华为职业认证通过者权益

获得华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- 1、华为e-learning 课程学习：登录*华为在线学习网站*，进入“*华为培训/在线学习*”栏目
  - **通过HCNA和HCNP认证：**可获得职业认证及基础类产品技术e-Learning课程权限
  - **通过HCIE认证：**可获得所有华为HCIE用户类e-Learning课程权限
  - **HCIE用户权限获取方式**：请提交您关联证书的“华为账号” 到 *Learning@huawei.com 申请权限*
- 2、华为培训教材下载
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。
- 3、华为在线公开课(LVC)优先参与
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证及产品技术培训课程，华为讲师授课
  - **方式**：开班计划请访问*华为LVC公开课*页面
- 4、学习工具 下载
  - *eNSP*：可扩展的、图形化网络仿真工具，可以实现网络设备的仿真模拟
  - *WLAN Planner*：室内放装AP的网络规划工具
  - *eDesk*：企业数通和安全设备运维管理平台，提供巡检、排障、补丁等功能
  - *HedEx Lite*：华为产品文档管理工具，支持浏览、搜索、升级和管理产品资料
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。

华为认证系列教程

HCNP-IENP
提升企业级网络性能
实验指导书

华为技术有限公司

版权声明

华为认证系列教程

HCNP-IENP提升企业级网络性能

实验指导书

第2.0版本

华为认证体系介绍

华为认证是华为凭借多年信息通信技术人才培养经验及对行业发展的深刻理解 ,基于ICT产业链人才职业发展生命周期 ,以学院化的职业技术认证为指引，搭载华为“云 - 管 - 端”融合技术，推出覆盖IP、IT、CT技术领域的认证体系，是业界唯一的ICT全技术领域认证体系。

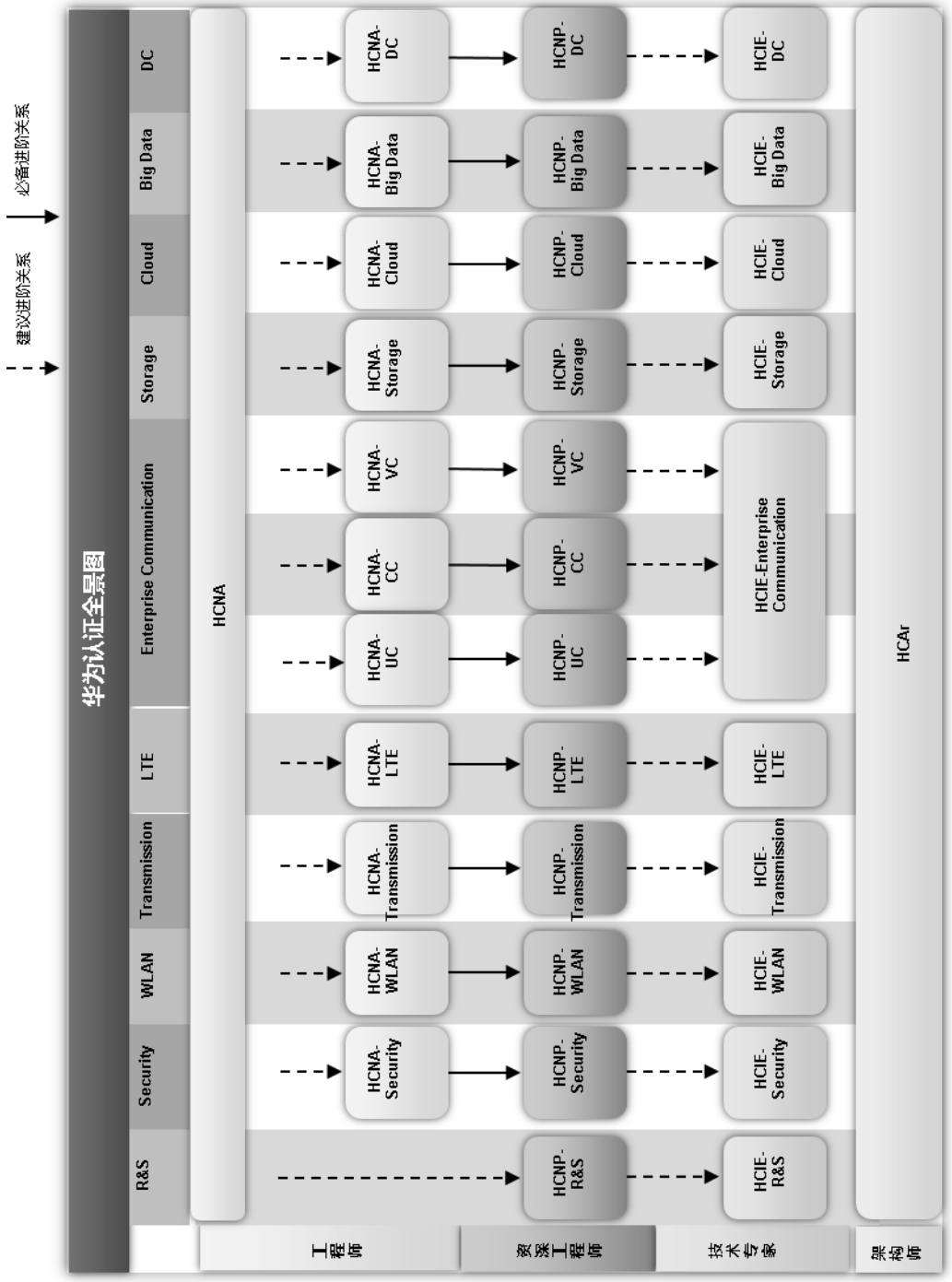
基于IP、IT、CT技术，华为公司提供了工程师、资深工程师和专家三类技术认证等级，为ICT从业者提供了层次化的培训认证。华为认证包括10个领域，12个技术方向的认证，是业界唯一覆盖ICT全技术领域的认证体系。

HCNA 是对企业网络初级知识和技能的认证。证明您具备配置和维护小型企业网络的能力。 HCNA 认证考查工程师协助设计、部署小型企业网络和基本网络运维的能力。目的是考察企业网络工程师使用华为网络设备搭建小型企业路由交换网络的能力，使之能承载基本的语音、无线、云、安全和存储等网络应用，满足企业对网络的使用需求。 HCNA 定位于企业网络技术领域具备初级知识和技能水平的专业人士。侧重于对初级企业网络技术的考察和认证。具备 HCNA 证书的工程师是公认的具备小型企业网络通用技术和基本设计能力的专业人士。

HCNP-R&S 是对企业网络高级知识和技能的认证。目的是帮助企业网络工程师使用华为网络设备搭建完整的中小型企业网络，并支撑企业所需的语音、无线、云、安全和存储等应用全面地集成到网络之中，满足企业各种应用对网络的使用需求，并提供较高的安全性、可用性和可靠性。HCNP-R&S 定位于企业网络技术领域具备高级知识和技能水平的专业人士。侧重于对中小型企业网络技术的考察和认证。具备 HCNP-R&S 证书的工程师是公认的具备中小型企业网络构建和管理能力的专业人士。

HCIE-R&S 是对企业网络专家级知识和技能的认证。目的是帮助企业网络高级工程师搭建完整的大型复杂企业网络，支撑企业所需的语音、无线、云、安全和存储等应用全面集成到网络之中，满足企业各种应用对网络的使用需求。同时能够提供完整的故障排除能力，可根据企业和网络技术发展来规划企业网络，并提高安全性、可用性和可靠性。HCIE-R&S 定位于企业网络技术领域中具备专家知识和技能水平的专业人士。侧重于对大型复杂企业网络技术的考察和认证。具备 HCIE-R&S 证书的工程师是公认的具备大型复杂企业网络构建、优化和管理能力的专业人士。

华为认证协助您打开行业之窗 ,开启改变之门 ,屹立在ICT世界的潮头浪尖！


必备进阶关系
建议进阶关系
华为认证全景图
R&S
Security
WLAN
Transmission
LTE
Enterprise Communication
Storage
Cloud
Big Data
DC
HCNA
HCNA-Security
HCNA-WLAN
HCNA-Transmission
HCNA-LTE
HCNA-UC
HCNA-CC
HCNA-VC
HCNA-Storage
HCNA-Cloud
HCNA-Big Data
HCNA-DC
HCNP-R&S
HCNP-Security
HCNP-WLAN
HCNP-Transmission
HCNP-LTE
HCNP-UC
HCNP-CC
HCNP-VC
HCNP-Storage
HCNP-Cloud
HCNP-Big Data
HCNP-DC
HCIE-R&S
HCIE-Security
HCIE-WLAN
HCIE-Transmission
HCIE-LTE
HCIE-Enterprise Communication
HCIE-Storage
HCIE-Cloud
HCIE-Big Data
HCIE-DC
HCAr
工程师
资深工程师
技术专家
架构师

华为认证全景图

前言

简介

本书为HCNP-IENP认证培训教程，适用于准备参加HCNP-IENP考试的学员，帮助学员系统掌握提升企业级网络性能的相关技术及其在华为通用路由平台VRP上的实现。

内容描述

Module 1系统介绍了MPLS和MPLS VPN技术的原理及配置，帮助读者掌握提升企业网络业务承载能力的方法。

Module 2、3、4、5、6详细介绍了DHCP、QoS技术、网络基础安全、VRRP、BFD的原理与配置方法，帮助读者全面深入地掌握提升企业网络服务质量和增强企业网络安全与高可靠性的相关理论与实践。

本书引导读者循序渐进地掌握路由技术在华为产品中的实现，读者也可以根据自身情况选择感兴趣的章节阅读。

读者知识背景

为了更好地掌握本书内容，阅读本书的读者应首先具备以下基本条件之一：

1) 参加过HCNA培训

2) 通过HCNA考试

3) 熟悉TCP/IP协议栈工作原理，熟悉IP地址

本书常用图标

路由器

三层交换机

二层交换机

防火墙

网云

以太网线缆

串行线缆

实验环境说明

组网介绍

本实验环境面向准备HCNP-IENP考试的网络工程师，实验设备包括路由器5台，交换机4台，防火墙1台。每套实验环境适用于2名学员同时上机操作。

设备介绍

为了满足HCNP-IENP实验需要，建议每套实验环境采用以下配置：

设备名称、型号与版本的对应关系如下：

设备名称	设备型号	软件版本
R1	AR 2220E	V2R7
R2	AR 2220E	V2R7
R3	AR 2220E	V2R7
R4	AR 2220E	V2R7
R5	AR 2220E	V2R7
S1	S5720-36C-EI-AC	V2R8
S2	S5720-36C-EI-AC	V2R8
S3	S3700-28TP-EI-AC	V1R6C5
S4	S3700-28TP-EI-AC	V1R6C5
FW1	USG6330	V100R001C30

目录

第一章 MPLS VPN配置 1

实验 1-1 MPLS LDP配置 1

实验 1-2 MPLS VPN配置 16

第二章 DHCP特性与配置 33

实验 2-1 DHCP配置 33

第三章 服务质量与流量控制 53

实验 3-1 QoS基础 53

实验 3-2 使用流策略实现流行为控制 73

第四章 防火墙 90

实验 4-1防火墙安全区域及安全策略配置 90

实验 4-2防火墙NAT配置 105

第五章 VRRP协议特性与配置 122

实验 5-1 VRRP配置实验 122

第六章 BFD特性与配置 146

实验 6-1 BFD与静态路由联动配置实验 146

实验 6-2 BFD与OSPF联动配置实验 159

实验 6-3 BFD与VRRP联动配置实验 167

第一章 MPLS VPN配置

实验 1-1 MPLS LDP 配置

学习目的

- 掌握启用和关闭MPLS的方法
- 掌握启用和关闭MPLS LDP配置的方法
- 掌握使用MPLS LDP配置LSP的方法
- 掌握在MPLS路由器上配置LDP LSP触发策略的方法

拓扑图

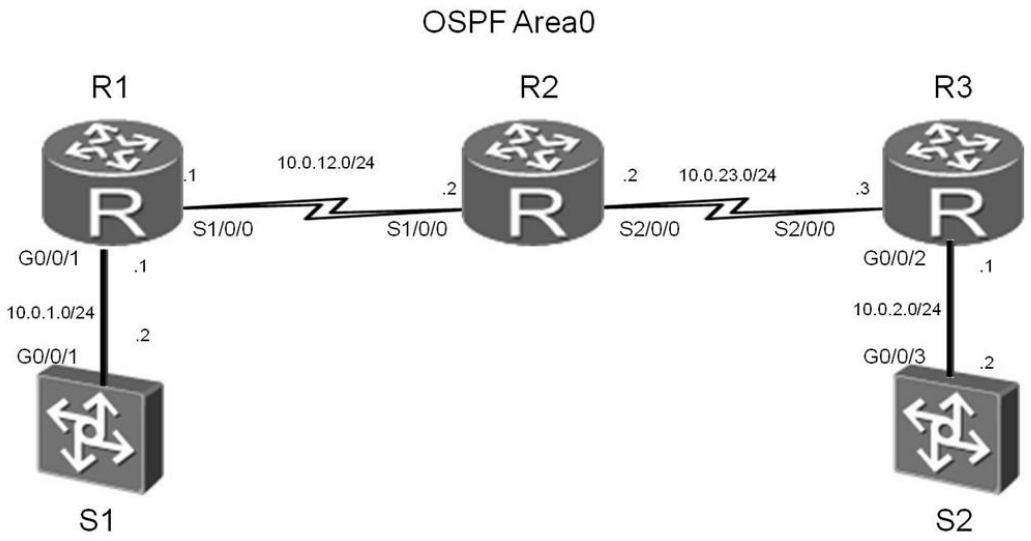


图3-1. MPLS LDP实验拓扑图

场景

你是公司的网络管理员。公司的网络采用了IP网络，为解决IP网络转发性能低下问题，决定使用MPLS技术来提高路由器的转发速度。而静态LSP由管理员

手工配置，LDP是专为标签发布而制定的标签分发协议,为了配置灵活采用LDP来建立MPLS LSP。

学习任务

步骤一. 基本配置与 IP 编址

给所有路由器配置IP地址和掩码。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname S1
[S1]interface Vlanif 1
[S1-Vlanif1]ip address 10.0.1.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.1.1 24
[R1-GigabitEthernet0/0/1]quit
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 24
[R1-Serial1/0/0]quit
[R1]interface loopback 0
[R1-LoopBack0]ip address 2.2.2.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 24
[R2-Serial1/0/0]quit
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]ip address 10.0.23.2 24
[R2-Serial2/0/0]quit
[R2]interface loopback 0
[R2-LoopBack0]ip address 3.3.3.3 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
```

```
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.2.1 24
[R3-GigabitEthernet0/0/2]quit
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ip address 10.0.23.3 24
[R3-Serial2/0/0]quit
[R3]interface loopback 0
[R3-LoopBack0]ip address 4.4.4.4 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname S2
[S2]interface Vlanif 1
[S2-Vlanif1]ip address 10.0.2.2 24
```

配置完成后，请自行测试直连链路的连通性。

步骤二. 配置单区域 OSPF

配置10.0.12.0/24、10.0.23.0/24、10.0.1.0/24、10.0.2.0/24四个网段属于OSPF区域0。

```
[S1]ospf 1 router-id 1.1.1.1
[S1-ospf-1]area 0
[S1-ospf-1-area-0.0.0.0]network 10.0.1.0 0.0.0.255

[R1]ospf 1 router-id 2.2.2.2
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 2.2.2.0 0.0.0.255

[R2]ospf 1 router-id 3.3.3.3
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 3.3.3.0 0.0.0.255


[R3]ospf 1 router-id 4.4.4.4
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255
```

```
[R3-ospf-1-area-0.0.0.0]network 10.0.2.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 4.4.4.0 0.0.0.255

[S2]ospf 1 router-id 5.5.5.5
[S2-ospf-1]area 0
[S2-ospf-1-area-0.0.0.0]network 10.0.2.0 0.0.0.255
```

配置完成后，查看设备的路由表，并测试全网的连通性。

```
[R2]ping 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=253 time=36 ms
    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=253 time=31 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=253 time=31 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=253 time=31 ms
    Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=253 time=31 ms

  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 31/32/36 ms

[R2]ping 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=253 time=38 ms
    Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=253 time=33 ms
    Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=253 time=33 ms
    Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=253 time=33 ms
    Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=253 time=33 ms

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 33/34/38 ms
```

使用display ip routing-table命令查看各路由器OSPF路由表。

```
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 19        Routes : 19
```

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

        2.2.2.2/32  OSPF    10   1562        D   10.0.12.1       Serial1/0/0
        3.3.3.0/24  Direct  0    0           D   3.3.3.3         LoopBack0
        3.3.3.3/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      3.3.3.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        4.4.4.4/32  OSPF    10   1562        D   10.0.23.3       Serial2/0/0
       10.0.1.0/24  OSPF    10   1563        D   10.0.12.1       Serial1/0/0
       10.0.2.0/24  OSPF    10   1563        D   10.0.23.3       Serial2/0/0
      10.0.12.0/24  Direct  0    0           D   10.0.12.2       Serial1/0/0
      10.0.12.1/32  Direct  0    0           D   10.0.12.1       Serial1/0/0
      10.0.12.2/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    10.0.12.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      10.0.23.0/24  Direct  0    0           D   10.0.23.2       Serial2/0/0
      10.0.23.2/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      10.0.23.3/32  Direct  0    0           D   10.0.23.3       Serial2/0/0
    10.0.23.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

步骤三. MPLS LDP 配置

在各MPLS路由器上配置全局MPLS和LDP。

```
[R1]mpls lsr-id 2.2.2.2
[R1]mpls
Info: Mpls starting, please wait... OK!
[R1-mpls]mpls ldp

[R2]mpls lsr-id 3.3.3.3
[R2]mpls
Info: Mpls starting, please wait... OK!
[R2-mpls]mpls ldp

[R3]mpls lsr-id 4.4.4.4
[R3]mpls
Info: Mpls starting, please wait... OK!
[R3-mpls]mpls ldp
```

在各MPLS路由器接口上配置MPLS和LDP。

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]mpls
[R1-Serial1/0/0]mpls ldp

[R2]interface Serial 1/0/0
[R2-Serial1/0/0]mpls
[R2-Serial1/0/0]mpls ldp
[R2-Serial1/0/0]quit
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]mpls
[R2-Serial2/0/0]mpls ldp

[R3]interface Serial 2/0/0
[R3-Serial2/0/0]mpls
[R3-Serial2/0/0]mpls ldp
```

配置完成后，在节点上执行display mpls ldp session命令，可以看到R1和R2和R3之间的本地LDP会话状态为“Operational”。

```
[R1]display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID           Status     LAM  SsnRole  SsnAge     KASent/Rcv
 ------------------------------------------------------------------------------
 3.3.3.3:0        Operational DU   Passive  0000:00:10  41/41
 ------------------------------------------------------------------------------
TOTAL: 1 session(s) Found.

[R2]display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID           Status     LAM  SsnRole  SsnAge     KASent/Rcv
 ------------------------------------------------------------------------------
 2.2.2.2:0        Operational DU   Active   0000:00:11  46/46
 4.4.4.4:0        Operational DU   Passive  0000:00:10  43/43
 ------------------------------------------------------------------------------
 TOTAL: 2 session(s) Found.
```

```
[R3]display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID           Status     LAM  SsnRole  SsnAge     KASent/Rcv
 ------------------------------------------------------------------------------
 3.3.3.3:0        Operational DU   Active   0000:00:11  46/46
 ------------------------------------------------------------------------------
 TOTAL: 1 session(s) Found.
```

步骤四. LDP 建立 LSP

在配置完成后，各MPLS路由器已根据默认的LDP触发策略建立LSP，即所有主机路由触发建立LDP LSP。

在各MPLS路由器上执行display mpls ldp lsp命令，可以看到所有主机路由都触发建立了LDP LSP。

```
[R1]display mpls ldp lsp
  LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop        OutInterface
 ------------------------------------------------------------------------------
 2.2.2.2/32         3/NULL          3.3.3.3        127.0.0.1       InLoop0
*2.2.2.2/32         Liberal/1024                   DS/3.3.3.3
 3.3.3.3/32         NULL/3          -              10.0.12.2       S1/0/0
 3.3.3.3/32         1024/3          3.3.3.3        10.0.12.2       S1/0/0
 4.4.4.4/32         NULL/1025       -              10.0.12.2       S1/0/0
 4.4.4.4/32         1025/1025       3.3.3.3        10.0.12.2       S1/0/0
 ------------------------------------------------------------------------------
 TOTAL: 5 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP
```

```
[R2]display mpls ldp lsp
 LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop        OutInterface
 ------------------------------------------------------------------------------
 2.2.2.2/32         NULL/3         -              10.0.12.1      S1/0/0
 2.2.2.2/32         1024/3         2.2.2.2         10.0.12.1      S1/0/0
 2.2.2.2/32         1024/3         4.4.4.4         10.0.12.1      S1/0/0
*2.2.2.2/32         Liberal/1024                   DS/4.4.4.4
 3.3.3.3/32         3/NULL         2.2.2.2         127.0.0.1      InLoop0
 3.3.3.3/32         3/NULL         4.4.4.4         127.0.0.1      InLoop0
*3.3.3.3/32         Liberal/1024                   DS/2.2.2.2
*3.3.3.3/32         Liberal/1025                   DS/4.4.4.4
 4.4.4.4/32         NULL/3         -              10.0.23.3      S2/0/0
 4.4.4.4/32         1025/3         2.2.2.2         10.0.23.3      S2/0/0
 4.4.4.4/32         1025/3         4.4.4.4         10.0.23.3      S2/0/0
*4.4.4.4/32         Liberal/1025                   DS/2.2.2.2
 ------------------------------------------------------------------------------
 TOTAL: 8 Normal LSP(s) Found.
 TOTAL: 4 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP


[R3]display mpls ldp lsp
  LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop        OutInterface
 ------------------------------------------------------------------------------
 2.2.2.2/32         NULL/1024      -              10.0.23.2      S2/0/0
 2.2.2.2/32         1024/1024      3.3.3.3         10.0.23.2      S2/0/0
 3.3.3.3/32         NULL/3         -              10.0.23.2      S2/0/0
 3.3.3.3/32         1025/3         3.3.3.3         10.0.23.2      S2/0/0
 4.4.4.4/32         3/NULL         3.3.3.3         127.0.0.1      InLoop0
*4.4.4.4/32         Liberal/1025                   DS/3.3.3.3
 ------------------------------------------------------------------------------
 TOTAL: 5 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
```

```
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP
```

通常情况下，使用缺省的触发策略，即由“host”方式触发建立LDP LSP。

在各MPLS路由器上将LDP LSP的触发策略修改为all，使路由表中的所有静态路由和IGP表项都可以触发建立LDP LSP。

```
[R1]mpls
[R1-mpls]lsp-trigger all

[R2]mpls
[R2-mpls]lsp-trigger all

[R3]mpls
[R3-mpls]lsp-trigger all
```

配置完成后，在各节点上执行display mpls ldp lsp命令，可以看到LDP LSP的建立情况。

```
[R1]display mpls ldp lsp
  LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop        OutInterface
 ------------------------------------------------------------------------------
 2.2.2.0/24        3/NULL          3.3.3.3        2.2.2.2        Loop0
 2.2.2.2/32        3/NULL          3.3.3.3        127.0.0.1      InLoop0
*2.2.2.2/32        Liberal/1024                   DS/3.3.3.3
*3.3.3.0/24        Liberal/3                     DS/3.3.3.3
 3.3.3.3/32        NULL/3          -              10.0.12.2      S1/0/0
 3.3.3.3/32        1024/3          3.3.3.3        10.0.12.2      S1/0/0
 4.4.4.4/32        NULL/1025       -             10.0.12.2      S1/0/0
 4.4.4.4/32        1025/1025       3.3.3.3        10.0.12.2      S1/0/0
 10.0.1.0/24       3/NULL          3.3.3.3       10.0.1.1       GE0/0/1
*10.0.1.0/24       Liberal/1026                  DS/3.3.3.3
 10.0.2.0/24       NULL/1027       -              10.0.12.2      S1/0/0
 10.0.2.0/24       1027/1027      3.3.3.3        10.0.12.2      S1/0/0
 10.0.12.0/24      3/NULL         3.3.3.3        10.0.12.1      S1/0/0
*10.0.12.0/24      Liberal/3                      DS/3.3.3.3
 10.0.23.0/24      NULL/3          -             10.0.12.2      S1/0/0
 10.0.23.0/24      1026/3         3.3.3.3        10.0.12.2      S1/0/0
 ------------------------------------------------------------------------------
```

```
 TOTAL: 12 Normal LSP(s) Found.
 TOTAL: 4 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP

[R2]display mpls ldp lsp
  LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop        OutInterface
 ------------------------------------------------------------------------------
*2.2.2.0/24        Liberal/3                  DS/2.2.2.2
 2.2.2.2/32        NULL/3         -           10.0.12.1      S1/0/0
 2.2.2.2/32        1024/3         2.2.2.2      10.0.12.1      S1/0/0
 2.2.2.2/32        1024/3         4.4.4.4      10.0.12.1      S1/0/0
*2.2.2.2/32        Liberal/1024               DS/4.4.4.4
 3.3.3.0/24        3/NULL         2.2.2.2      3.3.3.3        Loop0
 3.3.3.0/24        3/NULL         4.4.4.4      3.3.3.3        Loop0
 3.3.3.3/32        3/NULL         2.2.2.2      127.0.0.1      InLoop0
 3.3.3.3/32        3/NULL         4.4.4.4      127.0.0.1      InLoop0
*3.3.3.3/32        Liberal/1024               DS/2.2.2.2
*3.3.3.3/32        Liberal/1025               DS/4.4.4.4
*4.4.4.0/24        Liberal/3                  DS/4.4.4.4
 4.4.4.4/32        NULL/3         -           10.0.23.3      S2/0/0
 4.4.4.4/32        1025/3         2.2.2.2      10.0.23.3      S2/0/0
 4.4.4.4/32        1025/3         4.4.4.4      10.0.23.3      S2/0/0
*4.4.4.4/32        Liberal/1025               DS/2.2.2.2
 10.0.1.0/24       NULL/3         -           10.0.12.1      S1/0/0
 10.0.1.0/24       1026/3         2.2.2.2      10.0.12.1      S1/0/0
 10.0.1.0/24       1026/3         4.4.4.4      10.0.12.1      S1/0/0
*10.0.1.0/24       Liberal/1026               DS/4.4.4.4
 10.0.2.0/24       NULL/3         -           10.0.23.3      S2/0/0
 10.0.2.0/24       1027/3         2.2.2.2      10.0.23.3      S2/0/0
 10.0.2.0/24       1027/3         4.4.4.4      10.0.23.3      S2/0/0
*10.0.2.0/24       Liberal/1027               DS/2.2.2.2
 10.0.12.0/24      3/NULL         2.2.2.2      10.0.12.2      S1/0/0
 10.0.12.0/24      3/NULL         4.4.4.4      10.0.12.2      S1/0/0
*10.0.12.0/24      Liberal/3                  DS/2.2.2.2
*10.0.12.0/24      Liberal/1027               DS/4.4.4.4
 10.0.23.0/24      3/NULL         2.2.2.2      10.0.23.2      S2/0/0
```

```
 10.0.23.0/24      3/NULL        4.4.4.4        10.0.23.2      S2/0/0
*10.0.23.0/24      Liberal/1026                 DS/2.2.2.2
*10.0.23.0/24      Liberal/3                    DS/4.4.4.4
 ------------------------------------------------------------------------------
 TOTAL: 20 Normal LSP(s) Found.
 TOTAL: 12 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP

[R3]display mpls ldp lsp
  LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel   UpstreamPeer    NextHop        OutInterface
 ------------------------------------------------------------------------------
 2.2.2.2/32        NULL/1024     -              10.0.23.2      S2/0/0
 2.2.2.2/32        1024/1024     3.3.3.3         10.0.23.2      S2/0/0
*3.3.3.0/24        Liberal/3                    DS/3.3.3.3
 3.3.3.3/32        NULL/3        -              10.0.23.2      S2/0/0
 3.3.3.3/32        1025/3        3.3.3.3         10.0.23.2      S2/0/0
 4.4.4.0/24        3/NULL        3.3.3.3         4.4.4.4        Loop0
 4.4.4.4/32        3/NULL        3.3.3.3         127.0.0.1      InLoop0
*4.4.4.4/32        Liberal/1025                 DS/3.3.3.3
 10.0.1.0/24       NULL/1026     -              10.0.23.2      S2/0/0
 10.0.1.0/24       1026/1026     3.3.3.3         10.0.23.2      S2/0/0
 10.0.2.0/24       3/NULL        3.3.3.3         10.0.2.1       GE0/0/2
*10.0.2.0/24       Liberal/1027                 DS/3.3.3.3
 10.0.12.0/24      NULL/3        -              10.0.23.2      S2/0/0
 10.0.12.0/24      1027/3        3.3.3.3         10.0.23.2      S2/0/0
 10.0.23.0/24      3/NULL        3.3.3.3         10.0.23.3      S2/0/0
*10.0.23.0/24      Liberal/3                    DS/3.3.3.3
 ------------------------------------------------------------------------------
 TOTAL: 12 Normal LSP(s) Found.
 TOTAL: 4 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
```

```
 A '*' before a NextHop means the LSP is FRR LSP
```

