学习推荐

- 华为培训与认证官方网站
  - http://learning.huawei.com/cn/
- 华为在线学习
  - https://ilearningx.huawei.com/portal/#/portal/ebg/26
- 华为职业认证
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=zh
- 查找培训入口
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=zh

更多信息

- 华为培训APP

华为认证系列教程

HCIA-R&S进阶

华为网络技术与设备

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

HCIA-R&S华为网络技术与设备

实验指导书

第2.5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。

HCIA 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。HCIA 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。HCIA 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 HCIA 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。

HCIP-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。HCIP-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 HCIP-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！

本书常用图标

通用路由器

通用交换机

防火墙

网络云

以太网线缆

串口线缆

实验环境说明

组网介绍

本实验环境面向准备HCIA-R&S考试的网络工程师,内容由HCIA-R&S的VRP基础操作、路由协议原理、以太网交换技术、广域网技术、网络安全技术等部分的实验组成。

实验设备包括路由器3台，交换机4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HCIA-R&S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
S1	S5720-36C-EI-AC	V2R8
S2	S5720-36C-EI-AC	V2R8
S3	S5720-36C-EI-AC	V2R8
S4	S5720-36C-EI-AC	V2R8

目录

第一章 以太网与VLAN

实验 1-1 以太网接口和链路配置

学习目标

- 掌握接口速率的配置方法
- 掌握使用手动模式配置链路聚合的方法
- 掌握使用静态LACP模式配置链路聚合的方法
- 掌握在静态LACP模式下配置接口优先级的方法

拓扑图

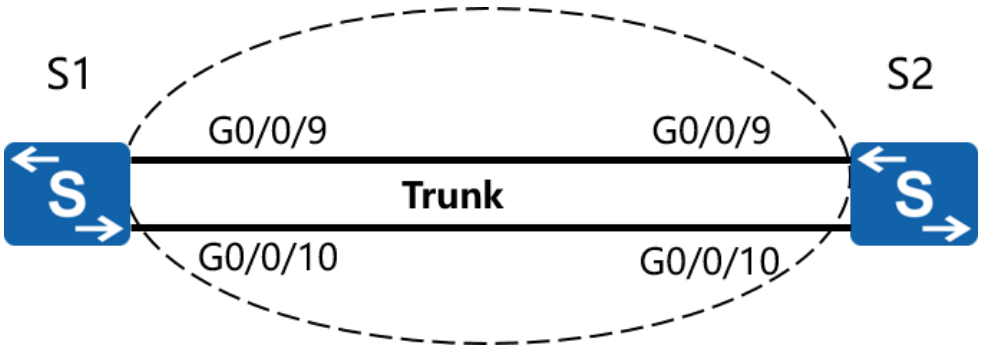

图1.1 以太网链路聚合拓扑图

场景

您是公司的网络管理员。现在公司购买了两台华为的S5700系列的交换机，为了提高交换机之间链路带宽以及可靠性 ,您需要在交换机上配置链路聚合功能。

操作步骤

步骤一 以太网交换机基础配置

华为交换机接口默认开启了自协商功能。在本任务中，需要手动配置S1与

S2上G0/0/9和G0/0/10接口的速率。

首先修改交换机的设备名称，然后查看S1上G0/0/9和G0/0/10接口的详细信息。

```
<Quidway>system-view
[Quidway]sysname S1
[S1]display interface GigabitEthernet 0/0/9
GigabitEthernet0/0/9 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : trunk(negotiated),
PVID :       1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is d0d0-4ba6-aab0
Current system time: 2016-11-23 14:18:37
Port Mode: COMMON COPPER
Speed : 1000,     Loopback: NONE
Duplex: FULL,     Negotiation: ENABLE
Mdi     : AUTO,     Flow-control: DISABLE
Last 300 seconds input rate 256 bits/sec, 0 packets/sec
Last 300 seconds output rate 912 bits/sec, 0 packets/sec
Input peak rate 13976 bits/sec, Record time: 2016-11-22 14:59:12
Output peak rate 13976 bits/sec, Record time: 2016-11-22 14:59:12

Input:   8802 packets, 1242101 bytes
  Unicast:                    854,   Multicast:                  7017
  Broadcast:                  931,   Jumbo:                        0
  Discard:                      0,   Pause:                         0
  Frames:                       0

  Total Error:                  0
  CRC:                          0,   Giants:                        0
  Jabbers:                      0,   Fragments:                     0
  Runts:                        0,   DropEvents:                    0
  Alignments:                   0,   Symbols:                       0
  Ignoreds:                     0

Output:   53495 packets, 7626413 bytes
  Unicast:                    231,   Multicast:                 49564
  Broadcast:                 3700,   Jumbo:                        0
  Discard:                      0,   Pause:                         0

  Total Error:                  0
  Collisions:                   0,   ExcessiveCollisions:           0
  Late Collisions:              0,   Deferreds:                     0
  Buffers Purged:               0
```

Input bandwidth utilization threshold : 80.00%
Output bandwidth utilization threshold: 80.00%
Input bandwidth utilization : 0%
Output bandwidth utilization : 0%

[S1]display interface GigabitEthernet 0/0/10
GigabitEthernet0/0/10 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : trunk(negotiated),
PVID : 1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is d0d0-4ba6-aab0
Current system time: 2016-11-23 14:22:22
Port Mode: COMMON COPPER
Speed : 1000, Loopback: NONE
Duplex: FULL, Negotiation: ENABLE
Mdi : AUTO, Flow-control: DISABLE
Last 300 seconds input rate 72 bits/sec, 0 packets/sec
Last 300 seconds output rate 1024 bits/sec, 0 packets/sec
Input peak rate 14032 bits/sec, Record time: 2016-11-22 14:59:12
Output peak rate 14032 bits/sec, Record time: 2016-11-22 14:59:12

Input: 7025 packets, 786010 bytes
Unicast: 0, Multicast: 7025
Broadcast: 0, Jumbo: 0
Discard: 0, Pause: 0
Frames: 0

Total Error: 0
CRC: 0, Giants: 0
Jabbers: 0, Fragments: 0
Runts: 0, DropEvents: 0
Alignments: 0, Symbols: 0
Ignoreds: 0

Output: 54507 packets, 7979793 bytes
Unicast: 150, Multicast: 49709
Broadcast: 4648, Jumbo: 0
Discard: 0, Pause: 0

Total Error: 0
Collisions: 0, ExcessiveCollisions: 0
Late Collisions: 0, Deferreds: 0
Buffers Purged: 0

Input bandwidth utilization threshold : 80.00%
Output bandwidth utilization threshold: 80.00%
Input bandwidth utilization : 0%
Output bandwidth utilization : 0%

在修改接口的速率之前应先关闭接口的自协商功能，然后将S1上的G0/0/9和G0/0/10接口的速率配置为100 Mbit/s。

```
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]undo negotiation auto
[S1-GigabitEthernet0/0/9]speed 100
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]undo negotiation auto
[S1-GigabitEthernet0/0/10]speed 100
```

同样的方法将S2上的G0/0/9和G0/0/10接口的速率配置为100 Mbit/s。

```
<Quidway>system-view
[Quidway]sysname S2
[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]undo negotiation auto
[S2-GigabitEthernet0/0/9]speed 100
[S2-GigabitEthernet0/0/9]quit
[S2]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]undo negotiation auto
[S2-GigabitEthernet0/0/10]speed 100
```

验证S1上的G0/0/9和G0/0/10接口的速率已配置成功。

```
[S1]display interface GigabitEthernet 0/0/9
GigabitEthernet0/0/9 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : trunk(negotiated),
PVID :  1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is d0d0-4ba6-aab0
Current system time: 2016-11-23 14:29:45
Port Mode: COMMON COPPER
Speed : 100,  Loopback: NONE
Duplex: FULL,  Negotiation: DISABLE
Mdi  : AUTO,  Flow-control: DISABLE
......output omit......
```

```
[S1]display interface GigabitEthernet 0/0/10
GigabitEthernet0/0/10 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : trunk(negotiated),
PVID :       1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is d0d0-4ba6-aab0
Current system time: 2016-11-23 14:32:53
Port Mode: COMMON COPPER
Speed : 100,       Loopback: NONE
Duplex: FULL,      Negotiation: DISABLE
Mdi     : AUTO,     Flow-control: DISABLE
……output omit……
```

步骤二　配置手动模式的链路聚合

在S1和S2上创建Eth-Trunk 1，然后将G0/0/9和G0/0/10接口加入Eth-Trunk 1(注意 :将接口加入Eth-Trunk前需确认成员接口下没有任何配置)。

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]eth-trunk 1
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1

[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]quit
[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]eth-trunk 1
[S2-GigabitEthernet0/0/9]quit
[S2]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]eth-trunk 1
```

验证Eth-Trunk的配置结果。

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL              Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1    Max Bandwidth-affected-linknumber: 8
Operate status: up               Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName                         Status         Weight
GigabitEthernet0/0/9             Up             1
```

```
GigabitEthernet0/0/10              Up              1

[S2]display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL               Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1    Max Bandwidth-affected-linknumber: 8
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName                          Status        Weight
GigabitEthernet0/0/9              Up            1
GigabitEthernet0/0/10             Up            1
```

回显信息中灰色阴影标注的部分表明Eth-Trunk工作正常，成员接口都已正确加入。

步骤三　配置静态 LACP 模式的链路聚合

删除S1和S2上的G0/0/9和G0/0/10接口下的配置。

```
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]undo eth-trunk
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]undo eth-trunk

[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]undo eth-trunk
[S2-GigabitEthernet0/0/9]quit
[S2]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]undo eth-trunk
```

创建Eth-Trunk 1并配置该Eth-Trunk为静态LACP模式。然后将G0/0/9和G0/0/10接口加入Eth-Trunk 1。

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]mode lacp
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]eth-trunk 1
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1

[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]mode lacp
```

```
[S2-Eth-Trunk1]quit
[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]eth-trunk 1
[S2-GigabitEthernet0/0/9]quit
[S2]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]eth-trunk 1
```

查看交换机上Eth-Trunk的信息，查看链路是否协商成功。

```
[S1]display eth-trunk
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: LACP
Preempt Delay: Disabled        Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768          System ID: d0d0-4ba6-aab0
Least Active-linknumber: 1    Max Active-linknumber: 8
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName              Status     PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/9     Selected 100M       32768       1         289       10111100      1
GigabitEthernet0/0/10   Selected 100M       32768       2         289       10111100      1

Partner:
--------------------------------------------------------------------------------
ActorPortName              SysPri     SystemID           PortPri PortNo PortKey PortState
GigabitEthernet0/0/9     32768      d0d0-4ba6-ac20   32768    1         289       10111100
GigabitEthernet0/0/10   32768      d0d0-4ba6-ac20   32768    2         289       10111100
```

在S1上配置LACP的系统优先级为100，使其成为LACP主动端。

```
[S1]lacp    priority 100
```

配置接口的优先级确定活动链路。

```
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]lacp priority 100
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]lacp priority 100
```

验证Eth-Trunk的配置结果。

```
[S1]display    eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: LACP
Preempt Delay: Disabled        Hash arithmetic: According to SIP-XOR-DIP
```

```
System Priority: 100            System ID: d0d0-4ba6-aab0
Least Active-linknumber: 1   Max Active-linknumber: 8
Operate status: up              Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName              Status     PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/9     Selected 100M       100        1        289       10111100      1
GigabitEthernet0/0/10   Selected 100M       100        2        289       10111100      1

Partner:
--------------------------------------------------------------------------------
ActorPortName              SysPri     SystemID           PortPri PortNo PortKey PortState
GigabitEthernet0/0/9     32768      d0d0-4ba6-ac20   32768    1        289       10111100
GigabitEthernet0/0/10   32768      d0d0-4ba6-ac20   32768    2        289       10111100

[S2]display   eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                       WorkingMode: LACP
Preempt Delay: Disabled       Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768        System ID: d0d0-4ba6-ac20
Least Active-linknumber: 1   Max Active-linknumber: 8
Operate status: up              Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName              Status     PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/9     Selected 100M       32768      1        289       10111100      1
GigabitEthernet0/0/10   Selected 100M       32768      2        289       10111100      1

Partner:
--------------------------------------------------------------------------------
ActorPortName              SysPri     SystemID           PortPri PortNo PortKey PortState
GigabitEthernet0/0/9     100        d0d0-4ba6-aab0   100      1        289       10111100
GigabitEthernet0/0/10   100        d0d0-4ba6-aab0   100      2        289       10111100
```

配置文件

```
[S1]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
#
 lacp priority 100
#
interface Eth-Trunk1
```

```
 mode lacp
#
interface GigabitEthernet0/0/9
 eth-trunk 1
 lacp priority 100
 undo negotiation auto
 speed 100
#
interface GigabitEthernet0/0/10
 eth-trunk 1
 lacp priority 100
 undo negotiation auto
 speed 100
#
return

[S2]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S2
#
interface Eth-Trunk1
 mode lacp
#
interface GigabitEthernet0/0/9
 eth-trunk 1
 undo negotiation auto
 speed 100
#
interface GigabitEthernet0/0/10
 eth-trunk 1
 undo negotiation auto
 speed 100
#
return
```

实验 1-2 VLAN 配置

学习目标

- 掌握VLAN的创建方法
- 掌握Access和Trunk类型接口的配置方法
- 掌握Hybird接口的配置方法
- 掌握将接口与VLAN关联的配置方法

拓扑图

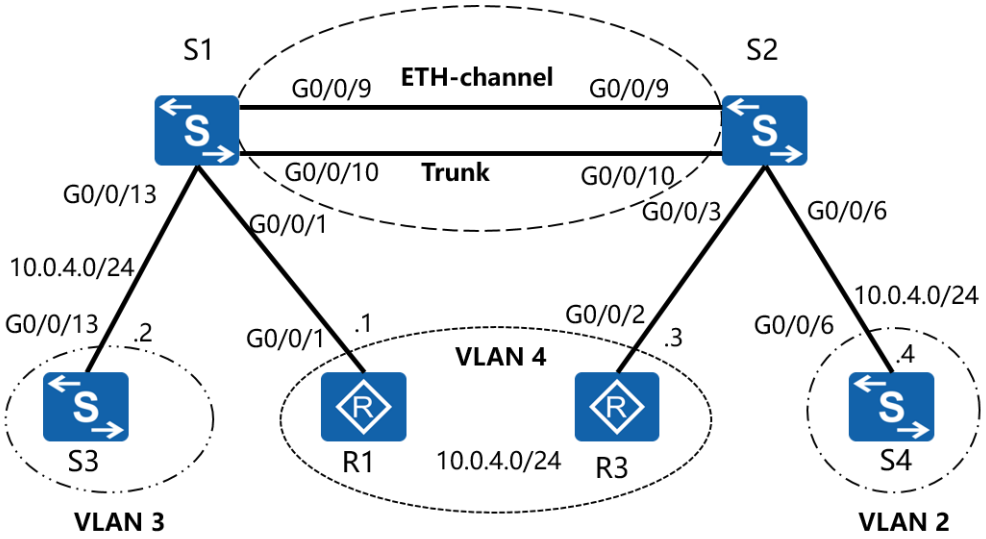

图1.2 VLAN配置实验拓扑图

场景

目前，公司网络内的所有主机都处在同一个广播域，网络中充斥着大量的广播流量。作为网络管理员，您需要将网络划分成多个VLAN来控制广播流量的泛洪。本实验中，您需要在交换机S1和S2上进行VLAN配置。

操作步骤

步骤一　实验环境准备

如果本任务中您使用的是空配置设备，那么请从步骤1开始配置。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

在S1和S2上创建Eth-Trunk 1并配置该Eth-Trunk为静态LACP模式。然后将G0/0/9和G0/0/10接口加入Eth-Trunk 1。

```
<Quidway>system-view
[Quidway]sysname S1
[S1]interface Eth-trunk 1
[S1-Eth-Trunk1]mode lacp
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet0/0/9
[S1-GigabitEthernet0/0/9]eth-trunk 1
[S1-GigabitEthernet0/0/9]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1
```

```
<Quidway>system-view
[Quidway]sysname S2
[S2]interface eth-trunk 1
[S2-Eth-Trunk1]mode lacp
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/9
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/10
```

步骤二　关闭不相关接口，并配置 Trunk

为了确保测试结果的准确性，需要关闭S3上的E0/0/1和E0/0/7端口以及S4上的E0/0/1和E0/0/14端口。

```
<Quidway>system-view
Enter system view, return user view with Ctrl+Z.
[Quidway]sysname S3
[S3]interface GigabitEthernet 0/0/1
[S3-GigabitEthernet0/0/1]shutdown
[S3-GigabitEthernet0/0/1]quit
[S3]interface GigabitEthernet 0/0/7
[S3-GigabitEthernet0/0/7]shutdown
```

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

```
[Quidway]sysname S4
[S4]interface GigabitEthernet 0/0/1
[S4-GigabitEthernet0/0/1]shutdown
[S4-GigabitEthernet0/0/1]quit
[S4]interface GigabitEthernet 0/0/14
[S4-GigabitEthernet0/0/14]shutdown
```

交换机端口的类型默认为Hybrid端口。将Eth-Trunk 1的端口类型配置为Trunk，并允许所有VLAN的报文通过该端口。

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]port link-type trunk
[S1-Eth-Trunk1]port trunk allow-pass vlan all

[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]port link-type trunk
[S2-Eth-Trunk1]port trunk allow-pass vlan all
```

步骤三　创建 VLAN

本实验中将S3、R1、R3和S4设备作为客户端主机。在S1和S2上分别创建VLAN，并使用两种不同方式将端口加入到已创建VLAN中。将所有连接客户端的端口类型配置为Access。

在S1上，将端口G0/0/13和G0/0/1分别加入到VLAN 3和VLAN 4。

在S2上，将端口G0/0/3和G0/0/6分别加入VLAN 4和VLAN 2。

```
[S1]interface GigabitEthernet0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]quit
[S1]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]quit
[S1]vlan 2
[S1-vlan2]vlan 3
[S1-vlan3]port GigabitEthernet0/0/13
[S1-vlan3]vlan 4
[S1-vlan4]port GigabitEthernet0/0/1

[S2]vlan batch 2 to 4
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]port link-type access
[S2-GigabitEthernet0/0/3]port default vlan 4
[S2-GigabitEthernet0/0/3]quit
```

```
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]port link-type access
[S2-GigabitEthernet0/0/6]port default vlan 2
```

