华为认证数通系列教程

HCIA-Datacom

实验指导手册

版本：2.0

华为技术有限公司

商标声明


和其它华为商标均为华为技术有限公司的商标。

本文档提及的其它所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其它原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址：　深圳市龙岗区坂田华为总部办公楼　邮编：518129

网址：　https://e.huawei.com

华为认证体系介绍

华为认证是华为公司基于“平台+生态”战略，围绕“云–管–端”协同的新ICT技术架构，打造的覆盖ICT（Information and Communications Technology，信息通信技术）全技术领域的认证体系，包含ICT基础设施、基础软硬件、云平台及云服务三类技术认证及项目管理认证。

根据ICT从业者的学习和进阶需求，华为认证分为工程师级别、高级工程师级别和专家级别三个认证等级。

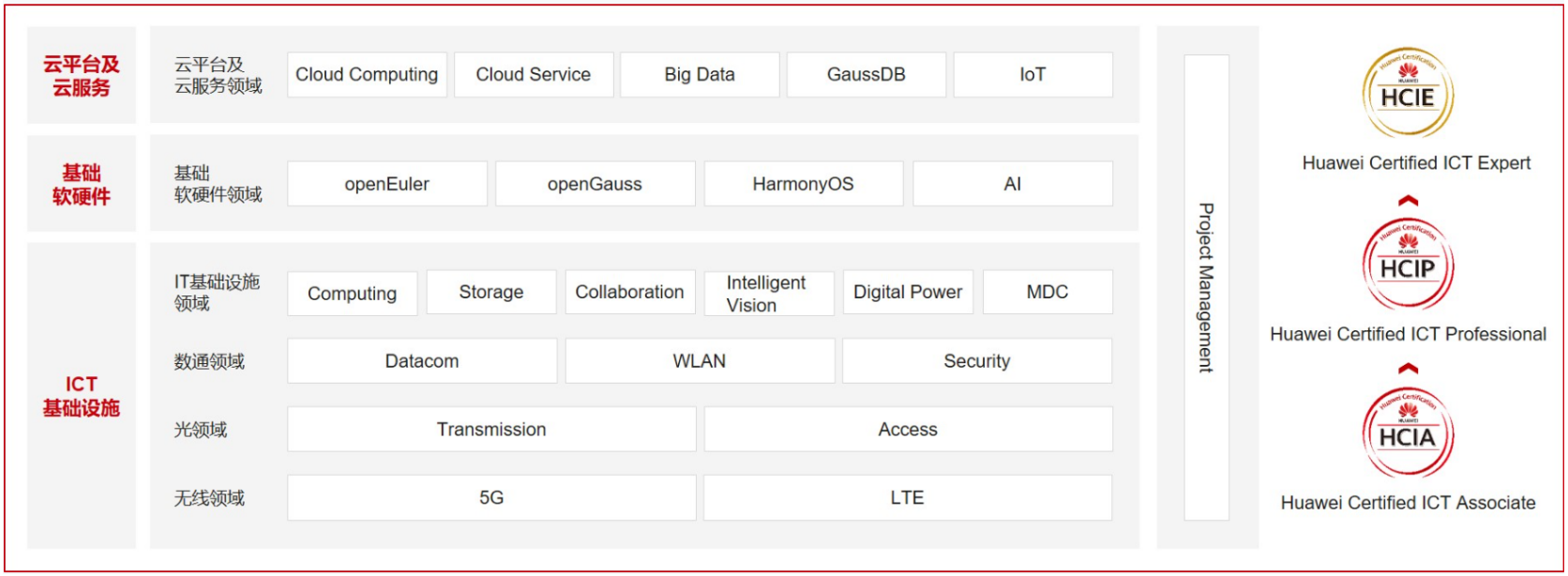
华为认证覆盖ICT全领域，符合ICT融合的技术趋势，致力于提供领先的人才培养体系和认证标准，培养数字化时代新型ICT人才，构建良性ICT人才生态。

HCIA-Datacom（Huawei Certified ICT Associate-Datacom，华为认证网络通信工程师数据通信方向）主要面向华为公司办事处、代表处一线工程师，以及其他希望学习华为数通产品技术人士。HCIA-Datacom V2.0认证在内容上涵盖路由交换基础知识、数据中心网络基础知识、WLAN基础知识、网络安全与服务基础知识、网络运维与排障等内容。

华为认证协助您打开行业之窗，开启改变之门，屹立在数通领域的潮头浪尖！

华为职业认证全景图

华为职业认证覆盖ICT全领域，致力于提供领先的人才培养体系和认证标准，培养数字化时代的新型ICT人才，构建良性的ICT人才生态。



前　言

简介

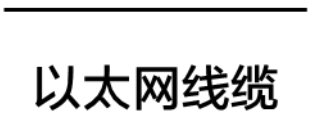
本书为 HCIA-Datacom 认证培训教程，适用于准备参加 HCIA-Datacom 考试的学员，或者希望了解路由交换原理、数据中心基本原理、WLAN 基本原理、网络安全与服务基础知识、网络运维与排障基础知识等相关技术的读者。

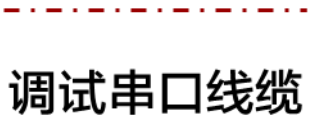
读者知识背景

本课程为华为认证基础课程，为了更好地掌握本书内容，阅读本书的读者应首先具备以下基本条件：

- 具有基本的计算机操作能力
- 对数据通信有基本的概念

本书常用图标





实验环境说明

为了满足 HCIA-Datacom 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
交换机	CloudEngine S5755-H24T4Y2CZ	V600R024C00SPC500
PoE交换机	CloudEngine S5755-H24P4Y2CZ	V600R024C00SPC500
无线接入点	AirEngine 5773-21	V600R024C00SPC100
路由器	AR5710-S8T2XE	V600R024C00SPC100

说明：推荐使用以上表格中的设备型号和软件版本，如果您使用的环境与以上表格内容不匹配，可能会出现配置命令、实现现象不匹配的情况。

恢复设备出厂配置

建议在完成本实验手册中的每一个实验前，先把相关交换机和路由器的配置恢复为出厂配置。

```
<HUAWEI> reset factory-configuration
Warning: Running this command will reset factory configuration and restart the device. Continue?
[Y/N] : y
Please wait....
Info: Reset factory configuration successfully!
```

目录

1 华为网络设备基本操作

1.1 实验介绍

1.1.1 关于本实验

本实验通过配置华为设备，了解并熟悉华为 YunShan OS 的基本操作。

1.1.2 实验目的

- 理解命令行视图的含义，以及进入、离开命令行视图的方法
- 掌握一些常见的命令
- 掌握使用命令行在线帮助的方法
- 掌握如何撤销命令
- 掌握如何使用命令行快捷键

1.1.3 实验组网介绍

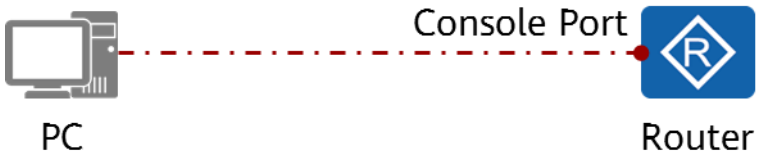


图1-1 华为网络设备基本操作实验拓扑

1.1.4 实验背景

如组网图所示，Router 是一台全新无配置的路由器，PC 通过串口线缆连接到 Router 的 Console Port，需要对 Router 进行一些初始化操作。

1.2 实验任务配置

1.2.1 配置思路

1. 完成设备命名、路由器接口 IP 地址等基础配置
2. 保存设备配置
3. 重启设备

1.2.2 配置步骤

步骤 1 通过 Console 方式登录到 Router 的 CLI，并设置密码

```
Please configure the login password (8-16)
Enter Password: Huawei@123
Confirm Password: Huawei@123
Info: Save the password now. Please wait for a moment.
Info: The max number of VTY users is 21, the number of current VTY users online is 0, and total number of terminal users online is 1.
        The current login time is XXXX-XX-XX XX:XX:XX.
```

步骤 2 查看设备基本信息

查看设备版本信息

```
<HUAWEI> display version
Huawei YunShan OS
Version 1.24.0.1 (AR5700 V600R024C00SPC100)
Copyright (C) 2021-2024 Huawei Technologies Co., Ltd.
HUAWEI AR5710-S8T2XE uptime is 0 day, 0 hour, 31 minutes

MPU(Master) 0 : uptime is   0 day, 0 hour, 30 minutes
          StartupTime XXXX/XX/XX    03:44:27
Memory         Size      : 4096 M bytes
Flash          Size      : 1024 M bytes
MPU version information:
1.PCB          Version : AR5710-S8T2XE VER A
2.MAB          Version : 0
3.Board        Type      : AR5710-S8T2XE
4.BIOS         Version : 1390
5.CPLD         Version : 258
```

从以上输出中得知，设备的软件版本为 V600R024C00SPC100，设备型号为 AR5710-S8T2XE，设备已启动 31 分钟。

步骤 3 完成设备基本配置

修改 Router 的名字为 Datacom-Router

```
<HUAWEI> system-view
Enter system view, return user view with return command.
[HUAWEI]
```

此时设备已经从用户视图进入到了系统视图。

```
[HUAWEI] sysname Datacom-Router
[Datacom-Router]
```

此时设备名称已经修改为 Datacom-Router。

华为设备提供丰富的功能，相应的也提供了多样的配置和查询命令。为便于用户使用这些命令，华为设备按功能分类将命令分别注册在不同的命令行视图下。配置某一功能时，需首先进入对应的命令行视图，然后执行相应的命令进行配置。

进入接口视图，配置接口的 IP 地址

```
[Datacom-Router] inter                          //输入<Tab>补全命令
[Datacom-Router] interface                      //interface 是唯一可选的关键字
[Datacom-Router] interface g                    //输入<Tab>补全命令
[Datacom-Router] interface GE                   //GE 是唯一可选的关键字
[Datacom-Router] interface GE 0/0/1             //手动补全命令
```

输入命令的某个关键字的前几个字母，按下<Tab>键，可以显示出完整的关键字，前提是这几个字母可以唯一标识出该关键字，否则，连续按下<Tab>键，可出现不同的关键字，用户可以从中选择所需要的关键字。如：

inter+<Tab>，因为当前视图下以 **inter** 开头的命令只有 **interface**，则命令直接补全为 **interface**，连续按多次<Tab>也不会变化。

```
[Datacom-Router-GE0/0/1]
```

此时已经进入到了接口 GE0/0/1 的视图

```
[Datacom-Router-GE0/0/1] undo portswitch
```

portswitch 命令用来将以太网接口从三层模式切换到二层模式。

undo portswitch 命令用来将以太网接口从二层模式切换到三层模式。

缺省情况下，AR5710-S8T2XE 的 GE0/0/0~GE0/0/7 接口为 LAN 侧接口（LAN 侧接口全部支持切换成 WAN 侧接口），LAN 侧接口也可以称为二层接口，不能配置 IP 地址，此处我们将 GE0/0/1 接口切换为 WAN 侧接口。

```
[Datacom-Router-GE0/0/1] i?
  icmp                                    identity
  ifg                                     ifit
  igmp                                    ip
  ipsec                                   ipv6
  isis
```

当用户输入命令时，如果只记得此命令关键字的开头一个或几个字符，可以使用部分帮助获取以该字符串开头的所有关键字的提示。如：

在 GE0/0/1 接口视图下，输入 **i+?**，则会显示当前视图下所有 **i** 开头的命令的可选项，此时可以用<Tab>键补全，也可以手动补全。其中，**icmp**，**igmp** 等为关键字。

```
[Datacom-Router-GE0/0/1] ip ?
  address              Set the IP address of an interface
  binding              Enable binding of an interface with a VPN instance
  forward-broadcast    Specify IP directed broadcast information
  option               IP option
  urpf                 Unicast reverse path forwarding check
  verify               IP verification
```

键入一条命令的部分关键字，后接以空格分隔的**?**，如果该位置为关键字，则列出全部关键字及其简单描述。如：

ip +空格+**?**，则会显示所有以 **ip** 为关键字的命令与对应的解释。

```
[Datacom-Router-GE0/0/1] ip address ?
  X.X.X.X          IP address
  bootp-alloc    IP address allocated by BOOTP
  dhcp-alloc     IP address allocated by DHCP
  unnumbered     Share an address with another interface

[Datacom-Router-GE0/0/1] ip address 192.168.1.1 ?
  INTEGER<0-32> Length of the IP address mask
  X.X.X.X            IP address mask

[Datacom-Router-GE0/0/1] ip address 192.168.1.1 24 ?
  sub     Indicate a subordinate address
  tag     Match tag of the route
  <cr>
```

<cr>表示该位置没有关键字或参数，直接键入回车即可执行。

```
[Datacom-Router-GE0/0/1] dis this
#
interface GE0/0/1
 ip address 192.168.1.1 255.255.255.0
```

```
#
return
```

display this 命令用来查看当前视图的配置。对于某些正在生效的配置参数，如果与缺省参数相同，则不显示；对于某些参数，虽然用户已经配置，但如果这些参数所在的命令没有成功提交，则不予显示。**display this** 命令常用于检查配置。

设备支持不完整关键字输入，即在当前视图下，当输入的字符能够匹配唯一的关键字时，可以不输入完整的关键字。该功能提供了一种快捷的输入方式，有助于提高操作效率。如：

在接口下使用 **dis this**，虽然没有输入完整的命令，但由于当前视图下匹配 **dis this** 的命令只有 **display this**，所以命令可以正常执行。类似的还有 **dis cu**、**d cu** 等同于 **display current-configuration**。

```
[Datacom-Router-GE0/0/1] quit
```

quit 命令用来从当前视图退回到较低级别视图，如果是用户视图，则退出系统。

此时发现接口 IP 地址配置错误，需要将该地址配置到 GE0/0/2 接口

```
[Datacom-Router] interface GE 0/0/1
[Datacom-Router-GE0/0/1] undo ip address
[Datacom-Router-GE0/0/1] quit
```

需要先删除 GE0/0/1 的 IP 地址配置，否则会产生地址冲突无法配置。

在命令前加 **undo** 关键字，即为 **undo** 命令行。**undo** 命令行一般用来恢复缺省情况、禁用某个功能或者删除某项配置。几乎每条配置命令都有对应的 **undo** 命令行。

```
[Datacom-Router] interface GE 0/0/2
[Datacom-Router-GE0/0/2] undo portswitch
[Datacom-Router-GE0/0/2] ip address 192.168.1.1 24
[Datacom-Router-GE0/0/2] quit
```

GE0/0/2 的接口 IP 地址已配置为 192.168.1.1/24。

（可选）配置用户界面断开连接的超时时间

```
[Datacom-Router] user-interface console 0
[Datacom-Router-ui-console0] idle-timeout 1440
[Datacom-Router-ui-console0] quit
```

user-interface console 0 命令用来进入 Console 用户界面视图。

idle-timeout 命令用来设置用户界面断开连接的超时时间。如果用户在一段时间内没有输入命令，系统将断开连接。此处将超时时间设置为 1440 分钟。

查看设备当前配置

```
[Datacom-Router] display current-configuration
```

```
!Software Version V600R024C00SPC100
!Last configuration was updated at XXXX-XX-XX 04:20:16+00:00
!Last configuration was saved at XXXX-XX-XX 04:20:29+00:00
!ase VRPV800R006C00B016D0127-0.0.1
!grpc VRPV800R006C00B016D0127-0.0.1
!kms_feature --
!md_tlm VRPV800R006C00B016D0127-0.0.1
!telem VRPV800R006C00B016D0127-0.0.1
#
pki realm default
#
sysname Datacom-Router
#
undo ftp server source all-interface
undo ftp ipv6 server source all-interface
#
ssl policy default
 pki-domain default
 ssl minimum version tls1.2
 cipher-suite exclude key-exchange rsa
 cipher-suite exclude cipher mode cbc
 cipher-suite exclude hmac sha1
 diffie-hellman modulus 3072
  ---- More ----
```

当执行某一命令后，如果显示的信息超过一屏时，系统会自动暂停输出信息，以方便用户查看。此时在显示信息的最底部会出现---- More ----的字样，此时可以通过：

1. 键入<Ctrl+C>或<Ctrl+Z>，停止显示或命令执行。
2. 键入空格键，继续显示下一屏信息。
3. 键入回车键，继续显示下一行信息。

步骤 4 保存设备当前配置

返回到用户视图

```
[Datacom-Router] quit
<Datacom-Router>
```

除了通过 quit 命令外，也可以通过：

1. return 命令，该命令可在任何视图下直接返回到用户视图。
2. <Ctrl+Z>快捷键，该快捷键可在任何视图下直接返回到用户视图。

保存配置

```
<Datacom-Router> save
Warning: The current configuration will be written to the device. Continue? [Y/N] : y   //输入 y 确认
```

```
Info: Please input the file name(*.cfg, *.zip, *.dat):      //输入回车，使用缺省文件名
Now saving the current configuration to the slot 0 .....
Info: Save the configuration successfully.
```

用户通过命令行可以修改设备的当前配置，而这些配置未被保存，如果要使当前配置在系统下次重启时仍然有效，在重启设备前，需要将当前配置保存到配置文件中。可以通过 **save** 直接保存到默认路径并覆盖原有的配置文件，也可以通过命令 **save** *configuration-file* 用来保存当前配置信息到存储设备中的指定文件中。该命令通常情况下不影响系统当前的启动配置文件。不输入文件名时，配置将默认保存到 **vrpcfg.zip**，并将其设置为下次启动文件。

比较当前配置与下一次启动所使用的配置

```
<Datacom-Router> compare configuration
Building configuration....
Info: The current configuration is the same as the next startup configuration file.
```

当前的配置与下次启动的配置文件内容一致。

步骤 5 操作设备的文件系统

查看当前目录下的文件列表

```
<Datacom-Router> dir
Directory of flash:/

  Idx  Attr       Size(Byte)  Date         Time          FileName
    0  drwx                -  Aug 21 XXXX 01:08:36   $_autobackup
    1  dr-x                -  Aug 21 XXXX 01:17:42   $_checkpoint
    2  dr-x                -  Jul 17 XXXX 01:00:00   $_install_mod
    3  dr-x                -  Aug 21 XXXX 01:06:51   $_license
    4  dr-x                -  Aug 21 XXXX 01:08:03   $_startup
    5  dr-x                -  Feb 28 XXXX 12:21:13   $_system
    6  dr-x                -  Aug 21 XXXX 01:16:14   $_user
    7  -rw-      235,889,380  Mar 12 XXXX 04:50:56   AR5700S-E_V600R024C00SPC100.cc
    8  -rw-        4,105,206  Feb 27 XXXX 11:50:04   AR5700S-E_V600R023SPH150.PAT
    9  -rw-          218,057  Feb 28 XXXX 12:21:19   application.txt
   10  -rw-          218,057  Feb 28 XXXX 12:21:19   application_touch.txt
   11  -rw-          223,888  Feb 28 XXXX 11:50:20   ase_url_backup.sdb
   12  drwx                -  Aug 21 XXXX 01:07:23   bootlogfile
   13  drwx                -  Feb 28 XXXX 12:17:09   default-sdb
   14  -rw-            3,725  Mar 01 XXXX 03:43:14   device.sys
   15  drwx                -  Aug 21 XXXX 01:16:29   dhcp
   16  drwx                -  Aug 21 XXXX 01:16:03   full_kpi
   17  drwx                -  Feb 27 XXXX 11:49:18   hips
   18  drwx                -  Aug 21 XXXX 01:06:52   hrp
   19  dr-x                -  Mar 01 XXXX 02:20:08   logfile
   20  drwx                -  Aug 21 XXXX 01:07:39   nlog
   21  drwx                -  Aug 21 XXXX 01:07:41   pki
```

```
  22   -rw-          9,815   Feb 28 XXXX 12:21:19    subcategory.txt
  23   drwx              -   Aug 21 XXXX 01:16:16    update
  24   -rw-          2,004   Mar 01 XXXX 03:43:14    vrpcfg.zip
  25   drwx              -   Aug 21 XXXX 01:16:14    webm
  26   drwx              -   Aug 21 XXXX 01:16:15    ztp
  27   -rw-        385,332   Feb 28 XXXX 12:02:43    ztp_XXXX0227115454.log
  28   -rw-          4,865   Feb 28 XXXX 14:26:19    ztp_XXXX0228122319.log
  29   -rw-        110,682   Mar 01 XXXX 03:30:44    ztp_XXXX0228142651.log
  30   -rw-         98,999   Mar 01 XXXX 01:58:52    ztp_XXXX0228142651.log.1.gz

732,844 KB total (483,000 KB free)
```

AR5700S-E_V600R024C00SPC100.cc：系统软件。系统软件必须以**.cc** 作为扩展名。

vrpcfg.zip：配置文件。配置文件必须以**.cfg** 或**.zip** 作为扩展名。

其余文件不再介绍，不同设备其输出信息也有所不同。

将当前的配置保存，同时命名为 test.cfg

```
<Datacom-Router> save test.cfg
Warning: Are you sure to save the configuration to flash:/test.cfg? [Y/N] : y
Now saving the current configuration to the slot 0
Info: Save the configuration successfully.
```

再次查看当前目录下的文件列表

```
<Datacom-Router> dir
Directory of flash:/

  Idx  Attr       Size(Byte)  Date         Time          FileName
    0  drwx                -  Aug 21 XXXX 01:08:36   $_autobackup
    1  dr-x                -  Aug 21 XXXX 01:17:42   $_checkpoint
    2  dr-x                -  Jul 17 XXXX 01:00:00   $_install_mod
    3  dr-x                -  Aug 21 XXXX 01:06:51   $_license
    4  dr-x                -  Aug 21 XXXX 01:08:03   $_startup
    5  dr-x                -  Feb 28 XXXX 12:21:13   $_system
    6  dr-x                -  Aug 21 XXXX 01:16:14   $_user
    7  -rw-      235,889,380  Mar 12 XXXX 04:50:56   AR5700S-E_V600R024C00SPC100.cc
    8  -rw-        4,105,206  Feb 27 XXXX 11:50:04   AR5700S-E_V600R023SPH150.PAT
    9  -rw-          218,057  Feb 28 XXXX 12:21:19   application.txt
   10  -rw-          218,057  Feb 28 XXXX 12:21:19   application_touch.txt
   11  -rw-          223,888  Feb 28 XXXX 11:50:20   ase_url_backup.sdb
   12  drwx                -  Aug 21 XXXX 01:07:23   bootlogfile
   13  drwx                -  Feb 28 XXXX 12:17:09   default-sdb
   14  -rw-            3,725  Mar 01 XXXX 03:54:11   device.sys
   15  drwx                -  Aug 21 XXXX 01:16:29   dhcp
   16  drwx                -  Aug 21 XXXX 01:16:03   full_kpi
   17  drwx                -  Feb 27 XXXX 11:49:18   hips
```

```
  18   drwx               -   Aug 21 XXXX 01:06:52   hrp
  19   dr-x               -   Mar 01 XXXX 02:20:08   logfile
  20   drwx               -   Aug 21 XXXX 01:07:39   nlog
  21   drwx               -   Aug 21 XXXX 01:07:41   pki
  22   -rw-           9,815   Feb 28 XXXX 12:21:19   subcategory.txt
  23   -rw-           5,018   Mar 01 XXXX 03:54:11   test.cfg
  24   drwx               -   Aug 21 XXXX 01:16:16   update
  25   -rw-           2,004   Mar 01 XXXX 03:43:14   vrpcfg.zip
  26   drwx               -   Aug 21 XXXX 01:16:14   webm
  27   drwx               -   Aug 21 XXXX 01:16:15   ztp
  28   -rw-         385,332   Feb 28 XXXX 12:02:43   ztp_XXXX0227115454.log
  29   -rw-           4,865   Feb 28 XXXX 14:26:19   ztp_XXXX0228122319.log
  30   -rw-         110,682   Mar 01 XXXX 03:30:44   ztp_XXXX0228142651.log
  31   -rw-          98,999   Mar 01 XXXX 01:58:52   ztp_XXXX0228142651.log.1.gz

732,844 KB total (482,876 KB free)
```

配置文件保存成功！

把该文件设置为设备下一次启动所使用的配置文件

```
<Datacom-Router> startup saved-configuration test.cfg
Info: Operating, please wait for a moment.....done.
Info: Succeeded in setting the configuration for booting system.
```

startup saved-configuration 命令用来配置系统下次启动时使用的配置文件。下次启动文件设置成功！

查看下一次启动所用的文件

```
<Datacom-Router> display startup
MainBoard:
  Configured startup system software:        flash:/AR5700S-E_V600R024C00SPC100.cc
  Startup system software:                    flash:/AR5700S-E_V600R024C00SPC100.cc
  Next startup system software:               flash:/AR5700S-E_V600R024C00SPC100.cc
  Startup saved-configuration file:          NULL
  Next startup saved-configuration file:     flash:/test.cfg
  Startup paf file:                           default
  Next startup paf file:                      default
  Startup patch package:                       NULL
  Next startup patch package:                  NULL
  Startup feature software:                   NULL
  Next startup feature software:              NULL
```

display startup 命令用来查看设备本次及下次启动相关的系统软件、备份系统软件、配置文件、License 文件、补丁文件以及语音文件等。

清除设备下次启动时加载的配置文件

```
<Datacom-Router> reset saved-configuration
Warning: The action will delete the saved configuration on the device.
The configuration will be erased to reconfigure. Continue? [Y/N] : y
Warning: Now the configuration on the device is being deleted.
Info: Succeeded in clearing the configuration on the device.
```

reset saved-configuration 命令用来清除设备上的启动配置文件中的配置信息。

步骤 6 重启设备

```
<Datacom-Router> reboot
MPU 0:
Next startup system software: flash:/AR5700S-E_V600R023C00SPC100.cc
Next startup saved-configuration file: NULL
Next startup paf file: default
Next startup patch package: flash:/AR5700S-E_V600R023SPH150.PAT
Warning: The current configuration will be saved to the next startup saved-configuration file. Continue?
[Y/N] : y
Now saving the current configuration.....
Save the configuration successfully.
Warning: The system will reboot. Continue? [Y/N] : y
```

reboot 命令用来重启设备，重启前提示用户是否保存配置。系统开始重启，等待 10 分钟左右。

```
Please Press ENTER.


Password: Huawei@123
Info: The max number of VTY users is 21, the number of current VTY users online is 0, and total number
of terminal users online is 1.
        The current login time is XXXX-XX-XX XX:XX:XX.
<Datacom-Router>
```

设备重启完成，输入密码后登录成功。

步骤 7 设置设备重启后恢复为出厂配置

```
<Datacom-Router> reset factory-configuration
Warning: Running this command will reset factory configuration and restart the device. Continue?
[Y/N] : y
Please wait....
Info: Reset factory configuration successfully!
<Datacom-Router>
```

执行 **reset factory-configuration** 命令后，系统会提示是否需要重启设备。输入 **y** 后，设备将重启，并清除设备上的业务配置和数据文件。

该命令会还原设备出厂配置，慎重执行该命令，最好在技术支持人员指导下使用。

步骤 8 设备重启后，验证是否已恢复至出厂配置

```
Please configure the login password (8-16)
Enter Password: Huawei@123
Confirm Password: Huawei@123
Info: Save the password now. Please wait for a moment.
Info: The max number of VTY users is 21, the number of current VTY users online is 0, and total number of terminal users online is 1.
      The current login time is XXXX-XX-XX XX:XX:XX.
```

可以看到设备已恢复至出厂配置。

1.3 思考题

1. 根据附录的功能键列表，自行熟悉并掌握华为 YunShan OS 功能键。
2. 步骤 5 中使用了 **reset saved-configuration** 命令清除配置内容，为什么重启过后设备的配置依然保留?

答案：因为在设备重启时，我们选择了保存配置文件。

```
Warning: The current configuration will be saved to the next startup saved-configuration file. Continue? [Y/N] : y
```

1.4 附录

表1-1 系统功能键

功能键	功能
<Ctrl+A>	将光标移动到当前行的开头。
<Ctrl+B>	将光标向左移动一个字符。
<Ctrl+C>	停止当前正在执行的功能。
<Ctrl+D>	删除当前光标所在位置的字符。
<Ctrl+E>	将光标移动到当前行的末尾。
<Ctrl+F>	将光标向右移动一个字符。
<Ctrl+H>	删除光标左侧的一个字符。

<Ctrl+I>	功能等同于Tab键。
<Ctrl+J>	功能等同于回车键。
<Ctrl+K>	在连接建立阶段终止呼出的连接。
<Ctrl+M>	功能等同于回车键。
<Ctrl+N>	显示历史命令缓冲区中的后一条命令。
<Ctrl+P>	显示历史命令缓冲区中的前一条命令。
<Ctrl+Q>	转义。
<Ctrl+R>	重新显示当前行信息。
<Ctrl+T>	终止呼出的连接。
<Ctrl+V>	粘贴剪贴板的内容。
<Ctrl+W>	删除光标左侧的一个字符串（字）。
<Ctrl+X>	删除光标左侧所有的字符。
<Ctrl+Y>	删除光标所在位置及其右侧所有的字符。
<Ctrl+Z>	返回到用户视图。
<Ctrl+]>	终止呼入的连接或重定向连接。
<Esc+B>	将光标向左移动一个字符串（字）。
<Esc+D>	删除光标右侧的一个字符串（字）。
<Esc+F>	将光标向右移动一个字符串（字）。
<Esc+N>	将光标向下移动一行。
<Esc+P>	将光标向上移动一行。
<Esc+<>	将光标所在位置指定为剪贴板的开始位置。
<Esc+>>	将光标所在位置指定为剪贴板的结束位置。

2 VLAN 配置实验

2.1 实验介绍

2.1.1 关于本实验

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detection，带冲突检测的载波监听多路访问）的共享通讯介质的数据网络通讯技术。当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至造成网络不可用等问题。通过交换机实现互连虽然可以解决冲突严重的问题，但仍然不能隔离广播报文和提升网络质量。

在这种情况下出现了 VLAN 技术，这种技术可以把一个 LAN 划分成多个逻辑的 VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文就被限制在一个 VLAN 内。

本实验通过配置华为交换机设备，了解并熟悉 VLAN 技术的相关配置。

2.1.2 实验目的

- 掌握 VLAN 的创建方法
- 掌握 Access、Trunk 和 Hybrid 类型接口的配置方法
- 掌握基于接口划分 VLAN 的配置方法
- 掌握基于 MAC 地址划分 VLAN 的配置方法
- 掌握 MAC 地址表及 VLAN 信息的查看方式

2.1.3 实验组网介绍

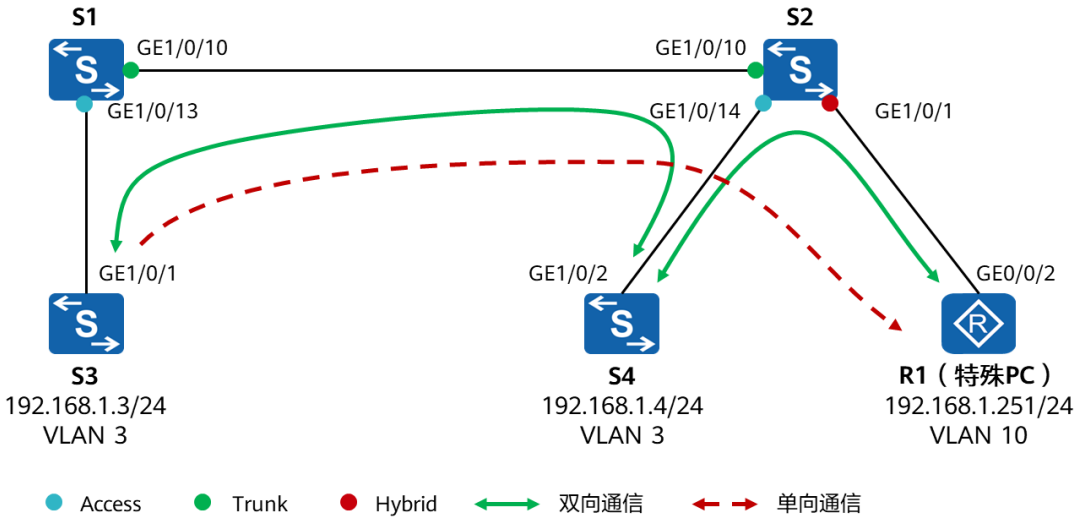


图2-1 VLAN 配置实验拓扑

2.1.4 实验背景

某公司根据业务需求，需要对其二层网络进行 VLAN 划分。R1 模拟特殊 PC，可以接收其它终端发送的数据包。

如实验拓扑图所示，可以在 S1 和 S2 上基于接口划分 VLAN，把业务相同的用户连接的接口划分到同一 VLAN。同时，可以在 S2 上基于 MAC 地址划分 VLAN，绑定 S4 的 MAC 地址。

2.2 实验任务配置

2.2.1 配置思路

1. 创建 VLAN
2. 配置交换机基于接口划分 VLAN
3. 配置交换机基于 MAC 地址划分 VLAN

2.2.2 配置步骤

步骤 1 配置设备名称并关闭多余接口

设备命名

略。

关闭 S1 的 GE1/0/1、GE1/0/11、GE1/0/12、GE1/0/14 接口

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] shutdown
[S1-GE1/0/1] quit
[S1] interface GE 1/0/11
[S1-GE1/0/11] shutdown
[S1-GE1/0/11] quit
[S1] interface GE 1/0/12
[S1-GE1/0/12] shutdown
[S1-GE1/0/12] quit
[S1] interface GE 1/0/14
[S1-GE1/0/14] shutdown
[S1-GE1/0/14] quit
```

关闭 S2 的 GE1/0/11、GE1/0/12、GE1/0/13 接口

```
[S2] interface GE 1/0/11
[S2-GE1/0/11] shutdown
[S2-GE1/0/11] quit
[S2] interface GE 1/0/12
[S2-GE1/0/12] shutdown
[S2-GE1/0/12] quit
[S2] interface GE 1/0/13
[S2-GE1/0/13] shutdown
[S2-GE1/0/13] quit
```

关闭 S3 的 GE1/0/2、GE1/0/3、GE1/0/4 接口

```
[S3] interface GE 1/0/2
[S3-GE1/0/2] shutdown
[S3-GE1/0/2] quit
[S3] interface GE 1/0/3
[S3-GE1/0/3] shutdown
[S3-GE1/0/3] quit
[S3] interface GE 1/0/4
[S3-GE1/0/4] shutdown
[S3-GE1/0/4] quit
```

关闭 S4 的 GE1/0/1、GE1/0/3、GE1/0/4 接口

```
[S4] interface GE 1/0/1
[S4-GE1/0/1] shutdown
[S4-GE1/0/1] quit
[S4] interface GE 1/0/3
```

```
[S4-GE1/0/3] shutdown
[S4-GE1/0/3] quit
[S4] interface GE 1/0/4
[S4-GE1/0/4] shutdown
[S4-GE1/0/4] quit
```

（可选）关闭设备的 ZTP 开局功能

```
[S1] quit
<S1> set ztp disable
Info: The ZTP process will be terminated. When restarting without a configuration file, the device will not start the ZTP process.
<S1> system-view
```

set ztp disable 命令用来关闭设备的 ZTP 开局功能。缺省情况下，设备空配置上电启动后，会自动执行 ZTP 开局流程。如果用户希望设备空配置启动时不进行 ZTP 开局，可以执行命令 **set ztp disable** 关闭 ZTP 开局功能。

将二层接口切换为三层接口

```
[R1] interface GE 0/0/2
[R1-GE0/0/2] undo portswitch
[R1-GE0/0/2] quit
```

```
[S3] interface GE 1/0/1
[S3-GE1/0/1] undo port link-type
[S3-GE1/0/1] undo portswitch
[S3-GE1/0/1] quit
```

```
[S4] interface GE 1/0/2
[S4-GE1/0/2] undo port link-type
[S4-GE1/0/2] undo portswitch
[S4-GE1/0/2] quit
```

步骤 2 配置设备 IP 地址

配置接口 IP 地址

```
[R1] interface GE0/0/2
[R1-GE0/0/2] ip address 192.168.1.251 24
[R1-GE0/0/2] quit
```

```
[S3] interface GE1/0/1
[S3-GE1/0/1] ip address 192.168.1.3 24
[S3-GE1/0/1] quit
```

```
[S4] interface GE1/0/2
[S4-GE1/0/2] ip address 192.168.1.4 24
[S4-GE1/0/2] quit
```

验证连通性

```
[R1] ping 192.168.1.3
  PING 192.168.1.3: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.3: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=5 ttl=254 time=1 ms

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

```
[R1] ping 192.168.1.4
  PING 192.168.1.4: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.4: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=5 ttl=254 time=1 ms

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

查看 R1 的 ARP 表项

```
[R1] display arp
ARP Entry Types: D - Dynamic, S - Static, I - Interface
EXP: Expire-time

IP ADDRESS       MAC ADDRESS     EXP(M) TYPE/VLAN       INTERFACE          VPN-INSTANCE
------------------------------------------------------------------------------------------
192.168.1.251    b0c7-8733-d661        I                GE0/0/2
192.168.1.3      20df-73f5-4372  20    D                GE0/0/2
192.168.1.4      20df-73f5-4332  20    D                GE0/0/2
```

```
192.168.1.1       b0c7-8733-d663          I                GE0/0/4          _management_vpn_
------------------------------------------------------------------------------
Total:4           Dynamic:2         Static:0      Interface:2
```

可以看到 R1 的 MAC 地址是 b0c7-8733-d661，S3 的 MAC 地址是 20df-73f5-4372，S4 的 MAC 地址是 20df-73f5-4332。

查看 S2 的 MAC 地址表

```
[S2] display mac-address
Flags: * - Backup
       # - forwarding logical interface, operations cannot be performed based
           on the interface.
BD   : bridge-domain    Age : dynamic MAC learned time in seconds
--------------------------------------------------------------------------------
MAC Address      VLAN/VSI/BD   Learned-From          Type                 Age
--------------------------------------------------------------------------------
20df-73f5-4332 1/-/-          GE1/0/14              dynamic              766
20df-73f5-4372 1/-/-          GE1/0/10              dynamic              508
20df-73f5-44e1 1/-/-          GE1/0/10              dynamic              799
b0c7-8733-d661 1/-/-          GE1/0/1               dynamic              601
--------------------------------------------------------------------------------
Total items: 4
```

可以看到 GE1/0/14 对应的 MAC 地址属于 S4，GE1/0/10 对应的 MAC 地址属于 S3，GE1/0/1 对应的 MAC 地址属于 R1。这三个 MAC 地址都通过动态学习获取。

说明：除以上三个 MAC 地址外，还有 1 个 MAC 地址，该 MAC 地址属于 S1 的系统 MAC 地址，您可以不用关注。

步骤 3 创建 VLAN

在交换机 S1 和 S2 上创建 VLAN 3、10

```
[S1] vlan batch 3 10
```

VLAN 3、10 创建成功。

vlan *vlan-id* 命令用来创建 VLAN 并进入 VLAN 视图，如果 VLAN 已存在，直接进入该 VLAN 的视图。

vlan batch { *vlan-id1* [**to** *vlan-id2*] }命令用来批量创建 VLAN。

```
[S2] vlan batch 3 10
```

步骤 4 配置基于接口划分 VLAN

配置交换机 S1 和 S2 连接终端的接口为 Access 接口，并将接口划入对应的 VLAN

```
[S1] interface GE 1/0/13
[S1-GE1/0/13] port link-type access
```

port link-type { access | hybrid | trunk }命令用来配置接口的链路类型。可以配置接口的类型为 Access、Trunk 或 Hybrid。

补充说明：

如果网络拓扑变更，以太网接口的链路类型也需要重新配置，配置较为繁琐。为了简化用户配置，可通过 LNP（Link-type Negotiation Protocol，链路类型协商协议）配置以太网接口的链路类型自协商功能，自动协商出接口的链路类型为 Access 或者 Trunk，并加入相应 VLAN。

1. 以太网接口的链路类型协商为 Access，缺省情况下加入 VLAN1。
2. 以太网接口的链路类型协商为 Trunk，缺省情况下加入 VLAN1～4094。

port link-type { negotiation-desirable | negotiation-auto }命令用来指定接口动态协商的类型。Negotiation-desirable 可主动发送协商报文，Negotiation-auto 不主动发送协商报文。

```
[S1-GE1/0/13] port default vlan 3
[S1-GE1/0/13] quit
```

port default vlan *vlan-id* 命令用来配置接口的缺省 VLAN。

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] port link-type access
[S2-GE1/0/1] port default vlan 10
[S2-GE1/0/1] quit
[S2] interface GE 1/0/14
[S2-GE1/0/14] port link-type access
[S2-GE1/0/14] port default vlan 3
[S2-GE1/0/14] quit
```

配置交换机 S1 和 S2 的互联接口为 Trunk 接口，并仅允许 VLAN 3、10 通过

```
[S1] interface GE1/0/10
[S1-GE1/0/10] port link-type trunk
[S1-GE1/0/10] port trunk allow-pass vlan 3 10
```

port trunk allow-pass vlan 命令用来配置 Trunk 类型接口加入的 VLAN。

```
[S1-GE1/0/10] undo port trunk allow-pass vlan 1
[S1-GE1/0/10] quit
```

undo port trunk allow-pass vlan 命令用来删除 Trunk 类型接口加入的 VLAN。

VLAN 1 默认就在允许通过列表中，若无实际业务用途，出于安全考虑，一般要将它删除。

```
[S2] interface GE1/0/10
```

```
[S2-GE1/0/10] port link-type trunk
[S2-GE1/0/10] port trunk allow-pass vlan 3 10
[S2-GE1/0/10] undo port trunk allow-pass vlan 1
[S2-GE1/0/10] quit
```