步骤五. LDP Inbound 策略配置

R1性能较低，如果不对R1收到的标签进行控制，则会建立大量的LSP，消耗大量内存，R1无法承受。

配置LDP Inbound策略，R1只接收到达R2的标签映射消息，使R1只建立到R2的LSP，从而减少资源的浪费。

在R1上执行display mpls lsp命令，查看已经建立的LSP。

```
[R1]display mpls lsp
------------------------------------------------------------------------------
              LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC              In/Out Label  In/Out IF                    Vrf Name
3.3.3.3/32        NULL/3       -/S1/0/0
3.3.3.3/32        1024/3       -/S1/0/0
2.2.2.2/32        3/NULL       -/-
4.4.4.4/32        NULL/1025    -/S1/0/0
4.4.4.4/32        1025/1025    -/S1/0/0
10.0.12.0/24      3/NULL       -/-
10.0.1.0/24       3/NULL       -/-
2.2.2.0/24        3/NULL       -/-
10.0.23.0/24      NULL/3       -/S1/0/0
10.0.23.0/24      1026/3       -/S1/0/0
10.0.2.0/24       NULL/1027    -/S1/0/0
10.0.2.0/24       1027/1027    -/S1/0/0
```

可以看到R1上建立了到R2、R3的LSP。在R1上配置Inbound策略，只允许到R2的路由通过。

```
[R1]ip ip-prefix prefix1 permit 10.0.12.0 24
[R1]mpls ldp
[R1-mpls-ldp]inbound peer 3.3.3.3 fec ip-prefix prefix1
[R1-mpls-ldp]quit
[R1]display mpls lsp
------------------------------------------------------------------------------
              LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC              In/Out Label  In/Out IF                    Vrf Name
2.2.2.2/32        3/NULL       -/-
10.0.12.0/24      3/NULL       -/-
```

```
10.0.1.0/24       3/NULL       -/-
2.2.2.0/24        3/NULL       -/-
```

附加实验：思考并验证

思考一下，步骤五中如果想在R1上只接收R1到R3的标签映射信息该怎么解决？

最终设备配置

```
<S1>display current-configuration
!Software Version V200R008C00SPC500
#
sysname S1
#
interface Vlanif1
 ip address 10.0.1.2 255.255.255.0
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
#
return
```

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
mpls lsr-id 2.2.2.2
 mpls
  lsp-trigger all
#
mpls ldp
 inbound peer 3.3.3.3 fec ip-prefix prefix1
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
```

```
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 10.0.1.1 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.0
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
  network 2.2.2.0 0.0.0.255
#
 ip ip-prefix prefix1 index 10 permit 10.0.12.0 24
#
return
```

```
<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
mpls lsr-id 3.3.3.3
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.2 255.255.255.0
 mpls
 mpls ldp
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.0.23.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
```

```
 ip address 3.3.3.3 255.255.255.0
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
  network 3.3.3.0 0.0.0.255
#
return

<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
mpls lsr-id 4.4.4.4
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.0.23.3 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/2
 ip address 10.0.2.1 255.255.255.0
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.0
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
  network 4.4.4.0 0.0.0.255
#
return

<S2>display current-configuration
```

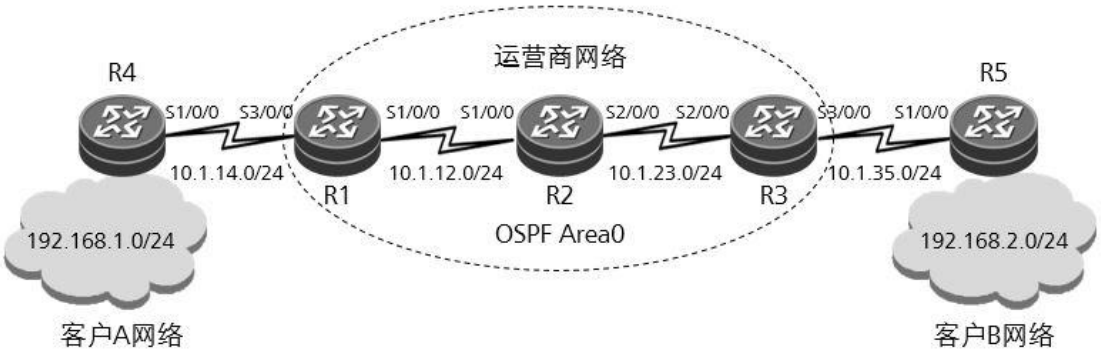
```
!Software Version V200R008C00SPC500
#
sysname S2
#
interface Vlanif1
 ip address 10.0.2.2 255.255.255.0
#
ospf 1 router-id 5.5.5.5
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
#
return
```

实验 1-2 MPLS VPN 配置

学习目的

- 掌握MPLS VPN实例的配置方法
- 掌握MP-BGP的配置方法
- 掌握MPLS LDP的配置方法
- 了解MPLS VPN路由传递与数据转发的过程

拓扑图



场景

某公司有两个网络，分别是网络A与网络B，该公司希望两个网络内的员工能通过私网路由相互访问。该公司希望在网络边缘设备上使用BGP协议将私网路由发送给运营商网络。运营商通过MP-BGP实现私网路由在公共网络上的传递，同时使用MPLS VPN技术保证客户网络信息的安全性和私密性。

学习任务

步骤一. 基本配置与 IP 编址

给所有路由器配置IP地址和掩码。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.1.12.1 24
[R1-Serial1/0/0]quit
[R1]interface Serial 3/0/0
[R1-Serial3/0/0]ip address 10.1.14.1 24
[R1-Serial3/0/0]quit
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 1.1.1.1 32

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.1.12.2 24
[R2-Serial1/0/0]quit
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]ip address 10.1.23.2 24
[R1-Serial2/0/0]quit
[R2]interface LoopBack 0
[R2-LoopBack0]ip address 2.2.2.2 32

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
```

```
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ip address 10.1.23.3 24
[R3-Serial2/0/0]quit
[R3]interface Serial 3/0/0
[R3-Serial3/0/0]ip address 10.1.35.3 24
[R3-Serial3/0/0]quit
[R3]interface LoopBack 0
[R3-LoopBack0]ip address 3.3.3.3 32

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
[R4]interface Serial 1/0/0
[R4-Serial1/0/0]ip address 10.1.14.4 24
[R4-Serial1/0/0]quit
[R4]interface LoopBack 0
[R4-LoopBack0]ip address 192.168.1.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R5
[R5]interface Serial 1/0/0
[R5-Serial1/0/0]ip address 10.1.35.5 24
[R5-Serial1/0/0]quit
[R5]interface LoopBack 0
[R5-LoopBack0]ip address 192.168.2.1 24
```

配置完成后，请自行测试直连链路的连通性。

步骤二. 配置运营商网络单区域 OSPF

配置10.1.12.0/24、10.1.23.0/24两个网段以及运营商网络各设备的LoopBack0接口属于OSPF Area0。

```
[R1]router id 1.1.1.1
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.1.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0

[R2]router id 2.2.2.2
[R2]ospf 1
[R2-ospf-1]area 0
```

```
[R2-ospf-1-area-0.0.0.0]network 10.1.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.1.23.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0

[R3]router id 3.3.3.3
[R3]ospf 1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.1.23.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 3.3.3.3 0.0.0.0
```

配置完成后，分别在R1，R2与R3上查看OSPF邻居关系的建立情况。

```
[R1]display ospf peer brief

       OSPF Process 1 with Router ID 1.1.1.1
               Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id         Interface                     Neighbor id     State
 0.0.0.0         Serial1/0/0                    2.2.2.2         Full
 ----------------------------------------------------------------------------
 Total Peer(s):    1

[R2]display ospf peer brief

       OSPF Process 1 with Router ID 2.2.2.2
               Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id         Interface                     Neighbor id     State
 0.0.0.0         Serial1/0/0                    1.1.1.1         Full
 0.0.0.0         Serial2/0/0                    3.3.3.3         Full
 ----------------------------------------------------------------------------
 Total Peer(s):    2

[R3]display ospf peer brief

       OSPF Process 1 with Router ID 3.3.3.3
               Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id         Interface                     Neighbor id     State
 0.0.0.0         Serial2/0/0                    2.2.2.2         Full
 ----------------------------------------------------------------------------
 Total Peer(s):    1
```

步骤三. 配置运营商网络边缘设备的 VPN 实例

在R1与R3上分别为客户A网络与客户B网络配置VPN实例。分配客户A网络的VPN实例为VPN1，RD值为1:1，Export Target与Import Target为1:2；分配给客户B网络的VPN实例为VPN2，RD值为2:2，Export Target与Import Target为1:2。

```
[R1]ip vpn-instance VPN1
[R1-vpn-instance-VPN1]route-distinguisher 1:1
[R1-vpn-instance-VPN1-af-ipv4]vpn-target 1:2 both
[R1-vpn-instance-VPN1-af-ipv4]quit
[R1-vpn-instance-VPN1]quit
[R1]interface Serial 3/0/0
[R1-Serial3/0/0]ip binding vpn-instance VPN1
Info: All IPv4 related configurations on this interface are removed!
Info: All IPv6 related configurations on this interface are removed!
[R1-Serial3/0/0] ip address 10.1.14.1 24

[R3]ip vpn-instance VPN2
[R3-vpn-instance-VPN2]route-distinguisher 2:2
[R3-vpn-instance-VPN2-af-ipv4]vpn-target 1:2 both
[R3-vpn-instance-VPN2-af-ipv4]quit
[R3-vpn-instance-VPN2]quit
[R3]interface Serial 3/0/0
[R3-Serial3/0/0]ip binding vpn-instance VPN2
Info: All IPv4 related configurations on this interface are removed!
Info: All IPv6 related configurations on this interface are removed!
[R3-Serial3/0/0]ip address 10.1.35.3 24
```

配置完成后，分别在R1与R3上查看配置的VPN实例。

```
[R1]display ip vpn-instance verbose
 Total VPN-Instances configured     : 1
 Total IPv4 VPN-Instances configured : 1
 Total IPv6 VPN-Instances configured : 0

 VPN-Instance Name and ID : VPN1, 1
  Interfaces : Serial3/0/0
 Address family ipv4
  Create date : 2016/09/20 14:51:08
  Up time : 0 days, 00 hours, 09 minutes and 34 seconds
  Route Distinguisher : 1:1
  Export VPN Targets :  1:2
```

```
  Import VPN Targets :  1:2
  Label Policy : label per route
  Log Interval : 5

[R3]display ip vpn-instance verbose
 Total VPN-Instances configured     : 1
 Total IPv4 VPN-Instances configured : 1
 Total IPv6 VPN-Instances configured : 0

 VPN-Instance Name and ID : VPN2, 1
  Interfaces : Serial3/0/0
 Address family ipv4
  Create date : 2016/09/20 15:02:52
  Up time : 0 days, 00 hours, 05 minutes and 32 seconds
  Route Distinguisher : 2:2
  Export VPN Targets :  1:2
  Import VPN Targets :  1:2
  Label Policy : label per route
  Log Interval : 5
```

步骤四. 配置客户网络边缘设备与运营商网络边缘设备使用 BGP 协议传递路由

客户A网络的AS号为14 ,运营商网络的AS号为123 ,客户B网络的AS号为35。客户网络边缘设备与运营商网络边缘设备建立BGP的邻居关系 ,使客户私网路由通过BGP协议通告给运营商网络边缘设备。

```
[R1]bgp 123
[R1-bgp]ipv4-family vpn-instance VPN1
[R1-bgp-VPN1]peer 10.1.14.4 as-number 14

[R3]bgp 123
[R3-bgp]ipv4-family vpn-instance VPN2
[R3-bgp-VPN2]peer 10.1.35.5 as-number 35

[R4]bgp 14
[R4-bgp]peer 10.1.14.1 as-number 123
[R4-bgp]network 192.168.1.0 24

[R5]bgp 35
[R5-bgp]peer 10.1.35.3 as-number 123
```

```
[R5-bgp]network 192.168.2.0 24
```

配置完成后，分别在R1与R4，R3与R5上查看BGP邻居关系的建立情况。

```
[R1]display bgp vpnv4 vpn-instance VPN1 peer
 BGP local router ID : 1.1.1.1
 Local AS number : 123
 VPN-Instance VPN1, Router ID 1.1.1.1:
 Total number of peers : 1             Peers in established state : 1

  Peer          V        AS  MsgRcvd  MsgSent  OutQ  Up/Down      State
PrefRcv

  10.1.14.4      4        14       7       8     0 00:05:21 Established      0

[R4]display bgp peer
 BGP local router ID : 10.1.14.4
 Local AS number : 14
 Total number of peers : 1             Peers in established state : 1

  Peer          V        AS  MsgRcvd  MsgSent  OutQ  Up/Down      State
PrefRcv

  10.1.14.1      4       123       4       6     0 00:02:56 Established      0

[R3]display bgp vpnv4 vpn-instance VPN2 peer
 BGP local router ID : 3.3.3.3
 Local AS number : 123
 VPN-Instance VPN2, Router ID 3.3.3.3:
 Total number of peers : 1             Peers in established state : 1

  Peer          V        AS  MsgRcvd  MsgSent  OutQ  Up/Down      State
PrefRcv

  10.1.35.5      4        35       7       8     0 00:05:16 Established      0

[R5]display bgp peer
 BGP local router ID : 192.168.1.1
 Local AS number : 35
 Total number of peers : 1             Peers in established state : 1

  Peer          V        AS  MsgRcvd  MsgSent  OutQ  Up/Down      State
PrefRcv
```

```
  10.1.35.3      4        123       8      10     0 00:06:04 Established      0
```

分别在R1与R3上查看VPN路由表学到的客户网络的私网路由。

```
[R1]display ip routing-table vpn-instance VPN1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Routing Tables: VPN1
        Destinations : 6       Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

     10.1.14.0/24  Direct  0    0           D   10.1.14.1       Serial3/0/0
     10.1.14.1/32  Direct  0    0           D   127.0.0.1       Serial3/0/0
     10.1.14.4/32  Direct  0    0           D   10.1.14.4       Serial3/0/0
   10.1.14.255/32  Direct  0    0           D   127.0.0.1       Serial3/0/0
   192.168.1.0/24  EBGP    255  0           D   10.1.14.4       Serial3/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[R3]display ip routing-table vpn-instance VPN2
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Routing Tables: VPN2
        Destinations : 6       Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

     10.1.35.0/24  Direct  0    0           D   10.1.35.3       Serial3/0/0
     10.1.35.3/32  Direct  0    0           D   127.0.0.1       Serial3/0/0
     10.1.35.5/32  Direct  0    0           D   10.1.35.5       Serial3/0/0
   10.1.35.255/32  Direct  0    0           D   127.0.0.1       Serial3/0/0
   192.168.2.0/24  EBGP    255  0           D   10.1.35.5       Serial3/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

步骤五. 配置运营商网络设备使用 MP-BGP 协议传递客户的私网路由

在R1与R3之间建立IBGP的邻居关系，采用MP-BGP协议在运营商网络中传

递客户的私网路由。

```
[R1]bgp 123
[R1-bgp]peer 3.3.3.3 as-number 123
[R1-bgp]peer 3.3.3.3 connect-interface LoopBack 0
[R1-bgp]ipv4-family vpnv4 unicast
[R1-bgp-af-vpnv4]peer 3.3.3.3 enable

[R3]bgp 123
[R3-bgp]peer 1.1.1.1 as-number 123
[R3-bgp]peer 1.1.1.1 connect-interface LoopBack 0
[R3-bgp]ipv4-family vpnv4 unicast
[R3-bgp-af-vpnv4]peer 1.1.1.1 enable
```

配置完成后，分别在R1与R3上查看MP-BGP邻居关系的建立情况。

```
[R1]display bgp vpnv4 all peer
 BGP local router ID : 1.1.1.1
 Local AS number : 123
 Total number of peers : 2             Peers in established state : 2

  Peer          V         AS  MsgRcvd  MsgSent  OutQ  Up/Down      State
PrefRcv

  3.3.3.3       4        123       4       7     0 00:02:10 Established      0

[R3]display bgp vpnv4 all peer
 BGP local router ID : 3.3.3.3
 Local AS number : 123
 Total number of peers : 2             Peers in established state : 2

  Peer          V         AS  MsgRcvd  MsgSent  OutQ  Up/Down      State
PrefRcv

  1.1.1.1       4        123       5       6     0 00:03:22 Established      0
```

步骤六. 配置运营商网络设备使用 MPLS LDP 协议转发客户的私网数据

在运营商网络的所有设备上开启MPLS LDP协议，使用标签转发客户网络的私网数据，达到用户数据与其他网络数据隔离的目的。

```
[R1]mpls lsr-id 1.1.1.1
[R1]mpls
[R1-mpls]mpls ldp
[R1-mpls-ldp]quit
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]mpls
[R1-Serial1/0/0]mpls ldp

[R2]mpls lsr-id 2.2.2.2
[R2]mpls
[R2-mpls]mpls ldp
[R2-mpls-ldp]quit
[R2]interface s1/0/0
[R2-Serial1/0/0]mpls
[R2-Serial1/0/0]mpls ldp
[R2-Serial1/0/0]quit
[R2]interface s2/0/0
[R2-Serial2/0/0]mpls
[R2-Serial2/0/0]mpls ldp

[R3]mpls lsr-id 3.3.3.3
[R3]mpls
[R3-mpls]mpls ldp
[R3-mpls-ldp]quit
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]mpls
[R3-Serial2/0/0]mpls ldp
```

配置完成后，分别在R1，R2与R3上查看MPLS LDP邻居关系的建立情况。

```
[R1]display mpls ldp peer
 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID              TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0           2.2.2.2          Serial1/0/0
 ------------------------------------------------------------------------------
 TOTAL: 1 Peer(s) Found.

[R2]display mpls ldp peer
 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
```

```
 ------------------------------------------------------------------------------
 PeerID              TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 1.1.1.1:0           1.1.1.1          Serial1/0/0
 3.3.3.3:0           3.3.3.3          Serial2/0/0
 ------------------------------------------------------------------------------
 TOTAL: 2 Peer(s) Found.

[R3]display mpls ldp peer
 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID              TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0           2.2.2.2          Serial2/0/0
 ------------------------------------------------------------------------------
 TOTAL: 1 Peer(s) Found.
```

步骤七. 在客户网络边缘设备上检查 A 网络与 B 网络的连通性

分别在R4与R5上使用LoopBack0模拟客户网络的用户，使用Ping命令检查A网络与B网络的连通性。

```
<R4>ping -a 192.168.1.1 192.168.2.1
  PING 192.168.2.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.2.1: bytes=56 Sequence=1 ttl=252 time=106 ms
    Reply from 192.168.2.1: bytes=56 Sequence=2 ttl=252 time=107 ms
    Reply from 192.168.2.1: bytes=56 Sequence=3 ttl=252 time=106 ms
    Reply from 192.168.2.1: bytes=56 Sequence=4 ttl=252 time=105 ms
    Reply from 192.168.2.1: bytes=56 Sequence=5 ttl=252 time=106 ms

  --- 192.168.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 105/106/107 ms

    <R5>ping -a 192.168.2.1 192.168.1.1
      PING 192.168.1.1: 56  data bytes, press CTRL_C to break
        Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=252 time=107 ms
        Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=252 time=105 ms
        Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=252 time=106 ms
```

```
  Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=252 time=106 ms
  Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=252 time=106 ms

--- 192.168.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 105/106/107 ms
```

分别在R4与R5上查看路由表中学习到的对端客户网络的私网路由。

```
<R4>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12        Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.1.14.0/24  Direct  0    0           D   10.1.14.4       Serial1/0/0
      10.1.14.1/32  Direct  0    0           D   10.1.14.1       Serial1/0/0
      10.1.14.4/32  Direct  0    0           D   127.0.0.1       Serial1/0/0
    10.1.14.255/32  Direct  0    0           D   127.0.0.1       Serial1/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     LoopBack0
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       LoopBack0
    192.168.2.0/24  EBGP    255  0           D   10.1.14.1       Serial1/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

<R5>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12        Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.1.35.0/24  Direct  0    0           D   10.1.35.5       Serial1/0/0
      10.1.35.3/32  Direct  0    0           D   10.1.35.3       Serial1/0/0
      10.1.35.5/32  Direct  0    0           D   127.0.0.1       Serial1/0/0
    10.1.35.255/32  Direct  0    0           D   127.0.0.1       Serial1/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

```
   192.168.1.0/24  EBGP    255  0          D   10.1.35.3       Serial1/0/0
   192.168.2.0/24  Direct  0    0          D   192.168.2.1     LoopBack0
   192.168.2.1/32  Direct  0    0          D   127.0.0.1       LoopBack0
 192.168.2.255/32  Direct  0    0          D   127.0.0.1       LoopBack0
255.255.255.255/32  Direct  0    0          D   127.0.0.1       InLoopBack0
```

附加实验：思考并验证

思考一下，在R1上新增了一个MPLS VPN的客户网络，如果要求实现与其他两个VPN客户网络的通信，该做哪些配置满足需求？

最终设备配置

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
router id 1.1.1.1
#
ip vpn-instance VPN1
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:2 export-extcommunity
  vpn-target 1:2 import-extcommunity
#
mpls lsr-id 1.1.1.1
mpls
#
mpls ldp
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.1.12.1 255.255.255.0
 mpls
 mpls ldp
#
interface Serial3/0/0
 link-protocol ppp
 ip binding vpn-instance VPN1
```

```
 ip address 10.1.14.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 123
 peer 3.3.3.3 as-number 123
 peer 3.3.3.3 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 3.3.3.3 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 3.3.3.3 enable
 #
 ipv4-family vpn-instance VPN1
  peer 10.1.14.4 as-number 14
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.12.0 0.0.0.255
#
return

<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
router id 2.2.2.2
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.1.12.2 255.255.255.0
```

```
 mpls
 mpls ldp
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.1.23.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 10.1.12.0 0.0.0.255
  network 10.1.23.0 0.0.0.255
#
return

<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
router id 3.3.3.3
#
ip vpn-instance VPN2
 ipv4-family
  route-distinguisher 2:2
  vpn-target 1:2 export-extcommunity
  vpn-target 1:2 import-extcommunity
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.1.23.3 255.255.255.0
 mpls
 mpls ldp
```

```
#
interface Serial3/0/0
 link-protocol ppp
 ip binding vpn-instance VPN2
 ip address 10.1.35.3 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
bgp 123
 peer 1.1.1.1 as-number 123
 peer 1.1.1.1 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 1.1.1.1 enable
 #
 ipv4-family vpn-instance VPN2
  peer 10.1.35.5 as-number 35
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.1.23.0 0.0.0.255
#
return

<R4>display current-configuration
[V200R007C00SPC600]
#
 sysname R4
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.1.14.4 255.255.255.0
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.0
```

```
#
bgp 14
 peer 10.1.14.1 as-number 123
 #
 ipv4-family unicast
  undo synchronization
  network 192.168.1.0
  peer 10.1.14.1 enable
#
return

<R5>display current-configuration
[V200R007C00SPC600]
#
 sysname R5
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.1.35.5 255.255.255.0
#
interface LoopBack0
 ip address 192.168.2.1 255.255.255.0
#
bgp 35
 peer 10.1.35.3 as-number 123
 #
 ipv4-family unicast
  undo synchronization
  network 192.168.2.0
  peer 10.1.35.3 enable
#
return
```

第二章 DHCP特性与配置

实验 2-1 DHCP 配置

学习目的

- 掌握IP Pool的配置方法
- 掌握DHCP服务器的配置方法
- 掌握DHCP客户端的配置方法
- 掌握DHCP中继的配置方法
- 掌握DHCP Snooping的基本功能配置方法

拓扑图

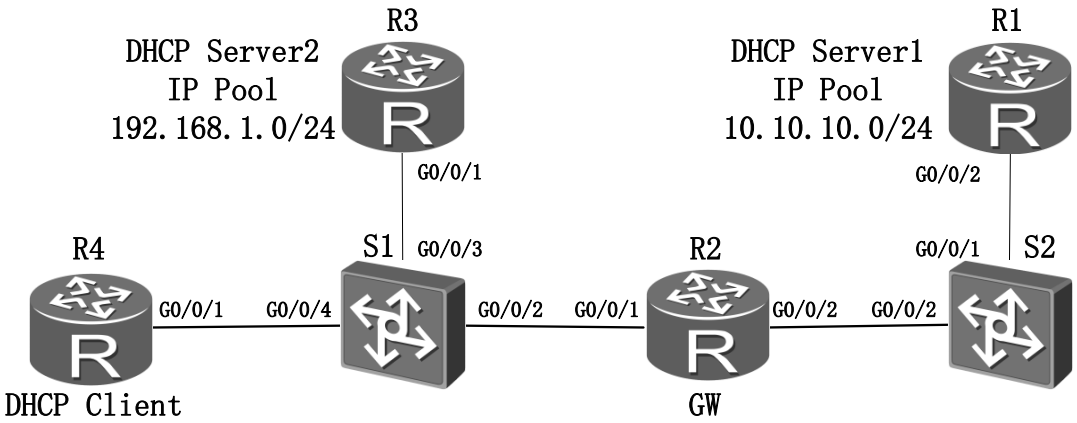


图1-1 DHCP配置

场景

你是公司的网络管理员，由于公司网络主机数量较多，使用静态地址分配难以管理，因此需要架设DHCP服务器。

R1路由器做DHCP服务器，R4为DHCP客户端，R2作为交换机S1下各设备的网关，由于DHCP Discover是广播报文不能穿越路由器，因此部署DHCP Relay将请求报文从R2发送到R1。S2不做任何配置，仅透明转发。

为了提升网络的安全性 ,防止其他DHCP服务器让客户端获取到错误的地址，在S1交换机上部署DHCP Snooping，要求R4可以获取到DHCP服务器1（R1）的地址 ,不应该获取到DHCP服务器2(R3)的地址。为了进一步增强安全防范，开启DHCP Snooping的部分特性防止DHCP饿死攻击和DHCP中间人攻击。

学习任务

步骤一. 基础配置与 IP 编址

给所有设备配置IP地址和掩码。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2]ip address 10.0.12.1 24
[R1-GigabitEthernet0/0/2]quit
[R1]interface loopback 0
[R1-LoopBack0]ip address 1.1.1.1 32

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.0.12.2 24
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.10.10.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 192.168.1.1 24
```

在R4的接口上配置DHCP客户端，使用DHCP方式获得IP地址：

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
[R4]dhcp enable
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1] ip address dhcp-alloc
```

给交换机配置名称，并关闭不必要的接口：

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname S1
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]shutdown
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]shutdown
[S1-GigabitEthernet0/0/10]quit
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]shutdown
[S1-GigabitEthernet0/0/13]quit
[S1]interface GigabitEthernet 0/0/14
[S1-GigabitEthernet0/0/14]shutdown

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname S2
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]shutdown
[S2-GigabitEthernet0/0/6]quit
[S2]interface GigabitEthernet 0/0/7
[S2-GigabitEthernet0/0/7]shutdown
```

验证R2和R1的互通：

```
[R1]ping 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=1 ms
```

```
  Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=1 ms
  Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=1 ms

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

步骤二. 配置 R1 和 R2 之间的路由

R1发布自己的环回口路由给R2，R2将自己连接S1的接口路由发布给R1，实现局域网网关和外网的互通。

```
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255

[R2]ospf 1
[R2-ospf-1]silent-interface GigabitEthernet 0/0/1
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.10.10.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
```

R2连接交换机的接口设置为silent接口，可以保证该网段的发布但不会在这个接口建立任何邻居。验证两个网络的互通：

```
[R2]ping -a 10.10.10.1 1.1.1.1
 PING 1.1.1.1: 56  data bytes, press CTRL_C to break
  Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms

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

步骤三. 配置 IP Pool

分别在R1和R3上创建两个地址池，R1的地址池范围为10.10.10.0/24，网关为R2的G0/0/0接口地址10.10.10.1，DNS地址使用1.1.1.1，为了保证该网络中一些静态地址不被分配，保留10.10.10.2-10不被DHCP动态分配。R3的地址池范围为192.168.1.0/24，网关地址为R3的G0/0/0接口地址192.168.1.1，DNS地址使用192.168.1.1，保留192.168.1.2-192.168.1.10不被DHCP动态分配，两台服务器的地址租期设置为3天。

```
[R1]ip pool DHCP
[R1-ip-pool-DHCP]gateway-list 10.10.10.1
[R1-ip-pool-DHCP]network 10.10.10.0 mask 255.255.255.0
[R1-ip-pool-DHCP]excluded-ip-address 10.10.10.2 10.10.10.10
[R1-ip-pool-DHCP]dns-list 1.1.1.1
[R1-ip-pool-DHCP]lease day 3

[R3]ip pool DHCP
[R3-ip-pool-DHCP]gateway-list 192.168.1.1
[R3-ip-pool-DHCP]network 192.168.1.0 mask 255.255.255.0
[R3-ip-pool-DHCP]excluded-ip-address 192.168.1.2 192.168.1.10
[R3-ip-pool-DHCP]dns-list 192.168.1.1
[R1-ip-pool-DHCP]lease day 3
```