确认S1和S2上已成功创建VLAN，且已将相应端口划分到对应的VLAN中。

```
<S1>display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------
VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/2(U)      GE0/0/3(U)      GE0/0/4(U)      GE0/0/5(U)
                GE0/0/6(D)      GE0/0/7(D)      GE0/0/8(D)      GE0/0/11(D)
                GE0/0/12(D)     GE0/0/14(U)     GE0/0/15(D)     GE0/0/16(D)
                GE0/0/17(D)     GE0/0/18(D)     GE0/0/19(D)     GE0/0/20(D)
                GE0/0/21(U)     GE0/0/22(U)     GE0/0/23(U)     GE0/0/24(D)
                GE0/0/25(D)     GE0/0/26(D)     GE0/0/27(D)     GE0/0/28(D)
                XGE0/0/1(D)     XGE0/0/2(D)     XGE0/0/3(D)     XGE0/0/4(D)
                Eth-Trunk1(U)
2    common  TG:Eth-Trunk1(U)
3    common  UT:GE0/0/13(U)
             TG:Eth-Trunk1(U)
4    common  UT:GE0/0/1(U)
             TG:Eth-Trunk1(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1    enable  default       enable  disable    VLAN 0001
2    enable  default       enable  disable    VLAN 0002
3    enable  default       enable  disable    VLAN 0003
4    enable  default       enable  disable    VLAN 0004
```

```
<S2>display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------
VID  Type     Ports
--------------------------------------------------------------------------------
1    common   UT:GE0/0/1(U)      GE0/0/2(U)      GE0/0/4(U)      GE0/0/5(U)
                GE0/0/7(D)      GE0/0/8(D)      GE0/0/11(U)     GE0/0/12(U)
                GE0/0/13(U)     GE0/0/14(D)     GE0/0/15(D)     GE0/0/16(D)
                GE0/0/17(D)     GE0/0/18(D)     GE0/0/19(D)     GE0/0/20(D)
                GE0/0/21(D)     GE0/0/22(D)     GE0/0/23(U)     GE0/0/24(U)
                GE0/0/25(D)     GE0/0/26(D)     GE0/0/27(D)     GE0/0/28(D)
                XGE0/0/1(D)     XGE0/0/2(D)     XGE0/0/3(D)     XGE0/0/4(D)
                Eth-Trunk1(U)
2    common   UT:GE0/0/6(D)
              TG:Eth-Trunk1(U)
3    common   TG:Eth-Trunk1(U)
4    common   UT:GE0/0/3(U)
              TG:Eth-Trunk1(U)
VID  Status   Property       MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1    enable   default        enable   disable     VLAN 0001
2    enable   default        enable   disable     VLAN 0002
3    enable   default        enable   disable     VLAN 0003
4    enable   default        enable   disable     VLAN 0004
```

回显信息中灰色阴影标注的部分表明接口已经加入到各个对应VLAN中，并且Eth-Trunk 1端口允许所有VLAN的报文通过。

步骤四　为客户端配置 IP 地址

分别为主机R1、S3、R3和S4配置IP地址。由于无法直接为交换机的物理接口分配IP地址，因此将S3和S4的本地管理接口VLANIF 1作为用户接口，配置IP地址。

```
<Huawei>system-view

[Huawei]sysname R1

[R1]interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]ip address 10.0.4.1 24


[S3]interface vlanif 1

[S3-vlanif1]ip address 10.0.4.2 24


<Huawei>system-view

[Huawei]sysname R3

[R3]interface GigabitEthernet0/0/2

[R3-GigabitEthernet0/0/2]ip address 10.0.4.3 24


[S4]interface vlanif 1

[S4-vlanif1]ip address 10.0.4.4 24
```

步骤五　检测设备连通性，验证 VLAN 配置结果

执行**ping**命令。同属VLAN 4中的R1和R3能够相互通信。其他不同VLAN间的设备无法通信。

```
[R1]ping 10.0.4.3

  PING 10.0.4.3: 56  data bytes, press CTRL_C to break

    Reply from 10.0.4.3: bytes=56 Sequence=1 ttl=255 time=6 ms

    Reply from 10.0.4.3: bytes=56 Sequence=2 ttl=255 time=2 ms

    Reply from 10.0.4.3: bytes=56 Sequence=3 ttl=255 time=2 ms

    Reply from 10.0.4.3: bytes=56 Sequence=4 ttl=255 time=2 ms

    Reply from 10.0.4.3: bytes=56 Sequence=5 ttl=255 time=2 ms
```

```
  --- 10.0.4.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 2/2/6 ms

[R1]ping 10.0.4.4
  PING 10.0.4.4: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
  --- 10.0.4.4 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

同样，还可以检测R1和S3以及R3和S4之间的连通性。此处不再赘述。

步骤六　配置 Hybrid 端口

配置端口的类型为Hybrid ,可以实现端口为来自不同VLAN报文打上标签或去除标签的功能。本任务中 ,需要通过配置Hybrid端口来允许VLAN 2和VLAN 4之间可以互相通信。

将S1上的G0/0/1端口和S2上的G0/0/3和G0/0/6端口的类型配置为Hybrid。同时，配置这些端口发送数据帧时能够去掉VLAN 2和VLAN 4的标签。

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port default vlan
[S1-GigabitEthernet0/0/1]port link-type hybrid
[S1-GigabitEthernet0/0/1]port hybrid untagged vlan 2 4
[S1-GigabitEthernet0/0/1]port hybrid pvid vlan 4
```

```
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]undo port default vlan
[S2-GigabitEthernet0/0/3]port link-type hybrid
[S2-GigabitEthernet0/0/3]port hybrid untagged vlan 2 4
[S2-GigabitEthernet0/0/3]port hybrid pvid vlan 4
[S2-GigabitEthernet0/0/3]quit
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]undo port default vlan
[S2-GigabitEthernet0/0/6]port link-type hybrid
[S2-GigabitEthernet0/0/6]port hybrid untagged vlan 2 4
[S2-GigabitEthernet0/0/6]port hybrid pvid vlan 2
```

执行**port hybrid pvid vlan**命令，可以配置端口收到数据帧时需要给数据帧添加的VLAN标签。同时**port hybrid untagged vlan**命令可以配置该端口在向主机转发数据帧之前，删除相应的VLAN标签。

执行**ping**命令。测试VLAN 3中的R1与R3是否还能通信。

```
<R1>ping 10.0.4.3
  PING 10.0.4.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.3: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.4.3: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.4.3: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.4.3: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 10.0.4.3: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 10.0.4.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/2/10 ms
```

执行**ping**命令，测试VLAN 2中的S4能否与VLAN 4中的R1通信。

```
<R1>ping 10.0.4.4
  PING 10.0.4.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.4: bytes=56 Sequence=1 ttl=255 time=41 ms
    Reply from 10.0.4.4: bytes=56 Sequence=2 ttl=254 time=2 ms
    Reply from 10.0.4.4: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 10.0.4.4: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 10.0.4.4: bytes=56 Sequence=5 ttl=254 time=2 ms
  --- 10.0.4.4 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/10/41 ms
```

通过配置Hybrid端口，使VLAN 2内的主机能够接收来自VLAN 4的报文，反之亦然。而没有配置Hybrid端口的VLAN 3中地址为10.0.4.2的主机仍无法与其他VLAN主机通信。

配置文件

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.1 255.255.255.0
#
return


[S3]display current-configuration
```

```
#
!Software Version V100R006C05
 sysname S3
#
interface Vlanif1
 ip address 10.0.4.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 shutdown
#
interface GigabitEthernet0/0/7
 shutdown
#
return

[S1]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
#
 vlan batch 2 to 4
#
 lacp priority 100
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 mode lacp
#
interface GigabitEthernet0/0/1
```

```
 port link-type hybrid
 port hybrid pvid vlan 4
 port hybrid untagged vlan 2 4
#
interface GigabitEthernet0/0/9
 undo negotiation auto
 speed 100
 eth-trunk 1
 lacp priority 100
#
interface GigabitEthernet0/0/10
 undo negotiation auto
 speed 100
 eth-trunk 1
 lacp priority 100
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 3
#
return

[S2]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S2
#
 vlan batch 2 to 4
#
interface Eth-Trunk1
```

```
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 mode lacp
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 4
 port hybrid untagged vlan 2 4
#
interface GigabitEthernet0/0/9
 undo negotiation auto
 speed 100
 eth-trunk 1
#
interface GigabitEthernet0/0/10
 undo negotiation auto
 speed 100
 eth-trunk 1
#
interface GigabitEthernet0/0/6
 port link-type hybrid
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2 4
#
return

[R3]display current-configuration
[V200R007C00SPC600]
#
 sysname R3
```

```
#
interface GigabitEthernet0/0/2
 ip address 10.0.4.3 255.255.255.0
#
return

[S4]display current-configuration
#
!Software Version V100R006C05
 sysname S4
#
interface Vlanif1
 ip address 10.0.4.4 255.255.255.0
#
interface GigabitEthernet0/0/1
 shutdown
#
interface GigabitEthernet0/0/14
 shutdown
#
return
```

实验 1-3 VLAN 间路由配置

学习目标

- 掌握用于VLAN间路由的Trunk接口的配置方法
- 掌握在单个物理接口上配置多个子接口的方法
- 掌握在VLAN间实现ARP通信的配置方法

拓扑图

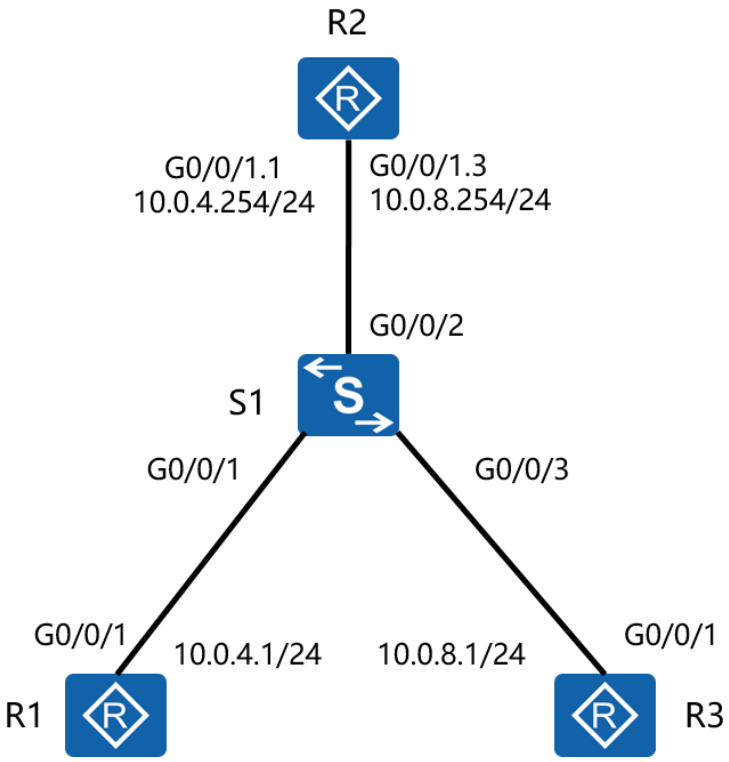

图 1.3 单臂路由实验拓扑图

场景

企业内部网络通常会通过划分不同的VLAN来隔离不同部门之间的二层通信，并保证各部门间的信息安全。但是由于业务需要，部分部门之间需要实现跨VLAN通信，网络管理员决定借助路由器，通过配置单臂路由实现R1与R3之间跨VLAN通信的需求。

操作步骤

步骤一　实验环境准备

如果本任务中您使用的是空配置设备，需要从步骤1开始配置，然后跳过步骤2。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

配置R1、R3和S1的设备名称，并按照拓扑图配置R1的G0/0/1接口的IP地址。

```
<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 10.0.4.1 24

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

<Quidway>system-view
[Quidway]sysname S1
```

步骤二　为 R3 配置 IP 地址

按照拓扑图配置R3上的G0/0/1接口的IP地址。

```
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.8.1 24
```

步骤三　创建 VLAN

在S1上创建VLAN 4和VLAN 8，将端口G0/0/1加入到VLAN 4中，将端口G0/0/3加入到VLAN 8中。

```
[S1]vlan batch 4 8
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 4
[S1-GigabitEthernet0/0/1]quit
[S1]interface GigabitEthernet0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 8
[S1-GigabitEthernet0/0/3]quit
```

将S1连接R2路由器的G0/0/2端口配置为Trunk接口，并允许VLAN 4和VLAN 8的报文通过。

```
[S1]interface GigabitEthernet0/0/2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan 4 8
```

步骤四　配置 R2 上的子接口实现 VLAN 间路由

由于路由器只有一个实际的物理接口与交换机S1相连，而实际上不同部门属于不同VLAN和不同网段，所以在路由器上配置不同的逻辑子接口来扮演不同的网关角色，在R2上配置子接口G0/0/1.1和G0/0/1.3，并作为VLAN 4和VLAN 8的网关。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/1.1
[R2-GigabitEthernet0/0/1.1]ip address 10.0.4.254 24
[R2-GigabitEthernet0/0/1.1]dot1q termination vid 4
[R2-GigabitEthernet0/0/1.1]arp broadcast enable
[R2-GigabitEthernet0/0/1.1]quit
[R2]interface GigabitEthernet0/0/1.3
[R2-GigabitEthernet0/0/1.3]ip address 10.0.8.254 24
[R2-GigabitEthernet0/0/1.3]dot1q termination vid 8
```

[R2-GigabitEthernet0/0/1.3]arp broadcast enable

在R1和R3上各配置一条默认路由指向各自的网关。

[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.254

[R3]ip route-static 0.0.0.0 0.0.0.0 10.0.8.254

配置完成后，检测R1与R3间的连通性。

```
<R1>ping 10.0.8.1
  PING 10.0.8.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.8.1: bytes=56 Sequence=1 ttl=254 time=10 ms
    Reply from 10.0.8.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.8.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.8.1: bytes=56 Sequence=4 ttl=254 time=10 ms
    Reply from 10.0.8.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 10.0.8.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/4/10 ms
```

```
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

10.0.4.0/24         Direct  0    0           D   10.0.4.254      GigabitEthernet0/0/1.1
10.0.4.254/32       Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1.1
```

10.0.4.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1.1
10.0.8.0/24	Direct	0	0	D	10.0.8.254	GigabitEthernet0/0/1.3
10.0.8.254/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1.3
10.0.8.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1.3
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

配置文件

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.4.254
#
return


[R2]display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/1.1
```

```
 dot1q termination vid 4
 ip address 10.0.4.254 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/1.3
 dot1q termination vid 8
 ip address 10.0.8.254 255.255.255.0
 arp broadcast enable
#
return

[R3]display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.8.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.8.254
#
return

[S1]display current-configuration
!Software Version V200R008C00SPC500
#
sysname S1
#
vlan batch 4 8
#
```

```
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 4
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 4 8
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 8
#
return
```

实验 1-4 配置三层交换

学习目标

- 掌握通过三层交换机实现VLAN间通信的配置方法
- 掌握通过以太网Trunk链路实现VLAN间通信的配置方法
- 掌握在不同VLAN间配置动态路由协议OSPF的方法

拓扑图

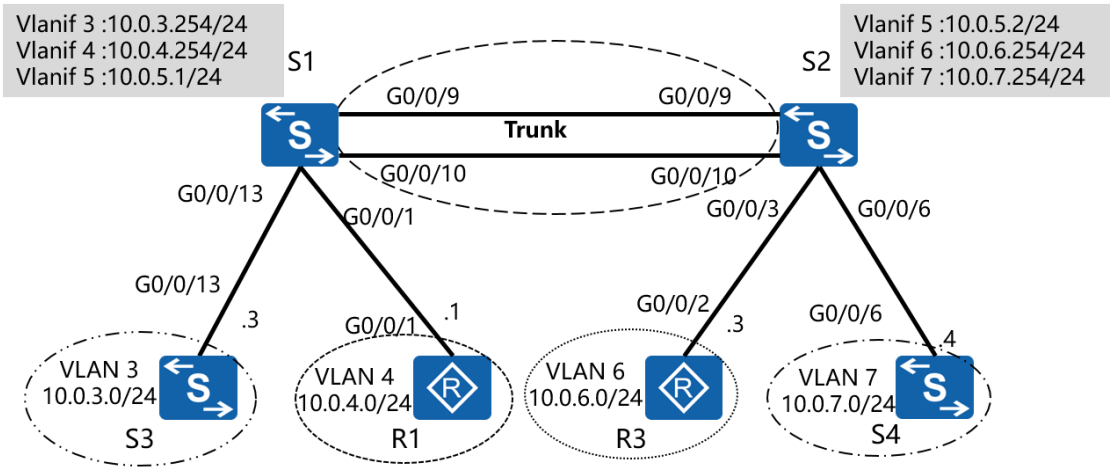

图1.4 三层交换实验拓扑图

场景

在企业网络中，通过使用三层交换机可以简便的实现VLAN间通信。作为企业的网络管理员，您需要在三层交换机配置VLANIF接口的三层功能，使得如上所示拓扑图中的网络能够实现VLAN间通信。此外，为了使S1和S2所连接的不同网络能够进行三层通信，还需要配置路由协议。

操作步骤

步骤一　实验环境准备

如果本任务中您使用的是空配置设备，需要从步骤1开始，然后跳过步骤2。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

将R1上的G0/0/1接口的IP地址配置为10.0.4.1/24，在S1和S2之间配置Eth-Trunk，并关闭S3和S4上的无关端口。

```
<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 10.0.4.1 24

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

<Quidway>system-view
[Quidway]sysname S1
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]mode lacp
[S1-Eth-Trunk1]port link-type trunk
[S1-Eth-Trunk1]port trunk allow-pass vlan all
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]eth-trunk 1
[S1-GigabitEthernet0/0/9]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1

