **telnetuser2** 配置授权用户角色
- # 进入设备管理类本地用户 **telnetuser1** 视图。
- ```
[Sysname] local-user telnetuser1 class manage
指定用户 telnetuser1 的授权角色 role1。
[Sysname-luser-manage-telnetuser1] authorization-attribute user-role role1
为保证用户仅使用授权的用户角色 role1，删除用户 telnetuser1 具有的缺省用户角色
network-operator。
[Sysname-luser-manage-telnetuser1] undo authorization-attribute user-role
network-operator
[Sysname-luser-manage-telnetuser1] quit
进入设备管理类本地用户 telnetuser2 视图。
[Sysname] local-user telnetuser2 class manage
指定用户 telnetuser2 的授权角色 role1。
[Sysname-luser-manage-telnetuser2] authorization-attribute user-role role1
为保证用户仅使用授权的用户角色 role1，删除用户 telnetuser2 具有的缺省用户角色
network-operator。
[Sysname-luser-manage-telnetuser2] undo authorization-attribute user-role
network-operator
[Sysname-luser-manage-telnetuser2] quit
```
- (7) 创建用户角色 **role2**，并配置用户角色规则
- # 创建用户角色 **role2**，进入用户角色视图。
- ```
[Sysname] role name role2
# 配置用户角色规则 1，允许执行进入接口视图命令以及进入接口视图后的相关命令。
[Sysname-role-role2] rule 1 permit command system-view ; interface *
```
- (8) 为用户角色 **role2** 配置 VLAN 资源控制策略
- # 进入用户角色 VLAN 策略视图，配置允许用户具有操作 VLAN 16~VLAN 20 的权限。
- ```
[Sysname-role-role2] vlan policy deny
[Sysname-role-role2-vlanpolicy] permit vlan 16 to 20
[Sysname-role-role2-vlanpolicy] quit
进入用户角色接口策略视图，配置允许用户具有操作接口 GigabitEthernet6/2~
GigabitEthernet6/3 的权限。
[Sysname-role-role2] interface policy deny
[Sysname-role-role2-ifpolicy] permit interface gigabitethernet 6/2 to gigabitethernet
6/3
[Sysname-role-role2-ifpolicy] quit
[Sysname-role-role2] quit
```
- (9) 为本地用户 **telnetuser1** 配置授权用户角色
- # 进入设备管理类本地用户 **telnetuser1** 视图。
- ```
[Sysname] local-user telnetuser1 class manage
# 指定用户 telnetuser1 的授权角色 role2。
```

```
[Sysname-luser-manage-telnetuser1] authorization-attribute user-role role2
[Sysname-luser-manage-telnetuser1] quit
```

6.6 验证配置

6.6.1 配置更改用户权限前的验证

(1) 查看用户角色和特性组信息

通过 **display role** 命令查看用户角色 **role1** 的信息。

```
<Sysname> display role name role1
Role: role1
  Description:
  VLAN policy: deny
  Permitted VLANs: 10 to 15
  Interface policy: deny
  Permitted interfaces: GigabitEthernet6/1
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
-----
Rule      Perm   Type  Scope      Entity
-----
1         permit      command    display *
2         permit      command    system-view ; vlan *
3         permit      command    system-view ; interface *
R:Read W:Write X:Execute
```

(2) 用户登录设备

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 **telnetuser1@bbb** 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50

*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

login: telnetuser1@bbb
Password:
<Sysname>
```

(3) 验证用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- o 能够创建 VLAN 15。
[Sysname] vlan 15
[Sysname-vlan15] quit
- o 不能创建 VLAN 20。
[Sysname] vlan 20

Permission denied.

- o 能够操作 GigabitEthernet6/1 接口。

```
[Sysname] interface gigabitethernet 6/1
[Sysname-GigabitEthernet6/1] ip address 1.1.1.1 24
[Sysname-GigabitEthernet6/1] quit
```

通过显示信息可以确认配置生效。

6.6.2 配置更改用户权限后的验证

- (1) 查看用户角色和特性组信息

通过 **display role** 命令查看用户角色 **role2** 的信息。

显示用户角色 **role2** 的信息。

```
<Sysname> display role name role2
Role: role2
  Description:
  VLAN policy: deny
  Permitted VLANs: 16 to 20
  Interface policy: deny
  Permitted interfaces: GigabitEthernet6/2~GigabitEthernet6/3
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
-----
Rule      Perm   Type  Scope      Entity
-----
1         permit  command  system-view ; interface *
R:Read W:Write X:Execute
```

- (2) 用户登录设备

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 **telnetuser1@bbb** 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50
```

```
*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****
```

```
login: telnetuser1@bbb
```

```
Password:
```

```
<Sysname>
```

- (3) 验证用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- o 可创建 VLAN 16。

```
[Sysname] vlan 16
[Sysname-vlan16] quit
```

- o 能够操作 GigabitEthernet6/2 接口。

```
[Sysname] interface gigabitethernet 6/2
[Sysname-GigabitEthernet6/2] ip address 2.2.2.2 24
[Sysname-GigabitEthernet6/2] quit
```

- 不能操作其它接口。（以进入 **GigabitEthernet6/0** 接口视图为例）

```
[Sysname] interface gigabitethernet 6/0
Permission denied.
```

通过显示信息可以确认配置生效。

6.7 配置文件

```
#
telnet server enable
#
interface GigabitEthernet1/0/1
ip address 192.168.1.50 24
#
line vty 0 63
authentication-mode scheme
user-role network-operator
#
domain bbb
authentication login local
authorization login local
#
role name role1
rule 1 permit command display *
rule 2 permit command system-view ; vlan *
rule 3 permit command system-view ; interface *
vlan policy deny
permit vlan 10 to 15
interface policy deny
permit interface GigabitEthernet6/1
#
role name role2
rule 1 permit command system-view ; interface *
vlan policy deny
permit vlan 16 to 20
interface policy deny
permit interface GigabitEthernet6/2 to GigabitEthernet6/3
#
local-user telnetuser1 class manage
password hash $h$6$kZwlrKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKhlrys50kytGf4
kT+nz5X1ZGASjc282CYAR6AlupH2jbmRoTcfDzZ9Gmw==
service-type telnet
authorization-attribute user-role role1
authorization-attribute user-role role2
#
local-user telnetuser2 class manage
```

```

password hash TPcgyTQJZShe$h$6$vaSj2xKc8yFiNdfQ$Jzb3PXo21t4jk KSZqJUvhjP634Wo1/
Qx8TLU748IHoeui0w5n/XRzpnqbNnpixikym39gGJCwYw==
service-type telnet
authorization-attribute user-role role1
#

```

7 配置用户具有切换用户角色权限举例

7.1 组网需求

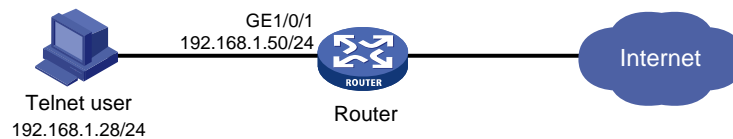
如图9所示，为了加强用户登录的安全性，采用本地 AAA 认证对登录设备的 Telnet 用户进行认证。登录设备的 Telnet 用户能够进行用户角色的切换，即在不下线的情况下，临时改变自身对系统的操作权限。当前 Telnet 用户被授权为用户角色 role1，用户角色 role1 具有如下权限：

- 允许执行系统预定义特性组 L3 相关的所有命令。
- 允许执行所有以 **display** 开头的命令。
- 允许执行所有以 **super** 开头的命令。
- 具有所有接口、VLAN 和 VPN 实例资源的操作权限。

现要求，Telnet 用户能够被切换到用户角色 role2 和 network-operator，其中用户角色 role2 具有如下权限：

- 允许执行系统预定义特性组 L2 相关的所有命令。
- 具有所有接口、VLAN 和 VPN 实例资源的操作权限。

图9 切换用户角色权限配置组网图



7.2 配置思路

- 缺省情况下，用户角色切换的认证方式为 **local**。在本例中 Telnet 用户登录设备的认证方式为本地 AAA 认证，因此，配置用户角色切换时的认证方式为 **local**。
- 为了使 Telnet 用户 **telnetuser** 能够进行切换用户角色，需要创建本地用户角色 **role1** 和 **role2**，并配置相应的配置用户角色规则和资源控制策略。
- 为了保证操作的安全性，Telnet 用户将用户角色切换到不同的用户角色时，需要配置相应切换密码。

7.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

7.4 配置注意事项

- 一个 ISP 域被配置为缺省的 ISP 域后将不能够被删除，必须首先使用命令 `undo domain default enable` 将其修改为非缺省 ISP 域，然后才可以被删除。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。
- 切换后的用户角色只对当前登录生效，用户重新登录后，又会恢复到原有用户角色。

7.5 配置步骤

(1) 配置接口

为接口 GigabitEthernet1/0/1 配置 IP 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 192.168.1.50 24
[Sysname-GigabitEthernet1/0/1] quit
```

(2) 配置 Telnet 用户登录设备的认证方式

开启设备的 Telnet 服务器功能。

```
[Sysname] telnet server enable
# 在编号为 0~63 的 VTY 用户线下，配置 Telnet 用户登录采用 AAA 认证方式。
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

(3) 配置 ISP 域 bbb 的 AAA 方法

创建 ISP 域 bbb，为 login 用户配置的 AAA 方法为本地认证、本地授权。

```
[Sysname] domain bbb
[Sysname-isp-bbb] authentication login local
[Sysname-isp-bbb] authorization login local
[Sysname-isp-bbb] quit
```

(4) 配置设备管理类本地用户 telnetuser 的密码和服务类型

创建设备管理类本地用户 telnetuser。

```
[Sysname] local-user telnetuser class manage
# 配置用户的密码是明文的 123456TESTplat&!。
[Sysname-luser-manage-telnetuser] password simple 123456TESTplat&!
# 指定用户的服务类型是 Telnet。
```

```
[Sysname-luser-manage-telnetuser] service-type telnet
[Sysname-luser-manage-telnetuser] quit
```

(5) 创建用户角色 role1，并配置用户角色规则

创建用户角色 role1，进入用户角色视图。

```
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行预定义特性组 L3 相关的所有命令。

- ```
[Sysname-role-role1] rule 1 permit execute read write feature-group L3
配置用户角色规则 2，允许用户执行所有以 display 开头的命令。
[Sysname-role-role1] rule 2 permit command display *
配置用户角色规则 3，允许用户执行所有以 super 开头的命令。
[Sysname-role-role1] rule 3 permit command super *
[Sysname-role-role1] quit
```
- (6) 创建用户角色 **role2**，并配置用户角色规则
- ```
# 创建用户角色 role2，进入用户角色视图。
[Sysname] role name role2
# 配置用户角色规则 1，允许用户执行预定义特性组 L2 相关的所有命令。
[Sysname-role-role2] rule 1 permit execute read write feature-group L2
[Sysname-role-role2] quit
```
- (7) 为本地用户配置授权用户角色
- ```
进入设备管理类本地用户 telnetuser 视图。
[Sysname] local-user telnetuser class manage
指定用户 telnetuser 的授权角色为 role1。
[Sysname-luser-manage-telnetuser] authorization-attribute user-role role1
为保证用户仅使用授权的用户角色 role1，删除用户 telnetuser 具有的缺省用户角色 network-operator。
[Sysname-luser-manage-telnetuser] undo authorization-attribute user-role network-operator
[Sysname-luser-manage-telnetuser] quit
```
- (8) 配置用户角色切换的方式及切换密码
- ```
# 配置 Telnet 用户切换用户角色时采用 local 认证方式（系统缺省值为 local）。
[Sysname] super authentication-mode local
# 配置 Telnet 用户将用户角色切换到 role2 时使用的密码为明文密码 123456TESTplat&!。
[Sysname] super password role role2 simple 123456TESTplat&!
# 配置 Telnet 用户将用户角色切换到 network-operator 时使用的密码为明文密码 987654TESTplat&!。
[Sysname] super password role network-operator simple 987654TESTplat&!
```

7.6 验证配置

- (1) 查看用户角色和特性组信息

通过 **display role** 命令查看用户角色 **role1**、**role2** 和 **network-operator** 的信息。

显示用户角色 **role1** 的信息。

```
<Sysname> display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
-----
```

Rule	Perm	Type	Scope	Entity
1	permit	RWX	feature-group	L3
2	permit		command	display *
3	permit		command	super *

R:Read W:Write X:Execute

显示用户角色 **role2** 的信息。

<Sysname> display role name role2

Role: role2

Description:

VLAN policy: permit (default)

Interface policy: permit (default)

VPN instance policy: permit (default)

Security zone policy: permit (default)

Rule	Perm	Type	Scope	Entity
1	permit	RWX	feature-group	L2

R:Read W:Write X:Execute

显示用户角色 **network-operator** 的信息。

<Sysname> display role name network-operator

Role: network-operator

Description: Predefined network operator role has access to all read commands on the Sysname

VLAN policy: permit (default)

Interface policy: permit (default)

VPN instance policy: permit (default)

Security zone policy: permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit		command	display *
sys-2	permit		command	xml
sys-3	deny		command	display history-command all
sys-4	deny		command	display exception *
sys-5	deny		command	display cpu-usage configuration *
sys-6	deny		command	display kernel exception *
sys-7	deny		command	display kernel deadlock *
sys-8	deny		command	display kernel starvation *
sys-9	deny		command	display kernel reboot *
sys-10	deny		command	display memory trace *
sys-11	deny		command	display kernel memory *
sys-12	permit		command	system-view ; local-user *
sys-13	permit		command	system-view ; swichto mdc *
sys-14	permit	R--	xml-element	-
sys-15	deny		command	display security-logfile summary
sys-16	deny		command	system-view ; info-center securi


```

ty-logfile directory *
sys-17 deny          command      security-logfile save
R:Read W:Write X:Execute

```

通过 **display role feature-group** 命令查看特性组 L2 和 L3 中包括的特性信息，此处不详细介绍。

(2) 用户登录设备

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 `telnetuser@bbb` 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50
```

```

*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

```

```

login: telnetuser@bbb
Password:
<Sysname>

```

(3) 验证切换用户角色前的用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- o 可执行特性组 L3 中特性相关的所有命令。（以创建 VPN 实例 `vpn1` 为例）

```

<Sysname> system-view
[Sysname] ip vpn-instance vpn1

```

- o 可执行所有以 **display** 开头的命令。（以显示系统当前日期和时间为例）

```

<Sysname> display clock
09:31:56 UTC Wed 01/01/2014
<Sysname>

```

(4) 验证切换用户角色

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- a. 在用户视图下使用 **super** 命令切换到用户角色 `role2`。

```

<Sysname> super role2
Password:
User privilege role is role2, and only those commands that authorized to the role can be used.
<Sysname>

```

- b. 切换到用户角色 `role2` 后，可执行特性组 L2 中特性相关的所有命令。（以创建 VLAN 10 为例）

```

<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] quit

```

- c. 切换到用户角色 `role2` 后，不能执行非特性组 L2 中特性相关的命令。（以切换到用户角色 `network-operator` 为例）

```
<Sysname> super network-operator
```

Permission denied.

- d. 切换到用户角色 **role2** 后，不能执行以 **display** 开头的命令。（以显示系统当前日期和时间为例）

```
<Sysname> display clock
Permission denied.
```

- e. Telnet 用户重新登录设备后，才能执行所有以 **super** 开头的命令。（以切换到用户角色 **network-operator** 并输入相应的切换密码为例）

```
C:\Documents and Settings\user> telnet 192.168.1.50
```

```
*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
```

```
login: telnetuser@bbb
```

```
Password:
```

```
<Sysname>
```

```
<Sysname> super network-operator
```

```
Password:
```

```
User privilege role is network-operator, and only those commands that authorized
to the role can be used.
```

```
<Sysname>
```

通过显示信息可以确认配置生效。

7.7 配置文件

```
#
telnet server enable
#
interface GigabitEthernet1/0/1
ip address 192.168.1.50 24
#
line vty 0 63
authentication-mode scheme
user-role network-operator
#
super password role role2 hash $h$6$D0kjHFtkkktzgr5g$e673xFnIcKytCj6EDAw+pvwgh3
/ung3WNWHnrUTnXT862B+s7PaLfKTdil8ef71RBOvuJvPAZHjiLjrMPyWHQw==
super password role network-operator hash $h$6$3s5KMmscn9hJ6gPx$IcxbNjUc8u4yxwR
m87b/Jki8BoPAXw/s5bEcPQjQj/cbbXwTVcnQGL91Wod7ssO2rX/wKzfyzAO5VhBTn9Q4zQ==
#
domain bbb
authentication login local
authorization login local
#
role name role1
```

```

rule 1 permit read write execute feature-group L3
rule 2 permit command display *
rule 3 permit command super *
#
role name role2
rule 1 permit read write execute feature-group L2
#
local-user telnetuser class manage
password hash $h$6$kZwlrKFsAY4lhgUz$+teVly8gmKN4Mr00VWgXQTB8ai94gKhlrys50kytGf4
kT+nz5X1ZGASjc282CYAR6AlupH2jbmRoTcfDzZ9Gmw==
service-type telnet
authorization-attribute user-role role1
#

```

8 配置具有流量控制执行权限举例

8.1 组网需求

如图 10 所示，某企业内部为隔离部门 A 和部门 B 之间流量，将不同 VLAN 划分给各部门使用。为了加强各部门网络管理员登录的安全性，采用 RADIUS 服务器对登录设备的 Telnet 用户进行认证、授权。具体需求如下：部门 A 和部门 B 的网络管理员通过 Telnet 登录设备时，分别使用 RADIUS 服务器上配置的用户名 admin-departA 和 admin-departB 以及对应的密码进行认证。

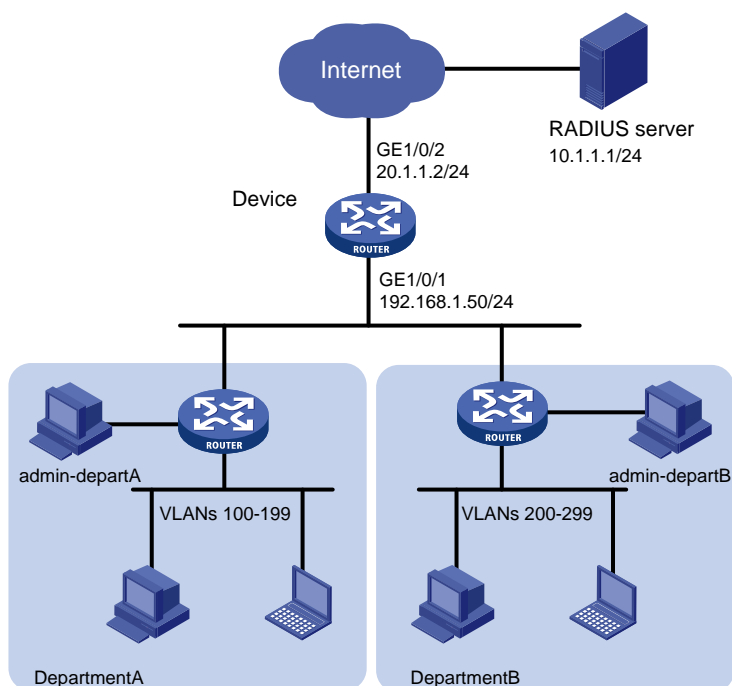
部门 A 网络管理员 admin-departA 有如下权限：

- 具有流量控制策略相关功能的配置权限。
- 禁止操作所有的接口和 VPN 资源。
- 只允许操作 VLAN 100~VLAN 199。

部门 B 网络管理员 admin-departB 有如下权限：

- 具有流量控制策略相关功能的配置权限。
- 禁止操作所有的接口和 VPN 资源。
- 只允许操作 VLAN 200~VLAN 299。

图10 具有部署流量控制策略的执行权限配置组网图



8.2 配置思路

- 创建用户角色 **departA-resource**，通过配置用户角色规则，使其具有 QoS 和 ACL 特性中所有命令的配置权限；通过配置资源控制策略，使其只具有 VLAN 100~VLAN 199 的操作权限，无法操作所有的接口和 VPN 资源。
- 创建用户角色 **departB-resource**，通过配置用户角色规则，使其具有 QoS 和 ACL 特性中所有命令的配置权限；通过配置资源控制策略，使其只具有 VLAN 200~VLAN 299 的操作权限，无法操作所有的接口和 VPN 资源。
- 在 RADIUS 服务器上配置对部门 A 网络管理员授权用户角色 **departA-resource**；对部门 B 网络管理员授权用户角色 **departB-resource**。

8.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

8.4 配置注意事项

由于 RADIUS 服务器的授权信息是随认证应答报文发给 RADIUS 客户端的，所以必须保证认证和授权方法相同。

8.5 配置步骤

8.5.1 设备配置

- (1) 配置接口地址和路由协议

为接口 GigabitEthernet1/0/1 配置 IP 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 192.168.1.50 24
[Sysname-GigabitEthernet1/0/1] quit
```

为接口 GigabitEthernet1/0/2 配置 IP 地址。

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ip address 20.1.1.2 24
[Sysname-GigabitEthernet1/0/2] quit
```

配置 OSPF 协议使网络互通。

```
[Sysname] ospf 1
[Sysname-ospf-1] area 0.0.0.0
[Sysname-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[Sysname-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[Sysname-ospf-1-area-0.0.0.0] quit
[Sysname-ospf-1] quit
```

- (2) 在设备上开启 Telnet 服务器功能，并配置 RADIUS 方案和 ISP 域

开启设备的 Telnet 服务器功能。

```
[Sysname] telnet server enable
```

在编号为 0~63 的 VTY 用户线下，配置 Telnet 用户登录采用 AAA 认证方式。

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

创建 RADIUS 方案 rad。

```
[Sysname] radius scheme rad
```

配置主认证/授权服务器的 IP 地址为 10.1.1.1，主计费服务器的 IP 地址为 10.1.1.1。

```
[Sysname-radius-rad] primary authentication 10.1.1.1
[Sysname-radius-rad] primary accounting 10.1.1.1
```

配置与认证/授权服务器、主计费服务器交互报文时的共享密钥为明文 aabbcc。

```
[Sysname-radius-rad] key authentication simple aabbcc
[Sysname-radius-rad] key accounting simple aabbcc
[Sysname-radius-rad] quit
```

创建 ISP 域 bbb，为 login 用户配置的 AAA 认证方法为 RADIUS 认证、RADIUS 授权、RADIUS 计费。

```
[Sysname] domain bbb
[Sysname-isp-bbb] authentication login radius-scheme rad
[Sysname-isp-bbb] authorization login radius-scheme rad
[Sysname-isp-bbb] accounting login radius-scheme rad
[Sysname-isp-bbb] quit
```

- (3) 在设备上配置用户角色 departA-resource

创建用户角色 **departA-resource**，配置用户角色规则，允许用户执行特性 QoS 和 ACL 中的所有命令。

```
[Sysname] role name departA-resource
[Sysname-role-departA-resource] rule 1 permit read write execute feature qos
[Sysname-role-departA-resource] rule 2 permit read write execute feature acl
```

配置 VLAN 资源控制策略，只具有 VLAN 100~VLAN 199 的操作权限。

```
[Sysname-role-departA-resource] vlan policy deny
[Sysname-role-departA-resource-vlanpolicy] permit vlan 100 to 199
[Sysname-role-departA-resource-vlanpolicy] quit
```

配置接口和 VPN 资源访问策略，禁止访问所有接口和 VPN 资源。

```
[Sysname-role-departA-resource] interface policy deny
[Sysname-role-departA-resource-ifpolicy] quit
[Sysname-role-departA-resource] vpn policy deny
[Sysname-role-departA-resource-vpnpolicy] quit
[Sysname-role-departA-resource] quit
```

(4) 在设备上配置用户角色 **departB-resource**

创建用户角色 **departB-resource**，配置用户角色规则，允许用户执行特性 QoS 和 ACL 中的所有命令。

```
[Sysname] role name departB-resource
[Sysname-role-departB-resource] rule 1 permit read write execute feature qos
[Sysname-role-departB-resource] rule 2 permit read write execute feature acl
```

配置 VLAN 资源控制策略，只具有 VLAN 200~VLAN 299 的操作权限。

```
[Sysname-role-departB-resource] vlan policy deny
[Sysname-role-departB-resource-vlanpolicy] permit vlan 200 to 299
[Sysname-role-departB-resource-vlanpolicy] quit
```

配置接口和 VPN 资源访问策略，禁止访问所有接口和 VPN 资源。

```
[Sysname-role-departB-resource] interface policy deny
[Sysname-role-departB-resource-ifpolicy] quit
[Sysname-role-departB-resource] vpn policy deny
[Sysname-role-departB-resource-vpnpolicy] quit
[Sysname-role-departB-resource] quit
```

8.5.2 RADIUS 服务器配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 RADIUS 服务器的基本配置。

增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置认证及计费的端口号分别为“1812”和“1813”；
- 设置与 AC 交互报文时使用的认证、计费共享密钥和确认共享密钥为“aabbcc”；

- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 20.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图11 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 ? 帮助

接入配置

认证端口 * <input type="text" value="1812"/>	计费端口 * <input type="text" value="1813"/>
组网方式 <input type="text" value="不启用混合组网"/>	业务类型 <input type="text" value="设备管理业务"/>
接入设备类型 <input type="text" value="H3C(General)"/>	接入设备分组 <input type="text" value="无"/>
共享密钥 * <input type="text" value="....."/>	确认共享密钥 * <input type="text" value="....."/>
业务分组 <input type="text" value="未分组"/>	

设备列表

设备名称	设备IP地址	设备型号	备注	删除
	20.1.1.2			

共有1条记录。

增加设备管理用户。

选择“用户”页签，单击导航树中的[接入用户管理/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 创建用户名，这里输入“admin-departA@bbb”，并配置密码和确认密码；
- 选择服务类型为“Telnet”；
- 添加用户角色名“departA-resource”；
- 添加所管理设备的 IP 地址，IP 地址范围为“20.1.1.0~20.1.1.10”；
- 单击<确定>按钮完成操作。

图12 增加设备管理用户

用户 > 设备管理用户 > 增加设备管理用户 ? 帮助

增加设备管理用户

设备管理用户基本信息

帐号名 *	<input type="text" value="admin-departA@bbb"/>	?
用户密码 *	<input type="password" value="•••••"/>	
密码确认 *	<input type="password" value="•••••"/>	
服务类型	<input type="text" value="Telnet"/>	
EXEC权限级别	<input type="text"/>	?
角色名	<input type="text" value="departA-resource"/>	

提示

注意：输入绑定的多个角色名时，每行只能写一个角色名，且角色名占用字节数与角色名个数（出现多个相同角色名时被视为一个角色名）总和不超过234。例如，假定输入10个角色，则角色占用字节数应不超过224个。

绑定的用户IP地址列表

起始IP地址	结束IP地址	删除
未找到符合条件的记录。		

所管理设备IP地址列表

起始IP地址	结束IP地址	删除
20.1.1.0	20.1.1.10	<input type="button" value="删除"/>

继续在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 创建用户名，这里输入“admin-departB@bbb”，并配置密码和确认密码；
- 选择服务类型为“Telnet”；
- 添加用户角色名“departB-resource”；
- 添加所管理设备的IP地址，IP地址范围为“20.1.1.0~20.1.1.10”；
- 单击<确定>按钮完成操作。

图13 增加设备管理用户

用户 > 设备管理用户 > 增加设备管理用户 ? 帮助

增加设备管理用户

设备管理用户基本信息

帐号名 * ?

用户密码 *

密码确认 *

服务类型

EXEC权限级别 ?

角色名

提示

注意：输入绑定的多个角色名时，每行只能写一个角色名，且角色名占用字节数与角色名个数（出现多个相同角色名时被视为一个角色名）总和不超过234。例如，假定输入10个角色，则角色占用字节数应不超过224个。

绑定的用户IP地址列表

起始IP地址	结束IP地址	删除
未找到符合条件的记录。		

所管理设备IP地址列表

起始IP地址	结束IP地址	删除
20.1.1.0	20.1.1.10	

8.6 验证配置

(1) 查看用户角色信息

通过 **display role** 命令查看用户角色 departA-resource 和 departB-resource 的信息。

显示用户角色 departA-resource 的信息。

```
<Sysname> display role name departA-resource
```

```
Role: departA-resource
```

```
Description:
```

```
VLAN policy: deny
```

```
Permitted VLANs: 100 to 199
```

```
Interface policy: deny
```

```
VPN instance policy: deny
```

```
Security zone policy: permit (default)
```

```
-----
```

Rule	Perm	Type	Scope	Entity

```

1      permit RWX   feature      qos
2      permit RWX   feature      acl
R:Read W:Write X:Execute

```

显示用户角色 departB-resource 的信息。

```
<Sysname> display role name departB-resource
```

```

Role: departB-resource
Description:
VLAN policy: deny
Permitted VLANs: 200 to 299
Interface policy: deny
VPN instance policy: deny
Security zone policy: permit (default)
-----

```

Rule	Perm	Type	Scope	Entity
1	permit RWX	feature	qos	
2	permit RWX	feature	acl	

```

1      permit RWX   feature      qos
2      permit RWX   feature      acl

```

```
R:Read W:Write X:Execute
```

(2) 用户登录设备

以部门 A 网络管理员登录设备为例进行验证。

部门 A 网络管理员向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 admin-departA @bbb 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50
```

```

*****
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

```

```
login: admin-departA@bbb
```

```
Password:
```

```
<Sysname>
```

(3) 验证用户权限

部门 A 网络管理员 admin-departA @bbb 成功登录设备后，可通过如下步骤验证用户的权限：

- o 可执行特性 QoS 和 ACL 中所有的命令。（以创建高级 ACL、流分类、流行为和 QoS 策略，并关联流分类和流行为为例）

创建高级 ACL，编号为 3000。

```
<Sysname> system-view
```

```
[Sysname] acl number 3000
```

配置 ACL 的匹配规则为匹配所有 FTP 数据流量。

```
[Sysname-acl-adv-3000] rule permit tcp destination-port eq ftp-data
```

```
[Sysname-acl-adv-3000] quit
```

创建流分类 1，匹配规则为匹配 ACL 3000。

```
[Sysname] traffic classifier 1
```

```
[Sysname-classifier-1] if-match acl 3000
```

```
[Sysname-classifier-1] quit
```

#创建流分类 1，流行为为流量监管，限速值为 2000kbps。

```
[Sysname] traffic behavior 1
```

```
[Sysname-behavior-1] car cir 2000
```

```
[Sysname-behavior-1] quit
```

#创建 QoS 策略 1，将流分类 1 和流行为 1 进行关联。

```
[Sysname] qos policy 1
```

```
[Sysname-qospolicy-1] classifier 1 behavior 1
```

```
[Sysname-qospolicy-1] quit
```

- 可操作 VLAN 100~VLAN 199。（以将 QoS 策略 1 应用到 VLAN 100~VLAN 107 的入方向为例）

将 QoS 策略 1 应用到 VLAN 100~VLAN 107 的入方向，即对所有主机的上行流量进行限速。

```
[Sysname] qos vlan-policy 1 vlan 100 to 107 inbound
```

- 不能操作其它 VLAN。（以将 QoS 策略 1 应用到 VLAN 200~VLAN 207 的入方向为例）

将 QoS 策略 1 应用到 VLAN 200~VLAN 207 的入方向，即对所有主机的上行流量进行限速。

```
[Sysname] qos vlan-policy 1 vlan 200 to 207 inbound
```

```
Permission denied.
```

通过显示信息可以确认配置生效。

部门 B 网络管理员 admin-departB@bbb 成功登录设备后，可通过如下步骤验证用户的权限：

- 可执行特性 QoS 和 ACL 中所有的命令。（以创建高级 ACL、流分类、流行为和 QoS 策略，并关联流分类和流行为为例）

创建高级 ACL，编号为 3001。

```
[Sysname] acl number 3001
```

配置 ACL 的匹配规则为匹配所有 FTP 数据流量。

```
[Sysname-acl-adv-3001] rule permit tcp destination-port eq ftp-data
```

```
[Sysname-acl-adv-3001] quit
```

创建流分类 2，匹配规则为匹配 ACL 3001。

```
[Sysname] traffic classifier 2
```

```
[Sysname-classifier-2] if-match acl 3001
```

```
[Sysname-classifier-2] quit
```

创建流分类 2，流行为为流量监管，限速值为 2000kbps。

```
[Sysname] traffic behavior 2
```

```
[Sysname-behavior-2] car cir 2000
```

```
[Sysname-behavior-2] quit
```

创建 QoS 策略 2，将流分类 2 和流行为 2 进行关联。

```
[Sysname] qos policy 2
```

```
[Sysname-qospolicy-2] classifier 1 behavior 2
```

```
[Sysname-qospolicy-2] quit
```

- 可操作 VLAN 200~VLAN 299。（以将 QoS 策略 2 应用到 VLAN 200~VLAN 207 的入方向为例）

```
[Sysname] qos vlan-policy 2 vlan 200 to 207 inbound
```

- 不能操作其它 VLAN。（以将 QoS 策略 2 应用到 VLAN 100~VLAN 107 的入方向为例）

```
[Sysname] qos vlan-policy 2 vlan 100 to 107 inbound
```

```
Permission denied.
```

通过显示信息可以确认配置生效。

8.7 配置文件

```
#
telnet server enable
#
interface GigabitEthernet1/0/1
 ip address 192.168.1.50 24
#
interface GigabitEthernet1/0/2
 ip address 20.1.1.2 24
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$JzDegvL0G5KZICJhzscTHLA4WasBVh0UOw==
 key accounting cipher $c$3$CdejNYYxvjW0Y+Zydi4rZgBwjYb4h6LKmg==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
role name departA-resource
 rule 1 permit read write execute feature qos
 rule 2 permit read write execute feature acl
 vlan policy deny
  permit vlan 100 to 199
 interface policy deny
 vpn-instance policy deny
#
role name departB-resource
 rule 1 permit read write execute feature qos
 rule 2 permit read write execute feature acl
```

```
vlan policy deny
  permit vlan 200 to 299
interface policy deny
vpn-instance policy deny
#
```

9 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“基础配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“基础配置命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-路由命令参考”

H3C MSR 系列路由器

以太网链路聚合配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 三层链路聚合配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	1
3.3 配置注意事项.....	1
3.4 配置步骤.....	2
3.4.1 Device A 的配置.....	2
3.4.2 Device B 的配置.....	2
3.5 验证配置.....	2
3.6 配置文件.....	3
4 参考资料.....	4

1 简介

本文档介绍以太网链路聚合特性的配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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以太网链路聚合特性。

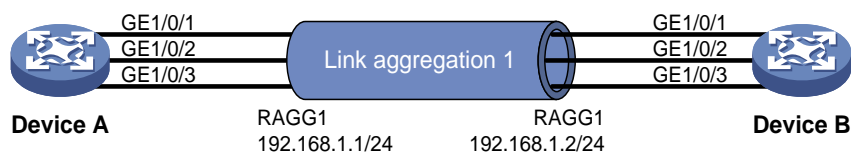
3 三层链路聚合配置举例

3.1 组网需求

如图 1 所示：

- Device A 与 Device B 通过各自的三层以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 相互连接。
- 在 Device A 和 Device B 上分别配置三层链路聚合组，并为对应的三层聚合接口配置 IP 地址和子网掩码。

图1 三层聚合配置示例图



3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.3 配置注意事项

由于静态聚合组中端口选中状态不受对端端口是否在聚合组中及是否处于选中状态的影响。这样有可能导致两端设备所确定的 **Selected** 状态端口不一致，当两端都支持配置静态和动态聚合模式的情况下，建议用户选择配置动态聚合模式。

3.4 配置步骤

3.4.1 Device A 的配置

创建三层聚合接口 1。（根据具体情况选择下面两种方式之一）

- 采用静态聚合模式

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
```

- 采用动态聚合模式

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] link-aggregation mode dynamic
```

为三层聚合接口 1 配置 IP 地址和子网掩码。

```
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

将接口 GigabitEthernet1/0/1~GigabitEthernet1/0/3 加入聚合组 1。

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] quit
```

3.4.2 Device B 的配置

Device B 上的配置与 Device A 相同，配置过程略。

3.5 验证配置

通过 **display link-aggregation verbose** 命令来显示聚合组的相关信息，以验证配置是否成功。

- 采用静态聚合模式的聚合组信息

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

```
Aggregate Interface: Route-Aggregation1
```

```
Aggregation Mode: Static
```

```
Loadsharing Type: Shar
```

```
Port          Status  Priority Oper-Key
```

```
-----
GE1/0/1       S       32768   1
GE1/0/2       S       32768   1
GE1/0/3       S       32768   1
```

结果说明：本端加入到静态聚合组内的成员端口都处于 **Selected** 状态，与对端对应端口是否是 **Selected** 状态无关。

- 采用动态聚合模式的聚合组信息

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

Aggregate Interface: Route-Aggregation1

Creation Mode: Manual

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 000f-e267-6c6a

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	1	{ACDEF}
GE1/0/2	S	32768	1	{ACDEF}
GE1/0/3	S	32768	1	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	1	32768	1	0x8000, 000f-e267-57ad	{ACDEF}
GE1/0/2	2	32768	1	0x8000, 000f-e267-57ad	{ACDEF}
GE1/0/3	3	32768	1	0x8000, 000f-e267-57ad	{ACDEF}

结果说明：本端和对端设备上聚合组内的成员端口都处于 **Selected** 状态。原因是在动态链路聚合中通过 **LACP** 协议报文交互，可使两端聚合组内的成员端口选中状态达成一致，可顺利实现对用户数据的转发。

3.6 配置文件

- Device A:

- 采用静态聚合模式

```
#
interface route-aggregation1
 ip address 192.168.1.1 255.255.255.0
#
```

- 采用动态聚合模式

```
#
interface route-aggregation1
 ip address 192.168.1.1 255.255.255.0
 link-aggregation mode dynamic
#
```

```
interface GigabitEthernet1/0/1
  port link-mode route
  port link-aggregation group 1
#
interface GigabitEthernet1/0/2
  port link-mode route
  port link-aggregation group 1
#
interface GigabitEthernet1/0/3
  port link-mode route
  port link-aggregation group 1
#
```

- Device B:
Device B 上的配置文件与 Device A 类似。

4 参考资料

- 《H3C MSR 系列路由器 命令参考(V7)》中的“二层技术-以太网交换命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“二层技术-以太网交换配置指导”

H3C MSR 系列路由器

端口隔离配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 使用限制.....	1
4 端口隔离典型配置举例.....	1
4.1 组网需求.....	1
4.2 使用版本.....	2
4.3 配置注意事项.....	2
4.4 配置步骤.....	2
4.5 验证配置.....	2
4.6 配置文件.....	3
5 相关资料.....	3

1 简介

本文档介绍了端口隔离的配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解端口隔离特性。

3 使用限制

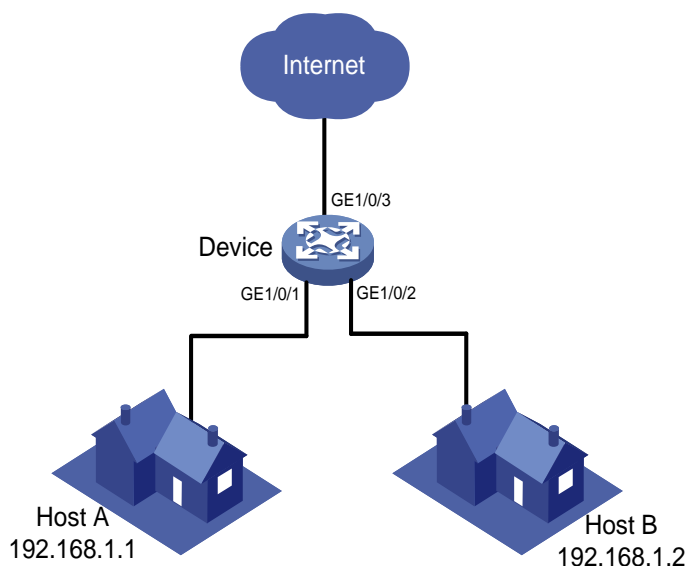
该特性仅在 SIC-4GSW/DSIC-9FSW/DSIC-9FSWP/HMIM-24GSW/HMIM-24GSW-PoE/HMIM-8GSW 接口卡，以及 MSR 3600-28 和 MSR 3600-51 款型的固定二层接口上支持。

4 端口隔离典型配置举例

4.1 组网需求

如 [图 1](#) 所示，小区用户 Host A、Host B 分别与 Device 的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 相连，Device 设备通过 GigabitEthernet1/0/3 端口与外部网络相连。现需要实现小区用户 Host A 和 Host B 之间二层报文不能互通，但可以和外部网络通信。

图1 端口隔离配置组网图



4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.3 配置注意事项

设备只支持一个隔离组，由系统自动创建隔离组 1，用户不可删除该隔离组或创建其他的隔离组。隔离组内可以加入的端口数量没有限制。

4.4 配置步骤

将端口 GigabitEthernet1/0/1 与 GigabitEthernet1/0/2 加入隔离组。

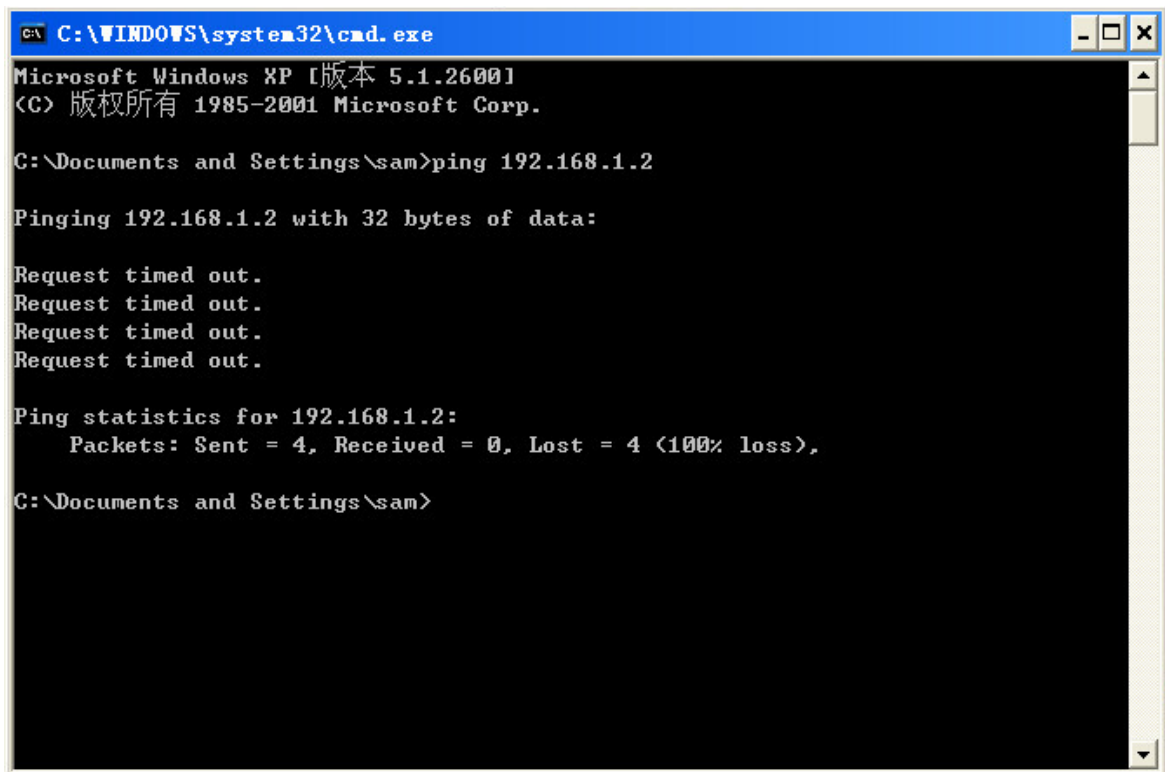
```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable
[Device-GigabitEthernet1/0/2] quit
```

4.5 验证配置

显示隔离组中的信息。

```
[Device] display port-isolate group
Port isolation group information:
Group ID: 1
Group members:
    GigabitEthernet1/0/1    GigabitEthernet1/0/2
```

以上信息显示 Device 上的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 已经加入隔离组，从而实现二层隔离，分别对应的 Host A 和 Host B 彼此之间不能 Ping 通，如下图 Host A ping Host B。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\sam>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\sam>
```

4.6 配置文件

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-isolate enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port-isolate enable
#
```

5 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“二层技术-以太网交换配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“二层技术-以太网交换命令参考”

H3C MSR 系列路由器

VLAN 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 使用限制.....	1
4 基于端口的 VLAN 典型配置举例.....	1
4.1 组网需求.....	1
4.2 使用版本.....	1
4.3 配置步骤.....	2
4.4 验证配置.....	2
4.5 配置文件.....	3
5 相关资料.....	3

1 简介

本文档介绍基于端口的 VLAN 的典型应用场景和配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 VLAN 特性。

3 使用限制

该特性仅在 SIC-4GSW/DSIC-9FSW/DSIC-9FSWP/HMIM-24GSW/HMIM-24GSW-PoE/HMIM-8GSW 接口卡，以及 MSR 3600-28 和 MSR 3600-51 款型的固定二层接口上支持。

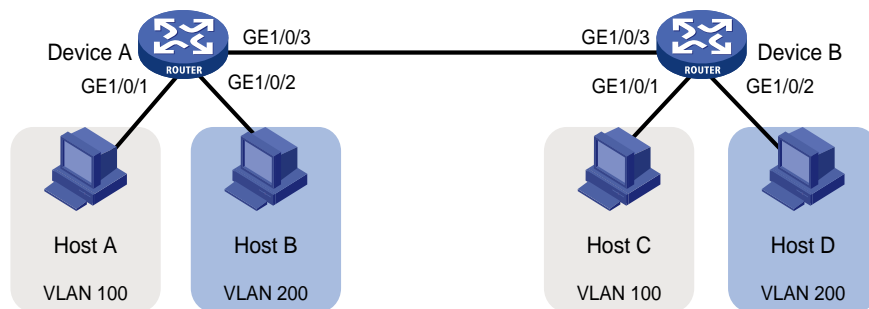
4 基于端口的 VLAN 典型配置举例

4.1 组网需求

如图 1 所示，Host A 和 Host C 属于部门 A，但是通过不同的设备接入公司网络；Host B 和 Host D 属于部门 B，也通过不同的设备接入公司网络。为了通信的安全性，以及避免广播报文泛滥，公司网络中使用 VLAN 技术来隔离部门间的二层流量。其中部门 A 使用 VLAN 100，部门 B 使用 VLAN 200。

现要求同一 VLAN 内的主机能够互通，即 Host A 和 Host C 能够互通，Host B 和 Host D 能够互通。

图1 基于端口的 VLAN 组网图



4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.3 配置步骤

(1) 配置 Device A

批量配置接口 GigabitEthernet1/0/1~GigabitEthernet1/0/3 工作在二层模式。

```
<DeviceA> system-view
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-mode bridge
[DeviceA-if-range] quit
```

创建 VLAN 100, 并将 GigabitEthernet1/0/1 加入 VLAN 100。

```
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

创建 VLAN 200, 并将 GigabitEthernet1/0/2 加入 VLAN 200。

```
[DeviceA] vlan 200
[DeviceA-vlan200] port gigabitethernet 1/0/2
[DeviceA-vlan200] quit
```

为了使 Device A 上 VLAN 100 和 VLAN 200 的报文能发送给 Device B, 将 GigabitEthernet1/0/3 的链路类型配置为 Trunk, 并允许 VLAN 100 和 VLAN 200 的报文通过。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

(2) Device B 上的配置与 Device A 上的配置相同, 不再赘述。

(3) 将 Host A 和 Host C 配置在一个网段, 例如 192.168.100.0/24; 将 Host B 和 Host D 配置在一个网段, 比如 192.168.200.0/24。

4.4 验证配置

(1) Host A 和 Host C 能够互相 ping 通, 但是均不能 ping 通 Host B。Host B 和 Host D 能够互相 ping 通, 但是均不能 ping 通 Host A。

(2) 通过查看显示信息验证配置是否成功。

查看 Device A 上 VLAN 100 和 VLAN 200 的配置信息, VLAN 100 的报文仅允许通过接口 GE1/0/3 和 GE1/0/1, VLAN 200 的报文仅允许通过接口 GE1/0/3 和 GE1/0/2。

```
[DeviceA-GigabitEthernet1/0/3] display vlan 100
```

```
VLAN ID: 100
VLAN type: Static
Route interface: Not configured
Description: VLAN 0100
Name: VLAN 0100
```

```
Tagged ports:
```

```
GigabitEthernet1/0/3
```

```
Untagged ports:
```

```
GigabitEthernet1/0/1
```

```
[DeviceA-GigabitEthernet1/0/3] display vlan 200
```

```
VLAN ID: 200
VLAN type: Static
```

```
Route interface: Not configured
Description: VLAN 0200
Name: VLAN 0200
Tagged ports:
  GigabitEthernet1/0/3
Untagged ports:
  GigabitEthernet1/0/2
```

4.5 配置文件

Device B 上的配置与 Device A 上的配置相同，此处仅以 Device A 的配置文件举例

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 200
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 100 200
#
```

5 相关资料

- 《H3C MSR 系列路由器 命令参考(V7)》中的“二层技术-以太网交换命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“二层技术-以太网交换配置指导”

H3C MSR 系列路由器

QinQ 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1-1
2 配置前提.....	2-1
3 使用限制.....	3-1
4 QinQ 配置举例.....	4-1
4.1 组网需求.....	4-1
4.2 配置思路.....	4-2
4.3 使用版本.....	4-2
4.4 配置注意事项.....	4-3
4.5 配置步骤.....	4-3
4.5.1 PE A 的配置.....	4-3
4.5.2 PE B 的配置.....	4-3
4.5.3 运营商网络设备的配置.....	4-4
4.6 验证配置.....	4-4
4.7 配置文件.....	4-5
5 相关资料.....	5-6

1 简介

本文档介绍了使用 QinQ 功能在运营商网络中传输用户数据的配置举例。

当端口上配置了 QinQ 功能后，不论从该端口收到的报文是否带有 VLAN Tag，设备都会为该报文封装本端口缺省 VLAN 的 Tag。



端口配置 QinQ 功能后，设备会将用户网络的 MAC 地址学习到 QinQ 封装的外层 VLAN 中。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 QinQ 特性。

3 使用限制

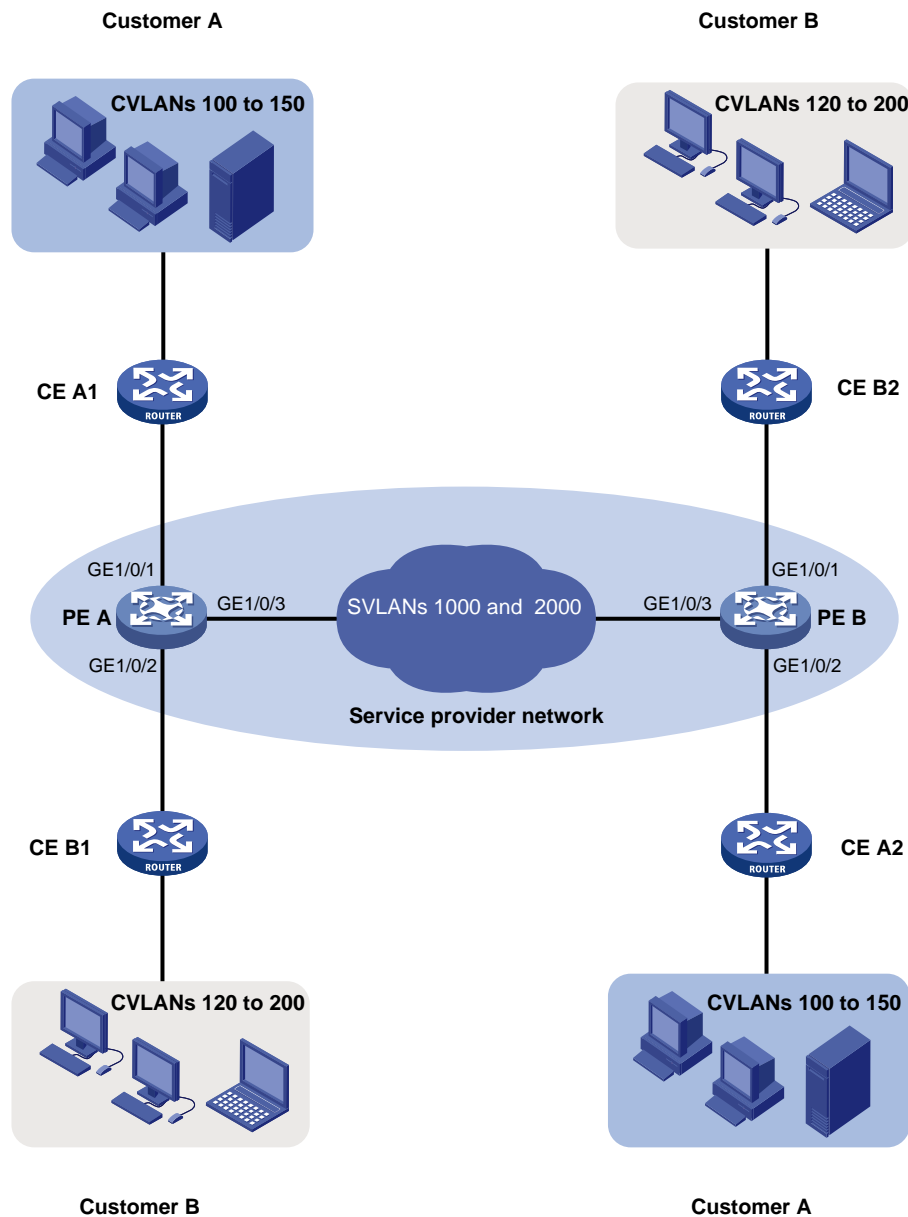
在 MSR 路由器上，仅 MSR3600-51 与 MSR3600-28 的固定交换以太网接口、配有 HMIM 24GSW、HMIM 24GSW-PoE 与 HMIM 8GSW 接口卡的 MSR 路由器支持 QinQ 功能。

4 QinQ 配置举例

4.1 组网需求

如图 1 所示，Customer A 和 Customer B 各有两个分支机构需要通过运营商网络进行通信。运营商网络中可用的 VLAN 资源包括 VLAN 1000 和 VLAN 2000。现要求通过配置 QinQ 功能，运营商网络能够利用 VLAN 1000 传输 Customer A 的数据，利用 VLAN 2000 传输 Customer B 的数据。

图1 QinQ 组网示意图



4.2 配置思路

- 请在 PE A 和 PE B 连接用户网络的端口上配置 QinQ 功能。
- 为了保证用户网络接收的数据中不会包含运营商网络的 VLAN 信息，需要配置开启 QinQ 功能的端口发送 PVID 的报文时不带 VLAN Tag。开启 QinQ 功能的端口的链路类型可以是 Access, Hybrid 或 Trunk。如果配置为 Hybrid 类型，需要配置该端口允许 PVID 的报文不带 VLAN Tag 通过。如果配置为 Trunk 类型，需要配置该端口允许 PVID 的报文通过。

4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.4 配置注意事项

- 开启 QinQ 的端口，需要配置端口的缺省 VLAN 为 QinQ 封装的外层 VLAN（SVLAN）。
- 需要保证 QinQ 报文传输路径上，报文的外层 VLAN Tag 不被修改或删除。
- QinQ 为报文加上外层 VLAN Tag 后，内层 VLAN Tag 将被当作报文的数据部分进行传输，报文长度将增加 4 个字节。因此建议用户适当增加 QinQ 报文传输路径上各接口的 MTU 值（至少为 1504 字节）。

4.5 配置步骤

4.5.1 PE A 的配置

```
# 创建 VLAN 1000 和 VLAN 2000。
<PE_A> system-view
[PE_A] vlan 1000
[PE_A-vlan1000] quit
[PE_A] vlan 2000
[PE_A-vlan2000] quit
# 配置端口 GigabitEthernet1/0/1 为 Access 端口，允许 VLAN 1000 的报文通过。
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port access vlan 1000
# 开启端口 GigabitEthernet1/0/1 的 QinQ 功能。
[PE_A-GigabitEthernet1/0/1] qinq enable
[PE_A-GigabitEthernet1/0/1] quit
# 配置端口 GigabitEthernet1/0/2 为 Access 端口，允许 VLAN 2000 的报文通过。
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port access vlan 2000
# 开启端口 GigabitEthernet1/0/2 的 QinQ 功能。
[PE_A-GigabitEthernet1/0/2] qinq enable
[PE_A-GigabitEthernet1/0/2] quit
# 配置端口 GigabitEthernet1/0/3 为 Trunk 端口，且允许 VLAN 1000 和 VLAN 2000 的报文通过，
取消允许 VLAN 1 通过。
[PE_A] interface gigabitethernet 1/0/3
[PE_A-GigabitEthernet1/0/3] port link-type trunk
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE_A-GigabitEthernet1/0/3] quit
```

4.5.2 PE B 的配置

```
# 创建 VLAN 1000 和 VLAN 2000。
<PE_B> system-view
[PE_B] vlan 1000
[PE_B-vlan1000] quit
[PE_B] vlan 2000
```

```

[PE_B-vlan2000] quit
# 配置端口 GigabitEthernet1/0/1 为 Access 端口，允许 VLAN 2000 的报文通过。
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port access vlan 2000
# 开启端口 GigabitEthernet1/0/1 的 QinQ 功能。
[PE_B-GigabitEthernet1/0/1] qinq enable
[PE_B-GigabitEthernet1/0/1] quit
# 配置端口 GigabitEthernet1/0/2 为 Access 端口，允许 VLAN 1000 的报文通过。
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port access vlan 1000
# 开启 GigabitEthernet1/0/2 端口的 QinQ 功能。
[PE_B-GigabitEthernet1/0/2] qinq enable
[PE_B-GigabitEthernet1/0/2] quit
# 配置端口 GigabitEthernet1/0/3 为 Trunk 端口，且允许 VLAN 1000 和 VLAN 2000 的报文通过，
取消允许 VLAN 1 通过。
[PE_B] interface gigabitethernet 1/0/3
[PE_B-GigabitEthernet1/0/3] port link-type trunk
[PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
[PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE_B-GigabitEthernet1/0/3] quit

```

4.5.3 运营商网络设备的配置

配置运营商网络中 PE A 到 PE B 之间的路径上的设备端口都允许 VLAN 1000 和 VLAN 2000 的报文携带 VLAN Tag 通过，且这些端口的 MTU 值至少为 1504 字节。

4.6 验证配置

- (1) 同一个公司跨越运营商网络的两个分支机构中处于同一 CVLAN 的两台 PC 互相进行 Ping 操作，可以 Ping 通，且这两台 PC 能够互相学习到对方的 MAC 地址。可见 CVLAN 信息能够跨越运营商网络进行透明传输。

Customer A 上同属于 VLAN 100 的两台 PC 可以 Ping 通，且学到对方的 MAC 地址。

```
C:\Windows\System32>ping 192.168.100.67
```

```

Pinging 192.168.100.67 with 32 bytes of data:
Reply from 192.168.100.67: bytes=32 time<1ms TTL=255
Reply from 192.168.100.67: bytes=32 time=11ms TTL=255
Reply from 192.168.100.67: bytes=32 time<1ms TTL=255
Reply from 192.168.100.67: bytes=32 time<1ms TTL=255

```

```

Ping statistics for 192.168.100.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms

```

```
C:\Windows\System32>arp -a
```

```

Interface: 192.168.100.24 --- 0x15
  Internet Address      Physical Address      Type
  192.168.100.67       0c-da-41-b2-1e-31    dynamic
  192.168.100.255      ff-ff-ff-ff-ff-ff    static
  224.0.0.22           01-00-5e-00-00-16    static
  224.0.0.252          01-00-5e-00-00-fc    static
  239.255.255.250      01-00-5e-7f-ff-fa    static

```

- (2) Customer A 和 Customer B 中处于同一 CVLAN(例如 VLAN 130)中的两台 PC 互相进行 Ping 操作。在其中一台 PC 上查看 ARP 表项，发现它没有学到对方的 MAC 地址。可见不同公司中同一 CVLAN 的流量被二层隔离。

4.7 配置文件

- PE A

```

#
vlan 1000
#
vlan 2000
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 1000
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2000
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000 2000
#

```

- PE B

```

#
vlan 1000
#
vlan 2000
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2000
 qinq enable
#

```

```
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 1000
  qinq enable
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 1000 2000
#
```

5 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“二层技术-以太网交换配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“二层技术-以太网交换命令参考”

H3C MSR 系列路由器

PPP 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 特性简介	1
2 配置前提	1
3 MP+CHAP 配置举例.....	1
3.1 组网需求	1
3.2 使用版本	1
3.3 配置注意事项.....	1
3.4 配置步骤	1
3.4.1 配置 Device A	1
3.4.2 配置 Device B	2
3.5 验证配置	3
3.6 配置文件	4
4 相关资料	5

1 特性简介

本文档介绍 PPP 协议相关的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

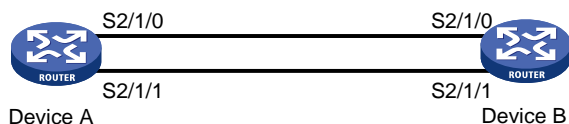
本文档假设您已了解了 PPP、MP、PPPoE、DHCP 协议。

3 MP+CHAP 配置举例

3.1 组网需求

如[图1](#)所示，设备 Device A 和 Device B 的 Serial2/1/0 和 Serial2/1/1 分别对应连接，使用 MP-Group 的方式建立 MP 链路，每个 PPP 链路使用 CHAP 进行认证。

图1 终端描述符捆绑 MP 组网图



3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.3 配置注意事项

- 配置采用 CHAP 认证时两端的用户名和密码必须一致。
- Serial 接口配置完成之后，需要执行 `undo shutdown` 命令开启接口。
- 创建 PPP 用户需要在 `local-user` 命令的 `class` 关键字后面选择 `network` 参数。

3.4 配置步骤

3.4.1 配置 Device A

- (1) 为 Device B 创建本地用户，设置本地用户的服务类型为 PPP。

```
<DeviceA> system-view
```


- ```
[DeviceA] local-user userb class network
[DeviceA-luser-network-userb] password simple hello
[DeviceA-luser-network-userb] service-type ppp
[DeviceA-luser-network-userb] quit
```
- (2) 配置串口 **Serial2/1/0**，通过缺省的 ISP 域 **system** 对 **Rotuer B** 进行 CHAP 认证。
- ```
[DeviceA] interface serial 2/1/0
[DeviceA-Serial2/1/0] link-protocol ppp
[DeviceA-Serial2/1/0] ppp authentication-mode chap domain system
[DeviceA-Serial2/1/0] quit
```
- (3) 配置串口 **Serial2/1/1**，通过缺省的 ISP 域 **system** 对 **Rotuer B** 进行 CHAP 认证。
- ```
[DeviceA] interface Serial 2/1/1
[DeviceA-Serial2/1/1] link-protocol ppp
[DeviceA-Serial2/1/1] ppp authentication-mode chap domain system
[DeviceA-Serial2/1/1] quit
```
- (4) 在系统缺省的 ISP 域 **system** 下，配置 PPP 用户使用本地认证方案。
- ```
[DeviceA] domain system
[DeviceA-isp-system] authentication ppp local
```
- (5) 创建 **MP-group** 接口，配置相应的 IP 地址。
- ```
<DeviceA> system-view
[DeviceA] interface mp-group 2/0/0
[DeviceA-MP-group2/0/0] ip address 1.1.1.1 24
[DeviceA-MP-group2/0/0] quit
```
- (6) 配置串口 **Serial2/1/0** 加入 **MP-Group 1** 并开启接口。
- ```
[DeviceA] interface serial 2/1/0
[DeviceA-Serial2/1/0] ppp mp mp-group 2/0/0
[DeviceA-Serial2/1/0] shutdown
[DeviceA-Serial2/1/0] undo shutdown
[DeviceA-Serial2/1/0] quit
```
- (7) 配置串口 **Serial2/1/1** 加入 **MP-Group 1** 并开启接口。
- ```
[DeviceA] interface Serial 2/1/1
[DeviceA-Serial2/1/1] ppp mp mp-group 2/0/0
[DeviceA-Serial2/1/1] shutdown
[DeviceA-Serial2/1/1] undo shutdown
[DeviceA-Serial2/1/1] quit
```

### 3.4.2 配置 Device B

- (1) 配置串口 **Serial2/1/0**，封装的链路层协议为 PPP，并配置采用 CHAP 认证时 Device B 的用户名和设置缺省的 CHAP 认证密码。
- ```
<DeviceB> system-view
[DeviceB] interface serial 2/1/0
[DeviceB-Serial2/1/0] link-protocol ppp
[DeviceB-Serial2/1/0] ppp chap user userb
[DeviceB-Serial2/1/0] ppp chap password simple hello
[DeviceB-Serial2/1/0] quit
```

- (2) 配置串口 **Serial2/1/1**，封装的链路层协议为 **PPP**，并配置采用 **CHAP** 认证时 **Device B** 的用户名和设置缺省的 **CHAP** 认证密码。

```
[DeviceB] interface Serial 2/1/1
[DeviceB-Serial2/1/1] link-protocol ppp
[DeviceB-Serial2/1/1] ppp chap user userb
[DeviceB-Serial2/1/1] ppp chap password simple hello
[DeviceB-Serial2/1/1] quit
```

- (3) 创建 **MP-group** 接口，配置相应的 **IP** 地址。

```
[DeviceB] interface mp-group 2/0/0
[DeviceB-Mp-group1] ip address 1.1.1.2 24
[DeviceB-Mp-group1] quit
```

- (4) 配置串口 **Serial2/1/0** 加入 **MP-Group 1** 并开启接口。

```
[DeviceB] interface serial 2/1/0
[DeviceB-Serial2/1/0] link-protocol ppp
[DeviceB-Serial2/1/0] ppp mp mp-group 2/0/0
[DeviceB-Serial2/1/0] shutdown
[DeviceB-Serial2/1/0] undo shutdown
[DeviceB-Serial2/1/0] quit
```

- (5) 配置串口 **Serial2/1/1** 加入 **MP-Group 1** 并开启接口。

```
[DeviceB] interface Serial 2/1/1
[DeviceB-Serial2/1/1] link-protocol ppp
[DeviceB-Serial2/1/1] ppp mp mp-group 2/0/0
[DeviceB-Serial2/1/1] shutdown
[DeviceB-Serial2/1/1] undo shutdown
[DeviceB-Serial2/1/1] quit
```

3.5 验证配置

- (1) 在 **Device A** 上查看 **MP** 的相关信息。

```
[DeviceA] display ppp mp
Template: MP-group2/0/0
max-bind: 16, fragment: enabled, min-fragment: 128
  Master link: MP-group2/0/0, Active members: 2, Bundle Multilink
  Peer's endPoint descriptor: MP-group2/0/0
  Sequence format: long (rcv)/long (sent)
  Bundle Up Time: 2014/07/22 16:51:40:835
  0 lost fragments, 5 reordered, 0 unassigned, 0 interleaved
  Sequence: 4 (rcv)/5 (sent)
  Active member channels: 2 members
    Serial2/1/0          Up-Time:2014/07/22 16:51:40:836
    Serial2/1/1          Up-Time:2014/07/22 16:51:53:542
```

- (2) 在 **Device A** 上查看 **MP-group2/0/0** 接口的相关信息。

```
[DeviceA] display interface mp-group 2/0/0
MP-group2/0/0
Current state: UP
Line protocol state: UP
Description: MP-group2/0/0 Interface
```

```

Bandwidth: 128kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 1.1.1.1/24 Primary
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened
Physical: MP, baudrate: 128000 bps
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 1 bytes/sec, 8 bits/sec, 0 packets/sec
Last 300 seconds output rate: 1 bytes/sec, 8 bits/sec, 0 packets/sec
Input: 8 packets, 466 bytes, 0 drops
Output: 8 packets, 456 bytes, 0 drops

```

(3) 在 DeviceA 上 ping 对端 IP 地址。

```

[DeviceA] ping 1.1.1.2
Ping 1.1.1.2 (1.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=25.749 ms
56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=25.751 ms
56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=25.521 ms
56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=25.512 ms
56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=25.599 ms
--- Ping statistics for 1.1.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 25.512/25.626/25.751/0.105 ms
<DeviceA>%Jul 22 17:08:22:460 2014 DeviceA PING/6/PING_STATISTICS: Ping statistics for 1.1.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 25.512/25.626/25.751/0.105 ms.

```

3.6 配置文件

- Device A:

```

#
interface Serial2/1/0
 ppp authentication-mode chap domain system
 ppp mp MP-group2/0/0
#
interface Serial2/1/1
 ppp authentication-mode chap domain system
 ppp mp MP-group2/0/0
#
interface MP-group2/0/0
 ip address 1.1.1.1 255.255.255.0
#
local-user 123 class network
 password cipher $c$3$5ulb/vg58eiBIm5EnilnsZ2cS2Cmwg==
 service-type ppp

```

- ```
authorization-attribute user-role network-operator
#
```
- **Device B:**

```
#
interface Serial2/1/0
 ppp chap password cipher c3$4kD4T3bLZ/lngijhEKIS70/oTbNSkw==
 ppp chap user 123
 ppp mp MP-group2/0/0
#
interface Serial2/1/1
 ppp chap password cipher c3$mVlcV3W+YQBgmXKePKpZV9tTcaFhXg==
 ppp chap user 123
 ppp mp MP-group2/0/0
#
interface MP-group2/0/0
 ip address 1.1.1.2 255.255.255.0
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“二层技术-广域网接入配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“二层技术-广域网接入命令参考”

# H3C MSR 系列路由器

## 建立 LAC-Auto-Initiated 模式 L2TP 隧道配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                    |   |
|--------------------|---|
| 1 简介.....          | 1 |
| 2 配置前提.....        | 1 |
| 3 配置举例.....        | 1 |
| 3.1 组网需求.....      | 1 |
| 3.2 配置思路.....      | 1 |
| 3.3 使用版本.....      | 1 |
| 3.4 配置步骤.....      | 1 |
| 3.4.1 LNS 的配置..... | 1 |
| 3.4.2 LAC 的配置..... | 2 |
| 3.5 验证配置.....      | 3 |
| 3.6 配置文件.....      | 3 |
| 4 相关资料.....        | 4 |

# 1 简介

本文档介绍 MSR 系列路由器建立 LAC-Auto-Initiated 模式 L2TP 隧道配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

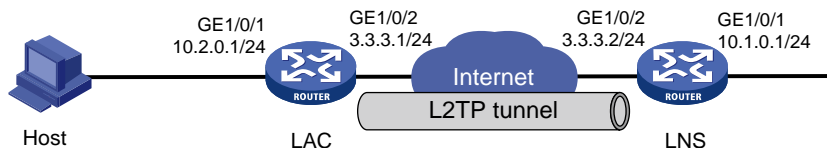
本文档假设您已了解 L2TP 特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，Host 通过 L2TP 隧道访问 LNS 右侧的网络。现要求：在 LAC 和 LNS 之间采用 LAC-Auto-Initiated 模式建立 L2TP 隧道。

图1 MSR 系列路由器建立 LAC-Auto-Initiated 模式 L2TP 隧道配置组网图



### 3.2 配置思路

为了使 LNS 在接收到合法的 LAC 的建立隧道请求后创建 L2TP 隧道，在 LNS 和 LAC 上配置开启隧道验证，并配置 PPP 用户和 Virtual-Template 接口等参数。

### 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.4 配置步骤

#### 3.4.1 LNS 的配置

# 配置接口 IP。

```
<LNS> system-view
[LNS] interface gigabitethernet1/0/1
```

```

[LNS-GigabitEthernet1/0/1] ip address 10.1.0.1 255.255.255.0
[LNS-GigabitEthernet1/0/1] quit
[LNS] interface gigabitethernet1/0/2
[LNS-GigabitEthernet1/0/2] ip address 3.3.3.2 255.255.255.0
[LNS-GigabitEthernet1/0/2] quit
配置网络接入类本地用户 pc，配置密码为 hello，并设置用户可以使用 PPP 服务。
[LNS] local-user pc class network
[LNS-luser-network-pc] password simple hello
[LNS-luser-network-pc] service-type ppp
[LNS-luser-network-pc] quit
创建接口 Virtual-Template1，配置接口的 IP 地址为 192.168.0.20/24，PPP 认证方式为 PAP，并指定为 PPP 用户分配的地址为 192.168.0.2。
[LNS] interface virtual-template 1
[LNS-Virtual-Template1] ip address 192.168.0.20 255.255.255.0
[LNS-Virtual-Template1] ppp authentication-mode pap
[LNS-Virtual-Template1] remote address 192.168.0.2
[LNS-Virtual-Template1] quit
配置域 system 对 PPP 用户采用本地验证。
[LNS] domain system
[LNS-isp-system] authentication ppp local
[LNS-isp-system] quit
开启 L2TP 功能，并创建 LNS 模式的 L2TP 组 1。
[LNS] l2tp enable
[LNS] l2tp-group 1 mode lns
配置 LNS 侧本端名称为 lns，指定接收呼叫的虚拟模板接口为 VT1，并配置隧道对端名称为 LAC。
[LNS-l2tp1] tunnel name lns
[LNS-l2tp1] allow l2tp virtual-template 1 remote lac
启用隧道验证功能，并设置隧道验证密钥为 aabbcc。
[LNS-l2tp1] tunnel authentication
[LNS-l2tp1] tunnel password simple aabbcc
[LNS-l2tp1] quit
配置访问 LAC 的私网路由，使得访问 PPP 用户的报文将通过 L2TP 隧道转发。
[LNS] ip route-static 10.2.0.0 24 192.168.0.2

```

### 3.4.2 LAC 的配置

```

开启 L2TP 功能。
<LAC> system-view
[LAC] l2tp enable
配置接口 IP
[LAC] interface gigabitethernet1/0/1
[LAC-GigabitEthernet1/0/1] port link-mode route
[LAC-GigabitEthernet1/0/1] ip address 10.2.0.1 255.255.255.0
[LAC-GigabitEthernet1/0/1] quit
[LAC] interface gigabitethernet1/0/2
[LAC-GigabitEthernet1/0/2] port link-mode route
[LAC-GigabitEthernet1/0/2] ip address 3.3.3.1 255.255.255.0

```



```

[LAC-GigabitEthernet1/0/2] quit
创建 LAC 模式的 L2TP 组 1。
[LAC] l2tp-group 1 mode lac
配置 LAC 侧本端名称为 LAC，并指定 LNS 的 IP 地址为 3.3.3.2。
[LAC-l2tp1] tunnel name lac
[LAC-l2tp1] lns-ip 3.3.3.2
开启隧道验证功能，并设置隧道验证密钥为 aabbcc。
[LAC-l2tp1] tunnel authentication
[LAC-l2tp1] tunnel password simple aabbcc
[LAC-l2tp1] quit
创建虚拟 PPP 接口 Virtual-PPP 1，配置 PPP 用户的用户名为 pc、密码为 hello，并配置 PPP 验证方式为 PAP。
[LAC] interface Virtual-PPP 1
[LAC-Virtual-PPP1] ip address ppp-negotiate
[LAC-Virtual-PPP1] ppp pap local-user pc password simple hello
[LAC-Virtual-PPP1] quit
配置私网路由，访问外网的报文将通过 L2TP 隧道转发。
[LAC] ip route-static 10.1.0.0 24 Virtual-PPP 1
触发 LAC 自动发起 L2TP 隧道建立请求，建立隧道时采用 L2TP 组 1 下配置的隧道参数。
[LAC] interface Virtual-ppp1
[LAC-Virtual-PPP1] l2tp-auto-client l2tp-group 1
[LAC-Virtual-PPP1] quit

```

### 3.5 验证配置

# 在 LNS 侧，通过命令 **display l2tp session** 可查看已建立的 L2TP 会话。

```

[LNS] display l2tp session
LocalSID RemoteSID LocalTID State
9400 1 36406 Established

```

# 在 LNS 侧，通过命令 **display l2tp tunnel** 可查看已建立的 L2TP 隧道。

```

[LNS] display l2tp tunnel
LocalTID RemoteTID State Sessions RemoteAddress RemotePort RemoteName
36406 13 Established 1 3.3.3.1 1701 lac

```

### 3.6 配置文件

- LNS:

```

#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.1 255.255.0.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 3.3.3.2 255.255.255.0
#
ip route-static 10.2.0.0 24 192.168.0.2

```

```

#
local-user pc class network
password cipher c3$tUCIDRzQtWl7DGjt8zjletI9YfXQnNf3
service-type ppp
authorization-attribute user-role network-operator
#
l2tp-group 1 mode lns
allow l2tp virtual-template 1 remote lac
tunnel name lns
tunnel password cipher c3$B09LxThNxJFm5UL+stnd3gnPNLffshOzMg==
#
l2tp enable
#

```

- **LAC :**

```

#
interface Virtual-PPP1
ppp pap local-user pc password cipher c3$5VijMUTzyEreI02qAkTT3jliYHnJYg86
ip address ppp-negotiate
l2tp-auto-client l2tp-group 1
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 3.3.3.1 255.255.255.0
#
ip route-static 10.1.0.0 24 Virtual-PPP1
#
l2tp-group 1 mode lac
lns-ip 3.3.3.2
tunnel name lac
tunnel password cipher c3$ZQaYutqU2rIW/2+D+jaDn+5fsDtE3YXs6A==
#
l2tp enable
#

```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“二层技术-广域网接入配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“二层技术-广域网接入命令参考”

# H3C MSR 系列路由器

## 建立 Client-Initiated 模式 L2TP 隧道配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                      |    |
|----------------------|----|
| 1 简介.....            | 1  |
| 2 配置前提.....          | 1  |
| 3 配置举例.....          | 1  |
| 3.1 组网需求.....        | 1  |
| 3.2 配置思路.....        | 1  |
| 3.3 使用版本.....        | 1  |
| 3.4 配置步骤.....        | 2  |
| 3.4.1 LNS 的配置.....   | 2  |
| 3.4.2 Host 侧的配置..... | 2  |
| 3.5 验证配置.....        | 15 |
| 3.6 配置文件.....        | 15 |
| 4 相关资料.....          | 16 |

# 1 简介

本文档介绍 MSR 系列路由器建立 Client-Initiated 模式 L2TP 隧道的配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

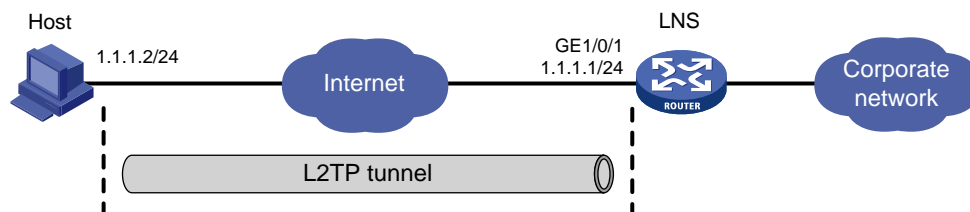
本文档假设您已了解 L2TP 特性。

## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，Host 通过 L2TP 隧道访问公司网络。现要求：LNS 可以接受来自主机发起的隧道建立请求，并建立 L2TP 隧道。

图1 MSR 系列路由器建立 Client-Initiated 模式 L2TP 隧道配置组网图



### 3.2 配置思路

为了保证合法用户正常接入从而建立 Client-Initiated 模式 L2TP 隧道，在 LNS 上配置 L2TP 用户侧认证，并创建 PPP 用户和用户所属的域，在 Host 侧需要使用设备上配置的用户名来发起隧道建立请求。

### 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置步骤

### 3.4.1 LNS 的配置

# 配置接口 GigabitEthernet1/0/1。

```
<LNS> system-view
[LNS] interface gigabitethernet 1/0/1
[LNS-GigabitEthernet1/0/1] ip address 1.1.1.1 24
[LNS-GigabitEthernet1/0/1] quit
```

# 创建 PPP 用户 user，并设置密码为 hello。

```
[LNS] local-user user class network
[LNS-luser-network-user] password simple hello
[LNS-luser-network-user] service-type ppp
[LNS-luser-network-user] quit
```

# 创建域 abc，对用户采用本地验证。

```
[LNS] domain abc
[LNS-isp-abc] authentication ppp local
[LNS-isp-abc] quit
```

# 开启 L2TP 功能。

```
[LNS] l2tp enable
```

# 创建接口 Virtual-Template1，配置接口的 IP 地址为 192.168.0.1/24，PPP 认证方式为 CHAP，并指定为 PPP 用户分配的 IP 地址为 192.168.0.2。

```
[LNS] interface virtual-template 1
[LNS-Virtual-Template1] ip address 192.168.0.1 24
[LNS-Virtual-Template1] ppp authentication-mode chap domain abc
[LNS-Virtual-Template1] remote address 192.168.0.2
[LNS-Virtual-Template1] quit
```

# 创建 LNS 模式的 L2TP 组 1，配置隧道本端名称为 LNS，指定接收呼叫的虚拟模板接口为 VT1。

```
[LNS] l2tp-group 1 mode lns
[LNS-l2tp1] tunnel name LNS
[LNS-l2tp1] allow l2tp virtual-template 1
[LNS-l2tp1] undo tunnel authentication
[LNS-l2tp1] quit
```

### 3.4.2 Host 侧的配置

# 配置 Host 的 IP 地址为 1.1.1.2，网关为 1.1.1.1。

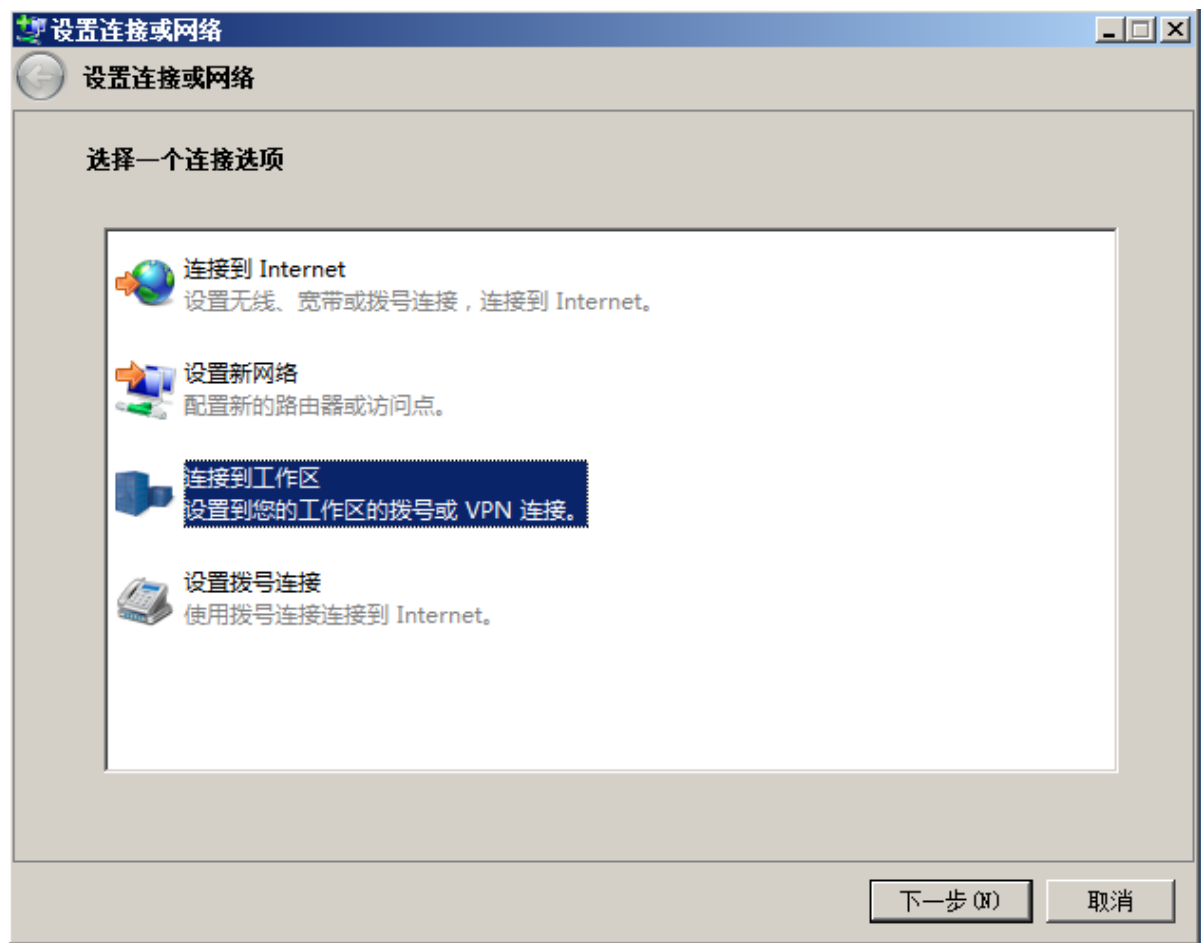
# 以 Windows 7 系统为例，进入网络和共享中心，点击“设置新的网络和连接”。

图2 新建网络连接



# 选择“连接到我的工作区”，点击“下一步”。

图3 选择一个连接选项



# 选择“使用我的 Internet 连接(VPN)”。

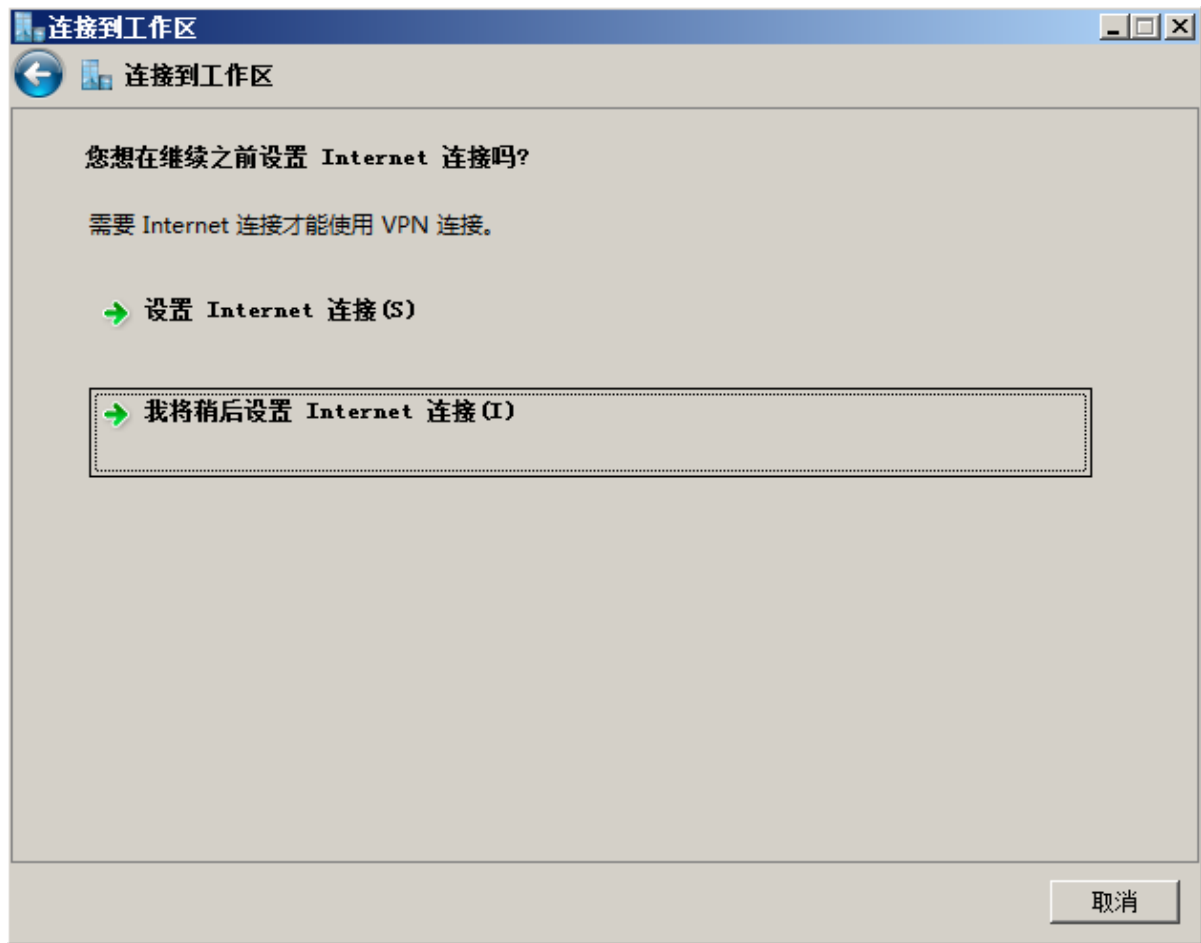


图4 选择连接方式



# 选择“我将稍后设置 Internet 连接”。

图5 设置 Internet 方式



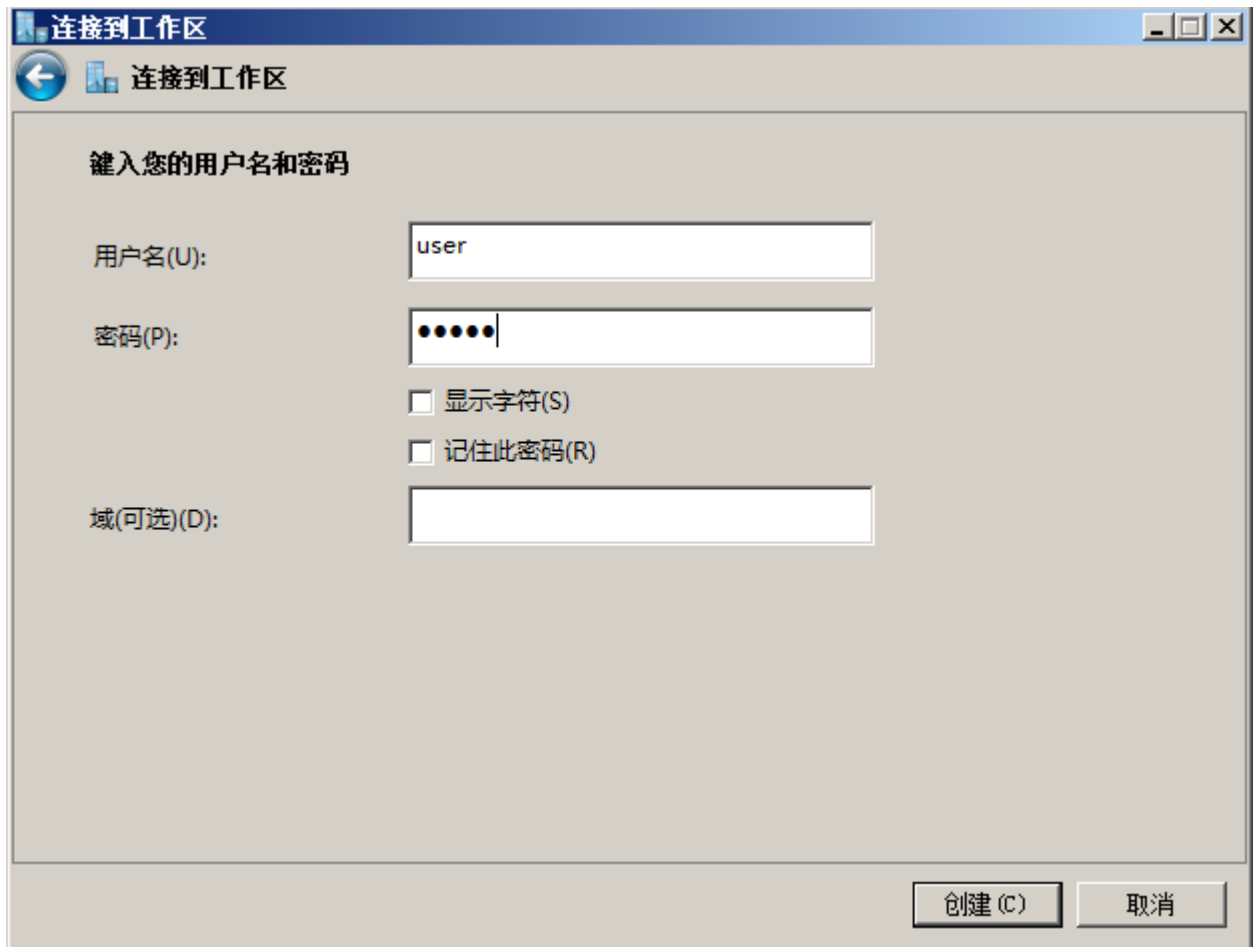
# 设置“Internet 地址”，该地址为 LNS 上主机侧的接口地址，选择“下一步”。

图6 设置 LNS 的地址



# 在对话框中输入设备上配置好的用户名和密码，选择“创建”。

图7 键入用户名和密码



连接到工作区

连接到工作区

键入您的用户名和密码

用户名(U): user

密码(P): ●●●●●

显示字符(S)

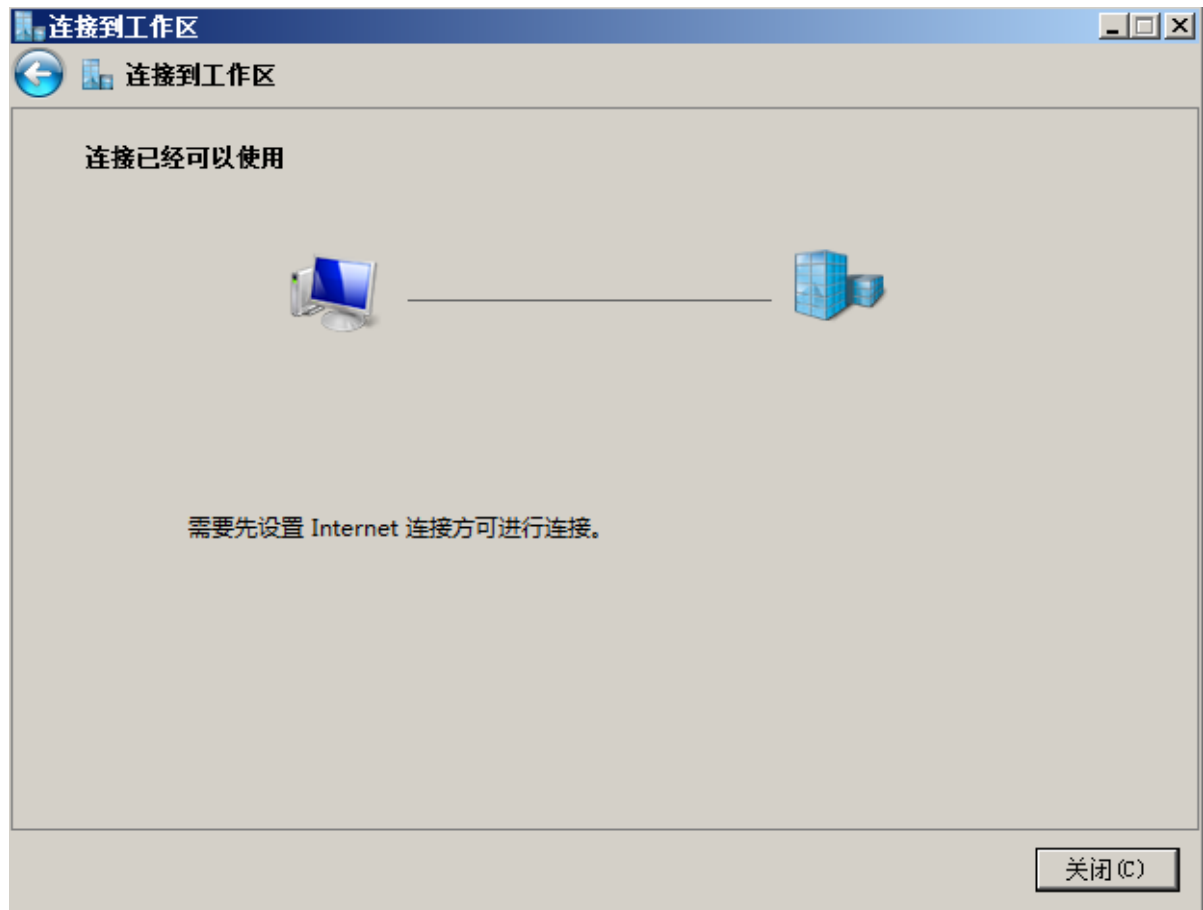
记住此密码(R)

域(可选)(D):

创建(C) 取消

# 此时显示连接已经可以使用，点击“关闭按钮”。

图8 连接创建成功



# 再次进入网络连接，发现新生成了一个网络连接“VPN 连接”，双击之后会出现登录窗口。

图9 新生成的连接

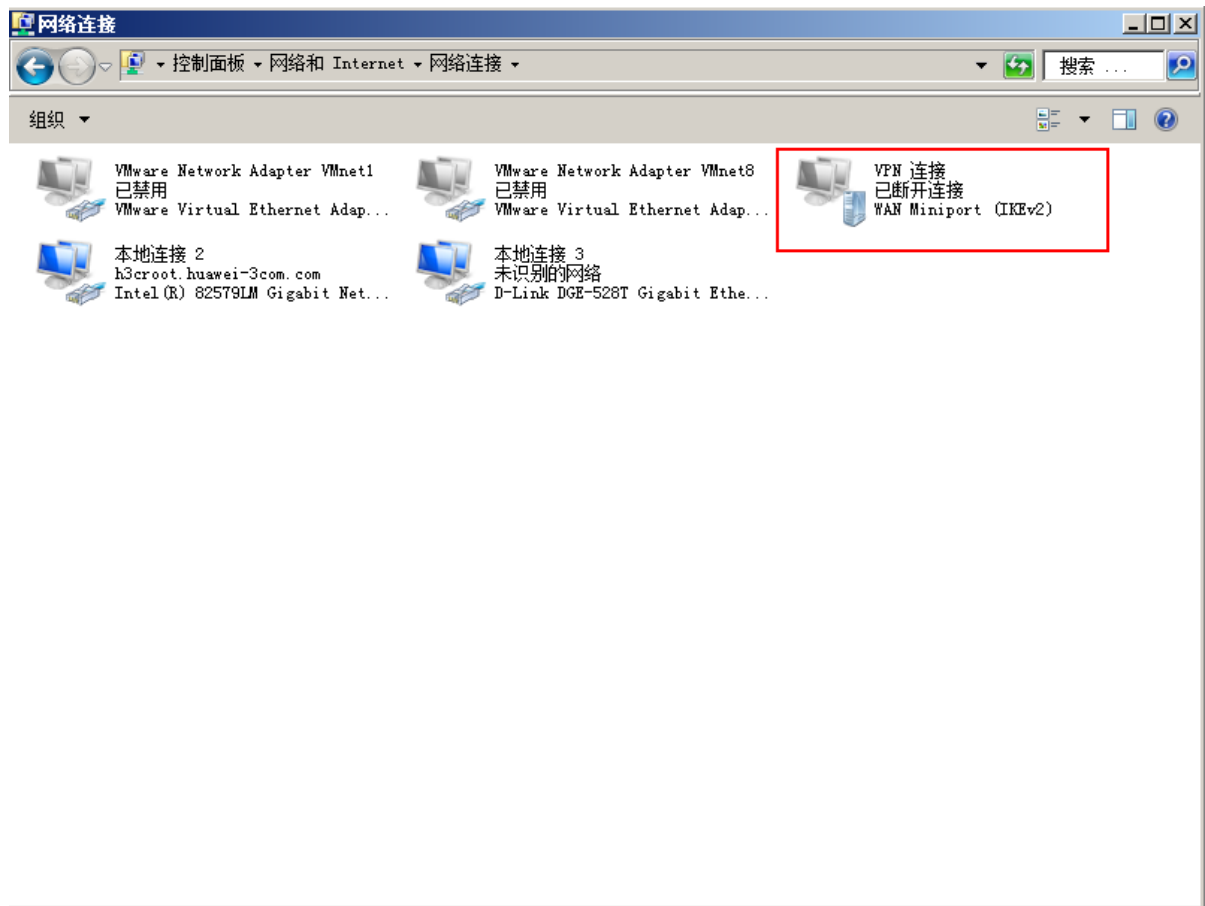
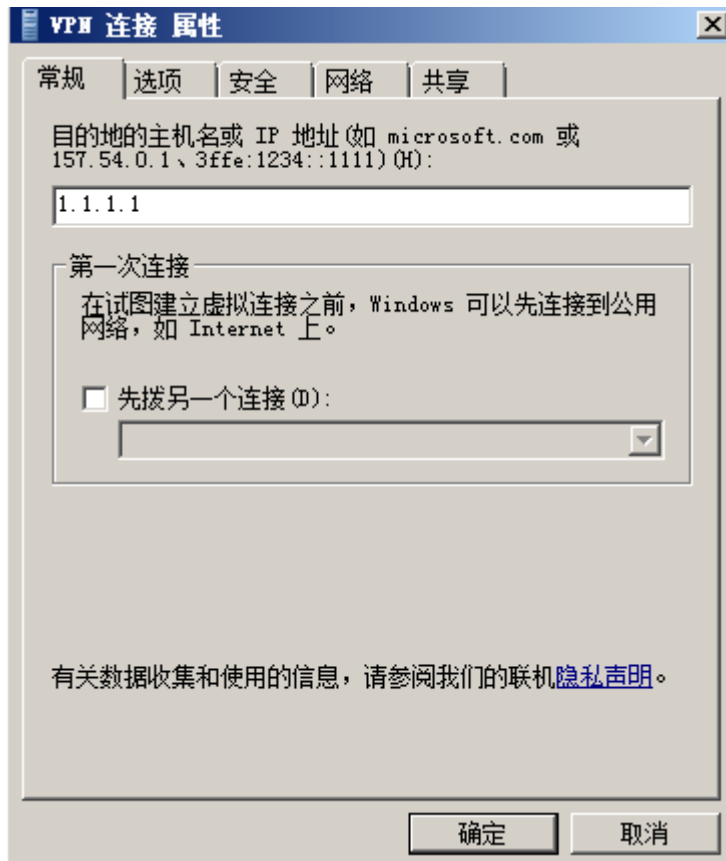


图10 登录窗口



# 配置“属性”，进入属性配置界面。

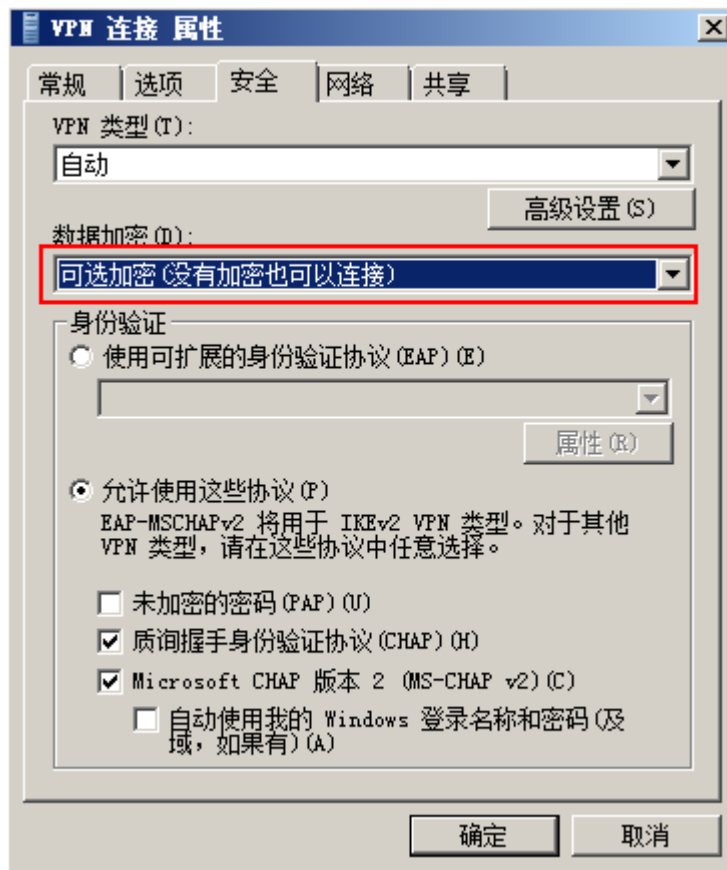
图11 VPN 连接属性



# 配置“安全”，数据加密选择“可选加密（没有加密也可以连接）”，点击“确定”。



图12 配置安全属性



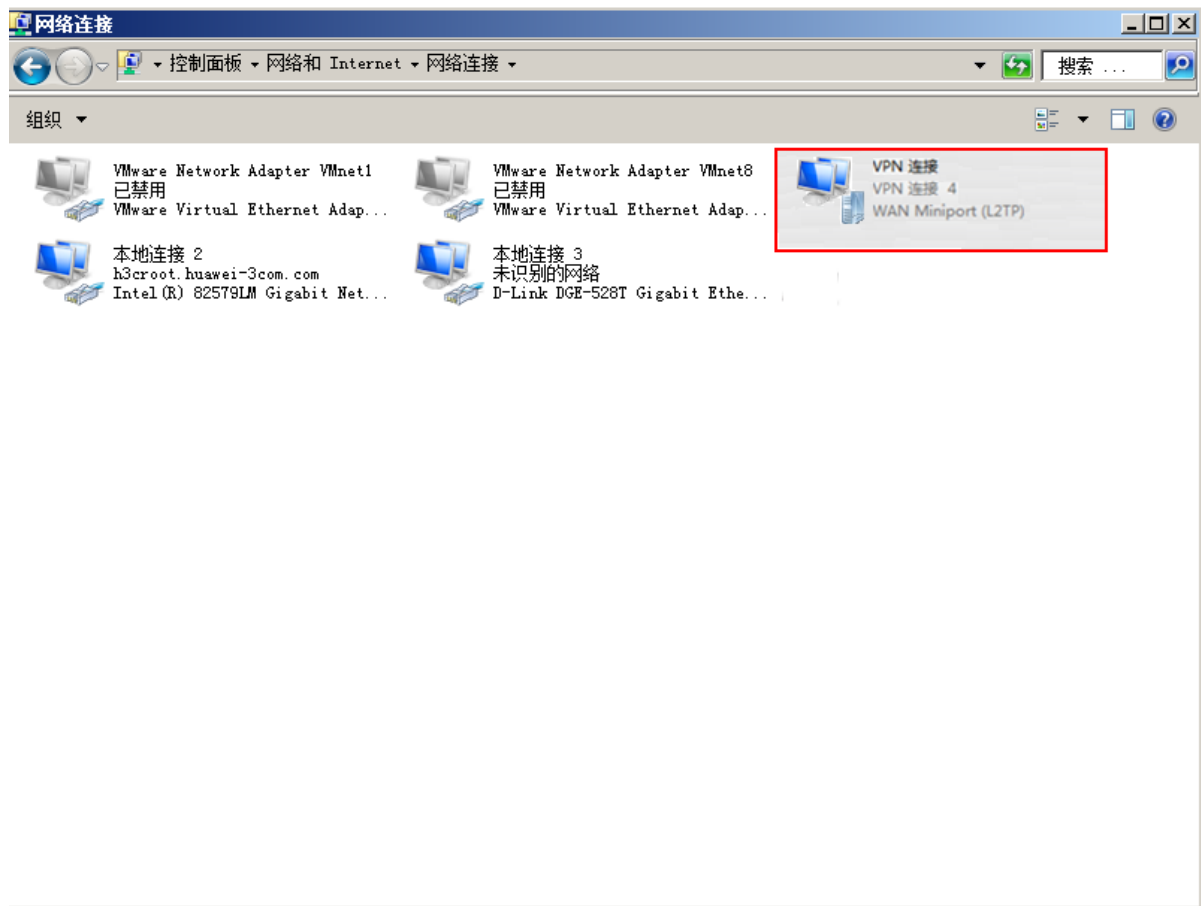
# 在登录窗口中输入在路由器设备上配置的用户名和密码: user@abc.com 和 hello, 点击“连接”。

图13 进行 L2TP 隧道连接



# 连接成功。

图14 连接成功



### 3.5 验证配置

# 在 LNS 上查看 L2TP 隧道已经建立。

```
[LNS] display l2tp tunnel
```

| LocalTID | RemoteTID | State       | Sessions | RemoteAddress | RemotePort | RemoteName |
|----------|-----------|-------------|----------|---------------|------------|------------|
| 11556    | 1         | Established | 1        | 1.1.1.2       | 1701       | Host       |

### 3.6 配置文件

```

interface Virtual-Templatel
 ppp authentication-mode chap domain abc
 remote address 192.168.0.2
 ip address 192.168.0.1 255.255.255.0

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 1.1.1.1 255.255.255.0

domain abc
```

```
authentication ppp local
#
local-user aa class network
password cipher c3$Rprc/RW4jluoNccTiRfV0t1OxEN0MegX
service-type ppp
authorization-attribute user-role network-operator
#
l2tp-group 1 mode lns
allow l2tp virtual-template 1
undo tunnel authentication
tunnel name LNS
#
l2tp enable
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“二层技术-广域网接入配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“二层技术-广域网接入命令参考”

# H3C MSR 系列路由器

## L2TP 多实例配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                         |   |
|-------------------------|---|
| 1 简介.....               | 1 |
| 2 配置前提.....             | 1 |
| 3 配置举例.....             | 1 |
| 3.1 组网需求.....           | 1 |
| 3.2 使用版本.....           | 1 |
| 3.3 配置步骤.....           | 1 |
| 3.3.1 Router C 的配置..... | 1 |
| 3.3.2 Router A 的配置..... | 3 |
| 3.3.3 Router B 的配置..... | 4 |
| 3.4 验证配置.....           | 4 |
| 3.5 配置文件.....           | 6 |
| 4 相关资料.....             | 8 |

# 1 简介

本文档介绍 MSR 系列路由器 L2TP 多实例配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

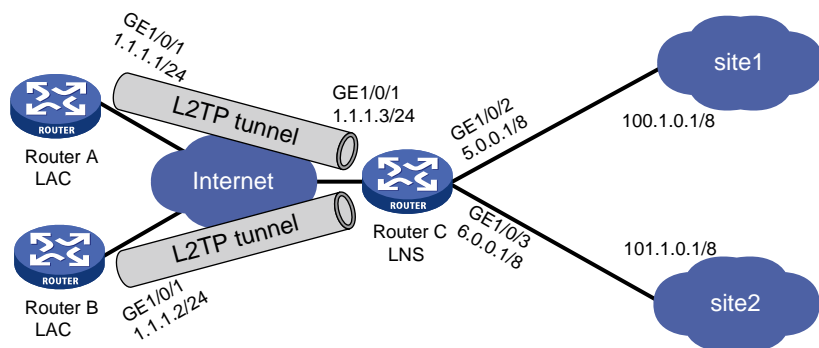
本文档假设您已了解 L2TP 特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，多个企业共用 Router C 作为 LNS，不同的企业用户分别连接 Router A 和 Router B 与各自的总部 site1 和 site2 进行通讯。现要求：在 Router C 上配置 L2TP 多实例功能，使其能够为 Router A 和 Router B 同时提供 L2TP 接入服务，实现不同企业的用户能够远程访问企业内部网络。

图1 L2TP 多实例典型配置举例组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置步骤

#### 3.3.1 Router C 的配置

# 全局开启 L2TP 功能。

```

<RouterC> system-view
[RouterC] l2tp enable
配置本地用户，并设置密码。
[RouterC] local-user 1 class network
[RouterC-luser-network-1] password simple 1234
[RouterC-luser-network-1] service-type ppp
[RouterC-luser-network-1] quit
[RouterC] local-user 2 class network
[RouterC-luser-network-2] password simple 1234
[RouterC-luser-network-2] service-type ppp
[RouterC-luser-network-2] quit
配置 VPN 实例 vpn1 和 vpn2。
[RouterC] ip vpn-instance vpn1
[RouterC-vpn-instance-vpn1] route-distinguisher 100:1
[RouterC-vpn-instance-vpn1] vpn-target 100:1 import-extcommunity
[RouterC-vpn-instance-vpn1] vpn-target 100:1 export-extcommunity
[RouterC-vpn-instance-vpn1] quit
[[RouterC] ip vpn-instance vpn2
[RouterC-vpn-instance-vpn2] route-distinguisher 200:1
[RouterC-vpn-instance-vpn2] vpn-target 200:1 import-extcommunity
[RouterC-vpn-instance-vpn2] vpn-target 200:1 export-extcommunity
[RouterC-vpn-instance-vpn2] quit
配置地址池。
[RouterC] ip pool 1 100.0.0.2 100.0.0.100
[RouterC] ip pool 2 101.0.0.2 101.0.0.100
创建虚拟模板接口 1。
[RouterC] interface virtual-template 1
在虚拟模板接口上采用 PAP 方式认证对端设备。
[RouterC-Virtual-Template1] ppp authentication-mode pap
接口使用地址池 1 为客户端分配地址。
[RouterC-Virtual-Template1] remote address pool 1
配置虚拟模板接口绑定 vpn1。
[RouterC-Virtual-Template1] ip binding vpn-instance vpn1
[RouterC-Virtual-Template1] ip address 100.0.0.1 8
[RouterC-Virtual-Template1] quit
创建虚拟模板接口 2。
[RouterC] interface virtual-template 2
在虚拟模板接口上采用 PAP 方式认证对端设备。
[RouterC-Virtual-Template2] ppp authentication-mode pap
接口使用地址池 2 为客户端分配地址。
[RouterC-Virtual-Template2] remote address pool 2
配置虚拟模板接口绑定 vpn1。
[RouterC-Virtual-Template2] ip binding vpn-instance vpn2
[RouterC-Virtual-Template2] ip address 101.0.0.1 8
[RouterC-Virtual-Template2] quit

```



# 创建 LNS 模式的 L2TP 组 1。

```
[RouterC] l2tp-group 1 mode lns
```

# 配置 LNS 侧本端名称为 lns-A, 指定接收呼叫的虚拟模板接口为 VT1, 并配置隧道对端名称为 lac-A。

```
[RouterC-l2tp1] tunnel name lns-A
```

```
[RouterC-l2tp1] undo tunnel authentication
```

```
[RouterC-l2tp1] allow l2tp virtual-template 1 remote lac-A
```

```
[RouterC-l2tp1] quit
```

# 创建 LNS 模式的 L2TP 组 1。

```
[RouterC] l2tp-group 2 mode lns
```

# 配置 LNS 侧本端名称为 lns-B, 指定接收呼叫的虚拟模板接口为 VT2, 并配置隧道对端名称为 lac-B。

```
[RouterC-l2tp2] tunnel name lns-B
```

```
[RouterC-l2tp2] undo tunnel authentication
```

```
[RouterC-l2tp2] allow l2tp virtual-template 2 remote lac-B
```

```
[RouterC-l2tp2] quit
```

# 配置接口地址并关联 VPN 实例。

```
[RouterC] interface gigabitEthernet 1/0/1
```

```
[RouterC-GigabitEthernet1/0/1] ip address 1.1.1.3 24
```

```
[RouterC-GigabitEthernet1/0/1] quit
```

```
[RouterC] interface gigabitEthernet 1/0/2
```

```
[RouterC-GigabitEthernet1/0/2] ip binding vpn-instance vpn1
```

```
[RouterC-GigabitEthernet1/0/2] ip address 5.0.0.1 8
```

```
[RouterC-GigabitEthernet1/0/2] quit
```

```
[RouterC] interface gigabitEthernet 1/0/3
```

```
[RouterC-GigabitEthernet1/0/3] ip binding vpn-instance vpn2
```

```
[RouterC-GigabitEthernet1/0/3] ip address 6.0.0.1 8
```

```
[RouterC-GigabitEthernet1/0/3] quit
```

### 3.3.2 Router A 的配置

# 全局开启 L2TP 功能。

```
<RouterA> system-view
```

```
[RouterA] l2tp enable
```

# 配置 L2TP 组。

```
[RouterA] l2tp-group 1 mode lac
```

# 配置 LAC 侧本端名称为 lac-A, 并指定 LNS 的 IP 地址为 1.1.1.3。

```
[RouterA-l2tp1] tunnel name lac-A
```

```
[RouterA-l2tp1] undo tunnel authentication
```

```
[RouterA-l2tp1] lns-ip 1.1.1.3
```

```
[RouterA-l2tp1] quit
```

# 创建和配置虚拟 PPP 接口, 配置 PPP 用户的用户名为 1、密码为 1234, 并配置 PPP 验证方式为 PAP。

```
[RouterA] interface virtual-PPP 1
```

```
[RouterA-Virtual-PPP1] ip address ppp-negotiate
```

```
[RouterA-Virtual-PPP1] ppp pap local-user 1 password simple 1234
```

```
[RouterA-Virtual-PPP1] quit
```

# 配置接口 GigabitEthernet1/0/1 的 IP 地址

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 1.1.1.1 24
[RouterA-GigabitEthernet1/0/1] quit
配置私网路由，访问公司总部的报文将通过 L2TP 隧道转发。
[RouterA] ip route-static 5.0.0.0 8 Virtual-PPP 1
配置触发 LAC 发起 L2TP 隧道建立请求。
[RouterA] interface virtual-PPP 1
[RouterA-Virtual-PPP1] l2tp-auto-client l2tp-group 1
[RouterA-Virtual-PPP1] quit
```

### 3.3.3 Router B 的配置

```
全局打开 L2TP 开关。
<RouterB> system-view
[RouterB] l2tp enable
配置 L2TP 组。
[RouterB] l2tp-group 1 mode lac
配置 LAC 侧本端名称为 lac-B，并指定 LNS 的 IP 地址为 1.1.1.3。
[RouterB-l2tp1] tunnel name lac-B
[RouterB-l2tp1] undo tunnel authentication
[RouterB-l2tp1] lns-ip 1.1.1.3
[RouterB-l2tp1] quit
创建和配置虚拟 PPP 接口，配置 PPP 用户的用户名为 2、密码为 1234，并配置 PPP 验证方式为 PAP。
[RouterB] interface virtual-PPP 1
[RouterB-Virtual-PPP1] ip address ppp-negotiate
[RouterB-Virtual-PPP1] ppp pap local-user 2 password simple 1234
[RouterB-Virtual-PPP1] quit
配置接口 GigabitEthernet1/0/1 的 IP 地址
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address 1.1.1.2 24
[RouterB-GigabitEthernet1/0/1] quit
配置私网路由，访问公司总部的报文将通过 L2TP 隧道转发。
[RouterB] ip route-static 6.0.0.0 8 virtual-PPP 1
配置触发 LAC 发起 L2TP 隧道建立请求。
[RouterB] interface virtual-PPP 1
[RouterB-Virtual-PPP1] l2tp-auto-client l2tp-group 1
[RouterB-Virtual-PPP1] quit
```

## 3.4 验证配置

- (1) 在 Router A 上，虚拟 PPP 接口分配 pool 1 中的 IP 地址。

```
[RouterA] display interface brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
```

| Interface | Link | Protocol | Main IP   | Description |
|-----------|------|----------|-----------|-------------|
| Aux0      | UP   | --       | --        |             |
| GE1/0/1   | UP   | UP       | 1.1.1.1   |             |
| GE1/0/2   | ADM  | DOWN     | 11.1.1.1  |             |
| InLoop0   | UP   | UP(s)    | --        |             |
| NULL0     | UP   | UP(s)    | --        |             |
| REG0      | DOWN | --       | --        |             |
| VPPP1     | UP   | UP       | 100.0.0.2 |             |

- (2) 在 Router B 上，虚拟 PPP 接口分配 pool 2 中的 IP 地址。

```
[RouterB] display interface brief
```

```
Brief information on interface(s) under route mode:
```

```
Link: ADM - administratively down; Stby - standby
```

```
Protocol: (s) - spoofing
```

| Interface | Link | Protocol | Main IP   | Description |
|-----------|------|----------|-----------|-------------|
| Aux0      | UP   | --       | --        |             |
| GE1/0/1   | UP   | UP       | 1.1.1.2   |             |
| GE1/0/2   | UP   | UP       | 12.1.1.1  |             |
| GE3/0     | ADM  | DOWN     | --        |             |
| InLoop0   | UP   | UP(s)    | --        |             |
| NULL0     | UP   | UP(s)    | --        |             |
| REG0      | DOWN | --       | --        |             |
| VPPP1     | UP   | UP       | 101.0.0.2 |             |

- (3) Router A 能 Ping 通 Router C 的地址 5.0.0.1，L2TP 隧道建立成功。

```
[RouterA] ping -a 100.0.0.2 5.0.0.1
```

```
Ping 5.0.0.1 (5.0.0.1): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 5.0.0.1: icmp_seq=0 ttl=128 time=0.452 ms
```

```
56 bytes from 5.0.0.1: icmp_seq=1 ttl=128 time=0.625 ms
```

```
56 bytes from 5.0.0.1: icmp_seq=2 ttl=128 time=0.673 ms
```

```
56 bytes from 5.0.0.1: icmp_seq=3 ttl=128 time=0.687 ms
```

```
56 bytes from 5.0.0.1: icmp_seq=4 ttl=128 time=0.679 ms
```

```
--- Ping statistics for 5.0.0.1 ---
```

```
5 packets transmitted, 5 packets received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 0.452/0.623/0.687/0.088 ms
```

- # 在 Router B 能 Ping 通 Router C 的地址 6.0.0.1，L2TP 隧道建立成功。

```
[RouterB] ping 6.0.0.1
```

```
Ping 6.0.0.1 (6.0.0.1): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 6.0.0.1: icmp_seq=0 ttl=128 time=0.452 ms
```

```
56 bytes from 6.0.0.1: icmp_seq=1 ttl=128 time=0.625 ms
```

```
56 bytes from 6.0.0.1: icmp_seq=2 ttl=128 time=0.673 ms
```

```
56 bytes from 6.0.0.1: icmp_seq=3 ttl=128 time=0.687 ms
```

```
56 bytes from 6.0.0.1: icmp_seq=4 ttl=128 time=0.679 ms
```

```
--- Ping statistics for 6.0.0.1 ---
```

```
5 packets transmitted, 5 packets received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 0.452/0.623/0.687/0.088 ms
```

## 3.5 配置文件

- Router C

```
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
ip vpn-instance vpn2
 route-distinguisher 200:1
 vpn-target 200:1 import-extcommunity
 vpn-target 200:1 export-extcommunity
#
ip pool 1 100.0.0.2 100.0.0.100
ip pool 2 101.0.0.2 101.0.0.100
#
interface Virtual-Template1
 ppp authentication-mode pap
 remote address pool 1
 ip binding vpn-instance vpn1
 ip address 100.0.0.1 255.0.0.0
#
interface Virtual-Template2
 ppp authentication-mode pap
 remote address pool 2
 ip binding vpn-instance vpn2
 ip address 101.0.0.1 255.0.0.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 1.1.1.3 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip binding vpn-instance vpn1
 ip address 5.0.0.1 255.0.0.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip binding vpn-instance vpn2
 ip address 6.0.0.1 255.0.0.0
#
local-user 1 class network
 password cipher c3$Wf7ut8Li9ryKmOvk53vSKPHvBQH0u8w=
 service-type ppp
 authorization-attribute user-role network-operator
```

```
#
local-user 2 class network
password cipher c3$rpUZj85qaeXDflgm1P5af58Kj/maHXM=
service-type ppp
authorization-attribute user-role network-operator
```

```
#
l2tp-group 1 mode lns
allow l2tp virtual-template 1 remote lac-A
undo tunnel authentication
tunnel name lns-A
```

```
#
l2tp-group 2 mode lns
allow l2tp virtual-template 2 remote lac-B
tunnel name lns-B
```

```
#
l2tp enable
```

- **Router A:**

```
#
interface Virtual-PPP1
ppp pap local-user 1 password cipher c3$CYBBKjOoTx2nLdklyFk5zUtfXOKC5f8=
ip address ppp-negotiate
l2tp-auto-client l2tp-group 1
```

```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 1.1.1.1 255.255.255.0
```

```
#
ip route-static 5.0.0.0 8 Virtual-PPP1
```

```
#
l2tp-group 1 mode lac
lns-ip 1.1.1.3
undo tunnel authentication
tunnel name lac-A
```

```
#
l2tp enable
```

- **Router B :**

```
#
interface Virtual-PPP1
ppp pap local-user 2 password cipher c3$w9MwmqfWlBN/bbkspWTwTE9V3Zxe6Sk=
ip address ppp-negotiate
l2tp-auto-client l2tp-group 1
```

```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 1.1.1.2 255.255.255.0
```

```
#
```

```
ip route-static 6.0.0.0 8 Virtual-PPPoE
#
l2tp-group 1 mode lac
 lns-ip 1.1.1.3
 undo tunnel authentication
 tunnel name lac-B
#
l2tp enable
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“二层技术-广域网接入配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“二层技术-广域网接入命令参考”

# H3C MSR 系列路由器

## L2TP 多域接入配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                      |    |
|----------------------|----|
| 1 简介.....            | 1  |
| 2 配置前提.....          | 1  |
| 3 配置举例.....          | 1  |
| 3.1 组网需求.....        | 1  |
| 3.2 配置思路.....        | 1  |
| 3.3 使用版本.....        | 2  |
| 3.4 配置步骤.....        | 2  |
| 3.4.1 LNS 的配置.....   | 2  |
| 3.4.2 Host 侧的配置..... | 3  |
| 3.5 验证配置.....        | 16 |
| 3.6 配置文件.....        | 16 |
| 4 相关资料.....          | 17 |



# 1 简介

本文档介绍 MSR 系列路由器 L2TP 多域接入配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 特性。

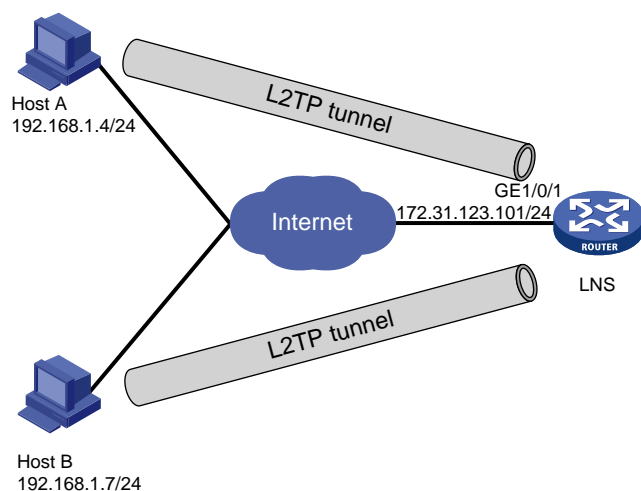
## 3 配置举例

### 3.1 组网需求

如图 1 所示，不同地区的主机 Host A 和 Host B 上通过 L2TP 隧道传输数据。具体应用需求如下：

- LNS 上设置两个域，分别为属于不同区域的用户提供接入服务；
- 不同域的用户获得不同网段的 IP 地址，实现与 LNS 互通。

图1 MSR 系列路由器 L2TP 多域接入配置组网图



### 3.2 配置思路

为了保证合法用户可以正常接入从而建立 Client-Initiated 模式 L2TP 隧道，在 LNS 上配置 L2TP 用户侧认证，并创建 PPP 用户和用户所属的域，在 Host 侧需要使用设备上配置的用户名来发起隧道建立请求。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置步骤

### 3.4.1 LNS 的配置

```
使能 L2TP。
<LNS> system-view
[LNS] l2tp enable
配置两个地址池，为不同域的用户分配不同网段的 IP 地址。
[LNS] ip pool 1 10.0.1.2 10.0.1.10
[LNS] ip pool 2 10.0.2.2 10.0.2.10
配置域 abc.com 关联地址池 1，并且配置 PPP 的认证方式为本地认证。
[LNS] domain abc.com
[LNS-isp-abc.com] authorization-attribute ip-pool 1
[LNS-isp-abc.com] authentication ppp local
[LNS-isp-abc.com] quit
配置域 abc2.com 关联地址池 2，并且配置 PPP 的认证方式为本地认证。
[LNS] domain abc2.com
[LNS-isp-abc2.com] authorization-attribute ip-pool 2
[LNS-isp-abc2.com] authentication ppp local
[LNS-isp-abc2.com] quit
创建接口 Virtual-Template1，配置接口的 IP 地址为 10.0.1.1/24，PPP 认证方式为 CHAP，并指
定从 pool1 为 PPP 用户分配的 IP 地址。
[LNS] interface virtual-template1
[LNS-Virtual-Template1] ppp authentication-mode chap domain abc.com
[LNS-Virtual-Template1] remote address pool 1
[LNS-Virtual-Template1] ip address 10.0.1.1 255.255.255.0
[LNS-Virtual-Template1] quit
创建接口 Virtual-Template2，配置接口的 IP 地址为 10.0.2.1/24，PPP 认证方式为 CHAP，并指
定从 pool2 为 PPP 用户分配的 IP 地址。
[LNS] interface virtual-template2
[LNS-Virtual-Template2] ppp authentication-mode chap domain abc2.com
[LNS-Virtual-Template2] remote address pool 2
[LNS-Virtual-Template2] ip address 10.0.2.1 255.255.255.0
[LNS-Virtual-Template2] quit
配置接口 GigabitEthernet1/0/1。
[LNS] interface gigabitethernet1/0/1
[LNS-GigabitEthernet1/0/1] port link-mode route
[LNS-GigabitEthernet1/0/1] ip address 172.31.123.101 255.255.255.0
[LNS-GigabitEthernet1/0/1] quit
创建用户 user1，密码为 hello，服务类型为 ppp。
[LNS] local-user user1 class network
[LNS-luser-network-user1] password simple hello
```

```
[LNS-luser-network-user1] service-type ppp
[LNS-luser-network-user1] quit
创建用户 user2, 密码为 hello, 服务类型为 ppp。
[LNS] local-user user2 class network
[LNS-luser-network-user2] password simple hello
[LNS-luser-network-user2] service-type ppp
[LNS-luser-network-user2] quit
创建 L2TP 组, 模式为 LNS, 关闭隧道验证。
[LNS] l2tp-group 1 mode lns
[LNS-l2tp1] allow l2tp virtual-template 1 remote user1.abc.com
[LNS-l2tp1] undo tunnel authentication
[LNS-l2tp1] quit
创建 L2TP 组, 模式为 LNS, 关闭隧道验证。
[LNS] l2tp-group 2 mode lns
[LNS-l2tp2] allow l2tp virtual-template 2 remote user2.abc2.com
[LNS-l2tp2] undo tunnel authentication
[LNS-l2tp2] quit
```

### 3.4.2 Host 侧的配置

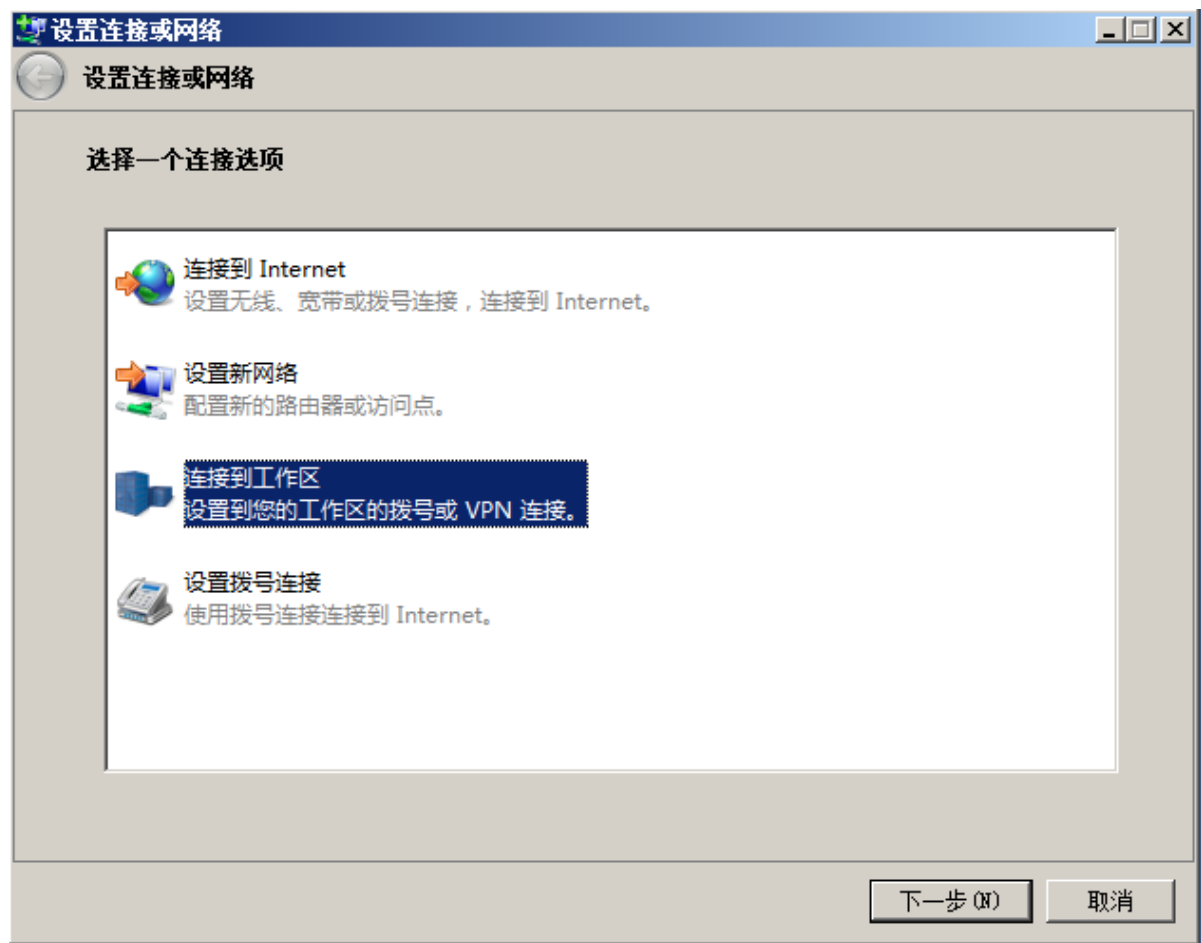
# 配置两台主机的 IP 地址为 192.168.1.4 和 192.168.2.7, 网关为各自网关地址。  
# 以 Windows 7 系统为例, 进入网络和共享中心, 点击“设置新的网络和连接”。

图2 新建网络连接



# 选择“连接到我的工作区”，点击“下一步”。

图3 选择一个连接选项



# 选择“使用我的 Internet 连接(VPN)”。

图4 选择连接方式



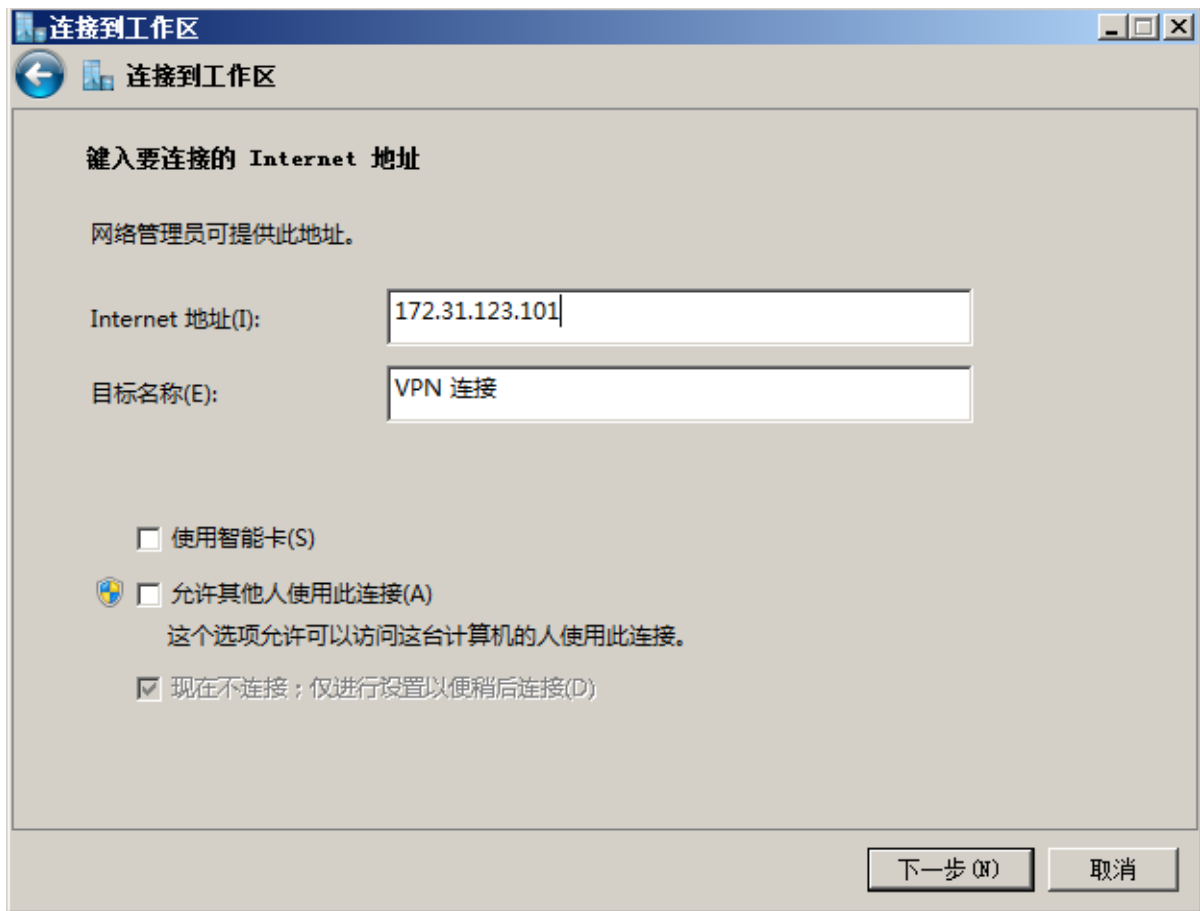
# 选择“我将稍后设置 Internet 连接”。

图5 设置 Internet 方式



# 设置“Internet 地址”，该地址为 LNS 上主机侧的接口地址，选择“下一步”。

图6 设置 LNS 的地址



# 在对话框中输入设备上配置好的用户名和密码，选择“创建”。



图7 键入用户名和密码

连接到工作区

键入您的用户名和密码

用户名(U): user1

密码(P): ●●●●●

显示字符(S)

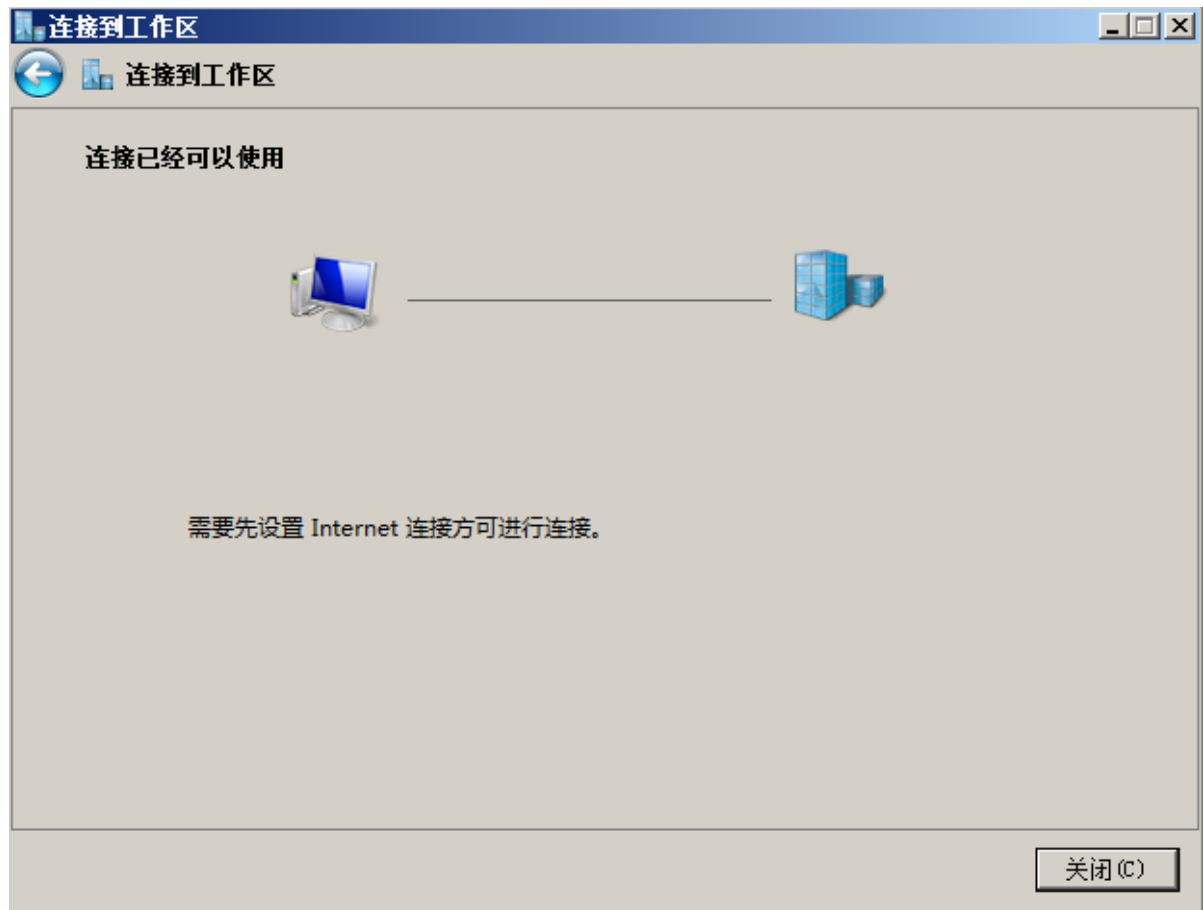
记住此密码(R)

域(可选)(D):

创建(C) 取消

# 此时显示连接已经可以使用，点击“关闭按钮”。

图8 连接创建成功



# 再次进入网络连接，发现新生成了一个网络连接“VPN 连接”，双击之后会出现登录窗口。

图9 新生成的连接

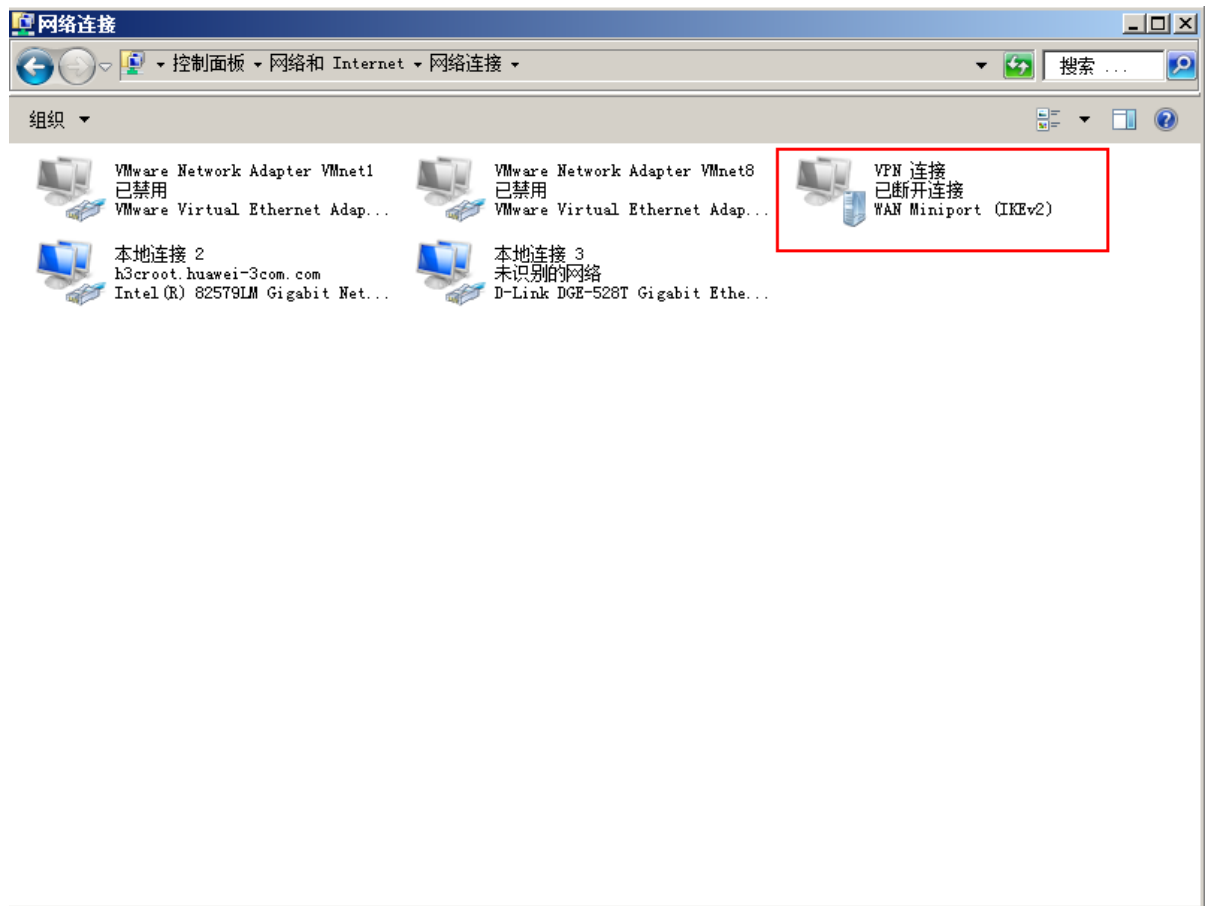
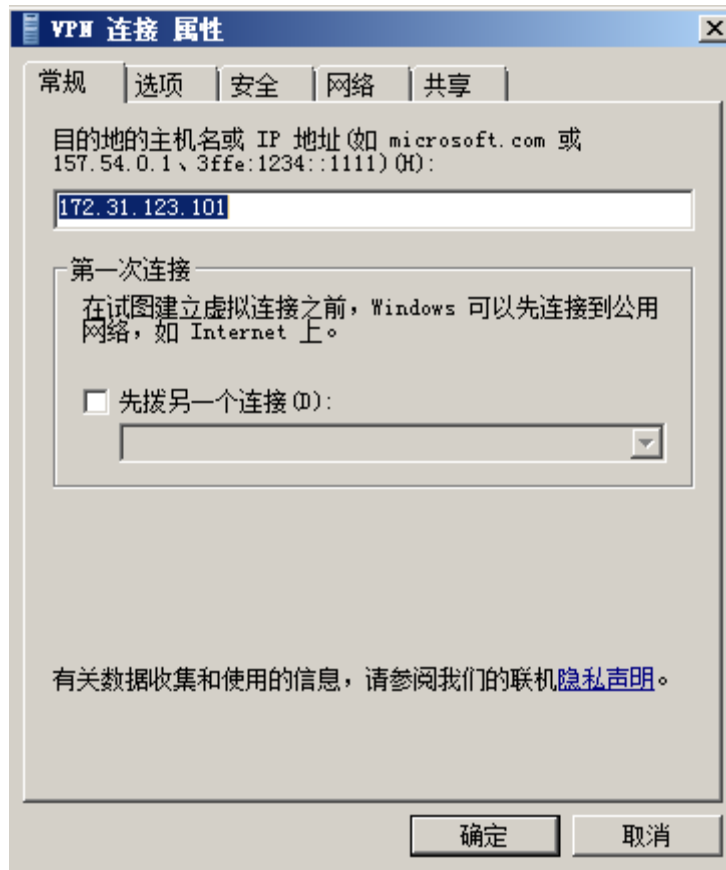


图10 登录窗口



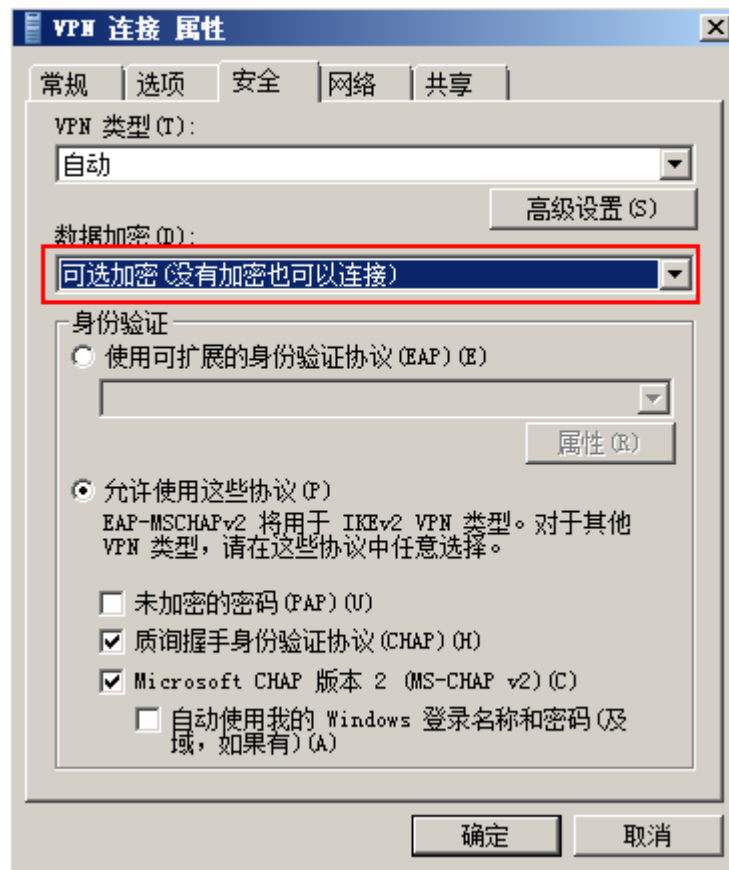
# 配置“属性”，进入属性配置界面。

图11 VPN 连接属性



# 配置“安全”，数据加密选择“可选加密（没有加密也可以连接）”，点击“确定”。

图12 配置安全属性



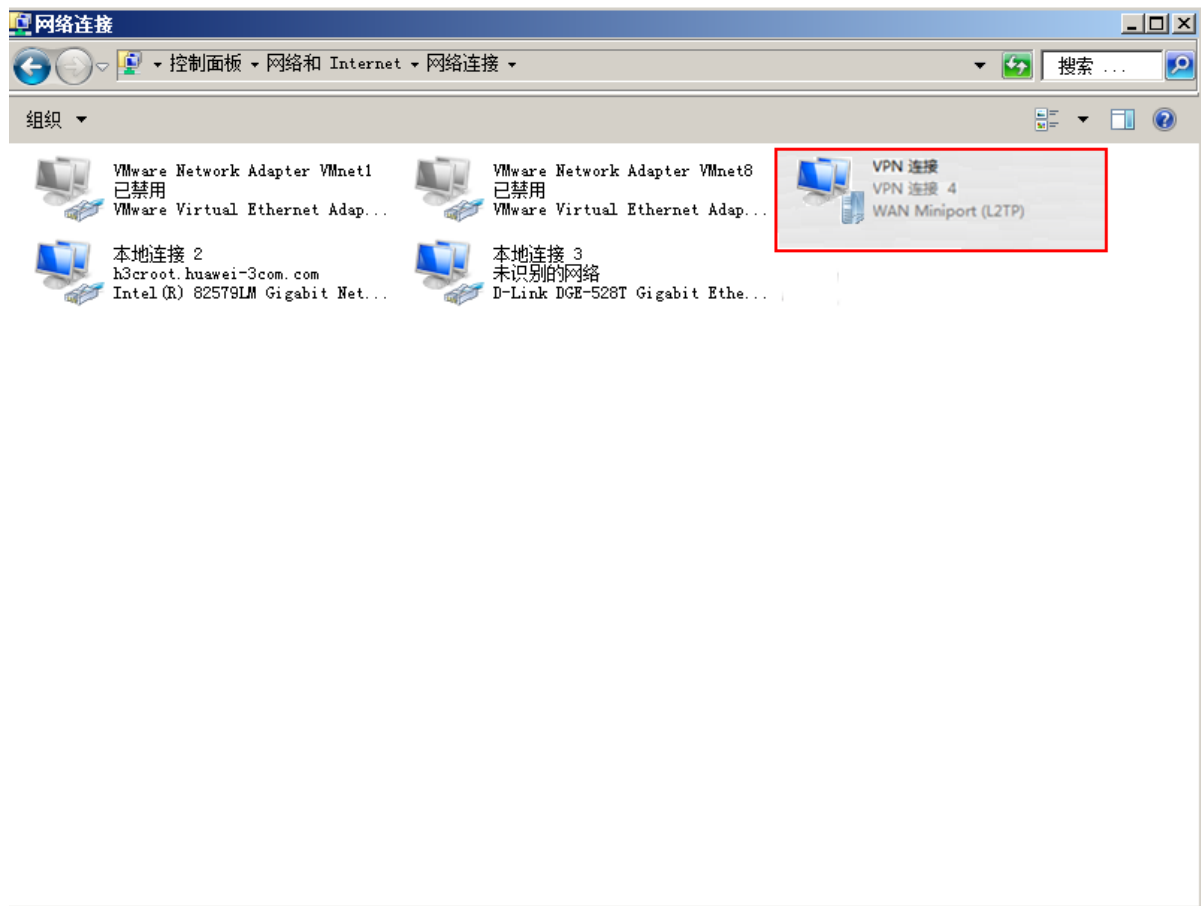
# 在登录窗口中输入在路由器设备上配置的用户名和密码: user1@abc.com 和 hello, 点击“连接”。

图13 进行 L2TP 隧道连接



# 连接成功。

图14 连接成功



### 3.5 验证配置

# 在 LNS 侧，通过命令 **display l2tp tunnel** 查看建立的 L2TP 隧道。

```
[LNS] display l2tp tunnel
```

| LocalTID | RemoteTID | State       | Sessions | RemoteAddress | RemotePort | RemoteName     |
|----------|-----------|-------------|----------|---------------|------------|----------------|
| 23287    | 1         | Established | 1        | 192.168.1.4   | 1701       | user1.abc.com  |
| 36956    | 35        | Established | 1        | 192.168.2.7   | 1701       | user2.abc2.com |

# 在 LNS 侧，通过命令 **display l2tp session** 可查看已建立的 L2TP 会话。

```
[LNS] display l2tp session
```

| LocalSID | RemoteSID | LocalTID | State       |
|----------|-----------|----------|-------------|
| 30933    | 1         | 23287    | Established |
| 21828    | 1         | 36956    | Established |

### 3.6 配置文件