验证地址池的配置：

```
<R1>display ip pool
 ---------------------------------------------------------------------------
  Pool-name       : DHCP
  Pool-No         : 0
  Lease           : 3 Days 0 Hours 0 Minutes
  Position        : Local         Status          : Unlocked
  Gateway-0       : 10.10.10.1
  Network         : 10.10.10.0
  Mask            : 255.255.255.0
  VPN instance    : --
  Address Statistic: Total      :253      Used       :0
                  Idle       :244      Expired    :0
                  Conflict   :0        Disable    :9


  IP address Statistic
    Total      :253
```

```
    Used       :0         Idle       :244
    Expired    :0         Conflict   :0         Disable   :9


<R3>display ip pool

--------------------------------------------------------------------------------
  Pool-name       : DHCP
  Pool-No         : 0
  Lease           : 3 Days 0 Hours 0 Minutes
  Position        : Local          Status           : Unlocked
  Gateway-0       : 192.168.1.1
  Network         : 192.168.1.0
  Mask            : 255.255.255.0
  VPN instance    : --
  Address Statistic: Total      :253      Used       :0
                  Idle       :244      Expired    :0
                  Conflict   :0        Disable    :9


  IP address Statistic
    Total      :253
    Used       :0         Idle       :244
    Expired    :0         Conflict   :0         Disable   :9
```

步骤四. 配置基于全局地址池的 DHCP 服务器

在上一步，已经配置好DHCP地址池的各个参数，但是此时并不能被客户端所使用，我们需要在全局和接口上配置启用DHCP功能：

```
[R3]dhcp enable
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]dhcp select global
```

在配置好R3的DHCP之后，R4应该可以正常获取到地址：

```
<R4>display ip interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 17, bytes : 5605, multicasts : 0
Directed-broadcast packets:
```

```
 received packets:          0, sent packets:         17
 forwarded packets:         0, dropped packets:          0
ARP packet input number:          0
  Request packet:                 0
  Reply packet:                   0
  Unknown packet:                 0
Internet Address is allocated by DHCP, 192.168.1.254/24
Broadcast address : 192.168.1.255
TTL being 1 packet number:        0
TTL invalid packet number:        0
ICMP packet input number:         0
  Echo reply:                     0
  Unreachable:                    0
  Source quench:                  0
  Routing redirect:               0
  Echo request:                   0
  Router advert:                  0
  Router solicit:                 0
  Time exceed:                    0
  IP header bad:                  0
  Timestamp request:              0
  Timestamp reply:                0
  Information request:            0
  Information reply:              0
  Netmask request:                0
  Netmask reply:                  0
  Unknown type:                   0
```

可以看到这个接口所使用的IP地址是通过DHCP方式获取的，IP地址为192.168.1.254。

步骤五. 配置 DHCP 中继

R3作为临时测试的DHCP Server配置已经完成，但我们实际想使用的DHCP Server为R1，因为DHCP Discover消息无法从客户端直接发给R1，因此在R2上我们需要配置DHCP中继，让R2作为S1所连接的LAN的网关，帮助这些客户端传递DHCP请求。

先在R1上启用DHCP：

```
[R1]dhcp enable
[R1]interface GigabitEthernet 0/0/2
```

```
[R1-GigabitEthernet0/0/2]dhcp select global
```

在R2上指定DHCP的服务器地址为10.0.12.1，在接口上配置DHCP中继：

```
[R2]dhcp enable
[R2]dhcp server group DHCP
[R2-dhcp-server-group-DHCP]dhcp-server 10.0.12.1
[R2-dhcp-server-group-DHCP]quit
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]dhcp select relay
[R2-GigabitEthernet0/0/1]dhcp relay server-select DHCP
```

在R2上验证DHCP中继的配置：

```
[R2]display dhcp server group
  Group-name         : DHCP
    (0)  Server-IP    : 10.0.12.1
    Gateway          : --
    VPN instance     : --
  1 DHCP server group(s) in total


[R2]display dhcp relay all
 DHCP relay agent running information of interface GigabitEthernet0/0/1 :
 Server group name     : DHCP
 Gateway address in use : 10.10.10.1
```

可以看到R2上配置了一个DHCP组，组里有一台服务器，地址为10.0.12.1，并且在R2的G0/0/1接口上启用了DHCP中继，中继将会把DHCP请求发送到组内的服务器10.0.12.1。

为了进一步验证DHCP中继是否部署成功，我们首先关闭R3的接口（为避免从R3获取地址），然后关闭R4的接口，最后开启接口，正常情况下，R4可以获取到10.10.10.0/24这个子网的地址。

```
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]shutdown

[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]shutdown
[R4-GigabitEthernet0/0/1]undo shutdown

[R4]display ip interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
```

```
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 36, bytes : 11866, multicasts : 0
Directed-broadcast packets:
 received packets:          0, sent packets:         36
 forwarded packets:         0, dropped packets:         0
ARP packet input number:          0
  Request packet:                 0
  Reply packet:                   0
  Unknown packet:                 0
Internet Address is allocated by DHCP, 10.10.10.254/24
Broadcast address : 10.10.10.255
TTL being 1 packet number:        0
TTL invalid packet number:        0
ICMP packet input number:         0
  Echo reply:                     0
  Unreachable:                    0
  Source quench:                  0
  Routing redirect:               0
  Echo request:                   0
  Router advert:                  0
  Router solicit:                 0
  Time exceed:                    0
  IP header bad:                  0
  Timestamp request:              0
  Timestamp reply:                0
  Information request:            0
  Information reply:              0
  Netmask request:                0
  Netmask reply:                  0
  Unknown type:                   0
```

R4成功获取到了地址，并且地址为10.10.10.254。查看R2上的数据统计和R1上地址池的状态。

```
<R2>display dhcp relay statistics
 The statistics of DHCP RELAY:
    DHCP packets received from clients    : 2
        DHCP DISCOVER packets received    : 1
        DHCP REQUEST packets received     : 1
        DHCP RELEASE packets received     : 0
        DHCP INFORM packets received      : 0
        DHCP DECLINE packets received     : 0
```

```
    DHCP packets sent to clients         : 2
       Unicast packets sent to clients   : 2
       Broadcast packets sent to clients : 0
    DHCP packets received from servers    : 2
       DHCP OFFER packets received       : 1
       DHCP ACK packets received         : 1
       DHCP NAK packets received         : 0
    DHCP packets sent to servers          : 2
    DHCP Bad packets received             : 0

    <R1>display ip pool

--------------------------------------------------------------------------------
  Pool-name       : DHCP
  Pool-No         : 0
  Lease           : 3 Days 0 Hours 0 Minutes
  Position        : Local          Status           : Unlocked
  Gateway-0       : 10.10.10.1
  Network         : 10.10.10.0
  Mask            : 255.255.255.0
  VPN instance    : --
  Address Statistic: Total      :253      Used       :1
                  Idle       :243      Expired    :0
                  Conflict   :0        Disable    :9


  IP address Statistic
    Total      :253
    Used       :1         Idle       :243
    Expired    :0         Conflict   :0         Disable   :9
```

查看R4的路由并测试R4到R1的环回口互通：

```
<R4>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Routing Tables: Public
        Destinations : 8       Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       0.0.0.0/0   Unr     60   0           D   10.10.10.1      GigabitEthernet
0/0/0
```

```
    10.10.10.0/24  Direct  0    0          D   10.10.10.254    GigabitEthernet
0/0/0
   10.10.10.254/32  Direct  0    0          D   127.0.0.1      GigabitEthernet
0/0/0
   10.10.10.255/32  Direct  0    0          D   127.0.0.1      GigabitEthernet
0/0/0
     127.0.0.0/8   Direct  0    0          D   127.0.0.1      InLoopBack0
     127.0.0.1/32  Direct  0    0          D   127.0.0.1      InLoopBack0
127.255.255.255/32  Direct  0    0          D   127.0.0.1      InLoopBack0
255.255.255.255/32  Direct  0    0          D   127.0.0.1      InLoopBack0

<R4>ping 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

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

步骤六. 配置 DHCP Snooping 和攻击防范特性

在上一个步骤，我们暂时关闭了R3的接口，这时R4只能通过R2的DHCP中继到R1获取地址，但是，如果我们想开启R3接口，又不想让R4从R3获取地址，应该怎么做？特别是某些SOHO级路由器默认启动DHCP，如果接入网络内，会有严重的安全隐患。这里推荐在S1交换机上开启DHCP Snooping技术，可以有效的防范非授权的DHCP服务器干扰局域网内的主机。

在此基础上，我们在交换机S1上再启用防饿死攻击和防中间人攻击，进一步保护通过DHCP方式获取地址的网络。

开始配置DHCP Snooping防止未授权DHCP提供地址：

```
[S1]dhcp enable
[S1]dhcp snooping enable
[S1]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]dhcp snooping enable
```

```
[S1-GigabitEthernet0/0/3]quit
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]dhcp snooping enable
```

默认情况下，开启DHCP Snooping的接口处于untrust状态：

```
[S1]display dhcp snooping
 DHCP snooping global running information :
 DHCP snooping                          : Enable
 Static user max number                  : 1024
 Current static user number              : 0
 Dhcp user max number                   : 1024    (default)
 Current dhcp user number                : 0
 Arp dhcp-snooping detect                : Disable  (default)
 Alarm threshold                        : 100     (default)
 Check dhcp-rate                        : Disable  (default)
 Dhcp-rate limit(pps)                    : 100     (default)
 Alarm dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate threshold               : 100     (default)
 Discarded dhcp packets for rate limit    : 0
 Bind-table autosave                    : Disable  (default)
 Offline remove mac-address              : Disable  (default)
 Client position transfer allowed        : Enable   (default)

 DHCP snooping running information for interface GigabitEthernet0/0/2 :
 DHCP snooping                          : Enable
 Trusted interface                       : No
 Dhcp user max number                    : 1024    (default)
 Current dhcp user number                : 0
 Check dhcp-giaddr                      : Disable  (default)
 Check dhcp-chaddr                      : Disable  (default)
 Alarm dhcp-chaddr                      : Disable  (default)
 Check dhcp-request                     : Disable  (default)
 Alarm dhcp-request                     : Disable  (default)
 Check dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate threshold               : 100
 Discarded dhcp packets for rate limit    : 0
 Alarm dhcp-reply                       : Disable  (default)

 DHCP snooping running information for interface GigabitEthernet0/0/3 :
 DHCP snooping                          : Enable
 Trusted interface                       : No
```

```
 Dhcp user max number                  : 1024    (default)
 Current dhcp user number               : 0
 Check dhcp-giaddr                    : Disable  (default)
 Check dhcp-chaddr                    : Disable  (default)
 Alarm dhcp-chaddr                    : Disable  (default)
 Check dhcp-request                   : Disable  (default)
 Alarm dhcp-request                   : Disable  (default)
 Check dhcp-rate                     : Disable  (default)
 Alarm dhcp-rate                     : Disable  (default)
 Alarm dhcp-rate threshold             : 100
 Discarded dhcp packets for rate limit    : 0
 Alarm dhcp-reply                     : Disable  (default)
```

R4再次重启接口，但这时无法从任何一台DHCP服务器获取到地址，因为连接这两个服务器的接口在S1上都是非信任状态：

```
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]shutdown
[R4-GigabitEthernet0/0/1]undo shutdown

[r4]display ip interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
Line protocol current state : DOWN
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 8, bytes : 2624, multicasts : 0
Directed-broadcast packets:
 received packets:          0, sent packets:          8
 forwarded packets:         0, dropped packets:         0
ARP packet input number:         0
  Request packet:               0
  Reply packet:                 0
  Unknown packet:               0
Internet protocol processing : disabled
Broadcast address : 0.0.0.0
TTL being 1 packet number:        0
TTL invalid packet number:        0
ICMP packet input number:         0
  Echo reply:                   0
  Unreachable:                  0
  Source quench:                0
  Routing redirect:             0
  Echo request:                 0
```

```
  Router advert:                0
  Router solicit:               0
  Time exceed:                  0
  IP header bad:                0
  Timestamp request:            0
  Timestamp reply:              0
  Information request:          0
  Information reply:            0
  Netmask request:              0
  Netmask reply:                0
  Unknown type:                 0
```

因为R2所中继的R1是信任的DHCP服务器，因此在交换机连接R2的接口上启用信任接口：

```
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]dhcp snooping trusted
```

检查该接口的Snooping状态：

```
[S1]display dhcp snooping interface GigabitEthernet 0/0/2
 DHCP snooping running information for interface GigabitEthernet0/0/2 :
 DHCP snooping                          : Enable
 Trusted interface                      : Yes
 Dhcp user max number                   : 1024     (default)
 Current dhcp user number               : 0
 Check dhcp-giaddr                      : Disable  (default)
 Check dhcp-chaddr                      : Disable  (default)
 Alarm dhcp-chaddr                      : Disable  (default)
 Check dhcp-request                     : Disable  (default)
 Alarm dhcp-request                     : Disable  (default)
 Check dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate threshold              : 100
 Discarded dhcp packets for rate limit  : 0
 Alarm dhcp-reply                       : Disable  (default)
```

R4可以重新获取到地址：

```
[R4]display ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 94, bytes : 30832, multicasts : 0
```

```
Directed-broadcast packets:
 received packets:          0, sent packets:         94
 forwarded packets:         0, dropped packets:         0
ARP packet input number:         0
  Request packet:               0
  Reply packet:                 0
  Unknown packet:               0
Internet Address is allocated by DHCP, 10.10.10.254/24
Broadcast address : 10.10.10.255
TTL being 1 packet number:       0
TTL invalid packet number:       0
ICMP packet input number:        0
  Echo reply:                   0
  Unreachable:                  0
  Source quench:                0
  Routing redirect:             0
  Echo request:                 0
  Router advert:                0
  Router solicit:               0
  Time exceed:                  0
  IP header bad:                0
  Timestamp request:            0
  Timestamp reply:              0
  Information request:          0
  Information reply:            0
  Netmask request:              0
  Netmask reply:                0
  Unknown type:                 0
```

此步骤配置完毕。假设R4是一台不被信任的主机，有可能从这台主机发起大量的DHCP请求耗尽地址池，因此在S1交换机与其相连的接口上启用防DHCP饿死攻击特性：

```
[S1]interface GigabitEthernet 0/0/4
[S1-GigabitEthernet0/0/4]dhcp snooping check dhcp-chaddr enable
```

检查配置状态为Enable ,这样从这个接口收到的DHCP请求都要检查chaddr字段，看是否和主机的硬件地址一致，如果不一致则不进行转发：

```
[S1]display dhcp snooping interface GigabitEthernet 0/0/4
 DHCP snooping running information for interface GigabitEthernet0/0/4 :
 DHCP snooping                       : Disable  (default)
 Trusted interface                    : No
```

```
 Dhcp user max number                   : 1024     (default)
 Current dhcp user number               : 0
 Check dhcp-giaddr                      : Disable  (default)
 Check dhcp-chaddr                      : Enable
 Alarm dhcp-chaddr                      : Disable  (default)
 Check dhcp-request                     : Disable  (default)
 Alarm dhcp-request                     : Disable  (default)
 Check dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate threshold              : 100
 Discarded dhcp packets for rate limit    : 0
 Alarm dhcp-reply                       : Disable  (default)
```

最后开启防中间人攻击的特性：

```
[S1]arp dhcp-snooping-detect enable
```

检查全局DHCP Snooping特性：

```
[S1]display dhcp snooping
 DHCP snooping global running information :
 DHCP snooping                          : Enable
 Static user max number                 : 1024
 Current static user number             : 0
 Dhcp user max number                   : 1024     (default)
 Current dhcp user number               : 0
 Arp dhcp-snooping detect               : Enable
 Alarm threshold                        : 100      (default)
 Check dhcp-rate                        : Disable  (default)
 Dhcp-rate limit(pps)                   : 100      (default)
 Alarm dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate threshold              : 100      (default)
 Discarded dhcp packets for rate limit    : 0
 Bind-table autosave                    : Disable  (default)
 Offline remove mac-address             : Disable  (default)
 Client position transfer allowed       : Enable   (default)
```

ARP dhcp-snooping detect已经启用，默认是关闭。至此DHCP安全防范配置完毕。

步骤七. 参考配置

```
<R1>display current-configuration
[V200R007C00SPC600]
```

```
#
 sysname R1
#
dhcp enable
#
ip pool DHCP
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
 excluded-ip-address 10.10.10.2 10.10.10.10
 lease day 3 hour 0 minute 0
 dns-list 1.1.1.1

interface GigabitEthernet0/0/2
 ip address 10.0.12.1 255.255.255.0
 dhcp select global
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.0.12.0 0.0.0.255
#
return

<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
dhcp enable
#
dhcp server group DHCP
 dhcp-server 10.0.12.1 0
#
interface GigabitEthernet0/0/1
 ip address 10.10.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select DHCP
#
interface GigabitEthernet0/0/2
```

```
 ip address 10.0.12.2 255.255.255.0
#
ospf 1
 silent-interface GigabitEthernet0/0/1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
  network 10.10.10.0 0.0.0.255
#
return
```

```
<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
dhcp enable
#
ip pool DHCP
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
 excluded-ip-address 192.168.1.2 192.168.1.10
 lease day 3 hour 0 minute 0
 dns-list 192.168.1.1
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 dhcp select global
#
return
```

```
<R4>display current-configuration
[V200R007C00SPC600]
#
 sysname R4
#
dhcp enable
#
interface GigabitEthernet0/0/1
 ip address dhcp-alloc
#
return
```

```
<SW1>display current-configuration
```

```
!Software Version V200R008C00SPC500
#
sysname S1
#
dhcp enable
#
dhcp snooping enable
arp dhcp-snooping-detect enable
#
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping trusted
#
interface GigabitEthernet0/0/3
 dhcp snooping enable
#
interface GigabitEthernet0/0/4
 dhcp snooping check dhcp-chaddr enable
#
interface GigabitEthernet0/0/9
 shutdown
#
interface GigabitEthernet0/0/10
 shutdown
#
interface GigabitEthernet0/0/13
 shutdown
#
interface GigabitEthernet0/0/14
 shutdown
#
return
```

```
<SW2>display current-configuration
!Software Version V200R008C00SPC500
#
sysname SW2
#
interface GigabitEthernet0/0/6
 shutdown
#
```

```
interface GigabitEthernet0/0/7
 shutdown
#
return
```

第三章 服务质量与流量控制

实验 3-1 QoS 基础

学习目的

- 掌握使用NQA分析SLA的方法
- 掌握进行优先级映射和流量监管的方法
- 掌握配置流量整形的方法
- 掌握实现基于队列和基于流分类的拥塞管理的方法
- 掌握配置WRED实现拥塞避免的方法

拓扑图

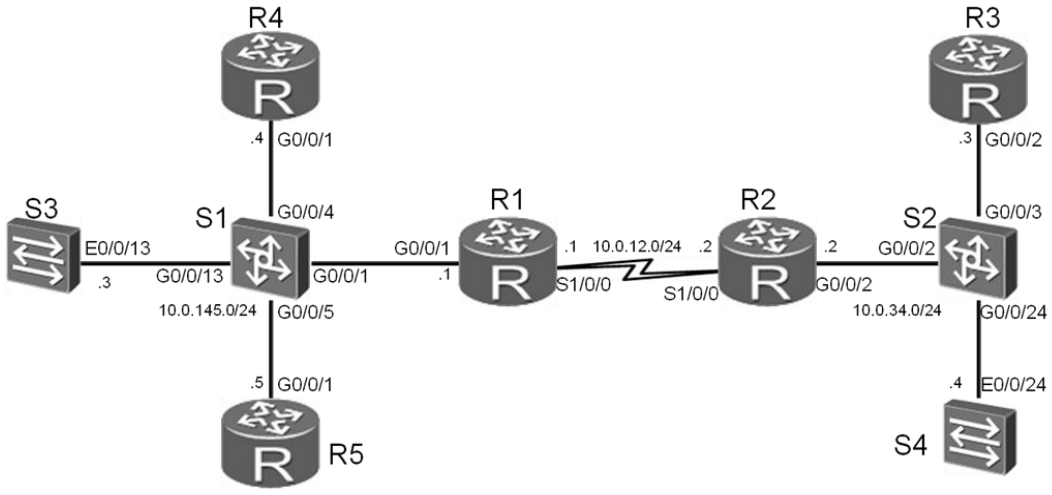


图2-1 QoS基础

场景

你是公司的网络管理员。公司网络分成两部分，其中R1与S1在公司总部，R2与S2在公司分部，之间通过专线实现互联。

随着网络的发展，内网带宽逐渐增大，而专线的带宽一直没有升级，所以网络中出现了比较严重的重要业务反应较慢，或无法正常使用的情况。

使用QoS的差分服务，你可以调整相应的QoS特性，保证重要的业务数据能更好的发送给目标。

实验中，S3和S4使用NQA相互发送数据，模拟大量数据流的发送。R3、R4与R5模拟客户端和服务器，测试重要应用是否可以正常使用。

学习任务

步骤一. 基础配置与 IP 编址

给所有路由器和交换机S3，S4配置IP地址和掩码。

配置时需要将R1接口S1/0/0的波特率配置为72000，模拟广域网链路因带宽不足而出现拥塞。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 255.255.255.0
[R1-Serial1/0/0]baudrate 72000
[R1-Serial1/0/0]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.145.1 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 255.255.255.0
[R2-Serial1/0/0]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.0.34.2 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.34.3 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
```

```
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 10.0.145.4 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R5
[R5]interface GigabitEthernet 0/0/1
[R5-GigabitEthernet0/0/1]ip address 10.0.145.5 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname S3
[S3]interface Vlanif 1
[S3-Vlanif1]ip address 10.0.145.3 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname S4
[S4]interface Vlanif 1
[S4-Vlanif1]ip address 10.0.34.4 255.255.255.0
```

配置完成后，测试直连链路的连通性。

```
[R1]ping -c 1 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=36 ms

  --- 10.0.12.2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 36/36/36 ms

[R1]ping -c 1 10.0.145.3
  PING 10.0.145.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.3: bytes=56 Sequence=1 ttl=255 time=35 ms

  --- 10.0.145.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/35/35 ms
```

```
[R1]ping -c 1 10.0.145.4
  PING 10.0.145.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.4: bytes=56 Sequence=1 ttl=255 time=6 ms

  --- 10.0.145.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/6/6 ms

[R1]ping -c 1 10.0.145.5
  PING 10.0.145.5: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.5: bytes=56 Sequence=1 ttl=255 time=6 ms

  --- 10.0.145.5 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/6/6 ms

[R2]ping -c 1 10.0.34.3
  PING 10.0.34.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=56 Sequence=1 ttl=255 time=5 ms

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

[R2]ping -c 1 10.0.34.4
  PING 10.0.34.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.4: bytes=56 Sequence=1 ttl=255 time=36 ms

  --- 10.0.34.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 36/36/36 ms
```

步骤二. 配置静态路由与 NQA

在所有路由器和交换机S3，S4上配置静态路由。

```
[R1]ip route-static 10.0.34.0 255.255.255.0 10.0.12.2

[R2]ip route-static 10.0.145.0 255.255.255.0 10.0.12.1

[R3]ip route-static 0.0.0.0 0.0.0.0 10.0.34.2

[R4]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[R5]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[S3]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[S4]ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
```

配置完成后，测试网络连通性。

```
[S3]ping -c 1 10.0.34.4
  PING 10.0.34.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.4: bytes=56 Sequence=1 ttl=252 time=40 ms

  --- 10.0.34.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/40/40 ms

[R4]ping -c 1 10.0.34.3
  PING 10.0.145.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.4: bytes=56 Sequence=1 ttl=255 time=3 ms

  --- 10.0.145.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms

[R5]ping -c 1 10.0.34.3
  PING 10.0.34.3: 56  data bytes, press CTRL_C to break
```

```
  Reply from 10.0.34.3: bytes=56 Sequence=1 ttl=253 time=44 ms

--- 10.0.34.3 ping statistics ---
  1 packet(s) transmitted
  1 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 44/44/44 ms
```

S3去往S4，R4和R5去往R3可以连通，证明网络通信正常。

公司总部和分部之间的链路为72K串行链路，因而在实际情况中很容易造成拥塞。

实验中使用NQA在网络中产生流量。S4作为NQA服务器端，S3作为NQA客户端。

定义UDP，Jitter两种NQA测试例，分别用来模拟企业网中的数据流量和语音流量。

通过设置NQA测试例中的一些参数来实现两种流量中任何一种单独存在的情况下不会产生拥塞，二者共存的情况下会产生拥塞，来模拟实际环境。

在S4设上配置NQA服务器端，监听的IP地址设为10.0.34.4，UDP端口号设为6000。

```
[S4]nqa-server udpecho 10.0.34.4 6000
```

在S3上配置UDP类型的NQA测试例模拟数据流量，其中**tos**设为28，包大小为5800字节，包间隔设为1s，周期设为3s，超时设为1s，并开启该测试。

```
[S3]nqa test-instance admin udp
[S3-nqa-admin-udp]test-type udp
[S3-nqa-admin-udp]destination-address ipv4 10.0.34.4
[S3-nqa-admin-udp]destination-port 6000
[S3-nqa-admin-udp]tos 28
[S3-nqa-admin-udp]datasize 5800
[S3-nqa-admin-udp]interval seconds 1
[S3-nqa-admin-udp]frequency 3
[S3-nqa-admin-udp]timeout 1
[S3-nqa-admin-udp]start now
```

查看UDP测试结果。

```
[S3]display nqa results test-instance admin udp
1 . Test 2 result   The test is finished
  Send operation times: 3              Receive response times: 3
  Completion:success                   RTD OverThresholds number: 0
```

```
  Attempts number:1                     Drop operation number:0
  Disconnect operation number:0         Operation timeout number:0
  System busy operation number:0        Connection fail number:0
  Operation sequence errors number:0    RTT Stats errors number:0
  Destination ip address:10.0.34.4
  Min/Max/Average Completion Time: 930/950/943
  Sum/Square-Sum  Completion Time: 2830/2669900
  Last Good Probe Time: 2010-10-10 18:10:02.4
  Lost packet ratio: 0 %
```

此时不丢包，链路没有产生拥塞。关闭UDP测试。

```
[S3]nqa test-instance admin udp
[S3-nqa-admin-udp]stop
```

在S3上配置Jitter类型的NQA测试例模拟语音流量，其中**tos**设为46，包大小为90字节，包间隔设为20ms，周期设为3s，超时设为1s，并开启该测试。

```
[S3]nqa test-instance admin jitter
[S3-nqa-admin-jitter]test-type jitter
[S3-nqa-admin-jitter]destination-address ipv4 10.0.34.4
[S3-nqa-admin-jitter]destination-port 6000
[S3-nqa-admin-jitter]tos 46
[S3-nqa-admin-jitter]datasize 90
[S3-nqa-admin-jitter]interval milliseconds 20
[S3-nqa-admin-jitter]frequency 3
[S3-nqa-admin-jitter]timeout 1
[S3-nqa-admin-jitter]start now
```

查看Jitter测试结果。

```
[S3]display nqa results test-instance admin jitter

 NQA entry(admin, jitter) :testflag is active ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                         ResponseProbe:60
   Completion:success                   RTD OverThresholds number:0
   Min/Max/Avg/Sum RTT:40/70/54/3260    RTT  Square Sum:179800
   NumOfRTT:60                          Drop operation number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   System busy operation number:0       Operation timeout number:0
   Min Positive SD:10                   Min Positive DS:10
   Max Positive SD:10                   Max Positive DS:10
   Positive SD Number:5                 Positive DS Number:11
```

```
  Positive SD Sum:50                  Positive DS Sum:110
  Positive SD Square Sum:500          Positive DS Square Sum:1100
  Min Negative SD:10                  Min Negative DS:10
  Max Negative SD:10                  Max Negative DS:20
  Negative SD Number:4                Negative DS Number:10
  Negative SD Sum:40                  Negative DS Sum:110
  Negative SD Square Sum:400          Negative DS Square Sum:1300
  Min Delay SD:20                     Min Delay DS:19
  Avg Delay SD:27                     Avg Delay DS:26
  Max Delay SD:35                     Max Delay DS:34
  Packet Loss SD:0                    Packet Loss DS:0
  Packet Loss Unknown:0               jitter out value:0.0937500
  jitter in value:0.2291667           NumberOfOWD:60
  OWD SD Sum:1630                     OWD DS Sum:1570
  TimeStamp unit: ms
```