在 S4 验证连通性

```
[S4] ping 192.168.1.3
  PING 192.168.1.3: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.3: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=5 ttl=254 time=1 ms

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

S3 和 S4 均属于 VLAN 3，因此可以 Ping 通。

```
[S4] ping 192.168.1.251
  PING 192.168.1.251: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

S4 和 R1 属于不同 VLAN，因此不能 Ping 通。

在 S4、R1 刷新 ARP 表项

```
[S4] quit
<S4> reset arp all
Warning: This operation will reset all dynamic ARP entries, and may cause services to be interrupted,
continue? [Y/N] : y
```

reset arp all 命令用来清除所有的 ARP 表项。

```
[R1] quit
<R1> reset arp all
```

```
Warning: This operation will reset all dynamic ARP entries, and may cause services to be interrupted,
continue? [Y/N] : y
```

在 S4 Ping 192.168.1.251，并查看 S4、R1 的 ARP 表项

```
<S4> ping 192.168.1.251
  PING 192.168.1.251: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

```
<S4> display arp
ARP Entry Types: D - Dynamic, S - Static, I - Interface, RD - Redirect
EXP: Expire-time VLAN: VLAN or Bridge Domain

IP ADDRESS      MAC ADDRESS     EXP(M) TYPE/VLAN       INTERFACE          VPN-INSTANCE
------------------------------------------------------------------------------
192.168.1.4     20df-73f5-4332          I                  GE1/0/2
192.168.1.3     20df-73f5-4372  17      D                  GE1/0/2
------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0     Interface:1     Redirect:0
```

在 S4 看不到 192.168.1.251 对应的 MAC 地址。

```
<R1> display arp
ARP Entry Types: D - Dynamic, S - Static, I - Interface
EXP: Expire-time

IP ADDRESS      MAC ADDRESS     EXP(M) TYPE/VLAN       INTERFACE          VPN-INSTANCE
------------------------------------------------------------------------------
192.168.1.251   b0c7-8733-d661          I                  GE0/0/2
192.168.1.1     b0c7-8733-d663          I                  GE0/0/4            _management_vpn_
------------------------------------------------------------------------------
Total:2         Dynamic:0       Static:0     Interface:2
```

在 R1 看不到 192.168.1.4 对应的 MAC 地址。

结合 S4 和 R1 的 ARP 表项进行分析：虽然 S4 会发送 ARP 请求，但该请求并不会发送给 R1，因为它们属于不同的 VLAN，广播报文被阻断。

步骤 5 将 S2 GE1/0/1 修改为 Hybrid 接口

修改 S2 GE1/0/1 接口的链路类型

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] port link-type hybrid
[S2-GE1/0/1] port hybrid pvid vlan 10
[S2-GE1/0/1] port hybrid untagged vlan 3 10
[S2-GE1/0/1] quit
```

port hybrid vlan 命令用来将 Hybrid 端口加入到指定的已经存在的 VLAN。**untagged/tagged** 用来指定该端口的出报文是否带 VLAN 标签。

配置完成后，S2 GE1/0/1 接口发送 VLAN 3 和 VLAN 10 的数据帧时，将数据帧中的 VLAN Tag 去掉。

在 S4 Ping 192.168.1.251，并查看 S4、R1 的 ARP 表项

```
<S4> ping 192.168.1.251
  PING 192.168.1.251: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

```
<S4> display arp
ARP Entry Types: D - Dynamic, S - Static, I - Interface, RD - Redirect
EXP: Expire-time VLAN: VLAN or Bridge Domain

IP ADDRESS      MAC ADDRESS     EXP(M) TYPE/VLAN        INTERFACE          VPN-INSTANCE
------------------------------------------------------------------------------
192.168.1.4     20df-73f5-4332          I                GE1/0/2
192.168.1.3     20df-73f5-4372    6     D                GE1/0/2
192.168.1.251   Incomplete        1     D                GE1/0/2
------------------------------------------------------------------------------
Total:3         Dynamic:2         Static:0      Interface:1      Redirect:0
```

在 S4 看不到 192.168.1.251 对应的 MAC 地址。

说明：在执行完 Ping 测命令后，等待几秒钟，在 S4 的 ARP 表中将看不到 192.168.1.254 这一行。

```
<R1> display arp
```

```
ARP Entry Types: D - Dynamic, S - Static, I - Interface
EXP: Expire-time

IP ADDRESS      MAC ADDRESS     EXP(M) TYPE/VLAN        INTERFACE          VPN-INSTANCE
------------------------------------------------------------------------------------------
192.168.1.251   b0c7-8733-d661          I                GE0/0/2
192.168.1.4     20df-73f5-4332  16     D                GE0/0/2
192.168.1.1     b0c7-8733-d663          I                GE0/0/4            _management_vpn_
------------------------------------------------------------------------------------------
Total:3         Dynamic:1       Static:0      Interface:2
```

在 R1 可以看到 192.168.1.4 对应的 MAC 地址是 20df-73f5-4332。

接下来结合 S4 和 R1 的 ARP 表项，分析为什么 R1 能获取到 S4 的 ARP 表项，而 S4 无法获取到 R1 的 ARP 表项：

1. S4 发送 ARP 广播请求，该数据帧到达 S2 后，S2 会添加上接口所属的 VLAN 标签，即 VLAN 3。
2. 之后 S2 会将该广播报文发送到所有属于 VLAN 3 的端口，由于 S2 GE1/0/1 端口在发送 VLAN 3 的数据帧时，将数据帧的标签剥离，因此该广播帧将会到达 R1。
3. R1 接收到 ARP 请求后，记录下 192.168.1.4 对应的 MAC 地址，然后以单播方式发送 ARP 应答报文
4. R1 的应答报文到达 S2 后，S2 会添加上 VLAN 标签 10。由于 S4 属于 VLAN3，因此 R1 的应答报文不会到达 S4。

查看 S2 的 VLAN 信息

```
[S2] display vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;          D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;                ST: Vlan-stacking;
#: ProtocolTransparent-vlan;     *: Management-vlan;
MAC-LRN: MAC-address learning;   STAT: Statistic;
BC: Broadcast; MC: Multicast;    UC: Unknown-unicast;
FWD: Forward;   DSD: Discard;
--------------------------------------------------------------------------------

VID         Ports
--------------------------------------------------------------------------------
  1         UT:100GE1/0/1(D)    100GE1/0/2(D)    GE1/0/1(U)       GE1/0/2(U)
                GE1/0/3(U)       GE1/0/4(D)       GE1/0/5(D)       GE1/0/6(D)
                GE1/0/7(D)       GE1/0/8(D)       GE1/0/9(D)       GE1/0/11(D)
                GE1/0/12(D)      GE1/0/13(D)      GE1/0/15(D)      GE1/0/16(D)
                GE1/0/17(D)      GE1/0/18(D)      GE1/0/19(D)      GE1/0/20(D)
                GE1/0/21(D)      GE1/0/22(D)      GE1/0/23(D)      GE1/0/24(D)
                25GE1/0/1(D)     25GE1/0/2(D)     25GE1/0/3(D)     25GE1/0/4(D)
```

```
  3            UT:GE1/0/1(U)        GE1/0/14(U)
               TG:GE1/0/10(U)
 10            UT:GE1/0/1(U)
               TG:GE1/0/10(U)

VID  Type       Status   Property   MAC-LRN STAT      BC   MC   UC   Description
--------------------------------------------------------------------------------
  1 common     enable   default    enable   disable FWD FWD FWD VLAN 0001
  3 common     enable   default    enable   disable FWD FWD FWD VLAN 0003
 10 common     enable   default    enable   disable FWD FWD FWD VLAN 0010
```

端口前面的 UT、TG 分别代表发送数据帧时，剥离 VLAN 标签（Untagged）和添加 VLAN 标签（Tagged）。

端口后面的 U、D 分别代表接口处于 Up 和 Down 状态。

可以看到 S2 GE1/0/1 端口在发送 VLAN 3 和 VLAN 10 的数据帧时，都会剥离 VLAN 标签。

查看 S2 的 MAC 地址表

```
[S2] display mac-address
Flags: * - Backup
       # - forwarding logical interface, operations cannot be performed based
           on the interface.
BD   : bridge-domain    Age : dynamic MAC learned time in seconds
--------------------------------------------------------------------------------
MAC Address      VLAN/VSI/BD   Learned-From          Type                 Age
--------------------------------------------------------------------------------
b0c7-8733-8c2e 1/-/-           GE1/0/3               dynamic               36
20df-73f5-4332 3/-/-           GE1/0/14              dynamic               33
20df-73f5-4372 3/-/-           GE1/0/10              dynamic               33
b0c7-8733-d661 10/-/-          GE1/0/1               dynamic             1144
--------------------------------------------------------------------------------
Total items: 4
```

可以看到 S2 从 VLAN 3 学习到 S3、S4 的 MAC 地址，从 VLAN 10 学习到 R1 的 MAC 地址。

步骤 6 配置基于 MAC 地址划分 VLAN

S4 模拟移动办公用户，希望可以通过 S2 的 GE1/0/14、GE1/0/15、GE1/0/16 任意一个端口接入网络，并且通过 VLAN 3 进行数据传递。

配置交换机 S2，让 S4 的 MAC 地址与 VLAN 3 关联

基于 MAC 划分 VLAN 指将 MAC 地址与 VLAN 关联，按照报文的源 MAC 地址来定义 VLAN 成员，将指定报文添加该 VLAN 的 Tag 后发送。用户在变换物理位置时，不需要重新划分 VLAN，提高了终端用户的安全性和接入的灵活性。

在之前的步骤中，已获知 S4 的 MAC 地址是 20df-73f5-4332。

```
[S2] vlan 3
[S2-vlan3] mac-vlan mac-address 20df-73f5-4332
[S2-vlan3] quit
```

mac-vlan mac-address 命令用来配置 MAC 地址与 VLAN 关联。

配置交换机 S2 的 GE1/0/14、GE1/0/15、GE1/0/16 接口为 Hybrid 接口，并允许基于 MAC 地址划分的 VLAN 通过当前 Hybrid 接口

在 Access 口和 Trunk 口上，只有基于 MAC 划分的 VLAN 和 PVID 相同时，才可以正常使用。所以基于 MAC 地址划分 VLAN 推荐在 Hybrid 口上配置，可以接收多个 VLAN 不带标签通过。

```
[S2] interface GE 1/0/14
[S2-GE1/0/14] port link-type hybrid
[S2-GE1/0/14] port hybrid untagged vlan 3 10
[S2-GE1/0/14] quit
```

注意：此处接口以不带 Tag 的方式加入 VLAN 10，目的是为了让 S4 和 R1 可以互通。

```
[S2] interface GE 1/0/15
[S2-GE1/0/15] port link-type hybrid
[S2-GE1/0/15] port hybrid untagged vlan 3 10
[S2-GE1/0/15] quit
[S2] interface GE 1/0/16
[S2-GE1/0/16] port link-type hybrid
[S2-GE1/0/16] port hybrid untagged vlan 3 10
[S2-GE1/0/16] quit
```

配置 S2，使能 GE1/0/14、GE1/0/15、GE1/0/16 接口基于 MAC 地址划分 VLAN 的功能

若想使通过接口的报文按照基于 MAC 地址划分的 VLAN 转发，必须使能接口的 MAC VLAN 功能。

```
[S2] interface GE 1/0/14
[S2-GE1/0/14] mac-vlan enable
[S2-GE1/0/14] quit
```

mac-vlan enable 命令用来使能接口的 MAC VLAN 功能。

```
[S2] interface GE 1/0/15
[S2-GE1/0/15] mac-vlan enable
[S2-GE1/0/15] quit
[S2] interface GE 1/0/16
[S2-GE1/0/16] mac-vlan enable
[S2-GE1/0/16] quit
```

步骤 7 查看配置信息

查看交换机的 VLAN 信息

```
[S1] display vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;              D: Down;              TG: Tagged;              UT: Untagged;
MP: Vlan-mapping;                         ST: Vlan-stacking;
#: ProtocolTransparent-vlan;      *: Management-vlan;
MAC-LRN: MAC-address learning;    STAT: Statistic;
BC: Broadcast; MC: Multicast;     UC: Unknown-unicast;
FWD: Forward;    DSD: Discard;
--------------------------------------------------------------------------------

VID              Ports
--------------------------------------------------------------------------------
    1            UT:100GE1/0/1(D)     100GE1/0/2(D)     GE1/0/2(U)        GE1/0/3(U)
                     GE1/0/4(D)        GE1/0/5(D)        GE1/0/6(D)        GE1/0/7(D)
                     GE1/0/8(D)        GE1/0/9(D)        GE1/0/11(D)       GE1/0/12(D)
                     GE1/0/14(D)       GE1/0/15(D)       GE1/0/16(D)       GE1/0/17(D)
                     GE1/0/18(D)       GE1/0/19(D)       GE1/0/20(D)       GE1/0/21(D)
                     GE1/0/22(D)       GE1/0/23(D)       GE1/0/24(D)       25GE1/0/1(D)
                     25GE1/0/2(D)      25GE1/0/3(D)      25GE1/0/4(D)
    3            UT:GE1/0/13(U)
                 TG:GE1/0/10(U)
   10            TG:GE1/0/10(U)

VID  Type        Status    Property    MAC-LRN STAT      BC    MC    UC    Description
--------------------------------------------------------------------------------
    1 common     enable    default     enable    disable FWD FWD FWD VLAN 0001
    3 common     enable    default     enable    disable FWD FWD FWD VLAN 0003
   10 common     enable    default     enable    disable FWD FWD FWD VLAN 0010
```

```
[S2] display vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;              D: Down;              TG: Tagged;              UT: Untagged;
MP: Vlan-mapping;                         ST: Vlan-stacking;
#: ProtocolTransparent-vlan;      *: Management-vlan;
MAC-LRN: MAC-address learning;    STAT: Statistic;
BC: Broadcast; MC: Multicast;     UC: Unknown-unicast;
FWD: Forward;    DSD: Discard;
--------------------------------------------------------------------------------

VID              Ports
--------------------------------------------------------------------------------
    1            UT:100GE1/0/1(D)     100GE1/0/2(D)     GE1/0/1(U)        GE1/0/2(U)
```

```
                  GE1/0/3(U)      GE1/0/4(D)      GE1/0/5(D)      GE1/0/6(D)
                  GE1/0/7(D)      GE1/0/8(D)      GE1/0/9(D)      GE1/0/11(D)
                  GE1/0/12(D)     GE1/0/13(D)     GE1/0/14(U)     GE1/0/15(D)
                  GE1/0/16(D)     GE1/0/17(D)     GE1/0/18(D)     GE1/0/19(D)
                  GE1/0/20(D)     GE1/0/21(D)     GE1/0/22(D)     GE1/0/23(D)
                  GE1/0/24(D)     25GE1/0/1(D)    25GE1/0/2(D)    25GE1/0/3(D)
                  25GE1/0/4(D)
  3          UT:GE1/0/1(U)      GE1/0/14(U)     GE1/0/15(D)     GE1/0/16(D)
             TG:GE1/0/10(U)
  10         UT:GE1/0/1(U)      GE1/0/14(U)     GE1/0/15(D)     GE1/0/16(D)
             TG:GE1/0/10(U)

VID  Type        Status  Property  MAC-LRN STAT      BC   MC   UC   Description
--------------------------------------------------------------------------------
   1 common    enable  default   enable  disable FWD  FWD  FWD  VLAN 0001
   3 common    enable  default   enable  disable FWD  FWD  FWD  VLAN 0003
  10 common    enable  default   enable  disable FWD  FWD  FWD  VLAN 0010
```

查看交换机的 MAC-VLAN 信息

```
[S2] display mac-vlan vlan 3
Total MAC VLAN address count: 1
------------------------------------------------
MAC Address       Mask              VLAN      Priority
------------------------------------------------
20df-73f5-4332    ffff-ffff-ffff    3         0
```

display mac-vlan 命令用来查看基于 MAC 地址划分 VLAN 的配置信息。

（可选）验证基于 MAC 划分 VLAN 的结果

调整交换机物理连线，将 S4 的 GE1/0/2 接口连接到 S2 的 GE1/0/15 或者 GE1/0/16 端口。

连接完成后，可以发现 S4 无论连接哪一个接口，S2 无需新增任何配置，S4 均可通过 VLAN 3 进行数据传递。

2.3 结果验证

检测设备连通性，验证 VLAN 配置结果。

在 S4 Ping S3 和 R1

```
<S4> ping 192.168.1.3
  PING 192.168.1.3: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.3: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=3 ttl=254 time=1 ms
```

```
    Reply from 192.168.1.3: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.1.3: bytes=56 Sequence=5 ttl=254 time=1 ms

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

```
<S4> ping 192.168.1.251
  PING 192.168.1.251: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.251: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 192.168.1.251: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 192.168.1.251: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.1.251: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 192.168.1.251: bytes=56 Sequence=5 ttl=255 time=1 ms

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

在 R1 Ping S3

```
<R1> ping 192.168.1.3
  PING 192.168.1.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

查看交换机的 MAC 地址表

```
[S1] display mac-address
Flags: * - Backup
       # - forwarding logical interface, operations cannot be performed based
           on the interface.
BD    : bridge-domain    Age : dynamic MAC learned time in seconds
--------------------------------------------------------------------------------
MAC Address      VLAN/VSI/BD    Learned-From          Type                  Age
```

```
--------------------------------------------------------------------------------
b0c7-8733-8c2e 1/-/-          GE1/0/2                dynamic              172
b0c7-8733-9786 1/-/-          GE1/0/3                dynamic              167
20df-73f5-4332 3/-/-          GE1/0/10               dynamic              174
20df-73f5-4372 3/-/-          GE1/0/13               dynamic              174
b0c7-8733-d661 10/-/-         GE1/0/10               dynamic              123
--------------------------------------------------------------------------------
Total items: 5
```

```
[S2] display mac-address
Flags: * - Backup
           # - forwarding logical interface, operations cannot be performed based
                on the interface.
BD    : bridge-domain     Age : dynamic MAC learned time in seconds
--------------------------------------------------------------------------------
MAC Address       VLAN/VSI/BD     Learned-From           Type                 Age
--------------------------------------------------------------------------------
20df-73f5-4332 3/-/-          GE1/0/14               dynamic              191
20df-73f5-4372 3/-/-          GE1/0/10               dynamic              342
b0c7-8733-d661 10/-/-         GE1/0/1                dynamic              2604
--------------------------------------------------------------------------------
Total items: 3
```

2.4 配置参考

2.4.1 S1 的配置

```
sysname S1
#
vlan batch 3 10
#
interface GE1/0/1
 undo portswitch
 shutdown
#
interface GE1/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 10
#
interface GE1/0/11
 shutdown
 port link-type access
#
```

```
interface GE1/0/12
 shutdown
 port link-type access
#
interface GE1/0/13
 port link-type access
 port default vlan 3
#
interface GE1/0/14
 shutdown
 port link-type access
#
```

2.4.2 S2 的配置

```
sysname S2
#
vlan batch 3 10
#
vlan 3
 mac-vlan mac-address 20df-73f5-4332
#
interface GE1/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 3 10
#
interface GE1/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 10
#
interface GE1/0/11
 shutdown
 port link-type access
#
interface GE1/0/12
 shutdown
 port link-type access
#
interface GE1/0/13
 shutdown
 port link-type access
#
interface GE1/0/14
 port link-type hybrid
```

```
 port hybrid untagged vlan 3 10
 mac-vlan enable
#
interface GE1/0/15
 port link-type hybrid
 port hybrid untagged vlan 3 10
 mac-vlan enable
#
interface GE1/0/16
 port link-type hybrid
 port hybrid untagged vlan 3 10
 mac-vlan enable
#
```

2.4.3 S3 的配置

```
sysname S3
#
interface GE1/0/1
 undo portswitch
 ip address 192.168.1.3 255.255.255.0
#
interface GE1/0/2
 shutdown
 port link-type access
#
interface GE1/0/3
 shutdown
 port link-type access
#
interface GE1/0/4
 shutdown
 port link-type access
#
```

2.4.4 S4 的配置

```
sysname S4
#
interface GE1/0/1
 shutdown
 port link-type access
#
interface GE1/0/2
 undo portswitch
```

```
 ip address 192.168.1.4 255.255.255.0
#
interface GE1/0/3
 shutdown
 port link-type access
#
interface GE1/0/4
 shutdown
 port link-type access
#
```

2.4.5 R1 的配置

```
sysname R1
#
interface GE0/0/2
 ip address 192.168.1.251 255.255.255.0
#
```

2.5 思考题

1. 在步骤 2 中，R1 能够 Ping 通 S3 和 S4，为什么?

答案：因为 S1 和 S2 所有接口状态默认属于同一个 VLAN，VLAN ID 为 1，因此 R1 能够 Ping 通 S3 和 S4。

2. 如果要求 R1 和 S3 能够相互 Ping 通，请问应该如何实现?

答案：可以将 S1 的 GE1/0/13 接口修改为 Hybrid 接口，并且以 Untag 方式发送 VLAN 10 的数据帧。

3 生成树配置实验

3.1 实验介绍

3.1.1 关于本实验

交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了 STP（Spanning Tree Protocol，生成树协议）。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 IEEE 802.1D 中定义的 STP 到 IEEE 802.1W 中定义的 RSTP（Rapid Spanning Tree Protocol，快速生成树协议），再到最新的 IEEE 802.1S 中定义的 MSTP（Multiple Spanning Tree Protocol，多生成树协议）。

本实验将通过完成 STP 的基本配置，帮助学员掌握 STP 的配置和原理，以及部分 RSTP 特性。

3.1.2 实验目的

- 掌握启用和禁用 STP/RSTP 的方法
- 掌握修改交换机 STP 模式的方法
- 掌握修改桥优先级，控制根桥选举的方法
- 掌握修改端口优先级，控制根端口和指定端口选举的方法
- 掌握修改端口开销，控制根端口和指定端口选举的方法
- 掌握边缘端口的配置方法
- 掌握启用和禁用 RSTP 的配置方法

3.1.3 实验组网介绍

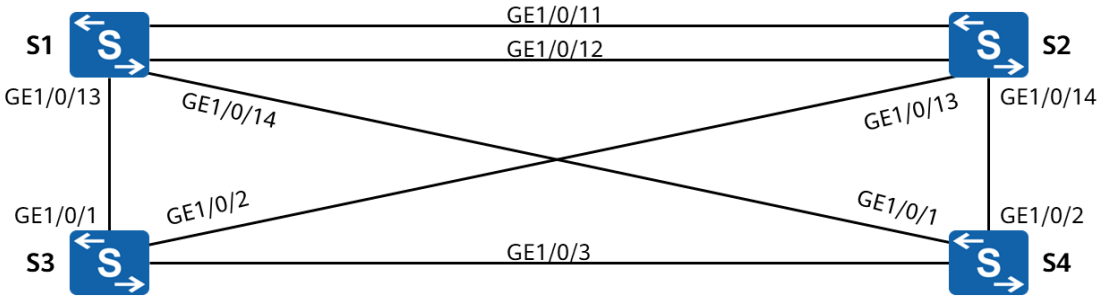


图3-1 生成树配置实验拓扑

3.1.4 实验背景

某公司的二层交换网络中，为了提高网络可靠性，故在二层交换网络中增加冗余链路。为了阻止冗余链路可能带来的广播风暴，MAC 地址漂移等负面影响，需要在交换机之间部署生成树协议。

说明：由于交换机的 MAC 地址不同，STP 的计算结果在不同的物理环境中会有所不同，请以您使用的组网环境为准。

3.2 实验任务配置

3.2.1 配置思路

1. 使能设备上的 STP 功能
2. 修改桥优先级来控制根桥的选举
3. 修改接口参数来控制端口角色
4. 修改设备运行 RSTP 协议
5. 配置 RSTP 边缘端口

3.2.2 配置步骤

步骤 1 关闭多余接口

#关闭 S1、S2、S3、S4 的接口

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] shutdown
```

```
[S1-GE1/0/1] quit
[S1] interface GE 1/0/10
[S1-GE1/0/10] shutdown
[S1-GE1/0/10] quit
```

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] shutdown
[S2-GE1/0/1] quit
[S2] interface GE 1/0/10
[S2-GE1/0/10] shutdown
[S2-GE1/0/10] quit
```

```
[S3] interface GE 1/0/4
[S3-GE1/0/4] shutdown
[S3-GE1/0/4] quit
```

```
[S4] interface GE 1/0/4
[S4-GE1/0/4] shutdown
[S4-GE1/0/4] quit
```

步骤 2 配置设备运行 STP

全局使能 STP 功能

```
[S1] stp enable
```

stp enable 命令用来使能交换设备或端口上的 STP/RSTP/MSTP 功能。缺省情况下，交换设备上的 STP 功能处于启用状态。

修改当前生成树工作模式为 STP

```
[S1] stp mode stp
```

stp mode {**mstp** | **rstp** | **stp**}命令用来配置交换设备的生成树协议工作模式。缺省情况下，设备的生成树工作模式为 MSTP 模式。当前设备的生成树模式已经被修改为 STP。

```
[S2] stp mode stp
```

```
[S3] stp mode stp
```

```
[S4] stp mode stp
```

查看生成树的状态，以 S1 为例

```
[S1] display stp
CIST Global Information:
  Mode                  :STP
  CIST Bridge           :32768.20df-73f5-44e1          //本设备的桥 ID
  Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  CIST Root/ERPC        :32768.20df-73f5-4331 / 20000      //根桥的桥 ID 和到根桥的 Cost
  CIST RegRoot/IRPC     :32768.20df-73f5-44e1 / 0 (This bridge is the root)
  CIST RootPortId       :128.14 (GE1/0/14)
  BPDU-Protection       :Disabled
  TC or TCN received    :45
  TC count per hello    :1
  STP Converge Mode     :Normal
  Share region-configuration :Enabled
  Time since last TC    :0 days 0h:0m:31s
  Number of TC          :16
  Last TC occurred      :GE1/0/14
  Topo Change Flag      :0
```

显示信息还包括各个接口的状态，在上述输出中已经按<Ctrl+C>结束显示。

查看各交换机上生成树的状态信息摘要

```
[S1] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
     0   GE1/0/11                    DESI  forwarding    none          20000     disable
     0   GE1/0/12                    DESI  forwarding    none          20000     disable
     0   GE1/0/13                    ALTE  discarding    none          20000     disable
     0   GE1/0/14                    ROOT  forwarding    none          20000     disable
```

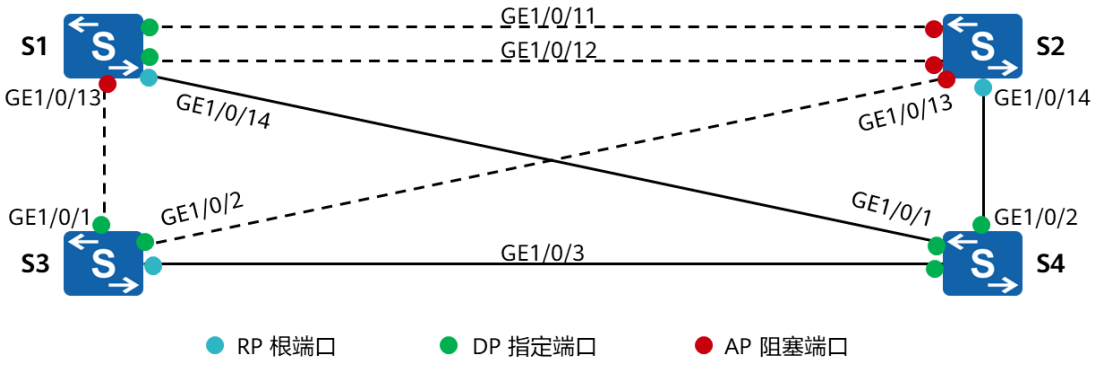
```
[S2] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
     0   GE1/0/11                    ALTE  discarding    none          20000     disable
     0   GE1/0/12                    ALTE  discarding    none          20000     disable
     0   GE1/0/13                    ALTE  discarding    none          20000     disable
     0   GE1/0/14                    ROOT  forwarding    none          20000     disable
```

```
[S3] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
     0   GE1/0/1                     DESI  forwarding    none          20000     disable
     0   GE1/0/2                     DESI  forwarding    none          20000     disable
     0   GE1/0/3                     ROOT  forwarding    none          20000     disable
```

```
[S4] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
     0   GE1/0/1                     DESI  forwarding    none          20000     disable
```

```
0   GE1/0/2          DESI   forwarding   none          20000   disable
0   GE1/0/3          DESI   forwarding   none          20000   disable
```

综合根桥 ID 信息以及各个交换机上的端口信息，可得当前拓扑如下：



虚线代表该链路不转发业务数据。

注：该拓扑仅供参考，不一定与实际实验环境中的生成树拓扑相同。

步骤 3 修改设备参数，使得 S1 成为根桥，S2 成为备份根桥

修改 S1 和 S2 的桥优先级

```
[S1] stp root primary
```

由于根桥在网络中的重要性，在根桥选举过程中，通常希望性能高、网络层次高的交换设备被选举为根桥。但是，性能高、网络层次高的交换设备其优先级不一定高，可以通过执行命令配置其为根桥。**stp root** 命令用来配置当前交换设备为指定生成树的根桥或备份根桥。

执行 **stp root primary** 命令指定当前交换设备为根桥，则表示该设备在指定生成树中的优先级为 0，且优先级不能修改。

```
[S2] stp root secondary
```

执行 **stp root secondary** 命令指定当前交换设备在指定生成树中为备份根桥，则表示该设备的优先级数值为 4096，且优先级不能修改。

在 S1 上查看当前 STP 状态

```
[S1] display stp
CIST Global Information:
  Mode                 :STP
  CIST Bridge          :0.20df-73f5-44e1
  Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  CIST Root/ERPC       :0.20df-73f5-44e1 / 0 (This bridge is the root)
  CIST RegRoot/IRPC    :0.20df-73f5-44e1 / 0 (This bridge is the root)
```

```
  CIST RootPortId        :0.0
  BPDU-Protection        :Disabled
  CIST Root Type         :Primary root
  TC or TCN received     :94
  TC count per hello     :0
  STP Converge Mode      :Normal
  Share region-configuration :Enabled
  Time since last TC     :0 days 0h:0m:1s
  Number of TC           :23
  Last TC occurred       :GE1/0/11
  Topo Change Flag       :0
```

此时自身桥 ID 与根桥 ID 相同，且根路径开销为 0，说明 S1 是当前网络的根桥。

在所有设备上查看 STP 状态摘要

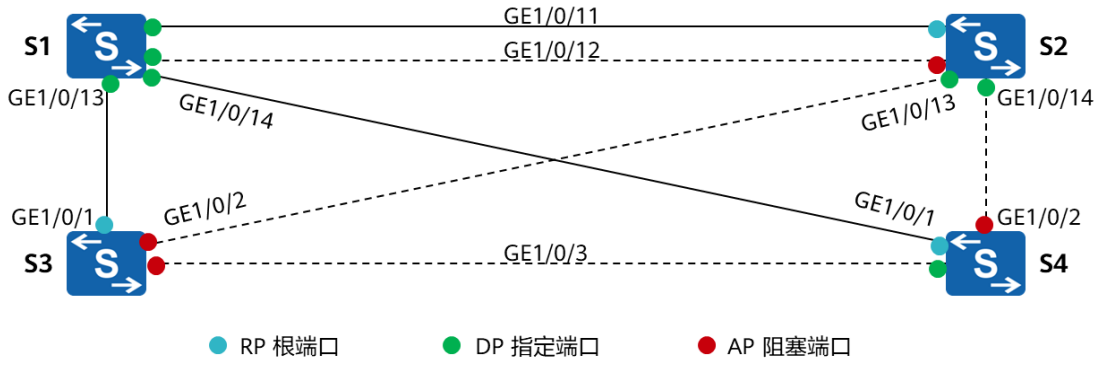
```
[S1] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
     0   GE1/0/11                    DESI  forwarding    none          20000     disable
     0   GE1/0/12                    DESI  forwarding    none          20000     disable
     0   GE1/0/13                    DESI  forwarding    none          20000     disable
     0   GE1/0/14                    DESI  forwarding    none          20000     disable
```

```
[S2] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
     0   GE1/0/11                    ROOT  forwarding    none          20000     disable
     0   GE1/0/12                    ALTE  discarding    none          20000     disable
     0   GE1/0/13                    DESI  forwarding    none          20000     disable
     0   GE1/0/14                    DESI  forwarding    none          20000     disable
```

```
[S3] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
     0   GE1/0/1                     ROOT  forwarding    none          20000     disable
     0   GE1/0/2                     ALTE  discarding    none          20000     disable
     0   GE1/0/3                     ALTE  discarding    none          20000     disable
```

```
[S4] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
     0   GE1/0/1                     ROOT  forwarding    none          20000     disable
     0   GE1/0/2                     ALTE  discarding    none          20000     disable
     0   GE1/0/3                     DESI  forwarding    none          20000     disable
```

综合根桥 ID 信息以及各个交换机上的端口信息，可得当前拓扑如下：



步骤 4 修改设备参数，使得 S4 的 GE1/0/2 接口成为根端口

查看 S4 上的 STP 状态信息

```
[S4] display stp
CIST Global Information:
  Mode                    :STP
  CIST Bridge             :32768.20df-73f5-4331
  Config Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  Active Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  CIST Root/ERPC          :0.20df-73f5-44e1 / 20000
  CIST RegRoot/IRPC       :32768.20df-73f5-4331 / 0 (This bridge is the root)
  CIST RootPortId         :128.1 (GE1/0/1)
  BPDU-Protection         :Disabled
  TC or TCN received      :96
  TC count per hello      :0
  STP Converge Mode       :Normal
  Share region-configuration :Enabled
  Time since last TC      :0 days 0h:6m:49s
  Number of TC            :18
  Last TC occurred        :GE1/0/1
  Topo Change Flag        :0
```

当前 S4 到 S1 的根路径开销为 20000。

修改 S4 的 GE 1/0/1 的 STP 开销值为 50000

```
[S4] interface GE 1/0/1
[S4-GE1/0/1] stp cost 50000
[S4-GE1/0/1] quit
```

查看当前 STP 状态信息摘要

```
[S4] display stp brief
 MSTID   Port                        Role  STP State     Protection    Cost      Edged
```

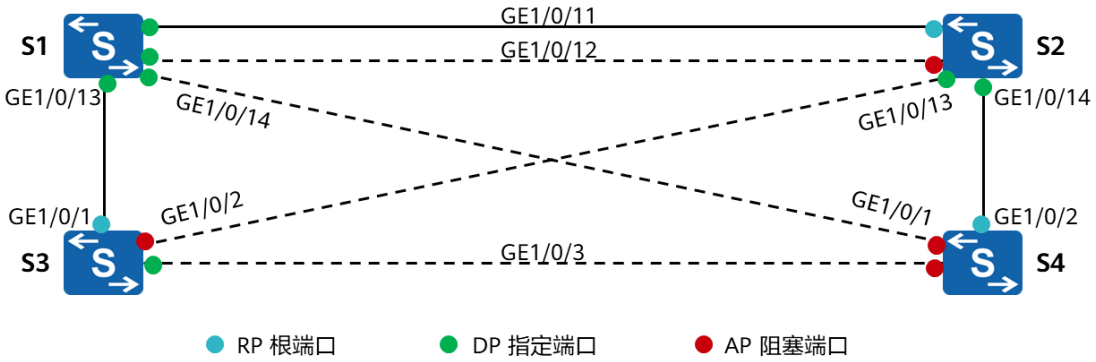
```
0   GE1/0/1          ALTE   discarding    none          50000    disable
0   GE1/0/2          ROOT   forwarding    none          20000    disable
0   GE1/0/3          ALTE   discarding    none          20000    disable
```

S4 的 GE1/0/2 接口已经成为根端口。

查看当前 STP 状态信息

```
[S4] display stp
CIST Global Information:
  Mode                  :STP
  CIST Bridge           :32768.20df-73f5-4331
  Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  CIST Root/ERPC        :0.20df-73f5-44e1 / 40000     //S4 到根桥的 Cost 值为 40000
  CIST RegRoot/IRPC     :32768.20df-73f5-4331 / 0 (This bridge is the root)
  CIST RootPortId       :128.2 (GE1/0/2)
  BPDU-Protection       :Disabled
  TC or TCN received    :178
  TC count per hello    :8
  STP Converge Mode     :Normal
  Share region-configuration :Enabled
  Time since last TC    :0 days 0h:0m:5s
  Number of TC          :22
  Last TC occurred      :GE1/0/2
  Topo Change Flag      :0
```

当前拓扑如下：



步骤 5 修改当前生成树工作模式为 RSTP

修改所有设备的生成树模式

```
[S1] stp mode rstp
```

```
[S2] stp mode rstp
```

```
[S3] stp mode rstp
```

```
[S4] stp mode rstp
```

查看设备上的生成树状态，仅以 S1 为例

```
[S1] display stp
CIST Global Information:
  Mode                  :RSTP
  CIST Bridge           :0.20df-73f5-44e1
  Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  CIST Root/ERPC        :0.20df-73f5-44e1 / 0 (This bridge is the root)
  CIST RegRoot/IRPC     :0.20df-73f5-44e1 / 0 (This bridge is the root)
  CIST RootPortId       :0.0
  BPDU-Protection       :Disabled
  CIST Root Type        :Primary root
  TC or TCN received    :97
  TC count per hello    :0
  STP Converge Mode     :Normal
  Share region-configuration :Enabled
  Time since last TC    :0 days 0h:5m:29s
  Number of TC          :26
  Last TC occurred      :GE1/0/11
  Topo Change Flag      :0
```

模式修改后，对生成树的整体拓扑无影响。

步骤 6 配置边缘端口

S3 的 GE 1/0/10-1/0/24 确认只会连接终端设备，需要被配置为边缘端口

```
[S3] interface range GE 1/0/10 to GE 1/0/24
```

通常，设备的以太网接口数比较多，并且在很多以太网接口下有相同的配置。如果对这些以太网接口进行逐个配置会较为繁琐，且容易输入错误。因此，将需要执行相同配置命令的以太网接口加入到一个临时端口组，在临时端口组配置命令时，系统会自动到临时端口组绑定的所有成员接口下执行这些命令行，完成以太网接口批量配置。

注：某些产品可能不支持临时接口组，需要对接口做单独配置。

```
[S3-port-group] stp edged-port enable
```

stp edged-port enable 命令用来配置当前端口为边缘端口。当前端口配置成边缘端口后，如果收到 BPDU 报文，交换设备会自动将边缘端口设置为非边缘端口，并重新进行生成树计算。

3.3 结果验证

1. 请根据实际收敛情况，标识出您使用的实验环境中的根桥以及端口角色。
2. 关闭任意交换机上的任意端口，观察是否能通过备份链路到达其它所有交换机。

3.4 配置参考

3.4.1 S1 的配置

```
sysname S1
#
stp mode rstp
stp instance 0 root primary
#
interface GE1/0/1
 shutdown
 port link-type access
#
interface GE1/0/10
 shutdown
 port link-type access
#
```

3.4.2 S2 的配置

```
sysname S2
#
stp mode rstp
stp instance 0 root secondary
#
interface GE1/0/1
 shutdown
 port link-type access
#
interface GE1/0/10
 shutdown
```

```
 port link-type access
#
```

3.4.3 S3 的配置

```
sysname S3
#
stp mode rstp
#
interface GE1/0/4
 shutdown
 port link-type access
#
interface GE1/0/10
 port link-type access
 stp edged-port enable
#
interface GE1/0/11
 port link-type access
 stp edged-port enable
#
interface GE1/0/12
 port link-type access
 stp edged-port enable
#
interface GE1/0/13
 port link-type access
 stp edged-port enable
#
interface GE1/0/14
 port link-type access
 stp edged-port enable
#
interface GE1/0/15
 port link-type access
 stp edged-port enable
#
interface GE1/0/16
 port link-type access
 stp edged-port enable
#
interface GE1/0/17
 port link-type access
 stp edged-port enable
#
interface GE1/0/18
```

```
 port link-type access
 stp edged-port enable
#
interface GE1/0/19
 port link-type access
 stp edged-port enable
#
interface GE1/0/20
 port link-type access
 stp edged-port enable
#
interface GE1/0/21
 port link-type access
 stp edged-port enable
#
interface GE1/0/22
 port link-type access
 stp edged-port enable
#
interface GE1/0/23
 port link-type access
 stp edged-port enable
#
interface GE1/0/24
 port link-type access
 stp edged-port enable
#
```

3.4.4 S4 的配置

```
sysname S4
#
stp mode rstp
#
interface GE1/0/1
 port link-type access
 stp instance 0 cost 50000
#
interface GE1/0/4
 shutdown
 port link-type access
#
```

3.5 思考题

1. S1 与 S2 之间的两条链路能否同时处于转发状态？为什么？

答案：不能，因为 S1 和 S2 之间的链路同时处于转发状态就构成了环路，所以必须有一条链路被阻塞。

4 以太网链路聚合实验

4.1 实验介绍

4.1.1 关于本实验

随着网络规模不断扩大，用户对骨干链路的带宽和可靠性提出越来越高的要求。在传统技术中，常用更换高速率的接口板或更换支持高速率接口板的设备的方式来增加带宽，但这种方案需要付出高额的费用，而且不够灵活。