```

ip pool 1 10.0.1.2 10.0.1.10
ip pool 2 10.0.2.2 10.0.2.10
#
```



```

interface Virtual-Template1
 ppp authentication-mode chap domain abc.com
 remote address pool 1
 ip address 10.0.1.1 255.255.255.0
#
interface Virtual-Template2
 ppp authentication-mode chap domain abc2.com
 remote address pool 2
 ip address 10.0.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 172.31.123.101 255.255.255.0
#
domain abc.com
 authorization-attribute ip-pool 1
 authentication ppp local
#
domain abc2.com
 authorization-attribute ip-pool 2
 authentication ppp local
#
user-group system
#
local-user user1 class network
 password cipher c3$UkOKC65RHN4wUaJ6sWyzHKC7a+N59kEJ
 service-type ppp
 authorization-attribute user-role network-operator
#
local-user user2 class network
 password cipher c3$JUujxfCIpEGTGw9HbO26xfm55GLo2g==
 service-type ppp
 authorization-attribute user-role network-operator
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1 remote user1.abc.com
 undo tunnel authentication
#
l2tp-group 2 mode lns
 allow l2tp virtual-template 2 remote user2.abc2.com
 undo tunnel authentication
#
l2tp enable
#

```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“二层技术-广域网接入配置指导”

- 《H3C MSR 系列路由器 命令参考 (V7)》中的“二层技术-广域网接入命令参考”

# H3C MSR 系列路由器

## L2TP over IPsec 配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                    |   |
|--------------------|---|
| 1 简介.....          | 1 |
| 2 配置前提.....        | 1 |
| 3 配置举例.....        | 1 |
| 3.1 组网需求.....      | 1 |
| 3.2 使用版本.....      | 1 |
| 3.3 配置步骤.....      | 1 |
| 3.3.1 LNS 的配置..... | 1 |
| 3.3.2 LAC 的配置..... | 3 |
| 3.4 验证配置.....      | 4 |
| 3.5 配置文件.....      | 7 |
| 4 相关资料.....        | 9 |

# 1 简介

本文档介绍 MSR 系列路由器 L2TP over IPsec 典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 和 IPsec 特性。

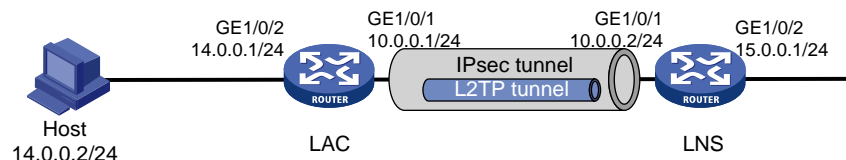
## 3 配置举例

### 3.1 组网需求

如图 1 所示，Host 通过 L2TP 隧道访问 LNS 一侧的网络。具体应用需求如下：

- LAC 与 LNS 自动建立 L2TP 隧道
- LAC 与 LNS 之间采用 IKE 方式建立 IPsec 安全隧道来对 L2TP 流量进行加密。

图1 MSR 系列路由器 L2TP over IPsec 典型配置组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置步骤

#### 3.3.1 LNS 的配置

```
配置本地用户 1，设置密码为 1234。
<LNS> system-view
[LNS] local-user 1 class network
[LNS-luser-network-1] password simple 1234
[LNS-luser-network-1] service-type ppp
[LNS-luser-network-1] quit
```

# 配置 ISP 域 system 对 PPP 用户采用本地验证。

```
[LNS] domain system
[LNS-isp-system] authentication ppp local
[LNS-isp-system] quit
```

# 使能 L2TP。

```
[LNS] l2tp enable
```

# 配置虚模板 Virtual-Template1 配置接口的 IP 地址为 192.168.0.1/24，PPP 认证方式为 PAP，并指定为 PPP 用户分配的 IP 地址为 192.168.0.2。

```
[LNS] interface virtual-template 1
[LNS-Virtual-Template1] ip address 192.168.0.1 24
[LNS-Virtual-Template1] ppp authentication-mode pap domain system
[LNS-Virtual-Template1] remote address 192.168.0.2
[LNS-Virtual-Template1] quit
```

# 创建 LNS 模式的 L2TP 组 1，配置隧道本端名称为 lns，指定接收呼叫的虚拟模板接口为 VT1，并配置 L2TP 隧道对端名为 lac。

```
[LNS] l2tp-group 1 mode lns
[LNS-l2tp1] tunnel name lns
[LNS-l2tp1] undo tunnel authentication
[LNS-l2tp1] allow l2tp virtual-template 1 remote lac
[LNS-l2tp1] quit
```

# 配置访问控制列表。

```
[LNS] acl number 3000
[LNS-acl-adv-3000] rule permit ip source 10.0.0.2 0 destination 10.0.0.1 0
[LNS-acl-adv-3000] quit
```

# 配置 IKE keychain。

```
[LNS] ike keychain l2tp
```

# 配置与地址为 10.0.0.1 的对端使用的预共享密钥为明文的 abcd。

```
[LNS-ike-keychain-l2tp] pre-shared-key address 10.0.0.1 key simple abcd
[LNS-ike-keychain-l2tp] quit
```

#在 IKE profile l2tp 中指定名称为 l2tp 的配置的 IKE keychain。

```
[LNS] ike profile l2tp
[LNS-ike-profile-l2tp] keychain l2tp
```

# 指定使用 IP 地址 10.0.0.2 标识本端身份。

```
[LNS-ike-profile-l2tp] local-identity address 10.0.0.2
```

# 指定需要匹配对端身份类型为 IP 地址，取值为 10.0.0.1。

```
[LNS-ike-profile-l2tp] match remote identity address 10.0.0.1
[LNS-ike-profile-l2tp] quit
```

# 配置 IPsec 安全协议。

```
[LNS] ipsec transform-set l2tp
```

# 配置 IPsec 安全提议采用的 ESP 加密算法为 CBC 模式的 3DES 算法。

```
[LNS-ipsec-transform-set-l2tp] esp encryption-algorithm 3des-cbc
```

# 配置 IPsec 安全提议采用的 ESP 认证算法为 MD5。

```
[LNS-ipsec-transform-set-l2tp] esp authentication-algorithm md5
[LNS-ipsec-transform-set-l2tp] quit
```

# 配置 IPsec 安全策略引用 ACL 3000 和名字为 l2tp 的 IPsec 安全提议，并指定 IPsec 隧道的对端 IPv4 地址为 10.0.0.1。

```
[LNS] ipsec policy l2tp 1 isakmp
[LNS-ipsec-policy-isakmp-l2tp-1] security acl 3000
[LNS-ipsec-policy-isakmp-l2tp-1] transform-set l2tp
[LNS-ipsec-policy-isakmp-l2tp-1] ike-profile l2tp
[LNS-ipsec-policy-isakmp-l2tp-1] remote-address 10.0.0.1
[LNS-ipsec-policy-isakmp-l2tp-1] quit
```

# 配置连接 LAC 的接口 GigabitEthernet1/0/1 的 IP 地址并使能 IPsec 安全策略。

# 配置接口 IP 地址并使能 IPsec 安全策略。

```
[LNS] interface gigabitethernet 1/0/1
[LNS-GigabitEthernet1/0/1] ip address 10.0.0.2 24
[LNS-GigabitEthernet1/0/1] ipsec apply policy l2tp
[LNS-GigabitEthernet1/0/1] quit
```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[LNS] interface gigabitethernet 1/0/2
[LNS-GigabitEthernet1/0/2] ip address 15.0.0.1 24
[LNS-GigabitEthernet1/0/2] quit
```

### 3.3.2 LAC 的配置

# 开启 L2TP 功能。

```
<LAC> system-view
[LAC] l2tp enable
```

# 创建 LAC 模式的 L2TP 组 1。

```
[LAC] l2tp-group 1 mode lac
```

# 配置 LAC 侧本端名称为 LAC，并指定 LNS 的 IP 地址为 10.0.0.2。

```
[LAC-l2tp1] tunnel name lac
[LAC-l2tp1] lns-ip 10.0.0.2
[LAC-l2tp1] undo tunnel authentication
[LAC-l2tp1] quit
```

# 配置访问控制列表。

```
[LAC] acl number 3000
```

# 配置 ACL 的规则。

```
[LAC-acl-adv-3000] rule permit ip source 10.0.0.1 0 destination 10.0.0.2 0
[LAC-acl-adv-3000] quit
```

# 配置 Virtual-ppp 口，配置 PPP 用户的用户名为 1，密码为 1234，并配置 PPP 验证方式为 PAP。

```
[LAC] interface virtual-PPP 1
[LAC-Virtual-PPP1] ip address ppp-negotiate
[LAC-Virtual-PPP1] ppp pap local-user 1 password simple 1234
[LAC-Virtual-PPP1] quit
```

# 配置私网路由，访问公司总部的报文将通过 L2TP 隧道转发。

```
[LAC] ip route-static 15.0.0.1 24 Virtual-PPP 1
```

# 配置 IKE keychain。

```
[LAC] ike keychain l2tp
```

```

配置与地址为 10.0.0.2 的对端使用的预共享密钥为明文的 abcd。
[LAC-ike-keychain-l2tp] pre-shared-key address 10.0.0.2 key simple abcd
[LAC-ike-keychain-l2tp] quit
在 IKE profile l2tp 中指定名称为 l2tp 的配置的 IKE keychain。
[LAC] ike profile l2tp
[LAC-ike-profile-l2tp] keychain l2tp
指定使用 IP 地址 10.0.0.1 标识本端身份。
[LAC-ike-profile-l2tp] local-identity address 10.0.0.1
指定需要匹配对端身份类型为 IP 地址，取值为 10.0.0.2。
[LAC-ike-profile-l2tp] match remote identity address 10.0.0.2
[LAC-ike-profile-l2tp] quit
配置 Ipsec 安全协议。
[LAC] ipsec transform-set l2tp
配置 IPsec 安全提议采用的 ESP 加密算法为 CBC 模式的 3DES 算法。
[LAC-ipsec-transform-set-l2tp] esp encryption-algorithm 3des-cbc
配置 IPsec 安全提议采用的 ESP 认证算法为 MD5。
[LAC-ipsec-transform-set-l2tp] esp authentication-algorithm md5
[LAC-ipsec-transform-set-l2tp] quit
配置 IPsec 安全策略引用 ACL 3000 和名字为 l2tp 的 IPsec 安全提议，并指定 IPsec 隧道的对端 IPv4 地址为 10.0.0.2。
[LAC] ipsec policy l2tp 1 isakmp
[LAC-ipsec-policy-isakmp-l2tp-1] security acl 3000
[LAC-ipsec-policy-isakmp-l2tp-1] transform-set l2tp
[LAC-ipsec-policy-isakmp-l2tp-1] ike-profile l2tp
[LAC-ipsec-policy-isakmp-l2tp-1] remote-address 10.0.0.2
[LAC-ipsec-policy-isakmp-l2tp-1] quit
配置接口 GigabitEthernet1/0/2 的 IP 地址。
[LAC] interface gigabitethernet 1/0/2
[LAC-GigabitEthernet1/0/2] ip address 14.0.0.1 24
[LAC-GigabitEthernet1/0/2] quit
配置连接 LNS 的接口 GigabitEthernet1/0/1 的 IP 地址并使能 IPsec 安全策略。
[LAC] interface gigabitethernet 1/0/1
[LAC-GigabitEthernet1/0/1] ip address 10.0.0.1 24
[LAC-GigabitEthernet1/0/1] ipsec apply policy l2tp
[LAC-GigabitEthernet1/0/1] quit
执行 l2tp-auto-client 命令触发 LAC 建立 L2TP 隧道。
[LAC] interface virtual-PPP 1
[LAC-Virtual-PPP1] l2tp-auto-client l2tp-group 1

```

### 3.4 验证配置

# LAC 上可以看到 L2TP 隧道和 L2TP 会话的建立情况。

```

[LAC] display l2tp tunnel

```

| LocalTID | RemoteTID | State       | Sessions | RemoteAddress | RemotePort | RemoteName |
|----------|-----------|-------------|----------|---------------|------------|------------|
| 23561    | 63423     | Established | 1        | 10.0.0.2      | 1701       | lns        |



```
[LAC] display l2tp session
```

```
LocalSID RemoteSID LocalTID State
1538 2562 23561 Established
```

# LNS 上可以看到 L2TP 隧道和 L2TP 会话的建立情况。

```
[LNS] display l2tp tunnel
```

```
LocalTID RemoteTID State Sessions RemoteAddress RemotePort RemoteName
63423 23561 Established 1 10.0.0.1 1701 lac
```

```
[LNS] display l2tp session
```

```
LocalSID RemoteSID LocalTID State
2562 1538 63423 Established
```

# LAC 上可以看到 IKE SA 和 IPsec SA 的建立情况。

```
[LAC] display ike sa
```

```
Connection-ID Remote Flag DOI

5 10.0.0.2 RD IPSEC
```

Flags:

RD--READY RL--REPLACED FD-FADING

```
[LAC]display ipsec sa
```

```

Interface: GigabitEthernet1/0/1

```

```

IPsec policy: l2tp
Sequence number: 1
Mode: isakmp

```

```
Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1443
Tunnel:
 local address: 10.0.0.1
 remote address: 10.0.0.2
```

```
Flow:
sour addr: 10.0.0.1/255.255.255.255 port: 0 protocol: ip
dest addr: 10.0.0.2/255.255.255.255 port: 0 protocol: ip
```

```
[Inbound ESP SAs]
```

```
SPI: 987342280 (0x3ad9a5c8)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843181/2339
Max received sequence-number: 319
Anti-replay check enable: Y
```

```
Anti-replay window size: 64
UDP encapsulation used for nat traversal: N
Status: active
```

```
[Outbound ESP SAs]
```

```
SPI: 2705574035 (0xa143c893)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843182/2339
Max sent sequence-number: 301
UDP encapsulation used for nat traversal: N
Status: active
```

# LNS 上可以看到 IKE SA 和 IPSec SA 的建立情况。

```
[LNS] display ike sa
```

| Connection-ID | Remote   | Flag | DOI   |
|---------------|----------|------|-------|
| 1             | 10.0.0.1 | RD   | IPSEC |

```
Flags:
```

```
RD--READY RL--REPLACED FD-FADING
```

```
[LNS] display ipsec sa
```

```

Interface: GigabitEthernet1/0/1

```

```

IPsec policy: l2tp
```

```
Sequence number: 1
```

```
Mode: isakmp

```

```
Tunnel id: 0
```

```
Encapsulation mode: tunnel
```

```
Perfect forward secrecy:
```

```
Path MTU: 1443
```

```
Tunnel:
```

```
local address: 10.0.0.2
```

```
remote address: 10.0.0.1
```

```
Flow:
```

```
sour addr: 10.0.0.2/255.255.255.255 port: 0 protocol: ip
```

```
dest addr: 10.0.0.1/255.255.255.255 port: 0 protocol: ip
```

```
[Inbound ESP SAs]
```

```
SPI: 2705574035 (0xa143c893)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843181/2300
Max received sequence-number: 310
```

```
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for nat traversal: N
Status: active
```

```
[Outbound ESP SAs]
```

```
SPI: 987342280 (0x3ad9a5c8)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843180/2300
Max sent sequence-number: 329
UDP encapsulation used for nat traversal: N
Status: active
```

# Host A 所属网段可以通过 L2TP 隧道访问外网。

```
[LAC] ping -a 14.0.0.1 15.0.0.1
```

```
Ping 15.0.0.1 (15.0.0.1) from 14.0.0.1: 56 data bytes, press escape sequence to break
56 bytes from 15.0.0.1: icmp_seq=0 ttl=255 time=0.462 ms
56 bytes from 15.0.0.1: icmp_seq=1 ttl=255 time=0.280 ms
56 bytes from 15.0.0.1: icmp_seq=2 ttl=255 time=0.276 ms
56 bytes from 15.0.0.1: icmp_seq=3 ttl=255 time=0.280 ms
56 bytes from 15.0.0.1: icmp_seq=4 ttl=255 time=0.280 ms
```

```
--- Ping statistics for 15.0.0.1 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.276/0.316/0.462/0.073 ms
```

```
[LAC]%Jul 3 14:01:16:689 2013 LAC PING/6/PING_STATIS_INFO: Ping statistics for 15.0.0.1:
5 packet(s) transmitted, 5 packet(
s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.276/0.316/0.462/0.073 ms.
```

## 3.5 配置文件

- LNS:

```
#
interface Virtual-Template1
 remote address 192.168.0.2
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 10.0.0.2 255.255.255.0
 ipsec apply policy l2tp
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 15.0.0.1 255.255.255.0
#
ip route-static 14.0.0.0 24 192.168.0.2
```

```

#
acl number 3000
 rule 0 permit ip source 10.0.0.2 0 destination 10.0.0.1 0
#
domain system
 authentication ppp local
#
local-user 1 class network
 password cipher c3$1dZEFYrvdICeeFOnqOoFpzXF8G0dZ+4=
 service-type ppp
 authorization-attribute user-role network-operator
#
ipsec transform-set l2tp
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy l2tp 1 isakmp
 transform-set l2tp
 security acl 3000
 remote-address 10.0.0.1
 ike-profile l2tp
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1 remote lac
 undo tunnel authentication
 tunnel name lns
#
l2tp enable
#
ike profile l2tp
 keychain l2tp
 local-identity address 10.0.0.2
 match remote identity address 10.0.0.1 255.255.255.255
#
ike keychain l2tp
 pre-shared-key address 10.0.0.1 255.255.255.255 key cipher
c3$7tvgeKfH6On3KIybUaywz5NDiHtwJqU=
#
• LAC:
#
interface Virtual-PPP1
 ppp pap local-user 1 password cipher c3$i132FpC8DcHeIet4NXtmz6ot44xY8ts=
 ip address ppp-negotiate
 l2tp-auto-client l2tp-group 1
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.0.1 255.255.255.0

```

```

ipsec apply policy l2tp
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 14.0.0.1 255.255.255.0
#
acl number 3000
rule 0 permit ip source 10.0.0.1 0 destination 10.0.0.2 0
#
domain system
authentication ppp local
#
ipsec transform-set l2tp
esp encryption-algorithm 3des-cbc
esp authentication-algorithm md5
#
ipsec policy l2tp 1 isakmp
transform-set l2tp
security acl 3000
remote-address 10.0.0.2
ike-profile l2tp
#
l2tp-group 1 mode lac
lns-ip 10.0.0.2
undo tunnel authentication
tunnel name lac
#
l2tp enable
#
ike profile l2tp
keychain l2tp
local-identity address 10.0.0.1
match remote identity address 10.0.0.2 255.255.255.255
#
ike keychain l2tp
pre-shared-key address 10.0.0.2 255.255.255.255 key cipher
c3$3ErJJ2M1lhES32CdsR3ofs5CdLvPJGk=
#

```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导 (V7)》中的“二层技术-广域网接入配置指导”
- 《H3C MSR 系列路由器 命令参考 (V7)》中的“二层技术-广域网接入命令参考”
- 《H3C MSR 系列路由器 配置指导 (V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考 (V7)》中的“安全命令参考”

# H3C MSR 系列路由器

## AAA 配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                                      |    |
|--------------------------------------|----|
| 1 简介.....                            | 1  |
| 2 配置前提.....                          | 1  |
| 3 Telnet 用户的 HWTACACS 认证和授权配置举例..... | 1  |
| 3.1 组网需求.....                        | 1  |
| 3.2 配置思路.....                        | 1  |
| 3.3 使用版本.....                        | 2  |
| 3.4 配置步骤.....                        | 2  |
| 3.4.1 配置 HWTACACS.....               | 2  |
| 3.4.2 配置 Device.....                 | 5  |
| 3.5 验证配置.....                        | 6  |
| 3.6 配置文件.....                        | 6  |
| 4 SSH 用户的 RADIUS 认证和授权配置举例.....      | 7  |
| 4.1 组网需求.....                        | 7  |
| 4.2 配置思路.....                        | 7  |
| 4.3 使用版本.....                        | 7  |
| 4.4 配置步骤.....                        | 8  |
| 4.4.1 配置 RADIUS 服务器.....             | 8  |
| 4.4.2 配置 Device.....                 | 9  |
| 4.5 验证配置.....                        | 11 |
| 4.6 配置文件.....                        | 11 |
| 5 相关资料.....                          | 11 |

# 1 简介

本文档介绍了 Telnet、SSH 用户通过 AAA 服务器进行登录认证和授权的配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解 AAA 特性。

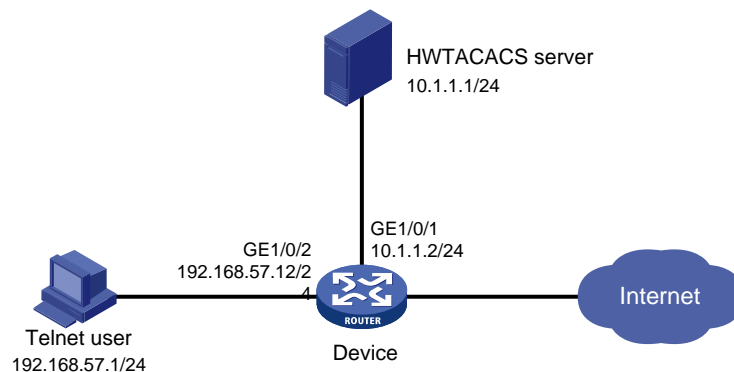
## 3 Telnet 用户的 HWTACACS 认证和授权配置举例

### 3.1 组网需求

如图 1 所示，要求在 Device 上配置实现：

- HWTACACS 服务器对登录 Device 的 Telnet 用户进行认证和授权，登录用户名为 `user@bbb`，密码为 `aabbcc`；
- 用户通过认证后可执行系统所有功能和资源的相关 `display` 命令。

图1 Telnet 用户的远端 HWTACACS 认证和授权配置组网图



### 3.2 配置思路

- 为了使 HWTACACS 服务器能够识别合法的用户，在 HWTACACS 服务器上添加合法的 Telnet 用户名和密码。
- 由于本例中用户登录 Device 要通过 AAA 处理，因此 Telnet 用户登录的用户界面认证方式配置为 `scheme`。



- 为了实现通过 HWTACACS 来进行认证和授权，需要在 Device 上配置 HWTACACS 方案并指定相应的认证和授权服务器，并将其应用于 Telnet 用户所属的 ISP 域。
- 为了在 Device 和 HWTACACS 服务器之间安全地传输用户密码，并且能在 Device 上验证服务器响应报文未被篡改，在 Device 和 HWTACACS 服务器上都要设置交互报文时所使用的共享密钥。

### 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.4 配置步骤

#### 3.4.1 配置 HWTACACS



说明

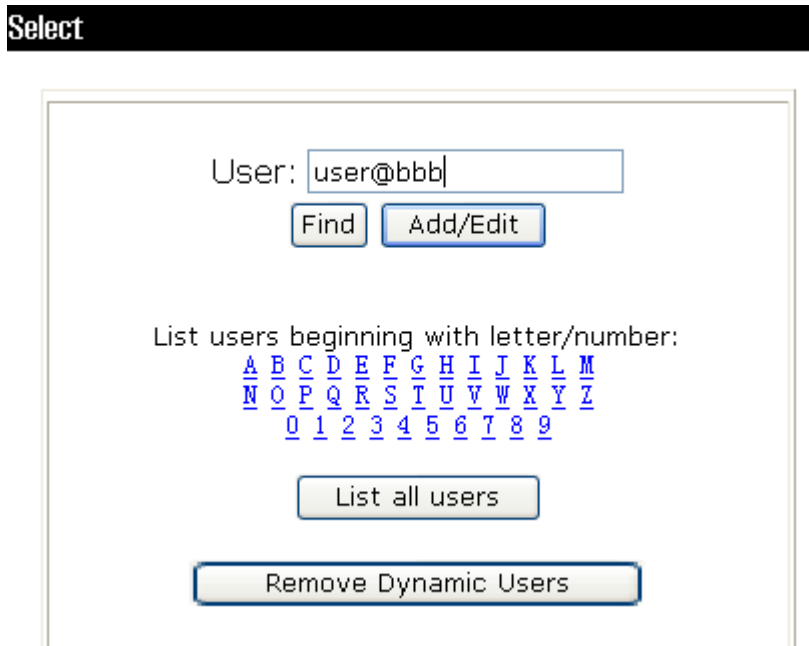
本文以 HWTACACS 服务器 ACS 4.0 为例，说明该例中 HWTACACS 的基本配置。

##### 1. 增加设备管理用户

# 登录进入 HWTACACS 管理平台, 点击左侧导航栏 “User-Setup” 增加设备管理用户。

- 在界面上输入用户名 “user@bbb” ；
- 点击按钮 “Add/Edit” 进入用户编辑页面。

图2 用户创建界面



## 2. 配置设备管理用户

# 在用户编辑页面上配置设备管理用户。

- 配置用户密码 “aabbcc”；
- 为用户选择组 “Group 1”；
- 单击 “Submit” 完成操作。

图3 用户密码配置界面

**User Setup**

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: [Masked]

Confirm Password: [Masked]

Separate (CHAP/MS-CHAP/ARAP)

Password: [Masked]

Confirm Password: [Masked]

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Group 1

Submit Cancel

## 3. 配置网络

# 点击左侧导航栏 “Network Configuration”，在 “AAA Client Hostname” 处任意命名（本例为 “Device”）后开始配置网络。

- “AAA Client IP Address” 一栏填写 Device 与 HWTACACS 服务器相连的接口的 IP 地址 “10.1.1.2”。
- “Key” 一栏填写 HWTACACS 服务器和设备通信时的共享密钥 “imc”，必须和 Device 上 HWTACACS 方案里配置的认证和授权共享密钥相同。
- 在 “Authenticate Using” 的下拉框里选择 “TACACS+ (Cisco IOS)”。
- 单击 “Submit+Apply” 按钮完成配置。

图4 网络配置界面

**Edit**

### Add AAA Client

AAA Client Hostname: Device

AAA Client IP Address: 10.1.1.2

Key: imc

Network Device Group: (Not Assigned)

Authenticate Using: TACACS+ (Cisco IOS)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Apply Cancel

#### 4. 设置组

# 单击左侧导航栏“Group Setup”，选取“Group 1”（与配置设备管理用户时为用户选择的组一致），单击“Edit Settings”进入编辑区。

- 在多选框中选择“Shell”（用户可以执行命令）；
- 在多选框中选择“Custom attributes”，并在文本框中输入：`roles=\network-operator\`（用户可执行系统所有功能和资源的相关 **display** 命令）；
- 单击“Submit”后完成操作。

图5 选择组界面

**Select**

### Group Setup

Group : 1: Group 1 (29 users)

Users in Group Edit Settings Rename Group

图6 组配置界面

TACACS+ Settings

PPP IP

In access control list

Out access control list

Route

Routing  Enabled

Custom attributes

Note: PPP LCP will be automatically enabled if this service is enabled

Shell (exec)

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify  Enabled

No escape  Enabled

No hangup  Enabled

Privilege level

Timeout

Custom attributes

roles="network-operator"

Submit Cancel

### 3.4.2 配置 Device

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ip address 192.168.57.12 255.255.255.0
[Device-GigabitEthernet1/0/2] quit
```

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.1.1.2 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

# 开启 Device 的 Telnet 服务器功能。

```
[Device] telnet server enable
```

# 配置 Telnet 用户登录的用户界面采用 scheme 方式。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

# 配置 HWTACACS 方案 hwtac。

```
[Device] hwtacacs scheme hwtac
```

# 配置主认证、授权和计费服务器的 IP 地址为 10.1.1.1，认证、授权和计费的端口号为 49（HWTACACS 服务器的认证、授权和计费端口为 TCP 端口 49）。

```

[Device-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Device-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Device-hwtacacs-hwtac] primary accounting 10.1.1.1 49
配置与认证、授权和计费服务器交互报文时的共享密钥均为明文 imc。
[Device-hwtacacs-hwtac] key authentication simple imc
[Device-hwtacacs-hwtac] key authorization simple imc
[Device-hwtacacs-hwtac] key accounting simple imc
[Device-hwtacacs-hwtac] quit
配置 ISP 域的 AAA 方案，为 login 用户配置 AAA 认证方法为 HWTACACS 认证、授权和计费。
[Device] domain bbb
[Device-isp-bbb] authentication login hwtacacs-scheme hwtac
[Device-isp-bbb] authorization login hwtacacs-scheme hwtac
[Device-isp-bbb] accounting login hwtacacs-scheme hwtac
[Device-isp-bbb] quit

```

### 3.5 验证配置

Telnet 用户可以使用用户名 `user@bbb` 和密码 `aabbcc` 通过认证，并且获得用户角色 `network-operator`（用户通过认证后可执行系统所有功能和资源的相关 `display` 命令）。

### 3.6 配置文件

```

#
telnet server enable
#
interface gigabitethernet1/0/2
port link-mode route
ip address 192.168.57.12 255.255.255.0
#
interface gigabitethernet1/0/1
port link-mode route
ip address 10.1.1.2 255.255.255.0
#
line vty 0 63
authentication-mode scheme
user-role network-operator
#
hwtacacs scheme hwtac
primary authentication 10.1.1.1
primary authorization 10.1.1.1
primary accounting 10.1.1.1
key authentication cipher c3$6ps2/dT38b2K2MDCMCDGYxrvyJNR+/jiKw==
key authorization cipher c3$xEldxJraE8Yof3rHHlVIgyCIb/uLlrZbgg==
key accounting cipher c3$kySCJbNA8DSs+l3HCqxunl8SE4me3vue5g==
#
domain bbb
authentication login hwtacacs-scheme hwtac
authorization login hwtacacs-scheme hwtac

```

```
accounting login hwtacacs-scheme hwtac
#
```

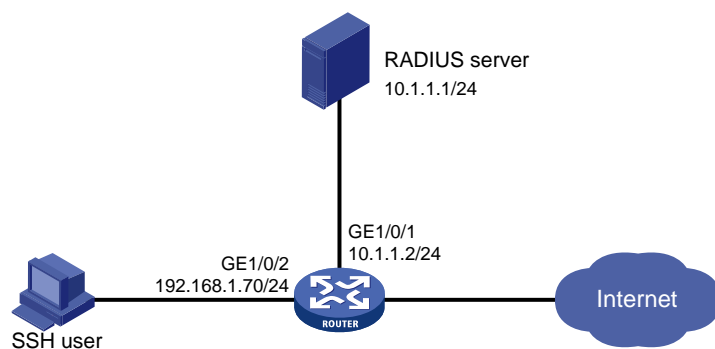
## 4 SSH 用户的 RADIUS 认证和授权配置举例

### 4.1 组网需求

如图7所示，要求在 Device 上配置实现：

- RADIUS 服务器对登录 Device 的 SSH 用户进行认证和授权，登录用户名为 *hello@bbb*，密码为 *aabbcc*；
- Device 向 RADIUS 服务器发送的用户名带域名，服务器根据用户名携带的域名来区分提供给用户的服务。
- 用户通过认证后可执行系统所有功能和资源的相关 **display** 命令。

图7 SSH 用户的远端 RADIUS 认证和授权配置组网图



### 4.2 配置思路

- 为了使 RADIUS 服务器能够识别合法的用户，在 RADIUS 服务器上添加合法的用户名和密码。
- 因为 SSH 用户登录 Device 要通过 AAA 处理，因此 SSH 用户登录的用户界面认证方式配置为 *scheme*。
- 为了实现通过 RADIUS 来进行认证和授权，需要在 Device 上配置 RADIUS 方案并指定相应的认证和授权服务器，并将其应用于 SSH 用户所属的 ISP 域。
- 为了在 Device 和 RADIUS 服务器之间安全地传输用户密码，并且能在 Device 上验证 RADIUS 服务器响应报文未被篡改，在 Device 和 RADIUS 服务器上都要设置交互报文时所使用的共享密钥。

### 4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.4 配置步骤

### 4.4.1 配置 RADIUS 服务器



说明

本文以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0102)、iMC EIA 7.0(E0201)），说明该例中 RADIUS 服务器的基本配置。

#### 1. 增加接入设备

# 登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置与 Device 交互报文时使用的认证和授权共享密钥为“expert”；
- 设置认证及计费的端口号分别为“1812”（RADIUS 服务器的认证端口为 UDP 端口 1812）和“1813”（RADIUS 服务器的计费端口为 UDP 端口 1813）；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C(General)”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

**接入配置**

|        |              |          |        |
|--------|--------------|----------|--------|
| 认证端口 * | 1812         | 计费端口 *   | 1813   |
| 组网方式   | 不启用混合组网      | 业务类型     | 设备管理业务 |
| 接入设备类型 | H3C(General) | 接入设备分组   | 无      |
| 共享密钥 * | .....        | 确认共享密钥 * | .....  |
| 业务分组   | 未分组          |          |        |

**设备列表**

选择 手工增加 全部清除

| 设备名称 | 设备IP地址   | 设备型号 | 备注 | 删除 |
|------|----------|------|----|----|
|      | 10.1.1.2 |      |    | 删除 |

共有1条记录。

确定 取消

#### 2. 增加设备管理用户

# 选择“用户”页签，单击导航树中的[接入用户管理/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 输入用户名“hello@bbb”和密码。
- 选择服务类型为“SSH”。

- 输入用户角色名“network-operator”
- 添加所管理设备的 IP 地址，IP 地址范围为“10.1.1.1~10.1.1.255”。
- 单击<确定>按钮完成操作。



说明

添加的所管理设备的 IP 地址范围要包含添加的接入设备的 IP 地址。

图9 增加设备管理用户

用户 > 设备管理用户 > 增加设备管理用户 ? 帮助

**增加设备管理用户**

**设备管理用户基本信息**

帐号名 \*  ?

用户密码 \*

密码确认 \*

服务类型

EXEC权限级别  ?

角色名

**提示**

注意：输入绑定的多个角色名时，每行只能写一个角色名，且角色名占用字节数与角色名个数（出现多个相同角色名时被视为一个角色名）总和不超过234。例如，假定输入10个角色，则角色占用字节数应不超过224个。

**绑定的用户IP地址列表**

| 起始IP地址      | 结束IP地址 | 删除 |
|-------------|--------|----|
| 未找到符合条件的记录。 |        |    |

**所管理设备IP地址列表**

| 起始IP地址   | 结束IP地址     | 删除                                |
|----------|------------|-----------------------------------|
| 10.1.1.1 | 10.1.1.255 | <input type="button" value="删除"/> |

#### 4.4.2 配置 Device

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ip address 192.168.1.70 255.255.255.0
[Device-GigabitEthernet1/0/2] quit
```

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.1.1.2 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```



**# 生成 RSA 及 DSA 密钥对。**

```
[Device] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++
.....+++++
..+++++++
.....+++++++
Create the key pair successfully.
```

```
[Device] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
..+++++++*
.....+......+......+......+.
...+......+......+......+.
Create the key pair successfully.
```

**# 使能 SSH 服务器功能。**

```
[Device] ssh server enable
```

**# 配置 SSH 用户登录采用 AAA 认证方式。**

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

**# 创建 RADIUS 方案 rad。**

```
[Device] radius scheme rad
```

**# 配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。**

```
[Device-radius-rad] primary authentication 10.1.1.1 1812
```

**# 配置主计费服务器的 IP 地址为 10.1.1.1，计费端口号为 1813。**

```
[Device-radius-rad] primary accounting 10.1.1.1 1813
```

**# 配置与认证和计费服务器交互报文时的共享密钥为明文 expert。**

```
[Device-radius-rad] key authentication simple expert
```

```
[Device-radius-rad] key accounting simple expert
```

**# 配置向 RADIUS 服务器发送的用户名要携带域名。**

```
[Device-radius-rad] user-name-format with-domain
```

```
[Device-radius-rad] quit
```

**# 创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 RADIUS 认证、授权和计费。**

```
[Device] domain bbb
```

```
[Device-isp-bbb] authentication login radius-scheme rad
```

```
[Device-isp-bbb] authorization login radius-scheme rad
```

```
[Device-isp-bbb] accounting login radius-scheme rad
```

```
[Device-isp-bbb] quit
```

## 4.5 验证配置

用户向 Device 发起 SSH 连接，在 SSH 客户端按照提示输入用户名 `hello@bbb` 和密码 `aabbcc` 通过认证，并且获得用户角色 `network-operator`（用户通过认证后可执行系统所有功能和资源的相关 `display` 命令）。

## 4.6 配置文件

```
#
interface gigabitethernet1/0/2
 port link-mode route
 ip address 192.168.1.70 255.255.255.0
#
interface gigabitethernet1/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher c3$63G7LzIQElGq4aFGTiYQafU+loQxS/cbLg==
 key accounting cipher c3$tUIVlyGISJ5X/yiTfWrmh8nyjBIF+1LFzQ==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

## 5 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“安全命令参考”

# H3C MSR 系列路由器

## 802.1X 本地认证配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                 |   |
|-----------------|---|
| 1 简介.....       | 1 |
| 2 配置前提.....     | 1 |
| 3 配置举例.....     | 1 |
| 3.1 组网需求.....   | 1 |
| 3.2 使用版本.....   | 1 |
| 3.3 配置注意事项..... | 1 |
| 3.4 配置步骤.....   | 1 |
| 3.5 验证配置.....   | 2 |
| 3.6 配置文件.....   | 3 |
| 4 相关资料.....     | 3 |

# 1 简介

本文档介绍 MSR 系列路由器 802.1X 本地认证的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

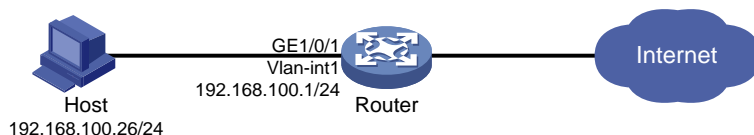
本文档假设您已了解 AAA 和 802.1X 特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，用户通过 Router 的端口 GigabitEthernet1/0/1 接入网络，要求：Router 对从该端口接入的用户采用基于端口的接入控制方式进行 802.1X 本地认证以控制其访问 Internet。

图1 802.1X 本地认证配置组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置注意事项

本例仅在安装了二层交换卡和有固定二层接口的设备上才能实现。

### 3.4 配置步骤

# 开启全局 802.1X 功能。

```
<Router> system-view
```

```
[Router] dot1x
```

# 配置虚接口 Vlan-interface1 的 IP 地址，作为 Host 的网关。

```
[Router] interface vlan-interface 1
```

```
[Router-Vlan-interface1] ip address 192.168.100.1 255.255.255.0
```

```

[Router-Vlan-interface1] quit
创建网络接入类本地用户 localuser，并配置用户密码和服务类型属性。
[Router] local-user localuser class network
[Router-luser-network-localuser] password simple localpass
[Router-luser-network-localuser] service-type lan-access
[Router-luser-network-localuser] quit
配置端口 GigabitEthernet1/0/1 的 802.1X 功能。
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] dot1x
配置基于端口的接入控制方式（默认为基于 MAC 地址）。
[Router-GigabitEthernet1/0/1] dot1x port-method portbased
[Router-GigabitEthernet1/0/1] quit

```

### 3.5 验证配置

# 使用命令 **display dot1x interface** 可以查看端口 GigabitEthernet1/0/1 上的 802.1X 的配置情况。

```

[Router] display dot1x interface gigabitethernet 1/0/1
Global 802.1X parameters:
 802.1X authentication : Enabled
 CHAP authentication : Enabled
 Max-tx period : 30 s
 Handshake period : 15 s
 Quiet timer : Disabled
 Quiet period : 60 s
 Supp timeout : 30 s
 Server timeout : 100 s
 Reauth period : 3600 s
 Max auth requests : 2
 SmartOn supp timeout : 30 s
 SmartOn retry counts : 3
 EAD assistant function : Disabled
 EAD timeout : 30 min
 Domain delimiter : @
Online 802.1X wired users : 0
GigabitEthernet1/0/1 is link-up
 802.1X authentication : Enabled
 Handshake : Enabled
 Handshake reply : Disabled
 Handshake security : Disabled
 Unicast trigger : Disabled
 Periodic reauth : Disabled
 Port role : Authenticator
 Authorization mode : Auto
 Port access control : Port-based
 Multicast trigger : Enabled
 Mandatory auth domain : Not configured

```

```
Guest VLAN : Not configured
Auth-Fail VLAN : Not configured
Critical VLAN : Not configured
Critical voice VLAN : Disabled
Re-auth server-unreachable : Logoff
Max online users : 4294967295
SmartOn : Disabled
```

```
EAPOL packets: Tx 3, Rx 0
Sent EAP Request/Identity packets : 3
 EAP Request/Challenge packets: 0
 EAP Success packets: 0
 EAP Failure packets: 0
 EAP Notification packets: 0
Received EAPOL Start packets : 0
 EAPOL LogOff packets: 0
 EAP Response/Identity packets : 0
 EAP Response/Challenge packets: 0
 Error packets: 0
Online 802.1X users: 0
```

# 当 Host 端输入正确的用户名和密码成功上线后，可使用命令 **display dot1x sessions** 查看到上线用户的连接情况。

## 3.6 配置文件

```
#
dot1x
#
interface Vlan-interface1
 ip address 192.168.100.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x port-method portbased
 dot1x
#
local-user localuser class network
 password cipher c3$YPkufRcxFR3KdpUCHFiNkns/YFPmbJkG/pQxBg==
 service-type lan-access
 authorization-attribute user-role network-operator
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“安全命令参考”

# H3C MSR 系列路由器

## 802.1X 结合 RADIUS 服务器配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                          |   |
|--------------------------|---|
| 1 简介.....                | 1 |
| 2 配置前提.....              | 1 |
| 3 配置举例.....              | 1 |
| 3.1 组网需求.....            | 1 |
| 3.2 使用版本.....            | 1 |
| 3.3 配置注意事项.....          | 2 |
| 3.4 配置步骤.....            | 2 |
| 3.4.1 配置 RADIUS 服务器..... | 2 |
| 3.4.2 Router 的配置.....    | 4 |
| 3.5 验证配置.....            | 5 |
| 3.6 配置文件.....            | 6 |
| 4 相关资料.....              | 7 |

# 1 简介

本文档介绍 MSR 系列路由器 802.1X 通过 RADIUS 服务器进行身份认证对用户实施接入控制的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 AAA 和 802.1X 特性。

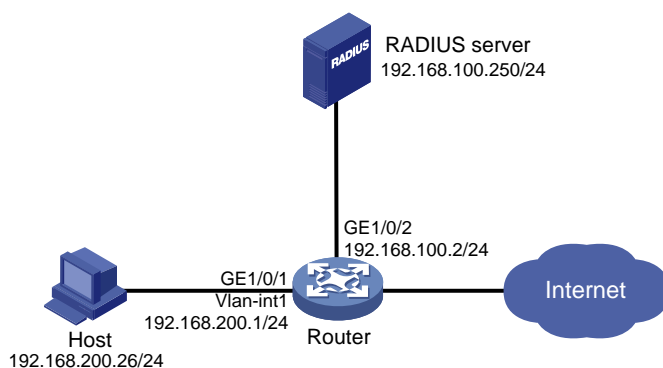
## 3 配置举例

### 3.1 组网需求

如图 1 所示，用户通过 Router 的端口 GigabitEthernet1/0/1 接入网络，iMC 作为 RADIUS 认证服务器，要求通过 RADIUS 服务器对该端口接入的用户进行 802.1X 认证以控制其访问 Internet。具体要求如下：

- Router 向 RADIUS 服务器发送的用户名不携带域名；
- Host 用户认证使用的用户名为 localuser；
- 在 Router 上配置本地认证作为备份认证方式，当 RADIUS 服务器无响应时，采用本地认证；
- 配置基于端口的接入控制方式，并采用强制认证域 bbb 认证 802.1X 用户。

图1 通过 RADIUS 服务器对用户进行 802.1X 认证配置组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置注意事项

- 本例仅在安装了二层交换卡和有固定二层接口的设备上才能实现。
- Router 和 RADIUS 服务器的参数（如共享密钥、认证与计费端口号等）配置要一致。

### 3.4 配置步骤

#### 3.4.1 配置 RADIUS 服务器

##### 1. 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击左侧导航树中的“接入策略管理 > 接入设备管理 > 接入设备配置”菜单项，进入“接入设备配置”页面；在该页面中单击“增加”按钮，进入“增加接入设备”页面。

- (1) 设置认证端口和计费端口分别为“1812”和“1813”；
- (2) 选择接入设备类型为“H3C (General)”；
- (3) 设置与 Device 交互报文时的共享密钥为“name”，并确认该共享密钥；
- (4) 选择或手工增加接入设备，添加 IP 地址为 192.168.100.2 的接入设备。
- (5) 其它参数采用缺省值，单击<确定>按钮完成操作。

图2 增加接入设备

接入配置

|        |               |          |        |
|--------|---------------|----------|--------|
| 认证端口 * | 1812          | 计费端口 *   | 1813   |
| 业务类型   | 不限            | 强制下线方式   | 断开用户连接 |
| 接入设备类型 | H3C (General) | 业务分组     | 未分组    |
| 共享密钥 * | name          | 确认共享密钥 * | name   |
| 接入位置分组 | 无             |          |        |

设备列表

选择 手工增加 增加IPv6设备 全部清除

| 设备名称 | 设备IP地址        | 设备型号 | 备注 | 删除 |
|------|---------------|------|----|----|
|      | 192.168.100.2 |      |    | 删除 |

共有1条记录。

确定 取消

##### # 增加服务配置。

选择“用户”页签，单击导航树中的“接入策略管理 > 接入服务管理”菜单项，进入“接入服务管理”页面，在该页面中单击“增加”按钮，进入“增加接入服务”页面。

- (1) 输入服务名“dot1x auth”；
- (2) 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加服务配置

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 \* dot1x auth 服务后缀

业务分组 \* 未分组 默认接入策略 \* 禁止接入

默认私有属性下发策略 \* 不使用 ?

默认单帐号最大绑定终端数 \* 0 ?

默认单帐号在线数量限制 \* 0 ?

单日累计在线最长时间(分钟) \* 0 ?

服务描述

可申请 ?

MAC Portal认证  无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | 优先级 | 修改 | 删除 |
|-------------|------|----------|-----|----|----|
| 未找到符合条件的记录。 |      |          |     |    |    |

确定 取消

## 2. # 增加接入用户。

选择“用户”页签，单击导航树中的“接入用户管理 > 接入用户”菜单项，进入“接入用户”列表页面，在该页面中单击<增加>按钮，进入“增加接入用户”页面。

- (1) 点击<增加用户>按钮，把接入用户关联到平台用户上。本例假设关联到平台用户 **test** 上；
- (2) 输入账号名“localuser”和密码“localpass”；
- (3) 在接入服务处选择“dot1x auth”；
- (4) 单击<确定>按钮完成操作。

图4 增加接入用户

用户 > 接入用户 > 增加接入用户

接入信息

用户姓名 \* test 选择 增加用户

帐号名 \* localuser ⓘ

预开用户  MAC地址认证用户  主机名用户  快速认证用户

密码 \* ..... 密码确认 \* .....

允许用户修改密码  启用用户密码控制策略  下次登录需修改密码

生效时间 ..... 失效时间 .....

最大闲置时长(分钟) ..... 在线数量限制 1

登录提示信息 .....

接入服务

| 服务名                                            | 服务后缀 | 状态  | 分配IP地址 |
|------------------------------------------------|------|-----|--------|
| <input type="checkbox"/> acl3000               |      | 可申请 |        |
| <input type="checkbox"/> acl3001               |      | 可申请 |        |
| <input type="checkbox"/> acl4000               |      | 可申请 |        |
| <input type="checkbox"/> byod                  |      | 可申请 |        |
| <input type="checkbox"/> DOT1X                 |      | 可申请 |        |
| <input checked="" type="checkbox"/> dot1x auth |      | 可申请 |        |

### 3.4.2 Router 的配置

# 配置虚接口 Vlan-interface1 的 IP 地址。

```
[Router] interface vlan-interface 1
[Router-Vlan-interface1] ip address 192.168.200.1 255.255.255.0
[Router-Vlan-interface1] quit
```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 192.168.100.2 255.255.255.0
[Router-GigabitEthernet1/0/2] quit
```

# 配置本地接入类用户 localuser 和密码。

```
[Router] local-user localuser class network
[Router-luser-network-localuser] password simple localpass
[Router-luser-network-localuser] service-type lan-access
[Router-luser-network-localuser] quit
```

# 创建 RADIUS 方案 radius1。

```
[Router] radius scheme radius1
```

# 配置主认证 RADIUS 服务器的 IP 地址为 192.168.100.250，端口号为 1812,密码为 name。

```
[Router-radius-radius1] primary authentication 192.168.100.250 1812 key simple name
```

# 配置主计费 RADIUS 服务器的 IP 地址为 192.168.100.250，端口号为 1813,密码为 name。

```
[Router-radius-radius1] primary accounting 192.168.100.250 1813 key simple name
```

# 配置发送给 RADIUS 服务器的用户名不携带域名。

```
[Router-radius-radius1] user-name-format without-domain
```

```
[Router-radius-radius1] quit
```

# 配置 ISP 域。

```
[Router] domain bbb
[Router-isp-bbb] authentication lan-access radius-scheme radius1 local
[Router-isp-bbb] authorization lan-access radius-scheme radius1 local
[Router-isp-bbb] accounting lan-access radius-scheme radius1 local
[Router-isp-bbb] quit
```

# 配置端口 GigabitEthernet1/0/1 的 802.1X 功能。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] dot1x
```

# 配置基于端口的接入控制方式（默认为基于 MAC 地址），并采用强制认证域 bbb 认证 802.1X 用户。

```
[Router-GigabitEthernet1/0/1] dot1x port-method portbased
[Router-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
[Router-GigabitEthernet1/0/1] quit
```

# 开启全局 802.1X。

```
<Router> system-view
[Router] dot1x
```

### 3.5 验证配置

# 使用命令 **display dot1x interface** 可以查看端口 GigabitEthernet1/0/1 上的 802.1X 的配置情况。

```
[Router] display dot1x interface gigabitethernet 1/0/1
```

Global 802.1X parameters:

```
802.1X authentication : Enabled
CHAP authentication : Enabled
Max-tx period : 30 s
Handshake period : 15 s
Quiet timer : Disabled
 Quiet period : 60 s
Supp timeout : 30 s
Server timeout : 100 s
Reauth period : 3600 s
Max auth requests : 2
SmartOn supp timeout : 30 s
SmartOn retry counts : 3
EAD assistant function : Disabled
 EAD timeout : 30 min
Domain delimiter : @
```

Online 802.1X wired users : 0

GigabitEthernet1/0/1 is link-up

```
802.1X authentication : Enabled
Handshake : Enabled
Handshake reply : Disabled
Handshake security : Disabled
Unicast trigger : Disabled
Periodic reauth : Disabled
Port role : Authenticator
Authorization mode : Auto
```

```

Port access control : Port-based
Multicast trigger : Enabled
Mandatory auth domain : bbb
Guest VLAN : Not configured
Auth-Fail VLAN : Not configured
Critical VLAN : Not configured
Critical voice VLAN : Disabled
Re-auth server-unreachable : Logoff
Max online users : 4294967295
SmartOn : Disabled

```

```

EAPOL packets: Tx 39, Rx 2
Sent EAP Request/Identity packets : 39
 EAP Request/Challenge packets: 0
 EAP Success packets: 0
 EAP Failure packets: 0
 EAP Notification packets: 0
Received EAPOL Start packets : 1
 EAPOL LogOff packets: 1
 EAP Response/Identity packets : 0
 EAP Response/Challenge packets: 0
 Error packets: 0
Online 802.1X users: 0

```

# 当 802.1X 用户输入正确的用户名和密码成功上线后，可使用命令 **display dot1x sessions** 查看到上线用户的连接情况。

# 断开与 RADIUS 服务器的连接后，用户重新输入用户名和密码进行 802.1X 认证可以成功上线。

## 3.6 配置文件

```

#
dot1x
#
interface Vlan-interface1
 ip address 192.168.200.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.100.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x mandatory-domain bbb
 dot1x port-method portbased
 dot1x
#
radius scheme radius1
 primary authentication 192.168.100.250 key cipher c3$Ua8m/JVT48sS4hXncslGCKRa
VEbAbk

```

```
primary accounting 192.168.100.250 key cipher c3$x0HaZfI2XD6iXBE5E/zTEgEopD8C
eyI=
user-name-format without-domain
#
domain bbb
authentication lan-access radius-scheme radius1 local
authorization lan-access radius-scheme radius1 local
accounting lan-access radius-scheme radius1 local
#
local-user localuser class network
password cipher c3$TFxtbGxKPaxP3LUXfHeUuky7uuaBi9jAmoCnWA==
service-type lan-access
authorization-attribute user-role network-operator
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“安全命令参考”



# H3C MSR 系列路由器

## IPsec 配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                                              |    |
|----------------------------------------------|----|
| 1 简介                                         | 1  |
| 2 配置前提                                       | 1  |
| 3 使用 iNode 客户端基于证书认证的 L2TP over IPsec 功能配置举例 | 1  |
| 3.1 组网需求                                     | 1  |
| 3.2 配置思路                                     | 1  |
| 3.3 使用版本                                     | 1  |
| 3.4 配置步骤                                     | 2  |
| 3.4.1 Device 的配置                             | 2  |
| 3.4.2 Host 的配置                               | 4  |
| 3.5 验证配置                                     | 11 |
| 3.6 配置文件                                     | 15 |
| 4 IPsec over GRE 的典型配置举例                     | 16 |
| 4.1 组网需求                                     | 16 |
| 4.2 配置思路                                     | 16 |
| 4.3 使用版本                                     | 17 |
| 4.4 配置步骤                                     | 17 |
| 4.4.1 Device A 的配置                           | 17 |
| 4.4.2 Device B 的配置                           | 18 |
| 4.5 验证配置                                     | 19 |
| 4.6 配置文件                                     | 21 |
| 5 GRE over IPsec 的典型配置举例                     | 22 |
| 5.1 组网需求                                     | 22 |
| 5.2 配置思路                                     | 23 |
| 5.3 使用版本                                     | 23 |
| 5.4 配置步骤                                     | 23 |
| 5.4.1 Device A 的配置                           | 23 |
| 5.4.2 Device B 的配置                           | 24 |
| 5.5 验证配置                                     | 25 |
| 5.6 配置文件                                     | 27 |
| 6 IPsec 同流双隧道的典型配置举例                         | 29 |
| 6.1 组网需求                                     | 29 |
| 6.2 使用版本                                     | 29 |

|                         |           |
|-------------------------|-----------|
| 6.3 配置步骤.....           | 29        |
| 6.3.1 Device A 的配置..... | 29        |
| 6.3.2 Device B 的配置..... | 30        |
| 6.4 验证配置.....           | 32        |
| 6.5 配置文件.....           | 33        |
| <b>7 相关资料.....</b>      | <b>35</b> |

# 1 简介

本文档介绍 IPsec 的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 IPsec 特性。

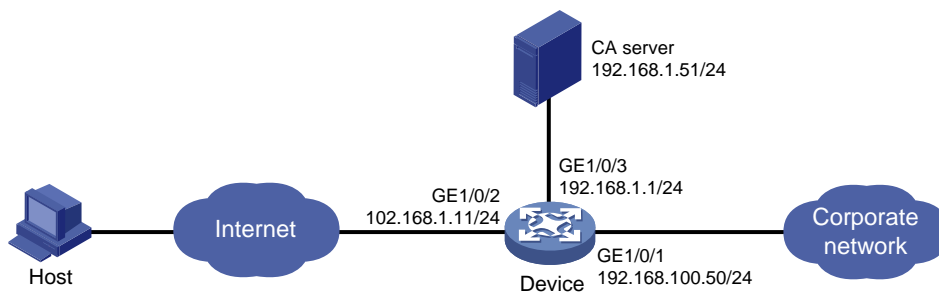
## 3 使用 iNode 客户端基于证书认证的 L2TP over IPsec 功能配置举例

### 3.1 组网需求

如图 1 所示，PPP 用户 Host 与 Device 建立 L2TP 隧道，Windows server 2003 作为 CA 服务器，要求：

- 通过 L2TP 隧道访问 Corporate network。
- 用 IPsec 对 L2TP 隧道进行数据加密。
- 采用 RSA 证书认证方式建立 IPsec 隧道。

图1 基于证书认证的 L2TP over IPsec 配置组网图



### 3.2 配置思路

由于使用证书认证方式建立 IPsec 隧道，所以需要在 ike profile 中配置 local-identity 为 dn，指定从本端证书中的主题字段取得本端身份。

### 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置步骤

### 3.4.1 Device 的配置

(1) 配置各接口 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.100.50 24
[Device-GigabitEthernet1/0/1] quit
```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ip address 102.168.1.11 24
[Device-GigabitEthernet1/0/2] quit
```

# 配置接口 GigabitEthernet1/0/3 的 IP 地址。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] ip address 192.168.1.1 24
[Device-GigabitEthernet1/0/3] quit
```

(2) 配置 L2TP

# 创建本地 PPP 用户 l2tpuser，设置密码为 hello。

```
[Device] local-user l2tpuser class network
[Device-luser-network-l2tpuser] password simple hello
[Device-luser-network-l2tpuser] service-type ppp
[Device-luser-network-l2tpuser] quit
```

# 配置 ISP 域 system 对 PPP 用户采用本地验证。

```
[Device] domain system
[Device-isp-system] authentication ppp local
[Device-isp-system] quit
```

# 启用 L2TP 服务。

```
[Device] l2tp enable
```

# 创建接口 Virtual-Template0，配置接口的 IP 地址为 172.16.0.1/24。

```
[Device] interface virtual-template 0
[Device-Virtual-Template0] ip address 172.16.0.1 255.255.255.0
```

# 配置 PPP 认证方式为 PAP。

```
[Device-Virtual-Template0] ppp authentication-mode pap
```

# 配置为 PPP 用户分配的 IP 地址为 172.16.0.2。

```
[Device-Virtual-Template0] remote address 172.16.0.2
[Device-Virtual-Template0] quit
```

# 创建 LNS 模式的 L2TP 组 1。

```
[Device] l2tp-group 1 mode lns
```

# 配置 LNS 侧本端名称为 lns。

```
[Device-l2tp1] tunnel name lns
```

# 关闭 L2TP 隧道验证功能。

```
[Device-l2tp1] undo tunnel authentication
```

# 指定接收呼叫的虚拟模板接口为 VT0。

```
[Device-l2tp1] allow l2tp virtual-template 0
[Device-l2tp1] quit
```

### (3) 配置 PKI 证书

# 配置 PKI 实体 security。

```
[Device] pki entity security
[Device-pki-entity-security] common-name device
[Device-pki-entity-security] quit
```

# 新建 PKI 域。

```
[Device] pki domain headgate
[Device-pki-domain-headgate] ca identifier LYQ
[Device-pki-domain-headgate] certificate request url
http://192.168.1.51/certsrv/mscep/mscep.dll
[Device-pki-domain-headgate] certificate request from ra
[Device-pki-domain-headgate] certificate request entity security
[Device-pki-domain-headgate] undo crl check enable
[Device-pki-domain-headgate] public-key rsa general name abc length 1024
[Device-pki-domain-headgate] quit
```

# 生成 RSA 算法的本地密钥对。

```
[Device] public-key local create rsa name abc
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

```
.....+++++
.+++++
```

Create the key pair successfully.

# 获取 CA 证书并下载至本地。

```
[Device] pki retrieve-certificate domain headgate ca
The trusted CA's finger print is:
 MD5 fingerprint:8649 7A4B EAD5 42CF 5031 4C99 BFS3 2A99
 SHA1 fingerprint:61A9 6034 181E 6502 12FA 5A5F BA12 0EAO 5187 031C
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully.
```

# 手工申请本地证书。

```
[Device] pki request-certificate domain headgate
Start to request general certificate ...
Certificate requested successfully.
```

### (4) 配置 IPsec 隧道

# 创建 IKE 安全提议。

```
[Device] ike proposal 1
[Device-ike-proposal-1] authentication-method rsa-signature
[Device-ike-proposal-1] encryption-algorithm 3des-cbc
[Device-ike-proposal-1] dh group2
[Device-ike-proposal-1] quit
```

```

配置 IPsec 安全提议。
[Device] ipsec transform-set tran1
[Device-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[Device-ipsec-transform-set-tran1] esp encryption-algorithm 3des
[Device-ipsec-transform-set-tran1] quit
配置 IKE profile。
[Device] ike profile profile1
[Device-ike-profile-profile1] local-identity dn
[Device-ike-profile-profile1] certificate domain headgate
[Device-ike-profile-profile1] proposal 1
[Device-ike-profile-profile1] match remote certificate device
[Device-ike-profile-profile1] quit
在采用数字签名认证时，指定总从本端证书中的主题字段取得本端身份。
[Device] ike signature-identity from-certificate
创建一条 IPsec 安全策略模板，名称为 template1，序列号为 1。
[Device] ipsec policy-template template1 1
[Device-ipsec-policy-template-template1-1] transform-set tran1
[Device-ipsec-policy-template-template1-1] ike-profile profile1
[Device-ipsec-policy-template-template1-1] quit
引用 IPsec 安全策略模板创建一条 IPsec 安全策略，名称为 policy1，顺序号为 1。
[Device] ipsec policy policy1 1 isakmp template template1
在接口上应用 IPsec 安全策略。
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ipsec apply policy policy1
[Device-GigabitEthernet1/0/2] quit

```

### 3.4.2 Host 的配置

(1) 从证书服务器上申请客户端证书

# 登录到证书服务器：<http://192.168.1.51/certsrv>，点击“申请一个证书”。

图2 进入申请证书页面

**欢迎**

使用此网站为您的 Web 浏览器，电子邮件客户端或其他程序申请一个证书。通过使用证书，您可以向通过 Web 通信的人确认您的身份，签署并加密邮件，并且，根据您申请的证书的类型，执行其他安全任务。

您也可以使用此网站下载证书颁发机构(CA)证书，证书链，或证书吊销列表(CRL)，或查看挂起的申请的状态。

有关证书服务的详细信息，请参阅[证书服务文档](#)。

**选择一个任务：**

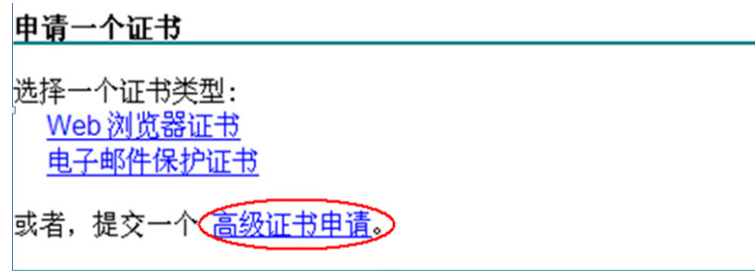
[申请一个证书](#)

[查看挂起的证书申请的状态](#)

[下载一个 CA 证书，证书链或 CRL](#)

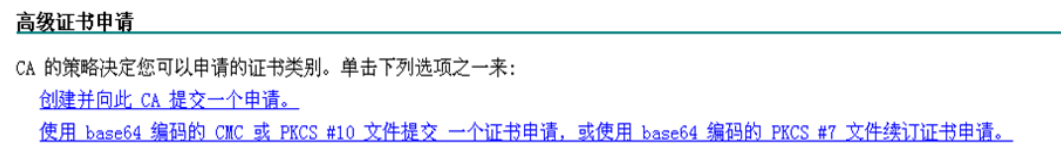
# 点击“高级证书申请”。

图3 高级证书申请



# 选择第一项：创建并向此 CA 提交一个申请。

图4 创建并向 CA 提交一个申请



# 填写相关信息。

- 需要的证书类型，选择“客户端身份验证证书”；
- 密钥选项的配置，勾选“标记密钥为可导出”前的复选框。

# 点击<提交>，弹出一提示框：在对话框中选择“是”。

# 点击安装此证书。

图5 安装证书



(2) iNode 客户端的配置（使用 iNode 版本为：iNode PC 5.2(E0409)）

# 打开 L2TP VPN 连接，并单击“属性...(Y)”。

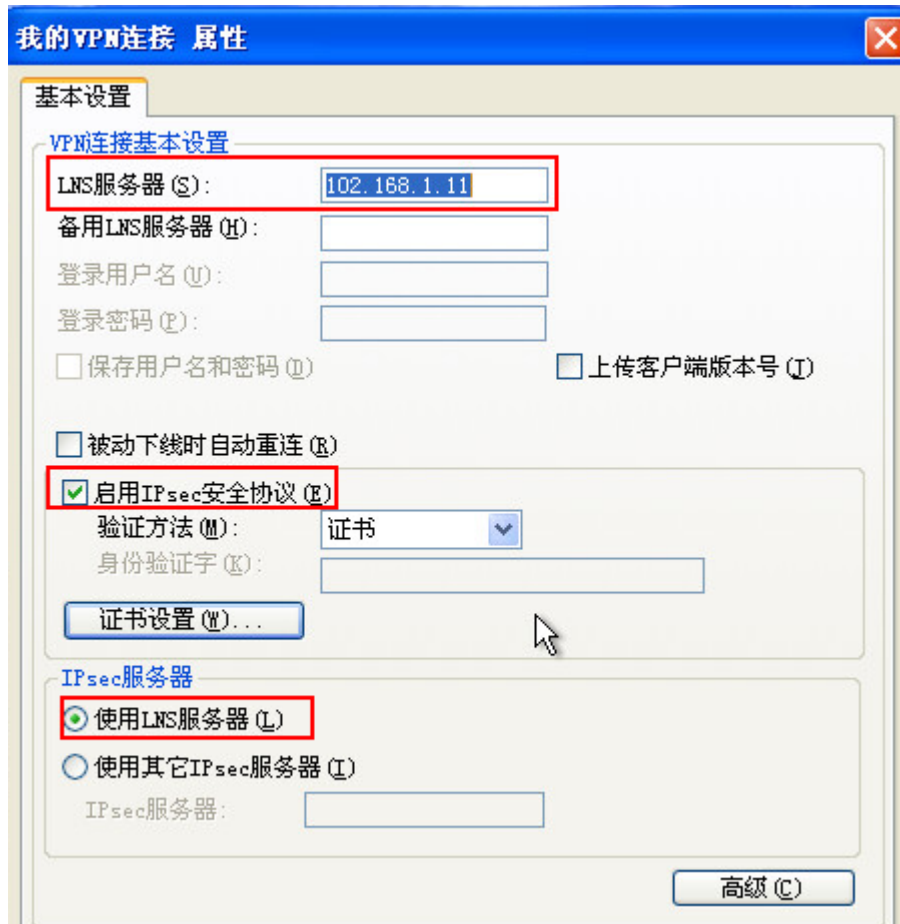


图6 打开 L2TP 连接



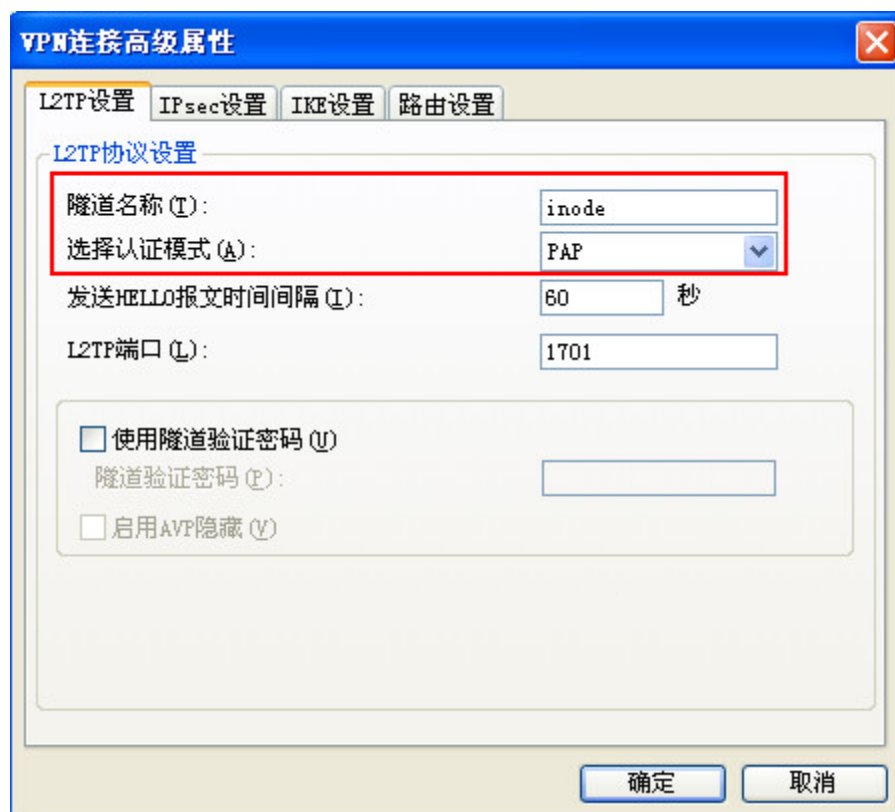
# 输入 LNS 服务器的地址，并启用 IPsec 安全协议，验证证方法选择证书认证。

图7 基本配置



# 单击<高级(C)>按钮，进入“L2TP 设置”页签，设置 L2TP 参数如下图所示。

图8 L2TP 设置



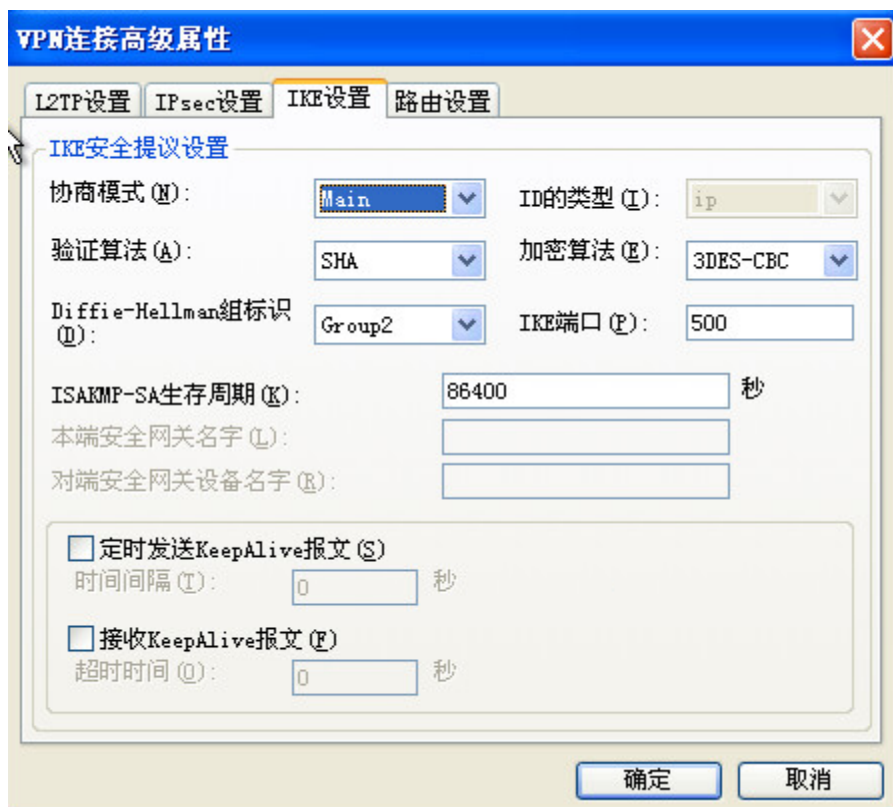
# 单击“IPsec 设置”页签，配置 IPsec 参数。

图9 IPsec 参数设置



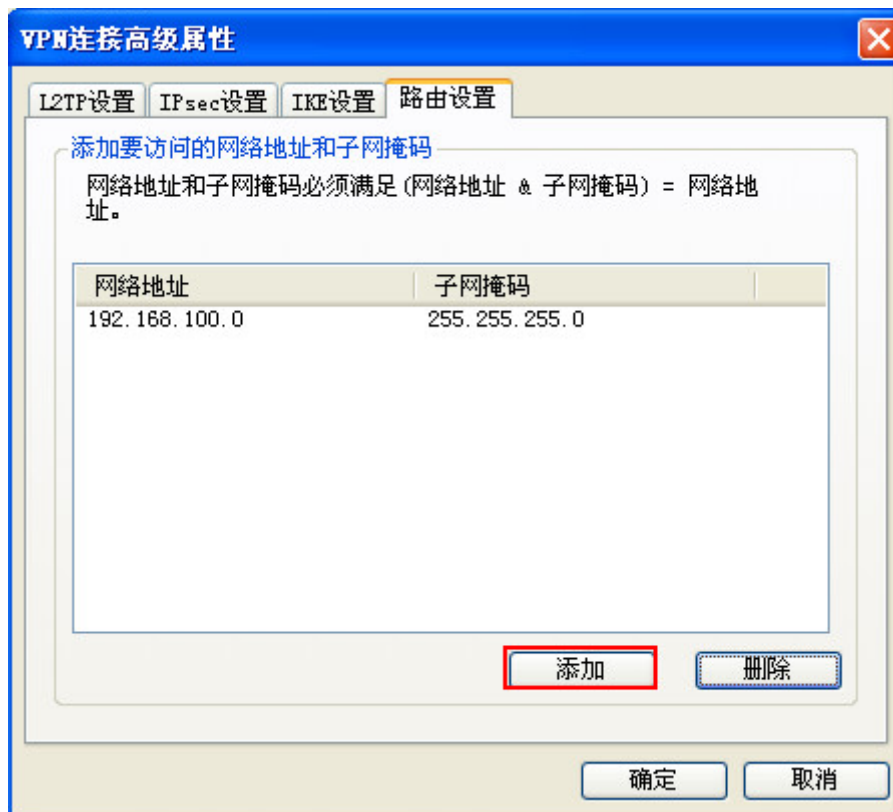
# 单击“IKE 设置”页签，配置 IKE 参数。

图10 IKE 参数设置



# 单击“路由设置”页签，添加访问 Corporate network 的路由。

图11 路由设置



# 完成上述配置后，单击<确定>按钮，回到 L2TP 连接页面。

### 3.5 验证配置

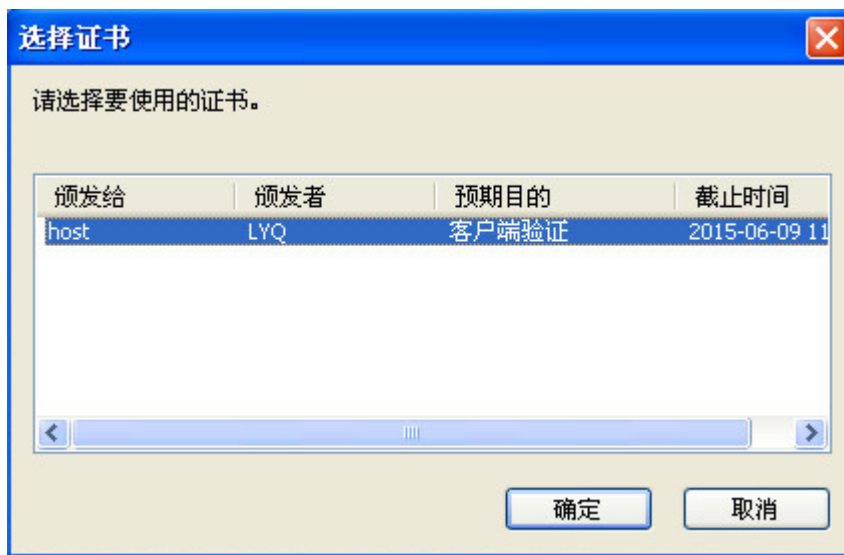
# 在 L2TP 连接对话框中，输入用户名“l2tpuser”和密码“hello”，单击<连接>按钮。

图12 连接 L2TP



# 在弹出的对话框中选择申请好的证书，单击<确定>按钮。

图13 证书选择



# 通过下图可以看到 L2TP 连接成功。

图14 连接成功



图15 连接成功





# 在 Device 上使用 **display ike sa** 命令，可以看到 IPsec 隧道第一阶段的 SA 正常建立。

```
<Device> display ike sa
 Connection-ID Remote Flag DOI

 10 102.168.1.1 RD IPSEC
```

```
Flags:
RD--READY RL--REPLACED FD-FADING
```

# 在 Device 上使用 **display ipsec sa** 命令可以看到 IPsec SA 的建立情况。

```
<Device> display ipsec sa

Interface: GigabitEthernet1/0/2

IPsec policy: policy1
Sequence number: 1
Mode: template

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1443
Tunnel:
 local address: 102.168.1.11
 remote address: 102.168.1.1
Flow:
sour addr: 102.168.1.11/255.255.255.255 port: 1701 protocol: udp
dest addr: 102.168.1.1/255.255.255.255 port: 0 protocol: udp

[Inbound ESP SAs]
SPI: 2187699078 (0x8265a386)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843197/3294
Max received sequence-number: 51
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 3433374591 (0xcca5237f)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843197/3294
Max sent sequence-number: 52
UDP encapsulation used for NAT traversal: N
Status: Active
```

## 3.6 配置文件

```
#
interface Virtual-Template0
 ppp authentication-mode pap
 remote address 172.16.0.2
 ip address 172.16.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 ip address 192.168.100.50 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 102.168.1.11 255.255.255.0
 ipsec apply policy policy1
#
interface GigabitEthernet1/0/3
 ip address 192.168.1.1 255.255.255.0
#
domain system
 authentication ppp local
#
local-user l2tpuser class network
 password cipher c3$nl46fURLtkCkcbdnB6irTXma+E6u0c+h
 service-type ppp
 authorization-attribute user-role network-operator
#
pki domain headgate
 ca identifier LYQ
 certificate request url http://192.168.1.51/certsrv/mscep/mscep.dll
 certificate request from ra
 certificate request entity security
 public-key rsa general name abc
 undo crl check enable
#
pki entity security
 common-name host
#
ipsec transform-set tran1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template template1 1
 transform-set tran1
 ike-profile profile1
#
ipsec policy policy1 1 isakmp template template1
#
l2tp-group 1 mode lns
```

```

allow l2tp virtual-template 0
undo tunnel authentication
tunnel name lns
#
l2tp enable
#
ike signature-identity from-certificate
#
ike profile profile1
certificate domain headgate
local-identity dn
match remote certificate device
proposal 1
#
ike proposal 1
authentication-method rsa-signature
encryption-algorithm 3des-cbc
dh group2
#

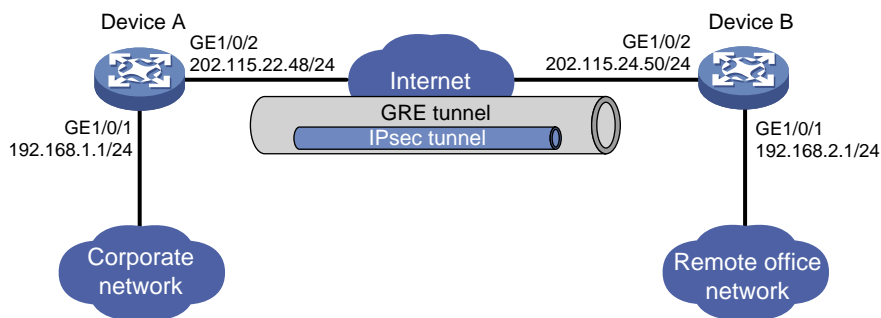
```

## 4 IPsec over GRE 的典型配置举例

### 4.1 组网需求

如图 16 所示，企业远程办公网络通过 IPsec VPN 接入企业总部，要求：通过 GRE 隧道传输两网络之间的 IPsec 加密数据。

图16 IPsec over GRE 组网图



### 4.2 配置思路

- 为了对数据先进行 IPsec 处理，再进行 GRE 封装，访问控制列表需匹配数据的原始范围，并且要将 IPsec 应用到 GRE 隧道接口上。
- 为了对网络间传输的数据先进行 IPsec 封装，再进行 GRE 封装，需要配置 IPsec 隧道的对端 IP 地址为 GRE 隧道的接口地址。

## 4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.4 配置步骤

### 4.4.1 Device A 的配置

#### (1) 配置各接口 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] tcp mss 1350
[DeviceA-GigabitEthernet1/0/1] quit
```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 202.115.22.48 255.255.255.0
[DeviceA-GigabitEthernet1/0/2] quit
```

#### (2) 配置 GRE 隧道

# 创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 0 mode gre
```

# 配置 Tunnel0 接口的 IP 地址为 10.1.1.1/24。

```
[DeviceA-Tunnel0] ip address 10.1.1.1 255.255.255.0
```

# 配置 Tunnel0 接口的源端地址为 202.115.22.48/24 (Device A 的 GigabitEthernet1/0/2 的 IP 地址)。

```
[DeviceA-Tunnel0] source 202.115.22.48
```

# 配置 Tunnel0 接口的目的端地址为 202.115.24.50/24 (Device B 的 GigabitEthernet1/0/2 的 IP 地址)。

```
[DeviceA-Tunnel0] destination 202.115.24.50
```

```
[DeviceA-Tunnel0] quit
```

# 配置从 Device A 经过 Tunnel0 接口到 Remote office network 的静态路由。

```
[DeviceA] ip route-static 192.168.2.1 255.255.255.0 tunnel 0
```

#### (3) 配置 IPsec VPN

# 配置 IKE keychain。

```
[DeviceA] ike keychain keychain1
[DeviceA-ike-keychain-keychain1] pre-shared-key address 10.1.1.2 255.255.255.0 key
simple 123
[DeviceA-ike-keychain-keychain1] quit
```

# 创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[DeviceA] acl number 3000
[DeviceA-acl-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
192.168.2.0 0.0.0.255
[DeviceA-acl-adv-3000] quit
```

# 配置 IPsec 安全提议。

```

[DeviceA] ipsec transform-set tran1
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。
[DeviceA] ipsec policy policy1 1 isakmp
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 10.1.1.2
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
在 GRE 隧道接口上应用安全策略。
[DeviceA] interface tunnel 0
[DeviceA-Tunnel0] ipsec apply policy policy1
[DeviceA-Tunnel0] quit

```

#### 4.4.2 Device B 的配置

##### (1) 配置各接口 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```

<DevoceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 192.168.2.1 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] tcp mss 1350
[DeviceB-GigabitEthernet1/0/1] quit

```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```

[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 202.115.24.50 255.255.255.0
[DeviceB-GigabitEthernet1/0/2] quit

```

##### (2) 配置 GRE 隧道

# 创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```

[DeviceB] interface tunnel 0 mode gre

```

# 配置 Tunnel0 接口的 IP 地址为 10.1.1.2/24。

```

[DeviceB-Tunnel0] ip address 10.1.1.2 255.255.255.0

```

# 配置 Tunnel0 接口的源端地址为 202.115.24.50/24 (Device B 的 GigabitEthernet1/0/2 的 IP 地址)。

```

[DeviceB-Tunnel0] source 202.115.24.50

```

# 配置 Tunnel0 接口的目的端地址为 202.115.22.48/24 (Device A 的 GigabitEthernet1/0/2 的 IP 地址)。

```

[DeviceB-Tunnel0] destination 202.115.22.48

```

```

[DeviceB-Tunnel0] quit

```

# 配置从 DeviceB 经过 Tunnel0 接口到 Corporate network 的静态路由。

```

[DeviceB] ip route-static 192.168.1.1 255.255.255.0 tunnel 0

```

##### (3) 配置 IPsec VPN

# 配置 IKE keychain。

```

[DeviceB] ike keychain keychain1

```

```

[DeviceB-ike-keychain-keychain1] pre-shared-key address 10.1.1.1 255.255.255.0 key
simple 123
[DeviceB-ike-keychain-keychain1] quit
创建 ACL3000, 定义需要 IPsec 保护的数据流。
[DeviceB] acl number 3000
[DeviceB-acl-adv-3000] rule 0 permit ip source 192.168.2.0 0.0.0.255 destination
192.168.1.0 0.0.0.255
[DeviceB-acl-adv-3000] quit
配置 IPsec 安全提议。
[DeviceB] ipsec transform-set tran1
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
创建一条 IKE 协商方式的 IPsec 安全策略, 名称为 policy1, 序列号为 1。
[DeviceB] ipsec policy policy1 1 isakmp
[DeviceB-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-policy1-1] remote-address 10.1.1.1
[DeviceB-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceB-ipsec-policy-isakmp-policy1-1] quit
在 GRE 隧道接口上应用安全策略。
[DeviceB] interface tunnel 0
[DeviceB-Tunnel0] ipsec apply policy policy1
[DeviceB-Tunnel0] quit

```

## 4.5 验证配置

# 以 Corporate network 的主机 192.168.1.2 向 Remote office network 的主机 192.168.2.2 发起通信为例, 从 192.168.1.2 ping 192.168.2.2, 会触发 IPsec 协商, 建立 IPsec 隧道, 在成功建立 IPsec 隧道后, 可以 ping 通。

```
C:\Users\corporatenetwork> ping 192.168.2.2
```

```
Pinging 192.168.2.2 with 32 bytes of data:
```

```
Request timed out.
```

```
Reply from 192.168.2.2: bytes=32 time=2ms TTL=254
```

```
Reply from 192.168.2.2: bytes=32 time=2ms TTL=254
```

```
Reply from 192.168.2.2: bytes=32 time=1ms TTL=254
```

```
Ping statistics for 192.168.2.2:
```

```
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

# 在 Device A 上使用 **display ike sa** 命令, 可以看到第一阶段的 SA 正常建立。

```
<DeviceA> display ike sa
```

| Connection-ID | Remote   | Flag | DOI   |
|---------------|----------|------|-------|
| 1             | 10.1.1.2 | RD   | IPSEC |

```
Flags:
```

RD--READY RL--REPLACED FD-FADING

# 在 Device A 上使用 **display ipsec sa** 命令可以看到 IPsec SA 的建立情况。

```
<DeviceA> display ipsec sa
```

```

Interface: Tunnel0

```

```

IPsec policy: policy1
```

```
Sequence number: 1
```

```
Mode: isakmp

```

```
Tunnel id: 0
```

```
Encapsulation mode: tunnel
```

```
Perfect forward secrecy:
```

```
Path MTU: 1419
```

```
Tunnel:
```

```
 local address: 10.1.1.1
```

```
 remote address: 10.1.1.2
```

```
Flow:
```

```
sour addr: 192.168.1.1/255.255.255.255 port: 0 protocol: ip
```

```
dest addr: 192.168.2.1/255.255.255.255 port: 0 protocol: ip
```

```
[Inbound ESP SAs]
```

```
 SPI: 3128557135 (0xba79fe4f)
```

```
 Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
```

```
 SA duration (kilobytes/sec): 1843200/3600
```

```
 SA remaining duration (kilobytes/sec): 1843199/3550
```

```
 Max received sequence-number: 3
```

```
 Anti-replay check enable: Y
```

```
 Anti-replay window size: 64
```

```
 UDP encapsulation used for NAT traversal: N
```

```
 Status: Active
```

```
[Outbound ESP SAs]
```

```
 SPI: 2643166978 (0x9d8b8702)
```

```
 Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
```

```
 SA duration (kilobytes/sec): 1843200/3600
```

```
 SA remaining duration (kilobytes/sec): 1843199/3550
```

```
 Max sent sequence-number: 3
```

```
 UDP encapsulation used for NAT traversal: N
```

```
 Status: Active
```

# 在 Device A 上通过命令 **display interface tunnel 0** 可以查看经过 GRE 隧道传输的流量情况。

```
<DeviceA> display interface tunnel 0
```

```
Tunnel0
```

```
Current state: UP
```

```
Line protocol state: UP
```

```
Description: Tunnel0 Interface
```

```

Bandwidth: 64kbps
Maximum Transmit Unit: 1476
Internet Address is 10.1.1.1/24 Primary
Tunnel source 202.115.22.48, destination 202.115.24.50
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
 GRE key disabled
 Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 40 packets, 3300 bytes, 0 drops
Output: 41 packets, 3464 bytes, 0 drops

```

# 从 Remote office network 的主机向 Corporate network 的主机发起通信验证方法相同,此不赘述。

## 4.6 配置文件

- Device A:

```

#
interface GigabitEthernet1/0/1
 ip address 192.168.1.1 255.255.255.0
 tcp mss 1350
#
interface GigabitEthernet1/0/2
 ip address 202.115.22.48 255.255.255.0
#
interface Tunnel0 mode gre
 ip address 10.1.1.1 255.255.255.0
 source 202.115.22.48
 destination 202.115.24.50
 ipsec apply policy policy1
#
ip route-static 192.168.2.0 24 Tunnel0
#
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000

```



```

 remote-address 10.1.1.2
#
 ike keychain keychain1
 pre-shared-key address 10.1.1.2 255.255.255.0 key cipher
 c3$n6jdlYtuR+K6mijQ8qp4hMMjV/iteA==
#
• Devoce B
#
interface GigabitEthernet1/0/1
 ip address 192.168.2.1 255.255.255.0
 tcp mss 1350
#
interface GigabitEthernet1/0/2
 ip address 202.115.22.50 255.255.255.0
#
interface Tunnel0 mode gre
 ip address 10.1.1.2 255.255.255.0
 source 202.115.24.50
 destination 202.115.22.48
 ipsec apply policy policy1
#
ip route-static 192.168.1.1 24 Tunnel0
#
acl number 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
 remote-address 10.1.1.1
#
 ike keychain keychain1
 pre-shared-key address 10.1.1.1 255.255.255.0 key cipher
 c3$n6jdlYtuR+K6mijQ8qp4hMMjV/iteA==
#

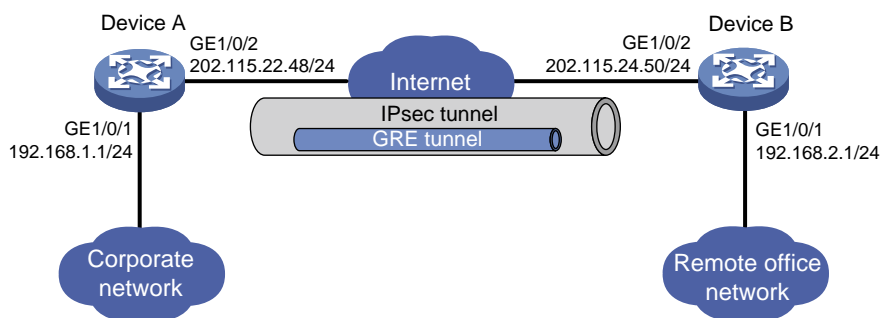
```

## 5 GRE over IPsec 的典型配置举例

### 5.1 组网需求

如图 17 所示，企业远程办公网络通过 GRE 隧道与企业总部传输数据，要求：对通过 GRE 隧道的数据进行 IPsec 加密处理。

图17 GRE over IPsec 组网图



## 5.2 配置思路

- 为了对经 GRE 封装的数据进行 IPsec 加密，将 IPsec 策略应用在物理接口上，访问控制列表源和目的地址为物理接口地址。
- 为了使 IPsec 保护整个 GRE 隧道，应用 IPsec 策略的接口和 GRE 隧道源、目的接口必须是同一接口。

## 5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 5.4 配置步骤

### 5.4.1 Device A 的配置

#### (1) 配置各接口 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 202.115.22.48 255.255.255.0
[DeviceA-GigabitEthernet1/0/2] quit
```

#### (2) 配置 GRE 隧道

# 创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 0 mode gre
配置 Tunnel0 接口的 IP 地址为 10.1.1.1/24。
[DeviceA-Tunnel0] ip address 10.1.1.1 255.255.255.0
```

# 配置 Tunnel0 接口的源端地址为 202.115.22.48/24 (Device A 的 GigabitEthernet1/0/2 的 IP 地址)。

```
[DeviceA-Tunnel0] source 202.115.22.48
```

# 配置 Tunnel0 接口的目的端地址为 202.115.24.50/24 (Device B 的 GigabitEthernet1/0/2 的 IP 地址)。

```
[DeviceA-Tunnel0] destination 202.115.24.50
```

```
[DeviceA-Tunnel0] quit
```

# 配置从 Device A 经过 Tunnel0 接口到 Remote office network 的静态路由。

```
[DeviceA] ip route-static 192.168.2.1 255.255.255.0 tunnel 0
```

### (3) 配置 IPsec VPN

# 配置 IKE keychain。

```
[DeviceA] ike keychain keychain1
```

```
[DeviceA-ike-keychain-keychain1] pre-shared-key address 202.115.24.50 255.255.255.0
key simple 123
```

```
[DeviceA-ike-keychain-keychain1] quit
```

# 创建 ACL3000, 定义需要 IPsec 保护的数据流。

```
[DeviceA] acl number 3000
```

```
[DeviceA-acl-adv-3000] rule 0 permit gre source 202.115.22.48 0 destination
202.115.24.50 0
```

```
[DeviceA-acl-adv-3000] quit
```

# 配置 IPsec 安全提议。

```
[DeviceA] ipsec transform-set tran1
```

```
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des
```

```
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[DeviceA-ipsec-transform-set-tran1] quit
```

# 创建一条 IKE 协商方式的 IPsec 安全策略, 名称为 policy1, 序列号为 1。

```
[DeviceA] ipsec policy policy1 1 isakmp
```

```
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
```

```
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 202.115.24.50
```

```
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set tran1
```

```
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
```

# 在接口 GigabitEthernet1/0/2 上应用安全策略。

```
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] ipsec apply policy policy1
```

```
[DeviceA-GigabitEthernet1/0/2] quit
```

## 5.4.2 Device B 的配置

### (1) 配置各接口 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceB> system-view
```

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] ip address 192.168.2.1 255.255.255.0
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] ip address 202.115.24.50 255.255.255.0
```

```
[DeviceB-GigabitEthernet1/0/2] quit
```

### (2) 配置 GRE 隧道

```

创建 Tunnel0 接口，并指定隧道模式为 GRE over IPv4 隧道。
[DeviceB] interface tunnel 0 mode gre
配置 Tunnel0 接口的 IP 地址为 10.1.1.2/24。
[DeviceB-Tunnel0] ip address 10.1.1.2 255.255.255.0
配置 Tunnel0 接口的源端地址为 202.115.24.50/24 (Device B 的 GigabitEthernet1/0/2 的 IP 地址)。
[DeviceB-Tunnel0] source 202.115.24.50
配置 Tunnel0 接口的目的端地址为 202.115.22.48/24 (Device A 的 GigabitEthernet1/0/2 的 IP 地址)。
[DeviceB-Tunnel0] destination 202.115.22.48
[DeviceB-Tunnel0] quit
配置从 DeviceB 经过 Tunnel0 接口到 Corporate network 的静态路由。
[DeviceB] ip route-static 192.168.1.1 255.255.255.0 tunnel 0

```

### (3) 配置 IPsec VPN

```

配置 IKE keychain。
[DeviceB] ike keychain keychain1
[DeviceB-ike-keychain-keychain1] pre-shared-key address 202.115.22.48 255.255.255.0
key simple 123
[DeviceB-ike-keychain-keychain1] quit
创建 ACL3000，定义需要 IPsec 保护的数据流。
[DeviceB] acl number 3000
[DeviceB-acl-adv-3000] rule 0 permit gre source 202.115.24.50 0 destination
202.115.22.48 0
[DeviceB-acl-adv-3000] quit
配置 IPsec 安全提议。
[DeviceB] ipsec transform-set tran1
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。
[DeviceB] ipsec policy policy1 1 isakmp
[DeviceB-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-policy1-1] remote-address 202.115.22.48
[DeviceB-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceB-ipsec-policy-isakmp-policy1-1] quit
在接口 GigabitEthernet1/0/2 上应用安全策略。
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ipsec apply policy policy1
[DeviceB-GigabitEthernet1/0/2] quit

```

## 5.5 验证配置

# 以 Corporate network 的主机 192.168.1.2 向 Remote office network 的主机 192.168.2.2 发起通信为例，从 192.168.1.2 ping 192.168.2.2，会触发 IPsec 协商，建立 IPsec 隧道，在成功建立 IPsec 隧道后，可以 ping 通。

```
C:\Users\corporatenetwork> ping 192.168.2.2
```

```
Pinging 192.168.2.2 with 32 bytes of data:
```

```
Request timed out.
```

```
Reply from 192.168.2.2: bytes=32 time=2ms TTL=254
```

```
Reply from 192.168.2.2: bytes=32 time=2ms TTL=254
```

```
Reply from 192.168.2.2: bytes=32 time=1ms TTL=254
```

```
Ping statistics for 192.168.2.2:
```

```
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

# 在 Device A 上使用 **display ike sa** 命令，可以看到第一阶段的 SA 正常建立。

```
<DeviceA> display ike sa
```

| Connection-ID | Remote        | Flag | DOI   |
|---------------|---------------|------|-------|
| 2             | 202.115.22.49 | RD   | IPSEC |

```
Flags:
```

```
RD--READY RL--REPLACED FD-FADING
```

# 在 Device A 上使用 **display ipsec sa** 命令可以看到 IPsec SA 的建立情况。

```
<DeviceA> display ipsec sa
```

```
Interface: GigabitEthernet1/0/2
```

```
IPsec policy: policy1
```

```
Sequence number: 1
```

```
Mode: isakmp
```

```
Tunnel id: 0
```

```
Encapsulation mode: tunnel
```

```
Perfect forward secrecy:
```

```
Path MTU: 1443
```

```
Tunnel:
```

```
 local address: 202.115.22.48
```

```
 remote address: 202.115.24.50
```

```
Flow:
```

```
sour addr: 202.115.22.48/255.255.255.255 port: 0 protocol: gre
```

```
dest addr: 202.115.24.50/255.255.255.255 port: 0 protocol: gre
```

```
[Inbound ESP SAs]
```

```
 SPI: 2130348402 (0x7efa8972)
```

```
 Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
```

```
 SA duration (kilobytes/sec): 1843200/3600
```

```
 SA remaining duration (kilobytes/sec): 1843199/3573
```

```
 Max received sequence-number: 3
```

```
 Anti-replay check enable: Y
```

```
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active
```

```
[Outbound ESP SAs]
```

```
SPI: 2811839266 (0xa7994322)
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3573
Max sent sequence-number: 3
UDP encapsulation used for NAT traversal: N
Status: Active
```

# 在 Device A 上通过命令 **display interface tunnel 0** 可以查看经过 GRE 隧道传输的流量情况。

```
<DeviceA> display interface tunnel 0
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1476
Internet Address is 10.1.1.1/24 Primary
Tunnel source 202.115.22.48, destination 202.115.24.50
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
GRE key disabled
Checksumming of GRE packets disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 43 packets, 3480 bytes, 0 drops
Output: 45 packets, 3740 bytes, 2 drops
```

# 从 Remote office network 的主机向 Corporate network 的主机发起通信验证方法相同,此不赘述。

## 5.6 配置文件

- Device A:

```
#
interface GigabitEthernet1/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 202.115.22.48 255.255.255.0
ipsec apply policy policy1
```

```

#
interface Tunnel0 mode gre
 ip address 10.1.1.1 255.255.255.0
 source 202.115.22.48
 destination 202.115.24.50
#
ip route-static 192.168.2.0 24 Tunnel0
#
acl number 3000
 rule 0 permit gre source 202.115.22.48 0 destination 202.115.24.50 0
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
 remote-address 202.115.24.50
#
ike keychain keychain1
 pre-shared-key address 202.115.24.50 255.255.255.0 key cipher c3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#

```

- **Devoce B:**

```

#
interface GigabitEthernet1/0/1
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 202.115.24.50 255.255.255.0
 ipsec apply policy policy1
#
interface Tunnel0 mode gre
 ip address 10.1.1.2 255.255.255.0
 source 202.115.24.50
 destination 202.115.22.48
#
ip route-static 192.168.1.1 24 Tunnel0
#
acl number 3000
 rule 0 permit ip source 202.115.24.50 0 destination 202.115.22.48 0
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp

```

```

transform-set tran1
security acl 3000
remote-address 202.115.22.48
#
ike keychain keychain1
pre-shared-key address 202.115.22.48 255.255.255.0 key cipher c3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#

```

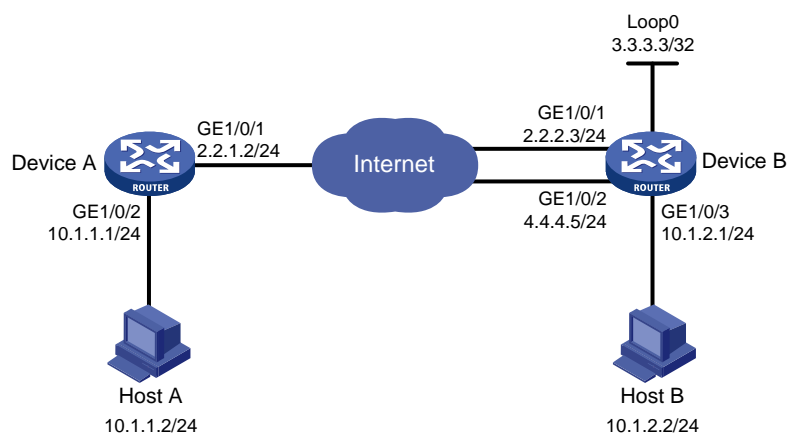
## 6 IPsec 同流双隧道的典型配置举例

### 6.1 组网需求

如图 18 所示组网，要求：

- 在 Device A 和 Device B 之间建立 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。
- Device B 上通过两条链路接入互联网，在这两条链路上配置相同的 IPsec 隧道形成备份。
- 使用 IKE 自动协商方式建立 SA，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96。
- 在 Device B 上配置共享源接口安全策略，实现数据流量在不同接口间平滑切换。

图18 IPsec 同流双隧道组网图



### 6.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 6.3 配置步骤

#### 6.3.1 Device A 的配置

- (1) 配置各接口 IP 地址



# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 2.2.1.2 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 10.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/2] quit
```

# 配置访问 10.1.2.0 网段的静态路由。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.3
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 4.4.4.5
```

# 配置到 Device B 上 Loopback0 接口的静态路由。

```
[DeviceA] ip route-static 3.3.3.3 255.255.255.255 2.2.2.3
[DeviceA] ip route-static 3.3.3.3 255.255.255.255 4.4.4.5
```

## (2) 配置 IPsec VPN

# 配置 IKE keychain。

```
[DeviceA] ike keychain keychain1
[DeviceA-ike-keychain-keychain1] pre-shared-key address 3.3.3.3 255.255.255.255 key
simple 123
[DeviceA-ike-keychain-keychain1] quit
```

# 创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[DeviceA] acl number 3000
[DeviceA-acl-adv-3000] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[DeviceA-acl-adv-3000] quit
```

# 配置 IPsec 安全提议。

```
[DeviceA] ipsec transform-set tran1
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
```

# 创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```
[DeviceA] ipsec policy policy1 1 isakmp
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 3.3.3.3
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
```

# 在接口 GigabitEthernet1/0/1 上应用安全策略。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy policy1
[DeviceA-GigabitEthernet1/0/1] quit
```

## 6.3.2 Device B 的配置

### (1) 配置各接口 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```

<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 2.2.2.3 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
配置接口 GigabitEthernet1/0/2 的 IP 地址。
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 4.4.4.5 255.255.255.0
[DeviceB-GigabitEthernet1/0/2] quit
配置接口 GigabitEthernet1/0/3 的 IP 地址。
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] ip address 10.1.2.1 255.255.255.0
[DeviceB-GigabitEthernet1/0/3] quit
配置接口 Loopback 0 的 IP 地址。
[DeviceB] interface loopback 0
[DeviceB-LoopBack0] ip address 3.3.3.3 255.255.255.0
[DeviceB-LoopBack0] quit
配置访问 10.1.1.0 网段的静态路由。
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 1/0/1 2.2.1.2
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 1/0/2 2.2.1.2

```

## (2) 配置 IPsec VPN

# 配置 IKE keychain。

```

[DeviceB] ike keychain keychain1
[DeviceB-ike-keychain-keychain1] pre-shared-key address 2.2.1.2 255.255.255.0 key
simple 123
[DeviceB-ike-keychain-keychain1] quit

```

# 创建 ACL3000，定义需要 IPsec 保护的数据流。

```

[DeviceB] acl number 3000
[DeviceB-acl-adv-3000] rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[DeviceB-acl-adv-3000] quit

```

# 配置 IPsec 安全提议。

```

[DeviceB] ipsec transform-set tran1
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit

```

# 创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，序列号为 1。

```

[DeviceB] ipsec policy policy1 1 isakmp
[DeviceB-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-policy1-1] remote-address 2.2.1.2
[DeviceB-ipsec-policy-isakmp-policy1-1] transform-set tran1
[DeviceB-ipsec-policy-isakmp-policy1-1] quit

```

# 在接口 GigabitEthernet1/0/1 上应用安全策略。

```

[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy policy1
[DeviceB-GigabitEthernet1/0/1] quit

```

# 在接口 GigabitEthernet1/0/2 上应用安全策略。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ipsec apply policy policy1
[DeviceB-GigabitEthernet1/0/2] quit
```

# 配置 IPsec 安全策略 **policy1** 为共享源接口安全策略，共享源接口为 **Loopback0**。

```
[DeviceB] ipsec policy policy1 local-address loopback 0
```

## 6.4 验证配置

# 从 Host A ping Host B，会触发 IPsec 协商，建立 IPsec 隧道，在成功建立 IPsec 隧道后，可以 ping 通。

```
C:\Users\hosta> ping 10.1.2.2
```

```
Pinging 10.1.2.2 with 32 bytes of data:
Request timed out.
Reply from 10.1.2.2: bytes=32 time=3ms TTL=126
Reply from 10.1.2.2: bytes=32 time=1ms TTL=126
Reply from 10.1.2.2: bytes=32 time=5ms TTL=126
```

```
Ping statistics for 10.1.2.2:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

# 在 Device A 上使用 **display ike sa** 命令，可以看到第一阶段的 SA 正常建立。

```
[DeviceA] display ike sa
```

| Connection-ID | Remote  | Flag | DOI   |
|---------------|---------|------|-------|
| 9             | 3.3.3.3 | RD   | IPSEC |

```
Flags:
RD--READY RL--REPLACED FD-FADING
```

# 在 Device A 上使用 **display ipsec sa** 命令可以看到 IPsec SA 的建立情况。

```
[DeviceA] display ipsec sa
```

```

Interface: GigabitEthernet1/0/1

IPsec policy: policy1
Sequence number: 1
Mode: isakmp

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1443
Tunnel:
 local address: 2.2.1.2
 remote address: 3.3.3.3
```

```
Flow:
sour addr: 10.1.1.0/255.255.255.0 port: 0 protocol: ip
dest addr: 10.1.2.0/255.255.255.0 port: 0 protocol: ip
```

```
[Inbound ESP SAs]
SPI: 1851852454 (0x6e6106a6)
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3035
Max received sequence-number: 3
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active
```

```
[Outbound ESP SAs]
SPI: 718692851 (0x2ad661f3)
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3035
Max sent sequence-number: 3
UDP encapsulation used for NAT traversal: N
Status: Active
```

# 从 Host B 向 Host A 发起通信验证方法相同，此不赘述。

## 6.5 配置文件

- Device A:

```
#
interface GigabitEthernet1/0/1
 ip address 2.2.1.2 255.255.255.0
 ipsec apply policy policy1
#
interface GigabitEthernet1/0/2
 ip address 10.1.1.1 255.255.255.0
#
ip route-static 3.3.3.3 32 2.2.2.3
ip route-static 3.3.3.3 32 4.4.4.5
ip route-static 10.1.2.0 24 2.2.2.3
ip route-static 10.1.2.0 24 4.4.4.5
#
acl number 3000
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
```

```

ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
 remote-address 3.3.3.3
#
ike keychain keychain1
 pre-shared-key address 3.3.3.3 255.255.255.255 key cipher
c3$n6jdlYtuR+K6mijQ8qp4hMMjV/iteA==
#

```

- **Device B:**

```

#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 ip address 2.2.2.3 255.255.255.0
 ipsec apply policy policy1
#
interface GigabitEthernet1/0/2
 ip address 4.4.4.5 255.255.255.0
 ipsec apply policy policy1
#
interface GigabitEthernet1/0/3
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 10.1.1.0 24 GigabitEthernet1/0/1 2.2.1.2
ip route-static 10.1.1.0 24 GigabitEthernet1/0/2 2.2.1.2
#
acl number 3000
 rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy policy1 1 isakmp
 transform-set tran1
 security acl 3000
 remote-address 2.2.1.2
#
ipsec policy policy1 local-address LoopBack0
#
ike keychain keychain1
 pre-shared-key address 2.2.1.2 255.255.255.0 key cipher c3$n6jdlYtuR+K6mijQ8
qp4hMMjV/iteA==
#

```

## 7 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“安全命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“二层技术-广域网接入配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“二层技术-广域网接入命令参考”

# H3C MSR 系列路由器

## Portal 配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                                |    |
|--------------------------------|----|
| 1 简介                           | 1  |
| 2 配置前提                         | 1  |
| 3 可跨三层 Portal 认证配置举例           | 1  |
| 3.1 组网需求                       | 1  |
| 3.2 配置思路                       | 2  |
| 3.3 使用版本                       | 2  |
| 3.4 配置注意事项                     | 2  |
| 3.5 配置步骤                       | 3  |
| 3.5.1 RADIUS/Portal server 的配置 | 3  |
| 3.5.2 Device A 的配置             | 8  |
| 3.5.3 Device B 的配置             | 8  |
| 3.6 验证配置                       | 9  |
| 3.7 配置文件                       | 11 |
| 4 可跨三层 Portal 认证方式扩展功能配置举例     | 12 |
| 4.1 组网需求                       | 12 |
| 4.2 配置思路                       | 13 |
| 4.3 使用版本                       | 13 |
| 4.4 配置注意事项                     | 13 |
| 4.5 配置步骤                       | 13 |
| 4.5.1 Device A 的配置             | 13 |
| 4.5.2 Device B 的配置             | 14 |
| 4.6 验证配置                       | 15 |
| 4.7 配置文件                       | 17 |
| 5 直接 Portal 认证配置举例             | 18 |
| 5.1 组网需求                       | 18 |
| 5.2 配置思路                       | 19 |
| 5.3 使用版本                       | 19 |
| 5.4 配置注意事项                     | 19 |
| 5.5 配置步骤                       | 20 |
| 5.5.1 Device 的配置               | 20 |
| 5.5.2 验证配置                     | 21 |
| 5.6 配置文件                       | 22 |





# 1 简介

本文档介绍了可跨三层 Portal 认证和直接 Portal 认证的典型配置举例。

- 当接入设备与用户之间跨越三层转发设备时，可采用可跨三层 Portal 认证方式。接入设备基于用户的 IP 地址下发 ACL 对接口上通过认证的用户报文转发进行控制。
- 当接入设备与用户之间未跨越三层转发设备时，可采用直接 Portal 认证方式。接口可以学习到用户的 MAC 地址，接入设备除了可以基于用户的 IP 地址下发 ACL 对接口上通过认证的用户报文转发进行控制，还可以利用学习到 MAC 地址增强对用户报文转发的控制力度。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解 Portal 特性。

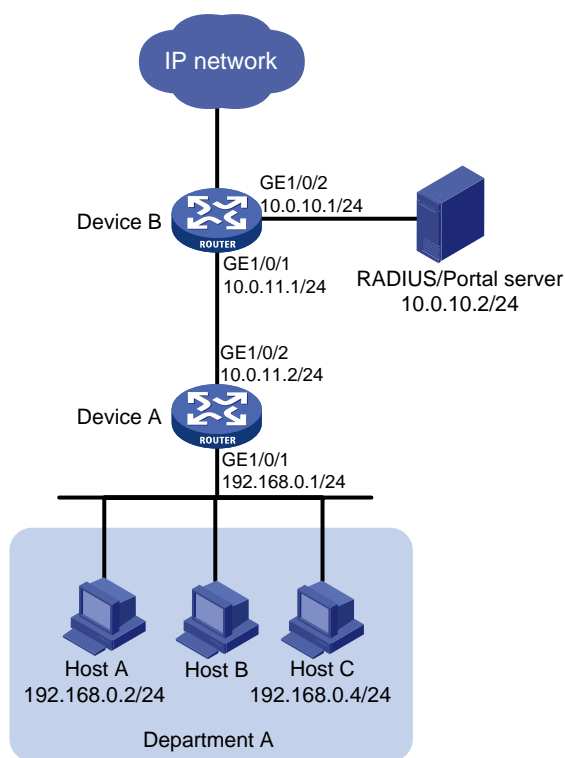
## 3 可跨三层 Portal 认证配置举例

### 3.1 组网需求

如图 1 所示，Device B 支持 Portal 认证功能，Host A、Host B 和 Host C 通过 Device A 接入到 Device B，要求：

- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 配置 Device B 采用可跨三层 Portal 认证。
- 用户在通过 Portal 认证前，只能访问 Portal Web 服务器。用户通过认证后，可以访问非受限互联网资源。
- 采用 RADIUS 服务器对 Portal 用户接入进行认证/授权和计费。
- 配置发送给 Portal 认证服务器的 Portal 报文的 BAS-IP 属性。
- 使能 RADIUS session control 功能来监听并接收 RADIUS 服务器发送的 session control 报文。

图1 可跨三层 Portal 认证配置组网图



## 3.2 配置思路

- 为了对 Department A 的网络访问进行 Portal 认证，需要在 Device B 上配置 Portal 服务器并且使能 Portal 认证。
- 为了实现通过 RADIUS 来对 Portal 用户进行认证/授权和计费，需要在 Device B 上配置 RADIUS 方案并指定相应的认证/授权服务器和计费服务器，并将其应用于 Portal 用户所属的认证域。
- 配置系统缺省的 ISP 域，所有接入用户共用此缺省域的认证/授权和计费方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置注意事项

目前仅支持使用 RADIUS 服务器对 Portal 用户进行认证/授权和计费，同时服务器需要配置路由，可以访问认证端口及用户 IP 地址所在网段。

## 3.5 配置步骤

### 3.5.1 RADIUS/Portal server 的配置



说明

下面以 iMC 为例(使用 iMC 版本为: iMC PLAT 7.0 (E0202)、iMC EIA 7.0 (E0202)), 说明 RADIUS server 和 Portal server 的基本配置。

#### # 增加接入设备

登录进入 iMC 管理平台, 选择“用户”页签, 单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项, 进入接入设备配置页面, 在该页面中单击<增加>按钮, 进入增加接入设备页面。

- 设置与 Device B 交互报文时的认证共享密钥为“expert”;
- 设置认证及计费的端口号分别为“1812”和“1813”;
- 选择业务类型为“LAN 接入业务”;
- 选择接入设备类型为“H3C (General)”;
- 选择或手工增加接入设备, 添加 IP 地址为 10.0.10.1 的接入设备;
- 其它参数采用缺省值, 并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 帮助

| 接入配置   |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 接入设备分组   | 无       |
| 共享密钥 * | *****        | 确认共享密钥 * | *****   |
| 业务分组   | 未分组          |          |         |

| 设备列表 |           |      |    |    |
|------|-----------|------|----|----|
| 选择   | 手工增加      | 全部清除 |    |    |
| 设备名称 | 设备IP地址    | 设备型号 | 备注 | 删除 |
|      | 10.0.10.1 |      |    |    |

共有1条记录。

确定 取消

#### # 增加接入策略

选择“用户”页签, 单击导航树中的[接入策略管理/接入策略管理]菜单项, 单击<增加>按钮, 进入“增加接入策略”页面。

- 接入策略名填写 portal (该名称可以自定义)。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

图3 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 帮助

### 基本信息

接入策略名 \*   
业务分组 \*   
描述

### 授权信息

接入时段  ? 分配IP地址 \*   
下行速率(Kbps)  上行速率(Kbps)   
优先级   启用RSA认证  
证书认证  不启用  EAP证书认证  WAP证书认证  
认证证书类型   
下发VLAN   
 下发User Profile 下发用户组  ?  
 下发ACL

### # 增加服务配置

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入服务器配置管理页面，在该页面中单击<增加>按钮，进入增加服务配置页面。

- 输入服务名为“Portal-auth”（该名称可以自定义）。
- 缺省接入策略选择“portal”，即上一步配置的接入策略名。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

图4 增加服务配置

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

### 基本信息

服务名 \*  服务后缀   
业务分组 \*  缺省接入策略 \*  ?  
缺省私有属性下发策略 \*  ?  
缺省BYOD页面 \*   
服务描述   
 可申请 ?  Portal无感知认证 ?

### 接入场景列表

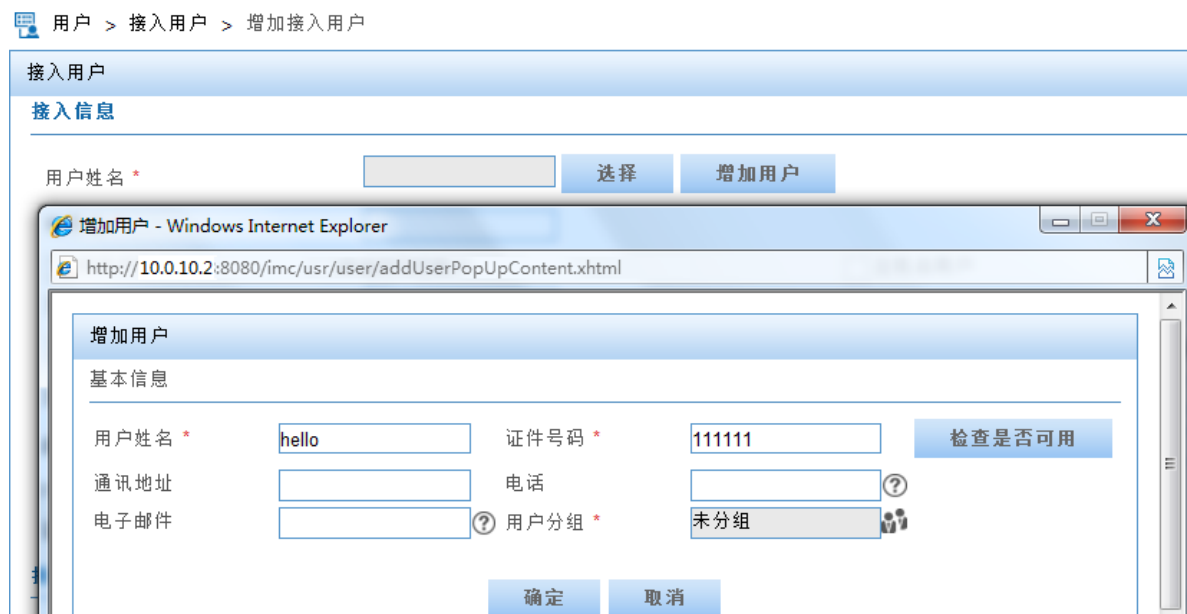
| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

### # 增加接入用户

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 单击<增加用户>按钮，手工增加用户姓名为“hello”（可自定义），证件号码为111111（可自定义）；
- 其它参数采用缺省值，并单击<确定>按钮完成操作；

图5 接入用户配置



- 输入帐号名“portal”和密码；
- 选择该用户所关联的接入服务为“Portal-auth”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加接入用户



### # 配置 Portal 主页

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，配置 Portal 主页，采用默认配置即可，并单击<确定>按钮完成操作。

图7 Portal 服务器配置页面

用户 > 接入策略管理 > Portal服务管理 > 服务器配置

### Portal服务器配置

**基本信息**

日志级别 \*

---

**Portal Server**

报文请求超时时长(秒) \*  ? 逃生心跳间隔时长(秒) \*  ?

用户心跳间隔时长(分钟) \*  ?

---

**Portal Web**

请求报文超时时长(秒) \*  ? 交互报文编码  ?

校验终端用户请求报文  使用缓存

HTTP心跳界面展示方式  HTTPS心跳界面展示方式

Portal主页

#### # 配置 Portal 认证的地址组范围

单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入“IP 地址组配置”页面，在该页面中单击<增加>按钮，进入“增加 IP 地址组配置”页面。

- 输入 IP 地址组名为“Portal\_user”；
- 输入起始地址为“192.168.0.0”、终止地址为“192.168.0.255”。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 其他采用默认配置；
- 单击<确定>按钮完成操作。

图8 增加 IP 地址组配置页面

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

### 增加IP地址组

IP地址组名 \*

起始地址 \*

终止地址 \*

业务分组

类型 \*

#### # 增加接入设备信息

单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入“设备配置”页面，在该页面中单击<增加>按钮，进入“增加设备信息”页面。

- 输入设备名为“NAS”；
- 输入IP地址为“10.0.11.1”，该地址为与接入用户相连的设备接口IP地址；
- 输入密钥为“portal”，该密钥与接入设备 Device B 上的配置保持一致；
- 选择组网方式为“三层”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9 增加设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息 帮助

**增加设备信息**

**设备信息**

|          |                                         |               |                                        |
|----------|-----------------------------------------|---------------|----------------------------------------|
| 设备名 *    | <input type="text" value="NAS"/>        | 业务分组 *        | <input type="text" value="未分组"/>       |
| 版本 *     | <input type="text" value="Portal 2.0"/> | IP地址 *        | <input type="text" value="10.0.11.1"/> |
| 监听端口 *   | <input type="text" value="2000"/>       | 本地Challenge * | <input type="text" value="否"/>         |
| 认证重发次数 * | <input type="text" value="0"/>          | 下线重发次数 *      | <input type="text" value="1"/>         |
| 支持逃生心跳 * | <input type="text" value="否"/>          | 支持用户心跳 *      | <input type="text" value="否"/>         |
| 密钥 *     | <input type="password" value="....."/>  | 确认密钥 *        | <input type="password" value="....."/> |
| 组网方式 *   | <input type="text" value="三层"/>         |               |                                        |
| 设备描述     | <input type="text"/>                    |               |                                        |

### # 配置端口组信息

返回[接入策略管理/Portal 服务管理/设备配置]菜单项，单击<端口组信息管理>按钮，进入“端口组信息配置”页面。

图10 设备信息列表

用户 > 接入策略管理 > Portal服务管理 > 设备配置 加入收藏 帮助

**设备信息查询**

|      |                      |      |                      |
|------|----------------------|------|----------------------|
| 设备名  | <input type="text"/> | 版本   | <input type="text"/> |
| 下发结果 | <input type="text"/> | 业务分组 | <input type="text"/> |

**增加**

| 设备名 | 版本         | 业务分组 | IP地址      | 最近一次下发时间 | 下发结果 | 操作                                                                                                    |
|-----|------------|------|-----------|----------|------|-------------------------------------------------------------------------------------------------------|
| NAS | Portal 2.0 | 未分组  | 10.0.11.1 |          | 未下发  | <input type="button" value="增加"/> <input type="button" value="删除"/> <input type="button" value="刷新"/> |

共有1条记录，当前第1 - 1，第 1/1 页。

在“端口组信息配置”页面中单击<增加>按钮，进入“增加端口组信息”页面。

- 输入端口组名为“group”；
- 选择IP地址组为“Portal\_user”，用户接入网络时使用的IP地址必须属于所选的IP地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。



图11 增加端口组信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息

| 增加端口组信息    |                                     |            |                                          |
|------------|-------------------------------------|------------|------------------------------------------|
| 端口组名 *     | <input type="text" value="group"/>  | 提示语言 *     | <input type="text" value="动态检测"/>        |
| 开始端口 *     | <input type="text" value="0"/>      | 终止端口 *     | <input type="text" value="222222"/>      |
| 协议类型 *     | <input type="text" value="HTTP"/>   | 快速认证 *     | <input type="text" value="否"/>           |
| 是否NAT *    | <input type="text" value="否"/>      | 错误透传 *     | <input type="text" value="是"/>           |
| 认证方式 *     | <input type="text" value="CHAP认证"/> | IP地址组 *    | <input type="text" value="Portal_user"/> |
| 心跳间隔(分钟) * | <input type="text" value="10"/>     | 心跳超时(分钟) * | <input type="text" value="30"/>          |
| 用户域名       | <input type="text"/>                | 端口组描述      | <input type="text"/>                     |
| 无感知认证      | <input type="text" value="不支持"/>    | 客户端防破解 *   | <input type="text" value="否"/>           |
| 用户属性类型     | <input type="text"/>                | 缺省认证页面     | <input type="text"/>                     |

### 3.5.2 Device A 的配置

# 配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.0.1 24
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 10.0.11.2 24
[DeviceA-GigabitEthernet1/0/2] quit
```

# 配置到 10.0.10.0/24 网段的静态路由，下一跳为 10.0.11.1。

```
[DeviceA] ip route-static 10.0.10.0 255.255.255.0 10.0.11.1
```

### 3.5.3 Device B 的配置

# 配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.0.11.1 24
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 10.0.10.1 24
[DeviceB-GigabitEthernet1/0/2] quit
```

# 配置 Portal 认证服务器：名称为 newpt，IP 地址为 10.0.10.2，密钥为明文 portal，监听 Portal 报文的端口为 50100（设备缺省端口号）。

```
[DeviceB] portal server newpt
[DeviceB-portal-server-newpt] ip 10.0.10.2 key simple portal
[DeviceB-portal-server-newpt] port 50100
[DeviceB-portal-server-newpt] quit
```

# 配置 Portal Web 服务器的 URL 为 `http://10.0.10.2:8080/portal`。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[DeviceB] portal web-server newpt
[DeviceB-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[DeviceB-portal-websvr-newpt] quit
```

# 在与 Device A 相连的接口上使能可跨三层方式的 Portal 认证。

```
[DeviceB] interface gigabitethernet1/0/1
[DeviceB-GigabitEthernet1/0/1] portal enable method layer3
```

# 在与 Device A 相连的接口上设置发送给 Portal 报文中的 BAS-IP 属性值为 10.0.11.1。

```
[DeviceB-GigabitEthernet1/0/1] portal bas-ip 10.0.11.1
```

# 在与 Device A 相连的接口上引用 Portal Web 服务器 newpt。

```
[DeviceB-GigabitEthernet1/0/1] portal apply web-server newpt
[DeviceB-GigabitEthernet1/0/1] quit
```

# 创建名字为 imc 的 RADIUS 方案并进入该方案视图。

```
[DeviceB] radius scheme imc
```

# 配置 RADIUS 方案主认证/计费服务器及其通信密钥。

```
[DeviceB-radius-imc] primary authentication 10.0.10.2
[DeviceB-radius-imc] primary accounting 10.0.10.2
[DeviceB-radius-imc] key authentication simple expert
[DeviceB-radius-imc] key accounting simple expert
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[DeviceB-radius-imc] user-name-format without-domain
[DeviceB-radius-imc] quit
```

# 配置名为 portal.com 的认证域。

```
[DeviceB] domain portal.com
```

# 配置 ISP 域的 AAA 方法。

```
[DeviceB-isp-portal.com] authentication portal radius-scheme imc
[DeviceB-isp-portal.com] authorization portal radius-scheme imc
[DeviceB-isp-portal.com] accounting portal radius-scheme imc
[DeviceB-isp-portal.com] quit
```

# 配置系统缺省的 ISP 域 portal.com，所有接入用户共用此缺省域的认证/授权和计费方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

```
[DeviceB] domain default enable portal.com
```

# 配置到 Department A 的静态路由。

```
[DeviceB] ip route-static 192.168.0.0 255.255.255.0 10.0.11.2
```

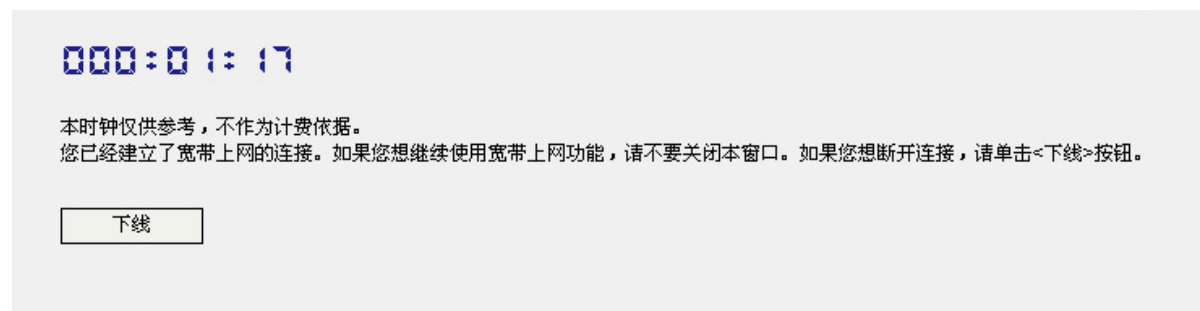
## 3.6 验证配置

# 用户既可以使用 H3C 的 iNode 客户端，也可以通过网页方式进行 Portal 认证。本例用网页方式进行 Portal 认证。用户在通过认证前，任何 Web 访问请求都会被重定向到认证页面 `http://10.0.10.2:8080/portal`，且发起的 Web 访问请求均被重定向到该认证页面，如 [图 12](#)。当用户通过认证后，跳转到 [图 13](#) 界面。

图12 Portal 认证页面



图13 Portal 用户认证成功页面



# 认证通过后，可通过执行以下显示命令查看 Device B 上生成的 Portal 在线用户信息。

```
[DeviceB] display portal user interface gigabitethernet 1/0/1
Total portal users: 1
Username: portal
 Portal server: newpt
 State: Online
 Authorization ACL: None
 VPN instance: --
MAC IP VLAN Interface
0000-0000-0000 192.168.0.2 -- GigabitEthernet1/0/1
```

## 3.7 配置文件

- Device A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.0.11.2 255.255.255.0
#
ip route-static 10.0.10.0 24 10.0.11.1
#
```

- Device B:

```
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.0.10.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.11.1 255.255.255.0
 portal enable method layer3
 portal bas-ip 10.0.11.1
 portal apply web-server newpt
#
ip route-static 192.168.0.0 24 10.0.11.2
#
radius session-control enable
#
radius scheme imc
 primary authentication 10.0.10.2
 primary accounting 10.0.10.2
 key authentication cipher c3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
 key accounting cipher c3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
 user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
 accounting portal radius-scheme imc
#
domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
```

```
portal server newpt
 ip 10.0.10.2 key cipher c3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```

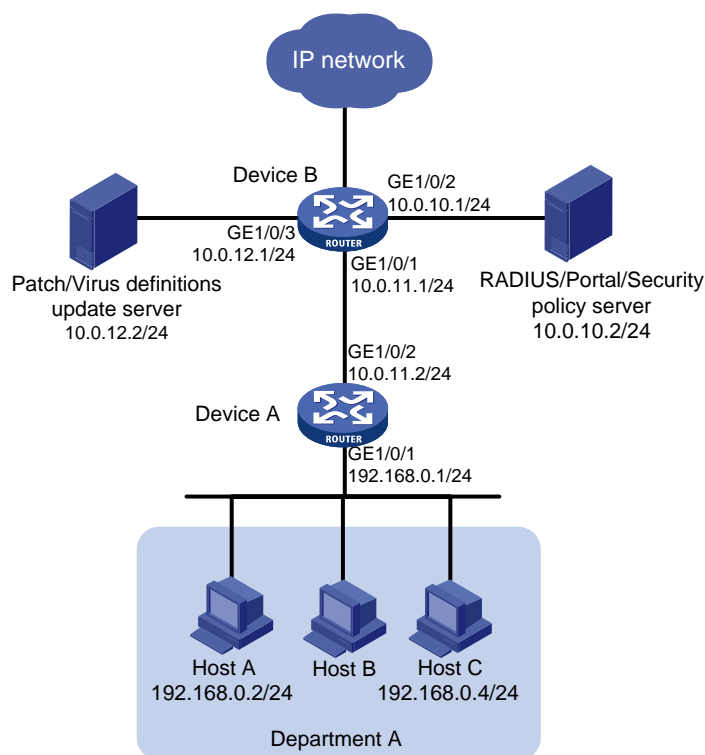
## 4 可跨三层 Portal 认证方式扩展功能配置举例

### 4.1 组网需求

如图 14 所示，Device B 支持 Portal 认证功能，Host A、Host B 和 Host C 通过 Device A 接入到 Device B，要求：

- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 配置 Device B 采用可跨三层 Portal 认证。
- 用户在通过 Portal 认证前，只能访问 Portal Web 服务器。
- 用户通过认证，但没有安装指定版本的防病毒软件，则对用户进行隔离，只允许访问病毒和补丁服务器。
- 用户通过认证，且安装了指定版本的防病毒软件，则通过安全策略检查，可正常访问网络。
- 采用 RADIUS 服务器对用户接入进行认证和授权，并采用安全策略服务器对登录成功的用户进行安全检查。
- 配置发送给 Portal 认证服务器的 Portal 报文的 BAS-IP 属性。
- 使能 RADIUS session control 功能来监听并接收 RADIUS 服务器发送的 session control 报文。

图14 Portal 三层认证扩展功能配置组网图



## 4.2 配置思路

- 为了对 Department A 的网络访问进行 Portal 认证，需要在 Device B 上配置 Portal 服务器并且使能 Portal 认证，认证通过前，所有客户端只能访问 Portal Web 服务器，用户访问任何网页都被重定向到 Portal Web 服务器主页面。
- 为了实现通过 RADIUS 来进行认证和授权，需要在 Device B 上配置 RADIUS 方案并指定相应的认证和授权服务器，并将其应用于 Portal 用户所属的认证域。
- 为了对登录成功的用户进行安全检查，需要创建 ACL 并制定规则，不符合检查要求的用户，只能访问病毒和补丁服务器，升级病毒库版本满足安全策略要求后，该用户才可访问所有网络资源。
- 配置系统缺省的 ISP 域，所有接入用户共用此缺省域的认证、授权方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

## 4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.4 配置注意事项

目前仅支持使用 RADIUS 服务器对 Portal 用户进行认证和授权，同时服务器需要配置路由，可以访问认证端口及用户 IP 地址所在网段。

## 4.5 配置步骤



- 请保证在 RADIUS 服务器、Portal 服务器上完成相应的配置，具体配置步骤请参见 [3.5.1 RADIUS/Portal server 的配置](#)。
  - 安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。
- 

### 4.5.1 Device A 的配置

# 配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.0.1 24
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 10.0.11.2 24
[DeviceA-GigabitEthernet1/0/2] quit
配置到 10.0.10.0/24 网段的静态路由，下一跳为 10.0.11.1。
[DeviceA] ip route-static 10.0.10.0 255.255.255.0 10.0.11.1
配置到 10.0.12.0/24 网段的静态路由，下一跳为 10.0.11.1。
```

```
[DeviceA] ip route-static 10.0.12.0 255.255.255.0 10.0.11.1
```

## 4.5.2 Device B 的配置

# 配置接口 GigabitEthernet 1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.0.11.1 24
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 10.0.10.1 24
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] ip address 10.0.12.1 24
[DeviceB-GigabitEthernet1/0/3] quit
```

# 配置 Portal 认证服务器：名称为 newpt，IP 地址为 10.0.10.2，密钥为明文 portal，监听 Portal 报文的端口为 50100（设备缺省端口号）。

```
[DeviceB] portal server newpt
[DeviceB-portal-server-newpt] ip 10.0.10.2 key simple portal
[DeviceB-portal-server-newpt] port 50100
[DeviceB-portal-server-newpt] quit
```

# 配置 Portal Web 服务器的 URL 为 http://10.0.10.2:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[DeviceB] portal web-server newpt
[DeviceB-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[DeviceB-portal-websvr-newpt] quit
```

# 在与 Device A 相连的接口上使能可跨三层方式的 Portal 认证。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] portal enable method layer3
```

# 在与 Device A 相连的接口上设置发送给 Portal 报文中的 BAS-IP 属性值为 10.0.11.1。

```
[DeviceB-GigabitEthernet1/0/1] portal bas-ip 10.0.11.1
```

# 在与 Device A 相连的接口上引用 Portal Web 服务器 newpt。

```
[DeviceB-GigabitEthernet1/0/1] portal apply web-server newpt
[DeviceB-GigabitEthernet1/0/1] quit
```

# 配置到 Department A 的静态路由。

```
[DeviceB] ip route-static 192.168.0.0 255.255.255.0 10.0.11.2
```

# 创建名字为 imc 的 RADIUS 方案并进入该方案视图。

```
[DeviceB] radius scheme imc
```

# 配置 RADIUS 方案相关参数，包括 RADIUS 服务器地址，认证密钥等。

```
[DeviceB-radius-imc] primary authentication 10.0.10.2
[DeviceB-radius-imc] primary accounting 10.0.10.2
[DeviceB-radius-imc] key authentication simple expert
[DeviceB-radius-imc] key accounting simple expert
```

# 配置 RADIUS 方案的安全策略服务器。

```
[DeviceB-radius-imc] security-policy-server 10.0.10.2
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[DeviceB-radius-imc] user-name-format without-domain
[DeviceB-radius-imc] quit
使能 RADIUS session control 功能。
[DeviceB] radius session-control enable
配置名为 portal.com 的认证域。
[DeviceB] domain portal.com
配置 ISP 域的 AAA 方法。
[DeviceB-isp-portal.com] authentication portal radius-scheme imc
[DeviceB-isp-portal.com] authorization portal radius-scheme imc
[DeviceB-isp-portal.com] accounting portal radius-scheme imc
[DeviceB-isp-portal.com] quit
配置系统缺省的 ISP 域 portal.com，所有接入用户共用此缺省域的认证/授权和计费方法，若用户
登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。
[DeviceB] domain default enable portal.com
配置 ACL 3000，只允许访问补丁和病毒服务器。
[DeviceB] acl number 3000
[DeviceB-acl-adv-3000] rule permit ip destination 10.0.12.2 0
[DeviceB-acl-adv-3000] rule deny ip
[DeviceB-acl-adv-3000] quit
配置 ACL 3001，允许所有 IP 地址通过。
[DeviceB] acl number 3001
[DeviceB-acl-adv-3001] rule permit ip
[DeviceB-acl-adv-3001] quit
```

## 4.6 验证配置

# 用户只能使用 H3C 的 iNode 客户端，进行 Portal 扩展功能认证。用户通过 iNode 客户端，新建 Portal 连接，输入正确的用户名和密码，登录成功。





然后，开始安全检查，安全检查不合格，进入隔离模式，查看设备上 Portal 用户，可看到下发了隔离 ACL 3000。

```
[DeviceB]display portal user all
Total portal users: 1
Username: cc16
 Portal server: newpt
 State: Online
 Authorization ACL: 3000
 VPN instance: --
 MAC IP VLAN Interface
 0000-0000-0000 192.168.0.2 -- GigabitEthernet1/0/1
```

# 升级病毒库，版本满足安全策略要求。客户端断开后，重新登录，认证成功后，进行安全检查，客户端提示安全检查合格，设备上查看通过认证的 Portal 用户信息，可见下发了安全 ACL 3001。

```
[DeviceB]display portal user all
Total portal users: 1
Username: cc16
 Portal server: newpt
 State: Online
 Authorization ACL: 3001
 VPN instance: --
 MAC IP VLAN Interface
```

```
0000-0000-0000 192.168.0.2 -- GigabitEthernet1/0/1
```

## 4.7 配置文件

- Device A:

```

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0

interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.0.11.2 255.255.255.0

ip route-static 10.0.10.0 24 10.0.11.1
ip route-static 10.0.12.0 24 10.0.11.1
#
```

- Device B:

```

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.11.1 255.255.255.0
portal enable method layer3
portal bas-ip 10.0.11.1
 portal apply web-server newpt

interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.0.10.1 255.255.255.0

interface GigabitEthernet1/0/3
 port link-mode route
 ip address 10.0.12.1 255.255.255.0

ip route-static 192.168.0.0 24 10.0.11.2

acl number 3000
 rule 0 permit ip destination 10.0.12.2 0
 rule 5 deny ip

acl number 3001
 rule 0 permit ip

radius session-control enable

radius scheme imc
 primary authentication 10.0.10.2
 primary accounting 10.0.10.2
```

```

security-policy-server 10.0.10.2
key authentication cipher c3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
key accounting cipher c3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
user-name-format without-domain
#
domain portal.com
authentication portal radius-scheme imc
authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
domain default enable portal.com
#
portal web-server newpt
url http://10.0.10.2:8080/portal
#
portal server newpt
ip 10.0.10.2 key cipher c3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#

```

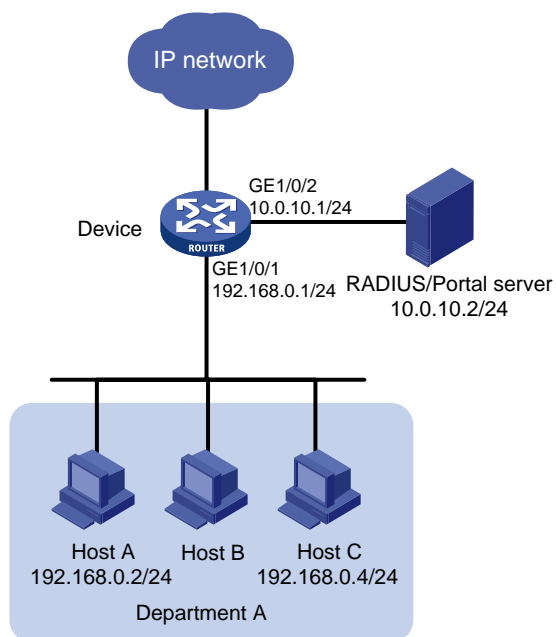
## 5 直接 Portal 认证配置举例

### 5.1 组网需求

如图 15 所示，Department A 客户端与接入设备直接相连，采用直接方式的 Portal 认证。

- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- Department A 下面的用户在通过 Portal 认证前，只能访问 Portal Web 服务器，无法访问内部其它网络或 Internet。用户通过认证后，可以正常访问网络。
- 采用 RADIUS 服务器对 Portal 用户接入进行认证/授权和计费。
- 配置发送给 Portal 认证服务器的 Portal 报文的 BAS-IP 属性。
- 使能 RADIUS session control 功能来监听并接收 RADIUS 服务器发送的 session control 报文。

图15 Portal 特性直接认证配置组网图



## 5.2 配置思路

- 为了对 Department A 的网络访问进行 Portal 认证，需要在 Device 上配置 Portal 服务器并且使能 Portal 认证。
- 为了实现通过 RADIUS 来对 Portal 用户进行认证/授权和计费，需要在 Device 上配置 RADIUS 方案并指定相应的认证/授权服务器和计费服务器，并将其应用于 Portal 用户所属的认证域。
- 配置系统缺省的 ISP 域，所有接入用户共用此缺省域的认证/授权和计费方法，若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。

## 5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 5.4 配置注意事项

目前仅支持使用 RADIUS 服务器对 Portal 用户进行认证/授权和计费，同时服务器需要配置路由，可以访问认证端口及用户 IP 地址所在网段。

## 5.5 配置步骤



说明

请保证在 RADIUS 服务器、Portal 服务器上完成相应的配置，具体配置步骤请参见 [3.5.1 RADIUS/Portal server 的配置](#)。其中“增加 Portal 设备”步骤中的选择组网方式改为“直连”，并将 IP 地址改为 192.168.0.1 即可。

### 5.5.1 Device 的配置

# 配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.0.1 24
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ip address 10.0.10.1 24
[Device-GigabitEthernet1/0/2] quit
```

# 配置 Portal 认证服务器：名称为 newpt，IP 地址为 10.0.10.2，密钥为明文 portal，监听 Portal 报文的端口为 50100（设备缺省端口号）。

```
[Device] portal server newpt
[Device-portal-server-newpt] ip 10.0.10.2 key simple portal
[Device-portal-server-newpt] port 50100
[Device-portal-server-newpt] quit
```

# 配置 Portal Web 服务器的 URL 为 http://10.0.10.2:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Device] portal web-server newpt
[Device-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[Device-portal-websvr-newpt] quit
```

# 在与客户端相连的接口上使能直接方式的 Portal 认证。

```
[Device] interface gigabitethernet1/0/1
[Device-GigabitEthernet1/0/1] portal enable method direct
```

# 在与客户端相连的接口上设置发送给 Portal 报文中的 BAS-IP 属性值为 192.168.0.1。

```
[Device-GigabitEthernet1/0/1] portal bas-ip 192.168.0.1
```

# 在与客户端相连的接口上引用 Portal Web 服务器 newpt。

```
[Device-GigabitEthernet1/0/1] portal apply web-server newpt
[Device-GigabitEthernet1/0/1] quit
```

# 创建名字为 imc 的 RADIUS 方案并进入该方案视图。

```
[Device] radius scheme imc
```

# 配置 RADIUS 方案主认证服务器及其通信密钥。

```
[Device-radius-imc] primary authentication 10.0.10.2
[Device-radius-imc] primary accounting 10.0.10.2
[Device-radius-imc] key authentication simple expert
[Device-radius-imc] key accounting simple expert
```

```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。
[Device-radius-imc] user-name-format without-domain
[Device-radius-imc] quit
使能 RADIUS session control 功能。
[Device] radius session-control enable
配置名为 portal.com 的认证域。
[Device] domain portal.com
配置 ISP 域的 AAA 方法。
[Device-isp-portal.com] authentication portal radius-scheme imc
[Device-isp-portal.com] authorization portal radius-scheme imc
[Device-isp-portal.com] accounting portal radius-scheme imc
[Device-isp-portal.com] quit
配置系统缺省的 ISP 域 portal.com，所有接入用户共用此缺省域的认证、授权方法，若用户登录
时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。
[Device] domain default enable portal.com

```

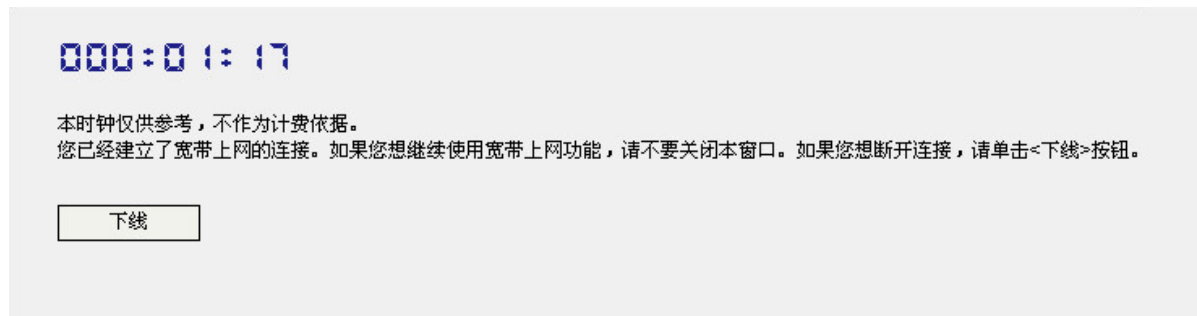
## 5.5.2 验证配置

# 用户既可以使用 H3C 的 iNode 客户端，也可以通过网页方式进行 Portal 认证。本例用网页方式进行 Portal 认证。用户在通过认证前，只能访问认证页面 <http://10.0.10.2:8080/portal>，且发起的 Web 访问请求均被重定向到该认证页面，如 [图 16](#)。当用户通过认证后，跳转到 [图 17](#) 界面。

图16 Portal 认证页面



图17 认证成功页面



# 认证通过后，可通过执行以下显示命令查看 Device 上生成的 Portal 在线用户信息。

```
[DeviceB] display portal user interface gigabitethernet 1/0/1
Total portal users: 1
Username: portal
 Portal server: newpt
 State: Online
 Authorization ACL: None
 VPN instance: --
MAC IP VLAN Interface
0015-e9a6-7cfe 192.168.0.2 -- GigabitEthernet1/0/1
```

## 5.6 配置文件

```
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.0.10.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
 portal enable method direct
 portal bas-ip 192.168.0.1
 portal apply web-server newpt
#
radius session-control enable
#
radius scheme imc
 primary authentication 10.0.10.2
 primary accounting 10.0.10.2
 key authentication cipher c3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
 key accounting cipher c3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
 user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
```

```
accounting portal radius-scheme imc
#
domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher c3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```

## 6 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“安全命令参考”



# H3C MSR 系列路由器

## SSH 配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                                                  |    |
|--------------------------------------------------|----|
| 1 特性简介 .....                                     | 1  |
| 2 配置前提 .....                                     | 1  |
| 3 设备作为 Stelnet 服务器配置举例（password 认证） .....        | 1  |
| 3.1 组网需求 .....                                   | 1  |
| 3.2 配置思路 .....                                   | 1  |
| 3.3 使用版本 .....                                   | 2  |
| 3.4 配置步骤 .....                                   | 2  |
| 3.5 验证配置 .....                                   | 3  |
| 3.6 配置文件 .....                                   | 4  |
| 4 设备作为 Stelnet 服务器配置举例（publickey 认证） .....       | 5  |
| 4.1 组网需求 .....                                   | 5  |
| 4.2 配置思路 .....                                   | 5  |
| 4.3 使用版本 .....                                   | 6  |
| 4.4 配置注意事项 .....                                 | 6  |
| 4.5 配置步骤 .....                                   | 6  |
| 4.5.1 配置 Host 作为 Stelnet 客户端 .....               | 6  |
| 4.5.2 配置 Device 作为 FTP 服务器 .....                 | 8  |
| 4.5.3 配置 FTP 客户端上传公钥文件 .....                     | 9  |
| 4.5.4 配置 Device 作为 Stelnet 服务器 .....             | 9  |
| 4.6 验证配置 .....                                   | 10 |
| 4.7 配置文件 .....                                   | 14 |
| 5 设备作为 Stelnet 客户端配置举例（password 认证） .....        | 15 |
| 5.1 组网需求 .....                                   | 15 |
| 5.2 配置思路 .....                                   | 15 |
| 5.3 使用版本 .....                                   | 15 |
| 5.4 配置步骤 .....                                   | 15 |
| 5.4.1 Stelnet 服务器的配置 .....                       | 15 |
| 5.4.2 Stelnet 客户端的配置 .....                       | 17 |
| 5.5 验证配置 .....                                   | 17 |
| 5.6 配置文件 .....                                   | 18 |
| 6 设备作为 SFTP 客户端配置举例（password-publickey 认证） ..... | 19 |
| 6.1 组网需求 .....                                   | 19 |

|                                          |           |
|------------------------------------------|-----------|
| 6.2 配置思路 .....                           | 19        |
| 6.3 使用版本 .....                           | 20        |
| 6.4 配置注意事项 .....                         | 20        |
| 6.5 配置步骤 .....                           | 20        |
| 6.5.1 SFTP 客户端的配置 .....                  | 20        |
| 6.5.2 配置 DeviceB 作为 FTP 服务器 .....        | 20        |
| 6.5.3 配置客户端 DeviceA 上传公钥文件 .....         | 21        |
| 6.5.4 配置 Device B 作为 SFTP 服务器 .....      | 21        |
| 6.6 验证配置 .....                           | 22        |
| 6.7 配置文件 .....                           | 24        |
| <b>7 SCP 文件传输配置举例（password 认证） .....</b> | <b>24</b> |
| 7.1 组网需求 .....                           | 24        |
| 7.2 配置思路 .....                           | 25        |
| 7.3 使用版本 .....                           | 25        |
| 7.4 配置步骤 .....                           | 26        |
| 7.4.1 配置 RADIUS 服务器 .....                | 26        |
| 7.4.2 配置 Device B .....                  | 27        |
| 7.4.3 配置 Device A .....                  | 28        |
| 7.5 验证配置 .....                           | 29        |
| 7.6 配置文件 .....                           | 29        |
| <b>8 相关资料 .....</b>                      | <b>29</b> |

# 1 特性简介

本文档介绍了使用 SSH（Secure Shell，安全外壳）功能实现安全的远程访问或文件管理的典型配置举例。

# 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解 SSH 特性。

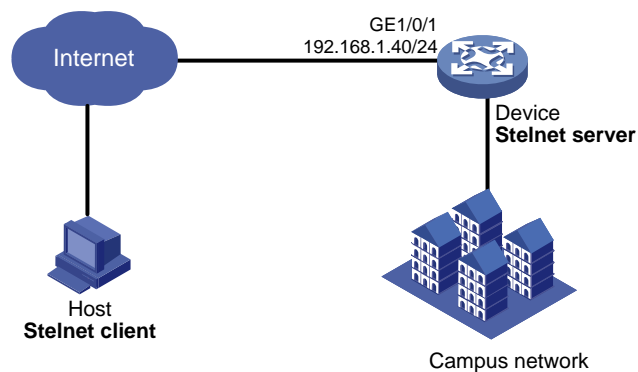
# 3 设备作为 Stelnet 服务器配置举例（password 认证）

## 3.1 组网需求

如图 1 所示，网络管理员需要通过 Internet 远程登录到校园网的网关设备（Device）上对其进行相关配置。为了提高对 Device 进行管理的安全性，可将 Device 配置为 Stelnet 服务器，并在 Host 上运行 Stelnet 客户端软件，在二者之间建立 SSH 连接。要求：

- Device 通过 SSH 的 password 认证方式对客户端进行认证，认证过程在 Device 本地完成；
- 网络管理员 Host 的登录用户名为 client001，密码为 aabbcc，登录设备后可以正常使用所有命令。

图1 设备作为 Stelnet 服务器配置组网图



## 3.2 配置思路

- 为了使 SSH 的版本协商和算法协商过程正常运行，且为了保证客户端对连接的服务器的认证正常进行，请在服务器端生成 RSA、DSA 密钥对。

- 为了采用本地认证的方式认证用户，需要在本地服务器 **Device** 上创建相应的本地用户，并在本地用户视图下配置密码。
- **Stelnet** 客户端通过 **VTY** 用户线访问设备。因此，需要配置登录用户线的认证方式为 **scheme** 方式。
- 为了使 **Stelnet** 用户登录设备后能正常使用所有命令，将用户角色设置为 **network-admin**，缺省情况下本地用户的用户角色为 **network-operator**。

### 3.3 使用版本

本举例是在 **R6728** 版本上进行配置和验证的。

### 3.4 配置步骤

# 生成 **RSA** 密钥对。

```
<Device> system-view
[Device] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++
.....+++++
..+++++++
.....+++++++
Create the key pair successfully.
```

# 生成 **DSA** 密钥对。

```
[Device] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
..+++++++*
.....+......+......+......+.
...+......+......+.
Create the key pair successfully.
```

# 使能 **SSH** 服务器功能。

```
[Device] ssh server enable
```

# 配置接口 **GigabitEthernet1/0/1** 的 **IP** 地址，客户端将通过该地址连接 **Stelnet** 服务器。

```
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.40 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

# 设置 **Stelnet** 客户端登录用户界面的认证方式为 **scheme**。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

```
[Device-line-vty0-63] quit
创建本地用户 client001，并设置用户密码、服务类型和用户角色。
[Device] local-user client001 class manage
New local user added.
[Device-luser-manage-client001] password simple aabbcc
[Device-luser-manage-client001] service-type ssh
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

### 3.5 验证配置



说明

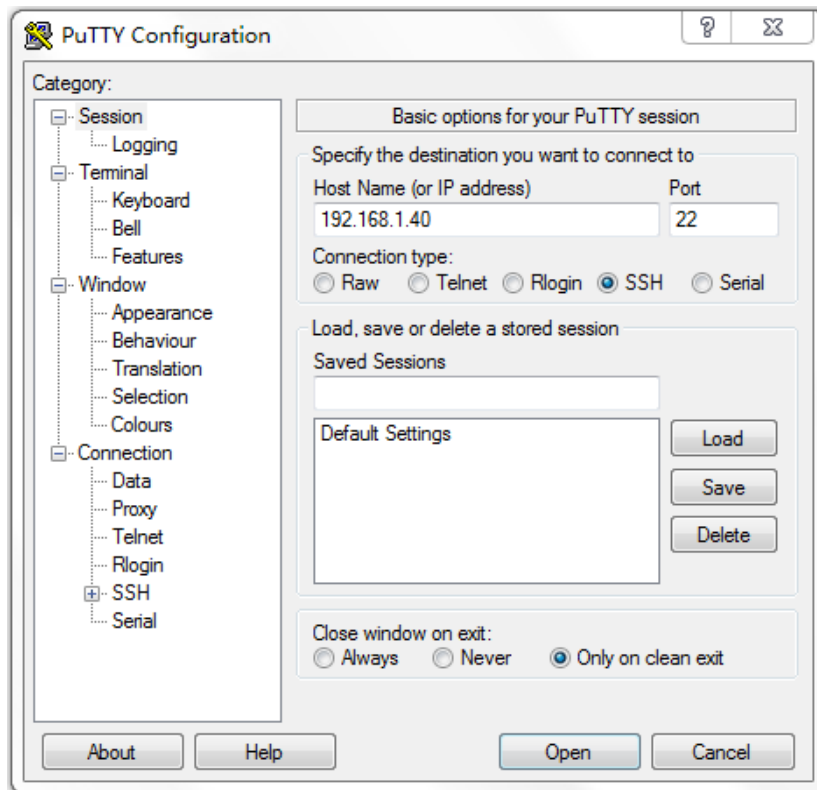
Stelnet 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.60 为例，说明 Stelnet 客户端的配置方法。