此时不丢包，链路没有产生拥塞。关闭Jitter测试。

```
[S3]nqa test-instance admin jitter
[S3-nqa-admin-jitter]stop
```

步骤三. 配置优先级映射

现在通过**ping**命令来模拟公司中一些不太重要的流量,并且针对这部分流量，将其DSCP优先级映射为BE，不做QoS保证。

配置R1的接口G0/0/1与S1/0/0信任报文的DSCP优先级。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]trust dscp override
[R1-GigabitEthernet0/0/1]interface Serial 1/0/0
[R1-Serial1/0/0]trust dscp
```

在接口G0/0/1上的**trust**命令中需要加上**override**参数，使得接下来在R1上配置优先级映射后，将DSCP值修改为映射后的值。

在R4上使用**ping**命令产生去往R3的流量，并且将**tos**设为26。

```
[R4]ping -tos 26 10.0.34.3
```

在R1上配置优先级映射关系，将该流量的DSCP报文优先级26映射为0，

```
[R1]qos map-table dscp-dscp
[R1-maptbl-dscp-dscp]input 26 output 0
```

查看R1上的优先级映射信息。

```
[R1]display qos map-table dscp-dscp
Input DSCP     DSCP
-------------------
 0             0
 1             1
 2             2
 3             3
 4             4
 5             5
 6             6
 7             7
 8             8
 9             9
10             10
11             11
12             12
13             13
14             14
15             15
16             16
17             17
18             18
19             19
20             20
21             21
22             22
23             23
24             24
25             25
26             0
27             27
28             28
29             29
30             30
```

此时可以观察到，现在已将DSCP优先级为26的报文优先级映射成为了0，而其余DSCP值都是默认映射值。

步骤四. 配置整形与监管

开启S3上的NQA的UDP与Jitter测试，模拟公司总部与分部之间的72K链路产生拥塞。

```
[S3]nqa test-instance admin udp
[S3-nqa-admin-udp]start now
[S3-nqa-admin-udp]quit
[S3]nqa test-instance admin jitter
[S3-nqa-admin-jitter]start now
```

在R4上使用**ping**命令实现模拟去往R3的流量，设置包大小为700字节，发10个包。

```
[R4]ping -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Reply from 10.0.34.3: bytes=700 Sequence=9 ttl=253 time=1944 ms
    Request time out

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    1 packet(s) received
    90.00% packet loss
    round-trip min/avg/max = 1944/1944/1944 ms
```

此时公司总部与分部之间的链路发生了严重拥塞，丢包现象严重。即使有通过的数据包，延迟也非常大。此时R4无法与R3建立正常通信。

下面将介绍分别通过使用流量监管和流量整形的方法来消除链路上的拥塞，使得公司总部的客户端R4与分部的客户端R3能够建立正常通信。

首先通过流量监管来消除拥塞。在S1上，针对拥塞流量在入接口G0/0/13上配置流量监管，CIR设为64kbit/s。

```
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]qos lr inbound cir 64
```

查看S1上流量监管的配置信息。

```
[S1]display qos lr inbound interface GigabitEthernet 0/0/13
GigabitEthernet0/0/13 lr inbound:
  cir: 64 Kbps, cbs: 8000 Byte
```

现在再回到R4上使用**ping**命令实现模拟去往R3的流量，设置包大小为700字节，发10个包。

```
[R4]ping -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=1412 ms
    Reply from 10.0.34.3: bytes=700 Sequence=2 ttl=253 time=255 ms
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=736 ms
    Reply from 10.0.34.3: bytes=700 Sequence=4 ttl=253 time=1746 ms
    Reply from 10.0.34.3: bytes=700 Sequence=5 ttl=253 time=246 ms
    Reply from 10.0.34.3: bytes=700 Sequence=6 ttl=253 time=746 ms
    Reply from 10.0.34.3: bytes=700 Sequence=7 ttl=253 time=1736 ms
    Reply from 10.0.34.3: bytes=700 Sequence=8 ttl=253 time=258 ms
    Reply from 10.0.34.3: bytes=700 Sequence=9 ttl=253 time=766 ms
    Reply from 10.0.34.3: bytes=700 Sequence=10 ttl=253 time=1736 ms

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 246/963/1746 ms
```

此时流量监管产生效果，不丢包，R4和R3之间能够建立起正常通信。

删除S1上流量监管配置。

```
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]undo qos lr inbound
```

现在通过流量整形的方式来达到消除拥塞的目的。在S3上，针对拥塞流量在出接口E0/0/13上配置流量整形，CIR设为64kbit/s。

```
[S3]interface Ethernet0/0/13
[S3-Ethernet0/0/13]qos lr outbound cir 64
```

在R4上使用**ping**命令实现模拟去往R3的流量，设置包大小为700字节，发10个包。

```
[R4]ping -s 700 -c 10 10.0.34.3
```

```
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=240 ms
    Reply from 10.0.34.3: bytes=700 Sequence=2 ttl=253 time=284 ms
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=334 ms
    Reply from 10.0.34.3: bytes=700 Sequence=4 ttl=253 time=224 ms
    Reply from 10.0.34.3: bytes=700 Sequence=5 ttl=253 time=344 ms
    Reply from 10.0.34.3: bytes=700 Sequence=6 ttl=253 time=275 ms
    Reply from 10.0.34.3: bytes=700 Sequence=7 ttl=253 time=534 ms
    Reply from 10.0.34.3: bytes=700 Sequence=8 ttl=253 time=184 ms
    Reply from 10.0.34.3: bytes=700 Sequence=9 ttl=253 time=204 ms
    Reply from 10.0.34.3: bytes=700 Sequence=10 ttl=253 time=314 ms

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 184/293/534 ms
```

此时流量监管产生效果，不丢包，R4和R3之间能够建立起正常通信。

删除S3上的流量整形配置，

```
[S3]interface Ethernet0/0/13
[S3-Ethernet0/0/13]undo qos lr outbound
```

现在再回到R4上使用**ping**命令实现模拟去往R3的流量，设置包大小为700字节，发10个包。

```
[R4]ping -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=1918 ms
    Request time out
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=1762 ms
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    2 packet(s) received
    80.00% packet loss
```

```
    round-trip min/avg/max = 1762/1840/1918 ms
```

删除配置之后，丢包严重，并且通过的数据包延迟也非常大。R4与R3之间无法建立起正常通信。

步骤五. 配置基于队列的拥塞管理与拥塞避免

为了解决公司总部与分部之间产生的网络拥塞，现在通过配置基于队列的拥塞管理和拥塞避免的方式解决。

在R1上创建WRED丢弃模板**data**，使其基于DSCP优先级进行丢弃，将阀值上限设为90，下限设为50，丢弃概率设为30。

```
[R1]drop-profile data
[R1-drop-profile-data]wred dscp
[R1-drop-profile-data]dscp af32 low-limit 50 high-limit 90 discard-percentage
30
```

在R1上创建队列模板queue-profile1，将数据流量放入WFQ队列，并和丢弃模板data绑定，将需要高优先级，低延迟保证的语音流量放入PQ队列。

```
[R1]qos queue-profile queue-profile1
[R1-qos-queue-profile-queue-profile1]schedule wfq 3 pq 5
[R1-qos-queue-profile-queue-profile1]queue 3 drop-profile data
```

在R1的S1/0/0上应用队列模板。

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]qos queue-profile queue-profile1
```

查看配置的队列模板信息。

```
[R1]display qos queue-profile queue-profile1
Queue-profile: queue-profile1
Queue  Schedule  Weight  Length(Bytes/Packets) Gts(CIR/CBS)
------------------------------------------------------------------
3      WFQ       10              0/0           -/-
5      PQ        -               0/0           -/-
```

此时数据流量与语音流量分别使用了WFQ与PQ队列。

查看配置的丢弃模板信息。

```
[R1]display drop-profile data
Drop-profile[1]: data
```

```
DSCP          Low-limit   High-limit  Discard-percentage
------------------------------------------------------------------
default         30          100         10
1               30          100         10
2               30          100         10
3               30          100         10
4               30          100         10
5               30          100         10
6               30          100         10
7               30          100         10
cs1             30          100         10
9               30          100         10
af11            30          100         10
11              30          100         10
af12            30          100         10
13              30          100         10
af13            30          100         10
15              30          100         10
cs2             30          100         10
17              30          100         10
af21            30          100         10
19              30          100         10
af22            30          100         10
21              30          100         10
af23            30          100         10
23              30          100         10
cs3             30          100         10
25              30          100         10
af31            30          100         10
27              30          100         10
af32            50          90          30
29              30          100         10
af33            30          100         10
31              30          100         10
cs4             30          100         10
33              30          100         10
af41            30          100         10
```

可以观察到配置上限，下限阀值与丢弃概率产生的效果，其余没有配置的丢弃模板设置对应的都是默认值。

步骤六. 配置基于流的拥塞管理与拥塞避免

为了解决公司总部与分部之间产生的网络拥塞，现在通过配置基于流的拥塞管理和拥塞避免的方式解决。

现在将公司总部的客户端R4与分部的客户端R3之间的流量定义为重要流量，通过对其做QoS保证，使得R4与R3能够建立正常的通信。

删除步骤五中R1接口S1/0/0上调用的队列模板。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]undo qos queue-profile
```

在R4上使用**ping**命令测试去往R3的连通性，设置源地址为10.0.145.4，包大小为700字节，发10个包。

```
[R4]ping -a 10.0.145.4 -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=1279 ms
    Request time out
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=1587 ms
    Reply from 10.0.34.3: bytes=700 Sequence=4 ttl=253 time=1827 ms
    Request time out
    Reply from 10.0.34.3: bytes=700 Sequence=6 ttl=253 time=1717 ms
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    4 packet(s) received
    60.00% packet loss
    round-trip min/avg/max = 1279/1602/1827 ms
```

此时公司总部与分部之间的链路发生严重拥塞，丢包现象严重，R4无法与R3建立正常通信。

在R1上创建ACL3001匹配从10.0.145.4去往10.0.34.3的流量。

```
[R1]acl number 3001
[R1-acl-adv-3001]rule 0 per ip source 10.0.145.4 0.0.0.0 destination 10.0.34.3
0.0.0.0
```

创建流分类**class-ef**，匹配ACL3001，创建流行为**behavior-ef**，配置队列调度方式为EF，带宽为10Kbps。

```
[R1]traffic classifier class-ef
[R1-classifier-class-ef]if-match acl 3001
[R1-classifier-class-ef]quit
[R1]traffic behavior behavior-ef
[R1-behavior-behavior-ef]queue ef bandwidth 10
```

创建流分类**class-af32**，匹配DSCP值为AF32的数据流量，创建流行为**behavior-af32**，配置队列调度方式为AF，带宽为30Kbps，与丢弃模板data绑定。

```
[R1]traffic classifier class-af32
[R1-classifier-class-af32]if-match dscp af32
[R1-classifier-class-af32]quit
[R1]traffic behavior behavior-af32
[R1-behavior-behavior-af32]queue af bandwidth 30
[R1-behavior-behavior-af32]drop-profile data
```

创建流策略**policy-1**，关联流分类**class-ef**和流动作**behavior-ef**，流分类**class-af32**和流动作**behavior-af32**，并在R1的接口S1/0/0上应用。

```
[R1]traffic policy policy-1
[R1-trafficpolicy-policy-1]classifier class-ef behavior behavior-ef
[R1-trafficpolicy-policy-1]classifier class-af32 behavior behavior-af32
[R1-trafficpolicy-policy-1]quit
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]traffic-policy policy-1 outbound
```

在R4上使用**ping**命令测试去往R3的连通性，设置每个包大小为700，源地址为10.0.145.4，个数为10。

```
[R4]ping -a 10.0.145.4 -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=694 ms
    Reply from 10.0.34.3: bytes=700 Sequence=2 ttl=253 time=391 ms
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=361 ms
    Reply from 10.0.34.3: bytes=700 Sequence=4 ttl=253 time=671 ms
    Reply from 10.0.34.3: bytes=700 Sequence=5 ttl=253 time=211 ms
    Reply from 10.0.34.3: bytes=700 Sequence=6 ttl=253 time=611 ms
    Reply from 10.0.34.3: bytes=700 Sequence=7 ttl=253 time=688 ms
    Reply from 10.0.34.3: bytes=700 Sequence=8 ttl=253 time=391 ms
    Reply from 10.0.34.3: bytes=700 Sequence=9 ttl=253 time=301 ms
    Reply from 10.0.34.3: bytes=700 Sequence=10 ttl=253 time=651 ms
```

```
  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 211/497/694 ms
```

将R4去往R3的流量设置为EF队列后，现在R4可以与R3建立正常通信。

附加实验：思考并验证

QoS是使用差分服务来实现对不同业务服务质量保证的，保证了带宽和延迟。试想一下，不使用QoS，通过增加带宽的方式是否可以彻底解决服务质量问题？

实验完成后，回想理论课程中关于QoS的逻辑处理过程。将路由器实现QoS的过程总结一下。

最终设备配置

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
acl number 3001
 rule 0 permit ip source 10.0.145.4 0 destination 10.0.34.3 0
#
drop-profile data
wred dscp
  dscp af32 low-limit 50 high-limit 90 discard-percentage 30
#
qos queue-profile queue-profile1
  queue 3 drop-profile data
  schedule wfq 3 pq 5
#
qos map-table dscp-dscp
  input 26 output 0
#
```

```
traffic classifier class-ef operator or
 if-match acl 3001
traffic classifier class-af32 operator or
 if-match dscp af32
#
traffic behavior behavior-ef
 queue ef bandwidth 10 cbs 250
traffic behavior behavior-af32
 queue af bandwidth 30
 drop-profile data
traffic behavior behavir-af32
 queue af bandwidth 30
#
traffic policy policy-1
 classifier class-ef behavior behavior-ef
 classifier class-af32 behavior behavior-af32
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
 trust dscp
 traffic-policy policy-1 outbound
 baudrate 72000
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.1 255.255.255.0
 trust dscp override
#
 ip route-static 10.0.34.0 255.255.255.0 10.0.12.2
#
return

<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.0.34.2 255.255.255.0
```

```
#
 ip route-static 10.0.145.0 255.255.255.0 10.0.12.1
#
return

<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/2
 ip address 10.0.34.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
#
return

<R4>display current-configuration
[V200R007C00SPC600]
#
 sysname R4
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.4 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return

<R5>display current-configuration
[V200R007C00SPC600]
#
 sysname R5
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.5 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return

<S3>display current-configuration
```

```
#
!Software Version V200R008C00SPC500
 sysname S3
#
interface Vlanif1
 ip address 10.0.145.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
nqa test-instance admin udp
 test-type udp
 destination-address ipv4 10.0.34.4
 destination-port 6000
 tos 28
 frequency 3
 interval seconds 1
 timeout 1
 datasize 5800
 start now
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.0.34.4
 destination-port 6000
 tos 46
 frequency 3
 interval milliseconds 20
 timeout 1
 datasize 90
 start now
#
return

<S4>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S4
#
interface Vlanif1
 ip address 10.0.34.4 255.255.255.0
#
 nqa-server udpecho 10.0.34.4 6000
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
```

```
#
return
```

实验 3-2 使用流策略实现流行为控制

学习目的

- 掌握配置端到端QoS的方法
- 掌握使用流策略实现流行为控制的方法

拓扑图

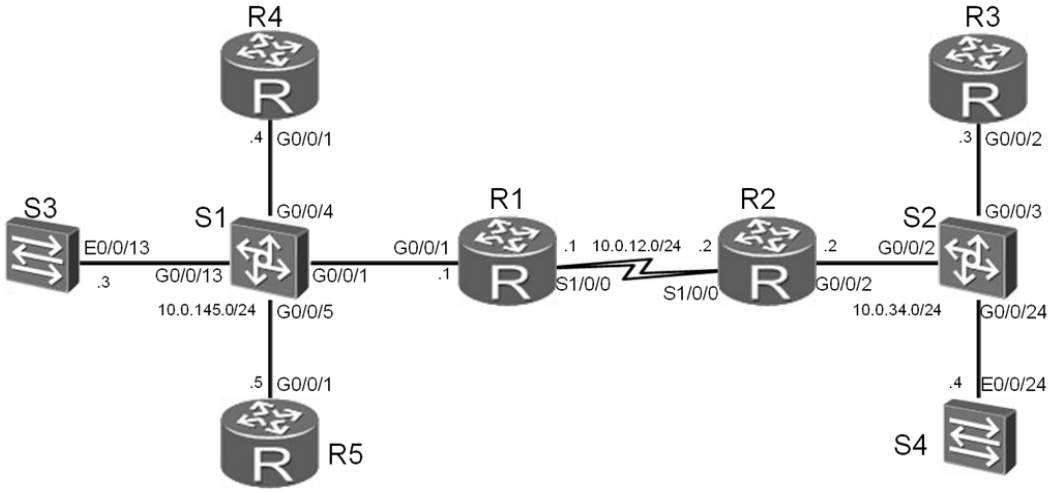


图2-2 使用流策略实现流行为控制

场景

你是公司的网络管理员。公司网络分成两部分，其中R1与S1在公司总部，R2与S2在公司分部，之间通过专线实现互联。随着网络的发展，内网带宽逐渐增大，而专线的带宽一直没有升级，所以网络中出现了比较严重的重要业务反应较慢，或无法正常使用的情况。

部署端到端QoS，你可以调整相应的QoS特性，保证重要的业务数据能更好的发送到目标，并通过流策略实现对流行为的控制。

学习任务

步骤一. 基础配置与 IP 编址

给所有路由器和交换机S3，S4配置IP地址和掩码。

```
<R1>system-view
Enter system view, return user view with Ctrl+Z.
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 255.255.255.0
[R1-Serial1/0/0]quit
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.145.1 255.255.255.0

<R2>system-view
Enter system view, return user view with Ctrl+Z.
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 255.255.255.0
[R2-Serial1/0/0]quit
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.0.34.2 255.255.255.0

<R3>system-view
Enter system view, return user view with Ctrl+Z.
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.34.3 255.255.255.0

<R4> system-view
Enter system view, return user view with Ctrl+Z.
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 10.0.145.4 255.255.255.0

<R5>system-view
Enter system view, return user view with Ctrl+Z.
[R5]interface GigabitEthernet 0/0/1
[R5-GigabitEthernet0/0/1]ip address 10.0.145.5 255.255.255.0

<S3>system-view
Enter system view, return user view with Ctrl+Z.
[S3]interface Vlanif 1
[S3-Vlanif1]ip address 10.0.145.3 255.255.255.0
```

```
<S4>system-view
Enter system view, return user view with Ctrl+Z.
[S4]interface Vlanif 1
[S4-Vlanif1]ip address 10.0.34.4 255.255.255.0
```

配置完成后，测试直连链路的连通性。

```
[R1]ping -c 1 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=36 ms

  --- 10.0.12.2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 36/36/36 ms

[R1]ping -c 1 10.0.145.3
  PING 10.0.145.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.3: bytes=56 Sequence=1 ttl=255 time=35 ms

  --- 10.0.145.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/35/35 ms

[R1]ping -c 1 10.0.145.4
  PING 10.0.145.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.4: bytes=56 Sequence=1 ttl=255 time=6 ms

  --- 10.0.145.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/6/6 ms

[R1]ping -c 1 10.0.145.5
  PING 10.0.145.5: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.5: bytes=56 Sequence=1 ttl=255 time=6 ms

  --- 10.0.145.5 ping statistics ---
```

```
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/6/6 ms

[R2]ping -c 1 10.0.34.3
  PING 10.0.34.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=56 Sequence=1 ttl=255 time=5 ms

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

[R2]ping -c 1 10.0.34.4
  PING 10.0.34.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.4: bytes=56 Sequence=1 ttl=255 time=36 ms

  --- 10.0.34.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 36/36/36 ms
```

步骤二. 配置静态路由

在所有路由器和交换机S3，S4上配置静态路由。

```
[R1]ip route-static 10.0.34.0 255.255.255.0 10.0.12.2

[R2]ip route-static 10.0.145.0 255.255.255.0 10.0.12.1

[R3]ip route-static 0.0.0.0 0.0.0.0 10.0.34.2

[R4]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[R5]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[S3]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
```

```
[S4]ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
```

配置完成后，测试网络连通性。

```
[S3]ping -c 1 10.0.34.4
  PING 10.0.34.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.4: bytes=56 Sequence=1 ttl=252 time=40 ms

  --- 10.0.34.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/40/40 ms

[R4]ping -c 1 10.0.34.3
  PING 10.0.145.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.4: bytes=56 Sequence=1 ttl=255 time=3 ms

  --- 10.0.145.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms

[R5]ping -c 1 10.0.34.3
  PING 10.0.34.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=56 Sequence=1 ttl=253 time=44 ms

  --- 10.0.34.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 44/44/44 ms
```

步骤三. 配置 DSCP 优先级的重标记

公司网络中有语音，视频，数据三种业务，但是由于公司总部与分部之间的专线仍然没有得到升级，所以网络不可避免的出现了拥塞。

通过配置端到端的QoS来实现语音报文的优先发送，视频报文的带宽保证。

将R4与R3之间的流量模拟为语音报文，将R5与R3之间的流量模拟为视频报

文，将S3与S4之间的报文模拟为数据报文。接下来将针对语音报文和视频报文做一系列相关的QoS策略，对数据报文采用默认的尽力而为的传输。

现在将语音报文的DSCP值标记为EF，视频报文的DSCP值标记为AF32。

在S1上创建ACL3001，3002，分别匹配R4去往R3，R5去往R3的流量。

```
[S1]acl number 3001
[S1-acl-adv-3001]rule 0 permit ip source 10.0.145.4 0 destination 10.0.34.3 0
[S1-acl-adv-3001]quit
[S1]acl number 3002
[S1-acl-adv-3002]rule 0 permit ip source 10.0.145.5 0 destination 10.0.34.3 0
```

在S1上创建流分类class-voice-s1，匹配ACL3001。创建流行为behavior-voice-s1，将DSCP优先级重标记为EF。

创建流策略policy-voice-s1，关联流分类class-voice-s1与流行为behavior-voice-s1，在S1上的G0/0/4接口入方向上调用该流策略。

```
[S1]traffic classifier class-voice-s1
[S1-classifier-class-voice-s1]if-match acl 3001
[S1-classifier-class-voice-s1]quit
[S1]traffic behavior behavior-voice-s1
[S1-behavior-behavior-voice-s1]remark dscp ef
[S1-behavior-behavior-voice-s1]quit
[S1]traffic policy policy-voice-s1
[S1-trafficpolicy-policy-voice-s1]classifier class-voice-s1 behavior
behavior-voice-s1
[S1-trafficpolicy-policy-voice-s1]quit
[S1]interface GigabitEthernet 0/0/4
[S1-GigabitEthernet0/0/4]traffic-policy policy-voice-s1 inbound
```

在S1上创建流分类class-video-s1，匹配ACL3002。创建流行为behavior-video-s1，将DSCP优先级重标记为AF32。

创建流策略policy-video-s1，关联流分类class-video-s1与流行为behavior-video-s1，在S1上的G0/0/5接口入方向上应用该流策略。

```
[S1]traffic classifier class-video-s1
[S1-classifier-class-video-s1]if-match acl 3002
[S1-classifier-class-video-s1]quit
[S1]traffic behavior behavior-video-s1
[S1-behavior-behavior-video-s1]remark dscp af32
[S1-behavior-behavior-video-s1]quit
[S1]traffic policy policy-video-s1
[S1-trafficpolicy-policy-video-s1]classifier class-video-s1 behavior
```

```
behavior-video-s1
[S1-trafficpolicy-policy-video-s1]quit
[S1]interface GigabitEthernet 0/0/5
[S1-GigabitEthernet0/0/5]traffic-policy policy-video-s1 inbound
```

在S2上创建ACL3001，3002，分别匹配R3去往R4，R3去往R5的流量。

```
[S2]acl number 3001
[S2-acl-adv-3001]rule 0 permit ip source 10.0.34.3 0 destination 10.0.145.4 0
[S2-acl-adv-3001]quit
[S2]acl number 3002
[S2-acl-adv-3002]rule 0 permit ip source 10.0.34.3 0 destination 10.0.145.5 0
```

在S2上创建流分类class-voice-s2，匹配ACL3001。创建流行为behavior-voice-s2，将DSCP优先级重标记为EF。

```
[S2]traffic classifier class-voice-s2
[S2-classifier-class-voice-s2]if-match acl 3001
[S2-classifier-class-voice-s2]quit
[S2]traffic behavior behavior-voice-s2
[S2-behavior-behavior-voice-s2]remark dscp ef
```

在S2上创建流分类class-video-s2，匹配ACL3002。创建流行为behavior-video-s2，将DSCP优先级重标记为AF32。

```
[S2]traffic classifier class-video-s2
[S2-classifier-class-video-s2]if-match acl 3002
[S2-classifier-class-video-s2]quit
[S2]traffic behavior behavior-video-s2
[S2-behavior-behavior-video-s2]remark dscp af32
```

在S2上创建流策略policy-voice-video-s2，关联流分类class-voice-s2与流行为behavior-voice-s2，关联流分类class-video-s2与流行为behavior-video-s2，在S2上的G0/0/3接口入方向上应用该流策略。

```
[S2]traffic policy policy-voice-video-s2
[S2-trafficpolicy-policy-voice-video-s2]classifier class-voice-s2 behavior
behavior-voice-s2
[S2-trafficpolicy-policy-voice-video-s2]classifier class-video-s2 behavior
behavior-video-s2
[S2-trafficpolicy-policy-voice-video-s2]quit
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]traffic-policy policy-voice-video-s2 inbound
```

步骤四. 配置流量整形和监管

在公司总部和分部的核心交换机上部署流量整形，缓解流量拥塞的问题。

在S1上的接口G0/0/1出方向上配置流量整形，CIR设为128kbit/s。

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]qos lr outbound cir 128
```

查看流量整形配置信息。

```
[S1]display qos lr outbound interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 lr outbound:
  cir: 128 Kbps, cbs: 16000 Byte
```

在S2上的接口G0/0/2出方向上配置流量整形，CIR设为128kbit/s。

```
[S2]interface GigabitEthernet 0/0/2
[S2-GigabitEthernet0/0/2]qos lr outbound cir 128
```

查看流量整形配置信息。

```
[S2]display qos lr outbound interface GigabitEthernet 0/0/2
GigabitEthernet0/0/2 lr outbound:
  cir: 128 Kbps, cbs: 16000 Byte
```

在公司总部和分部的出口路由器上部署流量监管，进一步缓解流量拥塞的问题。

在R1上的G0/0/1接口入方向上配置流量监管，CIR设为72kbit/s。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]qos car inbound cir 72
```

在R2上的G0/0/2接口入方向上配置流量监管，CIR设为72kbit/s。

```
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]qos car inbound cir 72
```

步骤五. 配置基于流策略的拥塞管理与拥塞避免

在公司总部与分部的出口路由器上部署基于流策略的拥塞管理与拥塞避免。保证语音流量低延迟，优先发送，保证视频流量拥有足够的带宽。

配置R1上的G0/0/1接口配置信任DSCP优先级。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]trust dscp
```

在R1上创建WRED丢弃模板video-r1，使其基于DSCP优先级进行丢弃，将阀值下限设为50，上限设为90，丢弃概率设为30，

```
[R1]drop-profile video-r1
[R1-drop-profile-video-r1]wred dscp
[R1-drop-profile-video-r1]dscp af32 low-limit 50 high-limit 90
discard-percentage 30
```

在R1上创建流分类class-af32-r1，匹配DSCP值为AF32的视频流量。创建流行为behavior-af32-r1，配置队列调度方式为AF，最大带宽占接口带宽百分比设为40，并与丢弃模板video-r1绑定。

```
[R1]traffic classifier class-af32-r1
[R1-classifier-class-af32-r1]if-match dscp af32
[R1-classifier-class-af32-r1]quit
[R1]traffic behavior behavior-af32-r1
[R1-behavior-behavior-af32-r1]queue af bandwidth pct 40
[R1-behavior-behavior-af32-r1]drop-profile video-r1
```

在R1上创建流分类class-ef-r1，匹配DSCP值为EF的语音流量。创建流行为behavior-ef-r1，配置队列的调度方式为EF，最大带宽占接口带宽百分比设为30。

```
[R1]traffic classifier class-ef-r1
[R1-classifier-class-ef-r1]if-match dscp ef
[R1-classifier-class-ef-r1]quit
[R1]traffic behavior behavior-ef-r1
[R1-behavior-behavior-ef-r1]queue ef bandwidth pct 30
```

在R1上创建流策略policy-r1，关联流分类class-af32-r1与流行为behavior-af32-r1，关联流分类class-ef-r1与流行为behavior-ef-r1，并在接口S1/0/0的出方向上应用。