<Quidway>system-view
[Quidway]sysname S2
[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]mode lacp
[S2-Eth-Trunk1]port link-type trunk
[S2-Eth-Trunk1]port trunk allow-pass vlan all
```

[S2-Eth-Trunk1]quit

[S2]interface GigabitEthernet 0/0/9

[S2-GigabitEthernet0/0/9]eth-trunk 1

[S2-GigabitEthernet0/0/9]interface GigabitEthernet 0/0/10

[S2-GigabitEthernet0/0/10]eth-trunk 1

<Quidway>system-view

[Quidway]sysname S3

[S3]interface GigabitEthernet 0/0/7

[S3-GigabitEthernet0/0/7]shutdown

<Quidway>system-view

[Quidway]sysname S4

[S4]interface GigabitEthernet 0/0/14

[S4-GigabitEthernet0/0/14]shutdown

步骤二　清除设备上原有的配置

清除设备上的VLAN路由和子接口配置。

[R1]undo ip route-static 0.0.0.0 0

[R2]undo interface GigabitEthernet 0/0/1.1

[R2]undo interface GigabitEthernet 0/0/1.3

[R3]interface GigabitEthernet 0/0/1

[R3-GigabitEthernet0/0/1]undo ip address

[R3-GigabitEthernet0/0/1]quit

[R3]undo ip route-static 0.0.0.0 0

[S1]undo vlan batch 4 8

Warning: The configurations of the VLAN will be deleted. Continue?[Y/N]:y

Info: This operation may take a few seconds. Please wait for a moment...done.

[S1]interface GigabitEthernet 0/0/2

[S1-GigabitEthernet0/0/2]undo port trunk allow-pass vlan 4 8

[S1-GigabitEthernet0/0/2]quit

[S1]interface GigabitEthernet 0/0/13

[S1-GigabitEthernet0/0/13]undo shutdown

[S2]interface GigabitEthernet0/0/6

[S2-GigabitEthernet0/0/6]undo shutdown

重新打开S1和S2间的Eth-Trunk接口。

[S1]interface Eth-Trunk 1

[S1-Eth-Trunk1]undo shutdown

[S2]interface Eth-Trunk 1

[S2-Eth-Trunk1]undo shutdown

步骤三　在 S1 和 S2 上批量创建 VLAN 3 到 VLAN 7

[S1]vlan batch 3 to 7

Info: This operation may take a few seconds. Please wait for a moment...done.

[S2]vlan batch 3 to 7

Info: This operation may take a few seconds. Please wait for a moment...done.

确认VLAN已成功创建。

[S1]display vlan

The total number of vlans is : 6

...output omit...

VID　Type　　Ports

----

1 common UT:GE0/0/1(U) GE0/0/2(D) GE0/0/3(U) GE0/0/4(U)
GE0/0/5(U) GE0/0/6(D) GE0/0/7(D) GE0/0/8(D)
GE0/0/11(D) GE0/0/12(D) GE0/0/13(D) GE0/0/14(D)
GE0/0/15(D) GE0/0/16(D) GE0/0/17(D) GE0/0/18(D)
GE0/0/19(D) GE0/0/20(D) GE0/0/21(U) GE0/0/22(U)
GE0/0/23(U) GE0/0/24(D) Eth-Trunk1(U)

3 common TG:Eth-Trunk1(U)

4 common TG:Eth-Trunk1(U)

5 common TG:Eth-Trunk1(U)

6 common TG:Eth-Trunk1(U)

7 common TG:Eth-Trunk1(U)

...output omit...

[S2]display vlan

The total number of vlans is : 6

...output omit...

VID Type Ports

---

1 common UT:GE0/0/1(U) GE0/0/2(D) GE0/0/3(U) GE0/0/4(U)
GE0/0/5(U) GE0/0/6(D) GE0/0/7(D) GE0/0/8(D)
GE0/0/11(U) GE0/0/12(U) GE0/0/13(U) GE0/0/14(D)
GE0/0/15(D) GE0/0/16(D) GE0/0/17(D) GE0/0/18(D)
GE0/0/19(D) GE0/0/20(D) GE0/0/21(D) GE0/0/22(D)
GE0/0/23(D) GE0/0/24(D) Eth-Trunk1(U)

3 common TG:Eth-Trunk1(U)

4 common TG:Eth-Trunk1(U)

5 common TG:Eth-Trunk1(U)

6 common TG:Eth-Trunk1(U)

7 common TG:Eth-Trunk1(U)

...output omit...

步骤四　配置 Eth-Trunk 链路

将S1上的G0/0/1和0/0/13端口分别加入VLAN 4和VLAN 3。将S2上的G0/0/3和G0/0/6端口分别加入VLAN 6和VLAN 7。

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]port trunk pvid vlan 5
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 4
[S1-GigabitEthernet0/0/1]quit
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]port default vlan 3

[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]port trunk pvid vlan 5
[S2-Eth-Trunk1]quit
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]port link-type access
[S2-GigabitEthernet0/0/3]port default vlan 6
[S2-GigabitEthernet0/0/3]quit
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]port link-type access
[S2-GigabitEthernet0/0/6]port default vlan 7
```

配置完成后，执行**display vlan**命令查看VLAN以及成员端口信息。

```
<S1>display vlan
The total number of vlans is : 6
...output omit...
```

```
VID  Type      Ports
--------------------------------------------------------------------------------
1    common    UT:GE0/0/2(D)       GE0/0/3(U)       GE0/0/4(U)       GE0/0/5(U)
                GE0/0/6(D)       GE0/0/7(D)       GE0/0/8(D)       GE0/0/11(D)
                GE0/0/12(D)      GE0/0/14(D)      GE0/0/15(D)      GE0/0/16(D)
                GE0/0/17(D)      GE0/0/18(D)      GE0/0/19(D)      GE0/0/20(D)
                GE0/0/21(U)      GE0/0/22(U)      GE0/0/23(U)      GE0/0/24(D)
                TG:Eth-Trunk1(U)
3    common UT:GE0/0/13(U)
                TG:Eth-Trunk1(U)
4    common UT:GE0/0/1(U)
                TG:Eth-Trunk1(U)
5    common UT:Eth-Trunk1(U)
6    common TG:Eth-Trunk1(U)
7    common TG:Eth-Trunk1(U)
...output omit...


<S2>display vlan
The total number of vlans is : 6
...output omit...
VID  Type      Ports
--------------------------------------------------------------------------------
1    common    UT:GE0/0/1(U)       GE0/0/2(D)       GE0/0/4(U)       GE0/0/5(U)
                GE0/0/6(D)       GE0/0/7(D)       GE0/0/8(D)       GE0/0/11(U)
                GE0/0/12(U)      GE0/0/13(U)      GE0/0/14(D)      GE0/0/15(D)
                GE0/0/16(D)      GE0/0/17(D)      GE0/0/18(D)      GE0/0/19(D)
                GE0/0/20(D)      GE0/0/21(D)      GE0/0/22(D)      GE0/0/23(D)
                TG:Eth-Trunk1(U)
3    common TG:Eth-Trunk1(U)
4    common TG:Eth-Trunk1(U)
```

5 common TG:Eth-Trunk1(U)

6 common UT:GE0/0/3(U)

TG:Eth-Trunk1(U)

7 common UT:GE0/0/6(U)

TG:Eth-Trunk1(U)

...output omit...

步骤五　配置 VLANIF 三层接口

分别为S1上的VLANIF 3、VLANIF 4和VLANIF 5以及S2上的VLANIF 5、VLANIF 6和VLANIF 7配置IP地址。

[S1]interface Vlanif 3

[S1-Vlanif3]ip address 10.0.3.254 24

[S1-Vlanif3]interface Vlanif 4

[S1-Vlanif4]ip address 10.0.4.254 24

[S1-Vlanif4]interface Vlanif 5

[S1-Vlanif5]ip address 10.0.5.1 24

[S2]interface Vlanif 5

[S2-Vlanif5]ip address 10.0.5.2 24

[S2-Vlanif5]interface Vlanif 6

[S2-Vlanif6]ip address 10.0.6.254 24

[S2-Vlanif6]interface Vlanif 7

[S2-Vlanif7]ip address 10.0.7.254 24

步骤六　为 R1、R3、S3 和 S4 配置 IP 地址和缺省路由

本实验中，R1、R3、S3和S4模拟客户端主机，四台设备都需要配置一个用户IP地址，其中S3和S4使用VLANIF 1接口配置IP地址，然后将S3的E0/0/13端口和S4的E0/0/6端口加入到VLAN 1中。R1的地址应配置为10.0.4.1/24。最后为每台设备配置一条缺省静态路由指向网关。

[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.254

```
[S3]interface Vlanif 1
[S3-Vlanif1]ip address 10.0.3.3 24
[S3-Vlanif1]quit
[S3]ip route-static 0.0.0.0 0.0.0.0 10.0.3.254

[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.6.3 24
[R3-GigabitEthernet0/0/2]quit
[R3]ip route-static 0.0.0.0 0.0.0.0 10.0.6.254

[S4]interface Vlanif 1
[S4-Vlanif1]ip address 10.0.7.4 24
[S4-Vlanif1]quit
[S4]ip route-static 0.0.0.0 0.0.0.0 10.0.7.254
```

步骤七　检测 VLAN 3 和 VLAN 4 间的连通性

检测R1和S3之间的连通性。

```
<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=37 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=253 time=2 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=253 time=10 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=253 time=3 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=253 time=2 ms
  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/10/37 ms
```

检测R1和R3之间的连通性。

```
<R1>ping 10.0.6.3
  PING 10.0.6.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
  --- 10.0.6.3 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

回显信息表明R1和R3无法互相通信。执行**tracert**命令，查找通信失败的原因。

```
[R1]tracert 10.0.6.3
traceroute to 10.0.6.3(10.0.6.3), max hops: 30 ,packet length: 40,press CTRL_C to break
 1 10.0.4.254 17 ms  4 ms  4 ms
 2  *  *  *
```

由显示信息可以看出，R1向目的地址10.0.6.3发送了数据报文，但是数据报文仅能到达地址为10.0.4.254的网关设备。

在网关设备S1上查看是否拥有到达目的网络的路由条目。

```
[S1]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
10.0.3.0/24         Direct  0    0           D   10.0.3.254      Vlanif3
```

10.0.3.254/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.0.4.0/24	Direct	0	0	D	10.0.4.254	Vlanif4
10.0.4.254/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.0.5.0/24	Direct	0	0	D	10.0.5.1	Vlanif5
10.0.5.1/32	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

由显示信息可以看出，由于网段10.0.6.0/24并非S1直连网段，且S1上也并未配置任何静态路由或用动态路由协议获取该网段路由信息，因而S1没有通往该网段的路由条目，S1就无法将数据包正确转发到该网段。

步骤八　在 S1 和 S2 上配置 OSPF 协议

```
[S1]ospf
[S1-ospf-1]area 0
[S1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255

[S2]ospf
[S2-ospf-1]area 0
[S2-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

配置完成后，待OSPF收敛完成，再查看S1的路由表。

```
[S1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

10.0.3.0/24         Direct  0    0           D   10.0.3.254      Vlanif3
10.0.3.254/32       Direct  0    0           D   127.0.0.1       InLoopBack0
```

10.0.4.0/24	Direct 0	0	D	10.0.4.254	Vlanif4
10.0.4.254/32	Direct 0	0	D	127.0.0.1	InLoopBack0
10.0.5.0/24	Direct 0	0	D	10.0.5.1	Vlanif5
10.0.5.1/32	Direct 0	0	D	127.0.0.1	InLoopBack0
10.0.6.0/24	OSPF 10	2	D	10.0.5.2	Vlanif5
10.0.7.0/24	OSPF 10	2	D	10.0.5.2	Vlanif5
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

可以观察到S1已经通过OSPF学习到了10.0.6.0/24和10.0.7.0/24这两条路由。再次检测R1和R3间的连通性。

```
[R1]ping 10.0.6.3
  PING 10.0.6.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.6.3: bytes=56 Sequence=1 ttl=253 time=11 ms
    Reply from 10.0.6.3: bytes=56 Sequence=2 ttl=253 time=1 ms
    Reply from 10.0.6.3: bytes=56 Sequence=3 ttl=253 time=10 ms
    Reply from 10.0.6.3: bytes=56 Sequence=4 ttl=253 time=1 ms
    Reply from 10.0.6.3: bytes=56 Sequence=5 ttl=253 time=1 ms
  --- 10.0.6.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/4/11 ms

[R1]ping 10.0.7.4
  PING 10.0.7.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.7.4: bytes=56 Sequence=1 ttl=253 time=30 ms
    Reply from 10.0.7.4: bytes=56 Sequence=2 ttl=252 time=2 ms
    Reply from 10.0.7.4: bytes=56 Sequence=3 ttl=252 time=3 ms
    Reply from 10.0.7.4: bytes=56 Sequence=4 ttl=252 time=2 ms
```

```
  Reply from 10.0.7.4: bytes=56 Sequence=5 ttl=252 time=2 ms

--- 10.0.7.4 ping statistics ---

  5 packet(s) transmitted

  5 packet(s) received

  0.00% packet loss

  round-trip min/avg/max = 2/7/30 ms
```

配置文件

```
[R1]display current-configuration

[V200R007C00SPC600]

#

 sysname R1

#

interface GigabitEthernet0/0/1

 ip address 10.0.4.1 255.255.255.0

#

ip route-static 0.0.0.0 0.0.0.0 10.0.4.254

#

return


[S1]display current-configuration

!Software Version V200R008C00SPC500

#

sysname S1

#

vlan batch 3 to 7

#

interface Vlanif3

 ip address 10.0.3.254 255.255.255.0

#
```

```
interface Vlanif4
 ip address 10.0.4.254 255.255.255.0
#
interface Vlanif5
 ip address 10.0.5.1 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk pvid vlan 5
 port trunk allow-pass vlan 2 to 4094
 mode lacp
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 4
#
interface GigabitEthernet0/0/9
 eth-trunk 1
#
interface GigabitEthernet0/0/10
 eth-trunk 1
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 3
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
```

```
return


[S2]display current-configuration
!Software Version V200R008C00SPC500
#
sysname S2
#
vlan batch 3 to 7
#
interface Vlanif5
 ip address 10.0.5.2 255.255.255.0
#
interface Vlanif6
 ip address 10.0.6.254 255.255.255.0
#
interface Vlanif7
 ip address 10.0.7.254 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk pvid vlan 5
 port trunk allow-pass vlan 2 to 4094
 mode lacp
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 6
#
interface GigabitEthernet0/0/6
 port link-type access
```

```
 port default vlan 7
#
interface GigabitEthernet0/0/9
 eth-trunk 1
#
interface GigabitEthernet0/0/10
 eth-trunk 1
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
return

[S3]display current-configuration
#
!Software Version V100R006C05
 sysname S3
#
interface Vlanif1
 ip address 10.0.3.3 255.255.255.0
#
interface GigabitEthernet0/0/7
 shutdown
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.3.254
#
return

[S4]display current-configuration
```

```
#
!Software Version V100R006C05
 sysname S4
#
interface Vlanif1
 ip address 10.0.7.4 255.255.255.0
#
interface GigabitEthernet0/0/14
 shutdown
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.7.254
#
return
```

第二章 企业广域网配置

实验 2-1 HDLC 和 PPP 配置

学习目标

- 掌握HDLC的基本配置方法
- 掌握DCE时钟波特率的配置方法
- 掌握PPP的基本配置方法
- 掌握PPP链路的PAP认证的配置方法
- 掌握PPP链路的CHAP认证的配置方法

拓扑图

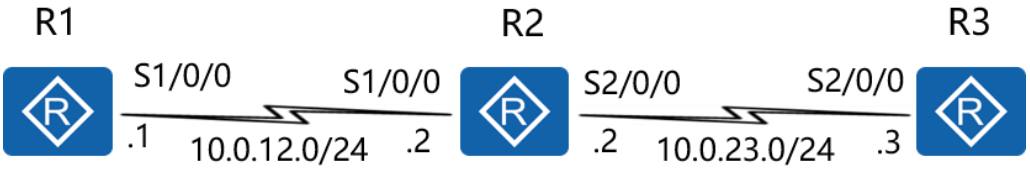

图2.1 HDLC和PPP配置实验拓扑图

场景

您是公司的网络管理员。公司总部有一台路由器R2，R1和R3分别是其他两个分部的路由器。现在您需要将总部网络和分部网络通过广域网连接起来。在广域网链路上尝试使用HDLC和PPP协议，并在使用PPP协议时配置了不同的认证方式保证安全。

操作步骤

步骤一 实验环境准备

如果本任务中您使用的是空配置设备，需要从步骤1开始，然后跳过步骤2。

如果使用的设备包含上一个实验的配置，请直接从步骤2开始。

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

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2

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

步骤二　清除设备上原有的配置

删除缺省静态路由的配置并关闭指定的以太网接口。删除无关的VLAN配置。

```
[R1]undo ip route-static 0.0.0.0 0
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]shutdown

[R3]undo ip route-static 0.0.0.0 0
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]shutdown

[S1]undo interface Vlanif 3
[S1]undo interface Vlanif 5
[S1]undo vlan batch 3 5 to 7
Warning: The configurations of the VLAN will be deleted. Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port default vlan
```

[S1-GigabitEthernet0/0/1]quit

[S1]undo ospf 1

Warning: The OSPF process will be deleted. Continue? [Y/N]:y

[S2]undo interface Vlanif 5

[S2]undo interface Vlanif 7

[S2]undo vlan batch 3 to 5 7

Warning: The configurations of the VLAN will be deleted. Continue?[Y/N]:y

Info: This operation may take a few seconds. Please wait for a moment...done.

[S2]interface GigabitEthernet 0/0/3

[S2-GigabitEthernet0/0/3]undo port default vlan

[S2-GigabitEthernet0/0/3]quit

[S2]undo ospf 1

Warning: The OSPF process will be deleted. Continue? [Y/N]:y

[S3]undo interface Vlanif 1

[S4]undo interface Vlanif 1

步骤三　为 R1、R2 和 R3 的串行接口配置 IP 地址

[R1]interface Serial 1/0/0

[R1-Serial1/0/0]ip address 10.0.12.1 24

[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

[R3]interface Serial 2/0/0

[R3-Serial2/0/0]ip address 10.0.23.3 24

步骤四　在串行接口上启用 HDLC 协议

[R1]interface Serial 1/0/0

[R1-Serial1/0/0]link-protocol hdlc

Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y

[R2]interface Serial 1/0/0

[R2-Serial1/0/0]link-protocol hdlc

Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y

[R2-Serial1/0/0]quit

[R2]interface Serial 2/0/0

[R2-Serial2/0/0]link-protocol hdlc

Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y

[R3]interface Serial 2/0/0

[R3-Serial2/0/0]link-protocol hdlc

Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y

配置完成后，查看串行接口的状态。以R1上的显示信息为例。

[R1]display interface Serial1/0/0

Serial1/0/0 current state : UP

Line protocol current state : UP

Last line protocol up time : 2016-03-10 11:25:08

Description:HUAWEI, AR Series, Serial1/0/0 Interface

Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)

Internet Address is 10.0.12.1/24

Link layer protocol is nonstandard HDLC

Last physical up time　: 2016-03-22 22:03:46

Last physical down time : 2016-03-22 22:03:44

Current system time: 2016-03-22 22:05:39

Physical layer is synchronous, Baudrate is 64000 bps

Interface is DCE, Cable type is V35, Clock mode is DCECLK1

Last 300 seconds input rate 2 bytes/sec 16 bits/sec 0 packets/sec

Last 300 seconds output rate 2 bytes/sec 16 bits/sec 0 packets/sec

Input: 9949 packets, 139374 bytes

Broadcast: 0, Multicast: 0

Errors: 0, Runts: 0

Giants: 0, CRC: 0

Alignments: 0, Overruns: 0

Dribbles: 0, Aborts: 0

No Buffers: 0, Frame Error: 0

Output: 9953 packets, 139474 bytes

Total Error: 0, Overruns: 0

Collisions: 0, Deferred: 0

DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP

Input bandwidth utilization : 0.07%

Output bandwidth utilization : 0.07%

确认该接口的物理状态和协议状态均已UP后，检测直连链路的连通性。

<R2>ping 10.0.12.1

PING 10.0.12.1: 56 data bytes, press CTRL_C to break

Reply from 10.0.12.1: bytes=56 Sequence=1 ttl=255 time=44 ms

Reply from 10.0.12.1: bytes=56 Sequence=2 ttl=255 time=39 ms

Reply from 10.0.12.1: bytes=56 Sequence=3 ttl=255 time=39 ms

Reply from 10.0.12.1: bytes=56 Sequence=4 ttl=255 time=40 ms

Reply from 10.0.12.1: bytes=56 Sequence=5 ttl=255 time=39 ms

--- 10.0.12.1 ping statistics ---

```
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 39/40/44 ms

[R2]ping 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=255 time=44 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=255 time=39 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=255 time=39 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=255 time=39 ms
  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 39/40/44 ms
```

步骤五　配置 OSPF

在三台路由器上都启用OSPF路由协议，并发布各自的直连路由。

```
[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

[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  10.0.23.0 0.0.0.255

[R3]ospf 1
```