# 安装 PuTTY0.60 软件。

# 打开 PuTTY.exe 程序，点击“Session”功能区，出现如图 2 所示的客户端配置界面。

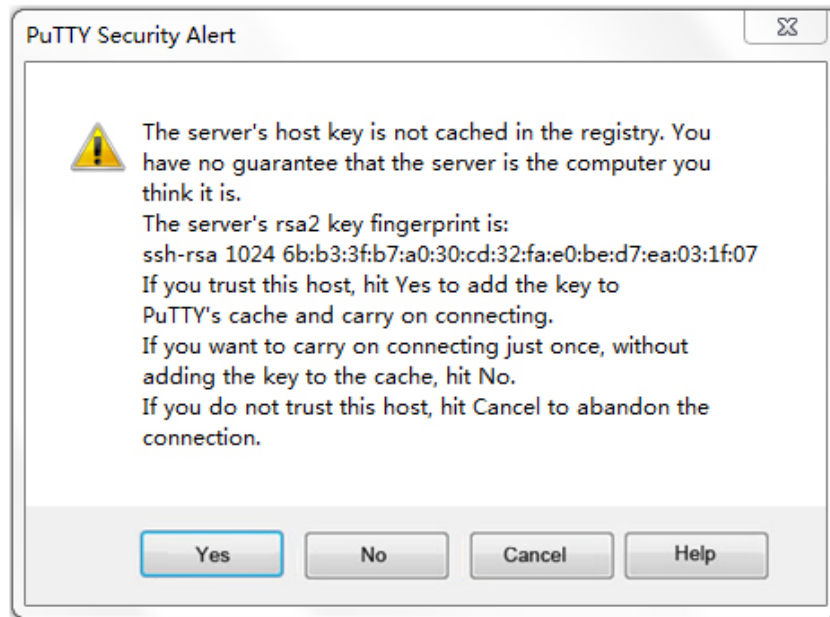
- 在“Host Name (or IP address)”文本框中输入 Stelnet 服务器的 IP 地址为 192.168.1.40。
- 在“Port”文本框中输入 SSH 协议端口号 22。
- 在“Connection type”区域选择 SSH 协议。

图2 Stelnet 客户端配置界面



# 在图2界面中，单击<Open>按钮。弹出“PuTTY Security Alert”对话框。

图3 Stelnet 客户端登录界面（一）



# 单击“是（Y）”按钮，并输入用户名“client001”和密码“aabbcc”，即可成功登录设备使用所有命令。

```
login as: client001
```

```
client001@192.168.1.40's password:
```

```

* Copyright (c) 2004-2021 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *

```

```
<Device>
```

## 3.6 配置文件

```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.1.40 255.255.255.0
#
line vty 0 63
authentication-mode scheme
#
ssh server enable
#
local-user client001 class manage
password hash h6$CqMnWdX6LIW/hz2Z$4+0Pumk+A98VlGVgqN3n/mEi7hJka9fEZpRZlPSNi9b
cBEXhpvIqaYTvIVBf7ZUNgnovFsqW7nYxjoToRDvYBg==
service-type ssh
```

```
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
```

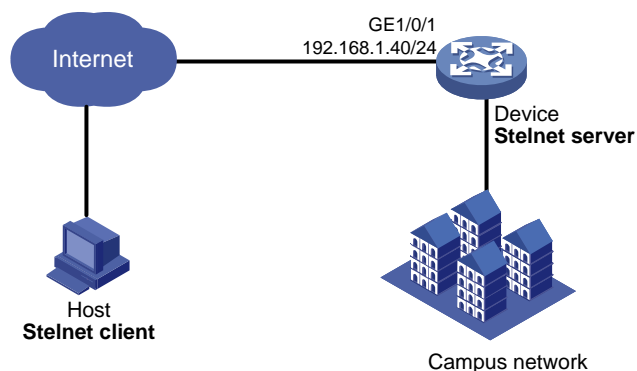
## 4 设备作为 Stelnet 服务器配置举例（publickey 认证）

### 4.1 组网需求

如图 4 所示，网络管理员需要通过 Internet 远程登录到校园网的网关设备（Device）上对其进行相关配置。为了提高对 Device 进行管理的安全性和认证强度，将 Device 配置为 Stelnet 服务器，要求：

- Device 通过 publickey 认证方式对 Stelnet 客户端进行认证，使用的公钥算法为 RSA。
- 网络管理员 Host 的登录用户名为 client001，登录设备后可以正常使用所有命令。
- 服务器端通过从公钥文件中导入的方式来配置客户端的公钥。

图4 设备作为 Stelnet 服务器配置组网图



### 4.2 配置思路

- 在服务器的配置过程中需要指定客户端的公钥信息，因此需要首先完成客户端密钥对的配置，再进行服务器的配置。
- 服务器在采用 publickey 方式验证客户端身份时，首先要比较客户端发送的 Stelnet 用户名、主机公钥是否与本地配置的 SSH 用户名以及相应的客户端主机公钥一致，在确认用户名和客户端主机公钥正确后，再利用数字签名对客户端进行验证，而该签名是客户端利用主机公钥对应的私钥计算出的。因此，需要在服务器端配置客户端的 RSA 主机公钥，并在客户端为该 SSH 用户指定与主机公钥对应的 RSA 主机私钥。
- 如果 SSH 服务器采用 publickey 方式认证客户端，必须在服务器上创建相应的 SSH 用户，以及同名的本地用户（用于下发授权属性：工作目录、用户角色）。
- Stelnet 客户端通过 VTY 用户线访问设备。因此，需要配置登录用户线的认证方式为 scheme 方式。
- 为了使 Stelnet 用户登录设备后要能正常使用所有命令，将用户的用户角色设置为 network-admin，缺省情况下本地用户的用户角色为 network-operator。



## 4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.4 配置注意事项

虽然一个客户端只会采用 RSA、DSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，请在服务器上同时生成 RSA、DS 密钥对。

## 4.5 配置步骤

### 4.5.1 配置 Host 作为 Stelnet 客户端

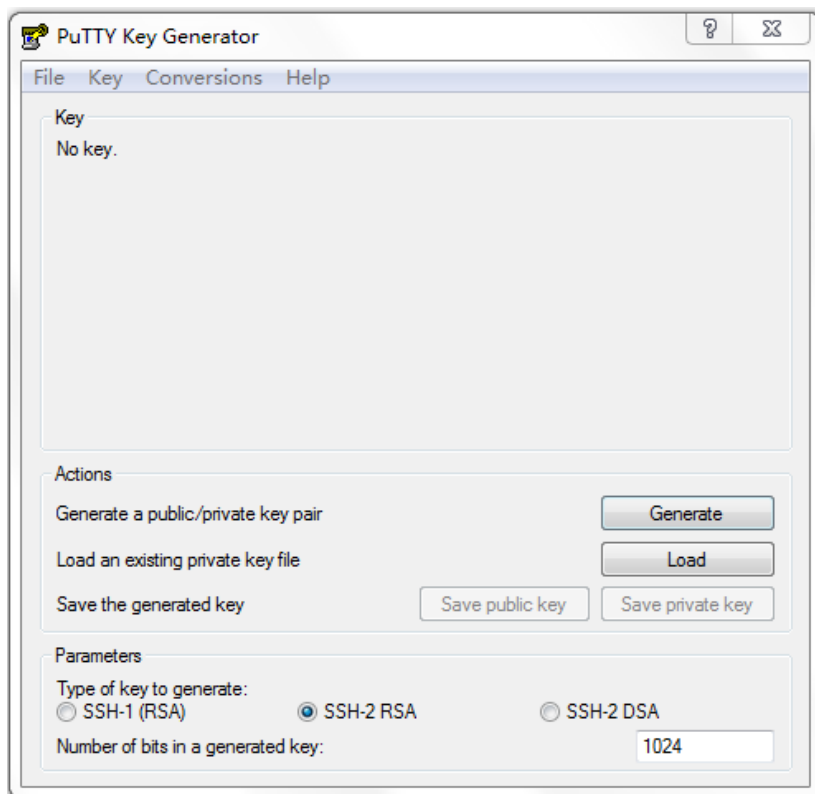


说明

客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.60 为例，说明 Stelnet 客户端的配置方法。

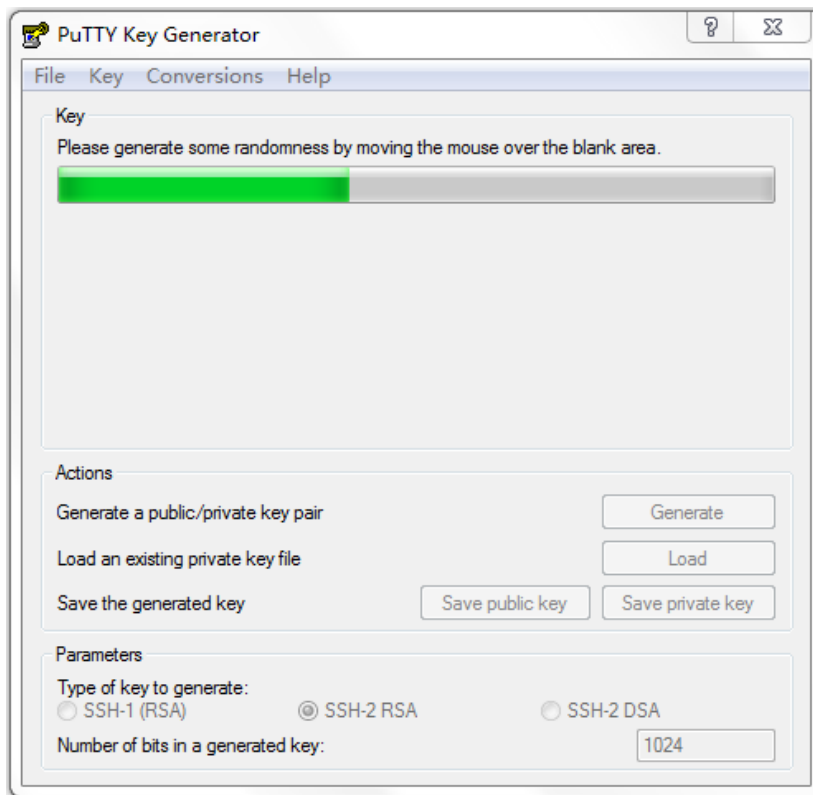
# 在客户端运行 PuTTYGen.exe，在参数栏中选择“SSH-2 RSA”，点击<Generate>，产生客户端密钥对。

图5 生成客户端密钥（1）



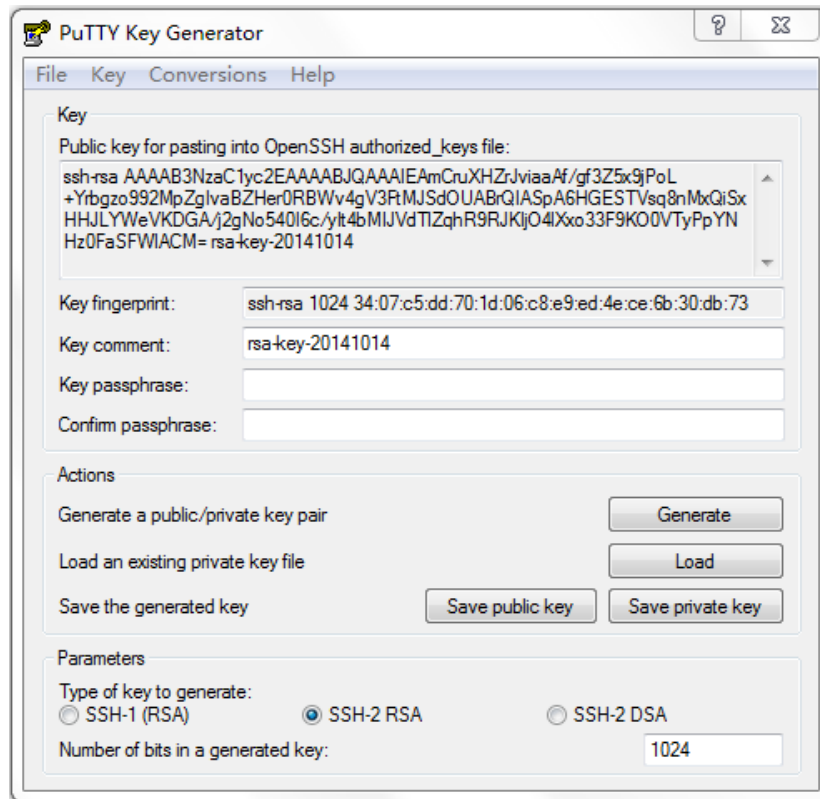
# 在产生密钥对的过程中需不停地移动鼠标，鼠标移动仅限于图6蓝色框中除绿色标记进程条外的地方，否则进程条会停止显示，密钥对将停止产生。

图6 生成客户端密钥（2）



# 密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击<保存>按钮将公钥文件保存在 D 盘。

图7 生成客户端密钥 (3)



# 点击<Save private key>存储私钥,选择保存的路径(例如 D:\),并输入私钥文件名为 private.ppk,点击保存。

## 4.5.2 配置 Device 作为 FTP 服务器

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<Device> system-view
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.40 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

# 在 Device 上创建一个 ftp 类型的本地用户,并设置密码为明文 ftp,服务类型为 FTP,用户角色为 network-admin,工作目录为 flash:/。

```
[Device] local-user ftp class manage
New local user added.
[Device-luser-manage-ftp] password simple ftp
[Device-luser-manage-ftp] authorization-attribute user-role network-admin
[Device-luser-manage-ftp] authorization-attribute work-directory flash:/
[Device-luser-manage-ftp] service-type ftp
[Device-luser-manage-ftp] quit
```

# 开启 Device 的 FTP 服务器功能。

```
[Device] ftp server enable
[Device] quit
```

### 4.5.3 配置 FTP 客户端上传公钥文件

```
Host 通过 FTP 登录并上传公钥文件 key.pub 到 Device。
<DeviceA>ftp 192.168.1.40
Press CTRL+C to abort.
Connected to 192.168.1.40 (192.168.1.40).
220 FTP service ready.
User (192.168.1.56:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put flash:/key.pub
227 Entering Passive Mode (192,168,1,40,41,116)
150 Accepted data connection
226 File successfully transferred
301 bytes sent in 0.000 seconds (1.05 Mbytes/s)
ftp> quit
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.
```

### 4.5.4 配置 Device 作为 Stelnet 服务器

```
生成 RSA 密钥对。
[Device] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....++++++
.....++++++
..+++++++
.....+++++++
Create the key pair successfully.
生成 DSA 密钥对。
[Device] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
..+++++++*
.....+.....+.....+.....+
...+.....+.....+...+
Create the key pair successfully.
使能 SSH 服务器功能。
```

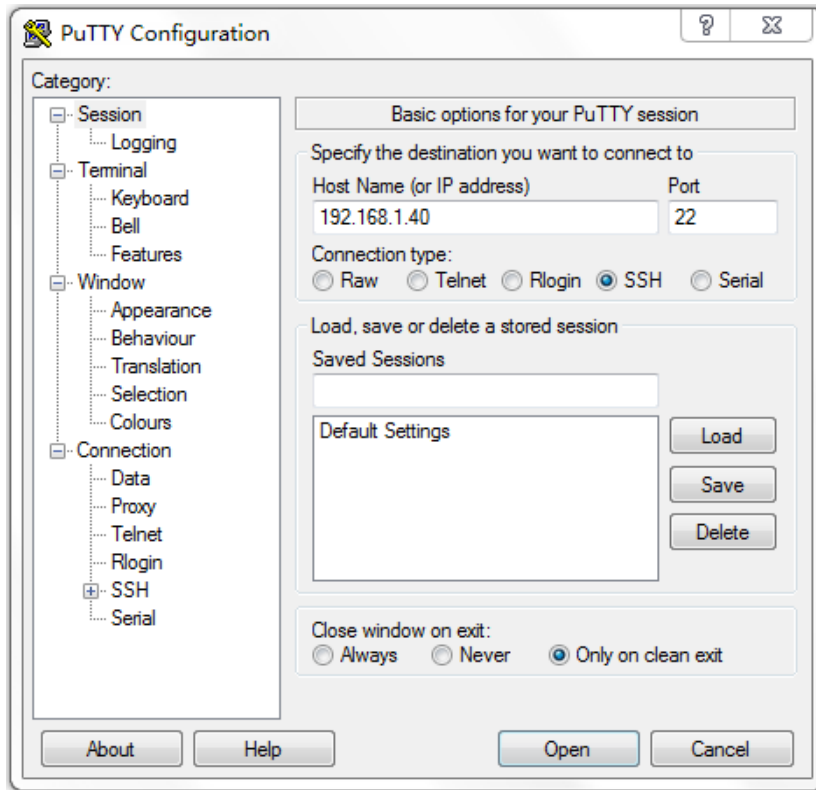
```
[Device] ssh server enable
设置 Stelnet 客户端登录用户界面的认证方式为 scheme。
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
从文件 key.pub 中导入客户端的公钥，并命名为 devicekey。
[Device] public-key peer devicekey import sshkey key.pub
设置 SSH 用户 client001 的认证方式为 publickey，并指定公钥为 devicekey。
[Device] ssh user client001 service-type stelnet authentication-type publickey assign
publickey devicekey
创建本地用户 client001，并设置服务类型为 SSH，用户角色为 network-admin。
[Device] local-user client001 class manage
New local user added.
[Device-luser-manage-client001] service-type ssh
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

## 4.6 验证配置

# 客户端打开 PuTTY.exe 程序，点击“Session”功能区，出现如图 8 所示的客户端配置界面。

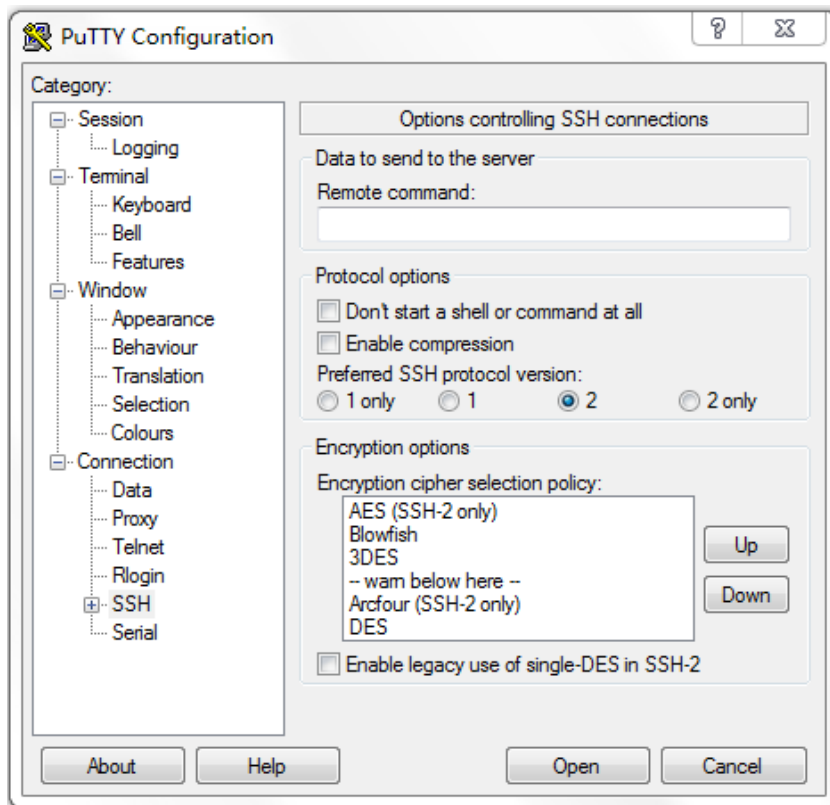
- 在“Host Name (or IP address)”文本框中输入 Stelnet 服务器的 IP 地址为 192.168.1.40。
- 在“Port”文本框中输入 SSH 协议端口号 22。
- 在“Connection type”区域选择 SSH 协议。

图8 Stelnet 客户端配置界面 (1)



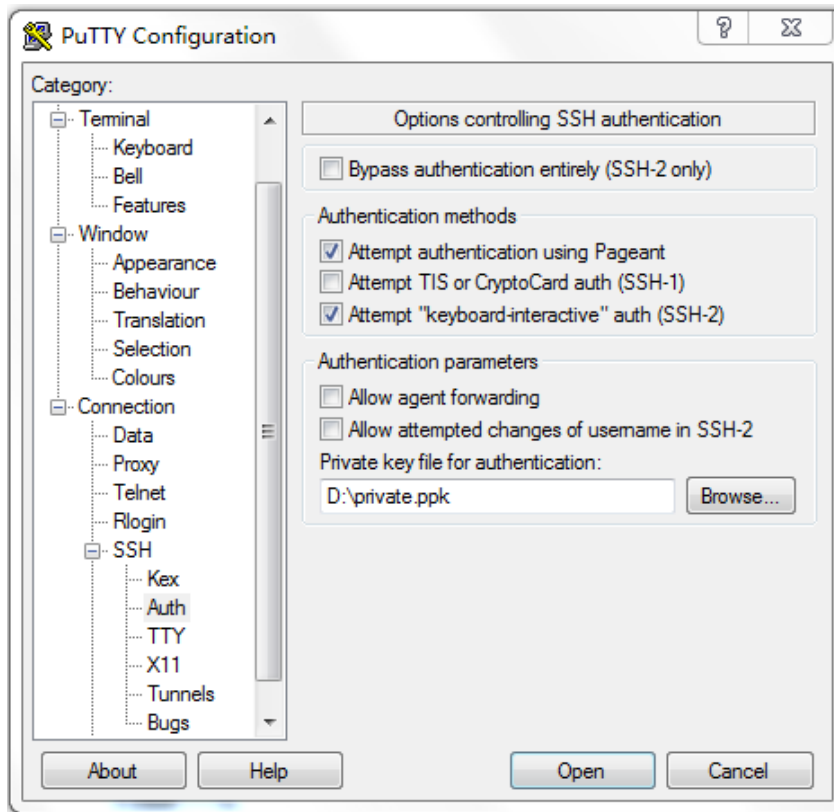
# 单击左侧导航栏“Connection->SSH”，出现如图9的界面。选择“Preferred SSH protocol version”为“2”。

图9 Stelnet 客户端配置界面 (2)



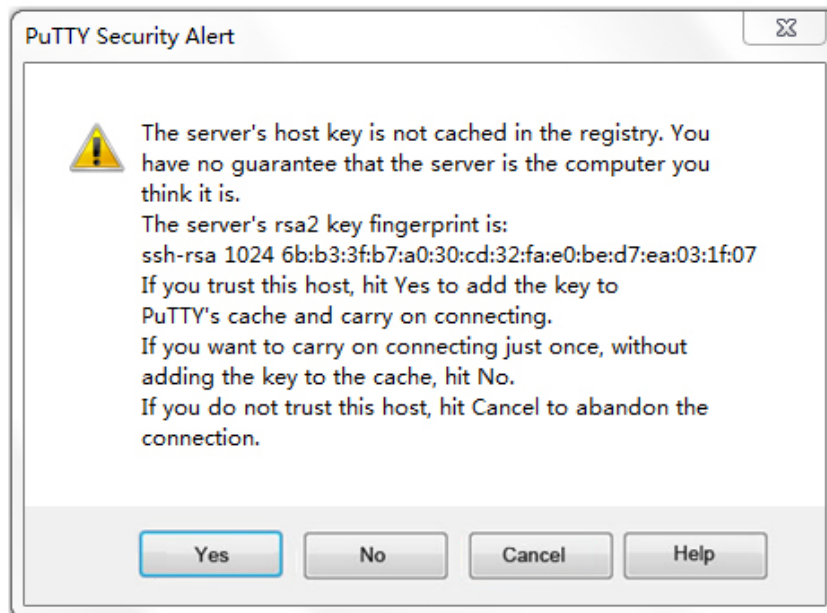
# 单击左侧导航栏“Connection->SSH”下面的“Auth”(认证), 出现如[图 10](#)的界面。单击<Browse...>按钮, 弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件 `private.ppk`。

图10 Stelnet 客户端配置界面（3）



# 单击<Open>按钮。弹出“PuTTY Security Alert”对话框。

图11 Stelnet 客户端登录界面（一）





# 单击“是 (Y)”按钮，按提示输入用户名 client001，即可进入 Device 的配置界面，用户角色为 network-admin。

```
login as: client001
```

```
Authenticating with public key "rsa-key-20140726"
```

```

* Copyright (c) 2004-2021 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *

```

```
<Device>
```

## 4.7 配置文件

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.1.40 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
ssh user client001 service-type stelnet authentication-type publickey assign publickey
devicekey
#
local-user client001 class manage
 service-type ssh
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
public-key peer Devicekey
 public-key-code begin
30819D300D06092A864886F70D010101050003818B0030818702818100A2DBC1FD76A837BEF5D322598442D6
753B2E8F7ADD6D6209C80843B206B309078AFE2416CB4FAD496A6627243EAD766D57AEA70B901B4B4566D9A6
51B133BAE34E9B9F04E542D64D0E9814D7E3CBCDBCAF28FF21EE4EADAE6DF52001944A40414DDFF280FF043B1
4838288BE7F9438DC71ABBC2C28BF78F34ADF3D1C912579A19020125
 public-key-code end
peer-public-key end
#
local-user ftp
 password cipher c3$sg9WgqO1w8vnAv2FKGTOYgFJm3nn2w==
 authorization-attribute work-directory flash:/
 authorization-attribute user-role network-operator
 service-type ftp
#
ftp server enable
#
```

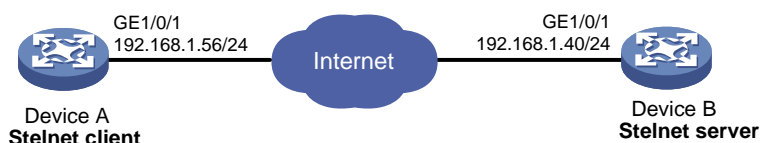
## 5 设备作为 Stelnet 客户端配置举例（password 认证）

### 5.1 组网需求

如图 12 所示，Device A 作为 Stelnet 客户端，采用 SSH 协议远程登录到 Device B 上。要求：

- Device B 采用本地认证的方式认证用户，Stelnet 服务器采用的认证方式为 password 认证。
- 登录用户名为 client001，密码为 aabbcc，用户登录设备后可以正常使用所有命令。
- 为提高安全性，需要以 Stelnet 客户端保存的主机公钥来验证 Stelnet 服务器，Stelnet 客户端只信任通过验证的 Stelnet 服务器并继续访问该服务器。

图12 设备作为 Stelnet 客户端配置组网图



### 5.2 配置思路

- 为了使 SSH 的版本协商和算法协商过程正常运行，且为了保证客户端对连接的服务器的认证正常进行，请在服务器端生成 RSA、DSA 密钥对。
- Stelnet 客户端通过 VTY 用户线访问设备。因此，需要配置登录用户线的认证方式为 scheme 方式。
- 为了采用本地认证的方式认证用户，需要在 Stelnet 服务器上创建相应的本地用户，并在本地用户视图下配置密码。
- 为了使 Stelnet 用户登录设备后能正常使用所有命令，将用户的用户角色设置为 network-admin，缺省情况下本地用户的用户角色为 network-operator。
- 因为需要以 Stelnet 客户端保存的主机公钥来验证 Stelnet 服务器，所以需要先将 Stelnet 服务器主机公钥配置在 Stelnet 客户端上。

### 5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 5.4 配置步骤

#### 5.4.1 Stelnet 服务器的配置

# 生成 RSA 密钥对。

```
<DeviceB> system-view
[DeviceB] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
```

```

Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++
.....+++++
..+++++++
.....+++++++
Create the key pair successfully.
生成 DSA 密钥对。
[DeviceB] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++*
.....+.....+.....+.....+
...+.....+.....+.....+
Create the key pair successfully.
使能 SSH 服务器功能。
[DeviceB] ssh server enable
配置接口 GigabitEthernet1/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 192.168.1.40 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
设置 Stelnet 客户端登录用户界面的认证方式为 scheme。
[DeviceB] line vty 0 63
[DeviceB-line-vty0-63] authentication-mode scheme
[DeviceB-line-vty0-63] quit
创建本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。
[DeviceB]local-user client001 class manage
New local user added.
[DeviceB-luser-manage-client001] password simple aabbcc
[DeviceB-luser-manage-client001]service-type ssh
[DeviceB-luser-manage-client001] authorization-attribute user-role network-admin
[DeviceB-luser-manage-client001]quit
显示服务器端 DSA 公钥内容。
[DeviceB] display public-key local dsa public

=====
Key name: dsakey(default)
Key type: DSA
Time when key pair created: 11:02:10 2014/08/07
Key code:

308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E

```

```
DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
```

## 5.4.2 Stelnet 客户端的配置

# 配置接口 GigabitEthernet1/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.1.56 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

# 指定服务器端的主机公钥名称为 key1，并进入公钥视图。

```
[DeviceA] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
```

# 在客户端配置服务器端的主机公钥(由于客户端缺省采用 DSA 主机公钥认证服务器，因此这里输入的是在在服务器端通过 **display public-key local dsa public** 命令显示公钥内容。)

```
[DeviceA-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F02818100D757262C
4584C44C211F18BD96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC
1EDBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD77FE6B1289
3DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B368950387811C7DA33021500C773218C73
7EC8EE993B4F2DED30F48EDACE915F0281810082269009E14EC474BAF2932E69D3B1F18517AD9594184CCDFC
EAE96EC4D5EF93133E84B47093C52B20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71
B020217091AC717B612391C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC0
28F4B1585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565AB73D4BA
295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30A2A9FF7E899628557E39CE
8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872061F9B4B08301ADC81F7EC1501FFB863C000
9536596CCB508596C3325892DC6D8C5C35B5
```

# 退出公钥视图，并保存用户输入的公钥。

```
[DeviceA-pkey-public-key-key1] peer-public-key end
[DeviceA] return
```

## 5.5 验证配置

# 建立到服务器 192.168.1.40 的 SSH 连接，并指定服务器端的主机公钥 key1。输入正确的用户名和密码之后，即可成功登录到 Device B 上，用户角色为 network-admin。

```
<DeviceA> ssh2 192.168.1.40 publickey key1
login as: client001
client001@192.168.1.40's password:
```

```

* Copyright (c) 2004-2021 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *

```

\*\*\*\*\*

<DeviceB>

## 5.6 配置文件

- DeviceA

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.1.56 255.255.255.0
#
public-key peer key1
public-key-code begin
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
 96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
 DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
 DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
 7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
 4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
 35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
 91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
 585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
 AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
 A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
 061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
public-key-code end
peer-public-key end
#
```

- DeviceB

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.1.40 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
#
local-user client001
 password cipher c3$o71Exx1XIKs9gJoxqSodHG1luT9rlZEd4w==
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
 service-type ssh
#
```

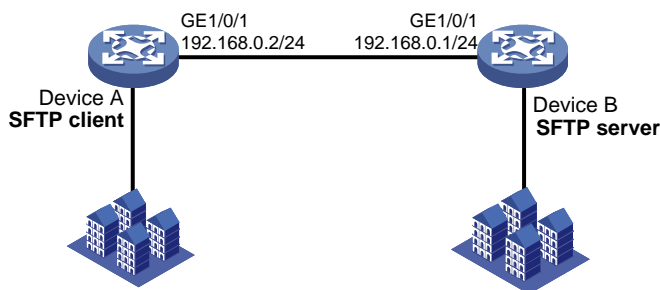
## 6 设备作为 SFTP 客户端配置举例 (password-publickey 认证)

### 6.1 组网需求

如图 13 所示, Device A 和 Device B 之间建立 SSH 连接, Device A 作为 SFTP 客户端登录到 Device B, 进行文件管理和文件传送等操作。要求:

- 为了保证高安全性和认证强度, 要求 Device B 通过 password-publickey 认证方式对客户端进行认证, 公钥算法为 RSA。
- 登录用户名为 client001, 密码为 aabbcc, 用户登录设备后可以正常使用所有命令。
- 服务器端通过从公钥文件中导入的方式来配置客户端的公钥。

图13 设备作为 SFTP 客户端配置组网图



### 6.2 配置思路

- 为了采用本地认证用户, 需在本地 SFTP 服务器 DeviceB 上创建相应的本地用户, 并在本地用户视图下配置密码。
- 服务器在采用 publickey 方式验证客户端身份时, 首先要比较客户端发送的 SSH 用户名、主机公钥是否与本地配置的 SSH 用户名以及相应的客户端主机公钥一致, 在确认用户名和客户端主机公钥正确后, 再对客户端发送的数字签名进行验证, 而该签名是客户端利用主机公钥对应的私钥计算出的。因此, 需要在服务器端配置客户端的 RSA 主机公钥, 并在客户端为该 SSH 用户指定与主机公钥对应的 RSA 主机私钥 (在向服务器发起连接时通过 identity-key 关键字指定公钥算法来实现)。
- 如果 SSH 服务器采用 publickey 方式认证客户端, 必须在 SFTP 服务器上创建相应的 SSH 用户, 以及同名的本地用户 (用于下发授权属性: 工作目录、用户角色)。
- 在服务器的配置过程中需要指定客户端的公钥信息, 因此需要首先完成客户端密钥对的配置, 再进行服务器的配置。
- 因为 SFTP 用户登录设备后要能正常使用所有命令, 所以将用户的用户角色设置为 network-admin, 缺省情况下本地用户的用户角色为 network-operator。

## 6.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 6.4 配置注意事项

虽然一个客户端只会采用 RSA、DSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，建议在服务器上同时生成 RSA、DSA 密钥对。

## 6.5 配置步骤

### 6.5.1 SFTP 客户端的配置

# 配置接口 GigabitEthernet1/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.0.2 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

# 生成 RSA 密钥对。

```
[DeviceA] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++
.....+++++
..+++++++
.....+++++++
Create the key pair successfully.
```

# 将生成的 RSA 主机公钥导出到指定文件 key.pub 中。

```
[DeviceA] public-key local export rsa ssh2 key.pub
[DeviceA] quit
```

### 6.5.2 配置 DeviceB 作为 FTP 服务器

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 192.168.0.1 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
```

# 在 Device 上创建一个 ftp 类型的本地用户，并设置密码为明文 ftp，服务类型为 FTP，用户角色为 network-admin，工作目录为 flash:/。

```
[DeviceB] local-user ftp class manage
New local user added.
```

```

[DeviceB-luser-manage-ftp] password simple ftp
[DeviceB-luser-manage-ftp] authorization-attribute user-role network-admin
[DeviceB-luser-manage-ftp] authorization-attribute work-directory flash:/
[DeviceB-luser-manage-ftp] service-type ftp
[DeviceB-luser-manage-ftp] quit
开启 Device 的 FTP 服务器功能。
[DeviceB] ftp server enable
[DeviceB] quit

```

### 6.5.3 配置客户端 DeviceA 上传公钥文件

# DeviceA 通过 FTP 登录并上传 flash:/路径下的公钥文件 key.pub 到 Device。

```

<DeviceA>ftp 192.168.0.1
Press CTRL+C to abort.
Connected to 192.168.0.1 (192.168.0.1).
220 FTP service ready.
User (192.168.0.2:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put flash:/key.pub
227 Entering Passive Mode (192,168,0,1,41,116)
150 Accepted data connection
226 File successfully transferred
301 bytes sent in 0.000 seconds (1.05 Mbytes/s)
ftp> quit
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.

```

### 6.5.4 配置 Device B 作为 SFTP 服务器

# 生成 RSA 密钥对。

```

<DeviceB> system-view
[DeviceB] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++
.....+++++
..+++++++
.....+++++++
Create the key pair successfully.

```

# 生成 DSA 密钥对。

```

[DeviceB] public-key local create dsa

```



```

The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.+++++*
.....+.....+.....+.....+
...+.....+.....+.....+
Create the key pair successfully.
启动 SFTP 服务器。
[DeviceB] sftp server enable
从文件 key.pub 中导入远端的公钥，并命名为 devicekey。
[DeviceB] public-key peer devicekey import sshkey key.pub
设置 SSH 用户 client001 的服务类型为 SFTP，认证方式为 password-publickey，并指定公钥为 devicekey。
[DeviceB] ssh user client001 service-type sftp authentication-type password-publickey assign publickey devicekey
创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin，工作目录为 flash:/。
[DeviceB] local-user client001 class manage
New local user added.
[DeviceB-luser-manage-client001] password simple aabbcc
[DeviceB-luser-manage-client001] service-type ssh
[DeviceB-luser-manage-client001] authorization-attribute user-role network-admin work-directory flash:/
[DeviceB-luser-manage-client001] quit

```

## 6.6 验证配置

```

与远程 SFTP 服务器建立连接。
<DeviceA >sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
输入用户密码 aabbcc 后进入 SFTP 客户端视图。
sftp>
显示服务器的当前目录，删除文件 z，并检查此文件是否删除成功。
sftp> dir -l
-rwxrwxrwx 1 1 1 1759 Aug 23 06:52 config.cfg
-rw-rw---- 1 1 1 301 Aug 7 16:52 key.pub
-rwxrwxrwx 1 1 1 0 Sep 01 06:22 new
-rwxrwxrwx 1 1 1 225 Sep 01 06:55 pub
-rwxrwxrwx 1 1 1 225 Aug 24 08:01 pubkey2

```

```

-rwxrwxrwx 1 1 1 0 Sep 01 08:00 z
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx 1 1 1 1759 Aug 23 06:52 config.cfg
-rw-rw---- 1 1 1 301 Aug 7 16:52 key.pub
-rwxrwxrwx 1 1 1 0 Sep 01 06:22 new
-rwxrwxrwx 1 1 1 225 Sep 01 06:55 pub
-rwxrwxrwx 1 1 1 225 Aug 24 08:01 pubkey2

```

# 新增目录 new1，并检查新目录是否创建成功。

```

sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx 1 1 1 1759 Aug 23 06:52 config.cfg
-rw-rw---- 1 1 1 301 Aug 7 16:52 key.pub
-rwxrwxrwx 1 1 1 0 Sep 01 06:22 new
drwxrwxrwx 1 1 1 0 Sep 02 06:30 new1
-rwxrwxrwx 1 1 1 225 Sep 01 06:55 pub
-rwxrwxrwx 1 1 1 225 Aug 24 08:01 pubkey2

```

# 将目录名 new1 更名为 new2，并查看是否更名成功。

```

sftp> rename new1 new2
sftp> dir -l
-rwxrwxrwx 1 1 1 1759 Aug 23 06:52 config.cfg
-rw-rw---- 1 1 1 301 Aug 7 16:52 key.pub
-rwxrwxrwx 1 1 1 0 Sep 01 06:22 new
drwxrwxrwx 1 1 1 0 Sep 02 06:33 new2
-rwxrwxrwx 1 1 1 225 Sep 01 06:55 pub
-rwxrwxrwx 1 1 1 225 Aug 24 08:01 pubkey2

```

# 从服务器上下载文件 pubkey2 到本地，并更名为 public。

```

sftp> get pubkey2 public
Fetching /pubkey2 to public
/public 100% 301 0.3KB/s 00:00

```

# 将本地文件 public 上传到服务器上，并查看上传是否成功。

```

sftp> put public
Uploading public to /public
public 100% 301 0.3KB/s 00:00

```

```

sftp> dir -l
-rwxrwxrwx 1 1 1 1759 Aug 23 06:52 config.cfg
-rw-rw---- 1 1 1 301 Aug 7 16:52 key.pub
-rwxrwxrwx 1 1 1 0 Sep 01 06:22 new
drwxrwxrwx 1 1 1 0 Sep 02 06:33 new2
-rwxrwxrwx 1 1 1 225 Sep 01 06:55 pub
-rwxrwxrwx 1 1 1 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 1 1 301 Jul 30 16:21 public

```

sftp>

# 退出 SFTP 客户端视图。

```

sftp> quit
<DeviceA>

```

## 6.7 配置文件

- DeviceA

```

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.2 255.255.255.0
#
```

- DeviceB

```

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0

sftp server enable
ssh user client001 service-type sftp authentication-type password-publickey assign
publickey devicekey

local-user client001 class manage
 service-type ssh
 password cipher c3$o7lExx1XIKs9gJoxqSodHG1luT9rlZEd4w==
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin

ftp server enable

local-user ftp class manage
 password simple ftp
 service-type ftp
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator

public-key peer devicekey
 public-key-code begin
30819F300D06092A864886F70D010101050003818D00308189
1BD316C0DBB9009503E78F31947B651F9950E9A6E9E256E1E
 public-key-code end
 peer-public-key end
#
```

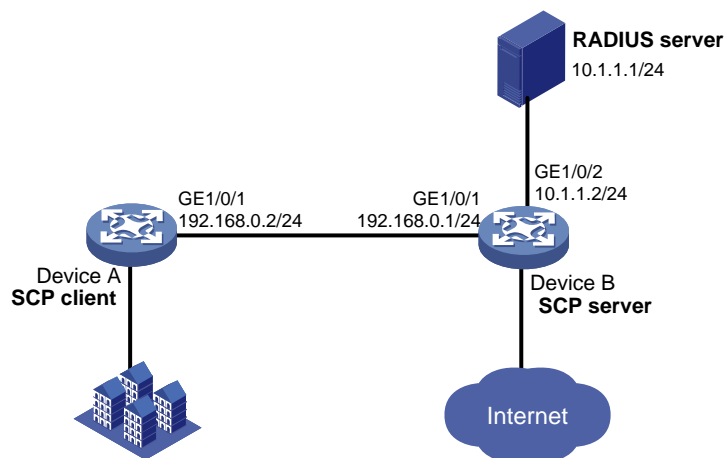
## 7 SCP 文件传输配置举例（password 认证）

### 7.1 组网需求

如图 14 所示，Device A 作为 SCP 客户端，Device B 作为 SCP 服务器。要求：

- 采用 password 认证方式对 SCP 客户端进行远程认证，用户能够通过 Device A 安全地登录到 Device B 上。
- 采用 RADIUS 服务器对登录 Device B 的 SCP 用户 Device A 进行认证和授权，登录用户名为 hello @bbb，密码为 aabbcc，Device A 登录 Device B 后可以正常使用所有命令；
- Device B 向 RADIUS 服务器发送的用户名带域名。

图14 SCP 文件传输配置组网图



## 7.2 配置思路

- 为了使 SSH 的版本协商和算法协商过程正常运行，且为了保证客户端对连接的服务器的认证正常进行，请在服务器端生成 RSA、DSA 密钥对。
- 采用 RADIUS 服务器对登录 Device B 的 SCP 用户 Device A 进行认证，需要在 RADIUS 服务器上添加用户名和密码。
- 为保证 RADIUS 客户端和 RADIUS 服务器之间信息交互的安全性，且为了防止用户密码在不安全的网络上传递时被窃取，需要在 Device B 和 RADIUS 服务器上设置相同的共享密钥。
- 为了使 Device A 登录 Device B 后可以正常使用所有命令，在 RADIUS 服务器上设置用户角色为 network-admin。
- 为了实现通过 RADIUS 来进行认证和授权，需要在 Device B 上配置 RADIUS 方案指定相应的认证和授权服务器，并配置认证 SSH 用户的 ISP 域。

## 7.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 7.4 配置步骤

### 7.4.1 配置 RADIUS 服务器



说明

本文以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0102)、iMC EIA 7.0(E0201)），说明该例中 RADIUS 服务器的基本配置。

#### 1. 增加接入设备

# 登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置认证及计费的端口号分别为“1812”（RADIUS 服务器的认证端口为 UDP 端口 1812）和“1813”（RADIUS 服务器的计费端口为 UDP 端口 1813）；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C(General)”；
- 设置与 Device 交互报文时使用的认证和授权共享密钥为“expert”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图15 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

接入配置

认证端口 *	1812	计费端口 *	1813
组网方式	不启用混合组网	业务类型	设备管理业务
接入设备类型	H3C(General)	接入设备分组	无
共享密钥 *	.....	确认共享密钥 *	.....
业务分组	未分组		

设备列表

选择	手工增加	全部清除		
设备名称	设备IP地址	设备型号	备注	删除
	10.1.1.2			删除

共有1条记录。

确定 取消

#### 2. 增加设备管理用户

# 选择“用户”页签，单击导航树中的[接入用户管理视图/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 输入用户名“hello@bbb”和密码“aabbcc”。
- 选择服务类型为“SSH”。
- 输入用户角色名“network-admin”

- 添加所管理设备的 IP 地址，IP 地址范围为“10.1.1.0~10.1.1.255”。
- 单击<确定>按钮完成操作。

图16 增加设备管理用户



## 7.4.2 配置 Device B

# 生成 RSA 密钥对。

```
<DeviceB> system-view
[DeviceB] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++
.....+++++
..+++++
.....+++++
Create the key pair successfully.
```

# 生成 DSA 密钥对。

```
[DeviceB] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
```

```

Input the modulus length [default = 1024]:
Generating Keys...
.+++++*
.....+.....+.....+.....+
...+.....+.....+...+
Create the key pair successfully.
配置接口 GigabitEthernet1/0/1 的 IP 地址，客户端将通过该地址连接 SCP 服务器。
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 192.168.0.1 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
配置接口 GigabitEthernet1/0/2 的 IP 地址。
[DeviceB] interface GigabitEthernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 10.1.1.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/2] quit
使能 SSH 服务器功能。
[DeviceB] ssh server enable
创建 RADIUS 方案 rad。
[DeviceB] radius scheme rad
配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。
[DeviceB-radius-rad] primary authentication 10.1.1.1 1812
配置主计费服务器的 IP 地址为 10.1.1.1，计费端口号为 1813。
[DeviceB-radius-rad] primary accounting 10.1.1.1 1813
配置与认证和计费服务器交互报文时的共享密钥为明文 expert。
[DeviceB-radius-rad] key authentication simple expert
[DeviceB-radius-rad] key accounting simple expert
配置向 RADIUS 服务器发送的用户名要携带域名。
[DeviceB-radius-rad] user-name-format with-domain
[DeviceB-radius-rad] quit
创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 RADIUS 认证、授权和计费。
[DeviceB] domain bbb
[DeviceB-isp-bbb] authentication login radius-scheme rad
[DeviceB-isp-bbb] authorization login radius-scheme rad
[DeviceB-isp-bbb] accounting login radius-scheme rad
[DeviceB-isp-bbb] quit

```

### 7.4.3 配置 Device A

```

配置接口 GigabitEthernet1/0/1 的 IP 地址。
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.0.2 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] quit

```

## 7.5 验证配置

# 与远程 SCP 服务器建立连接，并下载远端的 remote.bin 文件，下载到本地后更名为 local.bin。

```
<DeviceA> scp 192.168.0.1 get remote.bin local.bin
Username: hello@bbb
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
hello@bbb@192.168.0.1's password:
remote.bin 100% 8275KB 318.3KB/s 00:26.
```

## 7.6 配置文件

- DeviceA

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.2 255.255.255.0
#
```

- DeviceB

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher c3$63G7LzIQElGq4aFGTiYQafU+loQxS/cbLg==
 key accounting cipher c3$tUIVlyGISJ5X/yiTfWrmh8nyjBIF+1LFzQ==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

## 8 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“安全配置指导”



- 《H3C MSR 系列路由器 命令参考(V7)》中的“安全命令参考”

# H3C MSR 系列路由器

## OSPF 配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 OSPF 路由信息过滤配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	2
3.3 配置注意事项.....	2
3.4 配置步骤.....	2
3.4.1 配置各接口的 IP 地址.....	2
3.4.2 配置 OSPF 网络的基本功能.....	2
3.4.3 配置 RIP 网络的基本功能.....	3
3.4.4 将 RIP 路由和 OSPF 路由互相引入.....	4
3.4.5 配置 OSPF 的路由过滤功能.....	5
3.5 验证配置.....	6
3.6 配置文件.....	8
4 相关资料.....	11

# 1 简介

本文档介绍了 OSPF 路由信息过滤的配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 OSPF 路由信息过滤的特性。

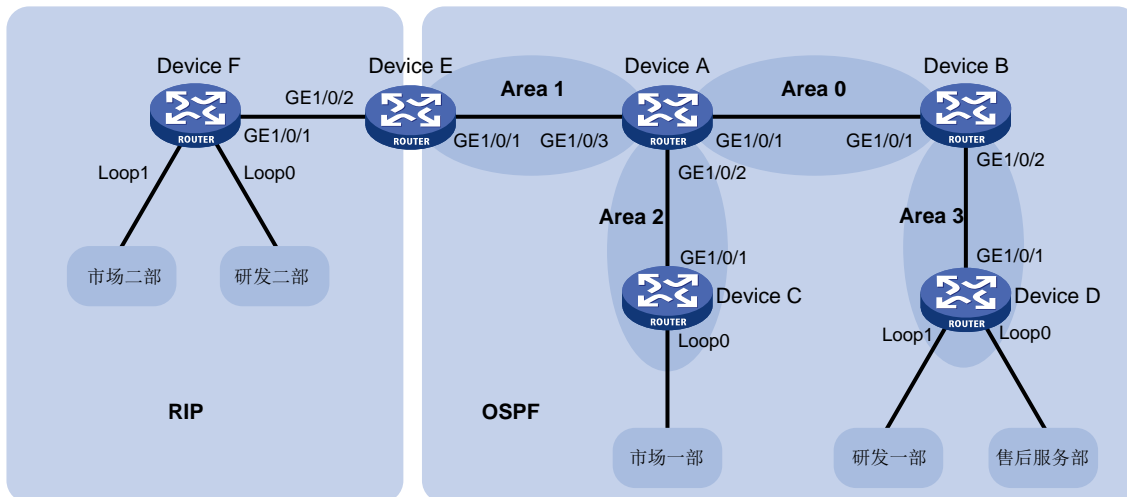
## 3 OSPF 路由信息过滤配置举例

### 3.1 组网需求

如图 1 所示，公司 A 使用 OSPF 路由协议实现公司设备全网互通，后来公司 A 扩张兼并了公司 B，要求将公司 B 采用的 RIP 路由协议与公司 A 的 OSPF 协议互相引入，使得各个部门可以实现互通。Device A 和 Device B 作为公司核心设备负责各个部门间的通信。由于业务需要，现要求通过下列措施控制并调整网络中的路由信息：

- 在 Device E 上对引入的路由信息进行过滤，使得研发二部所在网段无法被引入到 OSPF 内。
- 在 Device C 上使用路由信息的过滤功能，使得市场一部所在网段无法访问研发一部。
- 在 Device D 上使用路由信息的过滤功能，使得研发一部和售后服务部所在网段无法访问市场二部。

图1 OSPF 路由信息过滤组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	10.1.1.1/24	Device B	GE1/0/1	10.1.1.2/24
	GE1/0/2	10.2.1.1/24		GE1/0/2	10.3.1.1/24
	GE1/0/3	10.4.1.1/24			
Device C	GE1/0/1	10.2.1.2/24	Device D	GE1/0/1	10.3.1.2/24
	Loop0	192.168.3.1/24 (市场一部所在网段)		Loop0	192.168.1.1/24 (售后服务部所在网段)
				Loop1	192.168.2.1/24 (研发一部所在网段)
Device E	GE1/0/1	10.4.1.2/24	Device F	GE1/0/1	10.5.1.2/24
	GE1/0/2	10.5.1.1/24		Loop0	192.168.4.1/24 (研发二部所在网段)
				Loop1	192.168.5.1/24 (市场二部所在网段)

## 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.3 配置注意事项

- 路由信息过滤功能中对于引入外部路由信息时采用 **export** 关键字进行过滤，该参数只能在 ASBR 上生效。
- 路由信息过滤功能只是对路由表中相关路由信息过滤，并不是过滤掉 OSPF 中通告的 LSA。
- 由于路由通信是双向的，使用路由信息过滤功能将某一目的网段过滤后，该路由器下联的其它网段无法访问这个目的网段的设备，这个目的网段的设备也不能访问源地址网段的设备。
- 使用路由信息过滤功能配合 ACL 使用时，必须将最后一条规则设置为允许所有源地址通过才能避免将所有网段路由全部过滤掉。

## 3.4 配置步骤

### 3.4.1 配置各接口的 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

### 3.4.2 配置 OSPF 网络的基本功能

# 在 Device A 上使能指定网段的 OSPF 路由功能。

```
<DeviceA> system-view
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

```
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] area 2
[DeviceA-ospf-1-area-0.0.0.2] network 10.2.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.2] quit
[DeviceA-ospf-1] area 1
[DeviceA-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.1] quit
[DeviceA-ospf-1] quit
```

# 在 Device B 上使能指定网段的 OSPF 路由功能。

```
<DeviceB> system-view
[DeviceB] ospf
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] area 3
[DeviceB-ospf-1-area-0.0.0.3] network 10.3.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.3] quit
[DeviceB-ospf-1] quit
```

# 在 Device C 上使能指定网段的 OSPF 路由功能。

```
<DeviceC> system-view
[DeviceC] ospf
[DeviceC-ospf-1] area 2
[DeviceC-ospf-1-area-0.0.0.2] network 10.2.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.2] network 192.168.3.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.2] quit
[DeviceC-ospf-1] quit
```

# 在 Device D 上使能指定网段的 OSPF 路由功能。

```
<DeviceD> system-view
[DeviceD] ospf
[DeviceD-ospf-1] area 3
[DeviceD-ospf-1-area-0.0.0.3] network 10.3.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] network 192.168.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] network 192.168.2.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] quit
[DeviceD-ospf-1] quit
```

# 在 Device E 上使能指定网段的 OSPF 路由功能。

```
<DeviceE> system-view
[DeviceE] ospf
[DeviceE-ospf-1] area 1
[DeviceE-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.1] quit
[DeviceE-ospf-1] quit
```

### 3.4.3 配置 RIP 网络的基本功能

# 在 Device E 上使能指定网段的 RIP 功能。

```
<DeviceE> system-view
```

```
[DeviceE] rip
[DeviceE-rip-1] version 2
[DeviceE-rip-1] undo summary
[DeviceE-rip-1] network 10.5.1.0 0.0.0.255
[DeviceE-rip-1] quit
```

# 在 Device F 上使能指定网段的 RIP 功能。

```
<DeviceF> system-view
[DeviceF] rip
[DeviceF-rip-1] version 2
[DeviceF-rip-1] undo summary
[DeviceF-rip-1] network 10.5.1.0 0.0.0.255
[DeviceF-rip-1] network 192.168.4.0 0.0.0.255
[DeviceF-rip-1] network 192.168.5.0 0.0.0.255
[DeviceF-rip-1] quit
```

### 3.4.4 将 RIP 路由和 OSPF 路由互相引入

# 在 Device E 上将直连路由和 OSPF 路由引入到 RIP 网络中。

```
<DeviceE> system-view
[DeviceE] rip
[DeviceE-rip-1] import-route direct
[DeviceE-rip-1] import-route ospf
[DeviceE-rip-1] quit
```

# 在 Device E 上将直连路由和 RIP 路由引入到 OSPF 网络中。

```
[DeviceE] ospf
[DeviceE-ospf-1] import-route direct
[DeviceE-ospf-1] import-route rip
[DeviceE-ospf-1] quit
```

# 查看 Device E 的路由表信息。

```
[Device E]display ip routing-table
```

```
Destinations : 24 Routes : 24
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	OSPF	10	2	10.4.1.1	GE1/0/1
10.2.1.0/24	OSPF	10	2	10.4.1.1	GE1/0/1
10.3.1.0/24	OSPF	10	3	10.4.1.1	GE1/0/1
10.4.1.0/24	Direct	0	0	10.4.1.2	GE1/0/1
10.4.1.0/32	Direct	0	0	10.4.1.2	GE1/0/1
10.4.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.4.1.255/32	Direct	0	0	10.4.1.2	GE1/0/1
10.5.1.0/24	Direct	0	0	10.5.1.1	GE1/0/2
10.5.1.0/32	Direct	0	0	10.5.1.1	GE1/0/2
10.5.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.5.1.255/32	Direct	0	0	10.5.1.1	GE1/0/2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0

127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.1/32	OSPF	10	3	10.4.1.1	GE1/0/1
192.168.2.1/32	OSPF	10	3	10.4.1.1	GE1/0/1
192.168.3.1/32	OSPF	10	2	10.4.1.1	GE1/0/1
192.168.4.0/24	RIP	100	1	10.5.1.2	GE1/0/2
192.168.5.0/24	RIP	100	1	10.5.1.2	GE1/0/2
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表明 **Device E** 拥有路由域内所有网段路由，然后依次查看其他所有设备的路由表信息，路由域内所有的网段均可互通。

### 3.4.5 配置 OSPF 的路由过滤功能

# 在 **Device C** 上创建基本 ACL 并匹配需要拒绝访问的目的网段 192.168.2.0/24。

```
<DeviceC> system-view
[DeviceC] acl number 2000
[DeviceC-acl-basic-2000] rule 0 deny source 192.168.2.0 0.0.0.255
[DeviceC-acl-basic-2000] rule permit source any
[DeviceC-acl-basic-2000] quit
```

# 在 **Device C** 上通过指定访问控制列表 ACL 2000 来对要加入到路由表的路由信息进行过滤。

```
[DeviceC] ospf
[DeviceC-ospf-1] filter-policy 2000 import
[DeviceC-ospf-1] quit
```

# 在 **Device D** 上创建基本 ACL 并匹配需要拒绝访问的目的网段 192.168.5.0/24。

```
<DeviceD> system-view
[DeviceD] acl number 2000
[DeviceD-acl-basic-2000] rule 0 deny source 192.168.5.0 0.0.0.255
[DeviceD-acl-basic-2000] rule permit source any
[DeviceD-acl-basic-2000] quit
```

# 在 **Device D** 上通过指定访问控制列表 ACL 2000 来对要加入到路由表的路由信息进行过滤。

```
[DeviceD] ospf
[DeviceD-ospf-1] filter-policy 2000 import
[DeviceD-ospf-1] quit
```

# 在 **Device E** 上创建基本 ACL 并匹配需要拒绝访问的目的网段 192.168.4.0/24。

```
<DeviceE> system-view
[DeviceE] acl number 2000
[DeviceE-acl-basic-2000] rule 0 deny source 192.168.4.0 0.0.0.255
[DeviceE-acl-basic-2000] rule permit source any
[DeviceE-acl-basic-2000] quit
```

# 在 **Device E** 上通过指定访问控制列表 ACL 2000 来对引入 OSPF 的 RIP 路由信息进行过滤。

```
[DeviceE] ospf
[DeviceE-ospf-1] filter-policy 2000 export rip 1
[DeviceE-ospf-1] quit
```



## 3.5 验证配置

# 查看 Device C 的路由表信息。

```
[Device C]display ip routing-table
```

```
Destinations : 22 Routes : 22
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	OSPF	10	2	10.2.1.1	GE1/0/1
10.2.1.0/24	Direct	0	0	10.2.1.2	GE1/0/1
10.2.1.0/32	Direct	0	0	10.2.1.2	GE1/0/1
10.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.255/32	Direct	0	0	10.2.1.2	GE1/0/1
10.3.1.0/24	OSPF	10	3	10.2.1.1	GE1/0/1
10.4.1.0/24	OSPF	10	2	10.2.1.1	GE1/0/1
10.5.1.0/24	OSPF	150	1	10.2.1.1	GE1/0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.1/32	OSPF	10	3	10.2.1.1	GE1/0/1
192.168.3.0/24	Direct	0	0	192.168.3.1	Loop0
192.168.3.0/32	Direct	0	0	192.168.3.1	Loop0
192.168.3.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.3.255/32	Direct	0	0	192.168.3.1	Loop0
192.168.5.0/24	OSPF	150	1	10.2.1.1	GE1/0/1
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表明 Device C 的路由表中已经没有 192.168.2.0/24 网段的路由信息了。

# 在 Device C 上使用源地址 192.168.3.1 Ping 目标地址 192.168.2.1 进行验证。

```
[Device C]ping -a 192.168.3.1 192.168.2.1
```

```
Ping 192.168.2.1 (192.168.2.1) from 192.168.3.1: 56 data bytes, press CTRL_C to break
```

```
Request time out
```

```
Request time out
```

```
Request time out
```

```
Request time out
```

```
Request time out
```

```
--- Ping statistics for 192.168.2.1 ---
```

```
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

以上信息表明 Device C 通过过滤路由表中 192.168.2.0/24 网段的路由信息，使得市场一部所在网段无法访问研发一部所在网段。

# 查看 Device D 的路由表信息。

```
[Device D]display ip routing-table
```

Destinations : 25

Routes : 25

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	OSPF	10	2	10.3.1.1	GE1/0/1
10.2.1.0/24	OSPF	10	3	10.3.1.1	GE1/0/1
10.3.1.0/24	Direct	0	0	10.3.1.2	GE1/0/1
10.3.1.0/32	Direct	0	0	10.3.1.2	GE1/0/1
10.3.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.255/32	Direct	0	0	10.3.1.2	GE1/0/1
10.4.1.0/24	OSPF	10	3	10.3.1.1	GE1/0/1
10.5.1.0/24	OSPF	150	1	10.3.1.1	GE1/0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.0/24	Direct	0	0	192.168.1.1	Loop0
192.168.1.0/32	Direct	0	0	192.168.1.1	Loop0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.255/32	Direct	0	0	192.168.1.1	Loop0
192.168.2.0/24	Direct	0	0	192.168.2.1	Loop1
192.168.2.0/32	Direct	0	0	192.168.2.1	Loop1
192.168.2.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.2.255/32	Direct	0	0	192.168.2.1	Loop1
192.168.3.1/32	OSPF	10	3	10.3.1.1	GE1/0/1
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表明 Device D 的路由表中已经没有 192.168.5.0/24 网段的路由信息了。

# 在 Device D 上使用源地址 192.168.1.1 Ping 目标地址 192.168.5.1 进行验证。

```
[Device D]ping -a 192.168.1.1 192.168.5.1
Ping 192.168.5.1 (192.168.5.1) from 192.168.1.1: 56 data bytes, press CTRL_C to
break
Request time out
Request time out
Request time out
Request time out
Request time out
```

--- Ping statistics for 192.168.5.1 ---

5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss

# 在 Device D 上使用源地址 192.168.2.1 Ping 目标地址 192.168.5.1 进行验证。

```
[Device D] ping -a 192.168.2.1 192.168.5.1
Ping 192.168.5.1 (192.168.5.1) from 192.168.2.1: 56 data bytes, press CTRL_C to
break
Request time out
Request time out
```

```
Request time out
Request time out
Request time out
```

```
--- Ping statistics for 192.168.5.1 ---
```

```
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

以上信息表明 **Device D** 通过过滤路由表中 **192.168.5.0/24** 网段的路由信息，使得研发一部和售后服务部所在网段无法访问市场二部所在网段。

综合 **Device C** 和 **Device D** 的路由表信息，发现路由表中均没有 **192.168.4.0/24** 网段路由信息，说明设备已经将引入 **OSPF** 的 **RIP** 路由中研发二部所在网段过滤掉。

## 3.6 配置文件

- **Device A:**

```
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 area 0.0.0.1
 network 10.4.1.0 0.0.0.255
 area 0.0.0.2
 network 10.2.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 10.4.1.1 255.255.255.0
#
```

- **Device B :**

```
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 area 0.0.0.3
 network 10.3.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
```

```
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.3.1.1 255.255.255.0
#
```

- **Device C :**

```
#
ospf 1
 filter-policy 2000 import
 area 0.0.0.2
 network 10.2.1.0 0.0.0.255
 network 192.168.3.0 0.0.0.255
#
interface LoopBack0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.2.1.2 255.255.255.0
#
acl number 2000
 rule 0 deny source 192.168.2.0 0.0.0.255
 rule 5 permit
#
```

- **Device D :**

```
#
ospf 1
 filter-policy 2000 import
 area 0.0.0.3
 network 10.3.1.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.0
#
interface LoopBack1
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.3.1.2 255.255.255.0
#
acl number 2000
 rule 0 deny source 192.168.5.0 0.0.0.255
 rule 5 permit
#
```

- **Device E:**

```
#
```

```

ospf 1
 import-route direct
 import-route rip 1
 filter-policy 2000 export rip 1
 area 0.0.0.1
 network 10.4.1.0 0.0.0.255
#
rip 1
 undo summary
 version 2
 network 10.5.1.0 0.0.0.255
 import-route direct
 import-route ospf 1
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.4.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.5.1.1 255.255.255.0
#
acl number 2000
 rule 0 deny source 192.168.4.0 0.0.0.255
 rule 5 permit
#

```

- **Device F:**

```

#
rip 1
 undo summary
 version 2
 network 10.5.1.0 0.0.0.255
 network 192.168.4.0
 network 192.168.5.0
#
interface LoopBack0
 ip address 192.168.4.1 255.255.255.0
#
interface LoopBack1
 ip address 192.168.5.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.5.1.2 255.255.255.0
#

```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

# H3C MSR 系列路由器

## IS-IS 配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置注意事项.....	2
3.5 配置步骤.....	3
3.5.1 Router A 的配置.....	3
3.5.2 Router B 的配置.....	3
3.5.3 Router C 的配置.....	3
3.5.4 Router D 的配置.....	4
3.5.5 Router E 的配置.....	5
3.6 验证配置.....	5
3.7 配置文件.....	8
4 相关资料.....	9



# 1 简介

本文档介绍 IS-IS 典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 IS-IS 特性。

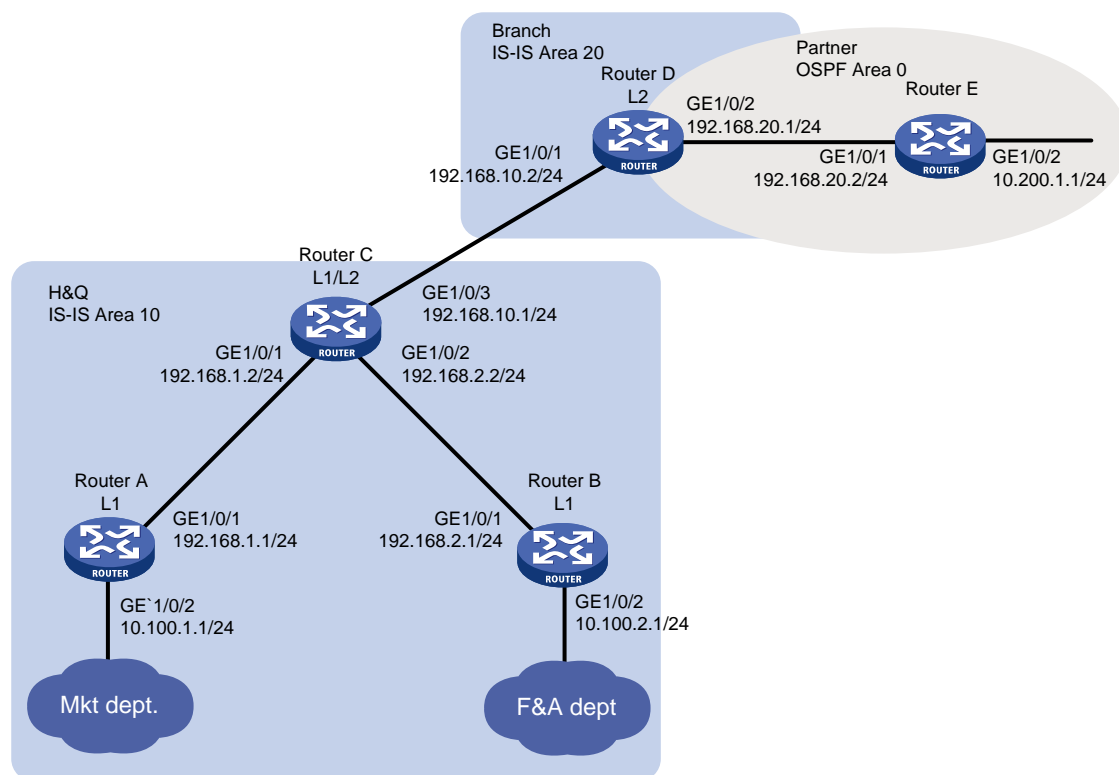
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，某公司总部和分部使用 IS-IS 路由协议进行互联。公司总部内为市场部（Mkt dept.）和财务部（F&A dept.）设置了独立的网络。该公司的合作伙伴使用的是 OSPF 路由协议。现要求：

- 公司总部内市场部和财务部可以通信；并通过配置路由渗透功能，实现总部与分部间，市场部与分部可以正常通信，财务部与分部无法通信，且分部无法查看到财务部的路由信息。
- 将合作伙伴的 OSPF 路由引入公司分部的网络中，并保证市场部与合作伙伴可以通信。
- 当总部的网关设备 Router C IS-IS 协议进程重启时，原有的通信不中断。

图1 IS-IS 配置组网图



## 3.2 配置思路

- 为了实现公司总部内市场部和财务部的相互通信，在 area 10 区域部署 Level-1 路由器。
- 为了使公司总部内财务部和公司分部不能相互通信，且公司分部无法查看财务部的路由，需要在 Router C 上配置 IS-IS 路由渗透并引用地址前缀列表来实现 Level-1 区域只将 10.100.1.0/24 网段的路由信息向 Level-2 发布。
- 为了实现公司总部内市场部与合作伙伴的网络互通，需要在 Router D 的 IS-IS 进程中引入 OSPF 进程的路由，并在 OSPF 进程中引入 IS-IS 进程的路由。
- 为了保证 Router C IS-IS 协议进程重启时，原有的通信不中断，需要在 Router C 上使能 IS-IS 协议的 GR（Graceful Restart，平滑重启）能力。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置注意事项

在设备平滑重启过程中，请勿变更拓扑，否则可能导致路由黑洞。

## 3.5 配置步骤

### 3.5.1 Router A 的配置

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Router A 的其它接口的 IP 地址，具体配置过程略。

# 配置 IS-IS 基本功能。

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.1921.6800.1001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] isis enable 1
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] isis enable 1
[RouterA-GigabitEthernet1/0/2] quit
```

### 3.5.2 Router B 的配置

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address 192.168.2.1 24
[RouterB-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Router B 的其它接口的 IP 地址，具体配置过程略。

# 配置 IS-IS 基本功能。

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] network-entity 10.1921.6800.2001.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] isis enable 1
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] isis enable 1
[RouterB-GigabitEthernet1/0/2] quit
```

### 3.5.3 Router C 的配置

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 1/0/1
```

```
[RouterC-GigabitEthernet1/0/1] ip address 192.168.1.2 24
[RouterC-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Router C 的其它接口的 IP 地址，具体配置过程略。

# 配置 IS-IS 基本功能。

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.1921.6801.0001.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] isis enable 1
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] isis enable 1
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] isis enable 1
[RouterC-GigabitEthernet1/0/3] quit
```

# 配置 IS-IS 路由渗透，并引用名为 1 的地址前缀列表，实现 Level-1 区域只将 10.100.1.0/24 网段的路由信息向 Level-2 发布。

```
[RouterC] ip prefix-list 1 permit 10.100.1.0 24
[RouterC] isis 1
[RouterC-isis-1] address-family ipv4
[RouterC-isis-1-ipv4] import-route isis level-1 into level-2 filter-policy prefix-list 1
[RouterC-isis-1-ipv4] quit
```

# 使能 IS-IS 协议的 GR 能力。

```
[RouterC -isis-1] graceful-restart
[RouterC -isis-1] quit
```

### 3.5.4 Router D 的配置

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterD> system-view
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] ip address 192.168.10.2 24
[RouterD-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Router D 的其它接口的 IP 地址，具体配置过程略。

# 配置 IS-IS 基本功能。

```
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.1921.6802.0001.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] isis enable 1
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] isis enable 1
[RouterD-GigabitEthernet1/0/2] quit
```

# 配置 OSPF 基本功能。

```
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

# 配置 IS-IS 进程引入 OSPF 进程的路由和直连路由。

```
[RouterD] isis 1
[RouterD-isis-1] address-family ipv4
[RouterD-isis-1-ipv4] import-route ospf
[RouterD-isis-1-ipv4] import-route direct
[RouterD-isis-1-ipv4] quit
[RouterD-isis-1] quit
```

# 配置 OSPF 进程引入 IS-IS 进程的路由和直连路由。

```
[RouterD] ospf 1
[RouterD-ospf-1] import-route isis 1
[RouterD-ospf-1] import-route direct
```

### 3.5.5 Router E 的配置

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterE> system-view
[RouterE] interface gigabitethernet 1/0/1
[RouterE-GigabitEthernet1/0/1] ip address 192.168.20.2 24
[RouterE-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Router E 的其它接口的 IP 地址，具体配置过程略。

# 配置 OSPF 基本功能。

```
[RouterE] ospf
[RouterE-ospf-1] area 0
[RouterE-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] network 10.200.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] quit
[RouterE-ospf-1] quit
```

## 3.6 验证配置

- (1) 在 Router D 上查看 IS-IS 路由表，可以查看到市场部（10.100.1.0/24）的路由，无法查看到财务部（10.100.2.0/24）的路由，说明公司分部只能与市场部通信。

```
[RouterD] display isis route

 Route information for IS-IS(1)

 Level-2 IPv4 Forwarding Table

IPv4 Destination IntCost ExtCost ExitInterface NextHop Flags

```

192.168.10.0/24	10	NULL	GE1/0/1	Direct	D/L/-
192.168.1.0/24	20	NULL	GE1/0/1	192.168.10.1	R/-/-
10.100.1.0/24	30	NULL	GE1/0/1	192.168.10.1	R/-/-
192.168.2.0/24	20	NULL	GE1/0/1	192.168.10.1	R/-/-
192.168.20.0/24	10	NULL	GE1/0/2	Direct	D/L/-

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

- (2) 在 Router C 上查看 IS-IS 路由表，可以看到 10.200.1.0/24 的路由，并且可以 ping 通 10.200.1.1，说明本公司与合作伙伴可以正常通信。

# 查看 Router C 上的 IS-IS 路由表。

[RouterC] display isis route

Route information for IS-IS(1)

Level-1 IPv4 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags
192.168.10.0/24	10	NULL	GE1/0/3	Direct	D/L/-
192.168.1.0/24	10	NULL	GE1/0/1	Direct	D/L/-
10.100.1.0/24	20	NULL	GE1/0/1	192.168.1.1	R/L/-
10.100.2.0/24	20	NULL	GE1/0/2	192.168.2.1	R/-/-
192.168.2.0/24	10	NULL	GE1/0/2	Direct	D/L/-

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

Level-2 IPv4 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags
192.168.10.0/24	10	NULL	GE1/0/3	Direct	D/L/-
10.200.1.0/24	10	0	GE1/0/3	192.168.10.2	R/-/-
192.168.20.0/24	10	0	GE1/0/3	192.168.10.2	R/-/-
192.168.1.0/24	10	NULL	GE1/0/1	Direct	D/L/-
192.168.2.0/24	10	NULL	GE1/0/2	Direct	D/L/-

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

# 从 Router C ping 10.200.1.1。

[RouterC] ping 10.200.1.1

Ping 10.200.1.1 (10.200.1.1): 56 data bytes, press CTRL\_C to break

56 bytes from 10.200.1.1: icmp\_seq=0 ttl=254 time=1.862 ms

56 bytes from 10.200.1.1: icmp\_seq=1 ttl=254 time=2.969 ms

56 bytes from 10.200.1.1: icmp\_seq=2 ttl=254 time=1.402 ms

56 bytes from 10.200.1.1: icmp\_seq=3 ttl=254 time=1.324 ms

```
56 bytes from 10.200.1.1: icmp_seq=4 ttl=254 time=1.510 ms
```

```
--- Ping statistics for 10.200.1.1 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 1.324/1.813/2.969/0.606 ms
```

- (3) 在 Router A 上持续 ping Router B, 期间在 Router C 上重启 IS-IS 进程, 查看 Router C 的 IS-IS 协议重启时, 通信是否中断。并使用 **display isis graceful-restart status** 命令, 可查看 Router C 上 IS-IS 协议的 GR 状态。

# 在 Router A 上持续 ping Router B。

```
[RouterA] ping -c 10000 10.100.2.1
```

```
Ping 10.100.2.1 (10.100.2.1): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 10.100.2.1: icmp_seq=0 ttl=254 time=1.185 ms
```

```
56 bytes from 10.100.2.1: icmp_seq=1 ttl=254 time=1.087 ms
```

```
.....
```

# 重启 Router C 的 IS-IS 进程。

```
[RouterC] reset isis all graceful-restart
```

```
Reset IS-IS process? [Y/N] :y
```

# 在 Router A 上查看到 IS-IS 协议重启时通信未发生中断。

```
[RouterA] ping -c 10000 10.100.2.1
```

```
Ping 10.100.2.1 (10.100.2.1): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 10.100.2.1: icmp_seq=0 ttl=254 time=1.185 ms
```

```
56 bytes from 10.100.2.1: icmp_seq=1 ttl=254 time=1.087 ms
```

```
56 bytes from 13.13.13.3: icmp_seq=2 ttl=254 time=1.672 ms
```

```
56 bytes from 13.13.13.3: icmp_seq=3 ttl=254 time=1.751 ms
```

```
56 bytes from 13.13.13.3: icmp_seq=4 ttl=254 time=1.816 ms
```

```
56 bytes from 13.13.13.3: icmp_seq=5 ttl=254 time=1.814 ms
```

# 查看 Router C 上 IS-IS 协议的 GR 状态。

```
[RouterC] display isis graceful-restart status
```

```
Restart information for IS-IS(1)
```

```

```

```
Restart status: COMPLETE
```

```
Restart phase: Finish
```

```
Restart t1: 3, count 10; Restart t2: 60; Restart t3: 300
```

```
SA Bit: supported
```

```
Level-1 restart information
```

```

```

```
Total number of interfaces: 3
```

```
Number of waiting LSPs: 0
```

```
Level-2 restart information
```

```

```

```
Total number of interfaces: 3
```

```
Number of waiting LSPs: 0
```

## 3.7 配置文件

- Router A:

```
#
isis 1
 is-level level-1
 network-entity 10.1921.6800.1001.00
#
interface GigabitEthernet1/0/1
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/2
 ip address 10.100.1.1 255.255.255.0
 isis enable 1
```

- Router B:

```
#
isis 1
 is-level level-1
 network-entity 10.1921.6800.2001.00
#
interface GigabitEthernet1/0/1
 ip address 192.168.2.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/2
 ip address 10.100.2.1 255.255.255.0
 isis enable 1
```

- Router C:

```
#
isis 1
 graceful-restart
 network-entity 10.1921.6801.0001.00
#
address-family ipv4 unicast
 import-route isis level-1 into level-2 filter-policy prefix-list 1
#
interface GigabitEthernet1/0/1
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/2
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
#
```



```
interface GigabitEthernet1/0/3
 ip address 192.168.10.1 255.255.255.0
 isis enable 1
#
 ip prefix-list 1 index 10 permit 10.100.1.0 24
#
```

- **Router D:**

```
#
isis 1
 is-level level-2
 network-entity 20.1921.6802.0001.00
#
 address-family ipv4 unicast
 import-route direct
 import-route ospf 1
#
ospf 1
 import-route direct
 import-route isis 1
 area 0.0.0.0
 network 192.168.20.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 ip address 192.168.10.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/2
 ip address 192.168.20.1 255.255.255.0
#
```

- **Router E:**

```
#
ospf 1
 area 0.0.0.0
 network 10.200.1.0 0.0.0.255
 network 192.168.20.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 ip address 192.168.20.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.200.1.1 255.255.255.0
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-路由命令参考”



# H3C MSR 系列路由器

## OSPFv3 配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 OSPFv3 路由信息过滤配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	2
3.3 配置注意事项.....	2
3.4 配置步骤.....	2
3.4.1 配置各接口的 IP 地址.....	2
3.4.2 配置 OSPFv3 网络的基本功能.....	2
3.4.3 配置 RIPng 网络的基本功能.....	4
3.4.4 将 RIPng 路由和 OSPFv3 路由互相引入.....	4
3.4.5 配置 OSPFv3 的路由过滤功能.....	6
3.5 验证配置.....	7
3.6 配置文件.....	10
4 相关资料.....	12

# 1 简介

本文档介绍了 OSPFv3 路由信息过滤的配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 OSPFv3 路由信息过滤的特性。

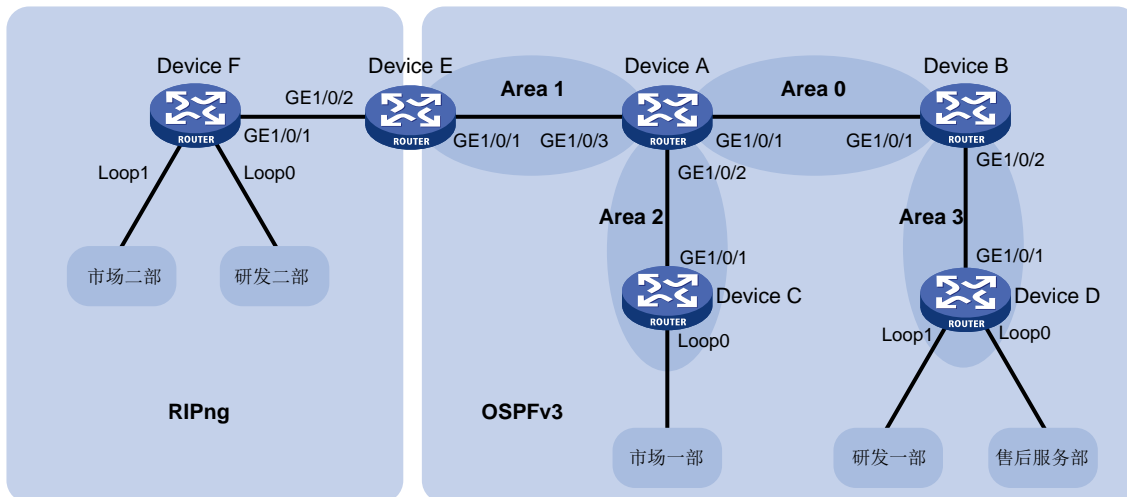
## 3 OSPFv3 路由信息过滤配置举例

### 3.1 组网需求

如图1所示，公司 A 使用 OSPFv3 路由协议实现公司设备全网互通，后来公司 A 扩张兼并了公司 B，要求将公司 B 采用的 RIPng 路由协议与公司 A 的 OSPFv3 协议互相引入，使得各个部门可以实现互通。Device A 和 Device B 作为公司核心设备负责各个部门间的通信。由于业务需要，现要求通过下列措施控制并调整网络中的路由信息：

- 在 Device E 上对引入的路由信息进行过滤，使得研发二部所在网段无法被引入到 OSPFv3 内。
- 在 Device C 上使用路由信息的过滤功能，使得市场一部所在网段无法访问研发一部。
- 在 Device D 上使用路由信息的过滤功能，使得研发一部和售后服务部所在网段无法访问市场二部。

图1 OSPFv3 路由信息过滤组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	1::1/64	Device B	GE1/0/1	1::2/64
	GE1/0/2	2::1/64		GE1/0/2	3::1/64
	GE1/0/3	4::1/64			
Device C	GE1/0/1	2::2/64	Device D	GE1/0/1	3::2/64
	Loop0	13::1/64 (市场一部所在网段)		Loop0	11::1/64 (售后服务部所在网段)
				Loop1	12::1/64 (研发一部所在网段)
Device E	GE1/0/1	4::2/64	Device F	GE1/0/1	5::2/64
	GE1/0/2	5::1/64		Loop0	14::1/64 (研发二部所在网段)
				Loop1	15::1/64 (市场二部所在网段)

## 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.3 配置注意事项

- 路由信息过滤功能中对于引入外部路由信息时采用 **export** 关键字进行过滤，该参数只能在 ASBR 上生效。
- 路由信息过滤功能只是对路由表中相关路由信息过滤，并不是过滤掉 OSPFv3 中通告的 LSA。
- 由于路由通信是双向的，使用路由信息过滤功能将某一目的网段过滤后，该路由器下联的其它网段无法访问这个目的网段的设备，这个目的网段的设备也不能访问源地址网段的设备。
- 使用路由信息过滤功能配合 ACL 使用时，必须将最后一条规则设置为允许所有源地址通过才能避免将所有网段路由被全部过滤掉。
- 配置 OSPFv3 时必须手工指定 Router ID。

## 3.4 配置步骤

### 3.4.1 配置各接口的 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipv6 address 1::1 64
```

# 请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

### 3.4.2 配置 OSPFv3 网络的基本功能

# 创建 OSPFv3 进程，并在 Device A 的接口上使能 OSPFv3 路由功能。

```
<DeviceA> system-view
[DeviceA] ospfv3
[DeviceA-ospfv3-1] router-id 6.6.6.6
[DeviceA-ospfv3-1] quit
```

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ospfv3 1 area 0
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ospfv3 1 area 2
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface GigabitEthernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] ospfv3 1 area 1
[DeviceA-GigabitEthernet1/0/3] quit
```

# 创建 OSPFv3 进程，并在 Device B 的接口上使能 OSPFv3 路由功能。

```
<DeviceB> system-view
[DeviceB] ospfv3
[DeviceB-ospfv3-1] router-id 5.5.5.5
[DeviceB-ospfv3-1] quit
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ospfv3 1 area 0
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface GigabitEthernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ospfv3 1 area 3
[DeviceB-GigabitEthernet1/0/2] quit
```

# 创建 OSPFv3 进程，并在 Device C 的接口上使能 OSPFv3 路由功能。

```
<DeviceC> system-view
[DeviceC] ospfv3
[DeviceC-ospfv3-1] router-id 4.4.4.4
[DeviceC-ospfv3-1] quit
[DeviceC] interface GigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ospfv3 1 area 2
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface LoopBack 0
[DeviceC-LoopBack0] ospfv3 1 area 2
[DeviceC-LoopBack0] quit
```

# 创建 OSPFv3 进程，并在 Device D 的接口上使能 OSPFv3 路由功能。

```
<DeviceD> system-view
[DeviceD] ospfv3
[DeviceD-ospfv3-1] router-id 3.3.3.3
[DeviceD-ospfv3-1] quit
[DeviceD] interface GigabitEthernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] ospfv3 1 area 3
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface LoopBack 0
[DeviceD-LoopBack0] ospfv3 1 area 3
[DeviceD-LoopBack0] quit
[DeviceD] interface LoopBack 1
[DeviceD-LoopBack0] ospfv3 1 area 3
[DeviceD-LoopBack0] quit
```

# 创建 OSPFv3 进程，并在 Device E 的接口上使能 OSPFv3 路由功能。

```
<DeviceE> system-view
```

```
[DeviceE] ospfv3
[DeviceE-ospfv3-1] router-id 2.2.2.2
[DeviceE-ospfv3-1] quit
[DeviceE] interface GigabitEthernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] ospfv3 1 area 1
[DeviceE-GigabitEthernet1/0/1] quit
```

### 3.4.3 配置 RIPng 网络的基本功能

# 创建 RIPng 进程，并在 Device E 的接口上使能 RIPng 路由功能。

```
<DeviceE> system-view
[DeviceE] ripng
[DeviceE-ripng-1] quit
[DeviceE] interface GigabitEthernet 1/0/2
[DeviceE-GigabitEthernet1/0/1] ripng 1 enable
[DeviceE-GigabitEthernet1/0/1] quit
```

# 创建 RIPng 进程，并在 Device F 的接口上使能 RIPng 路由功能。

```
<DeviceF> system-view
[DeviceF] ripng
[DeviceF-ripng-1] quit
[DeviceF] interface GigabitEthernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] ripng 1 enable
[DeviceF-GigabitEthernet1/0/1] quit
[DeviceF] interface LoopBack 0
[DeviceF-LoopBack0] ripng 1 enable
[DeviceF-LoopBack0] quit
[DeviceF] interface LoopBack 1
[DeviceF-LoopBack0] ripng 1 enable
[DeviceF-LoopBack0] quit
```

### 3.4.4 将 RIPng 路由和 OSPFv3 路由互相引入

# 在 Device E 上将直连路由和 OSPFv3 路由引入到 RIPng 网络中。

```
<DeviceE> system-view
[DeviceE] ripng
[DeviceE-ripng-1] import-route direct
[DeviceE-ripng-1] import-route ospfv3
[DeviceE-ripng-1] quit
```

# 在 Device E 上将直连路由和 RIPng 路由引入到 OSPFv3 网络中。

```
[DeviceE] ospfv3
[DeviceE-ospfv3-1] import-route direct
[DeviceE-ospfv3-1] import-route ripng
[DeviceE-ospfv3-1] quit
```

# 查看 Device E 的路由表信息。

```
[Device E]display ipv6 routing-table
```

```
Destinations : 15 Routes : 15
```



Destination: ::1/128	Protocol : Direct
NextHop : ::1	Preference: 0
Interface : InLoop0	Cost : 0
Destination: 1::/64	Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:124D	Preference: 10
Interface : GE1/0/1	Cost : 2
Destination: 2::/64	Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:124D	Preference: 10
Interface : GE1/0/1	Cost : 2
Destination: 3::/64	Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:124D	Preference: 10
Interface : GE1/0/1	Cost : 3
Destination: 4::/64	Protocol : Direct
NextHop : ::	Preference: 0
Interface : GE1/0/1	Cost : 0
Destination: 4::2/128	Protocol : Direct
NextHop : ::1	Preference: 0
Interface : InLoop0	Cost : 0
Destination: 5::/64	Protocol : Direct
NextHop : ::	Preference: 0
Interface : GE1/0/2	Cost : 0
Destination: 5::1/128	Protocol : Direct
NextHop : ::1	Preference: 0
Interface : InLoop0	Cost : 0
Destination: 11::1/128	Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:124D	Preference: 10
Interface : GE1/0/1	Cost : 3
Destination: 12::1/128	Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:124D	Preference: 10
Interface : GE1/0/1	Cost : 3
Destination: 13::1/128	Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:124D	Preference: 10
Interface : GE1/0/1	Cost : 2
Destination: 14::/64	Protocol : RIPng
NextHop : FE80::2E0:FCFF:FE11:19B5	Preference: 100
Interface : GE1/0/2	Cost : 1

```

Destination: 15::/64 Protocol : RIPng
NextHop : FE80::2E0:FCFF:FE11:19B5 Preference: 100
Interface : GE1/0/2 Cost : 1

Destination: FE80::/10 Protocol : Direct
NextHop : :: Preference: 0
Interface : InLoop0 Cost : 0

Destination: FF00::/8 Protocol : Direct
NextHop : :: Preference: 0
Interface : NULL0

```

以上显示信息表明 **Device E** 拥有路由域内所有网段路由，然后依次查看其他所有设备的路由表信息，路由域内所有的网段均可互通。

### 3.4.5 配置 OSPFv3 的路由过滤功能

# 在 **Device C** 上创建基本 IPv6 ACL 并匹配需要拒绝访问的目的网段 12::1/64。

```

<DeviceC> system-view
[DeviceC] acl ipv6 number 2000
[DeviceC-acl6-basic-2000] rule 0 deny source 12::1 64
[DeviceC-acl6-basic-2000] rule permit source any
[DeviceC-acl6-basic-2000] quit

```

# 在 **Device C** 上通过指定访问控制列表 IPv6 ACL 2000 来对要加入到路由表的路由信息进行过滤。

```

[DeviceC] ospfv3
[DeviceC-ospfv3-1] filter-policy 2000 import
[DeviceC-ospfv3-1] quit

```

# 在 **Device D** 上创建基本 IPv6 ACL 并匹配需要拒绝访问的目的网段 15::1/64。

```

<DeviceD> system-view
[DeviceD] acl ipv6 number 2000
[DeviceD-acl6-basic-2000] rule 0 deny source 15::1 64
[DeviceD-acl6-basic-2000] rule permit source any
[DeviceD-acl6-basic-2000] quit

```

# 在 **Device D** 上通过指定访问控制列表 IPv6 ACL 2000 来对要加入到路由表的路由信息进行过滤。

```

[DeviceD] ospfv3
[DeviceD-ospfv3-1] filter-policy 2000 import
[DeviceD-ospfv3-1] quit

```

# 在 **Device E** 上创建基本 IPv6 ACL 并匹配需要拒绝访问的目的网段 14::1/64。

```

<DeviceE> system-view
[DeviceE] acl ipv6 number 2000
[DeviceE-acl6-basic-2000] rule 0 deny source 14::1 64
[DeviceE-acl6-basic-2000] rule permit source any
[DeviceE-acl6-basic-2000] quit

```

# 在 **Device E** 上通过指定访问控制列表 IPv6 ACL 2000 来对引入 OSPFv3 的 RIPng 路由信息进行过滤。

```

[DeviceE] ospfv3
[DeviceE-ospfv3-1] filter-policy 2000 export ripng 1
[DeviceE-ospfv3-1] quit

```

## 3.5 验证配置

# 查看 Device C 的路由表信息。

```
[DeviceC]display ipv6 routing-table
```

```
Destinations : 13 Routes : 13
```

```
Destination: ::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0
```

```
Destination: 1::/64 Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:1245 Preference: 10
Interface : GE1/0/1 Cost : 2
```

```
Destination: 2::/64 Protocol : Direct
NextHop : :: Preference: 0
Interface : GE1/0/1 Cost : 0
```

```
Destination: 2::2/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0
```

```
Destination: 3::/64 Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:1245 Preference: 10
Interface : GE1/0/1 Cost : 3
```

```
Destination: 4::/64 Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:1245 Preference: 10
Interface : GE1/0/1 Cost : 2
```

```
Destination: 5::/64 Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:1245 Preference: 150
Interface : GE1/0/1 Cost : 1
```

```
Destination: 11::1/128 Protocol : OSPFv3
NextHop : FE80::2E0:FCFF:FE58:1245 Preference: 10
Interface : GE1/0/1 Cost : 3
```

```
Destination: 13::/64 Protocol : Direct
NextHop : :: Preference: 0
Interface : Loop0 Cost : 0
```

```
Destination: 13::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0
```

```
Destination: 15::/64 Protocol : OSPFv3
```

```

NextHop : FE80::2E0:FCFF:FE58:1245 Preference: 150
Interface : GE1/0/1 Cost : 1

Destination: FE80::/10 Protocol : Direct
NextHop : :: Preference: 0
Interface : InLoop0 Cost : 0

Destination: FF00::/8 Protocol : Direct
NextHop : :: Preference: 0
Interface : NULL0

```

以上显示信息表明 **Device C** 的路由表中已经没有 **12::/64** 网段的路由信息了。

**#** 在 **Device C** 上使用源地址 **13::1** Ping 目标地址 **12::1** 进行验证。

```

[DeviceC]ping ipv6 -a 13::1 12::1
Ping6(56 data bytes) 13::1 --> 12::1, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

```

```

--- Ping6 statistics for 12::1 ---

```

```

5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss

```

以上信息表明 **Device C** 通过过滤路由表中 **12::/64** 网段的路由信息，使得市场一部所在网段无法访问研发一部所在网段。

**#** 查看 **Device D** 的路由表信息。

```

[DeviceD]display ipv6 routing-table

```

```

Destinations : 14 Routes : 14

```

```

Destination: ::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: 1::/64 Protocol : OSPFv3
NextHop : FE80::2A0:FCFF:FE00:5815 Preference: 10
Interface : GE1/0/1 Cost : 2

Destination: 2::/64 Protocol : OSPFv3
NextHop : FE80::2A0:FCFF:FE00:5815 Preference: 10
Interface : GE1/0/1 Cost : 3

Destination: 3::/64 Protocol : Direct
NextHop : :: Preference: 0
Interface : GE1/0/1 Cost : 0

Destination: 3::3/128 Protocol : Direct
NextHop : ::1 Preference: 0

```

```

Interface : InLoop0 Cost : 0

Destination: 4::/64 Protocol : OSPFv3
NextHop : FE80::2A0:FCFF:FE00:5815 Preference: 10
Interface : GE1/0/1 Cost : 3

Destination: 5::/64 Protocol : OSPFv3
NextHop : FE80::2A0:FCFF:FE00:5815 Preference: 150
Interface : GE1/0/1 Cost : 1

Destination: 11::/64 Protocol : Direct
NextHop : :: Preference: 0
Interface : Loop0 Cost : 0

Destination: 11::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: 12::/64 Protocol : Direct
NextHop : :: Preference: 0
Interface : Loop1 Cost : 0

Destination: 12::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0

Destination: 13::1/128 Protocol : OSPFv3
NextHop : FE80::2A0:FCFF:FE00:5815 Preference: 10
Interface : GE1/0/1 Cost : 3

Destination: FE80::/10 Protocol : Direct
NextHop : :: Preference: 0
Interface : NULL0 Cost : 0

Destination: FF00::/8 Protocol : Direct
NextHop : :: Preference: 0
Interface : NULL0

```

以上显示信息表明 **Device D** 的路由表中已经没有 **15::/64** 网段的路由信息了。

**#** 在 **Device D** 上使用源地址 **11::1** Ping 目标地址 **15::1** 进行验证。

```

[DeviceD]ping ipv6 -a 11::1 15::1
Ping6(56 data bytes) 11::1 --> 15::1, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping6 statistics for 15::1 ---

```

```
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

# 在 Device D 上使用源地址 12::1 Ping 目标地址 15::1 进行验证。

```
[DeviceD]ping ipv6 -a 12::1 15::1
Ping6(56 data bytes) 12::1 --> 15::1, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
--- Ping6 statistics for 15::1 ---
```

```
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

以上信息表明 Device D 通过过滤路由表中 15::/64 网段的路由信息，使得研发一部和售后服务部所在网段无法访问市场二部所在网段。

综合 Device C 和 Device D 的路由表信息，发现路由表中均没有 14::/64 网段路由信息，说明设备已经将引入 OSPFv3 的 RIPng 路由中研发二部所在网段过滤掉。

## 3.6 配置文件

- Device A:

```
#
ospfv3 1
router-id 6.6.6.6
area 0.0.0.0
area 0.0.0.1
area 0.0.0.2
#
interface GigabitEthernet1/0/1
ospfv3 1 area 0.0.0.0
ipv6 address 1::1/64
#
interface GigabitEthernet1/0/2
ospfv3 1 area 0.0.0.2
ipv6 address 2::1/64
#
interface GigabitEthernet1/0/3
ospfv3 1 area 0.0.0.1
ipv6 address 4::1/64
#
```

- Device B :

```
#
ospfv3 1
router-id 5.5.5.5
area 0.0.0.0
area 0.0.0.2
area 0.0.0.3
#
```

```

interface GigabitEthernet1/0/1
 ospfv3 1 area 0.0.0.0
 ipv6 address 1::2/64
#
interface GigabitEthernet1/0/2
 ospfv3 1 area 0.0.0.3
 ipv6 address 3::1/64
#

```

- **Device C :**

```

#
ospfv3 1
 router-id 4.4.4.4
 filter-policy 2000 import
 area 0.0.0.2
#
interface LoopBack0
 ospfv3 1 area 0.0.0.2
 ipv6 address 13::1/64
#
interface GigabitEthernet1/0/1
 ospfv3 1 area 0.0.0.2
 ipv6 address 2::2/64
#
acl ipv6 number 2000
 rule 0 deny source 12::/64
 rule 5 permit
#

```

- **Device D :**

```

#
ospfv3 1
 router-id 3.3.3.3
 filter-policy 2000 import
 area 0.0.0.3
#
interface LoopBack0
 ospfv3 1 area 0.0.0.3
 ipv6 address 11::1/64
#
interface LoopBack1
 ospfv3 1 area 0.0.0.3
 ipv6 address 12::1/64
#
interface GigabitEthernet1/0/1
 ospfv3 1 area 0.0.0.3
 ipv6 address 3::3/64
#
acl ipv6 number 2000
 rule 0 deny source 15::/64
#

```

- ```

    rule 5 permit
#

```
- **Device E:**

```

#
ospfv3 1
  router-id 2.2.2.2
  import-route direct
import-route ripng 1
  filter-policy 2000 export ripng 1
  area 0.0.0.1
#
ripng 1
  import-route direct
  import-route ospfv3 1
#
interface GigabitEthernet1/0/1
  ospfv3 1 area 0.0.0.1
  ipv6 address 4::2/64
#
interface GigabitEthernet1/0/2
  ipv6 address 5::1/64
  ripng 1 enable
#
acl ipv6 number 2000
  rule 0 deny source 14::/64
  rule 5 permit
#

```
 - **Device F:**

```

#
ripng 1
#
interface LoopBack0
  ipv6 address 14::1/64
  ripng 1 enable
#
interface LoopBack1
  ipv6 address 15::1/64
  ripng 1 enable
#
interface GigabitEthernet1/0/1
  ipv6 address 5::2/64
  ripng 1 enable
#

```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”

- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

H3C MSR 系列路由器

IPv6 IS-IS 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

| | |
|-------------------------|---|
| 1 简介..... | 1 |
| 2 配置前提..... | 1 |
| 3 配置举例..... | 1 |
| 3.1 组网需求..... | 1 |
| 3.2 配置思路..... | 2 |
| 3.3 使用版本..... | 2 |
| 3.4 配置步骤..... | 2 |
| 3.4.1 Router A 的配置..... | 2 |
| 3.4.2 Router B 的配置..... | 3 |
| 3.4.3 Router C 的配置..... | 3 |
| 3.4.4 Router D 的配置..... | 4 |
| 3.4.5 Router E 的配置..... | 5 |
| 3.5 验证配置..... | 5 |
| 3.6 配置文件..... | 7 |
| 4 相关资料..... | 9 |

1 简介

本文档介绍 IPv6 IS-IS 典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 IPv6 IS-IS 特性。

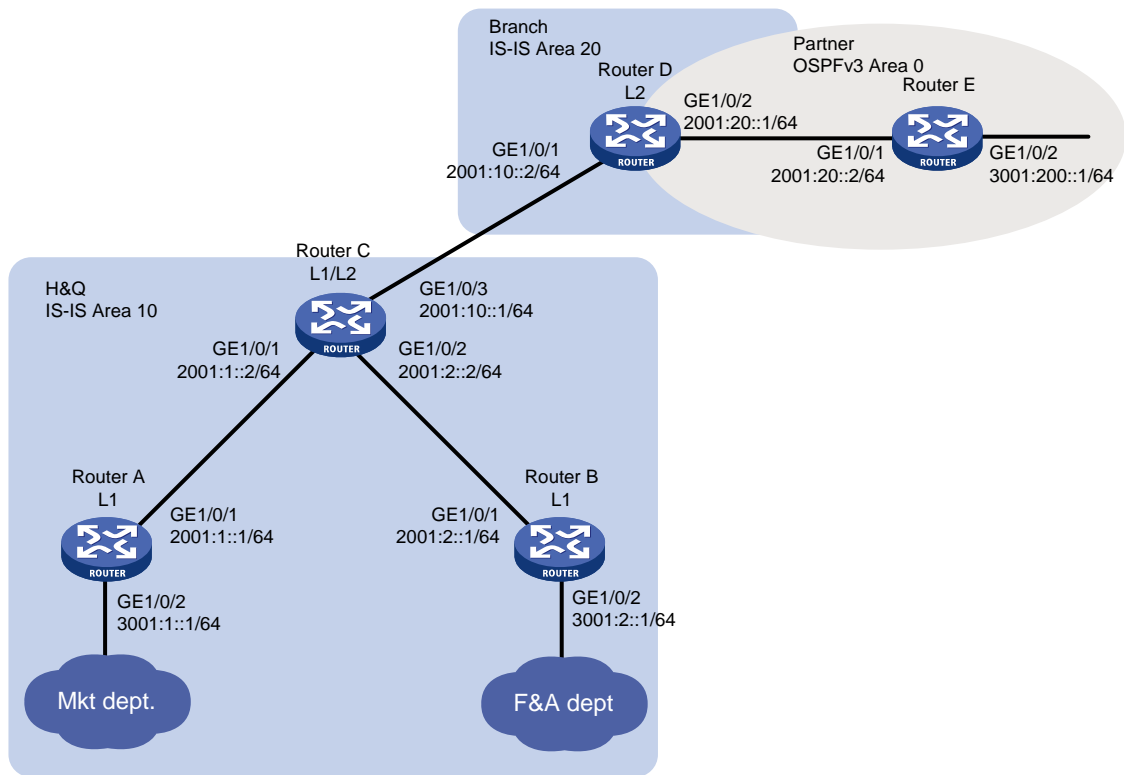
3 配置举例

3.1 组网需求

如[图 1](#)所示，某公司总部和分部使用 IPv6 IS-IS 路由协议进行互联。公司总部内为市场部(Mkt dept.)和财务部(F&A dept.)设置了独立的网络。该公司的合作伙伴使用的是 OSPFv3 路由协议。现要求：

- 公司总部内市场部和财务部可以通信；并通过配置路由渗透功能，实现总部与分部间，市场部分部可以正常通信，财务部与分部无法通信，且分部无法查看到财务部的路由信息。
- 将合作伙伴的 OSPFv3 路由引入公司分部的网络中，并保证市场部与合作伙伴可以通信。

图1 IPv6 IS-IS 配置组网图



3.2 配置思路

- 为了实现公司总部内市场部和财务部的相互通信，在 area 10 区域部署 Level-1 路由器。
- 为了使公司总部内财务部和公司分部不能相互通信，且公司分部无法查看财务部的路由，需要在 Router C 上配置 IS-IS 路由渗透并引用地址前缀列表来实现 Level-1 区域只将 3001:1::/64 网段的路由信息向 Level-2 发布。
- 为了实现公司总部内市场部与合作伙伴的网络互通，需要在 Router D 的 IS-IS 进程中引入 OSPF 进程的路由，并在 OSPF 进程中引入 IS-IS 进程的路由。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置步骤

3.4.1 Router A 的配置

配置接口 GigabitEthernet1/0/1 的 IPv6 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ipv6 address 2001:1::1 64
```

```
[RouterA-GigabitEthernet1/0/1] quit
# 请参考以上方法配置图 1 中 Router A 的其它接口的 IPv6 地址，具体配置过程略。
# 配置 IS-IS 基本功能。
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.3001.0001.0001.00
[RouterA-isis-1] address-family ipv6 unicast
[RouterA-isis-1-ipv6] quit
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] isis ipv6 enable 1
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] isis ipv6 enable 1
[RouterA-GigabitEthernet1/0/2] quit
```

3.4.2 Router B 的配置

```
# 配置接口 GigabitEthernet1/0/1 的 IPv6 地址。
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ipv6 address 2001:2::1 64
[RouterB-GigabitEthernet1/0/1] quit
# 请参考以上方法配置图 1 中 Router B 的其它接口的 IPv6 地址，具体配置过程略。
# 配置 IS-IS 基本功能。
[RouterB] isis 1
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] network-entity 10.3001.0002.0001.00
[RouterB-isis-1] address-family ipv6 unicast
[RouterB-isis-1-ipv6] quit
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] isis ipv6 enable 1
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] isis ipv6 enable 1
[RouterB-GigabitEthernet1/0/2] quit
```

3.4.3 Router C 的配置

```
# 配置接口 GigabitEthernet1/0/1 的 IPv6 地址。
<RouterC> system-view
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] ipv6 address 2001:1::2 64
[RouterC-GigabitEthernet1/0/1] quit
# 请参考以上方法配置图 1 中 Router C 的其它接口的 IPv6 地址，具体配置过程略。
# 配置 IS-IS 基本功能。
```

```

[RouterC] isis 1
[RouterC-isis-1] network-entity 10.2001.0010.0001.00
[RouterC-isis-1] address-family ipv6 unicast
[RouterC-isis-1-ipv6] quit
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] isis ipv6 enable 1
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] isis ipv6 enable 1
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] isis ipv6 enable 1
[RouterC-GigabitEthernet1/0/3] quit
# 配置 IPv6 IS-IS 路由渗透，并引用名为 1 的地址前缀列表，实现 Level-1 区域只将 3001:1::/64 网
段的路由信息向 Level-2 发布。
[RouterC] ipv6 prefix-list 1 permit 3001:1:: 64
[RouterC] isis 1
[RouterC-isis-1] address-family ipv6
[RouterC-isis-1-ipv6] import-route isisv6 level-1 into level-2 filter-policy prefix-list 1
[RouterC-isis-1-ipv6] quit
[RouterC-isis-1] quit

```

3.4.4 Router D 的配置

配置接口 GigabitEthernet1/0/1 的 IPv6 地址。

```

<RouterD> system-view
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] ipv6 address 2001:10::2 64
[RouterD-GigabitEthernet1/0/1] quit

```

请参考以上方法配置图 1 中 Router D 的其它接口的 IPv6 地址，具体配置过程略。

配置 IPv6 IS-IS 基本功能。

```

[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.2001.0020.0001.00
[RouterD-isis-1] address-family ipv6 unicast
[RouterD-isis-1-ipv6] quit
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] isis ipv6 enable 1
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] isis ipv6 enable 1
[RouterD-GigabitEthernet1/0/2] quit

```

配置 OSPFv3 基本功能。

```

[RouterD] ospfv3
[RouterD-ospfv3-1] router-id 4.4.4.4

```

```

[RouterD-ospfv3-1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] ospfv3 1 area 0
[RouterD-GigabitEthernet1/0/2] quit
# 配置 IPv6 IS-IS 进程引入 OSPFv3 进程的路由和直连路由。
[RouterD] isis 1
[RouterD-isis-1] address-family ipv6
[RouterD-isis-1-ipv6] import-route ospfv3
[RouterD-isis-1-ipv6] import-route direct
[RouterD-isis-1-ipv6] quit
[RouterD-isis-1] quit
# 配置 OSPFv3 进程引入 IPv6 IS-IS 进程的路由和直连路由。
[RouterD] ospfv3 1
[RouterD-ospfv3-1] import-route isisv6 1
[RouterD-ospfv3-1] import-route direct

```

3.4.5 Router E 的配置

```

# 配置接口 GigabitEthernet1/0/1 的 IPv6 地址。
<RouterE> system-view
[RouterE] interface gigabitethernet 1/0/1
[RouterE-GigabitEthernet1/0/1] ipv6 address 2001:20::2 64
[RouterE-GigabitEthernet1/0/1] quit
# 请参考以上方法配置图 1 中 Router E 的其它接口的 IPv6 地址，具体配置过程略。
# 配置 OSPFv3 基本功能。
[RouterE] ospfv3
[RouterE-ospfv3-1] router-id 5.5.5.5
[RouterE-ospfv3-1] quit
[RouterE] interface gigabitethernet 1/0/1
[RouterE-GigabitEthernet1/0/1] ospfv3 1 area 0
[RouterE-GigabitEthernet1/0/1] quit
[RouterE] interface gigabitethernet 1/0/2
[RouterE-GigabitEthernet1/0/2] ospfv3 1 area 0
[RouterE-GigabitEthernet1/0/2] quit

```

3.5 验证配置

- (1) 在 Router D 上查看 IPv6 IS-IS 路由表，可以查看到市场部（3001:1::/64）的路由，无法查看到财务部（3001:2::/64）的路由，说明公司分部只能与市场部通信。

```

[RouterD] display isis route ipv6

Route information for IS-IS(1)
-----

Level-2 IPv6 Forwarding Table
-----

```



```

Destination : 2001:10::                PrefixLen: 64
Flag        : D/L/-                    Cost      : 10
Next Hop    : Direct                   Interface: GE1/0/1

Destination : 2001:1::                  PrefixLen: 64
Flag        : R/-/-                    Cost      : 20
Next Hop    : FE80::7625:8AFF:FE02:4D13 Interface: GE1/0/1

Destination : 2001:2::                  PrefixLen: 64
Flag        : R/-/-                    Cost      : 20
Next Hop    : FE80::7625:8AFF:FE02:4D13 Interface: GE1/0/1

Destination : 3001:1::                PrefixLen: 64
Flag        : R/-/-                    Cost      : 30
Next Hop    : FE80::7625:8AFF:FE02:4D13 Interface: GE1/0/1

```

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set

- (2) 在 Router C 上查看 IPv6 IS-IS 路由表，可以看到 3001:200::1/64 的路由，并且可以 ping 通 3001:200::1，说明本公司与合作伙伴可以正常通信。

查看 Router C 上的 IPv6 IS-IS 路由表。

```
[RouterC] display isis route ipv6 level-2
```

```

Route information for IS-IS(1)
-----

Level-2 IPv6 Forwarding Table
-----

Destination : 2001:10::                PrefixLen: 64
Flag        : D/L/-                    Cost      : 10
Next Hop    : Direct                   Interface: GE1/0/3

Destination : 2001:1::                  PrefixLen: 64
Flag        : D/L/-                    Cost      : 10
Next Hop    : Direct                   Interface: GE1/0/1

Destination : 2001:2::                  PrefixLen: 64
Flag        : D/L/-                    Cost      : 10
Next Hop    : Direct                   Interface: GE1/0/2

Destination : 2001:20::                 PrefixLen: 64
Flag        : R/L/-                    Cost      : 20
Next Hop    : FE80::BAAF:67FF:FE30:3304 Interface: GE1/0/3

Destination : 3001:200::                PrefixLen: 64
Flag        : R/-/-                    Cost      : 20
Next Hop    : FE80::BAAF:67FF:FE30:3304 Interface: GE1/0/3

```

```

Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
# 从 Router C ping 3001:200::1。
[RouterC] ping ipv6 3001:200::1
Ping6(56 data bytes) 2001:10::1 --> 3001:200::1, press CTRL_C to break
56 bytes from 3001:200::1, icmp_seq=0 hlim=63 time=7.230 ms
56 bytes from 3001:200::1, icmp_seq=1 hlim=63 time=3.449 ms
56 bytes from 3001:200::1, icmp_seq=2 hlim=63 time=2.779 ms
56 bytes from 3001:200::1, icmp_seq=3 hlim=63 time=2.652 ms
56 bytes from 3001:200::1, icmp_seq=4 hlim=63 time=2.558 ms

--- Ping6 statistics for 3001:200::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.558/3.734/7.230/1.776 ms

```

3.6 配置文件

- Router A:

```

#
isis 1
  is-level level-1
  network-entity 10.3001.0001.0001.00
#
address-family ipv6 unicast
#
interface GigabitEthernet1/0/1
  isis ipv6 enable 1
  ipv6 address 2001:1::1/64
#
interface GigabitEthernet1/0/2
  isis ipv6 enable 1
  ipv6 address 3001:1::1/64
#

```

- Router B:

```

#
isis 1
  is-level level-1
  network-entity 10.3001.0002.0001.00
#
address-family ipv6 unicast
#
interface GigabitEthernet1/0/1
  isis ipv6 enable 1
  ipv6 address 2001:2::1/64
#
interface GigabitEthernet1/0/2
  isis ipv6 enable 1
  ipv6 address 3001:2::1/64

```

- ```

#
• Router C:
#
isis 1
 network-entity 10.2001.0010.0001.00
#
 address-family ipv6 unicast
 import-route isisv6 level-1 into level-2 filter-policy prefix-list 1
#
interface GigabitEthernet1/0/1
 isis ipv6 enable 1
 ipv6 address 2001:1::2/64
#
interface GigabitEthernet1/0/2
 isis ipv6 enable 1
 ipv6 address 2001:2::2/64
#
interface GigabitEthernet1/0/3
 isis ipv6 enable 1
 ipv6 address 2001:10::1/64
#
 ipv6 prefix-list 1 index 10 permit 3001:1:: 64
#
• Router D:
#
isis 1
 is-level level-2
 network-entity 20.2001.0020.0001.00
#
 address-family ipv6 unicast
 import-route direct
 import-route ospfv3 1
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
 import-route direct
 import-route isisv6 1
#
interface GigabitEthernet1/0/1
 isis ipv6 enable 1
 ipv6 address 2001:10::2/64
#
interface GigabitEthernet1/0/2
 ospfv3 1 area 0.0.0.0
 ipv6 address 2001:20::1/64
#
• Router E:

```

```
#
ospfv3 1
 router-id 5.5.5.5
 area 0.0.0.0
#
interface GigabitEthernet1/0/1
 ospfv3 1 area 0
 ipv6 address 2001:20::2/64
#
interface GigabitEthernet1/0/2
 ospfv3 1 area 0
 ipv6 address 3001:200::1/64
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-路由命令参考”

# H3C MSR 系列路由器

## BGP 基础配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 IPv4 BGP 基础配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	1
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.5.1 配置各接口的 IP 地址.....	2
3.5.2 配置 IBGP 连接.....	3
3.5.3 配置 EBGP 连接.....	4
3.5.4 配置 Router B 发布本地网段路由.....	6
3.6 验证配置.....	6
3.7 配置文件.....	7
4 BGP 与 IGP 交互配置举例.....	8
4.1 组网需求.....	8
4.2 配置思路.....	9
4.3 使用版本.....	9
4.4 配置注意事项.....	9
4.5 配置步骤.....	9
4.5.1 配置各接口的 IP 地址.....	9
4.5.2 配置 OSPF.....	10
4.5.3 配置 EBGP 连接.....	11
4.5.4 配置 BGP 与 IGP 交互.....	11
4.6 验证配置.....	12
4.7 配置文件.....	14
5 相关资料.....	15

# 1 简介

本文档介绍了 BGP 路由协议基础配置的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

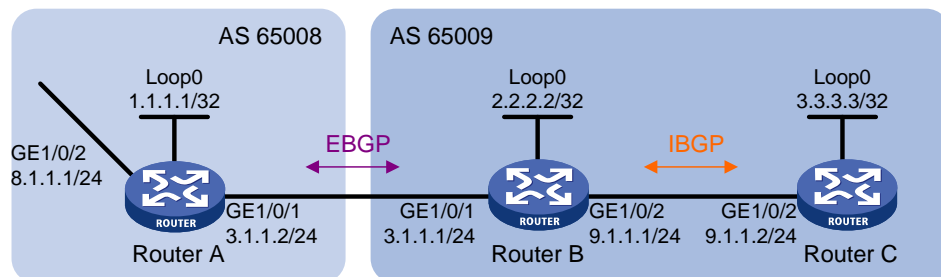
本文档假设您已了解 BGP 特性。

## 3 IPv4 BGP 基础配置举例

### 3.1 组网需求

如图 1 所示，Router A 和 Router B 之间建立 EBGP 连接，Router B 和 Router C 之间建立 IBGP 连接。现要求：Router C 能够访问 Router A 直连的 8.1.1.0/24 网段。

图1 BGP 基础配置组网图



### 3.2 配置思路

- 在 AS 65009 内部，保证 Router B 到 Router C 的 LoopBack 接口路由可达，Router C 到 Router B 的 LoopBack 接口路由可达，这样两个 IBGP 对等体才能建立 TCP 连接，本案例使用 OSPF 协议实现。
- 由于设备缺省情况下 BGP 不发布任何本地的网段路由，为了使 Router C 能够访问 Router A 直连的 8.1.1.0/24 网段，将 8.1.1.0/24 网段宣告进 Router A 的 BGP 进程中，将 3.1.1.0/24 网段和 9.1.1.0/24 网段宣告进 Router B 的 BGP 进程中。

### 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置注意事项

- 为了防止端口状态不稳定引起路由震荡，本举例使用 LoopBack 接口来创建 IBGP 对等体。
- 使用 LoopBack 接口创建 IBGP 对等体时，因为 LoopBack 接口不是两对等体实际连接的接口，所以，必须使用 **peer connect-interface** 命令将 LoopBack 接口配置为 BGP 连接的源接口。
- EBGP 邻居关系的两台路由器，处于不同的 AS 域，对端的 LoopBack 接口一般路由不可达，所以一般使用直连地址建立 EBGP 邻居。

## 3.5 配置步骤

### 3.5.1 配置各接口的 IP 地址

# 配置 Router A 接口 IP 地址。

```
<RouterA> system-view
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 1.1.1.1 255.255.255.255
[RouterA-LoopBack0] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] port link-mode route
[RouterA-GigabitEthernet1/0/1] ip address 3.1.1.2 255.255.255.0
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] port link-mode route
[RouterA-GigabitEthernet1/0/2] ip address 8.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/2] quit
```

# 配置 Router B 接口 IP 地址。

```
<RouterB> system-view
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 2.2.2.2 255.255.255.255
[RouterB-LoopBack0] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] port link-mode route
[RouterB-GigabitEthernet1/0/1] ip address 3.1.1.1 255.255.255.0
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet01//2] port link-mode route
[RouterB-GigabitEthernet1/0/2] ip address 9.1.1.1 255.255.255.0
[RouterB-GigabitEthernet1/0/2] quit
```

# 配置 Router C 接口 IP 地址。

```
<RouterC> system-view
[RouterC] interface loopback 0
[RouterC-LoopBack0] ip address 3.3.3.3 255.255.255.255
[RouterC-LoopBack0] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] port link-mode route
```



```
[RouterC-GigabitEthernet1/0/2] ip address 9.1.1.2 255.255.255.0
[RouterC-GigabitEthernet1/0/2] quit
```

## 3.5.2 配置 IBGP 连接

### (1) Router B 的配置

# 在 BGP 视图下，配置 Router ID 为 2.2.2.2。

```
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
```

# 创建 IBGP 对等体 3.3.3.3，使用接口 LoopBack0 作为建立 TCP 连接的源接口。

```
[RouterB-bgp] peer 3.3.3.3 as-number 65009
[RouterB-bgp] peer 3.3.3.3 connect-interface loopback 0
```

# 创建并进入 BGP IPv4 单播地址族视图，使能与对等体 3.3.3.3 交换 IPv4 单播路由信息的能力。

```
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] peer 3.3.3.3 enable
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

# 配置 OSPF 路由协议，保证路由器之间路由可达。

```
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

### (2) Router C 的配置

# 在 BGP 视图下，配置 Router ID 为 3.3.3.3。

```
[RouterC] bgp 65009
[RouterC-bgp] router-id 3.3.3.3
```

# 创建 IBGP 对等体 2.2.2.2，使用接口 LoopBack0 作为建立 TCP 连接的源接口。

```
[RouterC-bgp] peer 2.2.2.2 as-number 65009
[RouterC-bgp] peer 2.2.2.2 connect-interface loopback 0
```

# 创建并进入 BGP IPv4 单播地址族视图，使能与对等体 2.2.2.2 交换 IPv4 单播路由信息的能力。

```
[RouterC-bgp] address-family ipv4 unicast
[RouterC-bgp-ipv4] peer 2.2.2.2 enable
[RouterC-bgp-ipv4] quit
[RouterC-bgp] quit
```

# 配置 OSPF 路由协议，保证各路由器之间路由可达。

```
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

# 显示所有 BGP IPv4 单播对等体的简要信息，以 Router C 为例。

```
[RouterC] display bgp peer ipv4

BGP local router ID : 3.3.3.3
Local AS number : 65009
Total number of peers : 1 Peers in established state : 1

Peer AS MsgRcvd MsgSent OutQ PrefRcv Up/Down State

2.2.2.2 65009 2 2 0 0 00:00:13 Established
```

以上显示信息表明 Router B 和 Router C 之间的 IBGP 连接已经建立。

### 3.5.3 配置 EBGP 连接

#### (1) Router A 的配置

# 在 BGP 视图下，配置 Router ID 为 1.1.1.1。

```
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
在 BGP 视图下，创建 EBGP 对等体 3.1.1.1，指定对等体的 AS 号为 65009。
[RouterA-bgp] peer 3.1.1.1 as-number 65009
```

# 创建并进入 BGP IPv4 单播地址族视图，使能与对等体 3.1.1.1 交换 IPv4 单播路由信息的能力。

```
[RouterA-bgp] address-family ipv4 unicast
[RouterA-bgp-ipv4] peer 3.1.1.1 enable
将本地路由表中到达 8.1.1.0/24 网段的路由添加到 BGP 路由表中。
[RouterA-bgp-ipv4] network 8.1.1.0 24
[RouterA-bgp-ipv4] quit
[RouterA-bgp] quit
```

#### (2) Router B 的配置

# 在 BGP 视图下，创建 EBGP 对等体 3.1.1.2，指定对等体的 AS 号为 65008。

```
[RouterB] bgp 65009
[RouterB-bgp] peer 3.1.1.2 as-number 65008
```

# 创建并进入 BGP IPv4 单播地址族视图，使能与对等体 3.1.1.2 交换 IPv4 单播路由信息的能力。

```
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] peer 3.1.1.2 enable
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

# 查看 Router B 的 BGP 对等体的连接状态。

```
[RouterB] display bgp peer ipv4

BGP local router ID : 2.2.2.2
Local AS number : 65009
Total number of peers : 2 Peers in established state : 2

Peer AS MsgRcvd MsgSent OutQ PrefRcv Up/Down State

2.2.2.2 65009 2 2 0 0 00:00:13 Established
```

```

3.3.3.3 65009 4 4 0 0 00:02:49 Established
3.1.1.2 65008 2 2 0 0 00:00:05 Established

```

可以看出，Router B 与 Router C、Router B 与 Router A 之间的 BGP 连接均已建立。

# 查看 Router A 的 BGP 路由表。

```
[RouterA] display bgp routing-table ipv4
```

```
Total number of routes: 1
```

```
BGP local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - dampened, h - history,
 s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* > 8.1.1.0/24	8.1.1.1	0		32768	i

# 查看 Router B 的 BGP 路由表。

```
[RouterB] display bgp routing-table ipv4
```

```
Total number of routes: 1
```

```
BGP local router ID is 2.2.2.2
```

```
Status codes: * - valid, > - best, d - dampened, h - history,
 s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >e 8.1.1.0/24	3.1.1.2	0		0	65008i

# 查看 Router C 的 BGP 路由表。

```
[RouterC] display bgp routing-table ipv4
```

```
Total number of routes: 1
```

```
BGP local router ID is 3.3.3.3
```

```
Status codes: * - valid, > - best, d - dampened, h - history,
 s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
i 8.1.1.0/24	3.1.1.2	0	100	0	65008i

从路由表可以看出，Router A 没有学到 AS 65009 内部的任何路由，Router C 虽然学到了 AS 65008 中的 8.1.1.0 的路由，但因为下一跳 3.1.1.2 不可达，所以也不是有效路由。

### 3.5.4 配置 Router B 发布本地网段路由

# 创建并进入 BGP IPv4 单播地址族视图。

```
[RouterB] bgp 65009
[RouterB-bgp] address-family ipv4 unicast
```

# 配置 BGP 发布本地网段路由，以便 Router A 能够获取到网段 9.1.1.0/24 的路由，Router C 能够获取到网段 3.1.1.0/24 的路由。

```
[RouterB-bgp-ipv4] network 3.1.1.0 24
[RouterB-bgp-ipv4] network 9.1.1.0 24
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

# 查看 Router A 的 BGP 路由表。

```
[RouterA] display bgp routing-table ipv4
```

Total number of routes: 3

BGP local router ID is 1.1.1.1

Status codes: \* - valid, > - best, d - dampened, h - history,  
s - suppressed, S - stale, i - internal, e - external  
Origin: i - IGP, e - EGP, ? - incomplete

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >e 3.1.1.0/24	3.1.1.1	0		0	65009?
* > 8.1.1.0/24	8.1.1.1	0		32768	i
* >e 9.1.1.0/24	3.1.1.1	0		0	65009i

以上显示信息表明，在 Router B 上发布本地网段路由后，Router A 新增了到达 9.1.1.0/24 的路由。

# 查看 Router C 的 BGP 路由表。

```
[RouterC] display bgp routing-table ipv4
```

Total number of routes: 3

BGP local router ID is 3.3.3.3

Status codes: \* - valid, > - best, d - dampened, h - history,  
s - suppressed, S - stale, i - internal, e - external  
Origin: i - IGP, e - EGP, ? - incomplete

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >i 3.1.1.0/24	2.2.2.2	0	100	0	?
* >i 8.1.1.0/24	3.1.1.2	0	100	0	65008i
* >i 9.1.1.0/24	2.2.2.2	0	100	0	i

以上显示信息表明，到 8.1.1.0 的路由变为有效路由，下一跳为 Router A 的地址。

## 3.6 验证配置

# 使用 Ping 命令，在 Router C 上 ping Router A 的直连网段地址 8.1.1.1。

```
[RouterC] ping 8.1.1.1
Ping 8.1.1.1 (8.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=254 time=3.000 ms

--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/4.800/10.000/2.638 ms
以上信息表明 Router C 能够访问 Router A 直连的 8.1.1.0/24 网段。
```

### 3.7 配置文件

- Router A:

```
#
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/1
 ip address 3.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 8.1.1.1 255.255.255.0
#
bgp 65008
 router-id 1.1.1.1
 peer 3.1.1.1 as-number 65009
#
 address-family ipv4 unicast
 network 8.1.1.0 255.255.255.0
 peer 3.1.1.1 enable
#
```

- Router B:

```
#
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet1/0/1
 ip address 3.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 9.1.1.1 255.255.255.0
#
bgp 65009
 router-id 2.2.2.2
 peer 3.1.1.2 as-number 65008
```

```

peer 3.3.3.3 as-number 65009
peer 3.3.3.3 connect-interface Loopback0
#
address-family ipv4 unicast
network 3.1.1.0 24
network 9.1.1.0 24
peer 3.1.1.2 enable
peer 3.3.3.3 enable
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 9.1.1.0 0.0.0.255
#

```

- Router C:

```

#
interface Loopback0
ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet1/0/2
ip address 9.1.1.2 255.255.255.0
#
bgp 65009
router-id 3.3.3.3
peer 2.2.2.2 as-number 65009
peer 2.2.2.2 connect-interface Loopback0
#
address-family ipv4 unicast
peer 2.2.2.2 enable
#
ospf 1
area 0.0.0.0
network 3.3.3.3 0.0.0.0
network 9.1.1.0 0.0.0.255
#

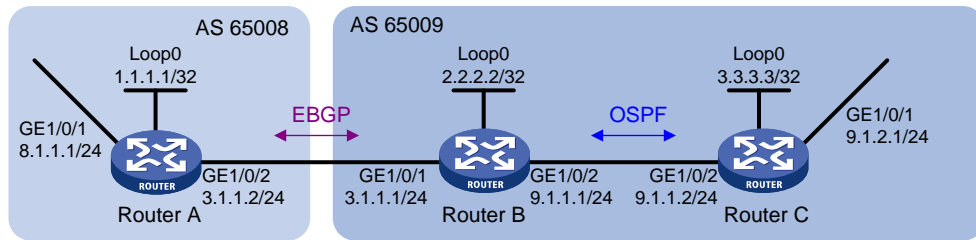
```

## 4 BGP 与 IGP 交互配置举例

### 4.1 组网需求

如图 2 所示，Router A 和 Router B 之间建立 EBGP 连接，Router B 和 Router C 之间建立 OSPF 连接。现要求：Router A 的直连网段 8.1.1.0/24 和 Router C 的直连网段 9.1.2.0/24 能够互访。

图2 BGP 与 IGP 交互配置组网图



## 4.2 配置思路

- 在 AS 65009 内部，保证 Router B 到 Router C 的 LoopBack 接口路由可达，Router C 到 Router B 的 LoopBack 接口路由可达，这样两个 IBGP 对等体才能建立 TCP 连接，本案例使用 OSPF 协议实现。
- 在 Router B 上将 BGP 和 OSPF 路由互相引入，使得 Router A 可以访问 9.1.2.0/24 网段，Router C 可以访问 8.1.1.0/24 网段。

## 4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.4 配置注意事项

- 为了防止端口状态不稳定引起路由震荡，本举例使用 LoopBack 接口来创建 IBGP 对等体。
- 使用 LoopBack 接口创建 IBGP 对等体时，因为 LoopBack 接口不是两对等体实际连接的接口，所以，必须使用 `peer connect-interface` 命令将 LoopBack 接口配置为 BGP 连接的源接口。
- EBGP 邻居关系的两台路由器，处于不同的 AS 域，对端的 LoopBack 接口一般路由不可达，所以一般使用直连地址建立 EBGP 邻居。

## 4.5 配置步骤

### 4.5.1 配置各接口的 IP 地址

# 配置 Router A 接口 IP 地址。

```
<RouterA> system-view
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 1.1.1.1 255.255.255.255
[RouterA-LoopBack0] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] port link-mode route
[RouterA-GigabitEthernet1/0/1] ip address 8.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] port link-mode route
[RouterA-GigabitEthernet1/0/2] ip address 3.1.1.2 255.255.255.0
[RouterA-GigabitEthernet1/0/2] quit
```

**# 配置 Router B 接口 IP 地址。**

```
<RouterB> system-view
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 2.2.2.2 255.255.255.255
[RouterB-LoopBack0] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] port link-mode route
[RouterB-GigabitEthernet1/0/1] ip address 3.1.1.1 255.255.255.0
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] port link-mode route
[RouterB-GigabitEthernet1/0/2] ip address 9.1.1.1 255.255.255.0
[RouterB-GigabitEthernet1/0/2] quit
```

**# 配置 Router C 接口 IP 地址。**

```
<RouterC> system-view
[RouterC] interface loopback 0
[RouterC-LoopBack0] ip address 3.3.3.3 255.255.255.255
[RouterC-LoopBack0] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] port link-mode route
[RouterC-GigabitEthernet1/0/1] ip address 9.1.2.1 255.255.255.0
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] port link-mode route
[RouterC-GigabitEthernet1/0/2] ip address 9.1.1.2 255.255.255.0
[RouterC-GigabitEthernet1/0/2] quit
```

## 4.5.2 配置 OSPF

### (1) Router B 的配置

**# 配置 OSPF 路由协议，保证各路由器之间路由可达。**

```
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

### (2) Router C 的配置

**# 配置 OSPF 路由协议，保证各路由器之间路由可达。**

```
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 9.1.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
```



```
[RouterC-ospf-1] quit
```

### 4.5.3 配置 EBGP 连接

#### (1) Router A 的配置

# 在 BGP 视图下，配置 Router ID 为 2.2.2.2。

```
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
```

# 在 BGP 视图下，创建 EBGP 对等体 3.1.1.1，指定对等体的 AS 号为 65009。

```
[RouterA-bgp] peer 3.1.1.1 as-number 65009
```

# 创建并进入 BGP IPv4 单播地址族视图，使能与对等体 3.1.1.1 交换 IPv4 单播路由信息的能力。

```
[RouterA-bgp] address-family ipv4 unicast
[RouterA-bgp-ipv4] peer 3.1.1.1 enable
```

# 将 8.1.1.0/24 网段通告到 BGP 路由表中，以便 Router B 获取到网段 8.1.1.0/24 的路由。

```
[RouterA-bgp-ipv4] network 8.1.1.0 24
[RouterA-bgp-ipv4] quit
```

```
[RouterA-bgp] quit
```

#### (2) Router B 的配置

# 在 BGP 视图下，配置 Router ID 为 2.2.2.2。

```
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
```

# 在 BGP 视图下，创建 EBGP 对等体 3.1.1.2，指定对等体的 AS 号为 65008。

```
[RouterB-bgp] peer 3.1.1.2 as-number 65008
```

# 创建并进入 BGP IPv4 单播地址族视图，使能与对等体 3.1.1.2 交换 IPv4 单播路由信息的能力。

```
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] peer 3.1.1.2 enable
```

```
[RouterB-bgp-ipv4] quit
```

```
[RouterB-bgp] quit
```

### 4.5.4 配置 BGP 与 IGP 交互

# 进入 BGP IPv4 单播地址族视图，将 OSPF 路由重分布到 BGP 路由中。

```
[RouterB] bgp 65009
[RouterB-bgp] address-family ipv4 unicast
```

```
[RouterB-bgp-ipv4] import-route ospf 1
```

```
[RouterB-bgp-ipv4] quit
```

```
[RouterB-bgp] quit
```

# 进入 OSPF 视图，将 BGP 路由重分布到 OSPF 路由中。

```
[RouterB] ospf 1
[RouterB-ospf-1] import-route bgp
```

```
[RouterB-ospf-1] quit
```

# 查看 Router A 的 BGP 路由表。

```
[RouterA] display bgp routing-table ipv4
```

Total number of routes: 3

BGP local router ID is 1.1.1.1

Status codes: \* - valid, > - best, d - dampened, h - history,  
s - suppressed, S - stale, i - internal, e - external  
Origin: i - IGP, e - EGP, ? - incomplete

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >	8.1.1.0/24	8.1.1.1	0		32768	i
* >e	9.1.2.0/24	3.1.1.1	1		0	65009?

# 查看 RouterC 的 OSPF 路由表。

[RouterC] display ospf routing

OSPF Process 1 with Router ID 3.3.3.3  
Routing Tables

Routing for Network

Destination	Cost	Type	NextHop	AdvRouter	Area
9.1.1.0/24	1	Transit	9.1.1.2	3.3.3.3	0.0.0.0
9.1.2.0/24	1	Stub	9.1.2.1	192.168.0.63	0.0.0.0
2.2.2.2/32	1	Stub	9.1.1.1	2.2.2.2	0.0.0.0

Routing for ASEs

Destination	Cost	Type	Tag	NextHop	AdvRouter
8.1.1.0/24	1	Type2	1	9.1.1.1	2.2.2.2

Total Nets: 3

Intra Area: 2 Inter Area: 0 ASE: 1 NSSA: 0

从 Router A 的 BGP 路由表和 Router C 的 OSPF 路由表可以看出, Switch B 上的 BGP 和 OSPF 已经互相引入。

## 4.6 验证配置

# 在 Router A 上使用源地址 8.1.1.1 Ping 目标地址 9.1.2.1 进行验证。

[RouterA] ping -a 8.1.1.1 9.1.2.1

Ping 9.1.2.1 (9.1.2.1) from 8.1.1.1: 56 data bytes, press CTRL\_C to break

56 bytes from 9.1.2.1: icmp\_seq=0 ttl=254 time=10.000 ms

56 bytes from 9.1.2.1: icmp\_seq=1 ttl=254 time=12.000 ms

56 bytes from 9.1.2.1: icmp\_seq=2 ttl=254 time=2.000 ms

56 bytes from 9.1.2.1: icmp\_seq=3 ttl=254 time=7.000 ms

56 bytes from 9.1.2.1: icmp\_seq=4 ttl=254 time=9.000 ms

--- Ping statistics for 9.1.2.1 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss

round-trip min/avg/max/std-dev = 2.000/8.000/12.000/3.406 ms

# 在 Router C 上使用源地址 9.1.2.1 Ping 目标地址 8.1.1.1 进行验证。

```
[RouterC] ping -a 9.1.2.1 8.1.1.1
Ping 8.1.1.1 (8.1.1.1) from 9.1.2.1: 56 data bytes, press CTRL_C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=254 time=9.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=254 time=3.000 ms
```

```
--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/4.400/9.000/2.332 ms
```

上述显示信息说明网段 9.1.2.0/24 与网段 8.1.1.0/24 能实现互通。

**# 在 Router A 上使用源地址 8.1.2.1 分别 Ping 目标地址 9.1.2.1 和 9.1.3.1 进行验证。**

```
[RouterA] ping -a 8.1.2.1 9.1.2.1
Ping 9.1.2.1 (9.1.2.1) from 8.1.2.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
--- Ping statistics for 9.1.2.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

```
[RouterA] ping -a 8.1.2.1 9.1.3.1
Ping 9.1.3.1 (9.1.3.1) from 8.1.2.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
--- Ping statistics for 9.1.3.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

**# 在 Router C 上使用源地址 9.1.3.1 分别 Ping 目标地址 8.1.1.1 和 8.1.2.1 进行验证。**

```
[RouterC] ping -a 9.1.3.1 8.1.1.1
Ping 8.1.1.1 (8.1.1.1) from 9.1.3.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

```
[RouterC] ping -a 9.1.3.1 8.1.2.1
Ping 8.1.2.1 (8.1.2.1) from 9.1.3.1: 56 data bytes, press CTRL_C to break
```

```
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
--- Ping statistics for 8.1.2.1 ---
```

```
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

上述信息说明两个自治区域之间只有网段 9.1.2.0/24 与网段 8.1.1.0/24 能实现互通，其他网段之间是无法互通的。

## 4.7 配置文件

- Router A:

```
#
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/1
 ip address 8.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 ip address 3.1.1.2 255.255.255.0
#
bgp 65008
 router-id 1.1.1.1
 peer 3.1.1.1 as-number 65009
#
 address-family ipv4 unicast
 network 8.1.1.0 255.255.255.0
 peer 3.1.1.1 enable
#
```

- Router B:

```
#
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet1/0/1
 ip address 3.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 9.1.1.1 255.255.255.0
#
bgp 65009
 router-id 2.2.2.2
 peer 3.1.1.2 as-number 65008
#
 address-family ipv4 unicast
```

```
import-route ospf 1
peer 3.1.1.2 enable
#
ospf 1
import-route bgp
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 9.1.1.0 0.0.0.255
#
```

- **Router C:**

```
#
interface Loopback0
ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet1/0/1
ip address 9.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
ip address 9.1.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 9.1.1.0 0.0.0.255
network 9.1.2.0 0.0.0.255
#
```

## 5 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

# H3C MSR 系列路由器

## 路由策略配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置步骤.....	2
3.4.1 配置各接口的 IP 地址.....	2
3.4.2 在 AS 100 内配置 OSPF 基本功能，保证设备间路由可达.....	2
3.4.3 配置 BGP 基本功能.....	3
3.4.4 配置路由策略.....	6
3.5 验证配置.....	7
3.6 配置文件.....	8
4 相关资料.....	11

# 1 简介

本文档介绍 MSR 系列路由器路由策略典型配置举例。

路由策略是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。

# 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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路由策略特性。

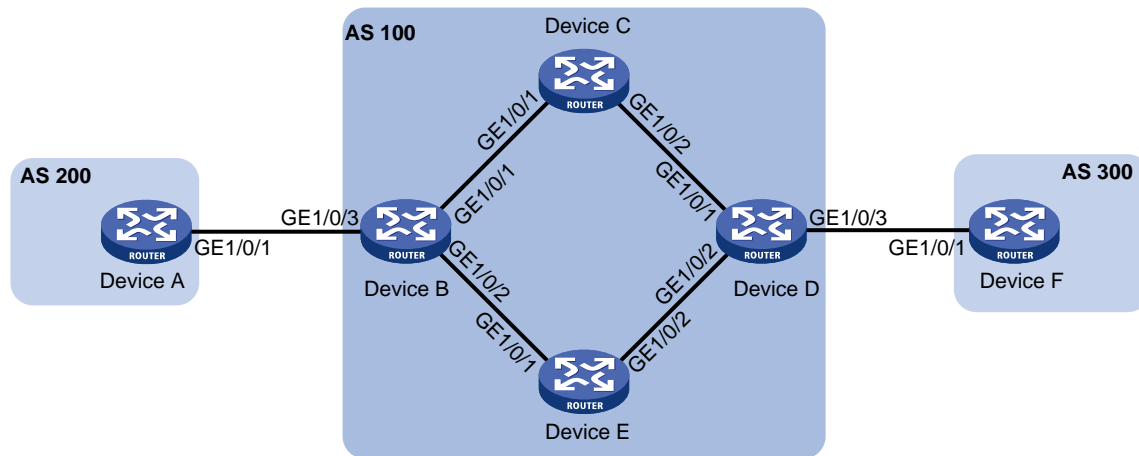
# 3 配置举例

## 3.1 组网需求

如图 1 所示，某公司的两个部门相距较远，Device A 和 Device F 分别作为这两个部门的出口设备，AS 100 内部使用 OSPF 作为 IGP。现要求：

- 通过部署 BGP，使两个部门可以通信；
- 通过配置路由策略，将 Device B<->Device C<->Device D 链路作为主链路，负责转发 Device A 和 Device F 之间的流量；当主链路断开时，自动切换到 Device B<->Device E<->Device D 这条路径进行通信。

图1 路由策略配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	120.1.0.1/24	Device D	GE1/0/1	10.2.0.101/24
Device B	GE1/0/1	10.1.0.101/24		GE1/0/2	13.1.1.101/24
	GE1/0/2	192.168.0.101/24		GE1/0/3	120.2.0.2/24



设备	接口	IP地址	设备	接口	IP地址
	GE1/0/3	120.1.0.2/24	Device E	GE1/0/1	192.168.0.102/24
Device C	GE1/0/1	10.1.0.102/24		GE1/0/2	13.1.1.102/24
	GE1/0/2	10.2.0.102/24	Device F	GE1/0/1	120.2.0.1/24

## 3.2 配置思路

- 为了使 Device B<->Device C<->Device D 成为主链路，需要：
  - 在 Device B 上配置路由策略来调整 AS 100 前往 AS 200 两条路径的本地优先级
    - Device D-> Device C-> Device B 的本地优先级为 200;
    - Device D-> Device E-> Device B 的本地优先级为缺省值 100;
  - 在 Device D 上配置路由策略来调整 AS 100 前往 AS 300 两条路径的本地优先级
    - Device B-> Device C-> Device D 的本地优先级为 200;
    - Device B-> Device E-> Device D 的本地优先级为缺省值 100。
- 为了使 AS 100 内通信的报文使用 BGP 而不是 OSPF 选路，需要将 IBGP 路由优先级配置高于 OSPF 路由优先级。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置步骤

### 3.4.1 配置各接口的 IP 地址

# 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 120.1.0.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

#请参考以上方法配置其它相关接口的 IP 地址，配置步骤这里省略。

### 3.4.2 在 AS 100 内配置 OSPF 基本功能，保证设备间路由可达

#### 1. 配置 Device B

```
<DeviceB> system-view
[DeviceB] ospf
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

## 2. 配置 Device C

```
<DeviceC> system-view
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

## 3. 配置 Device D

```
<DeviceD> system-view
[DeviceD] ospf
[DeviceD-ospf-1] import-route direct
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

## 4. 配置 Device E

```
<DeviceE> system-view
[DeviceE] ospf
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

### 3.4.3 配置 BGP 基本功能

#### 1. 配置 Device A

# 启动 BGP，指定本地 AS 号为 200，指定 BGP 路由器的 Router ID 为 1.1.1.1。

```
<DeviceA> system-view
[DeviceA] bgp 200
[DeviceA-bgp] router-id 1.1.1.1
```

# 配置 Device A 和 Device B 建立 EBGP 连接。

```
[DeviceA-bgp] peer 120.1.0.2 as-number 100
```

# 创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

```
[DeviceA-bgp] address-family ipv4 unicast
```

# 使能 Device A 与对等体 120.1.0.2 交换 IPv4 单播路由信息的能力。

```
[DeviceA-bgp-ipv4] peer 120.1.0.2 enable
```

# 在 BGP IPv4 单播地址族视图下，将本地路由表中到达 120.1.0.0/24 网段的路由添加到 BGP 路由表中。

```
[DeviceA-bgp-ipv4] network 120.1.0.0 255.255.255.0
[DeviceA-bgp-ipv4] quit
[DeviceA-bgp] quit
```

## 2. 配置 Device B

# 启动 BGP，指定本地 AS 号为 100，指定 BGP 路由器的 Router ID 为 2.2.2.2。

```
<DeviceB> system-view
```

```
[DeviceB] bgp 100
```

```
[DeviceB-bgp] router-id 2.2.2.2
```

# 配置 Device B 和 Device A 建立 EBGP 连接。

```
[DeviceB-bgp] peer 120.1.0.1 as-number 200
```

# 配置 Device B 和 Device D 建立 IBGP 连接。

```
[DeviceB-bgp] peer 10.2.0.101 as-number 100
```

```
[DeviceB-bgp] peer 13.1.1.101 as-number 100
```

# 创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

```
[DeviceB-bgp] address-family ipv4 unicast
```

# 使能 Device B 与对等体 10.2.0.101 交换 IPv4 单播路由信息的能力。

```
[DeviceB-bgp-ipv4] peer 10.2.0.101 enable
```

# 在 BGP IPv4 单播地址族视图下，配置向对等体 10.2.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。

```
[DeviceB-bgp-ipv4] peer 10.2.0.101 next-hop-local
```

# 使能 Device B 与对等体 13.1.1.101 交换 IPv4 单播路由信息的能力。

```
[DeviceB-bgp-ipv4] peer 13.1.1.101 enable
```

# 在 BGP IPv4 单播地址族视图下，配置向对等体 13.1.1.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。

```
[DeviceB-bgp-ipv4] peer 13.1.1.101 next-hop-local
```

# 使能 Device B 与对等体 120.1.0.1 交换 IPv4 单播路由信息的能力。

```
[DeviceB-bgp-ipv4] peer 120.1.0.1 enable
```

```
[DeviceB-bgp-ipv4] quit
```

```
[DeviceB-bgp] quit
```

## 3. 配置 Device D

# 启动 BGP，指定本地 AS 号为 100，指定 BGP 路由器的 Router ID 为 4.4.4.4。

```
<DeviceD> system-view
```

```
[DeviceD] bgp 100
```

```
[DeviceD-bgp] router-id 4.4.4.4
```

# 配置 Device D 和 Device B 建立 IBGP 连接。

```
[DeviceD-bgp] peer 10.1.0.101 as-number 100
```

```
[DeviceD-bgp] peer 192.168.0.101 as-number 100
```

# 配置 Device D 和 Device F 建立 EBGP 连接。

```
[DeviceD-bgp] peer 120.2.0.1 as-number 300
```

# 创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

```
[DeviceD-bgp] address-family ipv4 unicast
```

# 使能 Device D 与对等体 10.1.0.101 交换 IPv4 单播路由信息的能力。

```
[DeviceD-bgp-ipv4] peer 10.1.0.101 enable
```

# 在 BGP IPv4 单播地址族视图下，配置向对等体 10.1.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。

```
[DeviceD-bgp-ipv4] peer 10.1.0.101 next-hop-local
```

# 使能 Device D 与对等体 192.168.0.101 交换 IPv4 单播路由信息的能力。

```
[DeviceD-bgp-ipv4] peer 192.168.0.101 enable
在 BGP IPv4 单播地址族视图下，配置向对等体 192.168.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。
[DeviceD-bgp-ipv4] peer 192.168.0.101 next-hop-local
使能 Device D 与对等体 120.2.0.1 交换 IPv4 单播路由信息的能力。
[DeviceD-bgp-ipv4] peer 120.2.0.1 enable
[DeviceD-bgp-ipv4] quit
[DeviceD-bgp] quit
```

#### 4. 配置 Device F

#启动 BGP，指定本地 AS 号为 300，指定 BGP 路由器的 Router ID 为 6.6.6.6。

```
[DeviceF] bgp 300
[DeviceF-bgp] router-id 6.6.6.6
```

# 配置 Device F 和 Device D 建立 EBGP 连接。

```
[DeviceF-bgp] peer 120.2.0.2 as-number 100
```

# 创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

```
[DeviceF-bgp] address-family ipv4 unicast
```

# 在 BGP IPv4 单播地址族视图下，将本地路由表中到达 120.2.0.0/24 网段的路由添加到 BGP 路由表中。

```
[DeviceF-bgp-ipv4] network 120.2.0.0 255.255.255.0
```

# 使能 Device F 与对等体 120.2.0.2 交换 IPv4 单播路由信息的能力。

```
[DeviceF-bgp-ipv4] peer 120.2.0.2 enable
```

```
[DeviceF-bgp-ipv4] quit
```

```
[DeviceF-bgp] quit
```

# 完成以上配置后，在 Device B 上通过命令 **display bgp peer** 查看 BGP 对等体信息。

```
[DeviceB] display bgp peer ipv4
```

```
BGP local router ID: 2.2.2.2
```

```
Local AS number: 100
```

```
Total number of peers: 3
```

```
Peers in established state: 3
```

Peer	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
10.2.0.101	100	6	4	0	1	00:00:56	Established
13.1.1.101	100	6	5	0	1	00:00:56	Established
120.1.0.1	200	6	5	0	1	00:00:56	Established

以上信息可以看到 Device B 与 Device D 建立 IBGP 连接, Device B 与 Device A 建立 EBGP 连接, 且均处于 **Established** 状态。

# 完成以上配置后，从 Device A 上 ping Device F 的 IP 地址。

```
[DeviceA] ping 120.2.0.1
```

```
Ping 120.2.0.1 (120.2.0.1): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=1.189 ms
```

```
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=1.095 ms
```

```
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=1.086 ms
```

```
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=1.097 ms
```

```
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=1.089 ms
```

```
--- Ping statistics for 120.2.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.086/1.111/1.189/0.039 ms
```

以上显示信息表明 Device A 和 Device F 之间路由可达。

### 3.4.4 配置路由策略

#### 1. 配置 Device B

# 创建 ACL 2000，允许源 IP 地址为 120.1.0.0/24 的报文通过。

```
[DeviceB] acl number 2000
[DeviceB-acl-basic-2000] rule permit source 120.1.0.0 0.0.0.255
[DeviceB-acl-basic-2000] quit
```

# 配置路由策略，将从对等体 120.1.0.1 学习到的路由发布给对等体 10.2.0.101 时，设置本地优先级为 200。

```
[DeviceB] route-policy local-pre permit node 10
[DeviceB-route-policy-local-pre-10] if-match ip address acl 2000
[DeviceB-route-policy-local-pre-10] apply local-preference 200
[DeviceB-route-policy-local-pre-10] quit
```

```
[DeviceB] bgp 100
[DeviceB-bgp] address-family ipv4 unicast
[DeviceB-bgp-ipv4] peer 10.2.0.101 route-policy local-pre export
```

# 配置 EBGP 路由优先级为 255，配置 IBGP 路由优先级为 100，配置本地路由优先级为 130，使 IBGP 路由优先级优于 OSPF 路由。

```
[DeviceB-bgp-ipv4] preference 255 100 130
[DeviceB-bgp-ipv4] quit
[DeviceB-bgp] quit
```

#### 2. 配置 Device D

# 创建 ACL 2000，允许源 IP 地址为 120.2.0.0/24 的报文通过。

```
[DeviceD] acl number 2000
[DeviceD-acl-basic-2000] rule permit source 120.2.0.0 0.0.0.255
[DeviceD-acl-basic-2000] quit
```

# 配置路由策略，将从对等体 120.2.0.1 学习到的路由发布给对等体 10.1.0.101 时，设置本地优先级为 200。

```
[DeviceD] route-policy local-pre permit node 10
[DeviceD-route-policy-local-pre-10] if-match ip address acl 2000
[DeviceD-route-policy-local-pre-10] apply local-preference 200
[DeviceD-route-policy-local-pre-10] quit
```