```
[R1]traffic policy policy-r1
[R1-trafficpolicy-policy-r1]classifier class-af32-r1 behavior behavior-af32-r1
[R1-trafficpolicy-policy-r1]classifier class-ef-r1 behavior behavior-ef-r1
[R1-trafficpolicy-policy-r1]interface Serial 1/0/0
[R1-Serial1/0/0]traffic-policy policy-r1 outbound
```

在公司总部R1上配置完后，在公司分部R2上也作相应配置。

配置R2的接口G0/0/2信任DSCP优先级。

```
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]trust dscp
```

在R2上创建WRED丢弃模板video-r2，使其基于DSCP优先级进行丢弃，将阀值下限设为50，上限设为90，丢弃概率设为30，

```
[R2]drop-profile video-r2
[R2-drop-profile-video-r2]wred dscp
[R2-drop-profile-video-r2]dscp af32 low-limit 50 high-limit 90
discard-percentage 30
```

在R1上创建流分类class-af32-r2，匹配DSCP值为AF32的视频流量。创建流行为behavior-af32-r2，配置队列调度方式为AF，最大带宽占接口带宽百分比设为40，并与丢弃模板video-r2绑定。

```
[R2]traffic classifier class-af32-r2
[R2-classifier-class-af32-r2]if-match dscp af32
[R2-classifier-class-af32-r2]traffic behavior behavior-af32-r2
[R2-behavior-behavior-af32-r2]queue af bandwidth pct 40
[R2-behavior-behavior-af32-r2]drop-profile video-r2
```

在R1上创建流分类class-ef-r2，匹配DSCP值为EF的语音流量。创建流行为behavior-ef-r2，配置队列的调度方式为EF，最大带宽占接口带宽百分比设为30。

```
[R2]traffic classifier class-ef-r2
[R2-classifier-class-ef-r2]if-match dscp ef
[R2-classifier-class-ef-r2]traffic behavior behavior-ef-r2
[R2-behavior-behavior-ef-r2]queue ef bandwidth pct 30
```

在R1上创建流策略policy-r2，关联流分类class-af32-r2与流行为behavior-af32-r2，关联流分类class-ef-r1与流行为behavior-ef-r2，并在接口S1/0/0的出方向上应用。

```
[R2]traffic policy policy-r2
[R2-trafficpolicy-policy-r2]classifier class-af32-r2 behavior behavior-af32-r2
[R2-trafficpolicy-policy-r2]classifier class-ef-r2 behavior behavior-ef-r2
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]traffic-policy policy-r2 outbound
```

步骤六. 配置基于流策略实现流行为控制

公司总部现在出于优化的的目的将针对部分流量做控制，丢弃掉UDP端口号4000至5000部分的视频流量。

在R1上创建ACL3003，匹配从R5去往R3，UDP端口范围为4000至5000部分的流量。

```
[R1]acl number 3003
[R1-acl-adv-3003]rule 0 permit udp source-port range 4000 5000 source 10.0.145.5
0 destination 10.0.34.3 0
```

在R1上创建流分类class-drop，匹配ACL3003，

```
[R1]traffic classifier class-drop
[R1-classifier-class-drop]if-match acl 3003
```

在R1上创建流行为behavior-drop，配置命令**deny**，执行禁止动作，

```
[R1]traffic behavior behavior-drop
[R1-behavior-behavior-drop]deny
```

在R1上创建流策略policy-drop，关联流分类class-drop与流行为behavior-drop，并在接口G0/0/5的入方向上应用。

```
[R1]traffic policy policy-drop
[R1-trafficpolicy-policy-drop]classifier class-drop behavior behavior-drop
[R1-trafficpolicy-policy-drop]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]traffic-policy policy-drop inbound
```

查看配置信息。

```
[R1]display traffic policy user-defined policy-drop
  User Defined Traffic Policy Information:
    Policy: policy-drop
    Classifier: class-drop
    Operator: OR
    Behavior: behavior-drop
    Deny
```

附加实验：思考并验证

实验完成后，回顾QoS的知识框架，总结QoS中各项策略的使用范围与应用场景。

最终设备配置

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
acl number 3003
 rule 0 permit udp source 10.0.145.5 0 source-port range 4000 5000 destination
10.0.34.3 0
#
drop-profile video-r1
wred dscp
  dscp af32 low-limit 50 high-limit 90 discard-percentage 30
#
traffic classifier class-drop operator or
 if-match acl 3003
traffic classifier class-ef-r1 operator or
 if-match dscp ef
traffic classifier class-af32-r1 operator or
 if-match dscp af32
#
traffic behavior behavior-af32-r1
 queue af bandwidth pct 40
 drop-profile video-r1
traffic behavior behavior-ef-r1
 queue ef bandwidth pct 30
traffic behavior behavior-drop
 deny
#
traffic policy policy-drop
 classifier class-drop behavior behavior-drop
traffic policy policy-r1
 classifier class-af32-r1 behavior behavior-af32-r1
 classifier class-ef-r1 behavior behavior-ef-r1
#
```

```
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
 traffic-policy policy-r1 outbound
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.1 255.255.255.0
 trust dscp
 qos car inbound cir 72 cbs 13536 pbs 22536 green pass yellow pass red discard
 traffic-policy policy-drop inbound
#
 ip route-static 10.0.34.0 255.255.255.0 10.0.12.2
#
return
```

```
<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
drop-profile video-r2
wred dscp
  dscp af32 low-limit 50 high-limit 90 discard-percentage 30
#
traffic classifier class-ef-r2 operator or
 if-match dscp ef
traffic classifier class-af32-r2 operator or
 if-match dscp af32
#
traffic behavior behavior-af32-r2
 queue af bandwidth pct 40
 drop-profile video-r2
traffic behavior behavior-ef-r2
 queue ef bandwidth pct 30
#
traffic policy policy-r2
 classifier class-af32-r2 behavior behavior-af32-r2
 classifier class-ef-r2 behavior behavior-ef-r2
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.2 255.255.255.0
```

```
 traffic-policy policy-r2 outbound
#
interface GigabitEthernet0/0/2
 ip address 10.0.34.2 255.255.255.0
 trust dscp
 qos car inbound cir 72 cbs 13536 pbs 22536 green pass yellow pass red discard
#
 ip route-static 10.0.145.0 255.255.255.0 10.0.12.1
#
return

<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/2
 ip address 10.0.34.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
#
return

<R4>display current-configuration
[V200R007C00SPC600]
#
 sysname R4
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.4 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return

<R5>display current-configuration
[V200R007C00SPC600]
#
 sysname R5
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.5 255.255.255.0
```

```
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return

<S1>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
#
acl number 3001
 rule 0 permit ip source 10.0.145.4 0 destination 10.0.34.3 0
acl number 3002
 rule 0 permit ip source 10.0.145.5 0 destination 10.0.34.3 0
#
traffic classifier class-video-s1 operator and
 if-match acl 3002
traffic classifier class-voice-s1 operator and
 if-match acl 3001
#
traffic behavior behavior-video-s1
 remark dscp af32
traffic behavior behavior-voice-s1
 remark dscp ef
#
traffic policy policy-video-s1
 classifier class-video-s1 behavior behavior-video-s1
traffic policy policy-voice-s1
 classifier class-voice-s1 behavior behavior-voice-s1
#
interface GigabitEthernet0/0/1
 qos lr outbound cir 128 cbs 16000
#
interface GigabitEthernet0/0/4
 traffic-policy policy-voice-s1 inbound
#
interface GigabitEthernet0/0/5
 traffic-policy policy-video-s1 inbound
#
return

<S2>display current-configuration
```

```
#
!Software Version V200R008C00SPC500
 sysname S2
#
acl number 3001
 rule 0 permit ip source 10.0.34.3 0 destination 10.0.145.4 0
acl number 3002
 rule 0 permit ip source 10.0.34.3 0 destination 10.0.145.5 0
#
traffic classifier class-video-s2 operator and
 if-match acl 3002
traffic classifier class-voice-s2 operator and
 if-match acl 3001
#
traffic behavior behavior-video-s2
 remark dscp af32
traffic behavior behavior-voice-s2
 remark dscp ef
#
traffic policy policy-voice-video-s2
 classifier class-voice-s2 behavior behavior-voice-s2
 classifier class-video-s2 behavior behavior-video-s2
#
interface GigabitEthernet0/0/2
 qos lr outbound cir 128 cbs 16000
#
interface GigabitEthernet0/0/3
 traffic-policy policy-voice-video-s2 inbound
#
return

<S3>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S3
#
interface Vlanif1
 ip address 10.0.145.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return
```

```
<S4>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S4
#
interface Vlanif1
 ip address 10.0.34.4 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
#
return
```

第四章 防火墙

实验 4-1 防火墙安全区域及安全策略配置

学习目的

- 掌握防火墙安全区域的配置方法
- 掌握安全策略配置方法

拓扑图

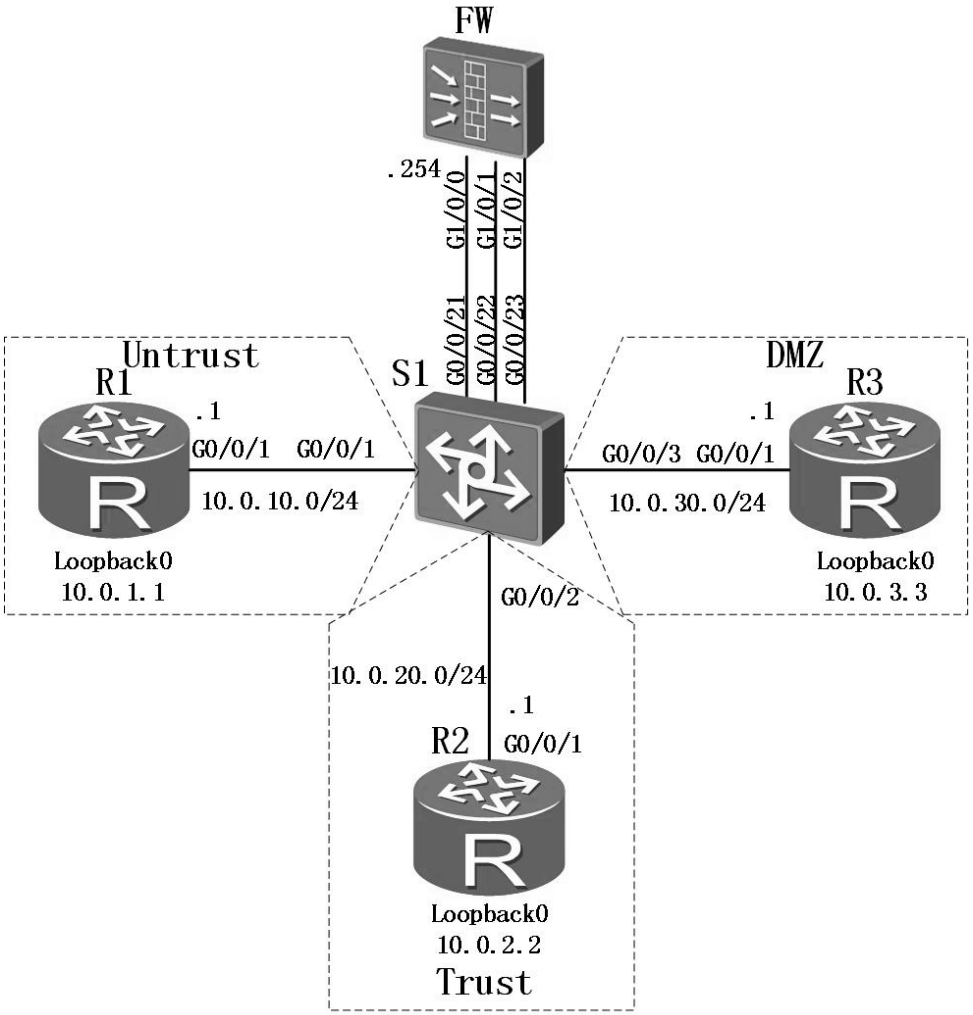


图1-1 防火墙区域配置

场景

你是你们公司的网络管理员。公司总部的网络分成了三个区域，包括内部区域（Trust）、外部区域（Untrust）和服务器区域（DMZ）。你设计通过防火墙来实现对数据的控制，确保公司内部网络安全，并通过DMZ区域对外网提供服务。

学习任务

步骤一. 登录设备（Console）

1．连接配置口电缆。

a. 关闭FW及配置终端的电源。

b. 通过配置电缆将配置终端的RS-232串口与FW的Console口相连。

c. 经安装检查后上电。

2．超级终端软件的配置（可以从Internet上获取如putty等免费超级终端软件。）。

a. 下载putty软件到本地并双击运行该软件。

b. 选择“Session”，将“Connection type”设置为“Serial”。

c. 配置通过串口连接设备的参数。具体参数配置如图5所示。

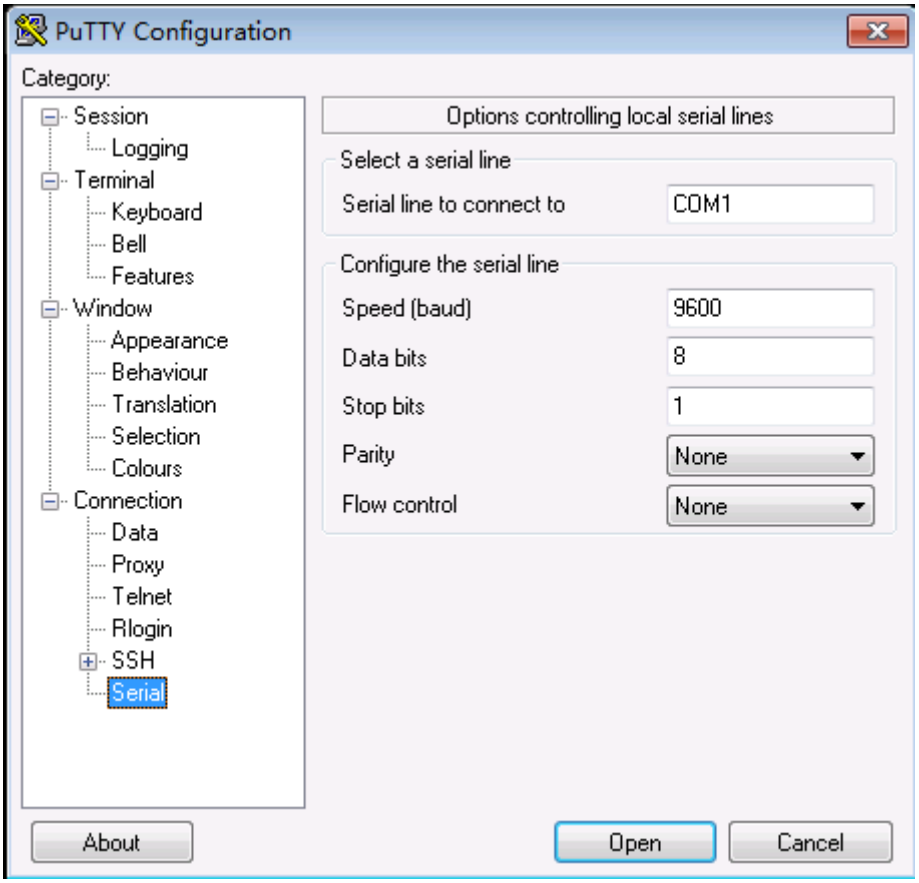


图5 putty软件Serial连接FW参数配置

d. 单击“Open”。

3. 按“Enter”键，按照提示输入缺省管理员账号“admin”和密码“Admin@123”。

4. 修改缺省管理员账号的密码，并进入CLI界面。

说明：为提高安全性，密码必须满足最小复杂度要求，即包含英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）、特殊字符（如!、@、#、$、%等）中的三种。

请牢记输入的新密码避免无法登录。

步骤二. 基本配置与 IP 编址

给路由器和防火墙配置地址，并配置静态路由，在交换机上配置VLAN。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
```

```
[R1-GigabitEthernet0/0/1]ip address 10.0.10.1 24
[R1-GigabitEthernet0/0/1]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.20.1 24
[R2-GigabitEthernet0/0/1]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.30.1 24
[R3-GigabitEthernet0/0/1]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24
```

防火墙默认会启用GigabitEthernet0/0/0接口的ip地址，为避免干扰，可以删除。

```
<USG6300>system-view
Enter system view, return user view with Ctrl+Z.
[USG6300]sysname FW
[FW]int GigabitEthernet 0/0/0
[FW-GigabitEthernet0/0/0]undo ip address
[FW-GigabitEthernet0/0/0]interface GigabitEthernet 1/0/0
[FW-GigabitEthernet1/0/0]ip address 10.0.10.254 24
[FW-GigabitEthernet1/0/0]interface GigabitEthernet 1/0/1
[FW-GigabitEthernet1/0/1]ip address 10.0.20.254 24
[FW-GigabitEthernet1/0/1]interface GigabitEthernet 1/0/2
[FW-GigabitEthernet1/0/2]ip address 10.0.30.254 24
[FW-GigabitEthernet1/0/2]quit
```

交换机上需要按照需求定义VLAN。

```
[Quidway]sysname S1
[S1]vlan batch 11 to 13
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 11
```

```
[S1-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type access
[S1-GigabitEthernet0/0/2]port default vlan 12
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 13
[S1-GigabitEthernet0/0/3]interface GigabitEthernet 0/0/21
[S1-GigabitEthernet0/0/21]port link-type access
[S1-GigabitEthernet0/0/21]port default vlan 11
[S1-GigabitEthernet0/0/21]interface GigabitEthernet 0/0/22
[S1-GigabitEthernet0/0/22]port link-type access
[S1-GigabitEthernet0/0/22]port default vlan 12
[S1-GigabitEthernet0/0/22]interface GigabitEthernet 0/0/23
[S1-GigabitEthernet0/0/23]port link-type access
[S1-GigabitEthernet0/0/23]port default vlan 13
```

在R1、R2和R3上配置缺省路由，在FW上配置明确的静态路由，实现三个Loopback0接口连接的网段之间路由畅通。

```
[R1]ip route-static 0.0.0.0 0 10.0.10.254

[R2]ip route-static 0.0.0.0 0 10.0.20.254

[R3]ip route-static 0.0.0.0 0 10.0.30.254

[FW]ip route-static 10.0.1.0 24 10.0.10.1
[FW]ip route-static 10.0.2.0 24 10.0.20.1
[FW]ip route-static 10.0.3.0 24 10.0.30.1
```

配置完成后检查防火墙路由信息。

```
[FW]display ip routing-table

Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Routing Tables: Public
       Destinations : 11      Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.1.0/24  Static  60   0           RD  10.0.10.1
GigabitEthernet1/0/0
```

```
      10.0.2.0/24  Static  60   0         RD  10.0.20.1
GigabitEthernet1/0/1
      10.0.3.0/24  Static  60   0         RD  10.0.30.1
GigabitEthernet1/0/2
     10.0.10.0/24  Direct  0    0          D  10.0.10.254
GigabitEthernet1/0/0
    10.0.10.254/32  Direct  0    0          D  127.0.0.1      InLoopBack0
     10.0.20.0/24  Direct  0    0          D  10.0.20.254
GigabitEthernet1/0/1
    10.0.20.254/32  Direct  0    0          D  127.0.0.1      InLoopBack0
     10.0.30.0/24  Direct  0    0          D  10.0.30.254
GigabitEthernet1/0/2
    10.0.30.254/32  Direct  0    0          D  127.0.0.1      InLoopBack0
      127.0.0.0/8   Direct  0    0          D  127.0.0.1      InLoopBack0
      127.0.0.1/32  Direct  0    0          D  127.0.0.1      InLoopBack0
```

步骤三. 配置防火墙区域

防火墙上默认有四个区域，分别是“local“、” trust “、” untrust “、” dmz “。实验中我们使用到“trust “、” untrust “和” dmz “三个区域，分别将对应接口加入各安全区域，由于默认配置将GE0/0/0加入了“trust”区域，为避免干扰，将其删除。

```
[FW]firewall zone dmz
[FW-zone-dmz]add interface GigabitEthernet 1/0/2
[FW-zone-dmz]firewall zone trust
[FW-zone-trust]add interface GigabitEthernet 1/0/1
[FW-zone-trust]undo add interface GigabitEthernet 0/0/0
[FW-zone-trust]fire zone untrust
[FW-zone-untrust]add interface GigabitEthernet 1/0/0
[FW-zone-untrust]quit
```

检查各接口的区域：

```
[FW]display zone interface

local
#
trust
 interface of the zone is (1):
```

```
    GigabitEthernet1/0/1
#
untrust
 interface of the zone is (1):
    GigabitEthernet1/0/0
#
dmz
 interface of the zone is (1):
    GigabitEthernet1/0/2
#
```

检查各区域的优先级：

```
[FW]display zone

local
 priority is 100
#
trust
 priority is 85
 interface of the zone is (1):
    GigabitEthernet1/0/1
#
untrust
 priority is 5
 interface of the zone is (1):
    GigabitEthernet1/0/0
#
dmz
 priority is 50
 interface of the zone is (1):
    GigabitEthernet1/0/2
#
```

可以看到三个接口已经被划分到相应的区域内，默认情况下不同区域间是不可互通的，因此此时路由器之间流量无法通过。

步骤四. 配置安全策略

如果防火墙域间没有配置安全策略，或查找安全策略时，所有的安全策略都没有命中，则默认执行域间的缺省包过滤动作（拒绝通过）。

配置安全策略，仅允许Trust区域访问其他区域，不允许其他区域之间的访问。

```
[FW]security-policy
[FW-policy-security]rule name policy_sec_1
[FW-policy-security-rule-policy_sec_1]source-zone trust
[FW-policy-security-rule-policy_sec_1]destination-zone untrust
[FW-policy-security-rule-policy_sec_1]action permit
[FW-policy-security-rule-policy_sec_1]rule name policy_sec_2
[FW-policy-security-rule-policy_sec_2]source-zone trust
[FW-policy-security-rule-policy_sec_2]destination-zone dmz
[FW-policy-security-rule-policy_sec_2]action permit
[FW-policy-security-rule-policy_sec_2]quit
[FW-policy-security]quit
```

检查配置结果：

```
[FW]display security-policy all

Total:3
RULE ID RULE NAME                    STATE     ACTION           HITTED
------------------------------------------------------------------------------
---
0      default                      enable    deny             0
1      policy_sec_1                  enable    permit           0
2      policy_sec_2                  enable    permit           0
------------------------------------------------------------------------------
---
[FW]display security-policy rule policy_sec_1

  (0 times matched)
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  action permit

[FW]display security-policy rule policy_sec_2

  (0 times matched)
 rule name policy_sec_2
  source-zone trust
  destination-zone dmz
  action permit
```

检查从trust到untrust和dmz的连通性：

```
[R2]ping -a 10.0.2.2 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

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

[R2]ping -a 10.0.2.2 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=254 time=1 ms

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

检查从untrust到trust和dmz的连通性：

```
[R1]ping -a 10.0.1.1 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
```

```
    0 packet(s) received
    100.00% packet loss

[R1]ping -a 10.0.1.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

检查从dmz到untrust和trust的连通性：

```
[R3]ping -a 10.0.3.3 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

[R3]ping -a 10.0.3.3 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
```

```
  100.00% packet loss
```

经过验证，以trust区域为源的数据可以访问untrust和dmz，但以其他区域为源的数据不能互访。

配置域间包过滤策略，允许Untrust区域访问DMZ区域的特定服务器。

DMZ区域有一个服务器，IP地址为10.0.3.3，需要对Untrust区域开放Telnet服务。同时为了测试网络，需要开放ICMP Ping测试功能。

```
[FW-policy-security-rule-policy_sec_3]source-zone untrust
[FW-policy-security-rule-policy_sec_3]destination-zone dmz
[FW-policy-security-rule-policy_sec_3]destination-address 10.0.3.3 mask
255.255.255.255
[FW-policy-security-rule-policy_sec_3]service icmp
[FW-policy-security-rule-policy_sec_3]service telnet
[FW-policy-security-rule-policy_sec_3]action permit
```

为了能在进行Telnet测试，在R3上开启Telnet功能。

```
[R3]telnet server enable
[R3]aaa
[R3-aaa]local-user test password irreversible-cipher Admin@123
[R3-aaa]local-user test service-type telnet
[R3-aaa]quit
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode aaa
[R3-ui-vty0-4]protocol inbound telnet
```

测试从R1(untrust)到R3(dmz)的ping和telnet：

```
<R1>ping 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=254 time=1 ms

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

```
<R1>ping 10.0.30.1
  PING 10.0.30.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.30.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

<R1>telnet 10.0.3.3
  Press CTRL_] to quit telnet mode
  Trying 10.0.3.3 ...
  Connected to 10.0.3.3 ...

Login authentication


Username:test
Password:

------------------------------------------------------------------------------
-
  User last login information:

------------------------------------------------------------------------------
-
  Access Type: Telnet
  IP-Address : 10.0.10.1
  Time       : 2016-09-25 03:29:23+00:00

------------------------------------------------------------------------------
-
<R3>quit

  Info:Configuration console exit, please retry to log on

  The connection was closed by the remote host
```

```
<R1>telnet 10.0.30.1
  Press CTRL_] to quit telnet mode
  Trying 10.0.30.1 ...
  Error: Can't connect to the remote host
<R1>
```

根据验证可知，只有访问指定地址的icmp和telnet可以通过，其他流量全部禁止。

最终设备配置

```
<S1>display current-configuration
!Software Version V200R008C00SPC500
#
sysname S1
#
vlan batch 11 to 13
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 13
#
interface GigabitEthernet0/0/21
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/22
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/23
 port link-type access
 port default vlan 13
```

```
#
return

<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.10.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.10.254
#
return

<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
interface GigabitEthernet0/0/1
 ip address 10.0.20.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.20.254
#
return

<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
aaa
 local-user test password irreversible-cipher Admin@123
 local-user test privilege level 0
 local-user test service-type telnet
```

```
#
interface GigabitEthernet0/0/1
 ip address 10.0.30.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
 telnet server enable
#
ip route-static 0.0.0.0 0.0.0.0 10.0.30.254
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound telnet
#
return
```

```
<FW>display current-configuration
#
 sysname FW
#
interface GigabitEthernet1/0/0
 ip address 10.0.10.254 255.255.255.0
#
interface GigabitEthernet1/0/1
 ip address 10.0.20.254 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.0.30.254 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/0
#
firewall zone dmz
```

```
 set priority 50
 add interface GigabitEthernet1/0/2
#
 ip route-static 10.0.1.0 255.255.255.0 10.0.10.1
 ip route-static 10.0.2.0 255.255.255.0 10.0.20.1
 ip route-static 10.0.3.0 255.255.255.0 10.0.30.1
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  action permit
 rule name policy_sec_2
  source-zone trust
  destination-zone dmz
  action permit
 rule name policy_sec_3
  source-zone untrust
  destination-zone dmz
  destination-address 10.0.3.3 mask 255.255.255.255
  service icmp
  service telnet
  action permit
#
return
```

实验 4-2 防火墙 NAT 配置

学习目的

- 掌握在防火墙上基于地址池配置NAPT的方法
- 掌握在防火墙上配置NAT Server的方法

拓扑图

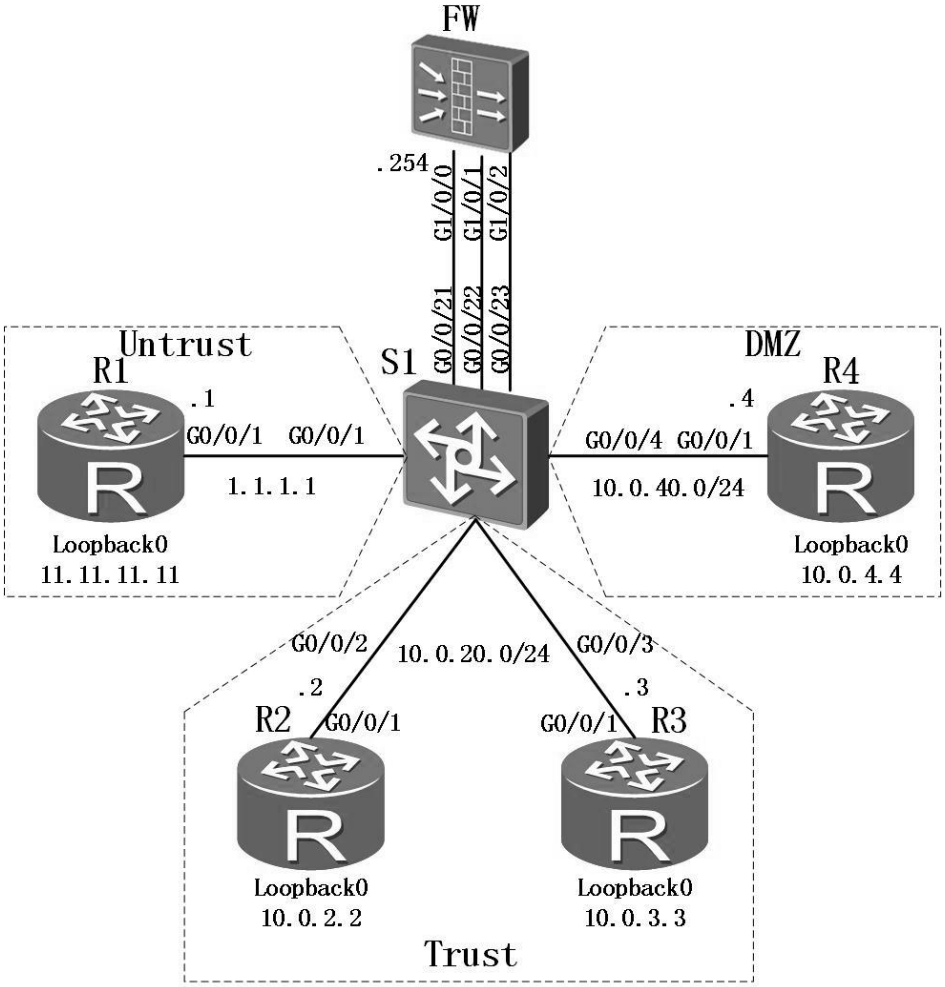


图1-4 防火墙NAT配置

场景

你是你们公司的网络管理员。公司的网络使用防火墙隔离成三个区域。现在内部网络Trust区域的用户需要能够访问外部区域。并且需要将DMZ区域中的一台服务器（IP地址为10.0.4.4）提供的Telnet服务和FTP服务发布出去，对外公开的地址为1.1.1.100/24。