采用链路聚合技术可以在不进行硬件升级的条件下，通过将多个物理接口捆绑为一个逻辑接口，达到增加链路带宽的目的。在实现增大带宽目的的同时，链路聚合采用备份链路的机制，可以有效的提高设备之间链路的可靠性。

链路聚合技术主要有以下三个优势：

- 增加带宽：链路聚合接口的最大带宽可以达到各成员接口带宽之和。
- 提高可靠性：当某条活动链路出现故障时，流量可以切换到其它可用的成员链路上，从而提高链路聚合接口的可靠性。
- 负载分担：在一个链路聚合组内，可以实现在各成员活动链路上的负载分担。

本实验将通过手工和 LACP 模式的以太网链路聚合的配置，帮助学员了解以太网链路聚合技术的配置及原理。

4.1.2 实验目的

- 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
- 掌握控制静态 LACP 模式下控制活动链路的方法
- 掌握静态 LACP 的部分特性的配置

4.1.3 实验组网介绍

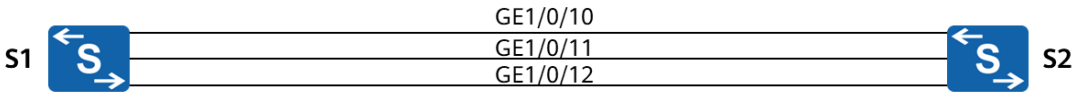


图4-1 以太网链路聚合实验拓扑

4.1.4 实验背景

在生成树实验中，S1 与 S2 之间的两条链路无法同时处于数据转发的状态。为了充分利用这两条链路的带宽，需要在 S1 和 S2 之间配置以太网链路聚合。

4.2 实验任务配置

4.2.1 配置思路

1. 配置手工模式链路聚合
2. 配置 LACP 模式链路聚合
3. 通过修改参数控制活动链路
4. 修改负载分担方式

4.2.2 配置步骤

步骤 1 配置手工链路聚合

创建 Eth-Trunk 接口

```
[S1] interface Eth-Trunk 1
```

interface eth-trunk 命令用来进入已经存在的 Eth-Trunk 接口，或创建并进入 Eth-Trunk 接口。数字 1 代表接口编号，编号范围根据设备情况有所不同。

```
[S2] interface Eth-Trunk 1
```

设置 Eth-Trunk 接口的聚合模式

```
[S1-Eth-Trunk1] mode manual load-balance
[S1-Eth-Trunk1] quit
```

mode 命令用来配置 Eth-Trunk 的工作模式，缺省情况下，Eth-Trunk 的工作模式为手工负载分担模式。

将成员接口加入聚合组

```
[S1] interface GE 1/0/10
[S1-GE1/0/10] undo port link-type
[S1-GE1/0/10] eth-trunk 1
[S1-GE1/0/10] quit
[S1] interface GE 1/0/11
[S1-GE1/0/11] undo port link-type
[S1-GE1/0/11] eth-trunk 1
[S1-GE1/0/11] quit
[S1] interface GE 1/0/12
[S1-GE1/0/12] undo port link-type
[S1-GE1/0/12] eth-trunk 1
[S1-GE1/0/12] quit
```

可进入到成员接口的接口视图下，逐一添加到 Eth-Trunk 接口。也可以在 Eth-Trunk 接口视图下通过 **trunkport** 命令批量添加接口。

```
[S2] interface GE 1/0/10
[S2-GE1/0/10] undo port link-type
[S2-GE1/0/10] quit
[S2] interface GE 1/0/11
[S2-GE1/0/11] undo port link-type
[S2-GE1/0/11] quit
[S2] interface GE 1/0/12
[S2-GE1/0/12] undo port link-type
[S2-GE1/0/12] quit
[S2] interface Eth-Trunk 1
[S2-Eth-Trunk1] trunkport GE 1/0/10 to 1/0/12
[S2-Eth-Trunk1] quit
```

将成员接口加入 Eth-Trunk 时，需要注意以下事项：

1. Eth-Trunk 接口不能嵌套，即 Eth-Trunk 接口的成员接口不能是 Eth-Trunk 接口。
2. 一个以太网接口只能加入到一个 Eth-Trunk 接口，如果需要加入其它 Eth-Trunk 接口，必须先退出原来的 Eth-Trunk 接口。
3. 如果本地设备使用了 Eth-Trunk，与成员接口直连的对端接口也必须捆绑为 Eth-Trunk 接口，两端才能正常通信。

查看 Eth-Trunk 接口状态

```
[S1] display eth-trunk 1
Eth-Trunk1's state information is:
Working Mode: Normal              Hash Arithmetic: src-dst-ip
```

```
Least Active-linknumber: 1     Max Bandwidth-affected-linknumber: 128
Operating Status: up           Number of Up Ports in Trunk: 3
--------------------------------------------------------------------------------
PortName                       Status      Weight
GE1/0/10                       Up          1
GE1/0/11                       Up          1
GE1/0/12                       Up          1
```

Eth-Trunk 接口的工作模式：

1. Normal：手工负载分担模式。
2. Static：静态 LACP 模式。
3. Dynamic：动态 LACP 模式。

步骤 2 配置 LACP 模式的链路聚合

删除现有 Eth-Trunk 接口下的成员接口

```
[S1] interface Eth-Trunk 1
[S1-Eth-Trunk1] undo trunkport GE 1/0/10 to 1/0/12
[S1-Eth-Trunk1] quit
```

```
[S2] interface Eth-Trunk 1
[S2-Eth-Trunk1] undo trunkport GE 1/0/10 to 1/0/12
[S2-Eth-Trunk1] quit
```

在修改 Eth-Trunk 接口的聚合模式之前，需要确保 Eth-Trunk 中没有任何成员接口。

修改聚合模式

```
[S1] interface Eth-Trunk 1
[S1-Eth-Trunk1] mode lacp-static
[S1-Eth-Trunk1] quit
```

mode lacp-static 指定 Eth-Trunk 接口工作模式为静态 LACP 模式。

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

将成员接口加入聚合组

```
[S1] interface Eth-Trunk 1
[S1-Eth-Trunk1] trunkport GE 1/0/10 to 1/0/12
[S1-Eth-Trunk1] quit
```

```
[S2] interface Eth-Trunk 1
```

```
[S2-Eth-Trunk1] trunkport GE 1/0/10 to 1/0/12
[S2-Eth-Trunk1] quit
```

查看 Eth-Trunk 接口状态

```
[S1] display eth-trunk 1

Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                         Working Mode: Static
Preempt Delay: Disabled           Hash Arithmetic: src-dst-ip
System Priority: 32768            System ID: 20df-73f5-44e1
Least Active-linknumber: 1        Max Active-linknumber: 128
Operating Status: up              Number Of Up Ports In Trunk: 3
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName                 Status     PortType PortPri PortNo PortKey PortState Weight
GE1/0/10(hr)                  Selected 1GE       32768    1       305     10111100  1
GE1/0/11(h)                   Selected 1GE       32768    2       305     10111100  1
GE1/0/12(h)                   Selected 1GE       32768    3       305     10111100  1

Partner:
--------------------------------------------------------------------------------
ActorPortName                 SysPri     SystemID         PortPri PortNo PortKey PortState
GE1/0/10                      32768      20df-73f5-4571   32768   1      305     10111100
GE1/0/11                      32768      20df-73f5-4571   32768   2      305     10111100
GE1/0/12                      32768      20df-73f5-4571   32768   3      305     10111100
```

步骤 3 配置活动接口数量

考虑到网络流量情况，当网络正常时，只需要 GE1/0/11 和 GE1/0/12 接口处于转发状态，GE1/0/10 接口作为备份。但当活动接口数量少于 2 时，直接关闭整个 Eth-Trunk 接口。

配置设备 S1 的 LACP 优先级，使其成为主动端设备

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

配置接口优先级，优选 GE1/0/11 和 GE1/0/12 接口

```
[S1] interface GE 1/0/10
[S1-GE1/0/10] lacp priority 40000
[S1-GE1/0/10] quit
```

使能了 LACP 模式链路聚合的两端设备均会收发 LACPDU 报文。

首先选举主动端设备：

1. 比较系统优先级字段，如果对端的系统优先级高于本端的系统优先级（默认为 32768，越小越优），则确定对端为 LACP 主动端。
2. 如果系统优先级相同，比较两端设备的 MAC 地址，MAC 地址小的一端为 LACP 主动端。
3. 选出主动端后，两端都会以主动端的接口优先级来选择活动接口，接口优先级越小越优，默认为 32768。

配置 Eth-trunk 活动接口数上限阈值和下限阈值

```
[S1] interface Eth-Trunk 1
[S1-Eth-Trunk1] lacp max active-linknumber 2
[S1-Eth-Trunk1] least active-linknumber 2
[S1-Eth-Trunk1] quit
```

在一个 Eth-Trunk 接口内，活动接口数可以影响到 Eth-Trunk 接口的状态和带宽。Eth-Trunk 接口的带宽是所有处于 Up 状态的成员口带宽之和。为保证 Eth-Trunk 接口的状态和带宽，可以设置以下两个阈值，以减小成员链路状态的变化带来的影响。

活动接口数下限阈值：当活动接口数小于配置的下限阈值时，Eth-Trunk 接口的状态转为 Down。设置活动接口数下限阈值的目的是为了保证最小带宽。**least active-linknumber** 命令用来配置链路聚合组活动接口数目的下限阈值。

活动接口数上限阈值：当活动接口数达到上限阈值后，之后再发生成员链路状态变为 Up 都不会使 Eth-Trunk 接口的带宽增加。设置活动接口数上限阈值的目的是在保证了带宽的情况下提高网络的可靠性。**lacp max active-linknumber** 命令用来配置链路聚合组活动接口数目的上限阈值。

开启抢占功能

```
[S1] interface Eth-Trunk 1
[S1-Eth-Trunk1] lacp preempt enable
[S1-Eth-Trunk1] quit
```

在 LACP 模式下，当活动链路中出现故障链路时，系统会从备用链路中选择优先级最高的链路替代故障链路；如果被替代的故障链路恢复了正常，而且该链路的优先级又高于替代自己的链路。这种情况下，如果使能了 LACP 优先级抢占功能，高优先级链路会抢占低优先级链路，回切到活动状态。**lacp preempt enable** 命令用来使能 LACP 模式下 LACP 优先级抢占的功能，缺省情况下，优先级抢占处于禁止状态。

查看当前 Eth-Trunk 接口状态

```
[S1] display eth-trunk 1

Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                         Working Mode: Static
```

```
Preempt Delay Time: 30          Hash Arithmetic: src-dst-ip
System Priority: 100            System ID: 20df-73f5-44e1
Least Active-linknumber: 2      Max Active-linknumber: 2
Operating Status: up            Number Of Up Ports In Trunk: 2
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName          Status     PortType PortPri PortNo PortKey PortState Weight
GE1/0/10(h)            Unselect 1GE       40000    1       305     10100000  1
GE1/0/11(hr)           Selected 1GE       32768    2       305     10111100  1
GE1/0/12(h)            Selected 1GE       32768    3       305     10111100  1

Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri     SystemID          PortPri PortNo PortKey PortState
GE1/0/10               32768      20df-73f5-4571    32768   1      305     10100000
GE1/0/11               32768      20df-73f5-4571    32768   2      305     10111100
GE1/0/12               32768      20df-73f5-4571    32768   3      305     10111100
```

当前 GE1/0/11 和 GE1/0/12 处于激活状态。

手工关闭 GE1/0/12 模拟链路故障

```
[S1] interface GE 1/0/12
[S1-GE1/0/12] shutdown
[S1-GE1/0/12] quit
```

```
[S1] display eth-trunk 1

Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                       Working Mode: Static
Preempt Delay Time: 30          Hash Arithmetic: src-dst-ip
System Priority: 100            System ID: 20df-73f5-44e1
Least Active-linknumber: 2      Max Active-linknumber: 2
Operating Status: up            Number Of Up Ports In Trunk: 2
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName          Status     PortType PortPri PortNo PortKey PortState Weight
GE1/0/10(h)            Selected 1GE       40000    1       305     10111100  1
GE1/0/11(hr)           Selected 1GE       32768    2       305     10111100  1
GE1/0/12               Unselect 1GE       32768    3       305     10100010  1

Partner:
```

```
--------------------------------------------------------------------------------
ActorPortName                SysPri    SystemID        PortPri PortNo PortKey PortState
GE1/0/10                     32768     20df-73f5-4571  32768   1      305     10111100
GE1/0/11                     32768     20df-73f5-4571  32768   2      305     10111100
GE1/0/12                     0         0000-0000-0000  0       0      0       10100011
```

GE1/0/10 已经转为激活状态。

再手工关闭 GE1/0/11 模拟链路故障

```
[S1] interface GE 1/0/11
[S1-GE1/0/11] shutdown
[S1-GE1/0/11] quit
```

```
[S1] display eth-trunk 1

Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                         Working Mode: Static
Preempt Delay Time: 30            Hash Arithmetic: src-dst-ip
System Priority: 100              System ID: 20df-73f5-44e1
Least Active-linknumber: 2        Max Active-linknumber: 2
Operating Status: down            Number Of Up Ports In Trunk: 0
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName                Status    PortType PortPri PortNo PortKey PortState Weight
GE1/0/10(h)                  Unselect  1GE      40000   1      305     10100000  1
GE1/0/11                     Unselect  1GE      32768   2      305     10100010  1
GE1/0/12                     Unselect  1GE      32768   3      305     10100010  1

Partner:
--------------------------------------------------------------------------------
ActorPortName                SysPri    SystemID        PortPri PortNo PortKey PortState
GE1/0/10                     32768     20df-73f5-4571  32768   1      305     10110000
GE1/0/11                     0         0000-0000-0000  0       0      0       10100011
GE1/0/12                     0         0000-0000-0000  0       0      0       10100011
```

由于设置了 Eth-Trunk 的活动链路下限阈值为 2，所以聚合组中可用活动接口数量少于 2 时，整个聚合组对应的接口将会被关闭。尽管此时 GE1/0/10 处于 UP 状态，但是仍处于 Unselect 状态。

步骤 4 修改负载分担模式

开启上一步中关闭的接口

```
[S1] interface GE 1/0/11
[S1-GE1/0/11] undo shutdown
[S1-GE1/0/11] quit
[S1] interface GE 1/0/12
[S1-GE1/0/12] undo shutdown
[S1-GE1/0/12] quit
```

大约 30 秒后，查看当前 Eth-Trunk1 的接口状态

```
[S1] display eth-trunk 1

Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                         Working Mode: Static
Preempt Delay Time: 30            Hash Arithmetic: src-dst-ip
System Priority: 100              System ID: 20df-73f5-44e1
Least Active-linknumber: 2        Max Active-linknumber: 2
Operating Status: up              Number Of Up Ports In Trunk: 2
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName          Status     PortType PortPri PortNo PortKey PortState Weight
GE1/0/10(h)            Unselect 1GE     40000    1       305     10100000  1
GE1/0/11(hr)           Selected 1GE     32768    2       305     10111100  1
GE1/0/12(h)            Selected 1GE     32768    3       305     10111100  1

Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri     SystemID         PortPri PortNo PortKey PortState
GE1/0/10               32768      20df-73f5-4571   32768   1      305     10110000
GE1/0/11               32768      20df-73f5-4571   32768   2      305     10111100
GE1/0/12               32768      20df-73f5-4571   32768   3      305     10111100
```

由于使能了 Eth-Trunk 接口的抢占功能，所以当 GE1/0/11 和 GE1/0/12 接口进入 UP 状态之后，这两个接口的优先级高于 GE1/0/10，所以 GE1/0/10 会进入 **unselect** 状态。同时因为系统为了保证链路的稳定性，默认的抢占延时为 30 秒，所以要在 30 秒后才会发生抢占。

修改 Eth-Trunk 接口的负载分担模式为基于目的 IP 地址

```
[S1] interface Eth-Trunk 1
[S1-Eth-Trunk1] load-balance dst-ip
[S1-Eth-Trunk1] quit
```

当需要将 Eth-Trunk 接口的流量分散到不同的链路上，最后能到达统一目的地时，使用 **load-balance** 命令配置 Eth-Trunk 接口负载分担模式，以确保出方向的流量在各物理链路间进行合

理的负载分担，避免链路阻塞。由于负载分担只对出方向的流量有效，因此链路两端接口的负载分担模式可以不一致，两端互不影响。

表4-1 load-balance 参数说明

参数	参数说明
dst-ip	指定基于目的IP地址进行负载分担。
src-ip	指定基于源IP地址进行负载分担。
src-dst-ip	指定基于源IP地址与目的IP地址的异或进行负载分担。
dst-mac	指定基于目的MAC地址进行负载分担。
src-mac	指定基于源MAC地址进行负载分担。
src-dst-mac	指定基于源MAC地址与目的MAC地址的异或进行负载分担。
round-robin	指定基于round-robin模式进行逐包负载分担。
enhanced	指定基于增强负载分担模板进行负载分担。
profile *profile-name*	指定负载分担模板名称。

4.3 配置参考

4.3.1 S1 的配置

```
sysname S1
#
lacp priority 100
#
interface Eth-Trunk1
 mode lacp-static
 least active-linknumber 2
 lacp preempt enable
 lacp max active-linknumber 2
 load-balance dst-ip
#
interface GE1/0/10
 eth-trunk 1
 lacp priority 40000
#
interface GE1/0/11
 eth-trunk 1
```

```
#
interface GE1/0/12
 eth-trunk 1
#
```

4.3.2 S2 的配置

```
sysname S2
#
interface Eth-Trunk1
 mode lacp-static
#
interface GE1/0/10
 eth-trunk 1
#
interface GE1/0/11
 eth-trunk 1
#
interface GE1/0/12
 eth-trunk 1
#
```

4.4 思考题

1. 配置 **least active-linknumber** 和 **lacp max active-linknumber** 时，对两个参数大小有什么要求?

答案：**least active-linknumber** 需要小于或等于 **lacp max active-linknumber**。

5 直连路由实验

5.1 实验介绍

5.1.1 关于本实验

当三层接口配置 IP 地址后，如果接口的物理状态和协议状态都正常，设备会自动基于 IP 地址生成直连路由。直连路由无需网络管理员手工干预，优先级最高。在某些场景下，路由设备仅根据直连路由即可实现不同网段终端的互通，例如实现 VLAN 之间互通。

划分 VLAN 后，不同 VLAN 的用户间不能二层互访，这样能起到隔离广播的作用。但实际应用中，不同 VLAN 的用户又常有互访的需求，此时就需要实现不同 VLAN 的用户互访，简称 VLAN 间互访。

华为提供了多种技术实现 VLAN 间互访，常用的两种技术为 VLANIF 接口和 Dot1q 终结子接口。

- Dot1q 终结子接口：子接口也是一种三层的逻辑接口。跟 VLANIF 接口一样，在子接口上配置 Dot1q 终结功能和 IP 地址后，设备也会添加相应的 MAC 表项并置位三层转发标志位，进而实现 VLAN 间的三层互通。Dot1q 终结子接口适用于通过一个三层以太网接口下接多个 VLAN 网络的环境。
- VLANIF 接口：VLANIF 接口是一种三层的逻辑接口。在 VLANIF 接口上配置 IP 地址后，设备会在 MAC 地址表中添加 VLANIF 接口的 MAC 地址+VID 表项，并且为表项的三层转发标志位置位。当报文的目的 MAC 地址匹配该表项后，会进行三层转发，进而实现 VLAN 间的三层互通。

本实验将通过这两种方式来实现 VLAN 间互访需求，帮助学员进一步理解跨 VLAN 互访的原理。

5.1.2 实验目的

- 掌握通过配置 Dot1q 终结子接口方法实现 VLAN 间互访
- 掌握通过配置 VLANIF 接口方法实现 VLAN 间互访
- 深入理解 VLAN 间互相访问的转发流程

5.1.3 实验组网介绍

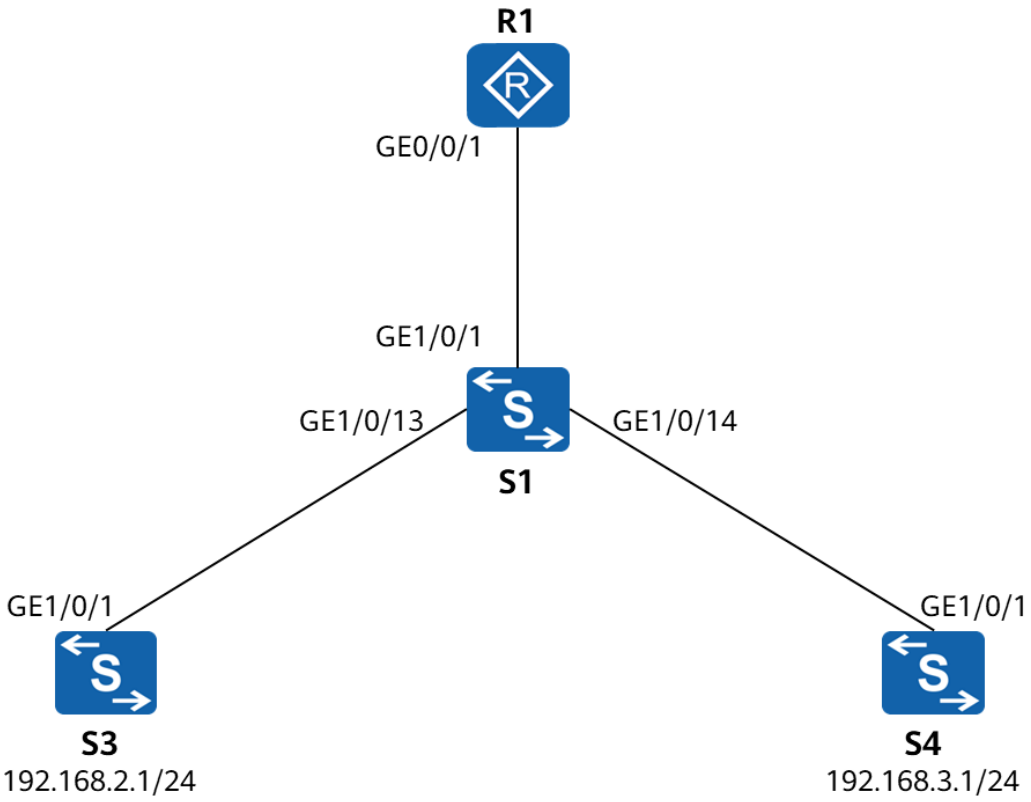


图5-1 直连路由实验拓扑

1. S3 和 S4 模拟终端用户，接口 IP 地址分别为 192.168.2.1/24 和 192.168.3.1/24。
2. S3 和 S4 的网关地址分别为 192.168.2.254 和 192.168.3.254。
3. 在 S1 上将 GE1/0/13 和 GE1/0/14 分别划入 VLAN2 和 VLAN3。

5.1.4 实验背景

S3 和 S4 处于不同的 VLAN，现要求通过 Dot1q 终结子接口和 VLANIF 接口分别实现 S3 与 S4 之间的互访需求。

5.2 实验任务配置

5.2.1 配置思路

1. 配置 Dot1q 终结子接口实现 VLAN 间互访
2. 配置 VLANIF 接口实现 VLAN 间互访

5.2.2 配置步骤

步骤 1 设备基础配置

S3 和 S4 的 IP 地址及网关配置

```
<S3> system-view
Enter system view, return user view with Ctrl+Z.
[S3] interface GE 1/0/1
[S3-GE1/0/1] undo port link-type
[S3-GE1/0/1] undo portswitch
[S3-GE1/0/1] ip address 192.168.2.1 24
[S3-GE1/0/1] quit
[S3] ip route-static 0.0.0.0 0 192.168.2.254
```

配置默认路由，相当于给设备配置了网关。

```
<S4> system-view
Enter system view, return user view with Ctrl+Z.
[S4] interface GE 1/0/1
[S4-GE1/0/1] undo port link-type
[S4-GE1/0/1] undo portswitch
[S4-GE1/0/1] ip address 192.168.3.1 24
[S4-GE1/0/1] quit
[S4] ip route-static 0.0.0.0 0 192.168.3.254
```

在 S1 上对 S3 和 S4 进行 VLAN 划分

```
[S1] vlan batch 2 3
[S1] interface GE 1/0/13
[S1-GE1/0/13] port link-type access
[S1-GE1/0/13] port default vlan 2
[S1-GE1/0/13] quit
[S1] interface GE 1/0/14
[S1-GE1/0/14] port link-type access
[S1-GE1/0/14] port default vlan 3
[S1-GE1/0/14] quit
```

步骤 2 通过 Dot1q 终结子接口实现 VLAN 间互访

配置 S1 上的 Trunk 接口

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] port link-type trunk
[S1-GE1/0/1] port trunk allow-pass vlan 2 3
[S1-GE1/0/1] quit
```

因为 VLAN 间互访数据要由 R1 来终结 VLAN，所以 S1 和 R1 之间的链路要允许 VLAN 2 和 VLAN 3 通过。

在 R1 上创建并配置 Dot1q 终结子接口

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] quit
[R1] interface GE 0/0/1.2
```

创建并进入子接口视图。2 代表子接口的编号，一般建议子接口编号与 VLAN ID 相同，方便记忆。

```
[R1-GE0/0/1.2] dot1q termination vid 2
```

dot1q termination vid *vlan-id* 命令用来配置子接口 Dot1q 终结的 VLAN ID。

以此配置为例：当 GE0/0/1 接口收到带有 VLAN 2 标签的数据之后，会交由 2 号子接口进行 VLAN 终结操作并做后续处理。从 2 号子接口发出的数据也会带上 VLAN 2 的标签。

```
[R1-GE0/0/1.2] ip address 192.168.2.254 24
[R1-GE0/0/1.2] quit
[R1] interface GE 0/0/1.3
[R1-GE0/0/1.3] dot1q termination vid 3
[R1-GE0/0/1.3] ip address 192.168.3.254 24
[R1-GE0/0/1.3] quit
```

检测 VLAN 间互访连通性

```
<S3> ping 192.168.3.1
  PING 192.168.3.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=254 time=110 ms
    Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=254 time=70 ms
    Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=254 time=100 ms

  --- 192.168.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
    0.00% packet loss
    round-trip min/avg/max = 40/76/110 ms
```

```
<S3> tracert 192.168.3.1
 traceroute to  192.168.3.1(192.168.3.1), max hops: 30 ,packet length: 40,press CTRL_C to break
 1 192.168.2.254  30 ms  50 ms  50 ms
 2 192.168.3.1    70 ms  60 ms  60 ms
```

此时 VLAN 2 和 VLAN 3 之间已经可以正常互访。

步骤 3 通过 VLANIF 接口实现 VLAN 间互访

清除上一步配置

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] undo port trunk allow-pass vlan 2 3
[S1-GE1/0/1] quit
```

```
[R1] undo interface GE 0/0/1.2
[R1] undo interface GE 0/0/1.3
```

在 S1 上创建相应的 VLANIF 接口

```
[S1] interface Vlanif 2
```

interface vlanif *vlan-id* 命令用来创建 VLANIF 接口并进入 VLANIF 接口视图。只有先通过命令创建 VLAN 后，才能执行 **interface vlanif** 命令创建 VLANIF 接口。

```
[S1-Vlanif2] ip address 192.168.2.254 24
[S1-Vlanif2] quit
[S1] interface Vlanif 3
[S1-Vlanif3] ip address 192.168.3.254 24
[S1-Vlanif3] quit
```

检测 VLAN 间互访连通性

```
<S3> ping 192.168.3.1
  PING 192.168.3.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=254 time=100 ms
    Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=254 time=50 ms
    Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=254 time=50 ms
    Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=254 time=60 ms
    Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=254 time=70 ms
  --- 192.168.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
    0.00% packet loss
    round-trip min/avg/max = 50/66/100 ms

<S3> tracert 192.168.3.1

 traceroute to  192.168.3.1(192.168.3.1), max hops: 30 ,packet length: 40,press CTRL_C to break
 1 192.168.2.254 40 ms  30 ms  20 ms
 2 192.168.3.1 40 ms  30 ms  40 ms
```

此时 VLAN 2 和 VLAN 3 之间已经可以正常互访。

5.3 配置参考

5.3.1 S1 的配置

```
sysname S1
#
vlan batch 2 to 3
#
interface Vlanif2
 ip address 192.168.2.254 255.255.255.0
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
#
interface GE1/0/13
 port link-type access
 port default vlan 2
#
interface GE1/0/14
 port link-type access
 port default vlan 3
#
```

5.3.2 S3 的配置

```
sysname S3
#
interface GE1/0/1
 undo portswitch
 ip address 192.168.2.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
```

```
#
```

5.3.3 S4 的配置

```
sysname S4
#
interface GE1/0/1
 undo portswitch
 ip address 192.168.3.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
```

5.4 思考题

1. VLANIF 接口在什么情况下会处于 UP 状态?

答案：当有任一允许此 VLAN 通过的物理接口进入 UP 状态，那么对应的 VLANIF 接口就会进入 UP 状态。

6 静态路由实验

6.1 实验介绍

6.1.1 关于本实验

IPv4（Internet Protocol Version 4）是 TCP/IP 协议族中最为核心的协议之一。它工作在 TCP/IP 参考模型的网际层，该层与 OSI 参考模型的网络层相对应。网络层提供了无连接数据传输服务，即网络在发送分组时不需要先建立连接，每一个分组（也就是 IP 数据报文）独立发送。

路由是数据通信网络中最基本的要素。路由信息就是指导 IP 报文发送的路径信息，路由的过程就是报文转发的过程。

本实验将通过 IPv4 地址以及 IPv4 静态路由的配置，帮助学员理解路由转发的基本原理。

6.1.2 实验目的

- 掌握接口 IPv4 地址的配置方法
- 理解 LoopBack 接口的作用与含义
- 理解直连路由的产生原则
- 掌握静态路由的配置方法并理解其生效的条件
- 掌握通过 Ping 工具测试网络层连通性
- 掌握并理解特殊静态路由的配置方法与应用场景

6.1.3 实验组网介绍

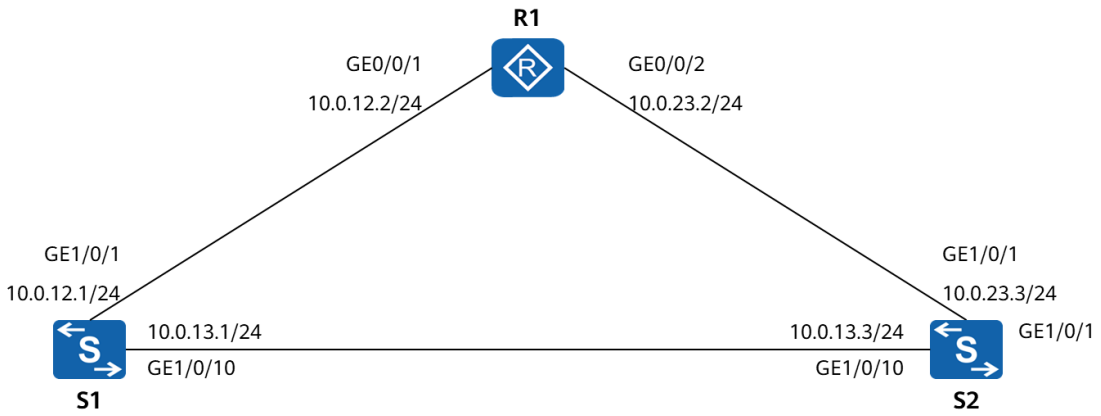


图6-1 静态路由实验拓扑

6.1.4 实验背景

R1、S1、S2 都是各自网络的网关设备，现在需要通过相应的配置，来实现这些网络之间的互通。

6.2 实验任务配置

6.2.1 配置思路

1. 配置网络设备各接口的 IP 地址
2. 配置静态路由来实现互通

6.2.2 配置步骤

步骤 1 设备基础配置

设备命名

略。

关闭不使用的端口

```
[S1] interface GE 1/0/11
[S1-GE1/0/11] shutdown
[S1-GE1/0/11] quit
```

```
[S1] interface GE 1/0/12
[S1-GE1/0/12] shutdown
[S1-GE1/0/12] quit
[S1] interface GE 1/0/13
[S1-GE1/0/13] shutdown
[S1-GE1/0/13] quit
[S1] interface GE 1/0/14
[S1-GE1/0/14] shutdown
[S1-GE1/0/14] quit
```

```
[S2] interface GE 1/0/11
[S2-GE1/0/11] shutdown
[S2-GE1/0/11] quit
[S2] interface GE 1/0/12
[S2-GE1/0/12] shutdown
[S2-GE1/0/12] quit
[S2] interface GE 1/0/13
[S2-GE1/0/13] shutdown
[S2-GE1/0/13] quit
[S2] interface GE 1/0/14
[S2-GE1/0/14] shutdown
[S2-GE1/0/14] quit
```

接口初始化配置

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] undo portswitch
[R1-GE0/0/2] quit
```

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] undo port link-type
[S1-GE1/0/1] undo portswitch
[S1-GE1/0/1] quit
[S1] interface GE 1/0/10
[S1-GE1/0/10] undo port link-type
[S1-GE1/0/10] undo portswitch
[S1-GE1/0/10] quit
```

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] undo port link-type
[S2-GE1/0/1] undo portswitch
[S2-GE1/0/1] quit
```

```
[S2] interface GE 1/0/10
[S2-GE1/0/10] undo port link-type
[S2-GE1/0/10] undo portswitch
[S2-GE1/0/10] quit
```

步骤 2 查看网络设备当前接口 IP 地址配置与路由表

查看网络设备上的接口状态，仅以 R1 为例

```
[R1] display ip interface brief
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(ed): error down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 3
The number of interface that is UP in Protocol is 1
The number of interface that is DOWN in Protocol is 5
Interface                   IP Address/Mask      Physical   Protocol  VPN
GE0/0/1                     unassigned           up         down      --
GE0/0/2                     unassigned           up         down      --
GE0/0/4                     192.168.1.1/24       down       down      _management...
MultiGE0/0/0                unassigned           down       down      --
MultiGE0/0/1                unassigned           down       down      --
NULL0                       unassigned           up         up(s)     --
```

display ip interface brief 命令用来查看接口与 IP 相关的简要信息，包括 IP 地址、子网掩码、物理状态和协议状态以及处于不同状态的接口数目等。

当前 R1 上的 GE0/0/1 和 GE0/0/2 接口由于尚未配置 IP 地址，所以 IP Address/Mask 字段为 **unassigned** 状态，Physical 字段为 **up** 状态，Protocol 字段为 **down** 状态。

查看网络设备上的路由表，仅以 R1 为例

```
[R1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 4        Routes : 4

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

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
```

InLoopBack0 为设备上默认创建的环回接口，它是一个特殊的、固定的 LoopBack 接口。

InLoopBack0 接口使用环回地址 127.0.0.1/8，用来接收所有发送给本机的数据包。该接口上的 IP 地址不可以改变，也不通过路由协议对外发布。

步骤 3 配置物理接口的 IP 地址

按照下表配置网络设备物理接口的 IP 地址

表6-1 设备物理接口 IP

网络设备	接口	IP Address/Mask
R1	GE0/0/1	10.0.12.2/24
	GE0/0/2	10.0.23.2/24
S1	GE1/0/1	10.0.12.1/24
	GE1/0/10	10.0.13.1/24
S2	GE1/0/1	10.0.23.3/24
	GE1/0/10	10.0.13.3/24

```
[R1] interface GE0/0/1
[R1-GE0/0/1] ip address 10.0.12.2 24
[R1-GE0/0/1] quit
[R1] interface GE0/0/2
[R1-GE0/0/2] ip address 10.0.23.2 24
[R1-GE0/0/2] quit
```

```
[S1] interface GE1/0/1
[S1-GE1/0/1] ip address 10.0.12.1 24
[S1-GE1/0/1] quit
[S1] interface GE1/0/10
[S1-GE1/0/10] ip address 10.0.13.1 24
[S1-GE1/0/10] quit
```

```
[S2] interface GE1/0/1
[S2-GE1/0/1] ip address 10.0.23.3 24
[S2-GE1/0/1] quit
[S2] interface GE1/0/10
[S2-GE1/0/10] ip address 10.0.13.3 24
[S2-GE1/0/10] quit
```

使用 Ping 工具测试连通性

```
[R1] 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=254 time=11 ms
    Reply from 10.0.12.1: bytes=56 Sequence=2 ttl=254 time=9 ms
    Reply from 10.0.12.1: bytes=56 Sequence=3 ttl=254 time=11 ms
    Reply from 10.0.12.1: bytes=56 Sequence=4 ttl=254 time=9 ms
    Reply from 10.0.12.1: bytes=56 Sequence=5 ttl=254 time=9 ms

  --- 10.0.12.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 9/9/11 ms
```

```
[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=11 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=254 time=7 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=254 time=11 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=254 time=10 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=254 time=8 ms

  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 7/9/11 ms
```

查看 R1 的路由表

```
[R1] display ip routing-table
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.12.0/24  Direct  0    0           D   10.0.12.2       GE0/0/1
        10.0.12.2/32  Direct  0    0           D   127.0.0.1       GE0/0/1
      10.0.12.255/32  Direct  0    0           D   127.0.0.1       GE0/0/1
        10.0.23.0/24  Direct  0    0           D   10.0.23.2       GE0/0/2
        10.0.23.2/32  Direct  0    0           D   127.0.0.1       GE0/0/2
```

```
10.0.23.255/32   Direct  0    0          D   127.0.0.1       GE0/0/2
127.0.0.0/8      Direct  0    0          D   127.0.0.1       InLoopBack0
127.0.0.1/32     Direct  0    0          D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0       D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0       D   127.0.0.1       InLoopBack0
```

可以看到，在接口 IP 地址配置完成之后，针对每个接口自动生成了三条直连路由。分别是：

1. 指向接口所在网段的路由。
2. 指向接口 IP 地址的主机路由。
3. 指向接口所在网段广播地址的主机路由。

注：主机路由就是掩码长度为 32 的路由。

步骤 4 创建并配置 LoopBack 接口

按照下表配置设备的 LoopBack 接口

表6-2 LoopBack 接口 IP

网络设备	接口	IP Address/Mask
R1	LoopBack0	10.0.2.2/32
S1	LoopBack0	10.0.1.1/32
S2	LoopBack0	10.0.3.3/32

LoopBack 接口属于设备上的逻辑接口，逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。LoopBack 接口创建后除非手工关闭该接口，否则 LoopBack 接口物理层状态和协议状态永远处于 UP 状态。一般情况下，LoopBack 接口使用 32 位掩码。使用 LoopBack 接口一般有如下目的：

1. 作为网络设备的管理地址。
2. 使用该接口地址作为动态路由协议的 Router ID。
3. 其它提高网络可靠性的用途。

本实验使用 LoopBack 接口模拟客户端。

```
[R1] interface LoopBack0
[R1-LoopBack0] ip address 10.0.2.2 32
[R1-LoopBack0] quit
```

```
[S1] interface LoopBack0
[S1-LoopBack0] ip address 10.0.1.1 32
[S1-LoopBack0] quit
```

```
[S2] interface LoopBack0
[S2-LoopBack0] ip address 10.0.3.3 32
[S2-LoopBack0] quit
```

查看路由表，以 R1 为例

```
[R1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.2.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.12.0/24  Direct  0    0           D   10.0.12.2       GE0/0/1
       10.0.12.2/32  Direct  0    0           D   127.0.0.1       GE0/0/1
     10.0.12.255/32  Direct  0    0           D   127.0.0.1       GE0/0/1
       10.0.23.0/24  Direct  0    0           D   10.0.23.2       GE0/0/2
       10.0.23.2/32  Direct  0    0           D   127.0.0.1       GE0/0/2
     10.0.23.255/32  Direct  0    0           D   127.0.0.1       GE0/0/2
        127.0.0.0/8  Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

此时已经生成了 LoopBack 接口的直连路由。

测试各 LoopBack 接口之间的连通性

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

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

ping –a *source-ip-address destination-ip-address* 命令用来指定发送 ICMP Echo Request 报文的源 IP 地址。如果不指定源 IP 地址，一般采用路由出接口的 IP 地址作为 ICMP Echo

Request 报文发送的源地址。此时由于 R1 上没有到达该目的 IP 的路由条目，所以无法 Ping 通。

步骤 5 配置静态路由

在 R1 上配置到达 S1 和 S2 的 LoopBack0 接口的路由条目

```
[R1] ip route-static 10.0.1.1 32 10.0.12.1
[R1] ip route-static 10.0.3.3 32 10.0.23.3
```

查看 R1 的路由表

```
[R1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 13          Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Static  60   0           RD  10.0.12.1       GE0/0/1
        10.0.2.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.3.3/32  Static  60   0           RD  10.0.23.3       GE0/0/2
       10.0.12.0/24  Direct  0    0           D   10.0.12.2       GE0/0/1
       10.0.12.2/32  Direct  0    0           D   127.0.0.1       GE0/0/1
     10.0.12.255/32  Direct  0    0           D   127.0.0.1       GE0/0/1
       10.0.23.0/24  Direct  0    0           D   10.0.23.2       GE0/0/2
       10.0.23.2/32  Direct  0    0           D   127.0.0.1       GE0/0/2
     10.0.23.255/32  Direct  0    0           D   127.0.0.1       GE0/0/2
        127.0.0.0/8  Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