```
[DeviceD] bgp 100
[DeviceD-bgp] address-family ipv4 unicast
[DeviceD-bgp-ipv4] peer 10.1.0.101 route-policy local-pre export
```

#配置 EBGP 路由优先级为 255，配置 IBGP 路由优先级为 100，配置本地路由优先级为 130，使 IBGP 路由优先级优于 OSPF 路由。

```
[DeviceD-bgp-ipv4] preference 255 100 130
[DeviceD-bgp-ipv4] quit
```

```
[DeviceD-bgp] quit
```

### 3.5 验证配置

# 在 Device B 上使用 **display bgp routing-table ipv4** 命令查看 BGP 路由表，可以看到 2 条 120.2.0.0/24 的路由，本地路由优先级分别为 100 和 200。

```
[DeviceB] display bgp routing-table ipv4
```

```
Total number of routes: 3
```

```
BGP local router ID is 2.2.2.2
```

```
Status codes: * - valid, > - best, d - dampened, h - history,
```

```
 s - suppressed, S - stale, i - internal, e - external
```

```
Origin: i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >e 120.1.0.0/24	120.1.0.1	0		0	200i
* >i 120.2.0.0/24	10.2.0.101	0	200	0	300i
* i	13.1.1.101	0	100	0	300i

# 在 Device A 上 **tracert Device F**，查看到报文传输路径是 Device A → Device B → Device C → Device D → Device F。（使用 Tracert 功能时，需要在中间设备（源端与目的端之间的设备）上执行 **ip ttl-expires enable** 命令，在目的端设备上执行 **ip unreachable enable** 命令）

```
[DeviceA] tracert 120.2.0.1
```

```
traceroute to 120.2.0.1 (120.2.0.1), 30 hops at most, 52 bytes each packet, press CTRL_C to break
```

```
 1 120.1.0.2 (120.1.0.2) 2.208 ms 1.119 ms 1.085 ms
 2 10.1.0.102 (10.1.0.102) 1.083 ms 1.100 ms 1.085 ms
 3 10.2.0.101 (10.2.0.101) 2.364 ms 1.099 ms 1.086 ms
 4 120.2.0.1 (120.2.0.1) 3.825 ms 3.693 ms 4.008 ms
```

# 主链路断开后再查看 Device B 的 BGP 路由表，存在 1 条 120.2.0.0/24 的路由。

```
[DeviceB] display bgp routing-table ipv4
```

```
Total number of routes: 2
```

```
BGP local router ID is 2.2.2.2
```

```
Status codes: * - valid, > - best, d - dampened, h - history,
```

```
 s - suppressed, S - stale, i - internal, e - external
```

```
Origin: i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >e 120.1.0.0/24	120.1.0.1	0		0	200i
* >i 120.2.0.0/24	13.1.1.101	0	100	0	300i

# 再次在 Device A 上 **tracert Device F**，查看到报文传输路径是 Device A → Device B → Device E → Device D → Device F

```
[DeviceA] tracert 120.2.0.1
```

traceroute to 120.2.0.1 (120.2.0.1), 30 hops at most, 52 bytes each packet, press CTRL\_C to break

```
1 120.1.0.2 (120.1.0.2) 2.308 ms 1.127 ms 1.091 ms
2 192.168.0.102 (192.168.0.102) 1.086 ms 1.102 ms 1.096 ms
3 13.1.1.101 (13.1.1.101) 2.451 ms 2.087 ms 1.092 ms
4 120.2.0.1 (120.2.0.1) 3.533 ms 3.818 ms 4.002 ms
```

以上信息表明主备链路切换成功。

## 3.6 配置文件

- Device A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 120.1.0.1 255.255.255.0
#
bgp 200
 router-id 1.1.1.1
 peer 120.1.0.2 as-number 100
#
 address-family ipv4 unicast
 network 120.1.0.0 255.255.255.0
 peer 120.1.0.2 enable
#
```

- Device B:

```
#
ospf 1
 import-route direct
 area 0.0.0.0
 network 10.1.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.101 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.0.2 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 10.2.0.101 as-number 100
 peer 13.1.1.101 as-number 100
```

```

peer 120.1.0.1 as-number 200
#
address-family ipv4 unicast
 preference 255 100 130
 peer 10.2.0.101 enable
 peer 10.2.0.101 next-hop-local
 peer 10.2.0.101 route-policy local-pre export
 peer 13.1.1.101 enable
 peer 13.1.1.101 next-hop-local
 peer 120.1.0.1 enable
#
route-policy local-pre permit node 10
 if-match ip address acl 2000
 apply local-preference 200
#
acl number 2000
 rule 0 permit source 120.1.0.0 0.0.0.255
#

```

- **Device C:**

```

#
ospf 1
 area 0.0.0.0
 network 10.1.0.0 0.0.0.255
 network 10.2.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.2.0.102 255.255.255.0
#

```

- **Device D:**

```

#
ospf 1
 import-route direct
 area 0.0.0.0
 network 10.2.0.0 0.0.0.255
 network 13.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.2.0.101 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.101 255.255.255.0

```



```

#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.2.0.2 255.255.255.0
#
bgp 100
 router-id 4.4.4.4
 peer 10.1.0.101 as-number 100
 peer 120.2.0.1 as-number 300
 peer 192.168.0.101 as-number 100
#
 address-family ipv4 unicast
 preference 255 100 130
 peer 10.1.0.101 enable
 peer 10.1.0.101 next-hop-local
 peer 10.1.0.101 route-policy local-pre export
 peer 192.168.0.101 enable
 peer 192.168.0.101 next-hop-local
 peer 120.2.0.1 enable
#
 route-policy local-pre permit node 10
 if-match ip address acl 2000
 apply local-preference 200
#
#
acl number 2000
 rule 0 permit source 120.2.0.0 0.0.0.255
#

```

- **Device E:**

```

#
ospf 1
 area 0.0.0.0
 network 13.1.1.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.102 255.255.255.0
#

```

- **Device F:**

```

#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 120.2.0.1 255.255.255.0

```

```
#
bgp 300
 router-id 6.6.6.6
 peer 120.2.0.2 as-number 100
#
 address-family ipv4 unicast
 network 120.2.0.0 255.255.255.0
 peer 120.2.0.2 enable
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

# H3C MSR 系列路由器

## 策略路由配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 使用限制.....	1
4 IPv4 策略路由配置举例.....	1
4.1 组网需求.....	1
4.2 配置思路.....	2
4.3 使用版本.....	2
4.4 配置步骤.....	2
4.5 验证配置.....	3
4.6 配置文件.....	3
5 IPv6 策略路由配置举例.....	4
5.1 组网需求.....	4
5.2 配置思路.....	5
5.3 使用版本.....	5
5.4 配置步骤.....	5
5.5 验证配置.....	6
5.6 配置文件.....	6
6 相关资料.....	7

# 1 简介

本文档介绍了策略路由的配置举例。

普通报文是根据目的 IP 地址来查找路由表转发的，策略路由是一种依据用户制定的策略进行路由选择的机制。策略路由可以基于到达报文的源地址、目的地址、IP 优先级、协议类型等字段灵活地进行路由选择。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解策略路由特性。

## 3 使用限制

配置重定向到下一跳时，不能将 IPv4 规则重定向到 IPv6 地址，反之亦然。

## 4 IPv4 策略路由配置举例

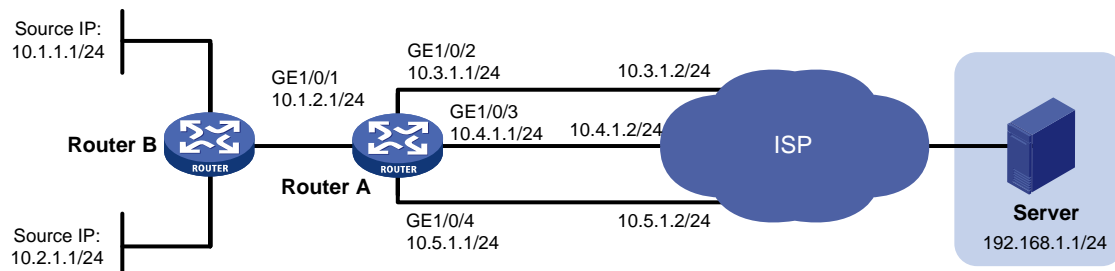
### 4.1 组网需求

如图 1 所示，缺省情况下，Router A 的接口 GigabitEthernet1/0/1 上收到的所有访问 Server 的报文根据路由表转发的下一跳均为 10.4.1.2。

现要求在 Router A 上配置 IPv4 策略路由，对于访问 Server 的报文实现如下要求：

- (1) 首先匹配接口 GigabitEthernet1/0/1 上收到的源 IP 地址为 10.2.1.1 的报文，将该报文的下一跳重定向到 10.5.1.2；
- (2) 其次匹配接口 GigabitEthernet1/0/1 上收到的 HTTP 报文，将该报文的下一跳重定向到 10.3.1.2。

图1 IPv4 策略路由典型配置组网图



## 4.2 配置思路

- 为了确保能同时满足对于两种不同类型的报文重定向到不同的下一跳,需要配置两个访问控制列表,一个用于匹配接口 **GigabitEthernet1/0/1** 上收到的源 IP 地址为 **10.2.1.1** 的报文,另一个用于匹配接口 **GigabitEthernet1/0/1** 上收到的 **HTTP** 报文,并在策略路由中创建两个节点,分别对匹配上的报文进行重定向;
- 同一条策略路由中,创建的节点编号越小,优先级越高。为了确保接口 **GigabitEthernet1/0/1** 上收到源 IP 地址为 **10.2.1.1** 的 **HTTP** 报文下一跳能优先被重定向到 **10.5.1.2**,需要在策略路由中配置该策略使用较小的节点编号(本例中使用 **0** 号节点,另一策略使用 **1** 号节点)。

## 4.3 使用版本

本举例是在 **R6728** 版本上进行配置和验证的。

## 4.4 配置步骤

# 配置接口 **GigabitEthernet 1/0/1** 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[RouterA-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中其它接口的 IP 地址,配置步骤这里省略。

# 配置静态路由,保证三条路径都可达,并且缺省下一跳为 **10.4.1.2**。

```
[RouterA] ip route-static 192.168.1.0 24 10.3.1.2
[RouterA] ip route-static 192.168.1.0 24 10.4.1.2 preference 40
[RouterA] ip route-static 192.168.1.0 24 10.5.1.2
```

# 定义访问控制列表 **ACL 3005**,用于匹配源 IP 地址为 **10.2.1.1** 的报文。

```
[RouterA] acl number 3005
[RouterA-acl-adv-3005] rule 0 permit ip source 10.2.1.1 0
[RouterA-acl-adv-3005] quit
```

# 定义访问控制列表 **ACL 3006**,用于匹配 **HTTP** 报文。

```
[RouterA] acl number 3006
[RouterA-acl-adv-3006] rule 0 permit tcp destination-port eq www
[RouterA-acl-adv-3006] quit
```

# 创建策略路由 **pbr1** 的 **0** 号节点,将匹配 **ACL 3005** 的报文下一跳重定向到 **10.5.1.2**。

```
[RouterA] policy-based-route pbr1 permit node 0
[RouterA-pbr-pbr1-0] if-match acl 3005
[RouterA-pbr-pbr1-0] apply next-hop 10.5.1.2
[RouterA-pbr-pbr1-0] quit
```

# 创建策略路由 **pbr1** 的 **1** 号节点,将匹配 **ACL 3006** 的报文下一跳重定向到 **10.3.1.2**。

```
[RouterA] policy-based-route pbr1 permit node 1
[RouterA-pbr-pbr1-1] if-match acl 3006
[RouterA-pbr-pbr1-1] apply next-hop 10.3.1.2
[RouterA-pbr-pbr1-1] quit
```

# 在 **Router A** 的接口 **GigabitEthernet1/0/1** 上应用策略。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip policy-based-route pbr1
[RouterA-GigabitEthernet1/0/1] quit
```

## 4.5 验证配置

# 通过 **display ip policy-based-route** 命令可以查看到当前策略路由配置已经配置成功:

```
[RouterA] display ip policy-based-route policy pbr1
Policy name: pbr1
 node 0 permit:
 if-match acl 3005
 apply next-hop 10.5.1.2
 node 1 permit:
 if-match acl 3006
 apply next-hop 10.3.1.2
```

# 通过 **tracert** 命令查看以下报文的转发路径（使用 **Tracert** 功能需要在中间设备上开启 **ICMP** 超时报文发送功能，在目的端开启 **ICMP** 目的不可达报文发送功能）:

- 源 IP 为 10.1.1.1 的非 HTTP 报文，重定向到 10.4.1.2 进行转发。

```
<Router> tracert -a 10.1.1.1 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1) from 10.1.1.1, 30 hops at most, 40 bytes
each packet, press CTRL_C to break
 1 10.1.2.1 (10.1.2.1) 2.178 ms 1.364 ms 1.058 ms
 2 10.4.1.2 (10.4.1.2) 1.548 ms 1.248 ms 1.112 ms
 3 192.168.1.1 (192.168.1.1) 1.594 ms 1.321 ms 1.093 ms
```

- 源 IP 为 10.2.1.1 的报文，重定向到 10.5.1.2 进行转发。

```
<Router> tracert -a 10.2.1.1 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1) from 10.2.1.1, 30 hops at most, 40 bytes
each packet, press CTRL_C to break
 1 10.1.2.1 (10.1.2.1) 1.721 ms 1.226 ms 1.050 ms
 2 10.5.1.2 (10.5.1.2) 4.494 ms 1.385 ms 1.170 ms
 3 192.168.1.1 (192.168.1.1) 1.448 ms 1.304 ms 1.093 ms
```

## 4.6 配置文件

```
#
policy-based-route pbr1 permit node 0
 if-match acl 3005
 apply next-hop 10.5.1.2
#
policy-based-route pbr1 permit node 1
 if-match acl 3006
 apply next-hop 10.3.1.2
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.2.1 255.255.255.0
 ip policy-based-route pbr1
```

```

#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.3.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 10.4.1.1 255.255.255.0
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 10.5.1.1 255.255.255.0
#
ip route-static 192.168.1.0 24 10.3.1.2
ip route-static 192.168.1.0 24 10.4.1.2 preference 40
ip route-static 192.168.1.0 24 10.5.1.2
#
acl number 3005
 rule 0 permit ip source 10.2.1.1 0
#
acl number 3006
 rule 0 permit tcp destination-port eq www
#

```

## 5 IPv6 策略路由配置举例

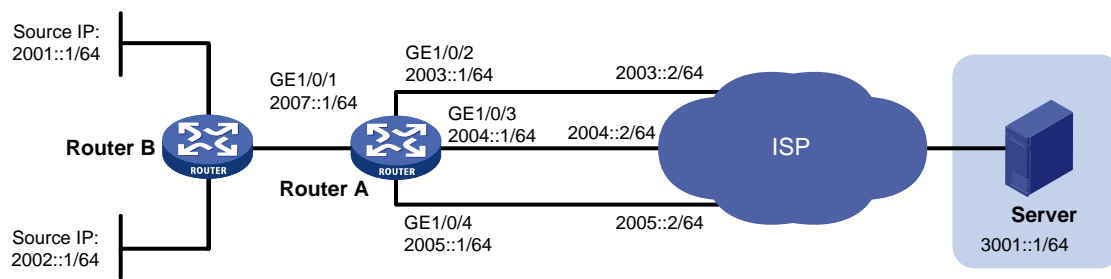
### 5.1 组网需求

如图2所示缺省情况下，Router A 的接口 GigabitEthernet1/0/1 上收到的所有访问 Server 的报文根据路由表转发的下一跳均为 2004::2。

现要求在 Router A 上配置 IPv4 策略路由，对于访问 Server 的报文实现如下要求：

- (1) 首先匹配接口 GigabitEthernet1/0/1 上收到的源 IPv6 地址为 2002::1 的报文，将该报文的下一跳重定向到 2005::2；
- (2) 其次匹配接口 GigabitEthernet1/0/1 上收到的 HTTP 报文，将该报文的下一跳重定向到 2003::2。

图2 IPv6 策略路由典型配置组网图





## 5.2 配置思路

- 为了确保能同时满足对于两种不同类型的报文重定向到不同的下一跳,需要配置两个访问控制列表,一个用于匹配接口 GigabitEthernet1/0/1 上收到的源 IPv6 地址为 2002::1 的报文,另一个用于匹配接口 GigabitEthernet1/0/1 上收到的 HTTP 报文,并在策略路由中创建两个节点,分别对匹配上的报文进行重定向;
- 同一条策略路由中,创建的节点编号越小,优先级越高。为了确保接口 GigabitEthernet1/0/1 上收到源 IPv6 地址为 2002::1 的 HTTP 报文下一跳能优先被重定向到 2005::2,需要在策略路由中配置该策略使用较小的节点编号(本例中使用 0 号节点,另一策略使用 1 号节点)。

## 5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 5.4 配置步骤

# 配置接口 GigabitEthernet1/0/1 的 IPv6 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ipv6 address 2007::1 64
[RouterA-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 2 中其它接口的 IPv6 地址,配置步骤这里省略。

# 配置静态路由,保证三条路径都可达,并且缺省下一跳为 2004::2/64。

```
[RouterA] ipv6 route-static 3001::1 64 2003::2
[RouterA] ipv6 route-static 3001::1 64 2004::2 preference 40
[RouterA] ipv6 route-static 3001::1 64 2005::2
```

# 定义 IPv6 访问控制列表 IPv6 ACL 3005,用于匹配源 IPv6 地址为 2002::1 的报文。

```
[RouterA] acl ipv6 number 3005
[RouterA-acl6-adv-3005] rule 0 permit ipv6 source 2002::1/128
[RouterA-acl6-adv-3005] quit
```

# 定义 IPv6 访问控制列表 IPv6 ACL 3006,用于匹配 GigabitEthernet 1/0/0 端口上收到的 HTTP 报文。

```
[RouterA] acl ipv6 number 3006
[RouterA-acl6-adv-3006] rule 0 permit tcp destination-port eq www
[RouterA-acl6-adv-3006] quit
```

# 创建 IPv6 策略路由 pbr1 的 0 号节点,将匹配 IPv6 ACL 3005 的报文下一跳重定向到 2005::2。

```
[RouterA] ipv6 policy-based-route pbr1 permit node 0
[RouterA-pbr6-pbr1-0] if-match acl 3005
[RouterA-pbr6-pbr1-0] apply next-hop 2005::2
[RouterA-pbr6-pbr1-0] quit
```

# 创建 IPv6 策略路由 pbr1 的 1 号节点,将匹配 IPv6 ACL 3006 的报文下一跳重定向到 2003::2。

```
[RouterA] ipv6 policy-based-route pbr1 permit node 1
[RouterA-pbr6-pbr1-1] if-match acl 3006
[RouterA-pbr6-pbr1-1] apply next-hop 2003::2
[RouterA-pbr6-pbr1-1] quit
```

# 在 Router A 的接口 GigabitEthernet1/0/1 上应用策略。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ipv6 policy-based-route pbr1
[RouterA-GigabitEthernet1/0/1] quit
```

## 5.5 验证配置

# 通过 **display ipv6 policy-based-route** 可以查看到当前 IPv6 策略路由配置已经生效:

```
[RouterA] display ipv6 policy-based-route policy pbr1
Policy name: pbr1
 node 0 permit:
 if-match acl 3005
 apply next-hop 2005::2
 node 1 permit:
 if-match acl 3006
 apply next-hop 2003::2
```

# 当 Router A 收到源 IPv6 地址为 2002::1 的报文时, 有如下结果:

- 当 2005::2 可达时, 报文被重定向到 2005::2;
- 当 2005::2 不可达时, 报文会根据普通的路由表转发到下一跳 2004::2。

# 当 Router A 收到 HTTP 报文时, 有如下结果:

- 当 2003::2 可达时, 报文被重定向到 2003::2;
- 当 2003::2 不可达时, 报文会根据普通的路由表转发到下一跳 2004::2。

## 5.6 配置文件

```
#
ipv6 policy-based-route pbr1 permit node 0
 if-match acl 3005
 apply next-hop 2005::2
#
ipv6 policy-based-route pbr1 permit node 1
 if-match acl 3006
 apply next-hop 2003::2
#
interface GigabitEthernet1/0/1
 port link-mode route
 ipv6 policy-based-route pbr1
 ipv6 address 2007::1/64
#
interface GigabitEthernet1/0/2
 port link-mode route
 ipv6 address 2003::1 64
#
interface GigabitEthernet1/0/3
 port link-mode route
 ipv6 address 2004::1 64
```

```
#
interface GigabitEthernet1/0/4
 port link-mode route
 ipv6 address 2005::1 64
#
 ipv6 route-static 3001:: 64 2003::2
 ipv6 route-static 3001:: 64 2004::2 preference 40
 ipv6 route-static 3001:: 64 2005::2
#
 acl ipv6 number 3005
 rule 0 permit ipv6 source 2002::1/128
#
 acl ipv6 number 3006
 rule 0 permit tcp destination-port eq www
#
```

## 6 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

# H3C MSR 系列路由器

## Tcl 脚本配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 使用 Tcl 脚本的 For 语句批量配置子接口地址配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	1
3.3 配置注意事项.....	1
3.4 配置步骤.....	1
3.5 验证配置.....	2
3.6 配置文件.....	2
4 使用 Tcl 脚本的 While 语句批量配置子接口地址配置举例.....	3
4.1 组网需求.....	3
4.2 使用版本.....	3
4.3 配置注意事项.....	3
4.4 配置步骤.....	3
4.5 验证配置.....	4
4.6 配置文件.....	4
5 相关资料.....	5

# 1 简介

本文档介绍 MSR 路由器使用 Tcl 脚本语言的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

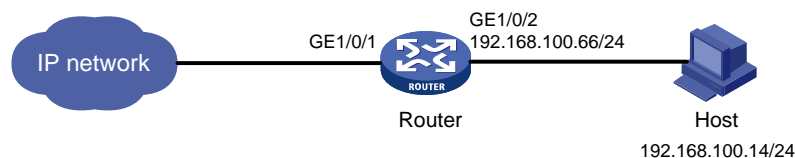
本文档假设您已了解 Tcl 脚本语言的特性。

## 3 使用 Tcl 脚本的 For 语句批量配置子接口地址配置举例

### 3.1 组网需求

如 [图 1](#) 所示，路由器 Router 连接配置主机，现要求：使用 For 语句的 Tcl 脚本，为接口 GigabitEthernet1/0/1 创建子接口 GigabitEthernet1/0/1.1~GigabitEthernet1/0/1.4，并配置相应的 IP 地址和 VLAN 终结。

图1 配置组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置注意事项

- 输入 Tcl 脚本命令，不支持输入 ? 键获得在线帮助和 Tab 键补全功能。
- 已经成功执行的 Tcl 脚本命令不会记录在历史命令缓冲区中，不能用上下光标键对命令进行调用。
- 在循环体执行过程中，任何操作命令无效。

### 3.4 配置步骤

# 进入 Tcl 配置视图

```
<Router> Tclsh
```

# 进入系统视图

```
<Router-Tcl> system-view
```

# 编写 For 语句的 Tcl 脚本。

```
[Router-Tcl] for {set i 1} {$i <= 4} {incr i 1} {
set j [expr $i+99]
```

# 配置子接口 GigabitEthernet1/0/1.1 地址为 1.1.1.1，GigabitEthernet1/0/1.2 ~ GigabitEthernet1/0/1.4 的子接口地址依次按序递增。

```
interface gigabitethernet 1/0/1.$i
ip add $i.1.1.1 24
```

# 配置子接口 GigabitEthernet1/0/1.1 终结的 VLAN ID 为 VLAN 100，GigabitEthernet1/0/1.2~ GigabitEthernet1/0/1.4 终结的 VLAN ID 均依次按序递增。

```
vlan-type dot1q vid $j}
```

```
[Router-Tcl-GigabitEthernet1/0/1.4] quit
```

### 3.5 验证配置

# 显示接口的概要信息，有对应的子接口生成，并配置相应的 IP 地址。

```
[Router] display interface brief
```

Brief information on interface(s) under route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) - spoofing

Interface	Link	Protocol	Main IP	Description
Aux1/0/1	UP	--	--	
GE1/0/1	UP	UP	192.168.100.65	wangguan
GE1/0/1.1	UP	UP	1.1.1.1	
GE1/0/1.2	UP	UP	2.1.1.1	
GE1/0/1.3	UP	UP	3.1.1.1	
GE1/0/1.4	UP	UP	4.1.1.1	
GE1/0/2	ADM	DOWN	--	
InLoop0	UP	UP(s)	--	
NULL0	UP	UP(s)	--	
REG0	DOWN	--	--	

# 通过 **display current-configuration interface** 命令，以 GigabitEthernet1/0/1.1 为例，观察到 VLAN 终结配置成功。

```
[Router] display current-configuration interface gigabitethernet 1/0/1.1
```

```
#
```

```
interface GigabitEthernet1/0/1.1
ip address 1.1.1.1 255.255.255.0
vlan-type dot1q vid 100
```

```
#
```

```
return
```

### 3.6 配置文件

Router 的 For 语句:

```
for {set i 1} {$i <= 4} {incr i 1} {
```

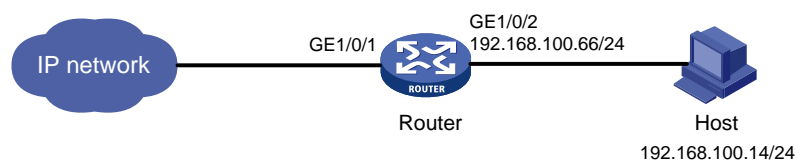
```
set j [expr $i+99]
interface gigabitEthernet 1/0/1.$i
ip address $i.1.1.1 24
vlan-type dot1q vid $j}
```

## 4 使用 Tcl 脚本的 While 语句批量配置子接口地址配置举例

### 4.1 组网需求

如图 2 所示，路由器 Router 连接配置主机，现要求：编写一个使用 While 语句的 Tcl 脚本，为接口 GigabitEthernet1/0/1 创建子接口 GigabitEthernet1/0/1.1~GigabitEthernet1/0/1.4，并配置相应的 IP 地址和 VLAN 终结。

图2 配置组网图



### 4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 4.3 配置注意事项

- While 语句必须在语句前预定义变量值
- 输入 Tcl 脚本命令，不支持输入 ? 键获得在线帮助和 Tab 键补全功能。
- 已经成功执行的 Tcl 脚本命令不会记录在历史命令缓冲区中，不能用上下光标键对命令进行调用。
- 在循环体执行过程中，任何操作命令无效。

### 4.4 配置步骤

```
进入 Tcl 配置视图
<Router> Tclsh
进入系统视图
<Router-Tcl> system-view
编写 While 语句的 Tcl 脚本，预定义变量 i 的值为 1。
[Router-Tcl] set i 1
1
[Router-Tcl] while {$i <= 4} {
set j [expr $i+99]
```



# 配置子接口 GigabitEthernet1/0/1.1 地址为 1.1.1.1，GigabitEthernet1/0/1.2 ~ GigabitEthernet1/0/1.4 的子接口地址依次按序递增。

```
interface gigabitethernet 1/0/1.$i
ip address $i.1.1.1 24
```

# 配置子接口 GigabitEthernet1/0/1.1 终结的 VLAN ID 为 100，GigabitEthernet1/0/1.2 ~ GigabitEthernet1/0/1.4 终结的 VLAN ID 均依次按序递增。

```
vlan-type dot1q vid $j
incr i}
[Router-Tcl-GigabitEthernet1/0/1.4] quit
```

## 4.5 验证配置

# 显示接口的概要信息，有对应的子接口生成，并配置相应的 IP 地址。

```
[Router] display interface brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface Link Protocol Main IP Description
Aux1/0/1 UP -- --
GE1/0/1 UP UP 192.168.100.65 wangguan
GE1/0/1.1 UP UP 1.1.1.1
GE1/0/1.2 UP UP 2.1.1.1
GE1/0/1.3 UP UP 3.1.1.1
GE1/0/1.4 UP UP 4.1.1.1
GE1/0/2 ADM DOWN --
InLoop0 UP UP(s) --
NULL0 UP UP(s) --
REG0 DOWN -- --
```

# 通过 **display current-configuration interface** 命令，以 GigabitEthernet1/0/1.1 为例，观察到 VLAN 终结配置成功。

```
[Router] display current-configuration interface gigabitethernet 1/0/1.1
#
interface GigabitEthernet1/0/1.1
 ip address 1.1.1.1 255.255.255.0
 vlan-type dot1q vid 100
#
return
```

## 4.6 配置文件

Router 的 While 语句：

```
set i 1
while {$i <= 4} {
set j [expr $i+99]
interface gigabitethernet 1/0/1.$i
ip address $i.1.1.1 24
vlan-type dot1q vid $j
```

```
incr i}
```

## 5 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“基础配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“基础配置命令参考”

# H3C MSR 系列路由器

## GRE 和 OSPF 结合使用配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	2
3.3 配置步骤.....	2
3.3.1 配置准备.....	2
3.3.2 配置 Device A.....	2
3.3.3 配置 Device B.....	3
3.3.4 配置 Device C.....	3
3.4 验证配置.....	4
3.5 配置文件.....	5
4 相关资料.....	6

# 1 简介

本文档介绍了 GRE 隧道和 OSPF 相结合使用的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解 GRE 隧道和 OSPF 的相关特性。

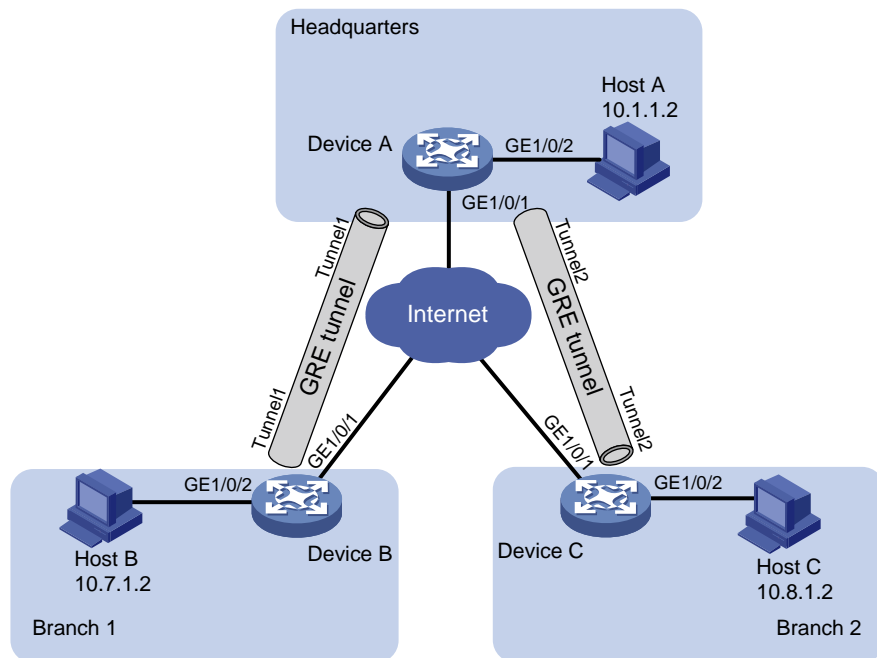
## 3 配置举例

### 3.1 组网需求

如图 1 所示，Device A 为某机构总部网关，Device B 和 Device C 为分支网关，运营商为各网关分配了公网 IP 地址，并保证网关之间可以通信，要求：

- 总部和分支之间建立 GRE 隧道，通过隧道使各总部、分支机构可以实现互访；
- 配置 OSPF 协议使网关上存在通过 Tunnel 接口到达目的地址的路由表项。

图1 GRE 和 OSPF 结合使用典型配置举例组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	191.2.1.1/24	Device B	GE1/0/1	191.3.1.1/24
	GE1/0/2	10.1.1.1/24		GE1/0/2	10.7.1.1/24
	Tunnel 1	10.5.1.1/24		Tunnel 1	10.5.1.2/24
	Tunnel 2	10.6.1.1/24			
Device C	GE1/0/1	191.4.1.1/24			
	GE1/0/2	10.8.1.1/24			
	Tunnel 2	10.6.1.2/24			

## 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.3 配置步骤

### 3.3.1 配置准备

配置网关设备之间的 IPv4 路由协议，确保设备之间 IPv4 报文能够正常交互，具体配置过程略。

### 3.3.2 配置 Device A

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 191.2.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置上图中 Device A 其它接口的 IP 地址，配置步骤这里省略。

# 创建 Tunnel1 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 1 mode gre
```

# 配置 Tunnel1 接口的 IP 地址。

```
[DeviceA-Tunnel1] ip address 10.5.1.1 24
```

# 配置 Tunnel1 接口的源接口为 GigabitEthernet1/0/1。

```
[DeviceA-Tunnel1] source GigabitEthernet 1/0/1
```

# 配置 Tunnel1 接口的目的端地址。

```
[DeviceA-Tunnel1] destination 191.3.1.1
```

```
[DeviceA-Tunnel1] quit
```

# 创建 Tunnel2 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 2 mode gre
```

# 配置 Tunnel2 接口的 IP 地址。

```
[DeviceA-Tunnel2] ip address 10.6.1.1 24
```

# 配置 Tunnel2 接口的源接口为 GigabitEthernet1/0/1。

```
[DeviceA-Tunnel2] source GigabitEthernet 1/0/1
```

# 配置 Tunnel2 接口的目的端地址。

```
[DeviceA-Tunnel2] destination 191.4.1.1
```

```
[DeviceA-Tunnel2] quit
```

# 启动 OSPF，并配置其 Router ID 为 10.6.1.1。

```
[DeviceA] router-id 10.6.1.1
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
```

### 3.3.3 配置 Device B

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 191.3.1.1 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置上图中 Device B 其它接口的 IP 地址，配置步骤这里省略。

# 创建 Tunnel1 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceB] interface tunnel 1 mode gre
```

# 配置 Tunnel1 接口的 IP 地址。

```
[DeviceB-Tunnel1] ip address 10.5.1.2 24
```

# 配置 Tunnel1 接口的源接口为 GigabitEthernet1/0/1。

```
[DeviceB-Tunnel1] source GigabitEthernet 1/0/1
```

# 配置 Tunnel1 接口的目的端地址。

```
[DeviceB-Tunnel1] destination 191.2.1.1
```

```
[DeviceB-Tunnel1] quit
```

# 启动 OSPF，并配置其 Router ID 为 10.7.1.1。

```
[DeviceB] router-id 10.7.1.1
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.7.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
```

### 3.3.4 配置 Device C

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address 191.4.1.1 255.255.255.0
[DeviceC-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置上图中 Device C 其它接口的 IP 地址，配置步骤这里省略。

# 创建 Tunnel2 接口，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceC] interface tunnel 2 mode gre
```

# 配置 Tunnel2 接口的 IP 地址。

```
[DeviceC-Tunnel2] ip address 10.6.1.2 24
```

# 配置 Tunnel1 接口的源接口为 GigabitEthernet1/0/1。

```
[DeviceC-Tunnel2] source GigabitEthernet 1/0/1
```

# 配置 Tunnel2 接口的目的端地址。

```
[DeviceC-Tunnel2] destination 191.2.1.1
[DeviceC-Tunnel2] quit
启动 OSPF, 并配置其 Router ID 为 10.8.1.1。
[DeviceC] router-id 10.8.1.1
[DeviceC] ospf 1
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.8.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
```

### 3.4 验证配置

- (1) 从 Host A 可以 ping 通 Host B。

```
C:\> ping 10.7.1.2
```

```
Pinging 10.7.1.2 with 32 bytes of data:
```

```
Reply from 10.7.1.2: bytes=32 time=19ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253
```

```
Ping statistics for 10.7.1.2:
```

```
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) ,
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

- (2) 从 Host A 可以 ping 通 Host C。

```
C:\> ping 10.8.1.2
```

```
Pinging 10.8.1.2 with 32 bytes of data:
```

```
Reply from 10.8.1.2: bytes=32 time=18ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253
```

```
Ping statistics for 10.8.1.2:
```

```
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) ,
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

- (3) 从 Host B 可以 ping 通 Host C。

```
C:\> ping 10.8.1.2
```

```
Pinging 10.8.1.2 with 32 bytes of data:
```

```
Reply from 10.8.1.2: bytes=32 time=20ms TTL=251
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251
```



```
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251
```

```
Ping statistics for 10.8.1.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) ,
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

## 3.5 配置文件

- Device A

```

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 191.2.1.1 255.255.255.0

interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.1.1.1 255.255.255.0

interface Tunnel1 mode gre
 source GigabitEthernet1/0/1
 destination 191.3.1.1
 ip address 10.5.1.1 255.255.255.0

interface Tunnel2 mode gre
 source GigabitEthernet1/0/1
 destination 191.4.1.1
 ip address 10.6.1.1 255.255.255.0

ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.5.1.0 0.0.0.255
 network 10.6.1.0 0.0.0.255
#
```

- Device B

```

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 191.3.1.1 255.255.255.0

interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.7.1.1 255.255.255.0

interface Tunnel1 mode gre
 source GigabitEthernet1/0/1
 destination 191.2.1.1
```

```
ip address 10.5.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.7.1.0 0.0.0.255
network 10.5.1.0 0.0.0.255
#
```

- **Device C**

```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 191.4.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 10.8.1.1 255.255.255.0
#
interface Tunnel2 mode gre
source GigabitEthernet1/0/1
destination 191.2.1.1
ip address 10.6.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.8.1.0 0.0.0.255
network 10.6.1.0 0.0.0.255
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-路由命令参考”

# H3C MSR 系列路由器

## IPv6 over IPv4 GRE 隧道配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.5.1 配置 Device A.....	2
3.5.2 配置 Device B.....	3
3.5.3 配置 Device C.....	3
3.6 验证配置.....	3
3.7 配置文件.....	4
4 相关资料.....	5

# 1 简介

本文档介绍了 IPv6 over IPv4 GRE 隧道的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解 IPv6 over IPv4 GRE 隧道的相关特性。

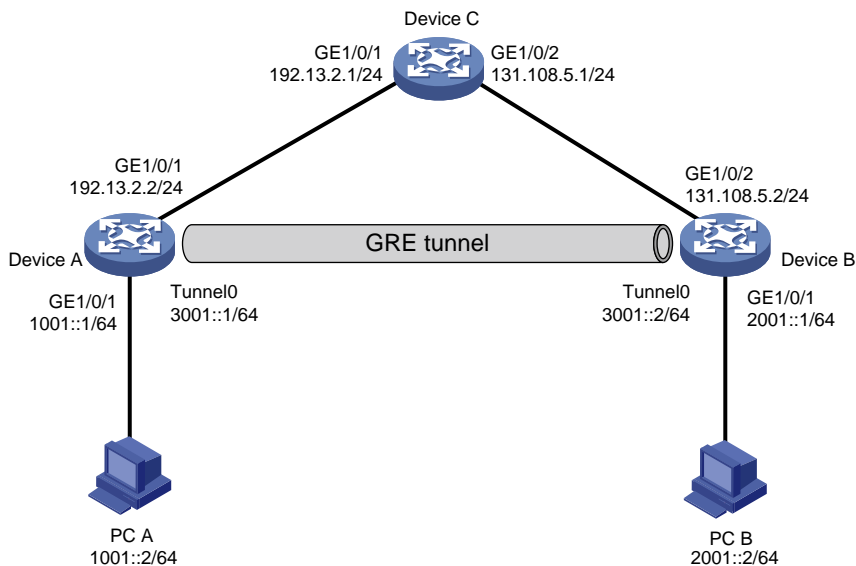
## 3 配置举例

### 3.1 组网需求

如图 1 所示，Device A、Device B、Device C 之间通过 IPv4 网络互连。Device A 和 Device B 分别连接 IPv6 主机 PC A 和 PC B。

要求通过在边界的双栈设备（Device A、Device B）之间建立 GRE 隧道，实现两台 IPv6 主机 PC A 和 PC B 的通信。

图1 IPv6 over IPv4 GRE 隧道配置组网图



## 3.2 配置思路

- 为实现两台 IPv6 主机 PC A 和 PC B 的通信，需要将 GRE 隧道模式为 GRE over IPv4，隧道接口配置为 IPv6 地址；
- 为了使 PC A 发往 PC B 的报文经由 GRE 隧道进行转发，需要在边界设备 Device A 上建立 Tunnel 转发的路由表项：目的地址是未进行 GRE 封装的报文的目的地址（即 PC B 的 IPv6 地址），下一跳是 GRE 隧道对端 Device B 的 Tunnel 接口地址或者直接指定出接口为 GRE 隧道接口。该路由表项可以通过配置静态路由来建立，也可以在 Tunnel 接口上和与 PC A 相连的三层接口上分别使能动态路由协议，由动态路由协议来建立。本例中选择配置静态路由方式。同理，Device B 上也需进行相应配置；
- 对于 GRE 隧道，必须确保隧道源端和目的端之间 IPv4 路由可达，因此需要在 Device A 和 Device B 上分别配置到对端的静态路由。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置注意事项

Tunnel 两端必须都配置隧道的源端地址和目的端地址，且本端配置的源端地址应该与对端配置的目的端地址相同、本端配置的目的端地址应该与对端配置的源端地址相同。

## 3.5 配置步骤

### 3.5.1 配置 Device A

# 配置接口 GigabitEthernet1/0/2 的 IPv6 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ipv6 address 1001::1 64
[DeviceA-GigabitEthernet1/0/2] quit
```

# 请参考以上方法配置上图中 Device A 其它接口的 IP 地址，配置步骤这里省略。

# 创建隧道接口 Tunnel0，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceA] interface tunnel 0 mode gre
```

# 配置 Tunnel0 接口的 IPv6 地址。

```
[DeviceA-Tunnel0] ipv6 address 3001::1 64
```

# 配置 Tunnel0 接口的源端地址。

```
[DeviceA-Tunnel0] source 192.13.2.2
```

# 配置 Tunnel0 接口的目的端地址。

```
[DeviceA-Tunnel0] destination 131.108.5.2
[DeviceA-Tunnel0] quit
```

# 配置从 Device A 经过 Tunnel0 接口到 PC B 的静态路由。

```
[DeviceA] ipv6 route-static 2001:: 64 tunnel 0
```

# 配置从 DeviceA 到达隧道目的端的静态路由。

```
[DeviceA] ip route-static 131.108.5.2 255.255.255.0 192.13.2.1
```

### 3.5.2 配置 Device B

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipv6 address 2001::1 64
[DeviceB-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置上图中 Device B 其它接口的 IP 地址，配置步骤这里省略。

# 创建隧道接口 Tunnel0，并指定隧道模式为 GRE over IPv4 隧道。

```
[DeviceB] interface tunnel 0 mode gre
```

# 配置 Tunnel0 接口的 IPv6 地址。

```
[DeviceB-Tunnel0] ipv6 address 3001::2 64
```

# 配置 Tunnel0 接口的源端地址。

```
[DeviceB-Tunnel0] source 131.108.5.2
```

# 配置 Tunnel0 接口的目的端地址。

```
[DeviceB-Tunnel0] destination 192.13.2.2
```

```
[DeviceB-Tunnel0] quit
```

# 配置从 DeviceB 经过 Tunnel0 接口到 PC A 的静态路由。

```
[DeviceB] ipv6 route-static 1001:: 64 Tunnel 0
```

# 配置 DeviceB 到达隧道目的端的静态路由。

```
[DeviceB] ip route-static 192.13.2.2 255.255.255.0 131.108.5.1
```

### 3.5.3 配置 Device C

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address 192.13.2.1 24
[DeviceC-GigabitEthernet1/0/1] quit
```

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] ip address 131.108.5.1 24
[DeviceC-GigabitEthernet1/0/2] quit
```

## 3.6 验证配置

PCA 和 PCB 之间可以互相 Ping 通。

```
C:\>ping6 2001::2
```

```
Pinging 2001::2
```

```
from 1001::1 with 32 bytes of data:
```

```
Reply from 2001::2: bytes=32 time<lms
```

```
Reply from 2001::2: bytes=32 time<lms
```

Reply from 2001::2: bytes=32 time<lms

Reply from 2001::2: bytes=32 time<lms

Ping statistics for 2001::2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

## 3.7 配置文件

- Device A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.13.2.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ipv6 address 1001::1/64
#
interface Tunnel0 mode gre
 ipv6 address 3001::1/64
 source 192.13.2.2
 destination 131.108.5.2
#
 ip route-static 131.108.5.2 255.255.255.0 192.13.2.1
#
 ipv6 route-static 2001:: 64 Tunnel 0
#
```

- Device B:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ipv6 address 2001::1/64
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 131.108.5.2 255.255.255.0
#
interface Tunnel0 mode gre
 ipv6 address 3001::2/64
 source 131.108.5.2
 destination 192.13.2.2
#
 ip route-static 192.13.2.2 255.255.255.0 131.108.5.1
#
 ipv6 route-static 1001:: 64 Tunnel 0
#
```



- Device C:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.13.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 131.108.5.1 255.255.255.0
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”

# H3C MSR 系列路由器

## ISATAP 隧道和 6to4 隧道相结合使用配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 ISATAP 隧道和 6to4 隧道相结合使用的典型配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置步骤.....	2
3.5 验证配置.....	4
3.6 配置文件.....	5
4 相关资料.....	6

# 1 简介

本文档介绍了 ISATAP 隧道和 6to4 隧道相结合使用的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解 ISATAP 隧道和 6to4 隧道的相关特性。

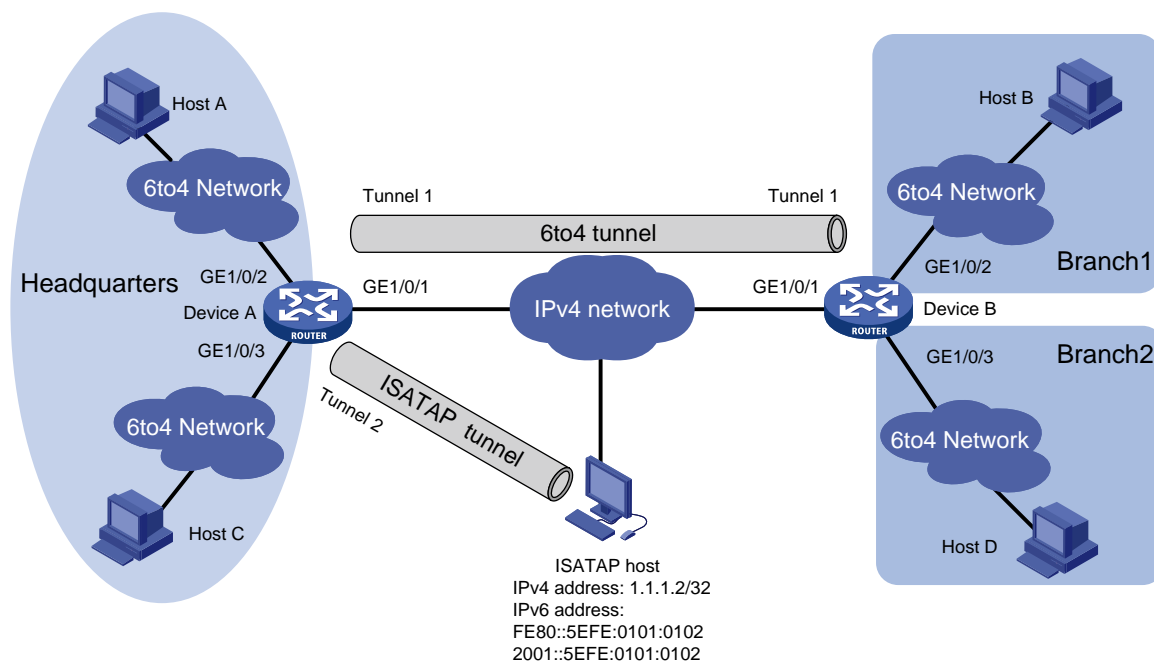
## 3 ISATAP 隧道和 6to4 隧道相结合使用的典型配置举例

### 3.1 组网需求

如图 1 所示，要求：

- 通过配置 6to4 隧道使各 6to4 网络分支机构与总部中的主机能够互通。
- Device A 提供 ISATAP 接入服务使一些 IPv4 网络中的双协议栈主机可以访问总部。

图1 ISATAP 隧道和 6to4 隧道相结合使用的配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	2.1.1.1/24	Device B	GE1/0/1	3.1.1.1/24
	GE1/0/2	2002:0201:0101:1::1/64		GE1/0/2	2002:0301:0101:1::1/64
	GE1/0/3	2002:0201:0101:2::1/64		GE1/0/3	2002:0301:0101:2::1/64
	Tunnel 1	3001::1/64		Tunnel 1	3001::2/64
	Tunnel 2	2001::5EFE:0201:0101/64			

## 3.2 配置思路

- 组网中的 6to4 网络可以表示为 2002:IPv4 地址::/64，其中内嵌在 IPv6 地址中的 IPv4 地址作为 6to4 隧道中封装后的 IPv4 报文头中的目的 IP 地址。
- 组网中的 ISATAP 主机地址的 IPv6 前缀可通过向 ISATAP 路由器发送请求得到，IPv4 地址作为接口 ID，其格式为：Prefix:0:5EFE:IPv4-destination-address。该 IPv4 地址可以作为 ISATAP 隧道的目的端地址。
- 为保证同一网络中的主机使用相同的地址前缀，在 Device A 和 Device B 上取消对 RA 消息发布的抑制，使得网络中的主机可以通过 Device A 和 Device B 发布的 RA 消息获取地址前缀等信息。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置步骤



说明

配置之前，请确保网关设备之间 IPv4 报文路由可达。

### (1) 配置 Device A

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 2.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Device A 其它接口的 IP 地址，配置步骤这里省略。

# 创建模式为 6to4 隧道的接口 Tunnel1。

```
[DeviceA] interface tunnel 1 mode ipv6-ipv4 6to4
```

# 配置 Tunnel1 接口的 IPv6 地址。

```
[DeviceA-Tunnel1] ipv6 address 3001::1/64
```

# 配置 Tunnel1 接口的源接口为 GigabitEthernet1/0/1（封装后的 IPv4 报文头中的源 IP 地址为配置的源接口的 IP 地址）。

```
[DeviceA-Tunnel1] source gigabitethernet 1/0/1
[DeviceA-Tunnel1] quit
```

```

配置到目的地址 2002:0301:0101::/48，下一跳为 Tunnel1 接口的静态路由。
[DeviceA] ipv6 route-static 2002:0301:0101:: 48 tunnel 1
创建模式为 ISATAP 隧道的接口 Tunnel2。
[DeviceA] interface tunnel 2 mode ipv6-ipv4 isatap
配置 Tunnel2 接口的 IPv6 地址。
[DeviceA-Tunnel2] ipv6 address 2001::5EFE:0201:0101 64
配置 Tunnel2 接口的源接口为 GigabitEthernet1/0/1（封装后的 IPv4 报文头中的源 IP 地址
为配置的源接口的 IP 地址）。
[DeviceA-Tunnel2] source gigabitethernet 1/0/1
[DeviceA-Tunnel2] quit
配置到目的地址 2001::/16，下一跳为 Tunnel2 接口的静态路由。
[DeviceA] ipv6 route-static 2001:: 16 tunnel 2
取消对 RA 消息发布的抑制，使主机可以通过交换机发布的 RA 消息获取地址前缀等信息。
[DeviceA] interface Tunnel 2
[DeviceA-Tunnel2] undo ipv6 nd ra halt
[DeviceA-Tunnel2] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo ipv6 nd ra halt
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface GigabitEthernet1/0/3
[DeviceA-GigabitEthernet1/0/3] undo ipv6 nd ra halt
[DeviceA-GigabitEthernet1/0/3] quit

```

## (2) 配置 Device B

```

配置接口 GigabitEthernet1/0/1 的 IP 地址。
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 3.1.1.1 24
[DeviceB-GigabitEthernet1/0/1] quit
请参考以上方法配置图 1 中 Device B 其它接口的 IP 地址，配置步骤这里省略。
创建模式为 6to4 隧道的接口 Tunnel1。
[DeviceB] interface tunnel 1 mode ipv6-ipv4 6to4
配置 Tunnel1 接口的 IPv6 地址。
[DeviceB-Tunnel1] ipv6 address 3001::2/64
配置 Tunnel1 接口的源接口为 GigabitEthernet1/0/1（封装后的 IPv4 报文头中的源 IP 地址
为配置的源接口的 IP 地址）。
[DeviceB-Tunnel1] source gigabitethernet 1/0/1
[DeviceB-Tunnel1] quit
配置到目的地址 2002:0201:0101::/48，下一跳为 Tunnel1 接口的静态路由。
[DeviceB] ipv6 route-static 2002:0201:0101:: 48 tunnel 1
取消对 RA 消息发布的抑制，使主机可以通过交换机发布的 RA 消息获取地址前缀等信息。
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo ipv6 nd ra halt
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3

```

```
[DeviceB-GigabitEthernet1/0/3] undo ipv6 nd ra halt
[DeviceB-GigabitEthernet1/0/3] quit
```

### (3) 配置 ISATAP 主机

ISATAP 主机上的具体配置与主机的操作系统有关，下面仅以 Windows XP 操作系统为例进行说明。

# 在主机上安装 IPv6 协议。

```
C:\>ipv6 install
```

# 配置 ISATAP 隧道。

```
C:\>netsh interface ipv6 isatap set router 2.1.1.1
```

# 完成上述配置后，查看 ISATAP 接口的信息。

```
C:\>ipv6 if 2
```

```
Interface 2: Automatic Tunneling Pseudo-Interface
 Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
 does not use Neighbor Discovery
 uses Router Discovery
 routing preference 1
 EUI-64 embedded IPv4 address: 1.1.1.2
 router link-layer address: 2.1.1.1
 preferred global 2001::5efe:1.1.1.2, life 29d23h59m46s/6d23h59m46s (public)
 preferred link-local fe80::5efe:1.1.1.2, life infinite
 link MTU 1500 (true link MTU 65515)
 current hop limit 255
 reachable time 42500ms (base 30000ms)
 retransmission interval 1000ms
 DAD transmits 0
 default site prefix length 48
```

我们可以看到主机获取了 2001::/64 的前缀，自动生成全球单播地址 2001::5efe:1.1.1.2，同时还有一行信息“uses Router Discovery”表明主机启用了路由器发现。

# 查看主机上的 IPv6 路由信息。

```
C:\>ipv6 rt
```

```
2001::/64 -> 2 pref lif+8=9 life 29d23h59m43s (autoconf)
::/0 -> 2/fe80::5efe:1.1.1.1 pref lif+256=257 life 29m43s (autoconf)
```

## 3.5 验证配置

# 完成以上配置之后，Host A 与 Host B 可以互相 Ping 通。

```
D:\>ping6 -s 2002:0201:0101:1::2 2002:0301:0101:1::2
```

```
Pinging 2002:0301:0101:1::2
```

```
from 2002:0201:0101:1::2 with 32 bytes of data:
```

```
Reply from 2002:0301:0101:1::2: bytes=32 time=13ms
```

```
Reply from 2002:0301:0101:1::2: bytes=32 time=1ms
```

```
Reply from 2002:0301:0101:1::2: bytes=32 time=1ms
```

```
Reply from 2002:0301:0101:1::2: bytes=32 time<1ms
```

```

Ping statistics for 2002:0301:0101:1::2:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 13ms, Average = 3ms
在 ISATAP 主机上 Ping Host A 的地址, 可以 Ping 通。
C:\Documents and Settings\Administrator>pingv6 2002:0201:0101:1::2

Pinging 2002:0201:0101:1::2 with 32 bytes of data:

Reply from 2002:0201:0101:1::2: time=33ms
Reply from 2002:0201:0101:1::2: time=32ms
Reply from 2002:0201:0101:1::2: time=32ms
Reply from 2002:0201:0101:1::2: time=33ms

Ping statistics for 2002:0201:0101:1::2:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 32ms, Maximum = 33ms, Average = 32ms

```

## 3.6 配置文件

- Device A
 

```

#
interface GigabitEthernet1/0/1
 ip address 2.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ipv6 address 2002:201:101:1::1/64
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/3
 ipv6 address 2002:201:101:2::1/64
 undo ipv6 nd ra halt
#
interface Tunnel1 mode ipv6-ipv4 6to4
 source GigabitEthernet1/0/1
 ipv6 address 3001::1/64
#
interface Tunnel2 mode ipv6-ipv4 isatap
 source GigabitEthernet1/0/1
 ipv6 address 2001::5EFE:201:101/64
 undo ipv6 nd ra halt
#
 ipv6 route-static 2001:: 16 Tunnel2
 ipv6 route-static 2002:301:101:: 48 Tunnel1
#

```
- Device B
 

```

#

```



```
interface GigabitEthernet1/0/1
 ip address 3.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ipv6 address 2002:301:101:1::1/64
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/3
 ipv6 address 2002:301:101:2::1/64
 undo ipv6 nd ra halt
#
interface Tunnel1 mode ipv6-ipv4 6to4
 source GigabitEthernet1/0/1
 ipv6 address 3001::2/64
#
 ipv6 route-static 2002:201:101:: 48 Tunnel1
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”

# H3C MSR 系列路由器

## IPv6 手动隧道+OSPFv3 功能配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 IPv6 手动隧道+OSPFv3 功能组合的配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	2
3.3 配置步骤.....	2
3.4 验证配置.....	4
3.5 配置文件.....	5
4 相关资料.....	7

# 1 简介

本文档介绍了 IPv6 手动隧道+OSPFv3 功能组合的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

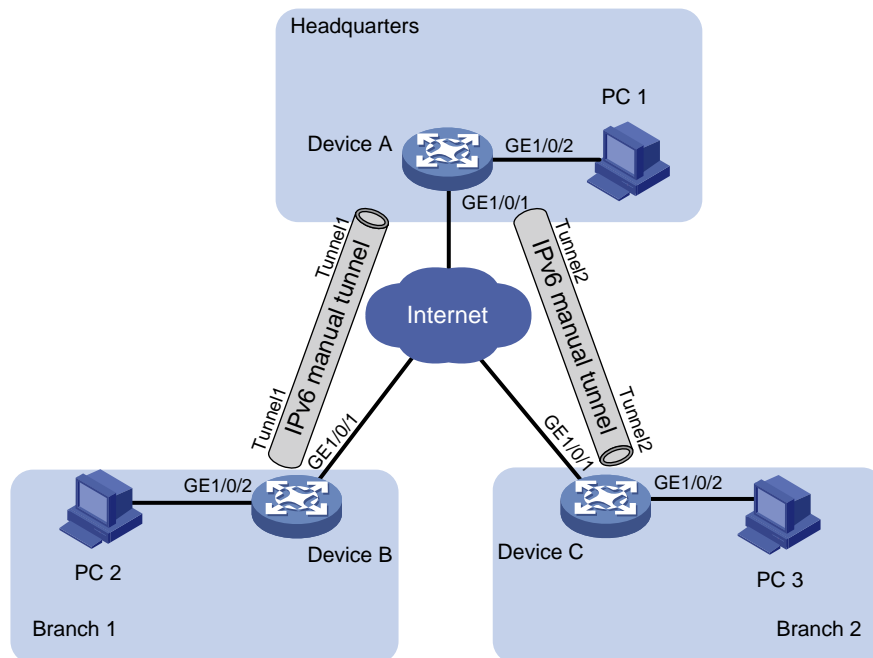
本文假设您已了解 IPv6 手动隧道和 OSPFv3 相关特性。

## 3 IPv6 手动隧道+OSPFv3 功能组合的配置举例

### 3.1 组网需求

如图 1 所示，某公司总部和分支机构的网络均为 IPv6 网络，Device A 为公司总部网关，Device B 和 Device C 分别为分支机构 Branch 1 和 Branch 2 的网关。要求在总部与各分支机构之间建立 IPv6 手动隧道，通过隧道使总部与各分支机构可以穿越 IPv4 网络实现互访；同时，配置 OSPFv3 协议使网关上存在通过 Tunnel 接口到达目的 IPv6 地址的转发路由，并实现分支机构与分支机构之间能够通过总部互访。

图1 IPv6 手动隧道+OSPFv3 功能组合配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	20.1.1.1/24	Device B	GE1/0/1	30.1.1.1/24
	GE1/0/2	2001::1/64		GE1/0/2	5001::1/64
	Tunnel1	3001::1/64		Tunnel1	3001::2/64
Device C	Tunnel2	4001::1/64			
	GE1/0/1	40.1.1.1/24			
	GE1/0/2	6001::1/64			
	Tunnel2	4001::2/64			

## 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.3 配置步骤



说明

配置之前，请确保网关设备之间 IPv4 报文路由可达。

### (1) 配置 IPv6 手动隧道

#### • 配置 Device A

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 20.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Device A 其它接口的 IP 地址，配置步骤这里省略。

# 创建模式为 IPv6 over IPv4 手动隧道的接口 Tunnel1。

```
[DeviceA] interface tunnel 1 mode ipv6-ipv4
```

# 配置 Tunnel1 接口的 IPv6 地址。

```
[DeviceA-Tunnel1] ipv6 address 3001::1/64
```

# 配置 Tunnel1 接口的源接口为 GigabitEthernet20/1（封装后的 IPv4 报文头中的源 IP 地址为配置的源接口的 IP 地址）。

```
[DeviceA-Tunnel1] source gigabitethernet 1/0/1
```

# 配置 Tunnel1 接口的目的端地址（封装后的 IPv4 报文头中的目的 IP 地址为配置的目的端地址）。

```
[DeviceA-Tunnel1] destination 30.1.1.1
```

```
[DeviceA-Tunnel1] quit
```

# 创建模式为 IPv6 over IPv4 手动隧道的接口 Tunnel2。

```
[DeviceA] interface tunnel 2 mode ipv6-ipv4
```

# 配置 Tunnel2 接口的 IPv6 地址。

```
[DeviceA-Tunnel2] ipv6 address 4001::1/64
```

# 配置 Tunnel2 接口的源接口为 GigabitEthernet1/0/1。

```
[DeviceA-Tunnel2] source gigabitethernet 1/0/1
```

# 配置 Tunnel2 接口的目的端地址。

```
[DeviceA-Tunnel2] destination 40.1.1.1
[DeviceA-Tunnel2] quit
```

- 配置 Device B

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 30.1.1.1 24
[DeviceB-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Device B 其它接口的 IP 地址，配置步骤这里省略。

# 创建模式为 IPv6 over IPv4 手动隧道的接口 Tunnel1。

```
[DeviceB] interface tunnel 1 mode ipv6-ipv4
```

# 配置 Tunnel1 接口的 IPv6 地址。

```
[DeviceB-Tunnel1] ipv6 address 3001::2/64
```

# 配置 Tunnel1 接口的源接口为 GigabitEthernet1/0/1（封装后的 IPv4 报文头中的源 IP 地址为配置的源接口的 IP 地址）。

```
[DeviceB-Tunnel1] source gigabitethernet 1/0/1
```

# 配置 Tunnel1 接口的目的端地址（封装后的 IPv4 报文头中的目的 IP 地址为配置的目的端地址）。

```
[DeviceB-Tunnel1] destination 20.1.1.1
[DeviceB-Tunnel1] quit
```

- 配置 Device C

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address 40.1.1.1 24
[DeviceC-GigabitEthernet1/0/1] quit
```

# 请参考以上方法配置图 1 中 Device C 其它接口的 IP 地址，配置步骤这里省略。

# 创建模式为 IPv6 over IPv4 手动隧道的接口 Tunnel2。

```
[DeviceC] interface tunnel 2 mode ipv6-ipv4
```

# 配置 Tunnel2 接口的 IPv6 地址。

```
[DeviceC-Tunnel2] ipv6 address 4001::2/64
```

# 配置 Tunnel2 接口的源接口为 GigabitEthernet1/0/1（封装后的 IPv4 报文头中的源 IP 地址为配置的源接口的 IP 地址）。

```
[DeviceC-Tunnel2] source gigabitethernet 1/0/1
```

# 配置 Tunnel1 接口的目的端地址（封装后的 IPv4 报文头中的目的 IP 地址为配置的目的端地址）。

```
[DeviceC-Tunnel2] destination 20.1.1.1
[DeviceC-Tunnel2] quit
```

(2) 配置 OSPFv3

- 配置 Device A

# 配置 Device A 的 Router ID 为 1.1.1.1。

```
[DeviceA] ospfv3
```

```
[DeviceA-ospfv3-1] router-id 1.1.1.1
[DeviceA-ospfv3-1] quit
在 Tunnel1 上开启 OSPFv3
[DeviceA] interface Tunnel 1
[DeviceA-Tunnel1] ospfv3 1 area 0
[DeviceA-Tunnel1] quit
在 Tunnel2 上开启 OSPFv3
[DeviceA] interface Tunnel 2
[DeviceA-Tunnel2] ospfv3 1 area 0
[DeviceA-Tunnel2] quit
在 GigabitEthernet1/0/2 上开启 OSPFv3
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ospfv3 1 area 0
[DeviceA-GigabitEthernet1/0/2] quit
```

- 配置 Device B

# 配置 Device B 的 Router ID 为 2.2.2.2。

```
[DeviceB] ospfv3
[DeviceB-ospfv3-1] router-id 2.2.2.2
[DeviceB-ospfv3-1] quit
```

# 在 Tunnel1 上开启 OSPFv3

```
[DeviceB] interface Tunnel 1
[DeviceB-Tunnel1] ospfv3 1 area 0
[DeviceB-Tunnel1] quit
```

# 在 GigabitEthernet1/0/2 上开启 OSPFv3

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ospfv3 1 area 0
[DeviceB-GigabitEthernet1/0/2] quit
```

- 配置 Device C

# 配置 Device C 的 Router ID 为 3.3.3.3。

```
[DeviceC] ospfv3
[DeviceC-ospfv3-1] router-id 3.3.3.3
[DeviceC-ospfv3-1] quit
```

# 在 Tunnel2 上开启 OSPFv3

```
[DeviceC] interface Tunnel 2
[DeviceC-Tunnel2] ospfv3 1 area 0
[DeviceC-Tunnel2] quit
```

# 在 GigabitEthernet1/0/2 上开启 OSPFv3

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] ospfv3 1 area 0
[DeviceC-GigabitEthernet1/0/2] quit
```

## 3.4 验证配置

# 从 PC2 上可以 ping 通 PC1。

```
D:\>ping6 -s 5001::3 2001::3
```

```
Pinging 2001::3
from 5001::3 with 32 bytes of data:

Reply from 2001::3: bytes=32 time=13ms
Reply from 2001::3: bytes=32 time=1ms
Reply from 2001::3: bytes=32 time=1ms
Reply from 2001::3: bytes=32 time<1ms

Ping statistics for 2001::3:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 13ms, Average = 3ms
从 PC2 上可以 ping 通 PC3。
D:\>ping6 -s 5001::3 6001::3
```

```
Pinging 6001::3
from 6001::3 with 32 bytes of data:

Reply from 6001::3: bytes=32 time=13ms
Reply from 6001::3: bytes=32 time=1ms
Reply from 6001::3: bytes=32 time=1ms
Reply from 6001::3: bytes=32 time<1ms

Ping statistics for 6001::3:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

## 3.5 配置文件

- Device A

```
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
interface GigabitEthernet1/0/1
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ospfv3 1 area 0.0.0.0
 ipv6 address 2001::1/64
#
interface Tunnel1 mode ipv6-ipv4
 ospfv3 1 area 0.0.0.0
 source GigabitEthernet1/0/1
 destination 30.1.1.1
```



```
 ipv6 address 3001::1/64
#
interface Tunnel2 mode ipv6-ipv4
 ospfv3 1 area 0.0.0.0
 source GigabitEthernet1/0/1
 destination 40.1.1.1
 ipv6 address 4001::1/64
```

- **Device B**

```
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
interface GigabitEthernet1/0/1
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ospfv3 1 area 0.0.0.0
 ipv6 address 5001::1/64
#
interface Tunnell mode ipv6-ipv4
 ospfv3 1 area 0.0.0.0
 source GigabitEthernet1/0/1
 destination 20.1.1.1
 ipv6 address 3001::2/64
```

- **Device C**

```
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
interface GigabitEthernet1/0/1
 ip address 40.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ospfv3 1 area 0.0.0.0
 ipv6 address 6001::1/64
#
interface Tunnel2 mode ipv6-ipv4
 ospfv3 1 area 0.0.0.0
 source GigabitEthernet1/0/1
 destination 20.1.1.1
 ipv6 address 4001::2/64
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

# H3C MSR 系列路由器

## 授权 ARP 功能配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 授权 ARP 功能在 DHCP 服务器上配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	1
3.3 配置步骤.....	1
3.3.1 Router 的配置.....	1
3.3.2 主机的配置.....	2
3.4 验证配置.....	2
3.5 配置文件.....	3
4 授权 ARP 功能在 DHCP 中继上配置举例.....	3
4.1 组网需求.....	3
4.2 配置思路.....	3
4.3 使用版本.....	3
4.4 配置步骤.....	3
4.4.1 Router A 的配置.....	3
4.4.2 Router B 的配置.....	4
4.4.3 主机的配置.....	4
4.5 验证配置.....	4
4.6 配置文件.....	5
5 参考资料.....	6

# 1 简介

本文档介绍 MSR 系列路由器授权 ARP 功能典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

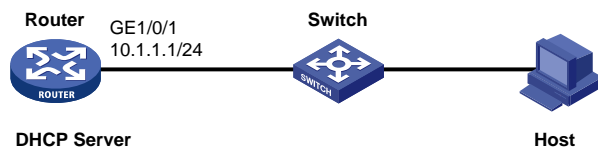
本文档假设您已了解授权 ARP 特性。

## 3 授权 ARP 功能在 DHCP 服务器上配置举例

### 3.1 组网需求

如[图 1](#)所示，Router 是 DHCP 服务器，为同一网段中的主机动态分配 IP 地址。现要求：启用授权 ARP 功能保证必须是通过 Router 分配 IP 地址的主机才能够通过 Router 访问外网。

图1 授权 ARP 功能在 DHCP 服务器上配置举例组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置步骤

#### 3.3.1 Router 的配置

# 配置接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[Router-GigabitEthernet1/0/1] quit
```

# 使能 DHCP 服务。

```
[Router] dhcp enable
```

# 配置 DHCP 地址池 1 动态分配的主地址网段为 10.1.1.0/24。

```
[Router] dhcp server ip-pool 1
[Router-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[Router-dhcp-pool-1] quit
使能接口授权 ARP 功能。
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] arp authorized enable
[Router-GigabitEthernet1/0/1] quit
```

### 3.3.2 主机的配置

配置主机 Host 的网卡自动获取 IP 地址。

### 3.4 验证配置

按照如上配置，主机通过 DHCP 获取 IP 地址，Router 记录授权 ARP 表项。

# 在主机 Host 上发现网卡通过 DHCP 方式动态获取到 IP 地址。

```
C:\Windows\System32>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter ???? 3:
```

```

Connection-specific DNS Suffix :
Link-local IPv6 Address : fe80::d083:44cb:9d9b:71b7%21
IPv4 Address. : 10.1.1.2
Subnet Mask : 255.255.255.0
Default Gateway : 10.1.1.1
```

# Host 获得 Router 分配的 IP 后，在 Router 上查看授权 ARP 信息。

```
[Router] display arp all
```

```

Type: S-Static D-Dynamic M-Multiport I-Invalid
IP address MAC address VLAN Interface Aging Type
10.1.1.2 000f-e123-4568 N/A GE1/0/1 18 D
```

# 将 Host 与 Switch 断开连接，修改 Host 的 IP 地址为静态地址，且与 Router 在同一网段，重新连接 Host 与 Switch，发现 Host 与 Router 不能互通。

```
C:\Windows\System32>ping 10.1.1.1
```

```
Pinging 10.1.1.1 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 10.1.1.1:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

# 通过命令 **display arp all** 查看 Router 的 ARP 授权表项。

```
[Router] display arp all
```

	Type: S-Static	D-Dynamic	M-Multiport	I-Invalid	
IP address	MAC address	VLAN	Interface		Aging Type

### 3.5 配置文件

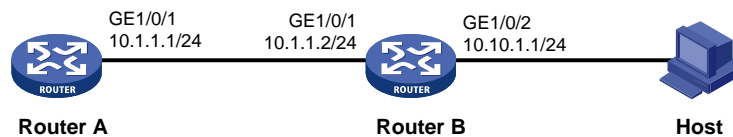
```
#
dhcp enable
#
dhcp server ip-pool 1
network 10.1.1.0 mask 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.1.1.1 255.255.255.0
arp authorized enable
#
```

## 4 授权 ARP 功能在 DHCP 中继上配置举例

### 4.1 组网需求

如图 2 所示，主机 Host 通过 DHCP 中继 Router B 与 DHCP 服务器 Router A 通信获取 IP 地址。现要求：在 DHCP Relay 上启用授权 ARP 功能保证客户端的合法性。

图2 授权 ARP 功能在 DHCP 中继上配置举例组网图



### 4.2 配置思路

配置 DHCP 中继用户地址表项记录功能与授权 ARP 配合，实现只允许匹配用户地址表项中绑定关系的报文通过 DHCP 中继。从而，保证非法主机不能通过 DHCP 中继与外部网络通信。

### 4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 4.4 配置步骤

#### 4.4.1 Router A 的配置

```
配置接口的 IP 地址。
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
```

```
[RouterA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/1] quit
使能 DHCP 服务。
[RouterA] dhcp enable
配置 DHCP 地址池 1 动态分配的主地址网段为 10.10.1.0/24。
[RouterA] dhcp server ip-pool 1
[RouterA-dhcp-pool-1] network 10.10.1.0 mask 255.255.255.0
[RouterA-dhcp-pool-1] gateway-list 10.10.1.1
[RouterA-dhcp-pool-1] quit
配置静态路由，其目的地址为 10.10.1.0/24，下一跳为 10.1.1.2。
[RouterA] ip route-static 10.10.1.0 24 10.1.1.2
```

#### 4.4.2 Router B 的配置

```
使能 DHCP 服务。
<RouterB> system-view
[RouterB] dhcp enable
配置接口的 IP 地址。
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[RouterB-GigabitEthernet0/0] quit
[RouterB] interface GigabitEthernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ip address 10.10.1.1 24
配置 GigabitEthernet1/0/2 接口工作在 DHCP 中继模式。
[RouterB-GigabitEthernet1/0/1] dhcp select relay
配置 GigabitEthernet1/0/2 接口对应 DHCP 服务器地址。
[RouterB-GigabitEthernet1/0/2] dhcp relay server-address 10.1.1.1
使能接口授权 ARP 功能。
[RouterB-GigabitEthernet1/0/2] arp authorized enable
[RouterB-GigabitEthernet1/0/2] quit
开启 DHCP 中继用户地址表项记录功能。
[RouterB] dhcp relay client-information record
```

#### 4.4.3 主机的配置

配置主机 Host 的网卡自动获取 IP 地址。

### 4.5 验证配置

# 在主机 Host 上发现网卡通过 DHCP 方式动态获取到 IP 地址。

```
C:\Windows\System32>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter ????: 3:
```



```

Connection-specific DNS Suffix :
Link-local IPv6 Address : fe80::d083:44cb:9d9b:71b7%21
IPv4 Address : 10.10.1.2
Subnet Mask : 255.255.255.0
Default Gateway : 10.10.1.1

```

# Host 获得 Router A 分配的 IP 后，在 Router B 查看授权 ARP 信息。

```

[RouterB] display arp all
 Type: S-Static D-Dynamic M-Multiport I-Invalid
IP address MAC address VLAN Interface Aging Type
10.1.1.1 0cda-41c7-057e N/A GE1/0/1 15 D
10.10.1.2 0066-61e2-f7f2 N/A GE1/0/2 20 D

```

# 将 Host 与 Router B 断开连接，修改 Host 的 IP 地址为静态地址，且与 Router B 在同一网段，重新连接 Host 与 Router B，发现 Host 与 Router B 不能互通。

```
C:\Windows\System32> ping 10.10.1.1
```

```
Pinging 10.10.1.1 with 32 bytes of data:
```

```

Request timed out.
Request timed out.
Request timed out.
Request timed out.

```

```
Ping statistics for 10.10.1.1:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

# 通过命令 **display arp all** 在 Router B 查看授权 ARP 信息。

```

[RouterB] display arp all
 Type: S-Static D-Dynamic M-Multiport I-Invalid
IP address MAC address VLAN Interface Aging Type
10.1.1.1 0cda-41c7-057e N/A GE1/0/1 15 D

```

## 4.6 配置文件

- Router A:

```

#
dhcp enable
#
dhcp server ip-pool 1
network 10.10.1.0 mask 255.255.255.0
gateway-list 10.10.1.1
#
interface GigabitEthernet1/0/1
port link-mode route
combo enable copper
ip address 10.1.1.1 255.255.255.0
#
ip route-static 10.10.1.0 24 10.1.1.2
#

```

- Router B:

```
#
dhcp enable
dhcp relay client-information record
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 10.10.1.1 255.255.255.0
arp authorized enable
dhcp select relay
dhcp relay server-address 10.1.1.1
#
```

## 5 参考资料

- 《H3C MSR 系列路由器 配置指导 (V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考 (V7)》中的“三层技术-IP 业务命令参考”
- 《H3C MSR 系列路由器 配置指导 (V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考 (V7)》中的“安全命令参考”

# H3C MSR 系列路由器

## ARP 防攻击特性配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介	1
2 配置前提	1
3 ARP 自动扫描和固化功能配置举例	1
3.1 组网需求	1
3.2 使用版本	2
3.3 配置步骤	2
3.4 验证配置	2
3.5 配置文件	3
4 ARP 主动确认功能配置举例	3
4.1 组网需求	3
4.2 使用版本	4
4.3 配置步骤	4
4.4 验证配置	4
4.5 配置文件	5
5 源 MAC 固定的 ARP 攻击检测功能配置举例	5
5.1 组网需求	5
5.2 配置思路	5
5.3 使用版本	6
5.4 配置步骤	6
5.5 验证配置	6
5.6 配置文件	7
6 ARP 源抑制功能配置举例	7
6.1 组网需求	7
6.2 使用版本	8
6.3 配置步骤	8
6.4 验证配置	9
6.5 配置文件	9
7 相关资料	10

# 1 简介

本文档介绍 MSR 系列路由器 ARP 防攻击特性典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 ARP 攻击防御特性。

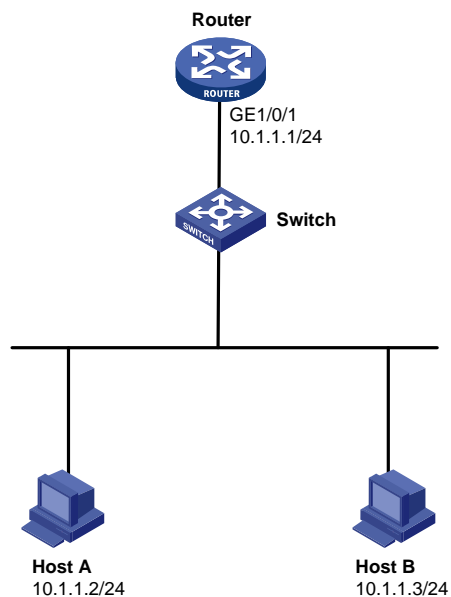
## 3 ARP 自动扫描和固化功能配置举例

### 3.1 组网需求

如图 1 所示，局域网内的主机 Host A 通过网关 Router 连接到外网。现要求：

- Router 通过 ARP 自动扫描功能建立局域网内主机 Host A 的动态 ARP 表项，然后通过 ARP 固化功能将动态 ARP 表项转换为静态 ARP 表项。
- 固化完成后，禁止网关学习动态 ARP 表项，新增主机 Host B 无法访问网关。

图1 ARP 自动扫描和固化功能配置举例组网图



## 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.3 配置步骤

# 配置接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 10.1.1.1 24
```

# 接口上启用 ARP 自动扫描功能（该命令只做执行，不生成配置文件）。

```
[Router-GigabitEthernet1/0/1] arp scan
This operation may take a long time to collect these ARP entries, and you can press CTRL_C
to break. Please specify a right range. C
ontinue? [Y/N]: y
Scanning ARP. Please wait...
Scanning is complete.
```

```
[Router-GigabitEthernet1/0/1]quit
```

# 当组网中仅有主机 Host A 时，启动扫描功能后，通过命令 **display arp** 查看网关路由器 Router 进行 ARP 扫描后学习到的 ARP 表项。

```
[Router] display arp
 Type: S-Static D-Dynamic M-Multiport I-Invalid
IP address MAC address VLAN Interface Aging Typ
10.1.1.2 0015-e943-7e6a N/A N/A N/A D
```

# 使用 ARP 固化将动态 ARP 转换为静态 ARP（该命令只做执行，不生成配置文件）。

```
[Router] arp fixup
Fixup ARP. Please wait...
Fixup is complete.
```

# 启动固化功能后，通过命令 **display arp** 查看网关路由器 Router 进行 ARP 固化后 ARP 表项。

```
[Router] display arp
 Type: S-Static D-Dynamic M-Multiport I-Invalid
IP address MAC address VLAN Interface Aging Type
10.1.1.2 0015-e943-7e6a N/A N/A N/A S
```

# 配置禁止接口 GigabitEthernet1/0/1 学习动态 ARP。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] arp max-learning-num 0
[Router-GigabitEthernet1/0/1] quit
```

## 3.4 验证配置

# 局域网中新增主机 Host B，查看 ARP 表项，没有 Host B 的 ARP 表项。

```
[Router] display arp
 Type: S-Static D-Dynamic M-Multiport I-Invalid
IP address MAC address VLAN Interface Aging Typ
10.1.1.2 0015-e943-7e6a N/A N/A N/A S
```

# 在 Host B 上 ping 不通网关。

```
C:\> ping 10.1.1.1
Pinging 10.1.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.1.1.1:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

### 3.5 配置文件

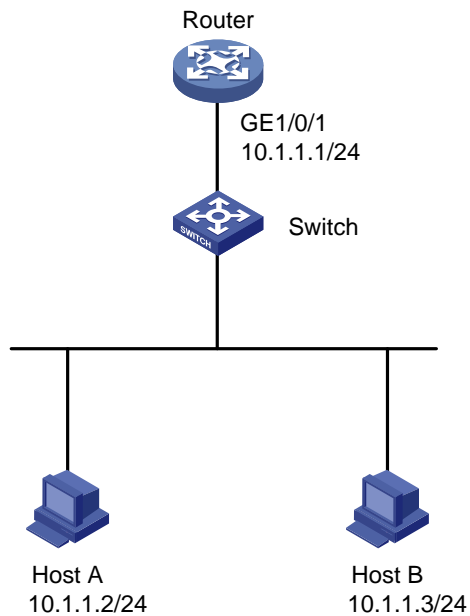
```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.1.1.1 255.255.255.0
arp max-learning-num 0
#
```

## 4 ARP 主动确认功能配置举例

### 4.1 组网需求

如图2所示，局域网中的主机 Host A 通过 Router 作为网关连接到外网。现要求：网关上启用 ARP 主动确认功能，防止攻击者使用仿冒 ARP 报文欺骗网关设备。

图2 ARP 主动确认功能配置举例组网图



## 4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.3 配置步骤

# 配置接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[Router-GigabitEthernet1/0/1] quit
```

# 配置 ARP 主动确认功能。

```
[Router] arp active-ack enable
```

## 4.4 验证配置

# 查看网关的 ARP 表项显示有 Host A 对应的 ARP 表项。

```
[Router] display arp
 Type: S-Static D-Dynamic M-Multiport I-Invalid
IP address MAC address VLAN Interface Aging Typ
10.1.1.2 000f-e123-4568 N/A GE1/0/1 20 D
```

# 打开 ARP 的报文调试信息开关。

```
<Router> terminal debugging
The current terminal is enabled to display debugging logs.
<Router> debugging arp packet
```

# 新增一台主机 Host B 仿冒 Host A 向网关发送伪造的 ARP 请求报文，其中 ARP 报文中的源 MAC 修改为 0086-0005-0004。网关 Router A 收到该 ARP 报文后，发现该报文对应的 ARP 表项的刷新时间超过一分钟，启用 ARP 表项正确性检查，网关会发送一个单播 ARP 请求报文（报文的目的 IP 地址、目的 MAC 地址采用 ARP 表项中的源 IP 地址、源 MAC 地址），如果在随后的 5s 内收到 ARP 应答报文，将对前期收到的 ARP 报文与此次收到的 ARP 应答报文进行比较（比较内容包括：源 IP 地址、源 MAC 地址）。在一定时间内收到的 ARP 应答报文：

```
*Jul 3 18:07:38:660 2013 Router ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender
MAC: 0086-0005-0004, sender IP: 10.1.1.2, target MAC: 0cda-41c7-057f, target IP: 10.1.1.1
*Jul 3 18:07:38:660 2013 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender
MAC: 0cda-41c7-057f, sender IP: 10.1.1.1, target MAC: 000f-e123-4568, target IP: 10.1.1.2
*Jul 3 18:07:38:660 2013 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 2, sender
MAC: 0cda-41c7-057f, sender IP: 10.1.1.1, target MAC: 0086-0005-0004, target IP: 10.1.1.2
*Jul 3 18:07:38:660 2013 Router ARP/7/ARP_RCV: Received an ARP message, operation: 2, sender
MAC: 000f-e123-4568, sender IP: 10.1.1.2, target MAC: 0cda-41c7-057f, target IP: 10.1.1.1
```

# 后收到的 ARP 报文是 Host A 发送的，该报文与 ARP 表项中的 IP 地址、MAC 地址一致，网关认为前期收到的 ARP 报文为攻击报文，通过命令 **display arp** 查看网关路由器的 ARP 表项不更新。

```
<Router> display arp
 Type: S-Static D-Dynamic M-Multiport I-Invalid
IP address MAC address VLAN Interface Aging Type
10.1.1.2 000f-e123-4568 N/A GE0/1 20 D
```



## 4.5 配置文件

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
#
arp active-ack enable
#
```

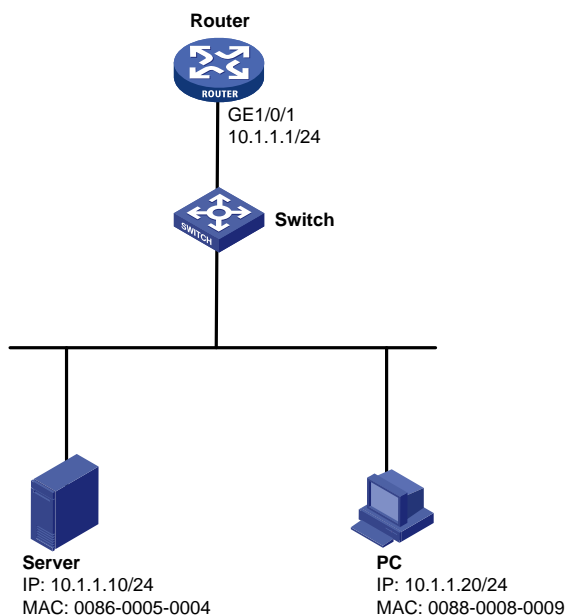
## 5 源 MAC 固定的 ARP 攻击检测功能配置举例

### 5.1 组网需求

如图 3 所示，局域网内服务器和主机通过网关 Router 与外部网络通信。在网关上使能源 MAC 固定的 ARP 攻击检测功能，具体需求如下：

- 对普通 PC，固定的时间（5 秒）内收到源 MAC 地址固定的 ARP 报文超过 30 时，会打印 Log 信息并对来自 PC 的 ARP 报文进行过滤。
- 配置服务器 Server 的 MAC 为保护 MAC，使服务器可以对网关发送大量 ARP 报文。

图3 源 MAC 固定的 ARP 攻击检测功能配置举例组网图



### 5.2 配置思路

为了使路由器在检测到 ARP 攻击时能够打印告警信息，并将由攻击源发送的 ARP 报文过滤掉，需要在开启源 MAC 固定 ARP 攻击检测功能时同时选择过滤模式。

## 5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 5.4 配置步骤

```
使能源 MAC 固定 ARP 攻击检测功能，并选择过滤模式。
<Router> system-view
[Router] arp source-mac filter
配置源 MAC 固定 ARP 报文攻击检测阈值为 30 个。
[Router] arp source-mac threshold 30
配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。
[Router] arp source-mac aging-time 60
将 0086-0005-0004 配置为保护 MAC。
[Router] arp source-mac exclude-mac 0086-0005-0004
配置接口 IP 地址。
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[Router-GigabitEthernet1/0/1] quit
```

## 5.5 验证配置

```
打开 ARP 的报文调试信息开关。
<Router> terminal debugging
The current terminal is enabled to display debugging logs.
<Router> debugging arp packet
PC 向网关设备 Router 发送 ARP 报文，发送频率为 6 个/秒，相当于 5 秒 30 个，设备上不打印 log 信息，未生成 ARP 防攻击检测表项。
<Router> display arp source-mac
Source-MAC VLAN ID Interface Aging-time
PC 向网关设备 Router 发送 ARP 报文，发送频率为 10 个/秒，相当于 5 秒 50 个同时生成 ARP 防攻击检测表项。
<Router> display arp source-mac
Source-MAC VLAN ID Interface Aging-time
0088-0008-0009 N/A GE0/1 48
此时设备上打印 log 信息如下。
*Jun 20 13:54:42:482 2013 Router ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0088-0008-0009, sender IP: 10.1.1.20, target MAC: 0cda-41c7-057f, target IP: 10.1.1.1
*Jun 20 13:54:42:482 2013 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 2, sender MAC: 0cda-41c7-057f, sender IP: 10.1.1.1, target MAC: 0088-0008-0009, target IP: 10.1.1.20
*Jun 20 13:54:42:582 2013 Router ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0088-0008-0009, sender IP: 10.1.1.20, target MAC: 0cda-41c7-057f, target IP: 10.1.1.1
```

```
*Jun 20 13:54:42:582 2013 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 2, sender MAC: 0cda-41c7-057f, sender IP: 10.1.1.1, target MAC: 0088-0008-0009, target IP: 10.1.1.20
```

```
*Jun 20 13:54:42:682 2013 Router ARP/7/ARP_RCV: Received an ARP message, operation: 1, sender MAC: 0088-0008-0009, sender IP: 10.1.1.20, target MAC: 0cda-41c7-057f, target IP: 10.1.1.1
```

```
*Jun 20 13:54:42:682 2013 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 2, sender MAC: 0cda-41c7-057f, sender IP: 10.1.1.1, target MAC: 0088-0008-0009, target IP: 10.1.1.20
```

# Server 向网关设备 Router 发送 ARP 报文，发送频率为 10 个/秒，相当于 5 秒 50 个，设备上不打印 log 信息，未生成 ARP 防攻击检测表项。

```
<Router> display arp source-mac
```

```
Source-MAC VLAN ID Interface Aging-time
```

## 5.6 配置文件

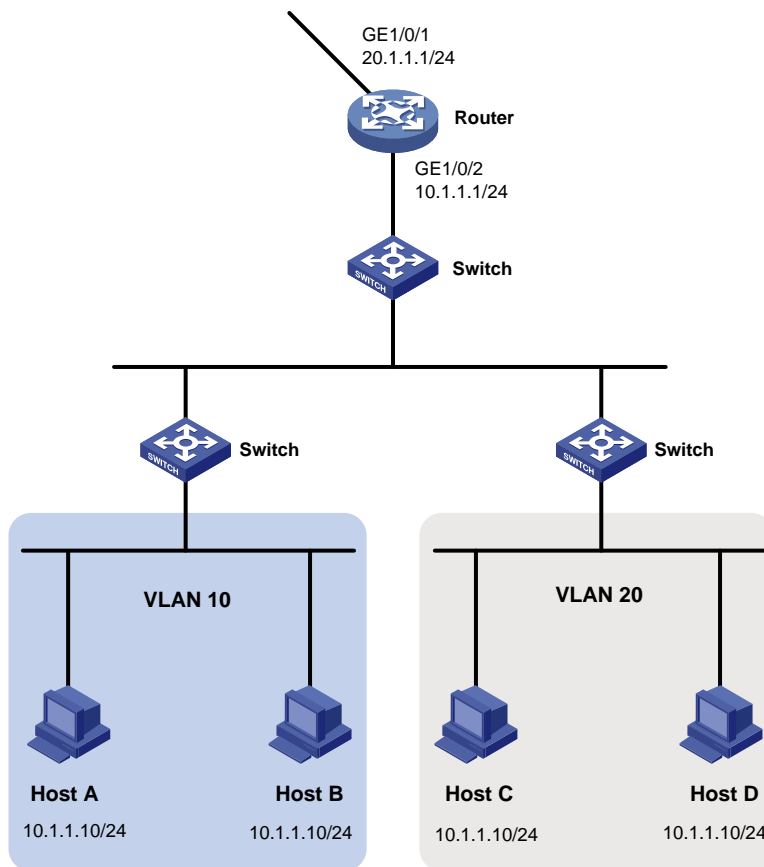
```
#
interface GigabitEthernet1/0/1
 portlink-mode route
 shutdown
 ip address 10.1.1.1 255.255.255.0
#
 arp source-mac filter
 arp source-mac aging-time 60
 arp source-mac exclude-mac 0086-0005-0004
#
```

## 6 ARP 源抑制功能配置举例

### 6.1 组网需求

如图 4 所示，某局域网内属于 VLAN 10 和 VLAN 20 的主机通过接入交换机连接到网关 Router 与外部网络通信。现要求：开启 ARP 源抑制功能，防止恶意用户使用同一源 IP 地址发送大量目标 IP 地址不能解析的 IP 报文来攻击设备。

图4 ARP 源抑制功能配置举例组网图



## 6.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 6.3 配置步骤

# 配置接口 IP 地址

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 20.1.1.1 24
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.1.1.1 24
[Router-GigabitEthernet1/0/2] quit
```

# 使能 ARP 源抑制功能。

```
[Router] arp source-suppression enable
```

# 配置 ARP 源抑制的阈值为 2。

```
[Router] arp source-suppression limit 2
```

## 6.4 验证配置

# Host D 向网关设备 Router A 发送目的 IP 为 20.1.1.2 的 IP 报文，20.1.1.2 这个地址在该局域网中不存在，验证网关设备在使能 ARP 源抑制情况下对 ARP 报文的处理情况。

# 打开 ARP 的报文调试信息开关。

```
<Router> terminal debugging
The current terminal is enabled to display debugging logs.
<Router> debugging arp packet
*Jul 23 17:29:03:061 2014 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 1,
sender MAC: d07e-28e6-6814, sender IP: 20.1.1.1, target MAC: 0000-0000-0000, tar
get IP: 20.1.1.2
*Jul 23 17:29:05:262 2014 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 1,
sender MAC: d07e-28e6-6814, sender IP: 20.1.1.1, target MAC: 0000-0000-0000, tar
get IP: 20.1.1.2
*Jul 23 17:29:07:462 2014 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 1,
sender MAC: d07e-28e6-6814, sender IP: 20.1.1.1, target MAC: 0000-0000-0000, tar
get IP: 20.1.1.2
*Jul 23 17:29:09:662 2014 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 1,
sender MAC: d07e-28e6-6814, sender IP: 20.1.1.1, target MAC: 0000-0000-0000, tar
get IP: 20.1.1.2
*Jul 23 17:29:11:862 2014 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 1,
sender MAC: d07e-28e6-6814, sender IP: 20.1.1.1, target MAC: 0000-0000-0000, tar
get IP: 20.1.1.2
*Jul 23 17:29:14:062 2014 Router ARP/7/ARP_SEND: Sent an ARP message, operation: 1,
sender MAC: d07e-28e6-6814, sender IP: 20.1.1.1, target MAC: 0000-0000-0000, tar
get IP: 20.1.1.2
```

通过调试信息发现，网络中每 5 秒内从某 IP 地址向设备发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值 2 时，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。

## 6.5 配置文件

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
#
 arp source-suppression enable
 arp source-suppression limit 2
#
```

## 7 相关资料

- 《H3C MSR 系列路由器 配置指导 (V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考 (V7)》中的“安全命令参考”

# H3C MSR 系列路由器

## ACL 配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 通过 MAC 地址过滤流量配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	1
3.3 配置思路.....	2
3.4 配置步骤.....	2
3.5 验证配置.....	2
3.6 配置文件.....	3
4 通过 IP 地址过滤流量配置举例.....	3
4.1 组网需求.....	3
4.2 使用版本.....	4
4.3 配置思路.....	4
4.4 配置步骤.....	4
4.5 验证配置.....	5
4.6 配置文件.....	6
5 通过指定的 TCP 协议过滤流量配置举例.....	7
5.1 组网需求.....	7
5.2 使用版本.....	8
5.3 配置思路.....	8
5.4 配置步骤.....	8
5.5 验证配置.....	9
5.6 配置文件.....	10
6 相关资料.....	11



# 1 简介

本文档介绍了 ACL（Access Control List，访问控制列表）的配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

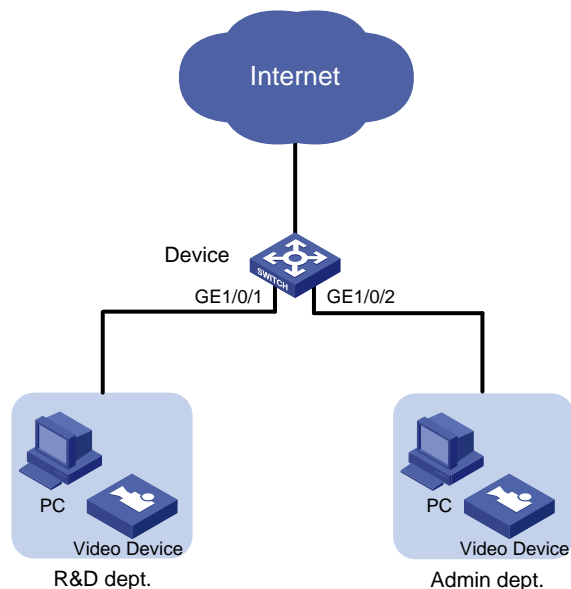
本文假设您已了解 ACL 特性。

## 3 通过 MAC 地址过滤流量配置举例

### 3.1 组网需求

如图 1 所示，研发部和管理部均部署了网络视频设备，这些视频设备的 MAC 地址为 000f-e2xx-xxxx，现要求限制这些设备仅每天的 8:30 到 18:00 才能够向外网发送数据。

图1 通过 MAC 地址过滤流量配置组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置思路

在受限设备的 IP 地址不定时，可以通过 MAC 地址来进行匹配；而对于具有相同 MAC 地址前缀的多台设备，也可以通过 MAC 地址掩码的方式来进行同时匹配。

### 3.4 配置步骤

# 配置接口的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ip address 10.1.2.1 24
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] ip address 200.1.1.2 24
[Device-GigabitEthernet1/0/3] quit
```

# 配置时间段 time1，时间范围为每天的 8:30~18:00。

```
[Device] time-range time1 8:30 to 18:00 daily
```

# 创建二层 ACL 4000，定义规则为在 time1 时间段内允许源 MAC 地址前缀为 000f-e2 的所有报文通过，其他时间拒绝。

```
[Device] acl number 4000
[Device-acl-ethernetframe-4000] rule permit source-mac 000f-e200-0000 ffff-ff00-0000
time-range time1
[Device-acl-ethernetframe-4000] rule deny source-mac 000f-e200-0000 ffff-ff00-0000
[Device-acl-ethernetframe-4000] quit
```

# 配置包过滤功能，应用二层 ACL 4000 对端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 收到的报文进行过滤。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] packet-filter 4000 inbound
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] packet-filter 4000 inbound
[Device-GigabitEthernet1/0/2] quit
```

# 配置到外网的缺省路由。

```
[Device] ip route-static 0.0.0.0 0.0.0.0 200.1.1.1
```

### 3.5 验证配置

# 执行 **display packet-filter** 命令查看包过滤功能的应用状态。

```
[Device] display packet-filter interface inbound
Interface: GigabitEthernet1/0/1
In-bound policy:
 ACL 4000
 MAC default action: Permit
```

```
Interface: GigabitEthernet1/0/2
In-bound policy:
ACL 4000
MAC default action: Permit
```

上述信息显示 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 端口上已经正确应用了包过滤功能。在每天的 8:30 到 18:00 时间段内，视频设备可以正常与外网中的设备进行通信；在其它时间段内，视频设备无法与外网中的设备进行通信。

## 3.6 配置文件

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 10.1.1.1 255.255.255.0
 packet-filter 4000 inbound
#
interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip address 10.1.2.1 255.255.255.0
 packet-filter 4000 inbound
#
interface GigabitEthernet1/0/3
 port link-mode route
 combo enable copper
 ip address 200.1.1.2 255.255.255.0
#
 ip route-static 0.0.0.0 0 200.1.1.1
#
 time-range timel 08:30 to 18:00 daily
#
acl number 4000
 rule 0 permit source-mac 000f-e200-0000 ffff-ff00-0000 time-range timel
 rule 5 deny source-mac 000f-e200-0000 ffff-ff00-0000
```

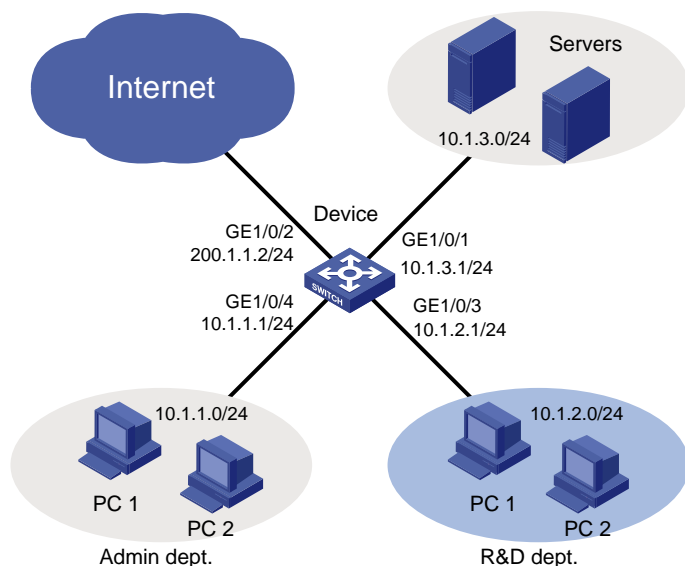
## 4 通过 IP 地址过滤流量配置举例

### 4.1 组网需求

如图 2 所示，某公司的网络分成管理部、研发部和服务器三个区域，通过 Device 设备与 Internet 连接。现要求通过 ACL 实现：

- 管理部任意时间都可以访问 Internet 和服务器，但不能访问研发部；
- 研发部在工作时间（周一至周五的 8:30~18:00）只能访问服务器，不能访问 Internet 和管理部；非工作时间可以访问 Internet 和服务器，但不能访问管理部。

图2 通过 IP 地址过滤流量配置组网图



## 4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.3 配置思路

- 为实现管理部不能访问研发部，需要创建 ACL 配置规则拒绝目的地址为 10.1.2.0/24 的报文，在 Device 的 GigabitEthernet1/0/4 的入方向进行过滤；
- 为实现研发部在工作时间只能访问服务器，需要创建 ACL 配置规则只允许目的地址为 10.1.3.0/24 的报文通过，并指定规则的生效时间段，在 Device 的 GigabitEthernet1/0/3 的入方向上进行过滤；
- 为实现研发部在非工作时间不能访问管理部，需要创建 ACL 配置规则拒绝目的地址为 10.1.1.0/24 的报文，在 Device 的 GigabitEthernet1/0/3 的入方向上进行过滤；
- 缺省情况下，ACL 规则的匹配顺序为配置顺序，因此在此例中，需要先创建指定时间段内只允许目的地址为 10.1.3.0/24 报文通过的规则，再创建指定时间段内拒绝其他报文通过的规则。

## 4.4 配置步骤

(1) 配置接口的 IP 地址

# 配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ip address 200.1.1.2 24
[Device-GigabitEthernet1/0/2] quit
```

# 请参考以上方法配置其他接口的 IP 地址，具体配置步骤省略。

(2) 配置到外网的缺省路由

```

[Device] ip route-static 0.0.0.0 0.0.0.0 200.1.1.1
(3) 配置管理部的网络权限
创建 IPv4 高级 ACL 3000。
[Device] acl number 3000
创建规则，过滤目的地址为 10.1.2.0/24 网段的报文。
[Device-acl-adv-3000] rule deny ip destination 10.1.2.0 0.0.0.255
[Device-acl-adv-3000] quit
配置包过滤功能，应用 IPv4 高级 ACL 3000 对端口 GigabitEthernet1/0/4 收到的 IP 报文进行过滤。
[Device] interface gigabitethernet 1/0/4
[Device-GigabitEthernet1/0/4] packet-filter 3000 inbound
[Device-GigabitEthernet1/0/4] quit
(4) 配置研发部的网络权限
配置时间段 worktime，指定周一至周五的 8:30~18:00 为工作时间。
[Device] time-range worktime 8:30 to 18:00 working-day
创建 IPv4 高级 ACL 3001。
[Device] acl number 3001
创建规则，允许时间段内目的地址为 10.1.3.0/24 网段的报文通过。
[Device-acl-adv-3001] rule permit ip destination 10.1.3.0 0.0.0.255 time-range worktime
创建规则，过滤时间段内其他的报文。
[Device-acl-adv-3001] rule deny ip time-range worktime
创建规则，过滤目的地址为 10.1.1.0/24 网段的报文。
[Device-acl-adv-3001] rule deny ip destination 10.1.1.0 0.0.0.255
[Device-acl-adv-3001] quit
配置包过滤功能，应用 IPv4 高级 ACL 3001 对端口 GigabitEthernet1/0/3 收到的 IP 报文进行过滤。
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] packet-filter 3001 inbound
[Device-GigabitEthernet1/0/3] quit

```

## 4.5 验证配置

# 执行 **display packet-filter** 命令查看包过滤功能的应用状态。

```

[Device] display packet-filter interface inbound
Interface: GigabitEthernet1/0/3
In-bound policy:
ACL 3001
IPv4 default action: Permit
Interface: GigabitEthernet1/0/4
In-bound policy:
ACL 3000
IPv4 default action: Permit

```

上述信息显示 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 端口上已经正确应用了包过滤功能。

# 在周一的上午 9:30, 从研发部的某台电脑上 ping Internet 上某个网站 (此网站仅为示例, 请根据实际情况进行验证), 结果无法 ping 通。

```
C:\>ping www.abc.com
```

```
Pinging www.abc.com [199.181.132.250] with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 199.181.132.250:
```

```
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>
```

# 在周一的上午 9:30, 从管理部的某台电脑上 ping Internet 上某个网站, 结果可以 ping 通。

```
C:\>ping www.abc.com
```

```
Pinging www.abc.com [199.181.132.250] with 32 bytes of data:
```

```
Reply from 199.181.132.250: bytes=32 time=1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122
```

```
Ping statistics for 199.181.132.250:
```

```
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>
```

# 在周一的晚上 19:30, 从研发部的某台电脑上 ping Internet 上某个网站, 结果可以 ping 通。

```
C:\>ping www.abc.com
```

```
Pinging www.abc.com [199.181.132.250] with 32 bytes of data:
```

```
Reply from 199.181.132.250: bytes=32 time=1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122
Reply from 199.181.132.250: bytes=32 time<1ms TTL=122
```

```
Ping statistics for 199.181.132.250:
```

```
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>
```

## 4.6 配置文件

```
#
```

```

interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip address 200.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 10.1.3.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 combo enable copper
 ip address 10.1.2.1 255.255.255.0
 packet-filter 3001 inbound
#
interface GigabitEthernet1/0/4
 port link-mode route
 combo enable copper
 ip address 10.1.1.1 255.255.255.0
 packet-filter 3000 inbound
#
 ip route-static 0.0.0.0 0 200.1.1.1
#
 time-range worktime 08:30 to 18:00 working-day
#
acl number 3000
 rule 0 deny ip destination 10.1.2.0 0.0.0.255
#
acl number 3001
 rule 0 permit ip destination 10.1.3.0 0.0.0.255 time-range worktime
 rule 5 deny ip time-range worktime
 rule 10 deny ip destination 10.1.1.0 0.0.0.255
#

```

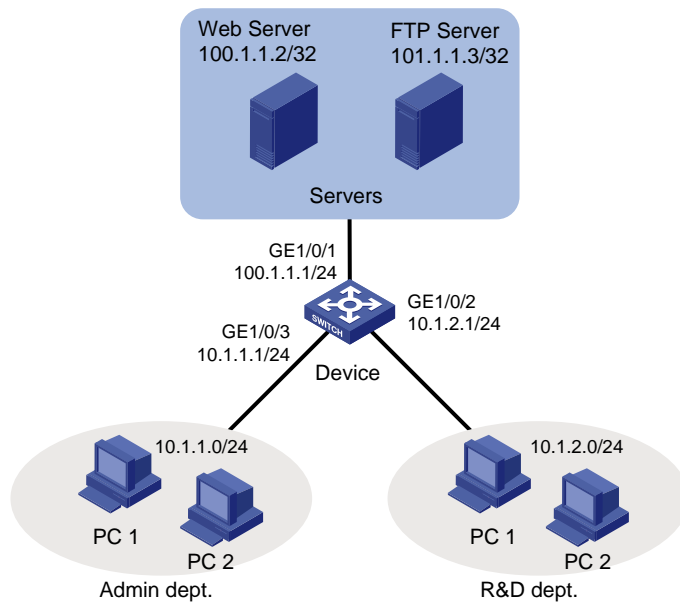
## 5 通过指定的 TCP 协议过滤流量配置举例

### 5.1 组网需求

如图 3 所示，某公司的网络分成管理部、研发部和服务器三个区域，通过 Device 设备互相连接。现要求通过 ACL 实现：

- Web 服务器只能向管理部的主机提供 HTTP 服务，且仅允许由主机向服务器发起和建立 TCP 连接，不允许由服务器向主机发起 TCP 连接；
- FTP 服务器只能向研发部的主机提供 FTP 服务，主机与 FTP 服务器之间进行通信时，不对 TCP 连接发起方进行限制；

图3 通过指定的 TCP 协议过滤流量配置组网图



## 5.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 5.3 配置思路

- 为了实现主机与 Web 服务器之间进行通信时，仅允许由主机向 Web 服务器发起和建立 TCP 连接，需要在高级 ACL 的规则中，指定 **established** 参数，用于匹配 TCP 报文头中 ACK 或 RST 置位的报文，即在已建立的 TCP 连接上传输的报文。
- 由于 TCP 连接发起方一般使用大于 1023 的 TCP 端口号，因此，由 Web 服务器向主机发送的端口号大于 1023、且 ACK 或 RST 位置位的报文，应视作已经存在的 TCP 连接，应该允许通过。其余的由 Web 服务器向主机发送的 TCP 报文都应拒绝通过。
- 要过滤 FTP 报文，需要同时拒绝 FTP 数据报文（TCP 端口号 20）和控制报文（TCP 端口号 21）通过。
- 要过滤 HTTP 服务，需要配置拒绝 TCP 目的端口号为 80 的报文（HTTP）通过的规则。

## 5.4 配置步骤

(1) 配置接口的 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] ip address 100.1.1.1 24
```

# 请参考以上方法配置其他接口的 IP 地址，具体配置步骤省略。

(2) 配置管理部的网络权限



# 创建 IPv4 高级 ACL 3000。

```
<Device> system-view
```

```
[Device] acl number 3000
```

# 创建规则，允许源地址为 100.1.1.2、目的地址为 10.1.1.0/24 网段、目的 TCP 端口号大于 1023、且 ACK 或 RST 位置位的报文通过。

```
[Device-acl-adv-3000] rule permit tcp established source 100.1.1.2 0 destination 10.1.1.0 0.0.0.255 destination-port gt 1023
```

# 创建规则，拒绝源地址为 100.1.1.0/24、目的地址为 10.1.1.0/24 网段的 TCP 报文通过。

```
[Device-acl-adv-3000] rule deny tcp source 100.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

# 创建规则，拒绝源地址为 100.1.1.3 的 FTP 报文通过。

```
[Device-acl-adv-3000] rule deny tcp source 100.1.1.3 0 source-port range 20 21
```

```
[Device-acl-adv-3000] quit
```

# 配置包过滤功能，应用 IPv4 高级 ACL 3000 对端口 GigabitEthernet1/0/3 发出的报文进行过滤。

```
[Device] interface gigabitethernet 1/0/3
```

```
[Device-GigabitEthernet1/0/3] packet-filter 3000 outbound
```

```
[Device-GigabitEthernet1/0/3] quit
```

### (3) 配置研发部的网络权限

# 创建 IPv4 高级 ACL 3001，配置规则拒绝源地址为 100.1.1.2 的 HTTP 报文通过。

```
[Device] acl number 3001
```

```
[Device-acl-adv-3001] rule deny tcp source 100.1.1.2 0 source-port eq 80
```

```
[Device-acl-adv-3001] quit
```

# 配置包过滤功能，应用 IPv4 高级 ACL 3001 对端口 GigabitEthernet1/0/2 发出的报文进行过滤。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] packet-filter 3001 outbound
```

```
[Device-GigabitEthernet1/0/2] quit
```

## 5.5 验证配置

# 执行 **display packet-filter** 命令查看包过滤功能的应用状态。

```
[Device] display packet-filter interface outbound
```

```
Interface: GigabitEthernet1/0/2
```

```
Out-bound policy:
```

```
ACL 3001
```

```
IPv4 default action: Permit
```

```
Interface: GigabitEthernet1/0/3
```

```
Out-bound policy:
```

```
ACL 3000
```

```
IPv4 default action: Permit
```

上述信息显示 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 端口上已经正确应用了包过滤功能。

# 在管理部的主机执行 **telnet 100.1.1.3 21** 命令测试是否可以访问 FTP 服务器的 21 端口。

```
C:\>telnet 100.1.1.3 21
```

```
Connecting To 100.1.1.3...Could not open connection to the host, on port 21:
```

```
Connect failed
```

```
C:\>
```

上述信息显示管理部的主机无法访问 FTP 服务器的 21 端口。

# 在管理部某台主机上设置共享文件夹，然后从 Web 服务器上 ping 该主机，可以 ping 通，但是无法访问共享文件夹。

```
C:\>ping 10.1.1.110
```

```
Pinging 10.1.1.110 with 32 bytes of data:
```

```
Reply from 10.1.1.110: bytes=32 time=2ms TTL=128
```

```
Reply from 10.1.1.110: bytes=32 time=14ms TTL=128
```

```
Reply from 10.1.1.110: bytes=32 time=1ms TTL=128
```

```
Reply from 10.1.1.110: bytes=32 time=1ms TTL=128
```

```
Ping statistics for 10.1.1.110:
```

```
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
 Minimum = 1ms, Maximum = 14ms, Average = 4ms
```

```
C:\>
```

# 在研发部的主机执行 telnet 100.1.1.2 80 命令测试是否可以访问 Web 服务器的 80 端口。

```
C:\>telnet 100.1.1.2 80
```

```
Connecting To 100.1.1.2...Could not open connection to the host, on port 80:
```

```
Connect failed
```

```
C:\>
```

上述信息显示管理部的主机无法访问 FTP 服务器的 21 端口。

## 5.6 配置文件

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip address 10.1.2.1 255.255.255.0
 packet-filter 3001 outbound
#
interface GigabitEthernet1/0/3
 port link-mode route
 combo enable copper
 ip address 10.1.1.1 255.255.255.0
 packet-filter 3000 outbound
```

```
#
acl number 3000
 rule 0 permit tcp source 100.1.1.2 0 destination 10.1.1.0 0.0.0.255 destination
-port gt 1023 established
 rule 5 deny tcp source 100.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 10 deny tcp source 100.1.1.3 0 source-port range ftp-data ftp
#
acl number 3001
 rule 0 deny tcp source 100.1.1.2 0 source-port eq www
```

## 6 相关资料

- 《H3C MSR 系列路由器 配置指导 (V7)》中的“ACL 和 QoS 配置指导”
- 《H3C MSR 系列路由器 命令参考 (V7)》中的“ACL 和 QoS 命令参考”

# H3C MSR 系列路由器

## 流量监管配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	3
3.3 使用版本.....	3
3.4 配置步骤.....	3
3.5 验证配置.....	5
3.6 配置文件.....	7
4 相关资料.....	9

# 1 简介

本文档介绍了流量监管的配置举例。

流量监管就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，以保护网络资源和运营商的利益。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解流量监管特性。

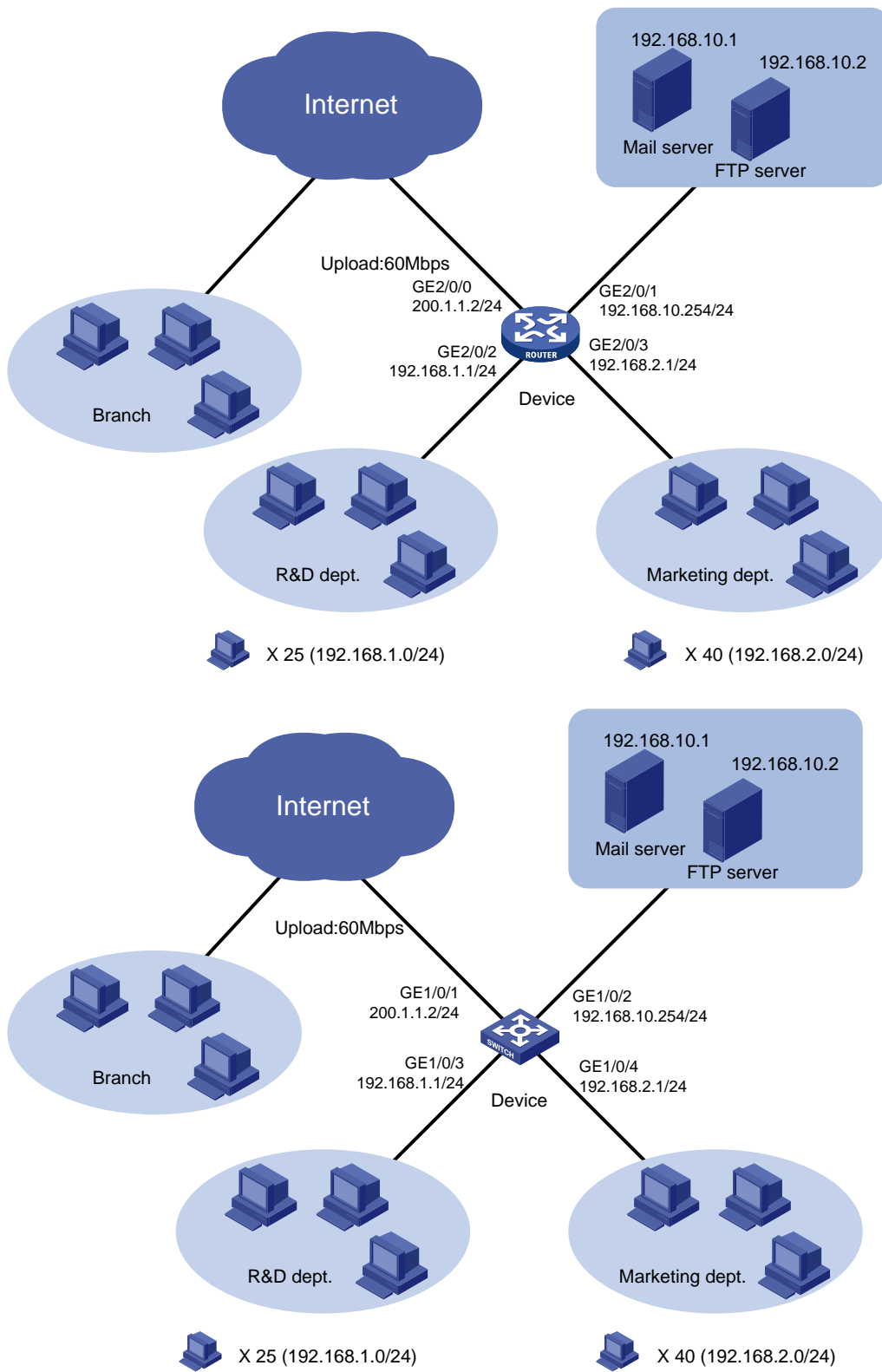
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，某公司网络通过专线接入 Internet，上行带宽为 60Mbps，所有终端设备均以 Device 作为网关设备。现要求使用流量监管功能，对上行至 Internet 的流量进行分类限速：

- HTTP 流量：总上行限速为 40Mbps，其中研发部 25 台主机分配 15Mbps 上行带宽；市场部 40 台主机分配 25Mbps 上行带宽。
- 邮件服务器代理所有客户端向外网发送电子邮件，限制上行带宽为 2Mbps。
- 远端分支机构可以通过 Internet 访问 FTP 服务器，限制上行的 FTP 的数据流量不超过 10Mbps。

图1 流量监管配置组网图



## 3.2 配置思路

要实现对不同特征数据流的流量监管，主要是明确匹配各业务数据的类规则。在本例中，需要使用 ACL 来匹配各种协议或来源的 IP 报文，并将这些分类规则与不同的流量监管动作进行绑定，即可实现对不同特征的数据进行不同的速率限制。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置步骤

### (1) 配置接口的 IP 地址

# 配置接口 GigabitEthernet1/0/1 的 IP 地址

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 200.1.1.2 24
[Device-GigabitEthernet1/0/1] quit
```

# 请参考上面的方法，分别配置其它接口的 IP 地址，具体步骤省略。

### (2) 配置对研发部 HTTP 上行流量的限制

# 创建高级 IPv4 ACL 3000，匹配研发部发送的 HTTP 流量（目的 TCP 端口 80）。

```
[Device] acl number 3000
[Device-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.1.0
0.0.0.255
[Device-acl-adv-3000] quit
```

# 创建类 rd\_http，匹配规则为 IPv4 ACL 3000。

```
[Device] traffic classifier rd_http
[Device-classifier-rd_http] if-match acl 3000
[Device-classifier-rd_http] quit
```

# 创建流行为 rd\_http，动作为流量监管，承诺速率 15Mbps。

```
[Device] traffic behavior rd_http
[Device-behavior-rd_http] car cir 15360
[Device-behavior-rd_http] quit
```

# 创建 QoS 策略 rd\_http。

```
[Device] qos policy rd_http
[Device-qospolicy-rd_http] classifier rd_http behavior rd_http
[Device-qospolicy-rd_http] quit
```

# 将策略应用到 GigabitEthernet1/0/3 端口的入方向。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos apply policy rd_http inbound
[Device-GigabitEthernet1/0/3] quit
```

### (3) 配置对市场部 HTTP 上行流量的限制

# 创建高级 IPv4 ACL 3001，匹配市场部发送的 HTTP 流量。

```
[Device] acl number 3001
```



```
[Device-acl-adv-3001] rule permit tcp destination-port eq 80 source 192.168.2.0
0.0.0.255
```

```
[Device-acl-adv-3001] quit
```

# 创建类 **mkt\_http**，匹配规则为 IPv4 ACL 3001。

```
[Device] traffic classifier mkt_http
```

```
[Device-classifier-mkt_http] if-match acl 3001
```

```
[Device-classifier-mkt_http] quit
```

# 创建流行为 **mkt\_http**，动作为流量监管，承诺速率为 25Mbps。

```
[Device] traffic behavior mkt_http
```

```
[Device-behavior-mkt_http] car cir 25600
```

```
[Device-behavior-mkt_http] quit
```

# 创建 QoS 策略 **mkt\_http**。

```
[Device] qos policy mkt_http
```

```
[Device-qospolicy-mkt_http] classifier mkt_http behavior mkt_http
```

```
[Device-qospolicy-mkt_http] quit
```

# 将策略应用到 **GigabitEthernet1/0/4** 端口的入方向。

```
[Device] interface gigabitethernet 1/0/4
```

```
[Device-GigabitEthernet1/0/4] qos apply policy mkt_http inbound
```

```
[Device-GigabitEthernet1/0/4] quit
```

#### (4) 配置对邮件服务器发送电子邮件流量的限制

# 创建高级 IPv4 ACL 3002，匹配邮件服务器向外发送邮件的数据。

```
[Device] acl number 3002
```

```
[Device-acl-adv-3002] rule permit tcp destination-port eq smtp source 192.168.10.1
0.0.0.0
```

```
[Device-acl-adv-3002] quit
```

# 创建类 **email**，匹配规则为 IPv4 ACL 3002。

```
[Device] traffic classifier email
```

```
[Device-classifier-email] if-match acl 3002
```

```
[Device-classifier-email] quit
```

# 创建流行为 **email**，动作为流量监管，承诺速率为 2Mbps。

```
[Device] traffic behavior email
```

```
[Device-behavior-email] car cir 2048
```

```
[Device-behavior-email] quit
```

# 创建 QoS 策略 **email&ftp**。

```
[Device] qos policy email&ftp
```

```
[Device-qospolicy-email&ftp] classifier email behavior email
```

```
[Device-qospolicy-email&ftp] quit
```

#### (5) 配置对分支机构的 FTP 流量的限制

# 创建基本 IPv4 ACL 2001，匹配 FTP 服务器发送的报文。

```
[Device] acl number 2001
```

```
[Device-acl-basic-2001] rule permit source 192.168.10.2 0.0.0.0
```

```
[Device-acl-basic-2001] quit
```

# 创建类 **ftp**，匹配规则为 IPv4 ACL 2001。

```
[Device] traffic classifier ftp
```

```
[Device-classifier-ftp] if-match acl 2001
```

```

[Device-classifier-ftp] quit
创建流行为 ftp，动作为流量监管，承诺速率为 10Mbps。
[Device] traffic behavior ftp
[Device-behavior-ftp] car cir 10240
[Device-behavior-ftp] quit
在 QoS 策略 email&ftp 中为类 ftp 指定流行为 ftp。
[Device] qos policy email&ftp
[Device-qospolicy-email&ftp] classifier ftp behavior ftp
[Device-qospolicy-email&ftp] quit
将策略应用到 GigabitEthernet1/0/1 端口的出方向。
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy email&ftp outbound
[Device-GigabitEthernet1/0/1] quit

```

### 3.5 验证配置

# 执行 **display qos policy interface** 命令查看端口上 QoS 策略的应用状态。

```

[Device] display qos policy interface

Interface: GigabitEthernet1/0/1

Direction: Outbound

Policy: email&ftp
Classifier: default-class
 Matched : 0 (Packets) 0 (Bytes)
 5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped : 0/0 (pps/bps)
 Operator: AND
 Rule(s) :
 If-match any
 Behavior: be
 -none-
Classifier: email
 Matched : 0 (Packets) 0 (Bytes)
 5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped : 0/0 (pps/bps)
 Operator: AND
 Rule(s) :
 If-match acl 3002
 Behavior: email
 Committed Access Rate:
 CIR 2048 (kbps), CBS 128000 (Bytes), EBS 0 (Bytes)
 Green action : pass
 Yellow action : pass

```

```
 Red action : discard
 Green packets : 0 (Packets) 0 (Bytes)
 Yellow packets : 0 (Packets) 0 (Bytes)
 Red packets : 0 (Packets) 0 (Bytes)
Classifier: ftp
Matched : 0 (Packets) 0 (Bytes)
5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped : 0/0 (pps/bps)
Operator: AND
Rule(s) :
 If-match acl 2001
Behavior: ftp
Committed Access Rate:
 CIR 10240 (kbps), CBS 640000 (Bytes), EBS 0 (Bytes)
 Green action : pass
 Yellow action : pass
 Red action : discard
 Green packets : 0 (Packets) 0 (Bytes)
 Yellow packets : 0 (Packets) 0 (Bytes)
 Red packets : 0 (Packets) 0 (Bytes)
```

Interface: GigabitEthernet1/0/3

Direction: Inbound

```
Policy: rd_http
Classifier: default-class
Matched : 313 (Packets) 29916 (Bytes)
5-minute statistics:
 Forwarded: 0/719 (pps/bps)
 Dropped : 0/0 (pps/bps)
Operator: AND
Rule(s) :
 If-match any
Behavior: be
 -none-
Classifier: rd_http
Matched : 0 (Packets) 0 (Bytes)
5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped : 0/0 (pps/bps)
Operator: AND
Rule(s) :
 If-match acl 3000
Behavior: rd_http
Committed Access Rate:
 CIR 15360 (kbps), CBS 960000 (Bytes), EBS 0 (Bytes)
```

```
Green action : pass
Yellow action : pass
Red action : discard
Green packets : 0 (Packets) 0 (Bytes)
Yellow packets: 0 (Packets) 0 (Bytes)
Red packets : 0 (Packets) 0 (Bytes)
```

Interface: GigabitEthernet1/0/4

Direction: Inbound

Policy: mkt\_http

Classifier: default-class

Matched : 0 (Packets) 0 (Bytes)

5-minute statistics:

Forwarded: 0/0 (pps/bps)

Dropped : 0/0 (pps/bps)

Operator: AND

Rule(s) :

If-match any

Behavior: be

-none-

Classifier: mkt\_http

Matched : 0 (Packets) 0 (Bytes)

5-minute statistics:

Forwarded: 0/0 (pps/bps)

Dropped : 0/0 (pps/bps)

Operator: AND

Rule(s) :

If-match acl 3001

Behavior: mkt\_http

Committed Access Rate:

CIR 25600 (kbps), CBS 1600000 (Bytes), EBS 0 (Bytes)

Green action : pass

Yellow action : pass

Red action : discard

Green packets : 0 (Packets) 0 (Bytes)

Yellow packets: 0 (Packets) 0 (Bytes)

Red packets : 0 (Packets) 0 (Bytes)

## 3.6 配置文件

```
#
traffic classifier email operator and
if-match acl 3002
#
traffic classifier ftp operator and
if-match acl 2001
```

```

#
traffic classifier mkt_http operator and
 if-match acl 3001
#
traffic classifier rd_http operator and
 if-match acl 3000
#
traffic behavior email
 car cir 2048 cbs 128000 ebs 0 green pass red discard yellow pass
#
traffic behavior ftp
 car cir 10240 cbs 640000 ebs 0 green pass red discard yellow pass
#
traffic behavior mkt_http
 car cir 25600 cbs 1600000 ebs 0 green pass red discard yellow pass
#
traffic behavior rd_http
 car cir 15360 cbs 960000 ebs 0 green pass red discard yellow pass
#
qos policy email&ftp
 classifier email behavior email
 classifier ftp behavior ftp
#
qos policy mkt_http
 classifier mkt_http behavior mkt_http
#
qos policy rd_http
 classifier rd_http behavior rd_http
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 200.1.1.2 255.255.255.0
 qos apply policy email&ftp outbound
#
interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip address 192.168.10.254 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 combo enable copper
 ip address 192.168.1.1 255.255.255.0
 qos apply policy rd_http inbound
#
interface GigabitEthernet1/0/4
 port link-mode route

```

```
combo enable copper
ip address 192.168.2.1 255.255.255.0
qos apply policy mkt_http inbound
#
acl number 2001
 rule 0 permit source 192.168.10.2 0
#
acl number 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq www
#
acl number 3001
 rule 0 permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
#
acl number 3002
 rule 0 permit tcp source 192.168.10.1 0 destination-port eq smtp
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“ACL 和 QoS 配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“ACL 和 QoS 命令参考”

# H3C MSR 系列路由器

## 流量整形配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	2
3.3 配置步骤.....	2
3.4 验证配置.....	3
3.5 配置文件.....	5
4 相关资料.....	6



# 1 简介

本文档介绍了 GTS（Generic Traffic Shaping，通用流量整形）的配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解流量整形特性。

## 3 配置举例

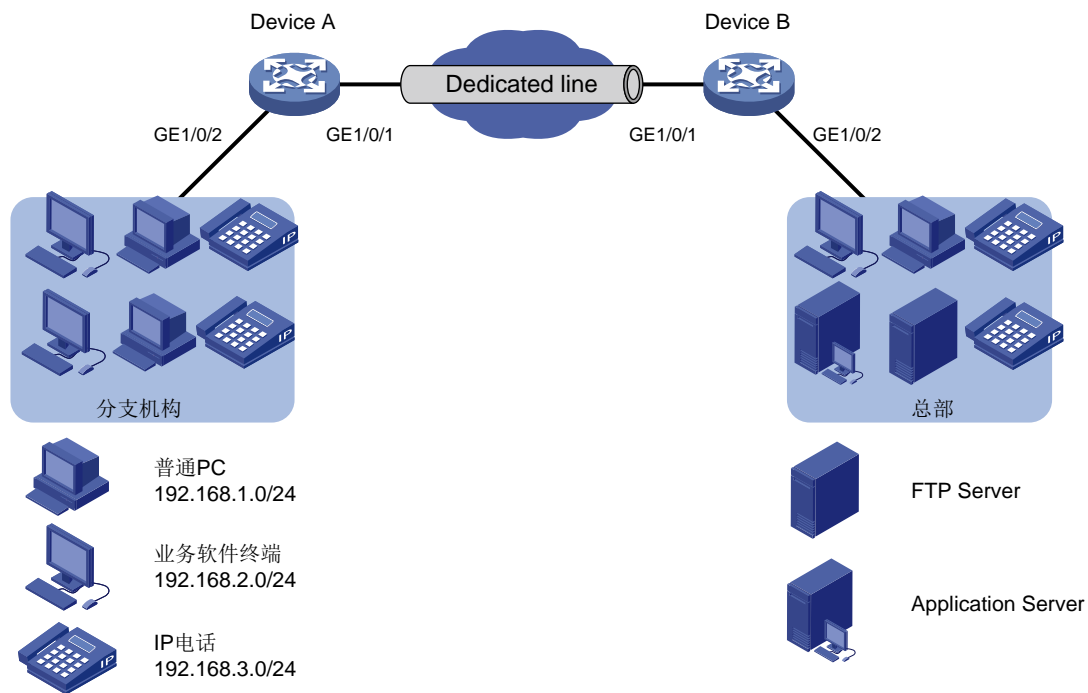
### 3.1 组网需求

如[图 1](#)所示，某公司通过专线连接分支机构（图中左侧网络）与总部（图中右侧网络），专线中传输的流量主要有三类：FTP 流量、业务应用流量、IP 语音流量。由于整个专线的速率为 20Mbps，在总部的边缘设备 Device B 上已经配置了相应的流量监管功能：

- IP 语音流量的承诺速率为 10M
- 业务应用流量的承诺速率为 3M
- FTP 流量的承诺速率为 7M

为配合总部的流量监管，要求在分支机构的设备 Device A 上配置流量整形功能，对各类流量中突发的超出部分进行缓存，避免数据丢失。

图1 流量整形配置组网图



## 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.3 配置步骤

(1) 在 Device A 上创建三个流分类，分别匹配三类报文的源 IP 网段。

# 创建基本 IPv4 ACL2000，匹配 IP 电话发送的流量（源地址为 192.168.3.0/24 网段）。

```
<DeviceA> system-view
[DeviceA] acl number 2000
[DeviceA-acl-basic-2000] rule permit source 192.168.3.0 0.0.0.255
[DeviceA-acl-basic-2000] quit
```

# 创建流分类 voice，匹配规则为 IPv4 ACL 2000。

```
[DeviceA] traffic classifier voice
[DeviceA-classifier-voice] if-match acl 2000
[DeviceA-classifier-voice] quit
```

# 创建基本 IPv4 ACL2001，匹配业务软件终端发送的流量（源地址为 192.168.2.0/24 网段）。

```
[DeviceA] acl number 2001
[DeviceA-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[DeviceA-acl-basic-2001] quit
```

# 创建流分类 service，匹配规则为 IPv4 ACL 2001。

```
[DeviceA] traffic classifier service
[DeviceA-classifier-service] if-match acl 2001
```

```

[DeviceA-classifier-service] quit
创建高级 IPv4 ACL 3000，匹配普通 PC 发送的 FTP 流量（源地址为 192.168.1.0/24 网段，
目的端口为 20）。
[DeviceA] acl number 3000
[DeviceA-acl-adv-3000] rule permit tcp destination-port eq 20 source 192.168.1.0
0.0.0.255
[DeviceA-acl-adv-3000] quit
创建流分类 ftp，匹配规则为 IPv4 ACL 3000。
[DeviceA] traffic classifier ftp
[DeviceA-classifier-ftp] if-match acl 3000
[DeviceA-classifier-ftp] quit

```

(2) 创建三个流行为，分别配置流量整形动作。

# 创建流行为 **voice**，为语音报文配置承诺速率为 10000Kbps。

```

[DeviceA] traffic behavior voice
[DeviceA-behavior-voice] gts cir 10000
[DeviceA-behavior-voice] quit

```

# 创建流行为 **service**，为业务应用报文配置承诺速率为 3000Kbps。

```

[DeviceA] traffic behavior service
[DeviceA-behavior-service] gts cir 3000
[DeviceA-behavior-service] quit

```

# 创建流行为 **ftp**，为 FTP 报文配置承诺速率为 7000Kbps。

```

[DeviceA] traffic behavior ftp
[DeviceA-behavior-ftp] gts cir 7000
[DeviceA-behavior-ftp] quit

```

(3) 创建 QoS 策略并应用

# 创建 QoS 策略 **shaping**，将上面三组流分类和流行为进行关联。

```

[DeviceA] qos policy shaping
[DeviceA-qospolicy-shaping] classifier voice behavior voice
[DeviceA-qospolicy-shaping] classifier service behavior service
[DeviceA-qospolicy-shaping] classifier ftp behavior ftp
[DeviceA-qospolicy-shaping] quit

```

# 将 QoS 策略应用到 **GigabitEthernet1/0/1** 端口的出方向。

```

[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy shaping outbound
[DeviceA-GigabitEthernet1/0/1] quit

```

## 3.4 验证配置

# 使用 **display qos policy interface** 命令查看流量整形功能的配置。

```

[Devicie] display qos policy interface outbound

```

```

Interface: GigabitEthernet1/0/1

```

```

Direction: Outbound

```

```

Policy: shaping

```

```
Classifier: default-class
 Matched : 0 (Packets) 0 (Bytes)
 5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped : 0/0 (pps/bps)
 Operator: AND
 Rule(s) :
 If-match any
 Behavior: be
 -none-

Classifier: voice
 Matched : 0 (Packets) 0 (Bytes)
 5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped : 0/0 (pps/bps)
 Operator: AND
 Rule(s) :
 If-match acl 2000
 Behavior: voice
 General Traffic Shaping:
 CIR 10000 (kbps), CBS 625000 (Bytes), EBS 0 (Bytes)
 Queue length: 50 (Packets)
 Queue size : 0 (Packets)
 Passed : 0 (Packets) 0 (Bytes)
 Discarded: 0 (Packets) 0 (Bytes)
 Delayed : 0 (Packets) 0 (Bytes)

Classifier: service
 Matched : 0 (Packets) 0 (Bytes)
 5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped : 0/0 (pps/bps)
 Operator: AND
 Rule(s) :
 If-match acl 2001
 Behavior: service
 General Traffic Shaping:
 CIR 3000 (kbps), CBS 187500 (Bytes), EBS 0 (Bytes)
 Queue length: 50 (Packets)
 Queue size : 0 (Packets)
 Passed : 0 (Packets) 0 (Bytes)
 Discarded: 0 (Packets) 0 (Bytes)
 Delayed : 0 (Packets) 0 (Bytes)

Classifier: ftp
 Matched : 0 (Packets) 0 (Bytes)
 5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped : 0/0 (pps/bps)
 Operator: AND
```

```
Rule(s) :
 If-match acl 3000
Behavior: ftp
General Traffic Shaping:
 CIR 7000 (kbps), CBS 437500 (Bytes), EBS 0 (Bytes)
 Queue length: 50 (Packets)
 Queue size : 0 (Packets)
 Passed : 0 (Packets) 0 (Bytes)
 Discarded: 0 (Packets) 0 (Bytes)
 Delayed : 0 (Packets) 0 (Bytes)
```

### 3.5 配置文件

```
#
traffic classifier ftp operator and
 if-match acl 3000
#
traffic classifier service operator and
 if-match acl 2001
#
traffic classifier voice operator and
 if-match acl 2000
#
traffic behavior ftp
 gts cir 7000 cbs 437500 ebs 0 queue-length 50
#
traffic behavior service
 gts cir 3000 cbs 187500 ebs 0 queue-length 50
#
traffic behavior voice
 gts cir 10000 cbs 625000 ebs 0 queue-length 50
#
qos policy shaping
 classifier voice behavior voice
 classifier service behavior service
 classifier ftp behavior ftp
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 qos apply policy shaping outbound
#
acl number 2000
 rule 0 permit source 192.168.3.0 0.0.0.255
#
acl number 2001
 rule 0 permit source 192.168.2.0 0.0.0.255
#
```

```
acl number 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq ftp-data
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“ACL 和 QoS 配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“ACL 和 QoS 命令参考”

# H3C MSR 系列路由器

## 基于控制平面应用 QoS 策略配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 对 ICMP 报文进行限速配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置步骤.....	2
3.5 验证配置.....	2
3.6 配置文件.....	3
4 对 ARP 报文进行限速配置举例.....	3
4.1 组网需求.....	3
4.2 配置思路.....	4
4.3 使用版本.....	4
4.4 配置步骤.....	4
4.5 验证配置.....	5
4.6 配置文件.....	5
5 相关资料.....	6



# 1 简介

本文档介绍了基于控制平面应用 QoS 策略的配置举例。

为了防止从数据平面上送控制平面的报文速率超过控制平面的处理能力，从而影响协议的正常运行，用户可以把 QoS 策略应用在控制平面上，通过对上送控制平面的报文进行过滤、限速等 QoS 处理，达到保护控制平面正常报文的收发、维护控制平面正常处理状态的目的。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

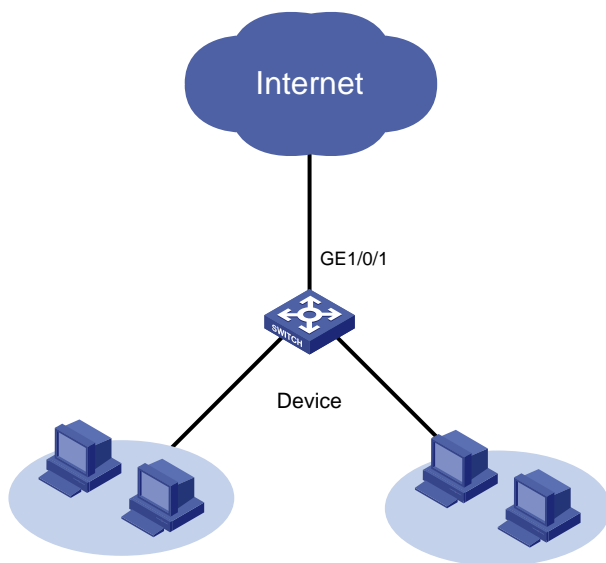
本文假设您已了解基于控制平面应用 QoS 策略特性。

## 3 对 ICMP 报文进行限速配置举例

### 3.1 组网需求

如图 1 所示，Device 收到 Internet 发来的大量 ICMP 报文，导致 CPU 占用率过高，设备性能下降，现要求在 Device 上配置基于控制平面应用 QoS 策略，对上送控制平面的 ICMP 报文限速为 640kbps，若超过流量限制则将违规报文丢弃。

图1 对 ICMP 报文进行限速配置组网图



## 3.2 配置思路

缺省情况下，设备会在控制平面上应用预定义的 QoS 策略，并默认生效。系统预定义的 QoS 策略信息可以通过 **display qos policy control-plane pre-defined** 命令查看，标识各种上送控制平面的报文类型，并对不同类型的报文设置有缺省的限速值。

根据需求，将 ICMP 报文的限速值修改为 640kbps，可以在流分类视图下通过 **if-match** 命令来进行报文分类，然后在对应的流行为下通过 **car** 命令配置期望的限速值，并对超出限制的报文进行丢弃。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置步骤

# 定义类 ICMP，匹配控制平面的 ICMP 协议报文。

```
<Device> system-view
[Device] traffic classifier ICMP
[Device-classifier-ICMP] if-match control-plane protocol icmp
[Device-classifier-ICMP] quit
```

# 定义流行为 ICMP，使用协议报文限速对匹配的报文进行限速。

```
[Device] traffic behavior ICMP
[Device-behavior-ICMP] car cir 640
[Device-behavior-ICMP] quit
```

# 定义 QoS 策略 ICMP，为类 ICMP 指定流行为 ICMP。

```
[Device] qos policy ICMP
[Device-qospolicy-ICMP] classifier ICMP behavior ICMP
[Device-qospolicy-ICMP] quit
```

# 将 QoS 策略 ICMP 应用到 2 号槽位业务板的控制平面。

```
[Device] control-plane slot 2
[Device-cp-slot2] qos apply policy ICMP inbound
[Device-cp-slot2] quit
```

## 3.5 验证配置

# 执行 **display qos policy control-plane** 命令查看控制平面 QoS 策略的应用状态。

```
[Device] display qos policy control-plane slot 2
```

```
Control plane slot 2
```

```
Direction: Inbound
```

```
Policy: ICMP
```

```
Classifier: default-class
```

```
Matched : 0 (Packets) 0 (Bytes)
```

```
Operator: AND
```

```

Rule(s) :
 If-match any
Behavior: be
 -none-
Classifier: ICMP
Matched : 0 (Packets) 0 (Bytes)
Operator: AND
Rule(s) :
 If-match control-plane protocol icmp
Behavior: ICMP
Committed Access Rate:
 CIR 640 (kbps), CBS 40000 (Bytes), EBS 0 (Bytes)
Green action : pass
Yellow action : pass
Red action : discard
Green packets : 0 (Packets) 0 (Bytes)
Red packets : 0 (Packets) 0 (Bytes)

```

上述信息显示 2 号槽位业务板上已经正确应用了控制平面 QoS 策略。

## 3.6 配置文件

```

#
traffic classifier ICMP operator and
 if-match control-plane protocol icmp
#
traffic behavior ICMP
 car cir 640 cbs 40000 ebs 0 green pass red discard yellow pass
#
qos policy ICMP
 classifier ICMP behavior ICMP
#
control-plane slot 2
 qos apply policy ICMP inbound

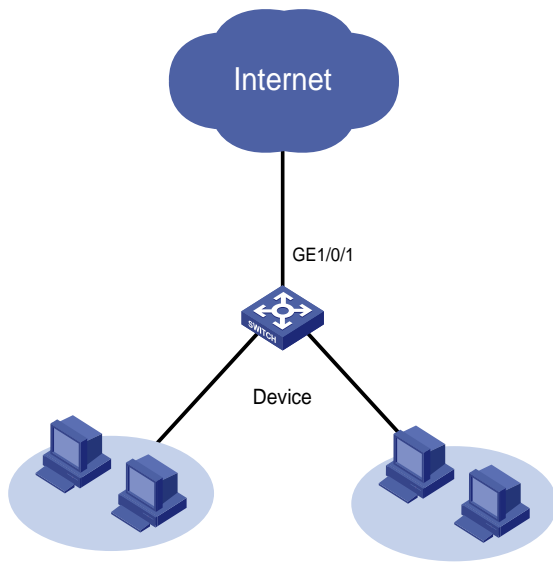
```

# 4 对 ARP 报文进行限速配置举例

## 4.1 组网需求

如图 2 所示，Device 收到 Internet 的 DoS 攻击（ARP 报文），导致 CPU 占用率过高，设备性能下降，现要求在 Device 上配置基于控制平面应用 QoS 策略，对上送控制平面的 ARP 报文进行限速，限速值为 1000kbps。

图2 对 ARP 报文进行限速配置组网图



## 4.2 配置思路

为实现对上送控制平面的 ARP 报文进行限速（限速值为 1000kbps），可以通过配置 **if-match control-plane protocol arp** 命令匹配 ARP 协议报文，并对匹配的 ARP 协议报文使用 **car** 命令进行限速。

## 4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.4 配置步骤

# 定义类 ARP，匹配收到的 ARP 协议报文。

```
<Device> system-view
[Device] traffic classifier ARP
[Device-classifier-ARP] if-match control-plane protocol arp
[Device-classifier-ARP] quit
```

# 定义流行为 ARP，使用流量监管对匹配的报文进行限速。

```
[Device] traffic behavior ARP
[Device-behavior-ARP] car cir 1000
[Device-behavior-ARP] quit
```

# 定义 QoS 策略 ARP，为类 ARP 指定流行为 ARP。

```
[Device] qos policy ARP
[Device-qospolicy-ARP] classifier ARP behavior ARP
[Device-qospolicy-ARP] quit
```

# 将 QoS 策略 ARP 应用在 2 号槽位的控制平面。

```
[Device] control-plane slot 2
```

```
[Device-cp-slot2] qos apply policy ARP inbound
[Device-cp-slot2] quit
```

## 4.5 验证配置

# 执行 **display qos policy control-plane** 命令查看控制平面 QoS 策略的应用状态。

```
[Device] display qos policy control-plane slot 2
```

```
Control plane slot 2
```

```
Direction: Inbound
```

```
Policy: ARP
```

```
Classifier: default-class
```

```
Matched : 0 (Packets) 0 (Bytes)
```

```
Operator: AND
```

```
Rule(s) :
```

```
 If-match any
```

```
Behavior: be
```

```
 -none-
```

```
Classifier: ARP
```

```
Matched : 12 (Packets) 552 (Bytes)
```

```
Operator: AND
```

```
Rule(s) :
```

```
 If-match control-plane protocol arp
```

```
Behavior: ARP
```

```
Committed Access Rate:
```

```
 CIR 1000 (kbps), CBS 62500 (Bytes), EBS 0 (Bytes)
```

```
Green action : pass
```

```
Yellow action : pass
```

```
Red action : discard
```

```
Green packets : 12 (Packets) 552 (Bytes)
```

```
Red packets : 0 (Packets) 0 (Bytes)
```

上述信息显示 2 号槽位上已经正确应用了控制平面 QoS 策略。

## 4.6 配置文件

```
#
traffic classifier ARP operator and
 if-match control-plane protocol arp
#
traffic behavior ARP
 car cir 1000 cbs 62500 ebs 0 green pass red discard yellow pass
#
qos policy ARP
 classifier ARP behavior ARP
#
control-plane slot 2
```

```
qos apply policy ARP inbound
```

## 5 相关资料

- 《H3C MSR 系列路由器 配置指导 (V7)》中的“ACL 和 QoS 配置指导”
- 《H3C MSR 系列路由器 命令参考 (V7)》中的“ACL 和 QoS 命令参考”

# H3C MSR 系列路由器

## IGMP Snooping 配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 使用限制.....	1
4 组策略配置举例.....	1
4.1 组网需求.....	1
4.2 配置思路.....	2
4.3 使用版本.....	2
4.4 配置注意事项.....	2
4.5 配置步骤.....	2
4.6 验证结果.....	4
4.7 配置文件.....	4
5 静态端口配置举例.....	5
5.1 组网需求.....	5
5.2 配置思路.....	6
5.3 使用版本.....	6
5.4 配置注意事项.....	6
5.5 配置步骤.....	7
5.6 验证结果.....	8
5.7 配置文件.....	9
6 相关资料.....	11



# 1 简介

本文档介绍了 IGMP Snooping 组策略和静态端口的典型配置举例。

IGMP Snooping (Internet Group Management Protocol Snooping, 互联网组管理协议窥探) 运行在二层设备上, 通过侦听三层设备与主机之间的 IGMP 报文来生成二层组播转发表, 从而实现组播数据报文不会在二层广播, 而是在二层组播给指定的接收者。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器, 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。

本文假设您已了解 IGMP Snooping 特性。

## 3 使用限制

IGMP Snooping 和 STP 特性仅在 SIC-4GSW/DSIC-9FSW/DSIC-9FSWP/HMIM-24GSW/HMIM-24GSW-PoE/HMIM-8GSW 接口卡, 以及 MSR 3600-28/MSR 3600-51 的固定二层接口上支持。

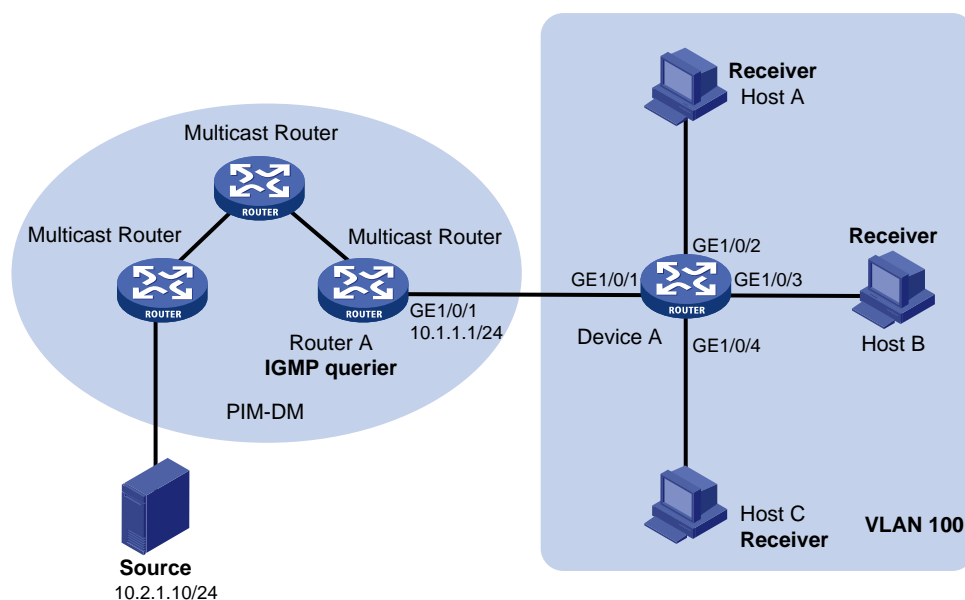
## 4 组策略配置举例

### 4.1 组网需求

如[图 1](#)所示, 用户网络 VLAN 100 通过 Device A 接入到 PIM-DM 域, Router A 上运行 IGMP, Device A 上运行 IGMP Snooping, 并由 Router A 充当 IGMP 查询器。要求通过在 Device A 上开启 IGMP Snooping 功能并配置组播组过滤器, 实现如下需求:

- 用户网络 VLAN 100 内的组播接收者 Host A 只能接收发往组播组 224.1.1.1 的组播数据, 其余所有组播接收者 (例如 Host B 和 Host C) 只能接收发往组播组 225.1.1.1 的组播数据;
- Device A 将收到的未知组播数据直接丢弃, 避免在其所属的 VLAN 100 内广播。

图1 组策略配置组网图



## 4.2 配置思路

- 缺省情况下，Device A 上 IGMP Snooping 版本为 2，只能对 IGMPv1 和 IGMPv2 报文进行处理，对 IGMPv3 报文则不进行处理，而是在 VLAN 内将其广播。为避免这种情况，需要配置 VLAN 100 内的 IGMP Snooping 版本为 3。
- 缺省情况下，在配置的 IGMP Snooping 策略允许的组播数据之外的其余组播数据报文会在用户网络 VLAN 100 内被广播，导致 VLAN 100 内的组播接收者可以收到这类组播报文。为避免这种情况，需要在 VLAN 100 内开启丢弃未知组播数据报文功能。
- 为实现 IGMP Snooping 组播组过滤器控制主机加入组播组的范围，需要为其创建相应的基本 ACL，并在该 ACL 规则中指定允许主机加入的组播组范围。

## 4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.4 配置注意事项

- 启动指定 VLAN 的 IGMP Snooping 前，应首先在系统视图下启动全局 IGMP Snooping 功能。
- 用户既可在 IGMP-Snooping 视图下对所有端口进行全局配置组播组过滤器，也可在接口视图下只对当前端口进行配置组播组过滤器，后者的配置优先级较高。

## 4.5 配置步骤

### (1) 配置准备

# 配置 PIM-DM 域内路由器上各接口的 IP 地址和子网掩码，具体配置过程略。

# 配置 PIM-DM 域内各路由器之间采用静态或动态路由协议进行互连，确保 PIM-DM 域内部在网络层互通，具体配置过程略。

# 在各路由器上配置 PIM-DM 协议，以建立组播路由转发表项，实现组播数据可以从组播源到达组播接收者，具体配置过程略。

## (2) 配置 Router A

# 使能 IP 组播路由。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
```