学习任务

步骤一. 基本配置与 IP 编址

给路由器和防火墙配置地址，并配置静态路由，在交换机上配置VLAN。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 1.1.1.1 24
[R1-GigabitEthernet0/0/1]interface loopback 0
[R1-LoopBack0]ip address 11.11.11.11 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.20.2 24
[R2-GigabitEthernet0/0/1]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.20.3 24
[R3-GigabitEthernet0/0/1]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 10.0.40.4 24
[R4-GigabitEthernet0/0/1]interface loopback 0
[R4-LoopBack0]ip address 10.0.4.4 24
```

防火墙默认会启用GigabitEthernet0/0/0接口的ip地址，为避免干扰，可以删除。

```
<USG6300>system-view
```

```
Enter system view, return user view with Ctrl+Z.
[USG6300]sysname FW
[FW]int GigabitEthernet 0/0/0
[FW-GigabitEthernet0/0/0]undo ip address
[FW-GigabitEthernet0/0/0]interface GigabitEthernet 1/0/0
[FW-GigabitEthernet1/0/0]ip address 10.0.10.254 24
[FW-GigabitEthernet1/0/0]interface GigabitEthernet 1/0/1
[FW-GigabitEthernet1/0/1]ip address 10.0.20.254 24
[FW-GigabitEthernet1/0/1]interface GigabitEthernet 1/0/2
[FW-GigabitEthernet1/0/2]ip address 10.0.40.254 24
[FW-GigabitEthernet1/0/2]quit
```

交换机上需要按照需求定义VLAN。

```
[Quidway]sysname S1
[S1]vlan batch 11 to 13
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 11
[S1-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type access
[S1-GigabitEthernet0/0/2]port default vlan 12
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 12
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/4
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 13
[S1-GigabitEthernet0/0/3]interface GigabitEthernet 0/0/21
[S1-GigabitEthernet0/0/21]port link-type access
[S1-GigabitEthernet0/0/21]port default vlan 11
[S1-GigabitEthernet0/0/21]interface GigabitEthernet 0/0/22
[S1-GigabitEthernet0/0/22]port link-type access
[S1-GigabitEthernet0/0/22]port default vlan 12
[S1-GigabitEthernet0/0/22]interface GigabitEthernet 0/0/23
[S1-GigabitEthernet0/0/23]port link-type access
[S1-GigabitEthernet0/0/23]port default vlan 13
```

在R2、R3和R4上配置缺省路由，在FW上配置明确的静态路由，实现四个Loopback0接口连接的网段之间的互通。R1无需定义缺省路由，原因是其作为Internet设备，它不需要知道内部和DMZ区域的私有网络信息。

```
[R2]ip route-static 0.0.0.0 0 10.0.20.254
```

```
[R3]ip route-static 0.0.0.0 0 10.0.20.254

[R4]ip route-static 0.0.0.0 0 10.0.40.254

[FW]ip route-static 10.0.2.0 24 10.0.20.2
[FW]ip route-static 10.0.3.0 24 10.0.20.3
[FW]ip route-static 10.0.4.0 24 10.0.40.4
[FW]ip route-static 0.0.0.0 0 1.1.1.1
```

配置完成后检查防火墙路由信息。

```
[FW]display ip routing-table
06:44:57  2016/09/25
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Routing Tables: Public
       Destinations : 12      Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       0.0.0.0/0   Static  60   0           RD  1.1.1.1
GigabitEthernet1/0/0
       1.1.1.0/24  Direct  0    0           D  1.1.1.254
GigabitEthernet1/0/0
     1.1.1.254/32  Direct  0    0           D  127.0.0.1       InLoopBack0
      10.0.2.0/24  Static  60   0           RD  10.0.20.2
GigabitEthernet1/0/1
      10.0.3.0/24  Static  60   0           RD  10.0.20.3
GigabitEthernet1/0/1
      10.0.4.0/24  Static  60   0           RD  10.0.40.4
GigabitEthernet1/0/2
     10.0.20.0/24  Direct  0    0           D  10.0.20.254
GigabitEthernet1/0/1
   10.0.20.254/32  Direct  0    0           D  127.0.0.1       InLoopBack0
     10.0.40.0/24  Direct  0    0           D  10.0.40.254
GigabitEthernet1/0/2
   10.0.40.254/32  Direct  0    0           D  127.0.0.1       InLoopBack0
     127.0.0.0/8   Direct  0    0           D  127.0.0.1       InLoopBack0
     127.0.0.1/32  Direct  0    0           D  127.0.0.1       InLoopBack0
```

步骤二. 将接口配置到安全区域

防火墙上默认有四个区域，分别是“local “、” trust “、” untrust “、” dmz “。实验中我们使用到“trust “、” untrust “和” dmz “三个区域，分别将对应接口加入各安全区域，由于默认配置将GE0/0/0加入了“trust”区域，为避免干扰，将其删除。

```
[FW]firewall zone dmz
[FW-zone-dmz]add interface GigabitEthernet 1/0/2
[FW-zone-dmz]firewall zone trust
[FW-zone-trust]add interface GigabitEthernet 1/0/1
[FW-zone-trust]undo add interface GigabitEthernet 0/0/0
[FW-zone-trust]fire zone untrust
[FW-zone-untrust]add interface GigabitEthernet 1/0/0
[FW-zone-untrust]quit
```

检查各接口的区域：

```
[FW]display zone interface

local
#
trust
 interface of the zone is (1):
    GigabitEthernet1/0/1
#
untrust
 interface of the zone is (1):
    GigabitEthernet1/0/0
#
dmz
 interface of the zone is (1):
    GigabitEthernet1/0/2
#
```

检查各区域的优先级：

```
[FW]display zone

local
 priority is 100
```

```
#
trust
 priority is 85
 interface of the zone is (1):
    GigabitEthernet1/0/1
#
untrust
 priority is 5
 interface of the zone is (1):
    GigabitEthernet1/0/0
#
dmz
 priority is 50
 interface of the zone is (1):
    GigabitEthernet1/0/2
#
```

可以看到三个接口已经被划分到相应的区域内，默认情况下不同区域间是不可互通的，因此此时路由器之间流量无法通过。

步骤三. 配置安全策略

如果防火墙域间没有配置安全策略，或查找安全策略时，所有的安全策略都没有命中，则默认执行域间的缺省包过滤动作（拒绝通过）。

配置从Trust区域的网段10.0.2.0和10.0.3.0发往Untrust区域的数据包被放行。从Untrust区域发往DMZ目标服务器10.0.4.4的Telnet和FTP请求被放行。

```
[FW]security-policy
[FW-policy-security]rule name policy_sec_1
[FW-policy-security-rule-policy_sec_1]source-zone trust
[FW-policy-security-rule-policy_sec_1]destination-zone untrust
[FW-policy-security-rule-policy_sec_1]source-address 10.0.2.0 mask
255.255.255.0
[FW-policy-security-rule-policy_sec_1]source-address 10.0.3.0 mask
255.255.255.0
[FW-policy-security-rule-policy_sec_1]action permit
[FW-policy-security-rule-policy_sec_1]rule name policy_sec_2
[FW-policy-security-rule-policy_sec_2]source-zone untrust
[FW-policy-security-rule-policy_sec_2]destination-zone dmz
[FW-policy-security-rule-policy_sec_2]destination-address 10.0.4.4 mask
255.255.255.255
```

```
[FW-policy-security-rule-policy_sec_2]service ftp
[FW-policy-security-rule-policy_sec_2]service telnet
[FW-policy-security-rule-policy_sec_2]action permit
```

步骤四. 配置基于源的 NAT

使用公网地址1.1.1.254转换源地址。

```
[FW]nat address-group group1
[FW-nat-address-group-group1]section 1.1.1.254 1.1.1.254
```

配置完成后，检查地址池状态。

```
[FW]display nat address-group

NAT address-group information:
 ID          : 0                    name         : group1
 sectionID    : 0                    sectionName   : ---
 startaddr    : 1.1.1.254             endaddr      : 1.1.1.254
 excludeIP    : 0                    excludePort   : 0
 reference    : 0                    vrrp         : ---
 vpninstance   : root                 natMode      : pat
 description   : ---

  Total   1 address-groups
```

配置源NAT策略。

```
[FW]nat-policy
[FW-policy-nat]rule name policy_nat_1
[FW-policy-nat-rule-policy_nat_1]source-zone trust
[FW-policy-nat-rule-policy_nat_1]destination-zone untrust
[FW-policy-nat-rule-policy_nat_1]source-address 10.0.2.2 24
[FW-policy-nat-rule-policy_nat_1]source-address 10.0.3.3 24
[FW-policy-nat-rule-policy_nat_1]action nat address-group group1
[FW-policy-nat-rule-policy_nat_1]
```

测试连通性：

```
[R2]ping 11.11.11.11
  PING 11.11.11.11: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
```

```
  Request time out
  Request time out

--- 11.11.11.11 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss

  [R2]ping -a 10.0.2.2 1.1.1.1
    PING 1.1.1.1: 56  data bytes, press CTRL_C to break
      Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=254 time=1 ms
      Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
      Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
      Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
      Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

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

  [R3]ping 11.11.11.11
    PING 11.11.11.11: 56  data bytes, press CTRL_C to break
      Request time out
      Request time out
      Request time out
      Request time out
      Request time out

    --- 11.11.11.11 ping statistics ---
      5 packet(s) transmitted
      0 packet(s) received
      100.00% packet loss

  [R3]ping -a 10.0.3.3 11.11.11.11
    PING 11.11.11.11: 56  data bytes, press CTRL_C to break
      Reply from 11.11.11.11: bytes=56 Sequence=1 ttl=254 time=1 ms
      Reply from 11.11.11.11: bytes=56 Sequence=2 ttl=254 time=1 ms
      Reply from 11.11.11.11: bytes=56 Sequence=3 ttl=254 time=1 ms
      Reply from 11.11.11.11: bytes=56 Sequence=4 ttl=254 time=1 ms
      Reply from 11.11.11.11: bytes=56 Sequence=5 ttl=254 time=1 ms
```

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

注意，直接测试R2和R3与11.11.11.11之间的连通性，显示不通。使用扩展Ping，指定了发送数据包的源地址为10.0.2.2后，实现了连通性。

原因是，直接发送数据包到10.0.1.1时，数据包的源地址为10.0.20.2，该地址不属于NAT转换的客户端地址范围。

```
[FW]display nat-policy all

Total:2
RULE ID RULE NAME                    STATE     ACTION           HITTED
------------------------------------------------------------------------------
---
0       default                      enable    no-nat           0
1       policy_nat_1                 enable    nat              2
------------------------------------------------------------------------------
---


[FW]display nat-policy rule policy_nat_1

  (2 times matched)
 rule name policy_nat_1
  source-zone trust
  destination-zone untrust
  source-address 10.0.2.0 mask 255.255.255.0
  source-address 10.0.3.0 mask 255.255.255.0
  action nat address-group group1
```

步骤五. 配置 NAT Server 和源 NAT 将服务器发布

配置NAT Server 对外服务地址1.1.1.254，telnet端口2323，ftp端口2121：

```
[FW]nat server policy_natserver_1 protocol tcp global 1.1.1.254 2323 inside
10.0.4.4 telnet no-reverse
[FW]nat server policy_natserver_2 protocol tcp global 1.1.1.254 2121 inside
10.0.4.4 ftp no-reverse
```

```
[FW]display nat server

Server in private network information:
 name            : policy_natserver_1
 zone            : ---
 interface       : ---
 global-start-addr : 1.1.1.254         global-end-addr   : ---
 inside-start-addr : 10.0.4.4          inside-end-addr   : ---
 global-start-port : 2323             global-end-port   : ---
 insideport       : 23(teln)
 globalvpn        : public            insidevpn        : public
 protocol         : tcp              vrrp             : ---
 no-reverse       : yes

 name            : policy_natserver_2
 zone            : ---
 interface       : ---
 global-start-addr : 1.1.1.254         global-end-addr   : ---
 inside-start-addr : 10.0.4.4          inside-end-addr   : ---
 global-start-port : 2121             global-end-port   : ---
 insideport       : 21(ftp)
 globalvpn        : public            insidevpn        : public
 protocol         : tcp              vrrp             : ---
 no-reverse       : yes

  Total   2 NAT servers
```

在R4上启用服务：

```
[R4]telnet server enable
[R4]ftp server enable
[R4-ui-vty0-4]authentication-mode aaa
[R4-ui-vty0-4]protocol inbound telnet
[R4-ui-vty0-4]quit
[R4]aaa
[R4-aaa]local-user test pass irreversible-cipher Admin@123
[R4-aaa]local-user test service telnet ftp
[R4-aaa]local-user test ftp-directory flash:/
[R4-aaa]local-user test privilege level 3
[R4-aaa]quit
```

FTP是多通道协议，NAT转换过程中需要配置NAT ALG功能。

在DMZ和Untrust域间配置NAT ALG，使服务器可以正常对外提供FTP服务。

```
[FW]firewall interzone dmz untrust
[FW-interzone-dmz-untrust]detect ftp
```

在R1上测试效果：

```
<R1>telnet 1.1.1.254 2323
  Press CTRL_] to quit telnet mode
  Trying 1.1.1.254 ...
  Connected to 1.1.1.254 ...

Login authentication


Username:test
Password:

------------------------------------------------------------------------------
-
  User last login information:

------------------------------------------------------------------------------
-
  Access Type: Telnet
  IP-Address : 1.1.1.1
  Time       : 2016-09-25 07:45:45+00:00

------------------------------------------------------------------------------
-
<R4>quit

<R1>ftp 1.1.1.254 2121
Trying 1.1.1.254 ...
Press CTRL+K to abort
Connected to 1.1.1.254.
220 FTP service ready.
User(1.1.1.254:(none)):test
331 Password required for test.
Enter password:
230 User logged in.

[R1-ftp]
```

Untrust区域可以访问DMZ区域提供的Telnet和FTP服务。

最终设备配置

```
 <S1>display current-configuration
!Software Version V200R008C00SPC500
#
sysname S1
#
vlan batch 11 to 13
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 13
#
interface GigabitEthernet0/0/21
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/22
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/23
 port link-type access
 port default vlan 13
#
```

```
return

<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 11.11.11.11 255.255.255.0
#
return

<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
interface GigabitEthernet0/0/1
 ip address 10.0.20.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.20.254
#
return


<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.20.3 255.255.255.0
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0                          #
ip route-static 0.0.0.0 0.0.0.0 10.0.20.254
```

```
#
return

<R4>display current-configuration
[V200R007C00SPC600]
#
 sysname R4
#
aaa
 local-user test password irreversible-cipher Admin@123
 local-user test privilege level 3
 local-user test ftp-directory flash:/
 local-user test service-type telnet ftp
#
interface GigabitEthernet0/0/1
 ip address 10.0.40.4 255.255.255.0
#
interface LoopBack0
 ip address 10.0.4.4 255.255.255.0
#
 ftp server enable
#
 telnet server enable
#
ip route-static 0.0.0.0 0.0.0.0 10.0.40.254
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound telnet
#
return

<FW>display current-configuration
#
 nat server policy_natserver_1 protocol tcp global 1.1.1.254 2323 inside 10.0.4.4
telnet no-reverse
 nat server policy_natserver_2 protocol tcp global 1.1.1.254 2121 inside 10.0.4.4
ftp no-reverse
#
 sysname FW
#
interface GigabitEthernet1/0/0
```

```
 ip address 1.1.1.254 255.255.255.0
#
interface GigabitEthernet1/0/1
 ip address 10.0.20.254 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.0.40.254 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/0
#
firewall zone dmz
 set priority 50
 add interface GigabitEthernet1/0/2
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
 ip route-static 10.0.2.0 255.255.255.0 10.0.20.2
 ip route-static 10.0.3.0 255.255.255.0 10.0.20.3
 ip route-static 10.0.4.0 255.255.255.0 10.0.40.4
#
 nat address-group group1
 section 0 1.1.1.254 1.1.1.254
#
security-policy
 rule name policy_sec_1
  source-zone trust
  destination-zone untrust
  source-address 10.0.2.0 mask 255.255.255.0
  source-address 10.0.3.0 mask 255.255.255.0
  action permit
 rule name policy_sec_2
```

```
  source-zone untrust
  destination-zone dmz
  destination-address 10.0.4.4 mask 255.255.255.255
  service ftp
  service telnet
  action permit
#
nat-policy
 rule name policy_nat_1
  source-zone trust
  destination-zone untrust
  source-address 10.0.2.0 mask 255.255.255.0
  source-address 10.0.3.0 mask 255.255.255.0
  action nat address-group group1
#
return
```

第五章 VRRP协议特性与配置

实验 5-1 VRRP 配置实验

实验目标

- 掌握VRRP组和虚拟地址的配置方式
- 掌握VRRP优先级配置方式
- 掌握VRRP的验证效果
- 掌握VRRP跟踪上行链路配置方式
- 掌握VRRP多组负载均衡的配置方式

拓扑图

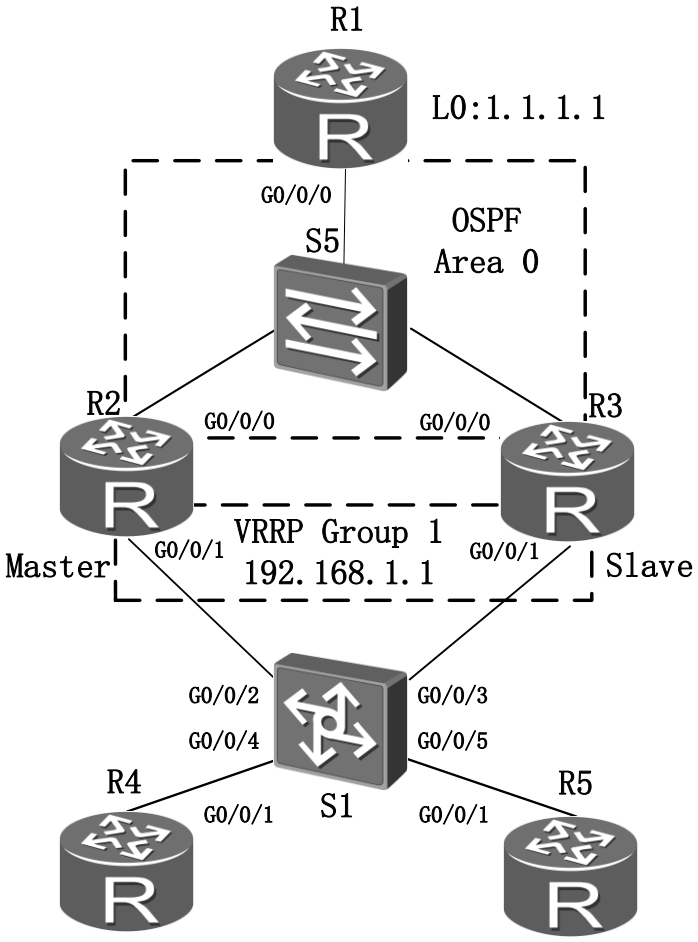


图1-1 VRRP实验拓扑

场景

R1作为局域网和外部网络的网关，通过交换机和汇聚路由器R2、R3互联，R2、R3、R4和R5通过交换机S1连接到一个LAN里，现在希望通过在R2和R3连接S1的接口上启用VRRP v2来实现主机上网的第一跳冗余，R2为master，R3为slave。交换机不做额外的配置，仅透明转发。

学习任务

步骤一. IP 编址与基本配置

给所有路由器配置IP地址信息。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface loopback 0
[R1-LoopBack0]ip address 1.1.1.1 32
[R1-LoopBack0]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 10.0.123.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 10.0.123.2 24
[R2-GigabitEthernet0/0/0]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/1]ip address 192.168.1.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ip address 10.0.123.3 24
[R3-GigabitEthernet0/0/0]interface GigabitEthernet0/0/1
[R3-GigabitEthernet0/0/1]ip address 192.168.1.3 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 192.168.1.4 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R5
[R5]interface GigabitEthernet 0/0/1
[R5-GigabitEthernet0/0/1]ip address 192.168.1.5 24
```

配置完成后，在R1上测试到R2和R3的连通性。

```
[R1]ping 10.0.123.2
  PING 10.0.123.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.123.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.123.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.123.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.123.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.123.2: bytes=56 Sequence=5 ttl=255 time=1 ms

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

[R1]ping 10.0.123.3
  PING 10.0.123.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.123.3: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.123.3: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.123.3: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.123.3: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.123.3: bytes=56 Sequence=5 ttl=255 time=1 ms

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

测试R2、R3、R4和R5之间的连通性，以R2为例。

```
[R2]ping 192.168.1.3
  PING 192.168.1.3: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.3: bytes=56 Sequence=1 ttl=255 time=27 ms
    Reply from 192.168.1.3: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 192.168.1.3 ping statistics ---
    5 packet(s) transmitted
```

```
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/6/27 ms

[R2]ping 192.168.1.4
  PING 192.168.1.4: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.4: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=5 ttl=255 time=1 ms

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

[R2]ping 192.168.1.5
  PING 192.168.1.5: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.5: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 192.168.1.5: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 192.168.1.5: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.1.5: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 192.168.1.5: bytes=56 Sequence=5 ttl=255 time=1 ms

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

步骤二. 配置 OSPF 协议和静态路由

R1的环回口0，R1、R2和R3互连接口运行在OSPF的区域0，R2和R3连接S1交换机的接口也要宣告进OSPF，但不建立邻居，只为发布路由，因此使用silent模式。

R4和R5为模拟PC，使用静态默认路由指向该网段的192.168.1.1（VRRP虚拟地址）。

最终实现的目标是R1可以学到192.168.1.0网段路由，R2和R3可以学到1.1.1.1路由。

```
[R1]ospf router-id 10.0.0.1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.123.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0

[R2]ospf router-id 10.0.0.2
[R2-ospf-1]silent-interface GigabitEthernet 0/0/1
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.123.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255

[R3]ospf router-id 10.0.0.3
[R3-ospf-1]silent-interface GigabitEthernet 0/0/1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.123.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255

[R4]ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
[R5]ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
```

配置完成后，观察各设备的路由表，以R1、R2和R4为例

```
   [R1]display ip routing-table
   Route Flags: R - relay, D - download to fib
   ------------------------------------------------------------------------------
   Routing Tables: Public
           Destinations : 9        Routes : 10

   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

           1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.123.0/24  Direct  0    0           D   10.0.123.1
GigabitEthernet0/0/0
        10.0.123.1/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/0
      10.0.123.255/32  Direct  0    0           D   127.0.0.1
```

```
GigabitEthernet0/0/0
        127.0.0.0/8   Direct  0    0          D   127.0.0.1      InLoopBack0
        127.0.0.1/32  Direct  0    0          D   127.0.0.1      InLoopBack0
   127.255.255.255/32  Direct  0    0          D   127.0.0.1      InLoopBack0
      192.168.1.0/24  OSPF    10   2          D   10.0.123.3
GigabitEthernet0/0/0
                    OSPF    10   2          D   10.0.123.2
GigabitEthernet0/0/0
   255.255.255.255/32  Direct  0    0          D   127.0.0.1      InLoopBack0

   [R2]display ip routing-table
   Route Flags: R - relay, D - download to fib
   ------------------------------------------------------------------------------
-----
   Routing Tables: Public
           Destinations : 12      Routes : 12

   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

         1.1.1.1/32  OSPF    10   1          D   10.0.123.1
GigabitEthernet0/0/0
         10.0.0.2/32  Direct  0    0          D   127.0.0.1      LoopBack0
       10.0.123.0/24  Direct  0    0          D   10.0.123.2
GigabitEthernet0/0/0
       10.0.123.2/32  Direct  0    0          D   127.0.0.1
GigabitEthernet0/0/0
     10.0.123.255/32  Direct  0    0          D   127.0.0.1
GigabitEthernet0/0/0
        127.0.0.0/8   Direct  0    0          D   127.0.0.1      InLoopBack0
        127.0.0.1/32  Direct  0    0          D   127.0.0.1      InLoopBack0
   127.255.255.255/32  Direct  0    0          D   127.0.0.1      InLoopBack0
      192.168.1.0/24  Direct  0    0          D   192.168.1.2
GigabitEthernet0/0/1
      192.168.1.2/32  Direct  0    0          D   127.0.0.1
GigabitEthernet0/0/1
     192.168.1.255/32  Direct  0    0          D   127.0.0.1
GigabitEthernet0/0/1
   255.255.255.255/32  Direct  0    0          D   127.0.0.1      InLoopBack0

   [R4]display ip routing-table
   Route Flags: R - relay, D - download to fib
   ------------------------------------------------------------------------------
```

```
-----
   Routing Tables: Public
           Destinations : 9       Routes : 9

   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

          0.0.0.0/0   Static  60   0           RD   192.168.1.1
GigabitEthernet0/0/1
         10.0.0.4/32  Direct  0    0           D   127.0.0.1       LoopBack0
        127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      192.168.1.0/24  Direct  0    0           D   192.168.1.4
GigabitEthernet0/0/1
      192.168.1.4/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/1
     192.168.1.255/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/1
   255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

从以上输出可以看到，R1可以学习到192.168.1.0/24路由，R2可以学习到1.1.1.1/32路由，R4有一条静态默认路由指向192.168.1.1。

步骤三. 配置 VRRP 组和虚拟地址

在R2和R3 的相应接口上启用VRRP并配置虚拟组ID和虚拟地址。

```
[R2-GigabitEthernet0/0/1]vrrp vrid 1 virtual-ip 192.168.1.1
```

由于R2先进行了配置，经历一个等待周期后发觉组内没有其他成员，因此自己成为Master。

```
[R3-GigabitEthernet0/0/1]vrrp vrid 1 virtual-ip 192.168.1.1
```

配置完成后，在R2和R3上观察VRRP状态。

```
[R2-GigabitEthernet0/0/1]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
```

```
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-22 18:00:03
    Last change time : 2016-07-22 18:00:07

[R3-GigabitEthernet0/0/1]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-22 18:03:16
    Last change time : 2016-07-22 18:03:16
```

R2成功当选Master路由器，R3为Slave路由器。但此时并没有配置优先级，主备优先级都是100，这种情况下如果R3先启动，那么主设备会变成R3，这种结果不是我们期望的。

步骤四. 配置 VRRP 设备优先级，验证主备切换

在R2和R3配置VRRP的优先级,优先级越大越高,因此R2是120,R3是110。

```
[R2-GigabitEthernet0/0/1]vrrp vrid 1 priority 120

[R3-GigabitEthernet0/0/1]vrrp vrid 1 priority 110
```

验证优先级修改后的结果。

```
[R2-GigabitEthernet0/0/1]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-22 18:00:03
    Last change time : 2016-07-22 18:00:07

[R3-GigabitEthernet0/0/1]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 120
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
```

```
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-22 18:03:16
    Last change time : 2016-07-22 18:03:16
```

由输出信息，发现优先级已经成功修改完毕，默认情况下VRRP开启抢占，如果修改R3的优先级更高，那么产生主备切换。

最后验证从R4到R1的互通。

```
[R4]ping 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=254 time=57 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 1.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/12/57 ms
```

由输出显示,虚拟网关已经正常工作,可以把R4所在LAN的数据转发到R1。正常情况下，由Master转发数据，因此流量经过R2。为了验证故障切换状态，我们开启R4到R1的长ping，并关闭R2连接S1的接口。