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

配置完成后，检查设备是否通过OSPF协议学习到了相应的路由。

```
<R1>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

        10.0.12.0/24  Direct  0    0           D   10.0.12.1       Serial1/0/0
        10.0.12.1/32  Direct  0    0           D   127.0.0.1       Serial1/0/0
        10.0.12.255/32  Direct  0    0           D   127.0.0.1       Serial1/0/0
        10.0.23.0/24  OSPF    10   3124        D   10.0.12.2       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
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

确认相应的路由信息都已通过OSPF协议学习到。

在R1上，执行**ping**命令，检测R1和R3间的连通性。

```
<R1>ping 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=254 time=44 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=254 time=39 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=254 time=39 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=254 time=40 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=254 time=39 ms
  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
```

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 39/40/44 ms

步骤六　管理串口连接

查看串行接口连接的线缆的类型、接口状态和时钟频率，并修改时钟频率。

<R1>display interface Serial1/0/0

Serial1/0/0 current state : UP

Line protocol current state : UP

Last line protocol up time : 2016-03-10 11:25:08

Description:HUAWEI, AR Series, Serial1/0/0 Interface

Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)

Internet Address is 10.0.12.1/24

Link layer protocol is nonstandard HDLC

Last physical up time　: 2016-03-10 11:23:55

Last physical down time : 2016-03-10 11:23:55

Current system time: 2016-03-10 11:51:12

Physical layer is synchronous, Baudrate is 64000 bps

Interface is DCE, Cable type is V35, Clock mode is DCECLK1

Last 300 seconds input rate 5 bytes/sec 40 bits/sec 0 packets/sec

Last 300 seconds output rate 2 bytes/sec 16 bits/sec 0 packets/sec

...output omit...

回显信息表明R1的S1/0/0接口连接的是DCE线缆，时钟频率是64000bit/s。DCE设备可以控制时钟频率和带宽。

将R1和R2间链路的时钟频率修改为128000bit/s。这一操作需在DCE设备R1上执行。

[R1]interface Serial 1/0/0

[R1-Serial1/0/0]baudrate 128000

配置完成后，查看串行接口的状态，确认时钟频率已修改。

<R1>display interface Serial1/0/0

Serial1/0/0 current state : UP

Line protocol current state : UP

Last line protocol up time : 2016-03-10 11:25:08

Description:HUAWEI, AR Series, Serial1/0/0 Interface

Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)

Internet Address is 10.0.12.1/24

Link layer protocol is nonstandard HDLC

Last physical up time : 2016-03-10 11:23:55

Last physical down time : 2016-03-10 11:23:55

Current system time: 2016-03-10 11:54:19

Physical layer is synchronous, Baudrate is 128000 bps

Interface is DCE, Cable type is V35, Clock mode is DCECLK1

Last 300 seconds input rate 6 bytes/sec 48 bits/sec 0 packets/sec

Last 300 seconds output rate 4 bytes/sec 32 bits/sec 0 packets/sec

...output omit...

步骤七　修改串行接口的封装类型为 PPP

在R1和R2以及R2和R3间修改串行接口使用PPP封装。链路两端必须配置相同的封装类型，否则接口状态会出现“Down”的情况。

[R1]interface Serial 1/0/0

[R1-Serial1/0/0]link-protocol ppp

Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y

[R2]interface Serial 1/0/0

[R2-Serial1/0/0]link-protocol ppp

Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y

[R2-Serial1/0/0]quit

[R2]interface Serial 2/0/0

[R2-Serial2/0/0]link-protocol ppp

Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y

[R3]interface Serial 2/0/0

[R3-Serial2/0/0]link-protocol ppp

Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y

配置完成后，检测链路连通性。

<R2>ping 10.0.12.1

PING 10.0.12.1: 56 data bytes, press CTRL_C to break

Reply from 10.0.12.1: bytes=56 Sequence=1 ttl=255 time=22 ms

Reply from 10.0.12.1: bytes=56 Sequence=2 ttl=255 time=27 ms

Reply from 10.0.12.1: bytes=56 Sequence=3 ttl=255 time=27 ms

Reply from 10.0.12.1: bytes=56 Sequence=4 ttl=255 time=27 ms

Reply from 10.0.12.1: bytes=56 Sequence=5 ttl=255 time=27 ms

--- 10.0.12.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 22/26/27 ms

<R2>ping 10.0.23.3

PING 10.0.23.3: 56 data bytes, press CTRL_C to break

Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=255 time=35 ms

Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=255 time=40 ms

Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=255 time=40 ms

Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=255 time=40 ms

Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=255 time=40 ms

--- 10.0.23.3 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 35/39/40 ms

如果无法**Ping**通，请查看接口状态，观察协议状态是否正常。

<R1>display interface Serial1/0/0

Serial1/0/0 current state : UP

Line protocol current state : UP

Last line protocol up time : 2016-03-10 12:35:41

Description:HUAWEI, AR Series, Serial1/0/0 Interface

Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)

Internet Address is 10.0.12.1/24

Link layer protocol is PPP

LCP opened, IPCP opened

Last physical up time : 2016-03-10 11:57:20

Last physical down time : 2016-03-10 11:57:19

Current system time: 2016-03-10 13:38:03

Physical layer is synchronous, Baudrate is 128000 bps

Interface is DCE, Cable type is V35, Clock mode is DCECLK1

Last 300 seconds input rate 7 bytes/sec 56 bits/sec 0 packets/sec

Last 300 seconds output rate 4 bytes/sec 32 bits/sec 0 packets/sec

...output omit...

步骤八　检查路由表项的变化

PPP配置完成后，路由器之间会建立数据链路层的连接。本地路由器会向远端路由器发送一条主机路由，路由信息中包含本地接口的IP地址，掩码为32位。

以R2为例，可以查看到R1和R3发送的主机路由。

[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
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	Serial1/0/0
10.0.12.255/32	Direct	0	0	D	127.0.0.1	Serial1/0/0
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	Serial2/0/0
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	Serial2/0/0
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

可以看出，路由表中已经包含通往R1和R3的路由。回顾下这两条路由的由来和功能，回答下面两个问题：

如果配置的是HDLC封装，路由表中还会有这两条路由吗？

如果R1和R2上的S1/0/0接口IP地址不在同一网段，它们之间还能够通过HDLC或PPP实现通信吗？

步骤九　在 R1 和 R2 间的 PPP 链路启用 PAP 认证功能。

配置PAP认证功能，并将R1配置为PAP认证方。

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ppp authentication-mode pap
[R1-Serial1/0/0]quit
[R1]aaa
[R1-aaa]local-user huawei password cipher huawei123
 info: A new user added
```

[R1-aaa]local-user huawei service-type ppp

将R2配置为PAP被认证方。

[R2]interface Serial 1/0/0

[R2-Serial1/0/0]ppp pap local-user huawei password cipher huawei123

配置完成后，检测R1和R2间的连通性，并可以通过**debug**功能观察PAP认证报文的交互。

<R1>debugging ppp pap packet

<R1>terminal debugging

<R1>display debugging

PPP PAP packets debugging switch is on

<R1>system-view

[R1]interface Serial 1/0/0

[R1-Serial1/0/0]shutdown

[R1-Serial1/0/0]undo shutdown

Mar 10 2016 14:44:22.440.1+00:00 R1 PPP/7/debug2:

PPP Packet:

Serial1/0/0 Input PAP(c023) Pkt, Len 22

State ServerListen, code Request(01), id 1, len 18

Host Len: 6 Name:huawei

[R1-Serial1/0/0]

Mar 10 2016 14:44:22.440.2+00:00 R1 PPP/7/debug2:

PPP Packet:

Serial1/0/0 Output PAP(c023) Pkt, Len 52

State WaitAAA, code Ack(02), id 1, len 48

Msg Len: 43 Msg:Welcome to use Access ROUTER, Huawei Tech.

[R1-Serial1/0/0]return

<R1>undo debugging all

Info: All possible debugging has been turned off

步骤十　在 R2 和 R3 间的 PPP 链路启用 CHAP 认证功能

将R3配置为CHAP的认证方。

[R3]interface Serial 2/0/0

[R3-Serial2/0/0]ppp authentication-mode chap

[R3-Serial2/0/0]quit

[R3]aaa

[R3-aaa]local-user huawei password cipher huawei123

info: A new user added

[R3-aaa]local-user huawei service-type ppp

[R3-aaa]quit

[R3]interface Serial 2/0/0

[R3-Serial2/0/0]shutdown

[R3-Serial2/0/0]undo shutdown

注意，此时R3上会有如下提示：

Mar 10 2016 15:06:00+00:00 R3 %%01PPP/4/PEERNOCHAP(l)[5]:On the interface Serial2/0/0, authentication failed and PPP link was closed because CHAP was disabled on the peer.

[R3-Serial2/0/0]

Mar 10 2016 15:06:00+00:00 R3 %%01PPP/4/RESULTERR(l)[6]:On the interface Serial2/0/0, LCP negotiation failed because the result cannot be accepted.

回显信息中灰色阴影标注的部分表明与对端认证时失败。

将R2配置为CHAP的被认证方。

[R2]interface Serial 2/0/0

[R2-Serial2/0/0]ppp chap user huawei

[R2-Serial2/0/0]ppp chap password cipher huawei123

配置完成后，接口变为Up状态。执行**ping**命令测试连通性。

```
<R2>ping 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=255 time=35 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=255 time=41 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=255 time=41 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=255 time=41 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=255 time=41 ms
  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/39/41 ms
```

步骤十一 使用 debug 命令查看 R2 和 R3 之间使用 CHAP 建立 PPP 连接的协商过程

查看R2与R3建立PPP连接时的协商情况，为了看到完整的协商过程，需要先关闭R2的S2/0/0接口，然后启动**debug**命令，再打开接口，即可看到完整协商过程。

首先关闭R2的物理接口。

```
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]shutdown
```

执行**debugging ppp chap all**和**terminal debugging**命令，查看**debug**信息。

```
[R2-Serial2/0/0]return
<R2>debugging ppp chap all
<R2>terminal debugging
Info: Current terminal debugging is on.
<R2>display debugging
PPP CHAP packets debugging switch is on
```

PPP CHAP events debugging switch is on

PPP CHAP errors debugging switch is on

PPP CHAP state change debugging switch is on

打开R2的物理接口，发起认证。

<R2>system-view

Enter system view, return user view with Ctrl+Z.

[R2]interface Serial 2/0/0

[R2-Serial2/0/0]undo shutdown

此时可以看到相应的**debug**信息输出如下：

Mar 10 2016 09:10:38.700.1+00:00 R2 PPP/7/debug2:

PPP State Change:

Serial2/0/0 CHAP : Initial --> ListenChallenge

[R2-Serial2/0/0]

Mar 10 2016 09:10:38.710.1+00:00 R2 PPP/7/debug2:

PPP Packet:

Serial2/0/0 Input CHAP(c223) Pkt, Len 25

State ListenChallenge, code Challenge(01), id 1, len 21

Value_Size: 16 Value: fc 9b 56 e1 53 e3 a6 26 1b 54 e5 e2 a1 ed 90 87

Name:

[R2-Serial2/0/0]

Mar 10 2016 09:10:38.710.2+00:00 R2 PPP/7/debug2:

PPP Event:

Serial2/0/0 CHAP Receive Challenge Event

state ListenChallenge

[R2-Serial2/0/0]

Mar 10 2016 09:10:38.710.3+00:00 R2 PPP/7/debug2:

PPP Packet:

Serial2/0/0 Output CHAP(c223) Pkt, Len 31

```
        State ListenChallenge, code Response(02), id 1, len 27
        Value_Size:   16   Value: f9 54   1 69 30 59 a0 af 52 a1 1d de 85 77 27 6b
        Name: huawei
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.710.4+00:00 R2 PPP/7/debug2:
  PPP State Change:
        Serial2/0/0 CHAP : ListenChallenge --> SendResponse
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.720.1+00:00 R2 PPP/7/debug2:
  PPP Packet:
        Serial2/0/0 Input   CHAP(c223) Pkt, Len 20
        State SendResponse, code SUCCESS(03), id 1, len 16
        Message: Welcome to .
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.720.2+00:00 R2 PPP/7/debug2:
  PPP Event:
        Serial2/0/0 CHAP Receive Success Event
        state SendResponse
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.720.3+00:00 R2 PPP/7/debug2:
  PPP State Change:
        Serial2/0/0 CHAP : SendResponse --> ClientSuccess
```

回显信息中灰色阴影标注的部分显示了协商状态的变化和发送的信息。

最后关闭**debug**功能。

```
[R2-Serial2/0/0]return
<R2>undo debugging all
Info: All possible debugging has been turned off
```

附加练习：分析并验证

为什么PPP中CHAP认证比PAP认证的安全性更高？

配置文件

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$B:%I)Io0H8)[%SB[idM3C/!#%$%$
 local-user huawei service-type ppp
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap
 ip address 10.0.12.1 255.255.255.0
 baudrate 128000
#
ospf 1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
```

```
#
return

[R2]display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user huawei password cipher %$%$u[hr6d<JVHR@->T7xr1<$.iv%$%$
 ip address 10.0.12.2 255.255.255.0
#
interface Serial2/0/0
 link-protocol ppp
 ppp chap user huawei
 ppp chap password cipher %$%$e{5h)gh"/Uz0mUC%vEx3$4<m%$%$
 ip address 10.0.23.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
return

[R3]display current-configuration
[V200R007C00SPC600]
#
 sysname R3
```

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$fZsyUk1=O=>:L4'ytgR~D*Im%$%$
 local-user huawei service-type ppp
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap
 ip address 10.0.23.3 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.23.0 0.0.0.255
#
return
```

实验 2-2 配置 PPPoE 客户端

学习目标

- 掌握PPPoE客户端拨号接口的配置方法
- 掌握PPPoE客户端认证的配置方法

拓扑图

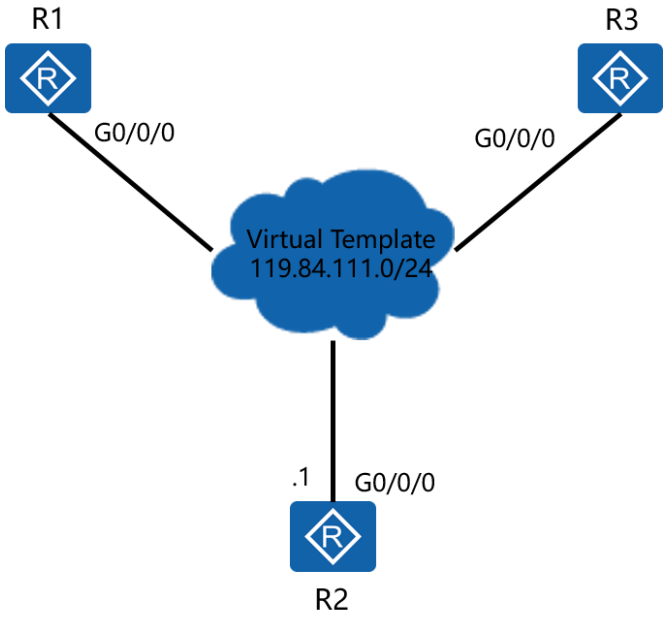

图2.2 配置PPPoE客户端实验拓扑图

场景

企业在运营商开通了高速DSL服务用于支持广域网业务。R1和R3分别是企业分支的边缘路由器，它们通过PPPoE服务器（R2）连接到运营商网络。您需要在企业的边缘路由器上进行PPPoE客户端的配置，让局域网中的主机可以通过PPPoE拨号访问外部资源。

操作步骤

步骤一　实验环境准备

如果本任务中您使用的是空配置设备，需要从步骤1开始配置，然后跳过步骤2。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

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

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2

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

步骤二　清除设备上原有的配置

关闭串行接口。

```
[R1]interface Serial 2/0/0
[R1-Serial2/0/0]shutdown

[R3]interface Serial 1/0/0
[R3-Serial1/0/0]shutdown
```

步骤三　配置 PPPoE 服务器

虽然PPPoE服务器不在企业网络中，但是本实验中仍需配置PPPoE服务器，以用于认证企业网络的边缘路由器R1和R3。

```
[R2]ip pool pool1
```

```
Info: It's successful to create an IP address pool.
[R2-ip-pool-pool1]network 119.84.111.0 mask 255.255.255.0
[R2-ip-pool-pool1]gateway-list 119.84.111.254
[R2-ip-pool-pool1]quit
[R2]interface Virtual-Template 1
[R2-Virtual-Template1]ppp authentication-mode chap
[R2-Virtual-Template1]ip address 119.84.111.254 255.255.255.0
[R2-Virtual-Template1]remote address pool pool1
[R2-Virtual-Template1]quit
```

在R2的G0/0/0接口绑定虚拟模板。

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]pppoe-server bind virtual-template 1
[R2-GigabitEthernet0/0/0]quit
```

为PPPoE被认证方创建合法的账号和密码。

```
[R2]aaa
[R2-aaa]local-user huawei1 password cipher huawei123
Info: Add a new user.
[R2-aaa]local-user huawei1 service-type ppp
[R2-aaa]local-user huawei2 password cipher huawei123
Info: Add a new user.
[R2-aaa]local-user huawei2 service-type ppp
[R2-aaa]quit
```

步骤四　配置 PPPoE 客户端

将R1配置为PPPoE客户端。需要在R1上创建拨号接口并开启PPP认证功能。配置PPP被认证方的用户名和密码（必须跟PPPoE服务器上的一致）。

```
[R1]dialer-rule
[R1-dialer-rule]dialer-rule 1 ip permit
```

```
[R1-dialer-rule]quit
[R1]interface Dialer 1
[R1-Dialer1]dialer user user1
[R1-Dialer1]dialer-group 1
[R1-Dialer1]dialer bundle 1
[R1-Dialer1]ppp chap user huawei1
[R1-Dialer1]ppp chap password cipher huawei123
[R1-Dialer1]dialer timer idle 300
[R1-Dialer1]dialer queue-length 8
[R1-Dialer1]ip address ppp-negotiate
[R1-Dialer1]quit
```

将PPPoE拨号接口绑定到出接口。

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]pppoe-client dial-bundle-number 1
[R1-GigabitEthernet0/0/0]quit
```

配置本端到PPPoE服务器的缺省静态路由。

```
[R1]ip route-static 0.0.0.0 0.0.0.0 Dialer 1
```

将R3配置为PPPoE客户端。配置步骤与R1一样。

```
[R3]dialer-rule
[R3-dialer-rule]dialer-rule 1 ip permit
[R3-dialer-rule]quit
[R3]interface Dialer 1
[R3-Dialer1]dialer user user2
[R3-Dialer1]dialer-group 1
[R3-Dialer1]dialer bundle 1
[R3-Dialer1]ppp chap user huawei2
```

```
[R3-Dialer1]ppp chap password cipher huawei123
[R3-Dialer1]dialer timer idle 300
[R3-Dialer1]dialer queue-length 8
[R3-Dialer1]ip address ppp-negotiate
[R3-Dialer1]quit

[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]pppoe-client dial-bundle-number 1
[R3-GigabitEthernet0/0/0]quit

[R3]ip route-static 0.0.0.0 0.0.0.0 Dialer 1
```