# 在接口 GigabitEthernet1/0/1 上使能 IGMP 功能并指定版本为 3。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] igmp version 3
[RouterA-GigabitEthernet1/0/1] quit
```

## (3) 配置 Device A

# 全局使能 IGMP Snooping。

```
<DeviceA> system-view
[DeviceA] igmp-snooping
[DeviceA-igmp-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 加入该 VLAN；在该 VLAN 内使能 IGMP Snooping 并指定版本为 3，同时开启丢弃未知组播数据报文功能。

```
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceA-vlan100] igmp-snooping enable
[DeviceA-vlan100] igmp-snooping version 3
[DeviceA-vlan100] igmp-snooping drop-unknown
[DeviceA-vlan100] quit
```

# 配置组播组过滤器 2000，以限定 VLAN 100 内的主机 Host A 只能加入组播组 224.1.1.1。

```
[DeviceA] acl number 2000
[DeviceA-acl-basic-2000] rule permit source 224.1.1.1 0
[DeviceA-acl-basic-2000] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] igmp-snooping group-policy 2000 vlan 100
[DeviceA-GigabitEthernet1/0/2] quit
```

# 配置组播组过滤器 2001，以限定 VLAN 100 内的其余所有主机只能加入组播组 225.1.1.1。

```
[DeviceA] acl number 2001
[DeviceA-acl-basic-2001] rule permit source 225.1.1.1 0
[DeviceA-acl-basic-2001] quit
[DeviceA] igmp-snooping
[DeviceA-igmp-snooping] group-policy 2001 vlan 100
[DeviceA-igmp-snooping] quit
```

## 4.6 验证结果

组播源分别向组播组 224.1.1.1、224.2.2.2 和 225.1.1.1 发送组播数据，Host A、Host B 和 Host C 也都加入了这三个组播组。

# 查看 Device A 上 VLAN 100 内动态组播组的 IGMP Snooping 转发表项信息。

```
[DeviceA] display igmp-snooping group vlan 100
Total 2 entries.
```

```
VLAN 100: Total 2 entries.
```

```
(0.0.0.0, 224.1.1.1)
```

```
Host slots (1 in total):
```

```
3
```

```
Host ports (1 in total):
```

```
GE1/0/2
```

```
(0.0.0.0, 225.1.1.1)
```

```
Host slots (1 in total):
```

```
3
```

```
Host ports (2 in total):
```

```
GE1/0/3
```

```
GE1/0/4
```

由此可见，Host A 所在的端口 GigabitEthernet1/0/2 已加入组播组 224.1.1.1，但未加入组播组 224.2.2.2 和 225.1.1.1；Host B 和 Host C 所在的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 均已加入组播组 225.1.1.1，但都未加入组播组 224.1.1.1 和 224.2.2.2，这表明组播组过滤器已生效。

## 4.7 配置文件

- Router A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 igmp enable
 igmp version 3
#
multicast routing
#
```

- Device A:

```
#
igmp-snooping
 group-policy 2001 vlan 100
#
vlan 100
 igmp-snooping enable
 igmp-snooping drop-unknown
 igmp-snooping version 3
```

```

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 igmp-snooping group-policy 2000 vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
acl number 2000
 rule 0 permit source 224.1.1.1 0
#
acl number 2001
 rule 0 permit source 225.1.1.1 0
#

```

## 5 静态端口配置举例

### 5.1 组网需求

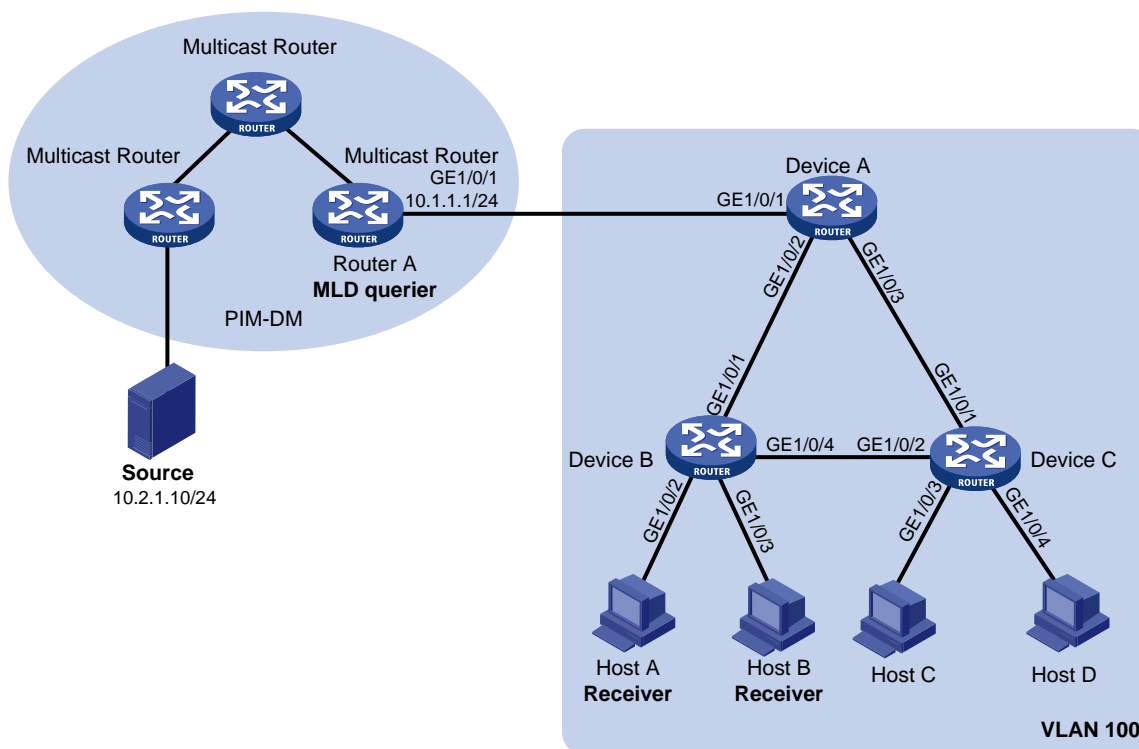
如[图2](#)所示，用户网络 VLAN 100 通过 Device A 接入到 PIM-DM 域，用户网络内的各设备上开启了 IGMP Snooping 功能，路由器 Router A 上运行 IGMPv2，成为本网段的 IGMP 查询器。

为提高用户网络数据传输的可靠性，用户网络使用了环形组网；同时为了避免环路，用户网络中开启了 STP 协议，Device A 到 Device B 的二条链路之一（例如 Device A—Device B 或 Device A—Device C—Device B）会被 STP 协议阻断。

要求通过配置静态路由器端口和静态成员端口实现如下需求：

- 当 Device A 到 Device B 的两条链路发生切换，且新链路的 STP 状态稳定后，组播数据可以立即通过新路径传递给接收者。
- 组播接收者 Host A、Host B 和 Host C 可固定的接收发往组播组 224.1.1.1 的组播数据。

图2 静态端口配置组网图



## 5.2 配置思路

- 缺省情况下，Device A 到 Device B 的两条链路发生切换且稳定后至少需要等待一个 IGMP 查询和响应周期，组播数据才能通过新路径传递给接收者，组播数据的传输在这个过程中将中断。为避免这种情况的发生，需要将 Device A 的 GigabitEthernet1/0/2、GigabitEthernet1/0/3 端口，Device B 的 GigabitEthernet1/0/4 端口和 Device C 的 GigabitEthernet1/0/2 端口配置为静态路由器端口，从而将组播流引到静态路由器端口上，使组播流能够快速切换到新路径上进行传输。
- 为使 Host A、Host B 和 Host C 成为组播组 224.1.1.1 的固定接收者，需要将 Device B 上的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 及 Device C 上的端口 GigabitEthernet1/0/3 均配置为组播组 224.1.1.1 的静态成员端口。

## 5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 5.4 配置注意事项

启动指定 VLAN 的 IGMP Snooping 前，应首先在系统视图下启动全局 IGMP Snooping 功能，否则将无法配置成功。

## 5.5 配置步骤

### (1) 配置准备

# 配置 PIM-DM 域内路由器上各接口的 IP 地址和子网掩码，具体配置过程略。

# 配置 PIM-DM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-DM 域内部在网络层互通，具体配置过程略。

# 在各路由器上配置 PIM-DM 协议，以建立组播路由转发表项，实现组播数据可以从组播源到达接收者，具体配置过程略。

### (2) 配置 Router A

# 使能 IP 组播路由。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
在接口 GigabitEthernet1/0/1 上使能 IGMP 功能。
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
```

### (3) 配置 Device A

# 全局使能 IGMP Snooping。

```
<DeviceA> system-view
[DeviceA] igmp-snooping
[DeviceA-igmp-snooping] quit
创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 加入该 VLAN，并在该 VLAN 内使能 IGMP Snooping。
```

```
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceA-vlan100] igmp-snooping enable
[DeviceA-vlan100] quit
```

# 把端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 配置为静态路由器端口。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[DeviceA-GigabitEthernet1/0/3] quit
```

### (4) 配置 Device B

# 全局使能 IGMP Snooping。

```
<DeviceB> system-view
[DeviceB] igmp-snooping
[DeviceB-igmp-snooping] quit
创建 VLAN 100，把端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/4 加入该 VLAN，并在该 VLAN 内使能 IGMP Snooping。
```

```
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/4
```

```

[DeviceB-vlan100] igmp-snooping enable
[DeviceB-vlan100] quit
把端口 GigabitEthernet1/0/4 配置为静态路由器端口。
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] igmp-snooping static-router-port vlan 100
[DeviceB-GigabitEthernet1/0/4] quit
在端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上配置静态加入组播组 224.1.1.1。
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] igmp-snooping static-group 224.1.1.1 vlan 100
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[DeviceB-GigabitEthernet1/0/3] quit

```

#### (5) 配置 Device C

```

全局使能 IGMP Snooping。
<DeviceC> system-view
[DeviceC] igmp-snooping
[DeviceC-igmp-snooping] quit
创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 加入该 VLAN，并
在该 VLAN 内使能 IGMP Snooping。
[DeviceC] vlan 100
[DeviceC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceC-vlan100] igmp-snooping enable
[DeviceC-vlan100] quit
把端口 GigabitEthernet1/0/2 配置为静态路由器端口。
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[DeviceC-GigabitEthernet1/0/2] quit
在端口 GigabitEthernet1/0/3 上配置静态加入组播组 224.1.1.1。
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[DeviceC-GigabitEthernet1/0/3] quit

```

## 5.6 验证结果

# 查看 Device A 上 VLAN 100 内静态路由器端口的信息。

```

[DeviceA] display igmp-snooping static-router-port vlan 100
VLAN 100:
 Router slots (1 in total):
 3
 Router ports (2 in total):
 GE1/0/2
 GE1/0/3

```

由此可见，Device A 上的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 已经成为了静态路由器端口。

# 查看 Device B 上 VLAN 100 内静态路由器端口的信息。



```
[DeviceB] display igmp-snooping static-router-port vlan 100
VLAN 100:
 Router slots (1 in total):
 3
 Router ports (1 in total):
 GE1/0/4
```

由此可见，Device B 上的端口 GigabitEthernet1/0/4 已经成为了静态路由器端口。

# 查看 Device B 上 VLAN 100 内静态组播组的 IGMP Snooping 转发表项信息。

```
[DeviceB] display igmp-snooping static-group vlan 100
Total 1 entries.
```

```
VLAN 100: Total 1 entries.
(0.0.0.0, 224.1.1.1)
 Host slots (1 in total):
 3
 Host ports (2 in total):
 GE1/0/2
 GE1/0/3
```

由此可见，Device B 上的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 已经成为了组播组 224.1.1.1 的静态成员端口。

# 查看 Device C 上 VLAN 100 内静态路由器端口的信息。

```
[DeviceC] display igmp-snooping static-router-port vlan 100
VLAN 100:
 Router slots (1 in total):
 3
 Router ports (1 in total):
 GE1/0/2
```

由此可见，Device C 上的端口 GigabitEthernet1/0/2 已经成为了静态路由器端口。

# 查看 Device C 上 VLAN 100 内静态组播组的 IGMP Snooping 转发表项信息。

```
[DeviceC] display igmp-snooping static-group vlan 100
Total 1 entries.
```

```
VLAN 100: Total 1 entries.
(0.0.0.0, 224.1.1.1)
 Host slots (1 in total):
 3
 Host ports (1 in total):
 GE1/0/3
```

由此可见，Device C 上的端口 GigabitEthernet1/0/3 已经成为了组播组 224.1.1.1 的静态成员端口。

## 5.7 配置文件

- RouterA:

```
#
interface GigabitEthernet1/0/1
port link-mode route
```

```
ip address 10.1.1.1 255.255.255.0
igmp enable
igmp version 3
#
multicast routing
#
```

- **Device A:**

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
```

- **Device B:**

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-group 224.1.1.1 vlan 100
#
```

```

interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
• Device C:
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#

```

## 6 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“IP 组播配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“IP 组播命令参考”

# H3C MSR 系列路由器

## IGMP 配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目录

1 简介	1
2 配置前提	1
3 IGMP 基本功能配置举例	1
3.1 组网需求	1
3.2 配置思路	2
3.3 使用版本	2
3.4 配置注意事项	2
3.5 配置步骤	2
3.6 验证配置	4
3.7 配置文件	4
4 IGMP SSM Mapping 典型配置举例	5
4.1 组网需求	5
4.2 使用版本	6
4.3 配置步骤	6
4.4 验证配置	7
4.5 配置文件	8
5 IGMP Proxying 典型配置举例	10
5.1 组网需求	10
5.2 配置思路	11
5.3 使用版本	11
5.4 配置注意事项	11
5.5 配置步骤	11
5.6 验证配置	12
5.7 配置文件	12
6 参考资料	13

# 1 简介

IGMP（Internet Group Management Protocol，互联网组管理协议）用于在三层设备和其直连网段中的用户主机之间建立和维护组播组成员关系。本文介绍了 IGMP 的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 IGMP 特性。

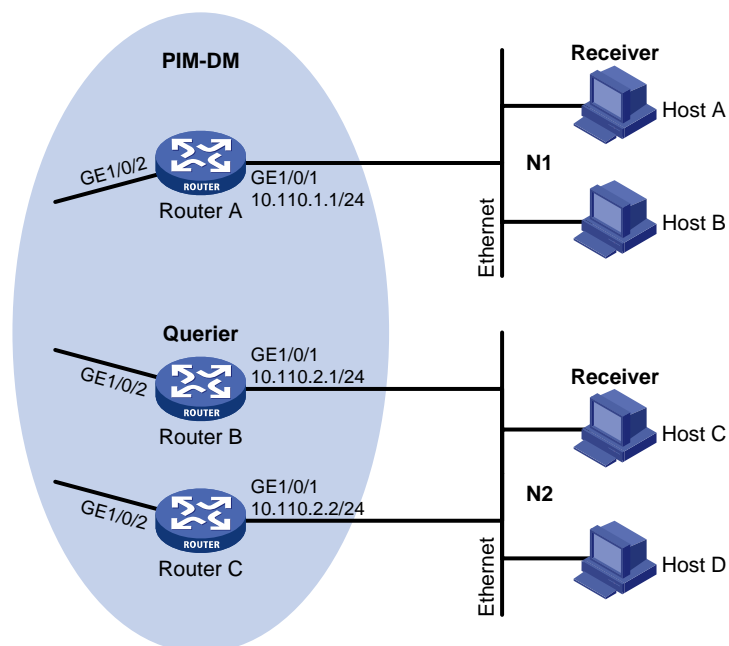
## 3 IGMP 基本功能配置举例

### 3.1 组网需求

如[图 1](#)所示，网络中运行 OSPF 和 PIM，接收者通过组播方式接收视频点播信息，不同组织的接收者组成末梢网络 N1 和 N2，Host A 和 Host C 分别为 N1 和 N2 中的组播信息接收者。Router A 与 N1 之间运行 IGMPv2，Router A 为 IGMP 查询器；Router B、Router C 与 N2 之间也分别运行 IGMPv2，且由于 Router B 的接口 IP 地址较小，因此由其充当 IGMP 查询器。现要求：

- 对网络 N1 内的接收者所能加入的组播组没有限制；
- 控制网络 N2 内的接收者只能加入组播组 224.1.1.1。

图1 IGMP 基本功能配置组网图



## 3.2 配置思路

- 因共享网段 N2 内有多台 IGMP 路由器，为实现本组网需求，需要在该共享网段内的所有 IGMP 路由器上都配置相同的 IGMP 组播组过滤器。
- 为实现 IGMP 组播组过滤器控制主机加入组播组的范围，需要为其创建基本 ACL，并在该 ACL 规则中指定允许主机加入的组播组范围。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置注意事项

由于不同版本 IGMP 协议的报文结构与种类不同，因此需要为同一网段上的所有路由器配置相同版本的 IGMP，否则 IGMP 将不能正常运行。

## 3.5 配置步骤

- (1) 配置 PIM-DM 域内各路由器的 IP 地址、单播路由协议和组播路由协议  
# 配置 PIM-DM 域内路由器上各接口的 IP 地址和子网掩码，具体配置过程略。  
# 配置 PIM-DM 域内的各路由器之间采用 OSPF 协议进行互连，确保 PIM-DM 域内部在网络层互通，并在各路由器上配置 PIM-DM 协议，以建立组播路由转发表项，实现组播数据可以从组播源到达接收者，具体配置过程略。
- (2) 配置 Router A

# 在 Router A 上使能 IP 组播路由，在接口 GigabitEthernet1/0/2 上使能 PIM-DM，并在主机侧接口 GigabitEthernet1/0/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

### (3) 配置 Router B

# 在 Router B 上使能 IP 组播路由，在接口 GigabitEthernet1/0/2 上使能 PIM-DM，并在主机侧接口 GigabitEthernet1/0/1 上使能 IGMP 及配置组播组过滤器，以在 Router B 上限制用户网络 N2 内的主机只能加入组播组 224.1.1.1。

```
<RouterB> system-view
[RouterB] acl number 2001
[RouterB-acl-basic-2001] rule permit source 224.1.1.1 0
[RouterB-acl-basic-2001] quit
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] igmp enable
[RouterB-GigabitEthernet1/0/1] igmp group-policy 2001
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] pim dm
[RouterB-GigabitEthernet1/0/2] quit
```

### (4) 配置 Router C

# 在 Router C 上使能 IP 组播路由，在接口 GigabitEthernet1/0/2 上使能 PIM-DM，并在主机侧接口 GigabitEthernet1/0/1 上使能 IGMP 及配置组播组过滤器，以在 Router C 上限制用户网络 N2 内的主机只能加入组播组 224.1.1.1。

```
<RouterC> system-view
[RouterC] acl number 2001
[RouterC-acl-basic-2001] rule permit source 224.1.1.1 0
[RouterC-acl-basic-2001] quit
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] igmp enable
[RouterC-GigabitEthernet1/0/1] igmp group-policy 2001
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] pim dm
[RouterC-GigabitEthernet1/0/2] quit
```



## 3.6 验证配置

配置完成后，用户网络 N2 内的组播接收者 Host C（地址为 10.110.2.10）分别发送组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，通过 `display igmp group` 命令查看 Router B 和 Router C 上 IGMP 组播组信息，验证配置效果：

# 查看 Router B 上 IGMP 组播组信息。

```
[RouterB] display igmp group
IGMP groups in total: 1.
GigabitEthernet1/0/1(10.110.2.1):
 IGMP groups reported in total: 1
 Group address Last reporter Uptime Expires
 224.1.1.1 10.110.2.10 00:02:04 00:01:15
```

# 查看 Router C 上 IGMP 组播组信息。

```
[RouterC] display igmp group
IGMP groups in total: 1..
GigabitEthernet1/0/1(10.110.2.2):
 IGMP groups reported in total: 1
 Group address Last reporter Uptime Expires
 224.1.1.1 10.110.2.10 00:02:04 00:01:15
```

Host C 发送了组播组地址为 224.1.1.1 和 224.1.1.2 的 IGMP 成员关系报告报文，而 Router B 和 Router C 上只有组播组 224.1.1.1 的 IGMP 组播组信息，由此可见在 Router B 和 Router C 上配置的 IGMP 组播组过滤器已生效，用户网络 N2 内的组播接收者只能加入组播组 224.1.1.1。

## 3.7 配置文件

- Router A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 igmp enable
#
interface GigabitEthernet1/0/2
 port link-mode route
 pim dm
#
multicast routing
#
```
- Router B:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 igmp enable
 igmp group-policy 2001
#
interface GigabitEthernet1/0/2
 port link-mode route
```

```
pim dm
#
multicast routing
#
acl number 2001
 rule 0 permit source 224.1.1.1 0
#
```

- Router C:

```
#
interface GigabitEthernet1/0/2
 port link-mode route
 pim dm
#
interface GigabitEthernet1/0/1
 port link-mode route
 igmp enable
 igmp group-policy 2001
#
multicast routing
#
acl number 2001
 rule 0 permit source 224.1.1.1 0
#
```

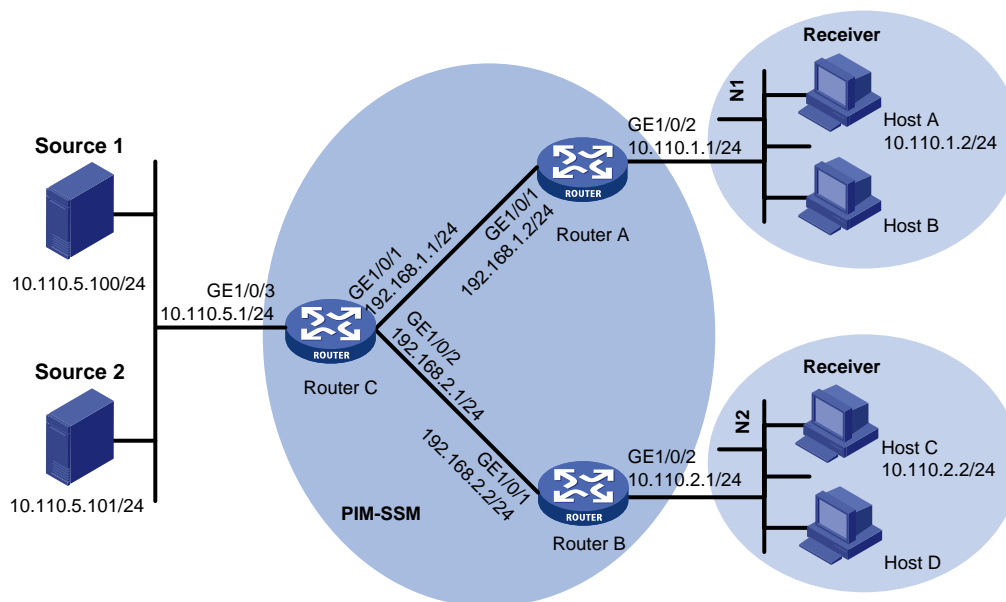
## 4 IGMP SSM Mapping 典型配置举例

### 4.1 组网需求

如图 2 所示，PIM-SSM 网络所服务的 SSM 组播组范围为 232.1.1.0/24，PIM-SSM 网络内连接用户网络 N1 和 N2 的边界路由器上均运行 IGMPv3 功能，而用户网络 N1、N2 内的主机 Host A 和 Host C 上只能运行 IGMPv1 或 IGMPv2，且不能升级至 IGMPv3；其他主机运行 IGMPv3。

现要求：通过在 IGMP 路由器上配置 IGMP SSM Mapping 功能，使 PIM-SSM 网络能够为用户网络 N1 内的接收者提供 SSM 组播服务，实现用户网络 N1 中的接收者只接收来自 Source 1 的组播报文。用户网络 N2 中的接收者只接收来自 Source 2 的组播报文。

图2 IGMP SSM Mapping 功能配置组网图



## 4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.3 配置步骤

### (1) 配置 IP 地址和单播路由协议

# 请按照图 2 配置各接口的 IP 地址和子网掩码，具体配置过程略。

# 配置 PIM-SSM 网络内的各路由器之间采用 OSPF 协议进行互连，具体配置过程略。

### (2) 使能 IP 组播路由，并使能 PIM-SM

# 在 Router A 上使能 IP 组播路由，在接口上使能 PIM-SM。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim sm
[RouterA-GigabitEthernet1/0/1] quit
```

Router B 的配置与 Router A 相似，配置过程略。

# 在 Router C 上使能 IP 组播路由，在各接口上使能 PIM-SM。

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] pim sm
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet1/0/2
```

```
[RouterC-GigabitEthernet1/0/2] pim sm
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] interface gigabitethernet1/0/3
[RouterC-GigabitEthernet1/0/3] pim sm
[RouterC-GigabitEthernet1/0/3] quit
```

(3) 配置 C-BSR 和 C-RP

# 在 Router C 上配置 C-BSR 和 C-RP 的位置。

```
[RouterC] pim
[RouterC-pim] c-bsr 192.168.1.1
[RouterC-pim] c-rp 192.168.1.1
[RouterC-pim] quit
```

(4) 在连接网络 N1 和 N2 的接口上使能 IGMPv3 功能

# 在 Router A 的接口 GigabitEthernet1/0/2 上使能 IGMPv3。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] igmp enable
[RouterA-GigabitEthernet1/0/2] igmp version 3
[RouterA-GigabitEthernet1/0/2] quit
```

Router B 的配置与 Router A 相似，配置过程略。

(5) 配置 SSM 组播组的地址范围

# 在 Router A 上配置 SSM 组播组地址范围为 232.1.1.0/24。

```
[RouterA] acl number 2000
[RouterA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[RouterA-acl-basic-2000] quit
[RouterA] pim
[RouterA-pim] ssm-policy 2000
[RouterA-pim] quit
```

Router B 和 Router C 的配置与 Router A 相同，配置过程略。

(6) 使能 IGMP SSM Mapping 功能，并配置 IGMP SSM Mapping 规则

# 在 Router A 上配置 IGMP SSM Mapping 规则，满足 N1 网络内组播报文接收者只接收来自组播源 Source 1 的组播数据的要求。

```
[RouterA] igmp
[RouterA-igmp] ssm-mapping 10.110.5.100 2000
[RouterA-igmp] quit
```

#在 Router B 上配置 IGMP SSM Mapping 规则，满足 N2 网络内组播报文接收者只接收来自组播源 Source 2 的组播数据的要求。

```
[RouterB] igmp
[RouterB-igmp] ssm-mapping 10.110.5.101 2000
[RouterB-igmp] quit
```

## 4.4 验证配置

配置完成后，Host A 和 Host C 都发送组播组地址为 232.1.1.1 的 IGMPv2 加入报文，在 Router A 和 Router B 上通过相关命令查看配置效果。

(1) Router A 上的显示信息

# 查看 Router A 上组播组 232.1.1.1 的 IGMP SSM Mapping 规则。

```
[RouterA] display igmp ssm-mapping 232.1.1.1
Group: 232.1.1.1
Source list:
10.110.5.100
查看 Router A 上的 PIM 路由表信息。
[RouterA] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 232.1.1.1)
 Protocol: pim-ssm, Flag:
 UpTime: 00:00:47
 Upstream interface: GigabitEthernet1/0/1
 Upstream neighbor: 192.168.1.1
 RPF prime neighbor: 192.168.1.1
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: GigabitEthernet1/0/2
 Protocol: igmp, UpTime: 00:00:47, Expires: -
```

## (2) Router B 上的显示信息

# 查看 Router B 上组播组 232.1.1.1 的 IGMP SSM Mapping 规则。

```
[RouterB] display igmp ssm-mapping 232.1.1.1
Group: 232.1.1.1
Source list:
10.110.5.101
查看 Router B 上的 PIM 路由表信息。
[RouterB] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.101, 232.1.1.1)
 Protocol: pim-ssm, Flag:
 UpTime: 00:00:47
 Upstream interface: GigabitEthernet1/0/1
 Upstream neighbor: 192.168.2.1
 RPF prime neighbor: 192.168.2.1
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: GigabitEthernet1/0/2
 Protocol: igmp, UpTime: 00:00:47, Expires: -
```

通过显示信息可知，在 Router A 和 Router B 上配置了 IGMP SSM Mapping 功能后，Router A 将接收者主机发来的 IGMPv2 成员关系报告报文中所包含的 (0.0.0.0, 232.1.1.1) 信息映射为 (10.110.5.100, 232.1.1.1) 信息，Router B 将接收者主机发来的 IGMPv2 成员关系报告报文中所包含的 (0.0.0.0, 232.1.1.1) 信息映射为 (10.110.5.101, 232.1.1.1) 信息，从而使接收者 Host A 只接收来自 Source 1 的组播报文，使接收者 Host C 只接收来自 Source 2 的组播报文。

## 4.5 配置文件

- RouterA:

```

#
interface GigabitEthernet1/0/1
 port link-mode route
 pim sm
#
interface GigabitEthernet1/0/2
 port link-mode route
 igmp enable
 igmp version 3
#
multicast routing
#
pim
 ssm-policy 2000
#
igmp
 ssm-mapping 10.110.5.100 2000
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#

```

- **Router B:**

```

#
interface GigabitEthernet1/0/1
 port link-mode route
 pim sm
#
interface GigabitEthernet1/0/2
 port link-mode route
 igmp enable
 igmp version 3
#
multicast routing
#
pim
 ssm-policy 2000
#
igmp
 ssm-mapping 10.110.5.100 2000
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#

```

- **Router C:**

```

#
interface GigabitEthernet1/0/1
 port link-mode route
 pim sm

```

```

#
interface GigabitEthernet1/0/2
 port link-mode route
 pim sm
#
interface GigabitEthernet1/0/3
 port link-mode route
 pim sm
#
multicast routing
#
pim
 c-bsr 192.168.1.1
 c-rp 192.168.1.1
#

```

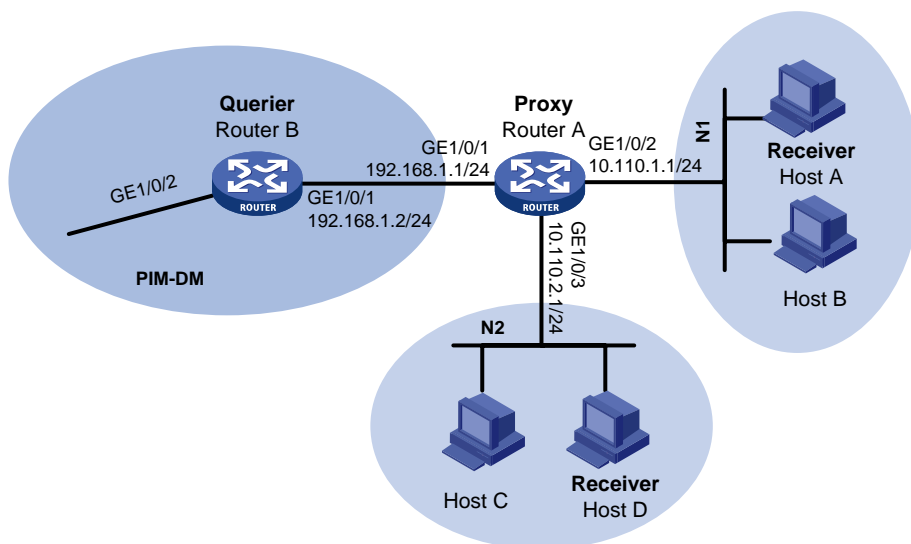
## 5 IGMP Proxying 典型配置举例

### 5.1 组网需求

如图3所示，用户网络 N1 和 N2 通过路由器 Router A 与 PIM-DM 域内的 IGMP 查询器 Router B 相连。

现要求通过在路由器 Router A 上配置 IGMP Proxying 功能，使其在不运行 PIM-DM 的情况下实现用户网络 N1、N2 内的接收者可以接收到通过 PIM-DM 域转发过来的组播数据报文。

图3 IGMP Proxying 功能配置组网图



## 5.2 配置思路

为实现本组网需求，需要在 IGMP 代理设备的上行接口上运行 IGMP Proxying 功能，上游设备将视 IGMP 代理设备为主机，而在其下行接口上运行 IGMP 协议，下游设备视 IGMP 代理设备为 IGMP 路由器。

## 5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 5.4 配置注意事项

- 在设备上开启 IGMP 代理功能时，须先使能 IP 组播路由。
- 一个接口上如果同时使能 IGMP 代理功能和 IGMP 协议，IGMP 协议将不会生效。在已使能 IGMP 代理功能的接口上配置其它 IGMP 命令时，只有 **igmp version** 命令会生效。
- 如果在一台设备上同时使能 IGMP 代理功能和组播路由协议（如 PIM 和 MSDP），组播路由协议将不会生效。

## 5.5 配置步骤

### (1) 配置 IP 地址

# 请按照图 3 配置各接口的 IP 地址和子网掩码，具体配置过程略。

# 配置 PIM-DM 网络内的各路由器之间采用 OSPF 协议进行互连，具体配置过程略。

### (2) 配置 Router A

# 在 Router A 上使能 IP 组播路由，并在朝向 Router B 侧的接口 GigabitEthernet1/0/1 上使能 IGMP 代理功能。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp proxy enable
[RouterA-GigabitEthernet1/0/2] quit
```

# 在 Router A 上朝向用户侧的接口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上使能 IGMP。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] igmp enable
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] interface gigabitethernet 1/0/3
[RouterA-GigabitEthernet1/0/3] igmp enable
[RouterA-GigabitEthernet1/0/3] quit
```

### (3) 配置 Router B

# 在 Router B 上使能 IP 组播路由，并在接口 GigabitEthernet1/0/2 上使能 PIM-DM。

```
<RouterB> system-view
[RouterB]multicast routing
```



```

[RouterB-mrib]quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/1] pim dm
[RouterB-GigabitEthernet1/0/1] quit
#在 Router B 上朝向用户侧的接口 GigabitEthernet1/0/1 上使能 IGMP。
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] igmp enable
[RouterB-GigabitEthernet1/0/1] quit

```

## 5.6 验证配置

配置完成后，用户网络 N1 内的组播接收者 Host A 发送组播组地址为 224.1.1.1 的 IGMP 成员关系报告报文，通过 **display igmp group** 命令查看 Router A 和 Router B 上 IGMP 组播组信息，检验配置效果：

# 查看 Router A 的 GigabitEthernet1/0/2 接口上 IGMP 组播组信息。

```

[RouterA] display igmp group interface GigabitEthernet1/0/2
GigabitEthernet1/0/2(10.110.1.1):
 IGMP groups reported in total: 1
 Group address Last reporter Uptime Expires
 224.1.1.1 10.110.1.10 00:02:04 00:01:15

```

# 查看 Router A 上 IGMP 代理记录的所有组播组信息。

```

[RouterA] display igmp proxy group
IGMP proxy group records in total: 1
GigabitEthernet1/0/1(192.168.1.1):
 IGMP proxy group records in total: 1
 Group address Member state Expires
 224.1.1.1 Delay 00:00:02

```

通过显示信息可知，Router A 的 GigabitEthernet1/0/2 接口接收到主机的 IGMP 成员关系报告报文后，建立并维护该组播组成员关系，对于下面的主机而言，Router A 的下行接口执行 IGMP 协议的路由器行为。

# 查看 Router B 的 GigabitEthernet1/0/1 接口上 IGMP 组播组信息。

```

[RouterB] display igmp group interface GigabitEthernet1/0/1
GigabitEthernet1/0/1(192.168.1.2):
 IGMP groups reported in total: 1
 Group address Last reporter Uptime Expires
 224.1.1.1 192.168.1.1 00:02:04 00:01:15

```

通过显示信息可知，Router B 的 GigabitEthernet1/0/1 接口接收到 IGMP Proxying 设备的 IGMP 成员关系报告报文后，建立并维护该组播组成员关系。由此可见，对于上游查询器 Router B 而言，Router A 的上行接口执行 IGMP 协议的主机行为。

## 5.7 配置文件

- Router A:
 

```

#
interface GigabitEthernet1/0/1
 port link-mode route

```

```
igmp proxy enable
#
interface GigabitEthernet1/0/2
port link-mode route
igmp enable
#
interface GigabitEthernet1/0/3
port link-mode route
igmp enable
#
multicast routing
#
```

- **Router B:**

```
#
interface GigabitEthernet1/0/1
port link-mode route
igmp enable
#
interface GigabitEthernet1/0/2
port link-mode route
pim dm
#
multicast routing
#
```

## 6 参考资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“IP 组播配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“IP 组播命令参考”

# H3C MSR 系列路由器

## 组播 VPN 配置举例

---

Copyright © 2021-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提.....	1
3 单 AS 内 MVPNT 模式 VPN 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.5.1 配置各设备接口 IP 地址.....	2
3.5.2 配置路由及基本 MPLS L3VPN.....	2
3.5.3 配置组播路由及相关功能及 MVPNT 模式 MVPN.....	2
3.6 验证配置.....	5
3.7 配置文件.....	6
4 A 类跨 AS 的 MDT 模式 MVPN 配置举例.....	8
4.1 组网需求.....	8
4.2 配置思路.....	9
4.3 使用版本.....	9
4.4 配置注意事项.....	9
4.5 配置步骤.....	10
4.5.1 配置各设备接口 IP 地址.....	10
4.5.2 配置路由和 OptionA 方式的跨域 MPLS L3VPN.....	10
4.5.3 配置组播路由及相关功能及 MDT 模式 MVPN.....	10
4.6 验证配置.....	14
4.7 配置文件.....	15
5 C 类跨 AS 的 MVPNT 模式 MVPN 配置举例.....	18
5.1 组网需求.....	18
5.2 配置思路.....	19
5.3 使用版本.....	19
5.4 配置步骤.....	19
5.4.1 配置各设备接口 IP 地址.....	19
5.4.2 配置路由和 OptionC 方式的跨域 MPLS L3VPN.....	20
5.4.3 配置组播路由及相关功能及 MDT 模式 MVPN.....	20

5.5 验证配置 .....	23
5.6 配置文件 .....	24
6 相关资料 .....	27

# 1 简介

本文档介绍组播 VPN 的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

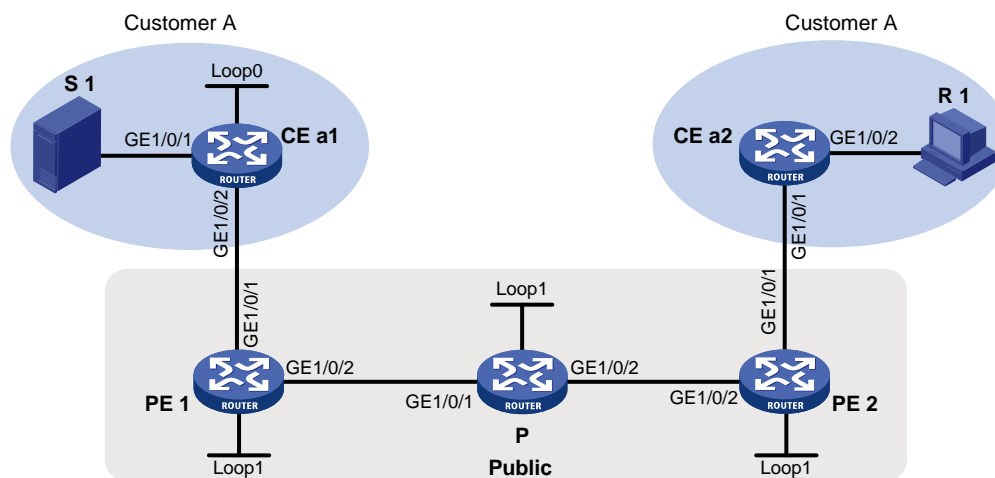
本文档假设您已了解组播 VPN 特性。

## 3 单 AS 内 MVPNT 模式 VPN 配置举例

### 3.1 组网需求

如图 1 所示，Customer A 有位于两地的分支机构，这两个分支机构已通过同一个运营商的 MPLS L3VPN 网络实现了两地间单播路由信息的正常交互。目前 Customer A 中的组播源与接收者分别位于不同的分支机构中，且各分支机构内运行的 PIM 协议模式为 PIM-SM。现要求通过 MVPNT 模式 MVPN 技术，实现组播接收者能够正常接收到组播源发来的组播数据。

图1 配置单 AS 内 MVPNT 模式 VPN 组网图



设备	接口	IP地址	设备	接口	IP地址
S 1	-	10.11.3.2/24	PE 2	GE1/0/2	192.168.2.2/24
PE 1	GE1/0/2	192.168.1.2/24		GE1/0/1	10.11.2.1/24
	GE1/0/1	10.11.1.1/24		Loop1	1.1.1.2/32
	Loop1	1.1.1.1/32	CE a1	GE1/0/1	10.11.3.1/24
P	GE1/0/1	192.168.1.1/24		GE1/0/2	10.11.1.2/24
	GE1/0/2	192.168.2.1/24		Loop0	2.2.2.2/32
	Loop1	3.3.3.3/32	CE a2	GE1/0/2	10.11.4.1/24
R 1	-	10.11.4.2/24		GE1/0/1	10.11.2.2/24

## 3.2 配置思路

为了实现上述组网需求，需要在公网的各设备上运行 PIM 协议（与私网中的 PIM 协议模式相互独立），并在各 PE 设备上配置 MVPNT 模式 MVPN。

## 3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 3.4 配置注意事项

- 配置 MVPNT 模式 MVPN 时，只有在指定了 Default-Group 和 MVPN 源接口，并获取到 MVPN 源接口的公网 IP 地址之后，MTI 才会生效。
- 属于同一 VPN 的所有接口（包括 PE 上绑定 VPN 实例的接口）上必须运行相同模式的 PIM 协议。
- 在不同的 PE 上，应该为相同 MDT 模式 MVPN 实例指定相同的 Default-Group。
- MVPN 源接口必须与建立 BGP 对等体时所使用的源接口相同，否则将无法获取正确的路由信息。

## 3.5 配置步骤

### 3.5.1 配置各设备接口 IP 地址

按图 1 配置各设备上的接口 IP 地址和子网掩码。

```
<CEa1> system-view
[CEa1] interface gigabitethernet 1/0/1
[CEa1-GigabitEthernet1/0/1] ip address 10.11.3.1 24
[CEa1-GigabitEthernet1/0/1] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface gigabitethernet 1/0/2
[CEa1-GigabitEthernet1/0/2] ip address 10.11.1.2 24
[CEa1-GigabitEthernet1/0/2] quit
```

PE 1、P、PE 2 和 CE a2 的配置与 CE a1 相似，配置过程略。

### 3.5.2 配置路由及基本 MPLS L3VPN

配置路由协议及基本 MPLS L3VPN，实现两地间单播路由信息互通。具体配置请参见《H3C MSR 系列路由器 配置指导(V7)》中的“MPLS 配置指导/MPLS L3VPN”。

### 3.5.3 配置组播路由相关功能及 MVPNT 模式 MVPN

- (1) 在公网实例中使能 IP 组播路由、公网接口上配置 PIM-SM 功能（包括 LoopBack 接口）  
# 在 PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```

<PE1> system-view
[PE1] multicast routing
[PE1-mrib] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] pim sm
[PE1-GigabitEthernet1/0/2] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit

```

# 在 P 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 1 接口指定为公网的 C-BSR 和 C-RP，其中 C-RP 服务于公网实例中所有组播组。

```

<P> system-view
[P] multicast routing
[P-mrib] quit
[P] interface gigabitethernet 1/0/1
[P-GigabitEthernet1/0/1] pim sm
[P-GigabitEthernet1/0/1] quit
[P] interface gigabitethernet 1/0/2
[P-GigabitEthernet1/0/2] pim sm
[P-GigabitEthernet1/0/2] quit
[P] interface loopback 1
[P-LoopBack1] pim sm
[P-LoopBack1] quit
[P] pim
[P-pim] c-bsr 3.3.3.3
[P-pim] c-rp 3.3.3.3
[P-pim] quit

```

# 在 PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```

<PE2> system-view
[PE2] multicast routing
[PE2-mrib] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] pim sm
[PE2-GigabitEthernet1/0/2] quit
[PE2] interface loopback 1
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit

```

- (2) 在 VPN 私网实例中使能 IP 组播路由、私网接口上配置 PIM-SM 功能，并在连接有接收者的 CE 上配置 IGMP

# 在 CE a1 上使能 IP 组播路由，在各接口上配置 PIM-SM，并将 LoopBack 0 接口指定为私网的 C-BSR 和 C-RP，其中 C-RP 服务于 Customer A 实例中所有组播组。

```

<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
[CEa1] interface gigabitethernet 1/0/1
[CEa1-GigabitEthernet1/0/1] pim sm
[CEa1-GigabitEthernet1/0/1] quit

```



```

[CEa1] interface gigabitethernet 1/0/2
[CEa1-GigabitEthernet1/0/2] pim sm
[CEa1-GigabitEthernet1/0/2] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit

```

**# 在 CE a2 上使能 IP 组播路由，在连接有接收者的接口上使能 IGMP，其余各接口上配置 PIM-SM。**

```

<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
[CEa2] interface gigabitethernet 1/0/1
[CEa2-GigabitEthernet1/0/1] pim sm
[CEa2-GigabitEthernet1/0/1] quit
[CEa2] interface gigabitethernet 1/0/2
[CEa2-GigabitEthernet1/0/2] igmp enable
[CEa2-GigabitEthernet1/0/2] quit

```

**# 在 PE 1 上配置 VPN 实例 Customer A，将接口 GigabitEthernet1/0/1 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。**

```

[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 100:1
[PE1-vpn-instance-customerA] vpn-target 100:1
[PE1-vpn-instance-customerA] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] ip binding vpn-instance customerA
[PE1-GigabitEthernet1/0/1] quit
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] pim sm
[PE1-GigabitEthernet1/0/1] quit

```

**# 在 PE 2 上配置 VPN 实例 Customer A，将接口 GigabitEthernet1/0/1 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。**

```

[PE2] ip vpn-instance customerA
[PE2-vpn-instance-customerA] route-distinguisher 100:1
[PE2-vpn-instance-customerA] vpn-target 100:1
[PE2-vpn-instance-customerA] quit
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] ip binding vpn-instance customerA
[PE2-GigabitEthernet1/0/1] quit
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
[PE2] interface gigabitethernet 1/0/1

```

```
[PE2-GigabitEthernet1/0/1] pim sm
[PE2-GigabitEthernet1/0/1] quit
```

(3) 创建 VPN 实例的 MVPN，并指定 Default-Group、MVPN 源接口和 Data-Group 范围

# 在 PE1 上创建 VPN 实例的 MVPN，并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE1] multicast-vpn vpn-instance customerA mode mdt
[PE1-mvpn-customerA] address-family ipv4
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE1-mvpn-customerA-ipv4] quit
[PE1-mvpn-customerA] quit
```

# 在 PE 2 上创建 VPN 实例的 MVPN，并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE2-mvpn-customerA] address-family ipv4
[PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE2-mvpn-customerA-ipv4] source loopback 1
[PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE2-mvpn-customerA] quit
```

## 3.6 验证配置

按照如上配置后，通过在 PE 及 P 设备上执行 **display pim routing-table** 命令，可以检查公网 Default-MDT 建立情况，以 P 设备为例：

```
[P] display pim routing-table
Total 1 (*, G) entry; 2 (S, G) entry

(*, 239.1.1.1)
 RP: 3.3.3.3 (local)
 Protocol: pim-sm, Flag: SPT LOC ACT
 UpTime: 02:54:43
 Upstream interface: Register
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
 Downstream interface(s) information:
 Total number of downstreams: 2
 1: GigabitEthernet1/0/1
 Protocol: pim-sm, UpTime: 02:54:43, Expires: -
 2: GigabitEthernet1/0/2
 Protocol: pim-sm, UpTime: 02:33:57, Expires: -

(1.1.1.1, 239.1.1.1)
 RP: 3.3.3.3 (local)
 Protocol: pim-sm, Flag: SPT LOC ACT
 UpTime: 01:57:13
 Upstream interface: GigabitEthernet1/0/1
```

```
Upstream neighbor: 192.168.1.2
RPF prime neighbor: 192.168.1.2
Downstream interface(s) information: None
```

```
(1.1.1.2, 239.1.1.1)
RP: 3.3.3.3 (local)
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 01:57:13
Upstream interface: GigabitEthernet1/0/2
Upstream neighbor: 192.168.2.2
RPF prime neighbor: 192.168.2.2
Downstream interface(s) information: None
```

由此可见，公网 P 设备上已建立 RPT (\*, 239.1.1.1) 和两棵相互独立的 SPT 树，这三棵树共同组成了该公网上的 Default-MVPNT。

### 3.7 配置文件

- PE 1:

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface GigabitEthernet1/0/1
 ip binding vpn-instance customerA
 ip address 10.11.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/2
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
 source LoopBack1
 default-group 239.1.1.1
 data-group 225.1.1.0 255.255.255.240
#
```
- PE 2:

```

#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface GigabitEthernet1/0/1
 ip binding vpn-instance customerA
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/2
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
 source LoopBack1
 default-group 239.1.1.1
 data-group 225.1.1.0 255.255.255.240
#

```

- **P:**

```

#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
interface GigabitEthernet1/0/1
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/2
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 3.3.3.3
 c-rp 3.3.3.3

```

- ```

#
• CE a1:
#
interface LoopBack0
  ip address 2.2.2.2 255.255.255.255
  pim sm
#
interface GigabitEthernet1/0/1
  ip address 10.11.3.1 255.255.255.0
  pim sm
#
interface GigabitEthernet1/0/2
  ip address 10.11.1.2 255.255.255.0
  pim sm
#
multicast routing
#
pim
  c-bsr 2.2.2.2
  c-rp 2.2.2.2
#
• CE a2:
#
interface GigabitEthernet1/0/1
  ip address 10.11.2.2 255.255.255.0
  pim sm
#
interface GigabitEthernet1/0/2
  ip address 10.11.4.1 255.255.255.0
  igmp enable
#
multicast routing
#

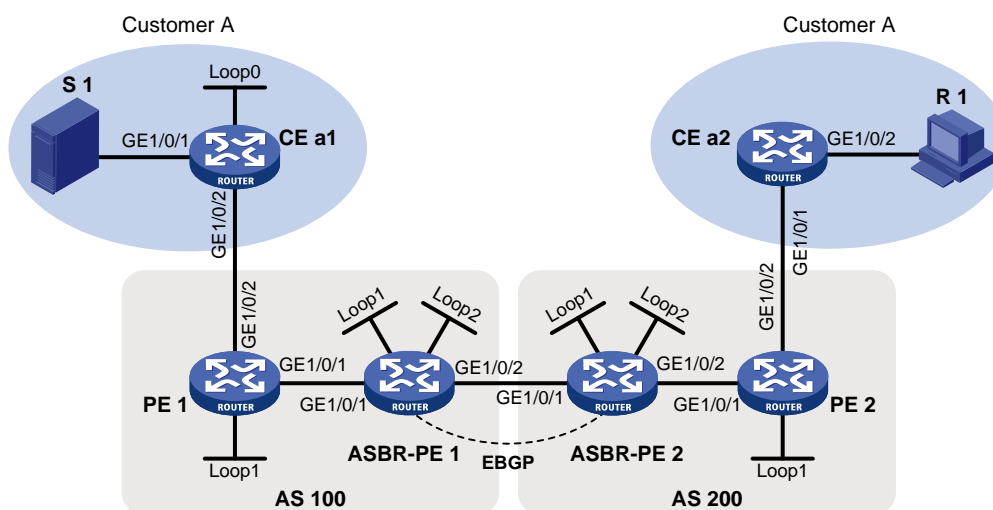
```

4 A类跨AS的MDT模式MVPN配置举例

4.1 组网需求

如图 2 所示，Customer A 有位于两地的分支机构，这两个分支机构跨越了两个运营商网络，并已通过跨域 VPN-OptionA 方案实现了两地间单播路由信息的正常交互。目前 Customer A 中的组播源与接收者分别位于不同的分支机构中，且各分支机构内运行的 PIM 协议模式为 PIM-SM。现要求通过 MDT 模式 MVPN 技术，实现组播接收者能够正常接收到组播源发来的组播数据。

图2 配置 A 类跨 AS 的 MDT 模式 MVPN 组网图



| 设备 | 接口 | IP地址 | 设备 | 接口 | IP地址 |
|-----------|---------|----------------|-----------|---------|----------------|
| S 1 | - | 10.11.3.2/24 | R 1 | - | 10.11.4.2/24 |
| PE 1 | GE1/0/1 | 192.168.1.2/24 | ASBR-PE 2 | GE1/0/1 | 192.168.2.2/24 |
| | GE1/0/2 | 10.11.1.1/24 | | GE1/0/2 | 192.168.3.2/24 |
| | Loop1 | 1.1.1.1/32 | | Loop1 | 1.1.1.3/32 |
| ASBR-PE 1 | GE1/0/1 | 192.168.1.1/24 | | Loop2 | 22.22.22.22/32 |
| | GE1/0/2 | 192.168.2.1/24 | PE 2 | GE1/0/1 | 192.168.3.1/24 |
| | Loop1 | 1.1.1.2/32 | | GE1/0/2 | 10.11.2.1/24 |
| | Loop2 | 11.11.11.11/32 | | Loop1 | 1.1.1.4/32 |
| CE a1 | GE1/0/1 | 10.11.3.1/24 | CE a2 | GE1/0/1 | 10.11.2.2/24 |
| | GE1/0/2 | 10.11.1.2/24 | | GE1/0/2 | 10.11.4.1/24 |
| | Loop0 | 2.2.2.2/32 | | | |

4.2 配置思路

为了实现上述组网需求，需要在每个 AS 内各建立一个独立的 MDT 模式 MVPN 实例。

4.3 使用版本

本举例是在 Release R0106 版本上进行配置和验证的。

4.4 配置注意事项

- 各 AS 内部运行的公网 PIM 模式可以不同，但属于同一 VPN 的所有接口（包括 ASBR 上绑定 VPN 实例的接口）上必须运行统一的 PIM 模式。
- 对于同一 AS 内的相同 VPN 实例的 MDT 模式 MVPN，应为其指定相同的 Default-Group，对于不同 AS 的相同 VPN 实例，为其 MDT 模式 MVPN 指定的 Default-Group 可以不同。

4.5 配置步骤

4.5.1 配置各设备接口 IP 地址

按图 2 配置各设备上的接口 IP 地址和子网掩码。

```
<CEa1> system-view
[CEa1] interface gigabitethernet 1/0/1
[CEa1-GigabitEthernet1/0/1] ip address 10.11.3.1 24
[CEa1-GigabitEthernet1/0/1] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface gigabitethernet 1/0/2
[CEa1-GigabitEthernet1/0/2] ip address 10.11.1.2 24
[CEa1-GigabitEthernet1/0/2] quit
```

PE 1、ASBR-PE 1、ASBR-PE 2、PE 2 和 CE a2 的配置与 CE a1 相似，配置过程略。

4.5.2 配置路由和 OptionA 方式的跨域 MPLS L3VPN

配置路由协议及 OptionA 方式的跨域 MPLS L3VPN，实现两地间单播路由信息互通。具体配置请参见《H3C MSR 系列路由器 配置指导(V7)》中的“MPLS 配置指导/MPLS L3VPN”。

4.5.3 配置组播路由相关功能及 MDT 模式 MVPN

- (1) 在各 AS 的公网实例中使能 IP 组播路由、公网接口上配置 PIM-SM 功能（包括 LoopBack 接口）

在 PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```
<PE1> system-view
[PE1] multicast routing
[PE1-mrib] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] pim sm
[PE1-GigabitEthernet1/0/1] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

在 ASBR-PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 2 接口指定为 AS 100 公网的 C-BSR 和 C-RP，其中 C-RP 服务于该公网实例中所有组播组。

```
<ASBR-PE1> system-view
[ASBR-PE1] multicast routing
[ASBR-PE1-mrib] quit
[ASBR-PE1] interface gigabitethernet 1/0/1
[ASBR-PE1-GigabitEthernet1/0/2] pim sm
[ASBR-PE1-GigabitEthernet1/0/2] quit
[ASBR-PE1] interface loopback 1
[ASBR-PE1-LoopBack1] pim sm
[ASBR-PE1-LoopBack1] quit
```

```

[ASBR-PE1] interface loopback 2
[ASBR-PE1-LoopBack2] pim sm
[ASBR-PE1-LoopBack2] quit
[ASBR-PE1] pim
[ASBR-PE1-pim] c-bsr 11.11.11.11
[ASBR-PE1-pim] c-rp 11.11.11.11
[ASBR-PE1-pim] quit

```

在 PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```

<PE2> system-view
[PE2] multicast routing
[PE2-mrib] quit
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] pim sm
[PE2-GigabitEthernet1/0/1] quit
[PE2] interface loopback 1
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit

```

在配置 ASBR-PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 2 接口指定为 AS 200 公网的 C-BSR 和 C-RP，其中 C-RP 服务于该公网实例中所有组播组。

```

<ASBR-PE2> system-view
[ASBR-PE2] multicast routing
[ASBR-PE2-mrib] quit
[ASBR-PE2] interface gigabitethernet 1/0/2
[ASBR-PE2-GigabitEthernet1/0/2] pim sm
[ASBR-PE2-GigabitEthernet1/0/2] quit
[ASBR-PE2] interface loopback 1
[ASBR-PE2-LoopBack1] pim sm
[ASBR-PE2-LoopBack1] quit
[ASBR-PE2] interface loopback 2
[ASBR-PE2-LoopBack2] pim sm
[ASBR-PE2-LoopBack2] quit
[ASBR-PE2] pim
[ASBR-PE2-pim] c-bsr 22.22.22.22
[ASBR-PE2-pim] c-rp 22.22.22.22
[ASBR-PE2-pim] quit

```

- (2) 在 VPN 私网实例中使能 IP 组播路由、私网接口上配置 PIM-SM 功能，并在连接有接收者的 CE 上配置 IGMP



说明

同一 AS 内的 ASBR 与 PE 的 VPN 实例的 VPN Target 应能匹配，不同 AS 的 PE 的 VPN 实例的 VPN Target 则不需要匹配。

在 CE a1 上使能 IP 组播路由，在各接口上配置 PIM-SM，并将 LoopBack 0 接口指定为私网的 C-BSR 和 C-RP，其中 C-RP 服务于 Customer A 实例中所有组播组。

```

<CEa1> system-view
[CEa1] multicast routing

```



```

[CEa1-mrib] quit
[CEa1] interface gigabitethernet 1/0/1
[CEa1-GigabitEthernet1/0/1] pim sm
[CEa1-GigabitEthernet1/0/1] quit
[CEa1] interface gigabitethernet 1/0/2
[CEa1-GigabitEthernet1/0/2] pim sm
[CEa1-GigabitEthernet1/0/2] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit

```

在 CE a2 上使能 IP 组播路由，在连接有接收者的接口上使能 IGMP，其余各接口上配置 PIM-SM。

```

<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
[CEa2] interface gigabitethernet 1/0/1
[CEa2-GigabitEthernet1/0/2] pim sm
[CEa2-GigabitEthernet1/0/2] quit
[CEa2] interface gigabitethernet 1/0/2
[CEa2-GigabitEthernet1/0/2] igmp enable
[CEa2-GigabitEthernet1/0/2] quit

```

在 PE 1 上配置 VPN 实例 Customer A，将接口 GigabitEthernet1/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```

[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 100:1
[PE1-vpn-instance-customerA] vpn-target 100:1
[PE1-vpn-instance-customerA] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] ip binding vpn-instance customerA
[PE1-GigabitEthernet1/0/2] quit
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] pim sm
[PE1-GigabitEthernet1/0/2] quit

```

在 PE 2 上配置 VPN 实例 Customer A，将接口 GigabitEthernet1/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM

```

[PE2] ip vpn-instance customerA
[PE2-vpn-instance] route-distinguisher 200:1
[PE2-vpn-instance] vpn-target 200:1
[PE2-vpn-instance] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] ip binding vpn-instance customerA

```

```
[PE2-GigabitEthernet1/0/2] quit
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] pim sm
[PE2-GigabitEthernet1/0/2] quit
```

在 ASBR-PE 1 上配置 VPN 实例 Customer A，将接口 GigabitEthernet1/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[ASBR-PE1] ip vpn-instance customerA
[ASBR-PE1-vpn-instance-customerA] route-distinguisher 100:1
[ASBR-PE1-vpn-instance-customerA] vpn-target 100:1
[ASBR-PE1-vpn-instance-customerA] quit
[ASBR-PE1] interface gigabitethernet 1/0/2
[ASBR-PE1-GigabitEthernet1/0/2] ip binding vpn-instance customerA
[ASBR-PE1-GigabitEthernet1/0/2] quit
[ASBR-PE1] multicast routing vpn-instance customerA
[ASBR-PE1-mrib-customerA] quit
[ASBR-PE1] interface gigabitethernet 1/0/2
[ASBR-PE1-GigabitEthernet1/0/2] pim sm
[ASBR-PE1-GigabitEthernet1/0/2] quit
```

在 ASBR-PE 2 上配置 VPN 实例 Customer A，将接口 GigabitEthernet1/0/1 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[ASBR-PE2] ip vpn-instance customerA
[ASBR-PE2-vpn-vpn-customerA] route-distinguisher 200:1
[ASBR-PE2-vpn-vpn-customerA] vpn-target 200:1
[ASBR-PE2-vpn-vpn-customerA] quit
[ASBR-PE2] interface gigabitethernet 1/0/1
[ASBR-PE2-GigabitEthernet1/0/1] ip binding vpn-instance customerA
[ASBR-PE2-GigabitEthernet1/0/1] quit
[ASBR-PE2] multicast routing vpn-instance customerA
[ASBR-PE2-mrib-customerA] quit
[ASBR-PE2] interface gigabitethernet 1/0/1
[ASBR-PE2-GigabitEthernet1/0/1] pim sm
[ASBR-PE2-GigabitEthernet1/0/1] quit
```

- (3) 在每个 AS 内各建立一个独立的 MDT 模式 MVPN，并指定 Default-Group、MVPN 源接口和 Data-Group 范围

在 PE1 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE1] multicast-vpn vpn-instance customerA mode mdt
[PE1-mvpn-customerA] address-family ipv4
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE1-mvpn-customerA-ipv4] quit
[PE1-mvpn-customerA] quit
```

在 ASBR-PE 1 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[ASBR-PE1] multicast-vpn vpn-instance customerA mode mdt
[ASBR-PE1-mvpn-customerA] address-family ipv4
[ASBR-PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[ASBR-PE1-mvpn-customerA-ipv4] source loopback 1
[ASBR-PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[ASBR-PE1-mvpn-customerA-ipv4] quit
[ASBR-PE1-mvpn-customerA] quit
```

在 PE 2 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[PE2] multicast-vpn vpn-instance customerA mode mdt
[PE2-mvpn-customerA] address-family ipv4
[PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE2-mvpn-customerA-ipv4] source loopback 1
[PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE2-mvpn-customerA] quit
```

在 ASBR-PE 2 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```
[ASBR-PE2] multicast-vpn vpn-instance customerA mode mdt
[ASBR-PE2-mvpn-customerA] address-family ipv4
[ASBR-PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[ASBR-PE2-mvpn-customerA-ipv4] source loopback 1
[ASBR-PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[ASBR-PE2-mvpn-customerA-ipv4] quit
[ASBR-PE2-mvpn-customerA] quit
```

4.6 验证配置

按照如上配置后，通过在 PE 及 ASBR-PE 设备上执行 **display pim routing-table** 命令，可以检查各 AS 的公网 Default-MDT 建立情况，以 ASBR-PE 1 设备为例：

```
[ASBR-PE1] display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, 239.1.1.1)
  RP: 11.11.11.11 (local)
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 02:54:43
  Upstream interface: Register
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: GigabitEthernet1/0/1
      Protocol: pim-sm, UpTime: 02:54:43, Expires: -
```

```
(1.1.1.1, 239.1.1.1)
  RP: 11.11.11.11 (local)
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 01:57:13
  Upstream interface: GigabitEthernet1/0/1
    Upstream neighbor: 192.168.1.2
    RPF prime neighbor: 192.168.1.2
  Downstream interface(s) information: None
```

由此可见，公网 ASBR-PE 1 设备上已建立 RPT (*, 239.1.1.1) 和 SPT(1.1.1.1, 239.1.1.1)，这两棵树共同组成了 AS 100 公网上的 Default-MDT。

4.7 配置文件

- PE 1:

```
#
ip vpn-instance customerA
  route-distinguisher 100:1
  vpn-target 100:1 import-extcommunity
  vpn-target 100:1 export-extcommunity
#
interface LoopBack1
  ip address 1.1.1.1 255.255.255.255
  pim sm
#
interface GigabitEthernet1/0/1
  ip address 192.168.1.2 255.255.255.0
  pim sm
#
interface GigabitEthernet1/0/2
  ip binding vpn-instance customerA
  ip address 10.11.1.1 255.255.255.0
  pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
  address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#
```

- PE 2:

```
#
ip vpn-instance customerA
  route-distinguisher 200:1
  vpn-target 200:1 import-extcommunity
```

```

vpn-target 200:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.4 255.255.255.255
 pim sm
#
interface GigabitEthernet1/0/1
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/2
 ip binding vpn-instance customerA
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
 source LoopBack1
 default-group 239.1.1.1
 data-group 225.1.1.0 255.255.255.240
#

```

- **ASBR-PE 1:**

```

#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 11.11.11.11 255.255.255.255
 pim sm
#
interface GigabitEthernet1/0/1
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/2
 ip binding vpn-instance customerA
 ip address 192.168.2.1 255.255.255.0
 pim sm

```

```

#
multicast routing
#
multicast routing vpn-instance customerA
#
pim
  c-bsr 11.11.11.11
  c-rp 11.11.11.11
#
multicast-vpn vpn-instance customerA mode mdt
  address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.1.1.0 255.255.255.240
#

```

- **ASBR-PE 2:**

```

#
ip vpn-instance customerA
  route-distinguisher 200:1
  vpn-target 200:1 import-extcommunity
  vpn-target 200:1 export-extcommunity
#
interface LoopBack1
  ip address 1.1.1.3 255.255.255.255
  pim sm
#
interface LoopBack2
  ip address 22.22.22.22 255.255.255.255
  pim sm
#
interface GigabitEthernet1/0/1
  ip binding vpn-instance customerA
  ip address 192.168.2.2 255.255.255.0
  pim sm
#
interface GigabitEthernet1/0/2
  ip address 192.168.3.2 255.255.255.0
  pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
pim
  c-bsr 22.22.22.22
  c-rp 22.22.22.22
#
multicast-vpn vpn-instance customerA mode mdt

```

```

address-family ipv4
source LoopBack1
default-group 239.1.1.1
data-group 225.1.1.0 255.255.255.240
#

```

- **CE a1:**

```

#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
pim sm
#
interface GigabitEthernet1/0/1
ip address 10.11.3.1 255.255.255.0
pim sm
#
interface GigabitEthernet1/0/2
ip address 10.11.1.2 255.255.255.0
pim sm
#
multicast routing
#
pim
c-bsr 2.2.2.2
c-rp 2.2.2.2
#

```
- **CE a2:**

```

#
interface GigabitEthernet1/0/1
ip address 10.11.2.2 255.255.255.0
pim sm
#
interface GigabitEthernet1/0/2
ip address 10.11.4.1 255.255.255.0
igmp enable
#
multicast routing
#

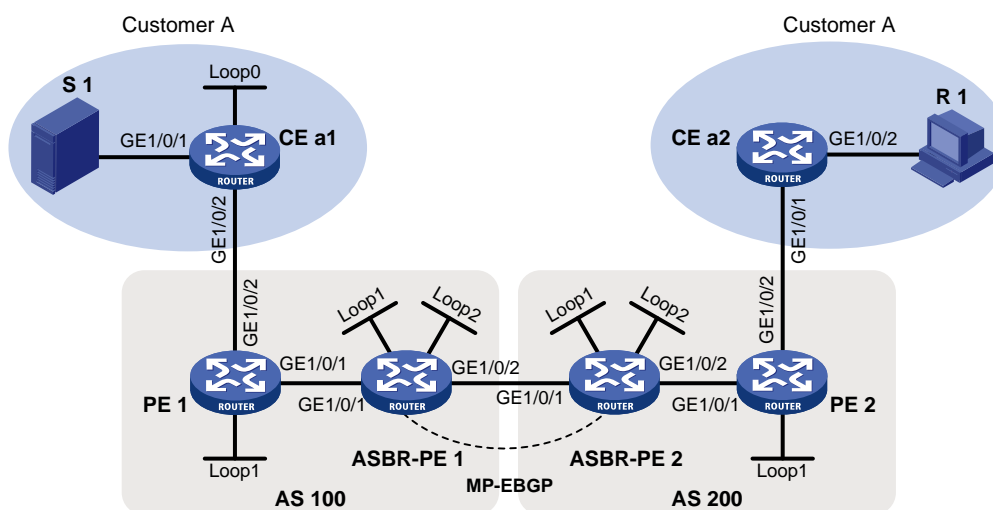
```

5 C类跨AS的MVPNT模式MVPN配置举例

5.1 组网需求

如图3所示，Customer A有位于两地的分支机构，这两个分支机构跨越了两个运营商网络，并已通过跨域VPN-OptionC方案实现了两地间单播路由信息的正常交互。目前Customer A中的组播源与接收者分别位于不同的分支机构中，且各分支机构内运行的PIM协议模式为PIM-SM。现要求通过MDT模式MVPN技术，实现组播接收者能够正常接收到组播源发来的组播数据。

图3 配置 C 类跨 AS 的 MDT 模式 MVPN 组网图



| 设备 | 接口 | IP地址 | 设备 | 接口 | IP地址 |
|----------|---------|----------------|----------|---------|----------------|
| S 1 | - | 10.11.3.2/24 | R 1 | - | 10.11.4.2/24 |
| PE 1 | GE1/0/1 | 192.168.1.2/24 | ASBR-PE2 | GE1/0/1 | 192.168.2.2/24 |
| | GE1/0/2 | 10.11.1.1/24 | | GE1/0/2 | 192.168.3.2/24 |
| | Loop1 | 1.1.1.1/32 | | Loop1 | 1.1.1.3/32 |
| ASBR-PE1 | GE1/0/1 | 192.168.1.1/24 | | Loop2 | 22.22.22.22/32 |
| | GE1/0/2 | 192.168.2.1/24 | PE 2 | GE1/0/1 | 192.168.3.1/24 |
| | Loop1 | 1.1.1.2/32 | | GE1/0/2 | 10.11.2.1/24 |
| | Loop2 | 11.11.11.11/32 | | Loop1 | 1.1.1.4/32 |
| CE a1 | GE1/0/1 | 10.11.3.1/24 | CE a2 | GE1/0/1 | 10.11.2.2/24 |
| | GE1/0/2 | 10.11.1.2/24 | | GE1/0/2 | 10.11.4.1/24 |
| | Loop0 | 2.2.2.2/32 | | | |

5.2 配置思路

- 为了实现上述组网需求，需要在所有 AS 内统一建立一个 MDT 模式 MVPN 实例。
- 为了使公网 PIM-SM 域之间组播源信息的共享，需要在各公网 PIM-SM 域的 RP 之间建立 MSDP 对等体。

5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 配置各设备接口 IP 地址

按图 3 配置各设备上的接口 IP 地址和子网掩码。

```
<CEa1> system-view
[CEa1] interface gigabitethernet 1/0/1
[CEa1-GigabitEthernet1/0/1] ip address 10.11.3.1 24
[CEa1-GigabitEthernet1/0/1] quit
```



```

[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface gigabitethernet 1/0/2
[CEa1-GigabitEthernet1/0/1] ip address 10.11.1.2 24
[CEa1-GigabitEthernet1/0/1] quit

```

PE 1、ASBR-PE 1、ASBR-PE 2、PE 2 和 CE a2 的配置与 CE a1 相似，配置过程略。

5.4.2 配置路由和 OptionC 方式的跨域 MPLS L3VPN

配置路由协议及 OptionC 方式的跨域 MPLS L3VPN，实现两地间单播路由信息互通。具体配置请参见《H3C MSR 系列路由器 配置指导(V7)》中的“MPLS 配置指导/MPLS L3VPN”。

5.4.3 配置组播路由相关功能及 MDT 模式 MVPN

- (1) 在各 AS 的公网实例中使能 IP 组播路由、公网接口上配置 PIM-SM 功能（包括 LoopBack 接口），并将各 AS 配置为独立的 PIM-SM 域

在 PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```

<PE1> system-view
[PE1] multicast routing
[PE1-mrib] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] pim sm
[PE1-GigabitEthernet1/0/1] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit

```

在 ASBR-PE 1 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 2 接口指定为 AS 100 公网的 C-BSR 和 C-RP，其中 C-RP 服务于该公网实例中所有组播组。。

使能 IP 组播路由，及配置 PIM-SM。

```

<ASBR-PE1> system-view
[ASBR-PE1] multicast routing
[ASBR-PE1-mrib] quit
[ASBR-PE1] interface gigabitethernet 1/0/1
[ASBR-PE1-GigabitEthernet1/0/1] pim sm
[ASBR-PE1-GigabitEthernet1/0/1] quit
[ASBR-PE1] interface gigabitethernet 1/0/2
[ASBR-PE1-GigabitEthernet1/0/2] pim sm
[ASBR-PE1-GigabitEthernet1/0/2] quit
[ASBR-PE1] interface loopback 1
[ASBR-PE1-LoopBack1] pim sm
[ASBR-PE1-LoopBack1] quit
[ASBR-PE1] interface loopback 2
[ASBR-PE1-LoopBack2] pim sm
[ASBR-PE1-LoopBack2] quit
[ASBR-PE1] pim
[ASBR-PE1-pim] c-bsr 11.11.11.11

```

```
[ASBR-PE1-pim] c-rp 11.11.11.11
```

```
[ASBR-PE1-pim] quit
```

在 ASBR-PE 1 上配置 BSR 的服务边界，将 AS 100 配置为独立的 PIM-SM 域。

```
[ASBR-PE1] interface gigabitethernet 1/0/2
```

```
[ASBR-PE1-GigabitEthernet1/0/2] pim bsr-boundary
```

```
[ASBR-PE1-GigabitEthernet1/0/2] quit
```

在 PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM。

```
<PE2> system-view
```

```
[PE2] multicast routing
```

```
[PE2-mrib] quit
```

```
[PE2] interface gigabitethernet 1/0/1
```

```
[PE2-GigabitEthernet1/0/1] pim sm
```

```
[PE2-GigabitEthernet1/0/1] quit
```

```
[PE2] interface loopback 1
```

```
[PE2-LoopBack1] pim sm
```

```
[PE2-LoopBack1] quit
```

在 ASBR-PE 2 上使能 IP 组播路由，在公网接口上配置 PIM-SM，并将 LoopBack 2 接口指定为 AS 200 公网的 C-BSR 和 C-RP，其中 C-RP 服务于该公网实例中所有组播组。。

```
<ASBR-PE2> system-view
```

```
[ASBR-PE2] multicast routing
```

```
[ASBR-PE2-mrib] quit
```

```
[ASBR-PE2] interface gigabitethernet 1/0/1
```

```
[ASBR-PE2-GigabitEthernet1/0/1] pim sm
```

```
[ASBR-PE2-GigabitEthernet1/0/1] quit
```

```
[ASBR-PE2] interface gigabitethernet 1/0/2
```

```
[ASBR-PE2-GigabitEthernet1/0/2] pim sm
```

```
[ASBR-PE2-GigabitEthernet1/0/2] quit
```

```
[ASBR-PE2] interface loopback 1
```

```
[ASBR-PE2-LoopBack1] pim sm
```

```
[ASBR-PE2-LoopBack1] quit
```

```
[ASBR-PE2] interface loopback 2
```

```
[ASBR-PE2-LoopBack2] pim sm
```

```
[ASBR-PE2-LoopBack2] quit
```

```
[ASBR-PE2] pim
```

```
[ASBR-PE2-pim] c-bsr 22.22.22.22
```

```
[ASBR-PE2-pim] c-rp 22.22.22.22
```

```
[ASBR-PE2-pim] quit
```

在 ASBR-PE 2 上配置 BSR 的服务边界，将 AS 200 配置为独立的 PIM-SM 域。

```
[ASBR-PE2] interface gigabitethernet 1/0/1
```

```
[ASBR-PE2-GigabitEthernet1/0/1] pim bsr-boundary
```

```
[ASBR-PE2-GigabitEthernet1/0/1] quit
```

- (2) 在各公网 PIM-SM 域的 RP 之间建立 MSDP 对等体，从而实现各 AS 公网 PIM-SM 域之间组播源信息的共享

在 ASBR-PE 1 上配置 MSDP 对等体。

```
[ASBR-PE1] msdp
```

```
[ASBR-PE1-msdp] encap-data-enable
```

```
[ASBR-PE1-msdp] peer 192.168.2.2 connect-interface gigabitethernet 1/0/2
```

在 ASBR-PE 2 上配置 MSDP 对等体。

```
[ASBR-PE2] msdp
[ASBR-PE2-msdp] encap-data-enable
[ASBR-PE2-msdp] peer 192.168.2.1 connect-interface gigabitethernet 1/0/1
```

- (3) 在 VPN 私网实例中使能 IP 组播路由、私网接口上配置 PIM-SM 功能，并在连接有接收者的 CE 上配置 IGMP



说明

对于同一个 VPN，不同 AS 的 PE 上为该 VPN 实例配置的 VPN Target 需要匹配。

在 CE a1 上使能 IP 组播路由，在各接口上配置 PIM-SM，并将 LoopBack 0 接口指定为私网的 C-BSR 和 C-RP，其中 C-RP 服务于 Customer A 实例中所有组播组。

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
[CEa1] interface gigabitethernet 1/0/2
[CEa1-GigabitEthernet1/0/2] pim sm
[CEa1-GigabitEthernet1/0/2] quit
[CEa1] interface gigabitethernet 1/0/2
[CEa1-GigabitEthernet1/0/2] pim sm
[CEa1-GigabitEthernet1/0/2] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

在配置 CE a2 上使能 IP 组播路由，在连接有接收者的接口上使能 IGMP，其余各接口上配置 PIM-SM。

```
<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
[CEa2] interface gigabitethernet 1/0/1
[CEa2-GigabitEthernet1/0/1] pim sm
[CEa2-GigabitEthernet1/0/1] quit
[CEa2] interface gigabitethernet 1/0/2
[CEa2-GigabitEthernet1/0/2] igmp enable
[CEa2-GigabitEthernet1/0/2] quit
```

在配置 PE 1 上配置 VPN 实例 Customer A，将接口 GigabitEthernet1/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```
[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 100:1
[PE1-vpn-instance-customerA] vpn-target 100:1
[PE1-vpn-instance-customerA] quit
```

```

[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] ip binding vpn-instance customerA
[PE1-GigabitEthernet1/0/2] quit
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] pim sm
[PE1-GigabitEthernet1/0/2] quit

```

在 PE 2 上配置 VPN 实例 Customer A，将接口 GigabitEthernet1/0/2 与该实例其进行关联，并使能该实例中的 IP 组播路由及在关联接口上配置 PIM-SM。

```

[PE2] ip vpn-instance customerA
[PE2-vpn-instance-customerA] route-distinguisher 200:1
[PE2-vpn-instance-customerA] vpn-target 100:1
[PE2-vpn-instance] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] ip binding vpn-instance customerA
[PE2-GigabitEthernet1/0/2] quit
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] pim sm
[PE2-GigabitEthernet1/0/2] quit

```

- (4) 在所有 AS 内统一建立一个 MVPN，并指定 Default-Group、MVPN 源接口和 Data-Group 范围

在 PE 1 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```

[PE1] multicast-vpn vpn-instance customerA mode mdt
[PE1-mvpn-customerA] address-family ipv4
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE1-mvpn-customerA] quit

```

在 PE 2 上创建 MDT 模式 MVPN 实例 customerA，进入 MVPN IPv4 地址族视图并指定 Default-Group、MVPN 源接口和 Data-Group 范围。

```

[PE2] multicast-vpn vpn-instance customerA mode mdt
[PE2-mvpn-customerA] address-family ipv4
[PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE2-mvpn-customerA-ipv4] source loopback 1
[PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE2-mvpn-customerA] quit

```

5.5 验证配置

按照如上配置后，通过在 PE 及 ASBR-PE 设备上执行 `display pim routing-table` 命令，可以检查公网 Default-MDT 建立情况，以 ASBR-PE 1 设备为例：

```

[ASBR-PE1] display pim routing-table
Total 1 (*, G) entry; 2 (S, G) entry

(*, 239.1.1.1)
  RP: 3.3.3.3 (local)
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 02:54:43
  Upstream interface: Register
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: GigabitEthernet1/0/1
      Protocol: pim-sm, UpTime: 02:54:43, Expires: -

(1.1.1.1, 239.1.1.1)
  RP: 3.3.3.3 (local)
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 01:57:13
  Upstream interface: GigabitEthernet1/0/1
    Upstream neighbor: 192.168.1.2
    RPF prime neighbor: 192.168.1.2
  Downstream interface(s) information: None

(1.1.1.4, 239.1.1.1)
  RP: 3.3.3.3 (local)
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 01:57:13
  Upstream interface: GigabitEthernet1/0/2
    Upstream neighbor: 192.168.2.2
    RPF prime neighbor: 192.168.2.2
  Downstream interface(s) information: None

```

由此可见，公网 ASBR-PE 1 设备上已建立 RPT (*, 239.1.1.1) 和两棵相互独立的 SPT 树，这三棵树共同组成了该公网 MDT 模式 MVPN 实例上的 Default-MDT。

5.6 配置文件

- PE 1:


```

#
ip vpn-instance customerA
  route-distinguisher 100:1
  vpn-target 100:1 import-extcommunity
  vpn-target 100:1 export-extcommunity
#
interface LoopBack1
  ip address 1.1.1.1 255.255.255.255
  pim sm
#

```

```

interface GigabitEthernet1/0/1
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/2
 ip binding vpn-instance customerA
 ip address 10.11.1.1 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
 source LoopBack1
 default-group 239.1.1.1
 data-group 225.1.1.0 255.255.255.240
#

```

- **PE 2:**

```

#
ip vpn-instance customerA
 route-distinguisher 200:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
interface LoopBack1
 ip address 1.1.1.4 255.255.255.255
 pim sm
#
interface GigabitEthernet1/0/1
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/2
 ip binding vpn-instance customerA
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
 source LoopBack1
 default-group 239.1.1.1
 data-group 225.1.1.0 255.255.255.240
#

```

- ```

#
• ASBR-PE 1:
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 11.11.11.11 255.255.255.255
 pim sm
#
interface GigabitEthernet1/0/1
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/2
 ip address 192.168.2.1 255.255.255.0
 pim sm
 pim bsr-boundary
#
multicast routing
#
pim
 c-bsr 11.11.11.11
 c-rp 11.11.11.11
#
msdp
 encap-data-enable
 peer 192.168.2.2 connect-interface GigabitEthernet1/0/2
#

```
- ```

#
• ASBR-PE 2:
#
interface LoopBack1
  ip address 1.1.1.3 255.255.255.255
  pim sm
#
interface LoopBack2
  ip address 22.22.22.22 255.255.255.255
  pim sm
#
interface GigabitEthernet1/0/1
  ip address 192.168.2.2 255.255.255.0
  pim sm
  pim bsr-boundary
#
interface GigabitEthernet1/0/2
  ip address 192.168.3.2 255.255.255.0
  pim sm

```

```

#
multicast routing
#
pim
  c-bsr 22.22.22.22
  c-rp 22.22.22.22
#
msdp
  encap-data-enable
  peer 192.168.2.1 connect-interface GigabitEthernet1/0/1
#
• CE a1:
#
interface LoopBack0
  ip address 2.2.2.2 255.255.255.255
  pim sm
#
interface GigabitEthernet1/0/1
  ip address 10.11.3.1 255.255.255.0
  pim sm
#
interface GigabitEthernet1/0/2
  ip address 10.11.1.2 255.255.255.0
  pim sm
#
multicast routing
#
pim
  c-bsr 2.2.2.2
  c-rp 2.2.2.2
#
• CE a2:
#
interface GigabitEthernet1/0/1
  ip address 10.11.2.2 255.255.255.0
  pim sm
#
interface GigabitEthernet1/0/2
  ip address 10.11.4.1 255.255.255.0
  igmp enable
#
multicast routing
#

```

6 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“IP 组播配置指导”

- 《H3C MSR 系列路由器 命令参考(V7)》中的“IP 组播命令参考”

H3C MSR 系列路由器

MPLS 基础配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

| | |
|-----------------------------|----|
| 1 简介..... | 1 |
| 2 配置前提..... | 1 |
| 3 静态 LSP 配置举例..... | 1 |
| 3.1 组网需求..... | 1 |
| 3.2 配置思路..... | 1 |
| 3.3 使用版本..... | 2 |
| 3.4 配置注意事项..... | 2 |
| 3.5 配置步骤..... | 2 |
| 3.6 验证配置..... | 4 |
| 3.7 配置文件..... | 4 |
| 4 利用 LDP 动态建立 LSP 配置举例..... | 6 |
| 4.1 组网需求..... | 6 |
| 4.2 配置思路..... | 6 |
| 4.3 使用版本..... | 7 |
| 4.4 配置步骤..... | 7 |
| 4.5 验证配置..... | 12 |
| 4.6 配置文件..... | 14 |
| 5 相关资料..... | 18 |

1 简介

本文档介绍通过静态方式和 LDP（Label Distribution Protocol，标签分发协议）方式建立 LSP 的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

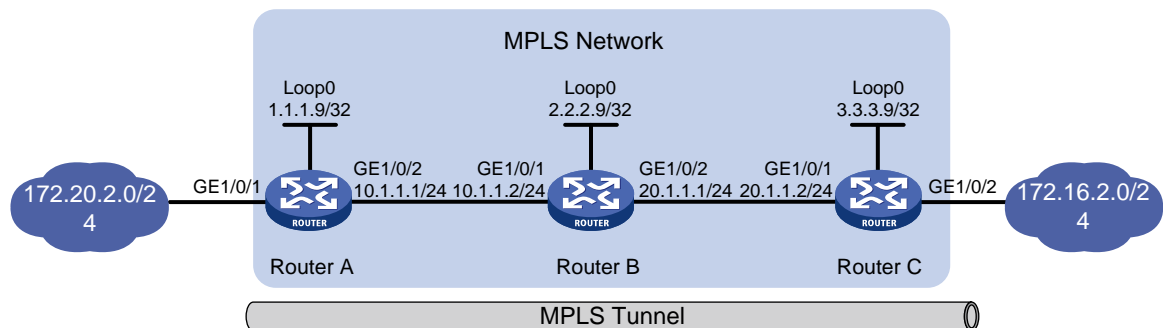
本文档假设您已了解静态 MPLS 和 LDP 特性。

3 静态 LSP 配置举例

3.1 组网需求

如图 1 所示，运营商网络运行 MPLS，Router A 和 Router C 作为 MPLS 的边缘设备，现要求在 172.20.2.0/24 网段和 172.16.2.0/24 网段间，通过配置静态 LSP 隧道，使这两个网段中互访的报文能够通过 LSP 在 MPLS 网络中进行传输。

图1 配置静态 LSP 组网图



3.2 配置思路

- 为了使设备能够按正确的路径转发 MPLS 报文，需要在手工配置 LSP 的标签时，确保上游 LSR 出标签的值就是下游 LSR 入标签的值。
- LSP 是一种单向通道，为了实现数据的双向正常传输，需要在数据传输的两个方向上分别配置一条静态 LSP，并指定各自的入节点、中间节点和出节点。

- 在静态 LSP 环境中，只需要 Ingress 节点上存在到达 FEC 目的地址的路由即可，Transit 和 Egress 节点上无需存在到达 FEC 目的地址的路由，因此本例中使用简单的静态路由即可完成路由配置。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 通过静态路由配置路由信息时，如果静态路由指定的是出接口，则静态 LSP 必须指定相同的出接口；如果静态路由指定的是下一跳，则静态 LSP 必须指定相同的下一跳。
- 配置 Ingress 和 Transit 时，本地的公网地址不能被指定为下一跳。
- 由于 MPLS 功能会在原有报文上封装一层或多层标签，因此建议用户在使能某接口的 MPLS 功能后，将该接口的 **jumboframe** 帧功能开启，并根据实际应用和标签嵌套层数配置相应的帧长，避免某些报文因超长而被丢弃。

3.5 配置步骤

- (1) 配置各接口的 IP 地址

按照图 1 配置各接口的 IP 地址和掩码，包括 LoopBack 接口，具体配置过程略。

- (2) 配置静态路由，使两条 LSP 的 Ingress 节点上存在到达 FEC 目的地址的路由。

配置 Router A。

```
<RouterA> system-view
[RouterA] ip route-static 172.16.2.0 24 10.1.1.2
```

配置 Router C。

```
<RouterC> system-view
[RouterC] ip route-static 172.20.2.0 24 20.1.1.1
```

配置完成后，在 Ingress 设备上执行 **display ip routing-table** 命令，可以看到静态路由已生效。以 Router A 为例：

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

```
Destinations : 18          Routes : 18
```

| Destination/Mask | Proto | Pre | Cost | NextHop | Interface |
|------------------|--------|-----|------|-----------|-----------|
| 0.0.0.0/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 1.1.1.9/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 10.1.1.0/24 | Direct | 0 | 0 | 10.1.1.1 | GE1/0/2 |
| 10.1.1.0/32 | Direct | 0 | 0 | 10.1.1.1 | GE1/0/2 |
| 10.1.1.1/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 10.1.1.255/32 | Direct | 0 | 0 | 10.1.1.1 | GE1/0/2 |
| 127.0.0.0/8 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 127.0.0.0/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 127.0.0.1/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |

```

127.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0
172.16.2.0/24 Static 60 0 10.1.1.2 GE1/0/2
172.20.2.0/24 Direct 0 0 172.20.2.1 GE1/0/1
172.20.2.0/32 Direct 0 0 172.20.2.1 GE1/0/1
172.20.2.1/32 Direct 0 0 127.0.0.1 InLoop0
172.20.2.255/32 Direct 0 0 172.20.2.1 GE1/0/1
224.0.0.0/4 Direct 0 0 0.0.0.0 NULL0
224.0.0.0/24 Direct 0 0 0.0.0.0 NULL0
255.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0

```

(3) 使能 MPLS 功能

配置 Router A。

```

[RouterA] mpls lsr-id 1.1.1.9
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] mpls enable
[RouterA-GigabitEthernet1/0/2] quit

```

配置 Router B。

```

[RouterB] mpls lsr-id 2.2.2.9
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] mpls enable
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] mpls enable
[RouterB-GigabitEthernet1/0/2] quit

```

配置 Router C。

```

[RouterC] mpls lsr-id 3.3.3.9
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] mpls enable
[RouterC-GigabitEthernet1/0/1] quit

```

(4) 创建从 Router A 到 Router C 的静态 LSP

为 Ingress 节点 Router A 配置一条到目的地址 172.16.2.1/24 的静态 LSP，LSP 的名称为 AtoC，下一跳地址为 10.1.1.2，出标签为 30。

```

[RouterA] static-lsp ingress AtoC destination 172.16.2.1 24 nexthop 10.1.1.2 out-label 30

```

为 Transit 节点 Router B 配置一条名为 AtoC 的静态 LSP，入标签为 30，下一跳地址为 20.1.1.2，出标签为 50。

```

[RouterB] static-lsp transit AtoC in-label 30 nexthop 20.1.1.2 out-label 50

```

为 Egress 节点 Router C 上配置一条名为 AtoC 的静态 LSP，入标签为 50。

```

[RouterC] static-lsp egress AtoC in-label 50

```

(5) 创建从 Router C 到 Router A 的静态 LSP

为 Ingress 节点 Router C 配置一条到目的地址 172.20.2.1/24 的静态 LSP，LSP 的名称为 CtoA，下一跳地址为 20.1.1.1，出标签为 40。

```

[RouterC] static-lsp ingress CtoA destination 172.20.2.1 24 nexthop 20.1.1.1 out-label 40

```

为 Transit 节点 Router B 配置一条名为 CtoA 的静态 LSP，入标签为 40，下一跳地址为 10.1.1.1，出标签为 70。

```
[RouterB] static-lsp transit CtoA in-label 40 nexthop 10.1.1.1 out-label 70
# 为 Egress 节点 Router A 配置一条名为 CtoA 的静态 LSP，入标签为 70。
[RouterA] static-lsp egress CtoA in-label 70
```

3.6 验证配置

配置完成后，可以在各路由器上通过 **display mpls static-lsp** 命令查看静态 LSP 的信息。
以 Router A 的显示信息为例：

```
[RouterA] display mpls static-lsp
Total: 2
Name          FEC                In/Out Label Nexthop/Out Interface  State
AtoC          172.16.2.0/24      NULL/30      10.1.1.2
CtoA          -/-                70/NULL      -           Up
```

在 Router A 上检测 Router A 到 Router C 静态 LSP 的可达性。

```
[RouterA] ping mpls -a 172.20.2.1 ipv4 172.16.2.0 24
MPLS ping FEC 172.16.2.0/24 with 100 bytes of data:
100 bytes from 20.1.1.2: Sequence=1 time=3 ms
100 bytes from 20.1.1.2: Sequence=2 time=2 ms
100 bytes from 20.1.1.2: Sequence=3 time=2 ms
100 bytes from 20.1.1.2: Sequence=4 time=2 ms
100 bytes from 20.1.1.2: Sequence=5 time=27 ms

--- Ping statistics for FEC 172.16.2.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/7/27 ms
```

在 Router C 上检测 Router C 到 Router A 静态 LSP 的可达性。

```
[RouterC] ping mpls -a 172.16.2.1 ipv4 172.20.2.0 24
MPLS ping FEC 172.20.2.0/24 with 100 bytes of data:
100 bytes from 10.1.1.1: Sequence=1 time=3 ms
100 bytes from 10.1.1.1: Sequence=2 time=2 ms
100 bytes from 10.1.1.1: Sequence=3 time=2 ms
100 bytes from 10.1.1.1: Sequence=4 time=2 ms
100 bytes from 10.1.1.1: Sequence=5 time=27 ms

--- Ping statistics for FEC 172.20.2.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/7/27 ms
```

3.7 配置文件

- Router A:

```
#
mpls lsr-id 1.1.1.9
#
interface LoopBack0
ip address 1.1.1.9 255.255.255.255
```

```

#
interface GigabitEthernet1/0/1
  port link-mode route
ip address 172.20.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
ip address 10.1.1.1 255.255.255.0
  mpls enable
#
  ip route-static 172.16.2.0 24 10.1.1.2
#
  static-lsp ingress AtoC destination 172.16.2.0 24 nexthop 10.1.1.2 out-label 30
  static-lsp egress CtoA in-label 70
#

```

- **Router B:**

```

#
  mpls lsr-id 2.2.2.9
#
interface LoopBack0
  ip address 2.2.2.9 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
ip address 10.1.1.2 255.255.255.0
  mpls enable
#
interface GigabitEthernet1/0/2
  port link-mode route
ip address 20.1.1.1 255.255.255.0
  mpls enable
#
  static-lsp transit AtoC in-label 30 nexthop 20.1.1.2 out-label 50
  static-lsp transit CtoA in-label 40 nexthop 10.1.1.1 out-label 70
#

```

- **Router C:**

```

#
  mpls lsr-id 3.3.3.9
#
interface LoopBack0
  ip address 3.3.3.9 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
ip address 20.1.1.2 255.255.255.0
  mpls enable
#

```



```

interface GigabitEthernet1/0/2
  port link-mode route
  ip address 172.16.2.1 255.255.255.0
#
  ip route-static 172.20.2.1 255.255.255.0 20.1.1.1
#
  static-lsp ingress CtoA destination 172.20.2.0 24 nexthop 20.1.1.1 out-label 40
  static-lsp egress AtoC in-label 50
#

```

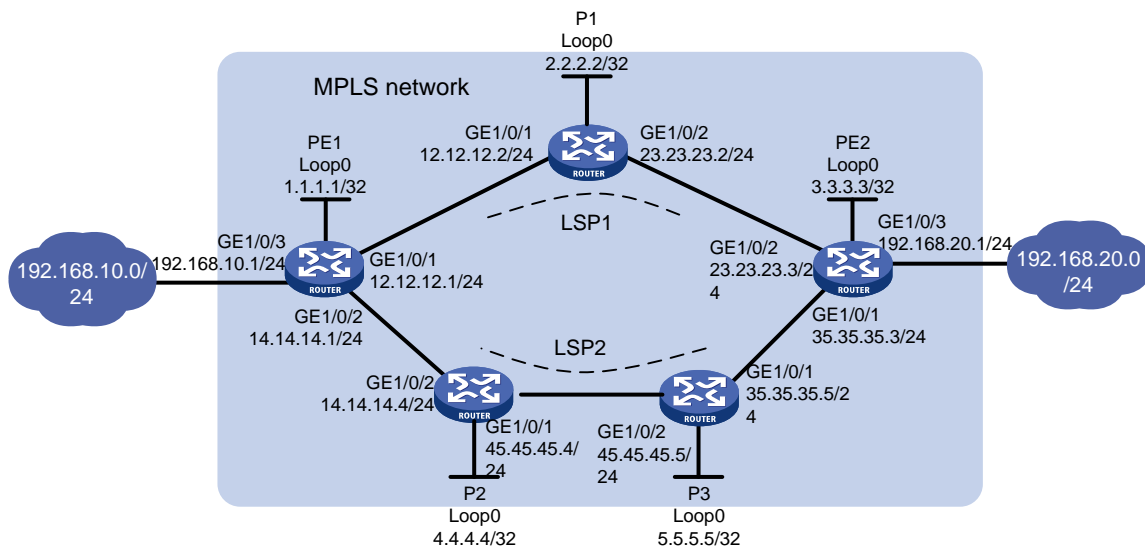
4 利用 LDP 动态建立 LSP 配置举例

4.1 组网需求

如图 2 所示，在运营商网络的 MPLS 区域中，PE 1 和 PE 2 之间有两条路由可达，现要求：

- 在 MPLS 网络中配置 LDP 协议，动态建立 LSP，使 192.168.10.0/24 网段与 192.168.20.0/24 网段之间转发的报文沿建立的 LSP 转发。
- 缺省情况下，报文通过 LSP 1 路径传输；当 P 1 故障时，报文通过 LSP 2 路径传输。
- 所有设备上只允许目的地址为 1.1.1.1/32、2.2.2.2/32、3.3.3.3/32、4.4.4.4/32、5.5.5.5/32、192.168.10.0/24 和 192.168.20.0/24 的路由表项触发 LDP 建立 LSP，其他路由表项不能触发 LDP 建立 LSP，以避免建立的 LSP 数量过多，影响设备性能。

图2 动态 LSP 配置组网图



4.2 配置思路

- 为了通过 LDP 动态创建 LSP，需要配置路由协议，使得各设备间路由可达，本例中使用 OSPF 路由协议。

- 为了实现缺省情况下报文通过 LSP 1 路径传输，并且当 P 1 故障时，报文通过 LSP 2 路径传输，需要配置 192.168.10.0/24 和 192.168.20.0/24 之间的主路由为 LSP 1，备份路由为 LSP 2（本例通过配置 OSPF 路由协议来实现：使能 OSPF 协议后，会自动计算出 LSP 1 路径的开销小于 LSP 2，所以走 LSP 1）。
- 为了只允许目的地址为 1.1.1.1/32、2.2.2.2/32、3.3.3.3/32、4.4.4.4/32、5.5.5.5/32、192.168.10.0/24 和 192.168.20.0/24 的路由表项触发 LDP 建立 LSP，需要配置 LSP 触发策略。

4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.4 配置步骤

(1) 配置各接口的 IP 地址

按照图 2 配置各接口的 IP 地址和掩码，包括 LoopBack 接口，具体配置过程略。

(2) 配置 OSPF，以保证各路由器之间路由可达

配置 PE 1。

```
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 P 1。

```
[P1] ospf 1
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

配置 P 2。

```
[P2] ospf 1
[P2-ospf-1] area 0
[P2-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 45.45.45.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

配置 P 3。

```
[P3] ospf 1
[P3-ospf-1] area 0
```

```
[P3-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[P3-ospf-1-area-0.0.0.0] network 45.45.45.0 0.0.0.255
[P3-ospf-1-area-0.0.0.0] network 35.35.35.0 0.0.0.255
[P3-ospf-1-area-0.0.0.0] quit
[P3-ospf-1] quit
```

配置 PE 2。

```
[PE2] ospf 1
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 35.35.35.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置完成后，在各路由器上执行 **display ospf routing** 命令，可以看到相互之间都学到了对方的路由。以 PE 1 为例：

```
[PE1] display ospf routing
```

```
OSPF Process 1 with Router ID 1.1.1.1
Routing Table
```

```
Routing for network
```

| Destination | Cost | Type | NextHop | AdvRouter | Area |
|-----------------|------|---------|--------------|-----------|---------|
| 45.45.45.0/24 | 2 | Transit | 14.14.14.4 | 5.5.5.5 | 0.0.0.0 |
| 35.35.35.0/24 | 3 | Transit | 14.14.14.4 | 5.5.5.5 | 0.0.0.0 |
| 35.35.35.0/24 | 3 | Transit | 12.12.12.2 | 5.5.5.5 | 0.0.0.0 |
| 192.168.10.0/24 | 1 | Stub | 192.168.10.1 | 1.1.1.1 | 0.0.0.0 |
| 5.5.5.5/32 | 2 | Stub | 14.14.14.4 | 5.5.5.5 | 0.0.0.0 |
| 14.14.14.0/24 | 1 | Transit | 14.14.14.1 | 4.4.4.4 | 0.0.0.0 |
| 23.23.23.0/24 | 2 | Transit | 12.12.12.2 | 3.3.3.3 | 0.0.0.0 |
| 4.4.4.4/32 | 1 | Stub | 14.14.14.4 | 4.4.4.4 | 0.0.0.0 |
| 3.3.3.3/32 | 2 | Stub | 12.12.12.2 | 3.3.3.3 | 0.0.0.0 |
| 12.12.12.0/24 | 1 | Transit | 12.12.12.1 | 2.2.2.2 | 0.0.0.0 |
| 2.2.2.2/32 | 1 | Stub | 12.12.12.2 | 2.2.2.2 | 0.0.0.0 |
| 1.1.1.1/32 | 0 | Stub | 1.1.1.1 | 1.1.1.1 | 0.0.0.0 |
| 192.168.20.0/24 | 3 | Stub | 12.12.12.2 | 3.3.3.3 | 0.0.0.0 |

```
Total nets: 13
```

```
Intra area: 13 Inter area: 0 ASE: 0 NSSA: 0
```

PE 1 和 P 1、P 2、P 3 和 PE 2 之间应建立起 OSPF 邻居关系，执行 **display ospf peer verbose** 命令可以看到邻居达到 FULL 状态。以 PE 1 为例：

```
[PE1] display ospf peer verbose
```

```
OSPF Process 1 with Router ID 1.1.1.1
Neighbors
```

```
Area 0.0.0.0 interface 14.14.14.1(GigabitEthernet1/0/2)'s neighbors
Router ID: 4.4.4.4 Address: 14.14.14.4 GR state: Normal
```

```
State: Full Mode: Nbr is master Priority: 1
DR: 14.14.14.4 BDR: 14.14.14.1 MTU: 0
Options is 0x42 (-|O|-|-|-|E|-)
Dead timer due in 40 sec
Neighbor is up for 00:03:30
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled
```

Neighbors

```
Area 0.0.0.0 interface 12.12.12.1(GigabitEthernet1/0/1)'s neighbors
Router ID: 2.2.2.2 Address: 12.12.12.2 GR state: Normal
State: Full Mode: Nbr is master Priority: 1
DR: 12.12.12.2 BDR: 12.12.12.1 MTU: 0
Options is 0x42 (-|O|-|-|-|E|-)
Dead timer due in 36 sec
Neighbor is up for 00:03:24
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled
```

(3) 配置 MPLS 基本能力，并使能 LDP

配置 PE 1。

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] mpls enable
[PE1-GigabitEthernet1/0/1] mpls ldp enable
[PE1-GigabitEthernet1/0/1] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] mpls enable
[PE1-GigabitEthernet1/0/2] mpls ldp enable
[PE1-GigabitEthernet1/0/2] quit
```

配置 P 1。

```
[P1] mpls lsr-id 2.2.2.2
[P1] mpls ldp
[P1-ldp] quit
[P1] interface gigabitethernet 1/0/1
[P1-GigabitEthernet1/0/1] mpls enable
[P1-GigabitEthernet1/0/1] mpls ldp enable
[P1-GigabitEthernet1/0/1] quit
[P1] interface gigabitethernet 1/0/2
[P1-GigabitEthernet1/0/2] mpls enable
[P1-GigabitEthernet1/0/2] mpls ldp enable
[P1-GigabitEthernet1/0/2] quit
```

配置 P 2。

```

[P2] mpls lsr-id 4.4.4.4
[P2] mpls ldp
[P2-ldp] quit
[P2] interface gigabitethernet 1/0/1
[P2-GigabitEthernet1/0/1] mpls enable
[P2-GigabitEthernet1/0/1] mpls ldp enable
[P2-GigabitEthernet1/0/1] quit
[P2] interface gigabitethernet 1/0/2
[P2-GigabitEthernet1/0/2] mpls enable
[P2-GigabitEthernet1/0/2] mpls ldp enable
[P2-GigabitEthernet1/0/2] quit

```

配置 P 3。

```

[P3] mpls lsr-id 5.5.5.5
[P3] mpls ldp
[P3-ldp] quit
[P3] interface gigabitethernet 1/0/1
[P3-GigabitEthernet1/0/1] mpls enable
[P3-GigabitEthernet1/0/1] mpls ldp enable
[P3-GigabitEthernet1/0/1] quit
[P3] interface gigabitethernet 1/0/2
[P3-GigabitEthernet1/0/2] mpls enable
[P3-GigabitEthernet1/0/2] mpls ldp enable
[P3-GigabitEthernet1/0/2] quit

```

配置 PE 2。

```

[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] mpls enable
[PE2-GigabitEthernet1/0/1] mpls ldp enable
[PE2-GigabitEthernet1/0/1] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] mpls enable
[PE2-GigabitEthernet1/0/2] mpls ldp enable
[PE2-GigabitEthernet1/0/2] quit

```

完成上述配置后，PE 1 和 P 1、P 2，P 2、P 3 和 PE 2 之间的本地 LDP 会话建立成功。

在各设备上执行 **display mpls ldp peer** 命令，可以看到 LDP 的对等体情况。以 PE 1 为例：

```

[PE1] display mpls ldp peer
Total number of peers: 2
Peer LDP ID          State          Role    GR    MD5    KA Sent/Rcvd
2.2.2.2:0            Operational    Passive Off   Off   55/55
4.4.4.4:0            Operational    Passive Off   Off   6/6

```

- (4) 配置 LSP 的触发策略，为目的地址为 1.1.1.1/32、2.2.2.2/32、3.3.3.3/32、4.4.4.4/32、5.5.5.5/32、192.168.10.0/24 和 192.168.20.0/24 的路由表项建立 LSP

在 PE 1 上创建 IP 地址前缀列表 PE1，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[PE1] ip prefix-list PE1 index 10 permit 1.1.1.1 32
[PE1] ip prefix-list PE1 index 20 permit 2.2.2.2 32
[PE1] ip prefix-list PE1 index 30 permit 3.3.3.3 32
[PE1] ip prefix-list PE1 index 40 permit 4.4.4.4 32
[PE1] ip prefix-list PE1 index 50 permit 5.5.5.5 32
[PE1] ip prefix-list PE1 index 60 permit 192.168.10.0 24
[PE1] ip prefix-list PE1 index 70 permit 192.168.20.0 24
[PE1] mpls ldp
[PE1-ldp] lsp-trigger prefix-list PE1
[PE1-ldp] quit
```

在 P 1 上创建 IP 地址前缀列表 P1，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P1] ip prefix-list P1 index 10 permit 1.1.1.1 32
[P1] ip prefix-list P1 index 20 permit 2.2.2.2 32
[P1] ip prefix-list P1 index 30 permit 3.3.3.3 32
[P1] ip prefix-list P1 index 40 permit 4.4.4.4 32
[P1] ip prefix-list P1 index 50 permit 5.5.5.5 32
[P1] ip prefix-list P1 index 60 permit 192.168.10.0 24
[P1] ip prefix-list P1 index 70 permit 192.168.20.0 24
[P1] mpls ldp
[P1-ldp] lsp-trigger prefix-list P1
[P1-ldp] quit
```

在 P 2 上创建 IP 地址前缀列表 P2，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P2] ip prefix-list P2 index 10 permit 1.1.1.1 32
[P2] ip prefix-list P2 index 20 permit 2.2.2.2 32
[P2] ip prefix-list P2 index 30 permit 3.3.3.3 32
[P2] ip prefix-list P2 index 40 permit 4.4.4.4 32
[P2] ip prefix-list P2 index 50 permit 5.5.5.5 32
[P2] ip prefix-list P2 index 60 permit 192.168.10.0 24
[P2] ip prefix-list P2 index 70 permit 192.168.20.0 24
[P2] mpls ldp
[P2-ldp] lsp-trigger prefix-list P2
[P2-ldp] quit
```

在 P 3 上创建 IP 地址前缀列表 P3，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P3] ip prefix-list P3 index 10 permit 1.1.1.1 32
[P3] ip prefix-list P3 index 20 permit 2.2.2.2 32
[P3] ip prefix-list P3 index 30 permit 3.3.3.3 32
[P3] ip prefix-list P3 index 40 permit 4.4.4.4 32
[P3] ip prefix-list P3 index 50 permit 5.5.5.5 32
[P3] ip prefix-list P3 index 60 permit 192.168.10.0 24
[P3] ip prefix-list P3 index 70 permit 192.168.20.0 24
[P3] mpls ldp
```

```
[P3-ldp] lsp-trigger prefix-list P3
[P3-ldp] quit
```

在 PE 2 上创建 IP 地址前缀列表 PE 2，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[PE2] ip prefix-list PE2 index 10 permit 1.1.1.1 32
[PE2] ip prefix-list PE2 index 20 permit 2.2.2.2 32
[PE2] ip prefix-list PE2 index 30 permit 3.3.3.3 32
[PE2] ip prefix-list PE2 index 40 permit 4.4.4.4 32
[PE2] ip prefix-list PE2 index 50 permit 5.5.5.5 32
[PE2] ip prefix-list PE2 index 60 permit 192.168.10.0 24
[PE2] ip prefix-list PE2 index 70 permit 192.168.20.0 24
[PE2] mpls ldp
[PE2-ldp] lsp-trigger prefix-list PE2
[PE2-ldp] quit
```

4.5 验证配置

配置完成后，在 PE 1 上执行 **display mpls ldp lsp** 命令，查看 LDP LSP 的建立情况，可以看到去往 192.168.20.0/24 网段的 LSP 缺省下一跳指向 P 1。

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 7      Ingress LSPs: 5      Transit LSPs: 5      Egress LSPs: 2
```

| FEC | In/Out Label | NextHop | OutInterface |
|-----------------|--------------|------------|--------------|
| 1.1.1.1/32 | 3/- | | |
| | -/1151(L) | | |
| | -/1151(L) | | |
| 2.2.2.2/32 | -/3 | 12.12.12.2 | GE1/0/1 |
| | 1151/3 | 12.12.12.2 | GE1/0/1 |
| | -/1150(L) | | |
| 3.3.3.3/32 | -/1150 | 12.12.12.2 | GE1/0/1 |
| | 1150/1150 | 12.12.12.2 | GE1/0/1 |
| | -/1148(L) | | |
| 4.4.4.4/32 | -/1149(L) | | |
| | -/3 | 14.14.14.4 | GE1/0/2 |
| | 1149/3 | 14.14.14.4 | GE1/0/2 |
| 5.5.5.5/32 | -/1148(L) | | |
| | -/1149 | 14.14.14.4 | GE1/0/2 |
| | 1148/1149 | 14.14.14.4 | GE1/0/2 |
| 192.168.10.0/24 | 1145/- | | |
| | -/1146(L) | | |
| | -/1146(L) | | |
| 192.168.20.0/24 | -/1147 | 12.12.12.2 | GE1/0/1 |
| | 1146/1147 | 12.12.12.2 | GE1/0/1 |
| | -/1147(L) | | |

使用 MPLS ping 检测 MPLS LSP 的有效性和可达性。

```
[PE1] ping mpls -a 192.168.10.1 ipv4 192.168.20.0 24
```

```
MPLS ping FEC 192.168.20.0/24 with 100 bytes of data:
100 bytes from 23.23.23.3: Sequence=1 time=2 ms
100 bytes from 23.23.23.3: Sequence=2 time=2 ms
100 bytes from 23.23.23.3: Sequence=3 time=2 ms
100 bytes from 23.23.23.3: Sequence=4 time=2 ms
100 bytes from 23.23.23.3: Sequence=5 time=2 ms
```

```
--- Ping statistics for FEC 192.168.20.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/2/2 ms
```

当 P 1 故障时, 在 PE 1 上执行 **display mpls ldp lsp** 命令, 查看 LDP LSP 的变化, 可以看到去往 192.168.20.0/24 网段的 LSP 下一跳指向 P 2。

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
  FECs: 7      Ingress LSPs: 5      Transit LSPs: 5      Egress LSPs: 2
```

| FEC | In/Out Label | Nexthop | OutInterface |
|-----------------|----------------------------------|------------|--------------|
| 1.1.1.1/32 | 3/-
-/1150(L) | | |
| 2.2.2.2/32 | -/1149
1150/1149 | 14.14.14.4 | GE1/0/2 |
| 3.3.3.3/32 | -/1148
1147/1148 | 14.14.14.4 | GE1/0/2 |
| 4.4.4.4/32 | -/3
1149/3 | 14.14.14.4 | GE1/0/2 |
| 5.5.5.5/32 | -/1151
1148/1151 | 14.14.14.4 | GE1/0/2 |
| 192.168.10.0/24 | 1151/-
-/1146(L)
-/1146(L) | | |
| 192.168.20.0/24 | -/1147
1146/1147 | 14.14.14.4 | GE1/0/2 |
| | | 14.14.14.4 | GE1/0/2 |

使用 MPLS ping 检测 MPLS LSP 的有效性和可达性。

```
[PE1] ping mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS ping FEC 192.168.20.0/24 with 100 bytes of data:
100 bytes from 35.35.35.3: Sequence=1 time=1 ms
100 bytes from 35.35.35.3: Sequence=2 time=1 ms
100 bytes from 35.35.35.3: Sequence=3 time=1 ms
100 bytes from 35.35.35.3: Sequence=4 time=1 ms
100 bytes from 35.35.35.3: Sequence=5 time=1 ms
```

```
--- Ping statistics for FEC 192.168.20.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 1/1/1 ms
```


4.6 配置文件

- PE1:

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
#
mpls lsr-id 1.1.1.1
#
mpls ldp
 lsp-trigger prefix-list PE1
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 12.12.12.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 14.14.14.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 192.168.10.1 255.255.255.0
#
 ip prefix-list PE1 index 10 permit 1.1.1.1 32
 ip prefix-list PE1 index 20 permit 2.2.2.2 32
 ip prefix-list PE1 index 30 permit 3.3.3.3 32
 ip prefix-list PE1 index 40 permit 4.4.4.4 32
 ip prefix-list PE1 index 50 permit 5.5.5.5 32
 ip prefix-list PE1 index 60 permit 192.168.10.0 24
 ip prefix-list PE1 index 70 permit 192.168.20.0 24
```

- P1:

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
```

```

network 12.12.12.0 0.0.0.255
network 23.23.23.0 0.0.0.255
#
mpls lsr-id 2.2.2.2
#
mpls ldp
  lsp-trigger prefix-list P1
#
interface LoopBack0
  ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
ip address 12.12.12.2 255.255.255.0
  mpls enable
  mpls ldp enable
#
interface GigabitEthernet1/0/2
  port link-mode route
ip address 23.23.23.2 255.255.255.0
  mpls enable
  mpls ldp enable
#
ip prefix-list P1 index 10 permit 1.1.1.1 32
ip prefix-list P1 index 20 permit 2.2.2.2 32
ip prefix-list P1 index 30 permit 3.3.3.3 32
ip prefix-list P1 index 40 permit 4.4.4.4 32
ip prefix-list P1 index 50 permit 5.5.5.5 32
ip prefix-list P1 index 60 permit 192.168.10.0 24
ip prefix-list P1 index 70 permit 192.168.20.0 24
#

```

- **P 2:**

```

#
ospf 1
  area 0.0.0.0
    network 4.4.4.4 0.0.0.0
    network 14.14.14.0 0.0.0.255
    network 45.45.45.0 0.0.0.255
#
mpls lsr-id 4.4.4.4
#
mpls ldp
  lsp-trigger prefix-list P2
#
interface LoopBack0
  ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet1/0/1

```

```

port link-mode route
ip address 45.45.45.4 255.255.255.0
mpls enable
mpls ldp enable
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 14.14.14.4 255.255.255.0
mpls enable
mpls ldp enable
#
ip prefix-list P2 index 10 permit 1.1.1.1 32
ip prefix-list P2 index 20 permit 2.2.2.2 32
ip prefix-list P2 index 30 permit 3.3.3.3 32
ip prefix-list P2 index 40 permit 4.4.4.4 32
ip prefix-list P2 index 50 permit 5.5.5.5 32
ip prefix-list P2 index 60 permit 192.168.10.0 24
ip prefix-list P2 index 70 permit 192.168.20.0 24

```

- **P3:**

```

#
ospf 1
area 0.0.0.0
network 5.5.5.5 0.0.0.0
network 35.35.35.0 0.0.0.255
network 45.45.45.0 0.0.0.255
#
mpls lsr-id 5.5.5.5
#
mpls ldp
lsp-trigger prefix-list P3
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 35.35.35.5 255.255.255.0
mpls enable
mpls ldp enable
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 45.45.45.5 255.255.255.0
mpls enable
mpls ldp enable
#
ip prefix-list P3 index 10 permit 1.1.1.1 32

```

```

ip prefix-list P3 index 20 permit 2.2.2.2 32
ip prefix-list P3 index 30 permit 3.3.3.3 32
ip prefix-list P3 index 40 permit 4.4.4.4 32
ip prefix-list P3 index 50 permit 5.5.5.5 32
ip prefix-list P3 index 60 permit 192.168.10.0 24
ip prefix-list P3 index 70 permit 192.168.20.0 24

```

#

- **PE2:**

#

```

ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 23.23.23.0 0.0.0.255
  network 33.0.0.0 0.0.0.255
  network 192.168.20.0 0.0.0.255

```

#

```
mpls lsr-id 3.3.3.3
```

#

```

mpls ldp
 lsp-trigger prefix-list PE2

```

#

```

interface LoopBack0
 ip address 3.3.3.3 255.255.255.255

```

#

```

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 35.35.35.3 255.255.255.0
 mpls enable
 mpls ldp enable

```

#

```

interface GigabitEthernet1/0/2
 port link-mode route
 ip address 23.23.23.3 255.255.255.0
 mpls enable
 mpls ldp enable

```

#

```

interface GigabitEthernet1/0/3
 port link-mode route
 ip address 192.168.20.1 255.255.255.0

```

#

```

ip prefix-list PE2 index 10 permit 1.1.1.1 32
ip prefix-list PE2 index 20 permit 2.2.2.2 32
ip prefix-list PE2 index 30 permit 3.3.3.3 32
ip prefix-list PE2 index 40 permit 4.4.4.4 32
ip prefix-list PE2 index 50 permit 5.5.5.5 32
ip prefix-list PE2 index 60 permit 192.168.10.0 24
ip prefix-list PE2 index 70 permit 192.168.20.0 24

```

#

5 相关资料

- 《H3C MSR 系列路由器 配置指导 (V7)》中的“MPLS 配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“MPLS 命令参考”

H3C MSR 系列路由器

MPLS L3VPN 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

| | |
|-----------------|----|
| 1 简介..... | 1 |
| 2 配置前提..... | 1 |
| 3 配置举例..... | 1 |
| 3.1 组网需求..... | 1 |
| 3.2 配置思路..... | 2 |
| 3.3 使用版本..... | 2 |
| 3.4 配置注意事项..... | 2 |
| 3.5 配置步骤..... | 2 |
| 3.6 验证配置..... | 10 |
| 3.7 配置文件..... | 10 |
| 4 相关资料..... | 15 |

1 简介

本文介绍了通过 MPLS L3VPN 技术提供 VPN 服务的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

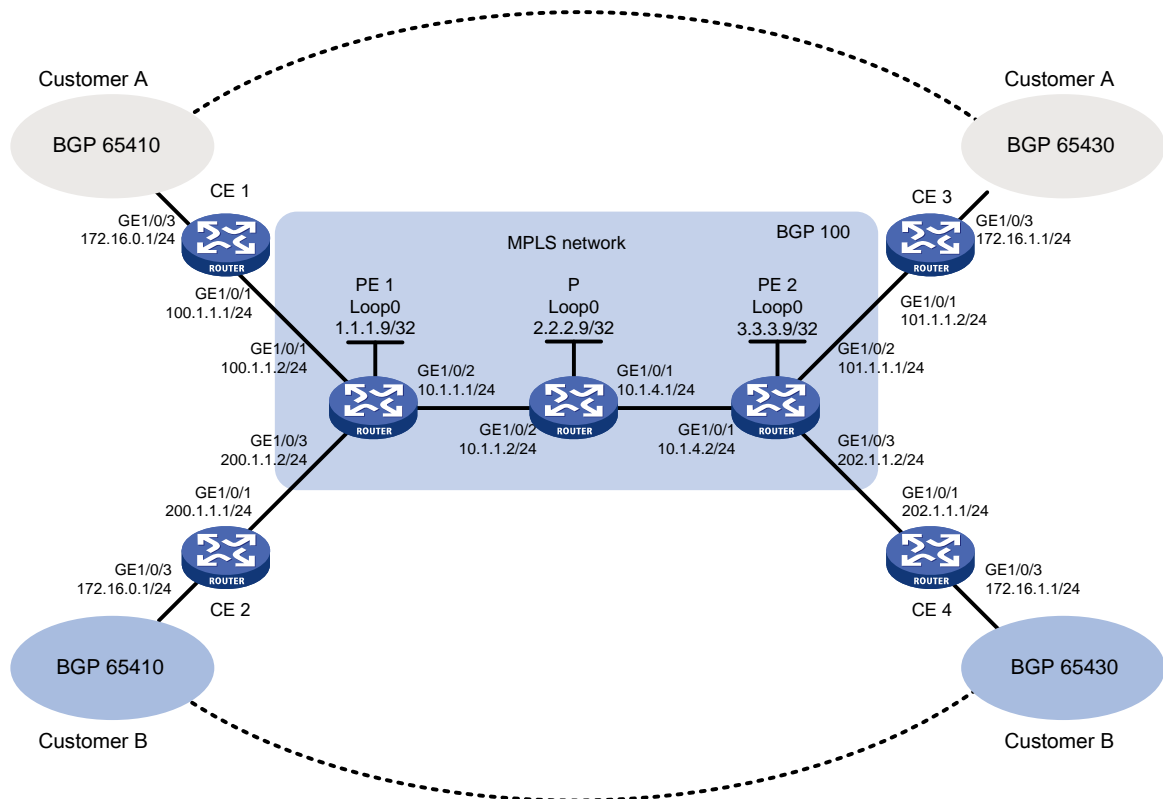
本文档假设您已了解 MPLS L3VPN 的特性。

3 配置举例

3.1 组网需求

如图 1 所示，Customer A 和 Customer B 分别有位于两地的分支机构，现要求通过 MPLS L3VPN 技术，实现用户分支机构间路由信息的正常交互，且用户数据可以通过 VPN 方式在各站点间安全传输，不会发送至私网 IP 地址相同的其它用户站点中。

图1 MPLS L3VPN 基本组网图



3.2 配置思路

- 为了使报文能够通过 MPLS 网络传输，需要在 MPLS 骨干网络中配置 IGP 路由协议，并利用 LDP 分发公网标签，作为 VPN 报文的外层标签。
- 为区分不同用户的路由信息，需要在 PE 上分别创建两个 VPN 实例，并为 VPN 实例配置 RD 和 RT，在各实例内通过 BGP 分别引入不同用户的私网路由。
- 在 PE 设备之间配置 MP-BGP 协议并建立对等体，用于传输 VPN 的私网路由信息并分发内层标签，即私网标签。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

由于在配置接口与 VPN 实例绑定后，接口上的 IP 地址等配置会清除，因此先配置接口与 VPN 实例的绑定关系，再进行其他配置。

3.5 配置步骤

1. 在 MPLS 骨干网上配置 IGP 协议（本例为 OSPF 协议），实现骨干网 PE 和 P 的互通

(1) 配置 PE 1

配置骨干网接口以及环回口地址。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] ip address 10.1.1.1 24
[PE1-GigabitEthernet1/0/2] quit
# 配置 OSPF 协议发布骨干网侧路由。
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

(2) 配置 P

配置骨干网接口以及环回口地址。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] interface gigabitethernet 1/0/2
[P-GigabitEthernet1/0/2] ip address 10.1.1.2 24
```

```

[P-GigabitEthernet1/0/2] quit
[P] interface gigabitethernet 1/0/1
[P-GigabitEthernet1/0/1] ip address 10.1.4.1 24
[P-GigabitEthernet1/0/1] quit
# 配置 OSPF 协议发布骨干网侧路由。
[P] ospf 1
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit

```

(3) 配置 PE 2

配置骨干网接口以及环回口地址。

```

<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] ip address 10.1.4.2 24
[PE2-GigabitEthernet1/0/1] quit

```

配置 OSPF 协议发布骨干网侧路由。

```

[PE2] ospf 1
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit

```

配置完成后，PE 1、P、PE 2 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 Full 状态。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback 路由。

以 PE 1 为例：

```
[PE1] display ospf peer verbose
```

```

OSPF Process 1 with Router ID 1.1.1.9
Neighbors

```

```

Area 0.0.0.0 interface 10.1.1.1(GE1/0/2)'s neighbors
Router ID: 2.2.2.9          Address: 10.1.1.2          GR State: Normal
State: Full  Mode: Nbr is Master  Priority: 1
DR: 10.1.1.2  BDR: 10.1.1.1  MTU: 0
Options is 0x02 (-|-|-|-|-|E|-)
Dead timer due in 38 sec
Neighbor is up for 17:30:25
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled

```

```
[PE1] display ip routing-table protocol ospf
```

```
Summary Count : 4
```

```
OSPF Routing table Status : <Active>
```

```
Summary Count : 2
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
3.3.3.9/32	O_INTRA	10	2	10.1.1.2	GE1/0/2
10.1.4.0/24	O_INTRA	10	2	10.1.1.2	GE1/0/2

```
OSPF Routing table Status : <Inactive>
```

```
Summary Count : 2
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.1.1.9/32	O_INTRA	10	0	0.0.0.0	Loop0
10.1.1.0/24	O_INTRA	10	1	0.0.0.0	GE1/0/2

2. 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

(1) 配置 PE 1

配置本节点的 LSR ID，并全局使能本节点的 LDP 能力。

```
[PE1] mpls lsr-id 1.1.1.9
```

```
[PE1] mpls ldp
```

```
[PE1-ldp] quit
```

使能接口的 MPLS 能力和使能接口的 LDP 支持 IPv4 能力。

```
[PE1] interface gigabitEthernet 1/0/2
```

```
[PE1-GigabitEthernet1/0/2] mpls enable
```

```
[PE1-GigabitEthernet1/0/2] mpls ldp enable
```

```
[PE1-GigabitEthernet1/0/2] quit
```

(2) 配置 P

配置本节点的 LSR ID，并全局使能本节点的 LDP 能力。

```
[P] mpls lsr-id 2.2.2.9
```

```
[P] mpls ldp
```

```
[P-ldp] quit
```

使能接口的 MPLS 能力和使能接口的 LDP 支持 IPv4 能力。

```
[P] interface gigabitEthernet 1/0/2
```

```
[P-GigabitEthernet1/0/2] mpls enable
```

```
[P-GigabitEthernet1/0/2] mpls ldp enable
```

```
[P-GigabitEthernet1/0/2] quit
```

```
[P] interface gigabitEthernet 1/0/1
```

```
[P-GigabitEthernet1/0/1] mpls enable
```

```
[P-GigabitEthernet1/0/1] mpls ldp enable
```

```
[P-GigabitEthernet1/0/1] quit
```

(3) 配置 PE 2

配置本节点的 LSR ID，并全局使能本节点的 LDP 能力。

```
[PE2] mpls lsr-id 3.3.3.9
```

```
[PE2] mpls ldp
```

```
[PE2-ldp] quit
```

使能接口的 MPLS 能力和使能接口的 LDP 支持 IPv4 能力。

```
[PE2] interface gigabitethernet 1/0/1
```

```
[PE2-GigabitEthernet1/0/1] mpls enable
```

```
[PE2-GigabitEthernet1/0/1] mpls ldp enable
```

```
[PE2-GigabitEthernet1/0/1] quit
```

上述配置完成后，PE 1、P、PE 2 之间应能建立 LDP 会话，执行 **display mpls ldp peer** 命令可以看到 LDP 会话的状态为 Operational。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。

以 PE 1 为例：

```
[PE1] display mpls ldp peer
```

```
Total number of peers: 1
```

Peer LDP ID	State	Role	GR	MD5	KA Sent/Rcvd
2.2.2.9:0	Operational	Passive	Off	Off	5/5

```
[PE1] display mpls ldp lsp
```

```
Status Flags: * - stale, L - liberal, B - backup
```

```
FECs: 4          Ingress: 1          Transit: 1          Egress: 3
```

FEC	In/Out Label	NextHop	OutInterface
1.1.1.9/32	3/- -/1151(L)		
2.2.2.9/32	-/3 1151/3	10.1.1.2	GE1/0/2
3.3.3.9/32	-/1150 1150/1150	10.1.1.2	GE1/0/2

3. 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

(1) 配置 PE 1

在 PE 1 上为 Customer A 创建 VPN 实例，名为“customerA”。

```
[PE1] ip vpn-instance customerA
```

为该实例配置 RD 为 100:1，用于形成 VPNv4 路由，以便区分不同用户相同网段的路由。

```
[PE1-vpn-instance-customerA] route-distinguisher 100:1
```

为该 VPN 实例配置 VPN Target 属性，其中接收路由的属性为 111:1，发布路由的属性为 222:1。

```
[PE1-vpn-instance-customerA] vpn-target 111:1 import-extcommunity
```

```
[PE1-vpn-instance-customerA] vpn-target 222:1 export-extcommunity
```

```
[PE1-vpn-instance-customerA] quit
```

按同样方式为 Customer B 创建 VPN 实例，名为“customerB”，并为其配置 RD 为 200:1，接收和发送的 VPN Target 属性分别为 333:1 和 444:1。

```
[PE1] ip vpn-instance customerB
```

```
[PE1-vpn-instance-customerB] route-distinguisher 200:1
```

```
[PE1-vpn-instance-customerB] vpn-target 333:1 import-extcommunity
```

```
[PE1-vpn-instance-customerB] vpn-target 444:1 export-extcommunity
```

```
[PE1-vpn-instance-customerB] quit
```

配置 GigabitEthernet 1/0/1 与 VPN 实例 customerA 进行绑定。

```
[PE1] interface gigabitethernet 1/0/1
```

```
[PE1-GigabitEthernet1/0/1] ip binding vpn-instance customerA
[PE1-GigabitEthernet1/0/1] ip address 100.1.1.2 24
[PE1-GigabitEthernet1/0/1] quit
```

配置 GigabitEthernet 1/0/3 与 VPN 实例 customerB 进行绑定。

```
[PE1] interface gigabitethernet 1/0/3
[PE1-GigabitEthernet1/0/3] ip binding vpn-instance customerB
[PE1-GigabitEthernet1/0/3] ip address 200.1.1.2 24
[PE1-GigabitEthernet1/0/3] quit
```

(2) 配置 PE 2

在 PE 2 上为 Customer A 创建 VPN 实例，名为“customerA”。

```
[PE2] ip vpn-instance customerA
```

为该 VPN 实例配置 RD，为便于识别，建议与 PE 1 上为该实例配置的 RD 保持一致。

```
[PE2-vpn-instance-customerA] route-distinguisher 100:1
```

为该 VPN 实例配置 VPN Target，需要注意的是接收和发送的属性要分别与 PE 1 上配置的发送和接收的属性保持一致。

```
[PE2-vpn-instance-customerA] vpn-target 222:1 import-extcommunity
[PE2-vpn-instance-customerA] vpn-target 111:1 export-extcommunity
[PE2-vpn-instance-customerA] quit
```

按同样方式配置 VPN 实例“customerB”，并配置相应的 RD 和 VPN Target。

```
[PE2] ip vpn-instance customerB
[PE2-vpn-instance-customerB] route-distinguisher 200:1
[PE2-vpn-instance-customerB] vpn-target 444:1 import-extcommunity
[PE2-vpn-instance-customerB] vpn-target 333:1 export-extcommunity
[PE2-vpn-instance-customerB] quit
```

分别将 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 与 customerA 和 customerB 实例进行绑定。

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] ip binding vpn-instance customerA
[PE2-GigabitEthernet1/0/2] ip address 101.1.1.1 24
[PE2-GigabitEthernet1/0/2] quit
[PE2] interface gigabitethernet 1/0/3
[PE2-GigabitEthernet1/0/3] ip binding vpn-instance customerB
[PE2-GigabitEthernet1/0/3] ip address 202.1.1.2 24
[PE2-GigabitEthernet1/0/3] quit
```

(3) 配置 CE

按图 1 配置各 CE 的接口 IP 地址，配置过程略。

配置完成后，在 PE 设备上执行 **display ip vpn-instance** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 PE 1 和 CE 1 为例：

```
[PE1] display ip vpn-instance
Total VPN-Instances configured : 2
VPN-Instance Name          RD          Create time
customerA                   100:1       2014/03/22 13:20:08
customerB                    200:1       2014/03/22 13:20:20
[PE1] ping -vpn-instance customerA 100.1.1.1
```

```

Ping 10.1.1.1 (100.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 100.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 100.1.1.1: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 100.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 100.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 100.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms

```

4. 在 PE 与 CE 之间建立 EBGp 对等体，引入 VPN 路由

(1) 配置 PE 1

在 PE 1 上创建 BGP 进程 100。

```
[PE1] bgp 100
```

将 CE 1 指定为对等体，并将 PE 1 的直连路由引入到 BGP-VPN 实例路由表中。

```

[PE1-bgp] ip vpn-instance customerA
[PE1-bgp-customerA] peer 100.1.1.1 as-number 65410
[PE1-bgp-customerA] address-family ipv4 unicast
[PE1-bgp-ipv4-customerA] peer 100.1.1.1 enable
[PE1-bgp-ipv4-customerA] import-route direct
[PE1-bgp-ipv4-customerA] quit
[PE1-bgp-customerA] quit

```

将 CE 2 指定为对等体，并将 PE 1 的直连路由引入到 BGP-VPN 实例路由表中。

```

[PE1-bgp] ip vpn-instance customerB
[PE1-bgp-customerB] peer 200.1.1.1 as-number 65410
[PE1-bgp-customerB] address-family ipv4 unicast
[PE1-bgp-ipv4-customerB] peer 200.1.1.1 enable
[PE1-bgp-ipv4-customerB] import-route direct
[PE1-bgp-ipv4-customerB] quit
[PE1-bgp-customerB] quit
[PE1-bgp] quit

```

(2) 配置 PE 2

在 PE 2 上创建 BGP 进程 100。

```
[PE2] bgp 100
```

将 CE 3 指定为对等体，并将 PE 2 的直连路由引入到 BGP-VPN 实例路由表中。

```

[PE2-bgp] ip vpn-instance customerA
[PE2-bgp-customerA] peer 101.1.1.2 as-number 65430
[PE2-bgp-customerA] address-family ipv4 unicast
[PE2-bgp-ipv4-customerA] peer 101.1.1.2 enable
[PE2-bgp-ipv4-customerA] import-route direct
[PE2-bgp-ipv4-customerA] quit
[PE2-bgp-customerA] quit

```

将 CE 4 指定为对等体，并将 PE 2 的直连路由引入到 BGP-VPN 实例路由表中。

```

[PE2-bgp] ip vpn-instance customerB
[PE2-bgp-customerB] peer 202.1.1.1 as-number 65430
[PE2-bgp-customerB] address-family ipv4 unicast

```

```
[PE2-bgp-ipv4-customerB] peer 202.1.1.1 enable
[PE2-bgp-ipv4-customerB] import-route direct
[PE2-bgp-ipv4-customerB] quit
[PE2-bgp-customerB] quit
[PE2-bgp] quit
```

(3) 配置 CE1

CE 1 上创建 BGP 进程 65410，并指定 PE 1 为对等体，对等体自治系统号为 100。

```
<CE1> system-view
[CE1] bgp 65410
[CE1-bgp] peer 100.1.1.2 as-number 100
```

使能 CE1 与对等体 100.1.1.2 交换 IPv4 单播路由信息的能力。

```
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 100.1.1.2 enable
```

将 CE 1 上连接站点的直连接口路由引入 EBGP。

```
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
[CE1-bgp] quit
```

(4) 配置 CE2

CE 2 上创建 BGP 进程 65410，并指定 PE 1 为对等体，对等体自治系统号为 100。

```
<CE2> system-view
[CE2] bgp 65410
[CE2-bgp] peer 200.1.1.2 as-number 100
```

使能 CE2 与对等体 200.1.1.2 交换 IPv4 单播路由信息的能力。

```
[CE2-bgp] address-family ipv4 unicast
[CE2-bgp-ipv4] peer 200.1.1.2 enable
```

将 CE 2 上连接站点的直连接口路由引入 EBGP。

```
[CE2-bgp-ipv4] import-route direct
[CE2-bgp-ipv4] quit
[CE2-bgp] quit
```

(5) 配置 CE3

CE 3 上创建 BGP 进程 65430，并指定 PE 2 为对等体，对等体自治系统号为 100。

```
<CE3> system-view
[CE3] bgp 65430
[CE3-bgp] peer 101.1.1.1 as-number 100
```

使能 CE3 与对等体 101.1.1.1 交换 IPv4 单播路由信息的能力。

```
[CE3-bgp] address-family ipv4 unicast
[CE3-bgp-ipv4] peer 101.1.1.1 enable
```

将 CE 3 上连接站点的直连接口路由引入 EBGP。

```
[CE3-bgp-ipv4] import-route direct
[CE3-bgp-ipv4] quit
[CE3-bgp] quit
```

(6) 配置 CE4

CE4 上创建 BGP 进程 65430，并指定 PE 2 为对等体，对等体自治系统号为 100。

```
<CE4> system-view
[CE4] bgp 65430
```

```
[CE4-bgp] peer 202.1.1.2 as-number 100
```

使能 CE4 与对等体 202.1.1.2 交换 IPv4 单播路由信息的能力。

```
[CE4-bgp] address-family ipv4 unicast
```

```
[CE4-bgp-ipv4] peer 202.1.1.2 enable
```

将 CE 4 上连接站点的直连接口路由引入 EBGP。

```
[CE4-bgp-ipv4] import-route direct
```

```
[CE4-bgp-ipv4] quit
```

```
[CE4-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer ipv4 vpn-instance** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 **Established** 状态。

以 PE 1 与 CE 1 的对等体关系为例：

```
[PE1] display bgp peer ipv4 vpn-instance customerA
```

```
BGP local router ID: 1.1.1.9
```

```
Local AS number: 100
```

```
Total number of peers: 1
```

```
Peers in established state: 1
```

Peer	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
100.1.1.1	65410	4	4	0	2	13:35:25	Established

5. 在 PE 之间建立 MP-IBGP 对等体

(1) 配置 PE 1

在 PE 1 上配置 PE 2 为 BGP 对等体，并指定连接时使用的接口为 Loopback0 接口。

```
[PE1] bgp 100
```

```
[PE1-bgp] peer 3.3.3.9 as-number 100
```

```
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
```

进入 BGP-VPNv4 地址族视图，指定 PE 2 为对等体。

```
[PE1-bgp] address-family vpnv4
```

```
[PE1-bgp-vpnv4] peer 3.3.3.9 enable
```

```
[PE1-bgp-vpnv4] quit
```

```
[PE1-bgp] quit
```

(2) 配置 PE 2

在 PE 2 上配置 PE 1 为 BGP 对等体，并指定连接时使用的接口为 Loopback0 接口。

```
[PE2] bgp 100
```

```
[PE2-bgp] peer 1.1.1.9 as-number 100
```

```
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
```

进入 BGP-VPNv4 地址族视图，指定 PE 1 为对等体。

```
[PE2-bgp] address-family vpnv4
```

```
[PE2-bgp-vpnv4] peer 1.1.1.9 enable
```

```
[PE2-bgp-vpnv4] quit
```

```
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer vpnv4** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 **Established** 状态。

```
[PE1] display bgp peer vpnv4
```

```
BGP local router ID: 1.1.1.9
```



```

Local AS number: 100
Total number of peers: 1                Peers in established state: 1

Peer                AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
3.3.3.9            100      8        8        0      0 00:00:08  Established

```

3.6 验证配置

在 PE 设备上执行 `display ip routing-table vpn-instance` 命令，可以看到去往对端 CE 的路由。

以 PE 1 上的 `customerA` 为例：

```
[PE1] display ip routing-table vpn-instance customerA
```

```

Destinations : 13          Routes : 13

Destination/Mask    Proto  Pre  Cost           NextHop           Interface
0.0.0.0/32          Direct 0    0              127.0.0.1         InLoop0
100.1.1.0/24        Direct 0    0              100.1.1.2         GE1/0/1
100.1.1.0/32        Direct 0    0              100.1.1.2         GE1/0/1
100.1.1.2/32        Direct 0    0              127.0.0.1         InLoop0
100.1.1.255/32      Direct 0    0              100.1.1.2         GE1/0/1
101.1.1.0/24        BGP    255  0              3.3.3.9           GE1/0/2
127.0.0.0/8         Direct 0    0              127.0.0.1         InLoop0
127.0.0.0/32        Direct 0    0              127.0.0.1         InLoop0
127.0.0.1/32        Direct 0    0              127.0.0.1         InLoop0
127.255.255.255/32 Direct 0    0              127.0.0.1         InLoop0
224.0.0.0/4         Direct 0    0              0.0.0.0           NULL0
224.0.0.0/24        Direct 0    0              0.0.0.0           NULL0
255.255.255.255/32 Direct 0    0              127.0.0.1         InLoop0

```

同一 VPN 的 CE 能够相互 Ping 通，不同 VPN 的 CE 不能相互 Ping 通。

例如：CE1 能够 Ping 通 CE 3（101.1.1.2），但不能 Ping 通 CE 4（202.1.1.1）。

3.7 配置文件

- PE 1:

```

#
ip vpn-instance customerA
 route-distinguisher 100:1
  vpn-target 111:1 import-extcommunity
  vpn-target 222:1 export-extcommunity
#
ip vpn-instance customerB
 route-distinguisher 200:1
  vpn-target 333:1 import-extcommunity
  vpn-target 444:1 export-extcommunity
#
ospf 1

```

```

area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
mpls lsr-id 1.1.1.9
#
mpls ldp
#
interface LoopBack0
  ip address 1.1.1.9 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip binding vpn-instance customerA
  ip address 100.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 10.1.1.1 255.255.255.0
  mpls enable
  mpls ldp enable
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip binding vpn-instance customerB
  ip address 200.1.1.2 255.255.255.0
#
bgp 100
  peer 3.3.3.9 as-number 100
  peer 3.3.3.9 connect-interface LoopBack0
#
  address-family vpnv4
    peer 3.3.3.9 enable
#
  ip vpn-instance customerA
    peer 100.1.1.1 as-number 65410
#
  address-family ipv4 unicast
    import-route direct
    peer 100.1.1.1 enable
#
  ip vpn-instance customerB
    peer 200.1.1.1 as-number 65410
#
  address-family ipv4 unicast
    import-route direct
    peer 200.1.1.1 enable
#

```

- **P:**

```
#
ospf 1
  area 0.0.0.0
    network 2.2.2.9 0.0.0.0
    network 10.1.1.0 0.0.0.255
    network 10.1.4.0 0.0.0.255
#
mpls lsr-id 2.2.2.9
#
mpls ldp
#
interface LoopBack0
  ip address 2.2.2.9 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 10.1.4.1 255.255.255.0
  mpls enable
  mpls ldp enable
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 10.1.1.2 255.255.255.0
  mpls enable
  mpls ldp enable
#
```

- **PE 2:**

```
#
ip vpn-instance customerA
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
#
ip vpn-instance customerB
  route-distinguisher 200:1
  vpn-target 333:1 export-extcommunity
  vpn-target 444:1 import-extcommunity
#
ospf 1
  area 0.0.0.0
    network 10.1.4.0 0.0.0.255
    network 3.3.3.9 0.0.0.0
#
mpls lsr-id 3.3.3.9
#
mpls ldp
#
```

```

interface LoopBack0
  ip address 3.3.3.9 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 10.1.4.2 255.255.255.0
  mpls enable
  mpls ldp enable
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip binding vpn-instance customerA
  ip address 101.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip binding vpn-instance customerB
  ip address 202.1.1.2 255.255.255.0
#
bgp 100
  peer 1.1.1.9 as-number 100
  peer 1.1.1.9 connect-interface LoopBack0
#
  address-family vpnv4
    peer 1.1.1.9 enable
#
  ip vpn-instance customerA
    peer 101.1.1.2 as-number 65430
#
    address-family ipv4 unicast
      import-route direct
      peer 101.1.1.2 enable
#
  ip vpn-instance customerB
    peer 202.1.1.1 as-number 65430
#
    address-family ipv4 unicast
      import-route direct
      peer 202.1.1.1 enable
#

```

- **CE 1:**

```

#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 100.1.1.1 255.255.255.0
#
bgp 65410
  peer 100.1.1.2 as-number 100

```

```

#
address-family ipv4 unicast
import-route direct
peer 100.1.1.2 enable
#
• CE 2:
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 200.1.1.1 255.255.255.0
#
bgp 65410
peer 200.1.1.2 as-number 100
#
address-family ipv4 unicast
import-route direct
peer 200.1.1.2 enable
#
• CE 3:
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 101.1.1.2 255.255.255.0
#
bgp 65430
peer 101.1.1.1 as-number 100
#
address-family ipv4 unicast
import-route direct
peer 101.1.1.1 enable
#
• CE 4:
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 202.1.1.1 255.255.255.0
#
bgp 65430
peer 202.1.1.2 as-number 100
#
address-family ipv4 unicast
import-route direct
peer 202.1.1.2 enable
#

```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“MPLS 配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“MPLS 命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

H3C MSR 系列路由器

HoVPN 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.6 验证配置.....	9
3.7 配置文件.....	10
4 相关资料.....	15

1 简介

本文档介绍 MPLS HoVPN 的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 HoVPN 特性。

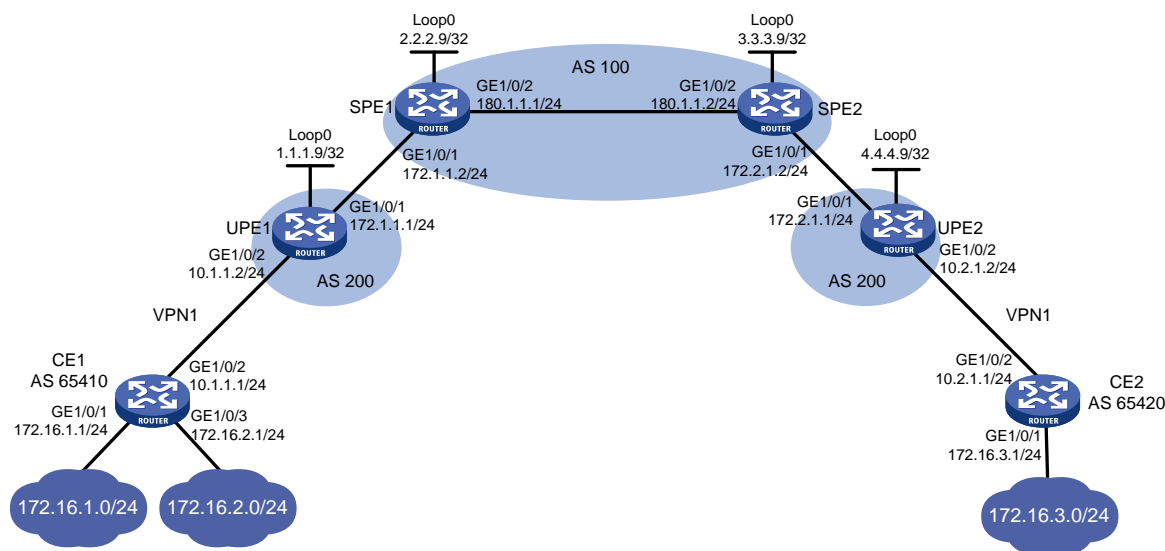
3 配置举例

3.1 组网需求

如图 1 所示，SPE 设备处于 AS 100 中，UPE 设备处于 AS 200 中，SPE 为运营商骨干网设备，UPE 为连接用户端 CE 的设备。UPE 1 和 UPE 2 分别连接属于 VPN 1 的 CE 1 和 CE 2。CE 1 连接两个网段，分别为：172.16.1.0/24 和 172.16.2.0/24；CE 2 下连 172.16.3.0/24 网段。

现要求在用户网络中部署 HoVPN 服务，并通过配置路由策略，限制不同 CE 下连网段之间的互相访问权限，使得 CE 1 的 172.16.1.0/24 和 CE 2 的 172.16.3.0/24 可以相互访问，CE 1 的 172.16.2.0/24 和 CE 2 的 172.16.3.0/24 不能相互访问。

图1 HoVPN 典型配置举例组网图



3.2 配置思路

此案例配置主要分为两部分：

- 在网络中配置 HoVPN 服务。
- 在 SPE 设备上配置路由策略，使得 SPE2 仅发布 CE1 的私网路由 172.16.1.0/24 给 UPE2。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 只有在 SPE 设备上配置了路由策略，并允许向 UPE 设备发布路由时，SPE 设备才会向 UPE 设备发布路由，即，在 HoVPN 组网中，路由策略为必选配置。
- 配置 SPE 与 UPE 之间建立 EBGP 对等体并发布标签时，仅使能与对等体交换标签的能力并不能进行标签的发布，还需配置路由策略才可为对等体发布标签。
- 由于在配置接口与 VPN 实例绑定后，接口上的 IP 地址等配置会清除，因此先配置接口与 VPN 实例的绑定关系，再进行其他配置。

3.5 配置步骤

1. 在 SPE 设备上使能 MPLS 和 MPLS LDP 功能，并配置 OSPF 作为 IGP 协议

(1) 配置 SPE1

配置设备环回口地址。

```
<SPE1> system-view
[SPE1] interface loopback 0
[SPE1-LoopBack0] ip address 2.2.2.9 32
[SPE1-LoopBack0] quit
```

配置设备的 LSR ID，并全局使能设备的 LDP 能力。

```
[SPE1] mpls lsr-id 2.2.2.9
[SPE1] mpls ldp
[SPE1-ldp] quit
```

配置设备接口地址，并使能接口的 MPLS 能力。

```
[SPE1] interface gigabitEthernet1/0/1
[SPE1-GigabitEthernet1/0/1] ip address 172.1.1.2 24
[SPE1-GigabitEthernet1/0/1] mpls enable
[SPE1-GigabitEthernet1/0/1] quit
```

配置设备接口地址，并使能接口的 MPLS 能力和接口的 LDP 支持 IPv4 能力。

```
[SPE1] interface gigabitEthernet1/0/2
[SPE1-GigabitEthernet1/0/2] ip address 180.1.1.1 24
[SPE1-GigabitEthernet1/0/2] mpls enable
[SPE1-GigabitEthernet1/0/2] mpls ldp enable
[SPE1-GigabitEthernet1/0/2] quit
```

配置 OSPF 作为 IGP 协议，使骨干网互通。

```

[SPE1] ospf 1
[SPE1-ospf-1] area 0
[SPE1-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[SPE1-ospf-1-area-0.0.0.0] network 180.1.1.0 0.0.0.255
[SPE1-ospf-1-area-0.0.0.0] quit
[SPE1-ospf-1] quit

```

(2) 配置 SPE2

配置设备环回口地址。

```

<SPE2> system-view
[SPE2] interface loopback 0
[SPE2-LoopBack0] ip address 3.3.3.9 32
[SPE2-LoopBack0] quit

```

配置设备的 LSR ID，并全局使能设备的 LDP 能力。

```

[SPE2] mpls lsr-id 3.3.3.9
[SPE2] mpls ldp
[SPE2-ldp] quit

```

配置设备接口地址，并使能接口的 MPLS 能力和接口的 LDP 支持 IPv4 能力。

```

[SPE2] interface gigabitEthernet1/0/2
[SPE2-GigabitEthernet1/0/2] ip address 180.1.1.2 24
[SPE2-GigabitEthernet1/0/2] mpls enable
[SPE2-GigabitEthernet1/0/2] mpls ldp enable
[SPE2-GigabitEthernet1/0/2] quit

```

配置设备接口地址，并使能接口的 MPLS 能力。

```

[SPE2] interface gigabitEthernet1/0/1
[SPE2-GigabitEthernet1/0/1] ip address 172.2.1.2 24
[SPE2-GigabitEthernet1/0/1] mpls enable
[SPE2-GigabitEthernet1/0/1] quit

```

配置 OSPF 作为 IGP 协议，使骨干网互通。

```

[SPE2] ospf 1
[SPE2-ospf-1] area 0
[SPE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[SPE2-ospf-1-area-0.0.0.0] network 180.1.1.0 0.0.0.255
[SPE2-ospf-1-area-0.0.0.0] quit
[SPE2-ospf-1] quit