配置的静态路由被加入到了 IP 路由表中。

测试连通性

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

  --- 10.0.1.1 ping statistics ---
```

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

还是无法 Ping 通 S1 LoopBack0 接口，因为此时 S1 上没有到达 R1 LoopBack0 的路由。

在 S1 上添加到达 R1 LoopBack0 的路由

```
[S1] ip route-static 10.0.2.2 32 10.0.12.2
```

测试连通性

```
[R1] ping -a 10.0.2.2 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=10 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=10 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=11 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=12 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/9/12 ms
```

此时 R1 的 LoopBack0 已经可以和 S1 的 LoopBack0 实现互通。

完成剩余路由条目的配置

```
[S1] ip route-static 10.0.3.3 32 10.0.13.3
```

```
[S2] ip route-static 10.0.1.1 32 10.0.13.1
[S2] ip route-static 10.0.2.2 32 10.0.23.2
```

配置完成后，请读者自行测试网络设备 LoopBack0 接口之间的连通性。

步骤 6 配置 R1 -> S2 -> S1 作为 R1 LoopBack0 到 S1 LoopBack0 接口的备份路径

配置 R1 和 S1 的静态路由

```
[R1] ip route-static 10.0.1.1 32 10.0.23.3 preference 100
```

```
[S1] ip route-static 10.0.2.2 32 10.0.13.3 preference 100
```

查看 R1 的路由表

```
[R1] display ip routing-table
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Static  60   0           RD  10.0.12.1       GE0/0/1
        10.0.2.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.3.3/32  Static  60   0           RD  10.0.23.3       GE0/0/2
       10.0.12.0/24  Direct  0    0           D   10.0.12.2       GE0/0/1
       10.0.12.2/32  Direct  0    0           D   127.0.0.1       GE0/0/1
     10.0.12.255/32  Direct  0    0           D   127.0.0.1       GE0/0/1
       10.0.23.0/24  Direct  0    0           D   10.0.23.2       GE0/0/2
       10.0.23.2/32  Direct  0    0           D   127.0.0.1       GE0/0/2
     10.0.23.255/32  Direct  0    0           D   127.0.0.1       GE0/0/2
        127.0.0.0/8  Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32   Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32   Direct  0    0           D   127.0.0.1       InLoopBack0
```

此时配置的 preference 为 100 的静态路由没有被加载到路由表中。

关闭 R1 GE0/0/1 接口，使得优先级高的路由失效

```
[R1] interface GE0/0/1
[R1-GE0/0/1] shutdown
[R1-GE0/0/1] quit
```

查看 R1 的路由表，随着高优先级路由失效，低优先级路由被激活

```
[R1] display ip routing-table
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Static  100  0           RD  10.0.23.3       GE0/0/2
        10.0.2.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.3.3/32  Static  60   0           RD  10.0.23.3       GE0/0/2
       10.0.23.0/24  Direct  0    0           D   10.0.23.2       GE0/0/2
       10.0.23.2/32  Direct  0    0           D   127.0.0.1       GE0/0/2
     10.0.23.255/32  Direct  0    0           D   127.0.0.1       GE0/0/2
```

```
        127.0.0.0/8     Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32    Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32    Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32    Direct  0    0           D   127.0.0.1       InLoopBack0
```

此时由于链路断开，原先的静态路由失效，低优先级的静态路由被激活。

检查连通性

```
[R1] ping -a 10.0.2.2 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=253 time=10 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=253 time=11 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=253 time=20 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=253 time=11 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=253 time=10 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/12/20 ms
```

追踪数据包路径

```
[R1] tracert -a 10.0.2.2 10.0.1.1
 traceroute to 10.0.1.1(10.0.1.1), max hops: 64, packet length: 40, press CTRL_C to break
 1 10.0.23.3 15 ms  1 ms  9 ms
 2 10.0.1.1 10 ms  10 ms  22 ms
```

Tracert 命令主要用于查看数据包从源端到目的端的路径信息。

可以看到数据包经过了 S2 的 GE1/0/10 转发给 S1。

注：部分实验环境下设备出于安全考虑，不会回复 ICMP 报文，实验现象可能会有所偏差，可以按<Ctrl+C>结束 tracert。

步骤 7 通过默认路由实现 R1 的 LoopBack0 接口和 S1 的 LoopBack0 接口互通

恢复接口并删除已经配置的路由条目

```
[R1] interface GE0/0/1
[R1-GE0/0/1] undo shutdown
[R1-GE0/0/1] quit
[R1] undo ip route-static 10.0.1.1 255.255.255.255 10.0.12.1
[R1] undo ip route-static 10.0.1.1 255.255.255.255 10.0.23.3
```

查看 R1 的路由表

```
[R1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 11          Routes : 11

Destination/Mask    Proto   Pre  Cost          Flags NextHop         Interface

        10.0.2.2/32  Direct  0    0             D   127.0.0.1       LoopBack0
       10.0.12.0/24  Direct  0    0             D   10.0.12.2       GE0/0/1
       10.0.12.2/32  Direct  0    0             D   127.0.0.1       GE0/0/1
     10.0.12.255/32  Direct  0    0             D   127.0.0.1       GE0/0/1
       10.0.23.0/24  Direct  0    0             D   10.0.23.2       GE0/0/2
       10.0.23.2/32  Direct  0    0             D   127.0.0.1       GE0/0/2
     10.0.23.255/32  Direct  0    0             D   127.0.0.1       GE0/0/2
        127.0.0.0/8  Direct  0    0             D   127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0             D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0             D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0             D   127.0.0.1       InLoopBack0
```

此时 R1 上没有到 S1 的 LoopBack0（10.0.1.1/32）的路由条目。

在 R1 上配置默认路由

```
[R1] ip route-static 0.0.0.0 0 10.0.12.1
```

查看 R1 的路由条目

```
[R1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 12          Routes : 12

Destination/Mask    Proto   Pre  Cost          Flags NextHop         Interface

        0.0.0.0/0   Static  60   0             RD  10.0.12.1       GE0/0/1
        10.0.2.2/32  Direct  0    0             D   127.0.0.1       LoopBack0
       10.0.12.0/24  Direct  0    0             D   10.0.12.2       GE0/0/1
       10.0.12.2/32  Direct  0    0             D   127.0.0.1       GE0/0/1
     10.0.12.255/32  Direct  0    0             D   127.0.0.1       GE0/0/1
       10.0.23.0/24  Direct  0    0             D   10.0.23.2       GE0/0/2
       10.0.23.2/32  Direct  0    0             D   127.0.0.1       GE0/0/2
     10.0.23.255/32  Direct  0    0             D   127.0.0.1       GE0/0/2
        127.0.0.0/8  Direct  0    0             D   127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0             D   127.0.0.1       InLoopBack0
```

```
127.255.255.255/32  Direct  0    0          D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0          D   127.0.0.1       InLoopBack0
```

默认路由已经被激活。

测试 R1 的 LoopBack0 接口到 S1 的 LoopBack0 接口的连通性

```
[R1] ping -a 10.0.2.2 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=13 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=11 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=8 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=12 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=11 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 8/11/13 ms
```

此时 R1 的 LoopBack0 接口到 S1 的 LoopBack0 接口之间可以互通。

6.3 结果验证

读者自行通过 Ping 和 Tracert 命令检查设备 LoopBack0 接口之间的连通性。

6.4 配置参考

6.4.1 R1 的配置

```
sysname R1
#
interface GE0/0/1
 ip address 10.0.12.2 255.255.255.0
#
interface GE0/0/2
 ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.255
#
ip route-static 0.0.0.0 0.0.0.0 10.0.12.1
```

```
ip route-static 10.0.3.3 255.255.255.255 10.0.23.3
#
```

6.4.2 S1 的配置

```
sysname S1
#
interface GE1/0/1
 undo portswitch
 ip address 10.0.12.1 255.255.255.0
#
interface GE1/0/10
 undo portswitch
 ip address 10.0.13.1 255.255.255.0
#
interface GE1/0/11
 shutdown
 port link-type access
#
interface GE1/0/12
 shutdown
 port link-type access
#
interface GE1/0/13
 shutdown
 port link-type access
#
interface GE1/0/14
 shutdown
 port link-type access
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ip route-static 10.0.2.2 255.255.255.255 10.0.12.2
ip route-static 10.0.2.2 255.255.255.255 10.0.13.3 preference 100
ip route-static 10.0.3.3 255.255.255.255 10.0.13.3
```

6.4.3 S2 的配置

```
sysname S2
#
interface GE1/0/1
 undo portswitch
 ip address 10.0.23.3 255.255.255.0
```

```
#
interface GE1/0/10
 undo portswitch
 ip address 10.0.13.3 255.255.255.0
#
interface GE1/0/11
 shutdown
 port link-type access
#
interface GE1/0/12
 shutdown
 port link-type access
#
interface GE1/0/13
 shutdown
 port link-type access
#
interface GE1/0/14
 shutdown
 port link-type access
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.255
#
ip route-static 10.0.1.1 255.255.255.255 10.0.13.1
ip route-static 10.0.2.2 255.255.255.255 10.0.23.2
```

6.5 思考题

1. 什么情况下，配置的静态路由会被添加到 IP 路由表中？若配置的下一跳不可达，该路由可以被加入到 IP 路由表吗？

答案：同时满足以下两个条件，静态路由会被添加到路由表中：

a) 该路由所配置的下一跳可达。

b) 这条路由是到达目的网段（主机）的最优路由。

所以当下一跳不可达时，不会被添加到 IP 路由表。

7 IP 地址自动配置实验

7.1 实验介绍

7.1.1 关于本实验

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一种用于集中对用户IP 地址进行动态管理和配置的技术。即使规模较小的网络，通过 DHCP 也可以使后续增加网络设备变得简单快捷。

DHCP 协议由 RFC 2131 定义，采用客户端/服务器通信模式，由客户端（DHCP Client）向服务器（DHCP Server）提出配置申请，服务器返回为客户端分配的配置信息。

DHCP 可以提供两种地址分配机制，网络管理员可以根据网络需求为不同的主机选择不同的分配策略。

- 动态分配机制：通过 DHCP 为主机分配一个有使用期限（这个使用期限通常叫做租期）的 IP 地址。这种分配机制适用于主机需要临时接入网络或者空闲地址数小于网络主机总数且主机不需要永久连接网络的场景。
- 静态分配机制：网络管理员通过 DHCP 为指定的主机分配固定的 IP 地址。相比手工静态配置 IP 地址，通过 DHCP 方式静态分配机制避免人工配置发生错误，方便管理员统一维护管理。

7.1.2 实验目的

- 掌握 DHCP 全局地址池的配置方法
- 掌握通过 DHCP 分配静态 IP 地址的方法

7.1.3 实验组网介绍

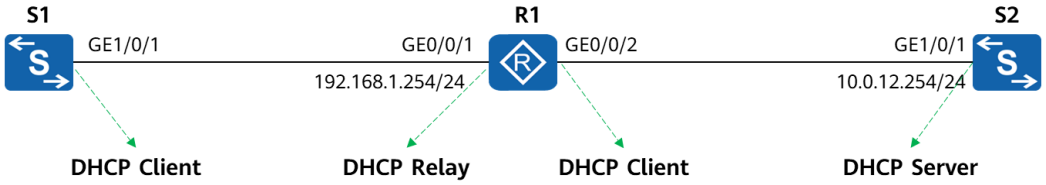


图7-1 IP 地址自动配置实验拓扑

1. S1 的 GE1/0/1 接口和 R1 的 GE0/0/2 接口作为 DHCP Client。
2. S2 作为 DHCP Server 为 S1 和 R1 分配 IP 地址。
3. R1 的 GE0/0/1 接口作为 DHCP Relay。

7.1.4 实验背景

某企业为了减少 IP 地址维护的工作量，增加 IP 地址的利用率，准备在网络内部署 DHCP 协议。

7.2 实验任务配置

7.2.1 配置思路

1. 配置 DHCP 服务器
2. 配置 DHCP 客户端
3. 配置 DHCP Relay

7.2.2 配置步骤

步骤 1 基本配置

关闭不使用的端口

```
[S2] interface GE 1/0/10
[S2-GE1/0/10] shutdown
[S2-GE1/0/10] quit
[S2] interface GE 1/0/11
[S2-GE1/0/11] shutdown
```

```
[S2-GE1/0/11] quit
[S2] interface GE 1/0/12
[S2-GE1/0/12] shutdown
[S2-GE1/0/12] quit
[S2] interface GE 1/0/13
[S2-GE1/0/13] shutdown
[S2-GE1/0/13] quit
[S2] interface GE 1/0/14
[S2-GE1/0/14] shutdown
[S2-GE1/0/14] quit
```

配置接口 IP 地址

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] undo port link-type
[S2-GE1/0/1] undo portswitch
[S2-GE1/0/1] ip address 10.0.12.254 24
[S2-GE1/0/1] quit
```

将 R1 GE0/0/1 和 GE0/0/2 切换为三层接口

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] undo portswitch
[R1-GE0/0/2] quit
```

步骤 2 开启 DHCP 功能

```
[S2] dhcp enable
```

dhcp enable 命令是 DHCP 相关功能的总开关，DHCP Client 和 DHCP Server 等功能都要在执行 **dhcp enable** 命令使能 DHCP 功能后才会生效。

```
[S1] dhcp enable
```

```
[R1] dhcp enable
```

步骤 3 配置地址池

配置全局地址池，该地址池用于为 R1 分配 IP 地址

```
[S2] ip pool for_r1
```

创建名为 for_r1 的地址池。

```
[S2-ip-pool-for_r1] network 10.0.12.0 mask 24
```

network 命令用来配置全局地址池下可分配的网段地址。

```
[S2-ip-pool-for_r1] dns-list 10.0.12.254
```

dns-list 命令用来为 DHCP Client 配置 DNS Server 地址。

```
[S2-ip-pool-for_r1] gateway-list 10.0.12.254
```

gateway-list 命令用来为 DHCP Client 配置出口网关地址。DHCP Client 在获取地址之后，会生成一条默认路由。

```
[S2-ip-pool-for_r1] lease day 2 hour 2
```

lease 命令用来配置地址池下的地址租期。当租期被设置为 **unlimited** 时，代表租期无限制。缺省情况下，IP 地址租期是 1 天。

配置全局地址池，该地址池用于为 S1 分配固定 IP 地址

查看 S1 GE1/0/1 接口的 MAC 地址。

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] undo port link-type
[S1-GE1/0/1] undo portswitch
[S1-GE1/0/1] quit
```

```
[S1] display interface GE 1/0/1
GE1/0/1 current state : UP (ifindex: 2)
Line protocol current state : DOWN
Description:
Route Port,The Maximum Transmit Unit is 1500,The Maximum Frame Length is 9216
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 20df-73f5-44e2
Port Mode:       COMMON COPPER,       Port Split:                    -
Speed:                    1000,       Loopback:                   NONE
Duplex:                   FULL,       Negotiation:                ENABLE
Input Flow-control: DISABLE,       Output Flow-control:        DISABLE
Mdi:                      AUTO
```

```
[S2] ip pool for_s1
[S2-ip-pool-for_s1] network 192.168.1.0 mask 24
[S2-ip-pool-for_s1] gateway-list 192.168.1.254
[S2-ip-pool-for_s1] static-bind ip-address 192.168.1.253 mac-address 20df-73f5-44e2
```

```
[S2-ip-pool-for_s1] quit
```

static-bind 命令用来将 DHCP Server 全局地址池下的 IP 地址与 MAC 地址进行绑定。20df-73f5-44e2 为当前实验环境下 S1 的 GE1/0/1 接口的 MAC 地址。配置完这条命令之后，后续 S1 会获得固定的 IP 地址 192.168.1.253。

步骤 4 开启 S2 GE1/0/1 接口的 DHCP Server 功能

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] dhcp select global
[S2-GE1/0/1] quit
```

dhcp select global 命令用来开启接口采用全局地址池的 DHCP Server 功能。当接口收到 DHCP Client 请求之后，会到所有全局地址池中查找对应的地址池，然后分配可用的地址给 DHCP Client。

步骤 5 配置 DHCP Client

```
[R1] interface GE 0/0/2
[R1-GE0/0/2] ip address dhcp-alloc
[R1-GE0/0/2] quit
```

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] ip address dhcp-alloc
[S1-GE1/0/1] quit
```

查看 R1 获取的 IP 地址

```
[R1] display ip interface GE 0/0/2
GE0/0/2 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
Directed-broadcast packets:
  received packets:              0, sent packets:                0
  forwarded packets:             0, dropped packets:             0
ARP packet input number:             0
    Request packet:                  0
    Reply packet:                    0
    Unknown packet:                  0
Internet Address is allocated by DHCP, 10.0.12.105/24
Broadcast address : 0.0.0.0
TTL being 1 packet number:           0
TTL invalid packet number:           0
ICMP packet input number:            0
```

```
  Echo reply:                    0
  Unreachable:                   0
  Source quench:                 0
  Routing redirect:              0
  Echo request:                  0
  Router advert:                 0
  Router solicit:                0
  Time exceed:                   0
  IP header bad:                 0
  Timestamp request:             0
  Timestamp reply:               0
  Information request:           0
  Information reply:             0
  Netmask request:               0
  Netmask reply:                 0
  Unknown type:                  0
```

可以看到 R1 获取的 IP 地址是 10.0.12.105/24。

注意：R1 获取的 IP 地址是随机分配的，不同实验环境有所不同。

查看 R1 GE0/0/2 接口的租约信息

```
[R1] display dhcp client interface GE 0/0/2
DHCP client lease information on interface GE0/0/2 :
  Current machine state          : Bound
  Internet address assigned via : DHCP
  Physical address               : b0c7-8733-d661
  IP address                     : 10.0.12.105
  Subnet mask                    : 255.255.255.0
  Gateway ip address             : 10.0.12.254
  DHCP server                    : 10.0.12.254
  Lease obtained at              : XXXX-03-06 04:36:00
  Lease expires at               : XXXX-03-08 06:36:00
  Lease renews at                : XXXX-03-07 05:36:00
  Lease rebinds at               : XXXX-03-08 00:21:00
  DNS                            : 10.0.12.254
  Request option list            : 1 3 6 15 28 33 44 121 184
  Class identifier               : huawei AR5710-S8T2XE
  Client identifier              : b0c7-8733-d661
```

可以看到有效期为 2 天 2 小时，且 DNS 地址为 10.0.12.254。

查看 R1 的路由表

```
[R1] display ip routing-table
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
```

```
Routing Table : _public_
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   OPR     60   0           D   10.0.12.254     GE0/0/2
       10.0.12.0/24 Direct  0    0           D   10.0.12.105     GE0/0/2
     10.0.12.105/32 Direct  0    0           D   127.0.0.1       GE0/0/2
     10.0.12.255/32 Direct  0    0           D   127.0.0.1       GE0/0/2
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

可以看到一条缺省路由，协议类型为 OPR，协议优先级为 60，下一跳指向网关。DHCP 服务器下发的缺省路由为 OPR 路由（Open Programming Route），默认优先级为 60，通过命令 **dhcp client default-route preference** 可以修改该缺省路由优先级。

查看 DHCP Server 地址池 for_r1 已分配的 IP 地址

```
[S2] display ip pool name for_r1 used

  Pool-name           : for_r1
  Pool-No             : 0
  Lease               : 2 Days 2 Hours 0 Minutes
  Domain-name         : -
  DNS-server0         : 10.0.12.254
  NBNS-server0        : -
  Netbios-type        : -
  Position            : Local
  Status              : Unlocked
  Gateway-0           : 10.0.12.254
  Network             : 10.0.12.0
  Mask                : 255.255.255.0
  VPN instance        : --
  Logging             : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total          :253          Used           :1
                     Idle           :252          Expired        :0
                     Conflict       :0            Disabled       :0

--------------------------------------------------------------------------------
  Network section
          Start            End          Total     Used Idle(Expired) Conflict Disabled
--------------------------------------------------------------------------------
        10.0.12.1      10.0.12.254      253         1          252(0)         0        0
--------------------------------------------------------------------------------
Client-ID format as follows:
```

```
  DHCP      : mac-address
  IPSec     : user-id/portnumber/vrf
  SSL-VPN : user-id/session-id
--------------------------------------------------------------------------------
 Index                IP              Client-ID      Type        Left    Status
--------------------------------------------------------------------------------
   104       10.0.12.105        b0c7-8733-d661     DHCP       179263    Used
--------------------------------------------------------------------------------
```

可以看到 DHCP Server 分配的 IP 地址就是 R1 获取的 IP 地址。

查看 S1 获取的 IP 地址

```
[S1] display ip interface GE 1/0/1
GE1/0/1 current state : UP
Line protocol current state : DOWN
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
Directed-broadcast packets:
 received packets:              0, sent packets:                0
 forwarded packets:             0, dropped packets:             0
ARP packet input number:              0
   Request packet:                    0
   Reply packet:                      0
   Unknown packet:                    0
Internet protocol processing : disabled
Broadcast address : 0.0.0.0
TTL being 1 packet number:            0
TTL invalid packet number:            0
ICMP packet input number:             0
   Echo reply:                        0
   Unreachable:                       0
   Source quench:                     0
   Routing redirect:                  0
   Echo request:                      0
   Router advert:                     0
   Router solicit:                    0
   Time exceed:                       0
   IP header bad:                     0
   Timestamp request:                 0
   Timestamp reply:                   0
   Information request:               0
   Information reply:                 0
   Netmask request:                   0
   Netmask reply:                     0
   Unknown type:                      0
```

可以看到 S1 未获取 IP 地址，这是因为 S1 和 DHCP Server 之间存在三层网络，因此需要部署 DHCP Relay。

查看 DHCP Server 地址池 for_s1 已分配的 IP 地址

```
[S2] display ip pool name for_s1 used

  Pool-name           : for_s1
  Pool-No             : 1
  Lease               : 1 Days 0 Hours 0 Minutes
  Domain-name         : -
  DNS-server0         : -
  NBNS-server0        : -
  Netbios-type        : -
  Position            : Local
  Status              : Unlocked
  Gateway-0           : 192.168.1.254
  Network             : 192.168.1.0
  Mask                : 255.255.255.0
  VPN instance        : --
  Logging             : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total          :253          Used           :1
                     Idle           :252          Expired        :0
                     Conflict       :0            Disabled       :0

--------------------------------------------------------------------------------
  Network section
          Start            End          Total      Used Idle(Expired) Conflict Disabled
--------------------------------------------------------------------------------
     192.168.1.1    192.168.1.254       253          1          252(0)          0       0
--------------------------------------------------------------------------------
Client-ID format as follows:
   DHCP      : mac-address
   IPSec     : user-id/portnumber/vrf
   SSL-VPN : user-id/session-id
--------------------------------------------------------------------------------
  Index                IP               Client-ID      Type          Left     Status
--------------------------------------------------------------------------------
    252    192.168.1.253          20df-73f5-44e2      DHCP            -     Static-bind
--------------------------------------------------------------------------------
```

可以看到为 S1 绑定的 IP 地址 192.168.1.253，但 S1 当前未获取到该 IP 地址。

步骤 6 配置 DHCP Relay

配置 R1，指定 DHCP Server 的 IP 地址

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] ip address 192.168.1.254 24
[R1-GE0/0/1] dhcp select relay
```

dhcp select relay 命令用来开启 DHCP 中继功能。

```
[R1-GE0/0/1] dhcp relay server-ip 10.0.12.254
[R1-GE0/0/1] quit
```

dhcp relay server-ip 命令用来在 DHCP 中继的接口上配置 DHCP 服务器地址。

配置 DHCP Server 到达 DHCP Relay 的路由

```
[S2] ip route-static 192.168.1.0 24 10.0.12.105
```

注意下一跳地址设置为 R1 GE0/0/2 接口获取的 IP 地址，不同实验环境，下一跳地址可能不同。

查看 S1 获取的 IP 地址

```
[S1] display ip interface GE 1/0/1
GE1/0/1 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
Directed-broadcast packets:
  received packets:              0, sent packets:                0
  forwarded packets:             0, dropped packets:             0
ARP packet input number:             1
    Request packet:                  0
    Reply packet:                    1
    Unknown packet:                  0
Internet Address is allocated by DHCP, 192.168.1.253/24
Broadcast address : 0.0.0.0
TTL being 1 packet number:           0
TTL invalid packet number:           0
ICMP packet input number:            0
    Echo reply:                      0
    Unreachable:                     0
    Source quench:                   0
    Routing redirect:                0
    Echo request:                    0
    Router advert:                   0
    Router solicit:                  0
    Time exceed:                     0
    IP header bad:                   0
    Timestamp request:               0
```

```
  Timestamp reply:                0
  Information request:            0
  Information reply:              0
  Netmask request:                0
  Netmask reply:                  0
  Unknown type:                   0
```

可以看到 S1 已获取到 IP 地址 192.168.1.253/24。

查看 S1 的路由表

```
[S1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   OPR     60   0           D   192.168.1.254   GE1/0/1
      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
    192.168.1.0/24  Direct  0    0           D   192.168.1.253   GE1/0/1
  192.168.1.253/32  Direct  0    0           D   127.0.0.1       GE1/0/1
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GE1/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

可以看到 S1 已经有一条指向网关的缺省路由。

验证 S1 到达 DHCP Server 的连通性

```
[S1] ping 10.0.12.254
  PING 10.0.12.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.254: bytes=56 Sequence=1 ttl=253 time=1 ms
    Reply from 10.0.12.254: bytes=56 Sequence=2 ttl=253 time=1 ms
    Reply from 10.0.12.254: bytes=56 Sequence=3 ttl=253 time=1 ms
    Reply from 10.0.12.254: bytes=56 Sequence=4 ttl=253 time=1 ms
    Reply from 10.0.12.254: bytes=56 Sequence=5 ttl=253 time=1 ms

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

可以看到 S1 已经可以访问 DHCP Server。

7.3 配置参考

7.3.1 S1 的配置

```
sysname S1
#
dhcp enable
#
interface GE1/0/1
 undo portswitch
 ip address dhcp-alloc
#
```

7.3.2 R1 的配置

```
sysname R1
#
dhcp enable
#
interface GE0/0/1
 ip address 192.168.1.254 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 10.0.12.254
#
interface GE0/0/2
 ip address dhcp-alloc
#
```

7.3.3 S2 的配置

```
sysname S2
#
ip pool for_r1
 network 10.0.12.0 mask 255.255.255.0
 dns-list 10.0.12.254
 gateway-list 10.0.12.254
 lease day 2 hour 2 minute 0
#
ip pool for_s1
 network 192.168.1.0 mask 255.255.255.0
 gateway-list 192.168.1.254
 static-bind ip-address 192.168.1.253 mac-address 20df-73f5-44e2
#
dhcp enable
#
```

```
interface GE1/0/1
 undo portswitch
 ip address 10.0.12.254 255.255.255.0
 dhcp select global
#
interface GE1/0/10
 shutdown
 port link-type access
#
interface GE1/0/11
 shutdown
 port link-type access
#
interface GE1/0/12
 shutdown
 port link-type access
#
interface GE1/0/13
 shutdown
 port link-type access
#
interface GE1/0/14
 shutdown
 port link-type access
#
ip route-static 192.168.1.0 255.255.255.0 10.0.12.105
```

7.4 思考题

1. 全局地址池和接口地址池的应用场景有什么不同呢?

答案：接口地址池适用于当前接口只给 DHCP Client 分配与接口同一网段的 IP 地址的场景。

全局地址池可以给 DHCP Client 分配与接口同网段的 IP 地址，也可以分配不同网段的 IP 地址（DHCP 中继组网）。

2. 若有多个全局地址池，如何确定该给 DHCP Client 分配哪一个全局地址池里的地址?

答案：无中继场景：在所有全局地址池中查找与接口同一网段的地址池，根据该地址池设置的参数进行分配。有中继场景：根据中继所请求的网段，在所有全局地址池中查找相同网段的地址池，根据该地址池设置的参数进行分配。

8 OSPF 配置实验

8.1 实验介绍

8.1.1 关于本实验

OSPF（Open Shortest Path First，开放式最短路径优先）是 IETF 组织开发的一个基于链路状态的 IGP（Interior Gateway Protocol，内部网关协议）。目前针对 IPv4 协议使用的是 OSPF Version 2（RFC2328）；OSPF 作为基于链路状态的协议，具有以下优点：

- OSPF 采用组播形式收发报文，这样可以减少对其它不运行 OSPF 网络设备的影响。
- OSPF 支持无类别域间路由。
- OSPF 支持对等价路由进行负载分担。
- OSPF 支持报文认证。

由于 OSPF 具有以上优势，使得 OSPF 作为优秀的内部网关协议被快速接受并广泛使用。

本实验将通过配置单区域 OSPF，帮助学员理解 OSPF 基本配置与原理。

8.1.2 实验目的

- 掌握 OSPF 的基本配置命令
- 掌握如何查看 OSPF 的运行状态
- 掌握如何通过 Cost 控制 OSPF 选路
- 掌握 OSPF 发布默认路由的方法
- 掌握 OSPF 认证配置方法

8.1.3 实验组网介绍

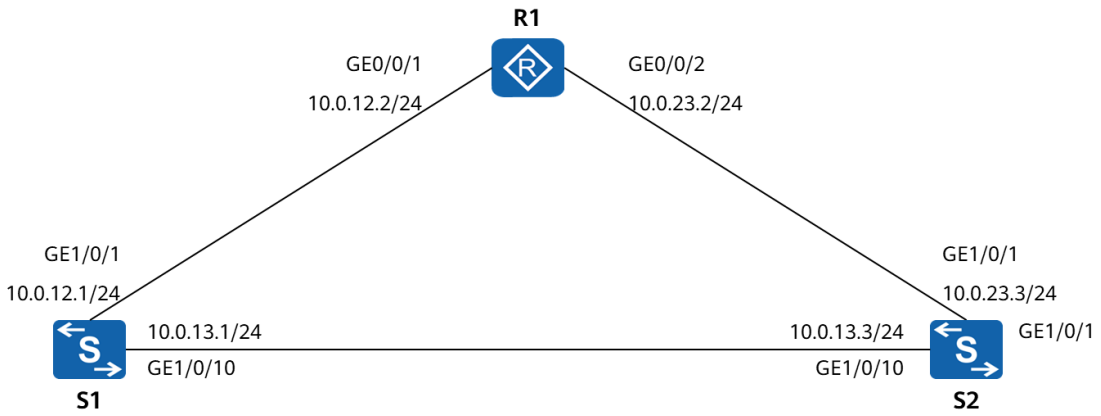


图8-1 OSPF 配置实验拓扑

8.1.4 实验背景

R1、S1、S2 都是各自网络的网关设备，现在需要通过 OSPF 动态路由协议，来实现这些网络之间的互通。

8.2 实验任务配置

8.2.1 配置思路

1. 创建 OSPF 进程并使能接口的 OSPF 功能
2. 配置 OSPF 认证
3. 通过 OSPF 发布默认路由
4. 通过修改 Cost 值控制 OSPF 选路

8.2.2 配置步骤

步骤 1 设备基础配置

设备命名

略。

关闭不使用的端口

```
[S1] interface GE 1/0/11
[S1-GE1/0/11] shutdown
[S1-GE1/0/11] quit
[S1] interface GE 1/0/12
[S1-GE1/0/12] shutdown
[S1-GE1/0/12] quit
[S1] interface GE 1/0/13
[S1-GE1/0/13] shutdown
[S1-GE1/0/13] quit
[S1] interface GE 1/0/14
[S1-GE1/0/14] shutdown
[S1-GE1/0/14] quit
```

```
[S2] interface GE 1/0/11
[S2-GE1/0/11] shutdown
[S2-GE1/0/11] quit
[S2] interface GE 1/0/12
[S2-GE1/0/12] shutdown
[S2-GE1/0/12] quit
[S2] interface GE 1/0/13
[S2-GE1/0/13] shutdown
[S2-GE1/0/13] quit
[S2] interface GE 1/0/14
[S2-GE1/0/14] shutdown
[S2-GE1/0/14] quit
```

接口初始化配置

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] undo portswitch
[R1-GE0/0/2] quit
```

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] undo port link-type
[S1-GE1/0/1] undo portswitch
[S1-GE1/0/1] quit
[S1] interface GE 1/0/10
[S1-GE1/0/10] undo port link-type
[S1-GE1/0/10] undo portswitch
[S1-GE1/0/10] quit
```

```
[S2] interface GE 1/0/1
```

```
[S2-GE1/0/1] undo port link-type
[S2-GE1/0/1] undo portswitch
[S2-GE1/0/1] quit
[S2] interface GE 1/0/10
[S2-GE1/0/10] undo port link-type
[S2-GE1/0/10] undo portswitch
[S2-GE1/0/10] quit
```

步骤 2 配置物理接口的 IP 地址

按照下表配置网络设备物理接口的 IP 地址

表8-1 设备物理接口 IP

网络设备	接口	IP Address/Mask
R1	GE0/0/1	10.0.12.2/24
	GE0/0/2	10.0.23.2/24
S1	GE1/0/1	10.0.12.1/24
	GE1/0/10	10.0.13.1/24
S2	GE1/0/1	10.0.23.3/24
	GE1/0/10	10.0.13.3/24

```
[R1] interface GE0/0/1
[R1-GE0/0/1] ip address 10.0.12.2 24
[R1-GE0/0/1] quit
[R1] interface GE0/0/2
[R1-GE0/0/2] ip address 10.0.23.2 24
[R1-GE0/0/2] quit
```

```
[S1] interface GE1/0/1
[S1-GE1/0/1] ip address 10.0.12.1 24
[S1-GE1/0/1] quit
[S1] interface GE1/0/10
[S1-GE1/0/10] ip address 10.0.13.1 24
[S1-GE1/0/10] quit
```

```
[S2] interface GE1/0/1
[S2-GE1/0/1] ip address 10.0.23.3 24
[S2-GE1/0/1] quit
[S2] interface GE1/0/10
[S2-GE1/0/10] ip address 10.0.13.3 24
```

```
[S2-GE1/0/10] quit
```

使用 Ping 工具测试连通性

```
[R1] 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=254 time=11 ms
    Reply from 10.0.12.1: bytes=56 Sequence=2 ttl=254 time=9 ms
    Reply from 10.0.12.1: bytes=56 Sequence=3 ttl=254 time=11 ms
    Reply from 10.0.12.1: bytes=56 Sequence=4 ttl=254 time=9 ms
    Reply from 10.0.12.1: bytes=56 Sequence=5 ttl=254 time=9 ms

  --- 10.0.12.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 9/9/11 ms
```

```
[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=11 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=254 time=7 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=254 time=11 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=254 time=10 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=254 time=8 ms

  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 7/9/11 ms
```

步骤 3 创建并配置 LoopBack 接口

按照下表配置设备的 LoopBack 接口

表8-2 LoopBack 接口 IP

网络设备	接口	IP Address/Mask
R1	LoopBack0	10.0.2.2/32
S1	LoopBack0	10.0.1.1/32
S2	LoopBack0	10.0.3.3/32

LoopBack 接口属于设备上的逻辑接口，逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口。LoopBack 接口创建后除非手工关闭该接口，否则 LoopBack 接口物理层状态和协议状态永远处于 UP 状态。一般情况下，LoopBack 接口使用 32 位掩码。使用 LoopBack 接口一般有如下目的：

1. 作为网络设备的管理地址。
2. 使用该接口地址作为动态路由协议的 Router ID。
3. 其它提高网络可靠性的用途。

```
[R1] interface LoopBack0
[R1-LoopBack0] ip address 10.0.2.2 32
[R1-LoopBack0] quit
```

```
[S1] interface LoopBack0
[S1-LoopBack0] ip address 10.0.1.1 32
[S1-LoopBack0] quit
```

```
[S2] interface LoopBack0
[S2-LoopBack0] ip address 10.0.3.3 32
[S2-LoopBack0] quit
```

测试各 LoopBack 接口之间的连通性

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

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

此时由于 R1 上没有到达该目的 IP 的路由条目，所以无法 Ping 通。

步骤 4 完成 OSPF 基本配置

创建 OSPF 进程

```
[R1] ospf 1
```

创建 OSPF 进程是配置与 OSPF 协议有关参数的首要步骤。OSPF 支持多进程，在同一台设备上可以运行多个不同的 OSPF 进程，它们之间互不影响，彼此独立。不同 OSPF 进程之间的路由交互相当于不同路由协议之间的路由交互。可以在创建 OSPF 进程时指定进程号，若不指定，默认进程号为 1。

创建 OSPF 区域并使能相应的接口

```
[R1-ospf-1] area 0
```

area 命令用来创建 OSPF 区域，并进入 OSPF 区域视图。

```
[R1-ospf-1-area-0.0.0.0] network 10.0.12.2 0.0.0.255
[R1-ospf-1-area-0.0.0.0] network 10.0.23.2 0.0.0.255
[R1-ospf-1-area-0.0.0.0] network 10.0.2.2 0.0.0.0
[R1-ospf-1-area-0.0.0.0] quit
[R1-ospf-1] quit
```

network *network-address wildcard-mask* 用来指定运行 OSPF 协议的接口。满足下面两个条件，OSPF 协议才能在接口上运行：

1. 接口的 IP 地址掩码长度≥**network** 命令中的掩码长度。
2. 接口的 IP 地址必须在 **network** 命令指定的网段范围之内。

此时三个接口都被使能，同时属于区域 0。

```
[S1] ospf
Warning: If router-id is not specified, the router ID may change after the restart or a router ID conflict may occur.
[S1-ospf-1] area 0
[S1-ospf-1-area-0.0.0.0] network 10.0.12.1 0.0.0.0
[S1-ospf-1-area-0.0.0.0] network 10.0.13.1 0.0.0.0
[S1-ospf-1-area-0.0.0.0] network 10.0.1.1 0.0.0.0
[S1-ospf-1-area-0.0.0.0] quit
[S1-ospf-1] quit
```

当 **network** 命令配置的 *wildcard-mask* 为全 0 时，如果接口的 IP 地址与 *network-address* 配置的 IP 地址相同，则此接口也会运行 OSPF 协议。

```
[S2] ospf
Warning: If router-id is not specified, the router ID may change after the restart or a router ID conflict may occur.
[S2-ospf-1] area 0
[S2-ospf-1-area-0.0.0.0] network 10.0.13.3 0.0.0.0
[S2-ospf-1-area-0.0.0.0] network 10.0.23.3 0.0.0.0
[S2-ospf-1-area-0.0.0.0] network 10.0.3.3 0.0.0.0
[S2-ospf-1-area-0.0.0.0] quit
[S2-ospf-1] quit
```

步骤 5 查看 OSPF 状态

查看 OSPF 邻居

```
[R1] display ospf peer
OSPF Process 1 with Router ID 10.0.12.2
 Area 0.0.0.0 interface 10.0.12.2 (GE0/0/1)'s neighbors
  Router ID: 10.0.12.1          Address : 10.0.12.1
  State      : Full             Mode      : Nbr is Slave      Priority: 1
  DR         : 10.0.12.2        BDR       : 10.0.12.1         MTU      : 0
  Dead timer due (in seconds) : 35
  Retrans timer interval      : 5
  Neighbor up time            : 00h02m13s
  Neighbor up time stamp      : XXXX-XX-XX 11:46:41
  Authentication Sequence     : 0

 Area 0.0.0.0 interface 10.0.23.2 (GE0/0/2)'s neighbors
  Router ID: 10.0.23.3          Address : 10.0.23.3
  State      : Full             Mode      : Nbr is Master     Priority: 1
  DR         : 10.0.23.2        BDR       : 10.0.23.3         MTU      : 0
  Dead timer due (in seconds) : 34
  Retrans timer interval      : 5
  Neighbor up time            : 00h00m47s
  Neighbor up time stamp      : XXXX-XX-XX 11:48:07
  Authentication Sequence     : 0
```

display ospf peer 命令用来显示 OSPF 中各区域邻居的信息。包括邻居所属的区域、邻居 Router ID、邻居状态、DR 和 BDR 等信息。

从输出信息得知，R1 的 Router ID 为 10.0.12.2，S1 的 Router ID 为 10.0.12.1，S2 的 Router ID 为 10.0.23.3。同时，也可以看到 R1 GE0/0/1 接口所在网段的 DR 是 R1，BDR 是 S1。

说明：不同实验环境的 DR、BDR、Router ID 可能不同，这是因为 OSPF Router ID 可以自动配置，DR 和 BDR 的选举是非抢占式的。

步骤 6 修改 OSPF 网络设备的 Router ID

修改 OSPF 网络设备的 Router ID 为 LoopBack0 接口的 IP 地址，并重启 OSPF 进程使 Router ID 生效

```
[R1] ospf 1 router-id 10.0.2.2
Warning: The operation will cause reset OSPF. Continue? [Y/N] : y
[R1-ospf-1] quit
```

```
[S1] ospf 1 router-id 10.0.1.1
Warning: The operation will cause reset OSPF. Continue? [Y/N] : y
[S1-ospf-1] quit
```

```
[S2] ospf 1 router-id 10.0.3.3
Warning: The operation will cause reset OSPF. Continue? [Y/N] : y
[S2-ospf-1] quit
```