步骤五　验证配置结果

执行**display pppoe-server session all**命令，查看PPPoE会话的状态和配置信息。

```
<R2>display pppoe-server session all
```

SID	Intf	State	OIntf	RemMAC	LocMAC
1	Virtual-Template1:0	UP	GE0/0/0	00e0.fc03.d0ae	00e0.fc03.7516
2	Virtual-Template1:1	UP	GE0/0/0	00e0.fc03.aedd	00e0.fc03.7516

从回显信息可以看出，会话状态正常。

查看R1和R3上的拨号接口的信息，并确认拨号接口能够从PPPoE服务器获取IP地址。

```
<R1>display ip interface brief
  *down: administratively down
  ^down: standby
  (l): loopback
  (s): spoofing
  The number of interface that is UP in Physical is 7
  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 6

Interface	IP Address/Mask	Physical	Protocol
Cellular0/0/0	unassigned	down	down
Cellular0/0/1	unassigned	down	down
Dialer1	119.84.111.253/32	up	up(s)
GigabitEthernet0/0/0	unassigned	up	down

...output omit...

<R3>display ip interface brief

...output omit...

Interface	IP Address/Mask	Physical	Protocol
Cellular0/0/0	unassigned	down	down
Cellular0/0/1	unassigned	down	down
Dialer1	119.84.111.252/32	up	up(s)
GigabitEthernet0/0/0	unassigned	up	down

...output omit...

配置文件

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
```

```
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$B:%I)Io0H8)[%SB[idM3C/!#%$%$
 local-user huawei service-type ppp
#
interface Dialer1
 link-protocol ppp
 ppp chap user huawei1
 ppp chap password cipher %$%$A8E~UjX}@;bhCL*C4w#<%"Ba%$%$
 ip address ppp-negotiate
 dialer user user1
 dialer bundle 1
 dialer queue-length 8
 dialer timer idle 300
 dialer-group 1
#
interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1
#
dialer-rule
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 0.0.0.0 Dialer1
#
return

[R2]display current-configuration
[V200R007C00SPC600]
#
```

```
 sysname R2
#
ip pool pool1
 gateway-list 119.84.111.254
 network 119.84.111.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei1 password cipher %$%$MjCY6,a82N4W`]F]3LMAKG9+%$%$
 local-user huawei1 service-type ppp
 local-user huawei2 password cipher %$%$Ctq55RX:]R,8Jc13{|,)KH!m%$%$
 local-user huawei2 service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool pool1
 ip address 119.84.111.254 255.255.255.0
#
interface GigabitEthernet0/0/0
 pppoe-server bind Virtual-Template 1
#
return

[R3]display current-configuration
```

```
[V200R007C00SPC600]
#
 sysname R3
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$fZsyUk1=O=>:L4'ytgR~D*Im%$%$
 local-user huawei service-type ppp
#
interface Dialer1
 link-protocol ppp
 ppp chap user huawei2
 ppp chap password cipher %$%$0f8(;^]1NS:q;SPo8TyP%.Ei%$%$
 ip address ppp-negotiate
 dialer user user2
 dialer bundle 1
 dialer queue-length 8
 dialer timer idle 300
 dialer-group 1
#
interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1
#
dialer-rule
```

```
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 0.0.0.0 Dialer1
#
return
```

第三章 IP安全配置

实验 3-1 配置 ACL 过滤企业数据

学习目标

- 掌握高级ACL的配置方法
- 掌握ACL在接口下的应用方法

拓扑图

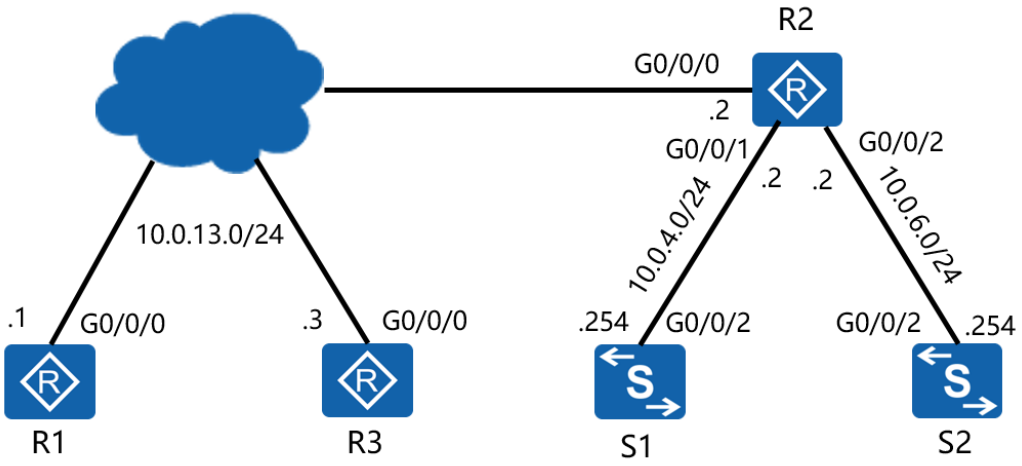

图3.1 配置ACL过滤企业数据实验拓扑图

场景

企业部署了三个网络，其中R2连接的是公司总部网络，R1和R3分别为两个不同分支网络的设备，这三台路由器通过广域网相连。你需要控制员工使用Telnet和FTP服务的权限，R1所在分支的员工只允许访问公司总部网络中的Telnet服务器，R3所在分支的员工只允许访问FTP服务器。

操作步骤

步骤一　实验环境准备

如果本任务中您使用的是空配置设备，需要从步骤1开始配置，然后跳过步骤2。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

```
[Huawei]sysname R1


[Huawei]sysname R2


[Huawei]sysname R3


[Huawei]sysname S1
[S1]vlan 4
[S1-vlan4]quit
[S1]interface vlanif 4
[S1-Vlanif4]ip address 10.0.4.254 24


[Huawei]sysname S2
[S2]vlan 6
[S2-vlan6]quit
[S2]interface vlanif 6
[S2-Vlanif6]ip address 10.0.6.254 24
```

步骤二　清除设备上原有的配置

删除设备上的OSPF配置、PPPoE拨号接口以及R2上的PPPoE服务器虚拟模板的配置。

```
[R1]ospf
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]undo network 10.0.0.0 0.255.255.255
[R1-ospf-1-area-0.0.0.0]quit
```

```
[R1-ospf-1]quit
[R1]undo ip route-static 0.0.0.0 0
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]undo pppoe-client dial-bundle-number 1
[R1]interface Dialer 1
[R1-Dialer1]undo dialer user
[R1]undo interface Dialer 1
[R1]dialer-rule
[R1-dialer-rule]undo dialer-rule 1

[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]undo network 10.0.0.0 0.255.255.255
[R2-ospf-1-area-0.0.0.0]quit
[R2-ospf-1]quit
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]undo pppoe-server bind
 Warning:All PPPoE sessions on this interface will be deleted, continue?[Y/N]:y
[R2-GigabitEthernet0/0/0]quit
[R2]undo interface Virtual-Template 1
[R2]undo ip pool pool1
[R2]aaa
[R2-aaa]undo local-user huawei1
[R2-aaa]undo local-user huawei2

[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]undo network 10.0.0.0 0.255.255.255
[R3-ospf-1-area-0.0.0.0]quit
[R3-ospf-1]quit
```

[R3]undo ip route-static 0.0.0.0 0

[R3]interface GigabitEthernet 0/0/0

[R3-GigabitEthernet0/0/0]undo pppoe-client dial-bundle-number 1

[R3-GigabitEthernet0/0/0]quit

[R3]interface Dialer 1

[R3-Dialer1]undo dialer user

[R3-Dialer1]quit

[R3]undo interface Dialer 1

[R3]dialer-rule

[R3-dialer-rule]undo dialer-rule 1

步骤三　配置 IP 地址

按照拓扑图中所示网络的地址进行IP编址的配置。

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]ip address 10.0.13.1 24

[R2]interface GigabitEthernet 0/0/0

[R2-GigabitEthernet0/0/0]ip address 10.0.13.2 24

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

[R2-GigabitEthernet0/0/1]ip address 10.0.4.2 24

[R2-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2

[R2-GigabitEthernet0/0/2]ip address 10.0.6.2 24

[R3]interface GigabitEthernet 0/0/0

[R3-GigabitEthernet0/0/0]ip address 10.0.13.3 24

配置S1和S2连接路由器的端口为Trunk端口，并通过修改PVID使物理端口加入三层VLANIF逻辑接口。

[S1]interface GigabitEthernet 0/0/2

[S1-GigabitEthernet0/0/2]port link-type trunk

[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan all

[S1-GigabitEthernet0/0/2]port trunk pvid vlan 4

[S1-GigabitEthernet0/0/2]quit

[S2]interface GigabitEthernet 0/0/2

[S2-GigabitEthernet0/0/2]port link-type trunk

[S2-GigabitEthernet0/0/2]port trunk allow-pass vlan all

[S2-GigabitEthernet0/0/2]port trunk pvid vlan 6

[S2-GigabitEthernet0/0/2]quit

步骤四　配置 OSPF 使网络互通

在R1、R2和R3上配置OSPF，三台设备均在区域0中，并发布各自的直连网段信息。

[R1]ospf

[R1-ospf-1]area 0

[R1-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255

[R2]ospf

[R2-ospf-1]area 0

[R2-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255

[R2-ospf-1-area-0.0.0.0]network 10.0.4.0 0.0.0.255

[R2-ospf-1-area-0.0.0.0]network 10.0.6.0 0.0.0.255

[R3]ospf

[R3-ospf-1]area 0

[R3-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255

在S1和S2上配置缺省静态路由，指定下一跳为各自连接的路由器网关。

[S1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.2

[S2]ip route-static 0.0.0.0 0.0.0.0 10.0.6.2

检测网络的连通性。

```
<R1>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=253 time=2 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=253 time=10 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=253 time=1 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=253 time=2 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=253 time=2 ms
  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
     round-trip min/avg/max = 1/3/10 ms

<R1>ping 10.0.6.254
  PING 10.0.6.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.6.254: bytes=56 Sequence=1 ttl=253 time=10 ms
    Reply from 10.0.6.254: bytes=56 Sequence=2 ttl=253 time=2 ms
    Reply from 10.0.6.254: bytes=56 Sequence=3 ttl=253 time=2 ms
    Reply from 10.0.6.254: bytes=56 Sequence=4 ttl=253 time=10 ms
    Reply from 10.0.6.254: bytes=56 Sequence=5 ttl=253 time=2 ms
  --- 10.0.6.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/5/10 ms

<R3>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
```

```
  Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=253 time=10 ms
  Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=253 time=2 ms
  Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=253 time=2 ms
  Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=253 time=10 ms
  Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=253 time=2 ms
--- 10.0.4.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
   round-trip min/avg/max = 2/5/10 ms

<R3>ping 10.0.6.254
  PING 10.0.6.254: 56  data bytes, press CTRL_C to break
  Reply from 10.0.6.254: bytes=56 Sequence=1 ttl=253 time=10 ms
  Reply from 10.0.6.254: bytes=56 Sequence=2 ttl=253 time=2 ms
  Reply from 10.0.6.254: bytes=56 Sequence=3 ttl=253 time=2 ms
  Reply from 10.0.6.254: bytes=56 Sequence=4 ttl=253 time=10 ms
  Reply from 10.0.6.254: bytes=56 Sequence=5 ttl=253 time=2 ms
--- 10.0.6.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/5/10 ms
```

步骤五　配置 ACL 过滤报文

将S1配置为Telnet服务器。

```
[S1]telnet server enable
[S1]user-interface vty 0 4
[S1-ui-vty0-4]protocol inbound all
[S1-ui-vty0-4]authentication-mode password
```

[S1-ui-vty0-4]set authentication password cipher huawei123

将S2配置为FTP服务器。

[S2]ftp server enable

[S2]aaa

[S2-aaa]local-user huawei password cipher huawei123

[S2-aaa]local-user huawei privilege level 3

[S2-aaa]local-user huawei service-type ftp

[S2-aaa]local-user huawei ftp-directory flash:/

在R2上配置ACL，只允许R1访问Telnet服务器，只允许R3访问FTP服务器。

[R2]acl 3000

[R2-acl-adv-3000]rule 5 permit tcp source 10.0.13.1 0.0.0.0 destination 10.0.4.254 0.0.0.0 destination-port eq 23

[R2-acl-adv-3000]rule 10 permit tcp source 10.0.13.3 0.0.0.0 destination 10.0.6.254 0.0.0.0 destination-port range 20 21

[R2-acl-adv-3000]rule 15 permit ospf

[R2-acl-adv-3000]rule 20 deny ip source any

[R2-acl-adv-3000]quit

在R2的G0/0/0接口应用ACL。

[R2]interface GigabitEthernet0/0/0

[R2-GigabitEthernet0/0/0]traffic-filter inbound acl 3000

验证ACL的应用结果。

<R1>telnet 10.0.4.254

Press CTRL_] to quit telnet mode

Trying 10.0.4.254 ...

Connected to 10.0.4.254 ...

Login authentication

Password:

Info: The max number of VTY users is 5, and the number

of current VTY users on line is 1.

<S1>

注意：执行**quit**命令，可以结束Telnet会话。

<R1>ftp 10.0.6.254

Trying 10.0.6.254 ...

Press CTRL+K to abort

Error: Failed to connect to the remote host.

注意：FTP连接的响应时间约为60秒。

<R3>telnet 10.0.4.254

Press CTRL_] to quit telnet mode

Trying 10.0.4.254 ...

Error: Can't connect to the remote host

<R3>ftp 10.0.6.254

Trying 10.0.6.254 ...

Press CTRL+K to abort

Connected to 10.0.6.254.

220 FTP service ready.

User(10.0.6.254:(none)):huawei

331 Password required for huawei.

Enter password:

230 User logged in.

[R3-ftp]

注意：可以执行**bye**命令，关闭FTP连接。

附加练习：分析并验证

为什么FTP要求ACL定义两个端口？

应在源端网络还是目标网络配置基本和高级ACL，为什么？

配置文件

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$B:%I)Io0H8)[%SB[idM3C/!#%$%$
 local-user huawei service-type ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.1 255.255.255.0
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.13.0 0.0.0.255
#
return
```

```
<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
acl number 3000
 rule 5 permit tcp source 10.0.13.1 0 destination 10.0.4.254 0 destination-port eq telnet
 rule 10 permit tcp source 10.0.13.3 0 destination 10.0.6.254 0 destination-port range ftp-data ftp
 rule 15 permit ospf
 rule 20 deny ip
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.2 255.255.255.0
 traffic-filter inbound acl 3000
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.0.6.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.4.0 0.0.0.255
  network 10.0.6.0 0.0.0.255
  network 10.0.13.0 0.0.0.255
#
return
```

```
<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.3 255.255.255.0
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.13.0 0.0.0.255
#
return

<S1>display current-configuration
!Software Version V200R008C00SPC500
#
sysname S1
#
vlan batch 3 to 4
#
telnet server enable
#
interface Vlanif4
 ip address 10.0.4.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 4
 port trunk allow-pass vlan 2 to 4094
```

```
#
ip route-static 0.0.0.0 0.0.0.0 10.0.4.2
#
user-interface con 0
user-interface vty 0 4
authentication-mode password
set authentication password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
Protocol inbound all
#
return

<S2>display current-configuration
!Software Version V200R008C00SPC500
#
sysname S2
#
FTP server enable
#
 vlan batch 6
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
 local-user huawei password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
 Local-user huawei privilege level 3
```

```
 local-user huawei ftp-directory flash:/
 local-user huawei service-type ftp
#
interface Vlanif6
 ip address 10.0.6.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 6
 port trunk allow-pass vlan 2 to 4094
#
ip route-static 0.0.0.0 0.0.0.0 10.0.6.2
#
return
```

实验 3-2 NAT 配置

学习目标

- 掌握动态NAT的配置方法
- 掌握Easy IP的配置方法

拓扑图

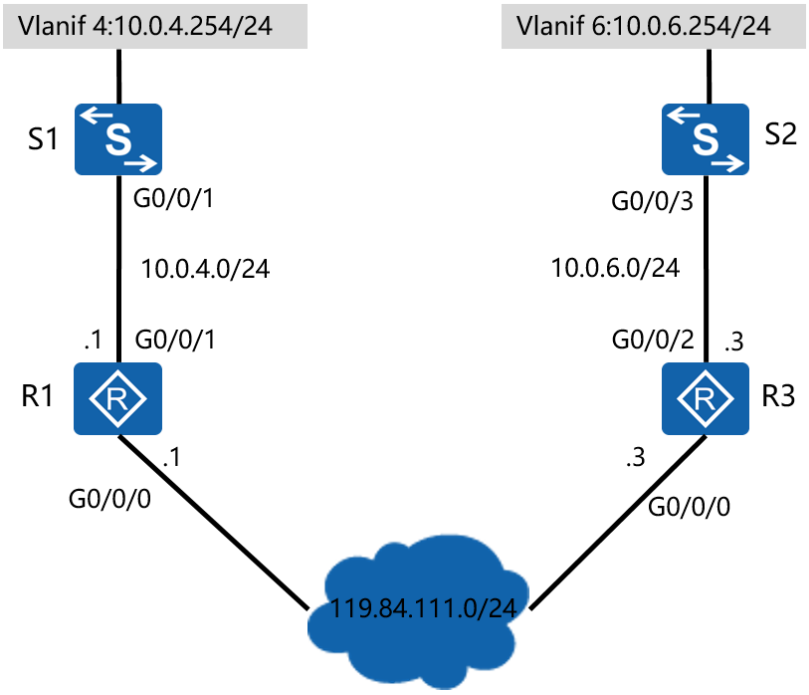

图3.2 NAT的配置实验拓扑图

场景

为了节省IP地址，通常企业内部使用的是私有地址。然而，企业用户不仅需要访问私网，也需要访问公网。作为企业的网络管理员，您需要在两个企业分支机构的边缘路由器R1和R3上通过配置NAT功能，使私网用户可以访问公网。本实验中，您需要在R1上配置动态NAT、在R3上配置Easy IP，实现地址转换。

操作步骤

步骤一　实验环境准备

如果本任务中您使用的是空配置设备，需要从步骤1开始配置，然后跳过步骤2。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

[Huawei]sysname R1

[R1]inter GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]ip address 10.0.4.1 24

[Huawei]sysname R3

[R3]interface GigabitEthernet0/0/2

[R3-GigabitEthernet0/0/2]ip address 10.0.6.3 24

[Huawei]sysname S1

[S1]vlan 4

[S1-vlan3]quit

[S1]interface vlanif 4

[S1-Vlanif4]ip address 10.0.4.254 24

[S1-Vlanif4]quit

[Huawei]sysname S2

[S2]vlan 6

[S2-vlan6]quit

[S2]interface vlanif 6

[S2-Vlanif6]ip address 10.0.6.254 24

[S2-Vlanif6]quit

步骤二　清除设备上原有的配置

将R1的G0/0/1接口重新连接到S1，R3的G0/0/2接口重新连接到S2，然后删除所有路由器的OSPF配置。

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]undo ip address

[R1]interface GigabitEthernet 0/0/1

[R1-GigabitEthernet0/0/1]undo shutdown

[R1]undo ospf 1

Warning: The OSPF process will be deleted. Continue? [Y/N]:y

[R2]undo ospf 1

Warning: The OSPF process will be deleted. Continue? [Y/N]:y

[R3-GigabitEthernet0/0/0]undo ip address

[R3]interface GigabitEthernet 0/0/2

[R3-GigabitEthernet0/0/2]undo shutdown

[R3]undo ospf 1

Warning: The OSPF process will be deleted. Continue? [Y/N]:y

删除S1和S2上指向R2的缺省静态路由。

[S1]undo ip route-static 0.0.0.0 0.0.0.0

[S2]undo ip route-static 0.0.0.0 0.0.0.0

步骤三　配置 IP 地址

在S1和S2上将连接路由器的端口配置为Trunk端口，并通过修改PVID使物理端口加入VLANIF三层逻辑口。

[S1]interface GigabitEthernet 0/0/1

[S1-GigabitEthernet0/0/1]port link-type trunk

[S1-GigabitEthernet0/0/1]port trunk pvid vlan 4

[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan all

[S1-GigabitEthernet0/0/1]quit

[S2]interface GigabitEthernet 0/0/3

[S2-GigabitEthernet0/0/3]port link-type trunk

[S2-GigabitEthernet0/0/3]port trunk pvid vlan 6

[S2-GigabitEthernet0/0/3]port trunk allow-pass vlan all

[R1]interface GigabitEthernet0/0/0

[R1-GigabitEthernet0/0/0]ip address 119.84.111.1 24

[R3]interface GigabitEthernet0/0/0