```

配置完成后，在 SPE 设备上执行 **display mpls ldp peer** 命令可以看到 LDP 会话建立成功，LDP 会话状态为 **Operational**；执行 **display ospf peer** 命令可以看到 OSPF 邻居关系已建立，状态为 **FULL**。

2. 配置 SPE 之间建立 MP-IBGP 对等体，交换 VPNv4 路由

配置 SPE 1 与 SPE 2 建立 MP-IBGP 对等体，交换 VPNv4 路由。

```

[SPE1] bgp 100
[SPE1-bgp] peer 3.3.3.9 as-number 100
[SPE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[SPE1-bgp] address-family vpnv4
[SPE1-bgp-vpnv4] peer 3.3.3.9 enable
[SPE1-bgp-vpnv4] quit

```

```
[SPE1-bgp] quit
```

配置 SPE 2 与 SPE 1 建立 MP-IBGP 对等体，交换 VPNv4 路由。

```
[SPE2] bgp 100
```

```
[SPE2-bgp] peer 2.2.2.9 as-number 100
```

```
[SPE2-bgp] peer 2.2.2.9 connect-interface loopback 0
```

```
[SPE2-bgp] address-family vpnv4
```

```
[SPE2-bgp-vpnv4] peer 2.2.2.9 enable
```

```
[SPE2-bgp-vpnv4] quit
```

```
[SPE2-bgp] quit
```

配置完成后，在 SPE1 和 SPE2 上执行 **display bgp peer vpnv4** 命令可以看到 BGP 对等体关系已建立，并达到 **Established** 状态。

3. 在 UPE 设备上使能 MPLS 功能

(1) 配置 UPE1

配置设备环回口地址。

```
<UPE1> system-view
```

```
[UPE1] interface loopback 0
```

```
[UPE1-LoopBack0] ip address 1.1.1.9 32
```

```
[UPE1-LoopBack0] quit
```

配置设备的 LSR ID。

```
[UPE1] mpls lsr-id 1.1.1.9
```

配置设备接口地址，并使能接口的 MPLS 能力。

```
[UPE1] interface gigabitEthernet1/0/1
```

```
[UPE1-GigabitEthernet1/0/1] ip address 172.1.1.1 24
```

```
[UPE1-GigabitEthernet1/0/1] mpls enable
```

```
[UPE1-GigabitEthernet1/0/1] quit
```

(2) 配置 UPE2

配置设备环回口地址。

```
<UPE2> system-view
```

```
[UPE2] interface loopback 0
```

```
[UPE2-Loopback0] ip address 4.4.4.9 32
```

```
[UPE2-Loopback0] quit
```

配置设备的 LSR ID。

```
[UPE2] mpls lsr-id 4.4.4.9
```

配置设备接口地址，并使能接口的 MPLS 能力。

```
[UPE2] interface gigabitEthernet1/0/1
```

```
[UPE2-GigabitEthernet1/0/1] ip address 172.2.1.1 24
```

```
[UPE2-GigabitEthernet1/0/1] mpls enable
```

```
[UPE2-GigabitEthernet1/0/1] quit
```

4. 配置 SPE 与 UPE 建立 EBGP 对等体，并交换带标签的路由，建立 BGP LSP

(1) 配置 SPE1

配置 UPE 1 与 SPE 1 建立 EBGP 对等体。

```
[SPE1] bgp 100
```

```
[SPE1-bgp] peer 172.1.1.1 as-number 200
```

在 BGP IPv4 单播地址族视图下，使能与对等体交换带标签 IPv4 路由的能力。

```

[SPE1-bgp] address-family ipv4
[SPE1-bgp-ipv4] peer 172.1.1.1 enable
[SPE1-bgp-ipv4] peer 172.1.1.1 label-route-capability
# 配置对向对等体发布的路由应用名为 policy1 的路由策略。
[SPE1-bgp-ipv4] peer 172.1.1.1 route-policy policy1 export
[SPE1-bgp-ipv4] network 2.2.2.9 255.255.255.255
[SPE1-bgp-ipv4] quit
[SPE1-bgp] quit
# 配置路由策略，为路由分配标签。
[SPE1] route-policy policy1 permit node 0
[SPE1-route-policy-policy1-0] apply mpls-label
[SPE1-route-policy-policy1-0] quit

```

(2) 配置 UPE1

```

# 配置 UPE 1 与 SPE 1 建立 EBGP 对等体。
[UPE1] bgp 200
[UPE1-bgp] peer 172.1.1.2 as-number 100
# 在 BGP IPv4 单播地址族视图下，使能与对等体交换带标签 IPv4 路由的能力。
[UPE1-bgp] address-family ipv4
[UPE1-bgp-ipv4] peer 172.1.1.2 enable
[UPE1-bgp-ipv4] peer 172.1.1.2 label-route-capability
# 配置对向对等体发布的路由应用名为 policy1 的路由策略。
[UPE1-bgp-ipv4] peer 172.1.1.2 route-policy policy1 export
[UPE1-bgp-ipv4] network 1.1.1.9 255.255.255.255
[UPE1-bgp-ipv4] quit
[UPE1-bgp] quit
# 配置路由策略，为路由分配标签。
[UPE1] route-policy policy1 permit node 0
[UPE1-route-policy-policy1-0] apply mpls-label
[UPE1-route-policy-policy1-0] quit

```

(3) 配置 SPE2

```

# 配置 UPE 2 与 SPE 2 建立 EBGP 对等体。
[SPE2] bgp 100
[SPE2-bgp] peer 172.2.1.1 as-number 200
# 在 BGP IPv4 单播地址族视图下，使能与对等体交换带标签 IPv4 路由的能力。
[SPE2-bgp] address-family ipv4
[SPE2-bgp-ipv4] peer 172.2.1.1 enable
[SPE2-bgp-ipv4] peer 172.2.1.1 label-route-capability
# 配置对向对等体发布的路由应用名为 policy1 的路由策略。
[SPE2-bgp-ipv4] peer 172.2.1.1 route-policy policy1 export
[SPE2-bgp-ipv4] network 3.3.3.9 255.255.255.255
[SPE2-bgp-ipv4] quit
[SPE2-bgp] quit
# 配置路由策略，为路由分配标签。
[SPE2] route-policy policy1 permit node 0
[SPE2-route-policy-policy1-0] apply mpls-label

```

```
[SPE2-route-policy-policy1-0] quit
```

(4) 配置 UPE2

配置 UPE 2 与 SPE 2 建立 EBGP 对等体。

```
[UPE2] bgp 200
```

```
[UPE2-bgp] peer 172.2.1.2 as-number 100
```

在 BGP IPv4 单播地址族视图下，使能与对等体交换带标签 IPv4 路由的能力。

```
[UPE2-bgp] address-family ipv4
```

```
[UPE2-bgp-ipv4] peer 172.2.1.2 enable
```

```
[UPE2-bgp-ipv4] peer 172.2.1.2 label-route-capability
```

配置对向对等体发布的路由应用名为 **policy1** 的路由策略。

```
[UPE2-bgp-ipv4] peer 172.2.1.2 route-policy policy1 export
```

```
[UPE2-bgp-ipv4] network 4.4.4.9 255.255.255.255
```

```
[UPE2-bgp-ipv4] quit
```

```
[UPE2-bgp] quit
```

配置路由策略，为路由分配标签。

```
[UPE2] route-policy policy1 permit node 0
```

```
[UPE2-route-policy-policy1-0] apply mpls-label
```

```
[UPE2-route-policy-policy1-0] quit
```

配置完成后，在各设备上执行 **display mpls lsp** 命令可以看到已在 SPE 与 UPE 之间建立 BGP LSP。

5. 配置 SPE 与 UPE 建立 MP-EBGP 对等体，使能 HoVPN 服务

(1) 配置 UPE1

配置 UPE 1 与 SPE 1 建立 MP-EBGP 对等体。

```
[UPE1] bgp 200
```

```
[UPE1-bgp] peer 2.2.2.9 as-number 100
```

```
[UPE1-bgp] peer 2.2.2.9 connect-interface loopback 0
```

```
[UPE1-bgp] address-family vpnv4
```

```
[UPE1-bgp-vpnv4] peer 2.2.2.9 enable
```

配置 UPE1 接受 AS_PATH 属性中已包含本地 AS 号的路由，以接收位于相同 AS 的 UPE2 的路由。

```
[UPE1-bgp-vpnv4] peer 2.2.2.9 allow-as-loop
```

```
[UPE1-bgp-vpnv4] quit
```

(2) 配置 SPE1

配置 VPN 实例 vpn1。

```
[SPE1] ip vpn-instance vpn1
```

```
[SPE1-vpn-instance-vpn1] route-distinguisher 100:1
```

```
[SPE1-vpn-instance-vpn1] vpn-target 100:1 both
```

```
[SPE1-vpn-instance-vpn1] quit
```

配置 SPE 1 与 UPE 1 建立 MP-EBGP 对等体，指定 UPE 1，并引入 VPN 路由。

```
[SPE1] bgp 100
```

```
[SPE1-bgp] peer 1.1.1.9 as-number 200
```

```
[SPE1-bgp] peer 1.1.1.9 connect-interface loopback 0
```

```
[SPE1-bgp] address-family vpnv4
```

```
[SPE1-bgp-vpnv4] peer 1.1.1.9 enable
```

```
[SPE1-bgp-vpnv4] peer 1.1.1.9 upe
[SPE1-bgp-vpnv4] quit
[SPE1-bgp] ip vpn-instance vpn1
[SPE1-bgp-vpn1] quit
[SPE1-bgp] quit
```

(3) 配置 UPE2

配置 UPE 2 与 SPE 2 建立 MP-EBGP 对等体。

```
[UPE2] bgp 200
[UPE2-bgp] peer 3.3.3.9 as-number 100
[UPE2-bgp] peer 3.3.3.9 connect-interface loopback 0
[UPE2-bgp] address-family vpnv4
[UPE2-bgp-vpnv4] peer 3.3.3.9 enable
```

配置 UPE2 接受 AS_PATH 属性中已包含本地 AS 号的路由，以接收位于相同 AS 的 UPE2 的路由。

```
[UPE2-bgp-vpnv4] peer 3.3.3.9 allow-as-loop
[UPE2-bgp-vpnv4] quit
```

(4) 配置 SPE2

配置 VPN 实例 vpn1。

```
[SPE2] ip vpn-instance vpn1
[SPE2-vpn-instance-vpn1] route-distinguisher 100:1
[SPE2-vpn-instance-vpn1] vpn-target 100:1 both
[SPE2-vpn-instance-vpn1] quit
```

配置 SPE 2 与 UPE 2 建立 MP-EBGP 对等体，指定 UPE 2，并引入 VPN 路由。

```
[SPE2] bgp 100
[SPE2-bgp] peer 4.4.4.9 as-number 200
[SPE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[SPE2-bgp] address-family vpnv4
[SPE2-bgp-vpnv4] peer 4.4.4.9 enable
[SPE2-bgp-vpnv4] peer 4.4.4.9 upe
[SPE2-bgp-vpnv4] quit
[SPE2-bgp] ip vpn-instance vpn1
[SPE2-bgp-vpn1] quit
[SPE2-bgp] quit
```

配置完成后，在 SPE 和 UPE 设备上执行 **display bgp peer vpnv4** 命令可以看到相互之间的 BGP 对等体关系已建立，并达到 **Established** 状态。

6. 配置 UPE 接入 CE

(1) 配置 UPE1

配置 VPN 实例 vpn1，将 CE 1 接入 UPE 1。

```
[UPE1] ip vpn-instance vpn1
[UPE1-vpn-instance-vpn1] route-distinguisher 100:1
[UPE1-vpn-instance-vpn1] vpn-target 100:1 both
[UPE1-vpn-instance-vpn1] quit
[UPE1] interface gigabitethernet1/0/2
[UPE1-Gigabitethernet1/0/2] ip binding vpn-instance vpn1
[UPE1-Gigabitethernet1/0/2] ip address 10.1.1.2 24
```

```
[UPE1-GigabitEthernet1/0/2] quit
# 配置 UPE 1 与 CE 1 建立 EBGP 对等体，并引入 VPN 路由。
```

```
[UPE1] bgp 200
[UPE1-bgp] ip vpn-instance vpn1
[UPE1-bgp-vpn1] peer 10.1.1.1 as-number 65410
[UPE1-bgp-vpn1] address-family ipv4 unicast
[UPE1-bgp-ipv4-vpn1] peer 10.1.1.1 enable
[UPE1-bgp-ipv4-vpn1] import-route direct
[UPE1-bgp-ipv4-vpn1] quit
[UPE1-bgp-vpn1] quit
```

(2) 配置 CE1

配置接口 IP 地址。

```
<CE1> system-view
[CE1] interface gigabitEthernet1/0/2
[CE1-GigabitEthernet1/0/2] ip address 10.1.1.1 255.255.255.0
[CE1-GigabitEthernet1/0/2] quit
```

配置 CE1 与 UPE1 建立 EBGP 对等体，并引入直连路由。

```
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.2 as-number 200
[CE1-bgp] address-family ipv4 unicast
[CE1-bgp-ipv4] peer 10.1.1.2 enable
[CE1-bgp-ipv4] import-route direct
[CE1-bgp-ipv4] quit
[CE1-bgp] quit
```

(3) 配置 UPE2

配置 VPN 实例 vpn1，将 CE 2 接入 UPE 2。

```
[UPE2] ip vpn-instance vpn1
[UPE2-vpn-instance-vpn1] route-distinguisher 100:1
[UPE2-vpn-instance-vpn1] vpn-target 100:1 both
[UPE2-vpn-instance-vpn1] quit
[UPE2] interface gigabitEthernet1/0/2
[UPE2-GigabitEthernet1/0/2] ip binding vpn-instance vpn1
[UPE2-GigabitEthernet1/0/2] ip address 10.2.1.2 24
[UPE2-GigabitEthernet1/0/2] quit
```

配置 UPE 2 与 CE 2 建立 EBGP 对等体，并引入 VPN 路由。

```
[UPE2] bgp 200
[UPE2-bgp] ip vpn-instance vpn1
[UPE2-bgp-vpn1] peer 10.2.1.1 as-number 65420
[UPE2-bgp-vpn1] address-family ipv4 unicast
[UPE2-bgp-ipv4-vpn1] peer 10.2.1.1 enable
[UPE2-bgp-ipv4-vpn1] import-route direct
[UPE2-bgp-ipv4-vpn1] quit
[UPE2-bgp-vpn1] quit
```

(4) 配置 CE 2

配置接口 IP 地址。

```
<CE2> system-view
```



```
[CE2] interface gigabitethernet1/0/2
[CE2-GigabitEthernet1/0/2] ip address 10.2.1.1 255.255.255.0
[CE2-GigabitEthernet1/0/2] quit
```

配置 CE 2 与 UPE 2 建立 EBGP 对等体，并引入直连路由。

```
[CE2] bgp 65420
[CE2-bgp] peer 10.2.1.2 as-number 200
[CE2-bgp] address-family ipv4 unicast
[CE2-bgp-ipv4] peer 10.2.1.2 enable
[CE2-bgp-ipv4] import-route direct
[CE2-bgp-ipv4] quit
[CE2-bgp] quit
```

配置完成后，在 UPE 和 CE 设备上执行 **display bgp peer ipv4** 命令可以看到相互之间的 BGP 对等体关系已建立，并达到 Established 状态。

7. 在 SPE 设备上配置路由策略，控制 VPN 之间路由的传播

(1) 配置 SPE1

配置 SPE 1 向 UPE 1 发送通过策略的路由信息，允许 CE 2 的路由发送给 UPE 1。

```
[SPE1] ip prefix-list list1 index 10 permit 172.16.3.0 24
[SPE1] route-policy policy2 permit node 0
[SPE1-route-policy-policy2-0] if-match ip address prefix-list list1
[SPE1-route-policy-policy2-0] quit
[SPE1] bgp 100
[SPE1-bgp] address-family vpnv4
[SPE1-bgp-vpnv4] peer 1.1.1.9 upe route-policy policy2 export
[SPE1-bgp-vpnv4] quit
[SPE1-bgp] quit
```

(2) 配置 SPE2

配置 SPE 2 向 UPE 2 发送通过策略的路由信息，允许 CE 1 的私网路由 172.16.1.0/24 发送给 UPE 2。

```
[SPE2] ip prefix-list list1 index 10 permit 172.16.1.0 24
[SPE2] route-policy policy2 permit node 0
[SPE2-route-policy-policy2-0] if-match ip address prefix-list list1
[SPE2-route-policy-policy2-0] quit
[SPE2] bgp 100
[SPE2-bgp] address-family vpnv4
[SPE2-bgp-vpnv4] peer 4.4.4.9 upe route-policy policy2 export
[SPE2-bgp-vpnv4] quit
[SPE2-bgp]quit
```

3.6 验证配置

配置完成后，可以看到 CE1 已经学习到 CE2 下连网段 172.16.3.0/24，如下：

```
[CE1] display ip routing-table
```

```
Destinations : 25          Routes : 25
```

```
Destination/Mask    Proto  Pre  Cost           NextHop           Interface
```

172.16.1.0/24	Direct	0	0	172.16.1.1	GE1/0/1
172.16.1.0/32	Direct	0	0	172.16.1.1	GE1/0/1
172.16.1.1/32	Direct	0	0	127.0.0.1	InLoop0
172.16.1.255/32	Direct	0	0	172.16.1.1	GE1/0/1
172.16.2.0/24	Direct	0	0	172.16.2.1	GE1/0/3
172.16.2.0/32	Direct	0	0	172.16.2.1	GE1/0/3
172.16.2.1/32	Direct	0	0	127.0.0.1	InLoop0
172.16.2.255/32	Direct	0	0	172.16.2.1	GE1/0/3
172.16.3.0/24	BGP	255	0	10.1.1.2	GE1/0/2

CE2 已经学习到 CE1 的下连网段 172.16.1.0/24，但并未学习到 CE1 的下连网段 172.16.2.0/24。如下：

```
<CE2> display ip routing-table
```

```
Destinations : 21          Routes : 21
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
172.16.1.0/24	BGP	255	0	10.2.1.2	GE1/0/2
172.16.3.0/24	Direct	0	0	172.16.3.1	GE1/0/1
172.16.3.0/32	Direct	0	0	172.16.3.1	GE1/0/1
172.16.3.1/32	Direct	0	0	127.0.0.1	InLoop0
172.16.3.255/32	Direct	0	0	172.16.3.1	GE1/0/1

CE1 的下连网段 172.16.1.0/24 可与 CE2 的下连网段 172.16.3.0/24 互通；CE1 的下连网段 172.16.2.0/24 不能与 CE2 的下连网段 172.16.3.0/24 互通。

3.7 配置文件

- CE1:

```
#
interface GigabitEthernet1/0/1
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 ip address 172.16.2.1 255.255.255.0
#
bgp 65410
 peer 10.1.1.2 as-number 200
#
 address-family ipv4 unicast
  import-route direct
 peer 10.1.1.2 enable
#
```

- CE2:

```
#
interface GigabitEthernet1/0/1
```

```

ip address 172.16.3.1 255.255.255.0
#
interface GigabitEthernet1/0/2
ip address 10.2.1.1 255.255.255.0
#
bgp 65420
peer 10.2.1.2 as-number 200
#
address-family ipv4 unicast
import-route direct
peer 10.2.1.2 enable
#

```

- **UPE1:**

```

#
ip vpn-instance vpn1
route-distinguisher 100:1
vpn-target 100:1 import-extcommunity
vpn-target 100:1 export-extcommunity
#
mpls lsr-id 1.1.1.9
#
interface LoopBack0
ip address 1.1.1.9 255.255.255.255
#
interface GigabitEthernet1/0/1
ip address 172.1.1.1 255.255.255.0
mpls enable
#
interface GigabitEthernet1/0/2
ip binding vpn-instance vpn1
ip address 10.1.1.2 255.255.255.0
#
bgp 200
peer 2.2.2.9 as-number 100
peer 2.2.2.9 connect-interface LoopBack0
peer 172.1.1.2 as-number 100
#
address-family ipv4 unicast
import-route direct
network 1.1.1.9 255.255.255.255
network 172.1.1.0 255.255.255.0
peer 172.1.1.2 enable
peer 172.1.1.2 route-policy hope export
peer 172.1.1.2 label-route-capability
#
address-family vpnv4
peer 2.2.2.9 enable
peer 2.2.2.9 allow-as-loop 1

```

```

#
ip vpn-instance vpn1
 peer 10.1.1.1 as-number 65410
#
 address-family ipv4 unicast
  import-route direct
  peer 10.1.1.1 enable
#
route-policy hope permit node 0
 apply mpls-label
#
● SPE1:
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 180.1.1.0 0.0.0.255
#
 mpls lsr-id 2.2.2.9
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface GigabitEthernet1/0/1
 ip address 172.1.1.2 255.255.255.0
 mpls enable
#
interface GigabitEthernet1/0/2
 ip address 180.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
bgp 100
 peer 1.1.1.9 as-number 200
 peer 1.1.1.9 connect-interface LoopBack0
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 peer 172.1.1.1 as-number 200
#
 address-family ipv4 unicast
  network 2.2.2.9 255.255.255.255

```

```

peer 172.1.1.1 enable
peer 172.1.1.1 route-policy policy1 export
peer 172.1.1.1 label-route-capability
#
address-family vpnv4
peer 1.1.1.9 enable
peer 1.1.1.9 upe
peer 1.1.1.9 upe route-policy policy2 export
peer 3.3.3.9 enable
#
ip vpn-instance vpn1
#
route-policy policy1 permit node 0
apply mpls-label
#
route-policy policy2 permit node 0
if-match ip address prefix-list list1
#
ip prefix-list list1 index 10 permit 172.16.3.0 24

```

- **UPE2:**

```

#
ip vpn-instance vpn1
route-distinguisher 100:1
vpn-target 100:1 import-extcommunity
vpn-target 100:1 export-extcommunity
#
mpls lsr-id 4.4.4.9
#
interface LoopBack0
ip address 4.4.4.9 255.255.255.255
#
interface GigabitEthernet1/0/1
ip address 172.2.1.1 255.255.255.0
mpls enable
#
interface GigabitEthernet1/0/2
ip binding vpn-instance vpn1
ip address 10.2.1.2 255.255.255.0
#
bgp 200
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack0
peer 172.2.1.2 as-number 100
#
address-family ipv4 unicast
network 4.4.4.9 255.255.255.255
peer 172.2.1.2 enable
peer 172.2.1.2 route-policy hope export

```

```

    peer 172.2.1.2 label-route-capability
#
address-family vpnv4
    peer 3.3.3.9 enable
    peer 3.3.3.9 allow-as-loop 1
#
ip vpn-instance vpn1
    peer 10.2.1.1 as-number 65420
#
address-family ipv4 unicast
    import-route direct
    peer 10.2.1.1 enable
#
route-policy hope permit node 0
    apply mpls-label

```

- **SPE2:**

```

#
ip vpn-instance vpn1
    route-distinguisher 100:1
    vpn-target 100:1 import-extcommunity
    vpn-target 100:1 export-extcommunity
#
ospf 1
    area 0.0.0.0
        network 3.3.3.9 0.0.0.0
        network 180.1.1.0 0.0.0.255
#
mpls lsr-id 3.3.3.9
#
mpls ldp
#
interface LoopBack0
    ip address 3.3.3.9 255.255.255.255
#
interface GigabitEthernet1/0/1
    ip address 172.2.1.2 255.255.255.0
    mpls enable
#
interface GigabitEthernet1/0/2
    ip address 180.1.1.2 255.255.255.0
    mpls enable
    mpls ldp enable
#
bgp 100
    router-id 3.3.3.9
    peer 2.2.2.9 as-number 100
    peer 2.2.2.9 connect-interface LoopBack0
    peer 4.4.4.9 as-number 200

```

```
peer 4.4.4.9 connect-interface LoopBack0
peer 172.2.1.1 as-number 200
#
address-family ipv4 unicast
  network 3.3.3.9 255.255.255.255
  peer 172.2.1.1 enable
  peer 172.2.1.1 route-policy policy1 export
  peer 172.2.1.1 label-route-capability
#
address-family vpnv4
  peer 2.2.2.9 enable
  peer 4.4.4.9 enable
  peer 4.4.4.9 upe
  peer 4.4.4.9 upe route-policy policy2 export
#
ip vpn-instance vpn1
#
route-policy policy1 permit node 0
  apply mpls-label
#
route-policy policy2 permit node 0
  if-match ip address prefix-list list1
#
ip prefix-list list1 index 10 permit 172.16.1.0 24
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“MPLS 配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“MPLS 命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

H3C MSR 系列路由器

MPLS TE 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	2
3 使用 RSVP-TE 配置 MPLS TE 隧道典型配置举例.....	3
3.1 组网需求.....	3
3.2 配置思路.....	3
3.3 使用版本.....	3
3.4 配置注意事项.....	4
3.5 配置步骤.....	4
3.6 验证配置.....	9
3.7 配置文件.....	13
4 MPLS TE FRR 典型配置举例.....	16
4.1 组网需求.....	16
4.2 配置思路.....	17
4.3 使用版本.....	17
4.4 配置注意事项.....	17
4.5 配置步骤.....	18
4.6 验证配置.....	26
4.7 配置文件.....	30
5 相关资料.....	34

1 简介

MPLS TE (Traffic Engineering, 流量工程) 结合了 MPLS 技术与流量工程, 通过建立沿着指定路径的 LSP 隧道进行资源预留 (这种 LSP 也称为 CRLSP, 即基于约束路由的 LSP), 使网络流量绕开拥塞节点, 达到平衡网络流量的目的。

1. 使用 RSVP-TE 建立 CRLSP

MPLS TE 可以通过静态和动态两种方式建立 CRLSP:

- 静态方式是指: 在流量经过的每一跳设备上 (包括 Ingress、Transit 和 Egress) 分别手工指定入标签、出标签、流量所需的带宽等信息, 从而建立满足约束条件的 CRLSP。静态方式的优点是配置简单, 缺点是不能根据网络的变化动态调整建立的 CRLSP;
- 动态方式是指: 根据链路状态信息计算出路径后, 通过标签分发协议 (如 RSVP-TE) 通告标签, 并在经过的节点上为流量预留所需的带宽资源, 从而建立满足约束条件的 CRLSP。该方式的优点是能根据网络的变化动态调整建立的 CRLSP, 且支持 CRLSP 备份、快速重路由等功能, 缺点是配置复杂。

本文着重介绍通过 RSVP-TE 动态建立 CRLSP, 从而建立 MPLS TE 隧道的典型配置举例。

2. MPLS TE FRR

MPLS TE 中有两种网络保护技术, 分别是 FRR 和 CRLSP 备份:

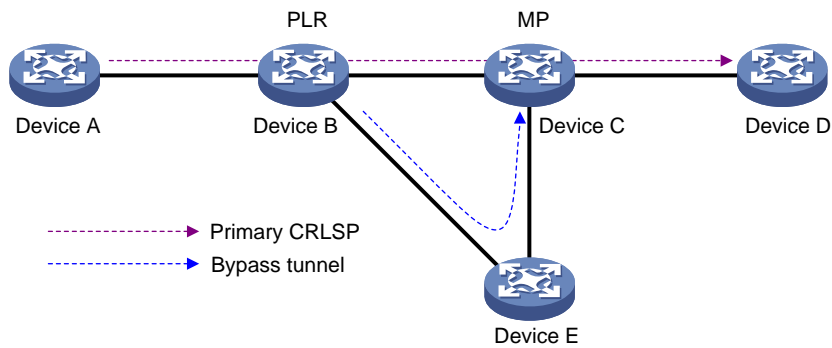
- FRR (Fast Reroute, 快速重路由) 是 MPLS TE 中实现网络局部保护的技术。开启隧道的 FRR 功能后, 当主 CRLSP 上的某条链路或某个节点失效时, 流量会被切换到 Bypass 隧道上。同时, 隧道的 Ingress 节点尝试建立新的 CRLSP。新的 CRLSP 建立成功后, 流量将切换到新的 CRLSP。FRR 的切换速度可以达到 50ms, 能够最大程度减少网络故障时数据的丢失。
- CRLSP 备份是指通过备份 CRLSP 对主 CRLSP 进行保护。当 Ingress 节点感知到主 CRLSP 不可用时, 将流量切换到备份 CRLSP 上, 当主 CRLSP 路径恢复后再将流量切换回来, 实现对主 CRLSP 的备份保护。

FRR 和 CRLSP 备份的不同之处在于: CRLSP 备份是一种端到端的路径保护, 对整条 CRLSP 提供保护, 而 FRR 则是一种局部保护措施, 只能保护 CRLSP 中的某条链路或某个节点。并且, FRR 是一种快速响应的临时性保护措施, 对于切换时间有严格要求, CRLSP 备份则没有时间要求。在实际应用中是配置 FRR 还是 CRLSP 备份, 可以根据上述两种技术的特点来进行选择。本文将介绍 FRR 的典型应用。

根据保护的對象不同, FRR 分为两类:

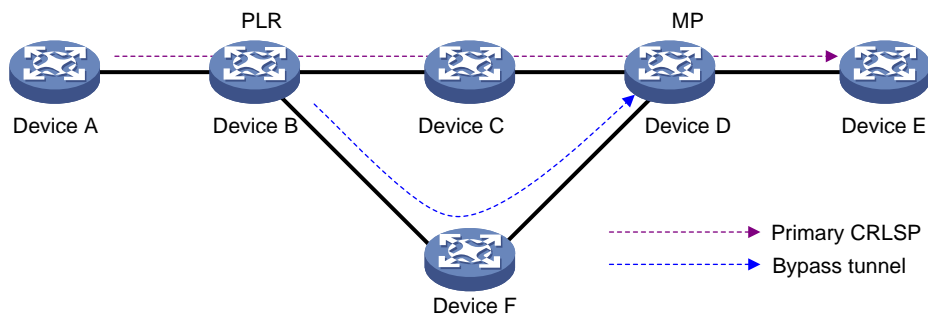
- 链路保护: 又称为 Next-hop (NHOP) 保护。PLR (Point of Local Repair, 本地修复节点) 和 MP (Merge Point, 汇聚点) 之间有直接链路连接, 主 CRLSP 经过这条链路。当这条链路失效时, 流量可以切换到 Bypass 隧道上。如图 1 所示, 主 CRLSP 是 Device A → Device B → Device C → Device D, Bypass 隧道是 Device B → Device E → Device C。

图1 FRR 链路保护示意图



- 节点保护：又称为 Next-next-hop (NNHOP) 保护。PLR 和 MP 之间通过一台设备连接，主 CRLSP 经过这台设备。当这台设备失效时，流量可以切换到 Bypass 隧道上。如图 2 所示，主 CRLSP 是 Device A→Device B→Device C→Device D→Device E，Bypass 隧道是 Device B→Device F→Device D，Device C 是被保护的设备。

图2 FRR 节点保护技术示意图



本文着重介绍链路保护的 MPLS TE FRR 典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 MPLS TE 特性。

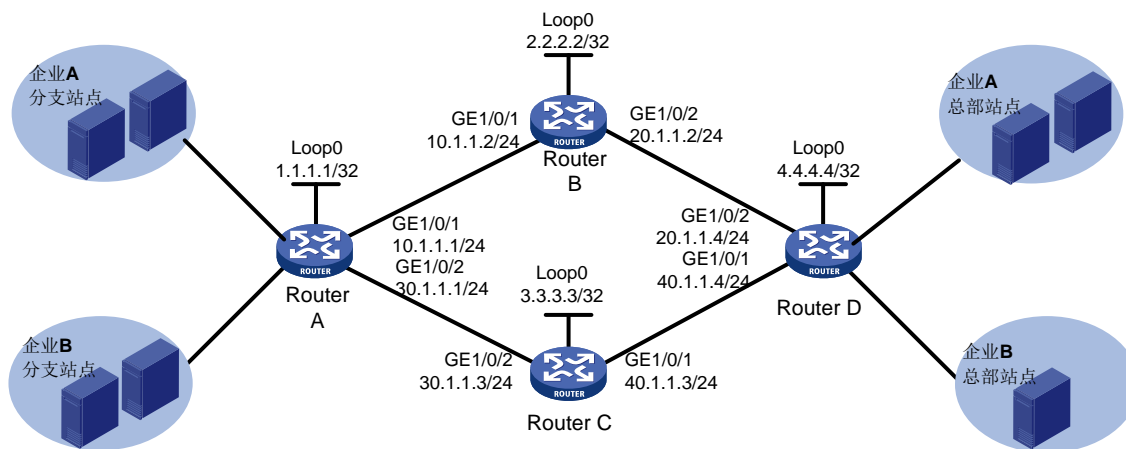
3 使用 RSVP-TE 配置 MPLS TE 隧道典型配置举例

3.1 组网需求

如图 3 所示，企业 A 和企业 B 分别有总部和分支机构两个站点，均通过运营商的 MPLS 网络进行互联。两企业的分支机构均有重要数据，需要穿越 MPLS 网络备份到总部服务器上。企业 A 的数据流量的最大带宽为 20000kbps，企业 B 的数据流量的最大带宽为 30000kbps。

MPLS 网络环境中，每条链路的最大带宽为 50000kbps，最大可预留带宽为 40000kbps，可通过部署 RSVP-TE 服务，自动为两个用户分别建立满足其带宽需求的 MPLS TE 隧道。

图3 使用 RSVP-TE 配置 MPLS TE 隧道典型配置举例组网图



3.2 配置思路

- 为了使用 RSVP-TE 配置 MPLS TE 隧道，需要在骨干网的设备上配置 MPLS、MPLS TE 和 RSVP-TE 功能。
- 为了满足两个企业用户同时在运营商 MPLS 网络中传输数据，并且拥有足够的隧道带宽，需要在 MPLS TE 隧道的 Ingress 节点上为两个用户分别创建 Tunnel 接口，并指定隧道带宽。
- 为了保证每条链路具有足够的带宽和最大可预留带宽，需要在 MPLS TE 隧道经过的各个接口上配置链路的 MPLS TE 属性，指定链路最大带宽和最大可预留带宽。
- 为了在各个节点上生成 TEDB，从而计算出到达某个节点的符合约束条件的最短路径，需要在骨干网中配置 OSPF 支持 MPLS TE，以便各个节点通过 OSPF 路由协议发布链路的 MPLS TE 相关属性。
- 为了实现使用 RSVP-TE 分发 MPLS TE 标签并建立 CRLSP，需要在 MPLS TE 隧道的 Ingress 节点上配置通过 RSVP-TE 自动建立 CRLSP。
- 为了使流量沿着 MPLS TE 隧道转发，需要在 MPLS TE 隧道的 Ingress 节点上配置静态路由，将流量引入 MPLS TE 隧道。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

在采用 RSVP-TE 动态建立 CRLSP 时,必须配置 IGP 的 TE 扩展(目前支持 OSPF TE 和 ISIS TE),否则,不能形成 TEDB (TE DataBase, 流量工程数据库)。在不配置 IGP 的 TE 扩展时计算出的路径是由 IGP 路由得到的,而不是 CSPF (Constraint-based Shortest Path First, 基于约束的最短路径优先) 计算出来的。

3.5 配置步骤

(1) 配置各接口的 IP 地址

按照图 3 配置各接口的 IP 地址和掩码,包括 LoopBack 接口,具体配置过程略。

(2) 配置 OSPF 协议,以保证各路由器之间路由可达

配置 Router A。

```
<RouterA> System-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
<RouterB> System-view
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
<RouterC> System-view
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 Router D。

```
<RouterD> System-view
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
```

```
[RouterD-ospf-1-area-0.0.0.0] quit
```

```
[RouterD-ospf-1] quit
```

配置完成后，在各路由器上执行 **display ip routing-table** 命令，可以看到相互之间都学到了对方的主机路由，包括 Loopback 接口对应的主机路由。以 Router A 为例：

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

```
Destinations : 21          Routes : 21
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.2/32	O_INTRA	10	1	10.1.1.2	GE1/0/1
3.3.3.3/32	O_INTRA	10	1	30.1.1.3	GE1/0/2
4.4.4.4/32	O_INTRA	10	2	10.1.1.2	GE1/0/1
10.1.1.0/24	Direct	0	0	10.1.1.1	GE1/0/1
10.1.1.0/32	Direct	0	0	10.1.1.1	GE1/0/1
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.1	GE1/0/1
20.1.1.0/24	O_INTRA	10	2	10.1.1.2	GE1/0/1
30.1.1.0/24	Direct	0	0	30.1.1.1	GE1/0/2
30.1.1.0/32	Direct	0	0	30.1.1.1	GE1/0/2
30.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.255/32	Direct	0	0	30.1.1.1	GE1/0/2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

(3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.1
```

```
[RouterA] mpls te
```

```
[RouterA-te] quit
```

```
[RouterA] rsvp
```

```
[RouterA-rsvp] quit
```

```
[RouterA] interface gigabitethernet 1/0/1
```

```
[RouterA-GigabitEthernet1/0/1] mpls enable
```

```
[RouterA-GigabitEthernet1/0/1] mpls te enable
```

```
[RouterA-GigabitEthernet1/0/1] rsvp enable
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

```
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] mpls enable
```

```
[RouterA-GigabitEthernet1/0/2] mpls te enable
```

```
[RouterA-GigabitEthernet1/0/2] rsvp enable
```

```
[RouterA-GigabitEthernet1/0/2] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] mpls enable
[RouterB-GigabitEthernet1/0/1] mpls te enable
[RouterB-GigabitEthernet1/0/1] rsvp enable
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] mpls enable
[RouterB-GigabitEthernet1/0/2] mpls te enable
[RouterB-GigabitEthernet1/0/2] rsvp enable
[RouterB-GigabitEthernet1/0/2] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.3
[RouterC] mpls te
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] mpls enable
[RouterC-GigabitEthernet1/0/1] mpls te enable
[RouterC-GigabitEthernet1/0/1] rsvp enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] mpls enable
[RouterC-GigabitEthernet1/0/2] mpls te enable
[RouterC-GigabitEthernet1/0/2] rsvp enable
[RouterC-GigabitEthernet1/0/2] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 4.4.4.4
[RouterD] mpls te
[RouterD-te] quit
[RouterD] rsvp
[RouterD-rsvp] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] mpls enable
[RouterD-GigabitEthernet1/0/1] mpls te enable
[RouterD-GigabitEthernet1/0/1] rsvp enable
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] mpls enable
[RouterD-GigabitEthernet1/0/2] mpls te enable
[RouterD-GigabitEthernet1/0/2] rsvp enable
[RouterD-GigabitEthernet1/0/2] quit
```

(4) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterA-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] mpls te max-link-bandwidth 50000
[RouterA-GigabitEthernet1/0/2] mpls te max-reservable-bandwidth 40000
[RouterA-GigabitEthernet1/0/2] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet1/0/2] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet1/0/2] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet1/0/2] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet1/0/2] quit
```

在 Router D 上配置链路的最大带宽和最大可预留带宽。

```
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterD-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterD-GigabitEthernet1/0/1] quit
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] mpls te max-link-bandwidth 50000
[RouterD-GigabitEthernet1/0/2] mpls te max-reservable-bandwidth 40000
[RouterD-GigabitEthernet1/0/2] quit
```

(5) 配置 OSPF TE，发布链路的 MPLS TE 属性

在 Router A 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterA] ospf
[RouterA-ospf-1] opaque-capability enable
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] mpls te enable
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```


在 Router B 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterB] ospf
[RouterB-ospf-1] opaque-capability enable
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] mpls te enable
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

在 Router C 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterC] ospf
[RouterC-ospf-1] opaque-capability enable
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] mpls te enable
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

在 Router D 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterD] ospf
[RouterD-ospf-1] opaque-capability enable
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] mpls te enable
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

(6) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel1，用于传输企业 A 的数据：目的地址为 Router D 的 LSR ID（4.4.4.4）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需的带宽为 20000kbps；开启路由记录功能。

```
[RouterA] interface tunnel 1 mode mpls-te
[RouterA-Tunnel1] ip address 7.1.1.1 255.255.255.0
[RouterA-Tunnel1] destination 4.4.4.4
[RouterA-Tunnel1] mpls te signaling rsvp-te
[RouterA-Tunnel1] mpls te bandwidth 20000
[RouterA-Tunnel1] mpls te record-route
[RouterA-Tunnel1] quit
```

在 Router A 上配置 MPLS TE 隧道 Tunnel2，用于传输企业 B 的数据：目的地址为 Router D 的 LSR ID（4.4.4.4）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需的带宽为 30000kbps；开启路由记录功能。

```
[RouterA] interface tunnel 2 mode mpls-te
[RouterA-Tunnel2] ip address 8.1.1.1 255.255.255.0
[RouterA-Tunnel2] destination 4.4.4.4
[RouterA-Tunnel2] mpls te signaling rsvp-te
[RouterA-Tunnel2] mpls te bandwidth 30000
[RouterA-Tunnel2] mpls te record-route
[RouterA-Tunnel2] quit
```

(7) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 20.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel1 转发。

```
[RouterA] ip route-static 20.1.1.0 24 tunnel 1 preference 1
```

在 Router A 上配置静态路由，使得到达网络 40.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel2 转发。

```
[RouterA] ip route-static 40.1.1.0 24 tunnel 2 preference 1
```

3.6 验证配置

配置完成后，在 Router A 上执行 **display interface tunnel** 命令可以看到 2 个隧道接口的状态为 UP。

```
[RouterA] display interface tunnel
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 7.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Tunnel2
Current state: UP
Line protocol state: UP
Description: Tunnel2 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 8.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
```

Input: 0 packets, 0 bytes, 0 drops

Output: 0 packets, 0 bytes, 0 drops

在 Router A 上执行 **display mpls te tunnel-interface** 命令可以看到 2 条隧道的详细信息。

```
[RouterA] display mpls te tunnel-interface
```

```
Tunnel Name          : Tunnel 1
Tunnel State         : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes    :
  LSP ID              : 46362          Tunnel ID            : 1
  Admin State         : Normal
  Ingress LSR ID     : 1.1.1.1        Egress LSR ID       : 4.4.4.4
  Signaling           : RSVP-TE       Static CRLSP Name   : -
  Resv Style          : SE
  Tunnel mode         : -
  Reverse-LSP name    : -
  Reverse-LSP LSR ID : -             Reverse-LSP Tunnel ID: -
  Class Type          : CT0           Tunnel Bandwidth     : 20000 kbps
  Reserved Bandwidth : 20000 kbps
  Setup Priority      : 7             Holding Priority     : 7
  Affinity Attr/Mask : 0/0
  Explicit Path       : -
  Backup Explicit Path : -
  Metric Type         : TE
  Record Route        : Enabled       Record Label         : Disabled
  FRR Flag            : Disabled      Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled     Backup Bandwidth Type: -
  Backup Bandwidth    : -
  Bypass Tunnel       : No           Auto Created         : No
  Route Pinning       : Disabled
  Retry Limit         : 3            Retry Interval       : 2 sec
  Reoptimization      : Disabled     Reoptimization Freq : -
  Backup Type         : None         Backup LSP ID        : -
  Auto Bandwidth      : Disabled     Auto Bandwidth Freq : -
  Min Bandwidth       : -           Max Bandwidth        : -
  Collected Bandwidth : -
```

```
Tunnel Name          : Tunnel 2
Tunnel State         : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes    :
  LSP ID              : 46362          Tunnel ID            : 2
  Admin State         : Normal
  Ingress LSR ID     : 1.1.1.1        Egress LSR ID       : 4.4.4.4
  Signaling           : RSVP-TE       Static CRLSP Name   : -
  Resv Style          : SE
  Tunnel mode         : -
  Reverse-LSP name    : -
  Reverse-LSP LSR ID : -             Reverse-LSP Tunnel ID: -
  Class Type          : CT0           Tunnel Bandwidth     : 30000 kbps
```

```

Reserved Bandwidth   : 30000 kbps
Setup Priority       : 7                Holding Priority    : 7
Affinity Attr/Mask  : 0/0
Explicit Path       : -
Backup Explicit Path : -
Metric Type         : TE
Record Route        : Enabled           Record Label         : Disabled
FRR Flag            : Disabled          Bandwidth Protection : Disabled
Backup Bandwidth Flag: Disabled         Backup Bandwidth Type: -
Backup Bandwidth    : -
Bypass Tunnel       : No                Auto Created         : No
Route Pinning       : Disabled
Retry Limit         : 3                 Retry Interval       : 2 sec
Reoptimization      : Disabled          Reoptimization Freq : -
Backup Type         : None              Backup LSP ID        : -
Auto Bandwidth      : Disabled          Auto Bandwidth Freq  : -
Min Bandwidth       : -                 Max Bandwidth        : -
Collected Bandwidth : -

```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel1 和 Tunnel2 为出接口的静态路由信息。

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

```
Destinations : 30          Routes : 30
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.2/32	O_INTRA	10	1	10.1.1.2	GE1/0/1
3.3.3.3/32	O_INTRA	10	1	30.1.1.3	GE1/0/2
4.4.4.4/32	O_INTRA	10	2	10.1.1.2	GE1/0/1
7.1.1.0/24	Direct	0	0	7.1.1.1	Tun1
7.1.1.0/32	Direct	0	0	7.1.1.1	Tun1
7.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
7.1.1.255/32	Direct	0	0	7.1.1.1	Tun1
8.1.1.0/24	Direct	0	0	8.1.1.1	Tun2
8.1.1.0/32	Direct	0	0	8.1.1.1	Tun2
8.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
8.1.1.255/32	Direct	0	0	8.1.1.1	Tun2
10.1.1.0/24	Direct	0	0	10.1.1.1	GE1/0/1
10.1.1.0/32	Direct	0	0	10.1.1.1	GE1/0/1
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.1	GE1/0/1
20.1.1.0/24	Static	1	0	0.0.0.0	Tun1
30.1.1.0/24	Direct	0	0	30.1.1.1	GE1/0/2
30.1.1.0/32	Direct	0	0	30.1.1.1	GE1/0/2
30.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.255/32	Direct	0	0	30.1.1.1	GE1/0/2
40.1.1.0/24	Static	1	0	0.0.0.0	Tun2

```

127.0.0.0/8          Direct 0 0          127.0.0.1          InLoop0
127.0.0.0/32        Direct 0 0          127.0.0.1          InLoop0
127.0.0.1/32        Direct 0 0          127.0.0.1          InLoop0
127.255.255.255/32 Direct 0 0          127.0.0.1          InLoop0
224.0.0.0/4         Direct 0 0          0.0.0.0            NULL0
224.0.0.0/24        Direct 0 0          0.0.0.0            NULL0
255.255.255.255/32 Direct 0 0          127.0.0.1          InLoop0

```

在 Router A 上执行 **display rsvp lsp verbose** 命令，可以看到 Tunnel 1 的 CRLSP 使用了 Router A—Router B—Router D 的路径；Tunnel 2 的 CRLSP 使用了 Router A—Router C—Router D 的路径。

```
[RouterA] display rsvp lsp verbose
```

```
Tunnel name: RouterA_t1
```

```

Destination: 4.4.4.4          Source: 1.1.1.1
Tunnel ID: 1                  LSP ID: 46362
LSR type: Ingress            Direction: Unidirectional
Setup priority: 7             Holding priority: 7
In-Label: -                   Out-Label: 1150
In-Interface: -              Out-Interface: GE1/0/1
Nexthop: 10.1.1.2            Exclude-any: 0
Include-Any: 0                Include-all: 0
Mean rate (CIR): 20000 kbps   Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                Class type: CT0

```

```
RRO number: 6
```

```

10.1.1.1/32      Flag: 0x00 (No FRR)
10.1.1.2/32      Flag: 0x40 (No FRR/In-Int)
2.2.2.2/32       Flag: 0x20 (No FRR/Node-ID)
20.1.1.2/32      Flag: 0x00 (No FRR)
20.1.1.4/32      Flag: 0x40 (No FRR/In-Int)
4.4.4.4/32       Flag: 0x20 (No FRR/Node-ID)

```

```
Fast Reroute protection: None
```

```
Tunnel name: RouterA_t2
```

```

Destination: 4.4.4.4          Source: 1.1.1.1
Tunnel ID: 2                  LSP ID: 46362
LSR type: Ingress            Direction: Unidirectional
Setup priority: 7             Holding priority: 7
In-Label: -                   Out-Label: 1150
In-Interface: -              Out-Interface: GE1/0/2
Nexthop: 30.1.1.3            Exclude-any: 0
Include-Any: 0                Include-all: 0
Mean rate (CIR): 30000 kbps   Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                Class type: CT0

```

```
RRO number: 6
```

```

30.1.1.1/32      Flag: 0x00 (No FRR)
30.1.1.3/32      Flag: 0x40 (No FRR/In-Int)
3.3.3.3/32       Flag: 0x20 (No FRR/Node-ID)
40.1.1.3/32      Flag: 0x00 (No FRR)
40.1.1.4/32      Flag: 0x40 (No FRR/In-Int)

```

Fast Reroute protection: None

经过验证,可以看到通过部署 RSVP-TE 服务,自动为两个用户分别建立了两条 CRLSP:经过 Router A—Router B—Router D 的带宽为 20000kbps 的 CRLSP 和经过 Router A—Router C—Router D 的带宽为 30000kbps 的 CRLSP。

3.7 配置文件

- Router A

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
 mpls te enable
#
 mpls lsr-id 1.1.1.1
#
 mpls te
#
 rsvp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 30.1.1.1 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Tunnel1 mode mpls-te
 ip address 7.1.1.1 255.255.255.0
 mpls te bandwidth ct0 20000
 mpls te record-route
```

```

destination 4.4.4.4
#
interface Tunnel2 mode mpls-te
ip address 8.1.1.1 255.255.255.0
mpls te bandwidth ct0 30000
mpls te record-route
destination 4.4.4.4
#
ip route-static 20.1.1.0 24 Tunnel1 preference 1
ip route-static 40.1.1.0 24 Tunnel2 preference 1
#

```

- **Router B**

```

#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
mpls te enable
#
mpls lsr-id 2.2.2.2
#
mpls te
#
rsvp
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.1.1.2 255.255.255.0
mpls enable
mpls te enable
mpls te max-link-bandwidth 50000
mpls te max-reservable-bandwidth 40000
rsvp enable
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 20.1.1.2 255.255.255.0
mpls enable
mpls te enable
mpls te max-link-bandwidth 50000
mpls te max-reservable-bandwidth 40000
rsvp enable
#

```

- **Router C**

```

#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 30.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  mpls te enable
#
mpls lsr-id 3.3.3.3
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 40.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 30.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#

```

- **Router D**

```

#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  mpls te enable
#
mpls lsr-id 4.4.4.4
#
mpls te
#

```



```

rsvp
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 40.1.1.4 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.1.1.4 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#

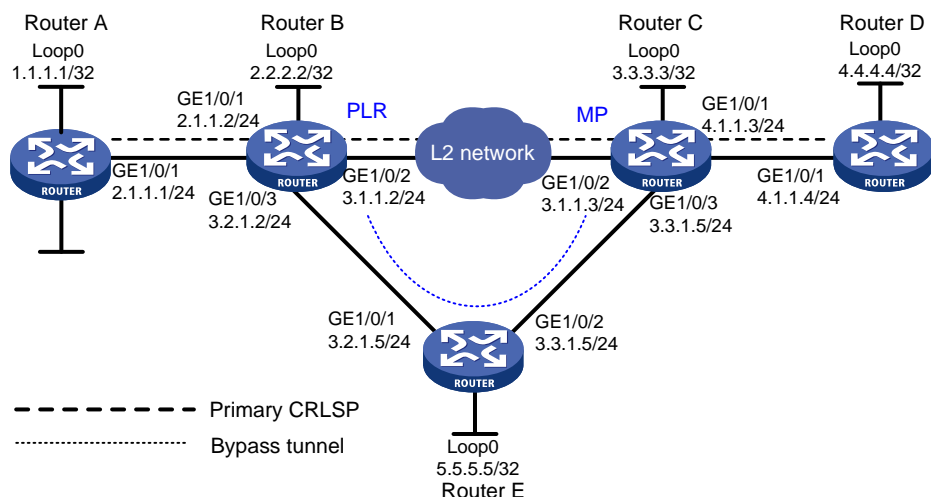
```

4 MPLS TE FRR 典型配置举例

4.1 组网需求

如图 4 所示，Router A->Router B->Router C->Router D 之间建立了一条 CRLSP，承载着某公司的语音业务。由于 Router B 和 Router C 两台路由器相隔较远，中间连有多台二层交换机，链路不太稳定，可能会发生故障，现要求使用 MPLS TE FRR 功能对 Router B->Router C 这段链路进行保护，当链路出现故障时，能快速切换到 Bypass CRLSP（Router A->Router B->Router E->Router C->Router D）。（假设 Primary 隧道和 Bypass 隧道的所需带宽均为 30000kbps；每条链路的最大带宽为 50000kbps，最大可预留带宽为 40000kbps）

图4 MPLS TE FRR 典型配置举例组网图



4.2 配置思路

- 为建立主备 CRLSP，需要在各 Router 上使能 MPLS、MPLS TE 和 RSVP-TE 基本能力。
- 由于组网需求中已经明确主 CRLSP 的路径和 Bypass CRLSP 的路径，需要通过显式路径的方式指定 MPLS TE 的主 CRLSP 和 Bypass CRLSP。
- 为实现被保护的主 CRLSP 链路发生故障后，PLR 能快速感知到，需要在主 CRLSP 保护链路两端的节点上（Router B 和 Router C）配置 BFD 联动 RSVP-TE，使 BFD 能够快速检测并通告 RSVP-TE 协议，以便将流量快速切换到 Bypass 隧道。
- 为实现当 BFD 检测到被保护链路故障后，主 CRLSP 上的流量能快速切换到 Bypass CRLSP，需在主 CRLSP 的 Ingress 节点上使能 MPLS TE FRR 功能。
- 为了保证主 CRLSP 链路故障时，MPLS TE 能在多条 Bypass 隧道可能同时并存的情况下，选择出最优的 Bypass 隧道，需要在 PLR 节点上配置 FRR 的 Bypass 隧道的优选时间间隔为 5 秒（缺省为 300 秒）。

4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.4 配置注意事项

- 只有使用 RSVP-TE 信令协议建立的 MPLS TE 隧道支持 FRR 功能。
- 不要在同一个接口同时配置快速重路由功能和 RSVP 认证功能。
- 由于 FRR 使用的 Bypass 隧道需要预先建立，占用额外的带宽，因此，在网络带宽余量不多的情况下，应该只对关键的接口或链路进行快速重路由保护。
- 用户在配置时应保证 Bypass 隧道的带宽不小于被保护的所有主 CRLSP 所需带宽之和，否则可能导致部分主 CRLSP 不能被 Bypass 隧道保护。

- Bypass 隧道一般不转发数据。如果 Bypass 隧道在保护主 CRLSP 的同时转发流量，需要为 Bypass 隧道提供足够的带宽。
- Bypass 隧道不能作为 VPN 等业务的承载隧道。
- 不能为 Bypass 隧道配置快速重路由功能。也就是说，Bypass 隧道不能同时作为主 CRLSP 被其他 Bypass 隧道保护，隧道不能被嵌套保护。
- Bypass 隧道不能经过被保护的接口或节点。
- 不要求带宽保护的主 CRLSP 和提供保护带宽的 Bypass 隧道绑定成功后，主 CRLSP 占用 Bypass 隧道的保护带宽。提供带宽保护的 Bypass 隧道的保护带宽先到先得，需要带宽保护的主 CRLSP 并不能抢占不需要带宽保护的主 CRLSP。
- 发生 FRR 切换后，如果修改 Bypass 隧道的保护带宽，使得保护带宽类型不同、保护带宽不够或者引起 FRR 保护类型(是否为主 CRLSP 提供带宽保护)变化，都将导致主 CRLSP Down。

4.5 配置步骤

- (1) 配置各接口的 IP 地址

按照图 4 配置各接口的 IP 地址和掩码，包括 LoopBack 接口，具体配置过程略。

- (2) 配置 OSPF 协议，以保证各路由器之间路由可达

配置 Router A。

```
<RouterA> System-view
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 2.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
<RouterB> System-view
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 2.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 3.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 3.2.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
<RouterC> System-view
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 3.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 3.3.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 4.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置 Router D。

```
<RouterD> System-view
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] network 4.1.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

配置 Router E。

```
<RouterE> System-view
[RouterE] ospf
[RouterE-ospf-1] area 0
[RouterE-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[RouterE-ospf-1-area-0.0.0.0] network 3.2.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] network 3.3.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] quit
[RouterE-ospf-1] quit
```

配置完成后，在各路由器上执行 **display ip routing-table** 命令，可以看到相互之间都学到了对方的主机路由，包括 Loopback 接口对应的主机路由。以 Router A 为例：

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

```
Destinations : 19
```

```
Routes : 19
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
2.1.1.0/24	Direct	0	0	2.1.1.1	GE1/0/1
2.1.1.0/32	Direct	0	0	2.1.1.1	GE1/0/1
2.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
2.1.1.255/32	Direct	0	0	2.1.1.1	GE1/0/1
2.2.2.2/32	O_INTRA	10	1	2.1.1.2	GE1/0/1
3.1.1.0/24	O_INTRA	10	2	2.1.1.2	GE1/0/1
3.2.1.0/24	O_INTRA	10	2	2.1.1.2	GE1/0/1
3.3.1.0/24	O_INTRA	10	3	2.1.1.2	GE1/0/1
3.3.3.3/32	O_INTRA	10	2	2.1.1.2	GE1/0/1
5.5.5.5/32	O_INTRA	10	2	2.1.1.2	GE1/0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

- (3) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力，并在 Router B 和 Router C 上配置 RSVP-TE 与 BFD 联动，以检测 Router B 和 Router C 之间链路的状态

配置 Router A

```
[RouterA] mpls lsr-id 1.1.1.1
```

```
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mpls enable
[RouterA-GigabitEthernet1/0/1] mpls te enable
[RouterA-GigabitEthernet1/0/1] rsvp enable
[RouterA-GigabitEthernet1/0/1] quit
```

配置 Router B。

```
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls te
[RouterB-te] quit
[RouterB] rsvp
[RouterB-rsvp] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] mpls enable
[RouterB-GigabitEthernet1/0/1] mpls te enable
[RouterB-GigabitEthernet1/0/1] rsvp enable
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] mpls enable
[RouterB-GigabitEthernet1/0/2] mpls te enable
[RouterB-GigabitEthernet1/0/2] rsvp enable
[RouterB-GigabitEthernet1/0/2] rsvp bfd enable
[RouterB-GigabitEthernet1/0/2] quit
[RouterB] interface gigabitethernet 1/0/3
[RouterB-GigabitEthernet1/0/3] mpls enable
[RouterB-GigabitEthernet1/0/3] mpls te enable
[RouterB-GigabitEthernet1/0/3] rsvp enable
[RouterB-GigabitEthernet1/0/3] quit
```

配置 Router C。

```
[RouterC] mpls lsr-id 3.3.3.3
[RouterC] mpls te
[RouterC-te] quit
[RouterC] rsvp
[RouterC-rsvp] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] mpls enable
[RouterC-GigabitEthernet1/0/1] mpls te enable
[RouterC-GigabitEthernet1/0/1] rsvp enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] mpls enable
[RouterC-GigabitEthernet1/0/2] mpls te enable
[RouterC-GigabitEthernet1/0/2] rsvp enable
[RouterC-GigabitEthernet1/0/2] rsvp bfd enable
[RouterC-GigabitEthernet1/0/2] quit
```

```
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] mpls enable
[RouterC-GigabitEthernet1/0/3] mpls te enable
[RouterC-GigabitEthernet1/0/3] rsvp enable
[RouterC-GigabitEthernet1/0/3] quit
```

配置 Router D。

```
[RouterD] mpls lsr-id 4.4.4.4
[RouterD] mpls te
[RouterD-te] quit
[RouterD] rsvp
[RouterD-rsvp] quit
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] mpls enable
[RouterD-GigabitEthernet1/0/1] mpls te enable
[RouterD-GigabitEthernet1/0/1] rsvp enable
[RouterD-GigabitEthernet1/0/1] quit
```

配置 Router E。

```
[RouterE] mpls lsr-id 5.5.5.5
[RouterE] mpls te
[RouterE-te] quit
[RouterE] rsvp
[RouterE-rsvp] quit
[RouterE] interface gigabitethernet 1/0/1
[RouterE-GigabitEthernet1/0/1] mpls enable
[RouterE-GigabitEthernet1/0/1] mpls te enable
[RouterE-GigabitEthernet1/0/1] rsvp enable
[RouterE-GigabitEthernet1/0/1] quit
[RouterE] interface gigabitethernet 1/0/2
[RouterE-GigabitEthernet1/0/2] mpls enable
[RouterE-GigabitEthernet1/0/2] mpls te enable
[RouterE-GigabitEthernet1/0/2] rsvp enable
[RouterE-GigabitEthernet1/0/2] quit
```

(4) 配置链路的 MPLS TE 属性

在 Router A 上配置链路的最大带宽和最大可预留带宽。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterA-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterA-GigabitEthernet1/0/1] quit
```

在 Router B 上配置链路的最大带宽和最大可预留带宽。

```
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet1/0/2] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet1/0/2] quit
```

```
[RouterB] interface gigabitethernet 1/0/3
[RouterB-GigabitEthernet1/0/3] mpls te max-link-bandwidth 50000
[RouterB-GigabitEthernet1/0/3] mpls te max-reservable-bandwidth 40000
[RouterB-GigabitEthernet1/0/3] quit
```

在 Router C 上配置链路的最大带宽和最大可预留带宽。

```
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet1/0/2] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet1/0/2] quit
[RouterC] interface gigabitethernet 1/0/3
[RouterC-GigabitEthernet1/0/3] mpls te max-link-bandwidth 50000
[RouterC-GigabitEthernet1/0/3] mpls te max-reservable-bandwidth 40000
[RouterC-GigabitEthernet1/0/3] quit
```

在 Router D 上配置链路的最大带宽和最大可预留带宽。

```
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterD-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterD-GigabitEthernet1/0/1] quit
```

在 Router E 上配置链路的最大带宽和最大可预留带宽。

```
[RouterE] interface gigabitethernet 1/0/1
[RouterE-GigabitEthernet1/0/1] mpls te max-link-bandwidth 50000
[RouterE-GigabitEthernet1/0/1] mpls te max-reservable-bandwidth 40000
[RouterE-GigabitEthernet1/0/1] quit
[RouterE] interface gigabitethernet 1/0/2
[RouterE-GigabitEthernet1/0/2] mpls te max-link-bandwidth 50000
[RouterE-GigabitEthernet1/0/2] mpls te max-reservable-bandwidth 40000
[RouterE-GigabitEthernet1/0/2] quit
```

(5) 配置 OSPF TE，发布链路的 MPLS TE 属性

Router A 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterA] ospf
[RouterA-ospf-1] opaque-capability enable
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] mpls te enable
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

Router B 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterB] ospf
[RouterB-ospf-1] opaque-capability enable
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] mpls te enable
[RouterB-ospf-1-area-0.0.0.0] quit
```

```
[RouterB-ospf-1] quit
```

Router C 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterC] ospf
```

```
[RouterC-ospf-1] opaque-capability enable
```

```
[RouterC-ospf-1] area 0
```

```
[RouterC-ospf-1-area-0.0.0.0] mpls te enable
```

```
[RouterC-ospf-1-area-0.0.0.0] quit
```

```
[RouterC-ospf-1] quit
```

Router D 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterD] ospf
```

```
[RouterD-ospf-1] opaque-capability enable
```

```
[RouterD-ospf-1] area 0
```

```
[RouterD-ospf-1-area-0.0.0.0] mpls te enable
```

```
[RouterD-ospf-1-area-0.0.0.0] quit
```

```
[RouterD-ospf-1] quit
```

Router E 上使能 OSPF 的 Opaque LSA 发布接收能力（缺省情况下处于开启状态），并在 OSPF 区域 0 内使能 MPLS TE 能力。

```
[RouterE] ospf
```

```
[RouterE-ospf-1] opaque-capability enable
```

```
[RouterE-ospf-1] area 0
```

```
[RouterE-ospf-1-area-0.0.0.0] mpls te enable
```

```
[RouterE-ospf-1-area-0.0.0.0] quit
```

```
[RouterE-ospf-1] quit
```

(6) 在主 CRLSP 的 Ingress 节点 Router A 上建立 MPLS TE 隧道

配置主 CRLSP 的显式路径，缺省采用严格下一跳方式。

```
[RouterA] explicit-path pri-path
```

```
[RouterA-explicit-path-pri-path] nexthop 2.1.1.2
```

```
[RouterA-explicit-path-pri-path] nexthop 3.1.1.3
```

```
[RouterA-explicit-path-pri-path] nexthop 4.1.1.4
```

```
[RouterA-explicit-path-pri-path] nexthop 4.4.4.4
```

```
[RouterA-explicit-path-pri-path] quit
```

配置主 CRLSP 的 MPLS TE 隧道 Tunnel4：目的地址为 Router D 的 LSR ID（4.4.4.4）；采用 RSVP-TE 信令协议建立 MPLS TE 隧道；隧道所需带宽为 30000kbps；隧道引用显式路径 pri-path。

```
[RouterA] interface tunnel4 mode mpls-te
```

```
[RouterA-Tunnel4] ip address 10.1.1.1 255.255.255.0
```

```
[RouterA-Tunnel4] destination 4.4.4.4
```

```
[RouterA-Tunnel4] mpls te signaling rsvp-te
```

```
[RouterA-Tunnel4] mpls te bandwidth 30000
```

```
[RouterA-Tunnel4] mpls te path preference 1 explicit-path pri-path
```

开启 MPLS TE 隧道的 FRR 功能。

```
[RouterA-Tunnel4] mpls te fast-reroute
```

```
[RouterA-Tunnel4] quit
```


配置完成后，在 Router A 上执行 **display interface tunnel** 命令，可以看到 Tunnel4 的状态为 UP。

```
[RouterA] display interface tunnel
Tunnel4
Current state: UP
Line protocol state: UP
Description: Tunnel4 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 10.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

在 Router A 上执行 **display mpls te tunnel-interface** 命令，可以看到隧道接口的详细信息。

```
[RouterA] display mpls te tunnel-interface
Tunnel Name          : Tunnel 4
Tunnel State         : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes   :
  LSP ID              : 37325          Tunnel ID            : 4
  Admin State         : Normal
  Ingress LSR ID     : 1.1.1.1        Egress LSR ID       : 4.4.4.4
  Signaling           : RSVP-TE       Static CRLSP Name   : -
  Resv Style         : SE
  Tunnel mode        : -
  Reverse-LSP name   : -
  Reverse-LSP LSR ID : -             Reverse-LSP Tunnel ID: -
  Class Type         : CT0            Tunnel Bandwidth     : 30000 kbps
  Reserved Bandwidth : 30000 kbps
  Setup Priority     : 7               Holding Priority     : 7
  Affinity Attr/Mask : 0/0
  Explicit Path      : pri-path
  Backup Explicit Path : -
  Metric Type        : TE
  Record Route       : Enabled        Record Label         : Enabled
  FRR Flag           : Enabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled     Backup Bandwidth Type: -
  Backup Bandwidth   : -
  Bypass Tunnel      : No             Auto Created         : No
  Route Pinning      : Disabled
```

```

Retry Limit          : 3          Retry Interval      : 2 sec
Reoptimization      : Disabled    Reoptimization Freq : -
Backup Type         : None        Backup LSP ID       : -
Auto Bandwidth      : Disabled    Auto Bandwidth Freq : -
Min Bandwidth       : -           Max Bandwidth       : -
Collected Bandwidth : -

```

(7) 在作为 PLR 的 Router B 上配置 Bypass 隧道

配置 Bypass 隧道的显式路径。

```

[RouterB] explicit-path by-path
[RouterB-explicit-path-by-path] nexthop 3.2.1.5
[RouterB-explicit-path-by-path] nexthop 3.3.1.3
[RouterB-explicit-path-by-path] nexthop 3.3.3.3
[RouterB-explicit-path-by-path] quit

```

配置 Bypass 隧道 Tunnel5: 目的地址为 Router C 的 LSR ID (3.3.3.3); 采用 RSVP-TE 信令协议建立 MPLS TE 隧道; 隧道所需带宽为 30000kbps; 隧道引用显式路径 by-path。

```

[RouterB] interface tunnel 5 mode mpls-te
[RouterB-Tunnel5] ip address 11.1.1.1 255.255.255.0
[RouterB-Tunnel5] destination 3.3.3.3
[RouterB-Tunnel5] mpls te signaling rsvp-te
[RouterA-Tunnel5] mpls te bandwidth 30000
[RouterB-Tunnel5] mpls te path preference 1 explicit-path by-path

```

配置 Bypass 隧道不对所能保护的带宽总量进行限制, 即不能提供带宽保护。

```

[RouterB-Tunnel5] mpls te backup bandwidth un-limited
[RouterB-Tunnel5] quit

```

将 Bypass 隧道绑定到被保护的接口。

```

[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] mpls te fast-reroute bypass-tunnel tunnel 5
[RouterB-GigabitEthernet1/0/2] quit

```

配置完成后, 在 Router B 上执行 **display interface tunnel** 命令可以看到接口 Tunnel5 的状态为 UP。

```

[RouterB] display interface tunnel
Tunnel5
Current state: UP
Line protocol state: DOWN
Description: Tunnel5 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 11.1.1.1/24 Primary
Tunnel source unknown, destination 3.3.3.3
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec

```

```
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

(8) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由，使得到达网络 4.1.1.0/24 的流量通过 MPLS TE 隧道接口 Tunnel4 转发。

```
[Router A] ip route-static 4.1.1.0 24 tunnel 4 preference 1
```

4.6 验证配置

在所有设备上执行 **display mpls lsp** 命令，可以看到 LSP 表项。在 Router B 上存在两条 LSP，通过 Bypass 隧道保护主 CRLSP。

```
[RouterA] display mpls lsp
```

FEC	Proto	In/Out Label	Interface/Out NHLFE
1.1.1.1/4/37325	RSVP	-/1150	GE1/0/1
2.1.1.2	Local	-/-	GE1/0/1
Tunnel4	Local	-/-	NHLFE1026

```
[RouterB] display mpls lsp
```

FEC	Proto	In/Out Label	Interface/Out NHLFE
1.1.1.1/4/37325	RSVP	1150/1147	GE1/0/2
Backup		1150/1147	Tun5
2.2.2.2/5/18928	RSVP	-/1149	GE1/0/3
3.1.1.3	Local	-/-	GE1/0/2
3.2.1.5	Local	-/-	GE1/0/3
Tunnel5	Local	-/-	NHLFE1027

```
[RouterC] display mpls lsp
```

FEC	Proto	In/Out Label	Interface/Out NHLFE
1.1.1.1/4/37325	RSVP	1147/3	GE1/0/1
2.2.2.2/5/18928	RSVP	3/-	-
4.1.1.4	Local	-/-	GE1/0/1

在 PLR 上 **shutdown** 被保护的出接口 GigabitEthernet1/0/2。

```
[RouterB] interface gigabitethernet 1/0/2
```

```
[RouterB-GigabitEthernet1/0/2] shutdown
```

```
[RouterB-GigabitEthernet1/0/2] quit
```

在 Router A 上执行 **display interface tunnel 4** 命令查看主 CRLSP 的状态，可以看到 Tunnel 接口仍然处于 UP 状态。

```
[RouterA] display interface tunnel 4
```

```
Tunnel4
```

```
Current state: UP
```

```
Line protocol state: UP
```

```
Description: Tunnel4 Interface
```

```
Bandwidth: 64kbps
```

```
Maximum Transmit Unit: 64000
```

```
Internet Address is 10.1.1.1/24 Primary
```

```
Tunnel source unknown, destination 4.4.4.4
```

```
Tunnel TTL 255
```

```
Tunnel protocol/transport CR_LSP
```

```
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
```

```

Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

```

在 Router A 上执行 **display mpls te tunnel-interface** 命令，可以看到隧道接口的详细信息。

```

[RouterA] display mpls te tunnel-interface
Tunnel Name          : Tunnel 4
Tunnel State         : Up (Main CRLSP up, Shared-resource CRLSP being set up)
Tunnel Attributes    :
  LSP ID              : 37325          Tunnel ID           : 4
  Admin State         : Normal
  Ingress LSR ID     : 1.1.1.1        Egress LSR ID      : 4.4.4.4
  Signaling           : RSVP-TE       Static CRLSP Name  : -
  Resv Style          : SE
  Tunnel mode         : -
  Reverse-LSP name    : -
  Reverse-LSP LSR ID : -             Reverse-LSP Tunnel ID: -
  Class Type          : CT0            Tunnel Bandwidth    : 30000 kbps
  Reserved Bandwidth : 30000 kbps
  Setup Priority      : 7              Holding Priority    : 7
  Affinity Attr/Mask : 0/0
  Explicit Path       : pri-path
  Backup Explicit Path : -
  Metric Type         : TE
  Record Route        : Enabled        Record Label        : Enabled
  FRR Flag            : Enabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled      Backup Bandwidth Type: -
  Backup Bandwidth    : -
  Bypass Tunnel       : No             Auto Created        : No
  Route Pinning       : Disabled
  Retry Limit         : 3              Retry Interval      : 2 sec
  Reoptimization      : Disabled       Reoptimization Freq : -
  Backup Type         : None           Backup LSP ID       : -
  Auto Bandwidth      : Disabled       Auto Bandwidth Freq : -
  Min Bandwidth       : -             Max Bandwidth       : -
  Collected Bandwidth : -

```

在 Router B 上执行 **display mpls lsp** 命令，可以看到 Bypass 隧道被使用。

```

[RouterB] display mpls lsp
FEC                Proto  In/Out Label  Interface/Out NHLFE
1.1.1.1/4/37325    RSVP  1150/1147    Tun5
2.2.2.2/5/18928    RSVP  -/1149       GE1/0/3
3.2.1.5            Local  -/-          GE1/0/3
Tunnel5            Local  -/-          NHLFE1027

```

在 PLR 上配置在多条旁路隧道中进行优选的时间间隔为 5 秒。

```
[RouterB] mpls te
[RouterB-te] fast-reroute timer 5
[RouterB-te] quit
```

在 PLR 上 **undo shutdown** 被保护的出接口 GigabitEthernet1/0/2。

```
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] undo shutdown
[RouterB-GigabitEthernet1/0/2] quit
```

在 Router A 上执行 **display interface tunnel 4** 命令查看主 CRLSP 的状态，可以看到 Tunnel 接口处于 up 状态。

```
[RouterA] display interface tunnel 4
Tunnel4
Current state: UP
Line protocol state: UP
Description: Tunnel4 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 64000
Internet Address is 10.1.1.1/24 Primary
Tunnel source unknown, destination 4.4.4.4
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

等待约 5 秒钟后，在 Router B 上执行 **display mpls lsp verbose** 命令，可以看到 Tunnel5 仍绑定到出接口 GigabitEthernet1/0/2，但未被使用。

```
[RouterB] display mpls lsp verbose
Destination : 4.4.4.4
FEC         : 1.1.1.1/4/53319
Protocol    : RSVP
LSR Type    : Transit
Service     : -
In-Label    : 1150
Path ID     : 0x540000003.1
State       : Active
Out-Label   : 1150
Nexthop     : 3.1.1.3
Out-Interface: GE1/0/2
BkLabel     : 1150
BkInterface : Tun5

Destination : 3.3.3.3
FEC         : 2.2.2.2/5/16429
```

```

Protocol      : RSVP
LSR Type      : Ingress
Service       : -
NHLFE ID     : 1025
State         : Active
Out-Label    : 1151
NextHop      : 3.2.1.5
Out-Interface: GE1/0/3

```

```

Destination   : 3.1.1.3
FEC           : 3.1.1.3
Protocol      : Local
LSR Type      : Ingress
Service       : -
NHLFE ID     : 1027
State         : Active
NextHop      : 3.1.1.3
Out-Interface: GE1/0/2

```

```

Destination   : 3.2.1.5
FEC           : 3.2.1.5
Protocol      : Local
LSR Type      : Ingress
Service       : -
NHLFE ID     : 1024
State         : Active
NextHop      : 3.2.1.5
Out-Interface: GE1/0/3

```

```

Destination   : 3.3.3.3
FEC           : Tunnel5
Protocol      : Local
LSR Type      : Ingress
Service       : -
NHLFE ID     : 268435461
State         : Active
Out-Interface: NHLFE1025

```

在 Router A 上执行 **display ip routing-table** 命令，可以看到路由表中有以 Tunnel4 为出接口的静态路由信息。

```

[RouterA] display ip routing-table
Destinations : 25          Routes : 25

```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
2.1.1.0/24	Direct	0	0	2.1.1.1	GE1/0/1
2.1.1.0/32	Direct	0	0	2.1.1.1	GE1/0/1
2.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0

2.1.1.255/32	Direct	0	0	2.1.1.1	GE1/0/1
2.2.2.2/32	O_INTRA	10	1	2.1.1.2	GE1/0/1
3.1.1.0/24	O_INTRA	10	2	2.1.1.2	GE1/0/1
3.2.1.0/24	O_INTRA	10	2	2.1.1.2	GE1/0/1
3.3.1.0/24	O_INTRA	10	3	2.1.1.2	GE1/0/1
3.3.3.3/32	O_INTRA	10	2	2.1.1.2	GE1/0/1
4.1.1.0/24	Static	1	0	0.0.0.0	Tun4
4.4.4.4/32	O_INTRA	10	3	2.1.1.2	GE1/0/1
5.5.5.5/32	O_INTRA	10	2	2.1.1.2	GE1/0/1
10.1.1.0/24	Direct	0	0	10.1.1.1	Tun4
10.1.1.0/32	Direct	0	0	10.1.1.1	Tun4
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.1	Tun4
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

4.7 配置文件

- Router A

```

#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 2.1.1.0 0.0.0.255
 mpls te enable
#
 mpls lsr-id 1.1.1.1
#
mpls te
#
explicit-path pri-path
 nexthop index 1 2.1.1.2 include strict
 nexthop index 101 3.1.1.3 include strict
 nexthop index 201 4.1.1.4 include strict
 nexthop index 301 4.4.4.4 include strict
#
rsvp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode route

```

```

ip address 2.1.1.1 255.255.255.0
mpls enable
mpls te enable
mpls te max-link-bandwidth 50000
mpls te max-reservable-bandwidth 40000
rsvp enable
#
interface Tunnel4 mode mpls-te
ip address 10.1.1.1 255.255.255.0
mpls te bandwidth ct0 30000
mpls te path preference 1 explicit-path pri-path
mpls te fast-reroute
destination 4.4.4.4
#
ip route-static 4.1.1.0 24 Tunnel4 preference 1
#

```

- **Router B**

```

#
ospf 1
area 0.0.0.0
network 2.1.1.0 0.0.0.255
network 2.2.2.2 0.0.0.0
network 3.1.1.0 0.0.0.255
network 3.2.1.0 0.0.0.255
mpls te enable
#
mpls lsr-id 2.2.2.2
#
mpls te
fast-reroute timer 5
#
explicit-path by-path
nexthop index 1 3.2.1.5 include strict
nexthop index 101 3.3.1.3 include strict
nexthop index 201 3.3.3.3 include strict
#
rsvp
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 2.1.1.2 255.255.255.0
mpls enable
mpls te enable
mpls te max-link-bandwidth 50000
mpls te max-reservable-bandwidth 40000

```



```

    rsvp enable
#
interface GigabitEthernet1/0/2
    port link-mode route
    ip address 3.1.1.2 255.255.255.0
    mpls enable
    mpls te enable
    mpls te max-link-bandwidth 50000
    mpls te max-reservable-bandwidth 40000
    mpls te fast-reroute bypass-tunnel Tunnel5
    rsvp enable
    rsvp bfd enable
#
interface GigabitEthernet1/0/3
    port link-mode route
    ip address 3.2.1.2 255.255.255.0
    mpls enable
    mpls te enable
    mpls te max-link-bandwidth 50000
    mpls te max-reservable-bandwidth 40000
    rsvp enable
#
interface Tunnel5 mode mpls-te
    ip address 11.1.1.1 255.255.255.0
    mpls te bandwidth ct0 30000
    mpls te path preference 1 explicit-path by-path
    mpls te backup bandwidth un-limited
    destination 3.3.3.3
#

```

- **Router C**

```

#
ospf 1
    area 0.0.0.0
        network 3.1.1.0 0.0.0.255
        network 3.3.1.0 0.0.0.255
        network 3.3.3.3 0.0.0.0
        network 4.1.1.0 0.0.0.255
    mpls te enable
#
    mpls lsr-id 3.3.3.3
#
mpls te
#
rsvp
#
interface LoopBack0
    ip address 3.3.3.3 255.255.255.255
#

```

```

interface GigabitEthernet1/0/1
  port link-mode route
  ip address 4.1.1.3 255.255.255.0
  mpls enable
  mpls te enable
  mpls te max-link-bandwidth 50000
  mpls te max-reservable-bandwidth 40000
  rsvp enable
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 3.1.1.3 255.255.255.0
  mpls enable
  mpls te enable
  mpls te max-link-bandwidth 50000
  mpls te max-reservable-bandwidth 40000
  rsvp enable
  rsvp bfd enable
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip address 3.3.1.3 255.255.255.0
  mpls enable
  mpls te enable
  mpls te max-link-bandwidth 50000
  mpls te max-reservable-bandwidth 40000
  rsvp enable
#

```

- **Router D**

```

#
ospf 1
  area 0.0.0.0
    network 4.1.1.0 0.0.0.255
    network 4.4.4.4 0.0.0.0
    mpls te enable
#
  mpls lsr-id 4.4.4.4
#
mpls te
#
rsvp
#
interface LoopBack0
  ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 4.1.1.4 255.255.255.0

```

```

mpls enable
mpls te enable
mpls te max-link-bandwidth 50000
mpls te max-reservable-bandwidth 40000
rsvp enable
#
• Router E
#
ospf 1
area 0.0.0.0
network 3.2.1.0 0.0.0.255
network 3.3.1.0 0.0.0.255
network 5.5.5.5 0.0.0.0
mpls te enable
#
mpls lsr-id 5.5.5.5
#
mpls te
#
rsvp
#
interface LoopBack0
ip address 5.5.5.5 255.255.255.255
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 3.2.1.5 255.255.255.0
mpls enable
mpls te enable
mpls te max-link-bandwidth 50000
mpls te max-reservable-bandwidth 40000
rsvp enable
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 3.3.1.5 255.255.255.0
mpls enable
mpls te enable
mpls te max-link-bandwidth 50000
mpls te max-reservable-bandwidth 40000
rsvp enable
#

```

5 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“MPLS 配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“MPLS 命令参考”

H3C MSR 系列路由器

MPLS OAM 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 BFD 检测 LSP 典型配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	2
3.3 配置步骤.....	2
3.4 验证配置.....	6
3.5 配置文件.....	7
4 BFD 检测 MPLS TE 典型配置举例.....	11
4.1 组网需求.....	11
4.2 使用版本.....	11
4.3 配置注意事项.....	12
4.4 配置步骤.....	12
4.5 验证配置.....	15
4.6 配置文件.....	17
5 相关资料.....	21

1 简介

本文档介绍 MPLS OAM 配置举例。

MPLS OAM（Operations, Administration and Maintenance，操作、管理和维护）功能为 MPLS 网络提供了数据平面连通性检测、数据平面与控制平面一致性校验、故障点定位等多种错误管理（Fault Management）工具。MPLS OAM 利用这些错误管理工具对 LSP、MPLS TE 隧道和 MPLS PW 进行检测和故障定位，降低了 MPLS 网络的管理和维护的复杂度，提高了 MPLS 网络的可用性。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 MPLS OAM 特性。

3 BFD 检测 LSP 典型配置举例

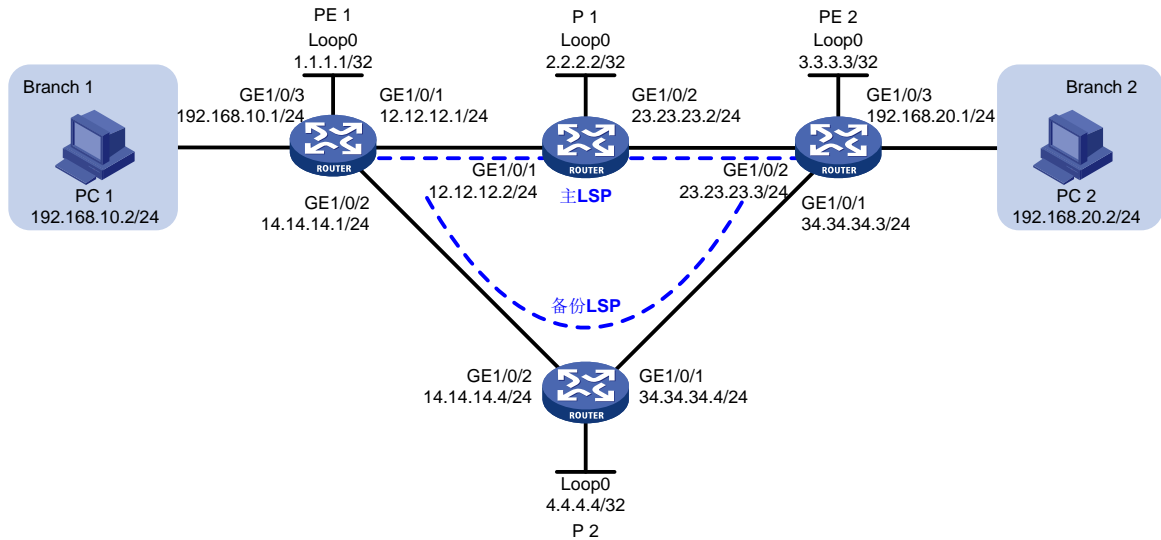
3.1 组网需求

如[图 1](#)所示，某公司有两个位于不同的地理位置的分支机构通过运营商的 MPLS 骨干网互联，两个分支机构之间需要进行实时业务的同步传输。该公司要求运营商提供高可靠性的服务，以保证实时业务的不间断性。

为满足该用户需求，可通过在 MPLS 骨干网中部署 LDP FRR 服务来提供主备两条 LSP 链路，并配置 LDP 与 BFD 联动技术提高主备链路的切换速度，具体实现如下：

- 正常情况下，使用主 LSP 链路转发 PE 1 和 PE 2 之间的流量。
- 使用 BFD 对主链路进行监测，当主链路发生故障时，BFD 能够快速感知并通告 LDP 协议，使得 PE 1 和 PE 2 之间的流量迅速切换到备 LSP 链路进行转发。

图1 BFD 检测 LSP 配置组网图



3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.3 配置步骤

- (1) 配置各接口的 IP 地址

配置 PE 1 接口 GigabitEthernet1/0/1 的 IP 地址。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] ip address 12.12.12.1 24
[PE1-GigabitEthernet1/0/1] quit
```

请参考以上方法配置图 1 中其它接口（包括 LoopBack 接口）的 IP 地址，配置步骤这里省略。

- (2) 在 MPLS 骨干网内配置 OSPF，以保证各路由器之间路由可达，并使能 OSPF 快速重路由功能。

配置 PE 1。

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] fast-reroute lfa
[PE1-ospf-1] quit
```

配置 P 1。

```
[P1] ospf
```

```
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

配置 PE 2。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 34.34.34.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] fast-reroute lfa
[PE2-ospf-1] quit
```

配置 P 2。

```
[P2] ospf
[P2-ospf-1] area 0
[P2-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 34.34.34.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

调整 P 2 上 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 OSPF cost 值，使备份 LSP 路径上的 OSPF 开销值大于主 LSP 路径。

```
[P2] interface gigabitethernet 1/0/1
[P2-GigabitEthernet1/0/1] ospf cost 10
[P2-GigabitEthernet1/0/1] quit
[P2] interface gigabitethernet 1/0/2
[P2-GigabitEthernet1/0/2] ospf cost 10
[P2-GigabitEthernet1/0/2] quit
```

(3) 配置 MPLS 基本能力，并使能 LDP

配置 PE 1。

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] mpls enable
[PE1-GigabitEthernet1/0/1] mpls ldp enable
[PE1-GigabitEthernet1/0/1] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] mpls enable
[PE1-GigabitEthernet1/0/2] mpls ldp enable
[PE1-GigabitEthernet1/0/2] quit
```

配置 P 1。

```
[P1] mpls lsr-id 2.2.2.2
```



```

[P1] mpls ldp
[P1-ldp] quit
[P1] interface gigabitethernet 1/0/1
[P1-GigabitEthernet1/0/1] mpls enable
[P1-GigabitEthernet1/0/1] mpls ldp enable
[P1-GigabitEthernet1/0/1] quit
[P1] interface gigabitethernet 1/0/2
[P1-GigabitEthernet1/0/2] mpls enable
[P1-GigabitEthernet1/0/2] mpls ldp enable
[P1-GigabitEthernet1/0/2] quit

```

配置 PE 2。

```

[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] mpls enable
[PE2-GigabitEthernet1/0/1] mpls ldp enable
[PE2-GigabitEthernet1/0/1] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] mpls enable
[PE2-GigabitEthernet1/0/2] mpls ldp enable
[PE2-GigabitEthernet1/0/2] quit

```

配置 P 2。

```

[P2] mpls lsr-id 4.4.4.4
[P2] mpls ldp
[P2-ldp] quit
[P2] interface gigabitethernet 1/0/1
[P2-GigabitEthernet1/0/1] mpls enable
[P2-GigabitEthernet1/0/1] mpls ldp enable
[P2-GigabitEthernet1/0/1] quit
[P2] interface gigabitethernet 1/0/2
[P2-GigabitEthernet1/0/2] mpls enable
[P2-GigabitEthernet1/0/2] mpls ldp enable
[P2-GigabitEthernet1/0/2] quit

```

完成上述配置后，在各设备上可以看到 LDP 会话的状态为 **operational**，会话建立成功。以 PE1 为例：

```

[PE1] display mpls ldp peer
Total number of peers: 2
Peer LDP ID          State           Role    GR   MD5  KA Sent/Rcvd
2.2.2.2:0            Operational    Passive Off  Off  55/55
4.4.4.4:0            Operational    Passive Off  Off  6/6

```

- (4) 配置 LSP 的触发策略，为目的地址为 192.168.10.0/24、192.168.20.0/24、1.1.1.1/32 和 3.3.3.3/32 的路由表项建立 LSP

在 PE 1 上创建 IP 地址前缀列表 PE1，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```

[PE1] ip prefix-list PE1 index 10 permit 192.168.10.0 24
[PE1] ip prefix-list PE1 index 20 permit 192.168.20.0 24

```

```
[PE1] ip prefix-list PE1 index 30 permit 1.1.1.1 32
[PE1] ip prefix-list PE1 index 40 permit 3.3.3.3 32
[PE1] mpls ldp
[PE1-ldp] lsp-trigger prefix-list PE1
[PE1-ldp] quit
```

在 P 1 上创建 IP 地址前缀列表 P1，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P1] ip prefix-list P1 index 10 permit 192.168.10.0 24
[P1] ip prefix-list P1 index 20 permit 192.168.20.0 24
[P1] ip prefix-list P1 index 30 permit 1.1.1.1 32
[P1] ip prefix-list P1 index 40 permit 3.3.3.3 32
[P1] mpls ldp
[P1-ldp] lsp-trigger prefix-list P1
[P1-ldp] quit
```

在 PE 2 上创建 IP 地址前缀列表 PE 2，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[PE2] ip prefix-list PE2 index 10 permit 192.168.10.0 24
[PE2] ip prefix-list PE2 index 20 permit 192.168.20.0 24
[PE2] ip prefix-list PE2 index 30 permit 1.1.1.1 32
[PE2] ip prefix-list PE2 index 40 permit 3.3.3.3 32
[PE2] mpls ldp
[PE2-ldp] lsp-trigger prefix-list PE2
[PE2-ldp] quit
```

在 P 2 上创建 IP 地址前缀列表 P2，并配置只有通过该列表过滤的路由表项能够触发 LDP 建立 LSP。

```
[P2] ip prefix-list P2 index 10 permit 192.168.10.0 24
[P2] ip prefix-list P2 index 20 permit 192.168.20.0 24
[P2] ip prefix-list P2 index 30 permit 1.1.1.1 32
[P2] ip prefix-list P2 index 40 permit 3.3.3.3 32
[P2] mpls ldp
[P2-ldp] lsp-trigger prefix-list P2
[P2-ldp] quit
```

配置完成后，在 PE 1 上执行 **display mpls ldp lsp** 命令，查看 LDP LSP 的建立情况，可以看到去往 192.168.20.0/24 网段的 LSP 建立完成。

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECS: 4          Ingress: 4          Transit: 4          Egress: 2

FEC                In/Out Label      Nexthop            OutInterface
1.1.1.1/32         3/-
                   -/1151(L)
                   -/1149(L)
3.3.3.3/32         -/1150            12.12.12.2        GE1/0/1
                   1150/1150        12.12.12.2        GE1/0/1
                   -/1150(B)        14.14.14.4        GE1/0/2
                   1150/1150(B)    14.14.14.4        GE1/0/2
192.168.10.0/24   1148/-
```

```

-/1148(L)
-/1148(L)
192.168.20.0/24 -/1147          12.12.12.2      GE1/0/1
                1147/1147        12.12.12.2      GE1/0/1
                -/1147(B)      14.14.14.4      GE1/0/2
                1147/1147(B)    14.14.14.4      GE1/0/2

```

- (5) 使能 MPLS 与 BFD 联动功能，并配置通过 BFD 检测 LSP 的连通性

配置 PE 1。

```

[PE1] mpls bfd enable
[PE1] mpls bfd 3.3.3.3 32

```

配置 PE 2。

```

[PE2] mpls bfd enable
[PE2] mpls bfd 1.1.1.1 32

```

3.4 验证配置

- (1) 配置完成后，在设备 PE 1 和 PE 2 上执行 **display mpls bfd** 命令，可以看到检测 LSP 的 BFD 会话的建立情况。以 PE 1 为例。

```

[PE1] display mpls bfd
Total number of sessions: 2, 2 up, 0 down, 0 init

FEC Type: LSP
FEC Info:
  Destination: 1.1.1.1
  Mask Length: 32
NHLFE ID: -
Local Discr: 513          Remote Discr: 513
Source IP: 1.1.1.1       Destination IP: 3.3.3.3
Session State: Up        Session Role: Active
Template Name: -

```

```

FEC Type: LSP
FEC Info:
  Destination: 3.3.3.3
  Mask Length: 32
NHLFE ID: 1028
Local Discr: 513          Remote Discr: 514
Source IP: 1.1.1.1       Destination IP: 127.0.0.1
Session State: Up        Session Role: Passive
Template Name: -

```

- (2) 在 PE 1 上使用 **tracert mpls ipv4** 命令查看到当前所使用的路径是主 LSP。（使用 Tracert 功能需要在中间设备上开启 ICMP 超时报文发送功能，在目的端开启 ICMP 目的不可达报文发送功能）

```

<PE1> tracert mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS trace route FEC 192.168.20.0/24
  TTL   Replier          Time    Type      Downstream
  0                               Ingress 12.12.12.2/[1141]

```

```

1      12.12.12.2          2 ms    Transit   23.23.23.3/[1141]
2      23.23.23.3          2 ms    Egress

```

- (3) 在 PE 1 上持续 ping PE 2，期间将 P 1 的 GigabitEthernet1/0/1 接口 **shutdown**，查看通信是否中断。

#在 PE 1 上持续 ping PE 2，

```

<PE1> ping -c 100000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=2.576 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=1.996 ms
...

```

关闭 P 1 的 GigabitEthernet1/0/1 接口。

```

[P1] interface gigabitethernet1/0/1
[P1-GigabitEthernet1/0/1] shutdown

```

#在 PE1 上查看到通讯断开后迅速恢复。

```

<PE1> ping -c 100000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=2.576 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=1.996 ms
...
56 bytes from 192.168.20.1: icmp_seq=7 ttl=254 time=2.214 ms
Request time out
56 bytes from 192.168.20.1: icmp_seq=9 ttl=254 time=2.659 ms
56 bytes from 192.168.20.1: icmp_seq=10 ttl=254 time=5.049 ms
56 bytes from 192.168.20.1: icmp_seq=11 ttl=254 time=2.098 ms
56 bytes from 192.168.20.1: icmp_seq=12 ttl=254 time=2.225 ms
56 bytes from 192.168.20.1: icmp_seq=13 ttl=254 time=2.187 ms

```

```

--- Ping statistics for 192.168.20.1 ---
14 packet(s) transmitted, 13 packet(s) received, 7.1% packet loss
round-trip min/avg/max/std-dev = 1.990/2.455/5.049/0.772 ms

```

- (4) 查看链路是否发生切换。

在 PE 1 上使用 **tracert mpls ipv4** 命令查看到当前路径是备份 LSP。

```

<PE1> tracert mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS trace route FEC 192.168.20.0/24

```

TTL	Replier	Time	Type	Downstream
0			Ingress	14.14.14.4/[1133]
1	14.14.14.4	2 ms	Transit	34.34.34.3/[1141]
2	34.34.34.3	2 ms	Egress	

3.5 配置文件

- PE 1


```

#
ospf 1

```

```

fast-reroute lfa
area 0.0.0.0
 network 1.1.1.1 0.0.0.0
 network 12.12.12.0 0.0.0.255
 network 14.14.14.0 0.0.0.255
 network 192.168.10.0 0.0.0.255
#
 mpls lsr-id 1.1.1.1
#
 mpls ldp
 lsp-trigger prefix-list PE1
#
 mpls bfd enable
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 12.12.12.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 14.14.14.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 192.168.10.1 255.255.255.0
#
 ip prefix-list PE1 index 10 permit 192.168.10.0 24
 ip prefix-list PE1 index 20 permit 192.168.20.0 24
 ip prefix-list PE1 index 30 permit 1.1.1.1 32
 ip prefix-list PE1 index 40 permit 3.3.3.3 32

#
 mpls bfd 3.3.3.3 32
#

```

- **PE 2**

```

#
ospf 1
 fast-reroute lfa
area 0.0.0.0
 network 3.3.3.3 0.0.0.0
 network 23.23.23.0 0.0.0.255

```

```

network 34.34.34.0 0.0.0.255
network 192.168.20.0 0.0.0.255
#
mpls lsr-id 3.3.3.3
#
mpls ldp
  lsp-trigger prefix-list PE2
#
mpls bfd enable
#
interface LoopBack0
  ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 34.34.34.3 255.255.255.0
  mpls enable
  mpls ldp enable
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 23.23.23.3 255.255.255.0
  mpls enable
  mpls ldp enable
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip address 192.168.20.1 255.255.255.0
#
ip prefix-list PE2 index 10 permit 192.168.10.0 24
ip prefix-list PE2 index 20 permit 192.168.20.0 24
ip prefix-list PE2 index 30 permit 1.1.1.1 32
ip prefix-list PE2 index 40 permit 3.3.3.3 32

#
mpls bfd 1.1.1.1 32
#
• P 1
#
ospf 1
  area 0.0.0.0
    network 2.2.2.2 0.0.0.0
    network 12.12.12.0 0.0.0.255
    network 23.23.23.0 0.0.0.255
#
mpls lsr-id 2.2.2.2
#
mpls ldp

```

```

lsp-trigger prefix-list P1
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 12.12.12.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 23.23.23.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list P1 index 10 permit 192.168.10.0 24
 ip prefix-list P1 index 20 permit 192.168.20.0 24
 ip prefix-list P1 index 30 permit 1.1.1.1 32
 ip prefix-list P1 index 40 permit 3.3.3.3 32

```

- **P 2**

```

#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 14.14.14.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
#
 mpls lsr-id 4.4.4.4
#
 mpls ldp
  lsp-trigger prefix-list P2
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 34.34.34.4 255.255.255.0
 ospf cost 10
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/2
 port link-mode route

```

```

ip address 14.14.14.4 255.255.255.0
ospf cost 10
mpls enable
mpls ldp enable
#
ip prefix-list P2 index 10 permit 192.168.10.0 24
ip prefix-list P2 index 20 permit 192.168.20.0 24
ip prefix-list P2 index 30 permit 1.1.1.1 32
ip prefix-list P2 index 40 permit 3.3.3.3 32
#

```

4 BFD 检测 MPLS TE 典型配置举例

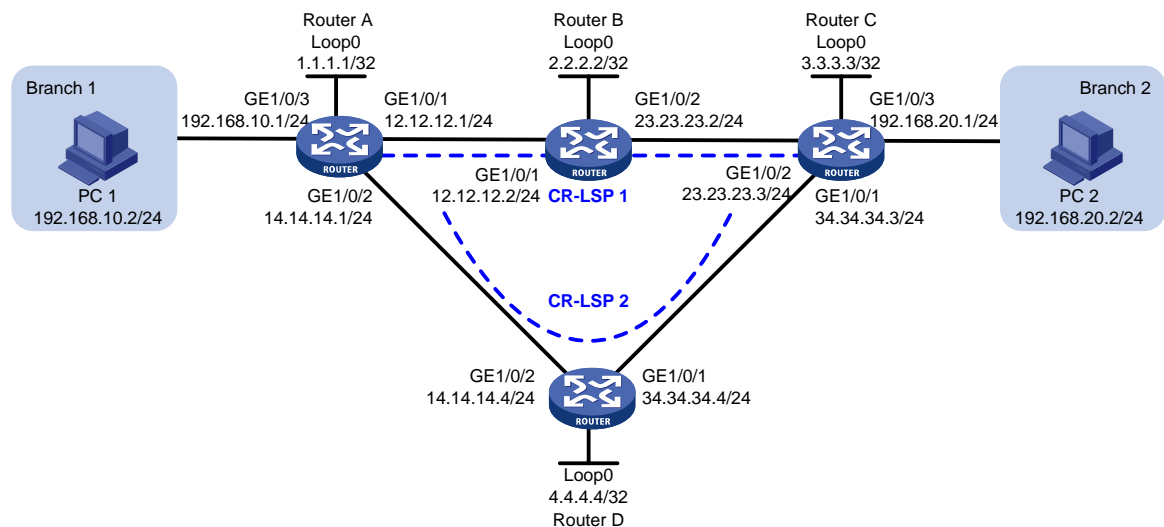
4.1 组网需求

如图 2 所示，某公司有两个位于不同的地理位置的分支机构通过 MPLS TE 隧道实现互联，两个分支机构之间需要进行实时业务的同步传输。该公司要求运营商提供高可靠性的服务，以保证实时业务的不间断性。

为满足该用户需求，可通过部署 CRLSP 备份服务来提供主备两条 CRLSP 链路，并使用 BFD 检测 MPLS TE 技术提高主备 CR-LSP 的切换速度，具体实现如下：

- 正常情况下，使用 CR-LSP 1 作为主 CR-LSP，负责转发 Router A 和 Router C 之间的流量。
- 使用 BFD 对主 CR-LSP 进行监测，当主 CR-LSP 发生故障时，BFD 能够快速感知并通告 RSVP 协议，使得 Router A 和 Router C 之间的流量迅速切换到 CR-LSP 2 进行转发。

图2 BFD 检测 MPLS TE 配置组网图



4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.3 配置注意事项

- OSPF TE 使用 Opaque Type 10 LSA 携带链路的 TE 属性信息，因此，配置 OSPF TE 时必须先使能 OSPF 的 Opaque 能力。
- 由于 MPLS TE 无法在 OSPF 虚连接上预留资源和分配标签，即 MPLS TE 无法通过 OSPF 虚连接建立 CRLSP 隧道。因此，配置 OSPF TE 时，OSPF 路由域内不能存在虚连接。

4.4 配置步骤

- (1) 配置各接口的 IP 地址

配置 Router A 接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 12.12.12.1 24
[RouterA-GigabitEthernet1/0/1] quit
```

请参考以上方法配置图 2 中其它接口（包括 LoopBack 接口）的 IP 地址，配置步骤这里省略。

- (2) 配置 LSR ID，开启 MPLS、MPLS TE 和 RSVP-TE 能力

配置 Router A。

```
[RouterA] mpls lsr-id 1.1.1.1
[RouterA] mpls te
[RouterA-te] quit
[RouterA] rsvp
[RouterA-rsvp] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mpls enable
[RouterA-GigabitEthernet1/0/1] mpls te enable
[RouterA-GigabitEthernet1/0/1] rsvp enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] mpls enable
[RouterA-GigabitEthernet1/0/2] mpls te enable
[RouterA-GigabitEthernet1/0/2] rsvp enable
[RouterA-GigabitEthernet1/0/2] quit
```

Router B、Router C 和 Router D 的配置与 Router A 相似，此处不再赘述，具体请参见配置文件。

- (3) 在 MPLS 骨干网内配置 OSPF，以保证各路由器之间路由可达，并使能 OSPF 的 Opaque LSA 发布接收能力，在 OSPF 区域 0 使能 MPLS TE 能力

配置 Router A。

```
[RouterA] ospf
[RouterA-ospf-1] opaque-capability enable
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] mpls te enable
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
```

```
[RouterA-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置 Router B。

```
[RouterB] ospf
[RouterB-ospf-1] opaque-capability enable
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] mpls te enable
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置 Router C。

```
[RouterC] ospf
[RouterC-ospf-1] opaque-capability enable
[RouterC ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] mpls te enable
[RouterC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[RouterC ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[RouterC ospf-1-area-0.0.0.0] network 34.34.34.0 0.0.0.255
[RouterC ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[RouterC ospf-1-area-0.0.0.0] quit
[RouterC ospf-1] quit
```

配置 Router D。

```
[RouterD] ospf
[RouterD-ospf-1] opaque-capability enable
[RouterD-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] mpls te enable
[RouterD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 34.34.34.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
```

(4) 配置 MPLS TE 隧道

在 Router A 上配置 MPLS TE 隧道 Tunnel3: 目的地址为 Router C 的 LSR ID (3.3.3.3); 采用 RSVP-TE 信令协议建立 MPLS TE 隧道; 隧道支持 CRLSP 热备份功能。

```
[RouterA] interface tunnel 3 mode mpls-te
[RouterA-Tunnel3] ip address 9.1.1.1 255.255.255.0
[RouterA-Tunnel3] destination 3.3.3.3
[RouterA-Tunnel3] mpls te signaling rsvp-te
[RouterA-Tunnel3] mpls te backup hot-standby
[RouterA-Tunnel3] quit
```

#创建隧道的显式路径, 设置 CR-LSP 1 优先级为 1, 作为主 CR-LSP, CR-LSP 2 优先级为 2, 作为备份 CR-LSP。

```
[RouterA] explicit-path cr-lsp1
```

```

[RouterA-explicit-path-cr-lsp1] nexthop 12.12.12.2
[RouterA-explicit-path-cr-lsp1] quit
[RouterA] explicit-path cr-lsp2
[RouterA-explicit-path-cr-lsp2] nexthop 14.14.14.4
[RouterA-explicit-path-cr-lsp2] quit
[RouterA] interface tunnel 3
[RouterA-Tunnel3] mpls te path preference 1 explicit-path cr-lsp1
[RouterA-Tunnel3] mpls te path preference 2 explicit-path cr-lsp2
[RouterA-Tunnel3] quit

```

在 Router C 上配置 MPLS TE 隧道 Tunnel3: 目的地址为 Router A 的 LSR ID (1.1.1.1); 采用 RSVP-TE 信令协议建立 MPLS TE 隧道; 隧道支持 CRLSP 热备份功能。

```

[RouterC] interface tunnel 3 mode mpls-te
[RouterC-Tunnel3] ip address 9.3.3.3 255.255.255.0
[RouterC-Tunnel3] destination 1.1.1.1
[RouterC-Tunnel3] mpls te signaling rsvp-te
[RouterC-Tunnel3] mpls te backup hot-standby
[RouterC-Tunnel3] quit

```

#创建隧道的显式路径, 设置 CR-LSP 1 优先级为 1, 作为主 CR-LSP, CR-LSP 2 优先级为 2, 作为备份 CR-LSP。

```

[RouterC] explicit-path cr-lsp1
[RouterC-explicit-path-cr-lsp1] nexthop 23.23.23.2
[RouterC-explicit-path-cr-lsp1] quit
[RouterC] explicit-path cr-lsp2
[RouterC-explicit-path-cr-lsp2] nexthop 34.34.34.4
[RouterC-explicit-path-cr-lsp2] quit
[RouterC] interface tunnel 3
[RouterC-Tunnel3] mpls te path preference 1 explicit-path cr-lsp1
[RouterC-Tunnel3] mpls te path preference 2 explicit-path cr-lsp2
[RouterC-Tunnel3] quit

```

(5) 配置静态路由使流量沿 MPLS TE 隧道转发

在 Router A 上配置静态路由, 使得到达网络 192.168.20.0/24 的流量通过 MPLS TE 隧道接口 Tunnel3 转发。

```

[RouterA] ip route-static 192.168.20.0 24 tunnel 3 preference 1

```

在 Router C 上配置静态路由, 使得到达网络 192.168.10.0/24 的流量通过 MPLS TE 隧道接口 Tunnel3 转发。

```

[RouterC] ip route-static 192.168.10.0 24 tunnel 3 preference 1

```

(6) 使能 MPLS 与 BFD 联动功能, 并配置通过 BFD 检测 TE 隧道的连通性

配置 Router A。

```

[RouterA] mpls bfd enable
[RouterA] interface tunnel 3
[RouterA-Tunnel3] mpls bfd
[RouterA-Tunnel3] quit

```

配置 Router C。

```

[RouterC] mpls bfd enable
[RouterC] interface tunnel 3
[RouterC-Tunnel3] mpls bfd

```

```
[RouterC-Tunnel3] quit
```

4.5 验证配置

- (1) 配置完成后，查看 MPLS TE 隧道是否成功建立。

#在 Router A 和 Router C 上执行 **display interface tunnel** 命令，可以看到 Tunnel3 的状态为 up，以 Router A 为例。

```
<RouterA> display interface tunnel
Tunnel3
Current state: UP
Line protocol state: UP
Description: Tunnel3 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1496
Internet Address is 9.1.1.1/24 Primary
Tunnel source unknown, destination 3.3.3.3
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

- (2) 在 Router A 上使用 **tracert mpls te** 命令查看到当前路径是 CR-LSP1。（使用 Tracert 功能需要在中间设备上开启 ICMP 超时报文发送功能，在目的端开启 ICMP 目的不可达报文发送功能）

```
<RouterA> tracert mpls te Tunnel 3
MPLS trace route TE tunnel Tunnel3
  TTL  Replier           Time   Type      Downstream
  0                               Ingress 12.12.12.2/[1140]
  1    12.12.12.2         30 ms  Transit  23.23.23.3/[3]
  2    23.23.23.3         2 ms   Egress
```

- (3) 使用 **display mpls bfd** 查看到 2 条 MPLS TE 隧道的 BFD 检测信息，分别检测主 CR-LSP 和备份 CR-LSP 的状态，以 Router A 为例。

```
<RouterA> display mpls bfd te tunnel 3
Total number of sessions: 2, 2 up, 0 down, 0 init

FEC Type: TE Tunnel
FEC Info:
  Send Addr: 1.1.1.1
  End Addr: 3.3.3.3
  Tunnel ID: 3
  LSP ID   : 6681
NHLFE ID: 1037
Local Discr: 513           Remote Discr: 513
Source IP: 1.1.1.1        Destination IP: 127.0.0.1
Session State: Up         Session Role: Passive
```

Template Name: -

FEC Type: TE Tunnel

FEC Info:

Send Addr: 1.1.1.1

End Addr: 3.3.3.3

Tunnel ID: 3

LSP ID : 6682

NHLFE ID: 1039

Local Discr: 514

Remote Discr: 514

Source IP: 1.1.1.1

Destination IP: 127.0.0.2

Session State: Up

Session Role: Passive

Template Name: -

- (4) 在 Router A 上持续 ping Router C, 期间将 Router B 的 GigabitEthernet1/0/1 接口 shutdown, 查看通信是否中断。

在 Router A 上持续 ping Router C,

```
<RouterA> ping -c 10000 -a 192.168.10.1 192.168.20.1
```

```
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C to break
```

```
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=3.443 ms
```

```
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=2.835 ms
```

```
...
```

关闭 Router B 的 GigabitEthernet1/0/1 接口。

```
[RouterB] interface gigabitethernet1/0/1
```

```
[RouterB-GigabitEthernet1/0/1] shutdown
```

在 Router A 上查看到通讯断开后迅速恢复。

```
<RouterA> ping -c 10000 -a 192.168.10.1 192.168.20.1
```

```
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C to break
```

```
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=3.443 ms
```

```
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=2.835 ms
```

```
...
```

```
56 bytes from 192.168.20.1: icmp_seq=22 ttl=254 time=3.503 ms
```

```
Request time out
```

```
56 bytes from 192.168.20.1: icmp_seq=24 ttl=254 time=2.434 ms
```

```
56 bytes from 192.168.20.1: icmp_seq=25 ttl=254 time=3.196 ms
```

```
56 bytes from 192.168.20.1: icmp_seq=26 ttl=254 time=3.592 ms
```

```
56 bytes from 192.168.20.1: icmp_seq=27 ttl=254 time=2.305 ms
```

```
56 bytes from 192.168.20.1: icmp_seq=28 ttl=254 time=2.139 ms
```

```
--- Ping statistics for 192.168.20.1 ---
```

```
29 packet(s) transmitted, 28 packet(s) received, 3.4% packet loss
```

```
round-trip min/avg/max/std-dev = 2.076/2.701/3.921/0.609 ms
```

- (5) 查看链路是否发生切换。

在 Router A 上使用 **tracert mpls te** 命令查看到当前路径是 CR-LSP2。

```
<RouterA> tracert mpls te Tunnel 3
```

```
MPLS trace route TE tunnel Tunnel3
```

TTL	Replier	Time	Type	Downstream
0			Ingress	14.14.14.4/[1142]
1	14.14.14.4	198 ms	Transit	34.34.34.3/[3]
2	34.34.34.3	7 ms	Egress	

使用 **display mpls bfd** 查看到 MPLS TE 隧道 CR-LSP2 的 BFD 检测信息，以 Router A 为例。

```
<RouterA> display mpls bfd te tunnel 3
Total number of sessions: 1, 1 up, 0 down, 0 init

FEC Type: TE Tunnel
FEC Info:
  Send Addr: 1.1.1.1
  End Addr: 3.3.3.3
  Tunnel ID: 3
  LSP ID   : 6682
NHLFE ID: 1039
Local Discr: 514
Source IP: 1.1.1.1
Session State: Up
Template Name: -
Remote Discr: 514
Destination IP: 127.0.0.2
Session Role: Passive
```

4.6 配置文件

- Router A:

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
 mpls te enable
#
 mpls lsr-id 1.1.1.1
#
 mpls te
#
 explicit-path cr-lsp1
  nexthop index 1 12.12.12.2 include strict
#
 explicit-path cr-lsp2
  nexthop index 1 14.14.14.4 include strict
#
 rsvp
#
 mpls bfd enable
#
 interface LoopBack0
```

```

ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 12.12.12.1 255.255.255.0
mpls enable
mpls te enable
rsvp enable
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 14.14.14.1 255.255.255.0
mpls enable
mpls te enable
rsvp enable
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 192.168.10.1 255.255.255.0
#
interface Tunnel3 mode mpls-te
ip address 9.1.1.1 255.255.255.0
mpls te path preference 1 explicit-path cr-lsp1
mpls te path preference 2 explicit-path cr-lsp2
mpls te backup hot-standby
mpls bfd
destination 3.3.3.3
#
ip route-static 192.168.20.0 24 Tunnel3 preference 1
#

```

- **Router B:**

```

#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 12.12.12.0 0.0.0.255
network 23.23.23.0 0.0.0.255
mpls te enable
#
mpls lsr-id 2.2.2.2
#
mpls te
#
rsvp
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#

```

```

interface GigabitEthernet1/0/1
  port link-mode route
  ip address 12.12.12.2 255.255.255.0
  mpls enable
  mpls te enable
  rsvp enable
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 23.23.23.2 255.255.255.0
  mpls enable
  mpls te enable
  rsvp enable
#

```

- **Router C:**

```

#
ospf 1
  area 0.0.0.0
    network 3.3.3.3 0.0.0.0
    network 23.23.23.0 0.0.0.255
    network 34.34.34.0 0.0.0.255
    network 192.168.20.0 0.0.0.255
  mpls te enable
#
  mpls lsr-id 3.3.3.3
#
mpls te
#
explicit-path cr-lsp1
  nexthop index 1 23.23.23.2 include strict
#
explicit-path cr-lsp2
  nexthop index 1 34.34.34.4 include strict
#
rsvp
#
  mpls bfd enable
#
interface LoopBack0
  ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 34.34.34.3 255.255.255.0
  mpls enable
  mpls te enable
  rsvp enable
#

```



```

interface GigabitEthernet1/0/2
  port link-mode route
  ip address 23.23.23.3 255.255.255.0
  mpls enable
  mpls te enable
  rsvp enable
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip address 192.168.20.1 255.255.255.0
#
interface Tunnel3 mode mpls-te
  ip address 9.3.3.3 255.255.255.0
  mpls te path preference 1 explicit-path cr-lsp1
  mpls te path preference 2 explicit-path cr-lsp2
  mpls te backup hot-standby
  mpls bfd
  destination 1.1.1.1
#
  ip route-static 192.168.10.0 24 Tunnel3 preference 1
#

```

- **Router D:**

```

#
ospf 1
  area 0.0.0.0
    network 4.4.4.4 0.0.0.0
    network 14.14.14.0 0.0.0.255
    network 34.34.34.0 0.0.0.255
    mpls te enable
#
  mpls lsr-id 4.4.4.4
#
mpls te
#
rsvp
#
interface LoopBack0
  ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 34.34.34.4 255.255.255.0
  mpls enable
  mpls te enable
  rsvp enable
#
interface GigabitEthernet1/0/2
  port link-mode route

```

```
ip address 14.14.14.4 255.255.255.0
mpls enable
mpls te enable
rsvp enable
#
```

5 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“MPLS 配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“MPLS 命令参考”

H3C MSR 系列路由器

作为重定向服务器 Telnet 重定向配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.6 验证配置.....	4
3.7 配置文件.....	6
4 相关资料.....	7

1 简介

本文介绍使用主机通过 Stelnet 方式登录到 MSR 路由器，由 MSR 路由器 Telnet 重定向到目的设备的配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

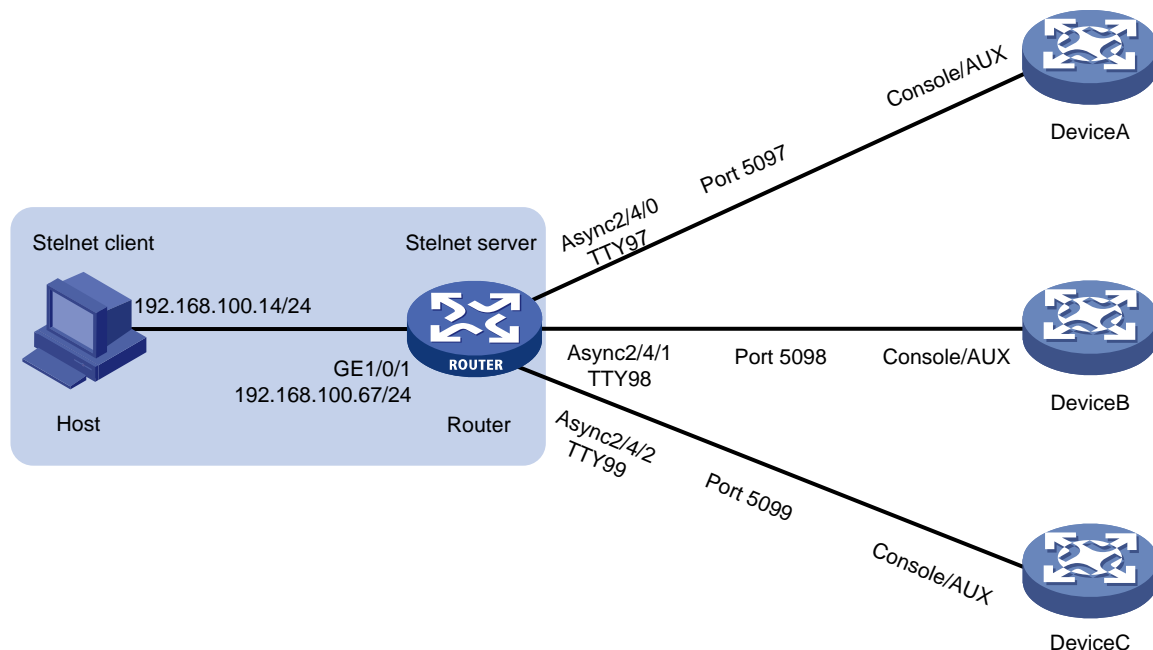
本文档假设您已了解 SSH 和重定向服务器的特性。

3 配置举例

3.1 组网需求

如图 1 所示，主机 Host 通过 SSH 方式访问 Router，Router 的异步串口通过全反线连接目的设备的 Console 口（AUX 口）。现要求：在 Router 上配置重定向服务器功能，使得 Host 能够通过 Telnet 重定向登录到目的设备。

图1 通过重定向服务器登录设备



3.2 配置思路

- 为了使 Host 能够通过 Stelnet 方式访问重定向服务器 Router，需要在 Router 上配置 Stelnet 服务器功能。
- 为了使重定向服务器能够通过异步串口进入目的设备 CLI 视图下进行配置，需要将异步串口的工作模式设置为流模式。
- 为了使 Host 能够通过重定向服务器登录目的设备，需要确认重定向服务器的异步串口和 TTY 用户线的对应关系，并在 TTY 用户线下配置重定向的监听端口号。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 在同一时刻，同一目的设备仅允许一个用户通过重定向服务器进行登录。
- 在使用同/异步串口时，需配置其工作在异步模式下，并使用转接器连接到目的设备。
- 全反线是连接主机串口和设备 Console 口的终端线，线序一般为 568B，一端为 12345678，即橙白、橙、绿白、蓝、蓝白、绿、棕白、棕；另一端全反过来，为 87654321，即棕、棕白、绿、蓝白、蓝、绿白、橙、橙白。

3.5 配置步骤

- (1) 配置接口地址，使 Host 到重定向服务器 Router 路由可达

为接口 GigabitEthernet1/0/1 配置 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.100.67 24
[Router-GigabitEthernet1/0/1] quit
```

- (2) 配置 Stelnet 服务器功能，使主机能够通过 Stelnet 方式访问重定向服务器 Router

生成 RSA 密钥对。

```
[Router] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024] :
Generating Keys...
.....++++++
.....++++++
.....++++++
.....++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Router] public-key local create dsa
```

```

The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024] :
Generating Keys...
.+++++*
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
...+.....+.....+.....+.....+.....+.....+.....+.....+.....
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....
.....+.....+.....+.....+.....+.....+.....+.....+.....+.....*
Create the key pair successfully.

```

使能 SSH 服务器功能。
[Router] ssh server enable
设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```

[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit

```

创建设备管理类本地用户 sshuser，并设置密码为 admin，服务类型为 SSH，用户角色为 network-admin。

```

[Router] local-user sshuser class manage
[Router-luser-manage-sshuser] password simple admin
[Router-luser-manage-sshuser] service-type ssh
[Router-luser-manage-sshuser] authorization-attribute user-role network-admin
[Router-luser-manage-sshuser] quit

```

配置 SSH 用户 sshuser 的服务器类型为 Stelnet，认证方式为 password 认证（此步骤可选）。

```

[Router] ssh user sshuser service-type stelnet authentication-type password

```

(3) 配置异步串口的工作模式为流模式。（以异步串口 Async2/4/0 为例进行配置说明，对端的目的是设备为 Device A）

```

[Router] interface async 2/4/0
[Router-Async2/4/0] async-mode flow
[Router-Async2/4/0] quit

```

(4) 配置 TTY 用户线

查看重定向服务器的异步串口与 TTY 用户线的对应关系。

```

[Router] display user-interface

```

Idx	Type	Tx/Rx	Modem	Auth	Int	Location
96	TTY 97	9600	-	N	Asy2/4/0	0/0
	97	TTY 98	9600	-	N	Asy2/4/1 0/0
	98	TTY 99	9600	-	N	Asy2/4/2 0/0
	99	TTY 100	9600	-	N	Asy2/4/3 0/0
	100	TTY 101	9600	-	N	Asy2/4/4 0/0
	101	TTY 102	9600	-	N	Asy2/4/5 0/0
	102	TTY 103	9600	-	N	Asy2/4/6 0/0
	103	TTY 104	9600	-	N	Asy2/4/7 0/0

```

104 TTY 105 9600 - N Asy2/4/8 0/0
105 TTY 106 9600 - N Asy2/4/9 0/0
106 TTY 107 9600 - N Asy2/4/10 0/0
.....

```

查看到与异步串口 Async2/4/0 对应的 TTY 用户线为 TTY 97。因此，对于 Async2/4/0 要连接的目的设备，需要配置 TTY 97。

使能 TTY 用户线的 Telnet 重定向功能。

```
[Router-line-tty97] line tty 97
```

```
[Router-line-tty97] redirect enable
```

设置 Telnet 重定向的监听端口号为 5097。

```
[Router-line-tty97] redirect listen-port 5097
```

设置 Telnet 重定向的空闲超时时间为 0，表示永不超时。

```
[Router-line-tty97] redirect timeout 0
```

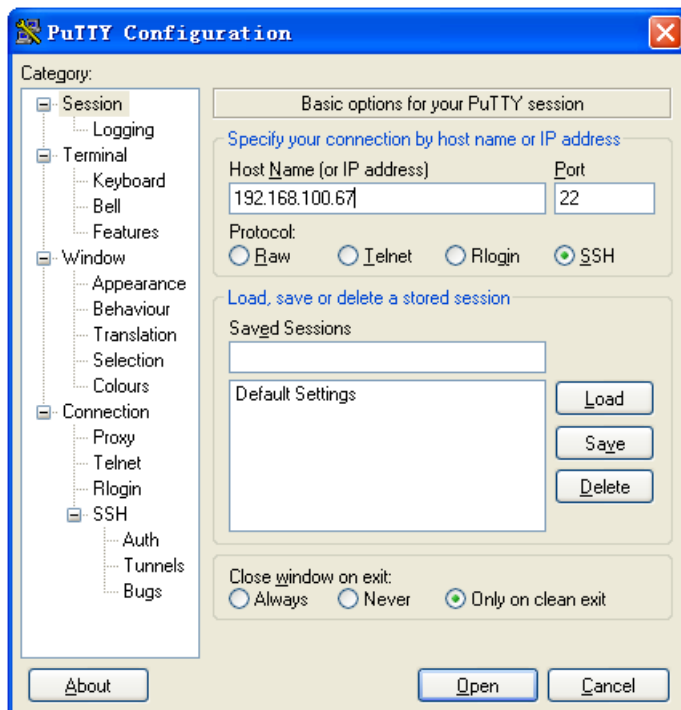
```
[Router-line-tty97] quit
```

3.6 验证配置

Host 使用 Stelnet 方式登录到重定向服务器，再通过重定向服务器 telnet 本地回环地址 + 重定向端口号方式登录到目的设备 Device A（以 PuTTY 工具为例）。

- (1) 打开 PuTTY 控制台，“Host Name”配置为重定向服务器的 IP 地址“192.168.100.67”，“Port”选择为 SSH 的缺省端口号“22”。

图2 打开 PuTTY 控制台



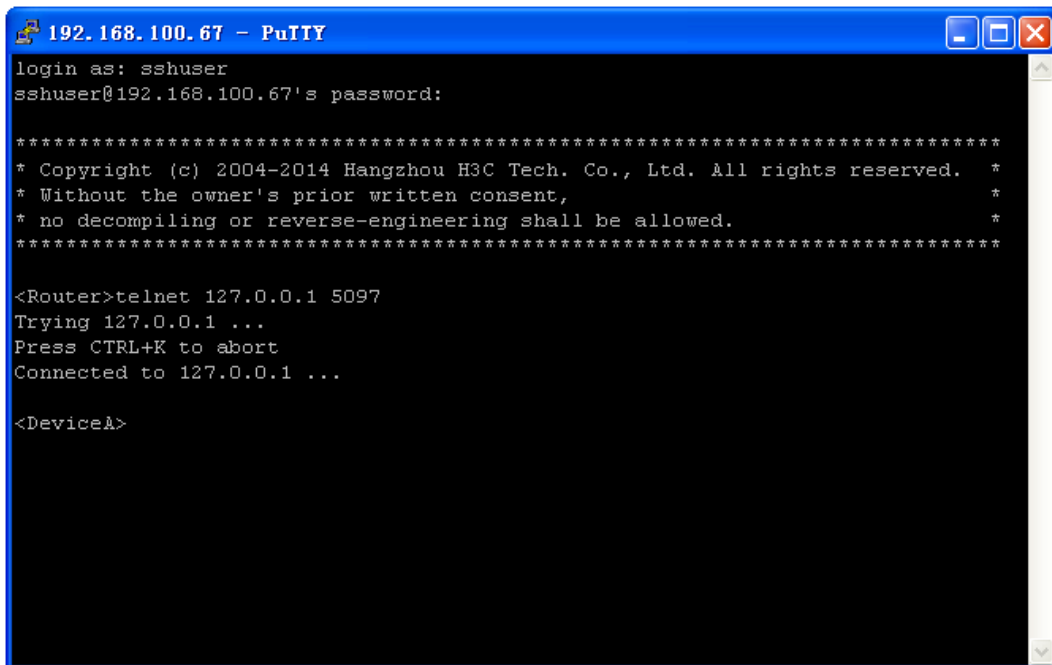
- (2) 配置完成后，单击<Open>按钮，输入用户名“sshuser”和密码“admin”，即登录到重定向服务器，如下图所示：

图3 输入用户名和密码



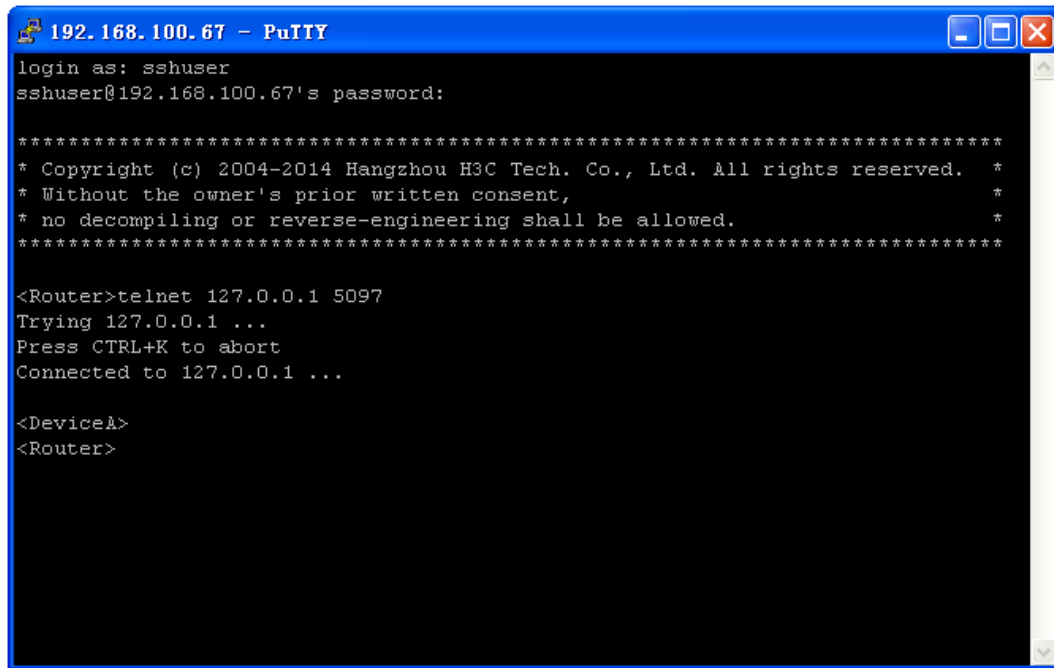
- (3) 在用户视图下键入命令 `telnet 127.0.0.1 5097`，两次回车（其中 127.0.0.1 为重定向服务器的本地回环地址），即登录到目的设备的 Console 口。

图4 通过重定向服务器登录目的设备



- (4) 如需要由目的设备视图下返回到重定向服务器视图，输入“Ctrl+K”即返回。

图5 返回到重定向服务器



3.7 配置文件

```
#
interface Async2/4/0
  async-mode flow
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 192.168.100.67 255.255.255.0
#
line tty 97
  redirect enable
  redirect listen-port 5097
  redirect timeout 0
#
ssh server enable
ssh user sshuser service-type stelnet authentication-type password
#
local-user sshuser class manage
  password hash $h$6$CDXc2RtzwtS8ZvBj$GIbeoERTWeK0CVKsJoUTMW3xNTgVT+qVm+aE0aLHVzr
5YqSBnKzdvjqcpFV9cUYFLEm2RBOAnLXaYKtNpPMi4Q==
  service-type ssh
  authorization-attribute user-role network-admin
  authorization-attribute user-role network-operator
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“基础配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“基础配置命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“安全命令参考”

H3C MSR 系列路由器

BFD 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 VRRP 与 BFD、Track 联动配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	3
3.4 配置注意事项.....	3
3.5 配置步骤.....	3
3.5.1 配置各接口的 IP 地址.....	3
3.5.2 配置上行设备 Device E 和 Device F 到 VRRP 组虚拟 IP 的静态路由.....	3
3.5.3 配置 VRRP 备份组.....	3
3.5.4 配置 BFD 功能.....	4
3.5.5 配置 Track 项.....	4
3.6 验证配置.....	5
3.7 配置文件.....	9
4 静态路由与 BFD 联动配置举例.....	11
4.1 组网需求.....	11
4.2 配置思路.....	11
4.3 使用版本.....	11
4.4 配置步骤.....	12
4.4.1 配置各接口的 IP 地址.....	12
4.4.2 配置静态路由.....	12
4.4.3 配置 Device A 的 BFD 功能.....	12
4.5 验证配置.....	13
4.6 配置文件.....	13
5 RIP 与 BFD 联动配置举例.....	15
5.1 组网需求.....	15
5.2 配置思路.....	16
5.3 使用版本.....	16
5.4 配置步骤.....	16
5.4.1 配置各接口的 IP 地址.....	16
5.4.2 配置 RIP 基本功能.....	16

5.4.3 配置 Device A 的 BFD 参数	17
5.5 验证配置	17
5.6 配置文件	18
6 OSPF 与 BFD 联动配置举例	20
6.1 组网需求	20
6.2 配置思路	21
6.3 使用版本	21
6.4 配置步骤	21
6.4.1 配置各接口的 IP 地址	21
6.4.2 配置 OSPF 基本功能	21
6.4.3 配置 BFD 功能	22
6.5 验证配置	22
6.6 配置文件	25
7 IS-IS 与 BFD 联动配置举例	26
7.1 组网需求	26
7.2 配置思路	27
7.3 使用版本	27
7.4 配置步骤	27
7.4.1 配置各接口的 IP 地址	27
7.4.2 配置 IS-IS 基本功能	27
7.4.3 配置 BFD 功能	28
7.5 验证配置	29
7.6 配置文件	31
8 BGP 与 BFD 联动配置举例	32
8.1 组网需求	32
8.2 配置思路	33
8.3 配置步骤	33
8.3.1 配置各接口的 IP 地址	33
8.3.2 在 AS 100 内配置 OSPF 功能，保证设备间路由可达	33
8.3.3 配置 BGP 功能	34
8.3.4 配置路由策略	36
8.3.5 配置 BFD 功能	36
8.4 验证配置	37
8.5 配置文件	40
9 策略路由与 BFD 联动配置举例	43
9.1 组网需求	43

9.2 配置思路	43
9.3 使用版本	43
9.4 配置步骤	43
9.4.1 配置各接口的 IP 地址	43
9.4.2 配置静态路由	44
9.4.3 配置 Device A 上的路由策略	44
9.4.4 配置 BFD 功能，并创建和 BFD 会话关联的 Track 项 11，检测 Device B 是否可达	44
9.5 验证配置	44
9.6 配置文件	45
10 相关资料	47

1 简介

本文档介绍了 BFD 与路由协议、VRRP 协议联动的配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

本文假设您已了解 BFD 特性、VRRP 特性、Track 特性以及 OSPF、IS-IS 等路由协议。

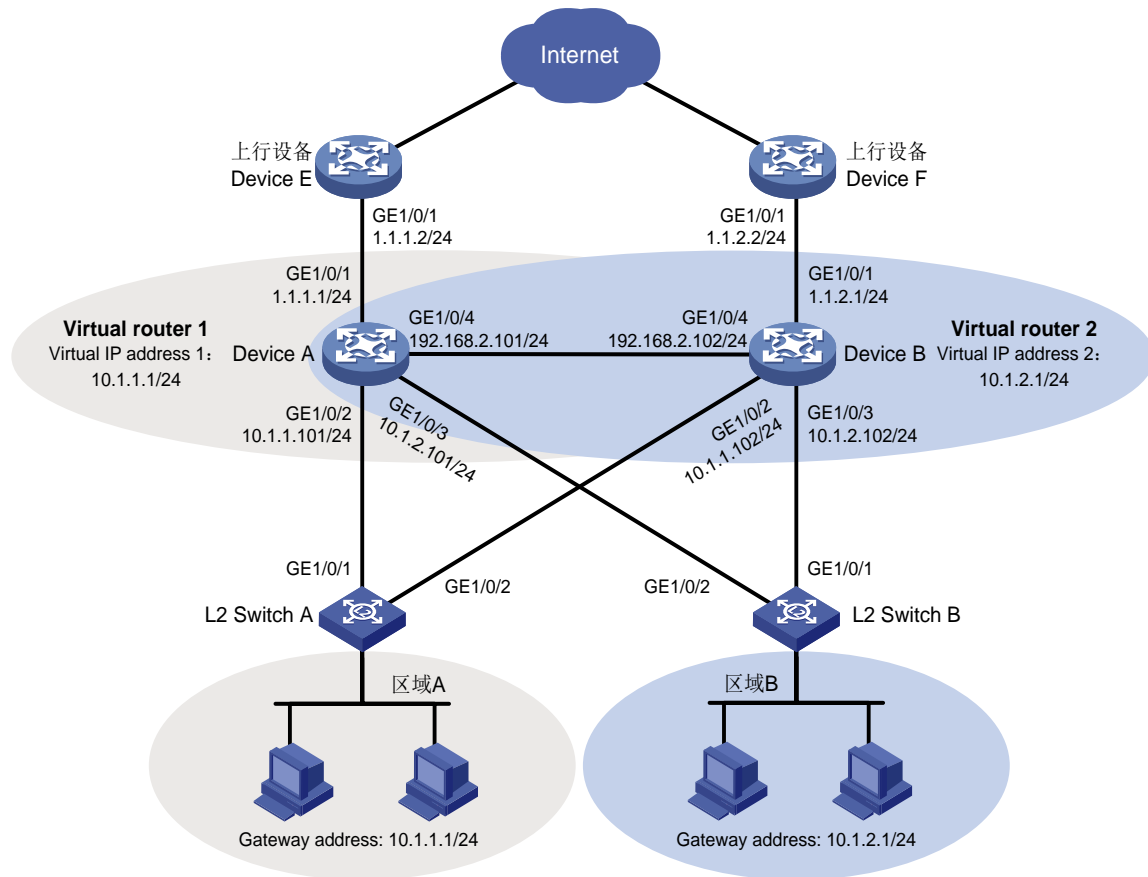
3 VRRP 与 BFD、Track 联动配置举例

3.1 组网需求

如[图1](#)所示，区域A和区域B用户所在网络的出口处部署了两台汇聚层设备(Device A和Device B)。现要求使用 VRRP 与 BFD、Track 联动功能，实现以下需求：

- 在 Device A 和 Device B 上分别配置两个 VRRP 备份组，Device A 是 VRRP 备份组 1 中的 Master 设备，Device B 是 VRRP 备份组 2 中的 Master 设备；
- 在正常情况下，区域 A 的用户将 VRRP 备份组 1 作为缺省网关，通过 Device A 进行数据转发，区域 B 用户将 VRRP 备份组 2 作为缺省网关，通过 Device B 进行数据转发。当一台网关设备出现故障时，另一台网关设备能够迅速承担受影响区域内主机流量的转发任务。
- 当网关设备 Device A（Device B）自身出现故障，或其上行接口出现故障时，局域网中的主机可以通过另一台设备网关设备 Device B（Device A）继续通信，避免通信中断；当 Device A（Device B）故障恢复后，继续承担网关功能；
- 当 Device A 或 Device B 的下行链路出现故障时，局域网中的主机通过接入设备 L2 Switch A 或 L2 Switch B 的 GigabitEthernet1/0/2 端口将数据转发给网关设备继续通信，避免通信中断；当 Device A 或 Device B 的下行链路故障恢复后，继续由 L2 Switch A 或 L2 Switch B 的 GigabitEthernet1/0/1 端口将数据发送给网关设备。

图1 VRRP 与 BFD、Track 联动配置组网图



3.2 配置思路

- 为了实现不同区域中用户数据流的负载分担，需要在 Device A 和 Device B 上分别创建两个 VRRP 备份组，并配置区域 A 内的主机都将 VRRP 备份组 1 作为网关，区域 B 内的主机都将 VRRP 备份组 2 作为网关；
- 为使 Device A 优先被选举为 VRRP 备份组 1 的 Master 设备，需要为其在 VRRP 备份组 1 中配置较高的优先级；为使 Device B 优先被选举为 VRRP 备份组 2 的 Master 设备，需要为其在 VRRP 备份组 2 中配置较高的优先级；
- 配置两个 VRRP 备份组都工作在抢占模式，以保证原 Master 设备故障恢复后，能再次抢占成为 Master；
- 通过 Device A 与 Device B 上配置 BFD 功能监视其上行接口的状态，当监测到其上行接口故障时，Device A 或 Device B 的优先级会自动降低指定的数额，使 VRRP 备份组 1 内 Device B 的优先级高于 Device A，或 VRRP 备份组 2 内 Device A 的优先级高于 Device B，从而实现主备切换；

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 请务必保证备份组中的所有设备上配置的 VRRP 版本一致，否则备份组无法正常工作。
- 为了避免对端发送大量的 ICMP 重定向报文造成网络拥塞，建议不要将 BFD echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段。
- 建议将备份组的虚拟 IP 地址和备份组中设备下行接口的 IP 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。

3.5 配置步骤

3.5.1 配置各接口的 IP 地址

- (1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 1.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

- (2) 请参考以上方法配置图 1 中其它接口的 IP 地址，配置步骤这里省略

3.5.2 配置上行设备 Device E 和 Device F 到 VRRP 组虚拟 IP 的静态路由

- (1) 配置 Device E

配置 Device E 到 VRRP 备份组 1 和 VRRP 备份组 2 的虚拟 IP 地址的静态路由。

```
<DeviceE> system-view
[DeviceE] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
[DeviceE] ip route-static 10.1.2.0 255.255.255.0 1.1.1.1
```

- (2) 配置 Device F

配置 Device F 到 VRRP 备份组 1 和 VRRP 备份组 2 的虚拟 IP 地址的静态路由。

```
<DeviceE> system-view
[DeviceF] ip route-static 10.1.1.0 255.255.255.0 1.1.2.1
[DeviceF] ip route-static 10.1.2.0 255.255.255.0 1.1.2.1
```

3.5.3 配置 VRRP 备份组

- (1) 配置 Device A

配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1，抢占延时为 5s。并且 VRRP 备份组 1 中 Device A 的优先级为 110，高于 Device B，成为 VRRP 备份组 1 的 Master。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] vrrp vrid 1 virtual-ip 10.1.1.1
[DeviceA-GigabitEthernet1/0/2] vrrp vrid 1 priority 110
[DeviceA-GigabitEthernet1/0/2] vrrp vrid 1 preempt-mode delay 5
```

```
[DeviceA-GigabitEthernet1/0/2] quit
# 配置 VRRP 备份组 2 的虚拟 IP 地址为 10.1.2.1，抢占延时为 5s。
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 10.1.2.1
[DeviceA-GigabitEthernet1/0/3] vrrp vrid 2 preempt-mode delay 5
[DeviceA-GigabitEthernet1/0/3] quit
```

(2) 配置 Device B

配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1，抢占延时为 5s。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 1 virtual-ip 10.1.1.1
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 1 preempt-mode delay 5
[DeviceB-GigabitEthernet1/0/2] quit
```

配置 VRRP 备份组 2 的虚拟 IP 地址为 10.1.2.1，抢占延时为 5s。并且 VRRP 备份组 2 中 Device B 的优先级为 110，高于 Device A，成为 VRRP 备份组 2 的 Master。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 10.1.2.1
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 priority 110
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 preempt-mode delay 5
[DeviceB-GigabitEthernet1/0/3] quit
```

3.5.4 配置 BFD 功能

(1) 配置 Device A

配置 BFD echo 报文方式的 Source IP，IP 地址可以任意指定，不要与实际接口地址相同。

```
[DeviceA] bfd echo-source-ip 10.10.10.10
```

(2) 配置 Device B

配置 BFD echo 报文方式的 Source IP，IP 地址可以任意指定，不要与实际接口地址相同。

```
[DeviceB] bfd echo-source-ip 11.11.11.11
```

3.5.5 配置 Track 项

(1) 配置 Device A

创建和 BFD 会话关联的 Track 项 1，检测上行设备 Device E 是否可达。

```
[DeviceA] track 1 bfd echo interface gigabitethernet 1/0/1 remote ip 1.1.1.2 local ip 1.1.1.1
```

配置备份组 1 监视 Track 项 1 的状态，当 Track 项状态为 Negative 时，Device A 在 VRRP 备份组 1 中的优先级减小 20，低于 Device B，以便 Device B 抢占成为 Master。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] vrrp vrid 1 track 1 priority reduced 20
[DeviceA-GigabitEthernet1/0/2] quit
```

(2) 配置 Device B

创建和 BFD 会话关联的 Track 项 1，检测上行设备 Device F 是否可达。

```
[DeviceB] track 1 bfd echo interface gigabitethernet 1/0/1 remote ip 1.1.2.2 local ip 1.1.2.1
```

配置备份组 2 监视 Track 项 1 的状态，当 Track 项状态为 Negative 时，Device B 在 VRRP 备份组 2 中的优先级减小 20，低于 Device A，以便 Device A 抢占成为 Master。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 track 1 priority reduced 20
[DeviceB-GigabitEthernet1/0/3] quit
```

3.6 验证配置

- (1) 网关设备 Device A、Device B 和链路均正常工作时，验证局域网内主机是否可以与外部网络通信

检查区域 A 的主机到目的端 1.1.1.2 是否可达。

```
<host A> ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
56 bytes from 1.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

检查区域 B 的主机到目的端 1.1.2.2 是否可达。

```
<host C> ping 1.1.2.2
PING 1.1.2.2 (1.1.2.2): 56 data bytes
56 bytes from 1.1.2.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.2.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.2.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.2.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.2.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

以上显示信息表示网关设备 Device A、Device B 和链路均正常工作时，区域 A 的主机和区域 B 的主机都可以访问 Internet。

查看 Device A 的 BFD 会话。

```
[DeviceA] display bfd session
```

```
Total Session Num: 1      Up Session Num: 1      Init Mode: Active
```

```
IPv4 Session Working Under Echo Mode:
```

LD	SourceAddr	DestAddr	State	Holdtime	Interface
65	1.1.1.1	1.1.1.2	Up	2000ms	GE1/0/1

以上显示信息表示 BFD 会话已经建立。

显示 Device A 上备份组的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Standard
Total number of virtual routers : 2
  Interface GigabitEthernet1/0/2
    VRID            : 1
    Admin Status    : Up
    Config Pri      : 110
    Preempt Mode    : Yes
    Auth Type       : None
    Virtual IP      : 10.1.1.1
    Virtual MAC     : 0000-5e00-0101
    Master IP       : 10.1.1.101
    Adver Timer     : 100
    State           : Master
    Running Pri     : 110
    Delay Time      : 5
  VRRP Track Information:
    Track Object    : 1
    State           : Positive
    Pri Reduced     : 20
  Interface GigabitEthernet1/0/3
    VRID            : 2
    Admin Status    : Up
    Config Pri      : 100
    Preempt Mode    : Yes
    Become Master   : 3600ms left
    Auth Type       : None
    Virtual IP      : 10.1.2.1
    Master IP       : 10.1.2.102
    Adver Timer     : 100
    State           : Backup
    Running Pri     : 100
    Delay Time      : 5
```

显示 Device B 上备份组的详细信息。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Standard
Total number of virtual routers : 2
  Interface GigabitEthernet1/0/2
    VRID            : 1
    Admin Status    : Up
    Config Pri      : 100
    Preempt Mode    : Yes
    Become Master   : 3100ms left
    Auth Type       : None
    Virtual IP      : 10.1.1.1
    Master IP       : 10.1.1.101
    Adver Timer     : 100
    State           : Backup
    Running Pri     : 100
    Delay Time      : 5
  Interface GigabitEthernet1/0/3
    VRID            : 2
    Admin Status    : Up
    Config Pri      : 110
    Preempt Mode    : Yes
    Auth Type       : None
    Virtual IP      : 10.1.2.1
    Adver Timer     : 100
    State           : Master
    Running Pri     : 110
    Delay Time      : 5
```

```
Virtual MAC      : 0000-5e00-0102
Master IP       : 10.1.2.102
VRRP Track Information:
Track Object    : 1                               State : Positive   Pri Reduced : 20
```

以上显示信息表示在备份组 1 中 Device A 为 Master，Device B 为 Backup，缺省网关为 10.1.1.1/24 的主机通过 Device A 访问 Internet；备份组 2 中 Device A 为 Backup，Device B 为 Master，缺省网关为 10.1.2.1/24 的主机通过 Device B 访问 Internet。

- (2) 当 Device A 监视的上行设备或上行链路状态为 down 时，验证局域网内主机是否可以与外部网络通信

检查区域 A 的主机到目的端 1.1.1.2 是否可达。

```
<host A> ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
56 bytes from 1.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

检查区域 B 的主机到目的端 1.1.1.2 是否可达。

```
<host C> ping 1.1.2.2
PING 1.1.2.2 (1.1.2.2): 56 data bytes
56 bytes from 1.1.2.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.2.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.2.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.2.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.2.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

以上显示信息表示当 Device A 监视的上行设备或上行链路状态为 down 时，区域 A 的主机和区域 B 的主机都可以访问 Internet。

查看 Device A 上的 BFD 会话。

```
[DeviceA] display bfd session

Total Session Num: 1      Up Session Num: 0      Init Mode: Active

IPv4 Session Working Under Echo Mode:

LD          SourceAddr      DestAddr      State      Holdtime      Interface
-----
65          1.1.1.1          1.1.1.2      Down      /             GE1/0/1
```

以上显示信息表示 BFD 会话已经终止。

显示 Device B 上备份组的详细信息。

```

[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Standard
Total number of virtual routers : 2
  Interface GigabitEthernet1/0/2
    VRID           : 1                Adver Timer   : 100
    Admin Status   : Up                State         : Master
    Config Pri     : 100               Running Pri   : 100
    Preempt Mode   : Yes               Delay Time    : 5
    Auth Type      : None
    Virtual IP     : 10.1.1.1
    Virtual MAC    : 0000-5e00-0101
    Master IP      : 10.1.1.102

  Interface GigabitEthernet1/0/3
    VRID           : 2                Adver Timer   : 100
    Admin Status   : Up                State         : Master
    Config Pri     : 110               Running Pri   : 110
    Preempt Mode   : Yes               Delay Time    : 5
    Auth Type      : None
    Virtual IP     : 10.1.2.1
    Virtual MAC    : 0000-5e00-0102
    Master IP      : 10.1.2.102
VRRP Track Information:
  Track Object     : 1                State : Positive  Pri Reduced : 20

```

以上显示信息表示当 **Device A** 监视的上行设备或上行链路状态为 **down** 时，**Device B** 抢占成为 **VRRP 备份组 1** 的 **Master**，主机通过 **Device B** 与外界通信。

当上行设备或上行链路状态恢复为 **UP** 后，查看 **Device A** 上的 **BFD** 会话。

```

[DeviceA] display bfd session

Total Session Num: 1      Up Session Num: 1      Init Mode: Active

IPv4 Session Working Under Echo Mode:

LD          SourceAddr      DestAddr      State      Holdtime      Interface
-----
65          1.1.1.1          1.1.1.2      Up         1932ms        GE1/0/1

```

以上显示信息表示 **BFD** 会话已经恢复。

当上行设备或上行链路状态恢复为 **UP** 后，显示 **Device A** 上备份组的详细信息。

```

[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Standard
Total number of virtual routers : 2
  Interface GigabitEthernet1/0/2
    VRID           : 1                Adver Timer   : 100
    Admin Status   : Up                State         : Master
    Config Pri     : 110               Running Pri   : 110
    Preempt Mode   : Yes               Delay Time    : 5

```

```

Auth Type      : None
Virtual IP     : 10.1.1.1
Virtual MAC    : 0000-5e00-0101
Master IP      : 10.1.1.101
VRRP Track Information:
Track Object   : 1                               State : Positive   Pri Reduced : 20

Interface GigabitEthernet1/0/3
VRID          : 2                               Adver Timer  : 100
Admin Status  : Up                             State        : Backup
Config Pri    : 100                            Running Pri  : 100
Preempt Mode  : Yes                            Delay Time   : 5
Become Master : 3550ms left
Auth Type     : None
Virtual IP    : 10.1.2.1
Master IP     : 10.1.2.102

```

以上显示信息表示当上行设备或上行链路状态恢复为 UP 后，Device A 在 VRRP 备份组 1 中恢复为原来的优先级并抢占成为该备份组的 Master，主机通过 Device A 与外界通信。

3.7 配置文件

- Device A:

```

#
bfd echo-source-ip 10.10.10.10
#
interface GigabitEthernet1/0/4
port link-mode route
ip address 192.168.2.101 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 10.1.1.101 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.1
vrrp vrid 1 priority 110
vrrp vrid 1 preempt-mode delay 5
vrrp vrid 1 track 1 priority reduced 20
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 10.1.2.101 255.255.255.0
vrrp vrid 2 virtual-ip 10.1.2.1
vrrp vrid 2 preempt-mode delay 5
#
track 1 bfd echo interface GigabitEthernet1/0/1 remote ip 1.1.1.2 local ip 1.1.1.1

```


- **Device B:**

```
#
bfd echo-source-ip 11.11.11.11
#
interface GigabitEthernet1/0/4
port link-mode route
ip address 192.168.2.102 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 10.1.1.102 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.1
vrrp vrid 1 preempt-mode delay 5
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 10.1.2.102 255.255.255.0
vrrp vrid 2 virtual-ip 10.1.2.1
vrrp vrid 2 priority 110
vrrp vrid 2 preempt-mode delay 5
vrrp vrid 2 track 1 priority reduced 20
#
track 1 bfd echo interface GigabitEthernet1/0/1 remote ip 1.1.2.2 local ip 1.1.2.1
```