查看 OSPF 邻居

```
[R1] display ospf peer
OSPF Process 1 with Router ID 10.0.2.2
 Area 0.0.0.0 interface 10.0.12.2 (GE0/0/1)'s neighbors
  Router ID: 10.0.1.1              Address : 10.0.12.1
  State      : Full                Mode      : Nbr is Slave        Priority: 1
  DR         : 10.0.12.2           BDR       : 10.0.12.1           MTU       : 0
  Dead timer due (in seconds) : 36
  Retrans timer interval      : 5
  Neighbor up time            : 00h00m38s
  Neighbor up time stamp      : XXXX-XX-XX 11:53:11
  Authentication Sequence     : 0

 Area 0.0.0.0 interface 10.0.23.2 (GE0/0/2)'s neighbors
  Router ID: 10.0.3.3              Address : 10.0.23.3
  State      : Full                Mode      : Nbr is Master       Priority: 1
  DR         : 10.0.23.2           BDR       : 10.0.23.3           MTU       : 0
  Dead timer due (in seconds) : 37
  Retrans timer interval      : 5
  Neighbor up time            : 00h00m09s
  Neighbor up time stamp      : XXXX-XX-XX 11:53:40
  Authentication Sequence     : 0
```

可以看到 Router ID 已经和各设备 LoopBack0 接口 IP 地址相同。

查看 IP 路由表中由 OSPF 学习到的路由

```
[R1] display ip routing-table protocol ospf
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
_public_ Routing Table : OSPF
         Destinations : 6        Routes : 7

OSPF routing table status : <Active>
         Destinations : 3        Routes : 4

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32 OSPF    10   1           D   10.0.12.1       GE0/0/1
        10.0.3.3/32 OSPF    10   1           D   10.0.23.3       GE0/0/2
       10.0.13.0/24 OSPF    10   2           D   10.0.23.3       GE0/0/2
```

```
                    OSPF    10    2             D    10.0.12.1       GE0/0/1

OSPF routing table status : <Inactive>
         Destinations : 3        Routes : 3

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.2.2/32  OSPF    10   0             10.0.2.2        LoopBack0
       10.0.12.0/24  OSPF    10   1             10.0.12.2       GE0/0/1
       10.0.23.0/24  OSPF    10   1             10.0.23.2       GE0/0/2
```

从输出结果可以看到有 3 条 OSPF 路由已放入 IP 路由表，其中 10.0.13.0/24 有两条等价路由，这是因为 R1 通过 S1 或者 S2 都可以到达该网络。R1 到达 S1 和 S2 环回口地址的 Cost 值为 1，出接口均为直连接口。

此外，有 3 条 OSPF 路由处于 **Inactive** 状态，不难看出这三条路由和接口配置 IP 地址后产生的直连路由相同，因为直连路由优先级最高，因此这三条 OSPF 路由未被放入路由表。

步骤 7 配置 OSPF 认证

在 R1 上配置接口认证

```
[R1] interface GE0/0/1
[R1-GE0/0/1] ospf authentication-mode hmac-sha256 1 cipher HCIA-Datacom
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] ospf authentication-mode hmac-sha256 1 cipher HCIA-Datacom
[R1-GE0/0/2] display this
#
interface GE0/0/2
 ip address 10.0.23.2 255.255.255.0
 ospf authentication-mode hmac-sha256 1
cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!Iy81!>Czw!oJ345&&,YP*U%`C,a@@'Gl}TD!!!!!2jp5!!!!!!=!!!!IJ^>%Jf#G9!yb:JKM|W'0jav3[$}ZQ[b>r:!!!!!%+%#
#
return
[R1-GE0/0/2] quit
```

由于 **cipher** 是密文口令类型，所以查看配置时以密文方式显示口令。

等待一会，查看当前的邻居状态

```
[R1] display ospf peer brief
```

由于其它网络设备还未配置认证，所以认证不通过，无邻居。

配置 S1 上的接口认证

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] ospf authentication-mode hmac-sha256 1 cipher HCIA-Datacom
```

```
[S1-GE1/0/1] quit
[S1] interface GE 1/0/10
[S1-GE1/0/10] ospf authentication-mode hmac-sha256 1 cipher HCIA-Datacom
[S1-GE1/0/10] quit
```

查看 S1 的邻居状态

```
[S1] display ospf peer

(M) Indicates MADJ neighbor

OSPF Process 1 with Router ID 10.0.1.1
 Area 0.0.0.0 interface 10.0.12.1 (GE1/0/1)'s neighbors
  Router ID: 10.0.2.2                Address : 10.0.12.2
  State      : Full                  Mode      : Nbr is Master          Priority: 1
  DR         : 10.0.12.2             BDR       : 10.0.12.1              MTU       : 0
  Dead timer due (in seconds) : 35
  Retrans timer interval      : 5
  Neighbor up time            : 00h00m34s
  Neighbor up time stamp      : XXXX-XX-XX 09:23:33
  Authentication Sequence     : 1013
```

此时 S1 已经和 R1 建立邻接关系。

在 S2 上配置区域认证

```
[S2] ospf
[S2-ospf-1] area 0
[S2-ospf-1-area-0.0.0.0] authentication-mode hmac-sha256 1 cipher HCIA-Datacom
[S2-ospf-1-area-0.0.0.0] quit
[S2-ospf-1] quit
```

查看 S2 上的邻居状态

```
[S2] display ospf peer brief

(M) Indicates MADJ neighbor

OSPF Process 1 with Router ID 10.0.3.3
                    Peer Statistic Information
Total number of peer(s): 2
 Peer(s) in full state: 2
--------------------------------------------------------------------------
 Area Id          Interface                  Neighbor id          State
 0.0.0.0          GE1/0/1                    10.0.2.2             Full
 0.0.0.0          GE1/0/10                   10.0.1.1             Full
--------------------------------------------------------------------------
```

此时 S2 已经和 R1、S1 建立邻接关系。说明 OSPF 接口认证与区域认证产生的效果都是在设备的 OSPF 接口上实现 OSPF 报文认证。

步骤 8 假设 R1 为网络出口，在 R1 上通告默认路由

在 R1 上通告默认路由

```
[R1] ospf
[R1-ospf-1] default-route-advertise always
[R1-ospf-1] quit
```

default-route-advertise 命令用来将默认路由通告到普通 OSPF 区域，如果没有配置 **always** 参数，本机路由表中必须有激活的非本 OSPF 进程的默认路由时，才向其它网络设备发布默认路由。本例中，本地路由表中没有默认路由，所以需要增加 **always** 参数。

查看 S1 与 S2 上的 IP 路由表

```
[S1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 15        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   10.0.12.2       GE1/0/1
       10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.2.2/32  OSPF    10   1           D   10.0.12.2       GE1/0/1
       10.0.3.3/32  OSPF    10   1           D   10.0.13.3       GE1/0/10
      10.0.12.0/24  Direct  0    0           D   10.0.12.1       GE1/0/1
      10.0.12.1/32  Direct  0    0           D   127.0.0.1       GE1/0/1
    10.0.12.255/32  Direct  0    0           D   127.0.0.1       GE1/0/1
      10.0.13.0/24  Direct  0    0           D   10.0.13.1       GE1/0/10
      10.0.13.1/32  Direct  0    0           D   127.0.0.1       GE1/0/10
    10.0.13.255/32  Direct  0    0           D   127.0.0.1       GE1/0/10
      10.0.23.0/24  OSPF    10   2           D   10.0.13.3       GE1/0/10
                    OSPF    10   2           D   10.0.12.2       GE1/0/1
      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
```

```
[S2] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
```

```
Routing Table : _public_
         Destinations : 15        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   10.0.23.2       GE1/0/1
       10.0.1.1/32  OSPF    10   1           D   10.0.13.1       GE1/0/10
       10.0.2.2/32  OSPF    10   1           D   10.0.23.2       GE1/0/1
       10.0.3.3/32  Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.12.0/24  OSPF    10   2           D   10.0.13.1       GE1/0/10
                    OSPF    10   2           D   10.0.23.2       GE1/0/1
      10.0.13.0/24  Direct  0    0           D   10.0.13.3       GE1/0/10
      10.0.13.3/32  Direct  0    0           D   127.0.0.1       GE1/0/10
    10.0.13.255/32  Direct  0    0           D   127.0.0.1       GE1/0/10
      10.0.23.0/24  Direct  0    0           D   10.0.23.3       GE1/0/1
      10.0.23.3/32  Direct  0    0           D   127.0.0.1       GE1/0/1
    10.0.23.255/32  Direct  0    0           D   127.0.0.1       GE1/0/1
       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
```

S1、S2 已经学习到默认路由。

步骤 9 通过修改 R1 相应接口的 Cost 值，使得 R1 的 LoopBack0 接口通过 R1 -> S1 -> S2 的路径访问 S2 的 LoopBack0 接口

从 R1 的路由表可知，R1 通过 R1 -> S2 的路径访问 S2 LoopBack0 接口的路由开销为 1，故只要使 R1 -> S2 的路由开销大于 2 即可。

```
[R1] interface GE 0/0/2
[R1-GE0/0/2] ospf cost 10
[R1-GE0/0/2] quit
```

查看 R1 的路由表

```
[R1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.0.1.1/32  OSPF    10   1           D   10.0.12.1       GE0/0/1
       10.0.2.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.3.3/32  OSPF    10   2           D   10.0.12.1       GE0/0/1
```

```
      10.0.12.0/24   Direct  0    0           D   10.0.12.2       GE0/0/1
      10.0.12.2/32   Direct  0    0           D   127.0.0.1       GE0/0/1
    10.0.12.255/32   Direct  0    0           D   127.0.0.1       GE0/0/1
      10.0.13.0/24   OSPF    10   2           D   10.0.12.1       GE0/0/1
      10.0.23.0/24   Direct  0    0           D   10.0.23.2       GE0/0/2
      10.0.23.2/32   Direct  0    0           D   127.0.0.1       GE0/0/2
    10.0.23.255/32   Direct  0    0           D   127.0.0.1       GE0/0/2
      127.0.0.0/8    Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32   Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32   Direct  0    0           D   127.0.0.1       InLoopBack0
```

此时 R1 访问 S2 LoopBack0 接口的下一跳为 S1。

通过 Tracert 命令验证

```
[R1] tracert -a 10.0.2.2 10.0.3.3
 traceroute to 10.0.3.3(10.0.3.3), max hops: 64, packet length: 40, press CTRL_C to break
 1 10.0.12.1 11 ms   10 ms   10 ms
 2 10.0.3.3 10 ms   12 ms   10 ms
```

8.3 结果验证

请自行验证以下内容：

1. 通过 Ping 功能检查设备各接口之间的连通性。
2. 通过关闭接口模拟链路故障，查看路由表的变化。

8.4 配置参考

8.4.1 R1 的配置

```
sysname R1
#
interface GE0/0/1
 ip address 10.0.12.2 255.255.255.0
 ospf authentication-mode hmac-sha256 1 cipher HCIA-Datacom
#
interface GE0/0/2
 ip address 10.0.23.2 255.255.255.0
 ospf authentication-mode hmac-sha256 1 cipher HCIA-Datacom
 ospf cost 10
```

```
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.255
#
ospf 1 router-id 10.0.2.2
 default-route-advertise always
 area 0.0.0.0
  network 10.0.2.2 0.0.0.0
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
```

8.4.2 S1 的配置

```
sysname S1
#
interface GE1/0/1
 undo portswitch
 ip address 10.0.12.1 255.255.255.0
 ospf authentication-mode hmac-sha256 1 cipher HCIA-Datacom
#
interface GE1/0/10
 undo portswitch
 ip address 10.0.13.1 255.255.255.0
 ospf authentication-mode hmac-sha256 1 cipher HCIA-Datacom
#
interface GE1/0/11
 shutdown
 port link-type access
#
interface GE1/0/12
 shutdown
 port link-type access
#
interface GE1/0/13
 shutdown
 port link-type access
#
interface GE1/0/14
 shutdown
 port link-type access
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ospf 1 router-id 10.0.1.1
```

```
 area 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 10.0.12.1 0.0.0.0
  network 10.0.13.1 0.0.0.0
#
```

8.4.3 S2 的配置

```
sysname S2
#
interface GE1/0/1
 undo portswitch
 ip address 10.0.23.3 255.255.255.0
#
interface GE1/0/10
 undo portswitch
 ip address 10.0.13.3 255.255.255.0
#
interface GE1/0/11
 shutdown
 port link-type access
#
interface GE1/0/12
 shutdown
 port link-type access
#
interface GE1/0/13
 shutdown
 port link-type access
#
interface GE1/0/14
 shutdown
 port link-type access
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.255
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  authentication-mode hmac-sha256 1 cipher HCIA-Datacom
  network 10.0.3.3 0.0.0.0
  network 10.0.13.3 0.0.0.0
  network 10.0.23.3 0.0.0.0
#
```

8.5 思考题

1. 步骤 9 中，S2 回复 R1 的 ICMP 报文的路径是什么样的？试着解释一下原因。

答案：S2 回复 R1 的路径是：S2 -> R1。OSPF 计算路由时，依据的是接口出方向的 Cost 之和。

9 IPv6 地址配置实验

9.1 实验介绍

9.1.1 关于本实验

IPv6（Internet Protocol Version 6）也被称为 IPng（IP Next Generation）。它是 IETF（Internet Engineering Task Force，Internet 工程任务组）设计的一套规范，是 IPv4 的下一代版本。

相比较于 IPv4，IPv6 具有如下优势：

- 近乎无限的地址空间
- 层次化的地址结构
- 即插即用
- 简化的报文头部
- 安全特性
- 移动性
- 增强的 QoS 特性等

本章将通过搭建一个 IPv6 网络，帮助学员了解 IPv6 的基本原理和地址配置。

9.1.2 实验目的

- 掌握静态 IPv6 地址的配置方法
- 掌握 IPv6 无状态地址配置方法
- 掌握 IPv6 静态路由的配置方法
- 掌握 IPv6 相关信息查看方法

9.1.3 实验组网介绍

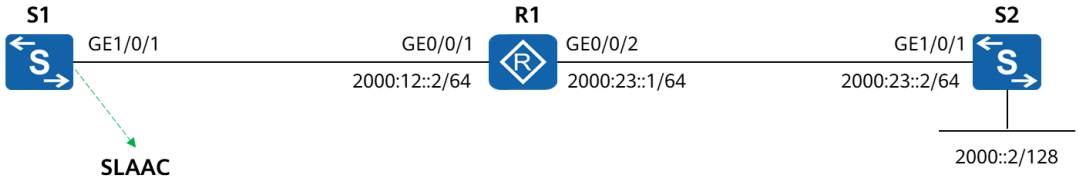


图9-1 IPv6 地址配置实验拓扑

1. R1 的两个接口均采用静态 IPv6 地址配置方法。
2. S1 的 GE1/0/1 接口采用无状态地址配置。
3. S1 获取 IPv6 地址后可以和 S2 LoopBack0 接口互通。

9.1.4 实验背景

某企业网络部署 IPv6 实现互通，需要对当前运行的网络设备进行配置。

9.2 实验任务配置

9.2.1 配置思路

1. 配置静态 IPv6 地址
2. 配置 IPv6 无状态地址分配
3. 配置 IPv6 静态路由

9.2.2 配置步骤

步骤 1 配置接口 IPv6 功能

使能接口的 IPv6 功能

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] undo port link-type
[S1-GE1/0/1] undo portswitch
[S1-GE1/0/1] ipv6 enable
[S1-GE1/0/1] quit
```

ipv6 enable 命令用来在接口上使能 IPv6 功能。

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ipv6 enable
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] undo portswitch
[R1-GE0/0/2] ipv6 enable
[R1-GE0/0/2] quit
```

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] undo port link-type
[S2-GE1/0/1] undo portswitch
[S2-GE1/0/1] ipv6 enable
[S2-GE1/0/1] quit
```

步骤 2 配置接口的 link-local 地址，并测试

配置接口自动生成 link-local 地址

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] ipv6 address auto link-local
[S1-GE1/0/1] quit
```

ipv6 address auto link-local 命令用来为接口配置自动生成的链路本地地址。

每个接口只能有一个链路本地地址，为了避免链路本地地址冲突，推荐使用链路本地地址的自动生成方式。当接口配置了 IPv6 全球单播地址后，同时会自动生成链路本地地址。

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] ipv6 address auto link-local
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] ipv6 address auto link-local
[R1-GE0/0/2] quit
```

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] ipv6 address auto link-local
[S2-GE1/0/1] quit
```

查看接口的 IPv6 状态信息，并测试连通性

```
[S1] display ipv6 interface GE 1/0/1
GE1/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::22DF:7300:2F5:44E2
```

```
  No global unicast address configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFF5:44E2
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
  ND Proxy is disabled
```

S1 GE1/0/1 接口的 link-local 地址是 FE80::22DF:7300:2F5:44E2。

说明：link-local 地址由设备自动生成，不同实验环境有所不同。

```
[R1] display ipv6 interface GE 0/0/1
GE0/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::B2C7:87FF:FE33:D660
  No global unicast address configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF33:D660
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
```

R1 GE0/0/1 接口的 link-local 地址是 FE80::B2C7:87FF:FE33:D660。

```
[R1] display ipv6 interface GE 0/0/2
GE0/0/2 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::B2C7:87FF:FE33:D661
  No global unicast address configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF33:D661
```

```
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
```

R1 GE0/0/2 接口的 link-local 地址是 FE80::B2C7:87FF:FE33:D661。

```
[S2] display ipv6 interface GE 1/0/1
GE1/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::22DF:7300:2F5:4572
  No global unicast address configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFF5:4572
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
  ND Proxy is disabled
```

S2 GE1/0/1 接口的 link-local 地址是 FE80::22DF:7300:2F5:4572。

测试 S1 与 R1 连通性

```
[S1] ping ipv6 FE80::B2C7:87FF:FE33:D660 -i GE 1/0/1
  PING FE80::B2C7:87FF:FE33:D660 : 56  data bytes, press CTRL_C to break
    Reply from FE80::B2C7:87FF:FE33:D660
    bytes=56 Sequence=1 hop limit=64 time=13 ms
    Reply from FE80::B2C7:87FF:FE33:D660
    bytes=56 Sequence=2 hop limit=64 time=2 ms
    Reply from FE80::B2C7:87FF:FE33:D660
    bytes=56 Sequence=3 hop limit=64 time=10 ms
    Reply from FE80::B2C7:87FF:FE33:D660
    bytes=56 Sequence=4 hop limit=64 time=4 ms
    Reply from FE80::B2C7:87FF:FE33:D660
    bytes=56 Sequence=5 hop limit=64 time=7 ms

  --- FE80::B2C7:87FF:FE33:D660 ping statistics---
```

```
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max=2/7/13 ms
```

当 Ping 测试的目的 IPv6 地址为 link-local 地址时，必须指定源接口或源 IPv6 地址。

步骤 3 配置接口静态 IPv6 地址

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] ipv6 address 2000:12::2 64
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] ipv6 address 2000:23::1 64
[R1-GE0/0/2] quit
```

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] ipv6 address 2000:23::2 64
[S2-GE1/0/1] quit
[S2] interface LoopBack 0
[S2-LoopBack0] ipv6 enable
[S2-LoopBack0] ipv6 address 2000::2 128
[S2-LoopBack0] quit
```

在 R1 Ping S2 的接口 IP 地址

```
[R1] ping ipv6 2000:23::2
  PING 2000:23::2 : 56  data bytes, press CTRL_C to break
    Reply from 2000:23::2
    bytes=56 Sequence=1 hop limit=63 time=11 ms
    Reply from 2000:23::2
    bytes=56 Sequence=2 hop limit=63 time=14 ms
    Reply from 2000:23::2
    bytes=56 Sequence=3 hop limit=63 time=9 ms
    Reply from 2000:23::2
    bytes=56 Sequence=4 hop limit=63 time=11 ms
    Reply from 2000:23::2
    bytes=56 Sequence=5 hop limit=63 time=10 ms

  --- 2000:23::2 ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max=9/11/14 ms
```

在 R1 查看 GE0/0/2 接口的 IPv6 邻居信息

```
[R1] display ipv6 neighbors GE 0/0/2
------------------------------------------------------------------------------
IPv6 Address : 2000:23::2
Link-layer    : 20df-73f5-4572                State       : REACH
Interface     : GE0/0/2                       Age         : 6
VLAN          : -                             CEVLAN      : -
VPN name      : -                             Is Router : TRUE
Secure FLAG   : UN-SECURE                     Nickname    : -
Source IP     : -
Destination IP: -
VNI           : -                             BD          : -

------------------------------------------------------------------------------
Total: 1          Dynamic: 1        Static: 0        Remote: 0
```

可以看到 S2 接口的 MAC 地址是 20df-73f5-4572，与 IPv4 通过 ARP 获取 MAC 地址不同，IPv6 通过 NS 和 NA 报文发现邻居设备的 MAC 地址。

步骤 4 配置 S1 通过无状态方式获取 IPv6 地址

配置 S1

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] ipv6 address auto global default
[S1-GE1/0/1] quit
```

ipv6 address auto global 命令用来使能无状态自动生成 IPv6 全局地址功能。

ipv6 address auto global default 命令用来使能设备将 RA 报文中源 IPv6 地址作为缺省路由的下一跳地址的功能。

配置 R1

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] ipv6 nd ra halt disable
[R1-GE0/0/1] ipv6 nd ra prefix 2000:12::/64 3600 1200
[R1-GE0/0/1] quit
```

ipv6 nd ra halt disable 命令用来开启系统发布 RA 报文的功能。

ipv6 nd ra prefix 命令用来配置 RA 报文中的前缀消息。

valid-lifetime 指定前缀信息的有效存活时间，有效存活时间用于确定前缀的 on-link 状态，此处设置为 3600 秒。若指定该参数，用户收到的 RA 报文，其前缀信息在指定时间内有效。

preferred-lifetime 指定通过无状态地址自动配置从前缀生成的地址保持首选的时间长度，此处设置为 1200 秒。首选存活时间小于等于有效存活时间。

查看 S1 获取的 IPv6 地址

```
[S1] display ipv6 interface GE 1/0/1
```

```
GE1/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::22DF:7300:2F5:44E2
  Global unicast address(es):
    2000:12::22DF:7300:2F5:44E2,
    subnet is 2000:12::/64 [SLAAC XXXX-XX-XX 02:22:01 3600S]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFF5:44E2
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
  ND Proxy is disabled
```

S1 已经自动配置了 IPv6 地址 2000:12::22DF:7300:2F5:44E2，地址前 64 位是 R1 通告的前缀，后 64 位和链路本地地址的最后 64 位相同。

查看 S1 的 IPv6 路由表

```
[S1] display ipv6 routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 7        Routes : 7

Destination  : ::                                PrefixLength : 0
NextHop      : FE80::B2C7:87FF:FE33:D660         Preference   : 64
Cost         : 0                                 Protocol     : ND
RelayNextHop : ::                                TunnelID     : 0x0
Interface    : GE1/0/1                           Flags        : D

Destination  : ::1                               PrefixLength : 128
NextHop      : ::1                               Preference   : 0
Cost         : 0                                 Protocol     : Direct
RelayNextHop : ::                                TunnelID     : 0x0
Interface    : InLoopBack0                       Flags        : D

Destination  : ::FFFF:127.0.0.0                  PrefixLength : 104
NextHop      : ::FFFF:127.0.0.1                  Preference   : 0
Cost         : 0                                 Protocol     : Direct
RelayNextHop : ::                                TunnelID     : 0x0
Interface    : InLoopBack0                       Flags        : D
```

```
  ---- More ----
```

S1 已经自动生成了下一跳为 R1 的链路本地地址的缺省路由，该路由的优先级为 64，协议类型为 ND。

在 S1 Ping S2 的环回口地址

```
[S1] ping ipv6 2000::2
  PING 2000::2 : 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 2000::2 ping statistics---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
    round-trip min/avg/max=0/0/0 ms
```

此时无法 Ping 通，因为 R1 和 S2 还没有配置路由。

步骤 5 配置 IPv6 静态路由

配置 R1 和 S2 的静态路由

```
[R1] ipv6 route-static 2000::2 128 2000:23::2
```

ipv6 route-static 命令用来配置公网 IPv6 静态路由。

```
[S2] ipv6 route-static 2000:12:: 64 2000:23::1
```

检测连通性

```
[S1] ping ipv6 2000::2
  PING 2000::2 : 56  data bytes, press CTRL_C to break
    Reply from 2000::2
    bytes=56 Sequence=1 hop limit=62 time=1 ms
    Reply from 2000::2
    bytes=56 Sequence=2 hop limit=62 time=1 ms
    Reply from 2000::2
    bytes=56 Sequence=3 hop limit=62 time=1 ms
    Reply from 2000::2
    bytes=56 Sequence=4 hop limit=62 time=1 ms
    Reply from 2000::2
    bytes=56 Sequence=5 hop limit=62 time=1 ms
```

```
  --- 2000::2 ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max=1/1/1 ms
```

S1 已经可以和 S2 的环回口互通。

9.3 配置参考

9.3.1 R1 的配置

```
sysname R1
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2000:12::2/64
 ipv6 address auto link-local
 ipv6 nd ra prefix 2000:12::/64 3600 1200
 ipv6 nd ra halt disable
#
interface GE0/0/2
 ipv6 enable
 ipv6 address 2000:23::1/64
 ipv6 address auto link-local
#
ipv6 route-static 2000::2 128 2000:23::2
```

9.3.2 S1 的配置

```
sysname S1
#
interface GE1/0/1
 undo portswitch
 ipv6 enable
 ipv6 address auto link-local
 ipv6 address auto global default
#
```

9.3.3 S2 的配置

```
sysname S2
```

```
#
interface GE1/0/1
 undo portswitch
 ipv6 enable
 ipv6 address 2000:23::2/64
 ipv6 address auto link-local
#
interface LoopBack0
 ipv6 enable
 ipv6 address 2000::2/128
#
ipv6 route-static 2000:12:: 64 2000:23::1
```

9.4 思考题

1. 为什么检查 link-local 地址之间的连通性时，必须指定源接口?

答案：因为网络设备上存在多个接口，且这些接口都属于 FE80::/10 网段，当目的 IPv6 地址为 link-local 地址时，无法通过查询路由表确定出接口，所以必须指定源接口。

10 ACL 配置实验

10.1 实验介绍

10.1.1 关于本实验

ACL（Access Control List，访问控制列表）是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。

ACL 本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用 ACL 的业务模块的处理策略来允许或阻止该报文通过。

10.1.2 实验目的

- 掌握 ACL 的配置方法
- 掌握 ACL 在接口下的应用方法
- 掌握流量过滤的基本方式

10.1.3 实验组网介绍

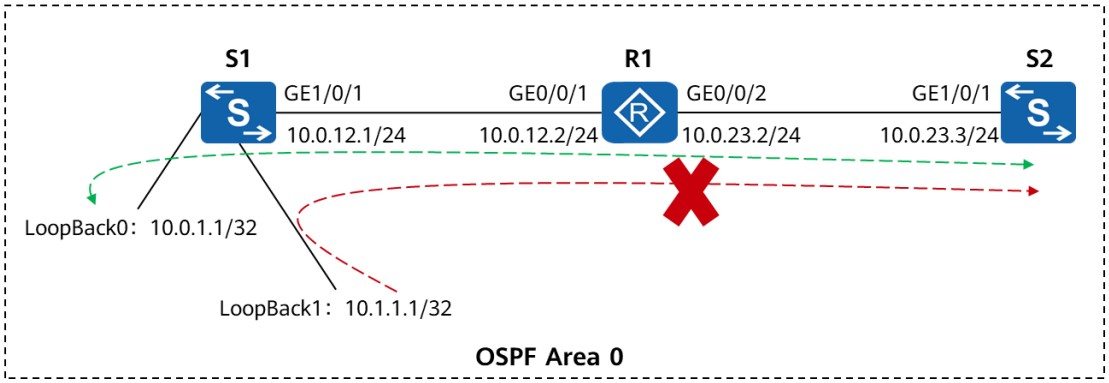


图10-1 ACL 配置实验拓扑

10.1.4 实验背景

如组网图所示，S1、R1、S2 之间路由可达。S1 上创建两个逻辑接口 LoopBack0 和 LoopBack1，地址分别为 10.0.1.1/32 和 10.1.1.1/32。

通过配置 ACL 实现 S1 的 Loopbak0 接口可以 Ping 通 S2 的接口地址，而 S1 的 Loopback1 接口不能 Ping 通。

10.2 实验任务配置

10.2.1 配置思路

1. 配置设备 IP 地址
2. 配置 OSPF，使得网络路由可达
3. 配置 ACL，匹配特定流量
4. 配置流量过滤

10.2.2 配置步骤

步骤 1 配置设备 IP 地址

配置 R1、S1 和 S2 的 IP 地址

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ip address 10.0.12.2 24
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] undo portswitch
[R1-GE0/0/2] ip address 10.0.23.2 24
[R1-GE0/0/2] quit
```

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] undo port link-type
[S1-GE1/0/1] undo portswitch
[S1-GE1/0/1] ip address 10.0.12.1 24
[S1-GE1/0/1] quit
[S1] interface LoopBack 0
[S1-LoopBack0] ip address 10.0.1.1 32
[S1-LoopBack0] quit
[S1] interface LoopBack 1
[S1-LoopBack1] ip address 10.1.1.1 32
```

```
[S1-LoopBack1] quit
```

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] undo port link-type
[S2-GE1/0/1] undo portswitch
[S2-GE1/0/1] ip address 10.0.23.3 24
[S2-GE1/0/1] quit
```

步骤 2 配置 OSPF 使网络互通

在 R1、S1 和 S2 上配置 OSPF，三台设备均在区域 0 中，实现全网互通

```
[R1] ospf
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 10.0.12.2 0.0.0.0
[R1-ospf-1-area-0.0.0.0] network 10.0.23.2 0.0.0.0
[R1-ospf-1-area-0.0.0.0] quit
[R1-ospf-1] quit
```

```
[S1] ospf
[S1-ospf-1] area 0
[S1-ospf-1-area-0.0.0.0] network 10.0.12.1 0.0.0.0
[S1-ospf-1-area-0.0.0.0] network 10.0.1.1 0.0.0.0
[S1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[S1-ospf-1-area-0.0.0.0] quit
[S1-ospf-1] quit
```

```
[S2] ospf
[S2-ospf-1] area 0
[S2-ospf-1-area-0.0.0.0] network 10.0.23.3 0.0.0.0
[S2-ospf-1-area-0.0.0.0] quit
[S2-ospf-1] quit
```

在 S1 上执行 Ping 命令，检测网络的连通性

```
[S1] ping -a 10.0.1.1 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=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=253 time=1 ms

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

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

```
[S1] ping -a 10.1.1.1 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=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=253 time=1 ms

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

步骤 3 配置 ACL 进行流量过滤

在 R1 上配置 ACL，拒绝源地址为 10.1.1.1 的报文，允许其它报文通过

```
[R1] acl 3000
[R1-acl4-advance-3000] rule deny ip source 10.1.1.1 0.0.0.0
[R1-acl4-advance-3000] rule permit ip
[R1-acl4-advance-3000] quit
```

使用 MQC 的方式配置流量策略

```
[R1] traffic classifier test
[R1-classifier-test] if-match acl 3000
[R1-classifier-test] quit
[R1] traffic behavior test
[R1-behavior-test] permit
[R1-behavior-test] quit
[R1] traffic policy test
[R1-trafficpolicy-test] classifier test behavior test
[R1-trafficpolicy-test] quit
```

在 R1 的 GE0/0/2 接口上进行流量过滤

```
[R1] interface GE 0/0/2
[R1-GE0/0/2] traffic-policy test outbound
[R1-GE0/0/2] quit
```

在 S1 上执行 Ping 命令，检测网络的连通性

```
[S1] ping -a 10.0.1.1 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=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=253 time=1 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=253 time=1 ms

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

```
[S1] ping -a 10.1.1.1 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

结合以上输出结果得知，通过在 R1 GE0/0/2 接口出方向调用 ACL 实现了 S1 LoopBack1 接口不能访问 S2 物理接口 IP 地址的需求。

10.3 配置参考

10.3.1 R1 的配置

```
sysname R1
#
acl number 3000
 rule 5 deny ip source 10.1.1.1 0
 rule 10 permit ip
#
traffic classifier test type or
 if-match acl 3000
#
traffic behavior test
```

```
#
traffic policy test
 classifier test behavior test precedence 5
#
interface GE0/0/1
 ip address 10.0.12.2 255.255.255.0
#
interface GE0/0/2
 ip address 10.0.23.2 255.255.255.0
 traffic-policy test outbound
#
ospf 1
 area 0.0.0.0
  network 10.0.12.2 0.0.0.0
  network 10.0.23.2 0.0.0.0
#
```

10.3.2 S1 的配置

```
sysname S1
#
interface GE1/0/1
 undo portswitch
 ip address 10.0.12.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
interface LoopBack1
 ip address 10.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 10.0.12.1 0.0.0.0
  network 10.1.1.1 0.0.0.0
#
```

10.3.3 S2 的配置

```
sysname S2
#
interface GE1/0/1
 undo portswitch
 ip address 10.0.23.3 255.255.255.0
```

```
#
ospf 1
 area 0.0.0.0
  network 10.0.23.3 0.0.0.0
#
```

10.4 思考题

1. 除了在 R1 GE0/0/2 的接口上配置流量策略外，还有哪些方式可以实现流量过滤的需求？

答案：在 R1 的 GE0/0/1 接口的入方向调用流量策略。

11 文件管理实验

11.1 实验介绍

11.1.1 关于本实验

设备支持多种文件管理方式，用户根据任务和安全性要求选择合适的文件管理方式。

用户可以通过 FTP（File Transfer Protocol）、TFTP（Trivial File Transfer Protocol）和 SFTP（Secure File Transfer Protocol）方式实现对文件的管理。

设备在进行文件管理的过程中，可以分别充当服务器和客户端的角色：

1. 设备作为服务器：可以从客户端访问设备，实现对本设备文件的管理，以及与客户端间的文件传输操作。
2. 设备作为客户端访问其它设备（服务器）：可以实现管理其它设备上的文件，以及与其它设备间进行文件传输操作。

11.1.2 实验目的

- 理解建立 FTP 连接的过程
- 掌握 FTP 服务器参数的配置
- 掌握与 FTP 服务器传输文件的方法

11.1.3 实验组网介绍

图11-1 文件管理实验拓扑

S1 模拟 FTP Client，R1 作为 FTP Server。

11.1.4 实验背景

S1 需要对 R1 的配置文件进行管理。

11.2 实验任务配置

11.2.1 配置思路

1. 配置 FTP 服务器功能及参数
2. 配置本地 FTP 用户
3. FTP Client 登录 FTP Server
4. FTP Client 进行文件操作

11.2.2 配置步骤

步骤 1 设备基础配置

配置设备 IP 地址

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ip address 10.0.12.2 24
[R1-GE0/0/1] quit
```

```
[S1] vlan 2
[S1-vlan2] quit
[S1] interface GE 1/0/1
[S1-GE1/0/1] port link-type access
[S1-GE1/0/1] port default vlan 2
[S1-GE1/0/1] quit
[S1] interface Vlanif 2
[S1-Vlanif2] ip address 10.0.12.1 24
[S1-Vlanif2] quit
```

保存配置文件（用与后续验证实验效果）

```
<S1> save test1.cfg
```

```
Warning: Are you sure to save the configuration to flash:/test1.cfg? [Y/N] : y
Now saving the current configuration to the slot 1
Info: Save the configuration successfully.
```

```
<R1> save test2.cfg
Warning: Are you sure to save the configuration to flash:/test2.cfg? [Y/N] : y
Now saving the current configuration to the slot 0
Info: Save the configuration successfully.
```

查看当前的文件列表

```
<S1> dir
Directory of flash:/

  Idx  Attr       Size(Byte)  Date          Time          FileName
    0  drwx                -  Jun 29 XXXX 14:26:08   $_autobackup
    1  dr-x                -  Jul 17 XXXX 01:00:00   $_install_mod
    2  dr-x                -  Jun 29 XXXX 14:26:27   $_license
    3  dr-x                -  Jun 29 XXXX 14:26:00   $_startup
    4  dr-x                -  Nov 04 XXXX 00:55:46   $_system
    5  dr-x                -  Jun 29 XXXX 14:26:51   $_user
    6  -rw-      307,109,260  Jun 29 XXXX 14:23:24   S5755_V600R023C10SPC500.cc
    7  drwx                -  Nov 03 XXXX 09:27:30   bootlogfile
    8  -rw-           10,649  Nov 04 XXXX 07:58:56   device.sys
    9  drwx                -  Jun 29 XXXX 14:27:50   dhcp
   10  drwx                -  Jun 29 XXXX 14:26:39   eva
   11  drwx                -  Jun 29 XXXX 14:26:48   full_kpi
   12  drwx                -  Jun 29 XXXX 14:32:40   hips
   13  dr-x                -  Nov 04 XXXX 07:55:00   logfile
   14  drwx                -  Jun 29 XXXX 14:25:53   pki
   15  -rw-            4,755  Nov 04 XXXX 07:58:56   test1.cfg
   16  drwx                -  Jun 29 XXXX 14:27:06   webm
   17  drwx                -  Jun 29 XXXX 14:26:52   ztp
   18  -rw-          300,184  Oct 30 XXXX 08:51:34   ztp_XXXX1029090647.log
   19  -rw-          264,243  Nov 03 XXXX 03:32:12   ztp_XXXX1030085831.log
   20  -rw-           94,817  Nov 02 XXXX 08:45:21   ztp_XXXX1030085831.log.1.gz
   21  -rw-          467,180  Nov 03 XXXX 08:08:17   ztp_XXXX1103033652.log
   22  -rw-          140,208  Nov 03 XXXX 09:24:42   ztp_XXXX1103081236.log
   23  -rw-           75,285  Nov 03 XXXX 10:03:01   ztp_XXXX1103093021.log
   24  -rw-        1,218,999  Nov 04 XXXX 00:50:39   ztp_XXXX1103100719.log
   25  -rw-          695,911  Nov 04 XXXX 07:59:23   ztp_XXXX1104005703.log

1,070,832 KB total (752,644 KB free)
```

```
<R1> dir
Directory of flash:/
```

```
Idx  Attr       Size(Byte)  Date         Time         FileName
  0  drwx                -  Aug 21 XXXX 01:08:36   $_autobackup
  1  dr-x                -  Aug 21 XXXX 01:17:42   $_checkpoint
  2  dr-x                -  Jul 17 XXXX 01:00:00   $_install_mod
  3  dr-x                -  Aug 21 XXXX 01:06:51   $_license
  4  dr-x                -  Mar 01 XXXX 04:15:07   $_startup
  5  dr-x                -  Mar 05 XXXX 05:46:51   $_system
  6  dr-x                -  Aug 21 XXXX 01:16:14   $_user
  7  -rw-      246,928,556  Jan 01 XXXX 00:02:31   AR5700S-E_V600R023C00SPC100.cc
  8  -rw-        4,105,206  Feb 27 XXXX 11:50:04   AR5700S-E_V600R023SPH150.PAT
  9  -rw-          218,057  Mar 05 XXXX 05:46:52   application.txt
 10  -rw-          218,057  Mar 05 XXXX 05:46:52   application_touch.txt
 11  -rw-          223,984  Mar 04 XXXX 04:14:58   ase_url_backup.sdb
 12  drwx                -  Aug 21 XXXX 01:07:23   bootlogfile
 13  drwx                -  Mar 05 XXXX 05:42:40   default-sdb
 14  -rw-            3,725  Mar 05 XXXX 10:43:54   device.sys
 15  drwx                -  Aug 21 XXXX 01:16:29   dhcp
 16  drwx                -  Aug 21 XXXX 01:16:03   full_kpi
 17  drwx                -  Feb 27 XXXX 11:49:18   hips
 18  drwx                -  Aug 21 XXXX 01:06:52   hrp
 19  dr-x                -  Mar 05 XXXX 08:45:06   logfile
 20  drwx                -  Aug 21 XXXX 01:07:39   nlog
 21  drwx                -  Aug 21 XXXX 01:07:41   pki
 22  -rw-            9,815  Mar 05 XXXX 05:46:52   subcategory.txt
 23  -rw-            5,018  Mar 01 XXXX 03:54:11   test.cfg
 24  -rw-            5,435  Mar 05 XXXX 10:43:54   test2.cfg
 25  drwx                -  Aug 21 XXXX 01:16:16   update
 26  -rw-            2,015  Mar 01 XXXX 04:05:01   vrpcfg.zip
 27  drwx                -  Aug 21 XXXX 01:16:14   webm
 28  drwx                -  Aug 21 XXXX 01:16:15   ztp
 29  -rw-          385,332  Feb 28 XXXX 12:02:43   ztp_XXXX0227115454.log
 30  -rw-            4,865  Feb 28 XXXX 14:26:19   ztp_XXXX0228122319.log
 31  -rw-          110,682  Mar 01 XXXX 03:30:44   ztp_XXXX0228142651.log
 32  -rw-           98,999  Mar 01 XXXX 01:58:52   ztp_XXXX0228142651.log.1.gz
 33  -rw-           40,629  Mar 01 XXXX 06:29:23   ztp_XXXX0301041933.log
 34  -rw-        1,154,512  Mar 02 XXXX 07:19:36   ztp_XXXX0301062955.log
 35  -rw-           96,754  Mar 01 XXXX 16:11:32   ztp_XXXX0301062955.log.1.gz
 36  -rw-          348,198  Mar 04 XXXX 05:48:49   ztp_XXXX0302072008.log
 37  -rw-           87,542  Mar 03 XXXX 20:19:18   ztp_XXXX0302072008.log.1.gz
 38  -rw-            2,497  Mar 04 XXXX 08:27:50   ztp_XXXX0304062522.log
 39  -rw-            2,590  Mar 04 XXXX 10:30:40   ztp_XXXX0304082822.log
 40  -rw-            6,725  Mar 05 XXXX 03:48:23   ztp_XXXX0305034700.log
 41  -rw-          944,257  Mar 05 XXXX 09:38:49   ztp_XXXX0305054854.log

732,844 KB total (488,160 KB free)
```

两台设备上的配置文件都已经保存成功。

说明：不同设备的文件数量不同，用户不用关注其它文件。

步骤 2 在 R1 上配置 FTP 服务器功能及参数

```
<R1> install feature-software WEAKEA
Info: Checking, please wait for a moment...done.
Info: The package has been installed will be skipped: WEAKEA.
<R1> system-view
Enter system view, return user view with return command.
[R1] ftp server enable
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
[R1] ftp server source all-interface
Warning: FTP server source configuration will take effect in the next login. Continue? [Y/N] : y
Warning: It expands the range of accessed IP.
```

ftp server enable 命令用来开启设备的 FTP 服务器功能，允许 FTP 用户登录。缺省情况下，FTP 服务器功能处于关闭状态。

ftp server source all-interface 用来指定 FTP 服务器的源接口。

其它可选的配置参数还包括：指定 FTP 服务器端口号和配置 FTP 连接空闲时间等。

步骤 3 配置本地 FTP 用户

```
[R1] aaa
[R1-aaa] local-user ftp-client password irreversible-cipher Huawei@123
Info: The initial password of ftp-client must be changed during login.
[R1-aaa] local-user ftp-client service-type ftp
Warning: If the service type of local users is configured multiple times, the new configuration overwrites the previous one. The new configuration may cause local user authentication to fail. Continue? [Y/N]: y
Warning: The user access modes include Telnet, FTP, or HTTP, so security risks exist.
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory) of a local user, the rights of users already online do not change. The change takes effect to users who go online after the change.
[R1-aaa] local-user ftp-client privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue? [Y/N] : y
```

配置 FTP 用户的级别。

```
[R1-aaa] local-user ftp-client ftp-directory flash:/
Info: The configured FTP path must be an absolute path, for example, flash:/ftp.
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory) of a local user, the rights of users already online do not change. The change takes effect to users who go online after the change.
```

配置 FTP 用户的授权目录，必须指定该目录，否则 FTP 用户无法成功登录。

步骤 4 FTP Client 登录 FTP Server

FTP 客户端登录 FTP Server

```
<S1> ftp 10.0.12.2
Warning: FTP is not secure. Using SFTP is recommended.
Trying 10.0.12.2 ...
Press CTRL + K to abort
Connected to 10.0.12.2.
220 FTP service ready.
User(10.0.12.2:(none)): ftp-client
331 Password required for ftp-client.
Enter password: Huawei@123
230 User logged in.
```

此时已经成功登录到 R1 的文件系统。

步骤 5 对 R1 文件系统做相应的操作

设置传输模式

```
[ftp] ascii
200 Type set to A.
```

设备支持的文件传输的数据类型包括 ASCII 和 Binary 模式。

ASCII 用于传输纯文本文件，Binary 用于传输系统软件、图形图像、声音影像、压缩文件、数据库等程序文件。由于我们需要下载的配置文件为纯文本文件，所以需要设置为 ASCII 模式。缺省情况下，文件传输方式为 ASCII 模式。

下载配置文件

```
[ftp] get test2.cfg
Warning: The file may not transfer correctly in ASCII mode.
213 5435
200 Port command okay.
150 Opening ASCII mode data connection for /test2.cfg.
/        100% [**********]
226 Transfer complete.