```
[R3-GigabitEthernet0/0/0]ip address 119.84.111.3 24
```

测试R1与S1和R3的连通性。

```
<R1>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=255 time=23 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=254 time=10 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
     round-trip min/avg/max = 1/7/23 ms

<R1>ping 119.84.111.3
  PING 119.84.111.3: 56  data bytes, press CTRL_C to break
    Reply from 119.84.111.3: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=255 time=10 ms
  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
     round-trip min/avg/max = 1/4/10 ms
```

步骤四　配置 ACL

在R1上配置高级ACL，匹配特定的流量进行NAT地址转换，特定流量为S1

向R3发起的Telnet连接的TCP流量，以及源IP为10.0.4.0/24网段的IP数据流。

[R1]acl 3000

[R1-acl-adv-3000]rule 5 permit tcp source 10.0.4.254 0.0.0.0 destination 119.84.111.3 0.0.0.0 destination-port eq 23

[R1-acl-adv-3000]rule 10 permit ip source 10.0.4.0 0.0.0.255 destination any

[R1-acl-adv-3000]rule 15 deny ip

在R3上配置基本ACL，匹配需要进行NAT地址转换的流量为源IP为10.0.6.0/24网段的数据流。

[R3]acl 2000

[R3-acl-basic-2000]rule permit source 10.0.6.0 0.0.0.255

步骤五　配置动态 NAT

在S1和S2上配置缺省静态路由，指定下一跳为私网的网关。

[S1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.1

[S2]ip route-static 0.0.0.0 0.0.0.0 10.0.6.3

在R1上配置动态NAT，首先配置地址池，然后在G0/0/0接口下将ACL与地址池关联起来，使得匹配ACL 3000的数据报文的源地址选用地址池中的某个地址进行NAT转换。

[R1]nat address-group 1 119.84.111.240 119.84.111.243

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]nat outbound 3000 address-group 1

将R3配置为Telnet服务器。

[R3]telnet server enable

[R3]user-interface vty 0 4

[R3-ui-vty0-4]authentication-mode password

[R3-ui-vty0-4]set authentication password cipher

Warning: The “password” authentication mode is not secure,and it is strongly recommended to use ” aaa” authentication mode.

```
Enter Password(<8-128>):huawei123
Confirm password:huawei123
[R3-ui-vty0-4]quit
```

配置完成后，查看地址池配置是否正确。

```
<R1>display nat address-group
 NAT Address-Group Information:
 --------------------------------------
 Index    Start-address          End-address
 --------------------------------------
 1        119.84.111.240     119.84.111.243
 --------------------------------------
       Total : 1
```

在S1上测试内网到外网的连通性。

```
<S1>ping 119.84.111.3
  PING 119.84.111.3: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

在S1上发起到达远端公网设备的Telnet连接。

```
<S1>telnet 119.84.111.3
```

Trying 119.84.111.3 ...

Press CTRL+K to abort

Connected to 119.84.111.3 ...

Login authentication

Password:

<R3>

Telnet成功后，不要结束该Telnet会话。此时，在R1上查看ACL和NAT会话的详细信息。

<R1>display acl 3000

Advanced ACL 3000, 3 rules

Acl's step is 5

rule 5 permit tcp source 10.0.4.254 0 destination 119.84.111.3 0 destination-port eq telnet (1 matches)

rule 10 permit ip source 10.0.4.0 0.0.0.255 (1 matches)

rule 15 deny ip

<R1>display nat session all

NAT Session Table Information:

Protocol : ICMP(1)

SrcAddr Vpn : 10.0.4.254

DestAddr Vpn : 119.84.111.3

Type Code IcmpId : 8 0 44003

NAT-Info

New SrcAddr : 119.84.111.242

New DestAddr : ----

New IcmpId : 10247

Protocol : TCP(6)

SrcAddr Port Vpn : 10.0.4.254 49646

DestAddr Port Vpn : 119.84.111.3 23

```
    NAT-Info
      New SrcAddr        : 119.84.111.242
      New SrcPort        : 10249
      New DestAddr       : ----
      New DestPort       : ----
  Total : 2
```

由于ICMP会话的生存周期只有20秒，所以如果NAT会话的显示结果中没有ICMP会话的信息，可以执行以下的命令延长ICMP会话的生存周期，然后再执行**Ping**命令后可查看到ICMP会话的信息。

```
[R1]firewall-nat session icmp aging-time 300
```

在R3的G0/0/0接口配置Easy IP，并关联ACL 2000。

```
[R3-GigabitEthernet0/0/0]nat outbound 2000
```

测试S2能否经过R3连通R1，并查看配置的NAT Outbound的信息。

```
<S2>ping 119.84.111.1
  PING 119.84.111.1: 56  data bytes, press CTRL_C to break
    Reply from 119.84.111.1: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 119.84.111.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 119.84.111.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 119.84.111.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 119.84.111.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 119.84.111.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
     round-trip min/avg/max = 1/1/1 ms

<R3>display acl 2000
```

```
Basic ACL 2000, 1 rule
Acl's step is 5
 rule 5 permit source 10.0.6.0 0.0.0.255 (1 matches)

<R3>display nat outbound acl 2000
 NAT Outbound Information: ----------------------------------------------------------------------
Interface                       Acl         Address-group/IP/Interface          Type
----------------------------------------------------------------------
GigabitEthernet0/0/0     2000                                119.84.111.3       easyip
----------------------------------------------------------------------
  Total : 1
```

配置文件

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
firewall-nat session icmp aging-time 300
#
acl number 3000
 rule 5 permit tcp source 10.0.4.254 0 destination 119.84.111.3 0 destination-port eq telnet
 rule 10 permit ip source 10.0.4.0 0.0.0.255
 rule 15 deny ip
#
 nat address-group 1 119.84.111.240 119.84.111.243
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.1 255.255.255.0
 nat outbound 3000 address-group 1
```

```
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.1 255.255.255.0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
#
return


<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
telnet server enable
#
acl number 2000
 rule 5 permit source 10.0.6.0 0.0.0.255
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.3 255.255.255.0
 nat outbound 2000
#
interface GigabitEthernet0/0/2
 ip address 10.0.6.3 255.255.255.0
#
user-interface con 0
```

```
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
user-interface vty 0 4
 authentication-mode password
 set authentication password cipher %$%$7ml|,!ccE$SQ~CZ{GtaE%hO>v}~bVk18p5qq<:UPtI:9hOA%%$%$
#
return


<S1>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
#
 vlan batch 4
#
interface Vlanif4
 ip address 10.0.4.254 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 4
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 4
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/14
```

```
 shutdown
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.4.1
#
user-interface con 0
user-interface vty 0 4
 set authentication password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
#
return


<S2>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S2
#
 vlan batch 6
#
interface Vlanif6
 ip address 10.0.6.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 6
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk pvid vlan 6
 port trunk allow-pass vlan 2 to 4094
#
```

```
interface GigabitEthernet0/0/23
 shutdown
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.6.3
#
user-interface con 0
user-interface vty 0 4
#
return
```

实验 3-3 本地 AAA 配置

学习目标

- 掌握本地AAA认证授权方案的配置方法
- 掌握创建域的方法
- 掌握认证用户优先级的配置方法

拓扑图

图3.3 本地AAA配置实验拓扑图

场景

您是企业的网络管理员，需要对企业服务器的资源访问进行控制，只有通过认证的用户才能访问特定的资源，因此您需要在R1和R3两台路由器上配置本地AAA认证，并基于域来对用户进行管理，并配置已认证用户的权限级别。

操作步骤

步骤一 实验环境准备

如果本任务中您使用的是空配置设备，需要从步骤1开始配置，然后跳过步骤2。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

```
[Huawei]sysname R1

[R1]interface GigabitEthernet0/0/0

[R1-GigabitEthernet0/0/0]ip address 119.84.111.1 24
```

[Huawei]sysname R3

[R3]inter GigabitEthernet0/0/0

[R3-GigabitEthernet0/0/0]ip address 119.84.111.3 24

步骤二　清除设备上原有的配置

删除R1和R3上原有NAT和ACL配置。

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]undo nat outbound 3000 address-group 1

[R1-GigabitEthernet0/0/0]quit

[R1]undo nat address-group 1

[R1]undo acl 3000

[R3]interface GigabitEthernet 0/0/0

[R3-GigabitEthernet0/0/0]undo nat outbound 2000

[R3-GigabitEthernet0/0/0]quit

[R3]undo acl 2000

步骤三　检测 R1 和 R3 间的连通性

<R1>ping 119.84.111.3

PING 119.84.111.3: 56 data bytes, press CTRL_C to break

Reply from 119.84.111.3: bytes=56 Sequence=1 ttl=255 time=70 ms

Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=255 time=20 ms

Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=255 time=10 ms

Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=255 time=20 ms

Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=255 time=10 ms

--- 119.84.111.3 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 10/26/70 ms

步骤四　在 R1 上配置 AAA 功能

在R1上配置认证方案为本地认证，授权方案为本地授权。

```
[R1]aaa
[R1-aaa]authentication-scheme auth1
Info: Create a new authentication scheme.
[R1-aaa-authen-auth1]authentication-mode local
[R1-aaa-authen-auth1]quit
[R1-aaa]authorization-scheme auth2
Info: Create a new authorization scheme.
[R1-aaa-author-auth2]authorization-mode local
[R1-aaa-author-auth2]quit
```

在R1上创建域“huawei“并将认证方案和授权方案与域关联起来，然后创建一个用户并将用户加入到域huawei。

```
[R1]telnet server enable
[R1]aaa
[R1-aaa]domain huawei
[R1-aaa-domain-huawei]authentication-scheme auth1
[R1-aaa-domain-huawei]authorization-scheme auth2
[R1-aaa-domain-huawei]quit
[R1-aaa]local-user user1@huawei password cipher huawei123
[R1-aaa]local-user user1@huawei service-type telnet
[R1-aaa]local-user user1@huawei privilege level 0
```

将R1配置为Telnet服务器，认证模式配置为AAA。

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
```

验证Telnet R1时是否要经过AAA认证。

```
<R3>telnet 119.84.111.1
  Press CTRL_] to quit telnet mode
  Trying 119.84.111.1 ...
  Connected to 119.84.111.1 ...

Login authentication

Username:user1@huawei
Password:
<R1>system-view
      ^
Error: Unrecognized command found at '^' position.
<R1>quit
```

可以看到用户user1@huawei Telnet R1后不能使用命令**system-view**进入系统试图，原因是用户操作权限配置的是级别0，因此操作受限。

步骤五　在 R3 上配置 AAA 功能

在R3上配置认证方案为本地认证，授权方案为本地授权。

```
[R3]aaa
[R3-aaa]authentication-scheme auth1
Info: Create a new authentication scheme.
[R3-aaa-authen-auth1]authentication-mode local
[R3-aaa-authen-auth1]quit
[R3-aaa]authorization-scheme auth2
Info: Create a new authorization scheme.
[R3-aaa-author-auth2]authorization-mode local
[R3-aaa-author-auth2]quit
```

在R3上创建域“huawei“并将认证方案和授权方案与域关联起来，然后创

建一个用户并将用户加入到域huawei。

```
[R3]telnet server enable
[R3]aaa
[R3-aaa]domain huawei
[R3-aaa-domain-huawei]authentication-scheme auth1
[R3-aaa-domain-huawei]authorization-scheme auth2
[R3-aaa-domain-huawei]quit
[R3-aaa]local-user user3@huawei password cipher huawei123
[R3-aaa]local-user user3@huawei service-type telnet
[R3-aaa]local-user user3@huawei privilege level 0
```

在R3上配置为Telnet服务，并将认证模式配置为AAA。

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode aaa
```

验证Telnet R1时是否要经过AAA认证。

```
.<R1>telnet 119.84.111.3
  Press CTRL_] to quit telnet mode
  Trying 119.84.111.1 ...
  Connected to 119.84.111.1 ...
Login authentication
Username:user3@huawei
Password:
<R3>system-view
      ^
Error: Unrecognized command found at '^' position.
<R3>
```

可以看到用户user3@huawei同样是因为登录后操作权限配置的是级别0，因此操作受限。

步骤六　验证 AAA 的配置结果

```
<R1>display domain name huawei
  Domain-name                          : huawei
  Domain-state                         : Active
  Authentication-scheme-name   : auth1
  Accounting-scheme-name       : default
  Authorization-scheme-name            : auth2
  Service-scheme-name          : -
  RADIUS-server-template       : -
  HWTACACS-server-template             : -
  User-group                   : -

<R1>display local-user username user1@huawei
  The contents of local user(s):
  Password                     : ****************
  State                        : active
  Service-type-mask            : T
  Privilege level              : 0
  Ftp-directory                : -
  Access-limit                 : -
  Accessed-num                 : 0
  Idle-timeout                 : -
  User-group                   : -

<R3>display domain name huawei
  Domain-name                          : huawei
  Domain-state                         : Active
  Authentication-scheme-name   : auth1
  Accounting-scheme-name       : default
```

```
  Authorization-scheme-name           : auth2
  Service-scheme-name          : -
  RADIUS-server-template       : -
  HWTACACS-server-template          : -
  User-group                   : -

<R3>display local-user username user3@huawei
  The contents of local user(s):
  Password                     : ****************
  State                        : active
  Service-type-mask            : T
  Privilege level              : 0
  Ftp-directory                : -
  Access-limit            : -
  Accessed-num                 : 0
  Idle-timeout            : -
  User-group              : -
```

配置文件

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
telnet server enable
#
aaa
 authentication-scheme default
 authentication-scheme auth1
 authorization-scheme default
```

```
 authorization-scheme auth2
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme auth1
  authorization-scheme auth2
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$B:%I)Io0H8)[%SB[idM3C/!#%$%$
 local-user huawei service-type ppp
 local-user user1@huawei password cipher %$%$^L*5IP'0^A!;R)R*L=LFcXgv%$%$
 local-user user1@huawei privilege level 0
 local-user user1@huawei service-type telnet
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.1 255.255.255.0
 nat outbound 3000 address-group 1   //may remain from previous labs
#
user-interface con 0
 authentication-mode password
 set authentication password
cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return


<R3>display current-configuration
[V200R007C00SPC600]
```

```
#
 sysname R3
#
telnet server enable
#
aaa
 authentication-scheme default
 authentication-scheme auth1
 authorization-scheme default
 authorization-scheme auth2
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme auth1
  authorization-scheme auth2
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$fZsyUk1=O=>:L4'ytgR~D*Im%$%$
 local-user huawei service-type ppp
 local-user user3@huawei password cipher %$%$WQt.;bEsR<8fz3LCiPY,che_%$%$
 local-user user3@huawei privilege level 0
 local-user user3@huawei service-type telnet
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.3 255.255.255.0
 nat outbound 2000      //may remain from previous labs
#
user-interface con 0
 authentication-mode password
```

```
 set authentication password
cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$

user-interface vty 0 4

 authentication-mode aaa

#

return
```

实验 3-4 IPSec VPN 配置

学习目标

- 掌握IPSec提议的配置方法
- 掌握使用ACL定义感兴趣流的方法
- 掌握IPSec策略的配置方法
- 掌握在接口绑定IPSec策略的方法

拓扑图

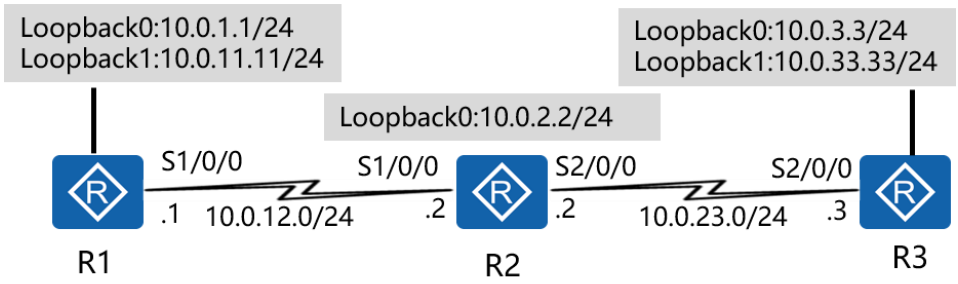

图3.4 IPSec VPN实验拓扑图

场景

企业的某些私有数据在公网传输时要确保完整性和机密性。作为企业的网络管理员，您需要在企业总部的边缘路由器（R1）和分支机构路由器（R3）之间部署IPSec VPN解决方案，建立IPSec隧道，用于安全传输来自指定部门的数据流。

操作步骤

步骤一　实验环境准备

如果本任务中您使用的是空配置设备，需要从步骤1开始配置，然后跳过步骤2。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

```
<Huawei>system-view
```

```
[Huawei]sysname R1
[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 10.0.1.1 24

<Huawei>system-view
[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 10.0.2.2 24

<Huawei>system-view
[Huawei]sysname R3
[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 10.0.3.3 24
```