- **Device E:**

```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 1.1.1.2 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
ip route-static 10.1.2.0 255.255.255.0 1.1.1.1
#
```

- **Device F:**

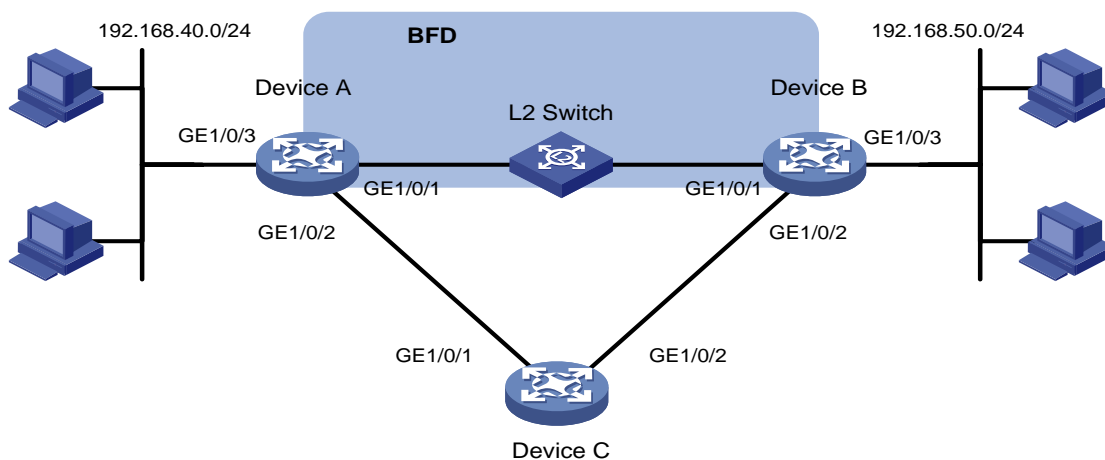
```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 1.1.2.2 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 1.1.2.1
ip route-static 10.1.2.0 255.255.255.0 1.1.2.1
#
```

4 静态路由与 BFD 联动配置举例

4.1 组网需求

某公司内部网络如图 2 所示，从 Device A 到 Device B 有两条转发路径，下一跳分别为 Device B 和 Device C。由于 Device A 和 Device B 之间物理距离较远，通过一个二层交换机 L2 Switch 作为中继。假设 Device B 不支持 BFD，要求在 Device A 上使用静态路由与 BFD 联动技术，实现当 Device B 与二层交换机 L2 Switch 之间的链路出现故障（如链路 down）时，Device A 能快速感知，并将流量切换到 Device C 的链路上。

图2 静态路由与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	192.168.10.101/24	Device B	GE1/0/1	192.168.10.102/24
	GE1/0/2	192.168.20.101/24		GE1/0/2	192.168.30.101/24
	GE1/0/3	192.168.40.101/24		GE1/0/3	192.168.50.101/24
Device C	GE1/0/1	192.168.20.102/24			
	GE1/0/2	192.168.30.102/24			

4.2 配置思路

- 由于需要两端设备均支持 BFD，才能够使用控制报文方式，本例中 Device B 不支持 BFD，在 Device A 上配置的 BFD 功能仅能使用 echo 报文方式。
- echo 报文方式下必须配置 echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段，避免对端发送大量的 ICMP 重定向报文造成网络拥塞。

4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置各接口的 IP 地址

- (1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.10.101 24
[DeviceA-GigabitEthernet1/0/1] quit
```

- (2) 请参考以上方法配置图 2 中其它接口的 IP 地址，配置步骤这里省略

4.4.2 配置静态路由

- (1) 配置 Device A

配置 Device A 到 192.168.50.0/24 网段的静态路由，Device A 到 Device B 的流量优先走 Device A → L2 Switch → Device B 链路，当此链路发生故障时，流量切换到 Device A → Device C → Device B 链路上。

```
[DeviceA] ip route-static 192.168.50.0 24 gigabitethernet 1/0/1 192.168.10.102 bfd
echo-packet
[DeviceA] ip route-static 192.168.50.0 24 gigabitethernet 1/0/2 192.168.20.102
preference 65
```

- (2) 配置 Device B

配置 Device B 到 192.168.40.0/24 网段的静态路由，Device B 到 Device A 的流量优先走 Device B → L2 Switch → Device A 链路，当此链路发生故障时，流量切换到 Device B → Device C → Device A 链路上。

```
[DeviceB] ip route-static 192.168.40.0 24 gigabitethernet 1/0/1 192.168.10.101
[DeviceB] ip route-static 192.168.40.0 24 gigabitethernet 1/0/2 192.168.30.102
preference 65
```

- (3) 配置 Device C

配置 Device C 到 192.168.40.0/24 和 192.168.50.0/24 网段的静态路由。

```
[DeviceC] ip route-static 192.168.40.0 24 gigabitethernet 1/0/1 192.168.20.101
[DeviceC] ip route-static 192.168.50.0 24 gigabitethernet 1/0/2 192.168.30.101
```

4.4.3 配置 Device A 的 BFD 功能

静态路由支持的 BFD 会话方式为 echo 报文方式，该方式下必须配置 BFD echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 BFD echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段。

```
[DeviceA] bfd echo-source-ip 10.10.10.10
```

配置接口接收 BFD echo 报文的最小时间间隔为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-echo-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] quit
```

4.5 验证配置

- (1) Device A 和 Device B 设备及之间的链路均正常工作时

在 Device A 查看静态路由信息。

```
[DeviceA] display ip routing-table protocol static
```

```
Summary Count : 1
```

```
Static Routing table Status : <Active>
```

```
Summary Count : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
192.168.50.0/24	Static	65	0	192.168.20.102	GE1/0/2

```
Static Routing table Status : <Inactive>
```

```
Summary Count : 0
```

以上显示信息表示 Device A 经过 L2 Switch 到达 Device B。

查看 BFD 会话。

```
[DeviceA] display bfd session
```

```
Total Session Num: 1      Up Session Num: 1      Init Mode: Active
```

```
IPv4 Session Working Under Echo Mode:
```

LD/RD	SourceAddr	DestAddr	State	Holdtime	Interface
67	192.168.10.101	192.168.10.102	Up	2000ms	GE1/0/1

以上显示信息表示 BFD 会话已经创建。

- (2) Device B 与 L2 Switch 之间的链路出现故障时

查看静态路由。

```
[DeviceA] display ip routing-table protocol static
```

```
Summary Count : 1
```

```
Static Routing table Status : <Active>
```

```
Summary Count : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
192.168.50.0/24	Static	65	0	192.168.20.102	GE1/0/2

```
Static Routing table Status : <Inactive>
```

```
Summary Count : 0
```

以上显示信息表示 Device A 经过 Device C 到达 Device B。

4.6 配置文件

- Device A:

```

#
bfd echo-source-ip 10.10.10.10
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.10.101 255.255.255.0
bfd min-echo-receive-interval 100
bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 192.168.20.101 255.255.255.0
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 192.168.40.101 255.255.255.0
#
ip route-static 192.168.50.0 24 GigabitEthernet1/0/1 192.168.10.102 bfd echo-packet
ip route-static 192.168.50.0 24 GigabitEthernet1/0/2 192.168.20.102 preference 65
#

```

- **Device B:**

```

#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.10.102 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 192.168.30.101 255.255.255.0
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 192.168.50.101 255.255.255.0
#
ip route-static 192.168.40.0 24 GigabitEthernet1/0/1 192.168.10.101
ip route-static 192.168.40.0 24 GigabitEthernet1/0/2 192.168.30.102 preference 65
#

```

- **Device C:**

```

#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.20.102 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 192.168.30.102 255.255.255.0
#
ip route-static 192.168.40.0 24 GigabitEthernet1/0/1 192.168.20.101

```

```

ip route-static 192.168.50.0 24 GigabitEthernet1/0/2 192.168.30.101
#

```

5 RIP 与 BFD 联动配置举例

5.1 组网需求

如图3所示，某公司通过一台二层交换机作为中继将两个相距较远的部门连接。Device A、Device B、Device C 上运行 RIP，建立 RIP 邻居关系，保证网络层相互可达。

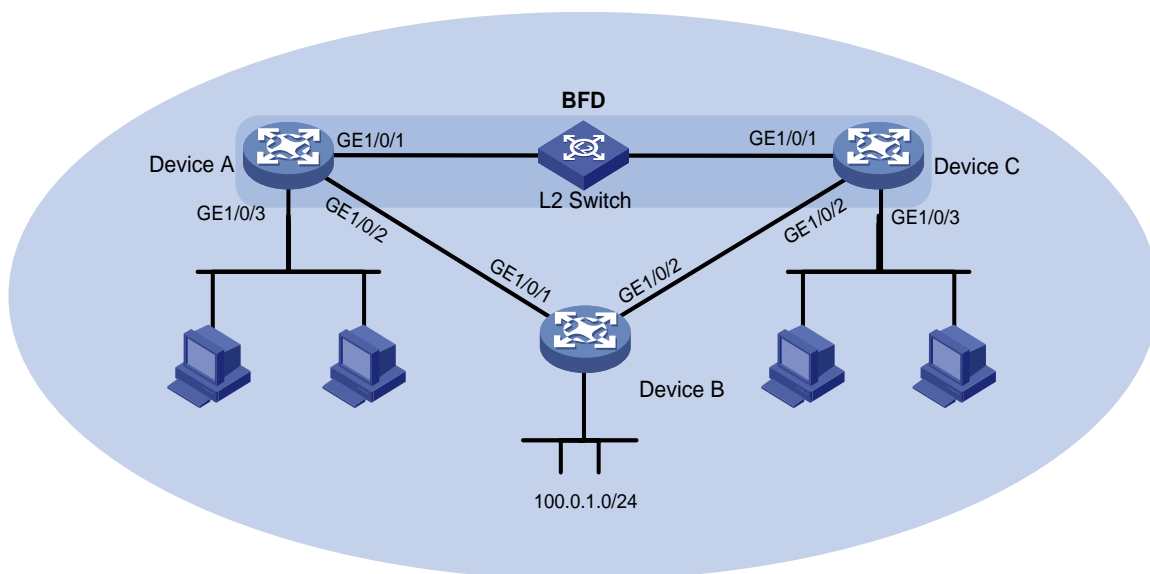
公司希望在 Device A 上使用 RIP 与 BFD 联动技术，实现当 Device C 与二层交换机之间的链路出现故障（如链路 down）时，BFD 能够快速感知并通告 RIP 协议。

已知 Device C 不支持 BFD 功能，公司希望使用 RIP 与 BFD 联动技术，采用 BFD echo 报文方式实现当 Device A 或 Device C 与二层交换机之间的链路出现故障时，BFD 能够快速感知并通告 RIP 协议。

现要求通过在 Device A 和 Device C 上配置 RIP 与 BFD 联动功能，实现：

- 监测通过 L2 Switch 通信的链路；
- 当链路出现故障时设备能够快速感知并通告 RIP 协议，快速切换到 Device B 链路进行通信。

图3 RIP 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	10.1.0.101/24	Device B	GE1/0/1	192.168.0.102/24
	GE1/0/2	192.168.0.101/24		GE1/0/2	13.1.1.101/24
	GE1/0/3	120.1.1.1/24			
Device C	GE1/0/1	10.1.0.102/24			
	GE1/0/2	13.1.1.102/24			
	GE1/0/3	121.1.1.1/24			

5.2 配置思路

- 由于需要两端设备均支持 BFD，才能够使用控制报文方式，本例中 Device C 不支持 BFD，在 Device A 上配置的 BFD 功能仅能使用 echo 报文方式。
- echo 报文方式下必须配置 echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段，避免对端发送大量的 ICMP 重定向报文造成网络拥塞。

5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 配置各接口的 IP 地址

- (1) 配置 Device A 各接口的 IP 地址

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.0.101 24
[DeviceA-Ten-GigabitEthernet3/0/1] quit
```

- (2) 请参考以上方法配置图 3 中其它接口的 IP 地址，配置步骤这里省略

5.4.2 配置 RIP 基本功能

- (1) 配置 Device A

配置 Device A 的 RIP 基本功能，引入直连路由，并使能 RIP 的 BFD 功能。

```
<DeviceA> system-view
[DeviceA] rip 1
[DeviceA-rip-1] version 2
[DeviceA-rip-1] undo summary
[DeviceA-rip-1] network 10.1.0.0
[DeviceA-rip-1] network 192.168.0.0
[DeviceA-rip-1] import-route direct
[DeviceA-rip-1] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] rip bfd enable
[DeviceA-GigabitEthernet1/0/1] quit
```

- (2) 配置 Device B

配置 Device B 的 RIP 基本功能，引入直连路由，并使能 RIP 的 BFD 功能。

```
<DeviceB> system-view
[DeviceB] rip 1
[DeviceB-rip-1] version 2
[DeviceB-rip-1] undo summary
[DeviceB-rip-1] network 192.168.0.0
[DeviceB-rip-1] network 13.1.1.0
[DeviceB-rip-1] import-route direct
```

```
[DeviceB-rip-1] quit
```

(3) 配置 Device C

配置 Device C 的 RIP 基本功能，引入直连路由，并使能 RIP 的 BFD 功能。

```
<DeviceC> system-view
[DeviceC] rip 1
[DeviceC-rip-1] version 2
[DeviceC-rip-1] undo summary
[DeviceC-rip-1] network 10.1.0.0
[DeviceC-rip-1] network 13.1.1.0
[DeviceC-rip-1] import-route direct
[DeviceC-rip-1] quit
```

5.4.3 配置 Device A 的 BFD 参数

RIP 支持的 BFD 会话方式为 echo 报文方式，该方式下必须配置 BFD echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 BFD echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段。

```
[DeviceA] bfd echo-source-ip 11.11.11.11
```

配置接口接收 BFD echo 报文的最小时间间隔为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-echo-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] quit
```

5.5 验证配置

查看 Device A 上 BFD 会话信息，显示 BFD 会话已被创建，且状态为 Up。

```
[DeviceA] display bfd session verbose
Total Session Num: 1      Up Session Num: 1      Init Mode: Active

IPv4 Session Working Under Echo Mode:
  Local Discr: 2049
  Source IP: 10.1.0.101      Destination IP: 10.1.0.102
  Session State: Up          Interface: GigabitEthernet1/0/1
  Hold Time: 218ms          Act Tx Inter: 100ms
  Min Rx Inter: 100ms       Detect Inter: 300ms
  Rx Count: 464             Tx Count: 465
  Connect Type: Direct      Running Up for: 00:00:46
  Detect Mode: Async        Slot: 0
  Protocol: RIP
  Diag Info: No Diagnostic
```

查看 Device A 上学到的路由 121.1.1.0/24，可以看到 Device A 经过 L2 Switch 到达 Device C。

```
<DeviceA> display ip routing-table 121.1.1.0 24 verbose
```

```
Summary Count : 1
```

```
Destination: 121.1.1.0/24
```



```

Protocol: RIP                Process ID: 1
SubProtID: 0x1              Age: 04h20m37s
Cost: 1                     Preference: 100
Tag: 0                      State: Active Adv
OrigTblID: 0x0             OrigVrf: default-vrf
TableID: 0x2               OrigAs: 0
NBRID: 0x26000002         LastAs: 0
AttrID: 0xffffffff         Neighbor: 10.1.0.102
Flags: 0x1008c            OrigNextHop: 10.1.0.102
Label: NULL                RealNextHop: 10.1.0.102
BkLabel: NULL              BkNextHop: N/A
Tunnel ID: Invalid         Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid       BkInterface: N/A

```

当 Device C 和二层交换机之间的链路发生故障, BFD 快速检测到链路发生变化并立刻通告 RIP。

```
%Oct 9 18:42:17:650 2013 Device A BFD/5/BFD_CHANGE_FSM: -MDC=1;Sess[10.1.0.101/10.1.0.102,
LD/RD:2049/2049, Interface: GigabitEthernet1/0/1, SessType:Echo, LinkType:INET] , Sta: UP->
DOWN, Diag:1
```

查看 Device A 上学到的路由 121.1.1.0/24, 可以看到 Device A 经过 Device B 到达 Device C。

```
<DeviceA> display ip routing-table 121.1.1.0 24 verbose
```

```
Summary Count : 1
```

```
Destination: 121.1.1.0/24
```

```

Protocol: RIP                Process ID: 2
SubProtID: 0x1              Age: 04h20m37s
Cost: 2                     Preference: 100
Tag: 0                      State: Active Adv
OrigTblID: 0x0             OrigVrf: default-vrf
TableID: 0x2               OrigAs: 0
NBRID: 0x26000002         LastAs: 0
AttrID: 0xffffffff         Neighbor: 192.168.0.102
Flags: 0x1008c            OrigNextHop: 192.168.0.102
Label: NULL                RealNextHop: 192.168.0.102
BkLabel: NULL              BkNextHop: N/A
Tunnel ID: Invalid         Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid       BkInterface: N/A

```

5.6 配置文件

- Device A:

```

#
bfd echo-source-ip 11.11.11.11
#
rip 1
undo summary
version 2
network 10.0.0.0
network 192.168.0.0

```

```

import-route direct
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.1.0.101 255.255.255.0
bfd min-transmit-interval 100
bfd min-receive-interval 100
bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 192.168.0.101 255.255.255.0
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 120.1.1.1 255.255.255.0
#

```

- **Device B:**

```

#
rip 1
undo summary
version 2
network 192.168.0.0
network 13.1.1.0
import-route direct
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 13.1.1.101 255.255.255.0
#

```

- **Device C:**

```

#
rip 1
undo summary
version 2
network 10.1.0.0
network 13.1.1.0
import-route direct
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2

```

```

port link-mode route
ip address 13.1.1.102 255.255.255.0
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 121.1.1.1 255.255.255.0
#

```

6 OSPF 与 BFD 联动配置举例

6.1 组网需求

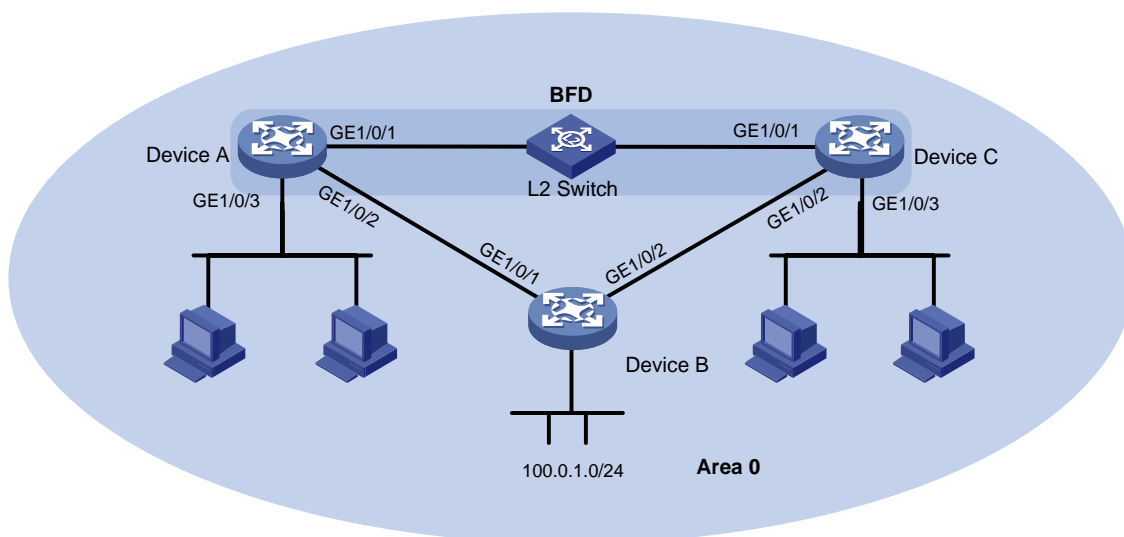
如图4所示，某公司通过一台二层交换机作为中继将两个相距较远的部门连接。Device A、Device B、Device C 上运行 OSPF，建立 OSPF 邻居关系，保证网络层相互可达。

已知 Device A 和 Device C 都支持 BFD 功能，要求使用 OSPF 与 BFD 联动技术，采用 BFD 控制报文方式实现当 Device A 或 Device C 与二层交换机之间的链路出现故障（如链路 down）时，BFD 能够快速感知并通告 OSPF 协议。

现要求通过在 Device A 和 Device C 上配置 OSPF 与 BFD 联动功能，实现：

- 监测通过 L2 Switch 通信的链路；
- 当链路出现故障时设备能够快速感知并通告 OSPF 协议，快速切换到 Device B 链路进行通信。

图4 OSPF 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	10.1.0.101/24	Device B	GE1/0/1	192.168.0.102/24
	GE1/0/2	192.168.0.101/24		GE1/0/2	13.1.1.101/24
	GE1/0/3	120.1.1.1/24			
Device C	GE1/0/1	10.1.0.102/24			
	GE1/0/2	13.1.1.102/24			
	GE1/0/3	121.1.1.1/24			

6.2 配置思路

Device A 和 Device C 都支持 BFD，可以使用 BFD 控制报文方式，通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。

6.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

6.4 配置步骤

6.4.1 配置各接口的 IP 地址

- (1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.0.101 24
[DeviceA-GigabitEthernet1/0/1] quit
```

- (2) 请参考以上方法配置图 4 中其它接口的 IP 地址，配置步骤这里省略

6.4.2 配置 OSPF 基本功能

- (1) 配置 Device A

配置 Device A 的 OSPF 基本功能，并使能 OSPF 的 BFD 功能。

```
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 120.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ospf bfd enable
[DeviceA-GigabitEthernet1/0/1] quit
```

- (2) 配置 Device B

配置 Device B 的 OSPF 基本功能。

```
[DeviceB] ospf
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

- (3) 配置 Device C

配置 Device C 的 OSPF 基本功能，并使能 OSPF 的 BFD 功能。

```
[DeviceC] ospf
[DeviceC-ospf-1] area 0
```

```
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 121.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ospf bfd enable
[DeviceC-GigabitEthernet1/0/1] quit
```

6.4.3 配置 BFD 功能

(1) 配置 Device A

配置 BFD 会话建立前的运行模式为主动模式（缺省为主动模式）。

```
[DeviceA] bfd session init-mode active
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device C

配置 BFD 会话建立前的运行模式为主动模式（缺省为主动模式）。

```
[DeviceC] bfd session init-mode active
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceC-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceC-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceC-GigabitEthernet1/0/1] quit
```

6.5 验证配置

检查 Device A 连接的主机 host A（120.1.1.2）到 Device C 连接的主机 host C（121.1.1.2）是否可达。

```
<host A> ping 121.1.1.2
PING 121.1.1.2 (121.1.1.2): 56 data bytes
56 bytes from 121.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 121.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 121.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 121.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 121.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 121.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

round-trip min/avg/max = 7.17/11.01/22.43 ms

查看 Device A 上 OSPF 邻居信息, 显示 Device A 和 Device C 已建立 OSPF 邻居关系。

[DeviceA] display ospf peer verbose

```
OSPF Process 1 with Router ID 2.2.2.2
Neighbors
```

```
Area 0.0.0.0 interface 10.1.0.101(Vlan-interface10)'s neighbors
Router ID: 1.1.1.1      Address: 10.1.0.102      GR State: Normal
  State: Full  Mode: Nbr is Slave  Priority: 1
  DR: 10.1.0.101  BDR: 10.1.0.102  MTU: 0
  Options is 0x42 (-|O|-|-|-|E|-)
  Dead timer due in 39 sec
  Neighbor is up for 00:09:01
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 5
  BFD status: Enabled(Control mode)
```

BFD 会话已被创建, 且状态为 UP。

[DeviceA] display bfd session verbose

```
Total session number: 1  Up session number: 1  Init mode: Active

IPv4 session working under Ctrl mode:
  Local Discr: 10      Remote Discr: 1
  Source IP: 10.1.0.101  Destination IP: 10.1.0.102
  Session State: Up      Interface: GigabitEthernet1/0/1
  Min Trans Inter: 100ms  Act Trans Inter: 1000ms
  Min Recv Inter: 100ms  Act Detect Inter: 5000ms
  Rx Count: 3971      Tx Count: 3776
  Connect Type: Direct  Running Up for: 00:06:52
  Hold Time: 214ms      Auth mode: None
  Detect Mode: Async      Slot: 0
  Protocol: OSPF
  Diag Info: No Diagnostic
```

[DeviceC] display bfd session verbose

```
Total session number: 1  Up session number: 1  Init mode: Active

IPv4 session working under Ctrl mode:
  Local Discr: 1      Remote Discr: 10
  Source IP: 10.1.0.102  Destination IP: 10.1.0.101
  Session State: Up      Interface: GigabitEthernet1/0/1
  Min Trans Inter: 100ms  Act Trans Inter: 1000ms
  Min Recv Inter: 100ms  Act Detect Inter: 5000ms
  Min Trans Inter: 100ms  Act Trans Inter: 1000ms
  Min Recv Inter: 100ms  Act Detect Inter: 5000ms
  Rx Count: 3971      Tx Count: 3776
  Connect Type: Direct  Running Up for: 00:06:52
```

```
Hold Time: 214ms                      Auth mode: None
Detect Mode: Async                      Slot: 0
Protocol: OSPF
Diag Info: No Diagnostic
```

在 Device A 上查看 121.1.1.0/24 的路由信息，可以看出 Device A 和 Device C 是通过 L2 Switch 进行通信的。

```
<DeviceA> display ip routing-table 121.1.1.0 verbose
```

```
Summary Count : 1
```

```
Destination: 120.1.1.0/24
```

```
Protocol: OSPF                      Process ID: 1
SubProtID: 0x1                      Age: 04h20m37s
Cost: 1                             Preference: 10
Tag: 0                              State: Active Adv
OrigTblID: 0x0                      OrigVrf: default-vrf
TableID: 0x2                       OrigAs: 0
NBRID: 0x26000002                 LastAs: 0
AttrID: 0xffffffff                Neighbor: 0.0.0.0
Flags: 0x1008c                   OrigNextHop: 10.1.0.102
Label: NULL                       RealNextHop: 10.1.0.102
BkLabel: NULL                     BkNextHop: N/A
Tunnel ID: Invalid                Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid              BkInterface: N/A
```

当 Device C 和二层交换机之间的链路状态变为 Down，BFD 快速检测到链路发生变化立刻通告 OSPF。

```
%Apr 2 11:34:26:880 2014 DeviceA BFD/5/BFD_CHANGE_FSM:
Sess[10.1.0.101/10.1.0.102,1026/1026
,GigabitEthernet1/0/1,Ctrl] , Sta: UP-> DOWN, Diag: 5
```

```
%Apr 2 11:34:27:011 2014 DeviceA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.1.0.102
GigabitEthernet1/0/1) from Full to Down.
```

查看 121.1.1.0/24 的路由信息，可以看出 Device A 和 Device C 已经切换到 Device B 进行通信。

```
<Device A> display ip routing-table 121.1.1.0 verbose
```

```
Summary Count : 1
```

```
Destination: 121.1.1.0/24
```

```
Protocol: OSPF                      Process ID: 1
SubProtID: 0x1                      Age: 04h20m37s
Cost: 2                             Preference: 10
Tag: 0                              State: Active Adv
OrigTblID: 0x0                      OrigVrf: default-vrf
TableID: 0x2                       OrigAs: 0
NBRID: 0x26000002                 LastAs: 0
AttrID: 0xffffffff                Neighbor: 0.0.0.0
Flags: 0x1008c                   OrigNextHop: 192.168.0.102
Label: NULL                       RealNextHop: 192.168.0.102
BkLabel: NULL                     BkNextHop: N/A
```

Tunnel ID: Invalid Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid BkInterface: N/A

6.6 配置文件

- Device A:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 120.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.101 255.255.255.0
 ospf bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.1.1 255.255.255.0
```

- Device B:

```
#
ospf 1
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.101 255.255.255.0
```

- Device C:

```
#
ospf 1
 area 0.0.0.0
```



```
network 10.1.0.0 0.0.0.255
network 13.1.1.0 0.0.0.255
network 121.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.1.0.102 255.255.255.0
ospf bfd enable
bfd min-transmit-interval 100
bfd min-receive-interval 100
bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 13.1.1.102 255.255.255.0
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 121.1.1.1 255.255.255.0
#
```

7 IS-IS 与 BFD 联动配置举例

7.1 组网需求

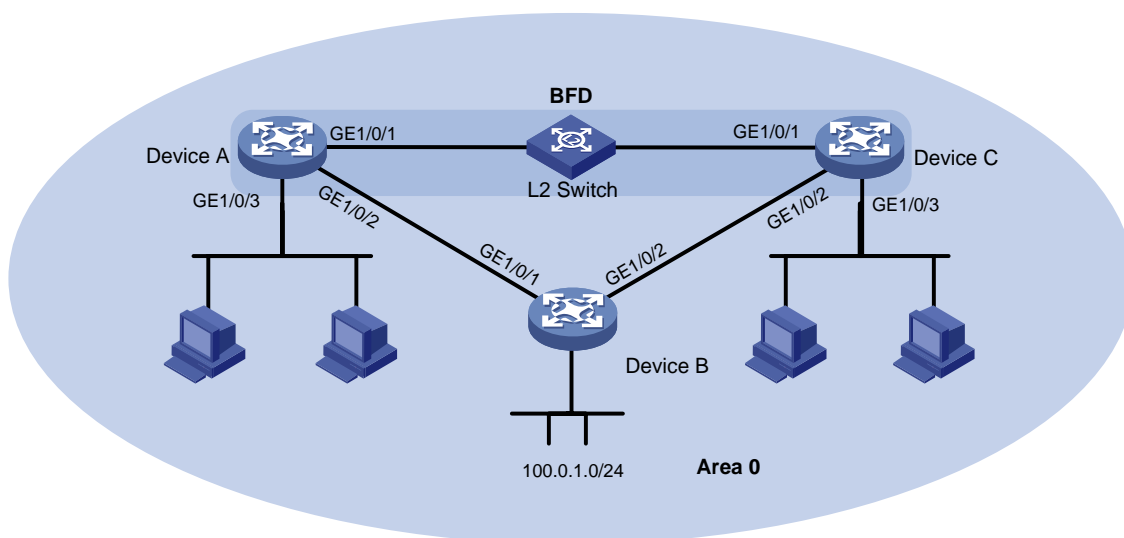
如[图 5](#)所示，某公司通过一台二层交换机作为中继将两个相距较远的部门连接。Device A、Device B、Device C 上运行 IS-IS，建立 IS-IS 邻居关系，保证网络层相互可达。

已知 Device A 和 Device C 都支持 BFD 功能，公司希望使用 IS-IS 与 BFD 联动技术，采用 BFD 控制报文方式实现当 Device A 或 Device C 与二层交换机之间的链路出现故障（如链路 down）时，BFD 能够快速感知并通告 IS-IS 协议。

现要求通过在 Device A 和 Device C 上配置 IS-IS 与 BFD 联动功能，实现：

- 监测通过 L2 Switch 通信的链路；
- 当链路出现故障时设备能够快速感知并通告 IS-IS 协议，快速切换到 Device B 链路进行通信。

图5 IS-IS 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	GE1/0/1	10.1.0.101/24	Device B	GE1/0/1	192.168.0.102/24
	GE1/0/2	192.168.0.101/24		GE1/0/2	13.1.1.101/24
	GE1/0/3	120.1.1.1/24			
Device C	GE1/0/1	10.1.0.102/24			
	GE1/0/2	13.1.1.102/24			
	GE1/0/3	121.1.1.1/24			

7.2 配置思路

Device A 和 Device C 都支持 BFD，可以使用 BFD 控制报文方式，通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。

7.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

7.4 配置步骤

7.4.1 配置各接口的 IP 地址

- (1) 配置 Device A 各接口的 IP 地址

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.0.101 24
[DeviceA-GigabitEthernet1/0/1] quit
```

- (2) 请参考以上方法配置图 5 中其它接口的 IP 地址，配置步骤这里省略

7.4.2 配置 IS-IS 基本功能

- (1) 配置 Device A

配置 Device A 的 IS-IS 基本功能，并使能 IS-IS 的 BFD 功能。

```
[DeviceA] isis
[DeviceA-isis-1] network-entity 10.0000.0000.0001.00
[DeviceA-isis-1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] isis enable
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] isis enable
[DeviceA-GigabitEthernet1/0/1] isis bfd enable
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device B

配置 Device B 的 IS-IS 基本功能。

```
[DeviceB] isis
[DeviceB-isis-1] network-entity 10.0000.0000.0003.00
[DeviceB-isis-1] quit
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] isis enable
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] isis enable
[DeviceB-GigabitEthernet1/0/2] quit
```

(3) 配置 Device C

配置 Device C 的 IS-IS 基本功能，并使能 IS-IS 的 BFD 功能。

```
[DeviceC] isis
[DeviceC-isis-1] network-entity 10.0000.0000.0002.00
[DeviceC-isis-1] quit
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] isis enable
[DeviceC-GigabitEthernet1/0/1] isis bfd enable
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] isis enable
[DeviceC-GigabitEthernet1/0/2] quit
```

7.4.3 配置 BFD 功能

(1) 配置 Device A

配置 BFD 会话建立前的运行模式为主动模式（缺省为主动模式）。

```
[DeviceA] bfd session init-mode active
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] bfd min-transmit-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd min-receive-interval 100
[DeviceA-GigabitEthernet1/0/1] bfd detect-multiplier 3
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device C

配置 BFD 会话建立前的运行模式为主动模式（缺省为主动模式）。

```
[DeviceC] bfd session init-mode active
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceC] interface gigabitethernet 1/0/1
```

```
[DeviceC-GigabitEthernet1/0/1] bfd min-transmit-interval 100
```

```
[DeviceC-GigabitEthernet1/0/1] bfd min-receive-interval 100
```

```
[DeviceC-GigabitEthernet1/0/1] bfd detect-multiplier 3
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

7.5 验证配置

查看 Device A 上 IS-IS 邻居信息，显示 Device A 和 Device C 已建立 IS-IS 邻居关系。

```
[DeviceA] display isis peer verbose
```

```
Peer information for IS-IS(1)
-----

System ID: 0000.0000.0002
Interface: GigabitEthernet1/0/1      Circuit Id: 0000.0000.0002.01
State: Up      HoldTime: 6s      Type: L1(L1L2)      PRI: 64
Area address(es): 00
Peer IP address(es): 10.1.0.102
Peer local circuit ID: 1
Peer circuit SNPA address: ce9d-d91d-d100
Uptime: 00:01:19
Adj protocol: IPv4
Graceful Restart capable
  Restarting signal: No
  Suppress adjacency advertisement: No
Local topology:
  0
Remote topology:
  0
```

查看 Device A 和 Device C 上 BFD 会话信息，显示 BFD 会话已被创建，且状态为 Up。

```
[DeviceA] display bfd session verbose
```

```
Total Session Num: 1      Up Session Num: 1      Init Mode: Active

IPv4 Session Working Under Ctrl Mode:
  Local Discr: 2049      Remote Discr: 2049
  Source IP: 10.1.0.101      Destination IP: 10.1.0.102
Session State: Up      Interface: GigabitEthernet1/0/1
  Min Tx Inter: 100ms      Act Tx Inter: 1000ms
  Min Rx Inter: 100ms      Detect Inter: 5000ms
  Rx Count: 3693      Tx Count: 3703
  Connect Type: Direct      Running Up for: 00:06:09
  Hold Time: 201ms      Auth mode: None
```

```

Detect Mode: Async                               Slot: 0
Protocol: ISIS_BR_L1/ISIS_BR_L2
Diag Info: No Diagnostic
[DeviceC] display bfd session verbose
Total Session Num: 1      Up Session Num: 1      Init Mode: Active

IPv4 Session Working Under Ctrl Mode:
Local Discr: 2049                               Remote Discr: 2049
Source IP: 10.1.0.102                           Destination IP: 10.1.0.101
Session State: Up                               Interface: GigabitEthernet1/0/1
Min Tx Inter: 100ms                             Act Tx Inter: 1000ms
Min Rx Inter: 100ms                             Detect Inter: 5000ms
Rx Count: 4299                                  Tx Count: 4299
Connect Type: Direct                             Running Up for: 00:07:10
Hold Time: 210ms                                Auth mode: None
Detect Mode: Async                               Slot: 0
Protocol: ISIS_BR_L1/ISIS_BR_L2
Diag Info: No Diagnostic

```

在 Device A 上查看 121.1.1.0/24 的路由信息，可以看出 Device A 和 Device C 是通过 L2 Switch 进行通信的。

```
<DeviceA> display ip routing-table 121.1.1.0 verbose
```

```
Summary Count : 1
```

```

Destination: 121.1.1.0/24
Protocol: isis                                Process ID: 1
SubProtID: 0x1                               Age: 04h20m37s
Cost: 20                                     Preference: 15
Tag: 0                                       State: Active Adv
OrigTblID: 0x2                               OrigVrf: default-vrf
TableID: 0x2                                 OrigAs: 0
NBRID: 0x26000002                           LastAs: 0
AttrID: 0xffffffff                          Neighbor: 0.0.0.0
Flags: 0x1008c                               OrigNextHop: 10.1.0.102
Label: NULL                                  RealNextHop: 10.1.0.102
BkLabel: NULL                                BkNextHop: N/A
Tunnel ID: Invalid                           Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid                         BkInterface: N/A

```

当 Device C 和二层交换机之间的链路 Down 了，BFD 快速检测到链路发生变化并立刻通告 IS-IS。

```

%Oct 9 16:11:24:163 2013 DeviceC BFD/5/BFD_CHANGE_FSM: -MDC=1; Sess[10.1.0.102/10.1.0.101,
LD/RD:2049/2049, Interface: GigabitEthernet1/0/1, SessType:Ctrl, LinkType:INET] , S
ta: UP-> DOWN, Diag: 1
%Oct 9 16:11:24:164 2013 DeviceC ISIS/5/ISIS_NBR_CHG: -MDC=1; IS-IS 1, Level-1 adj
acency 0000.0000.0001 (GigabitEthernet1/0/1), state change to: DOWN.
%Oct 9 16:11:24:164 2013 DeviceC ISIS/5/ISIS_NBR_CHG: -MDC=1; IS-IS 1, Level-2 adj
acency 0000.0000.0001 (GigabitEthernet1/0/1), state change to: DOWN.

```

7.6 配置文件

- **Device A:**

```
#
isis 1
 network-entity 10.0000.0000.0001.00
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.101 255.255.255.0
isis enable 1
 isis bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.1.1 255.255.255.0
#
```

- **Device B:**

```
#
isis 1
 network-entity 10.0000.0000.0003.00
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.102 255.255.255.0
isis enable 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.101 255.255.255.0
isis enable 1
#
```

- **Device C:**

```
#
isis 1
 network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet1/0/1
 port link-mode route
```

```

ip address 10.1.0.102 255.255.255.0
isis enable 1
isis bfd enable
bfd min-transmit-interval 100
bfd min-receive-interval 100
bfd detect-multiplier 3
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 13.1.1.102 255.255.255.0
isis enable 1
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 121.1.1.1 255.255.255.0
#

```

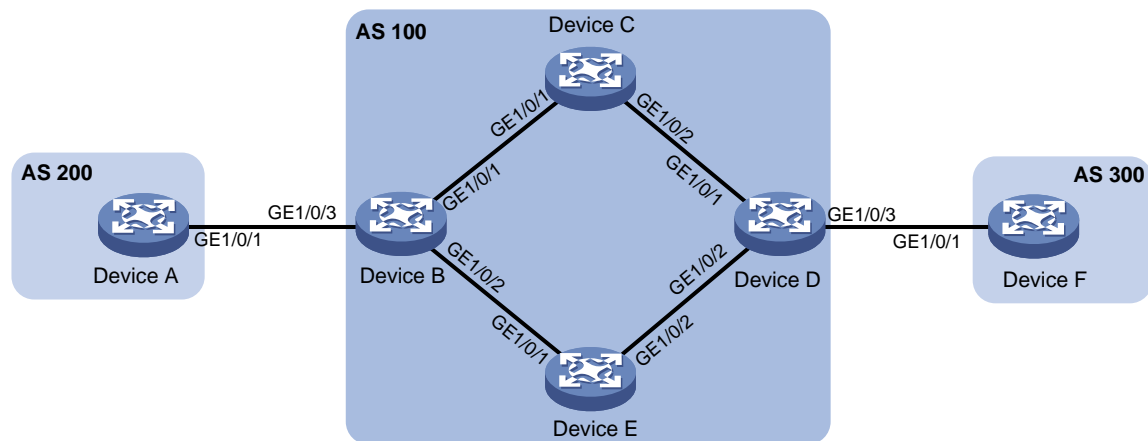
8 BGP 与 BFD 联动配置举例

8.1 组网需求

如图 6 所示，某公司的两个部门相距较远，Device A 和 Device F 分别作为这两个部门的出口设备，现通过部署 BGP，使两个部门可以进行业务通信。已知 Device B 和 Device D 都支持 BFD 功能，公司希望使用 BGP 与 BFD 联动技术，采用 BFD 控制报文方式检测 AS 200 与 AS 300 之间通信的主链路状态，实现当 Device B 或 Device D 之间的链路出现故障（如链路 down）时，BFD 能够快速感知并通告 BGP 协议。具体要求如下：

- 在 AS 100 内使用 OSPF 作为 IGP。
- 配置 Device B<->Device C<->Device D 链路作为主链路，负责转发 Device A 和 Device F 之间的流量，并采用 BFD 控制报文的方式检测主链路。
- 当主链路发生故障时，BFD 能够快速检测并通告 BGP 协议，使得迅速切换到 Device B<->Device E<->Device D 这条路径进行通信。

图6 BGP 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
----	----	------	----	----	------

Device A	GE1/0/1	120.1.0.1/24	Device D	GE1/0/1	10.2.0.101/24
Device B	GE1/0/1	10.1.0.101/24		GE1/0/2	13.1.1.101/24
	GE1/0/2	192.168.0.101/24		GE1/0/3	120.2.0.2/24
	GE1/0/3	120.1.0.2/24	Device E	GE1/0/1	192.168.0.102/24
Device C	GE1/0/1	10.1.0.102/24		GE1/0/2	13.1.1.102/24
	GE1/0/2	10.2.0.102/24	Device F	GE1/0/1	120.2.0.1/24

8.2 配置思路

- Device B 和 Device D 都支持 BFD，可以使用 BFD 控制报文方式，通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。
- 为了使 Device B<->Device C<->Device D 成为主链路，需要通过路由策略配置其路由开销低于链路 Device B<->Device E<->Device D 的路由开销。

8.3 配置步骤

8.3.1 配置各接口的 IP 地址

- (1) 配置 Device A 各接口的 IP 地址

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 120.1.0.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

- (2) 请参考以上方法配置图 6 中其它接口的 IP 地址，配置步骤这里省略

8.3.2 在 AS 100 内配置 OSPF 功能，保证设备间路由可达

- (1) 配置 Device B

```
[DeviceB] ospf
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

- (2) 配置 Device C

```
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

- (3) 配置 Device D

```
[DeviceD] ospf
[DeviceD-ospf-1] import-route direct
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
```



```
[DeviceD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

(4) 配置 Device E

```
[DeviceE] ospf
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

8.3.3 配置 BGP 功能

(1) 配置 Device A

启动 BGP，指定本地 AS 号为 200。

```
[DeviceA] bgp 200
[DeviceA-bgp] router-id 1.1.1.1
```

配置 Device A 和 Device B 建立 EBGP 连接。

```
[DeviceA-bgp] peer 120.1.0.2 as-number 100
```

创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

```
[DeviceA-bgp] address-family ipv4 unicast
```

在 BGP IPv4 单播地址族视图下，将本地路由表中到达 120.1.0.0/24 网段的路由添加到 BGP 路由表中。

```
[DeviceA-bgp-ipv4] network 120.1.0.0 255.255.255.0
```

使能 Device A 与对等体 120.1.0.2 交换 IPv4 单播路由信息的能力。

```
[DeviceA-bgp-ipv4] peer 120.1.0.2 enable
[DeviceA-bgp-ipv4] quit
```

(2) 配置 Device B

启动 BGP，指定本地 AS 号为 100。

```
[DeviceB] bgp 100
[DeviceB-bgp] router-id 2.2.2.2
```

配置 Device B 和 Device A 建立 EBGP 连接。

```
[DeviceB-bgp] peer 120.1.0.1 as-number 200
```

配置 Device B 和 Device D 建立 IBGP 连接。

```
[DeviceB-bgp] peer 10.2.0.101 as-number 100
[DeviceB-bgp] peer 13.1.1.101 as-number 100
```

创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。

```
[DeviceB-bgp] address-family ipv4 unicast
```

使能 Device B 与对等体 10.2.0.101 交换 IPv4 单播路由信息的能力。

```
[DeviceB-bgp-ipv4] peer 10.2.0.101 enable
```

在 BGP IPv4 单播地址族视图下，配置向对等体 10.2.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。

```
[DeviceB-bgp-ipv4] peer 10.2.0.101 next-hop-local
```

使能 Device B 与对等体 13.1.1.101 交换 IPv4 单播路由信息的能力。

```
[DeviceB-bgp-ipv4] peer 13.1.1.101 enable
# 在 BGP IPv4 单播地址族视图下，配置向对等体 13.1.1.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。
[DeviceB-bgp-ipv4] peer 13.1.1.101 next-hop-local
# 使能 Device B 与对等体 120.1.0.1 交换 IPv4 单播路由信息的能力。
[DeviceB-bgp-ipv4] peer 120.1.0.1 enable
[DeviceB-bgp-ipv4] quit
```

(3) 配置 Device D

```
# 启动 BGP，指定本地 AS 号为 100。
[DeviceD] bgp 100
[DeviceD-bgp] router-id 4.4.4.4
# 配置 Device D 和 Device B 建立 IBGP 连接。
[DeviceD-bgp] peer 10.1.0.101 as-number 100
[DeviceD-bgp] peer 192.168.0.101 as-number 100
# 配置 Device D 和 Device F 建立 EBGP 连接。
[DeviceD-bgp] peer 120.2.0.1 as-number 300
# 创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。
[DeviceD-bgp] address-family ipv4 unicast
# 使能 Device D 与对等体 10.1.0.101 交换 IPv4 单播路由信息的能力。
[DeviceD-bgp-ipv4] peer 10.1.0.101 enable
# 在 BGP IPv4 单播地址族视图下，配置向对等体 10.1.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。
[DeviceD-bgp-ipv4] peer 10.1.0.101 next-hop-local
# 使能 Device D 与对等体 192.168.0.101 交换 IPv4 单播路由信息的能力。
[DeviceD-bgp-ipv4] peer 192.168.0.101 enable
# 在 BGP IPv4 单播地址族视图下，配置向对等体 192.168.0.101 发布 BGP 路由时，将下一跳属性修改为自身的地址。
[DeviceD-bgp-ipv4] peer 192.168.0.101 next-hop-local
# 使能 Device D 与对等体 120.2.0.1 交换 IPv4 单播路由信息的能力。
[DeviceD-bgp-ipv4] peer 120.2.0.1 enable
[DeviceD-bgp-ipv4] quit
```

(4) 配置 Device F

```
#启动 BGP，指定本地 AS 号为 300。
[DeviceF] bgp 300
[DeviceF-bgp] router-id 6.6.6.6
# 配置 Device F 和 Device D 建立 EBGP 连接。
[DeviceF-bgp] peer 120.2.0.2 as-number 100
# 创建 BGP IPv4 单播地址族，并进入 BGP IPv4 单播地址族视图。
[DeviceF-bgp] address-family ipv4 unicast
# 在 BGP IPv4 单播地址族视图下，将本地路由表中到达 120.2.0.0/24 网段的路由添加到 BGP 路由表中。
[DeviceF-bgp-ipv4] network 120.2.0.0 255.255.255.0
# 使能 Device F 与对等体 120.2.0.2 交换 IPv4 单播路由信息的能力。
```

```
[DeviceF-bgp-ipv4] peer 120.2.0.2 enable
[DeviceF-bgp-ipv4] quit
```

8.3.4 配置路由策略

(1) 配置 Device B

创建 ACL 2000，允许源 IP 地址为 120.1.0.0/24 的报文通过。

```
[DeviceB] acl number 2000
[DeviceB-acl-basic-2000] rule permit source 120.1.0.0 0.0.0.255
[DeviceB-acl-basic-2000] quit
```

配置向对等体 10.2.0.101 发布的路由设置本地优先级为 200，并配置 IBGP 路由优先级为 100。

```
[DeviceB] route-policy local-pre permit node 10
[DeviceB-route-policy-local-pre] if-match ip address acl 2000
[DeviceB-route-policy-local-pre] apply local-preference 200
[DeviceB-route-policy-local-pre] quit
[DeviceB] bgp 100
[DeviceB-bgp] address-family ipv4 unicast
[DeviceB-bgp-ipv4] peer 10.2.0.101 route-policy local-pre export
[DeviceB-bgp-ipv4] preference 255 100 130
[DeviceB-bgp-ipv4] quit
```

(2) 配置 Device D

创建 ACL 2000，允许源 IP 地址为 120.2.0.0/24 的报文通过。

```
[DeviceD] acl number 2000
[DeviceD-acl-basic-2000] rule permit source 120.2.0.0 0.0.0.255
[DeviceD-acl-basic-2000] quit
```

配置向对等体 10.1.0.101 发布的路由设置本地优先级为 200，并配置 IBGP 路由优先级为 100。

```
[DeviceD] route-policy local-pre permit node 10
[DeviceD-route-policy-local-pre] if-match ip address acl 2000
[DeviceD-route-policy-local-pre] apply local-preference 200
[DeviceD-route-policy-local-pre] quit
[DeviceD] bgp 100
[DeviceD-bgp] address-family ipv4 unicast
[DeviceD-bgp-ipv4] peer 10.1.0.101 route-policy local-pre export
[DeviceD-bgp-ipv4] preference 255 100 130
[DeviceD-bgp-ipv4] quit
```

8.3.5 配置 BFD 功能

(1) 配置 Device B

```
[DeviceB] bgp 100
[DeviceB-bgp] peer 10.2.0.101 bfd
[DeviceB-bgp] quit
```

(2) 配置 Device D

```
[DeviceD] bgp 100
[DeviceD-bgp] peer 10.1.0.101 bfd
```

```
[DeviceD-bgp] quit
```

8.4 验证配置

从 Device A 上 ping Device F 的 IP 地址，可以互通。

```
[DeviceA] ping 120.2.0.1
Ping 120.2.0.1 (120.2.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=1.189 ms
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=1.095 ms
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=1.086 ms
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=1.097 ms
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=1.089 ms
```

```
--- Ping statistics for 120.2.0.1 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.086/1.111/1.189/0.039 ms
```

在 Device B 上通过命令 **display bgp peer** 查看 BGP 对等体信息，可以看到 Device B 与 Device D 建立 IBGP 连接，Device B 与 Device A 建立 EBGP 连接，且均处于 Established 状态。

```
[DeviceB] display bgp peer ipv4
```

```
BGP local router ID: 2.2.2.2
```

```
Local AS number: 100
```

```
Total number of peers: 3
```

```
Peers in established state: 3
```

Peer	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
10.2.0.101	100	6	4	0	1	00:00:56	Established
13.1.1.101	100	6	5	0	1	00:00:56	Established
120.1.0.1	200	6	5	0	1	00:00:56	Established

查看 Device B 上 BFD 会话信息，显示 BFD 会话已被创建，且状态为 Up。

```
[DeviceB] display bfd session verbose
```

```
Total Session Num: 1      Up Session Num: 0      Init Mode: Active
```

```
IPv4 Session Working Under Ctrl Mode:
```

```
Local Discr: 2049
```

```
Remote Discr: 0
```

```
Source IP: 10.1.0.101
```

```
Destination IP: 10.2.0.101
```

```
Session State: UP
```

```
Interface: N/A
```

```
Min Tx Inter: 1000ms
```

```
Act Tx Inter: 1000ms
```

```
Min Rx Inter: 1000ms
```

```
Detect Inter: 5000ms
```

```
Rx Count: 0
```

```
Tx Count: 910
```

```
Connect Type: Indirect
```

```
Running Up for: 00:00:00
```

```
Hold Time: 0ms
```

```
Auth mode: None
```

```
Detect Mode: Async
```

```
Slot: 0
```

```
Protocol: BGP
```

```
Diag Info: No Diagnostic
```

在 Device B 上查看 120.2.0.0/24 的路由信息，可以看出 Device B 通过 Device B<—>Device C<—>Device D 这条路径与 120.2.0.0/24 网段通信。

[DeviceB] display ip routing-table 120.2.0.0 24 verbose

Summary Count : 3

Destination: 120.2.0.0/24

Protocol: BGP	Process ID: 0
SubProtID: 0x1	Age: 00h24m48s
Cost: 0	Preference: 100
Tag: 0	State: Active Adv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0x2	OrigAs: 300
NibID: 0x15000001	LastAs: 300
AttrID: 0x1	Neighbor: 10.2.0.101
Flags: 0x10060	OrigNextHop: 10.2.0.101
Label: NULL	RealNextHop: 10.1.0.102
BkLabel: NULL	BkNextHop: N/A
Tunnel ID: Invalid	Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid	BkInterface: N/A

Destination: 120.2.0.0/24

Protocol: OSPF	Process ID: 1
SubProtID: 0x8	Age: 00h26m19s
Cost: 1	Preference: 150
Tag: 1	State: Inactive Adv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0x2	OrigAs: 0
NibID: 0x13000005	LastAs: 0
AttrID: 0xffffffff	Neighbor: 0.0.0.0
Flags: 0x41	OrigNextHop: 10.1.0.102
Label: NULL	RealNextHop: 10.1.0.102
BkLabel: NULL	BkNextHop: N/A
Tunnel ID: Invalid	Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid	BkInterface: N/A

Destination: 120.2.0.0/24

Protocol: OSPF	Process ID: 1
SubProtID: 0x8	Age: 00h26m19s
Cost: 1	Preference: 150
Tag: 1	State: Inactive Adv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0x2	OrigAs: 0
NibID: 0x13000003	LastAs: 0
AttrID: 0xffffffff	Neighbor: 0.0.0.0
Flags: 0x41	OrigNextHop: 192.168.0.102
Label: NULL	RealNextHop: 192.168.0.102
BkLabel: NULL	BkNextHop: N/A
Tunnel ID: Invalid	Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid	BkInterface: N/A

在 Device B<—>Device C<—>Device D 链路发生故障后，从 Device A 上 ping Device F 的 IP 地址，可以互通。

```
<DeviceA> ping 120.2.0.1
Ping 120.1.0.1 (120.2.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=0.680 ms
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=0.295 ms
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=0.423 ms
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=0.464 ms
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=0.445 ms
```

```
--- Ping statistics for 120.2.0.1 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.295/0.461/0.680/0.124 ms
```

在 Device B 上查看 120.2.0.0/24 的路由信息，可以看出 Device B 通过 Device B<—>Device E<—>Device D 这条路径与 120.2.0.0/24 网段通信。

```
<DeviceB> display ip routing-table 120.2.0.0 24 verbose
```

```
Summary Count : 2
```

```
Destination: 120.2.0.0/24
```

Protocol: BGP	Process ID: 0
SubProtID: 0x1	Age: 00h00m18s
Cost: 0	Preference: 100
Tag: 0	State: Active Adv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0x2	OrigAs: 300
NibID: 0x15000001	LastAs: 300
AttrID: 0x1	Neighbor: 10.2.0.101
Flags: 0x10060	OrigNextHop: 10.2.0.101
Label: NULL	RealNextHop: 192.168.0.102
BkLabel: NULL	BkNextHop: N/A
Tunnel ID: Invalid	Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid	BkInterface: N/A

```
Destination: 120.2.0.0/24
```

Protocol: OSPF	Process ID: 1
SubProtID: 0x8	Age: 00h00m18s
Cost: 1	Preference: 150
Tag: 1	State: Inactive Adv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0x2	OrigAs: 0
NibID: 0x13000001	LastAs: 0
AttrID: 0xffffffff	Neighbor: 0.0.0.0
Flags: 0x41	OrigNextHop: 192.168.0.102
Label: NULL	RealNextHop: 192.168.0.102
BkLabel: NULL	BkNextHop: N/A
Tunnel ID: Invalid	Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid	BkInterface: N/A

8.5 配置文件

- Device A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 120.1.0.1 255.255.255.0
#
bgp 200
 router-id 1.1.1.1
 peer 120.1.0.2 as-number 200
#
 address-family ipv4 unicast
  network 120.1.0.0 255.255.255.0
  peer 120.1.0.2 enable
```

- Device B:

```
#
ospf 1
import-route direct
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.0.101 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 192.168.0.101 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 120.1.0.2 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 10.2.0.101 as-number 100
 peer 10.2.0.101 bfd
 peer 13.1.1.101 as-number 100
 peer 120.1.0.1 as-number 200
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.2.0.101 enable
  peer 10.2.0.101 next-hop-local
  peer 10.2.0.101 route-policy local-pre export
```

```

peer 13.1.1.101 enable
peer 13.1.1.101 next-hop-local
peer 120.1.0.1 enable
#
route-policy local-pre permit node 10
  if-match ip address acl 2000
  apply local-preference 200
#
acl number 2000
  rule 0 permit source 120.1.0.0 0.0.0.255
#

```

- **Device C:**

```

#
ospf 1
  area 0.0.0.0
    network 10.1.0.0 0.0.0.255
    network 10.2.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 10.2.0.102 255.255.255.0
#

```

- **Device D**

```

#
ospf 1
  import-route direct
  area 0.0.0.0
    network 10.2.0.0 0.0.0.255
    network 13.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 10.2.0.101 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 13.1.1.101 255.255.255.0
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip address 120.1.0.2 255.255.255.0
#
bgp 100
  router-id 4.4.4.4

```



```

peer 10.1.0.101 as-number 100
peer 10.1.0.101 bfd
peer 120.2.0.1 as-number 300
peer 192.168.0.101 as-number 100
#
address-family ipv4 unicast
  preference 255 100 130
  peer 10.1.0.101 enable
  peer 10.1.0.101 next-hop-local
  peer 10.1.0.101 route-policy local-pre export
  peer 192.168.0.101 enable
  peer 192.168.0.101 next-hop-local
  peer 120.2.0.1 enable
#
acl number 2000
  rule 0 permit source 120.2.0.0 0.0.0.255
#

```

- **Device E:**

```

#
ospf 1
  area 0.0.0.0
    network 13.1.1.0 0.0.0.255
    network 192.168.0.0 0.0.0.255
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 192.168.0.102 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 13.1.1.102 255.255.255.0
#

```

- **Device F:**

```

#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 120.2.0.1 255.255.255.0
#
bgp 300
  router-id 6.6.6.6
  peer 120.2.0.2 as-number 100
#
address-family ipv4 unicast
  network 120.2.0.0 255.255.255.0
  peer 120.2.0.2 enable
#

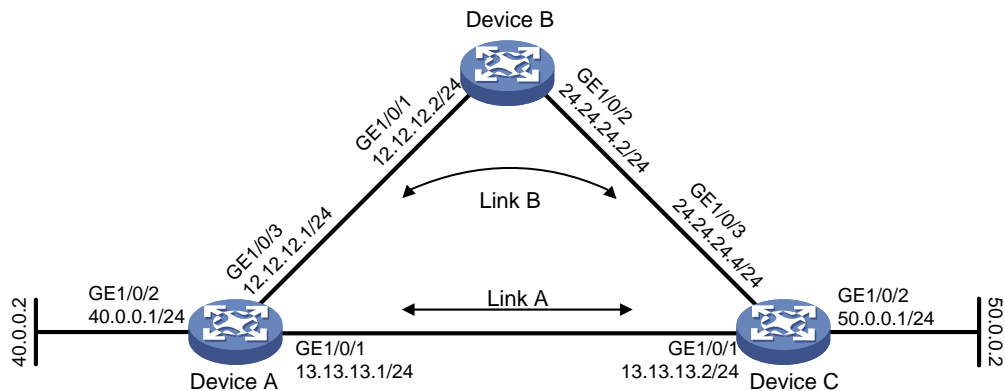
```

9 策略路由与 BFD 联动配置举例

9.1 组网需求

某公司内部网络如图7所示，从 Device A 到 Device C 有两条转发路径：Link A 和 Link B。下一跳分别为 Device B 和 Device C。Link A 为直连链路，Link B 为非直连链路。已知 Device C 不支持 BFD 功能，公司希望使用策略路由与 BFD 联动技术，实现源 IP 为 40.0.0.2 的报文优先选择 Link B，当 Device A 和 Device B 的链路出现故障（如链路 down）时，Device A 能快速感知，并将流量切换到 Link A 的链路上。

图7 策略路由与 BFD 联动配置组网图



9.2 配置思路

- 由于需要两端设备均支持 BFD，才能够使用控制报文方式，本例中 Device C 不支持 BFD，在 Device A 上配置的 BFD 功能仅能使用 echo 报文方式。
- echo 报文方式下必须配置 echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段，避免对端发送大量的 ICMP 重定向报文造成网络拥塞。

9.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

9.4 配置步骤

9.4.1 配置各接口的 IP 地址

- (1) 配置 Device A 各接口的 IP 地址

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 40.0.0.1 24
[DeviceA-GigabitEthernet1/0/2] quit
```

- (2) 请参考以上方法配置图7中其它接口的 IP 地址，配置步骤这里省略

9.4.2 配置静态路由

(1) 配置 Device A

配置 Device A 到 Device C 50.0.0.0 网段的静态路由。

```
[DeviceA] ip route-static 50.0.0.0 24 gigabitethernet 1/0/1 13.13.13.2
```

(2) 配置 Device B

配置 Device B 到 Device C 50.0.0.0 网段的静态路由。

```
[DeviceB] ip route-static 50.0.0.0 24 gigabitethernet 1/0/2 24.24.24.4
```

9.4.3 配置 Device A 上的路由策略

配置匹配源 IP 地址为 40.0.0.2 的 IP 报文的 ACL 规则。

```
[DeviceA] acl number 3010
```

```
[DeviceA-acl-adv-3010] rule 0 permit ip source 40.0.0.2 0
```

```
[DeviceA-acl-adv-3010] quit
```

配置策略路由由 aaa，使满足 ACL 规则报文的下一跳为 12.12.12.2，并与 track 11 绑定。

```
[DeviceA] policy-based-route aaa permit node 5
```

```
[DeviceA-pbr-aaa-5] if-match acl 3010
```

```
[DeviceA-pbr-aaa-5] apply next-hop 12.12.12.2 track 11
```

```
[DeviceA-pbr-aaa-5] quit
```

在接口上应用路由策略 aaa。

```
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] ip policy-based-route aaa
```

```
[DeviceA-GigabitEthernet1/0/2] quit
```

9.4.4 配置 BFD 功能，并创建和 BFD 会话关联的 Track 项 11，检测 Device B 是否可达

策略路由支持的 BFD 会话方式为 echo 报文方式，该方式下必须配置 BFD echo 报文的源 IP 地址。IP 地址可以任意指定，不需要与实际接口地址对应。建议不要将 BFD echo 报文的源 IP 地址配置为属于该设备任何一个接口所在网段。

```
[DeviceA] bfd echo-source-ip 3.3.3.3
```

配置发送和接收单跳 BFD 控制报文的最小时间间隔都为 100ms，单跳 BFD 检测时间倍数为 3。

```
[DeviceA] interface gigabitethernet 1/0/3
```

```
[DeviceA-GigabitEthernet1/0/3] bfd min-echo-receive-interval 100
```

```
[DeviceA-GigabitEthernet1/0/3] bfd detect-multiplier 3
```

```
[DeviceA-GigabitEthernet1/0/3] quit
```

```
[DeviceA] track 11 bfd echo interface gigabitethernet 1/0/3 remote ip 12.12.12.2 local ip 12.12.12.1
```

9.5 验证配置

查看 Device A 上源地址为 40.0.0.0 网段的流量，可以看到该网段当前流量优先从 GigabitEthernet1/0/3 接口（即 Link B）转发出去。

```
<DeviceA> reset counters interface
```

```
<DeviceA> display counters outbound interface
```

```
Interface          Total (pkts)   Broadcast (pkts)   Multicast (pkts)   Err (pkts)
```

```

GE1/0/1          0          0          0          0
GE1/0/2          585414      0          0          0
GE1/0/3          0          0          0          0

```

查看 BFD 会话信息，显示 BFD 会话已被创建，且状态为 Up。

```
[DeviceA] display bfd session verbose
```

```
Total Session Num: 1      Up Session Num: 1      Init Mode: Active
```

```
IPv4 Session Working Under Echo Mode:
```

```

Local Discr: 2049
Source IP: 12.12.12.1      Destination IP: 12.12.12.2
Session State: Up          Interface: GigabitEthernet1/0/3
Min Tx Inter: 1000ms      Act Tx Inter: 1000ms
Min Rx Inter: 100ms       Detect Inter: 5000ms
Rx Count: 128234          Tx Count: 371950
Connect Type: Direct      Running Up for: 00:01:04
Detect Mode: Async        Chassis/Slot: 1/0
Protocol: TRACK
Diag Info: No Diagnostic

```

当 Device A 和 Device B 间链路故障后，BFD 会话 Down。

```
%Dec 10 16:39:46:210 2013 DeviceA BFD/5/BFD_CHANGE_FSM: -MDC=1; Sess[12.12.12.1/12.12.12.2, LD/RD:2049/2049, Interface: GigabitEthernet1/0/3, SessType:Echo, LinkType:INET] , S
```

```
ta: UP-> DOWN, Diag: 1
```

```
%Dec 10 16:39:47:342 2013 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; GigabitEtherne2/0/3 link status is down.
```

```
%Dec 10 16:39:47:343 2013 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol on the interface GigabitEthernet1/0/3 is down.
```

```
%Dec 10 16:39:47:343 2013 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; GigabitEthernet1/0/3 link status is down.
```

清除流量后重新查看 Device A 上源地址为 40.0.0.0 网段的流量，可以看到当前流量从 GigabitEthernet1/0/1 接口（即 Link A）转发出去。

```
<DeviceA> reset counters interface
```

```
<DeviceA> display counters outbound interface
```

Interface	Total (pkts)	Broadcast (pkts)	Multicast (pkts)	Err (pkts)
GE1/0/1	863764	0	0	0
GE1/0/2	0	0	0	0
GE1/0/3	0	0	0	0

9.6 配置文件

- Device A

```

#
bfd echo-source-ip 3.3.3.3
#
policy-based-route aaa permit node 5
if-match acl 3010
apply next-hop 12.12.12.2 track 11
#

```

```

interface GigabitEthernet1/0/1
  port link-mode route
  ip address 13.13.13.1 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 40.0.0.1 255.255.255.0
  ip policy-based-route aaa
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip address 12.12.12.1 255.255.255.0
  bfd min-echo-receive-interval 10
  bfd detect-multiplier 3
#
ip route-static 50.0.0.0 24 GigabitEthernet1/0/1 13.13.13.2
#
  ip local policy-based-route aaa
#
acl number 3010
  rule 0 permit ip source 40.0.0.2 0
#
  track 11 bfd echo interface GigabitEthernet1/0/3 remote ip 12.12.12.2 local ip 12.
12.12.1
#

```

- **Device B**

```

#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 12.12.12.2 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 24.24.24.2 255.255.255.0
#
ip route-static 50.0.0.0 24 GigabitEthernet1/0/2 24.24.24.4

```

- **Device C**

```

#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 13.13.13.2 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 50.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/3
  port link-mode route

```

```
ip address 24.24.24.4 255.255.255.0  
#
```

10 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“可靠性配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“可靠性命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

H3C MSR 系列路由器

VRRP 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 VRRP 单备份组配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	2
3.3 使用版本.....	2
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.5.1 Device A 的配置.....	2
3.5.2 Device B 的配置.....	3
3.6 验证配置.....	3
3.7 配置文件.....	5
4 VRRP 多备份组配置举例.....	5
4.1 组网需求.....	5
4.2 配置思路.....	6
4.3 使用版本.....	6
4.4 配置注意事项.....	7
4.5 配置步骤.....	7
4.5.1 Device A 的配置.....	7
4.5.2 Device B 的配置.....	8
4.6 验证配置.....	8
4.7 配置文件.....	11
5 VRRP 负载均衡模式配置举例.....	12
5.1 组网需求.....	12
5.2 配置思路.....	13
5.3 使用版本.....	13
5.4 配置注意事项.....	13
5.5 配置步骤.....	14
5.5.1 Device A 的配置.....	14
5.5.2 Device B 的配置.....	15
5.5.3 Device C 的配置.....	15
5.5.4 验证配置.....	16
5.5.5 配置文件.....	22

6 VRRP with IPsec 配置举例	23
6.1 组网需求	23
6.2 配置思路	23
6.3 使用版本	24
6.4 配置注意事项.....	24
6.5 配置步骤	24
6.5.1 Device A 的配置.....	24
6.5.2 Device B 的配置.....	25
6.5.3 Device C 的配置	27
6.6 验证配置	28
6.7 配置文件	32
7 相关资料	34

1 简介

本文档介绍 VRRP 的配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 VRRP、STP 和 IPsec 特性。

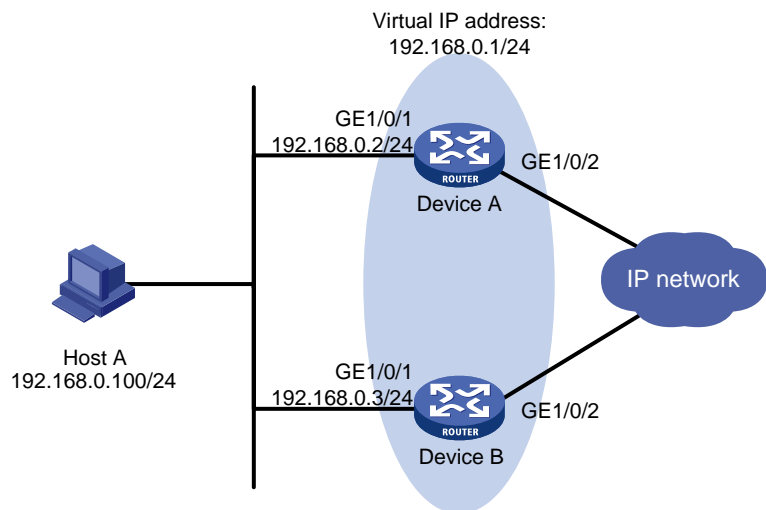
3 VRRP 单备份组配置举例

3.1 组网需求

如图 1 所示，Host A 所在网络的出口处部署了两台网关设备。现要求使用 VRRP 主备备份功能，将这两台设备组成一台虚拟路由器，作为 Host A 的缺省网关。具体应用需求如下：

- 在正常情况下，由 Device A 承担网关功能，转发 Host A 发送至外网的流量；
- 当 Device A 或者 Device A 的上行接口出现故障时，由 Device B 接替 Device A 承担网关功能；
- 当 Device A 或者 Device A 的上行接口故障恢复后，由 Device A 继续承担网关功能。

图1 VRRP 单备份组配置组网图



3.2 配置思路

- 为了让 Device A 成为 Master，需要为 Device A 配置较高的优先级；
- 将 VRRP 组的抢占模式和监视上行接口状态功能结合使用，可以使 Master 设备根据上行接口的状态自动调整自身的 VRRP 优先级，从而使 VRRP 组内的角色发生转变，实现主备切换；
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。
- IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本(缺省情况使用 VRRPv3)。请确保 IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本一致，否则备份组无法正常工作。
- 删除 IP 地址所有者上的 VRRP 备份组，将导致地址冲突。建议先修改配置了备份组的接口的 IP 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- 对于同一个 VRRP 备份组的成员设备，必须保证虚拟路由器的 IP 地址配置完全一样。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级比备份组内其他设备的优先级要低，确保备份组内有其他设备被选为 Master。

3.5 配置步骤

3.5.1 Device A 的配置

```
# 配置接口 IP 地址。
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.0.2 24
# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 192.168.0.1。
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 192.168.0.1
# 设置 Device A 在 VRRP 备份组 1 中的优先级为 110，高于 Device B 的优先级 100，以保证 Device A 成为 Master 负责转发流量。
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 priority 110
# 设置 Device A 工作在抢占方式，以保证 Device A 故障恢复后，能再次抢占成为 Master，即只要 Device A 正常工作，就由 Device A 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 5
[DeviceA-GigabitEthernet1/0/1] quit
# 创建和上行接口 GigabitEthernet1/0/2 物理状态关联的 Track 项 1。
[DeviceA] track 1 interface gigabitethernet 1/0/2
```

配置监视 Track 项 1，Track 项的状态为 Negative 时，Device A 在 VRRP 备份组中的优先级降低的数值为 50。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 track 1 priority reduced 50
[DeviceA-GigabitEthernet1/0/1] quit
```

3.5.2 Device B 的配置

配置接口 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 192.168.0.3 24
```

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 192.168.0.1。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 192.168.0.1
```

设置 Device B 在 VRRP 备份组 1 中的优先级为 100。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 priority 100
```

设置 Device B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 5
[DeviceB-GigabitEthernet1/0/1] quit
```

3.6 验证配置

配置完成后，在 Host A 上可以 ping 通 Host B。

通过 **display vrrp verbose** 命令查看配置后的结果，显示 Device A 上 VRRP 备份组 1 的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
  Interface GigabitEthernet1/0/1
    VRID          : 1                      Adver Timer   : 100
    Admin Status  : Up                    State         : Master
    Config Pri    : 110                   Running Pri   : 110
    Preempt Mode  : Yes                    Delay Time    : 5
    Auth Type     : None
    Virtual IP    : 192.168.0.1
    Virtual MAC   : 0000-5e00-0101
    Master IP     : 192.168.0.2
  VRRP Track Information:
    Track Object  : 1                      State : Positive  Pri Reduced : 50
```

通过 **display vrrp verbose** 命令查看配置后的结果，显示 Device B 上 VRRP 备份组 1 的详细信息。

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
  Interface GigabitEthernet1/0/1
```

```

VRID          : 1                      Adver Timer   : 100
Admin Status  : Up                      State         : Backup
Config Pri    : 100                     Running Pri   : 100
Preempt Mode  : Yes                     Delay Time    : 5
Become Master : 412ms left
Auth Type     : None
Virtual IP    : 192.168.0.1
Master IP     : 192.168.0.2

```

以上显示信息表示在 VRRP 备份组 1 中 Device A 为 Master 路由器，Device B 为 Backup 路由器，Host A 发送给 Host B 的报文通过 Device A 转发。

Device A 出现故障后，在 Host A 上仍然可以 ping 通 Host B。

通过 **display vrrp verbose** 命令查看 Device B 上 VRRP 备份组的详细信息，Device A 出现故障后，显示 Device B 上 VRRP 备份组 1 的详细信息。

```

[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
  Interface GigabitEthernet1/0/1
    VRID          : 1                      Adver Timer   : 100
    Admin Status  : Up                      State         : Master
    Config Pri    : 100                     Running Pri   : 100
    Preempt Mode  : Yes                     Delay Time    : 5
    Auth Type     : None
    Virtual IP    : 192.168.0.1
    Virtual MAC   : 0000-5e00-0101
    Master IP     : 192.168.0.3

```

以上显示信息表示 Device A 出现故障后，Device B 成为 Master 路由器，Host A 发送给 Host B 的报文通过 Device B 转发。

Device A 故障恢复后，显示 Device A 上 VRRP 备份组 1 的详细信息。

```

[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
  Interface GigabitEthernet1/0/1
    VRID          : 1                      Adver Timer   : 100
    Admin Status  : Up                      State         : Master
    Config Pri    : 110                     Running Pri   : 110
    Preempt Mode  : Yes                     Delay Time    : 5
    Auth Type     : None
    Virtual IP    : 192.168.0.1
    Virtual MAC   : 0000-5e00-0101
    Master IP     : 192.168.0.2

```

```

VRRP Track Information:
  Track Object    : 1                      State : Positive  Pri Reduced : 50

```

以上显示信息表示 Device A 故障恢复后，Device A 会抢占成为 Master，Host A 发送给 Host B 的报文仍然通过 Device A 转发。

3.7 配置文件

- Device A:

```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.0.2 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.0.1
vrrp vrid 1 priority 110
vrrp vrid 1 preempt-mode delay 5
vrrp vrid 1 track 1 priority reduced 50
#
track 1 interface GigabitEthernet 1/0/2
#
```
- Device B:

```
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.0.3 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.0.1
vrrp vrid 1 priority 100
vrrp vrid 1 preempt-mode delay 5
#
```

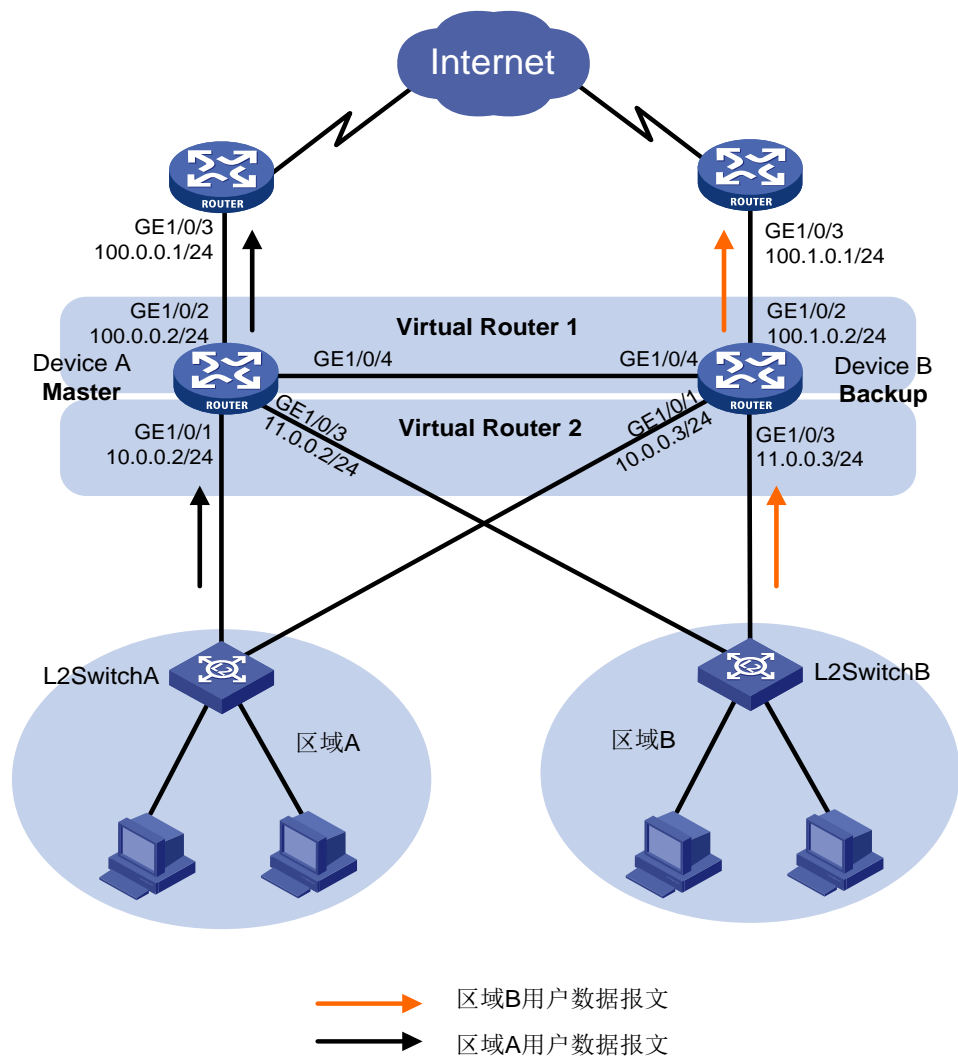
4 VRRP 多备份组配置举例

4.1 组网需求

如图 2 所示，某公司为了实现网关设备的冗余备份，以及内网主机流量的负载分担，在内部网络的出口处部署了两台设备，并使用 VRRP 负载分担功能，将这两台设备组成两台虚拟路由器，分别作为区域 A 和区域 B 的缺省网关。具体应用需求如下：

- Device A 是 VRRP 备份组 1 中的 Master 设备，Device B 是 VRRP 备份组 2 中的 Master 设备。在正常情况下，区域 A 的用户通过 Device A 进行数据转发，区域 B 的用户通过 Device B 进行数据转发。
- 当 Device A 或者 Device A 的上行接口发生故障后，Device B 能够迅速承担区域 A 内主机流量的转发任务；Device A 故障恢复后，继续承担 VRRP 备份组 1 的网关功能；
- 当 Device B 或者 Device B 的上行接口故障发生故障后，Device A 能够迅速承担区域 B 内主机流量的转发任务；Device B 故障恢复后，继续承担 VRRP 备份组 2 的网关功能。

图2 VRRP 多备份组配置组网图



4.2 配置思路

- 为了让 Device A 和 Device B 分别成为 VRRP 备份组 1 和 VRRP 备份组 2 中的 Master，需要在 VRRP 备份组 1 中为 Device A 配置较高的优先级，在 VRRP 备份组 2 中为 Device B 配置较高的优先级。
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。

4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.4 配置注意事项

- VRRP 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。
- IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本(缺省情况使用 VRRPv3)。请确保 IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本一致，否则 VRRP 备份组无法正常工作。
- 删除 IP 地址所有者上的 VRRP 备份组，将导致地址冲突。建议先修改配置了 VRRP 备份组的接口的 IP 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级比 VRRP 备份组内其他设备的优先级要低，确保 VRRP 备份组内有其他设备被选为 Master 设备。
- 对于同一个 VRRP 备份组的成员设备，如下配置必须保证完全一样：
 - 虚拟路由器的 IP 地址个数
 - 每个备份组虚拟路由器的 IP 地址
 - 定时器间隔时间

4.5 配置步骤

4.5.1 Device A 的配置

配置接口 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.0.0.2 24
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上方法配置图 2 中其它接口的 IP 地址，配置步骤这里省略。

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.0.0.1，并配置 Device A 在 VRRP 备份组 1 中的优先级为 120，高于 Device B 的优先级。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.0.0.1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 priority 120
[DeviceA-GigabitEthernet1/0/1] quit
```

创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 11.0.0.1。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 11.0.0.1
[DeviceA-GigabitEthernet1/0/3] quit
```

设置 Device A 工作在抢占方式，配置抢占延迟时间为 5 秒。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 5
[DeviceA-GigabitEthernet1/0/1] quit
```

创建和上行接口 GigabitEthernet1/0/2 物理状态关联的 Track 项 1。

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
```

配置监视 Track 项 1，Track 项的状态为 Negative 时，Device A 在 VRRP 备份组 1 中的优先级降低的数值为 50。


```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 track 1 priority reduced 50
[DeviceA-GigabitEthernet1/0/1] quit
```

4.5.2 Device B 的配置

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.0.0.3 24
[DeviceB-GigabitEthernet1/0/1] quit
# 请参考以上方法配置图2中其它接口的 IP 地址，配置步骤省略。
# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.0.0.1。
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.0.0.1
[DeviceB-GigabitEthernet1/0/1] quit
# 创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 11.0.0.1，并配置 Device B 在 VRRP
备份组 2 中的优先级为 120，高于 Device A 的优先级。
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 11.0.0.1
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 priority 120
# 设置 Device B 工作在抢占方式，配置抢占延迟时间为 5 秒。
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 preempt-mode delay 5
[DeviceB-GigabitEthernet1/0/3] quit
# 创建和上行接口 Gigabitethernet 1/0/2 物理状态关联的 Track 项 2。
[DeviceB] track 2 interface gigabitethernet 1/0/2
# 配置监视 Track 项 2，Track 项的状态为 Negative 时，Device B 在 VRRP 备份组 2 中的优先级降
低的数值为 50。
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] vrrp vrid 2 track 2 priority reduced 50
[DeviceB-GigabitEthernet1/0/3] quit
```

4.6 验证配置

(1) 配置完成后，区域 A 和区域 B 中的主机都可以 ping 通外网。

检查区域 A 的主机到目的端 100.0.0.1 是否可达。

```
<host A> ping 100.0.0.1
PING 100.0.0.1 (100.0.0.1): 56 data bytes
56 bytes from 100.0.0.1: seq=0 ttl=128 time=22.43 ms
56 bytes from 100.0.0.1: seq=1 ttl=128 time=7.17 ms
56 bytes from 100.0.0.1: seq=2 ttl=128 time=8.91 ms
56 bytes from 100.0.0.1: seq=3 ttl=128 time=7.45 ms
56 bytes from 100.0.0.1: seq=4 ttl=128 time=9.11 ms

--- 100.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

检查区域 B 的主机到目的端 100.1.0.1 是否可达。

```

<host C> ping 100.1.0.1
PING 100.1.0.1 (100.1.0.1): 56 data bytes
56 bytes from 100.1.0.1: seq=0 ttl=128 time=22.43 ms
56 bytes from 100.1.0.1: seq=1 ttl=128 time=7.17 ms
56 bytes from 100.1.0.1: seq=2 ttl=128 time=8.91 ms
56 bytes from 100.1.0.1: seq=3 ttl=128 time=7.45 ms
56 bytes from 100.1.0.1: seq=4 ttl=128 time=9.11 ms

--- 100.1.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms

```

(2) 通过 **display vrrp verbose** 命令查看配置后的结果。

查看 Device A 上全部 IPv4 VRRP 备份组的详细信息，显示 Device A 在 VRRP 备份组 1 中为 Master 设备，在 VRRP 备份组 2 中为 Backup 设备。

```

[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode          : Standard
Total number of virtual routers : 2

Interface GigabitEthernet1/0/1
  VRID                : 1                    Adver Timer   : 100
  Admin Status        : Up                  State         : Master
  Config Pri          : 120                 Running Pri    : 120
  Preempt Mode        : Yes                 Delay Time     : 5
  Auth Type           : None
  Virtual IP          : 10.0.0.1
  Virtual MAC         : 0000-5e00-0101
  Master IP           : 10.0.0.2

VRRP Track Information:
Track Object          : 1                    State : Positive  Pri Reduced : 50

Interface GigabitEthernet1/0/3
  VRID                : 2                    Adver Timer   : 100
  Admin Status        : Up                  State         : Backup
  Config Pri          : 100                 Running Pri    : 100
  Preempt Mode        : Yes                 Delay Time     : 0
  Auth Type           : None
  Become Master       : 3550ms left
  Virtual IP          : 11.0.0.1
  Master IP           : 11.0.0.3

```

查看 Device B 上全部 IPv4 VRRP 备份组的详细信息，显示 Device B 在备份组 1 中为 Backup 设备，在备份组 2 中为 Master 设备。

```

[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode          : Standard
Total number of virtual routers : 2

Interface GigabitEthernet1/0/1
  VRID                : 1                    Adver Timer   : 100

```

```

Admin Status      : Up                               State          : Backup
Config Pri       : 100                             Running Pri    : 100
Preempt Mode     : Yes                             Delay Time     : 0
Auth Type        : None
Become Master    : 3500ms left
Virtual IP       : 10.0.0.1
Master IP        : 10.0.0.2

```

Interface GigabitEthernet1/0/3

```

VRID              : 2                               Adver Timer    : 100
Admin Status     : Up                               State          : Master
Config Pri       : 120                             Running Pri    : 120
Preempt Mode     : Yes                             Delay Time     : 5
Auth Type        : None
Virtual IP       : 11.0.0.1
Virtual MAC      : 0000-5e00-0102
Master IP        : 11.0.0.3

```

VRRP Track Information:

```

Track Object     : 2                               State : Positive  Pri Reduced : 50

```

Device A 出现故障后，通过 **display vrrp verbose** 命令查看 Device B 上备份组的详细信息。可以看到 Device B 抢占为备份组 1 的 Master。

[DeviceB] display vrrp verbose

IPv4 Virtual Router Information:

```

Running Mode     : Standard

```

Total number of virtual routers : 2

Interface GigabitEthernet1/0/1

```

VRID              : 1                               Adver Timer    : 100
Admin Status     : Up                               State          : Master
Config Pri       : 100                             Running Pri    : 100
Preempt Mode     : Yes                             Delay Time     : 0
Auth Type        : None
Virtual IP       : 10.0.0.1
Virtual MAC      : 0000-5e00-0101
Master IP        : 10.0.0.3

```

Interface GigabitEthernet1/0/3

```

VRID              : 2                               Adver Timer    : 100
Admin Status     : Up                               State          : Master
Config Pri       : 120                             Running Pri    : 120
Preempt Mode     : Yes                             Delay Time     : 5
Auth Type        : None
Virtual IP       : 11.0.0.1
Virtual MAC      : 0000-5e00-0102
Master IP        : 11.0.0.3

```

VRRP Track Information:

```

Track Object     : 2                               State : Positive  Pri Reduced : 50

```

以上显示信息表示 Device A 出现故障后，区域 A 和区域 B 中的主机仍然可以 ping 通外网。

当 Device A 故障恢复后，显示 Device A 上备份组的详细信息。

```

[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Standard
  Total number of virtual routers : 2
  Interface GigabitEthernet1/0/1
    VRID           : 1
    Admin Status   : Up
    Config Pri     : 120
    Preempt Mode   : Yes
    Auth Type      : None
    Virtual IP     : 10.0.0.1
    Virtual MAC    : 0000-5e00-0101
    Master IP      : 10.0.0.2
    Adver Timer    : 100
    State          : Master
    Running Pri    : 120
    Delay Time     : 5
  VRRP Track Information:
    Track Object   : 1
    State          : Positive
    Pri Reduced    : 50

  Interface GigabitEthernet1/0/3
    VRID           : 2
    Admin Status   : Up
    Config Pri     : 100
    Preempt Mode   : Yes
    Become Master  : 3550ms left
    Auth Type      : None
    Virtual IP     : 11.0.0.1
    Master IP      : 11.0.0.3
    Adver Timer    : 100
    State          : Backup
    Running Pri    : 100
    Delay Time     : 0

```

以上显示信息表示当 Device A 故障恢复后，Device A 在 VRRP 备份组 1 中恢复为原来的优先级并抢占成为该备份组的 Master，区域 A 内的主机通过 Device A 与外界通信。

4.7 配置文件

- Device A:


```

#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 10.0.0.2 255.255.255.0
  vrrp vrid 1 virtual-ip 10.0.0.1
  vrrp vrid 1 priority 120
  vrrp vrid 1 preempt-mode delay 5
  vrrp vrid 1 track 1 priority reduced 50
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 100.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/3
  port link-mode route
  ip address 11.0.0.2 255.255.255.0
  vrrp vrid 2 virtual-ip 11.0.0.1

```

- ```

#
 track 1 interface GigabitEthernet 1/0/2
#

```
- **Device B:**

```

#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.0.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.1
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 100.1.0.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 11.0.0.3 255.255.255.0
 vrrp vrid 2 priority 120
 vrrp vrid 2 preempt-mode delay 5
 vrrp vrid 2 track 2 priority reduced 50
#
 track 2 interface GigabitEthernet 1/0/2
#

```

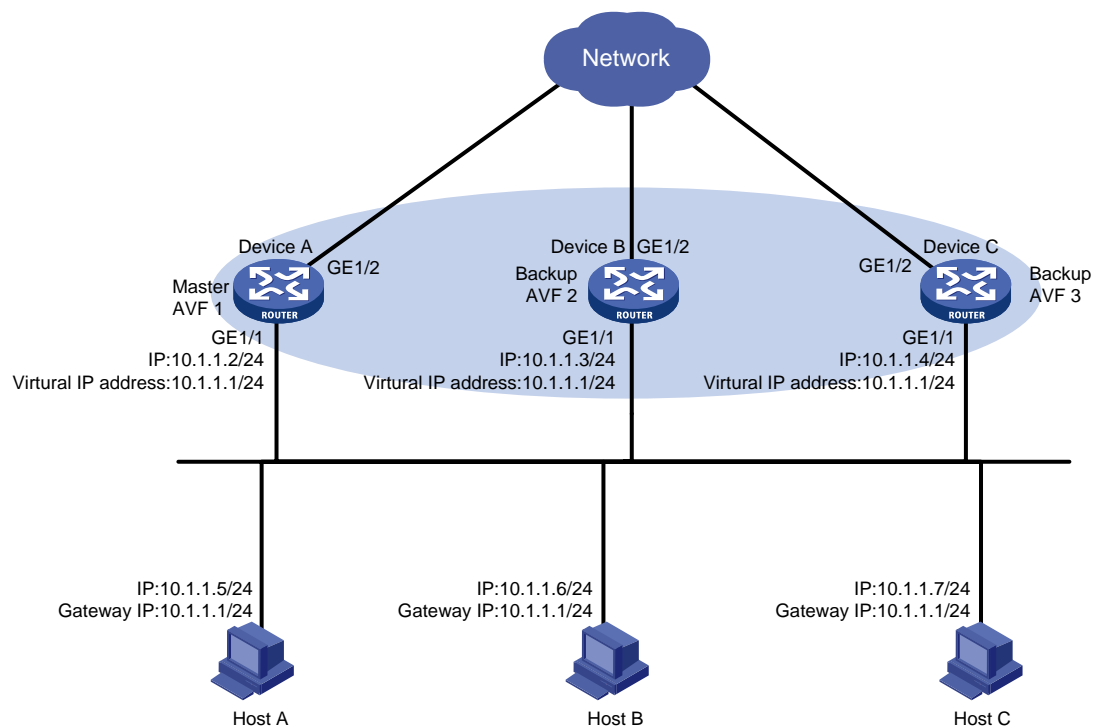
## 5 VRRP 负载均衡模式配置举例

### 5.1 组网需求

如[图 3](#)所示，Host A、Host B 和 Host C 所在网络的出口处部署了三台路由器。现要求使用 VRRP 负载均衡功能，将 Device A、Device B 和 Device C 组成一台虚拟路由器，作为局域网内主机的缺省网关。具体应用需求如下：

- 实现 VRRP 备份组中三台路由器都可以转发报文，实现流量负载分担，充分利用网关资源；
- 当 Device A、Device B 或 Device C 自身或其上行接口出现故障时，Host A、Host B 和 Host C 可以通过其他正常运行的设备继续通信，避免通信中断；当 Device A、Device B 或 Device C 故障恢复后，继续承担网关功能。

图3 VRRP 负载均衡模式配置组网图



## 5.2 配置思路

- 为了使 Device A 优先与 Device B 和 Device C 被选举为 VRRP 备份组的 Master 设备，需要为其配置高于 Device B 和 Device C 的优先级；为了使 Device B 优先于 Device C 被选举为 VRRP 备份组的 Master 设备，需要为其配置高于 Device C 的优先级；
- 为了避免由于故障造成 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间；
- 在 Device A、Device B 和 Device C 上配置虚拟转发器通过 Track 项监视上行接口的状态。当上行接口出现故障时，降低该接口所在设备虚拟转发器的权重，以便其他设备接管该设备的转发任务，避免通信中断；
- 为了保证原 Master 设备故障恢复后，能再次抢占成为 Master，需要配置 VRRP 备份组工作在抢占模式。

## 5.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 5.4 配置注意事项

- VRRP 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。

- IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本(缺省情况使用 VRRPv3)。请确保 IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本一致，否则 VRRP 备份组无法正常工作。
- 删除 IP 地址所有者上的 VRRP 备份组，将导致地址冲突。建议先修改配置了 VRRP 备份组的接口的 IP 地址，再删除该接口上的 VRRP 备份组，以避免地址冲突。
- VRRP 工作在负载均衡模式时，备份组的虚拟 IP 地址和接口的 IP 地址不能相同，否则 VRRP 负载均衡功能将无法正常工作。
- 当监视的上行链路出现故障时，配置的权重降低数额需保证 VF Owner 的权重低于失效下限，即权重降低的数额大于 245，其它的虚拟转发器才能接替 VF Owner 成为 AVF。
- 对于同一个 VRRP 备份组的成员设备，必须保证备份组虚拟路由器的 IP 地址配置完全一样。
- 用户在配置降低权重幅度时，需要确保降低后的优先级比 VRRP 备份组内其他设备的优先级要低，确保 VRRP 备份组内有其他设备被选为 Master。

## 5.5 配置步骤

### 5.5.1 Device A 的配置

#### (1) 配置接口

# 配置接口的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[DeviceA-GigabitEthernet1/0/1] quit
```

#### (2) 配置 VRRP

# 配置 VRRP 工作在负载均衡模式。

```
[DeviceA] vrrp mode load-balance
```

# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.1.1.1
```

# 配置 Device A 在 VRRP 备份组 1 中的优先级为 120，高于 Device B 的优先级 110 和 Device C 的优先级 100，以保证 Device A 成为 Master。

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 priority 120
```

# 配置 Device A 工作在抢占方式，以保证 Device A 故障恢复后，能再次抢占成为 Master，即只要 Device A 正常工作，Device A 就会成为 Master。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。

```
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 5
[DeviceA-GigabitEthernet1/0/1] quit
```

#### (3) 配置 Track

# 创建和 GigabitEthernet1/0/2 物理状态关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Device A 的上行接口出现故障。

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
```

# 配置虚拟转发器监视 Track 项 1。Track 项的状态为 **Negative** 时，降低 Device A 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device A 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] vrrp vrid 1 track 1 weight reduced 250
[DeviceA-GigabitEthernet1/0/1] quit
```

## 5.5.2 Device B 的配置

### (1) 配置接口

# 配置接口的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.1.1.3 24
[DeviceB-GigabitEthernet1/0/1] quit
```

### (2) 配置 VRRP

# 配置 VRRP 工作在负载均衡模式。

```
[DeviceB] vrrp mode load-balance
```

# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.1.1.1
```

# 配置 Device B 在 VRRP 备份组 1 中的优先级为 110，高于 Device C 的优先级，以保证 Device A 出现故障时，Device B 成为 Master。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 priority 110
```

# 配置 Device B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 5
[DeviceB-GigabitEthernet1/0/1] quit
```

### (3) 配置 Track

# 创建和 GigabitEthernet1/0/2 物理状态关联的 Track 项 1。如果 Track 项的状态为 **Negative**，则说明 Device B 的上行接口出现故障。

```
[DeviceB] track 1 interface gigabitethernet 1/0/2
```

# 配置虚拟转发器监视 Track 项 1。Track 项的状态为 **Negative** 时，降低 Device B 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device B 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 1 track 1 weight reduced 250
[DeviceB-GigabitEthernet1/0/1] quit
```

## 5.5.3 Device C 的配置

### (1) 配置接口

# 配置接口的 IP 地址。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address 10.1.1.4 24
```



```
[DeviceC-GigabitEthernet1/0/1] quit
```

## (2) 配置 VRRP

# 配置 VRRP 工作在负载均衡模式。

```
[DeviceA] vrrp mode load-balance
```

# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 10.1.1.1。

```
[DeviceC] interface gigabitEthernet 1/0/1
```

```
[DeviceC-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 10.1.1.1
```

# 配置 Device C 工作在抢占方式，抢占延迟时间为 5 秒。

```
[DeviceC-GigabitEthernet1/0/1] vrrp vrid 1 preempt-mode delay 5
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

## (3) 配置 Track

# 创建和 GigabitEthernet1/0/2 物理状态关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 Device C 的上行接口出现故障。

```
[DeviceC] track 1 interface gigabitEthernet 1/0/2
```

# 配置虚拟转发器监视 Track 项 1。Track 项的状态为 Negative 时，降低 Device C 上虚拟转发器的权重，使其低于失效下限 10，即权重降低的数额大于 245，以便其他设备接替 Device C 的转发任务。本例中，配置虚拟转发器权重降低数额为 250。

```
[DeviceC] interface gigabitEthernet 1/0/1
```

```
[DeviceC-GigabitEthernet1/0/1] vrrp vrid 1 track 1 weight reduced 250
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

## 5.5.4 验证配置

(1) 配置完成后，在 Host A 上可以 ping 通外网，通过 **display vrrp verbose** 命令查看配置后的结果

# 显示 Device A 上 VRRP 备份组的详细信息。

```
[DeviceA] display vrrp verbose
```

```
IPv4 Virtual Device Information:
```

```
Running Mode : Load Balance
```

```
Total number of virtual routers : 1
```

```
Interface GigabitEthernet1/0/1
```

```
VRID : 1 Adver Timer : 100
```

```
Admin Status : Up State : Master
```

```
Config Pri : 120 Running Pri : 120
```

```
Preempt Mode : Yes Delay Time : 5
```

```
Auth Type : None
```

```
Virtual IP : 10.1.1.1
```

```
Member IP List : 10.1.1.2 (Local, Master)
```

```
 : 10.1.1.3 (Backup)
```

```
 : 10.1.1.4 (Backup)
```

```
Forwarder Information: 3 Forwarders 1 Active
```

```
Config Weight : 255
```

```
Running Weight : 255
```

```
Forwarder 01
```

```
State : Active
```

```
Virtual MAC : 000f-e2ff-0011 (Owner)
```

```
Owner ID : 0000-5e01-1101
Priority : 255
Active : local
```

**Forwarder 02**

```
State : Listening
Virtual MAC : 000f-e2ff-0012 (Learnt)
Owner ID : 0000-5e01-1103
Priority : 127
Active : 10.1.1.3
```

**Forwarder 03**

```
State : Listening
Virtual MAC : 000f-e2ff-0013 (Learnt)
Owner ID : 0000-5e01-1105
Priority : 127
Active : 10.1.1.4
```

**Forwarder Weight Track Information:**

```
Track Object : 1 State : Positive Weight Reduced : 250
```

# 显示 Device B 上 VRRP 备份组的详细信息。

```
[DeviceB] display vrrp verbose
```

IPv4 Virtual Device Information:

```
Running Mode : Load Balance
```

Total number of virtual routers : 1

Interface GigabitEthernet1/0/1

```
VRID : 1 Adver Timer : 100
Admin Status : Up State : Backup
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : 10.1.1.1
Member IP List : 10.1.1.3 (Local, Backup)
 10.1.1.2 (Master)
 10.1.1.4 (Backup)
```

Forwarder Information: 3 Forwarders 1 Active

```
Config Weight : 255
Running Weight : 255
```

**Forwarder 01**

```
State : Listening
Virtual MAC : 000f-e2ff-0011 (Learnt)
Owner ID : 0000-5e01-1101
Priority : 127
Active : 10.1.1.2
```

**Forwarder 02**

```
State : Active
Virtual MAC : 000f-e2ff-0012 (Owner)
Owner ID : 0000-5e01-1103
Priority : 255
Active : local
```

**Forwarder 03**

```

State : Listening
Virtual MAC : 000f-e2ff-0013 (Learnt)
Owner ID : 0000-5e01-1105
Priority : 127
Active : 10.1.1.4
Forwarder Weight Track Information:
Track Object : 1 State : Positive Weight Reduced : 250

```

# 显示 Device C 上 VRRP 备份组的详细信息。

```

[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
Running Mode : Load Balance
Total number of virtual routers : 1
Interface GigabitEthernet1/0/1
VRID : 1 Adver Timer : 100
Admin Status : Up State : Backup
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : 10.1.1.1
Member IP List : 10.1.1.4 (Local, Backup)
 10.1.1.2 (Master)
 10.1.1.3 (Backup)
Forwarder Information: 3 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
State : Listening
Virtual MAC : 000f-e2ff-0011 (Learnt)
Owner ID : 0000-5e01-1101
Priority : 127
Active : 10.1.1.2
Forwarder 02
State : Listening
Virtual MAC : 000f-e2ff-0012 (Learnt)
Owner ID : 0000-5e01-1103
Priority : 127
Active : 10.1.1.3
Forwarder 03
State : Active
Virtual MAC : 000f-e2ff-0013 (Owner)
Owner ID : 0000-5e01-1105
Priority : 255
Active : local
Forwarder Weight Track Information:
Track Object : 1 State : Positive Weight Reduced : 250

```

以上显示信息表示在 VRRP 备份组 1 中 Device A 为 Master，Device B 和 Device C 为 Backup。Device A、Device B 和 Device C 上各自存在一个 AVF，并存在作为备份的两个 LVF。

(2) Device A 的上行接口（GigabitEthernet1/0/2）出现故障后

# 显示 Device A 上 VRRP 备份组的详细信息。

```
[DeviceA] display vrrp verbose
IPv4 Virtual Device Information:
 Running Mode : Load Balance
Total number of virtual routers : 1
 Interface GigabitEthernet1/0/1
 VRID : 1 Adver Timer : 100
 Admin Status : Up State : Master
 Config Pri : 120 Running Pri : 120
 Preempt Mode : Yes Delay Time : 5
 Auth Type : None
 Virtual IP : 10.1.1.1
 Member IP List : 10.1.1.2 (Local, Master)
 : 10.1.1.3 (Backup)
 : 10.1.1.4 (Backup)
Forwarder Information: 3 Forwarders 0 Active
 Config Weight : 255
 Running Weight : 5
Forwarder 01
 State : Initialize
 Virtual MAC : 000f-e2ff-0011 (Owner)
 Owner ID : 0000-5e01-1101
 Priority : 0
 Active : 10.1.1.4
Forwarder 02
 State : Initialize
 Virtual MAC : 000f-e2ff-0012 (Learnt)
 Owner ID : 0000-5e01-1103
 Priority : 0
 Active : 10.1.1.3
Forwarder 03
 State : Initialize
 Virtual MAC : 000f-e2ff-0013 (Learnt)
 Owner ID : 0000-5e01-1105
 Priority : 0
 Active : 10.1.1.4
Forwarder Weight Track Information:
 Track Object : 1 State : Negative Weight Reduced : 250
```

# 显示 Device C 上 VRRP 备份组的详细信息。

```
[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
 Running Mode : Load Balance
Total number of virtual routers : 1
 Interface GigabitEthernet1/0/1
 VRID : 1 Adver Timer : 100
 Admin Status : Up State : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
```

```

Auth Type : None
Become Master : 3550ms left
Virtual IP : 10.1.1.1
Member IP List : 10.1.1.4 (Local, Backup)
 10.1.1.2 (Master)
 10.1.1.3 (Backup)
Forwarder Information: 3 Forwarders 2 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
State : Active
Virtual MAC : 000f-e2ff-0011 (Take Over)
Owner ID : 0000-5e01-1101
Priority : 85
Active : local
Redirect Time : 93 secs
Time-out Time : 1293 secs
Forwarder 02
State : Listening
Virtual MAC : 000f-e2ff-0012 (Learnt)
Owner ID : 0000-5e01-1103
Priority : 85
Active : 10.1.1.3
Forwarder 03
State : Active
Virtual MAC : 000f-e2ff-0013 (Owner)
Owner ID : 0000-5e01-1105
Priority : 255
Active : local
Forwarder Weight Track Information:
Track Object : 1 State : Positive Weight Reduced : 250

```

以上显示信息表示 Device A 的上行接口出现故障后，Device A 上虚拟转发器的权重降低为 5，低于失效下限。Device A 上所有虚拟转发器的状态均变为 **Initialized**，不能再用于转发。Device C 成为虚拟 MAC 地址 000f-e2ff-0011 对应虚拟转发器的 AVF，接管 Device A 的转发任务。

# Timeout Timer 超时后（约 1800 秒后），查看 Device C 上 VRRP 备份组的详细信息。

```

[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
Running Mode : Load Balance
Total number of virtual routers : 1
Interface GigabitEthernet1/0/1
VRID : 1 Adver Timer : 100
Admin Status : Up State : Backup
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Become Master : 3550ms left
Virtual IP : 10.1.1.1

```

```

Member IP List : 10.1.1.4 (Local, Backup)
 10.1.1.2 (Master)
 10.1.1.3 (Backup)
Forwarder Information: 2 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 02
State : Listening
Virtual MAC : 000f-e2ff-0012 (Learnt)
Owner ID : 0000-5e01-1103
Priority : 127
Active : 10.1.1.3
Forwarder 03
State : Active
Virtual MAC : 000f-e2ff-0013 (Owner)
Owner ID : 0000-5e01-1105
Priority : 255
Active : local
Forwarder Weight Track Information:
Track Object : 1 State : Positive Weight Reduced : 250

```

以上显示信息表示，**Timeout Timer** 超时后，删除虚拟 MAC 地址 000f-e2ff-0011 对应的虚拟转发器，不再转发目的 MAC 地址为该 MAC 的报文。

### (3) Device A 出现故障后

# 显示 Device B 上 VRRP 备份组的详细信息。

```

[DeviceB] display vrrp verbose
IPv4 Standby Information:
Run Mode : Load Balance
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface GigabitEthernet1/0/1
VRID : 1 Adver Timer : 1
Admin Status : Up State : Master
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : 10.1.1.1
Member IP List : 10.1.1.3 (Local, Master)
 10.1.1.4 (Backup)
Forwarder Information: 2 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 02
State : Active
Virtual MAC : 000f-e2ff-0012 (Owner)
Owner ID : 0000-5e01-1103
Priority : 255
Active : local
Forwarder 03

```

```

State : Listening
Virtual MAC : 000f-e2ff-0013 (Learnt)
Owner ID : 0000-5e01-1105
Priority : 127
Active : 10.1.1.4
Forwarder Weight Track Information:
Track Object : 1 State : Positive Weight Reduced : 250

```

以上显示信息表示 **Device A** 出现故障后，**Device B** 的优先级高于 **Device C**，将抢占成为 **Master**。

### 5.5.5 配置文件

- **Device A:**

```

#
 vrrp mode load-balance
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 weight reduced 250
#
track 1 interface GigabitEthernet1/0/2

```

- **Device B:**

```

#
 vrrp mode load-balance
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 weight reduced 250
#
track 1 interface GigabitEthernet1/0/2

```

- **Device C:**

```

#
 vrrp mode load-balance
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.4 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 preempt-mode delay 5

```

```

vrp vrid 1 track 1 weight reduced 250
#
track 1 interface GigabitEthernet1/0/2

```

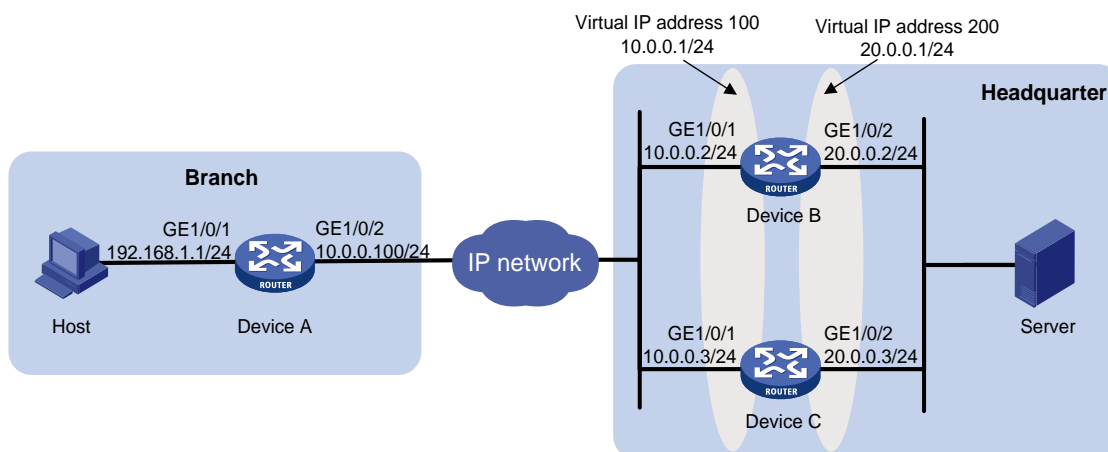
## 6 VRRP with IPsec 配置举例

### 6.1 组网需求

如图 4 所示，Device A 作为某公司分支机构的网关设备，Device B 和 Device C 是公司总部网关设备。Device B 和 Device C 通过部署 VRRP 协议，实现设备冗余备份，提高可靠性。该分支机构内的主机可以访问公司总部内部服务器的资源。具体应用需求如下：

- 在正常情况下，Device B 作为 Master 负责流量的转发；
- 当 Device B 出现故障时，由 Device C 接替其流量转发任务；
- 要求在 Device A 和公司总部出口网关之间部署 IPsec 隧道，以保证分支机构内网网段 192.168.1.0/24 和总部内网网段 20.0.0.0/24 之间数据的完整性和机密性。

图4 VRRP with IPsec 配置组网图



### 6.2 配置思路

- 由于 IPsec 隧道是点到点建立的，为保护主机与服务器之间数据的安全性，需要 Device A 与 VRRP 备份组 100 中的 Master 建立 IPsec 隧道。
- 为了避免 VRRP 组发生主备切换时造成 IPsec 隧道的中断，可以通过配置 DPD 功能保证 Device A 可以及时的检测到对端路由器的状态，并重新与 VRRP 备份组中的其他路由器进行 IKE 协商。
- 为了让 Device B 成为 Master，需要为 Device B 配置较高的优先级。
- 将 VRRP 组的抢占模式和监视上行接口状态功能结合使用，可以使 Master 设备根据连接总部内网接口 GigabitEthernet 1/0/2 的状态自动调整自身的 VRRP 优先级，从而使 VRRP 组内的角色发生转变，实现主备切换。
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。



## 6.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 6.4 配置注意事项

- VRRP 备份组的虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。
- IPv4 VRRP 既可以使用 VRRPv2 版本, 也可以使用 VRRPv3 版本(缺省情况使用 VRRPv3)。请确保 IPv4 VRRP 备份组中的所有路由器上配置的 IPv4 VRRP 版本一致, 否则 VRRP 备份组无法正常工作。
- 删除 IP 地址所有者上的 VRRP 备份组, 将导致地址冲突。建议先修改配置了 VRRP 备份组的接口的 IP 地址, 再删除该接口上的 VRRP 备份组, 以避免地址冲突。
- IPsec 隧道两端配置的 ACL 的源地址和目的地址必须对称。
- IKE 协商双方配置的预共享密钥必须相同。
- 对于同一个 VRRP 备份组的成员设备, 必须保证备份组虚拟路由器的 IP 地址完全一样。
- 用户在配置降低优先级幅度时, 需要确保降低后的优先级比 VRRP 备份组内其他设备的优先级要低, 确保 VRRP 备份组内有其他设备被选为 Master。

## 6.5 配置步骤

### 6.5.1 Device A 的配置

```
配置接口的 IP 地址。
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip address 10.0.0.100 255.255.255.0
[DeviceA-GigabitEthernet1/0/2] quit
配置到 20.0.0.0/24 网段的静态路由。
[DeviceA] ip route-static 20.0.0.0 255.255.255.0 10.0.0.1
配置 ACL 3000, 指定 IPsec 需要保护的数据流。
[DeviceA] acl number 3000
[DeviceA-acl-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 20.0.0.0
0.0.0.255
[DeviceA-acl-adv-3000] quit
配置流量触发 IKE DPD 探测间隔时间为 10 秒, 重传时间间隔为 5 秒, 探测模式为按需探测。
[DeviceA] ike dpd interval 10 retry 5 on-demand
创建 IKE Keychain, 并配置与对端地址为虚拟 IP 地址 10.0.0.1 使用的预共享密钥为明文的 123456。
[DeviceA] ike keychain test
[DeviceA-ike-keychain-test] pre-shared-key address 10.0.0.1 key simple 123456
[DeviceA-ike-keychain-test] quit
```

# 创建 IKE profile，指定采用预共享密钥时使用的 IKE Keychain，并配置使用 IP 地址 10.0.0.100 标识本端身份信息、使用 VRRP 备份组 100 的虚拟 IP 地址 10.0.0.1 来匹配对端身份。

```
[DeviceA] ike profile test
[DeviceA-ike-profile-test] keychain test
[DeviceA-ike-profile-test] local-identity address 10.0.0.100
[DeviceA-ike-profile-test] match remote identity address 10.0.0.1
[DeviceA-ike-profile-test] quit
```

# 创建 IPsec 安全提议 test，安全封装模式、安全协议类型均采用系统缺省值。

```
[DeviceA] ipsec transform-set test
```

# 配置 ESP 协议采用的加密算法为采用 64 比特的 DES 算法，认证算法为 MD5。

```
[DeviceA-ipsec-transform-set-test] esp encryption-algorithm des-cbc
[DeviceA-ipsec-transform-set-test] esp authentication-algorithm md5
[DeviceA-ipsec-transform-set-test] quit
```

# 创建 IPsec 安全策略 test、顺序号为 1、采用 IKE 方式协商 IPsec SA 的 IPsec 安全策略，并进入 IPsec 安全策略视图。

```
[DeviceA] ipsec policy test 1 isakmp
```

# 指定 IPsec 隧道的本端 IP 地址为 10.0.0.100。

```
[DeviceA-ipsec-policy-isakmp-test-1] local-address 10.0.0.100
```

# 指定 IPsec 隧道的对端 IP 地址为 10.0.0.1。

```
[DeviceA-ipsec-policy-isakmp-test-1] remote-address 10.0.0.1
```

# 配置 IPsec 安全策略引用 ACL 3000。

```
[DeviceA-ipsec-policy-isakmp-test-1] security acl 3000
```

# 配置 IPsec 安全策略引用安全提议 test。

```
[DeviceA-ipsec-policy-isakmp-test-1] transform-set test
```

# 配置 IPsec 安全策略引用名为 test 的 IKE profile。

```
[DeviceA-ipsec-policy-isakmp-test-1] ike-profile test
[DeviceA-ipsec-policy-isakmp-test-1] quit
```

# 应用 IPsec 策略。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ipsec apply policy test
[DeviceA-GigabitEthernet1/0/2] quit
```

## 6.5.2 Device B 的配置

# 配置接口的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.0.0.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 20.0.0.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/2] quit
```

# 配置到 192.168.1.0/24 网段的静态路由。

```
[DeviceB] ip route-static 192.168.1.0 255.255.255.0 10.0.0.100
```

# 配置 ACL 3000，指定 IPsec 需要保护的数据流。

```

[DeviceB] acl number 3000
[DeviceB-acl-adv-3000] rule 0 permit ip source 20.0.0.0 0.0.0.255 destination 192.168.1.0
0.0.0.255
[DeviceB-acl-adv-3000] quit
创建 IKE Keychain，并配置与对端地址为 10.0.0.100 使用的预共享密钥为明文的 123456。
[DeviceB] ike keychain test
[DeviceB-ike-keychain-test] pre-shared-key address 10.0.0.100 key simple 123456
[DeviceB-ike-keychain-test] quit
创建 IKE profile，指定采用预共享密钥时使用的 IKE Keychain，并配置使用 VRRP 备份组 100
的虚拟 IP 地址 10.0.0.1 标识本端身份信息、使用 DeviceA 的上行接口地址 10.0.0.100 来匹配对端
身份。
[DeviceB] ike profile test
[DeviceB-ike-profile-test] keychain test
[DeviceB-ike-profile-test] local-identity address 10.0.0.1
[DeviceB-ike-profile-test] match remote identity address 10.0.0.100
[DeviceB-ike-profile-test] quit
创建 IPsec 安全提议 test，安全封装模式、安全协议类型均采用系统缺省值。
[DeviceB] ipsec transform-set test
配置 ESP 协议采用的加密算法为采用 64 比特的 DES 算法，认证算法为 MD5。
[DeviceB-ipsec-transform-set-test] esp encryption-algorithm des-cbc
[DeviceB-ipsec-transform-set-test] esp authentication-algorithm md5
[DeviceB-ipsec-transform-set-test] quit
创建 IPsec 安全策略 test、顺序号为 1、采用 IKE 方式协商 IPsec SA 的 IPsec 安全策略，并进入
IPsec 安全策略视图。
[DeviceB] ipsec policy test 1 isakmp
指定 IPsec 隧道的本端 IP 地址为 10.0.0.1。
[DeviceB-ipsec-policy-isakmp-test-1] local-address 10.0.0.1
指定 IPsec 隧道的对端 IP 地址为 10.0.0.100。
[DeviceB-ipsec-policy-isakmp-test-1] remote-address 10.0.0.100
配置 IPsec 安全策略引用 ACL 3000。
[DeviceB-ipsec-policy-isakmp-test-1] security acl 3000
配置 IPsec 安全策略引用安全提议 test。
[DeviceB-ipsec-policy-isakmp-test-1] transform-set test
配置 IPsec 安全策略引用名为 test 的 IKE profile。
[DeviceB-ipsec-policy-isakmp-test-1] ike-profile test
[DeviceB-ipsec-policy-isakmp-test-1] quit
应用 IPsec 策略。
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy test
[DeviceB-GigabitEthernet1/0/1] quit
创建 Track 项 1，监视 GigabitEthernet1/0/2 接口状态。
[DeviceB] track 1 interface gigabitethernet 1/0/2
创建 VRRP 备份组 100，配置虚拟 IP 地址为 10.0.0.1。
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 100 virtual-ip 10.0.0.1

```

# 设备在 VRRP 备份组中的优先级默认为 100，因此配置 Device B 在 VRRP 备份组 100 中的优先级为 150。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 100 priority 150
```

# 配置监视指定的 Track 项 1，当 Track 项 1 的状态为 Negative 时，Device B 在备份组 100 中的优先级降低 60，使其低于默认值。

```
[DeviceB-GigabitEthernet1/0/1] vrrp vrid 100 track 1 priority reduce 60
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

# 创建 Track 项 2，监视 GigabitEthernet1/0/1 接口状态。

```
[DeviceB] track 2 interface gigabitethernet 1/0/1
```

# 创建 VRRP 备份组 200，配置虚拟 IP 地址为 20.0.0.1。

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 200 virtual-ip 20.0.0.1
```

# 设备在 VRRP 备份组中的优先级默认为 100，因此配置 Device B 在 VRRP 备份组 200 中的优先级为 150。

```
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 200 priority 150
```

# 配置监视指定的 Track 项 2，当 Track 项 2 的状态为 Negative 时，Device B 在备份组 200 中的优先级降低 60，使其低于默认值。

```
[DeviceB-GigabitEthernet1/0/2] vrrp vrid 200 track 2 priority reduce 60
```

```
[DeviceB-GigabitEthernet1/0/2] quit
```

### 6.5.3 Device C 的配置

# 配置接口的 IP 地址。

```
<DeviceC> system-view
```

```
[DeviceC] interface gigabitethernet 1/0/1
```

```
[DeviceC-GigabitEthernet1/0/1] ip address 10.0.0.3 255.255.255.0
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

```
[DeviceC] interface gigabitethernet 1/0/2
```

```
[DeviceC-GigabitEthernet1/0/2] ip address 20.0.0.3 255.255.255.0
```

```
[DeviceC-GigabitEthernet1/0/2] quit
```

# 配置到 192.168.1.0/24 网段的静态路由。

```
[DeviceC] ip route-static 192.168.1.0 255.255.255.0 10.0.0.100
```

# 配置 ACL 3000，指定 IPsec 需要保护的数据流。

```
[DeviceC] acl number 3000
```

```
[DeviceC-acl-adv-3000] rule 0 permit ip source 20.0.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
```

```
[DeviceC-acl-adv-3000] quit
```

# 创建 IKE Keychain，并配置与对端地址为 10.0.0.100 使用的预共享密钥为明文的 123456

```
[DeviceC] ike keychain test
```

```
[DeviceC-ike-keychain-test] pre-shared-key address 10.0.0.100 key simple 123456
```

```
[DeviceC-ike-keychain-test] quit
```

# 创建 IKE profile，指定采用预共享密钥时使用的 IKE Keychain，并配置使用 VRRP 备份组 100 的虚拟 IP 地址 10.0.0.1 标识本端身份信息、使用 Device A 的上行接口地址 10.0.0.100 来匹配对端身份。

```
[DeviceC] ike profile test
```

```

[DeviceC-ike-profile-test] keychain test
[DeviceC-ike-profile-test] local-identity address 10.0.0.1
[DeviceC-ike-profile-test] match remote identity address 10.0.0.100
[DeviceC-ike-profile-test] quit
创建 IPsec 安全提议 test，安全封装模式、安全协议类型均采用系统缺省值。
[DeviceC] ipsec transform-set test
配置 ESP 协议采用的加密算法为采用 64 比特的 DES 算法，认证算法为 MD5。
[DeviceC-ipsec-transform-set-test] esp encryption-algorithm des-cbc
[DeviceC-ipsec-transform-set-test] esp authentication-algorithm md5
[DeviceC-ipsec-transform-set-test] quit
创建 IPsec 安全策略 test、顺序号为 1、采用 IKE 方式协商 IPsec SA 的 IPsec 安全策略，并进入
IPsec 安全策略视图。
[DeviceC] ipsec policy test 1 isakmp
指定 IPsec 隧道的本端 IP 地址为 10.0.0.1。
[DeviceC-ipsec-policy-isakmp-test-1] local-address 10.0.0.1
指定 IPsec 隧道的对端 IP 地址为 10.0.0.100。
[DeviceC-ipsec-policy-isakmp-test-1] remote-address 10.0.0.100
配置 IPsec 安全策略引用 ACL 3000。
[DeviceC-ipsec-policy-isakmp-test-1] security acl 3000
配置 IPsec 安全策略引用安全提议 test。
[DeviceC-ipsec-policy-isakmp-test-1] transform-set test
配置 IPsec 安全策略引用名为 test 的 IKE profile。
[DeviceC-ipsec-policy-isakmp-test-1] ike-profile test
[DeviceC-ipsec-policy-isakmp-test-1] quit
应用 IPsec 策略。
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ipsec apply policy test
[DeviceC-GigabitEthernet1/0/1] quit
创建 VRRP 备份组 100，配置虚拟 IP 地址为 10.0.0.1。
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] vrrp vrid 100 virtual-ip 10.0.0.1
[DeviceC-GigabitEthernet1/0/1] quit
创建 VRRP 备份组 200，配置虚拟 IP 地址为 20.0.0.1。
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] vrrp vrid 200 virtual-ip 20.0.0.1
[DeviceC-GigabitEthernet1/0/2] quit

```

## 6.6 验证配置

- (1) 在 Device B 和 Device C 上分别查看 VRRP 备份组的信息。可以看到在 VRRP 备份组 100 和 VRRP 备份组 200 中，Master 均为 Device B，Backup 均为 Device C。

# 在 Device B 上查看 VRRP 备份组信息。

```

[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode : Standard

```

Total number of virtual routers : 2

Interface GigabitEthernet1/0/1

|              |                  |             |          |
|--------------|------------------|-------------|----------|
| VRID         | : 100            | Adver Timer | : 100    |
| Admin Status | : Up             | State       | : Master |
| Config Pri   | : 150            | Running Pri | : 150    |
| Preempt Mode | : Yes            | Delay Time  | : 0      |
| Auth Type    | : None           |             |          |
| Virtual IP   | : 10.0.0.1       |             |          |
| Virtual MAC  | : 0000-5e00-0164 |             |          |
| Master IP    | : 10.0.0.2       |             |          |

VRRP Track Information:

|              |     |       |            |             |      |
|--------------|-----|-------|------------|-------------|------|
| Track Object | : 1 | State | : Positive | Pri Reduced | : 60 |
|--------------|-----|-------|------------|-------------|------|

Interface GigabitEthernet1/0/2

|              |                  |             |          |
|--------------|------------------|-------------|----------|
| VRID         | : 200            | Adver Timer | : 100    |
| Admin Status | : Up             | State       | : Master |
| Config Pri   | : 150            | Running Pri | : 150    |
| Preempt Mode | : Yes            | Delay Time  | : 0      |
| Auth Type    | : None           |             |          |
| Virtual IP   | : 20.0.0.1       |             |          |
| Virtual MAC  | : 0000-5e00-0102 |             |          |
| Master IP    | : 20.0.0.2       |             |          |

VRRP Track Information:

|              |     |       |            |             |      |
|--------------|-----|-------|------------|-------------|------|
| Track Object | : 2 | State | : Positive | Pri Reduced | : 60 |
|--------------|-----|-------|------------|-------------|------|

# 在 Device C 上查看 VRRP 备份组信息。

[DeviceC] display vrrp verbose

IPv4 Virtual Router Information:

Running Mode : Standard

Total number of virtual routers : 2

Interface GigabitEthernet1/0/1

|               |               |             |          |
|---------------|---------------|-------------|----------|
| VRID          | : 100         | Adver Timer | : 100    |
| Admin Status  | : Up          | State       | : Backup |
| Config Pri    | : 100         | Running Pri | : 100    |
| Preempt Mode  | : Yes         | Delay Time  | : 0      |
| Become Master | : 3480ms left |             |          |
| Auth Type     | : None        |             |          |
| Virtual IP    | : 10.0.0.1    |             |          |
| Master IP     | : 10.0.0.2    |             |          |

Interface GigabitEthernet1/0/2

|               |               |             |          |
|---------------|---------------|-------------|----------|
| VRID          | : 200         | Adver Timer | : 100    |
| Admin Status  | : Up          | State       | : Backup |
| Config Pri    | : 100         | Running Pri | : 100    |
| Preempt Mode  | : Yes         | Delay Time  | : 0      |
| Become Master | : 2820ms left |             |          |
| Auth Type     | : None        |             |          |
| Virtual IP    | : 20.0.0.1    |             |          |
| Master IP     | : 20.0.0.2    |             |          |

- (2) 从分支机构 ping 总部网关的 IP 地址 20.0.0.1，触发 IKE 协商，SA 协商成功后可以 ping 通。

```
<DeviceA> ping -a 192.168.1.1 20.0.0.1
PING 30.1.1.123: 56 data bytes, press CTRL_C to break
Request time out
Reply from 20.0.0.1: bytes=56 Sequence=1 ttl=127 time=2 ms
Reply from 20.0.0.1: bytes=56 Sequence=2 ttl=127 time=1 ms
Reply from 20.0.0.1: bytes=56 Sequence=3 ttl=127 time=1 ms
Reply from 20.0.0.1: bytes=56 Sequence=4 ttl=127 time=2 ms

--- 20.0.0.1 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

- (3) 通过 **display ike sa** 命令分别在 Device A 和 Device B 上查看到 IKE SA 的建立情况。

# 在 Device A 上查看 IKE SA 的信息，可以看到 Device A 的 IKE SA 对端地址为 VRRP 备份组的虚拟 IP 地址。

```
[DeviceA] display ike sa
 Connection-ID Remote Flag DOI

 29 10.0.0.1 RD IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

# 在 Device B 上查看 IKE SA 的信息，可以看到 Device B 的 IKE SA 对端地址为 Device A 上 GigabitEthernet1/0/2 接口的 IP 地址。

```
[DeviceB] display ike sa
 Connection-ID Remote Flag DOI

 17 10.0.0.100 RD IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

- (4) 通过 **display ipsec sa brief** 命令分别在 Device A 和 Device B 上查看到 IPsec SA 的建立情况，可以看到 IPsec 隧道已成功建立

# 在 Device A 上查看 IPsec SA 的信息。

```
[DeviceA] display ipsec sa brief

Interface/Global Dst Address SPI Protocol Status

GE1/0/2 10.0.0.1 4051765865 ESP active
GE1/0/2 10.0.0.100 1860835944 ESP active
```

# 在 Device B 上查看 IPsec SA 的信息。

```
[DeviceB] display ipsec sa brief

Interface/Global Dst Address SPI Protocol Status

GE1/0/1 10.0.0.100 1860835944 ESP active
```

```
GE1/0/1 10.0.0.1 4051765865 ESP active
```

- (5) 手工关闭 Device B 的 GigabitEthernet1/0/1 接口，Device B 的 VRRP 状态切换到 Backup，Device C 的 VRRP 状态切换到 Master。重新从分支机构 ping 总部的 IP 地址 20.0.0.1，DPD 检测 IKE 对等体无响应，删除本端 SA，重新与 Device C 进行 IKE 协商，建立新的 SA 后，可以 ping 通总部 IP 地址。

# 在 Device B 上查看当前 VRRP 的状态信息。

```
[DeviceB] display vrrp
IPv4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 2
Interface VRID State Run Adver Auth Virtual
 Pri Timer Type Type IP

GE1/0/1 100 Initialize 150 1 None 10.0.0.1
GE1/0/2 200 Backup 90 1 None 20.0.0.1
```

# 在 Device C 上查看当前 VRRP 的状态信息，已经从 Backup 状态切换成 Master 状态。

```
[DeviceC] display vrrp
IPv4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 2
Interface VRID State Run Adver Auth Virtual
 Pri Timer Type Type IP

GE1/0/1 100 Master 100 1 None 10.0.0.1
GE1/0/2 200 Master 100 1 None 20.0.0.1
```

# 从 Device A 上 ping 总部网关 IP 地址 20.0.0.1，可以 ping 通。

```
<DeviceA> ping -a 192.168.1.1 20.0.0.1
PING 20.0.0.1: 56 data bytes, press CTRL_C to break
 Reply from 20.0.0.1: bytes=56 Sequence=0 ttl=127 time=2 ms
 Reply from 20.0.0.1: bytes=56 Sequence=1 ttl=127 time=1 ms
 Reply from 20.0.0.1: bytes=56 Sequence=2 ttl=127 time=1 ms
 Reply from 20.0.0.1: bytes=56 Sequence=3 ttl=127 time=1 ms
 Reply from 20.0.0.1: bytes=56 Sequence=4 ttl=127 time=2 ms

--- 20.0.0.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/2 ms
```

# 通过 **display ike sa** 命令中的标识符 connection-id 字段，可以判断 Device A 上已经重新协商了 SA。

```
[DeviceA] display ike sa
Connection-ID Remote Flag DOI

30 10.0.0.1 RD IPSEC
```

flag meaning



```
RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK--REKEY
在 Device C 上可以查看到 SA 信息。
```

```
[DeviceC] display ike sa
 Connection-ID Remote Flag DOI

 3 10.0.0.100 RD IPSEC

flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK--REKEY
```

```
[DeviceC] display ipsec sa brief
total phase-2 IPv4 SAs: 2
Interface/Global Dst Address SPI Protocol Status

GE1/0/1 10.0.0.100 1235764751 ESP active
GE1/0/1 10.0.0.1 799485439 ESP active
```

- (6) 当 Device B 的 GE1/1 接口重新 UP 时, VRRP 状态切换为 Master, 从分支到总部的数据流会重新发送到 Device B 上, 通过 DPD 特性, Device A 删除 SA 重新与 Device B 进行 IKE 协商, 协商成功后分支到总部的数据流会在新的 IPsec 隧道上得以传输。验证方法与上一个步骤相同, 此处省略。

## 6.7 配置文件

- Device A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.0.0.100 255.255.255.0
 ipsec apply policy test
#
ip route-static 20.0.0.0 255.255.255.0 10.0.0.1
#
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 20.0.0.0 0.0.0.255
#
ipsec transform-set test
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy test 1 isakmp
 transform-set test
 security acl 3000
 local-address 10.0.0.100
 remote-address 10.0.0.1
```

```

ike-profile test
#
ike dpd interval 10 on-demand
#
ike profile test
keychain test
local-identity address 10.0.0.100
match remote identity address 10.0.0.1 255.255.255.0
#
ike keychain test
pre-shared-key address 10.0.0.1 255.255.255.255 key cipher
c3$VPq7TeKUusm/5GG8rHfZGHQR+Rbrhbk=
#

```

- **Device B:**

```

#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.0.0.2 255.255.255.0
ipsec apply policy test
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 20.0.0.2 255.255.255.0
#
ip route-static 192.168.1.0 255.255.255.0 10.0.0.100
#
acl number 3000
rule 0 permit ip source 20.0.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec transform-set test
esp encryption-algorithm des-cbc
esp authentication-algorithm md5
#
ipsec policy test 1 isakmp
transform-set test
security acl 3000
local-address 10.0.0.1
remote-address 10.0.0.100
ike-profile test
#
ike profile test
keychain test
local-identity address 10.0.0.1
match remote identity address 10.0.0.100 255.255.255.0
#
ike keychain test
pre-shared-key address 10.0.0.100 255.255.255.255 key cipher
c3$VPq7TeKUusm/5GG8rHfZGHQR+Rbrhbk=

```

- Device C:
 

```

#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.0.0.3 255.255.255.0
ipsec apply policy test
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.0.0.3 255.255.255.0

#
ip route-static 192.168.1.0 255.255.255.0 10.0.0.100
#
acl number 3000
 rule 0 permit ip source 20.0.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec transform-set test
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy test 1 isakmp
 transform-set test
 security acl 3000
 local-address 10.0.0.1
 remote-address 10.0.0.100
 ike-profile test
#
ike profile test
 keychain test
 local-identity address 10.0.0.1
 match remote identity address 10.0.0.100 255.255.255.0
#
ike keychain test
 pre-shared-key address 10.0.0.100 255.255.255.255 key cipher
c3$VPq7TeKUusm/5GG8rHfZGHQR+Rbrhbk=
#

```

## 7 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“可靠性配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“可靠性命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“安全配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“安全命令参考”

# H3C MSR 系列路由器

## SNMP 配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                            |    |
|----------------------------|----|
| 1 简介.....                  | 1  |
| 2 配置前提.....                | 1  |
| 3 SNMPv1/SNMPv2c 配置举例..... | 1  |
| 3.1 组网需求.....              | 1  |
| 3.2 使用版本.....              | 1  |
| 3.3 配置注意事项.....            | 1  |
| 3.4 配置步骤.....              | 2  |
| 3.4.1 设备的配置.....           | 2  |
| 3.4.2 NMS 的配置.....         | 2  |
| 3.5 验证配置.....              | 3  |
| 3.6 配置文件.....              | 5  |
| 4 SNMPv3 配置举例.....         | 5  |
| 4.1 组网需求.....              | 5  |
| 4.2 使用版本.....              | 5  |
| 4.3 配置注意事项.....            | 6  |
| 4.4 配置步骤.....              | 6  |
| 4.4.1 设备的配置.....           | 6  |
| 4.4.2 NMS 的配置.....         | 6  |
| 4.4.3 验证配置.....            | 8  |
| 4.5 配置文件.....              | 10 |
| 5 相关资料.....                | 10 |

# 1 简介

本文档介绍了 SNMP 功能典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

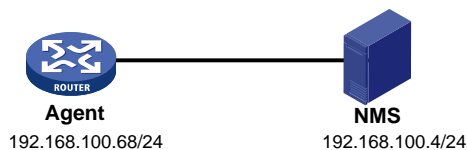
本文档假设您已了解 SNMP 特性。

## 3 SNMPv1/SNMPv2c 配置举例

### 3.1 组网需求

如图 1 所示，服务器作为 NMS 通过 SNMPv1/SNMPv2c 协议对设备进行配置文件备份，并且当设备出现故障时能够主动向 NMS 发送告警信息。

图1 SNMPv1/v2c 功能典型配置组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置注意事项

- SNMPv2c 与 SNMPv1 配置方法完全一致，本举例中以配置 SNMPv2c 为例进行介绍。
- 用户在设备和 NMS 上配置的 SNMP 版本号和团体字必须一致，否则，NMS 无法对设备进行管理维护。
- 不同厂商的 NMS 软件配置方法不同，本配置举例中，以 IMC PLAT 7.0 (E0202)为例进行介绍。

## 3.4 配置步骤

### 3.4.1 设备的配置

# 设置 Agent 使用的 SNMP 版本为 v2c、只读团体名为 readtest，读写团体名为 writetest。

```
<Agent> system-view
[Agent] snmp-agent sys-info version v2c
[Agent] snmp-agent community read readtest
[Agent] snmp-agent community write writetest
```

# 设置设备的联系人和位置信息，以方便维护。

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

# 设置允许向 NMS 发送告警信息，使用的团体名为 readtest。

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
readtest v2c
```

### 3.4.2 NMS 的配置

# 增加设备。

登录进入 IMC 管理平台，选择“资源”页签，单击导航树中的[增加设备]菜单项，进入增加设备配置页面。

- 设置设备的主机名或 IP 地址为“192.168.100.68”；
- 其它参数采用缺省值。

图2 增加设备配置页面

资源 > 增加设备 帮助

**设备基本信息**

主机名或IP地址 \* 192.168.100.68

设备标签

掩码

设备分组

登录方式 Telnet

将设备的Trap发送到本网管系统

设备支持Ping操作

Ping不通也加入

将LoopBack地址作为管理IP

**配置SNMP参数**

设置

|         |         |
|---------|---------|
| 参数类型    | SNMPv2c |
| 只读团体字   | *****   |
| 读写团体字   | *****   |
| 超时时间(秒) | 4       |
| 重试次数    | 3       |

+ 配置Telnet参数

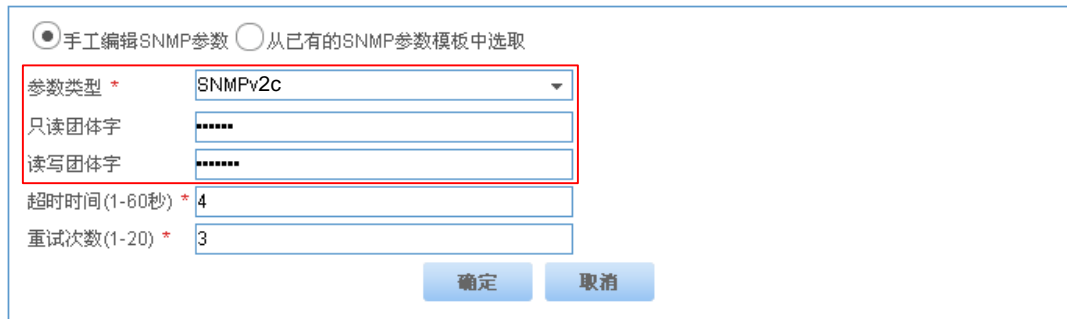
+ 配置SSH参数

确定 取消

# 在该页面中单击“配置 SNMP 参数”按钮，展开配置 SNMP 参数页面，单击“设置”，在弹出的对话框中设置如下内容。

- 设置参数类型为“SNMPv2c”；
- 设置只读团体字为“readtest”；
- 设置读写团体字为“writetest”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 SNMP 参数设置页面



The image shows a configuration dialog box for SNMP parameters. At the top, there are two radio buttons: "手工编辑SNMP参数" (selected) and "从已有的SNMP参数模板中选取". Below this, there are five input fields: "参数类型 \*" (SNMPv2c), "只读团体字" (\*\*\*\*\*), "读写团体字" (\*\*\*\*\*), "超时时间(1-60秒) \*" (4), and "重试次数(1-20) \*" (3). At the bottom, there are two buttons: "确定" (OK) and "取消" (Cancel).

# 在“增加设备”页面单击<确定>按钮，iMC 返回增加设备成功信息。

图4 增加设备成功页面



The image shows a success message box titled "资源 > 设备信息" with a "帮助" icon. The message reads: "增加设备完成，您可继续选择如下操作：". Below this, there are three links: "设备详细信息" (查看刚刚增加的设备详细信息。), "复制增加" (采用这个设备的SNMP、Telnet、SSH参数新增加设备。), and "增加设备" (采用default模板参数增加设备。).

# 增加设备成功后，用户即可通过 iMC（NMS）对设备进行配置、管理和维护。不同 NMS 管理软件配置不同，关于 NMS 的详细配置，具体请参考 NMS 的相关手册。

## 3.5 验证配置

### (1) Agent 向 NMS 发送 Trap 信息

# 完成以上配置之后，在设备上的某个空闲接口执行 **shutdown** 或 **undo shutdown** 操作，设备会向 NMS 发送接口状态改变的 Trap。

# 在“告警 > 告警浏览 > 全部告警”页面中可以查看上述 Trap 信息。



图5 全部告警视图页面



(2) 在 NMS 上备份 Agent 配置文件

# 在“资源 > 设备视图”页签点击“Agent”，进入如图 6 页面，点击右侧的“备份配置文件”。

图6 备份配置文件



# 操作成功后会显示如下页面。

图7 备份配置文件成功

业务 > 设备配置一览表 > Agent(192.168.100.68) > 备份配置文件结果

| 备份配置文件结果                                                                                                                       |              |        |                     |                                       |                                           |                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------|--------------|--------|---------------------|---------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------|
|  手工备份设备结束。共备份“1”个设备，其中：备份成功“1”个设备，备份失败“0”个设备。 |              |        |                     |                                       |                                           |                                                                                     |
| 设备名称                                                                                                                           | 设备型号         | 配置文件类型 | 时间                  | 结果                                    | 配置文件名称                                    | 详细步骤                                                                                |
| Agent(192.168.100.68)                                                                                                          | H3C MSR56-60 | 启动     | 2014-04-30 10:14:44 | 共备份“2”个配置文件，其中：启动配置文件“1”个，运行配置文件“1”个。 | 192.168.100.68_startup_20140430101439.cfg |  |
| Agent(192.168.100.68)                                                                                                          | H3C MSR56-60 | 运行     | 2014-04-30 10:14:43 | 备份成功。                                 | 192.168.100.68_running_20140430101434.cfg |  |
|                                                                                                                                |              |        | 2014-04-30 10:14:28 | 备份配置文件开始。                             |                                           |                                                                                     |

## 3.6 配置文件

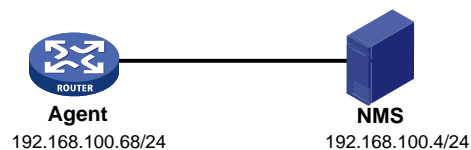
```
#
snmp-agent
snmp-agent community read readtest
snmp-agent community write writetest
snmp-agent sys-info contact Mr.Wang-Tel:3306
snmp-agent sys-info location telephone-closet,3rd-floor
snmp-agent sys-info version v2c
snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname readtest v2c
snmp-agent trap enable arp
#
```

## 4 SNMPv3 配置举例

### 4.1 组网需求

如图8所示，服务器作为 NMS 通过 SNMPv3 协议对设备进行配置文件备份，提供更高的安全性，并且当设备出现故障时能够主动向 NMS 发送告警信息。

图8 SNMPv3 功能典型配置组网图



### 4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

## 4.3 配置注意事项

- 用户需要分别对设备和 NMS 配置 SNMP 功能，设备与 NMS 的 SNMP 配置必须一致，否则，NMS 无法对设备进行管理和维护。
- 不同厂商的 NMS 软件配置方法不同，本配置举例中，以 IMC PLAT 7.0 (E0202)为例进行介绍。
- SNMPv3 接收 Trap 报文的目的主机的安全参数要使用设备已配置的 v3 用户，且安全模型要一致。

## 4.4 配置步骤

### 4.4.1 设备的配置

# 设置 Agent 使用的 SNMP 版本为 v3。

```
<Agent> system-view
```

```
[Agent] snmp-agent sys-info version v3
```

# 创建 MIB 视图，名字为 mibtest，包含 mib-2 子树（OID 为“1.3.6.1”）所有对象。

```
[Agent] snmp-agent mib-view included mibtest 1.3.6.1
```

# 创建 SNMPv3 组 managev3group，并配置与该组绑定的 SNMPv3 用户与 NMS 建立连接时，均进行认证和加密，NMS 可以对设备进行读写的视图均为 mibtest。

```
[Agent] snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest notify-view mibtest
```

# 设置 SNMPv3 用户名为 managev3user，认证算法为 SHA-1，认证密码为 123456TESTauth&!，加密算法为 AES，加密密码是 123456TESTencr&!。

```
[Agent] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

# 设置设备的联系人和位置信息，以方便维护。

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
```

```
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

# 开启 SNMP 告警功能。

```
[Agent] snmp-agent trap enable
```

# 设置接收 SNMP 告警信息的目的主机 IP 地址，即 NMS 的 IP 地址，配置安全认证参数为 managev3user。

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname managev3user v3 privacy
```

### 4.4.2 NMS 的配置

# 登录 iMC，选择“系统管理”页签，单击导航树中的[资源管理/SNMP 模板]菜单项，进入 SNMP 模板配置页面，在该页面中单击<增加>按钮，进入增加 SNMP 模板配置页面。

- 配置 SNMP 模板的名称为 SNMPv3。
- 选择参数类型为 SNMPv3 Priv-Aes128 Auth-Sha。
- 配置 SNMP 用户名为 managev3user。
- 认证密码为 123456TESTauth&!