```
    [R2-GigabitEthernet0/0/1]shutdown
```

在主备切换的过程中，R4丢了2个数据包，但后续数据正常转发。

```
[R4]ping -c 1000 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
```

```
  Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=6 ttl=254 time=1 ms
  Request time out
  Request time out
  Reply from 1.1.1.1: bytes=56 Sequence=9 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=10 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=11 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=12 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=13 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=14 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=15 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=16 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=17 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=18 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=19 ttl=254 time=1 ms
  Reply from 1.1.1.1: bytes=56 Sequence=20 ttl=254 time=1 ms

 --- 1.1.1.1 ping statistics ---
  20 packet(s) transmitted
  18 packet(s) received
  10.00% packet loss
  round-trip min/avg/max = 1/1/1 ms
```

由于主备切换，R3成为Master。

```
[R3-GigabitEthernet0/0/1]display vrrp
 GigabitEthernet0/0/1 | Virtual Router 1
  State : Master
  Virtual IP : 192.168.1.1
  Master IP : 192.168.1.3
  PriorityRun : 110
  PriorityConfig : 110
  MasterPriority : 110
  Preempt : YES   Delay Time : 0 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Create time : 2016-07-22 18:03:16
```

```
  Last change time : 2016-07-22 18:29:41
```

步骤五. 配置跟踪上行链路特性

VRRP主备切换是通过侦听通告报文实现的，如果Slave路由器侦听不到Master的消息或自己优先级更高，那么执行抢占（默认无抢占等待时间）。

如果故障点发生在上行链路，主备不切换，那么所有上网流量到达R2之后将无法转发。因此这里引入一个VRRP的特性——跟踪上行链路。确保在上行链路出现故障的时候，R2自动降低自己的优先级，R3可以执行抢占，从而将流量引导到备用路由器和备用上行链路进行转发。

在R2上配置跟踪上行接口，设置惩罚值为30，即当链路失效，R2的运行优先级会变为90，低于R3的110：

```
[R2-GigabitEthernet0/0/1]vrrp vrid 1 track interface GigabitEthernet 0/0/0
reduced 30
```

检查跟踪配置：

```
[R2-GigabitEthernet0/0/1]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0   Priority reduced : 30
    IF state : UP
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 17:32:27 UTC-08:00
```

在R4上开启长ping，同时shutdown R2的上行接口：

```
[R2-GigabitEthernet0/0/0]shutdown

[R2-GigabitEthernet0/0/0]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
    PriorityRun : 90
    PriorityConfig : 120
    MasterPriority : 110
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0   Priority reduced : 30
    IF state : DOWN
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 19:57:46 UTC-08:00

<R3>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 110
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-25 17:20:00 UTC-08:00
    Last change time : 2016-07-25 19:56:24 UTC-08:00
```

检查主备状态R3成为Master，流量成功引导到R3上网。

将R2上行链路恢复，优先级恢复，重新抢占成为Master路由器（此过程的R4丢包数量较多，原因是OSPF路由没有快速收敛的缘故，加快路由收敛部分请阅读OSPF实验）。

```
[R2-GigabitEthernet0/0/0]undo shutdown
[R2]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0   Priority reduced : 30
    IF state : UP
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 20:04:40 UTC-08:00
```

注意：因为在接口up之后，R2上行接口要重新建立OSPF邻居，如果没有配置OSPF快速收敛，将会有数秒钟无法转发数据。因此建议回切时配置抢占延时，延时时间要大于OSPF收敛时间。

```
[R2-GigabitEthernet0/0/1]vrrp vrid 1 preempt-mode timer delay 10
```

再次检查VRRP，延时抢占已经配置成功。

```
[R2-GigabitEthernet0/0/1]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
```

```
  MasterPriority : 120
  Preempt : YES   Delay Time : 10 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Track IF : GigabitEthernet0/0/0   Priority reduced : 30
  IF state : UP
  Create time : 2016-07-25 17:14:56 UTC-08:00
  Last change time : 2016-07-25 20:04:40 UTC-08:00
```

步骤六. 配置 VRRP 多组负载均衡

在正常状态下，所有流量都从Master设备转发，Slave设备处于闲置状态。

如果想实现双网关的负载均衡，可以采用VRRP多组的方式：在R2和R3上分别建立VRRP组1，虚拟地址为192.168.1.1，Master设备是R2，VRRP组2，虚拟地址为192.168.1.254，Master设备是R3。并且将R4的默认网关指向192.168.1.1，R5的默认网关指向192.168.1.254。这样的设计，可以将这个网段上的主机上网流量，分担到两台网关上。

下面是具体配置：

```
[R2-GigabitEthernet0/0/1]vrrp vrid 2 virtual-ip 192.168.1.254
[R2-GigabitEthernet0/0/1]vrrp vrid 2 priority 110

[R3-GigabitEthernet0/0/1]vrrp vrid 2 virtual-ip 192.168.1.254
[R3-GigabitEthernet0/0/1]vrrp vrid 2 priority 120
[R3-GigabitEthernet0/0/1]vrrp vrid 2 track interface GigabitEthernet0/0/0
reduced 30

[R5]undo ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
[R5]ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
```

在R2和R3上查看双组负载均衡状态：

```
<R2>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
```

```
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 10 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0   Priority reduced : 30
    IF state : UP
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 20:04:40 UTC-08:00

  GigabitEthernet0/0/1 | Virtual Router 2
    State : Backup
    Virtual IP : 192.168.1.254
    Master IP : 192.168.1.3
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 120
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-25 17:15:54 UTC-08:00
    Last change time : 2016-07-25 17:20:30 UTC-08:00

<R3>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 110
```

```
  PriorityConfig : 110
  MasterPriority : 120
  Preempt : YES   Delay Time : 0 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Create time : 2016-07-25 17:20:00 UTC-08:00
  Last change time : 2016-07-25 20:03:15 UTC-08:00

 GigabitEthernet0/0/1 | Virtual Router 2
  State : Master
  Virtual IP : 192.168.1.254
  Master IP : 192.168.1.3
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES   Delay Time : 0 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0102
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Track IF : GigabitEthernet0/0/0   Priority reduced : 30
  IF state : UP
  Create time : 2016-07-25 17:20:14 UTC-08:00
  Last change time : 2016-07-25 17:20:23 UTC-08:00
```

使用tracert来确认发到两条默认路由的数据被哪个网关来处理，可以看到从R4发出的数据由组1的Master转发，R5发出的数据由组2的Master转发：

```
<R4>tracert 1.1.1.1

 traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C
t
o break
```

```
 1 192.168.1.2 80 ms  40 ms  40 ms

 2 10.0.123.1 100 ms  70 ms  70 ms

<R5>tracert 1.1.1.1

 traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C
t
o break

 1 192.168.1.3 50 ms  30 ms  50 ms

 2 10.0.123.1 60 ms  90 ms  60 ms
```

验证上行链路失效后的流量切换：

```
[R2-GigabitEthernet0/0/0]shutdown
<R4>tracert 1.1.1.1

 traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C
t
o break

 1 192.168.1.3 50 ms  40 ms  50 ms

 2 10.0.123.1 70 ms  80 ms  50 ms

<R5>tracert 1.1.1.1

 traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C
t
o break

 1 192.168.1.3 40 ms  50 ms  40 ms

 2 10.0.123.1 70 ms  100 ms  90 ms
```

观察切换后的VRRP双组状态：

```
<R2>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
```

```
    State : Backup
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
    PriorityRun : 90
    PriorityConfig : 120
    MasterPriority : 110
    Preempt : YES   Delay Time : 10 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0   Priority reduced : 30
    IF state : DOWN
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 20:48:28 UTC-08:00

  GigabitEthernet0/0/1 | Virtual Router 2
    State : Backup
    Virtual IP : 192.168.1.254
    Master IP : 192.168.1.3
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 120
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-25 17:15:54 UTC-08:00
    Last change time : 2016-07-25 17:20:30 UTC-08:00

<R3>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
```

```
  PriorityRun : 110
  PriorityConfig : 110
  MasterPriority : 110
  Preempt : YES   Delay Time : 0 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Create time : 2016-07-25 17:20:00 UTC-08:00
  Last change time : 2016-07-25 20:46:42 UTC-08:00

GigabitEthernet0/0/1 | Virtual Router 2
  State : Master
  Virtual IP : 192.168.1.254
  Master IP : 192.168.1.3
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES   Delay Time : 0 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0102
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Track IF : GigabitEthernet0/0/0   Priority reduced : 30
  IF state : UP
  Create time : 2016-07-25 17:20:14 UTC-08:00
  Last change time : 2016-07-25 17:20:23 UTC-08:00
```

正常状态R2和R3负载分担，R2出现故障，R3可以接管R2的所有流量，至此VRRP双组负载均衡配置完毕。

配置文件参考

```
<R1>display current-configuration
```

```
#
 sysname R1
#
interface GigabitEthernet0/0/0
 ip address 10.0.123.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.0.123.1 0.0.0.0
#
return
```

```
<R2>display current-configuration
#
 sysname R2
#
interface GigabitEthernet0/0/0
 shutdown
 ip address 10.0.123.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 10
 vrrp vrid 1 track interface GigabitEthernet0/0/0 reduced 30
 vrrp vrid 2 virtual-ip 192.168.1.254
 vrrp vrid 2 priority 110
#
ospf 1
 silent-interface GigabitEthernet0/0/1
 area 0.0.0.0
  network 10.0.123.2 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

```
<R3>display current-configuration
```

```
#
 sysname R3
#
interface GigabitEthernet0/0/0
 ip address 10.0.123.3 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 110
 vrrp vrid 2 virtual-ip 192.168.1.254
 vrrp vrid 2 priority 120
 vrrp vrid 2 track interface GigabitEthernet0/0/0 reduced 30
#
ospf 1
 silent-interface GigabitEthernet0/0/1
 area 0.0.0.0
  network 10.0.123.3 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

```
<R4>display current-configuration
#
 sysname R4
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.4 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
#
return
```

```
<R5>display current-configuration
#
 sysname R5
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.5 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
```

```
return
```

第六章 BFD特性与配置

实验 6-1 BFD 与静态路由联动配置实验

实验目标

- 掌握BFD与静态路由联动实现浮动路由

拓扑图

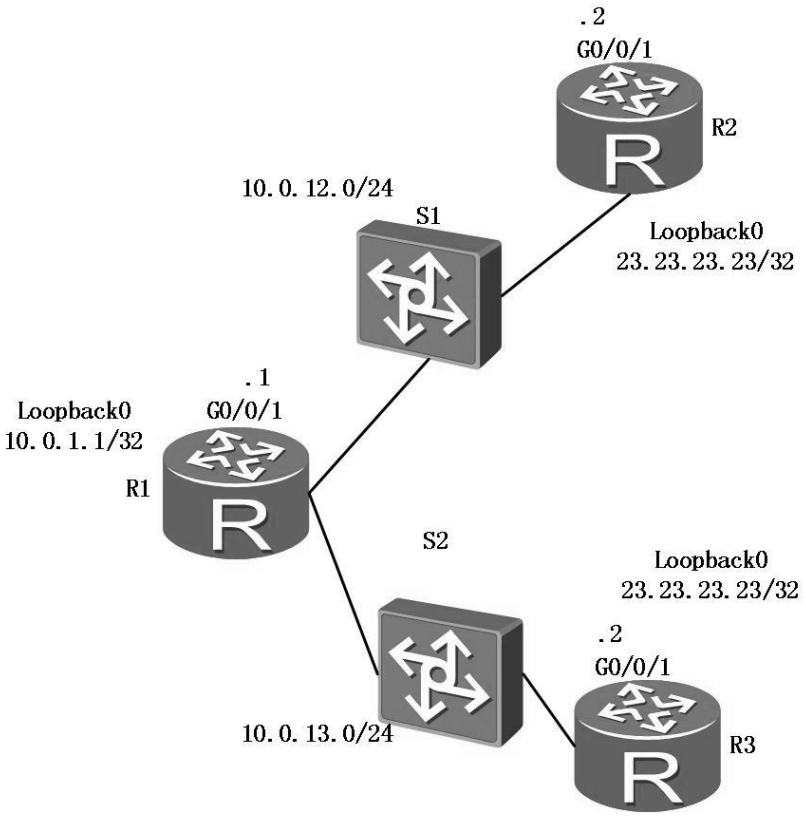


图1-1 BFD与静态路由联动实验拓扑

场景

R1通过S1和S2与R2和R3相连，由于设备之间使用静态路由互通，经过R2或R3都可以到达目标网络23.23.23.23/32，R2作为主用下一跳，R3作为备用下

一跳，由于不是直连链路，因此接口状态不会影响到静态路由的有效性，此时使用BFD进行检测，当检测失效时，使用备份静态路由进行数据转发。

学习任务

步骤一. IP 编址与基本配置

给所有路由器配置IP地址信息，并检查：

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.12.1 24
[R1-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2]ip address 10.0.13.1 24
[R1-GigabitEthernet0/0/2]interface LoopBack 0
[R1-LoopBack0]ip add 10.0.1.1 32

[R1]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 9
The number of interface that is DOWN in Physical is 3
The number of interface that is UP in Protocol is 6
The number of interface that is DOWN in Protocol is 6

Interface                   IP Address/Mask     Physical   Protocol
Cellular0/0/0               unassigned          down       down
Cellular0/0/1               unassigned          down       down
GigabitEthernet0/0/0        unassigned          up         down
GigabitEthernet0/0/1        10.0.12.1/24        up         up
GigabitEthernet0/0/2        10.0.13.1/24        up         up
GigabitEthernet0/0/3        unassigned          up         down
LoopBack0                   10.0.1.1/32         up         up(s)
NULL0                       unassigned          up         up(s)
Serial1/0/0                 unassigned          up         up
Serial2/0/0                 unassigned          up         down
```

```
Serial3/0/0                    unassigned         up        up
Serial4/0/0                    unassigned         down      down


<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/1]interface LoopBack 0
[R2-LoopBack0]ip address 23.23.23.23 32
[R2-LoopBack0]quit

[R2]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 9
The number of interface that is DOWN in Physical is 4
The number of interface that is UP in Protocol is 5
The number of interface that is DOWN in Protocol is 8

Interface                      IP Address/Mask     Physical   Protocol
Cellular0/0/0                   unassigned         down       down
Cellular0/0/1                   unassigned         down       down
Ethernet4/0/0                   unassigned         down       down
Ethernet4/0/1                   unassigned         down       down
GigabitEthernet0/0/0             unassigned         up         down
GigabitEthernet0/0/1             10.0.12.2/24       up         up
GigabitEthernet0/0/2             unassigned         up         down
GigabitEthernet0/0/3             unassigned         up         down
LoopBack0                       23.23.23.23/32      up         up(s)
NULL0                          unassigned          up         up(s)
Serial1/0/0                     unassigned         up         up
Serial2/0/0                     unassigned         up         up
Serial3/0/0                     unassigned         up         down


<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
```

```
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.13.2 24
[R3-GigabitEthernet0/0/2]interface LoopBack 0
[R3-LoopBack0]ip address 23.23.23.23 32
[R3-LoopBack0]quit

[R3]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 9
The number of interface that is DOWN in Physical is 4
The number of interface that is UP in Protocol is 5
The number of interface that is DOWN in Protocol is 8

Interface                   IP Address/Mask     Physical   Protocol
Cellular0/0/0                unassigned         down       down
Cellular0/0/1                unassigned         down       down
Ethernet4/0/0                unassigned         down       down
Ethernet4/0/1                unassigned         down       down
GigabitEthernet0/0/0          unassigned         up         down
GigabitEthernet0/0/1          unassigned         up         down
GigabitEthernet0/0/2          10.0.13.2/24       up         up
GigabitEthernet0/0/3          unassigned         up         down
LoopBack0                    23.23.23.23/32      up         up(s)
NULL0                       unassigned          up         up(s)
Serial1/0/0                  unassigned         up         down
Serial2/0/0                  unassigned         up         up
Serial3/0/0                  unassigned         up         up
```

检查R1到R2和R3接口的连通性：

```
[R1]ping 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=1 ms
```

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

[R1]ping 10.0.13.2
  PING 10.0.13.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.13.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=5 ttl=255 time=1 ms

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

步骤二. BFD 配置

在主用路径上启用BFD配置，检测R1到R2接口：

```
[R1]bfd
[R1-bfd]quit
[R1]bfd 1 bind peer-ip 10.0.12.2 source-ip 10.0.12.1 auto
[R1-bfd-session-1]commit
[R1-bfd-session-1]quit

[R2]bfd
[R2-bfd]quit
[R2]bfd 1 bind peer-ip 10.0.12.1 source-ip 10.0.12.2 auto
[R2-bfd-session-1]commit
[R2-bfd-session-1]quit
```

检查BFD会话信息：

```
[R1]display bfd session all
--------------------------------------------------------------------------------
----
Local Remote    PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
----
8192  8192      10.0.12.2       Up        S_AUTO_PEER       -
--------------------------------------------------------------------------------
----
    Total UP/DOWN Session Number : 1/0

[R2]display bfd session all
--------------------------------------------------------------------------------
----
Local Remote    PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
----
8192  8192      10.0.12.1       Up        S_AUTO_PEER       -
--------------------------------------------------------------------------------
----
    Total UP/DOWN Session Number : 1/0
```

步骤三. 配置 BFD 与静态路由联动

在R2和R3上配置去往R1环回口的静态路由：

```
[R2]ip route-static 10.0.0.0 8 10.0.12.1
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
--------------------------------------------------------------------------------
--
Routing Tables: Public
        Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.0/8   Static  60   0           RD   10.0.12.1
GigabitEthernet0/0/1
     10.0.12.0/24  Direct  0    0           D   10.0.12.2
GigabitEthernet0/0/1
     10.0.12.2/32  Direct  0    0           D   127.0.0.1
```

```
GigabitEthernet0/0/1
    10.0.12.255/32  Direct  0    0          D   127.0.0.1
GigabitEthernet0/0/1
    23.23.23.23/32  Direct  0    0          D   127.0.0.1       LoopBack0
     127.0.0.0/8   Direct  0    0          D   127.0.0.1       InLoopBack0
     127.0.0.1/32  Direct  0    0          D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0          D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0          D   127.0.0.1       InLoopBack0

[R3]ip route-static 10.0.0.0 8 10.0.13.1
[R3]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Routing Tables: Public
        Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

     10.0.0.0/8   Static  60   0          RD   10.0.13.1
GigabitEthernet0/0/2
     10.0.13.0/24  Direct  0    0          D   10.0.13.2
GigabitEthernet0/0/2
     10.0.13.2/32  Direct  0    0          D   127.0.0.1
GigabitEthernet0/0/2
    10.0.13.255/32  Direct  0    0          D   127.0.0.1
GigabitEthernet0/0/2
    23.23.23.23/32  Direct  0    0          D   127.0.0.1       LoopBack0
     127.0.0.0/8   Direct  0    0          D   127.0.0.1       InLoopBack0
     127.0.0.1/32  Direct  0    0          D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0          D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0          D   127.0.0.1       InLoopBack0
```

在R1上配置两条静态路由并联动BFD：

```
[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.12.2 track bfd-session 1
[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.13.2 preference 100
```

由于去往R3的路由preference为100 ,高于去往R2的60 ,因此在路由表中：

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
```

```
--
Routing Tables: Public
        Destinations : 12       Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       0.0.0.0/0   Static  60   0           RD   10.0.12.2
GigabitEthernet0/0/1
      10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
     10.0.12.0/24  Direct  0    0           D   10.0.12.1
GigabitEthernet0/0/1
     10.0.12.1/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/1
   10.0.12.255/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/1
     10.0.13.0/24  Direct  0    0           D   10.0.13.1
GigabitEthernet0/0/2
     10.0.13.1/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/2
   10.0.13.255/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/2
     127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
     127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[R1]display ip routing-table 0.0.0.0 0.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Routing Table : Public
Summary Count : 2

Destination: 0.0.0.0/0
    Protocol: Static          Process ID: 0
  Preference: 60                  Cost: 0
     NextHop: 10.0.12.2         Neighbour: 0.0.0.0
       State: Active Adv Relied       Age: 00h01m19s
         Tag: 0                Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x80000001
RelayNextHop: 0.0.0.0           Interface: GigabitEthernet0/0/1
```

```
    TunnelID: 0x0                Flags: RD

Destination: 0.0.0.0/0
     Protocol: Static         Process ID: 0
   Preference: 100                 Cost: 0
      NextHop: 10.0.13.2        Neighbour: 0.0.0.0
        State: Inactive Adv Relied    Age: 00h01m03s
          Tag: 0                Priority: medium
        Label: NULL              QoSInfo: 0x0
   IndirectID: 0x80000002
 RelayNextHop: 0.0.0.0          Interface: GigabitEthernet0/0/2
    TunnelID: 0x0                Flags: R
```

检查正常状态下连通性：

```
[R1]ping -a 10.0.1.1 23.23.23.23
  PING 23.23.23.23: 56  data bytes, press CTRL_C to break
    Reply from 23.23.23.23: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=5 ttl=255 time=1 ms

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

在R1上开启长ping，在此时shutdownR2的接口：

```
[R1]ping -c 100 23.23.23.23

[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]shutdown
```

在R1上观察ping的效果：

```
[R1]ping -c 100 23.23.23.23
  PING 23.23.23.23: 56  data bytes, press CTRL_C to break
    Reply from 23.23.23.23: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=4 ttl=255 time=1 ms
```

```
  Reply from 23.23.23.23: bytes=56 Sequence=5 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=6 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=7 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=8 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=9 ttl=255 time=1 ms
  Request time out
  Request time out
  Reply from 23.23.23.23: bytes=56 Sequence=12 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=13 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=14 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=15 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=16 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=17 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=18 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=19 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=20 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=21 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=22 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=23 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=24 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=25 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=26 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=27 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=28 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=29 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=30 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=31 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=32 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=33 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=34 ttl=255 time=1 ms
  Reply from 23.23.23.23: bytes=56 Sequence=35 ttl=255 time=1 ms

 --- 23.23.23.23 ping statistics ---
  35 packet(s) transmitted
  33 packet(s) received
  5.71% packet loss
  round-trip min/avg/max = 1/1/1 ms
```

在这时检查BFD会话：

```
[R1]display bfd session all
--------------------------------------------------------------------------------
----
```

```
Local Remote     PeerIpAddr      State     Type        InterfaceName
------------------------------------------------------------------------------
----
8192  0          10.0.12.2       Down      S_AUTO_PEER       -
------------------------------------------------------------------------------
----
    Total UP/DOWN Session Number : 0/1
```

在R1上检查路由信息：

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Routing Tables: Public
        Destinations : 12       Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       0.0.0.0/0   Static  100  0           RD   10.0.13.2
GigabitEthernet0/0/2
      10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
     10.0.12.0/24  Direct  0    0           D   10.0.12.1
GigabitEthernet0/0/1
     10.0.12.1/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/1
   10.0.12.255/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/1
     10.0.13.0/24  Direct  0    0           D   10.0.13.1
GigabitEthernet0/0/2
     10.0.13.1/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/2
   10.0.13.255/32  Direct  0    0           D   127.0.0.1
GigabitEthernet0/0/2
     127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
     127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[R1]display ip routing-table 0.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
```

```
Routing Table : Public
Summary Count : 2

Destination: 0.0.0.0/0
    Protocol: Static         Process ID: 0
  Preference: 60                 Cost: 0
     NextHop: 10.0.12.2        Neighbour: 0.0.0.0
       State: Invalid Adv Relied     Age: 00h05m27s
         Tag: 0               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x80000001
RelayNextHop: 0.0.0.0          Interface: GigabitEthernet0/0/1
    TunnelID: 0x0                Flags: R

Destination: 0.0.0.0/0
    Protocol: Static         Process ID: 0
  Preference: 100                Cost: 0
     NextHop: 10.0.13.2        Neighbour: 0.0.0.0
       State: Active Adv Relied      Age: 00h05m11s
         Tag: 0               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x80000002
RelayNextHop: 0.0.0.0          Interface: GigabitEthernet0/0/2
    TunnelID: 0x0                Flags: RD
```

如果不配置BFD检测的话，在R1上没有任何机制可以判断静态路由是否有效，因此BFD在这种场景非常重要。

配置文件参考

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.0.13.1 255.255.255.0
```

```
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
bfd 1 bind peer-ip 10.0.12.2 source-ip 10.0.12.1 auto
 commit
#
ip route-static 0.0.0.0 0.0.0.0 10.0.12.2 track bfd-session 1
ip route-static 0.0.0.0 0.0.0.0 10.0.13.2 preference 100
#
return
```

```
<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.2 255.255.255.0
#
interface LoopBack0
 ip address 23.23.23.23 255.255.255.255
#
bfd 1 bind peer-ip 10.0.12.1 source-ip 10.0.12.2 auto
 commit
#
ip route-static 10.0.0.0 255.0.0.0 10.0.12.1
#
return
```

```
<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/2
 ip address 10.0.13.2 255.255.255.0
#
interface LoopBack0
 ip address 23.23.23.23 255.255.255.255
```

```
#
ip route-static 10.0.0.0 255.0.0.0 10.0.13.1
#
return
```

实验 6-2 BFD 与 OSPF 联动配置实验

实验目标

- 掌握BFD在OSPF环境下的快速配置

拓扑图

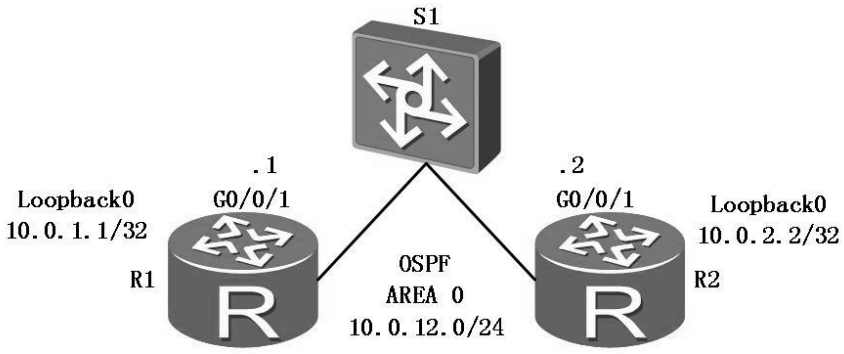


图1-1 BFD与OSPF联动实验拓扑

场景

两台路由器R1和R2经过S1彼此互连，并将各自的接口运行于OSPF区域 0，由于不是接口直接相连，若其中一台的接口Down，另一台不会立即感知，需要等待4倍的Hello时间来删除邻居 ,在这段时间内 数据转发都会处于非正常状态。在这种场景下，可以通过BFD检测来加快OSPF的收敛速度。

学习任务

步骤一. IP 编址与基本配置

给所有路由器配置IP地址信息。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.12.1 24
[R1-GigabitEthernet0/0/1]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 32
[R1-LoopBack0]quit
```

配置好地址立即在每台路由器进行检查。

```
[R1]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 9
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 9

Interface                   IP Address/Mask     Physical   Protocol
Cellular0/0/0               unassigned          down       down
Cellular0/0/1               unassigned          down       down
GigabitEthernet0/0/0        unassigned          *down      down
GigabitEthernet0/0/1        10.0.12.1/24        up         up
GigabitEthernet0/0/2        unassigned          *down      down
GigabitEthernet0/0/3        unassigned          *down      down
LoopBack0                   10.0.1.1/32         up         up(s)
NULL0                       unassigned          up         up(s)
Serial1/0/0                 unassigned          *down      down
Serial2/0/0                 unassigned          *down      down
Serial3/0/0                 unassigned          *down      down
Serial4/0/0                 unassigned          *down      down

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/1]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 32
```

```
[R2-LoopBack0]quit
[R2]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 10
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 10

Interface                       IP Address/Mask     Physical   Protocol
Cellular0/0/0                  unassigned          down       down
Cellular0/0/1                   unassigned          down       down
Ethernet4/0/0                   unassigned          *down      down
Ethernet4/0/1                   unassigned          *down      down
GigabitEthernet0/0/0             unassigned          *down      down
GigabitEthernet0/0/1             10.0.12.2/24        up         up
GigabitEthernet0/0/2             unassigned          *down      down
GigabitEthernet0/0/3             unassigned          *down      down
LoopBack0                       10.0.2.2/32         up         up(s)
NULL0                           unassigned          up         up(s)
Serial1/0/0                     unassigned          *down      down
Serial2/0/0                     unassigned          *down      down
Serial3/0/0                     unassigned          *down      down
```

检查R1到R2的连通性：

```
[R1]ping 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.12.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

步骤二. OSPF 配置

按照拓扑将R1和R2路由器的接口包括环回口0划入OSPF区域0：

```
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]quit
[R1-ospf-1]quit

[R2]ospf 1
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.2.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]quit
[R2-ospf-1]quit
```