步骤二　清除设备上原有的配置

删除R1和R3上G0/0/0接口的IP地址 ,并关闭无关接口。打开R2上相关接口。

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]undo ip address
```

[R1-GigabitEthernet0/0/0]quit

[R1]interface GigabitEthernet 0/0/1

[R1-GigabitEthernet0/0/1]shutdown

[R1-GigabitEthernet0/0/1]quit

[R1]interface Serial 1/0/0

[R1-Serial1/0/0]undo shutdown

[R2]interface Serial 1/0/0

[R2-Serial1/0/0]undo shutdown

[R2]interface Serial 2/0/0

[R2-Serial2/0/0]undo shutdown

[R3]interface GigabitEthernet 0/0/0

[R3-GigabitEthernet0/0/0]undo ip address

[R3]interface GigabitEthernet 0/0/2

[R3-GigabitEthernet0/0/2]shutdown

[R3]interface Serial 2/0/0

[R3-Serial2/0/0]undo shutdown

步骤三　创建逻辑接口

[R1-LoopBack0]interface loopback 1

[R1-LoopBack1]ip address 10.0.11.11 24

[R3-LoopBack0]interface loopback 1

[R3-LoopBack1]ip address 10.0.33.33 24

步骤四　配置 OSPF

在R1、R2和R3上配置OSPF，将Loopback 0的IP地址作为路由器的Router ID，使用OSPF的默认进程1，并将公网网段10.0.12.0/24和10.0.23.0/24以及环回接口地址通告在OSPF区域0。

```
[R1]ospf router-id 10.0.1.1
[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 10.0.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.11.0 0.0.0.255

[R2]ospf router-id  10.0.2.2
[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  10.0.23.0 0.0.0.255

[R3]ospf router-id  10.0.3.3
[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  10.0.3.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network  10.0.33.0 0.0.0.255
```

待OSPF收敛完成后，查看OSPF邻居以及路由表。

```
<R2>display ospf peer brief

        OSPF Process 1 with Router ID 10.0.2.2

                Peer Statistic Information

 ----------------------------------------------------------------------------

 Area Id          Interface                     Neighbor id      State

 0.0.0.0          Serial1/0/0                   10.0.1.1         Full

 0.0.0.0          Serial2/0/0                   10.0.3.3         Full

 ----------------------------------------------------------------------------


<R1>display ip routing-table

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

Routing Tables: Public

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.0/24	Direct	0	0	D	10.0.1.1	LoopBack0
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.255/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.2.2/32	OSPF	10	781	D	10.0.12.2	Serial1/0/0
10.0.3.3/32	OSPF	10	2343	D	10.0.12.2	Serial1/0/0
10.0.11.0/24	Direct	0	0	D	10.0.11.11	LoopBack1
10.0.11.11/32	Direct	0	0	D	127.0.0.1	LoopBack1
10.0.11.255/32	Direct	0	0	D	127.0.0.1	LoopBack1
10.0.12.0/24	Direct	0	0	D	10.0.12.1	Serial1/0/0
10.0.12.1/32	Direct	0	0	D	127.0.0.1	Serial1/0/0
10.0.12.2/32	Direct	0	0	D	10.0.12.2	Serial1/0/0
10.0.12.255/32	Direct	0	0	D	127.0.0.1	Serial1/0/0
10.0.23.0/24	OSPF	10	2343	D	10.0.12.2	Serial1/0/0
10.0.33.33/32	OSPF	10	2343	D	10.0.12.2	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
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

如果实验2-1中的配置未被清除，即路由器串口的时钟频率仍为128000 bit/s，则路由表中会显示OSPF开销值如下。

<R3>display ip routing-table

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

Routing Tables: Public

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	OSPF	10	3124	D	10.0.23.2	Serial2/0/0
10.0.2.2/32	OSPF	10	1562	D	10.0.23.2	Serial2/0/0
10.0.3.0/24	Direct	0	0	D	10.0.3.3	LoopBack0
10.0.3.3/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.3.255/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.11.11/32	OSPF	10	3124	D	10.0.23.2	Serial2/0/0
10.0.12.0/24	OSPF	10	3124	D	10.0.23.2	Serial2/0/0
10.0.23.0/24	Direct	0	0	D	10.0.23.3	Serial2/0/0
10.0.23.2/32	Direct	0	0	D	10.0.23.2	Serial2/0/0
10.0.23.3/32	Direct	0	0	D	127.0.0.1	Serial2/0/0
10.0.23.255/32	Direct	0	0	D	127.0.0.1	Serial2/0/0
10.0.33.0/24	Direct	0	0	D	10.0.33.33	LoopBack1
10.0.33.33/32	Direct	0	0	D	127.0.0.1	LoopBack1
10.0.33.255/32	Direct	0	0	D	127.0.0.1	LoopBack1
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

步骤五　配置 ACL 定义感兴趣流

配置高级ACL来定义IPSec VPN的感兴趣流。高级ACL能够基于特定的参数来匹配流量。

[R1]acl 3001

[R1-acl-adv-3001]rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255

[R3]acl 3001

[R3-acl-adv-3001]rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255

步骤六　配置 IPSec VPN 提议

创建IPSec提议，并进入IPSec提议视图来指定安全协议。注意确保隧道两端的设备使用相同的安全协议。

```
[R1]ipsec proposal tran1
[R1-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R1-ipsec-proposal-tran1]esp encryption-algorithm 3des

[R3]ipsec proposal tran1
[R3-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R3-ipsec-proposal-tran1]esp encryption-algorithm 3des
```

执行**display ipsec proposal**命令，验证配置结果。

```
[R1]display ipsec proposal
Number of proposals: 1
IPSec proposal name    :    tran1
 Encapsulation mode    :    Tunnel
 Transform             :    esp-new
 ESP protocol          :    Authentication SHA1-HMAC-96
                            Encryption       3DES

[R3]display ipsec proposal
Number of proposals: 1
IPSec proposal name    :    tran1
 Encapsulation mode    :    Tunnel
 Transform             :    esp-new
 ESP protocol          :    Authentication SHA1-HMAC-96
                            Encryption       3DES
```

步骤七　创建 IPSec 策略

手工创建IPSec策略 ,每一个IPSec安全策略都使用唯一的名称和序号来标识，IPSec策略中会应用IPSec提议中定义的安全协议、认证算法、加密算法和封装模式，手工创建的IPSec策略还需配置安全联盟（SA）中的参数。

```
[R1]ipsec policy P1 10 manual
[R1-ipsec-policy-manual-P1-10]security acl 3001
[R1-ipsec-policy-manual-P1-10]proposal tran1
[R1-ipsec-policy-manual-P1-10]tunnel remote 10.0.23.3
[R1-ipsec-policy-manual-P1-10]tunnel local 10.0.12.1
[R1-ipsec-policy-manual-P1-10]sa spi outbound esp 54321
[R1-ipsec-policy-manual-P1-10]sa spi inbound esp 12345
[R1-ipsec-policy-manual-P1-10]sa string-key outbound esp simple huawei
[R1-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei
```

```
[R3]ipsec policy P1 10 manual
[R3-ipsec-policy-manual-P1-10]security acl 3001
[R3-ipsec-policy-manual-P1-10]proposal tran1
[R3-ipsec-policy-manual-P1-10]tunnel remote 10.0.12.1
[R3-ipsec-policy-manual-P1-10]tunnel local 10.0.23.3
[R3-ipsec-policy-manual-P1-10]sa spi outbound esp 12345
[R3-ipsec-policy-manual-P1-10]sa spi inbound esp 54321
[R3-ipsec-policy-manual-P1-10]sa string-key outbound esp simple huawei
[R3-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei
```

执行**display ipsec policy**命令，验证配置结果。

```
<R1>display ipsec policy
==========================================
IPSec policy group: "P1"
Using interface:
==========================================
```

Sequence number: 10

Security data flow: 3001

Tunnel local address: 10.0.12.1

Tunnel remote address: 10.0.23.3

Qos pre-classify: Disable

Proposal name:tran1

Inbound AH setting:

AH SPI:

AH string-key:

AH authentication hex key:

Inbound ESP setting:

ESP SPI: 12345 (0x3039)

ESP string-key: huawei

ESP encryption hex key:

ESP authentication hex key:

Outbound AH setting:

AH SPI:

AH string-key:

AH authentication hex key:

Outbound ESP setting:

ESP SPI: 54321 (0xd431)

ESP string-key: huawei

ESP encryption hex key:

ESP authentication hex key:

<R3>display ipsec policy

==========

IPSec policy group: "P1"

Using interface:

==========

Sequence number: 10

Security data flow: 3001

Tunnel local address: 10.0.23.3

Tunnel remote address: 10.0.12.1

Qos pre-classify: Disable

Proposal name:tran1

Inbound AH setting:

  AH SPI:

  AH string-key:

  AH authentication hex key:

Inbound ESP setting:

  ESP SPI: 54321 (0xd431)

  ESP string-key: huawei

  ESP encryption hex key:

  ESP authentication hex key:

Outbound AH setting:

  AH SPI:

  AH string-key:

  AH authentication hex key:

Outbound ESP setting:

  ESP SPI: 12345 (0x3039)

  ESP string-key: huawei

  ESP encryption hex key:

  ESP authentication hex key:

步骤八　在接口下应用 IPSec 策略

在物理接口应用IPSec策略，接口将对感兴趣流量进行IPSec加密处理。

[R1]interface Serial 1/0/0

[R1-Serial1/0/0]ipsec policy P1

[R3]interface Serial 2/0/0

[R3-Serial2/0/0]ipsec policy P1

步骤九　检测网络的连通性

验证设备对不感兴趣流量不进行IPSec加密处理。

```
<R1>ping -a 10.0.11.11 10.0.33.33
  PING 10.0.33.33: 56  data bytes, press CTRL_C to break
    Reply from 10.0.33.33: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 10.0.33.33: bytes=56 Sequence=2 ttl=254 time=50 ms
    Reply from 10.0.33.33: bytes=56 Sequence=3 ttl=254 time=50 ms
    Reply from 10.0.33.33: bytes=56 Sequence=4 ttl=254 time=60 ms
    Reply from 10.0.33.33: bytes=56 Sequence=5 ttl=254 time=50 ms
  --- 10.0.33.33 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/54/60 ms

<R1>display ipsec statistics esp
 Inpacket count                : 0
 Inpacket auth count           : 0
 Inpacket decap count          : 0
 Outpacket count               : 0
 Outpacket auth count          : 0
 Outpacket encap count         : 0
 Inpacket drop count           : 0
 Outpacket drop count          : 0
 BadAuthLen count              : 0
 AuthFail count                : 0
 InSAAclCheckFail count        : 0
```

```
 PktDuplicateDrop count             : 0
 PktSeqNoTooSmallDrop count         : 0
 PktInSAMissDrop count              : 0
```

验证设备将对感兴趣流量进行IPSec加密处理。

```
<R1>ping -a 10.0.1.1 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=255 time=80 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=77 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=255 time=77 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=255 time=80 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=255 time=77 ms
  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 77/78/80 ms

<R1>display ipsec statistics esp
 Inpacket count                     : 5
 Inpacket auth count          : 0
 Inpacket decap count         : 0
 Outpacket count              : 5
 Outpacket auth count         : 0
 Outpacket encap count        : 0
 Inpacket drop count          : 0
 Outpacket drop count         : 0
 BadAuthLen count                   : 0
 AuthFail count                     : 0
 InSAAclCheckFail count             : 0
```

PktDuplicateDrop count : 0

PktSeqNoTooSmallDrop count : 0

PktInSAMissDrop count : 0

配置文件

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
acl number 3001
 rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.12.1
 tunnel remote 10.0.23.3
 sa spi inbound esp 12345
 sa string-key inbound esp simple huawei
 sa spi outbound esp 54321
 sa string-key outbound esp simple huawei
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap
```

```
 ip address 10.0.12.1 255.255.255.0
 ipsec policy P1
 baudrate 128000
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.0.11.11 255.255.255.0
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.11.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+
L,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return


<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
```

```
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user huawei password cipher %$%$u[hr6d<JVHR@->T7xr1<$.iv%$%$
 ip address 10.0.12.2 255.255.255.0
#
interface Serial2/0/0
 link-protocol ppp
 ppp chap user huawei
 ppp chap password cipher %$%$e{5h)gh"/Uz0mUC%vEx3$4<m%$%$
 ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2dk#ikaWI.*(,%
$%$
user-interface vty 0 4
#
return


<R3>display current-configuration
[V200R007C00SPC600]
#
```

```
 sysname R3
#
acl number 3001
 rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255


#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.23.3
 tunnel remote 10.0.12.1
 sa spi inbound esp 54321
 sa string-key inbound esp simple huawei
 sa spi outbound esp 12345
 sa string-key outbound esp simple huawei
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap
 ip address 10.0.23.3 255.255.255.0
 ipsec policy P1
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
interface LoopBack1
```

```
 ip address 10.0.33.33 255.255.255.0
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
  network 10.0.33.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return
```

实验 3-5 GRE 隧道配置

学习目标

- 掌握GRE隧道封装的配置方法
- 掌握GRE隧道接口的配置方法
- 理解GRE Keepalive功能的实现原理

拓扑图

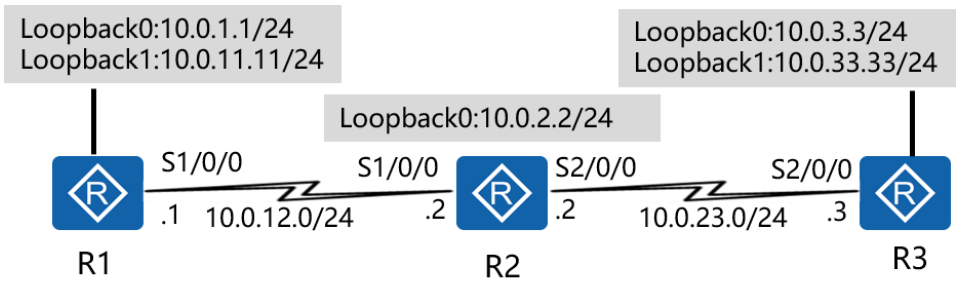

图3.5 GRE隧道配置实验拓扑图

场景

您是企业的网络管理员，当企业总部和分支机构间需要互相发布加密的路由信息时，仅通过IPSec VPN方案是无法实现的。由于IPSec VPN无法承载使用组播发送的路由协议数据包，因此您还需要在现有的IPSec网络中配置GRE隧道解决此问题。

操作步骤

注意：开始配置本实验前，必须先完成实验3-4。

步骤一　创建 GRE 隧道

创建隧道接口并为该接口配置一个公网IP地址，然后指定接口封装类型为GRE，并配置隧道的实际源地址以及实际目的地址。

[R1]interface Tunnel 0/0/1

[R1-Tunnel0/0/1]ip address 100.1.1.1 24

[R1-Tunnel0/0/1]tunnel-protocol gre

[R1-Tunnel0/0/1]source 10.0.12.1

[R1-Tunnel0/0/1]destination 10.0.23.3

[R3]interface Tunnel 0/0/1

[R3-Tunnel0/0/1]ip address 100.1.1.2 24

[R3-Tunnel0/0/1]tunnel-protocol gre

[R3-Tunnel0/0/1]source 10.0.23.3

[R3-Tunnel0/0/1]destination 10.0.12.1

步骤二　配置 OSPF 进程 2 用于隧道路由

将隧道接口所在的网络通告在OSPF进程1，从OSPF进程1中删除网络10.0.12.0/24和10.0.23.0/24。创建链OSPF进程2，并将网络10.0.12.0/24和10.0.23.0/24通告到OSPF进程2。

[R1]ospf 1

[R1-ospf-1]area 0

[R1-ospf-1-area-0.0.0.0]network 100.1.1.0 0.0.0.255

[R1-ospf-1-area-0.0.0.0]undo network 10.0.12.0 0.0.0.255

[R1]ospf 2 router-id 10.0.1.1

[R1-ospf-2]area 0

[R1-ospf-2-area-0.0.0.0]network 10.0.12.0 0.0.0.255

[R3]ospf 1

[R3-ospf-1]area 0

[R3-ospf-1-area-0.0.0.0]network 100.1.1.0 0.0.0.255

[R3-ospf-1-area-0.0.0.0]undo network 10.0.23.0 0.0.0.255

[R3]ospf 2 router-id 10.0.3.3

[R3-ospf-2]area 0

[R3-ospf-2-area-0.0.0.0]network 10.0.23.0 0.0.0.255

路由器会为不同的OSPF进程创建不同的LSDB，R1和R3中分别有LSDB 1和LSDB 2，两个数据库彼此独立，不会同步路由信息。因此R2学习不到R1和R3通告在进程2中的路由。

执行**display interface Tunnel 0/0/1**命令，验证配置结果。

<R1>display interface Tunnel 0/0/1

Tunnel0/0/1 current state : UP

Line protocol current state : UP

Last line protocol up time : 2016-03-17 17:10:16

Description:HUAWEI, AR Series, Tunnel0/0/1 Interface

Route Port,The Maximum Transmit Unit is 1500

Internet Address is 100.1.1.1/24

Encapsulation is TUNNEL, loopback not set

Tunnel source 10.0.12.1 (Serial1/0/0), destination 10.0.23.3

Tunnel protocol/transport GRE/IP, key disabled

keepalive disabled

Checksumming of packets disabled

Current system time: 2016-03-17 17:35:39

Last 300 seconds input rate 0 bytes/sec, 0 packets/sec

Last 300 seconds output rate 9 bytes/sec, 0 packets/sec

Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec

Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec

0 packets input, 0 bytes, 0 drops

145 packets output, 14320 bytes, 0 drops

Input bandwidth utilization : --

Output bandwidth utilization : --

<R3>display interface Tunnel 0/0/1

Tunnel0/0/1 current state : UP

Line protocol current state : UP

Last line protocol up time : 2016-03-17 17:10:40

Description:HUAWEI, AR Series, Tunnel0/0/1 Interface

Route Port,The Maximum Transmit Unit is 1500

Internet Address is 100.1.1.2/24

Encapsulation is TUNNEL, loopback not set

Tunnel source 10.0.23.3 (Serial2/0/0), destination 10.0.12.1

Tunnel protocol/transport GRE/IP, key disabled

keepalive disabled

Checksumming of packets disabled

Current system time: 2016-03-17 17:36:44

Last 300 seconds input rate 0 bytes/sec, 0 packets/sec

Last 300 seconds output rate 9 bytes/sec, 0 packets/sec

Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec

Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec

0 packets input, 0 bytes, 0 drops

162 packets output, 14420 bytes, 15 drops

Input bandwidth utilization : --

Output bandwidth utilization : --

步骤三 将 GRE 流量定义为感兴趣流量

重新配置ACL定义感兴趣流量。

[R1]acl 3001

[R1-acl-adv-3001]rule 5 permit gre source 10.0.12.1 0 destination 10.0.23.3 0

[R3]acl 3001

[R3-acl-adv-3001]rule 5 permit gre source 10.0.23.3 0 destination 10.0.12.1 0

步骤四 验证路由信息通过 GRE 封装后可由 IPSec VPN 传输

执行**display ip routing-table**命令，查看IPv4路由表。

<R1>display ip routing-table

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

Routing Tables: Public

Destinations : 21 Routes : 21

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.0/24	Direct	0	0	D	10.0.1.1	LoopBack0
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.255/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.2.2/32	OSPF	10	781	D	10.0.12.2	Serial1/0/0
10.0.3.3/32	OSPF	10	1562	D	100.1.1.2	Tunnel0/0/1
10.0.11.0/24	Direct	0	0	D	10.0.11.11	LoopBack1
10.0.11.11/32	Direct	0	0	D	127.0.0.1	LoopBack1
10.0.11.255/32	Direct	0	0	D	127.0.0.1	LoopBack1
10.0.12.0/24	Direct	0	0	D	10.0.12.1	Serial1/0/0
10.0.12.1/32	Direct	0	0	D	127.0.0.1	Serial1/0/0
10.0.12.2/32	Direct	0	0	D	10.0.12.2	Serial1/0/0
10.0.12.255/32	Direct	0	0	D	127.0.0.1	Serial1/0/0
10.0.23.0/24	OSPF	10	2343	D	10.0.12.2	Serial1/0/0
10.0.33.33/32	OSPF	10	1562	D	100.1.1.2	Tunnel0/0/1
100.1.1.0/24	Direct	0	0	D	100.1.1.1	Tunnel0/0/1
100.1.1.1/32	Direct	0	0	D	127.0.0.1	Tunnel0/0/1
100.1.1.255/32	Direct	0	0	D	127.0.0.1	Tunnel0/0/1
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>display ip routing-table

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

Routing Tables: Public

Destinations : 21 Routes : 21

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	OSPF	10	1562	D	100.1.1.1	Tunnel0/0/1
10.0.2.2/32	OSPF	10	1562	D	10.0.23.2	Serial2/0/0
10.0.3.0/24	Direct	0	0	D	10.0.3.3	LoopBack0
10.0.3.3/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.3.255/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.11.11/32	OSPF	10	1562	D	100.1.1.1	Tunnel0/0/1
10.0.12.0/24	OSPF	10	3124	D	10.0.23.2	Serial2/0/0
10.0.23.0/24	Direct	0	0	D	10.0.23.3	Serial2/0/0
10.0.23.2/32	Direct	0	0	D	10.0.23.2	Serial2/0/0
10.0.23.3/32	Direct	0	0	D	127.0.0.1	Serial2/0/0
10.0.23.255/32	Direct	0	0	D	127.0.0.1	Serial2/0/0
10.0.33.0/24	Direct	0	0	D	10.0.33.33	LoopBack1
10.0.33.33/32	Direct	0	0	D	127.0.0.1	LoopBack1
10.0.33.255/32	Direct	0	0	D	127.0.0.1	LoopBack1
100.1.1.0/24	Direct	0	0	D	100.1.1.2	Tunnel0/0/1
100.1.1.2/32	Direct	0	0	D	127.0.0.1	Tunnel0/0/1
100.1.1.255/32	Direct	0	0	D	127.0.0.1	Tunnel0/0/1
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

可以观察到，GRE隧道建立后，路由器可以将OSPF协议报文通过GRE封装后进行交互，从而获取对端路由信息。清除IPSec统计信息后，再通过**Ping**命令测试网络连通性。