FTP: 5435 byte(s) received in 0.143 second(s) 37.111Kbyte(s)/sec.
```

删除配置文件

```
[ftp] delete test2.cfg
Warning: File test2.cfg will be deleted. Continue? [Y/N] : y
250 DELE command successful.
```

上传配置文件

```
[ftp] put test1.cfg
```

```
Warning: The file may not transfer correctly in ASCII mode.
200 Port command okay.
150 Opening ASCII mode data connection for /test1.cfg.
/        100% [**********]
226 Transfer complete.

FTP: 4755 byte(s) send in 0.927 second(s) 5.008Kbyte(s)/sec.
```

断开 FTP 连接

```
[ftp] bye
221 Server closing.
<S1>
```

11.3 结果验证

查看当前 S1 和 R1 的文件目录：

```
<S1> dir | include test
  Idx  Attr      Size(Byte)  Date          Time          FileName
   15  -rw-           4,755  Nov 04 XXXX 07:58:56   test1.cfg
   16  -rw-           5,435  Nov 04 XXXX 08:18:08   test2.cfg
```

可以看到 S1 已经下载了 R1 的配置文件 test2.cfg。**include test** 指定输出的信息中必须包含 **test** 关键字。

```
<R1> dir | include test
  Idx  Attr      Size(Byte)  Date          Time          FileName
   23  -rw-           4,755  Mar 05 20XX 11:05:19   test1.cfg
```

可以看到 R1 的配置文件 test2.cfg 已不存在，并且已获取 S1 的配置文件 test1.cfg。

11.4 配置参考

11.4.1 S1 的配置

```
sysname R1
#
vlan batch 2
#
interface Vlanif2
 ip address 10.0.12.1 255.255.255.0
```

```
#
interface GE1/0/1
 port link-type access
 port default vlan 2
#
```

11.4.2 R1 的配置

```
sysname R1
#
ftp server enable
ftp server source all-interface
#
aaa
 local-user ftp-client password irreversible-cipher Huawei@123
 local-user ftp-client privilege level 3
 local-user ftp-client ftp-directory flash:/ read execute write
 local-user ftp-client service-type ftp
#
interface GE0/0/1
 ip address 10.0.12.2 255.255.255.0
#
```

11.5 思考题

1. FTP 默认情况下工作在主动模式还是被动模式?

答案：主动模式。

12 远程登录实验

12.1 实验介绍

12.1.1 关于本实验

AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称，是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

这三种安全功能的具体作用如下：

- 认证：验证用户是否可以获得网络访问权。
- 授权：授权用户可以使用哪些服务。
- 计费：记录用户使用网络资源的情况。

用户可以使用 AAA 提供的一种或多种安全服务。例如，公司仅仅想让员工在访问某些特定资源的时候进行身份认证，那么网络管理员只要配置认证服务器即可。但是若希望对员工使用网络的情况进行记录，那么还需要配置计费服务器。

如上所述，AAA 是一种管理框架，它提供了授权部分用户去访问特定资源，同时可以记录这些用户操作行为的一种安全机制，因其具有良好的可扩展性，并且容易实现用户信息的集中管理而被广泛使用。AAA 可以通过多种协议来实现，在实际应用中，最常使用 RADIUS 协议。

本实验将通过配置本地 AAA 对远程 Telnet 用户进行管控。

12.1.2 实验目的

- 掌握本地 AAA 认证授权方案的配置方法
- 掌握创建域的方法
- 掌握本地用户的创建方法
- 理解基于域的用户管理的原理

12.1.3 实验组网介绍

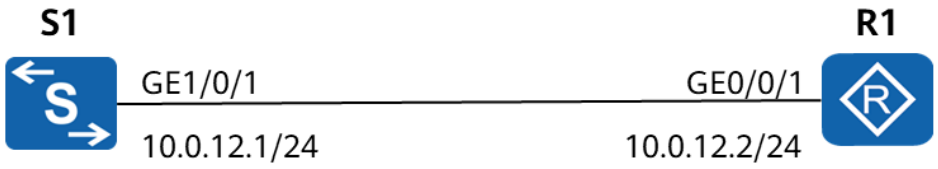


图12-1 远程登录实验拓扑

12.1.4 实验背景

S1 模拟一台客户端设备。现在需要在 R1 上对管理 R1 的用户进行资源控制，只有通过认证的用户才能访问特定的资源，因此您需要在 S1 和 R1 两台网络设备上配置本地 AAA 认证，并基于域来实现对用户进行管理。

12.2 实验任务配置

12.2.1 配置思路

1. 配置 AAA 方案
2. 创建域并在域下应用 AAA 方案
3. 配置本地用户

12.2.2 配置步骤

步骤 1 设备基础配置

配置 R1 和 S1 互联的 IP 地址

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ip address 10.0.12.2 24
[R1-GE0/0/1] quit
```

```
[S1] interface GE 1/0/1
```

```
[S1-GE1/0/1] undo port link-type
[S1-GE1/0/1] undo portswitch
[S1-GE1/0/1] ip address 10.0.12.1 24
[S1-GE1/0/1] quit
```

步骤 2 配置 AAA 方案

配置认证、授权方案

```
[R1] aaa
```

进入 AAA 视图。

```
[R1-aaa] authentication-scheme datacom
```

创建名为 datacom 的认证方案。

```
[R1-aaa-authen-datacom] authentication-mode local
```

设置认证方案的认证方式为本地认证。

```
[R1-aaa-authen-datacom] quit
[R1-aaa] authorization-scheme datacom
```

创建名为 datacom 的授权方案。

```
[R1-aaa-author-datacom] authorization-mode local
```

设置授权方案的授权方式为本地授权。

```
[R1-aaa-author-datacom] quit
[R1-aaa] quit
```

设备作为 AAA 服务器时被称为本地 AAA 服务器，本地 AAA 服务器支持对用户进行认证和授权，不支持对用户进行计费。

与远端 AAA 服务器相似，本地 AAA 服务器需要配置本地用户的用户名、密码、授权信息等。使用本地 AAA 服务器进行认证和授权比远端 AAA 服务器的速度快，可以降低运营成本，但是存储信息量受设备硬件条件限制。

步骤 3 创建域并在域下应用 AAA 方案

```
[R1] aaa
[R1-aaa] domain datacom
```

设备对用户的管理是基于域的，每个用户都属于一个域，一个域是由属于同一个域的用户构成的群体。简单地说，用户属于哪个域就使用哪个域下的 AAA 配置信息。创建名为 datacom 的域。

```
[R1-aaa-domain-datacom] authentication-scheme datacom
```

指定对该域内的用户采用名为 datacom 的认证方案。

```
[R1-aaa-domain-datacom] authorization-scheme datacom
[R1-aaa-domain-datacom] quit
```

指定对该域内的用户采用名为 datacom 的授权方案。

步骤 4 配置本地用户

创建本地用户及其密码

```
[R1-aaa] local-user hcia@datacom password irreversible-cipher Huawei@123
Info: The initial password of hcia@datacom must be changed during login.
```

如果用户名中带域名分隔符@，则认为@前面的部分是纯用户名，后面部分是域名。如果没有@，则整个字符串为用户名，域为默认域。

配置本地用户的接入类型、级别等参数

```
[R1-aaa] local-user hcia@datacom service-type telnet
Warning: If the service type of local users is configured multiple times, the new configuration overwrites the previous one. The new configuration may cause local user authentication to fail. Continue? [Y/N]: y
Warning: The user access modes include Telnet, FTP, or HTTP, so security risks exist.
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory) of a local user, the rights of users already online do not change. The change takes effect to users who go online after the change.
```

local-user service-type 命令用来配置本地用户的接入类型。系统提供对用户的接入类型管理，即对所有用户配置一定的接入类型，只有用户的接入方式与系统为该用户配置的接入类型匹配，用户才能登录。如此处设置的接入类型为 **telnet**，则此用户无法通过 Web 方式接入设备，一个用户可以有多种接入类型。

表12-1 service-type 参数说明

参数	参数说明
none	不指定任何接入类型。
http	指定用户类型为HTTP用户。
ftp	指定用户类型为FTP用户。
ssh	指定用户类型为SSH用户。

telnet	指定用户类型为Telnet用户，通常指网络管理员。
terminal	指定用户类型为终端用户，通常指Console口用户。

```
[R1-aaa] local-user hcia@datacom privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue?
[Y/N] : y
[R1-aaa] return
```

指定本地用户的级别。不同级别的用户登录后，只能使用等于或低于自己级别的命令。

步骤 5 开启 R1 上的 Telnet 功能

在 R1 安装弱安全算法/协议特性包 WEAKEA

```
<R1> install feature-software WEAKEA
Info: Checking, please wait for a moment...done.
Info: Start to install the package WEAKEA.
Info: Operating, please wait for a moment..This operation will install weak algorithm software, and
weak algorithms will be allowed to be used.
.....done.
Info: Succeeded in installing the software.
```

由于协议和算法自身的安全性能不同，用户配置时使用的某些协议或算法可能存在安全风险。出于安全性考虑，不建议使用不安全协议和算法，如果确实需要使用，需安装弱安全算法/协议特性包 WEAKEA。设备默认自带弱安全算法/协议特性包 WEAKEA。

```
<R1> system-view
[R1] telnet server enable
```

开启设备的 Telnet 服务器功能，部分设备默认开启。

```
[R1] telnet server-source all-interface
Warning: Telnet server source configuration will take effect in the next login. Continue? [Y/N] : y
Warning: It expands the range of accessed IP.
```

指定 Telnet 服务器的源接口为设备上所有配置了 IP 地址接口。

```
[R1] user-interface vty 0 4
```

user-interface vty 命令用来进入 VTY 用户界面视图。在该视图下用户可以配置 Telnet 和 SSH 的相关参数。**vty** 取值范围是 0～20。

缺省情况下，设备以出厂配置启动时，vty 接口数为 5，认证方式为 AAA，协议为 SSH。

```
[R1-ui-vty0-4] authentication-mode aaa
```

authentication-mode 命令用来设置登录用户界面的验证方式。缺省情况下，用户界面没有使用该命令配置认证方式。登录用户界面必须配置验证方式，否则用户无法成功登录设备。

```
[R1-ui-vty0-4] protocol inbound telnet
Warning: TELNET is not a secure protocol. SSH protocol is recommended.
[R1-ui-vty0-4] quit
```

protocol inbound 命令用来指定所在的用户界面所支持的协议。

步骤 6 检验配置效果

在 S1 安装弱安全算法/协议特性包 WEAKEA

```
<S1> install feature-software WEAKEA
Info: Checking, please wait for a moment...done.
Info: Start to install the package WEAKEA.
Info: Operating, please wait for a moment..This operation will install weak algorithm software, and
weak algorithms will be allowed to be used.
.....done.
Info: Succeeded in installing the software.
```

从 S1 远程 Telnet 访问 R1

```
<S1> telnet 10.0.12.2
Trying 10.0.12.2 ...
Press CTRL+K to abort
Connected to 10.0.12.2 ...
Warning: Telnet is not a secure protocol, and it is recommended to use Stelnet.

Username: hcia@datacom
Password: Huawei@123
Warning: The initial password poses security risks.The password needs to be changed, Continue? [Y/N] :y
Please enter old password: Huawei@123
Please enter new password: Huawei@1234
Please confirm new password: Huawei@1234
The password has been changed successfully.
Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number
of terminal users online is 2.
        The current login time is XXXX-XX-XX 00:04:42.
<R1>
```

默认情况下，初次登录时，必须修改用户密码，修改完成后即可登录到 R1 上。

在 R1 上查看登录的用户

```
<R1> display users
NOTE:
User-Intf: The absolute number and the relative number of user interface
```

```
Authen: Whether the authentication passes
Author: Command line authorization flag
--------------------------------------------------------------------------------
  User-Intf    Delay       Type    Network Address    Authen     Author    Username
--------------------------------------------------------------------------------
  0    CON 0   00:01:50    --      0                  pass       no        Unspecified

* 34  VTY 0    00:00:00    TEL     10.0.12.1          pass       no        hcia@datacom
```

可以看到 S1 已经成功登录 R1，登录方式为 Telnet，VTY 编号为 0。

步骤 7 开启 R1 上的 STelnet 功能

Telnet 服务不安全，在现网中推荐使用 STelnet。

创建 SSH 用户

```
[R1] ssh user sshclient@datacom
[R1] ssh user sshclient@datacom authentication-type password
[R1] ssh user sshclient@datacom service-type stelnet
```

当用户使用 password、password-rsa、password-x509v3-rsa、password-dsa 或 password-ecc、password-sm2、password-x509v3-ecdsa-sha2、password-sm2-sm3 认证方式登录设备时，需要在 AAA 视图下创建同名的本地用户。

创建本地 AAA 用户

```
[R1] aaa
[R1-aaa] local-user sshclient@datacom password irreversible-cipher Huawei@123
[R1-aaa] local-user sshclient@datacom privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue? [Y/N] : y
[R1-aaa] local-user sshclient@datacom service-type ssh
Warning: If the service type of local users is configured multiple times, the new configuration overwrites the previous one. The new configuration may cause local user authentication to fail. Continue? [Y/N] : y
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory) of a local user, the rights of users already online do not change. The change takes effect to users who go online after the change.
[R1-aaa] quit
```

配置 SSH 服务器

```
[R1] ssh server-source all-interface
Warning: SSH server source configuration will take effect in the next login. Continue? [Y/N] : y
Warning: It expands the range of accessed IP.
[R1] stelnet server enable
Info: Succeeded in starting the STelnet server.
Warning: After configuring the source interface or source address, the IPV4/IPV6 listening socket will be created.
```

配置 VTY 用户界面支持 SSH 协议

```
[R1] user-interface vty 5 10
[R1-ui-vty5-10] authentication-mode aaa
[R1-ui-vty5-10] protocol inbound ssh
[R1-ui-vty5-10] quit
```

步骤 8 从 S1 远程 STelnet 访问 R1

开启 SSH 客户端首次登录功能

```
[S1] ssh client first-time enable
Warning: After this command is run, the SSH client unconditionally trusts the connected SSH server.
```

ssh client first-time enable 命令用来开启 SSH 客户端首次登录功能。

当 STelnet/SFTP 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的公钥进行有效性检查，因为此时 STelnet/SFTP 客户端还没有保存 SSH 服务器的公钥。

S1 STelnet 登录 R1

```
[S1] stelnet 10.0.12.2
Trying 10.0.12.2 ...
Press CTRL + K to abort
Connected to 10.0.12.2 ...
The server's key fingerprint is ssh-rsa 3072 CFokN9ZDH/07wxl9QXw8A5Seh8BfGEKmq9WBelWtEjg.
The server is not authenticated. Continue to access it? [Y/N] : y
Save the server's public key? [Y/N] : y
The server's public key will be saved with the name 10.0.12.2. Please wait...
Please input the username: sshclient@datacom
Enter password: Huawei@123
Warning: The initial password poses security risks.
The password needs to be changed, Continue? [Y/N] : y
Please enter old password: Huawei@123
Please enter new password: Huawei@1234
Please confirm new password: Huawei@1234
The password has been changed successfully.

Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number of terminal users online is 2.
        The current login time is XXXX-XX-XX 11:19:58.
<R1>
```

在登录过程中，S1 自动分配并保存 R1 的公钥。

查看已登录 R1 的用户

```
<R1> display users
```

```
NOTE:
User-Intf: The absolute number and the relative number of user interface
Authen: Whether the authentication passes
Author: Command line authorization flag
------------------------------------------------------------------------------
  User-Intf    Delay       Type    Network Address    Authen     Author    Username
------------------------------------------------------------------------------
  0    CON 0   00:01:12    --      0                  pass       no        Unspecified

* 39  VTY 5    00:00:00    SSH     10.0.12.1          pass       no        sshclient@datacom
```

可以看到用户名 sshclient@datacom 的登录类型为 SSH，VTY 编号为 5。

步骤 9 本地 AAA 用户管理

查看 AAA 的概要信息

```
[R1] display aaa configuration
  Domain Name Delimiter                 : @
  Domainname parse direction            : Left to right
  Domainname location                   : After-delimiter
  Administrator user default domain: default_admin
  Normal user default domain            : default
  Domain                                : total: 256       used: 3
  Authentication-scheme                 : total: 32        used: 2
  Accounting-scheme                     : total: 32        used: 1
  Authorization-scheme                  : total: 32        used: 2
  Service-scheme                        : total: 256       used: 0
  Recording-scheme                      : total: 32        used: 0
  Local-user                            : total: 512       used: 2
  Local-user block retry-interval   : 5 Min(s)
  Local-user block retry-time       : 3
  Local-user block time             : 5 Min(s)
  Remote-admin-user block retry-interval : 5 Min(s)
  Remote-admin-user block retry-time     : 30
  Remote-admin-user block time           : 5 Min(s)
  Session timeout invalid enable    : No
```

display aaa configuration 命令用来查看 AAA 的概要信息，如域、认证方案、授权方案、计费方案的使用情况。

从以上输出中可以看到以下信息：

1. 域名分隔符：@
2. 本地用户数： 可以创建的本地用户数 512 个，已创建 2 个本地用户
3. 本地账号用户的重试时间间隔：5 分钟
4. 本地账号连续认证失败的限制次数：3 次
5. 本地账号的锁定时间：5 分钟

查看所有认证失败的 IP 地址

```
[R1] display vty ip-block all
[R1] display ssh server ip-block all
```

display vty ip-block all 命令用来查看所有认证失败的 IP 地址。

display ssh server ip-block all 命令用来查看所有 SSH 认证失败的客户端 IP 地址。

当前没有因认证失败锁定的 IP 地址。

如果 IP 地址被锁定，可使用以下命令解锁：

1. **activate ssh server ip-block ip-address** 命令用来解除对 SSH 连接中认证失败的 IP 地址的阻止。
2. **activate vty ip-block ip-address** 命令用来解除对 Telnet 连接中认证失败的 IP 地址的锁定。

如果不想开启 IP 地址锁定功能，可使用以下命令：

1. **telnet server ip-block disable** 命令用来去使能 Telnet IP 地址锁定功能。
2. **ssh server ip-block disable** 命令用来去使能 SSH 服务器上的客户端 IP 地址锁定功能。

查看本地用户信息

```
[R1] display local-user username hcia@datacom
  The contents of local user(s):
  Password                 : ****************
  State                    : active
  Service-type-mask        : S
  Privilege level          : 3
  Ftp-directory            : -
  Access-limit             : Yes
  Access-limit-max         : 4294967295
  Accessed-num             : 0
  Idle-timeout             : -
  User-group               : -
  Password-force-change: Yes
  Original-password        : No
  Password-set-time        : XXXX-XX-XX 10:32:34
  Password-expired         : No
  Password-expire-time : XXXX-XX-XX 10:32:34
  Account-expire-time   : -
  Last login ip            : 10.0.12.1
  Last login time          : XXXX-XX-XX 10:32:19
  Login fail count         : 0
```

display local-user username *user-name* 命令用来查看本地管理员用户的属性。

display local-user state { **active** | **block** }命令用来查看处于激活或者阻塞状态的本地管理员用户。处于激活状态的用户可以处理认证请求，处于阻塞状态的用户直接拒绝认证请求。

如果用户被锁定，可以使用 **local-user** *user-name* **state active**，将本地用户设置为激活状态。

12.3 配置参考

12.3.1 R1 的配置

```
sysname R1
#
telnet server enable
telnet server-source all-interface
#
aaa
 authentication-scheme datacom
  authentication-mode local
 authorization-scheme datacom
  authorization-mode local
 domain datacom
  authentication-scheme datacom
  accounting-scheme default
  authorization-scheme datacom
 local-user hcia@datacom password irreversible-cipher Huawei@123
 local-user hcia@datacom privilege level 3
 local-user hcia@datacom service-type telnet
 local-user sshclient@datacom password irreversible-cipher Huawei@123
 local-user sshclient@datacom privilege level 3
 local-user sshclient@datacom service-type ssh
#
interface GE0/0/1
 ip address 10.0.12.2 255.255.255.0
#
stelnet server enable
ssh user sshclient@datacom
ssh user sshclient@datacom authentication-type password
ssh user sshclient@datacom service-type stelnet
ssh server-source all-interface
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound telnet
#
user-interface vty 5 20
 authentication-mode aaa
 protocol inbound ssh
```

```
#
```

12.3.2 S1 的配置

```
sysname S1
#
rsa peer-public-key 10.0.12.2
 public-key-code begin
 3082018A
  02820181
      00C7CD46 93D06C46 836FC539 DF9B3B40 63C4AE66 AD4AB5FF 5E333806 BB7AC5FE
      D60936B1 4C404CBB 8B9402D2 82075518 0CF755AF B64F31A0 77427356 4B7C028E
      F27DE79A BAC9ADFC B5A7EF1D EF0397D5 4C9E7A7F 6D81F95F E31B6D55 53091B99
      4472F713 F10F21A5 F984AE33 B3FA315C 173A33FB 0927BFBF 16C73F77 7A0040E8
      1CDF54DA 4CAB9010 C4BBF15F 1A64961D F95EE0E3 E8383EFF F5A257F6 888024B8
      3D2289E2 138E1DA4 790F1C73 F46754FB 55F0D0A0 131315BB 101D1C42 7926CC6C
      7CE3FC43 7B31581B B49A8392 DE303467 22EF0D84 E1EB1FDE 0869D679 DB188EFF
      53E5F166 46BBFCA1 D466CA23 1E853A7A 7A3797A0 24DD941C 52556147 329D3CE6
      3E8C6B33 02DD9EE5 4A077D7E 5D163BEE C4E4983B BCCECB44 81BD2BF1 D0AEB438
      C5C2524B 95371BDD AAB9ACF7 FA00F0A5 65B9FBAA 918168F2 B4B867F8 3F2B22AA
      550B5C50 08D71D83 B9D5B59D BC1DD579 D07910E5 6F8A1344 896797BB 3E9B3B57
      EB034801 D8DD5AC8 7F7D255A 27D1E357 D221644B ADCA0CEA C79CCB91 ADD3AC4A
      91
  0203
      010001
 public-key-code end
 peer-public-key end
#
interface GE1/0/1
 undo portswitch
 ip address 10.0.12.1 255.255.255.0
#
ssh client first-time enable
ssh client peer 10.0.12.2 assign rsa-key 10.0.12.2
#
```

12.4 思考题

1. 为什么 STelnet 比 Telnet 更安全?

答案：STelnet 基于 SSH 协议，支持加密传输、密钥+密码双重认证；而 Telnet 明文发送账号、密码和指令，易被窃听和中间人攻击，因此 STelnet 更安全。

13 NAT 配置实验

13.1 实验介绍

13.1.1 关于本实验

NAT（Network Address Translation，网络地址转换）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。作为减缓 IP 地址枯竭的一种过渡方案，NAT 通过地址重用的方法来满足 IP 地址的需要，可以在一定程度上缓解 IP 地址空间枯竭的压力。NAT 除了解决 IP 地址短缺的问题，还带来了两个好处：

- 有效避免来自外网的攻击，可以很大程度上提高网络安全性。
- 控制内网主机访问外网，同时也可以控制外网主机访问内网，解决了内网和外网不能互通的问题。

本实验将通过配置不同场景下的 NAT 帮助学员理解 NAT 技术的原理。

13.1.2 实验目的

- 掌握 NAPT 的配置方法
- 掌握 Easy IP 的配置方法
- 掌握 NAT Server 的配置方法

13.1.3 实验组网介绍

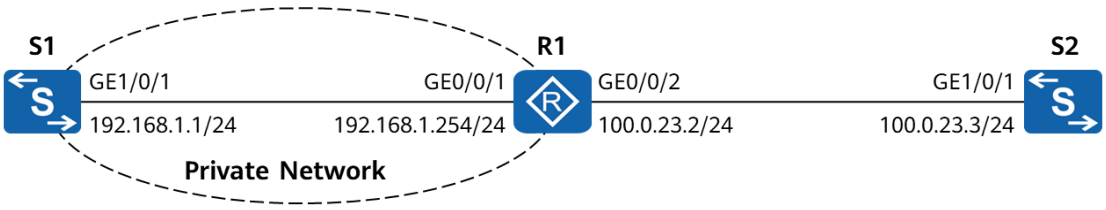


图13-1 NAT 配置实验拓扑

1. R1 和 S1 之间的网络属于企业内部网络，使用私网 IPv4 地址。
2. S1 模拟私网客户端。R1 作为 S1 的网关，同时也是连接公网的出口路由器。

3. S2 模拟公网。

13.1.4 实验背景

由于 IPv4 地址紧缺，企业内部一般使用私网 IPv4 地址。然而，企业网络用户时常会有访问公网的需求，同时部分企业还会对外提供相应的服务。此时需要配置 NAT 来实现这些需求。

13.2 实验任务配置

13.2.1 配置思路

1. 配置 NAPT
2. 配置 Easy IP
3. 配置 NAT Server

13.2.2 配置步骤

步骤 1 基本配置

接口 IP 地址和路由配置

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] undo port link-type
[S1-GE1/0/1] undo portswitch
[S1-GE1/0/1] ip address 192.168.1.1 24
[S1-GE1/0/1] quit
[S1] ip route-static 0.0.0.0 0 192.168.1.254
```

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ip address 192.168.1.254 24
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] undo portswitch
[R1-GE0/0/2] ip address 100.0.23.2 24
[R1-GE0/0/2] quit
[R1] ip route-static 0.0.0.0 0 100.0.23.3
```

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] undo port link-type
```

```
[S2-GE1/0/1] undo portswitch
[S2-GE1/0/1] ip address 100.0.23.3 24
[S2-GE1/0/1] quit
```

配置 S1 的 Telnet 功能（用于后续实验验证）

```
<S1> install feature-software WEAKEA
Info: Operating, please wait for a moment.....done.
Info: Succeeded in installing the software.
<S1> system-view
[S1] telnet server enable
[S1] telnet server-source all-interface
Warning: Telnet server source configuration will take effect in the next login. Continue? [Y/N] : y
[S1] aaa
[S1-aaa] local-user hcia-datacom password irreversible-cipher Huawei@123
[S1-aaa] local-user hcia-datacom service-type telnet
Warning: If the service type of local users is configured multiple times, the new configuration overwrites the previous one. The new configuration may cause local user authentication to fail. Continue? [Y/N]: y
Warning: The user access modes include Telnet, FTP, or HTTP, so security risks exist.
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory) of a local user, the rights of users already online do not change. The change takes effect to users who go online after the change.
[S1-aaa] local-user hcia-datacom privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue? [Y/N] : y
[S1-aaa] quit
[S1] user-interface vty 0 4
[S1-ui-vty0-4] authentication-mode aaa
[S1-ui-vty0-4] protocol inbound telnet
[S1-ui-vty0-4] quit
```

步骤 2 配置 NAPT

假设该公司获得了 100.1.23.1 至 100.1.23.254 这段公网 IP，现需要配置 NAPT。

配置 NAT 地址池

```
[R1] nat address-group test 1
[R1-address-group-test] section 1 100.1.23.1 100.1.23.254
[R1-address-group-test] mode pat
[R1-address-group-test] quit
```

nat address-group 命令用来配置 NAT 地址池。

section 命令用来配置地址段。

mode pat 命令用来配置地址池模式为 PAT。缺省情况下，地址池的应用模式为 NAPT 模式。

配置 NAT 策略

```
[R1] nat-policy
[R1-policy-nat] rule name test
[R1-policy-nat-rule-test] source-address range 192.168.1.1 192.168.1.254
[R1-policy-nat-rule-test] action source-nat address-group test
[R1-policy-nat-rule-test] quit
[R1-policy-nat] quit
```

source-address range 用来配置 NAT 的规则的匹配条件。

action 用来配置 NAT 规则的动作，**source-nat** 表示对该数据流进行源地址 NAT 转换。

在 R1 的 GE0/0/2 开启 NAT 功能

```
[R1] interface GE 0/0/2
[R1-GE0/0/2] nat enable
[R1-GE0/0/2] quit
```

在 S2 上配置到达 NAT 地址池的静态路由。

```
[S2] ip route-static 100.1.23.0 24 100.0.23.2
```

在 S1 测试连通性

```
[S1] ping -c 1000 100.0.23.3
  PING 100.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 100.0.23.3: bytes=56 Sequence=1 ttl=254 time=11 ms
    Reply from 100.0.23.3: bytes=56 Sequence=2 ttl=254 time=14 ms
    Reply from 100.0.23.3: bytes=56 Sequence=3 ttl=254 time=8 ms
    Reply from 100.0.23.3: bytes=56 Sequence=4 ttl=254 time=9 ms
    Reply from 100.0.23.3: bytes=56 Sequence=5 ttl=254 time=10 ms
    Reply from 100.0.23.3: bytes=56 Sequence=6 ttl=254 time=9 ms
    Reply from 100.0.23.3: bytes=56 Sequence=7 ttl=254 time=3 ms
```

在 S1 连续 Ping 测 1000 个数据包。

查看 R1 上的 NAT 会话表

```
[R1] display session all verbose
  Session Table Information:
    Protocol               : 1 (ICMP)
    SrcAddr VPN            : 192.168.1.1
    DestAddr VPN           : 100.0.23.3
    Type Code IcmpId       : 8 0 5999
    Time To Live           : 19 s
    NAT Info
      New SrcAddr          : 100.1.23.200
      New DestAddr         : -
      New IcmpId           : 2048
```

```
  Total : 1
```

S1 的地址被转换为 100.1.23.200。

步骤 3 配置 Easy IP

修改 NAT 策略，将 NAT 动作设置为 Easy IP。

```
[R1] nat-policy
[R1-policy-nat] rule name test
[R1-policy-nat-rule-test] action source-nat easy-ip
[R1-policy-nat-rule-test] quit
[R1-policy-nat] quit
```

在 S1 测试连通性

```
[S1] ping -c 1000 100.0.23.3
  PING 100.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 100.0.23.3: bytes=56 Sequence=1 ttl=254 time=11 ms
    Reply from 100.0.23.3: bytes=56 Sequence=2 ttl=254 time=14 ms
    Reply from 100.0.23.3: bytes=56 Sequence=3 ttl=254 time=8 ms
    Reply from 100.0.23.3: bytes=56 Sequence=4 ttl=254 time=9 ms
    Reply from 100.0.23.3: bytes=56 Sequence=5 ttl=254 time=10 ms
    Reply from 100.0.23.3: bytes=56 Sequence=6 ttl=254 time=9 ms
    Reply from 100.0.23.3: bytes=56 Sequence=7 ttl=254 time=3 ms
```

在 S1 连续 Ping 测 1000 个数据包。

查看 NAT 会话表

```
[R1] display session all verbose
  Session Table Information:
    Protocol               : 1 (ICMP)
    SrcAddr VPN            : 192.168.1.1
    DestAddr VPN           : 100.0.23.3
    Type Code IcmpId       : 8 0 8882
    Time To Live           : 20 s
    NAT Info
      New SrcAddr          : 100.0.23.2
      New DestAddr         : -
      New IcmpId           : 2048

  Total : 1
```

此时 S1 的源地址被转换为 100.0.23.2，即 R1 GE0/0/2 接口的 IP 地址。

步骤 4 配置 NAT Server

假设 S1 要向公网提供网络服务（用 Telnet 模拟），由于 S1 没有公网 IP 地址，故需要在 R1 的出接口上配置 NAT Server。

在 R1 上配置 NAT Server

```
[R1] nat server for_telnet protocol tcp global 100.0.23.2 telnet inside 192.168.1.1 telnet
```

nat server 命令用来定义一个内部服务器的映射表，外部用户可以通过地址和端口转换来访问内部服务器的某项服务。

S2 通过 Telnet 远程登录到 S1

```
<S2> install feature-software WEAKEA
<S2> telnet 100.0.23.2
Trying 100.0.23.2 ...
Press CTRL+K to abort
Connected to 100.0.23.2 ...
Warning: Telnet is not a secure protocol, and it is recommended to use Stelnet.