检查OSPF接口状态和邻居状态：

```
[R1]display ospf interface

        OSPF Process 1 with Router ID 10.0.12.1
               Interfaces

 Area: 0.0.0.0         (MPLS TE not enabled)
 IP Address      Type        State    Cost    Pri   DR            BDR
 10.0.12.1       Broadcast    Waiting  1       1     0.0.0.0        0.0.0.0
 10.0.1.1        P2P         P-2-P    0       1     0.0.0.0        0.0.0.0

[R2]display ospf interface

        OSPF Process 1 with Router ID 10.0.12.2
               Interfaces

 Area: 0.0.0.0         (MPLS TE not enabled)
 IP Address      Type        State    Cost    Pri   DR            BDR
 10.0.12.2       Broadcast    BDR      1       1     10.0.12.1      10.0.12.2
 10.0.2.2        P2P         P-2-P    0       1     0.0.0.0        0.0.0.0
```

检查OSPF邻居状态：

```
[R1]display ospf peer brief

       OSPF Process 1 with Router ID 10.0.12.1
               Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id         Interface                     Neighbor id     State
 0.0.0.0         GigabitEthernet0/0/1            10.0.12.2       Full
 ----------------------------------------------------------------------------
 Total Peer(s):    1

[R2]display ospf peer brief

       OSPF Process 1 with Router ID 10.0.12.2
               Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id         Interface                     Neighbor id     State
 0.0.0.0         GigabitEthernet0/0/1            10.0.12.1       Full
 ----------------------------------------------------------------------------
 Total Peer(s):    1
```

邻居已经是Full的状态，OSPF配置完毕。

步骤三. 配置 BFD session

需要在系统全局下开启BFD，并且在OSPF视图下启用联动BFD。

```
[R1]bfd
[R1-bfd]quit
[R1]ospf
[R1-ospf-1]bfd all
[R1-ospf-1]bfd all-interfaces enable
[R1-ospf-1]quit

[R2]bfd
[R2-bfd]quit
[R2]ospf
[R2-ospf-1]bfd all
[R2-ospf-1]bfd all-interfaces en
[R2-ospf-1]quit
```

在两端都配置完毕后检查BFD session状态：

```
[R1]display bfd session all
```

```
--------------------------------------------------------------------------------
----
Local Remote     PeerIpAddr      State     Type         InterfaceName
--------------------------------------------------------------------------------
----
8192  8192       10.0.12.2       Up        D_IP_IF      GigabitEthernet0/0/1
--------------------------------------------------------------------------------
----
    Total UP/DOWN Session Number : 1/0

[R2]display bfd se all
--------------------------------------------------------------------------------
----
Local Remote     PeerIpAddr      State     Type         InterfaceName
--------------------------------------------------------------------------------
----
8192  8192       10.0.12.1       Up        D_IP_IF      GigabitEthernet0/0/1
--------------------------------------------------------------------------------
----
    Total UP/DOWN Session Number : 1/0

[R1]display ospf bfd session all

       OSPF Process 1 with Router ID 10.0.12.1
  Area 0.0.0.0 interface 10.0.12.1(GigabitEthernet0/0/1)'s BFD Sessions

 NeighborId:10.0.12.2       AreaId:0.0.0.0
Interface:GigabitEthernet0/0/1
 BFDState:up               rx    :1000           tx      :1000
 Multiplier:3              BFD Local Dis:8192     LocalIpAdd:10.0.12.1
 RemoteIpAdd:10.0.12.2      Diagnostic Info:No diagnostic information
```

测试BFD效果，在R2接口上shutdown：

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]shutdown
```

在R1上若观察debug日志，会出现如下内容：

```
<R1>debug ospf bfd
Sep 23 2016 03:39:25+00:00 R1 %%01BFD/4/STACHG_TODWN(l)[23]:BFD session changed
to Down. (SlotNumber=0, Discriminator=8192, Diagnostic=DetectDown,
```

```
Applications=OSPF, ProcessPST=False, BindInterfaceName=GigabitEthernet0/0/1,
InterfacePhysicalState=Up, InterfaceProtocolState=Up)
<R1>
Sep 23 2016 03:39:25+00:00 R1 %%01OSPF/3/NBR_CHG_DOWN(l)[24]:Neighbor
event:neighbor state changed to Down. (ProcessId=1, NeighborAddress=10.0.12.2,
NeighborEvent=KillNbr, NeighborPreviousState=Full, NeighborCurrentState=Down)
<R1>
Sep 23 2016 03:39:25+00:00 R1 %%01OSPF/3/NBR_DOWN_REASON(l)[25]:Neighbor state
leaves full or changed to Down. (ProcessId=1, NeighborRouterId=10.0.12.2,
NeighborAreaId=0,
NeighborInterface=GigabitEthernet0/0/1,NeighborDownImmediate reason=Neighbor
Down Due to Kill Neighbor, NeighborDownPrimeReason=BFD Session Down,
NeighborChangeTime=2016-09-23 03:39:25)
```

还有其他关联性日志，此处略，重点是以上的第三条日志。

重新开启接口：

```
[R2-GigabitEthernet0/0/1]undo shutdown

[R1]display bfd session all
--------------------------------------------------------------------------------
----
Local Remote     PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
----
8193  8193       10.0.12.2       Up        D_IP_IF     GigabitEthernet0/0/1
--------------------------------------------------------------------------------
----
    Total UP/DOWN Session Number : 1/0
[R1]display bfd ospf se all
          ^
Error: Unrecognized command found at '^' position.
[R1]display ospf bfd session all

       OSPF Process 1 with Router ID 10.0.12.1
  Area 0.0.0.0 interface 10.0.12.1(GigabitEthernet0/0/1)'s BFD Sessions

 NeighborId:10.0.12.2       AreaId:0.0.0.0
Interface:GigabitEthernet0/0/1
 BFDState:up               rx    :1000           tx      :1000
 Multiplier:3              BFD Local Dis:8193     LocalIpAdd:10.0.12.1
 RemoteIpAdd:10.0.12.2      Diagnostic Info:No diagnostic information
```

```
[R2]display bfd session all
--------------------------------------------------------------------------------
----
Local Remote     PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
----
8193  8193       10.0.12.1       Up        D_IP_IF     GigabitEthernet0/0/1
--------------------------------------------------------------------------------
----
    Total UP/DOWN Session Number : 1/0

[R2]display ospf bfd session all

       OSPF Process 1 with Router ID 10.0.12.2
  Area 0.0.0.0 interface 10.0.12.2(GigabitEthernet0/0/1)'s BFD Sessions

 NeighborId:10.0.12.1       AreaId:0.0.0.0
Interface:GigabitEthernet0/0/1
 BFDState:up               rx    :1000           tx      :1000
 Multiplier:3              BFD Local Dis:8193     LocalIpAdd:10.0.12.2
 RemoteIpAdd:10.0.12.1      Diagnostic Info:No diagnostic information
```

BFD重新建立。

配置文件参考

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ospf 1
 bfd all-interfaces enable
```

```
 area 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 10.0.12.0 0.0.0.255
#
return
```

```
<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.255
#
ospf 1
 bfd all-interfaces enable
 area 0.0.0.0
  network 10.0.2.2 0.0.0.0
  network 10.0.12.0 0.0.0.255
#
return
```

实验 6-3 BFD 与 VRRP 联动配置实验

实验目标

- 掌握BFD与VRRP联动检测非直连接口

拓扑图

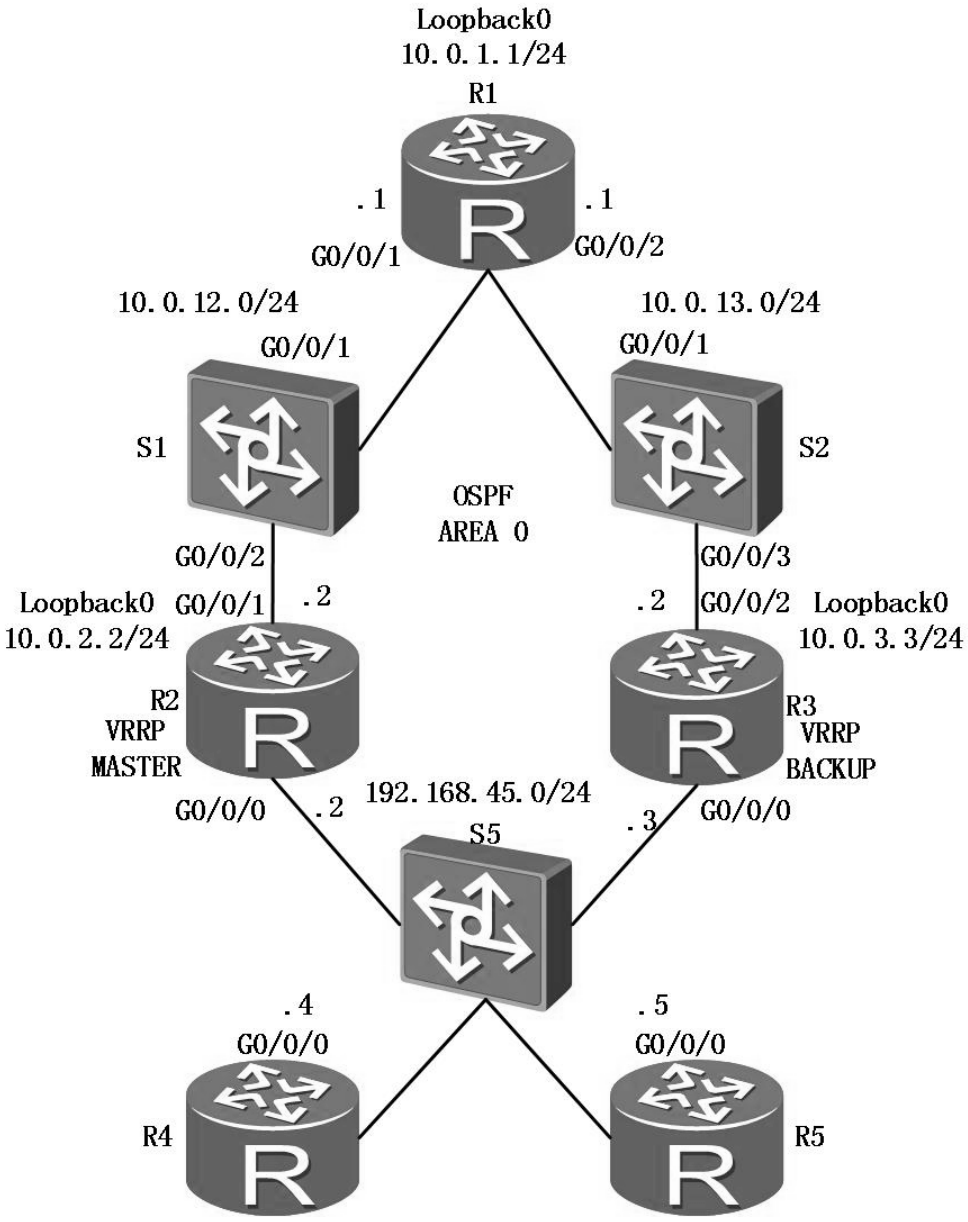


图1-1 BFD与VRRP联动实验拓扑

场景

R1通过两台交换机S1、S2和R2、R3互连，R2和R3运行VRRP作为局域网内R4和R5的网关，R2工作在VRRP MASTER模式，R3工作在BACKUP模式。为了避免R2的非直连上行链路Down后，上行流量依旧从R2转发形成路由黑洞的问题，配置BFD联动VRRP，当R1和R2互联接口Down掉，立即降低R2的VRRP优

先级，由R3作为MASTER转发上行流量。

学习任务

步骤一. IP 编址与基本配置

给所有路由器配置IP地址信息。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 10.0.1.1 24
[R1-LoopBack0]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.12.1 24
[R1-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2]ip address 10.0.13.1 24
[R1-GigabitEthernet0/0/2]quit

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface LoopBack 0
[R2-LoopBack0]ip address 10.0.2.2 24
[R2-LoopBack0]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 192.168.45.2 24
[R2-GigabitEthernet0/0/0]quit

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface LoopBack 0
[R3-LoopBack0]ip address 10.0.3.3 24
[R3-LoopBack0]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.13.2 24
[R3-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ip address 192.168.45.3 24
[R3-GigabitEthernet0/0/0]quit
```

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
[R4]interface GigabitEthernet 0/0/0
[R4-GigabitEthernet0/0/0]ip address 192.168.45.4 24
[R4-GigabitEthernet0/0/0]quit

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R5
[R5]interface GigabitEthernet 0/0/0
[R5-GigabitEthernet0/0/0]ip address 192.168.45.5 24
[R5-GigabitEthernet0/0/0]quit
```

为避免干扰，在SW1和SW2上分别划分VLAN：

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname SW1
[SW1]vlan 12
[SW1-vlan12]quit
[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1]port link-type access
[SW1-GigabitEthernet0/0/1]port default vlan 12
[SW1-GigabitEthernet0/0/1]int GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2]port link-type access
[SW1-GigabitEthernet0/0/2]port default vlan 12
[SW1-GigabitEthernet0/0/2]quit

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname SW2
[SW2]vlan 13
[SW2-vlan13]quit
[SW2]interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1]port link-type access
[SW2-GigabitEthernet0/0/1]port default vlan 13
[SW2-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/3]port link-type access
[SW2-GigabitEthernet0/0/3]port default vlan 13
[SW2-GigabitEthernet0/0/3]quit
```

配置完毕后检查地址配置：

```
[R1]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 9
The number of interface that is DOWN in Physical is 3
The number of interface that is UP in Protocol is 6
The number of interface that is DOWN in Protocol is 6

Interface                   IP Address/Mask     Physical   Protocol
Cellular0/0/0                unassigned         down       down
Cellular0/0/1                unassigned         down       down
GigabitEthernet0/0/0          unassigned         up         down
GigabitEthernet0/0/1          10.0.12.1/24       up         up
GigabitEthernet0/0/2          10.0.13.1/24       up         up
GigabitEthernet0/0/3          unassigned         up         down
LoopBack0                    10.0.1.1/24        up         up(s)
NULL0                        unassigned         up         up(s)
Serial1/0/0                  unassigned         up         up
Serial2/0/0                  unassigned         up         down
Serial3/0/0                  unassigned         up         up
Serial4/0/0                  unassigned         down       down

R2]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 9
The number of interface that is DOWN in Physical is 4
The number of interface that is UP in Protocol is 6
The number of interface that is DOWN in Protocol is 7

Interface                   IP Address/Mask     Physical   Protocol
Cellular0/0/0                unassigned         down       down
Cellular0/0/1                unassigned         down       down
Ethernet4/0/0                unassigned         down       down
```

```
Ethernet4/0/1                  unassigned          down      down
GigabitEthernet0/0/0            192.168.45.2/24     up        up
GigabitEthernet0/0/1            10.0.12.2/24        up        up
GigabitEthernet0/0/2            unassigned          up        down
GigabitEthernet0/0/3            unassigned          up        down
LoopBack0                      10.0.2.2/24         up        up(s)
NULL0                          unassigned          up        up(s)
Serial1/0/0                     unassigned          up        up
Serial2/0/0                     unassigned          up        up
Serial3/0/0                     unassigned          up        down

[R3]dislay ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 9
The number of interface that is DOWN in Physical is 4
The number of interface that is UP in Protocol is 6
The number of interface that is DOWN in Protocol is 7

Interface                      IP Address/Mask     Physical   Protocol
Cellular0/0/0                   unassigned          down      down
Cellular0/0/1                   unassigned          down      down
Ethernet4/0/0                   unassigned          down      down
Ethernet4/0/1                   unassigned          down      down
GigabitEthernet0/0/0            192.168.45.3/24     up        up
GigabitEthernet0/0/1            unassigned          up        down
GigabitEthernet0/0/2            10.0.13.2/24        up        up
GigabitEthernet0/0/3            unassigned          up        down
LoopBack0                      10.0.3.3/24         up        up(s)
NULL0                          unassigned          up        up(s)
Serial1/0/0                     unassigned          up        down
Serial2/0/0                     unassigned          up        up
Serial3/0/0                     unassigned          up        up

[R4]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
```

```
(E): E-Trunk down
The number of interface that is UP in Physical is 6
The number of interface that is DOWN in Physical is 5
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 8

Interface                      IP Address/Mask     Physical   Protocol
Cellular0/0/0                   unassigned          down       down
Cellular0/0/1                   unassigned          down       down
Ethernet2/0/0                   unassigned          up         down
Ethernet2/0/1                   unassigned          down       down
GigabitEthernet0/0/0             192.168.45.4/24     up         up
GigabitEthernet0/0/1             unassigned          up         down
GigabitEthernet0/0/2             unassigned          down       down
GigabitEthernet0/0/3             unassigned          up         down
NULL0                          unassigned          up         up(s)
Serial1/0/0                     unassigned          up         up
Serial1/0/1                     unassigned          down       down

[R5]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 6
The number of interface that is DOWN in Physical is 5
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 8

Interface                      IP Address/Mask     Physical   Protocol
Cellular0/0/0                   unassigned          down       down
Cellular0/0/1                   unassigned          down       down
Ethernet2/0/0                   unassigned          up         down
Ethernet2/0/1                   unassigned          down       down
GigabitEthernet0/0/0             192.168.45.5/24     up         up
GigabitEthernet0/0/1             unassigned          up         down
GigabitEthernet0/0/2             unassigned          down       down
GigabitEthernet0/0/3             unassigned          up         down
NULL0                          unassigned          up         up(s)
Serial1/0/0                     unassigned          up         up
Serial1/0/1                     unassigned          down       down
```

检查R1到R2和R3的连通性：

```
[R1]ping 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.12.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[R1]ping 10.0.13.2
  PING 10.0.13.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 10.0.13.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.13.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

步骤二. OSPF 和静态路由配置

按照拓扑配置R1、R2和R3的OSPF，对于局域网的路由，通过network的方式引入OSPF，但需要启用silent-interface：

```
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.1.1 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]quit
```

```
[R1-ospf-1]quit
```

修改在R1上的OSPF开销，以便于下行流量的选路以R2方向为主：

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ospf cost 90
[R1-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2]ospf cost 100
[R1-GigabitEthernet0/0/2]quit

[R2]ospf 1
[R2-ospf-1]silent-interface GigabitEthernet 0/0/0
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.2.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 192.168.45.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]quit
[R2-ospf-1]quit
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ospf cost 90
[R2-GigabitEthernet0/0/1]quit

[R3]ospf 1
[R3-ospf-1]silent-interface GigabitEthernet 0/0/0
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.3.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 192.168.45.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]quit
[R3-ospf-1]quit
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ospf cost 100
[R3-GigabitEthernet0/0/2]quit
```

OSPF邻居收敛后检查路由信息：

```
[R1]display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Public routing table : OSPF
        Destinations : 3       Routes : 3
```

```
OSPF routing table status : <Active>
        Destinations : 3        Routes : 3

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.2.2/32  OSPF    10   90          D   10.0.12.2
GigabitEthernet0/0/1
      10.0.3.3/32  OSPF    10   100         D   10.0.13.2
GigabitEthernet0/0/2
   192.168.45.0/24  OSPF    10   91          D   10.0.12.2
GigabitEthernet0/0/1

OSPF routing table status : <Inactive>
        Destinations : 0        Routes : 0

[R2]display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
Public routing table : OSPF
        Destinations : 3        Routes : 3

OSPF routing table status : <Active>
        Destinations : 3        Routes : 3

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.1.1/32  OSPF    10   90          D   10.0.12.1
GigabitEthernet0/0/1
      10.0.3.3/32  OSPF    10   190         D   10.0.12.1
GigabitEthernet0/0/1
     10.0.13.0/24  OSPF    10   190         D   10.0.12.1
GigabitEthernet0/0/1

OSPF routing table status : <Inactive>
        Destinations : 0        Routes : 0

[R3]display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
--
```

```
Public routing table : OSPF
        Destinations : 3       Routes : 3

OSPF routing table status : <Active>
        Destinations : 3       Routes : 3

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.1.1/32  OSPF    10   100          D   10.0.13.1
GigabitEthernet0/0/2
      10.0.2.2/32  OSPF    10   190          D   10.0.13.1
GigabitEthernet0/0/2
     10.0.12.0/24  OSPF    10   190          D   10.0.13.1
GigabitEthernet0/0/2

OSPF routing table status : <Inactive>
        Destinations : 0       Routes : 0
```

最后在R4和R5上配置默认路由指向VRRP地址：

```
[R4]ip route-static 0.0.0.0 0 192.168.45.1
[R5]ip route-static 0.0.0.0 0 192.168.45.1
```

步骤三. 配置 VRRP

在R2和R3的下行接口配置VRRP：

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]vrrp vrid 45 virtual-ip 192.168.45.1
[R2-GigabitEthernet0/0/0]vrrp vrid 45 priority 150
[R2-GigabitEthernet0/0/0]quit

[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]vrrp vrid 45 virtual-ip 192.168.45.1
[R3-GigabitEthernet0/0/0]quit
```

检查VRRP主备状态：

```
[R2]display vrrp
  GigabitEthernet0/0/0 | Virtual Router 45
```

```
    State : Master
    Virtual IP : 192.168.45.1
    Master IP : 192.168.45.2
    PriorityRun : 150
    PriorityConfig : 150
    MasterPriority : 150
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-012d
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-09-25 15:18:54
    Last change time : 2016-09-25 15:18:57

[R3]display vrrp
  GigabitEthernet0/0/0 | Virtual Router 45
    State : Backup
    Virtual IP : 192.168.45.1
    Master IP : 192.168.45.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 150
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-012d
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-09-25 15:21:49
    Last change time : 2016-09-25 15:21:49
```

步骤四. 配置 BFD 联动

在R1和R2上启用BFD，配置联动VRRP，如果BFD检测失效，立即降低优先级：

```
[R1]bfd
[R1-bfd]bfd 1 bind peer-ip 192.168.45.2 source-ip 10.0.12.1 auto
[R1-bfd-session-1]commit
[R1-bfd-session-1]quit

[R2]bfd
[R2-bfd]bfd 1 bind peer-ip 10.0.12.1 source-ip 192.168.45.2 auto
[R2-bfd-session-1]commit
[R2-bfd-session-1]quit
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]vrrp vrid 45 track bfd-session session-name 1 reduce
60
```

检查联动配置：

```
[R2]display vrrp
 GigabitEthernet0/0/0 | Virtual Router 45
   State : Master
   Virtual IP : 192.168.45.1
   Master IP : 192.168.45.2
   PriorityRun : 150
   PriorityConfig : 150
   MasterPriority : 150
   Preempt : YES   Delay Time : 0 s
   TimerRun : 1 s
   TimerConfig : 1 s
   Auth type : NONE
   Virtual MAC : 0000-5e00-012d
   Check TTL : YES
   Config type : normal-vrrp
   Backup-forward : disabled
   Track BFD : 1  Priority reduced : 60
   BFD-session state : UP
   Create time : 2016-09-25 15:18:54
   Last change time : 2016-09-25 15:18:57
```

检查BFD的session：

```
[R2]display bfd session all
--------------------------------------------------------------------------------
----
Local Remote    PeerIpAddr     State    Type        InterfaceName
```

```
------------------------------------------------------------------------------
----
8192  8192      10.0.12.1       Up       S_AUTO_PEER       -
------------------------------------------------------------------------------
----
    Total UP/DOWN Session Number : 1/0
```

测试BFD效果，先在R4上启用长ping然后在R1接口上shutdown：

```
[R4]ping -c 100 10.0.1.1

[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]shutdown
```

在R4上观察ping的结果：

```
[R4]ping -c 100 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=6 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=7 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=8 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=9 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=10 ttl=254 time=1 ms
    Request time out
    Request time out
    Reply from 10.0.1.1: bytes=56 Sequence=13 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=14 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=15 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=16 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=17 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=18 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=19 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=20 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=21 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=22 ttl=254 time=1 ms
    Reply from 10.0.1.1: bytes=56 Sequence=23 ttl=254 time=1 ms
```

```
  Reply from 10.0.1.1: bytes=56 Sequence=24 ttl=254 time=1 ms
  Reply from 10.0.1.1: bytes=56 Sequence=25 ttl=254 time=1 ms
  Reply from 10.0.1.1: bytes=56 Sequence=26 ttl=254 time=1 ms
  Reply from 10.0.1.1: bytes=56 Sequence=27 ttl=254 time=1 ms
  Reply from 10.0.1.1: bytes=56 Sequence=28 ttl=254 time=1 ms
  Reply from 10.0.1.1: bytes=56 Sequence=29 ttl=254 time=1 ms
  Reply from 10.0.1.1: bytes=56 Sequence=30 ttl=254 time=1 ms
  Reply from 10.0.1.1: bytes=56 Sequence=31 ttl=254 time=1 ms
  Reply from 10.0.1.1: bytes=56 Sequence=32 ttl=254 time=1 ms

 --- 10.0.1.1 ping statistics ---
  32 packet(s) transmitted
  30 packet(s) received
  6.25% packet loss
  round-trip min/avg/max = 1/1/1 ms
```

查看此时的VRRP状态

```
[R2]display vrrp
 GigabitEthernet0/0/0 | Virtual Router 45
  State : Backup
  Virtual IP : 192.168.45.1
  Master IP : 192.168.45.3
  PriorityRun : 90
  PriorityConfig : 150
  MasterPriority : 100
  Preempt : YES   Delay Time : 0 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-012d
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Track BFD : 1  Priority reduced : 60
  BFD-session state : DOWN
  Create time : 2016-09-25 15:18:54
  Last change time : 2016-09-25 15:27:26
```

BFD联动VRRP检测非直连上行链路成功，在R5上的结论应该和R4相同，略。

配置文件参考

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.1 255.255.255.0
 ospf cost 90
#
interface GigabitEthernet0/0/2
 ip address 10.0.13.1 255.255.255.0
 ospf cost 100
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
bfd 1 bind peer-ip 192.168.45.2 source-ip 10.0.12.1 auto
 commit
#
ospf 1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
  network 10.0.13.0 0.0.0.255
#
return

<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
bfd
#
interface GigabitEthernet0/0/0
 ip address 192.168.45.2 255.255.255.0
```

```
 vrrp vrid 45 virtual-ip 192.168.45.1
 vrrp vrid 45 priority 150
 vrrp vrid 45 track bfd-session session-name 1 reduced 60
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.2 255.255.255.0
 ospf cost 90
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
bfd 1 bind peer-ip 10.0.12.1 source-ip 192.168.45.2 auto
 commit
#
ospf 1
 silent-interface GigabitEthernet0/0/0
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
  network 192.168.45.0 0.0.0.255
#
return
```

```
<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/0
 ip address 192.168.45.3 255.255.255.0
 vrrp vrid 45 virtual-ip 192.168.45.1
#
interface GigabitEthernet0/0/2
 ip address 10.0.13.2 255.255.255.0
 ospf cost 100
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
ospf 1
 silent-interface GigabitEthernet0/0/0
 area 0.0.0.0
```

```
  network 10.0.3.0 0.0.0.255
  network 10.0.13.0 0.0.0.255
  network 192.168.45.0 0.0.0.255
#
return

<R4>display current-configuration
[V200R007C00SPC600]
#
 sysname R4
#
interface GigabitEthernet0/0/0
 ip address 192.168.45.4 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.45.1
#
return

<R5>display current-configuration
[V200R007C00SPC600]
#
 sysname R5
#
interface GigabitEthernet0/0/0
 ip address 192.168.45.5 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.45.1
#
return

<SW1>display current-configuration
!Software Version V200R008C00SPC500
#
sysname SW1
#
vlan batch 12
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/2
```

```
 port link-type access
 port default vlan 12
#
return

<SW2>display current-configuration
!Software Version V200R008C00SPC500
#
sysname SW2
#
vlan batch 13
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 13
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 13
#
return
```

华为职业认证通过者权益

获得华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*）享有如下特权：

- 1、华为e-learning 课程学习：登录*华为在线学习网站*，进入“*华为培训/在线学习*”栏目
  - **通过HCNA和HCNP认证：**可获得职业认证及基础类产品技术e-Learning课程权限
  - **通过HCIE认证：**可获得所有华为HCIE用户类e-Learning课程权限
  - **HCIE用户权限获取方式**：请提交您关联证书的“华为账号” 到 *Learning@huawei.com 申请权限*
- 2、华为培训教材下载
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。
- 3、华为在线公开课(LVC)优先参与
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证及产品技术培训课程，华为讲师授课
  - **方式**：开班计划请访问*华为LVC公开课*页面
- 4、学习工具 下载
  - *eNSP*：可扩展的、图形化网络仿真工具，可以实现网络设备的仿真模拟
  - *WLAN Planner*：室内放装AP的网络规划工具
  - *eDesk*：企业数通和安全设备运维管理平台，提供巡检、排障、补丁等功能
  - *HedEx Lite*：华为产品文档管理工具，支持浏览、搜索、升级和管理产品资料
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。