```
<R1>reset ipsec statistics esp

[R1]ping -a 10.0.1.1 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=255 time=69 ms
  Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=70 ms
  Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=255 time=68 ms
  Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=255 time=68 ms
  Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=255 time=68 ms
--- 10.0.3.3 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 68/68/70 ms

<R1>display ipsec statistics esp
 Inpacket count                : 8
 Inpacket auth count           : 0
 Inpacket decap count          : 0
 Outpacket count               : 8
 Outpacket auth count          : 0
 Outpacket encap count         : 0
 Inpacket drop count           : 0
 Outpacket drop count          : 0
 BadAuthLen count              : 0
 AuthFail count                : 0
 InSAAclCheckFail count        : 0
 PktDuplicateDrop count        : 0
 PktSeqNoTooSmallDrop count    : 0
 PktInSAMissDrop count         : 0
```

如上IPSec ESP统计信息可以看出，OSPF协议交互的报文（包括hello报文）进行了GRE封装后再被IPSec VPN加密传输。

步骤五　给 GRE 隧道配置 Keepalive 功能

[R1]interface Tunnel 0/0/1

[R1-Tunnel0/0/1]keepalive period 3

验证隧道接口的Keepalive功能是否已开启。

<R1>display interface Tunnel 0/0/1

Tunnel0/0/1 current state : UP

Line protocol current state : UP

Last line protocol up time : 2016-03-18 09:50:21

Description:HUAWEI, AR Series, Tunnel0/0/1 Interface

Route Port,The Maximum Transmit Unit is 1500

Internet Address is 100.1.1.1/24

Encapsulation is TUNNEL, loopback not set

Tunnel source 10.0.12.1 (Serial1/0/0), destination 10.0.23.3

Tunnel protocol/transport GRE/IP, key disabled

keepalive enable period 3 retry-times 3

Checksumming of packets disabled

Current system time: 2016-03-18 11:05:49

Last 300 seconds input rate 0 bytes/sec, 0 packets/sec

Last 300 seconds output rate 8 bytes/sec, 0 packets/sec

Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec

Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec

0 packets input, 0 bytes, 0 drops

503 packets output, 47444 bytes, 0 drops

Input bandwidth utilization : --

Output bandwidth utilization : --

配置文件

<R1>display current-configuration

[V200R007C00SPC600]

```
#
 sysname R1
#
acl number 3001
 rule 5 permit gre source 10.0.12.1 0 destination 10.0.23.3 0
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.12.1
 tunnel remote 10.0.23.3
 sa spi inbound esp 12345
 sa string-key inbound esp simple huawei
 sa spi outbound esp 54321
 sa string-key outbound esp simple huawei
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap
 ip address 10.0.12.1 255.255.255.0
 ipsec policy P1
 baudrate 128000
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
```

```
interface LoopBack1
 ip address 10.0.11.11 255.255.255.0
#
interface Tunnel0/0/1
 ip address 100.1.1.1 255.255.255.0
 tunnel-protocol gre
 keepalive period 3
 source 10.0.12.1
 destination 10.0.23.3
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.11.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
ospf 2 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return

<R2>display current-configuration
```

```
[V200R007C00SPC600]
#
 sysname R2
#
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user huawei password cipher %$%$u[hr6d<JVHR@->T7xr1<$.iv%$%$
 ip address 10.0.12.2 255.255.255.0
#
interface Serial2/0/0
 link-protocol ppp
 ppp chap user huawei
 ppp chap password cipher %$%$e{5h)gh"/Uz0mUC%vEx3$4<m%$%$
 ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2dk#ikaWI.*(,%
$%$
user-interface vty 0 4
#
```

```
return


<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
acl number 3001
 rule 5 permit gre source 10.0.23.3 0 destination 10.0.12.1 0
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.23.3
 tunnel remote 10.0.12.1
 sa spi inbound esp 54321
 sa string-key inbound esp simple huawei
 sa spi outbound esp 12345
 sa string-key outbound esp simple huawei
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap
 ip address 10.0.23.3 255.255.255.0
 ipsec policy P1
#
```

```
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
interface LoopBack1
 ip address 10.0.33.33 255.255.255.0
#
interface Tunnel0/0/1
 ip address 100.1.1.2 255.255.255.0
 tunnel-protocol gre
 source 10.0.23.3
 destination 10.0.12.1
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.0 0.0.0.255
  network 10.0.33.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
ospf 2 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59
~..*g,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return
```

第四章 构建IPv6网络

实验 4-1 部署 IPv6 网络

学习目标

- 掌握基本IPv6地址的配置方法
- 掌握OSPFv3路由协议的配置方法
- 掌握DHCPv6服务器功能的配置方法
- 掌握IPv6 display命令的使用

拓扑图

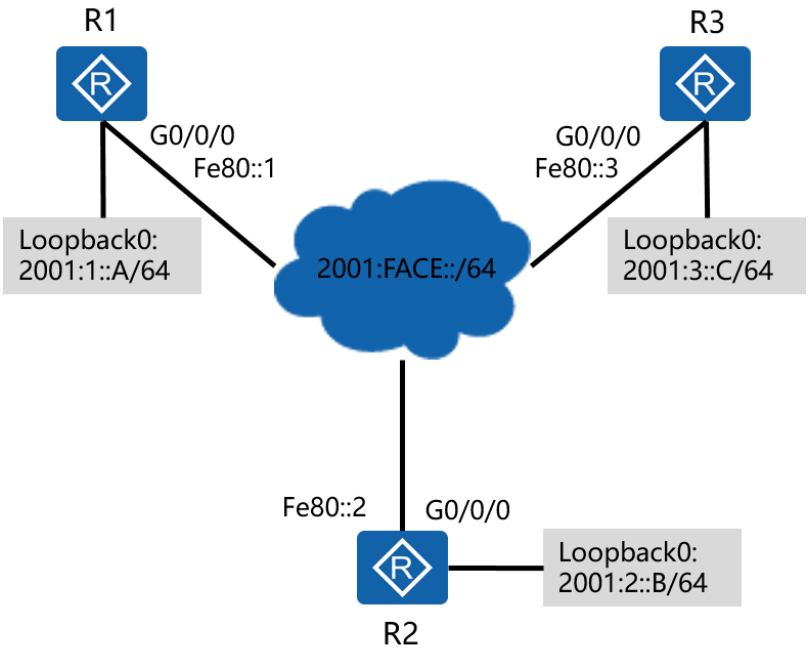

图4.1 部署IPv6网络实验拓扑图

场景

目前，企业网络还是IPv4网络，但是随着技术的进步与更迭，企业的网络需要从IPv4迁移至IPv6 ,作为管理员的您首先需要在现有网络上进行IPv6网络的设

计改造。在本实验中，您需要部署有状态IPv6地址分配方案以及IPv6路由协议。

操作步骤

步骤一　实验环境准备

如果本任务中您使用的是空配置设备，则从步骤1开始配置。如果使用的设备包含上一个实验的配置，请直接从步骤2开始配置。

<huawei>system-view

[huawei]sysname R1

<huawei>system-view

[huawei]sysname R2

<huawei>system-view

[huawei]sysname R3

步骤二　配置 IPv6 地址

在路由器的环回接口上配置IPv6全球单播地址，在所有路由器的G0/0/0接口配置本地链路地址。

[R1]ipv6

[R1]interface loopback 0

[R1-LoopBack0]ipv6 enable

[R1-LoopBack0]ipv6 address 2001:1::A 64

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]ipv6 enable

[R1-GigabitEthernet0/0/0]ipv6 address fe80::1 link-local

[R2]ipv6

[R2]interface loopback 0

[R2-LoopBack0]ipv6 enable

```
[R2-LoopBack0]ipv6 address 2001:2::B 64
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ipv6 enable
[R2-GigabitEthernet0/0/0]ipv6 address fe80::2 link-local

[R3]ipv6
[R3]interface loopback 0
[R3-LoopBack0]ipv6 enable
[R3-LoopBack0]ipv6 address 2001:3::C 64
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ipv6 enable
[R3-GigabitEthernet0/0/0]ipv6 address fe80::3 link-local
```

配置完成后，查看IPv6接口信息。

```
<R1>display ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::1
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

IPv6接口可以通过加入多个组播组（如FF02::1和FF02::2）来进行重复地址

检测（DAD），证实本地链路地址是独一无二的，以支持无状态地址自动配置（SLAAC）。

步骤三　配置 OSPFv3

在路由器上开启OSPFv3进程，并指定R1、R2和R3的路由器ID。然后在接口下使能OSPFv3进程并指定所属区域。

```
[R1]ospfv3 1
[R1-ospfv3-1]router-id 1.1.1.1
[R1-ospfv3-1]quit
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ospfv3 1 area 0
[R1-GigabitEthernet0/0/0]quit
[R1]interface loopback 0
[R1-LoopBack0]ospfv3 1 area 0

[R2]ospfv3 1
[R2-ospfv3-1]router-id 2.2.2.2
[R2-ospfv3-1]quit
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ospfv3 1 area 0
[R2-GigabitEthernet0/0/0]quit
[R2]interface loopback 0
[R2-LoopBack0]ospfv3 1 area 0

[R3]ospfv3 1
[R3-ospfv3-1]router-id 3.3.3.3
[R3-ospfv3-1]quit
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ospfv3 1 area 0
[R3-GigabitEthernet0/0/0]quit
```

```
[R3]interface loopback 0
[R3-LoopBack0]ospfv3 1 area 0
```

在R1和R3上执行**display ospfv3 peer**命令，查看OSPFv3的邻居关系。

```
<R1>display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State            Dead Time   Interface  Instance ID
2.2.2.2         1     Full/Backup      00:00:30    GE0/0/0    0
3.3.3.3         1     Full/DROther     00:00:40    GE0/0/0    0
```

```
<R3>display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State            Dead Time   Interface  Instance ID
1.1.1.1         1     Full/DR          00:00:32    GE0/0/0    0
2.2.2.2         1     Full/Backup      00:00:38    GE0/0/0    0
```

可以观察到邻居关系为Full，其中如果1.1.1.1不是DR，可以执行下面的命令重启OSPFv3进程。

```
<R1>reset ospfv3 1 graceful-restart
```

使用**Ping ipv6**检测对端本地链路地址和LoopBack 0接口的全球单播地址是否可达。

```
<R1>ping ipv6 fe80::3 -i GigabitEthernet 0/0/0
  PING fe80::3 : 56  data bytes, press CTRL_C to break
    Reply from FE80::3
    bytes=56 Sequence=1 hop limit=64   time = 2 ms
    Reply from FE80::3
    bytes=56 Sequence=2 hop limit=64   time = 2 ms
```

```
  Reply from FE80::3
  bytes=56 Sequence=3 hop limit=64   time = 11 ms
  Reply from FE80::3
  bytes=56 Sequence=4 hop limit=64   time = 2 ms
  Reply from FE80::3
  bytes=56 Sequence=5 hop limit=64   time = 2 ms
--- fe80::3 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/3/11 ms

<R1>ping ipv6 2001:3::C
  PING 2001:3::C : 56   data bytes, press CTRL_C to break
  Reply from 2001:3::C
  bytes=56 Sequence=1 hop limit=64   time = 11 ms
  Reply from 2001:3::C
  bytes=56 Sequence=2 hop limit=64   time = 6 ms
  Reply from 2001:3::C
  bytes=56 Sequence=3 hop limit=64   time = 2 ms
  Reply from 2001:3::C
  bytes=56 Sequence=4 hop limit=64   time = 2 ms
  Reply from 2001:3::C
  bytes=56 Sequence=5 hop limit=64   time = 6 ms
--- 2001:3::C ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/5/11 ms
```

步骤四　配置 DHCPv6 分配 IPv6 地址

在R2上开启DHCPv6服务器功能，为其它设备配置IPv6地址。然后创建IPv6地址池并指定地址池中IPv6地址的前缀和前缀长度，再配置IPv6地址池中不参与自动分配的IPv6地址（通常为网关地址）以及DNS服务器的IPv6地址。

[R2]dhcp enable

[R2] dhcpv6 duid ll

Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it? [Y/N]y

[R2]dhcpv6 pool pool1

[R2-dhcpv6-pool-pool1]address prefix 2001:FACE::/64

[R2-dhcpv6-pool-pool1]dns-server 2001:444e:5300::1

[R2-dhcpv6-pool-pool1]excluded-address 2001:FACE::1

[R2-dhcpv6-pool-pool1]quit

在G0/0/0接口配置IPv6地址为地址池中网关地址，并配置DHCPv6服务器功能和指定的地址池名称。

[R2]interface GigabitEthernet 0/0/0

[R2-GigabitEthernet0/0/0]ipv6 address 2001:FACE::1 64

[R2-GigabitEthernet0/0/0]dhcpv6 server pool1

在R1和R3上配置DHCPv6客户端功能，并在相应接口下配置通过DHCPv6自动获取IPv6地址功能。

[R1]dhcp enable

[R1] dhcpv6 duid ll

Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it? [Y/N]y

[R1]interface Gigabitethernet 0/0/0

[R1-GigabitEthernet0/0/0]ipv6 address auto dhcp

[R3]dhcp enable

[R3] dhcpv6 duid ll

Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it? [Y/N]y

[R3]interface GigabitEthernet 0/0/0

[R3-GigabitEthernet0/0/0]ipv6 address auto dhcp

在R2上执行**display dhcpv6 pool**命令，查看DHCPv6地址池的信息。

<R2>display dhcpv6 pool

DHCPv6 pool: pool1

Address prefix: 2001:FACE::/64

Lifetime valid 172800 seconds, preferred 86400 seconds

2 in use, 0 conflicts

Excluded-address 2001:FACE::1

1 excluded addresses

Information refresh time: 86400

DNS server address: 2001:444E:5300::1

Conflict-address expire-time: 172800

Active normal clients: 2

在R1和R3上执行**display ipv6 interface brief**命令，查看通过DHCPv6获取的IPv6地址。

[R1]display ipv6 interface brief

*down: administratively down

(l): loopback

(s): spoofing

Interface Physical Protocol

GigabitEthernet0/0/0 up up

[IPv6 Address] 2001:FACE::2

LoopBack0 up up(s)

[IPv6 Address] 2001:1::A

[R3]display ipv6 interface brief

*down: administratively down

(l): loopback

(s): spoofing

Interface Physical Protocol

GigabitEthernet0/0/0 up up

[IPv6 Address] 2001:FACE::3

LoopBack0 up up(s)

[IPv6 Address] 2001:3::C

配置文件

<R1>display current-configuration

[V200R007C00SPC600]

#

sysname R1

#

ipv6

#

dhcp enable

#

ospfv3 1

router-id 1.1.1.1

#

interface GigabitEthernet0/0/0

ipv6 enable

ip address 10.0.13.1 255.255.255.0

ipv6 address FE80::1 link-local

ospfv3 1 area 0.0.0.0

ipv6 address auto dhcp

#

```
interface LoopBack0
 ipv6 enable
 ip address 10.0.1.1 255.255.255.0
 ipv6 address 2001:1::A/64
 ospfv3 1 area 0.0.0.0
#
user-interface con 0
 authentication-mode password
 set authentication password
cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return

<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
ipv6
#
dhcp enable
#
dhcpv6 pool pool1
 address prefix 2001:FACE::/64
 excluded-address 2001:FACE::1
 dns-server 2001:444E:5300::1
#
ospfv3 1
```

```
 router-id 2.2.2.2
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ip address 10.0.13.2 255.255.255.0
 ipv6 address 2001:FACE::1/64
 ipv6 address FE80::2 link-local
 ospfv3 1 area 0.0.0.0
 traffic-filter inbound acl 3000
 dhcpv6 server pool1
#
interface LoopBack0
 ipv6 enable
 ip address 10.0.2.2 255.255.255.0
 ipv6 address 2001:2::B/64
 ospfv3 1 area 0.0.0.0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2dk#ikaWI.*(,%
$%$
user-interface vty 0 4
#
return


<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
```

```
ipv6
#
dhcp enable
#
ospfv3 1
 router-id 3.3.3.3
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ip address 10.0.13.3 255.255.255.0
 ipv6 address FE80::3 link-local
 ospfv3 1 area 0.0.0.0
 ipv6 address auto dhcp
#
interface LoopBack0
 ipv6 enable
 ip address 10.0.3.3 255.255.255.0
 ipv6 address 2001:3::C/64
 ospfv3 1 area 0.0.0.0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59
~..*g,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return
```

学习推荐

- 华为培训与认证官方网站
  - http://learning.huawei.com/cn/
- 华为在线学习
  - https://ilearningx.huawei.com/portal/#/portal/ebg/26
- 华为职业认证
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=zh
- 查找培训入口
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=zh

更多信息

- 华为培训APP