Username: hcia-datacom
Password: Huawei@123
Warning: The initial password poses security risks.The password needs to be changed, Continue? [Y/N] :
y
Please enter old password: Huawei@123
Please enter new password: Huawei@1234
Please confirm new password: Huawei@1234
The password has been changed successfully.
Info: The max number of VTY users is 5, the number of current VTY users online is 1, and total number
of terminal users online is 2.
        The current login time is XXXX-XX-XX XX:XX:XX.
<S1>
```

查看 R1 上的 NAT 会话表

```
[R1] display session all verbose
  Session Table Information:
    Protocol               : 6 (TCP)
    SrcAddr Port VPN       : 100.0.23.3 58637
    DestAddr Port VPN      : 100.0.23.2 23
    Time To Live           : 596 s
    NAT Info
      New SrcAddr          : -
      New SrcPort          : -
      New DestAddr         : 192.168.1.1
      New DestPort         : 23

    Protocol               : 1 (ICMP)
    SrcAddr VPN            : 192.168.1.1
    DestAddr VPN           : 100.0.23.3
```

```
    Type Code IcmpId     : 8 0 8882
    Time To Live         : 19 s
    NAT Info
      New SrcAddr        : 100.0.23.2
      New DestAddr       : -
      New IcmpId         : 2048

  Total : 2
```

从输出结果可以看到 S2 对 100.0.23.2 23 的访问已被转换为 192.168.1.1 23。

13.3 配置参考

13.3.1 S1 的配置

```
sysname S1
#
telnet server enable
telnet server-source all-interface
#
aaa
 local-user hcia-datacom password irreversible-cipher Huawei@123
 local-user hcia-datacom privilege level 3
 local-user hcia-datacom service-type telnet
#
interface GE1/0/1
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound telnet
#
```

13.3.2 R1 的配置

```
sysname R1
#
interface GE0/0/1
 ip address 192.168.1.254 255.255.255.0
#
interface GE0/0/2
```

```
 ip address 100.0.23.2 255.255.255.0
 nat enable
#
ip route-static 0.0.0.0 0.0.0.0 100.0.23.3
#
nat address-group test 1
 mode pat
 section 1 100.1.23.1 100.1.23.254
#
nat server for_telnet protocol tcp global 100.0.23.2 telnet inside 192.168.1.1 telnet
#
nat-policy
 rule name test
  source-address range 192.168.1.1 192.168.1.254
  action source-nat easy-ip
#
```

13.3.3 S2 的配置

```
sysname S2
#
interface GE1/0/1
 undo portswitch
 ip address 100.0.23.3 255.255.255.0
#
ip route-static 100.1.23.0 255.255.255.0 100.0.23.2
#
```

13.4 思考题

1. 在配置 NAT Server 时，转换前的目的端口和转换后的目的端口是否需要相同?

答案：不需要。

14 WAC+FIT AP 组网实验

14.1 实验介绍

14.1.1 关于本实验

以有线电缆或光纤作为传输介质的有线局域网应用广泛，但有线传输介质的铺设成本高，位置固定，移动性差。随着人们对网络的便携性和移动性的要求日益增强，传统的有线网络已经无法满足需求，WLAN 技术应运而生。目前，WLAN 已经成为一种经济、高效的网络接入方式。通过 WLAN 技术，用户可以方便地接入到无线网络，并在无线网络覆盖区域内自由移动。

本实验将通过典型 WAC+FIT AP 组网的模式，帮助学员理解构建基础 WLAN 网络的整体流程与配置。

14.1.2 实验目的

- 掌握 FIT AP 上线的配置方法
- 掌握各种无线模板配置命令
- 掌握 WLAN 配置的基本流程

14.1.3 实验组网介绍

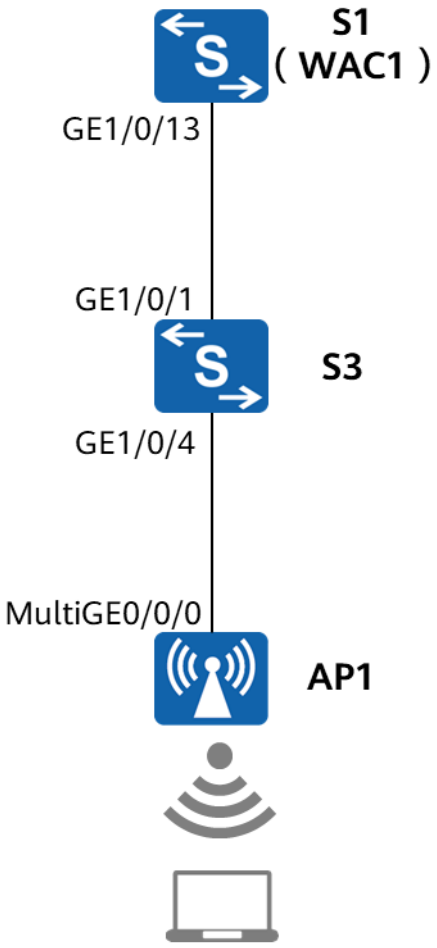


图14-1 WAC+FIT AP 组网实验拓扑

1. S1 支持 WLAN-AC 功能（若实际环境所用交换机不支持，可用普通 WAC 替代），作为 WAC 使用（后面内容中的 WAC1 就是 S1）。
2. WAC1 与 AP1 处于同一个二层网络。
3. WAC1 作为 DHCP 服务器给 AP1 和 STA 分配 IP 地址。
4. 业务数据采用直接转发模式。

14.1.4 数据规划

表14-1 WLAN 数据规划

配置项	配置参数

AP1管理VLAN	VLAN 100
STA业务VLAN	VLAN 101
DHCP服务器	WAC1作为DHCP服务器为AP1分配IP地址
	WAC1作为DHCP服务器为STA分配IP地址
AP1的IP地址池	192.168.100.1-192.168.100.253/24
STA的IP地址池	192.168.101.1-192.168.101.253/24
WAC1的源接口IP地址	VLANIF100：192.168.100.254/24
AP组	名称：ap-group1
	引用模板：VAP模板HCIA-WLAN、域管理模板default
域管理模板	名称：default
	国家码：中国（CN）
SSID模板	名称：HCIA-WLAN
	SSID名称：HCIA-WLAN
安全模板	名称：HCIA-WLAN
	安全策略：WPA-WPA2+PSK+AES
	密码：HCIA-Datacom
VAP模板	名称：HCIA-WLAN
	转发模式：直接转发
	业务VLAN：VLAN 101
	引用模板：SSID模板HCIA-WLAN、安全模板HCIA-WLAN

14.1.5 实验背景

某企业网络需要用户通过 WLAN 接入网络，以满足移动办公的最基本需求。

14.2 实验任务配置

14.2.1 配置思路

1. 配置有线网络侧互通
2. 配置 AP1 上线：

a) 创建 AP 组，用于将需要进行相同配置的 AP 都加入到 AP 组，实现统一配置

b) 配置 WAC1 的系统参数，包括国家码、WAC1 与 AP1 之间通信的源接口

c) 配置 AP 上线的认证方式并离线导入 AP1，实现 AP1 正常上线

3. 配置 STA 上线：配置 WLAN 业务参数并下发给 AP1，实现 STA 访问网络

14.2.2 配置步骤

步骤 1 设备基本配置

设备命名（拓扑中的 S1 命名为 WAC1）

略。

关闭不使用的端口

```
[WAC1] interface GE 1/0/1
[WAC1-GE1/0/1] shutdown
[WAC1-GE1/0/1] quit
[WAC1] interface GE 1/0/10
[WAC1-GE1/0/10] shutdown
[WAC1-GE1/0/10] quit
[WAC1] interface GE 1/0/11
[WAC1-GE1/0/11] shutdown
[WAC1-GE1/0/11] quit
[WAC1] interface GE 1/0/12
[WAC1-GE1/0/12] shutdown
[WAC1-GE1/0/12] quit
[WAC1] interface GE 1/0/14
[WAC1-GE1/0/14] shutdown
[WAC1-GE1/0/14] quit
```

```
[S3] interface GE 1/0/2
[S3-GE1/0/2] shutdown
[S3-GE1/0/2] quit
```

```
[S3] interface GE 1/0/3
[S3-GE1/0/3] shutdown
[S3-GE1/0/3] quit
```

步骤 2 有线侧网络配置

VLAN 配置

```
[WAC1] vlan batch 100 101
[WAC1] interface GE 1/0/13
[WAC1-GE1/0/13] port link-type trunk
[WAC1-GE1/0/13] port trunk allow-pass vlan 100 101
[WAC1-GE1/0/13] quit
```

```
[S3] vlan batch 100 101
[S3] interface GE 1/0/1
[S3-GE1/0/1] port link-type trunk
[S3-GE1/0/1] port trunk allow-pass vlan 100 101
[S3-GE1/0/1] quit
[S3] interface GE 1/0/4
[S3-GE1/0/4] port link-type trunk
[S3-GE1/0/4] port trunk allow-pass vlan 100 101
[S3-GE1/0/4] port trunk pvid vlan 100
[S3-GE1/0/4] quit
```

配置接口 IP 地址

```
[WAC1] interface Vlanif 100
[WAC1-Vlanif100] ip address 192.168.100.254 24
[WAC1-Vlanif100] quit
[WAC1] interface Vlanif 101
[WAC1-Vlanif101] ip address 192.168.101.254 24
[WAC1-Vlanif101] quit
```

DHCP 配置

```
[WAC1] dhcp enable
[WAC1] interface Vlanif 100
[WAC1-Vlanif100] dhcp select interface
[WAC1-Vlanif100] dhcp server option 43 sub-option 2 ip-address 192.168.100.254
[WAC1-Vlanif100] quit
[WAC1] interface Vlanif 101
[WAC1-Vlanif101] dhcp select interface
[WAC1-Vlanif101] quit
```

通过配置 Option 43 字段为 AP1 指定 WAC1 的 IPv4 地址。

步骤 3 配置 AP1 上线

创建名为 ap-group1 的 AP 组

```
[WAC1] wlan
[WAC1-wlan] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] quit
```

创建域管理模板，在域管理模板下配置 WAC1 的国家码

```
[WAC1-wlan] regulatory-domain-profile name default
```

域管理模板提供对 AP 的国家码、调优信道集合和调优带宽等配置。

缺省情况下，系统上存在名为 default 的域管理模板。故当前进入了默认存在的 default 模板。

```
[WAC1-wlan-regulate-domain-default] country-code cn
Info: The current country code is same with the input country code.
[WAC1-wlan-regulate-domain-default] quit
```

国家码用来标识 AP 射频所在的国家，不同国家码规定了不同的 AP 射频特性，包括 AP 的发送功率、支持的信道等。配置国家码是为了使 AP 的射频特性符合不同国家或区域的法律法规要求。缺省情况下，设备的国家码标识为 **CN**。

在 AP 组下引用域管理模板

```
[WAC1-wlan] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] regulatory-domain-profile default
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue? [Y/N]: y
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan] quit
```

在 AP 组视图下，**regulatory-domain-profile** 命令用来将指定的域管理模板引用到 AP 组。缺省情况下，AP 组下引用名为 default 的域管理模板。缺省的域管理模板中国家码为中国，2.4G 调优信道包括 1、6、11，5G 调优信道集合包括 149、153、157、161、165 。故这一步和上一步的配置在实际操作时可以省略。

配置 WAC1 建立 CAPWAP 隧道的源接口

```
[WAC1] capwap source interface Vlanif 100
Set the DTLS PSK(contains 8-32 plain-text characters, or 128 or 148 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): Huawei@123
Confirm PSK: Huawei@123
Info: Deliver DTLS PSK to devices using CAPWAP connections. It may take a few minutes.
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters, underscores, and digits, and must start with a letter): admin
```

```
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 128-268 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): Huawei@123
Confirm password: Huawei@123
Set the PSK of the global offline management VAP(plain-text password of 8-63 characters or cipher-text password of 128-188 characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): Huawei@123
Confirm PSK: Huawei@123
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be interrupted.
Info: Ensure that the management VLAN for devices is within the VLAN range mapping the source interface. Otherwise, the devices cannot go online.
```

capwap source interface 命令用来配置 WAC 建立 CAPWAP 隧道使用的接口，用于 WAC 和 AP 间建立 CAPWAP 隧道通信。

配置 CAPWAP 源接口时，会检查和安全相关的配置是否已存在，包括 DTLS 加密的 PSK、登录 AP 的用户名和密码、全局离线管理 VAP 的登录密码，均已存在才能成功配置，否则会提示用户先完成相关的配置。

在 WAC1 上离线导入 AP1，并将 AP1 加入配置好的 AP 组 ap-group1 中

WAC 上添加 AP 的方式有三种：

1. 离线导入 AP：预先配置 AP 的 MAC 地址和 SN，当 AP 与 WAC 连接时，如果 WAC 发现 AP 和预先增加的 AP 的 MAC 地址和 SN 匹配，则 WAC 开始与 AP 建立连接。
2. 自动发现 AP：当配置 AP 的认证模式为不认证或配置 AP 的认证模式为 MAC 或 SN 认证且将 AP 加入 AP 白名单中，则当 AP 与 WAC 连接时，AP 将被 WAC 自动发现并正常上线。
3. 手工确认未认证列表中的 AP：当配置 AP 的认证模式为 MAC 或 SN 认证，但 AP 没有离线导入且不在已设置的 AP 白名单中，则该 AP 会被记录到未授权的 AP 列表中。需要用户手工确认后，此 AP 才能正常上线。

```
[WAC1] wlan
[WAC1-wlan] ap auth-mode mac-auth
```

ap auth-mode 命令用来配置 AP 认证模式，只有通过认证的 AP 才能允许上线。除了 MAC 地址认证之外，还支持 SN 认证和不认证。缺省情况下，AP 认证模式为 MAC 地址认证。

通过 LLDP 查看 AP 的 MAC 地址

```
[S3] display lldp neighbor interface GE 1/0/4
GE1/0/4 has 1 neighbor(s):

Neighbor index                :1
Chassis type                  :MAC Address
Chassis ID                    :c0a9-389c-1b40
Port ID subtype               :Interface Name
Port ID                       :MultiGE0/0/0
```

```
Port description                    :--
System name                         :HUAWEI
System description                  :Huawei AP
Huawei YunShan OS
Version 1.24.0.1 (AirEngine 5700 V600R024C00SPC100)
Copyright (C) 2021-2024 Huawei Technologies Co., Ltd.
HUAWEI AirEngine5773-21
System capabilities supported       :wlanAccessPoint
System capabilities enabled         :wlanAccessPoint
Management address type             :IPv4
```

注：AP 的 MAC 地址和 SN 还可以通过设备包装箱内 MAC 地址标签和 SN 标签查询得到。

根据 AP 的 MAC 地址添加 AP

```
[WAC1-wlan] ap-id 1 ap-mac c0a9-389c-1b40
```

ap-id 命令用来离线增加 AP 设备或进入 AP 视图。

当增加 AP 时，若使用 MAC 认证，需要配置 **ap-mac** 参数；若使用 SN 认证，则需要配置 **ap-sn** 参数。

当进入 AP 视图时，只需要输入 **ap-id** 即可进入相应的 AP 视图。

```
[WAC1-wlan-ap-1] ap-name AP1
```

ap-name 命令用来配置单个 AP 的名称，注意各个 AP 的名字不能重复。如果未配置 AP 的名称，那么 AP 上线后默认的名称为 AP 的 MAC 地址。

```
[WAC1-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N] : y
[WAC1-wlan-ap-1] quit
[WAC1-wlan] quit
```

ap-group 命令用来配置 AP 所加入的组，WAC1 会给 AP 下发相应 ap-group 内的配置。比如此处 AP1 被加入了 ap-group1，那么 ap-group1 关联的域管理模板、射频模板、VAP 模板都会被下发给 AP1。缺省情况下，未配置 AP 加入的组，修改 AP 所加入的组后，WAC1 会下发配置，AP 将自动重启，并加入到修改后的 AP 组中。

等待几分钟，查看当前的 AP 信息

```
[WAC1] display ap all
Total AP information:
nor    : normal              [1]
ExtraInfo : Extra information
Total: 1
---------------------------------------------------------------------------------------------
```

```
ID      MAC            Name Group      IP              Type              State  STA  Uptime
ExtraInfo
-------------------------------------------------------------------------------------------
1       c0a9-389c-1b40 AP1   ap-group1 192.168.100.23 AirEngine5773-21 nor    0    4M:36S -
-------------------------------------------------------------------------------------------
```

display ap 命令用来查看 AP 信息，包括 AP 的 IP 地址、AP 的型号（AirEngine5773-21）、AP 的状态（nor）、上线时长等。

此外，还可以在命令后面加 **by-state** *state*、**by-ssid** *ssid* 来查筛选处于特定状态或者使用指定 SSID 的 AP。

可以看到此时两台 AP 都处于正常状态。

表14-2 AP 状态表

AP状态	描述
commit-failed（cmtfa）	AP上线后WLAN业务配置下发失败状态。
committing（cmt）	AP上线后WLAN业务配置正在下发状态。
config（cfg）	AP上线过程中WLAN业务配置正在下发状态。
config-failed（cfgfa）	AP上线过程中的WLAN业务配置下发失败状态。
download（dload）	AP正在升级状态。
fault	AP上线失败状态。
idle	AP和AC建链前的初始状态。
normal（nor）	AP正常状态。
standby（stdby）	AP在备AC上的正常状态。
ver-mismatch（vmiss）	AC和AP的版本不匹配状态。
countryCode-mismatch（cmiss）	AC和AP的国家码不匹配状态。
type-mismatch（tmiss）	AP类型不匹配状态。
unauth	AP未认证状态。

步骤 4 配置 WLAN 业务参数

创建名为 HCIA-WLAN 的安全模板，并配置安全策略

```
[WAC1] wlan
[WAC1-wlan] security-profile name HCIA-WLAN
[WAC1-wlan-sec-prof-HCIA-WLAN] security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
[WAC1-wlan-sec-prof-HCIA-WLAN] quit
```

security psk 命令用来配置 WPA/WPA2 的预共享密钥认证和加密。

当前使用 WPA 和 WPA2 混合方式，用户终端使用 WPA 或 WPA2 都可以进行认证。预共享密钥（PSK）为 HCIA-Datacom。通过 AES 加密算法加密用户数据。

创建名为 HCIA-WLAN 的 SSID 模板，并配置 SSID 名称为 HCIA-WLAN

```
[WAC1-wlan] ssid-profile name HCIA-WLAN
```

创建名为 HCIA-WLAN 的 SSID 模板。

```
[WAC1-wlan-ssid-prof-HCIA-WLAN] ssid HCIA-WLAN
[WAC1-wlan-ssid-prof-HCIA-WLAN] quit
```

配置 SSID 名称为 HCIA-WLAN。

创建名为 HCIA-WLAN 的 VAP 模板，配置业务数据转发模式、业务 VLAN，并且引用安全模板和 SSID 模板

```
[WAC1-wlan] vap-profile name HCIA-WLAN
```

vap-profile 命令用来创建 VAP 模板。

在 VAP 模板下可以配置数据转发模式，此外，VAP 模板能够引用 SSID 模板、安全模板、流量模板等。

```
[WAC1-wlan-vap-prof-HCIA-WLAN] forward-mode direct-forward
```

forward-mode 命令用来配置 VAP 模板下的数据转发方式，缺省情况下，VAP 模板下的数据转发方式为直接转发。

```
[WAC1-wlan-vap-prof-HCIA-WLAN] service-vlan vlan-id 101
```

service-vlan 命令用于配置 VAP 的业务 VLAN，当 STA 接入无线网络之后，从 AP 转发出来的用户数据就会带上 **service-vlan** 的 Tag。

```
[WAC1-wlan-vap-prof-HCIA-WLAN] security-profile HCIA-WLAN
```

引用安全模板 HCIA-WLAN。

```
[WAC1-wlan-vap-prof-HCIA-WLAN] ssid-profile HCIA-WLAN
[WAC1-wlan-vap-prof-HCIA-WLAN] quit
```

引用 SSID 模板 HCIA-WLAN。

配置 AP 组引用 VAP 模板，AP 上射频 0 和射频 1 都使用 VAP 模板 HCIA-WLAN 的配置

```
[WAC1-wlan] ap-group name ap-group1
```

```
[WAC1-wlan-ap-group-ap-group1] vap-profile HCIA-WLAN wlan 1 radio all
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan] quit
```

vap-profile 命令用来将指定的 VAP 模板引用到射频。执行该命令之后，VAP 下所有的配置，包括 VAP 引用的各类模板下的配置都会下发给到 AP 的射频。

```
[WAC1] display vap all
WID : WLAN ID
Total: 2
--------------------------------------------------------------------------------
AP ID AP name   RfID WID  BSSID            Status     Auth type       STA   SSID
--------------------------------------------------------------------------------
1     AP1       0    1    C0A9-389C-1B40 ON         WPA/WPA2-PSK    0     HCIA-WLAN
1     AP1       1    1    C0A9-389C-1B50 ON         WPA/WPA2-PSK    0     HCIA-WLAN
--------------------------------------------------------------------------------
```

display vap 命令用来查看业务型 VAP 的相关信息。可以看到 SSID 的名称为 HCIA-WLAN，认证方式为 WPA/WPA2-PSK，当前接入的终端数量为 0。

14.3 结果验证

请读者使用 STA 完成以下验证：

1. 使用 STA 接入 SSID 为 HCIA-WLAN 的无线信号，查看 STA 获取的 IP 地址，同时在 STA Ping 192.168.101.254。
2. STA 连接后，在 WAC1 上使用命令：**display station all** 查看 STA 信息。

14.4 配置参考

14.4.1 WAC1 的配置

```
sysname WAC1
#
vlan batch 100 to 101
#
dhcp enable
#
wlan
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
 ssid-profile name HCIA-WLAN
```

```
  ssid HCIA-WLAN
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 101
  ssid-profile HCIA-WLAN
  security-profile HCIA-WLAN
 ap-group name default
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
  radio 1
   vap-profile HCIA-WLAN wlan 1
  radio 2
   vap-profile HCIA-WLAN wlan 1
 ap-id 1 type-id 220 ap-mac c0a9-389c-1b40 ap-sn 21500867674ER9004989
  ap-name AP1
  ap-group ap-group1
 provision-ap
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select interface
 dhcp server option 43 sub-option 2 ip-address 192.168.100.254
#
interface Vlanif101
 ip address 192.168.101.254 255.255.255.0
 dhcp select interface
#
interface GE1/0/1
 shutdown
 port link-type access
#
interface GE1/0/10
 shutdown
 port link-type access
#
interface GE1/0/11
 shutdown
 port link-type access
#
interface GE1/0/12
 shutdown
 port link-type access
#
interface GE1/0/13
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GE1/0/14
```

```
 shutdown
 port link-type access
#
```

14.4.2 S3 的配置

```
sysname S3
#
vlan batch 100 to 101
#
interface GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GE1/0/2
 shutdown
 port link-type access
#
interface GE1/0/3
 shutdown
 port link-type access
#
interface GE1/0/4
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
```

14.5 思考题

1. 如果想让 AP1 释放一个用于访客接入的信号，在 WAC1 上需要做什么样的操作呢?

答案：先创建一个 SSID 模板，SSID 名称按需设置。然后创建一个新的 VAP 模板，最后在 AP 组下调用该 VAP 模板。

15 网络编程自动化实验（可选）

15.1 实验介绍

15.1.1 关于本实验

通过本实验，读者将掌握 Python paramiko 库的常用方法。

15.1.2 实验目的

- 掌握 Python 基本语法
- 掌握 paramiko 基本方法

15.1.3 实验组网介绍

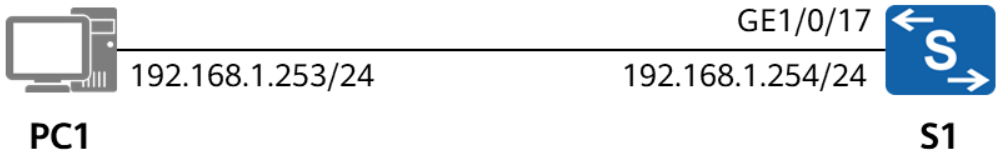


图15-1 网络编程自动化实验拓扑

15.1.4 实验背景

某公司现有一台交换机，IP 地址为 192.168.1.254/24。现在需要编写自动化脚本，查看设备当前配置文件。

15.2 实验任务配置

15.2.1 配置思路

1. 完成设备 STelnet 预配置：配置 STelnet 密码，开启 STelnet 功能和允许 STelnet 登录。
2. 编写 Python 脚本：调用 paramiko 登录设备，然后查看配置。

15.2.2 配置步骤

步骤 1 完成交换机的 STelnet 预配置

将 PC 连接至交换机的任意一个端口，此处以 GE1/0/17 端口为例，配置 IP 地址

```
[S1] interface GE 1/0/17
[S1-GE1/0/17] undo port link-type
[S1-GE1/0/17] undo portswitch
[S1-GE1/0/17] ip address 192.168.1.254 24
[S1-GE1/0/17] quit
```

配置 PC 的 IP 地址为 192.168.1.253/24

略

配置设备 STelnet 服务

```
[S1] stelnet server enable
[S1] ssh user python
[S1] ssh user python authentication-type password
[S1] ssh user python service-type stelnet
[S1] ssh server-source all-interface
Warning: SSH server source configuration will take effect in the next login. Continue? [Y/N] : y
Warning: It expands the range of accessed IP.
[S1] user-interface vty 0 4
[S1-ui-vty0-4] authentication-mode aaa
[S1-ui-vty0-4] protocol inbound ssh
[S1-ui-vty0-4] quit
[S1] aaa
[S1-aaa] local-user python password irreversible-cipher Huawei@123
[S1-aaa] local-user python privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue? [Y/N] : y
[S1-aaa] local-user python service-type ssh
Warning: If the service type of local users is configured multiple times, the new configuration overwrites the previous one. The new configuration may cause local user authentication to fail. Continue? [Y/N] : y
[S1-aaa] local-user python password-force-change disable
[S1-aaa] quit
```

本地管理员用户首次登录设备时，必须修改密码。通过命令 **local-user** *user-name* **password-force-change disable**，可以配置指定用户名的本地管理员用户在首次登录时，不修改密码。

PC 通过 CMD 登录测试。

```
C:\Users\XXX> ssh python@192.168.1.254
Warning: STelnet is not a secure protocol, and it is recommended to use Stelnet.
The authenticity of host '192.168.1.254 (192.168.1.254)' can't be established.
RSA key fingerprint is SHA256:ujt5Iv8B8yajsM7ieIIrkH2CZfUMSBcTA9bEAFQONls.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.254' (RSA) to the list of known hosts.
python@192.168.1.254's password: Huawei@123
Info: The max number of VTY users is 5, the number of current VTY users online is 1, and total number of terminal users online is 2.
        The current login time is XXXX-XX-XX 07:11:42.
<S1>
```

STelnet 配置成功！

步骤 2 Python 代码编写

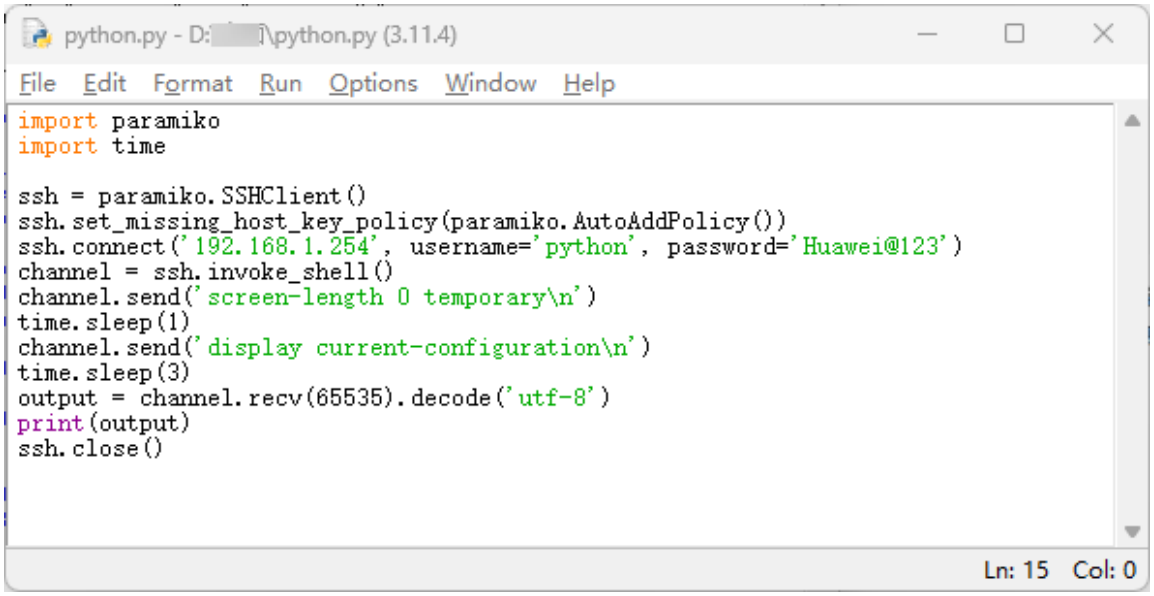
```
import paramiko
import time

ssh = paramiko.SSHClient()
ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
ssh.connect('192.168.1.254', username='python', password='Huawei@123')
channel = ssh.invoke_shell()
channel.send('screen-length 0 temporary\n')
time.sleep(1)
channel.send('display current-configuration\n')
time.sleep(3)
output = channel.recv(65535).decode('utf-8')
print(output)
ssh.close()
```

新建 python.py 文件，打开方式选择记事本，将代码编写完成后保存。

步骤 3 编译器执行

鼠标右键点击 python.py 文件，选择 Edit with IDLE，即使用 Python 自带的编译器打开。

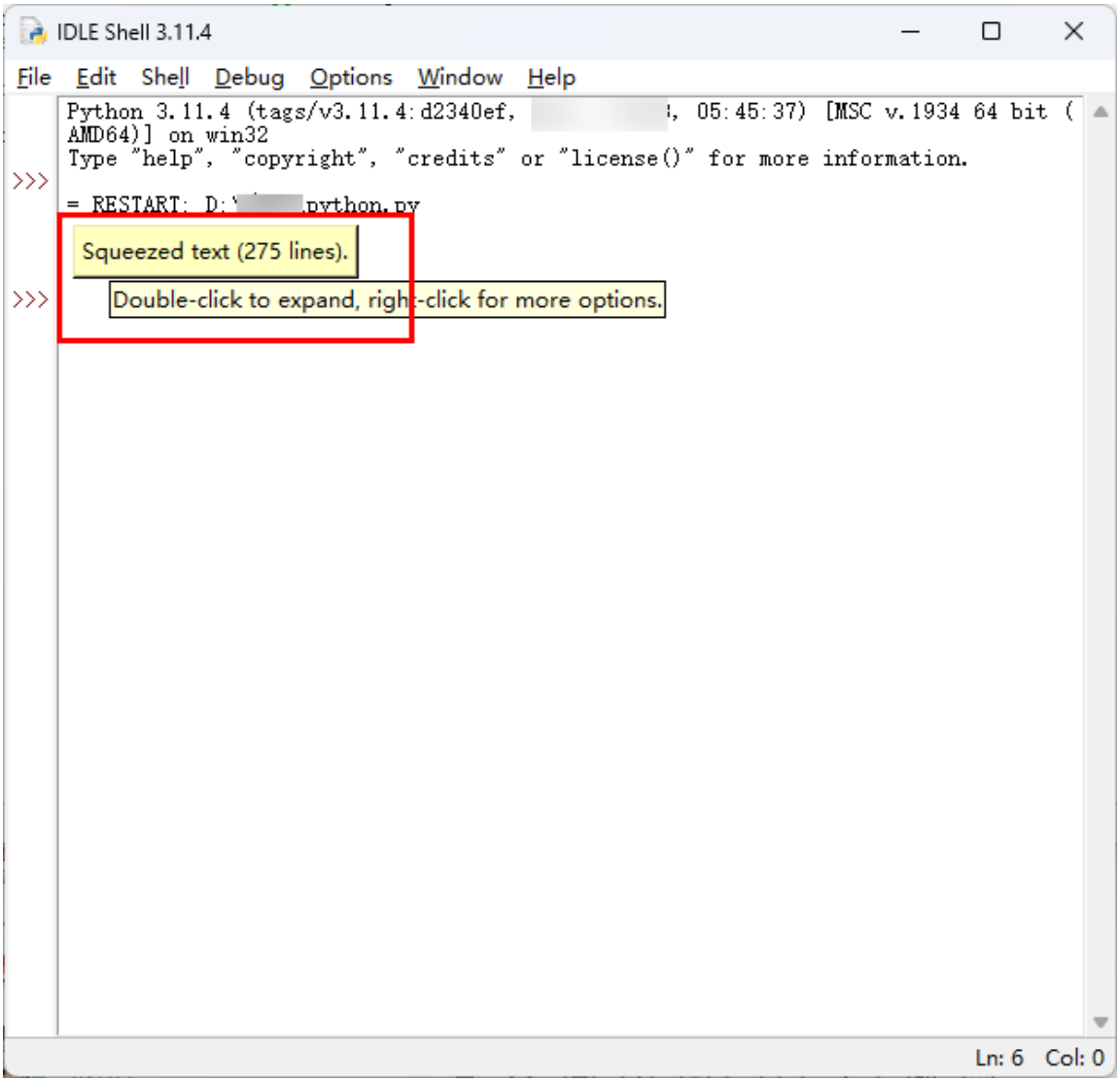
说明：如果右键菜单中没有 Edit with IDLE，可以在安装 Python 后，搜索 IDLE，然后点击 File -> Open 选择文件路径后打开文件。



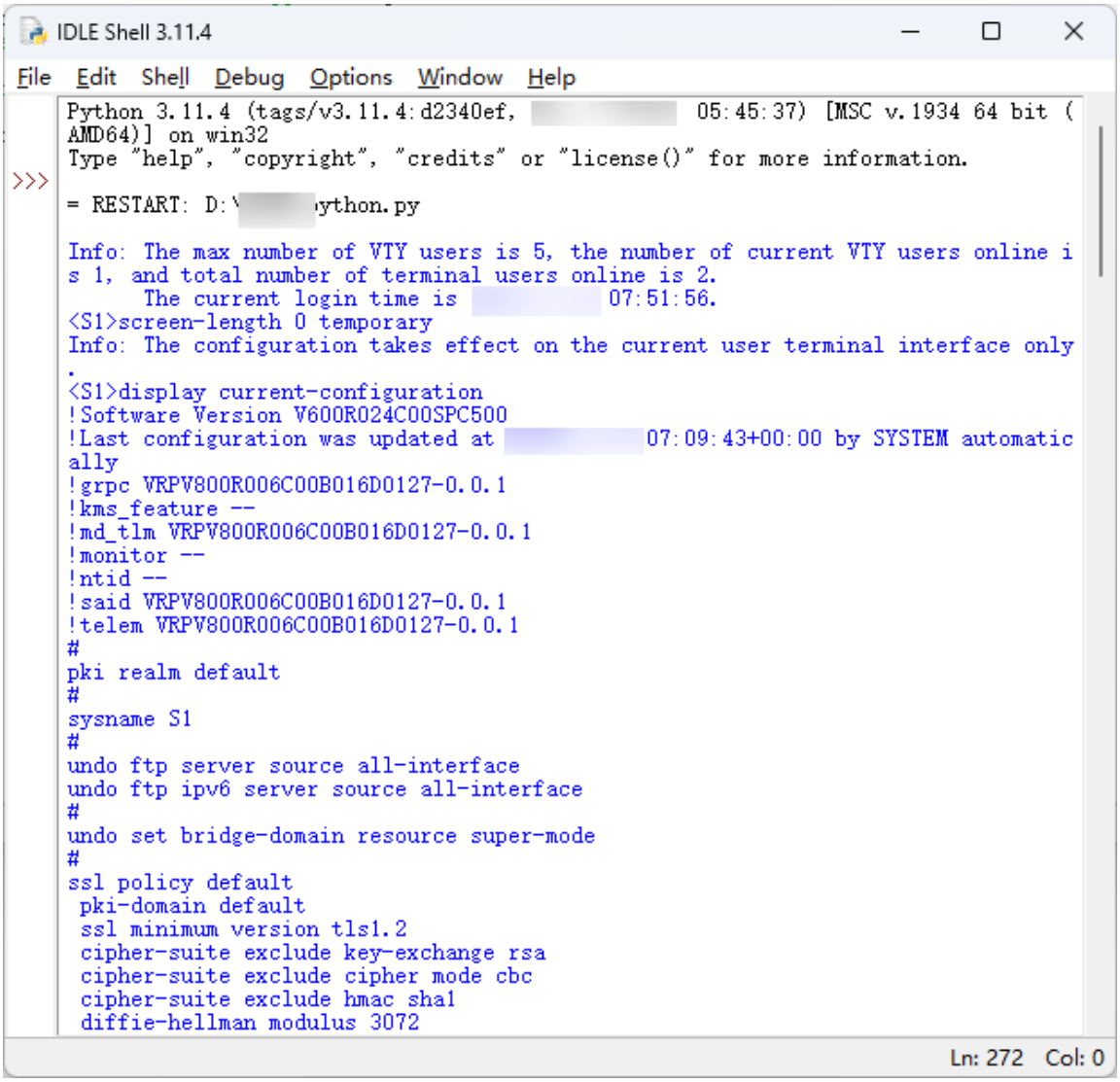
打开后选择工具栏中的 Run 或者使用快捷键 F5 运行 Python 脚本。您也可以使用其它编译器。

说明：请确保在使用此脚本时，您的环境中已安装 paramiko 库。如果未安装，可以在终端的 CMD 界面输入 **pip install paramiko** 命令进行安装。

步骤 4 输出结果



由于输出内容过多，需要双击查看所有输出内容。



15.2.3 代码解析

步骤 1 导入模块

```
import paramiko
import time
```

导入本段代码中需要使用的 paramiko 和 time 两个模块。time 模块无需安装。paramiko 模块需要手动安装，如果遇到安装问题，请参考 paramiko 安装指导文档：https://www.paramiko.org/installing.html。

本章节未介绍的 paramiko 方法请参考 paramiko API 文档：https://docs.paramiko.org/en/stable/。

Python 默认无间隔按顺序执行所有代码，在使用 praramiko 向交换机发送配置命令时可能会遇到响应不及时或者设备回显信息显示不全。此时，可以使用 time 模块下的 sleep 方法来人为暂停程序。

步骤 2 登录设备

```
ssh = paramiko.SSHClient()
```

创建 SSHClient 类的实例对象，这个对象将用于建立 SSH 连接和执行远程命令。

```
ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
```

设置自动添加未知主机密钥的策略。当首次连接新服务器时，会自动将主机密钥添加到本地 known_hosts 文件中（存在安全风险，仅建议在测试环境使用）。

```
ssh.connect('192.168.1.254', username='python', password='Huawei@123')
```

调用 paramiko 的 connect 方法，通过 SSH 协议与 IP 为 192.168.1.254 的设备建立连接，并使用用户名 python 和密码 Huawei@123 进行身份验证。连接成功后，后续命令即可在该远程设备上执行。

步骤 3 输入配置命令

```
channel = ssh.invoke_shell()
```

创建一个交互式的 shell 会话。与直接使用 exec_command 方法执行单个命令不同，invoke_shell 方法允许你与远程设备进行更复杂的交互，比如连续执行多个命令、处理命令提示符等。

```
channel.send('screen-length 0 temporary\n')
```

通过已建立的 SSH 连接向远程设备发送命令 **screen-length 0 temporary**。

screen-length temporary 命令用来设置指定终端屏幕的临时显示行数。缺省情况下，终端屏幕的每屏显示 24 行。*screen-length* 取值为 0 时表示关闭分屏功能。

```
time.sleep(1)
```

让程序暂停 1 秒钟，以便给远程设备足够的时间来处理命令并生成输出。

```
channel.send('display current-configuration\n')
time.sleep(3)
```

发送命令 **display current-configuration**，等待 3 秒钟。

```
output = channel.recv(65535).decode('utf-8')
```

channel.recv(65535)：这里的 recv 方法用于从 SSH 通道接收数据。参数 65535 指定了接收缓冲区的大小，即最多接收 65535 字节的数据。这个值可以根据实际需要调整，但通常设置为一个较大的值以确保能够接收完整的输出。

.decode('utf-8')：接收到的数据是以字节形式存在的，decode('utf-8') 方法将这些字节数据解码为字符串，以便于后续处理和显示。

output = 是用于将接收到的数据存储到变量 output 中。

```
print(output)
```

打印输出。

步骤 4 关闭会话

```
ssh.close()
```

调用 close()关闭当前会话。设备 VTY 连接数量有限，在执行完脚本后需要关闭此会话。

15.3 配置参考

15.3.1 S1 的配置

```
sysname S1
#
aaa
 local-user python password irreversible-cipher Huawei@123
 local-user python password-force-change disable
 local-user python privilege level 3
 local-user python service-type ssh
#
interface GE1/0/17
 undo portswitch
 ip address 192.168.1.254 255.255.255.0
#
stelnet server enable
ssh user python
ssh user python authentication-type password
ssh user python service-type stelnet
ssh server-source all-interface
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
```

15.4 思考题

1. 在本实验中，Python 代码执行时每次只发送了一条命令，如果想要一次性发送多条命令，有什么方法可以实现?

答案：可以使用以下代码：

```
import paramiko

# 定义网络设备的连接信息
ip = '192.168.1.254'
username = 'python'
password = 'Huawei@123'

# 创建一个 SSH 客户端
client = paramiko.SSHClient()
# 自动添加远程主机的 SSH 密钥
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())

try:
    # 连接到网络设备
    client.connect(ip, username=username, password=password)

    # 创建一个交互式的 shell
    shell = client.invoke_shell()

    # 等待设备的命令提示符
    while not shell.recv_ready():
        pass
    output = shell.recv(1024).decode('utf-8')

    # 定义要执行的命令列表
    commands = [
        'dis cu',
        'dis version',
        'dis ip int brief'
    ]

    # 逐条执行命令
    for command in commands:
        shell.send(f'{command}\n')
        while not shell.recv_ready():
            pass
        output = shell.recv(1024).decode('utf-8')
        print(output)

finally:
    # 关闭连接
  client.close()
```

以上代码仅做参考。

16 网络故障排除实验

16.1 实验介绍

16.1.1 关于本实验

作为一名网络工程师，不但需要具备规划和部署网络业务的能力，还需要具备当网络出现故障时，能够按照一定的流程进行故障定位和故障处理的能力。

在有线网络中，常见的故障有终端地址获取失败、网络环路、接口震荡、连通性问题等。在WLAN 中，常见的故障有 AP 上线失败、STA 上线失败等。

本实验将通过几个典型故障，帮助学员掌握故障处理的基本流程和常见的故障排查命令。

16.1.2 实验目的

- 掌握园区网络故障处理基本流程
- 掌握园区网络故障排查命令

16.1.3 实验组网介绍

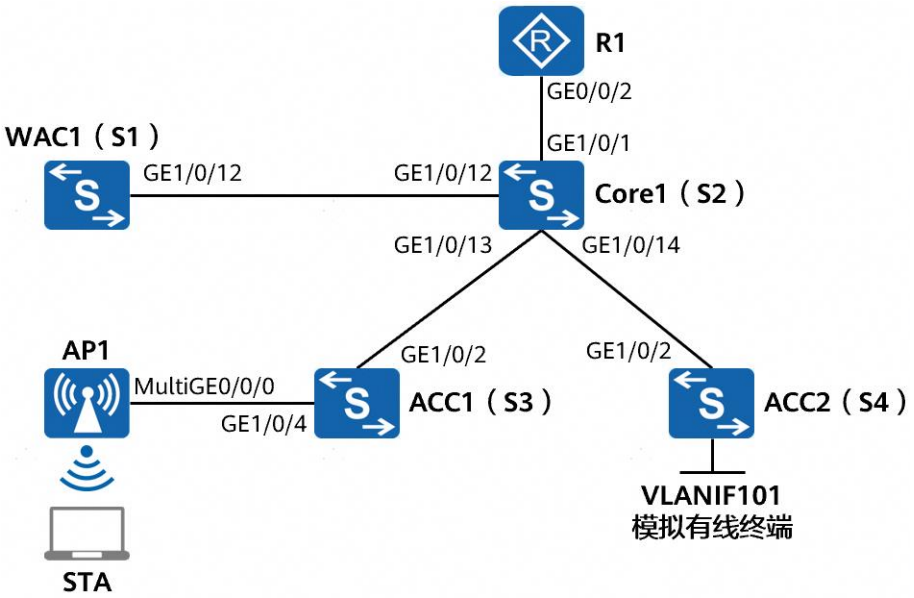


图16-1 网络故障排除实验拓扑

1. Core1（即 S2）为园区核心交换机，Core1 以下设备为二层设备。
2. Core1、WAC1、R1 间通过 OSPF 实现互联互通；Core1 为三层业务网关，作为 DHCP 服务器为无线和有线终端分配 IP 地址。其中有线终端使用 ACC2（即 S4）上 VLANIF101 接口模拟。
3. WAC1（即 S1）支持 WLAN-AC 功能（若实际环境所用交换机不支持，可用普通 WAC 替代），作为 WAC 使用；WAC1 与 AP1 处于三层网络，Core1 作为 DHCP 服务器给 AP1 分配 IP 地址，业务数据采用直接转发模式。

16.1.4 实验背景

某小型企业准备搭建一张园区网络供企业内人员办公使用，管理员按照业务规划完成网络部署后，发现存在终端 IP 地址获取失败、网络不通、AP 上线失败、STA 搜索不到无线信号等问题。

因此管理员对本网络进行了故障排除，以恢复业务网络的正常使用。

16.1.5 实验规划

表16-1 VLAN 规划

VLAN编号	VLAN描述
3	AP管理VLAN
10	Core1与R1互联VLAN
11	Core1与WAC1互联VLAN
100	无线终端业务VLAN
101	有线终端业务VLAN

表16-2 IP 地址规划

网络设备	接口	IP Address/Mask
Core1	VLANIF 3	192.168.3.254/24
	VLANIF 10	192.168.10.1/30
	VLANIF 11	192.168.11.1/30
	VLANIF 100	192.168.100.254/24
	VLANIF 101	192.168.101.254/24

	LoopBack 0	10.0.1.1/32
R1	GE0/0/2	192.168.10.2/30
	LoopBack 0	10.0.2.2/32
WAC1	VLANIF 11	192.168.11.2/30
	LoopBack 0	10.0.3.3/32

表16-3 WLAN 数据规划

配置项	配置参数
AP管理VLAN	VLAN 3
STA业务VLAN	VLAN 100
DHCP服务器	Core1作为DHCP服务器为AP1分配管理IP地址
	Core1作为DHCP服务器为STA分配业务IP地址
AP的IP地址池	192.168.3.1-192.168.3.253/24
STA的IP地址池	192.168.100.1-192.168.100.253/24
WAC的源接口IP地址	VLANIF11：192.168.11.2/30
AP组	名称：ap-group1
	引用模板：VAP模板HCIA-WLAN、域管理模板default
域管理模板	名称：default
	国家码：中国（CN）
SSID模板	名称：HCIA-WLAN
	SSID名称：HCIA-Guest
安全模板	名称：HCIA-WLAN
	安全策略：WPA-WPA2+PSK+AES
	密码：HCIA-Datacom
VAP模板	名称：HCIA-WLAN

	转发模式：直接转发
	业务VLAN：VLAN 100
	引用模板：SSID模板HCIA-WLAN、安全模板HCIA-WLAN

16.2 实验任务配置

16.2.1 配置思路

1. 导入预配，完成网络业务配置
2. 排查有线终端获取 IP 地址失败问题
3. 排查三层网络连通性异常问题
4. 排查 AP 上线失败问题
5. 排查 STA 无法搜索到无线信号问题

16.2.2 配置步骤

步骤 1 设备基础配置

关闭交换机的 ZTP 功能

Core1、ACC1、ACC2 与 WAC1 均采用以下配置关闭 ZTP 功能。