- 加密密码为 123456TESTencr&!。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9 增加 SNMP 模板页面

# 选择“资源”页签，单击导航树中的[资源管理/增加设备]菜单项，进入增加设备配置页面，在该页面中输入设备的主机名或 IP 地址，并单击<配置 SNMP 参数/设置>链接。

图10 增加设备页面

# 进入 SNMP 参数设置页面配置 SNMP 参数

- 选择“从已有的SNMP参数模板中选取”。
- 选择名称为“SNMPv3”的SNMP模板。
- 单击<确定>按钮完成操作，返回到“增加设备”页面。

图11 SNMP参数设置页面

| 模板名称                                    | 参数类型                        | 用户名          | 超时时间(秒) | 重试次数 |
|-----------------------------------------|-----------------------------|--------------|---------|------|
| <input type="radio"/> default           | SNMPv2c                     |              | 4       | 3    |
| <input checked="" type="radio"/> SNMPv3 | SNMPv3 Priv-Aes128 Auth-Sha | managev3user | 4       | 3    |

共有2条记录，当前第1 - 2，第 1/1 页。

# 在“增加设备”页面单击<确定>按钮，iMC 返回增加设备成功信息。

图12 增加设备成功页面

增加设备完成，您可继续选择如下操作：

- [设备详细信息](#)：查看刚刚增加的设备详细信息。
- [复制增加](#)：采用这个设备的SNMP、Telnet、SSH参数新增加设备。
- [增加设备](#)：采用default模板参数增加设备。

# 增加设备成功后，用户即可通过 iMC（NMS）对设备进行配置、管理和维护。不同 NMS 管理软件配置不同，关于 NMS 的详细配置，具体请参考 NMS 的相关手册。

### 4.4.3 验证配置

#### (1) Agent 向 NMS 发送 Trap 信息

# 完成以上配置之后，在设备上的某个空闲接口执行 **shutdown** 或 **undo shutdown** 操作，设备会向 NMS 发送接口状态改变的 Trap。

# 在“告警 > 告警浏览 > 全部告警”页面中可以查看上述 Trap 信息。

图13 全部告警视图页面



(2) 在 NMS 上备份 Agent 配置文件

# 在“资源 > 设备视图”页签点击“Agent”，进入如下页面，点击右侧的“备份配置文件”。

图14 备份配置文件



# 操作成功后会显示如下页面。

图15 备份配置文件成功

业务 > 设备配置一览表 > Agent(192.168.100.68) > 备份配置文件结果

| 备份配置文件结果                                                                                                                       |              |        |                     |                                       |                                           |                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------|--------------|--------|---------------------|---------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------|
|  手工备份设备结束。共备份“1”个设备，其中：备份成功“1”个设备，备份失败“0”个设备。 |              |        |                     |                                       |                                           |                                                                                     |
| 设备名称                                                                                                                           | 设备型号         | 配置文件类型 | 时间                  | 结果                                    | 配置文件名称                                    | 详细步骤                                                                                |
|                                                                                                                                |              |        | 2014-04-30 10:14:44 | 共备份“2”个配置文件，其中：启动配置文件“1”个，运行配置文件“1”个。 |                                           |                                                                                     |
| Agent(192.168.100.68)                                                                                                          | H3C MSR56-60 | 启动     | 2014-04-30 10:14:43 | 备份成功。                                 | 192.168.100.68_startup_20140430101439.cfg |  |
| Agent(192.168.100.68)                                                                                                          | H3C MSR56-60 | 运行     | 2014-04-30 10:14:43 | 备份成功。                                 | 192.168.100.68_running_20140430101434.cfg |  |
|                                                                                                                                |              |        | 2014-04-30 10:14:28 | 备份配置文件开始。                             |                                           |                                                                                     |

## 4.5 配置文件

```
#
snmp-agent
snmp-agent sys-info contact Mr.Wang-Tel:3306
snmp-agent sys-info location telephone-closet,3rd-floor
snmp-agent sys-info version v3
snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest notify-view mibtest
snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname managev3user v3 privacy
snmp-agent mib-view included mibtest internet
snmp-agent usm-user v3 managev3user managev3group cipher authentication-mode sha
c3$4CcVHVR5z0PUt42S65Q7t5CinLsNC0qt45linidSxj6AdbAipck= privacy-mode aes128
c3$u3MpkHY9/mUEWZpDydimSpuDZP6HCeW2p3GmEqHT5Eys5A==
snmp-agent trap enable arp
snmp-agent trap enable radius
#
```

## 5 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“网络管理和监控配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“网络管理和监控命令参考”

# H3C MSR 系列路由器

## Sampler 结合 IPv4 NetStream 使用配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目录

|               |   |
|---------------|---|
| 1 简介.....     | 1 |
| 2 配置前提.....   | 1 |
| 3 配置举例.....   | 1 |
| 3.1 组网需求..... | 1 |
| 3.2 使用版本..... | 1 |
| 3.3 配置步骤..... | 2 |
| 3.4 验证配置..... | 2 |
| 3.5 配置文件..... | 3 |
| 4 相关资料.....   | 4 |

# 1 简介

本文档介绍通过 **Sampler** 结合 **IPv4 NetStream** 使用的典型配置举例。

## 2 配置前提

本文档适用于使用 **Comware V7** 软件版本的 **MSR** 系列路由器，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 **Sampler** 特性和 **IPv4 NetStream** 特性。

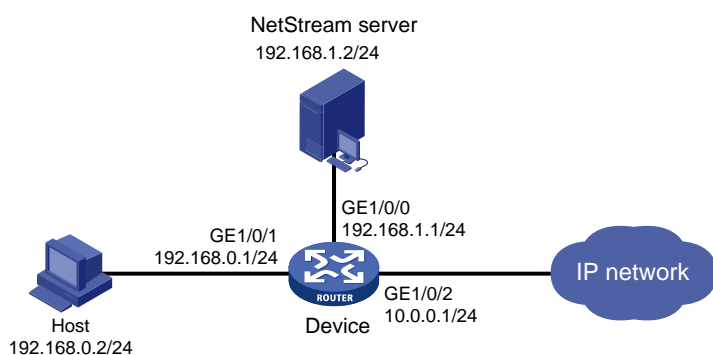
## 3 配置举例

### 3.1 组网需求

如图 1 所示，路由器作为局域网内主机访问外网的网关，现要求通过 **NetStream** 功能使用采样器对路由器上 **GigabitEthernet1/0/1** 出方向和 **GigabitEthernet1/0/2** 入方向的流量进行统计，再将统计的信息输出到 **Netstream** 服务器上。具体应用需求如下：

- 在接口 **GigabitEthernet1/0/1** 的出方向上配置随机采样，每 200 个报文中抽取一个报文进行 **NetStream** 统计。
- 在接口 **GigabitEthernet1/0/2** 的入方向上配置固定采样，每 100 个报文中抽取一个报文进行 **NetStream** 统计。

图1 Sampler 结合 IPv4 NetStream 使用配置组网图



### 3.2 使用版本

本举例是在 **R6728** 版本上进行配置和验证的。

### 3.3 配置步骤

# 创建一个名为 **samplerin** 的采样器，采用固定采样方式，设置采样率为 100，即 100 个报文中抽取第一个报文。

```
<Device> system-view
[Device] sampler samplerin mode fixed packet-interval 100
```

# 创建一个名为 **samplerout** 的采样器，采用随机采样方式，设置采样率为 200，即 200 个报文中抽取任意一个报文。

```
[Device] sampler samplerout mode random packet-interval 200
```

# 配置接口 **GigabitEthernet1/0/2** 地址，在此接口的入方向开启 **NetStream** 功能，使用 **samplerin** 采样器对该接口的流量进行采样。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ip address 10.0.0.1 24
[Device-GigabitEthernet1/0/2] ip netstream inbound
[Device-GigabitEthernet1/0/2] ip netstream sampler samplerin inbound
[Device-GigabitEthernet1/0/2] quit
```

# 配置接口 **GigabitEthernet1/0/1** 地址，在此接口的出方向开启 **NetStream** 功能，使用 **samplerout** 采样器对该接口的流量进行采样。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.0.1 24
[Device-GigabitEthernet1/0/1] ip netstream outbound
[Device-GigabitEthernet1/0/1] ip netstream sampler samplerout outbound
[Device-GigabitEthernet1/0/1] quit
```

# 配置接口 **GigabitEthernet1/0/0** 地址。

```
[Device] interface gigabitethernet 1/0/0
[Device-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[Device-GigabitEthernet1/0/0] quit
```

# 配置 **NetStream** 普通流统计信息输出的目的地址为 **192.168.1.2** 和目的 **UDP** 端口号为 **5000**。

```
[Device] ip netstream export host 192.168.1.2 5000
```

### 3.4 验证配置

# 通过 **display sampler** 命令查看采样器的配置信息。

```
[Device] display sampler
Sampler name: samplerout
Mode: random; Packet-interval: 200
Sampler name: samplerin
Mode: fixed; Packet-interval: 100
```

# 路由器运行一段时间后，通过 **display ip netstream cache** 命令来查看 **NetStream** 流缓存区的配置和状态信息。

```
[Device] display ip netstream cache
IP NetStream cache information:
Active flow timeout : 30 min
Inactive flow timeout : 30 sec
Max number of entries : 10000
```

```

IP active flow entries : 1
MPLS active flow entries : 0
L2 active flow entries : 0
IPL2 active flow entries : 0
IP flow entries counted : 7
MPLS flow entries counted : 0
L2 flow entries counted : 0
IPL2 flow entries counted : 0
Last statistics resetting time : Never

```

IP packet size distribution (157 packets in total):

```

1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.000 .929 .031 .006 .000 .006 .000 .000 .000 .000 .025 .000 .000 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608 >4608
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

```

| Protocol   | Total Flows | Packets /sec | Flows /sec | Packets /flow | Active(sec) /flow | Idle(sec) /flow |
|------------|-------------|--------------|------------|---------------|-------------------|-----------------|
| TCP-other  | 3           | 0            | 0          | 26            | 7                 | 30              |
| ICMP       | 1           | 0            | 0          | 1             | 0                 | 30              |
| UDP-BOOTP  | 1           | 0            | 0          | 4             | 15                | 30              |
| TCP-Telnet | 2           | 0            | 0          | 35            | 24                | 30              |

| Type | DstIP(Port)         | SrcIP(Port)        | Pro | ToS | If(Direct) | Pkts |
|------|---------------------|--------------------|-----|-----|------------|------|
|      | DstMAC(VLAN)        | SrcMAC(VLAN)       |     |     |            |      |
|      | TopLblType(IP/MASK) | Lbl-Exp-S-List     |     |     |            |      |
| IP   | 192.168.0.1(23)     | 192.168.0.2(56839) | 6   | 0   | GE1/0/1(I) | 1    |

# 通过 **display ip netstream export** 命令来查看 NetStream 统计输出报文的信息。

```
[Device] display ip netstream export
```

```
IP export information:
```

```

Flow source interface : Not specified
Flow destination VPN instance : Not specified
Flow destination IP address (UDP) : 192.168.1.2 (5000)
Version 5 exported flows number : 0
Version 5 exported UDP datagrams number (failed): 0 (0)
Version 9 exported flows number : 8
Version 9 exported UDP datagrams number (failed): 6 (6)

```

### 3.5 配置文件

```

#
sampler samplerout mode random packet-interval 200
sampler samplerin mode fixed packet-interval 100
#

```

```
ip netstream export host 192.168.1.2 5000
#
interface GigabitEthernet1/0/0
port link-mode route
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.0.1 255.255.255.0
ip netstream outbound
ip netstream sampler samplerout outbound
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 10.0.0.1 255.255.255.0
ip netstream inbound
ip netstream sampler samplerin inbound
#
```

## 4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“网络管理和监控配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“网络管理和监控命令参考”

# H3C MSR 系列路由器

## NQA 配置举例

---

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                           |    |
|---------------------------|----|
| 1 简介.....                 | 1  |
| 2 配置前提 .....              | 1  |
| 3 UDP-jitter 测试配置举例 ..... | 1  |
| 3.1 组网需求 .....            | 1  |
| 3.2 使用版本 .....            | 1  |
| 3.3 配置注意事项.....           | 1  |
| 3.4 配置步骤 .....            | 1  |
| 3.5 验证配置 .....            | 2  |
| 3.6 配置文件 .....            | 4  |
| 4 SNMP 测试配置举例.....        | 4  |
| 4.1 组网需求 .....            | 4  |
| 4.2 使用版本 .....            | 4  |
| 4.3 配置注意事项.....           | 4  |
| 4.4 配置步骤 .....            | 5  |
| 4.5 验证配置 .....            | 5  |
| 4.6 配置文件 .....            | 6  |
| 5 TCP 测试配置举例 .....        | 6  |
| 5.1 组网需求 .....            | 6  |
| 5.2 使用版本 .....            | 6  |
| 5.3 配置注意事项.....           | 6  |
| 5.4 配置步骤 .....            | 7  |
| 5.5 验证配置 .....            | 7  |
| 5.6 配置文件 .....            | 8  |
| 6 UDP-echo 测试配置举例 .....   | 8  |
| 6.1 组网需求 .....            | 8  |
| 6.2 使用版本 .....            | 8  |
| 6.3 配置注意事项.....           | 8  |
| 6.4 配置步骤 .....            | 8  |
| 6.5 验证配置 .....            | 9  |
| 6.6 配置文件 .....            | 9  |
| 7 Voice 测试配置举例 .....      | 10 |
| 7.1 组网需求 .....            | 10 |

|                            |           |
|----------------------------|-----------|
| 7.2 使用版本 .....             | 10        |
| 7.3 配置注意事项.....            | 10        |
| 7.4 配置步骤 .....             | 10        |
| 7.5 验证配置 .....             | 11        |
| 7.6 配置文件 .....             | 13        |
| <b>8 DLSw 测试配置举例 .....</b> | <b>13</b> |
| 8.1 组网需求 .....             | 13        |
| 8.2 使用版本 .....             | 13        |
| 8.3 配置注意事项.....            | 13        |
| 8.4 配置步骤 .....             | 13        |
| 8.5 验证配置 .....             | 14        |
| 8.6 配置文件 .....             | 14        |
| <b>9 相关资料 .....</b>        | <b>14</b> |



# 1 简介

本文档介绍 NQA 的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 NQA 特性。

## 3 UDP-jitter 测试配置举例

### 3.1 组网需求

如[图 1](#)所示，Device A 和 Device B 之间的网络承载了语音、视频等实时性业务，对时延抖动（Delay jitter）的要求较高。现要求配置 UDP-jitter 测试方案，使用户可以根据实际需要随时调用该测试方案测试本端（Device A）和指定目的端（Device B）之间传送报文的时延抖动，从而判断网络是否可以承载实时性业务。

图1 UDP-jitter 测试组网图



### 3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 3.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。
- 在进行 UDP-jitter 类型测试前，必须配置 Device B 为 NQA 服务器。

### 3.4 配置步骤

- (1) 配置 Device B

# 使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

## (2) 配置 Device A

# 创建 UDP-jitter 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-jitter
配置测试操作的目的地址和目的端口号
[DeviceA-nqa-admin-test-udp-jitter] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-jitter] destination port 9000
测试组每次测试之间的时间间隔为 1000 毫秒。
[DeviceA-nqa-admin-test-udp-jitter] frequency 1000
[DeviceA-nqa-admin-test-udp-jitter] quit
```

## 3.5 验证配置

# 启动 UDP-jitter 测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 UDP-jitter 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

# 以上配置完成后，显示 UDP-jitter 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
 Send operation times: 10 Receive response times: 10
 Min/Max/Average round trip time: 1/1/1
 Square-Sum of round trip time: 10
 Last packet received time: 2014-07-30 09:46:36.9
Extended results:
 Packet loss ratio: 0%
 Failures due to timeout: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
 Packets out of sequence: 0
 Packets arrived late: 0
UDP-jitter results:
RTT number: 10
 Min positive SD: 1 Min positive DS: 0
 Max positive SD: 1 Max positive DS: 0
 Positive SD number: 1 Positive DS number: 0
 Positive SD sum: 1 Positive DS sum: 0
 Positive SD average: 1 Positive DS average: 0
 Positive SD square-sum: 1 Positive DS square-sum: 0
 Min negative SD: 0 Min negative DS: 0
 Max negative SD: 0 Max negative DS: 0
```

```

Negative SD number: 0
Negative SD sum: 0
Negative SD average: 0
Negative SD square-sum: 0
One way results:
Max SD delay: 0
Min SD delay: 0
Number of SD delay: 0
Sum of SD delay: 0
Square-Sum of SD delay: 0
SD lost packets: 0
Lost packets for unknown reason: 0
Negative DS number: 0
Negative DS sum: 0
Negative DS average: 0
Negative DS square-sum: 0
Max DS delay: 0
Min DS delay: 0
Number of DS delay: 0
Sum of DS delay: 0
Square-Sum of DS delay: 0
DS lost packets: 0

```

# 显示 UDP-jitter 测试的统计结果。

```
[DeviceA] display nqa statistics admin test
```

```
NQA entry (admin admin, tag test) test statistics:
```

```

NO. : 1
Start time: 2014-07-30 09:46:22.7
Life time: 14 seconds
Send operation times: 150 Receive response times: 150
Min/Max/Average round trip time: 1/4/1
Square-Sum of round trip time: 165

```

```
Extended results:
```

```

Packet loss ratio: 0%
Failures due to timeout: 0
Failures due to internal error: 0
Failures due to other errors: 0
Packets out of sequence: 0
Packets arrived late: 0

```

```
UDP-jitter results:
```

```

RTT number: 150
Min positive SD: 1
Max positive SD: 6
Positive SD number: 11
Positive SD sum: 16
Positive SD average: 1
Positive SD square-sum: 46
Min negative SD: 5
Max negative SD: 5
Negative SD number: 1
Negative SD sum: 5
Negative SD average: 5
Negative SD square-sum: 25
Min positive DS: 1
Max positive DS: 1
Positive DS number: 5
Positive DS sum: 5
Positive DS average: 1
Positive DS square-sum: 5
Min negative DS: 1
Max negative DS: 1
Negative DS number: 1
Negative DS sum: 1
Negative DS average: 1
Negative DS square-sum: 1

```

```
One way results:
```

```

Max SD delay: 0
Min SD delay: 0
Number of SD delay: 0
Sum of SD delay: 0
Square-Sum of SD delay: 0
Max DS delay: 0
Min DS delay: 0
Number of DS delay: 0
Sum of DS delay: 0
Square-Sum of DS delay: 0

```

```
SD lost packets: 0 DS lost packets: 0
Lost packets for unknown reason: 0
```

## 3.6 配置文件

- Device B:

```
#
nqa server enable
nqa server udp-echo 10.2.2.2 9000
#
```
- Device A:

```
#
nqa entry admin test
type udp-jitter
destination ip 10.2.2.2
destination port 9000
frequency 1000
#
```

## 4 SNMP 测试配置举例

### 4.1 组网需求

如图 2 所示，Device A 为 NQA 客户端，现要求配置 SNMP 测试方案，使用户可以根据实际需要随时调用该测试方案测试从 Device A 发出 SNMP 协议查询报文到收到 SNMP agent（Device B）响应报文所用的时间。

图2 SNMP 测试配置组网图



### 4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 4.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 在进行 SNMP 类型测试前，必须在 Device B 上配置 SNMP 功能。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。

## 4.4 配置步骤

### (1) 配置 Device B (SNMP Agent)

# 启动 SNMP Agent 服务，设置 SNMP 版本为 all、只读团体名为 public、读写团体名为 private。

```
<DeviceB> system-view
[DeviceB] snmp-agent
[DeviceB] snmp-agent sys-info version all
[DeviceB] snmp-agent community read public
[DeviceB] snmp-agent community write private
```

### (2) 配置 Device A

# 创建 SNMP 查询类型的测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type snmp
```

# 配置测试操作的地址为 SNMP agent 的 IP 地址。

```
[DeviceA-nqa-admin-test-snmp] destination ip 10.2.2.2
```

# 开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-snmp] history-record enable
[DeviceA-nqa-admin-test-snmp] quit
```

## 4.5 验证配置

# 启动测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 SNMP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

# 以上配置完成后，显示 SNMP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
```

NQA entry (admin admin, tag test) test results:

```
Send operation times: 1 Receive response times: 1
Min/Max/Average round trip time: 1/1/1
Square-Sum of round trip time: 1
Last succeeded probe time: 2014-07-30 10:07:28.2
```

Extended results:

```
Packet loss ratio: 0%
Failures due to timeout: 0
Failures due to internal error: 0
Failures due to other errors: 0
```

# 显示 SNMP 测试的历史记录。

```
[DeviceA] display nqa history admin test
```

NQA entry (admin admin, tag test) history record(s):

| Index | Response | Status    | Time                  |
|-------|----------|-----------|-----------------------|
| 1     | 1        | Succeeded | 2014-07-30 10:07:28.2 |

## 4.6 配置文件

- Device B:

```
#
snmp-agent
snmp-agent local-engineid 800063A20300E0FC123456
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version all
#
```
- Device A:

```
#
nqa entry admin test
type snmp
destination ip 10.2.2.2
history-record enable
#
```

## 5 TCP 测试配置举例

### 5.1 组网需求

如图 3 所示，客户端(Device A)和服务器(Device B)指定端口(9000)之间建立 TCP 连接，现要求配置 TCP 测试方案，使用户可以根据实际需要测试建立 TCP 连接所需的时间，从而判断服务器指定端口上提供的服务是否可用，以及服务性能。

图3 TCP 测试配置组网图



### 5.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 5.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 在进行 TCP 类型测试前，必须配置 Device B 为 NQA 服务器。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。

## 5.4 配置步骤

### (1) 配置 Device B

# 使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，TCP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

### (2) 配置 Device A

# 创建 TCP 类型的测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type tcp
配置测试操作的目的地址和目的端口号
[DeviceA-nqa-admin-test-tcp] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-tcp] destination port 9000
开启 NQA 测试组的历史记录保存功能。
[DeviceA-nqa-admin-test-tcp] history-record enable
[DeviceA-nqa-admin-test-tcp] quit
```

## 5.5 验证配置

# 启动测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 TCP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

# 以上配置完成后，显示 TCP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 1/1/1
 Square-Sum of round trip time: 1
 Last succeeded probe time: 2014-07-30 10:37:29.5
Extended results:
 Packet loss ratio: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

# 显示 TCP 测试的历史记录。

```
[DeviceA] display nqa history admin test
```

```
NQA entry (admin admin, tag test) history record(s):
```

| Index | Response | Status        | Time                  |
|-------|----------|---------------|-----------------------|
| 2     | 1        | Succeeded     | 2014-07-30 10:37:29.5 |
| 1     | 0        | Unknown error | 2014-07-30 10:34:55.9 |

## 5.6 配置文件

- Device B:

```
#
nqa server enable
nqa server tcp-connect 10.2.2.2 9000
#
```
- Device A:

```
#
nqa entry admin test
type tcp
destination ip 10.2.2.2
destination port 9000
history-record enable
#
```

## 6 UDP-echo 测试配置举例

### 6.1 组网需求

如图 4 所示，客户端(Device A)和服务器(Device B)指定端口之间建立 UDP 连接，现要求配置 UDP-echo 测试方案，使用户可以根据实际需要随时调用该测试方案测试本端（Device A）和指定目的端（Device B）的端口 8000 之间的连通性以及 UDP 报文的往返时间。

图4 UDP-echo 测试配置组网图



### 6.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

### 6.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 在进行 UDP-echo 类型测试前，必须配置 DeviceB 为 NQA 服务器。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。

### 6.4 配置步骤

- (1) 配置 Device B



# 使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 8000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 8000
```

## (2) 配置 Device A

# 创建 UDP-echo 类型的测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-echo
配置测试操作的目的地址和目的端口号。
[DeviceA-nqa-admin-test-udp-echo] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-echo] destination port 8000
开启 NQA 测试组的历史记录保存功能。
[DeviceA-nqa-admin-test-udp-echo] history-record enable
[DeviceA-nqa-admin-test-udp-echo] quit
```

## 6.5 验证配置

# 启动测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 UDP-echo 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

# 以上配置完成后，显示 UDP-echo 测试中一次测试的结果。

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 1/1/1
 Square-Sum of round trip time: 1
 Last succeeded probe time: 2014-07-30 11:10:35.2
Extended results:
 Packet loss ratio: 0%
 Failures due to timeout: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

# 显示 UDP-echo 测试的历史记录。

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history record(s):
Index Response Status Time
1 1 Succeeded 2014-07-30 11:10:35.2
```

## 6.6 配置文件

- Device B:

```
#
nqa server enable
nqa server udp-echo 10.2.2.2 8000
```

- ```
#
• Device A:
#
nqa entry admin test
  type udp-echo
  destination ip 10.2.2.2
  destination port 8000
  history-record enable
#
```

7 Voice 测试配置举例

7.1 组网需求

如图 5 所示，Device A 和 Device B 之间的网络承载了语音业务，现要求配置 Voice 测试方案，使用户可以根据实际需要随时调用该测试方案测试本端（Device A）和指定的目的端（Device B）之间传送语音报文的时延抖动和网络语音质量参数。

图5 Voice 测试配置组网图



7.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

7.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 在进行 Voice 类型测试前，必须配置 Device B 为 NQA 服务器。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。

7.4 配置步骤

(1) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

(2) 配置 Device A

创建 Voice 类型的测试组。

```

<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type voice
# 配置测试操作的地址和目的端口号
[DeviceA-nqa-admin-test-voice] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-voice] destination port 9000
[DeviceA-nqa-admin-test-voice] quit

```

7.5 验证配置

启动测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 Voice 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

以上配置完成后，显示 Voice 测试中一次测试的结果。

```
[DeviceA] display nqa result admin test
```

NQA entry (admin admin, tag test) test results:

```

Send operation times: 157          Receive response times: 157
Min/Max/Average round trip time: 1/3/1
Square-Sum of round trip time: 165
Last packet received time: 2014-07-30 14:27:52.8

```

Extended results:

```

Packet loss ratio: 0%
Failures due to timeout: 0
Failures due to internal error: 0
Failures due to other errors: 0
Packets out of sequence: 0
Packets arrived late: 0

```

Voice results:

RTT number: 157

```

Min positive SD: 2          Min positive DS: 1
Max positive SD: 4          Max positive DS: 1
Positive SD number: 2       Positive DS number: 5
Positive SD sum: 6          Positive DS sum: 5
Positive SD average: 3      Positive DS average: 1
Positive SD square-sum: 20  Positive DS square-sum: 5
Min negative SD: 2          Min negative DS: 1
Max negative SD: 4          Max negative DS: 1
Negative SD number: 2       Negative DS number: 6
Negative SD sum: 6          Negative DS sum: 6
Negative SD average: 3      Negative DS average: 1
Negative SD square-sum: 20  Negative DS square-sum: 6

```

One way results:

```

Max SD delay: 0          Max DS delay: 0
Min SD delay: 0          Min DS delay: 0
Number of SD delay: 0    Number of DS delay: 0
Sum of SD delay: 0       Sum of DS delay: 0

```

```

    Square-Sum of SD delay: 0                Square-Sum of DS delay: 0
    SD lost packets: 0                      DS lost packets: 0
    Lost packets for unknown reason: 0
Voice scores:
    MOS value: 0.00                        ICPIF value: 0
# 显示 Voice 测试的统计结果。
[DeviceA] display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
NO. : 1
    Start time: 2014-07-30 14:30:30.0
    Life time: 204 seconds
    Send operation times: 4000             Receive response times: 4000
    Min/Max/Average round trip time: 1/32/1
    Square-Sum of round trip time: 12853
Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
Voice results:
RTT number: 4000
    Min positive SD: 1                    Min positive DS: 1
    Max positive SD: 32                   Max positive DS: 1
    Positive SD number: 76                Positive DS number: 72
    Positive SD sum: 567                  Positive DS sum: 72
    Positive SD average: 7                Positive DS average: 1
    Positive SD square-sum: 9011          Positive DS square-sum: 72
    Min negative SD: 1                    Min negative DS: 1
    Max negative SD: 20                   Max negative DS: 1
    Negative SD number: 87                Negative DS number: 67
    Negative SD sum: 569                  Negative DS sum: 67
    Negative SD average: 7                Negative DS average: 1
    Negative SD square-sum: 6715          Negative DS square-sum: 67
One way results:
    Max SD delay: 0                      Max DS delay: 0
    Min SD delay: 0                      Min DS delay: 0
    Number of SD delay: 0                Number of DS delay: 0
    Sum of SD delay: 0                    Sum of DS delay: 0
    Square-Sum of SD delay: 0            Square-Sum of DS delay: 0
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
Voice scores:
    Max MOS value: 4.40                  Min MOS value: 4.40
    Max ICPIF value: 0                   Min ICPIF value: 0

```

7.6 配置文件

- Device B:

```
#
nqa server enable
nqa server udp-echo 10.2.2.2 8000
#
```
- Device A:

```
#
nqa entry admin test
type voice
destination ip 10.2.2.2
destination port 9000
#
```

8 DLSw 测试配置举例

8.1 组网需求

如图6所示，Device B 为支持 DLSw 的设备，现要求配置 DLSw 测试方案，使用户可以根据实际需要随时调用该测试方案测试 DLSw 设备的响应时间。

图6 DLSw 测试配置组网图



8.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

8.3 配置注意事项

- 进行 NQA 测试之前，请确保各设备之间路由可达。
- 测试组开始测试后就不能再进入该测试组视图和测试类型视图进行配置修改，测试结束后才可以进入该测试组视图和测试类型视图。

8.4 配置步骤

```
# 创建 DLSw 类型的测试组。
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dlsw
# 配置测试操作的地址。
```

```
[DeviceA-nqa-admin-test-dlsw] destination ip 10.2.2.2
# 开启 NQA 测试组的历史记录保存功能。
[DeviceA-nqa-admin-test-dlsw] history-record enable
[DeviceA-nqa-admin-test-dlsw] quit
```

8.5 验证配置

```
# 启动测试操作。
[DeviceA] nqa schedule admin test start-time now lifetime forever
# 测试执行一段时间后，停止 DLSw 测试操作。
[DeviceA] undo nqa schedule admin test
# 以上配置完成后，显示 DLSw 测试中最后一次测试的结果。
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 1                Receive response times: 1
    Min/Max/Average round trip time: 19/19/19
    Square-Sum of round trip time: 361
    Last succeeded probe time: 2014-07-22 10:40:27.7
Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
# 显示 DLSw 测试的历史记录。
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history records:
    Index      Response      Status          Time
    ---      -
    1          19           Succeeded      2014-07-22 10:40:27.7
```

8.6 配置文件

```
#
nqa entry admin test
type dlsw
destination ip 10.2.2.2
history-record enable
#
```

9 相关资料

- 《H3C MSR 系列路由器 命令参考(V7)》中的“网络管理和监控命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“网络管理和监控配置指导”

H3C MSR 系列路由器

EAA 监控策略配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 路由震荡抑制配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	1
3.4 配置注意事项.....	2
3.5 配置步骤.....	2
3.5.1 Router A 配置.....	2
3.5.2 Router B 配置.....	2
3.6 验证配置.....	4
3.7 配置文件.....	5
4 配置文件回滚配置举例.....	6
4.1 组网需求.....	6
4.2 配置思路.....	6
4.3 使用版本.....	6
4.4 配置注意事项.....	6
4.5 配置步骤.....	7
4.6 验证配置.....	8
4.7 配置文件.....	9
5 设备运行状态自动监控和维护配置举例.....	10
5.1 组网需求.....	10
5.2 使用版本.....	10
5.3 配置注意事项.....	10
5.4 配置步骤.....	11
5.5 验证配置.....	11
5.6 配置文件.....	13
6 视频会议带宽自动保障配置举例.....	13
6.1 组网需求.....	13
6.2 使用版本.....	14
6.3 配置注意事项.....	14
6.4 配置步骤.....	14

6.5 验证配置	16
6.6 配置文件	16
7 基于链路质量的主备切换配置举例	17
7.1 组网需求	17
7.2 配置思路	17
7.3 使用版本	17
7.4 配置注意事项	17
7.5 配置步骤	18
7.5.1 Router A 配置	18
7.5.2 Router B 配置	21
7.5.3 Router C 配置	22
7.6 验证配置	22
7.7 配置文件	25
8 相关资料	27

1 简介

本文档介绍使用 EAA 监控策略进行网络监控的典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 EAA 监控策略的特性。

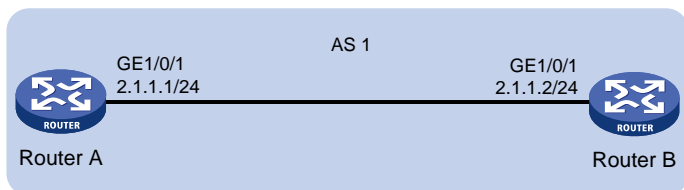
3 路由震荡抑制配置举例

3.1 组网需求

如[图 1](#)所示，Router A 和 Router B 运行 BGP 协议，为了防止 BGP 邻居反复 Up/Down 时，造成网络路由震荡，现需要在 Router B 上实现如下要求：

- 当在 10 分钟内 BGP 邻居 Up/Down 三次时，自动关闭 BGP 对等体。
- 配置每隔 60 分钟，自动配置启用一次 BGP 对等体邻居。

图1 路由震荡抑制配置组网图



3.2 配置思路

- 为了使当 Router A 和 Router B 的 BGP 邻居连续 Up/Down 三次时，自动关闭 BGP 对等体，可以配置 EAA 监控策略。
- 为了使 Router A 和 Router B 能够每隔 60 分钟，自动启用一次 BGP 对等体邻居，需要配置定时执行任务。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置注意事项

- 同一个 EAA 监控策略下，只能配置一个触发事件和运行时间。当多次执行 **event** 或者 **running-time** 命令时，则最近配置并且 **commit** 的生效。
- 如果新配置的动作的编号和已有动作的编号相同，则最近配置并且 **commit** 的生效。
- 给 CLI 监控策略配置事件、动作、用户角色和运行时间后，必须执行 **commit** 命令，该策略才会启用，该策略下的配置才会生效。

3.5 配置步骤

3.5.1 Router A 配置

(1) 配置接口地址

配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 2.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/1] quit
```

(2) 配置 BGP 路由

在 BGP 视图下，指定 BGP 路由器的 Router ID 为 2.1.1.1，创建 IBGP 对等体 2.1.1.2。

```
[RouterA] bgp 1
[RouterA-bgp] router-id 2.1.1.1
[RouterA-bgp] peer 2.1.1.2 as-number 1
```

创建并进入 BGP IPv4 单播地址族视图，将直连接口重分布到 BGP 路由中。

```
[RouterA-bgp] address-family ipv4 unicast
[RouterA-bgp-ipv4] import-route direct
```

使能与对等体 2.1.1.2 交换 IPv4 单播路由信息的能力。

```
[RouterA-bgp-ipv4] peer 2.1.1.2 enable
[RouterA-bgp-ipv4] quit
```

3.5.2 Router B 配置

(1) 配置接口地址

配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address 2.1.1.2 255.255.255.0
[RouterB-GigabitEthernet1/0/1] quit
```

(2) 配置 BGP 路由

在 BGP 视图下，指定 BGP 路由器的 Router ID 为 2.1.1.2，创建 IBGP 对等体 2.1.1.1。

```
[RouterB] bgp 1
[RouterB-bgp] router-id 2.1.1.2
[RouterB-bgp] peer 2.1.1.1 as-number 1
```

创建并进入 BGP IPv4 单播地址族视图，将直连接口重分布到 BGP 路由中。

```
[RouterB-bgp] address-family ipv4 unicast
[RouterB-bgp-ipv4] import-route direct
# 使能与对等体 2.1.1.1 交换 IPv4 单播路由信息的能力。
[RouterB-bgp-ipv4] peer 2.1.1.1 enable
[RouterB-bgp-ipv4] quit
```

(3) 配置 CLI 监控策略

创建 CLI 监控策略 1。

```
[RouterB] rtm cli-policy 1
```

为 CLI 监控策略 1 配置监控事件：当优先级高于或等于 5、内容中含有 2.1.1.1 state has changed from ESTABLISHED to IDLE 的日志在 10 分钟（600 秒）内出现过 3 次时，触发执行策略。

```
[RouterB-rtm-1] event syslog priority 5 msg "2.1.1.1 state has changed from ESTABLISHED to IDLE" occurs 3 period 600
```

为 CLI 监控策略 1 配置动作：当事件发生时，进入到系统模式。

```
[RouterB-rtm-1] action 0 cli system-view
```

为 CLI 监控策略 1 配置动作：当事件发生时，进入到 BGP 视图下。

```
[RouterB-rtm-1] action 1 cli bgp 1
```

为 CLI 监控策略 1 配置动作：当事件发生时，进入 BGP IPv4 单播地址族视图。

```
[RouterB-rtm-1] action 2 cli address-family ipv4 unicast
```

为 CLI 监控策略 1 配置动作：当事件发生时，在 BGP IPv4 单播地址族视图下，禁止本地路由器与对等体 2.1.1.1 交换 IPv4 单播路由信息的能力。

```
[RouterB-rtm-1] action 3 cli undo peer 2.1.1.1 enable
```

配置执行 CLI 监控策略 1 时使用的用户角色为 network-admin。

```
[RouterB-rtm-1] user-role network-admin
```

启用 CLI 监控策略 1。

```
[RouterB-rtm-1] commit
```

```
[RouterB-rtm-1] quit
```

(4) 配置定时执行任务

创建名称为 1 的工作任务并进入 Job 视图。

```
[RouterB] scheduler job 1
```

为 Job 分配命令，以进入系统视图。

```
[RouterB-job-1] command 0 system-view
```

为 Job 分配命令，以进入 BGP 视图。

```
[RouterB-job-1] command 1 bgp 1
```

为 Job 分配命令，进入 BGP IPv4 单播地址族视图。

```
[RouterB-job-1] command 2 address-family ipv4 unicast
```

为 Job 分配命令，在 BGP IPv4 单播地址族视图下，使能本地路由器与对等体 2.1.1.1 交换 IPv4 单播路由信息的能力。

```
[RouterB-job-1] command 3 peer 2.1.1.1 enable
```

```
[RouterB-job-1] quit
```

(5) 配置 Schedule

创建名为 1 的 Schedule，并进入 Schedule 视图。

```
[RouterB] scheduler schedule 1
```

```
# 为 Schedule 分配名为 1 的 job。
[RouterB-schedule-1] job 1
# 为 Schedule 配置循环执行的时间，每隔 60 分钟执行一次。
[RouterB-schedule-1] time repeating interval 60
[RouterB-schedule-1] quit
```

3.6 验证配置

通过 **display rtm policy registered** 命令查看，可以看到策略名为 1，策略类型为 CLI 的策略。

```
<RouterB> display rtm policy registered
Total number: 1
Type   Event           TimeRegistered      PolicyName
CLI    SYSLOG           Jun 18 09:41:06 2014 1
```

当在 10 分钟内，Router A 和 Router B 的 BGP 邻居三次 Up/Down 时，观察到 Router B 上会生成如下日志，表示策略运行成功。

```
%Jun 18 14:19:26:246 2014 Router RTM/6/RTM_POLICY: CLI policy 1 is running successfully.
```

在 RouterB 上进入 BGP 视图下，查看 BGP 路由配置，观察到在 BGP IPv4 单播地址族视图下，禁止与对等体 2.1.1.1 交换 IPv4 单播路由信息的能力。

```
[RouterB-bgp] display this
#
bgp 1
  router-id 2.1.1.2
  peer 2.1.1.1 as-number 1
  #
  address-family ipv4 unicast
    import-route direct
  #
Return
```

在 60 分钟后，在 Router B 上进入 BGP 视图下，查看 BGP 路由配置，观察到在 BGP IPv4 单播地址族视图下，使能与对等体 2.1.1.1 交换 IPv4 单播路由信息的能力。

```
[RouterB-bgp] display this
#
bgp 1
  router-id 2.1.1.2
  peer 2.1.1.1 as-number 1
  #
  address-family ipv4 unicast
    import-route direct
    peer 2.1.1.1 enable
  #
Return
```

```
[RouterB-bgp] quit
```

使用命令 **display bgp peer ipv4** 查看到 Router A 和 Router B 形成 BGP 对等体邻居。

```
[RouterB] display bgp peer ipv4
```

```

BGP local router ID: 2.1.1.2
Local AS number: 1
Total number of peers: 1                Peers in established state: 1

Peer                AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
2.1.1.1            1      23      23      0      1 00:16:04  Established

```

3.7 配置文件

- Router A:

```

#
interface GigabitEthernet1/0/1
 ip address 2.1.1.1 255.255.255.0
#
bgp 1
 router-id 2.1.1.1
 peer 2.1.1.2 as-number 1
#
 address-family ipv4 unicast
  import-route direct
  peer 2.1.1.2 enable
#

```

- Router B:

```

#
interface GigabitEthernet1/0/1
 ip address 2.1.1.2 255.255.255.0
#
bgp 1
 router-id 2.1.1.2
 peer 2.1.1.1 as-number 1
#
 address-family ipv4 unicast
  import-route direct
  peer 2.1.1.1 enable
#
rtm cli-policy 1
 event syslog priority 5 msg "2.1.1.1 state has changed from ESTABLISHED to IDLE" occurs
 3 period 600
 action 0 cli system-view
 action 1 cli bgp 1
 action 2 cli address-family ipv4 unicast
 action 3 cli undo peer 2.1.1.1 enable
 user-role network-admin
#
scheduler job 1
 command 0 system-view
 command 1 bgp 1

```

```

command 2 address-family ipv4 unicast
command 3 peer 2.1.1.1 enable
#
scheduler schedule 1
  job 1
    time repeating interval 60
#

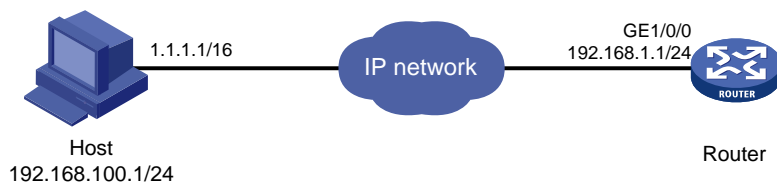
```

4 配置文件回滚配置举例

4.1 组网需求

如图2所示，管理员远程配置 Router，为避免某些配置导致路由不可达，可提前备份配置文件，使用 NQA 监控网络连通情况，当网络不通时，使用 EAA 策略触发自定义命令，自动恢复备份的可用配置并重启设备。

图2 配置文件回滚配置组网图



4.2 配置思路

通过使用 EAA 监控策略监控 NQA 告警项中的阈值状态，当监测的对象超出指定类型的阈值时，自动触发 EAA 监控策略。阈值状态（MIB 值）的具体说明如下：

- 当阈值状态为 `invalid`（MIB 值为 1），表示 NQA 测试组未启动；
- 当阈值状态为 `overThreshold`（MIB 值为 2），表示检查监测的对象超出指定类型的阈值；
- 当阈值状态为 `belowThreshold`（MIB 值为 3），表示检查监测的对象没有超出指定类型的阈值。

4.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.4 配置注意事项

- 同一个 EAA 监控策略下，只能配置一个触发事件和运行时间。当多次执行 `event` 或者 `running-time` 命令时，则最近配置并且 `commit` 的生效。
- 如果新配置的动作的编号和已有动作的编号相同，则最近配置并且 `commit` 的生效。
- 给 CLI 监控策略配置事件、动作、用户角色和运行时间后，必须执行 `commit` 命令，该策略才会启用，该策略下的配置才会生效。

4.5 配置步骤

(1) 配置接口地址并保存配置文件

配置接口 **GigabitEthernet1/0/0** 的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] port link-mode route
[Router-GigabitEthernet1/0/0] ip address 192.168.1.1 255.255.255.0
[Router-GigabitEthernet1/0/0] quit
```

配置到主机 **Host** 的静态路由。

```
[Router] ip route 192.168.100.0 255.255.255.0 192.168.1.1
```

先把当前正在使用的正常配置备份，文件名为 **eea_test_backup.cfg**。

```
[Router] save eea_test_backup.cfg
```

```
The current configuration will be saved to cfa0:/eea_test_backup.cfg. Continue? [Y/N] :y
```

```
Now saving current configuration to the device.
```

```
Saving configuration cfa0:/eea_test_backup.cfg.Please wait...
```

```
Configuration is saved to device successfully.
```

(2) 配置 NQA 测试组

创建 **ICMP-echo** 类型的 NQA 测试组，管理员名为 **admin**，测试操作标签为 **test**，并配置测试操作的目的地址为 **192.168.100.1**。

```
[Router] nqa entry admin test
[Router-nqa-admin-test] type icmp-echo
[Router-nqa-admin-test-icmp-echo] data-size 20
[Router-nqa-admin-test-icmp-echo] destination ip 192.168.100.1
```

配置测试组连续两次测试开始时间的间隔为 **1000** 毫秒，探测的超时时间为 **500** 毫秒。

```
[Router-nqa-admin-test-icmp-echo] frequency 1000
[Router-nqa-admin-test-icmp-echo] probe timeout 500
```

开启 NQA 测试组的历史记录保存功能，配置一个测试组中能够保存的最大历史记录数为 **10** 个。

```
[Router-nqa-admin-test-icmp-echo] history-record enable
[Router-nqa-admin-test-icmp-echo] history-record number 10
```

创建编号为 **1** 的阈值告警组，监测 **ICMP-echo** 探测的失败次数。NQA 测试组启动前，初始的阈值状态为 **invalid**。每次探测结束后，检查测试组启动以来连续的探测失败次数，若达到或超过 **5** 次，阈值状态置为 **over-threshold**；反之，置为 **below-threshold**。

```
[Router-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type none
```

```
[Router-nqa-admin-test-icmp-echo] quit
```

启动管理员为 **admin**，标签为 **test** 的测试组进行测试，测试组的启动时间为立即开始测试，持续时间为一直进行测试。

```
[Router] nqa schedule admin test start-time now lifetime forever
```

开启 **SNMP**。

```
[Router] snmp-agent
```

(3) 配置 CLI 监控策略

创建 CLI 监控策略 **1**。


```

[Router] rtm cli-policy 1
# 为 CLI 监控策略 1 配置监控事件：系统每 5 秒检查 MIB 对象
1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.1 的值，当该值等于 2 时触发执行监控策略并关闭
监控开关，当等于 3 时重新启动监控。

[Router-rtm-1] event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.1 monitor-obj
get start-op eq start-val 2 restart-op eq restart-val 3 interval 5
# 为 CLI 监控策略 1 配置动作：当事件发生时，配置下次启动配置文件为
eaa_test_backup.cfg。

[Router-rtm-1] action 0 cli startup saved-configuration eaa_test_backup.cfg
# 为 CLI 监控策略 1 配置动作：当事件发生时，重启设备。

[Router-rtm-1] action 1 reboot
# 启用 CLI 监控策略 1。

[Router-rtm-1] commit
[Router-rtm-1] quit

```

4.6 验证配置

通过 **display rtm policy registered** 命令查看，可以看到策略名为 1，策略类型为 CLI 的策略。

```

[Router] display rtm policy registered
Total number: 1
Type  Event          TimeRegistered      PolicyName
CLI   SNMP              Jul 10 15:31:37 2014 1

```

修改 Router 的 GigabitEthernet1/0/0 接口的 IP 地址，使得 Router 到主机的路由不可达。

```

[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Router-GigabitEthernet1/0/0] quit

```

观察到设备重新启动。

```
%Jul 10 15:33:40:112 2013 Router DEV/5/SYSTEM_REBOOT: System is rebooting now.
```

```

System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start heavy memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing...Done.

```

```

*****
*
*           H3C MSR36-40 BootWare, Version 1.42           *
*
*****
Copyright (c) 2004-2014 Hangzhou H3C Technologies Co., Ltd.

```

```

Compiled Date       : Apr  1 2014
CPU ID              : 0x3
Memory Type        : DDR3 SDRAM

```

```
Memory Size      : 2048MB
BootWare Size    : 1024KB
Flash Size       : 8MB
cfa0 Size        : 497MB
CPLD Version     : 2.0
PCB Version      : 2.0
```

BootWare Validating...

Press Ctrl+B to access EXTENDED-BOOTWARE MENU...

Loading the main image files...

Loading file

```
cfa0:/msr36-cmw710-system-r0106.bin.....
.....Done.
```

```
Loading file cfa0:/msr36-cmw710-security-r0106.bin...Done.
```

```
Loading file cfa0:/msr36-cmw710-voice-r0106.bin.....Done.
```

```
Loading file cfa0:/msr36-cmw710-data-r0106.bin.....Done.
```

```
Loading file cfa0:/msr36-cmw710-boot-r0106.bin.....Done.
```

```
Image file cfa0:/msr36-cmw710-boot-r0106.bin is self-decompressing.....Done.
```

System image is starting...

Line con1 is available.

Press ENTER to get started.

```
<Router>%Jul 10 16:15:08:059 2014 Router SHELL/5/SHELL_LOGIN: Console logged in from con1.
```

```
<Router>
```

4.7 配置文件

```
#
nqa entry admin test
  type icmp-echo
  data-size 20
  destination ip 192.168.100.1
  frequency 1000
  history-record enable
  history-record number 10
  probe timeout 500
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type none
#
nqa schedule admin test start-time now lifetime forever
#
interface GigabitEthernet1/0/0
  port link-mode route
  ip address 192.168.1.1 255.255.255.0
#
ip route 192.168.100.0 255.255.255.0 192.168.1.1
```

```

#
snmp-agent
snmp-agent local-engineid 800063A280000605B36B9E00000001
snmp-agent sys-info version v3
#
rtm cli-policy 1
event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.1 monitor-obj get start-op eq
start-val 2 restart-op eq restart-val 3 interval 5
action 0 cli startup saved-configuration eaa_test_backup.cfg
action 1 reboot
user-role network-admin
#

```

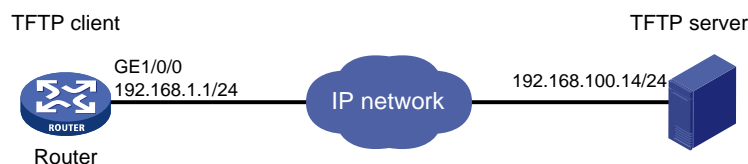
5 设备运行状态自动监控和维护配置举例

5.1 组网需求

如图 3 所示，Router 到 TFTP 服务器路由可达，为防止 Router 的 CPU 利用率过高，现要求使用 EAA 策略进行自动监控，当设备 CPU 使用率高于 80% 时，进行如下操作：

- 显示当前时间的内存信息、接口统计信息和路由表信息并保存到指定文件。
- 将指定文件上传到指定的 TFTP 服务器上。
- 上传到 TFTP 服务器后，Router 删除本地的指定文件。

图3 设备运行状态自动监控和维护配置组网图



5.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

5.3 配置注意事项

- 同一个 EAA 监控策略下，只能配置一个触发事件和运行时间。当多次执行 **event** 或者 **running-time** 命令时，则最近配置并且 **commit** 的生效。
- 如果新配置的动作的编号和已有动作的编号相同，则最近配置并且 **commit** 的生效。
- 给 CLI 监控策略配置事件、动作、用户角色和运行时间后，必须执行 **commit** 命令，该策略才会启用，该策略下的配置才会生效。

5.4 配置步骤

配置接口 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] port link-mode route
[Router-GigabitEthernet1/0/0] ip address 192.168.1.1 255.255.255.0
[Router-GigabitEthernet1/0/0] quit
```

开启 SNMP。

```
[Router] snmp-agent
```

创建 CLI 监控策略 1。

```
[Router] rtm cli-policy 1
```

为 CLI 监控策略 1 配置监控事件：系统每 5 秒检查 CPU 使用率（MIB 对象 1.3.6.1.4.1.25506.2.6.1.1.1.6.16），当该值大于 80 时触发执行监控策略并关闭监控开关，当小于 40 时重新启动监控。

```
[Router-rtm-1] event snmp oid 1.3.6.1.4.1.25506.2.6.1.1.1.6.16 monitor-obj get start-op
gt start-val 80 restart-op lt restart-val 40 interval 5
```

为 CLI 监控策略 1 配置动作：当事件发生时，显示设备当前的日期时间，并将显示信息保存到指定文件 test1.txt。

```
[Router-rtm-1] action 0 cli display clock >> test1.txt
```

为 CLI 监控策略 1 配置动作：当事件发生时，显示内存使用情况，并将显示信息以追加方式保存到指定文件 test1.txt。

```
[Router-rtm-1] action 1 cli display memory >> test1.txt
```

为 CLI 监控策略 1 配置动作：当事件发生时，显示指定接口当前的运行状态，并将显示信息以追加方式保存到指定文件 test1.txt。

```
[Router-rtm-1] action 2 cli display interface >> test1.txt
```

为 CLI 监控策略 1 配置动作：当事件发生时，显示路由表的信息，并将显示信息以追加方式保存到指定文件 test1.txt。

```
[Router-rtm-1] action 3 cli display ip routing-table >> test1.txt
```

为 CLI 监控策略 1 配置动作：当事件发生时，将本地的指定文件 test1.txt 上传到 TFTP 服务器 192.168.100.14 上。

```
[Router-rtm-1] action 4 cli tftp 192.168.100.14 put test1.txt
```

为 CLI 监控策略 1 配置动作：当事件发生时，永久删除文件 test1.txt，并确认。

```
[Router-rtm-1] action 5 cli delete /unreserved test1.txt
```

```
[Router-rtm-1] action 6 cli y
```

```
[Router-rtm-1] user-role network-admin
```

启用 CLI 监控策略 1。

```
[Router-rtm-1] commit
```

```
[Router-rtm-1] quit
```

5.5 验证配置

通过 `display rtm policy registered` 命令查看，可以看到策略名为 1，策略类型为 CLI 的策略。

```
[Router] display rtm policy registered
```

```
Total number: 1
```

```
Type Event TimeRegistered PolicyName
CLI SNMP Jul 10 15:31:37 2014 1
```

当设备 CPU 占用率超过 80%，可以观察到设备 CLI 监控策略运行成功。

```
%Jul 14 10:57:22:127 2014 Router RTM/6/RTM_POLICY: CLI policy 1 is running successfully.
```

查看日志服务器，有 test1.txt 文件生成，打开文件查看到显示系统当前的时间、日期、本地时区配置，内存使用情况，接口当前的运行状态和路由表的信息。

```
11:14:55 UTC Mon 07/14/2014
```

```
The statistics about memory is measured in KB:
```

```
Slot 0:
```

	Total	Used	Free	Shared	Buffers	Cached	FreeRatio
Mem:	2028984	540492	1488492	0	564	156532	73.4%
-/+ Buffers/Cache:		383396	1645588				
Swap:	0	0	0				

```
Slot 1:
```

	Total	Used	Free	Shared	Buffers	Cached	FreeRatio
Mem:	2028984	468996	1559988	0	312	126668	76.9%
-/+ Buffers/Cache:		342016	1686968				
Swap:	0	0	0				

```
Slot 2:
```

	Total	Used	Free	Shared	Buffers	Cached	FreeRatio
Mem:	4081140	1162996	2918144	0	0	42416	71.5%
-/+ Buffers/Cache:		1120580	2960560				
Swap:	0	0	0				

```
Aux0/0/1
```

```
Current state: Administratively DOWN
```

```
Description: Aux0/0/1 Interface
```

```
Bandwidth: 9kbps
```

```
Internet protocol processing: disabled
```

```
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
```

```
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
```

```
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
```

```
Last clearing of counters: Never
```

```
Physical layer: asynchronous, Baudrate: 9600 bps
```

```
Phy-mru: 1700
```

```
.....
```

```
Destinations : 16 Routes : 16
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	Direct	0	0	10.1.1.1	GE1/0/2
10.1.1.0/32	Direct	0	0	10.1.1.1	GE1/0/2

10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.1	GE1/0/2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.100.0/24	Direct	0	0	192.168.100.68	GE1/0/1
192.168.100.0/32	Direct	0	0	192.168.100.68	GE1/0/1
192.168.100.68/32	Direct	0	0	127.0.0.1	InLoop0
192.168.100.255/32	Direct	0	0	192.168.100.68	GE1/0/1
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

5.6 配置文件

```
#
interface GigabitEthernet1/0/0
  port link-mode route
  ip address 192.168.1.1 255.255.255.0
#
snmp-agent
#
rtm cli-policy 1
  event snmp oid 1.3.6.1.4.1.25506.2.6.1.1.1.1.6.16 monitor-obj get start-op gt start-val 80
  restart-op lt restart-val 40 interval 5
  action 0 cli display clock >> test1.txt
  action 1 cli display memory >> test1.txt
  action 2 cli display interface >> test1.txt
  action 3 cli display ip routing-table >> test1.txt
  action 4 cli tftp 192.168.100.14 put test1.txt
  action 5 cli delete /unreserved test1.txt
  action 6 cli y
user-role network-admin
#
```

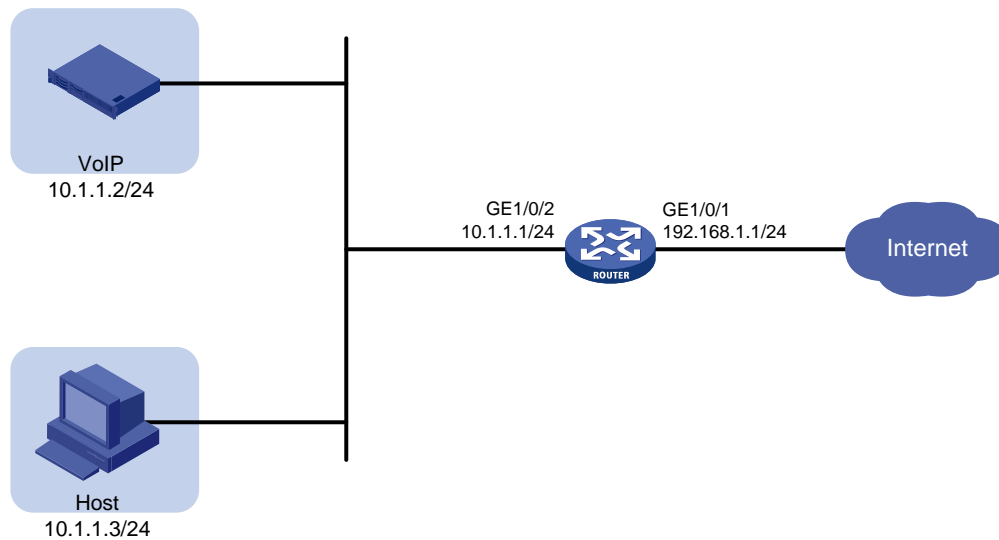
6 视频会议带宽自动保障配置举例

6.1 组网需求

如图 4 所示，用户主机和 VoIP 视频系统通过路由器 Router 访问 Internet，当召开视频会议时，要占用较多带宽，需要对主机的上网流量进行限制。现要求使用 EAA 监控策略进行自动监控，具体要求如下：

- 当每秒视频报文流量大于等于 100000 个数据包时，则限制主机报文通过，仅允许视频报文通过。当每秒视频报文流量小于 100000 个数据包时，则允许视频和主机报文通过。

图4 视频会议带宽自动保障配置组网图



6.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

6.3 配置注意事项

- 同一个 EAA 监控策略下，只能配置一个触发事件和运行时间。当多次执行 **event** 或者 **running-time** 命令时，则最近配置并且 **commit** 的生效。
- 如果新配置的动作的编号和已有动作的编号相同，则最近配置并且 **commit** 的生效。
- 给 CLI 监控策略配置事件、动作、用户角色和运行时间后，必须执行 **commit** 命令，该策略才会启用，该策略下的配置才会生效。

6.4 配置步骤

(1) 配置接口地址

配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.1.1.1 255.255.255.0
[Router-GigabitEthernet1/0/2] quit
```

(2) 配置 ACL 策略

创建 ACL 3001，仅允许源地址为 10.1.1.2 的报文通过。

```
[Router] acl number 3001
```

```
[Router-acl-adv-3001] rule 0 permit ip source 10.1.1.2 0
[Router-acl-adv-3001] quit
```

创建 ACL 3002，不允许源地址为 10.1.1.2 的报文通过，允许其他报文通过。

```
[Router] acl number 3002
[Router-acl-adv-3002] rule 0 deny ip source 10.1.1.2 0
[Router-acl-adv-3002] rule 5 permit ip
[Router-acl-adv-3002] quit
```

在接口 GigabitEthernet1/0/2 的出方向上匹配 ACL 3001 的数据包进行流量监管。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] qos car inbound acl 3001 cir 1000
[Router-GigabitEthernet1/0/2] quit
```

(3) 开启 SNMP 功能并配置环境变量

开启 SNMP Agent 功能。

```
[Router] snmp-agent
# 创建监控策略的环境变量，设置环境变量 video，其值为 0。
[Router] rtm environment video 0
```

(4) 配置 CLI 监控策略 1

创建 CLI 监控策略 1。

```
[Router] rtm cli-policy 1
```

为 CLI 监控策略 1 配置监控事件：系统每 10 秒检查报文个数（MIB 对象 1.3.6.1.4.1.25506.2.8.2.2.3.1.31.1.3001.0），监控值大于等于 0 时执行 action 配置的动作（即每次都会执行）。

```
[Router-rtm-1] event snmp oid 1.3.6.1.4.1.25506.2.8.2.2.3.1.31.1.3001.0 monitor-obj
get start-op ge start-val 0 restart-op ge restart-val 0 interval 10
```

为 CLI 监控策略 1 配置动作：当事件发生时，清除 ACL 3001 的统计信息。

```
[Router-rtm-1] action 0 cli reset acl counter 3001
```

为 CLI 监控策略 1 配置动作：当事件发生时，从用户视图进入 Tcl 配置视图。

```
[Router-rtm-1] action 1 cli tclsh
```

为 CLI 监控策略 1 配置动作：当事件发生时，从用户视图进入系统视图。

```
[Router-rtm-1] action 2 cli system-view
```

为 CLI 监控策略 1 配置动作：当事件发生时，检查收到的视频设备报文数量，如果超过 100000 个数据包，则在接口 GigabitEthernet1/0/2 配置仅允许视频流量 10.1.1.2 的报文通过，限制其他流量流量承诺信息速率为 1024 kbps。

```
[Router-rtm-1] action 3 cli if { $_oid_value > 100000 && $video == 0 } { rtm environment
video 1; interface gigabitethernet 1/0/2; qos car inbound acl 3002 cir 1024}
```

为 CLI 监控策略 1 配置动作：当事件发生时，检查收到的视频设备报文数量，如果不到 100000 个数据包，则接口 GigabitEthernet1/0/2 配置允许其他流量的报文通过。

```
[Router-rtm-1] action 4 cli if { $_oid_value < 100000 && $video == 1 } { rtm environment
video 0; interface gigabitethernet 1/0/2; undo qos car inbound acl 3002}
```

启用 CLI 监控策略 1。

```
[Router-rtm-1] commit
[Router-rtm-1] quit
```


6.5 验证配置

通过 **display rtm policy registered** 命令查看，可以看到策略名为 1，策略类型为 CLI 的策略。

```
[Router] display rtm policy registered
Total number: 1
Type   Event           TimeRegistered      PolicyName
CLI    SNMP              Jul 11 16:07:51 2014 1
```

当 Router 接口 GigabitEthernet1/0/2 每秒视频报文流量大于等于 100000 个数据包时，查看到日志信息显示 EAA 策略 1 执行成功。

```
%Jul 11 16:13:46:552 2014 Router RTM/6/RTM_POLICY: CLI policy 1 is running successfully.
```

6.6 配置文件

```
#
acl number 3001
  rule 0 permit ip source 10.1.1.2 0
#
acl number 3002
  rule 0 deny ip source 10.1.1.2 0
  rule 5 permit ip
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
  port link-mode route
  ip address 10.1.1.1 255.255.255.0
  qos car inbound acl 3001 cir 1000
#
snmp-agent
#
rtm cli-policy 1
  event snmp oid 1.3.6.1.4.1.25506.2.8.2.2.3.1.31.1.3001.0 monitor-obj get start-op ge
start-val 0 restart-op ge restart-val 0 interval 10
  action 0 cli reset acl counter 3001
  action 1 cli tclsh
  action 2 cli system-view
  action 3 cli if { $_oid_value > 100000 && $video == 0 } { rtm environment video 1; interface
GigabitEthernet1/0/2; qos car inbound acl 3002 cir 1024}
  action 4 cli if { $_oid_value < 100000 && $video == 1 } { rtm environment video 0; interface
GigabitEthernet1/0/2; undo qos car inbound acl 3002}
  user-role network-admin
  commit
#
rtm environment video 0
#
```

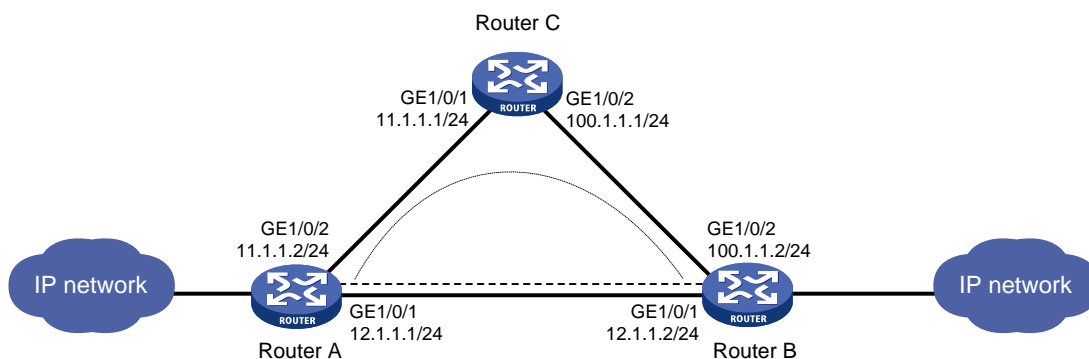
7 基于链路质量的主备切换配置举例

7.1 组网需求

如图5所示，Router A 和 Router B 路由可达，正常情况下，Router A 到 Router B 的直连链路作为主链路，经 Router C 的链路为备份链路。在 Router A 上配置 EAA 监控策略，具体要求如下：

- 当主链路丢包率超过 20%，或者延时大于 200ms 时，流量切换到备份链路。
- 当主链路没有丢包，并且延时小于 100ms，流量再恢复到主链路进行转发。

图5 基于链路质量的主备切换配置组网图



7.2 配置思路

通过使用 EAA 监控策略监控 NQA 告警项中的阈值状态，当监测的对象超出指定类型的阈值时，自动触发 EAA 监控策略。阈值状态（MIB 值）的具体说明如下：

- 当阈值状态为 `invalid`（MIB 值为 1），表示 NQA 测试组未启动；
- 当阈值状态为 `overThreshold`（MIB 值为 2），表示检查监测的对象超出指定类型的阈值；
- 当阈值状态为 `belowThreshold`（MIB 值为 3），表示检查监测的对象没有超出指定类型的阈值。

7.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

7.4 配置注意事项

- 同一个 EAA 监控策略下，只能配置一个触发事件和运行时间。当多次执行 `event` 或者 `running-time` 命令时，则最近配置并且 `commit` 的生效。
- 如果新配置的动作的编号和已有动作的编号相同，则最近配置并且 `commit` 的生效。
- 给 CLI 监控策略配置事件、动作、用户角色和运行时间后，必须执行 `commit` 命令，该策略才会启用，该策略下的配置才会生效。

7.5 配置步骤

7.5.1 Router A 配置

(1) 配置接口地址

配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] port link-mode route
[RouterA-GigabitEthernet1/0/1] ip address 12.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] port link-mode route
[RouterA-GigabitEthernet1/0/2] ip address 11.1.1.2 255.255.255.0
[RouterA-GigabitEthernet1/0/2] quit
```

(2) 配置 NQA 测试组

创建 ICMP-echo 类型的 NQA 测试组，管理员名为 1，测试操作标签为 1，并配置测试操作的目的地址为 12.1.1.2。

```
[RouterA] nqa entry 1 1
[RouterA-nqa-1-1] type icmp-echo
[RouterA-nqa-1-1-icmp-echo] destination ip 12.1.1.2
```

配置测试组连续两次测试开始时间的的时间间隔为 15000 毫秒，探测的超时时间为 800 毫秒，一次 ICMP-echo 测试中探测的次数为 15 次。

```
[RouterA-nqa-1-1-icmp-echo] frequency 15000
[RouterA-nqa-1-1-icmp-echo] probe timeout 800
[RouterA-nqa-1-1-icmp-echo] probe count 15
```

创建编号为 1 的阈值告警组，监测 ICMP-echo 探测的持续时间，阈值上限为 200 毫秒，下限为 0 毫秒。NQA 测试组启动前，初始的阈值状态为 invalid。每次测试结束后，检查本次测试的平均探测持续时间，若超出阈值，阈值状态置为 over-threshold；反之，置为 below-threshold。

```
[RouterA-nqa-1-1-icmp-echo] reaction 1 checked-element probe-duration threshold-type
average threshold-value 200 0 action-type none
```

创建编号为 2 的阈值告警组，监测 ICMP-echo 探测的失败次数。NQA 测试组启动前，初始的阈值状态为 invalid。NQA 测试组启动前，初始的阈值状态为 invalid。每次测试结束后，检查本次测试中累计的持续时间超出阈值的探测次数，若达到或超过 3 次，阈值状态置为 over-threshold；反之，置为 below-threshold。

```
[RouterA-nqa-1-1-icmp-echo] reaction 2 checked-element probe-fail threshold-type
accumulate 3 action-type none
```

创建编号为 3 的阈值告警组，监测 ICMP-echo 探测的持续时间，阈值上限为 100 毫秒，下限为 0 毫秒。NQA 测试组启动前，初始的阈值状态为 invalid。每次测试结束后，检查本次测试的平均探测持续时间，若超出阈值，阈值状态置为 over-threshold；反之，置为 below-threshold。

```
[RouterA-nqa-1-1-icmp-echo] reaction 3 checked-element probe-duration threshold-type
average threshold-value 100 0 action-type none
```

创建编号为 4 的阈值告警组，监测 ICMP-echo 探测的失败次数。NQA 测试组启动前，初始的阈值状态为 invalid。NQA 测试组启动前，初始的阈值状态为 invalid。每次测试结束后，检查本次测试中累计的持续时间超出阈值的探测次数，若达到或超过 1 次，阈值状态置为 over-threshold；反之，置为 below-threshold。

```
[RouterA-nqa-1-1-icmp-echo] reaction 4 checked-element probe-fail threshold-type  
accumulate 1 action-type none
```

```
[RouterA-nqa-1-1-icmp-echo] quit
```

开启 NQA 客户端功能。

```
[RouterA] nqa agent enable
```

启动管理员为 1，标签为 1 的测试组进行测试，测试组的启动时间为立即开始测试，持续时间为一直进行测试。

```
[RouterA] nqa schedule 1 1 start-time now lifetime forever
```

开启 SNMP Agent 功能。

```
[RouterA] snmp-agent
```

(3) 配置监控策略的环境变量

创建监控策略的环境变量，设置环境变量 delay，其值为 0。

```
[RouterA] rtm environment delay 0
```

创建监控策略的环境变量，设置环境变量 loss，其值为 0。

```
[RouterA] rtm environment loss 0
```

创建监控策略的环境变量，设置环境变量 backup，其值为 0。

```
[RouterA] rtm environment backup 0
```

(4) 配置 CLI 监控策略 1

创建 CLI 监控策略 1。

```
[RouterA] rtm cli-policy 1
```

为 CLI 监控策略 1 配置监控事件：系统每 10 秒检查 MIB 对象

1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.1 的值，当该值等于 2 时触发执行监控策略并关闭监控开关，当等于 3 时重新启动监控。

```
[RouterA-rtm-1] event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.1  
monitor-obj get start-op eq start-val 2 restart-op eq restart-val 3 interval 10
```

为 CLI 监控策略 1 配置动作：当事件发生时，配置从用户视图进入 Tcl 配置视图。

```
[RouterA-rtm-1] action 0 cli tclsh
```

为 CLI 监控策略 1 配置动作：当事件发生时，进入系统视图。

```
[RouterA-rtm-1] action 1 cli system-view
```

为 CLI 监控策略 1 配置动作：当事件发生时，将环境变量 delay 的值由 0 变为 1。

```
[RouterA-rtm-1] action 2 cli if { $delay==0 } { rtm environment delay 1 }
```

为 CLI 监控策略 1 配置动作：当事件发生时，将环境变量 backup 的值由 0 变为 1，并配置到 100.1.1.0/24、指定下一跳为 11.1.1.1、优先级为 10 的静态路由。

```
[RouterA-rtm-1] action 3 cli if { $backup==0 } { rtm environment backup 1; ip route-static  
100.1.1.0 24 11.1.1.1 preference 10 }
```

启用 CLI 监控策略 1。

```
[RouterA-rtm-1] commit
```

```
[RouterA-rtm-1] quit
```

(5) 配置 CLI 监控策略 2

创建 CLI 监控策略 2。

```
[RouterA] rtm cli-policy 2
```

为 CLI 监控策略 2 配置监控事件：系统每 10 秒检查 MIB 对象

1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.2 的值，当该值等于 2 时触发执行监控策略并关闭监控开关，当等于 3 时重新启动监控。

```
[RouterA-rtm-2] event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.2
monitor-obj get start-op eq start-val 2 restart-op eq restart-val 3 interval 10
```

为 CLI 监控策略 2 配置动作：当事件发生时，配置从用户视图进入 Tcl 配置视图。

```
[RouterA-rtm-2] action 0 cli tclsh
```

为 CLI 监控策略 2 配置动作：当事件发生时，进入系统视图。

```
[RouterA-rtm-2] action 1 cli system-view
```

为 CLI 监控策略 2 配置动作：当事件发生时，将环境变量 loss 的值由 0 变为 1。

```
[RouterA-rtm-2] action 2 cli if { $loss==0 } { rtm environment loss 1 }
```

为 CLI 监控策略 2 配置动作：当事件发生时，将环境变量 backup 的值由 0 变为 1，并配置到 100.1.1.0/24、指定下一跳为 11.1.1.1、优先级为 10 的静态路由。

```
[RouterA-rtm-2] action 3 cli if { $backup==0 } { rtm environment backup 1; ip route-static
100.1.1.0 24 11.1.1.1 preference 10 }
```

启用 CLI 监控策略 2。

```
[RouterA-rtm-2] user-role network-admin
```

```
[RouterA-rtm-2] commit
```

(6) 配置 CLI 监控策略 3

创建 CLI 监控策略 3。

```
[RouterA] rtm cli-policy 3
```

为 CLI 监控策略 3 配置监控事件：系统每 10 秒检查 MIB 对象

1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.3 的值，当该值等于 2 时触发执行监控策略并关闭监控开关，当等于 3 时重新启动监控。

```
[RouterA-rtm-3] event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.3
monitor-obj get start-op eq start-val 3 restart-op eq restart-val 2 interval 10
```

为 CLI 监控策略 3 配置动作：当事件发生时，配置从用户视图进入 Tcl 配置视图。

```
[RouterA-rtm-3] action 0 cli tclsh
```

为 CLI 监控策略 3 配置动作：当事件发生时，进入系统视图。

```
[RouterA-rtm-3] action 1 cli system-view
```

为 CLI 监控策略 3 配置动作：当事件发生时，将环境变量 delay 的值由 1 变为 0。

```
[RouterA-rtm-3] action 2 cli if { $delay==1 } { rtm environment delay 0 }
```

为 CLI 监控策略 3 配置动作：当事件发生时，在 5000 毫秒后发生变化。

```
[RouterA-rtm-3] action 3 cli after 5000
```

为 CLI 监控策略 3 配置动作：当事件发生时，将环境变量 backup 和 loss 的值变为 0，并删除配置到 100.1.1.0/24、指定下一跳为 11.1.1.1、优先级为 10 的静态路由。

```
[RouterA-rtm-3] action 4 cli if { $backup==1 && $loss==0 } { undo ip route-static
100.1.1.0 24 11.1.1.1 preference 10; rtm environment backup 0 }
```

启用 CLI 监控策略 3。

```
[RouterA-rtm-3] user-role network-admin
```

```
[RouterA-rtm-3] commit
```

(7) 配置 CLI 监控策略 4

创建 CLI 监控策略 4。

```
[RouterA] rtm cli-policy 4
```

为 CLI 监控策略 4 配置监控事件：系统每 10 秒检查 MIB 对象

1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.4 的值，当该值等于 2 时触发执行监控策略并关闭监控开关，当等于 3 时重新启动监控。

```
[RouterA-rtm-4] event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.4
monitor-obj get start-op eq start-val 3 restart-op eq restart-val 2 interval 10
```

为 CLI 监控策略 4 配置动作：当事件发生时，配置从用户视图进入 Tcl 配置视图。

```
[RouterA-rtm-4] action 0 cli tclsh
```

为 CLI 监控策略 4 配置动作：当事件发生时，进入系统视图。

```
[RouterA-rtm-4] action 1 cli system-view
```

为 CLI 监控策略 4 配置动作：当事件发生时，将环境变量 loss 的值由 1 变为 0。

```
[RouterA-rtm-4] action 2 cli if { $loss==1 } { rtm environment loss 0 }
```

为 CLI 监控策略 4 配置动作：当事件发生时，在 5000 毫秒后发生变化。

```
[RouterA-rtm-4] action 3 cli after 5000
```

为 CLI 监控策略 4 配置动作：当事件发生时，将环境变量 backup 和 delay 的值保持为 0，并删除配置到 100.1.1.0/24、指定下一跳为 11.1.1.1、优先级为 10 的静态路由。

```
[RouterA-rtm-4] action 4 cli if { $backup==1 && $delay==0 } { undo ip route-static
100.1.1.0 24 11.1.1.1 preference 10; rtm environment backup 0 }
```

启用 CLI 监控策略 4。

```
[RouterA-rtm-4] user-role network-admin
```

```
[RouterA-rtm-4] commit
```

```
[RouterA-rtm-4] quit
```

7.5.2 Router B 配置

(1) 配置接口地址

配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterB> system-view
```

```
[RouterB] interface gigabitethernet 1/0/1
```

```
[RouterB-GigabitEthernet1/0/1] port link-mode route
```

```
[RouterB-GigabitEthernet1/0/1] ip address 12.1.1.2 255.255.255.0
```

```
[RouterB-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[RouterB] interface gigabitethernet 1/0/2
```

```
[RouterB-GigabitEthernet1/0/2] port link-mode route
```

```
[RouterB-GigabitEthernet1/0/2] ip address 100.1.1.2 255.255.255.0
```

```
[RouterB-GigabitEthernet1/0/2] quit
```

(2) 配置 OSPF 路由，使得 Router C 到 Router B 网络互通

```
[RouterB] ospf 1
```

```
[RouterB-ospf-1] area 0.0.0.0
```

```
[RouterB-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
```

```
[RouterB-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
```

```
[RouterB-ospf-1-area-0.0.0.0] quit
```

```
[RouterB-ospf-1] quit
```

7.5.3 Router C 配置

(1) 配置接口地址

配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] port link-mode route
[RouterC-GigabitEthernet1/0/1] ip address 11.1.1.1 255.255.255.0
[RouterC-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] port link-mode route
[RouterC-GigabitEthernet1/0/2] ip address 100.1.1.1 255.255.255.0
[RouterC-GigabitEthernet1/0/2] quit
```

(2) 配置 OSPF 路由，使得 Router B 到 Router C 网络互通

```
[RouterC] ospf 1
[RouterC-ospf-1] area 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

7.6 验证配置

显示所有监控策略的详细信息。

```
<RouterA> display rtm policy registered verbose
Total number: 4

Policy Name: 1
Policy Type: CLI
Event Type: SNMP
TimeRegistered: Jul 14 15:04:24 2014
User-role: network-admin

Policy Name: 2
Policy Type: CLI
Event Type: SNMP
TimeRegistered: Jul 14 15:14:50 2014
User-role: network-admin

Policy Name: 3
Policy Type: CLI
Event Type: SNMP
TimeRegistered: Jul 14 15:17:32 2014
User-role: network-admin

Policy Name: 4
```

```
Policy Type: CLI
Event Type: SNMP
TimeRegistered: Jul 14 15:18:33 2014
User-role: network-admin
```

- (1) 当 Router A 到 Router B 的报文延时为 300 毫秒时，超过阈值 200 毫秒，观察 Router A 显示信息。

查看到日志信息显示 EAA 策略 1 执行成功。

```
%Jul 14 14:50:16:677 2014 RouterA RTM/6/RTM_POLICY: CLI policy 1 is running successfully.
```

使用 **display rtm environment** 命令用来显示用户自定义的 EAA 环境变量配置，观察到环境变量 **backup** 的值变为 1，**delay** 的值变为 1。

```
[RouterA] display rtm environment
```

Name	Value
backup	1
delay	1
loss	0

使用 **display this** 命令显示当前视图下生效的配置，观察到有到 100.1.1.0/24 的静态路由，Router A 到 Router B 的报文切换路由到备份链路。

```
[RouterA] display this
```

```
#
 sysname RouterA
#
 nqa schedule 1 1 start-time now lifetime forever
#
 ip route-static 100.1.1.0 24 11.1.1.1 preference 10
#
 snmp-agent
 snmp-agent local-engineid 800063A280000605B36B9E00000001
 snmp-agent sys-info version v3
#
 rtm environment backup 1
 rtm environment delay 1
 rtm environment loss 0
#
```

Return

- (2) 当 Router A 到 Router B 的报文丢包率为 25%时，超过阈值，观察 Router A 显示信息。

查看到日志信息显示 EAA 策略 2 执行成功。

```
%Jul 14 15:15:23:802 2014 RouterA RTM/6/RTM_POLICY: CLI policy 2 is running successfully.
```

使用 **display rtm environment** 命令用来显示用户自定义的 EAA 环境变量配置，观察到环境变量 **loss** 的值变为 1。

```
[RouterA] display rtm environment
```

Name	Value
backup	1
delay	1
loss	1

使用 **display this** 命令显示当前视图下生效的配置，观察到 Router A 的报文切仍然经备份链路到 Router B。

```
[RouterA] display this
#
  sysname RouterA
#
  nqa schedule 1 1 start-time now lifetime forever
#
  ip route-static 100.1.1.0 24 11.1.1.1 preference 10
#
  snmp-agent
  snmp-agent local-engineid 800063A280000605B36B9E00000001
  snmp-agent sys-info version v3
#
  rtm environment backup 1
  rtm environment delay 1
  rtm environment loss 1
#
Return
```

(3) 当 Router A 到 Router B 的报文延时恢复正常，丢包率仍为 25% 时，观察 Router A 显示信息。

查看到日志信息显示 EAA 策略 3 执行成功。

```
%Jul 14 15:19:13:771 2014 RouterA RTM/6/RTM_POLICY: CLI policy 3 is running
successfully.
```

使用 **display rtm environment** 命令用来显示用户自定义的 EAA 环境变量配置，观察到环境变量 **delay** 的值变为 0。

```
[RouterA] display rtm environment
Name                Value
-----
backup              1
delay               0
loss                1
```

使用 **display this** 命令显示当前视图下生效的配置，观察到 Router A 的报文切仍然经备份链路到 Router B。

```
[RouterA] display this
#
  sysname RouterA
#
  nqa schedule 1 1 start-time now lifetime forever
#
  ip route-static 100.1.1.0 24 11.1.1.1 preference 10
#
  snmp-agent
  snmp-agent local-engineid 800063A280000605B36B9E00000001
  snmp-agent sys-info version v3
#
  rtm environment backup 1
  rtm environment delay 0
  rtm environment loss 1
```

```
#
Return
```

- (4) 当 Router A 到 Router B 的报文延时和丢包率恢复正常时，观察 Router A 显示信息。

```
# 查看到日志信息显示 EAA 策略 4 执行成功。
```

```
%Jul 14 15:19:13:771 2014 RouterA RTM/6/RTM_POLICY: CLI policy 4 is running successfully.
```

```
# 使用 display rtm environment 命令用来显示用户自定义的 EAA 环境变量配置，观察到环境变量 backup、delay 和 loss 的值变为 0。
```

```
[RouterA] display rtm environment
```

Name	Value
backup	0
delay	0
loss	0

```
# 使用 display this 命令显示当前视图下生效的配置。
```

```
[RouterA] display this
```

```
#
 sysname RouterA
#
 nqa schedule 1 1 start-time now lifetime forever
#
 snmp-agent
 snmp-agent local-engineid 800063A280000605B36B9E00000001
 snmp-agent sys-info version v3
#
 rtm environment backup 0
 rtm environment delay 0
 rtm environment loss 0
#
Return
```

7.7 配置文件

- Router A:

```
#
nqa entry 1 1
 type icmp-echo
 destination ip 12.1.1.2
 frequency 15000
 probe count 15
 probe timeout 800
 reaction 1 checked-element probe-duration threshold-type average threshold-value 200
0 action-type none
 reaction 2 checked-element probe-fail threshold-type accumulate 3 action-type none
 reaction 3 checked-element probe-duration threshold-type average threshold-value 100
0 action-type none
 reaction 4 checked-element probe-fail threshold-type accumulate 1 action-type none
#
```

```

nga schedule 1 1 start-time now lifetime forever
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 12.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 11.1.1.2 255.255.255.0
#
snmp-agent
#
rtm cli-policy 1
event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.1 monitor-obj get start-op
eq start-val 2 restart-op eq restart-val 3 interval 10
action 0 cli tclsh
action 1 cli system-view
action 2 cli if { $delay==0 } { rtm environment delay 1 }
action 3 cli if { $backup==0 } { rtm environment backup 1; ip route-static 100.1.1.0
24 11.1.1.1 preference 10 }
user-role network-admin
#
rtm cli-policy 2
event snmp oid 1.3.6.1.4.1.25256.8.3.1.13.1.11.1.49.1.49.2 monitor-obj get start-op
eq start-val 2 restart-op eq restart-val 3 interval 10
action 0 cli tclsh
action 1 cli system-view
action 2 cli if { $loss==0 } { rtm environment loss 1 }
action 3 cli if { $backup==0 } { rtm environment backup 1; ip route-static 100.1.1.0
24 11.1.1.1 preference 10 }
user-role network-admin
#
rtm cli-policy 3
event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.3 monitor-obj get start-op
eq start-val 3 restart-op eq restart-val 2 interval 10
action 0 cli tclsh
action 1 cli system-view
action 2 cli if { $delay==1 } { rtm environment delay 0 }
action 3 cli after 5000
action 4 cli if { $backup==1 && $loss==0 } { undo ip route-static 100.1.1.0 24 11.1.1.1
preference 10; rtm environment backup 0 }
user-role network-admin
#
rtm cli-policy 4
event snmp oid 1.3.6.1.4.1.25506.8.3.1.13.1.11.1.49.1.49.4 monitor-obj get start-op
eq start-val 3 restart-op eq restart-val 2 interval 10
action 0 cli tclsh
action 1 cli system-view
action 2 cli if { $loss==1 } { rtm environment loss 0 }

```

```

action 3 cli after 5000
action 4 cli if { $backup==1 && $delay==0 } { undo ip route-static 100.1.1.0 24 11.1.1.1
preference 10; rtm environment backup 0 }
user-role network-admin
#
rtm environment backup 1
rtm environment delay 1
rtm environment loss 1
#

```

- **Router B:**

```

#
interface GigabitEthernet1/0/1
port link-mode route
ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 100.1.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 12.1.1.0 0.0.0.255
network 100.1.1.0 0.0.0.255
#

```

- **Router C:**

```

#
interface GigabitEthernet1/0/1
port link-mode route
ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 100.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 11.1.1.0 0.0.0.255
network 100.1.1.0 0.0.0.255
#

```

8 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“网络管理和监控配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“网络管理和监控命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 路由配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 路由命令参考”

H3C MSR 系列路由器

NTP 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介	1
2 配置前提	1
3 IPv6 NTP 服务器/客户端模式典型配置举例	1
3.1 组网需求	1
3.2 使用版本	1
3.3 配置步骤	2
3.3.1 Device A 的配置	2
3.3.2 Device B 的配置	2
3.3.3 Device C 的配置	2
3.4 验证配置	2
3.5 配置文件	3
4 IPv6 NTP 组播模式典型配置举例	3
4.1 组网需求	3
4.2 使用版本	4
4.3 配置步骤	4
4.3.1 Device C 的配置	4
4.3.2 Device D 的配置	4
4.3.3 Device B 的配置	5
4.3.4 Device A 的配置	5
4.4 验证配置	5
4.5 配置文件	6
5 带身份验证的 NTP 广播模式典型配置举例	7
5.1 组网需求	7
5.2 使用版本	7
5.3 配置步骤	7
5.3.1 Device A 的配置	7
5.3.2 Device B 的配置	8
5.4 验证配置	8
5.5 配置文件	9
6 相关资料	9

1 简介

本章介绍了与 NTP 有关的各种典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

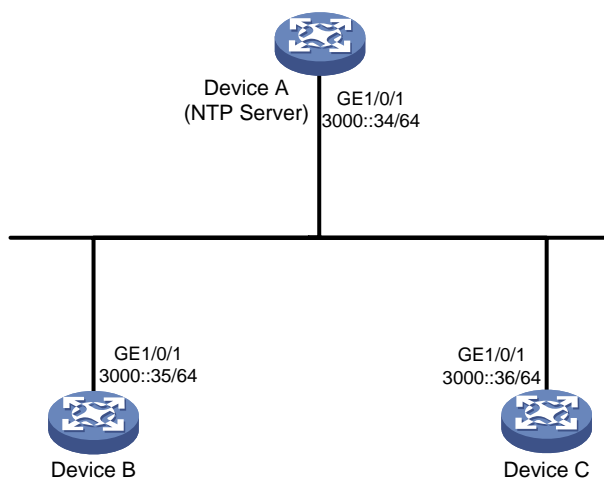
本文档假设您已了解 NTP 特性。

3 IPv6 NTP 服务器/客户端模式典型配置举例

3.1 组网需求

如图 1 所示，IPv6 网络中有一台时间服务器 Device A，为网络中的其它设备提供精确的时间服务，为保证网络中所有设备的时间保持一致，现要求配置 IPv6 NTP 服务器/客户端模式，使所有设备能从时间服务器 Device A 上获得时钟同步。

图1 配置 IPv6 NTP 服务器/客户端模式组网图



3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.3 配置步骤

3.3.1 Device A 的配置

```
# 配置接口 GigabitEthernet1/0/1 的 IP 地址。
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipv6 address 3000::34 64
[DeviceA-GigabitEthernet1/0/1] quit
# 开启 NTP 功能。
[DeviceA] ntp-service enable
# 设置本地时钟作为参考时钟，层数为 2。
[DeviceA] ntp-service refclock-master 2
```

3.3.2 Device B 的配置

```
# 配置接口的 IP 地址，配置步骤这里省略。
# 开启 NTP 功能。
<DeviceB> system-view
[DeviceB] ntp-service enable
# 设置 NTP Server 为 Device B 的时间服务器。
[DeviceB] ntp-service ipv6 unicast-server 3000::34
```

3.3.3 Device C 的配置

```
# 配置接口的 IP 地址，配置步骤这里省略。
# 开启 NTP 功能。
<DeviceC> system-view
[DeviceC] ntp-service enable
# 设置 NTP Server 为 Device C 的时间服务器。
[DeviceC] ntp-service ipv6 unicast-server 3000::34
```

3.4 验证配置

以上配置完成后，Device B 和 Device C 向 Device A 进行时间同步。以 Device B 为例，查看 NTP 的运行状态。

```
[DeviceB] display ntp-service status
Clock status: synchronized
Clock stratum: 3
System peer: 3000::34
Local mode: client
Reference clock ID: 95.197.17.40
Leap indicator: 00
Clock jitter: 0.003479 s
Stability: 0.000 pps
Clock precision: 2^-18
```



```

Root delay: 1.95313 ms
Root dispersion: 28.38135 ms
Reference time: d5ed8cd5.577006ea Wed, Sep 25 2013 16:24:53.341
此时 Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。
# 查看 Device B 的 NTP 会话信息，可以看到 Device B 与 Device A 建立了连接。
[DeviceB] display ntp-service ipv6 sessions
      source          reference          stra reach poll  now offset  delay disper
*****
[12345] 3000::34      127.127.1.0        2   127   64   67  -0.123  0.3356  5.3405
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
Total sessions: 1

```

3.5 配置文件

- 设备 Device A:

```

#
interface GigabitEthernet1/0/1
  ipv6 address 3000::34/64
#
ntp-service enable
ntp-service refclock-master 2
#

```
- 设备 Device B:

```

#
interface GigabitEthernet1/0/1
  ipv6 address 3000::35/64
#
ntp-service enable
ntp-service ipv6 unicast-server 3000::34
#

```
- 设备 Device C:

```

#
interface GigabitEthernet1/0/1
  ipv6 address 3000::36/64
#
ntp-service enable
ntp-service ipv6 unicast-server 3000::34
#

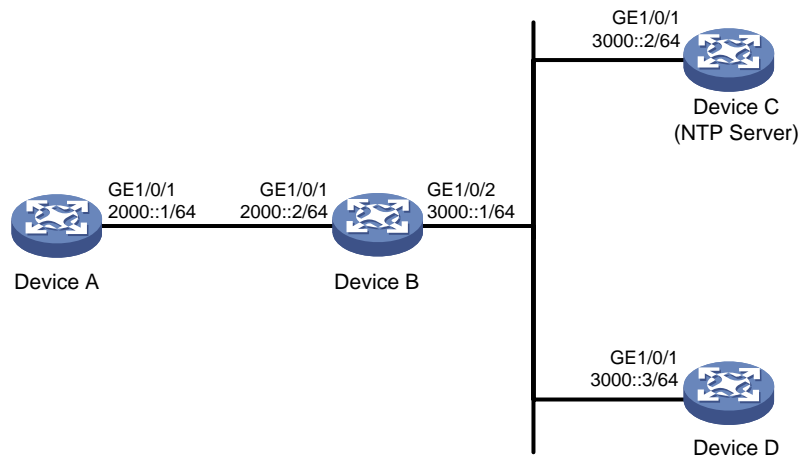
```

4 IPv6 NTP 组播模式典型配置举例

4.1 组网需求

如图 2 所示，IPv6 网络中有一台时间服务器 Device C，网络中设备较多，而且这些设备分布在不同网段中，为了便于管理，现要求配置 IPv6 NTP 组播模式，使网络中所有设备的时间保持一致。

图2 配置 IPv6 NTP 组播模式组网图



4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.3 配置步骤

4.3.1 Device C 的配置

配置路由协议，以保证各设备间能够路由可达，配置步骤这里省略。

开启 NTP 功能。

```
<DeviceC> system-view
```

```
[DeviceC] ntp-service enable
```

设置本地时钟作为参考时钟，层数为 2。

```
[DeviceC] ntp-service refclock-master 2
```

配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
[DeviceC] interface gigabitethernet 1/0/1
```

```
[DeviceC-GigabitEthernet1/0/1] ipv6 address 3000::2 64
```

设置 Device C 为 IPv6 组播服务器，从 GigabitEthernet1/0/1 向组播地址 FF24::1 发送 NTP 组播报文。

```
[DeviceC-GigabitEthernet1/0/1] ntp-service ipv6 multicast-server ff24::1
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

4.3.2 Device D 的配置

配置路由协议，以及接口的 IP 地址，以保证各设备间能够路由可达，配置步骤这里省略。

开启 NTP 功能。

```
<DeviceD> system-view
```

```
[DeviceD] ntp-service enable
```

设置 Device D 为组播客户端，从 GigabitEthernet1/0/1 监听组播报文。

```
[DeviceD] interface gigabitethernet 1/0/1
```

```
[DeviceD-GigabitEthernet1/0/1] ntp-service ipv6 multicast-client ff24::1
```

```
[DeviceD-GigabitEthernet1/0/1] quit
```

4.3.3 Device B 的配置

配置路由协议，以及接口的 IP 地址，以保证各设备间能够路由可达，配置步骤这里省略。

开启 NTP 功能。

```
<DeviceB> system-view
```

```
[DeviceB] ntp-service enable
```

设置 Device B 为组播客户端，从 GigabitEthernet1/0/1 监听组播报文。

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/1] ntp-service ipv6 multicast-client ff24::1
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

由于 Device A 与 Device C 不在同一网段，所以 Device B 上需要配置组播功能，否则 Device A 收不到 Device C 发出的组播报文。

配置组播功能。

```
[DeviceB] ipv6 multicast routing
```

```
[DeviceB-mrib6] quit
```

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/1] ipv6 pim dm
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] mld enable
```

```
[DeviceB-GigabitEthernet1/0/1] mld static-group ff24::1
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

4.3.4 Device A 的配置

配置路由协议，以及接口的 IP 地址，以保证各设备间能够路由可达，配置步骤这里省略。

开启 NTP 功能。

```
<DeviceA> system-view
```

```
[DeviceA] ntp-service enable
```

设置 Device A 为组播客户端，从 GigabitEthernet1/0/1 监听组播报文。

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] ntp-service ipv6 multicast-client ff24::1
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```

4.4 验证配置

以 Device A 为例，查看 NTP 的运行状态。

```
[DeviceA] display ntp-service status
```

```
Clock status: synchronized
```

```
Clock stratum: 3
```

```
System peer: 3000::2
```

```
Local mode: bclient
```

```
Reference clock ID: 165.84.121.65
```

```
Leap indicator: 00
```

```
Clock jitter: 0.000061 s
```

```
Stability: 0.000 pps
Clock precision: 2^-18
Root delay: 1.69373 ms
Root dispersion: 1950.18005 ms
Reference time: d5ee9b15.2f3a684d Thu, Sep 26 2013 11:37:57.184
```

此时 Device A 已经与 Device C 同步，层数比 Device C 的层数大 1，为 3。

4.5 配置文件

- 设备 Device A:

```
#
ntp-service enable
#
interface GigabitEthernet1/0/1
  ipv6 address 2000::1/64
  ntp-service ipv6 multicast-client ff24::1
#
```
- 设备 Device B:

```
#
ntp-service enable
#
ipv6 multicast routing
#
mld-snooping
#
interface GigabitEthernet1/0/1
  ipv6 address 3000::1/64
  ipv6 pim dm
  ntp-service ipv6 multicast-client ff24::1
#
interface GigabitEthernet1/0/1
  ipv6 address 2000::2/64
  mld enable
  mld static-group ff24::1
#
```
- 设备 Device C:

```
#
ntp-service enable
ntp-service refclock-master 2
#
interface GigabitEthernet1/0/1
  ipv6 address 3000::2/64
  ntp-service ipv6 multicast-server ff24::1
#
```
- 设备 Device D:

```
#
ntp-service enable
```

```
#
interface GigabitEthernet1/0/1
  ipv6 address 3000::3/64
  ntp-service ipv6 multicast-client ff24::1
#
```

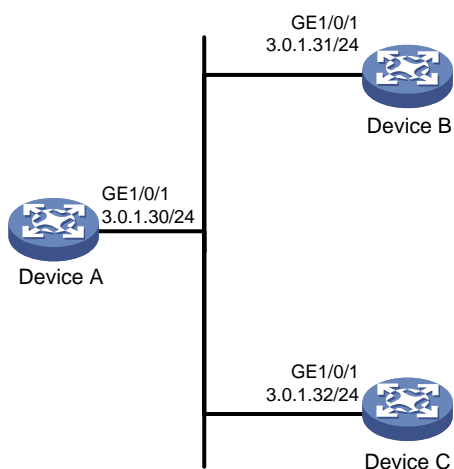
5 带身份验证的 NTP 广播模式典型配置举例

5.1 组网需求

如图 3 所示，网络中设备较多，所有设备都位于同一个网段（3.0.1.0/24）中，为了使网络中所有设备的时间保持一致，现要求：

- 配置 NTP 广播模式。
- NTP 广播客户端与 NTP 广播服务器进行时间同步前，必须先进行身份验证，以保证时钟同步的安全性，防止攻击者将自己伪装成一个时钟服务器而对客户时钟发起攻击。

图3 带身份验证的 NTP 广播模式典型配置举例组网图



5.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

5.3 配置步骤

5.3.1 Device A 的配置

开启 NTP 功能。

```
<DeviceA> system-view
```

```
[DeviceA] ntp-service enable
```

设置本地时钟作为参考时钟，层数为 2。

```
[DeviceA] ntp-service refclock-master 2
```

配置 NTP 验证，密钥编号为 88，密钥为 123456。

```
[DeviceA] ntp-service authentication enable
[DeviceA] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[DeviceA] ntp-service reliable authentication-keyid 88
```

设置 Device A 为 NTP 广播服务器并指定密钥编号。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 3.0.1.30 24
[DeviceA-GigabitEthernet1/0/1] ntp-service broadcast-server authentication-keyid 88
[DeviceA-GigabitEthernet1/0/1] quit
```

5.3.2 Device B 的配置

开启 NTP 功能。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

配置 NTP 验证，密钥编号与密钥与 Device A 完全相同。

```
[DeviceB] ntp-service authentication enable
[DeviceB] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[DeviceB] ntp-service reliable authentication-keyid 88
```

设置 Device B 为 NTP 广播客户端。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ntp-service broadcast-client
[DeviceB-GigabitEthernet1/0/1] ip address 3.0.1.31 24
[DeviceB-GigabitEthernet1/0/1] quit
```

以上配置将 Device B 配置为从 GigabitEthernet1/0/1 监听广播报文，接收到 Device A 发出的广播报文后与自己的时钟进行同步。



除 IP 地址外，Device C 与 DeviceB 的其他配置完全相同，此处不再赘述。

5.4 验证配置

以 Device B 为例，查看 NTP 的运行状态。

```
[DeviceA] display ntp-service status
Clock status: synchronized
Clock stratum: 3
System peer: 3.0.1.30
Local mode: bclient
Reference clock ID: 3.0.1.30
Leap indicator: 00
Clock jitter: 0.000092 s
Stability: 0.000 pps
Clock precision: 2^-18
Root delay: 2.42615 ms
```

Root dispersion: 1950.98877 ms
Reference time: d5eed631.2f498d71 Thu, Sep 26 2013 15:50:09.184
此时 Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。

5.5 配置文件

- 设备 Device A:

```
#  
interface GigabitEthernet1/0/1  
 ip address 3.0.1.30 255.255.255.0  
 ntp-service broadcast-server authentication-keyid 88  
#  
 ntp-service enable  
 ntp-service authentication enable  
 ntp-service authentication-keyid 88 authentication-mode md5 cipher  
 $c$3$iJudDKiqCVO+gOaG53  
 63/fz4M3dQvHo2Fw==  
 ntp-service reliable authentication-keyid 88  
 ntp-service refclock-master 2  
#
```

- 设备 Device B、Device C:

```
#  
interface GigabitEthernet1/0/1  
 ip address 3.0.1.31 255.255.255.0  
 ntp-service broadcast-client  
#  
 ntp-service enable  
 ntp-service authentication enable  
 ntp-service authentication-keyid 88 authentication-mode md5 cipher  
 $c$3$pU6KvpS80MadhM2zM  
 CCSR07HX4qEbJhHvQ==  
 ntp-service reliable authentication-keyid 88  
#
```

6 相关资料

- 《H3C MSR 系列路由器 命令参考(V7)》中的“网络管理和监控命令参考”
- 《H3C MSR 系列路由器 配置指导(V7)》中的“网络管理和监控配置指导”

H3C MSR 系列路由器

RMON 配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 RMON 统计功能配置举例.....	1
3.1 组网需求.....	1
3.2 使用版本.....	1
3.3 配置步骤.....	1
3.4 验证配置.....	2
3.5 配置文件.....	2
4 RMON 历史统计功能配置举例.....	2
4.1 组网需求.....	2
4.2 使用版本.....	3
4.3 配置步骤.....	3
4.4 验证配置.....	3
4.5 配置文件.....	5
5 RMON 告警功能配置举例.....	5
5.1 组网需求.....	5
5.2 配置思路.....	5
5.3 使用版本.....	6
5.4 配置注意事项.....	6
5.5 配置步骤.....	6
5.5.1 Router 的配置.....	6
5.5.2 NMS 的配置.....	7
5.6 验证配置.....	8
5.7 配置文件.....	8
6 相关资料.....	9

1 简介

本文档介绍 MSR 系列路由器 RMON 典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

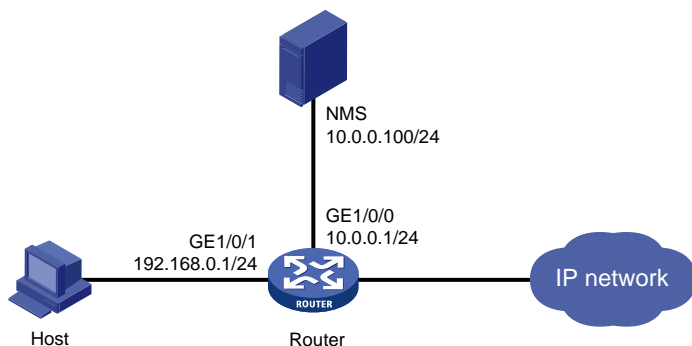
本文档假设您已了解 RMON 特性。

3 RMON 统计功能配置举例

3.1 组网需求

如图1所示，Router 作为主机 Host 的网关，NMS 对 Router 进行实时的监控管理。现需要通过 RMON 功能对主机 Host 的流量进行统计，以便管理员进行查看。

图1 RMON 统计功能配置组网图



3.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.3 配置步骤

配置路由器接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.0.0.1 24
[Router-GigabitEthernet1/0/0] quit
```

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.0.1 24
# 创建 GigabitEthernet1/0/1 接口的统计表项，表项的索引号为 10，创建者为 user1。
[Router-GigabitEthernet1/0/1] rmon statistics 10 owner user1
[Router-GigabitEthernet1/0/1] quit
```

3.4 验证配置

统计表项配置完成后，系统就开始对接口 GigabitEthernet1/0/1 接收的报文进行分类统计。统计的结果可以通过 **display rmon statistics** 命令查看。

```
[Router] display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 10 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets      : 21657      , etherStatsPkts      : 307
  etherStatsBroadcastPkts : 56      , etherStatsMulticastPkts : 34
  etherStatsUndersizePkts : 0      , etherStatsOversizePkts : 0
  etherStatsFragments   : 0      , etherStatsJabbers    : 0
  etherStatsCRCAlignErrors : 0      , etherStatsCollisions : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size:
  64      : 235      , 65-127 : 67      , 128-255 : 4
  256-511: 1      , 512-1023: 0      , 1024-1518: 0
```

3.5 配置文件

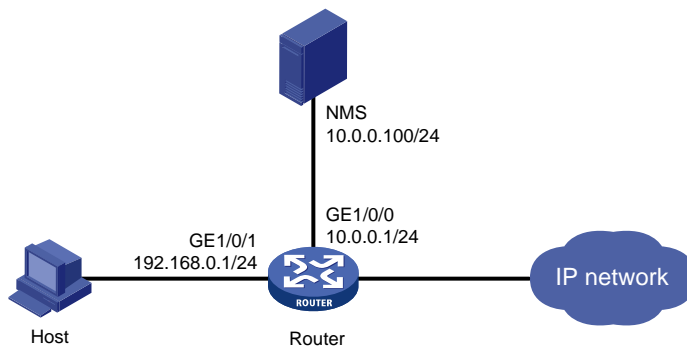
```
#
interface GigabitEthernet1/0/0
 port link-mode route
 ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
 rmon statistics 10 owner user1
#
```

4 RMON 历史统计功能配置举例

4.1 组网需求

如图2所示，Router 作为主机 Host 的网关。现需要通过 RMON 功能对 GigabitEthernet1/0/1 接口的入流量进行周期性的统计，以便管理员可以随时了解接口的流量。

图2 RMON 历史统计功能配置组网图



4.2 使用版本

本举例是在 R6728 版本上进行配置和验证的。

4.3 配置步骤

配置路由器接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.0.0.1 24
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.0.1 24
# 创建索引号为 1，表容量为 8，采样时间为 60 秒的历史控制表项，创建者为 user1。
[Router-GigabitEthernet1/0/1] rmon history 1 buckets 8 interval 60 owner user1
[Router-GigabitEthernet1/0/1] quit
```

4.4 验证配置

历史控制表项配置完成后，系统就开始对接口 GigabitEthernet1/0/1 接收的报文进行周期性分类统计，每 1 分钟统计一次，历史统计列表里会保存最近的 8 次统计的结果，以便管理员查看。统计的结果可以通过 **display rmon history** 命令查看。

```
[Router] display rmon history
HistoryControlEntry 1 owned by user1 is VALID
  Sampled interface      : GigabitEthernet1/0/1<ifIndex.3>
  Sampling interval      : 60(sec) with 8 buckets max
  Sampling record 1 :
    dropevents           : 0           , octets                : 834
    packets              : 8           , broadcast packets     : 1
    multicast packets    : 6           , CRC alignment errors : 0
    undersize packets    : 0           , oversize packets     : 0
    fragments           : 0           , jabbers              : 0
    collisions           : 0           , utilization           : 0
```

```

Sampling record 2 :
  dropevents      : 0          , octets           : 962
  packets         : 10         , broadcast packets : 3
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets   : 0
  fragments       : 0         , jabbers           : 0
  collisions      : 0         , utilization        : 0

Sampling record 3 :
  dropevents      : 0          , octets           : 830
  packets         : 8          , broadcast packets : 0
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets   : 0
  fragments       : 0         , jabbers           : 0
  collisions      : 0         , utilization        : 0

Sampling record 4 :
  dropevents      : 0          , octets           : 933
  packets         : 8          , broadcast packets : 0
  multicast packets : 7         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets   : 0
  fragments       : 0         , jabbers           : 0
  collisions      : 0         , utilization        : 0

Sampling record 5 :
  dropevents      : 0          , octets           : 898
  packets         : 9          , broadcast packets : 2
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets   : 0
  fragments       : 0         , jabbers           : 0
  collisions      : 0         , utilization        : 0

Sampling record 6 :
  dropevents      : 0          , octets           : 898
  packets         : 9          , broadcast packets : 2
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets   : 0
  fragments       : 0         , jabbers           : 0
  collisions      : 0         , utilization        : 0

Sampling record 7 :
  dropevents      : 0          , octets           : 766
  packets         : 7          , broadcast packets : 0
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets   : 0
  fragments       : 0         , jabbers           : 0
  collisions      : 0         , utilization        : 0

Sampling record 8 :
  dropevents      : 0          , octets           : 1154
  packets         : 13         , broadcast packets : 1
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets   : 0
  fragments       : 0         , jabbers           : 0

```

```
collisions : 0 , utilization : 0
```

4.5 配置文件

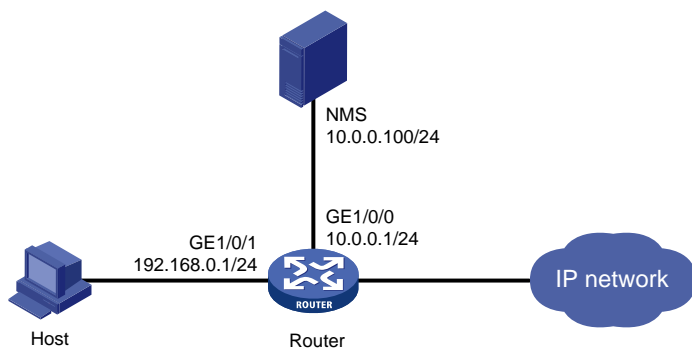
```
#
interface GigabitEthernet1/0/0
  port link-mode route
  ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-mode route
  ip address 192.168.0.1 255.255.255.0
  rmon history 1 buckets 8 interval 60 owner user1
#
```

5 RMON 告警功能配置举例

5.1 组网需求

如图 3 所示，路由器作为主机 Host 的网关，NMS 对路由器进行实时的监控管理。现需要通过 RMON 功能对主机 Host 的流量进行统计，以 5 秒的采样间隔采样，并且当路由器 GigabitEthernet1/0/1 接口收到的报文总字节数达到或超过 10000 字节，或者小于等于 5000 字节时，路由器会向 NMS 发送相应的告警信息。

图3 RMON 告警功能配置组网图



5.2 配置思路

- 为了实现 NMS 对路由器进行管理监控，需要在路由器上配置 SNMP Agent 功能；
- 使路由器可以周期性监控 GigabitEthernet1/0/1 接口的流量，需要先定义一个 RMON 统计表项对接口流量进行统计；
- 当 GigabitEthernet1/0/1 接口流量异常时，为了路由器可以向 NMS 发送 Trap 告警信息，需要在路由器上创建一个告警表项，并设置该表项的告警阈值。

5.3 使用版本

本举例是在 R0106 版本和 iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)上进行配置和验证的。

5.4 配置注意事项

为保证 NMS 和路由器可以正常通信，如下参数配置必须保证完全一样：

- SNMP 版本
- 可读团体名
- 读写团体名

5.5 配置步骤

5.5.1 Router 的配置

- (1) 配置路由器接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.0.0.1 24
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.0.1 24
[Router-GigabitEthernet1/0/1] quit
```

- (2) 配置 SNMP Agent 功能。

配置 NMS 上运行 SNMP v1，访问设备时使用的可读团体名为 public，可写团体名为 private，NMS 的 IP 地址为 10.0.0.100

```
[Router] snmp-agent
[Router] snmp-agent community read public
[Router] snmp-agent community write private
[Router] snmp-agent sys-info version v1
[Router] snmp-agent trap enable
[Router] snmp-agent target-host trap address udp-domain 10.0.0.100 params securityname public
```

创建 GigabitEthernet1/0/1 接口的统计表项，表项的索引号为 10，创建者为 user1。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] rmon statistics 10 owner user1
[Router-GigabitEthernet1/0/1] quit
```

创建告警表项 1，对节点 1.3.6.1.4.1.25506.2.125.1.1.1 以 5 秒的采样间隔进行绝对值采样，当该接口收到的报文总字节数达到或超过 10000 字节，或者小于等于 5000 字节时，会触发事件 1，路由器向 NMS 发送相应的 Trap 信息，创建者为 user1。

```
[Router] rmon event 1 trap public owner user1
[Router] rmon alarm 1 1.3.6.1.4.1.25506.2.125.1.1.1 5 absolute rising-threshold 10000
1 falling-threshold 5000 1 owner user1
```

5.5.2 NMS 的配置

增加设备

登录进入 IMC 管理平台，选择“资源”页签，单击导航树中的[增加设备]菜单项，进入增加设备配置页面。

- 设置设备的主机名或 IP 地址为“10.0.0.1”；
- 设置设备标签为“Router”；
- 选择登录方式为“Telnet”；
- 其它参数采用缺省值。

图4 增加设备页面

资源 > 增加设备 ? 帮助

设备基本信息

主机名或IP地址 *

设备标签

掩码

设备分组

登录方式

将设备的Trap发送到本网管系统

设备支持Ping操作 ?

Ping不通也加入 ?

将LoopBack地址作为管理IP

+ 配置 SNMP 参数

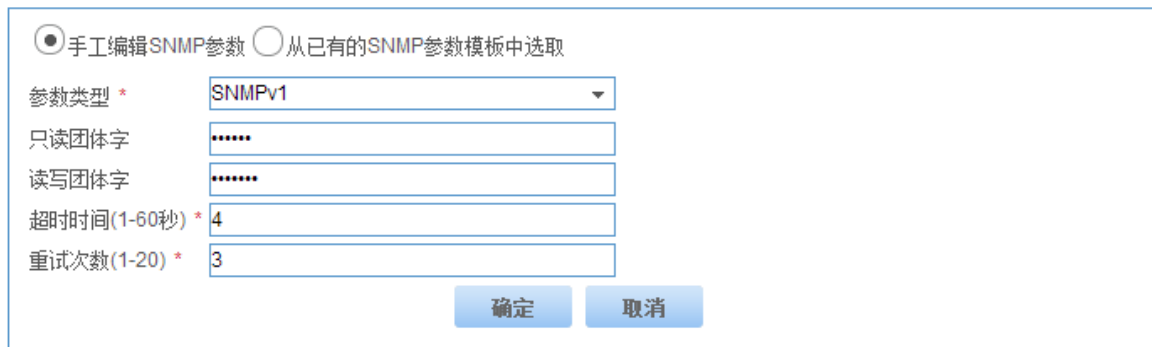
+ 配置 Telnet 参数

+ 配置 SSH 参数

在该页面中单击<配置 SNMP 参数>按钮，展开配置 SNMP 参数页面，单击<设置>按钮，弹出 SNMP 参数设置页面。

- 设置参数类型为“SNMPv1”；
- 设置只读团体字为“public”；
- 设置读写团体字尾“private”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 SNMP 参数设置页面



The screenshot shows a configuration window for SNMP parameters. At the top, there are two radio buttons: '手工编辑SNMP参数' (selected) and '从已有的SNMP参数模板中选取'. Below this are five input fields: '参数类型 *' (SNMPv1), '只读团体字' (*****), '读写团体字' (*****), '超时时间(1-60秒) *' (4), and '重试次数(1-20) *' (3). At the bottom right, there are two buttons: '确定' (OK) and '取消' (Cancel).

5.6 验证配置

通过 **display rmon alarm** 命令查看 RMON 告警表项信息。

```
[Router] display rmon alarm 1
AlarmEntry 1 owned by user1 is VALID.
  Sample type          : absolute
  Sampled variable    : 1.3.6.1.4.1.25506.2.125.1.1.1<etherStatsOctets.1>
  Sampling interval (in seconds) : 5
  Rising threshold    : 10000(associated with event 1)
  Falling threshold   : 5000(associated with event 1)
  Alarm sent upon entry startup : risingOrFallingAlarm
  Latest value        : 0
```

通过 **display rmon statistics** 命令可以查看以太网接口的统计信息。

```
[Router] display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 10 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets      : 57329      , etherStatsPkts      : 455
  etherStatsBroadcastPkts : 53      , etherStatsMulticastPkts : 353
  etherStatsUndersizePkts : 0      , etherStatsOversizePkts : 0
  etherStatsFragments   : 0      , etherStatsJabbers    : 0
  etherStatsCRCAlignErrors : 0      , etherStatsCollisions : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size :
  64      : 7      , 65-127 : 413      , 128-255 : 35
  256-511: 0      , 512-1023: 0      , 1024-1518: 0
```

5.7 配置文件

```
#
interface GigabitEthernet1/0/0
  port link-mode route
  ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
```

```
port link-mode route
ip address 192.168.0.1 255.255.255.0
rmon statistics 10 owner user1
#
snmp-agent
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version v1
snmp-agent target-host trap address udp-domain 10.0.0.100 params securityn
ame public
#
rmon event 1 trap public owner user1
#
rmon alarm 1 1.3.6.1.4.1.25506.2.125.1.1.1 5 absolute rising-threshold 10000 1
falling-threshold 5000 1 owner user1
```

6 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“网络管理和监控配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“网络管理和监控命令参考”

H3C MSR 系列路由器

POS 终端为流接入且应用为流连接方式配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	1
3.4 配置步骤.....	1
3.5 验证配置.....	2
3.6 配置文件.....	2
4 相关资料.....	2

1 简介

本文档介绍 MSR 系列路由器 POS 终端为流接入且应用为流连接方式配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

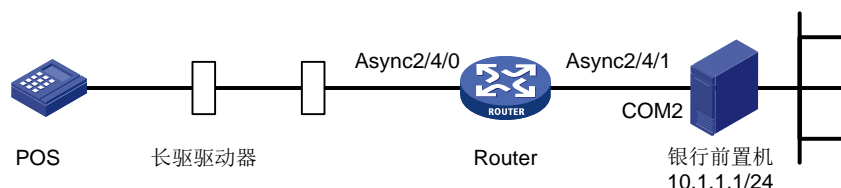
本文档假设您已了解 POS 终端接入特性。

3 配置举例

3.1 组网需求

如图 1 所示，POS 机通过串口连接到 Router。Router 通过串口连接到银行前置机的 COM 口。银行前置机启用 POS 接入服务程序并使用 COM 口进行数据的收发。现要求：POS 机通过流连接方式连接到前置机。

图1 终端为流接入方式且应用为流连接方式组网图



3.2 配置思路

配置 POS 应用模板和终端模板为流连接实现流类型连接方式。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置步骤

使能 POS 接入服务。

```
<Router> system-view  
[Router] posa server enable
```

配置 Router 到前置机的应用模板 1，为流连接方式。

```
[Router] posa app 1 type flow
[Router-posa-appl] quit
# 配置应用模板 1 的连接接口为 Async2/4/1。
[Router] interface async 2/4/1
[Router-Async2/4/1] async-mode flow
[Router-Async2/4/1] posa bind app 1
[Router-Async2/4/1] quit
# 配置终端模板 1 的接入接口为 Async2/4/0。
[Router] interface async 2/4/0
[Router-Async2/4/0] async-mode flow
[Router-Async2/4/0] posa bind terminal 1
[Router-Async2/4/0] quit
# 将目的地址为 01f1 的报文映射到应用模板 1。
[Router] posa map destination 01f1 app 1
```

3.5 验证配置

POS 机发送 POS 请求报文，经过 POS 终端接入设备的处理，前置机收到请求报文，并发送 POS 应答报文，POS 机收到应答报文。

3.6 配置文件

```
#
posa app 1 type flow
#
  posa server enable
  posa map destination 01f1 app 1
#
interface Async2/4/0
  async-mode flow
  posa bind terminal 1
#
interface Async2/4/1
  async-mode flow
  posa bind app 1
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“终端接入配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“终端接入命令参考”

H3C MSR 系列路由器

POS 终端为 TCP 接入且应用为 TCP 连接方式配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 使用版本.....	1
3.4 配置步骤.....	1
3.5 验证配置.....	2
3.6 配置文件.....	2
4 相关资料.....	2

1 简介

本文档介绍 POS 终端为 TCP 接入且应用为 TCP 连接方式配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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。

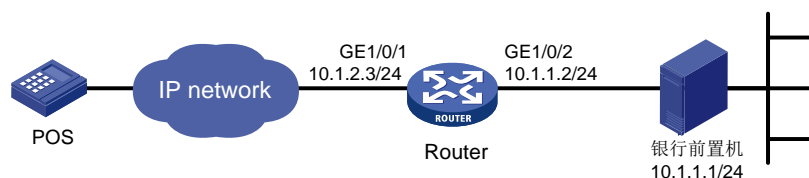
本文档假设您已了解 POS 终端接入特性。

3 配置举例

3.1 组网需求

如[图 1](#)所示，POS 机通过 POS 接入设备 Router 连接到前置机 Server。银行前置机启用程序并使用监听端口号为 2000。现要求：POS 机为 TCP 接入且终端接入设备 Router A 以 TCP 的方式连接到银行前置机。

图1 终端为 TCP 接入方式且应用为 TCP 连接方式配置组网图



3.2 配置思路

为实现 POS 机使用 TCP 接入方式且应用为 TCP 连接方式，需要将应用模板和终端模板均配置为 TCP 连接。

3.3 使用版本

本举例是在 R6728 版本上进行配置和验证的。

3.4 配置步骤

使能 POS 终端接入服务。

```
<Router> system-view
[Router] posa server enable
```

```

# 配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 IP。
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 10.1.2.3 24
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2.] ip address 10.1.1.2 24
[Router-GigabitEthernet1/0/2] quit
# 配置设备到银行前置机的应用模板 1，为 TCP 连接方式。
[Router] posa app 1 type tcp
# 配置应用模板 1 对应前置机的 IP 地址为 10.1.1.1，端口号为 2000。
[Router-posa-app1] ip 10.1.1.1 port 2000
[Router-posa-app1] quit
# 配置终端模板 1 为 TCP 接入方式，监听端口为 3000。
[Router] posa terminal 1 type tcp listen-port 3000
# 配置应用模板 1 为默认应用。
[Router] posa map default app 1

```

3.5 验证配置

以太网 POS 机发送 POS 请求报文，经过 POS 终端接入设备的处理，银行前置机收到请求报文，并发送 POS 应答报文，POS 机收到应答报文。

3.6 配置文件

```

#
posa app 1 type tcp
 ip 10.1.1.1 port 2000
#
posa server enable
posa terminal 1 type tcp listen-port 3000
posa map default app 1
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.2.3 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#

```

4 相关资料

- 《H3C MSR 系列路由器 配置指导（V7）》中的“终端接入配置指导”
- 《H3C MSR 系列路由器 命令参考（V7）》中的“终端接入命令参考”

H3C MSR 系列路由器

IPsec 数字证书认证配置举例

Copyright © 2022-2023 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1-1
2 配置前提.....	2-1
3 IKE 野蛮模式及 RSA 数字签名认证配置举例.....	3-1
3.1 组网需求.....	3-1
3.2 配置步骤.....	3-2
3.2.1 配置 Device A.....	3-2
3.2.2 配置 Device B.....	3-4
3.3 验证配置.....	3-6
4 IKE 国密主模式及 SM2-DE 数字信封认证配置举例.....	4-7
4.1 组网需求.....	4-7
4.2 配置步骤.....	4-8
4.2.1 配置 Device A.....	4-8
4.2.2 配置 Device B.....	4-10
4.3 验证配置.....	4-11
5 IKEv2 RSA 数字签名认证配置举例.....	5-13
5.1 组网需求.....	5-13
5.2 配置步骤.....	5-14
5.2.1 配置 Device A.....	5-14
5.2.2 配置 Device B.....	5-16
5.3 验证配置.....	5-18

1 简介

本文档介绍 H3C MSR 系列路由器 IPsec 数字证书认证典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，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 IPsec、IKE 和 IKEv2 特性。

3 IKE 野蛮模式及 RSA 数字签名认证配置举例



说明

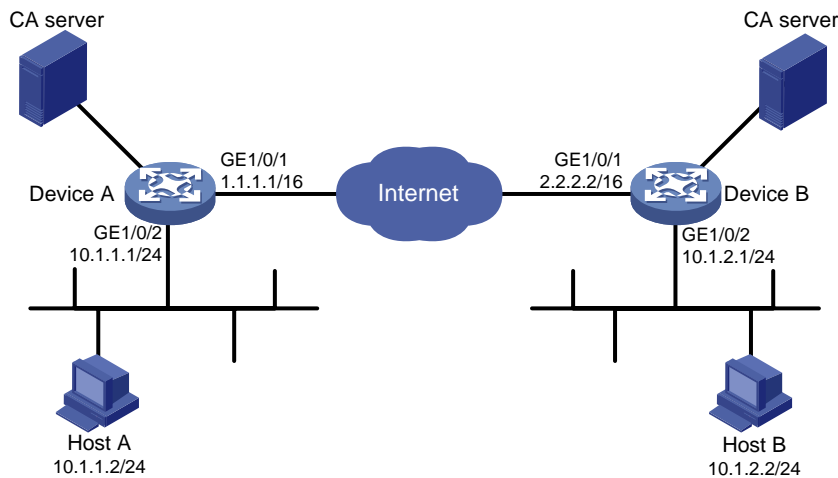
设备运行于 FIPS 模式时，不支持本例。

3.1 组网需求

在 Device A 和 Device B 之间建立一个 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。

- Device A 和 Device B 之间采用 IKE 协商方式建立 IPsec SA。
- Device A 和 Device B 均使用 RSA 数字签名的认证方法。
- IKE 第一阶段的协商模式为野蛮模式。
- Device A 侧子网的 IP 地址为动态分配，并作为发起方。

图1 IKE 野蛮模式及 RSA 数字签名认证典型组网图



3.2 配置步骤



说明

在开始下面的配置之前，假设已完成如下配置：

- DeviceA 和 DeviceB 已获取到 CA 证书 ca.cer 和服务器证书 server.pfx。

3.2.1 配置 Device A

配置各接口的 IP 地址，具体略。

配置 IPv4 高级 ACL 3101，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
<DeviceA> system-view
[DeviceA] acl advanced 3101
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[DeviceA-acl-ipv4-adv-3101] quit
```

创建 IPsec 安全提议 tran1。

```
[DeviceA] ipsec transform-set tran1
# 配置安全协议对 IP 报文的封装形式为隧道模式。
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceA-ipsec-transform-set-tran1] protocol esp
# 配置 ESP 协议采用的加密算法为 DES，认证算法为 HMAC-SHA1。
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
```

创建 PKI 实体 entity1。

```

[DeviceA] pki entity entity1
# 配置 PKI 实体的通用名。
[DeviceA-pki-entity-entity1] common-name devicea
[DeviceA-pki-entity-entity1] quit
# 配置 PKI 域 domain1。
<DeviceA> system-view
[DeviceA] pki domain domain1
[DeviceA-pki-domain-domain1] public-key rsa general name rsa1
[DeviceA-pki-domain-domain1] undo crl check enable
[DeviceA-pki-domain-domain1] quit
# 导入 CA 证书 ca.cer 和服务证书 server.pfx。
[DeviceA] pki import domain domain1 der ca filename ca.cer
[DeviceA] pki import domain domain1 p12 local filename server.pfx
# 配置证书访问策略 policy1。
<DeviceA> system-view
[DeviceA] pki certificate access-control-policy policy1
[DeviceA-pki-cert-acp-policy1] rule 1 permit group1
# 配置证书属性规则。
[DeviceA] pki certificate attribute-group group1
[DeviceA-pki-cert-attribute-group-group1] attribute 1 subject-name dn ctn 1
对端证书 subject-name DN 中需包含（ctn）规则中定义的字符串才被认为是有效的证书。本例使用的证书 subject-name DN 中包含字符“1”，因此在这里使用参数 ctn 1。
# 创建 IKE profile，名称为 profile1。
[DeviceA] ike profile profile1
# 指定引用的 PKI 域为 domain1。
[DeviceA-ike-profile-profile1] certificate domain domain1
# 配置第一阶段的协商模式为野蛮模式。
[DeviceA-ike-profile-profile1] exchange-mode aggressive
# 配置使用本端数字证书中获得的 DN 名作为本端身份标识。
[DeviceA-ike-profile-profile1] local-identity dn
# 配置匹配对端身份规则为对端数字证书中的 DN 名。
[DeviceA-ike-profile-profile1] match remote certificate policy1
[DeviceA-ike-profile-profile1] quit
# 创建 IKE 提议 10。
[DeviceA] ike proposal 10
# 指定 IKE 提议使用的认证算法为 HMAC-MD5。
[DeviceA-ike-proposal-10] authentication-algorithm md5
# 指定使用 RSA 数字签名认证方法。
[DeviceA-ike-proposal-10] authentication-method rsa-signature
[DeviceA-ike-proposal-10] quit
# 创建一条 IKE 协商方式的 IPsec 安全策略，名称为 map1，顺序号为 10。
[DeviceA] ipsec policy map1 10 isakmp
# 配置 IPsec 隧道的对端 IP 地址为 2.2.2.2。
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2

```

```

# 指定引用的安全提议为 tran1。
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
# 指定引用 ACL 3101。
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3101
# 指定引用的 IKE profile 为 profile1。
[DeviceA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
# 在接口 GigabitEthernet1/0/1 上应用 IPsec 安全策略 map1。
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy map1
[DeviceA-GigabitEthernet1/0/1] quit
# 配置到 Host B 所在子网的静态路由。1.1.1.2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 1.1.1.2

```

3.2.2 配置 Device B

```

# 配置各接口的 IP 地址，具体略。
# 配置 IPv4 高级 ACL 3101，定义要保护由子网 10.1.2.0/24 去往子网 10.1.1.0/24 的数据流。
<DeviceB> system-view
[DeviceB] acl advanced 3101
[DeviceB-acl-ipv4-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[DeviceB-acl-ipv4-adv-3101] quit
# 创建 IPsec 安全提议 tran1。
[DeviceB] ipsec transform-set tran1
# 配置安全协议对 IP 报文的封装形式为隧道模式。
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
# 配置采用的安全协议为 ESP。
[DeviceB-ipsec-transform-set-tran1] protocol esp
# 配置 ESP 协议采用的加密算法为 DES，认证算法为 HMAC-SHA1。
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
# 创建 PKI 实体 entity2。
[DeviceB] pki entity entity2
# 配置 PKI 实体的通用名。
[DeviceB-pki-entity-entity2] common-name deviceb
[DeviceB-pki-entity-entity2] quit
# 配置 PKI 域 domain2。
<DeviceB> system-view
[DeviceB] pki domain domain2
[DeviceB-pki-domain-domain2] public-key rsa general name rsa1
[DeviceB-pki-domain-domain2] undo crl check enable
[DeviceB-pki-domain-domain2] quit

```



```

# 导入 CA 证书 ca.cer 和服务器证书 server.pfx。
[DeviceB] pki import domain domain2 der ca filename ca.cer
[DeviceB] pki import domain domain2 p12 local filename server.pfx
# 配置证书访问策略 policy1。
<DeviceB> system-view
[DeviceB] pki certificate access-control-policy policy1
[DeviceB-pki-cert-acp-policy1] rule 1 permit group1
# 配置证书属性规则。
[DeviceB] pki certificate attribute-group group1
[DeviceB-pki-cert-attribute-group-group1] attribute 1 subject-name dn ctn 1
对端证书 subject-name DN 中需包含（ctn）规则中定义的字符串才被认为是有效的证书。本例使用的证书 subject-name DN 中包含字符“1”，因此在这里使用参数 ctn 1。
# 创建 IKE profile，名称为 profile2。
[DeviceB] ike profile profile2
# 指定引用的 PKI 域为 domain2。
[DeviceB-ike-profile-profile2] certificate domain domain2
# 配置第一阶段的协商模式为野蛮模式。
[DeviceB-ike-profile-profile2] exchange-mode aggressive
# 配置使用本端数字证书中获得的 DN 名作为本端身份标识。
[DeviceB-ike-profile-profile2] local-identity dn
# 配置匹配对端身份规则为对端数字证书中的 DN 名。
[DeviceB-ike-profile-profile2] match remote certificate policy1
[DeviceB-ike-profile-profile2] quit
# 创建 IKE 提议 10。
[DeviceB] ike proposal 10
# 指定 IKE 提议使用的认证算法为 HMAC-MD5。
[DeviceB-ike-proposal-10] authentication-algorithm md5
# 指定使用 RSA 数字签名认证方法。
[DeviceB-ike-proposal-10] authentication-method rsa-signature
[DeviceB-ike-proposal-10] quit
# 创建一条 IPsec 安全策略模板，名称为 template1，序号为 1。
[DeviceB] ipsec policy-template template1 1
# 指定引用的安全提议为 tran1。
[DeviceB-ipsec-policy-template-template1-1] transform-set tran1
# 指定引用 ACL 3101。
[DeviceB-ipsec-policy-template-template1-1] security acl 3101
# 指定引用的 IKE profile 为 profile2。
[DeviceB-ipsec-policy-template-template1-1] ike-profile profile2
[DeviceB-ipsec-policy-template-template1-1] quit
# 引用 IPsec 安全策略模板创建一条 IPsec 安全策略，名称为 use1，序号为 1。
[DeviceB] ipsec policy use1 1 isakmp template template1
# 在接口 GigabitEthernet1/0/1 上应用 IPsec 安全策略 use1。
[DeviceB] interface gigabitethernet 1/0/1

```

```
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy use1
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

配置到 Host A 所在子网的静态路由。2.2.2.1 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。

```
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 2.2.2.1
```

3.3 验证配置

以上配置完成后，Device A 和 Device B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKE 协商。

可通过如下显示信息查看到 Device A 和 Device B 上的 IKE 提议。

```
[DeviceA] display ike proposal
```

Priority	Authentication method	Authentication algorithm	Encryption algorithm	Diffie-Hellman group	Duration (seconds)
10	RSA-SIG	MD5	DES-CBC	Group 1	86400
default	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400

```
[DeviceB] display ike proposal
```

Priority	Authentication method	Authentication algorithm	Encryption algorithm	Diffie-Hellman group	Duration (seconds)
10	RSA-SIG	MD5	DES-CBC	Group 1	86400
default	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400

可通过如下显示信息查看到 Device A 上 IKE 第一阶段协商成功后生成的 IKE SA。

```
[DeviceA] display ike sa
```

Connection-ID	Remote	Flag	DOI
1	2.2.2.2	RD	IPsec

Flags:

```
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

可通过如下显示信息查看到 Device A 上 IKE 第二阶段协商生成的 IPsec SA。

```
[DeviceA] display ipsec sa
```

```
Interface: GigabitEthernet1/0/1
```

```
-----  
IPsec policy: map1  
Sequence number: 10  
Mode: ISAKMP  
-----
```

```
Tunnel id: 0  
Encapsulation mode: tunnel  
Perfect Forward Secrecy:  
Inside VPN:  
Extended Sequence Numbers enable: N
```

```
Traffic Flow Confidentiality enable: N
Path MTU: 1456
Tunnel:
    local address: 1.1.1.1
    remote address: 2.2.2.2
Flow:
    sour addr: 10.1.1.0/255.255.255.0 port: 0 protocol: ip
    dest addr: 10.1.2.0/255.255.255.0 port: 0 protocol: ip
[Inbound ESP SAs]
    SPI: 3264152513 (0xc28f03c1)
    Connection ID: 90194313219
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843200/3484
    Max received sequence-number:
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

[Outbound ESP SAs]
    SPI: 738451674 (0x2c03e0da)
    Connection ID: 64424509441
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843200/3484
    Max sent sequence-number:
    UDP encapsulation used for NAT traversal: N
    Status: Active
```

Device B 上也会产生相应的 IKE SA 和 IPsec SA，查看方式与 Device A 同，此处略。

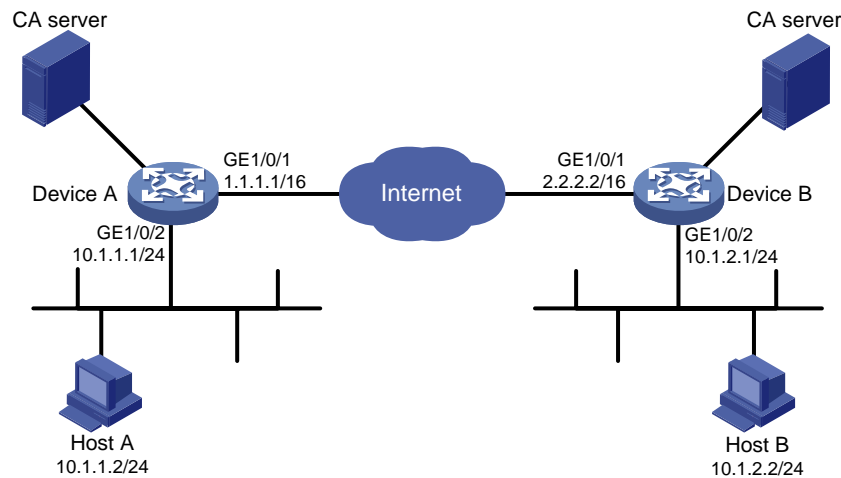
4 IKE 国密主模式及 SM2-DE 数字信封认证配置举例

4.1 组网需求

在 Device A 和 Device B 之间建立一个 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。

- Device A 和 Device B 之间采用 IKE 协商方式建立 IPsec SA。
- Device A 和 Device B 均使用 SM2-DE 数字信封的认证方法。
- IKE 第一阶段的协商模式为国密主模式。

图2 IKE 国密主模式及 SM2-DE 数字信封认证配置组网图



4.2 配置步骤



说明

在开始下面的配置之前，假设已完成如下配置：

- DeviceA 和 DeviceB 已获取到 CA 证书 ca.cer 和服务证书 server.pfx。

4.2.1 配置 Device A

配置各接口的 IP 地址，具体略。

配置 IPv4 高级 ACL 3101，定义要保护由子网 10.1.1.0/24 去子网 10.1.2.0/24 的数据流。

```
<DeviceA> system-view
[DeviceA] acl advanced 3101
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[DeviceA-acl-ipv4-adv-3101] quit
```

创建 IPsec 安全提议 tran1。

```
[DeviceA] ipsec transform-set tran1
# 配置安全协议对 IP 报文的封装形式为隧道模式。
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceA-ipsec-transform-set-tran1] protocol esp
# 配置 ESP 协议采用的加密算法为 SM4-CBC，认证算法为 SM3。
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm sm4-cbc
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sm3
[DeviceA-ipsec-transform-set-tran1] quit
```

创建 PKI 实体 entity1。

```

[DeviceA] pki entity entity1
# 配置 PKI 实体的通用名。
[DeviceA-pki-entity-entity1] common-name devicea
[DeviceA-pki-entity-entity1] quit
# 配置 PKI 域 domain1。
<DeviceA> system-view
[DeviceA] pki domain domain1
[DeviceA-pki-domain-domain1] public-key sm2 general name sm2-1
[DeviceA-pki-domain-domain1] undo crl check enable
[DeviceA-pki-domain-domain1] quit
# 导入 CA 证书 ca.cer 和服务证书 server.pfx。
[DeviceA] pki import domain domain1 der ca filename ca.cer
[DeviceA] pki import domain domain1 p12 local filename server.pfx
# 创建 IKE 提议 10。
[DeviceA] ike proposal 10
# 指定 IKE 提议使用的认证方法为 SM2-DE。
[DeviceA-ike-proposal-10] authentication-method sm2-de
# 指定 IKE 提议使用的认证算法为 SM3
[DeviceA-ike-proposal-10] authentication-algorithm sm3
# 指定 IKE 提议使用的加密算法为 SM4-CBC
[DeviceA-ike-proposal-10] encryption-algorithm sm4-cbc
[DeviceA-ike-proposal-10] quit
# 创建 IKE profile，名称为 profile1。
[DeviceA] ike profile profile1
# 配置第一阶段的协商模式为国密主模式。
[DeviceA-ike-profile-profile1] exchange-mode gm-main
# 配置 IKE 协商采用 SM2-DE 数字信封认证时使用的 PKI 域为 domain1。
[DeviceA-ike-profile-profile1] certificate domain domain1
# 配置引用序号为 10 的 IKE 安全提议。
[DeviceA-ike-profile-profile1] proposal 10
# 配置本端的身份信息为 IP 地址 1.1.1.1。
[DeviceA-ike-profile-profile1] local-identity address 1.1.1.1
# 配置匹配对端身份的规则为 IP 地址 2.2.2.2/16。
[DeviceA-ike-profile-profile1] match remote identity address 2.2.2.2 255.255.0.0
[DeviceA-ike-profile-profile1] quit
# 创建一条 IKE 协商方式的 IPsec 安全策略，名称为 map1，序号为 10。
[DeviceA] ipsec policy map1 10 isakmp
# 配置 IPsec 隧道的对端 IP 地址为 2.2.2.2。
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
# 指定引用 ACL 3101。
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3101
# 指定引用的安全提议为 tran1。
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
# 指定引用的 IKE profile 为 profile1。

```

```
[DeviceA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

在接口 GigabitEthernet1/0/1 上应用 IPsec 安全策略 map1。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy map1
[DeviceA-GigabitEthernet1/0/1] quit
```

配置到 Host B 所在子网的静态路由。1.1.1.2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 1.1.1.2
```

4.2.2 配置 Device B

配置各接口的 IP 地址，具体略。

配置 IPv4 高级 ACL 3101，定义要保护由子网 10.1.2.0/24 去往子网 10.1.1.0/24 的数据流。

```
<DeviceB> system-view
[DeviceB] acl advanced 3101
[DeviceB-acl-ipv4-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[DeviceB-acl-ipv4-adv-3101] quit
```

创建 IPsec 安全提议 tran1。

```
[DeviceB] ipsec transform-set tran1
# 配置安全协议对 IP 报文的封装形式为隧道模式。
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceB-ipsec-transform-set-tran1] protocol esp
# 配置 ESP 协议采用的加密算法为 SM4-CBC，认证算法为 SM3。
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm sm4-cbc
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sm3
[DeviceB-ipsec-transform-set-tran1] quit
```

创建 PKI 实体 entity2。

```
[DeviceB] pki entity entity2
# 配置 PKI 实体的通用名。
[DeviceB-pki-entity-entity2] common-name deviceb
[DeviceB-pki-entity-entity2] quit
```

配置 PKI 域 domain2。

```
<DeviceB> system-view
[DeviceB] pki domain domain2
[DeviceB-pki-domain-domain2] public-key sm2 general name sm2-1
[DeviceB-pki-domain-domain2] undo crl check enable
[DeviceB-pki-domain-domain2] quit
```

导入 CA 证书 ca.cer 和服务器证书 server.pfx。

```
[DeviceB] pki import domain domain2 der ca filename ca.cer
[DeviceB] pki import domain domain2 pl2 local filename server.pfx
```

创建 IKE 提议 10。

```
[DeviceB] ike proposal 10
```

```

# 指定 IKE 提议使用的认证方法为 SM2-DE。
[DeviceB-ike-proposal-10] authentication-method sm2-de
# 指定 IKE 提议使用的认证算法为 SM3
[DeviceB-ike-proposal-10] authentication-algorithm sm3
# 指定 IKE 提议使用的加密算法为 SM4-CBC
[DeviceB-ike-proposal-10] encryption-algorithm sm4-cbc
[DeviceB-ike-proposal-10] quit
# 创建 IKE profile，名称为 profile1。
[DeviceB] ike profile profile1
# 配置第一阶段的协商模式为国密主模式。
[DeviceB-ike-profile-profile1] exchange-mode gm-main
# 配置 IKE 协商采用 SM2-DE 数字信封认证时使用的 PKI 域为 domain2。
[DeviceB-ike-profile-profile1] certificate domain domain2
# 配置引用序号为 10 的 IKE 安全提议。
[DeviceB-ike-profile-profile1] proposal 10
# 配置本端的身份信息为 IP 地址 2.2.2.2。
[DeviceB-ike-profile-profile1] local-identity address 2.2.2.2
# 配置匹配对端身份的规则为 IP 地址 1.1.1.1/16。
[DeviceB-ike-profile-profile1] match remote identity address 1.1.1.1 255.255.0.0
[DeviceB-ike-profile-profile1] quit
# 创建一条 IKE 协商方式的 IPsec 安全策略，名称为 use1，顺序号为 10。
[DeviceB] ipsec policy use1 10 isakmp
# 配置 IPsec 隧道的对端 IP 地址为 1.1.1.1。
[DeviceB-ipsec-policy-isakmp-use1-10] remote-address 1.1.1.1
# 指定引用 ACL 3101。
[DeviceB-ipsec-policy-isakmp-use1-10] security acl 3101
# 指定引用的安全提议为 tran1。
[DeviceB-ipsec-policy-isakmp-use1-10] transform-set tran1
# 指定引用的 IKE profile 为 profile1。
[DeviceB-ipsec-policy-isakmp-use1-10] ike-profile profile1
[DeviceB-ipsec-policy-isakmp-use1-10] quit
# 在接口 GigabitEthernet1/0/1 上应用 IPsec 安全策略 use1。
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy use1
# 配置到 Host A 所在子网的静态路由。2.2.2.1 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 2.2.2.1

```

4.3 验证配置

以上配置完成后，Device A 和 Device B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKE 协商。

可通过如下显示信息查看到 Device A 和 Device B 上的 IKE 提议。

```
[DeviceA] display ike proposal
Priority Authentication Authentication Encryption Diffie-Hellman Duration
          method          algorithm  algorithm  group      (seconds)
-----
10      SM2-DE             SM3        SM4-CBC    Group 1    86400
default PRE-SHARED-KEY       SHA1       DES-CBC    Group 1    86400
```

```
[DeviceB] display ike proposal
Priority Authentication Authentication Encryption Diffie-Hellman Duration
          method          algorithm  algorithm  group      (seconds)
-----
10      SM2-DE             SM3        SM4-CBC    Group 1    86400
default PRE-SHARED-KEY       SHA1       DES-CBC    Group 1    86400
```

可通过如下显示信息查看到 Device A 上 IKE 第一阶段协商成功后生成的 IKE SA。

```
[DeviceA] display ike sa
Connection-ID Remote          Flag      DOI
-----
1           2.2.2.2          RD        IPsec
```

```
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

可通过如下显示信息查看到 IKE 第二阶段协商生成的 IPsec SA。

```
[DeviceA] display ipsec sa
-----
Interface: GigabitEthernet1/0/1
-----

IPsec policy: map1
Sequence number: 10
Mode: ISAKMP
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1456
Tunnel:
  local address: 1.1.1.1
  remote address: 2.2.2.2
Flow:
  sour addr: 10.1.1.0/255.255.255.0 port: 0 protocol: ip
  dest addr: 10.1.2.0/255.255.255.0 port: 0 protocol: ip
```

```
[Inbound ESP SAs]
SPI: 1451246811 (0x568044db)
Connection ID: 90194313219
```



```
Transform set: ESP-ENCRYPT-SM4-CBC ESP-AUTH-SM3
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active
```

[Outbound ESP SAs]

```
SPI: 2692887942 (0xa0823586)
Connection ID: 64424509441
Transform set: ESP-ENCRYPT-SM4-CBC ESP-AUTH-SM3
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max sent sequence-number:
UDP encapsulation used for NAT traversal: N
Status: Active
```

Device B 上也会产生相应的 IKE SA 和 IPsec SA，查看方式与 Device A 同，此处略。

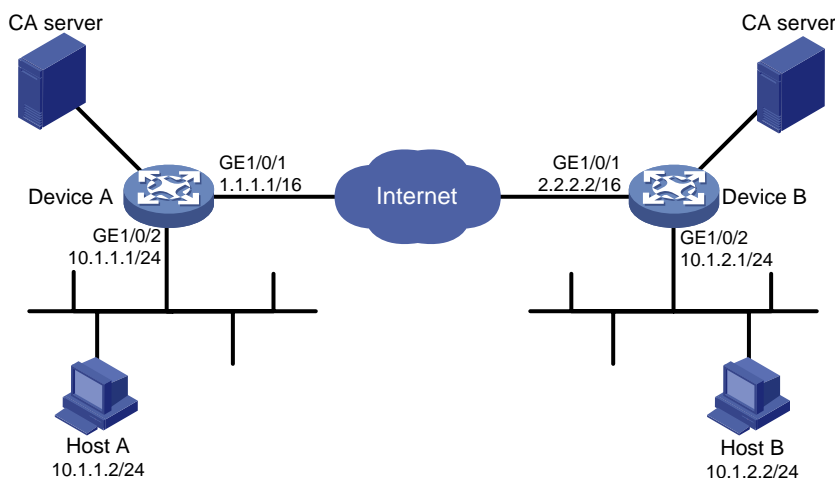
5 IKEv2 RSA 数字签名认证配置举例

5.1 组网需求

在 Device A 和 Device B 之间建立 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。

- Device A 和 Device B 之间采用 IKEv2 协商方式建立 IPsec SA。
- Device A 和 Device B 均使用 RSA 数字签名的认证方法。
- Device A 侧子网的 IP 地址为动态分配，并作为发起方。

图3 IKEv2 RSA 数字签名认证典型组网图



5.2 配置步骤



说明

在开始下面的配置之前，假设已完成如下配置：

- DeviceA 和 DeviceB 已获取到 CA 证书 ca.cer 和服务器证书 server.pfx。

5.2.1 配置 Device A

配置各接口的 IP 地址，具体略。

配置 ACL 3101，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
<DeviceA> system-view
[DeviceA] acl advanced 3101
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[DeviceA-acl-ipv4-adv-3101] quit
```

创建 IPsec 安全提议 tran1。

```
[DeviceA] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceA-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 DES，认证算法为 HMAC-SHA1。

```
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
```

创建 PKI 实体 entity1。

```
[DeviceA] pki entity entity1
```

配置 PKI 实体的通用名。

```
[DeviceA-pki-entity-entity1] common-name devicea
[DeviceA-pki-entity-entity1] quit
```

配置 PKI 域 domain1。

```
<DeviceA> system-view
[DeviceA] pki domain domain1
[DeviceA-pki-domain-domain1] public-key rsa general name rsa1
[DeviceA-pki-domain-domain1] undo crl check enable
[DeviceA-pki-domain-domain1] quit
```

导入 CA 证书 ca.cer 和服务器证书 server.pfx。

```
[DeviceA] pki import domain domain1 der ca filename ca.cer
[DeviceA] pki import domain domain1 p12 local filename server.pfx
```

配置证书访问策略 policy1。

```
<DeviceA> system-view
[DeviceA] pki certificate access-control-policy policy1
```

```

[DeviceA-pki-cert-acp-policy1] rule 1 permit group1
# 配置证书属性规则。
[DeviceA] pki certificate attribute-group group1
[DeviceA-pki-cert-attribute-group-group1] attribute 1 subject-name dn ctn 1
对端证书 subject-name DN 中需包含（ctn）规则中定义的字符串才被认为是有效的证书。本例使用的证书 subject-name DN 中包含字符“1”，因此在这里使用参数 ctn 1。
# 创建 IKEv2 profile，名称为 profile1。
[DeviceA] ikev2 profile profile1
# 指定本端的身份认证方式为 RSA 数字签名。
[DeviceA-ikev2-profile-profile1] authentication-method local rsa-signature
# 指定对端的身份认证方式为 RSA 数字签名。
[DeviceA-ikev2-profile-profile1] authentication-method remote rsa-signature
# 指定引用的 PKI 域为 domain1。
[DeviceA-ikev2-profile-profile1] certificate domain domain1
# 配置使用本端数字证书中获得的 DN 名作为本端身份标识。
[DeviceA-ikev2-profile-profile1] identity local dn
# 配置匹配对端身份规则为对端数字证书中的 DN 名。
[DeviceA-ikev2-profile-profile1] match remote certificate policy1
[DeviceA-ikev2-profile-profile1] quit
# 创建 IKEv2 提议 10。
[DeviceA] ikev2 proposal 10
# 指定 IKEv2 提议使用的完整性校验算法为 HMAC-MD5。
[DeviceA-ikev2-proposal-10] integrity md5
# 指定 IKEv2 提议使用的加密算法为 3DES。
[DeviceA-ikev2-proposal-10] encryption 3des-cbc
# 指定 IKEv2 提议使用的 DH group 为 group1。
[DeviceA-ikev2-proposal-10] dh group1
# 指定 IKEv2 提议使用的 PRF 算法为 HMAC-MD5。
[DeviceA-ikev2-proposal-10] prf md5
[DeviceA-ikev2-proposal-10] quit
# 创建 IKEv2 安全策略 1。
[DeviceA] ikev2 policy 1
# 指定引用的 IKEv2 proposal 10。
[DeviceA-ikev2-policy-1] proposal 10
[DeviceA-ikev2-policy-1] quit
# 创建一条 IKEv2 协商方式的 IPsec 安全策略，名称为 map1，序号为 10。
[DeviceA] ipsec policy map1 10 isakmp
# 配置 IPsec 隧道的对端 IP 地址为 2.2.2.2。
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
# 指定引用的安全提议为 tran1。
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
# 指定引用 ACL 3101。
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3101

```

指定引用的 IKEv2 profile 为 profile1。

```
[DeviceA-ipsec-policy-isakmp-map1-10] ikev2-profile profile1  
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

在接口 GigabitEthernet1/0/1 上应用 IPsec 安全策略 map1。

```
[DeviceA] interface gigabitethernet 1/0/1  
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy map1  
[DeviceA-GigabitEthernet1/0/1] quit
```

配置到 Host B 所在子网的静态路由。1.1.1.2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 1.1.1.2
```

5.2.2 配置 Device B

配置各接口的 IP 地址，具体略。

配置 ACL 3101，定义要保护由子网 10.1.2.0/24 去子网 10.1.1.0/24 的数据流。

```
[DeviceB] acl advanced 3101  
[DeviceB-acl-ipv4-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0  
0.0.0.255  
[DeviceB-acl-ipv4-adv-3101] quit
```

创建 IPsec 安全提议 tran1。

```
[DeviceB] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceB-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 DES，认证算法为 HMAC-SHA-1-96。

```
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc  
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1  
[DeviceB-ipsec-transform-set-tran1] quit
```

创建 PKI 实体 entity2。

```
[DeviceB] pki entity entity2
```

配置 PKI 实体的通用名。

```
[DeviceB-pki-entity-entity2] common-name deviceb  
[DeviceB-pki-entity-entity2] quit
```

配置 PKI 域 domain2。

```
<DeviceB> system-view  
[DeviceB] pki domain domain2  
[DeviceB-pki-domain-domain2] public-key rsa general name rsa1  
[DeviceB-pki-domain-domain2] undo crl check enable  
[DeviceB-pki-domain-domain2] quit
```

导入 CA 证书 ca.cer 和服务器证书 server.pfx。

```
[DeviceB] pki import domain domain2 der ca filename ca.cer  
[DeviceB] pki import domain domain2 p12 local filename server.pfx
```

配置证书访问策略 policy1。

```
<DeviceB> system-view
```

```

[DeviceB] pki certificate access-control-policy policy1
[DeviceB-pki-cert-acp-policy1] rule 1 permit group1
# 配置证书属性规则。
[DeviceB] pki certificate attribute-group group1
[DeviceB-pki-cert-attribute-group-group1] attribute 1 subject-name dn ctn 1
对端证书 subject-name DN 中需包含 (ctn) 规则中定义的字符串才被认为是有效的证书。本例使用的证书 subject-name DN 中包含字符 “1”，因此在这里使用参数 ctn 1。
# 创建 IKEv2 profile，名称为 profile2。
[DeviceB] ikev2 profile profile2
# 指定本端的身份认证方式为 RSA 数字签名。
[DeviceB-ikev2-profile-profile2] authentication-method local rsa-signature
# 指定对端的身份认证方式为 RSA 数字签名。
[DeviceB-ikev2-profile-profile2] authentication-method remote rsa-signature
# 配置使用本端数字证书中获得的 DN 名作为本端身份标识。
[DeviceB-ikev2-profile-profile2] identity local dn
# 配置匹配对端身份规则为对端数字证书中的 DN 名。
[DeviceB-ikev2-profile-profile2] match remote certificate policy1
[DeviceB-ikev2-profile-profile2] quit
# 创建 IKEv2 提议 10。
[DeviceB] ikev2 proposal 10
# 指定 IKEv2 提议使用的完整性校验算法为 HMAC-MD5。
[DeviceB-ikev2-proposal-10] integrity md5
# 指定 IKEv2 提议使用的加密算法为 3DES。
[DeviceB-ikev2-proposal-10] encryption 3des-cbc
# 指定 IKEv2 提议使用的 DH group 为 group1。
[DeviceB-ikev2-proposal-10] dh group1
# 指定 IKEv2 提议使用的 PRF 算法为 HMAC-MD5。
[DeviceB-ikev2-proposal-10] prf md5
[DeviceB-ikev2-proposal-10] quit
# 创建 IKEv2 安全策略 1。
[DeviceB] ikev2 policy 1
# 指定引用的 IKEv2 proposal 10。
[DeviceB-ikev2-policy-1] proposal 10
[DeviceB-ikev2-policy-1] quit
# 创建一条 IPsec 安全策略模板，名称为 template1，顺序号为 1。
[DeviceB] ipsec policy-template template1 1
# 配置 IPsec 隧道的对端 IP 地址为 1.1.1.1。
[DeviceB-ipsec-policy-template-templatel-1] remote-address 1.1.1.1
# 指定引用 ACL 3101。
[DeviceB-ipsec-policy-template-templatel-1] security acl 3101
# 指定引用的安全提议为 tran1。
[DeviceB-ipsec-policy-template-templatel-1] transform-set tran1
# 指定引用的 IKEv2 profile 为 profile2。

```

```
[DeviceB-ipsec-policy-template-templatel-1] ikev2-profile profile2
[DeviceB-ipsec-policy-template-templatel-1] quit
# 引用 IPsec 安全策略模板创建一条 IPsec 安全策略，名称为 use1，顺序号为 1。
[DeviceB] ipsec policy use1 1 isakmp template templatel
# 在接口 GigabitEthernet1/0/1 上应用 IPsec 安全策略 use1。
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy use1
[DeviceB-GigabitEthernet1/0/1] quit
# 配置到 Host A 所在子网的静态路由。2.2.2.1 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 2.2.2.1
```

5.3 验证配置

以上配置完成后，Device A 和 Device B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKEv2 协商。

可通过如下显示信息查看到 Device A 和 Device B 上的 IKEv2 提议。

```
[DeviceA] display ikev2 proposal 10
IKEv2 proposal : 10
  Encryption : 3DES-CBC
  Integrity : MD5
  PRF : MD5
  DH Group : MODP768/Group1
[DeviceB] display ikev2 proposal 10
IKEv2 proposal : 10
  Encryption : 3DES-CBC
  Integrity : MD5
  PRF : MD5
  DH Group : MODP768/Group1
```

可通过如下显示信息查看到 Device A 和 Device B 上的 IKEv2 安全策略。

```
[DeviceA] display ikev2 policy 1
IKEv2 policy : 1
  Priority: 100
  Match Local : any
  Match VRF : public
  Proposal : 10
[DeviceB] display ikev2 policy 1
IKEv2 policy : 1
  Priority: 100
  Match Local : any
  Match VRF : public
  Proposal : 10
```

可通过如下显示信息查看到 Device A 上 IKEv2 协商成功后生成的 IKEv2 SA。

```
[DeviceA] display ikev2 sa
Tunnel ID   Local                               Remote                               Status
-----
```

```

1          1.1.1.1/500          2.2.2.2/500          EST
Status:
IN-NEGO: Negotiating, EST: Established, DEL:Deleting
# 可通过如下显示信息查看到 Device A 上 IKEv2 协商生成的 IPsec SA。
[DeviceA] display ipsec sa
-----
Interface: GigabitEthernet1/0/1
-----

-----
IPsec policy: map1
Sequence number: 10
Mode: ISAKMP
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1456
Tunnel:
    local address: 1.1.1.1
    remote address: 2.2.2.2
Flow:
    sour addr: 10.1.1.0/255.255.255.0   port: 0   protocol: ip
    dest addr: 10.1.2.0/255.255.255.0   port: 0   protocol: ip

[Inbound ESP SAs]
SPI: 3264152513 (0xc28f03c1)
Connection ID: 141733920771
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max received sequence-number:
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 738451674 (0x2c03e0da)
Connection ID: 141733920770
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843200/3484
Max sent sequence-number:
UDP encapsulation used for NAT traversal: N

```

Status: Active

Device B 上也会产生相应的 IKEv2 SA 和 IPsec SA，并自动获取 CA 证书，自动申请本地证书，查看方式与 Device A 同，此处略。