```
<HUAWEI> set ztp disable
Info: The ZTP process will be terminated. When restarting without a configuration file, the device will not start the ZTP process.
<HUAWEI> system-view
[HUAWEI]
```

步骤 2 导入预配置

在 R1 的系统视图下，导入 R1 的预配置

```
#
sysname R1
#
interface GE0/0/1
 shutdown
#
interface GE0/0/2
```

```
 undo portswitch
 ip address 192.168.10.2 255.255.255.252
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.255
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 192.168.10.2 0.0.0.0
#
lldp enable
#
```

在 WAC1 的系统视图下，导入 WAC1 的预配置

```
#
sysname WAC1
#
vlan batch 11 100
#
interface Vlanif11
 ip address 192.168.11.2 255.255.255.252
#
interface GE1/0/1
 shutdown
#
interface GE1/0/10
 shutdown
#
interface GE1/0/11
 shutdown
#
interface GE1/0/12
 port link-type access
 port default vlan 11
#
interface GE1/0/13
 shutdown
#
interface GE1/0/14
 shutdown
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.255
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.3 0.0.0.0
```

```
  network 192.168.11.2 0.0.0.0
#
wlan
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
 ssid-profile name HCIA-WLAN
  ssid HCIA-Guest
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 100
  security-profile HCIA-WLAN
 regulatory-domain-profile name default
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
  radio 1
   vap-profile HCIA-WLAN wlan 1
  radio 2
   vap-profile HCIA-WLAN wlan 1
#
capwap source interface vlanif 11
  Huawei@123
  Huawei@123
  admin
  Huawei@123
  Huawei@123
  Huawei@123
  Huawei@123
#
```

在 Core1 的系统视图下，导入 Core1 的预配置

```
#
sysname Core1
#
dhcp enable
#
vlan batch 3 10 to 11 100 to 101
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.3.254
 dhcp server option 43 sub-option 2 ip-address 192.168.11.2
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.252
#
interface Vlanif11
```

```
 ip address 192.168.11.1 255.255.255.252
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.100.254
#
interface Vlanif101
 shutdown
 ip address 192.168.101.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.101.254
#
interface GE1/0/1
 port link-type access
 port default vlan 10
#
interface GE1/0/10
 shutdown
#
interface GE1/0/11
 shutdown
#
interface GE1/0/12
 port link-type access
 port default vlan 11
#
interface GE1/0/13
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 100
#
interface GE1/0/14
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.10.1 0.0.0.0
  network 192.168.11.1 0.0.0.0
  network 192.168.100.0 0.0.0.255
  network 192.168.101.0 0.0.0.255
```

```
#
```

在 ACC1 的系统视图下，导入 ACC1 的预配置

```
#
sysname ACC1
#
vlan batch 3 100
#
interface GE1/0/1
 shutdown
#
interface GE1/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 100
#
interface GE1/0/3
 shutdown
#
interface GE1/0/4
 port link-type trunk
 port trunk pvid vlan 3
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 100
#
```

在 ACC2 的系统视图下，导入 ACC2 的预配置

```
#
sysname ACC2
#
vlan batch 101
#
interface Vlanif101
 ip address dhcp-alloc
#
interface GE1/0/1
 shutdown
#
interface GE1/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 101
#
interface GE1/0/3
 shutdown
```

```
#
interface GE1/0/4
 port link-type access
 port default vlan 101
#
```

步骤 3 排查故障：有线终端无法获取 IP 地址

查看有线终端无法获取 IP 地址的故障现象

在 ACC2 上 Ping 有线终端的业务网关地址。

```
[ACC2] ping 192.168.101.254
  PING 192.168.101.254: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

可以看到，Ping 测失败。

在 ACC2 上查看 VLANIF101 是否获得 IP 地址。

```
[ACC2] display ip interface Vlanif 101
Vlanif101 current state :          UP
Line protocol current state :      DOWN
The Maximum Transmit Unit :        1500 bytes
input packets : 0,        bytes :      0,    multicasts : 0
output packets : 0,       bytes :      0,    multicasts : 0
Directed-broadcast packets:
 received packets:                 0,    sent packets:        0
 forwarded packets:                0,    dropped packets:     0
Internet protocol processing :     disabled
Broadcast address : 0.0.0.0
TTL being 1 packet number:              0
TTL invalid packet number:              0
ICMP packet input number:               0
  Echo reply:                           0
  Unreachable:                          0
  Source quench:                        0
  Routing redirect:                     0
  Echo request:                         0
```

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

可以看到，ACC2 的 VLANIF101 接口未获取有线业务网段 192.168.101.0/24 中的地址。

检查设备互联接口状态是否正常（即检查 DHCP 客户端与服务器之间的链路是否正常）

在 ACC2 上查看接口状态。

```
[ACC2] display interface brief | include up
PHY: Physical
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(b): BFD down
(e): ETHOAM down
(d): Dampening Suppressed
(p): port alarm down
(dl): DLDP down
(c): CFM down
(sd): STP instance discarding
(ms): MACsec down
(ed): error down
(lb): LBDT block
InUti/OutUti: input utility rate/output utility rate
Interface         PHY     Protocol  InUti    OutUti   inErrors  outErrors
GE1/0/2           up      up        0.01%    0.01%    0         0
Vlanif101         up      down      --       --       0         0
```

可以看到，ACC2 与 Core1 互联的直连物理接口状态正常；ACC2 的 VLANIF101 接口物理状态正常，但是协议状态 **down**。说明 DHCP 客户端与服务器之间的物理链路正常。

检查接口放通 VLAN 是否正确

```
[ACC2] display vlan
The total number of vlans is : 2
--------------------------------------------------------------------------------
U: Up;          D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;                ST: Vlan-stacking;
```

```
#: ProtocolTransparent-vlan;          *: Management-vlan;
MAC-LRN: MAC-address learning;       STAT: Statistic;
BC: Broadcast;      MC: Multicast;   UC: Unknown-unicast;
FWD: Forward;       DSD: Discard;
--------------------------------------------------------------------------------
VID                 Ports
--------------------------------------------------------------------------------
  1                 UT: ......
101                 TG:GE1/0/2(U)

VID  Type       Status   Property   MAC-LRN STAT      BC   MC   UC   Description
--------------------------------------------------------------------------------
  1 common     enable   default    enable   disable FWD FWD FWD VLAN 0001
101 common     enable   default    enable   disable FWD FWD FWD VLAN 0101
```

```
[Core1] display vlan
The total number of vlans is : 6
--------------------------------------------------------------------------------
U: Up;              D: Down;             TG: Tagged;             UT: Untagged;
MP: Vlan-mapping;                        ST: Vlan-stacking;
#: ProtocolTransparent-vlan;             *: Management-vlan;
MAC-LRN: MAC-address learning;           STAT: Statistic;
BC: Broadcast;      MC: Multicast;       UC: Unknown-unicast;
FWD: Forward;       DSD: Discard;
--------------------------------------------------------------------------------
VID                 Ports
--------------------------------------------------------------------------------
  1                 UT: ......
  3                 TG:GE1/0/13(U)
 10                 UT:GE1/0/1(U)
 11                 UT:GE1/0/12(U)
100                 TG:GE1/0/13(U)
101                 TG:GE1/0/14(U)

VID  Type       Status   Property   MAC-LRN STAT      BC   MC   UC   Description
--------------------------------------------------------------------------------
  1 common     enable   default    enable   disable FWD FWD FWD VLAN 0001
  3 common     enable   default    enable   disable FWD FWD FWD VLAN 0003
 10 common     enable   default    enable   disable FWD FWD FWD VLAN 0010
 11 common     enable   default    enable   disable FWD FWD FWD VLAN 0011
100 common     enable   default    enable   disable FWD FWD FWD VLAN 0100
101 common     enable   default    enable   disable FWD FWD FWD VLAN 0101
```

可以看到，ACC2 与 Core1 的互联口已放通业务 VLAN 101。

检查 DHCP 客户端配置是否正确

在 ACC2 上查看 VLANIF101 接口配置。

```
[ACC2] interface Vlanif 101
[ACC2-Vlanif101] display this
#
interface Vlanif101
 ip address dhcp-alloc
#
return
[ACC2-Vlanif101] quit
```

可以看到，ACC2 的 VLANIF101 接口已配置为通过 DHCP 方式动态获取 IP 地址。

检查 DHCP 服务器配置是否正确

在 Core1 上查看接口地址池的配置情况。

```
[Core1] display ip pool interface Vlanif101

  Pool-name              :     Vlanif101
  Pool-No                :     2
  Lease                  :     1 Days 0 Hours 0 Minutes
  Domain-name            :     -
  DNS-server0            :     -
  NBNS-server0           :     -
  Netbios-type           :     -
  Position               :     Interface
  Status                 :     Unlocked
  Gateway-0              :     192.168.101.254
  Network                :     192.168.101.0
  Mask                   :     255.255.255.0
  VPN instance           :     --
  Logging                :     Disable
  Conflicted address recycle interval: -
  Address Statistic: Total          :253            Used           :0
                     Idle           :253            Expired        :0
                     Conflict       :0              Disabled       :0


 ------------------------------------------------------------------------------------------------------
  Network section
   Start           End                 Total     Used     Idle(Expired)   Conflict   Disabled
 ------------------------------------------------------------------------------------------------------
   192.168.101.1   192.168.101.254     253       0        253(0)          0          0
 ------------------------------------------------------------------------------------------------------
```

可以看到，有线终端业务 IP 地址池范围正确，但是未分配任何 IP 地址。

综上所述可以判断出，Core1 的接口地址池配置正确但是未分配地址，因此需要进一步检查该接口地址池的接口状态。

检查 Core1 的 VLANIF101 接口状态

```
[Core1] display interface Vlanif 101
Vlanif101 current state :      Administratively DOWN (ifindex: 40)
Line protocol current state : DOWN
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.101.254/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 20df-73f5-4575
Physical is VLANIF
Current system time: XXXX-XX-XX 09:23:21
      Input bandwidth utilization   : --
      Output bandwidth utilization : --
```

可以看到，Core1 的 VLANIF101 接口状态为 **Administratively DOWN**，说明该接口被管理员误操作键入了 **shutdown** 命令。

进一步检查 Core1 的 VLANIF101 的接口配置。

```
[Core1] interface Vlanif 101
[Core1-Vlanif101] display this
#
interface Vlanif101
 shutdown
 ip address 192.168.101.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.101.254
#
return
```

可以看到，VLANIF101 接口被 **shutdown**，通过输入 **undo shutdown** 恢复接口状态。

```
[Core1-Vlanif101] undo shutdown
[Core1-Vlanif101] quit
```

再次在 ACC2 上查看 VLANIF101 是否获得 IP 地址

```
[ACC2] display ip interface Vlanif 101
Vlanif101 current state :      UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets :     0,     bytes :     0,     multicasts : 0
output packets :    0,     bytes :     0,     multicasts : 0
Directed-broadcast packets:
 received packets:0,          sent packets:          0
 forwarded packets: 0,        dropped packets:     0
Internet Address is allocated by DHCP, 192.168.101.170/24
Broadcast address : 0.0.0.0
TTL being 1 packet number:              0
```

```
TTL invalid packet number:          0
ICMP packet input number:           0
  Echo reply:                       0
  Unreachable:                      0
  Source quench:                    0
  Routing redirect:                 0
  Echo request:                     0
  Router advert:                    0
  Router solicit:                   0
  Time exceed:                      0
  IP header bad:                    0
  Timestamp request:                0
  Timestamp reply:                  0
  Information request:              0
  Information reply:                0
  Netmask request:                  0
  Netmask reply:                    0
  Unknown type:                     0
```

可以看到，ACC2 的 VLANIF101 接口已成功通过 DHCP 获取有线业务网段 192.168.101.0/24 中的一个业务 IP 地址。

再次在 ACC2 上 Ping 测有线业务网关地址

```
[ACC2] ping 192.168.101.254
  PING 192.168.101.254: 56  data bytes, press CTRL_C to break
    Reply from 192.168.101.254: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.101.254: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.101.254: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.101.254: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.101.254: bytes=56 Sequence=5 ttl=254 time=1 ms

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

可以看到，ACC2 已成功 Ping 通 Core1 上有线业务网段的网关地址。

有线终端无法获取 IP 地址问题已解决。

步骤 4 排查故障：三层网络连通性异常

查看三层网络连通性异常的故障现象

该网络业务要求三层设备（Core1、R1 和 WAC1）之间的环回口均可互相 Ping 通。

在 Core1 上 Ping R1 的环回口地址（10.0.2.2）。

```
[Core1] ping 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

可以看到，Ping 测失败。

检查设备互联接口状态是否正常

```
[Core1] display interface brief | include up
PHY: Physical
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(b): BFD down
(e): ETHOAM down
(d): Dampening Suppressed
(p): port alarm down
(dl): DLDP down
(c): CFM down
(sd): STP instance discarding
(ms): MACsec down
(ed): error down
(lb): LBDT block
InUti/OutUti: input utility rate/output utility rate
Interface         PHY     Protocol  InUti    OutUti   inErrors  outErrors
GE1/0/1           up      up        0.01%    0.01%    0         0
GE1/0/12          up      up        0.01%    0.01%    0         0
GE1/0/13          up      up        0.01%    0.01%    0         0
GE1/0/14          up      up        0.01%    0.01%    0         0
LoopBack0         up      up(s)     --       --       0         0
Vlanif3           up      up        --       --       0         0
Vlanif10          up      up        --       --       0         0
Vlanif11          up      up        --       --       0         0
Vlanif100         up      up        --       --       0         0
Vlanif101         up      up        --       --       0         0
```

可以看到，Core1 与 R1 的互联口状态正常。

检查接口放通 VLAN 是否正确

```
[Core1] display vlan
The total number of vlans is : 6
--------------------------------------------------------------------------------
U: Up;              D: Down;          TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                     ST: Vlan-stacking;
#: ProtocolTransparent-vlan;          *: Management-vlan;
MAC-LRN: MAC-address learning;        STAT: Statistic;
BC: Broadcast;      MC: Multicast;    UC: Unknown-unicast;
FWD: Forward;       DSD: Discard;
--------------------------------------------------------------------------------
VID                 Ports
--------------------------------------------------------------------------------
   1                UT: ......
   3                TG:GE1/0/13(U)
  10                UT:GE1/0/1(U)
  11                UT:GE1/0/12(U)
 100                TG:GE1/0/13(U)
 101                TG:GE1/0/14(U)

VID  Type       Status   Property   MAC-LRN STAT      BC   MC   UC   Description
--------------------------------------------------------------------------------
   1 common     enable   default    enable  disable FWD  FWD  FWD  VLAN 0001
   3 common     enable   default    enable  disable FWD  FWD  FWD  VLAN 0003
  10 common     enable   default    enable  disable FWD  FWD  FWD  VLAN 0010
  11 common     enable   default    enable  disable FWD  FWD  FWD  VLAN 0011
 100 common     enable   default    enable  disable FWD  FWD  FWD  VLAN 0100
 101 common     enable   default    enable  disable FWD  FWD  FWD  VLAN 0101
```

可以看到，Core1 与 R1 的互联口已放通互联 VLAN 10。

检查接口 IP 地址配置是否正确

```
[Core1] display ip interface brief
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(ed): error down
The number of interface that is UP in Physical is 7
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 7
The number of interface that is DOWN in Protocol is 1
Interface           IP Address/Mas          Physical   Protocol  VPN
LoopBack0           10.0.1.1/32             up         up(s)     --
Vlanif3             192.168.3.254/24        up         up        --
```

```
Vlanif10        192.168.10.1/30     up         up          --
Vlanif11        192.168.11.1/30     up         up          --
Vlanif100       192.168.100.254/24  up         up          --
Vlanif101       192.168.101.254/24  up         up          --
```

```
[R1] display ip interface brief
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(ed): error down
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 2
The number of interface that is UP in Protocol is 4
The number of interface that is DOWN in Protocol is 2
Interface         IP Address/Mask      Physical   Protocol  VPN
GE0/0/2           192.168.10.2/30      up         up        --
LoopBack0         10.0.2.2/32          up         up(s)     --
```

可以看到，Core1 与 R1 的互联口和环回口 IP 地址均配置正确，且状态正常。

检查路由是否正常

```
[Core1] display ip routing-table
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 21        Routes : 21
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
10.0.1.1/32         Direct  0    0         D     127.0.0.1       LoopBack0
10.0.3.3/32         OSPF    10   1         D     192.168.11.2    Vlanif11
127.0.0.0/8         Direct  0    0         D     127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0         D     127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0         D     127.0.0.1       InLoopBack0
192.168.3.0/24      Direct  0    0         D     192.168.3.254   Vlanif3
192.168.3.254/32    Direct  0    0         D     127.0.0.1       Vlanif3
192.168.3.255/32    Direct  0    0         D     127.0.0.1       Vlanif3
192.168.10.0/30     Direct  0    0         D     192.168.10.1    Vlanif10
192.168.10.1/32     Direct  0    0         D     127.0.0.1       Vlanif10
192.168.10.3/32     Direct  0    0         D     127.0.0.1       Vlanif10
192.168.11.0/30     Direct  0    0         D     192.168.11.1    Vlanif11
192.168.11.1/32     Direct  0    0         D     127.0.0.1       Vlanif11
192.168.11.3/32     Direct  0    0         D     127.0.0.1       Vlanif11
192.168.100.0/24    Direct  0    0         D     192.168.100.254 Vlanif100
```

```
192.168.100.254/32    Direct  0    0    D   127.0.0.1       Vlanif100
192.168.100.255/32    Direct  0    0    D   127.0.0.1       Vlanif100
192.168.101.0/24      Direct  0    0    D   192.168.101.254 Vlanif101
192.168.101.254/32    Direct  0    0    D   127.0.0.1       Vlanif101
192.168.101.255/32    Direct  0    0    D   127.0.0.1       Vlanif101
255.255.255.255/32    Direct  0    0    D   127.0.0.1       InLoopBack0
```

可以看到，Core1 的 IP 路由表中存在与 R1 直连网段路由，但是没有学习到 R1 的环回口地址的 OSPF 路由。

```
[R1] display ip routing-table
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
10.0.1.1/32         OSPF    10   1           D   192.168.10.1    GE0/0/2
10.0.2.2/32         Direct  0    0           D   127.0.0.1       LoopBack0
10.0.3.3/32         OSPF    10   2           D   192.168.10.1    GE0/0/2
127.0.0.0/8         Direct  0    0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
192.168.3.0/24      OSPF    10   2           D   192.168.10.1    GE0/0/2
192.168.10.0/30     Direct  0    0           D   192.168.10.2    GE0/0/2
192.168.10.2/32     Direct  0    0           D   127.0.0.1       GE0/0/2
192.168.10.3/32     Direct  0    0           D   127.0.0.1       GE0/0/2
192.168.11.0/30     OSPF    10   2           D   192.168.10.1    GE0/0/2
192.168.100.0/24    OSPF    10   2           D   192.168.10.1    GE0/0/2
192.168.101.0/24    OSPF    10   2           D   192.168.10.1    GE0/0/2
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

可以看到，R1 的 IP 路由表中存在与 Core1 直连网段路由和 Core1 的环回口地址的 OSPF 路由，同时也有自身环回口地址的直连路由。

综上所述可以判断出，Core1 与 R1 的 OSPF 邻居正常，但是 R1 没有将 LoopBack0 地址相关路由引入 OSPF，因此 Core1 无法学习到。

检查 R1 的 OSPF 配置

```
[R1] ospf 1
[R1-ospf-1] display this
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 192.168.10.2 0.0.0.0
#
```

```
return
```

可以看到，R1 没有在 LoopBack0 启用 OSPF。

修改 R1 的 OSPF 配置，在 LoopBack0 接口启用 OSPF

```
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 10.0.2.2 0.0.0.0
[R1-ospf-1-area-0.0.0.0] quit
[R1-ospf-1] quit
```

再次检查 Core1 的 IP 路由表

```
[Core1] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 22        Routes : 22
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
10.0.1.1/32         Direct  0    0           D   127.0.0.1       LoopBack0
10.0.2.2/32         OSPF    10   1           D   192.168.10.2    Vlanif10
10.0.3.3/32         OSPF    10   1           D   192.168.11.2    Vlanif11
127.0.0.0/8         Direct  0    0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
192.168.3.0/24      Direct  0    0           D   192.168.3.254   Vlanif3
192.168.3.254/32    Direct  0    0           D   127.0.0.1       Vlanif3
192.168.3.255/32    Direct  0    0           D   127.0.0.1       Vlanif3
192.168.10.0/30     Direct  0    0           D   192.168.10.1    Vlanif10
192.168.10.1/32     Direct  0    0           D   127.0.0.1       Vlanif10
192.168.10.3/32     Direct  0    0           D   127.0.0.1       Vlanif10
192.168.11.0/30     Direct  0    0           D   192.168.11.1    Vlanif11
192.168.11.1/32     Direct  0    0           D   127.0.0.1       Vlanif11
192.168.11.3/32     Direct  0    0           D   127.0.0.1       Vlanif11
192.168.100.0/24    Direct  0    0           D   192.168.100.254 Vlanif100
192.168.100.254/32  Direct  0    0           D   127.0.0.1       Vlanif100
192.168.100.255/32  Direct  0    0           D   127.0.0.1       Vlanif100
192.168.101.0/24    Direct  0    0           D   192.168.101.254 Vlanif101
192.168.101.254/32  Direct  0    0           D   127.0.0.1       Vlanif101
192.168.101.255/32  Direct  0    0           D   127.0.0.1       Vlanif101
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

可以看到，Core1 已经学习到 R1 的环回口地址的 OSPF 路由。

再次在 Core1 上检测与 R1 环回口的连通性

```
[Core1] ping 10.0.2.2
```

```
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=255 time=1 ms

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

可以看到，Core1 已成功 Ping 通 R1 的环回口地址。

三层网络连通性异常问题已解决。

步骤 5 排查故障：AP1 上线 WAC1 失败

查看 AP1 上线失败的故障现象

在 WAC1 上查看 AP1 的上线情况。

```
[WAC1] display ap all
Total AP information:
unauth: unauthed            [1]
ExtraInfo : Extra information
Total: 1
------------------------------------------------------------------------------------------------------------
ID      MAC               Name   Group   IP Type                 State    STA   Uptime ExtraInfo
------------------------------------------------------------------------------------------------------------
-       c0a9-389c-1b40    -      -       -    AirEngine5773-21   unauth   -     -      -
------------------------------------------------------------------------------------------------------------
```

可以看到，AP1 未上线，且状态为 **unauth**。

查看 AP1 上线失败的具体原因

```
[WAC1] display ap online-fail-record all
Total APs: 1 Total records: 1
------------------------------------------------------------------------------------------------------------
MAC               Last fail time              Reason
------------------------------------------------------------------------------------------------------------
c0a9-389c-1b40    20XX-11-26/09:43:43         The AP is not in the MAC whitelist
------------------------------------------------------------------------------------------------------------
```

可以看到，AP1 未上线的具体原因是 **The AP is not in the MAC whitelist**，也就是 AP1 不在 MAC 白名单中。

将 AP1 手动添加至 MAC 认证列表

在 WAC1 上添加 AP1，同时配置 AP1 的名称和所属 AP 组。

```
[WAC1] wlan
[WAC1-wlan] ap-id 1 ap-mac c0a9-389c-1b40
[WAC1-wlan-ap-1] ap-name AP1
[WAC1-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N]: y
[WAC1-wlan-ap-1] quit
[WAC1-wlan] quit
```

AP1 的 MAC 地址可以通过在 WAC1 上执行命令 **display ap all** 获取到。

过一段时间后，再次查看 AP1 的上线情况

```
[WAC1] display ap all
Total AP information:
nor    : normal              [1]
ExtraInfo : Extra information
Total: 1
-------------------------------------------------------------------------------------------------------------------
ID MAC               Name Group      IP              Type              State  STA  Uptime ExtraInfo
-------------------------------------------------------------------------------------------------------------------
1  c0a9-389c-1b40    AP1  ap-group1  192.168.3.158   AirEngine5773-21  nor    0    22S    -
-------------------------------------------------------------------------------------------------------------------
```

可以看到，AP1 已成功上线 WAC1，其状态为 **nor**（即 normal）。

AP1 上线 WAC1 失败问题已解决。

步骤 6 排查故障：STA 无法搜索到无线信号

查看 STA 无法搜索到无线信号的故障现象

AP1 上线成功后，尝试用 STA 在附近搜索无线信号“HCIA-Guest”，但是未搜到。

所以登录 WAC1 检查 VAP 状态信息。

```
[WAC1] display vap all
WID : WLAN ID
Total: 2
-------------------------------------------------------------------------------------------------------------
AP ID AP name   RfID WID  BSSID          Status  Auth type        STA  SSID
-------------------------------------------------------------------------------------------------------------
1     AP1       0    1    C0A9-389C-1B40 ON      WPA/WPA2-PSK     0    HUAWEI-WLAN
1     AP1       1    1    C0A9-389C-1B50 ON      WPA/WPA2-PSK     0    HUAWEI-WLAN
-------------------------------------------------------------------------------------------------------------
```

可以看到，当前的 VAP 关联的 SSID 名称为“HUAWEI-WLAN”。

检查 WLAN 业务的配置信息

在 WAC1 上查看 VAP 和 SSID 模板的配置信息。

```
[WAC1] wlan
[WAC1-wlan] display this
#
wlan
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase Huawei@123 aes
 ssid-profile name HCIA-WLAN
  ssid HCIA-Guest
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 100
  security-profile HCIA-WLAN
 regulatory-domain-profile name default
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
  radio 1
   vap-profile HCIA-WLAN wlan 1
  radio 2
   vap-profile HCIA-WLAN wlan 1
 ap-id 1 type-id 220 ap-mac c0a9-389c-1b40 ap-sn 21500867674ER9004989
  ap-name AP1
  ap-group ap-group1
#
return
```

可以看到，WAC1 的 SSID 模板配置正确，但是 VAP 模板下未引用已配置的 SSID 模板。

修正 WLAN 的 VAP 模板配置

在 WAC1 上手动在 VAP 模板下引用 SSID 模板。

```
[WAC1-wlan] vap-profile name HCIA-WLAN
[WAC1-wlan-vap-prof-HCIA-WLAN] ssid-profile HCIA-WLAN
Warning: This action may cause service interruption. Continue? [Y/N]: y
[WAC1-wlan-vap-prof-HCIA-WLAN] quit
[WAC1-wlan] quit
```

再次查看 VAP 状态信息

```
[WAC1] display vap all
WID : WLAN ID
Total: 2
--------------------------------------------------------------------------------------------------------
AP ID AP name   RfID WID   BSSID            Status   Auth type          STA    SSID
--------------------------------------------------------------------------------------------------------
1     AP1       0    1     C0A9-389C-1B40 ON       WPA/WPA2-PSK   0      HCIA-Guest
```

```
1       AP1         1     1     C0A9-389C-1B50 ON          WPA/WPA2-PSK   0       HCIA-Guest
-------------------------------------------------------------------------------------------------------------
```

可以看到，SSID 信息已更新为“HCIA-Guest”。

STA 无法搜索到无线信号问题已解决。

16.3 结果验证

请读者使用无线终端 STA 完成以下验证：

1. 使用 STA 搜索并接入 SSID 为“HCIA-Guest”的无线信号，在终端的“命令提示符”界面查看 STA 获取的 IP 地址，同时在 STA 上执行命令 **ping 192.168.100.254**。
2. STA 连接 SSID 后，在 WAC1 上使用命令 **display station all** 查看 STA 信息。
3. STA 获取地址后，在 Core1 上使用命令 **display ip pool interface Vlanif100 used** 查看接口地址池的地址分配情况。
4. STA 获取地址后，执行命令 **ping 10.0.3.3**，测试与 WAC1 的三层连通性。

请读者使用有线终端（ACC2 的 VLANIF101）完成以下验证：

1. 在 ACC2 上通过命令 **display ip interface Vlanif 101** 查看 VLANIF101 动态获取的 IP 地址，同时在 ACC2 上执行命令 **ping -a *动态获取的 IP 地址* 192.168.101.254**。
2. VLANIF101 获取地址后，在 Core1 上使用命令 **display ip pool interface Vlanif101 used** 查看接口地址池的地址分配情况。
3. VLANIF101 获取地址后，执行命令 **ping 10.0.2.2**，测试与 R1 的三层连通性。

16.4 配置参考

16.4.1 R1 的配置

```
#
sysname R1
#
interface GE0/0/1
 shutdown
#
interface GE0/0/2
 ip address 192.168.10.2 255.255.255.252
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.255
```

```
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.2.2 0.0.0.0
  network 192.168.10.2 0.0.0.0
#
lldp enable
#
return
```

16.4.2 WAC1 的配置

```
#
sysname WAC1
#
wlan
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
 ssid-profile name HCIA-WLAN
  ssid HCIA-Guest
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 100
  ssid-profile HCIA-WLAN
  security-profile HCIA-WLAN
 regulatory-domain-profile name default
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
  radio 1
   vap-profile HCIA-WLAN wlan 1
  radio 2
   vap-profile HCIA-WLAN wlan 1
 ap-id 1 type-id 220 ap-mac c0a9-389c-1b40 ap-sn 21500867674ER9004989
  ap-name AP1
  ap-group ap-group1
#
capwap source interface vlanif 11
#
vlan batch 11 100
#
interface Vlanif11
 ip address 192.168.11.2 255.255.255.252
#
interface GE1/0/1
 shutdown
#
```

```
interface GE1/0/10
 shutdown
#
interface GE1/0/11
 shutdown
#
interface GE1/0/12
 port link-type access
 port default vlan 11
#
interface GE1/0/13
 shutdown
#
interface GE1/0/14
 shutdown
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.255
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.3 0.0.0.0
  network 192.168.11.2 0.0.0.0
#
return
```

16.4.3 Core1 的配置

```
#
sysname Core1
#
dhcp enable
#
vlan batch 3 10 to 11 100 to 101
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.3.254
 dhcp server option 43 sub-option 2 ip-address 192.168.11.2
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.252
#
interface Vlanif11
 ip address 192.168.11.1 255.255.255.252
```

```
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.100.254
#
interface Vlanif101
 ip address 192.168.101.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.101.254
#
interface GE1/0/1
 port link-type access
 port default vlan 10
#
interface GE1/0/10
 shutdown
#
interface GE1/0/11
 shutdown
#
interface GE1/0/12
 port link-type access
 port default vlan 11
#
interface GE1/0/13
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 100
#
interface GE1/0/14
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.10.1 0.0.0.0
  network 192.168.11.1 0.0.0.0
  network 192.168.100.0 0.0.0.255
  network 192.168.101.0 0.0.0.255
#
return
```

16.4.4 ACC1 的配置

```
#
sysname ACC1
#
vlan batch 3 100
#
interface GE1/0/1
 shutdown
#
interface GE1/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 100
#
interface GE1/0/3
 shutdown
#
interface GE1/0/4
 port link-type trunk
 port trunk pvid vlan 3
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 100
#
return
```

16.4.5 ACC2 的配置

```
#
sysname ACC2
#
vlan batch 101
#
interface Vlanif101
 ip address dhcp-alloc
#
interface GE1/0/1
 shutdown
#
interface GE1/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 101
#
interface GE1/0/3
```

```
 shutdown
#
return
```

16.5 思考题

1. 当要检测网络间连通性问题时，一般采用哪些测试工具?

答案:

使用 Ping 命令检查网络连接及主机是否可达。

使用 Tracert 命令检查数据包从发送端到目的地所经过的设备节点和网络可达性。

2. AP1 上线 WAC1 失败的常见原因有哪些?

答案:

硬件问题：物理设备故障、连接部件故障、供电模块故障等。

软件问题：网络配置错误（如 DHCP 配置错误、网络互通配置错误、AP 认证配置错误、黑白名单配置错误等）、软件版本不匹配、WAC 的 License 不足等。

17 园区网络综合实验

17.1 实验介绍

17.1.1 关于本实验

信息社会通信网络无处不在，而园区网络一直处在网络的战略核心位置。可以说在一个城市中，除了马路和家庭之外，都是园区，包括工厂、政府机关、商场、写字楼、校园等。据统计，90%的城市居民工作与生活在园区，80%的 GDP（Gross Domestic Product，国内生产总值）创造在园区，而每个人每天有 18 个小时都身处在园区中。园区网络作为园区通向数字世界的基础设施，是园区建设不可或缺的一部分，在日常办公、研发生产、运营管理中扮演着越来越重要的角色。

本实验将通过一个园区网络的综合实验，帮助学员理解园区网络中常见技术的应用。

17.1.2 实验目的

- 掌握园区二层网络的配置方法
- 掌握园区三层网络的配置方法
- 掌握园区无线网络的配置方法
- 掌握园区网络安全与服务的配置方法

17.1.3 实验组网介绍

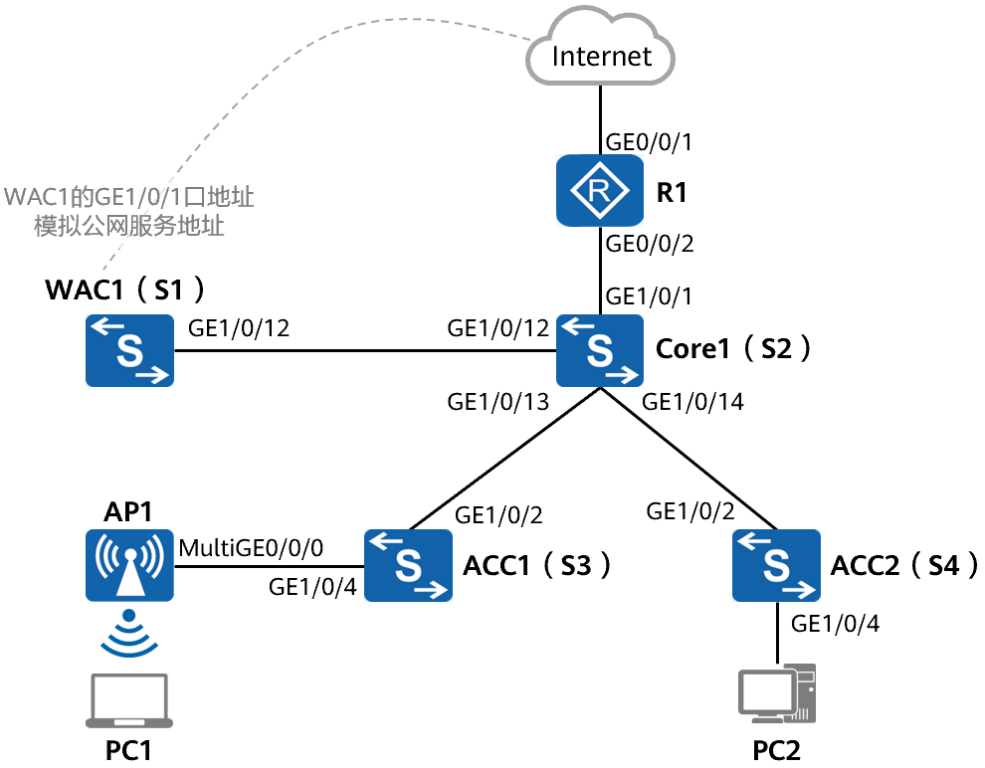


图17-1 园区网络综合实验拓扑

1. Core1（即 S2）作为根桥，Core1 以下设备为二层设备。
2. Core1、WAC1、R1 间通过 OSPF 实现互联互通；Core1 为三层业务网关，作为 DHCP 服务器为 PC1 和 PC2 分配 IP 地址。
3. WAC1（即 S1）支持 WLAN-AC 功能（若实际环境所用交换机不支持，可用普通 WAC 替代），作为 WAC 使用；WAC1 与 AP1 处于三层网络，Core1 作为 DHCP 服务器给 AP1 分配 IP 地址，业务数据采用直接转发模式。
4. 通过 NAT 策略限制只有内网有线用户可以访问公网服务。
5. 管理员通过 STelnet 能够远程登录所有设备进行运维调测。
6. Core1 作为核心交换机需要备份配置文件到 FTP 服务器（WAC1）。

17.1.4 实验背景

某小型企业准备搭建一张园区网络供企业内人员办公使用，网络设备需要集中管理和监控。该园区存在有线与无线终端约 50 人，终端设备接入网络后能动态获取业务 IP 地址，同时有线用户可以访问外部网络。

17.2 实验任务配置

17.2.1 配置思路

1. 配置交换机、WAC 和路由器的接口和 VLAN，配置三层接口地址、路由，使得网络互通
2. 配置核心交换机的 DHCP 功能，使交换机作为 DHCP 服务器为 AP 和无线/有线用户分配 IP 地址
3. 配置 WAC 的无线业务，实现 AP 和 STA 上线
4. 配置出口 NAT 功能，实现有线用户能够访问公网服务
5. 配置 SSH 和 FTP 功能，实现核心设备能够远程管理接入设备，同时核心设备的配置文件可以备份到 FTP 服务器上

17.2.2 配置步骤

步骤 1 设备基础配置

设备命名

略。

关闭交换机的 ZTP 功能

```
<Core1> set ztp disable
Info: The ZTP process will be terminated. When restarting without a configuration file, the device will not start the ZTP process.
<Core1> system-view
[Core1]
```

ACC1、ACC2、WAC1 与 Core1 的配置相同，不再赘述。

关闭不使用的端口

```
[WAC1] interface GE 1/0/10
[WAC1-GE1/0/10] shutdown
[WAC1-GE1/0/10] quit
[WAC1] interface GE 1/0/11
[WAC1-GE1/0/11] shutdown
[WAC1-GE1/0/11] quit
[WAC1] interface GE 1/0/13
[WAC1-GE1/0/13] shutdown
[WAC1-GE1/0/13] quit
[WAC1] interface GE 1/0/14
[WAC1-GE1/0/14] shutdown
[WAC1-GE1/0/14] quit
```

```
[Core1] interface GE 1/0/10
[Core1-GE1/0/10] shutdown
[Core1-GE1/0/10] quit
[Core1] interface GE 1/0/11
[Core1-GE1/0/11] shutdown
[Core1-GE1/0/11] quit
```

```
[ACC1] interface GE 1/0/1
[ACC1-GE1/0/1] shutdown
[ACC1-GE1/0/1] quit
[ACC1] interface GE 1/0/3
[ACC1-GE1/0/3] shutdown
[ACC1-GE1/0/3] quit
```

```
[ACC2] interface GE 1/0/1
[ACC2-GE1/0/1] shutdown
[ACC2-GE1/0/1] quit
[ACC2] interface GE 1/0/3
[ACC2-GE1/0/3] shutdown
[ACC2-GE1/0/3] quit
```

将 R1 和 WAC1 的二层接口切换为三层接口

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] quit
[R1] interface GE 0/0/2
[R1-GE0/0/2] undo portswitch
[R1-GE0/0/2] quit
```

```
[WAC1] interface GE 1/0/1
[WAC1-GE1/0/1] undo port link-type
[WAC1-GE1/0/1] undo portswitch
[WAC1-GE1/0/1] quit
```

说明：WAC1 的 GE1/0/1 口与 R1 的 GE0/0/1 口互联，用于模拟公网服务。

开启 R1 的 LLDP 功能

```
[R1] lldp enable
Info: Global LLDP is enabled successfully.
```

检查 Core1 的 LLDP 邻居关系

```
[Core1] display lldp neighbor brief
Local Interface     Exptime(s) Neighbor     Interface       Neighbor Device
------------------------------------------------------------------------------
GE1/0/1             116                     GE0/0/2         R1
GE1/0/12            109                     GE1/0/12        WAC1
GE1/0/13            100                     GE1/0/2         ACC1
GE1/0/14            109                     GE1/0/2         ACC2
```

步骤 2 配置基于接口划分 VLAN

请基于下表，配置 Core1、ACC1、ACC2 和 WAC1 的 VLAN。

表17-1 VLAN 规划

VLAN编号	VLAN描述
2	交换机管理VLAN
3	AP管理VLAN
10	Core1与R1互联VLAN
11	Core1与WAC1互联VLAN
100	无线终端业务VLAN
101	有线终端业务VLAN

在交换机 Core1 上创建 VLAN 2、3、10、11、100 和 101，并将对应接口划入相应的 VLAN

```
[Core1] vlan batch 2 to 3 10 to 11 100 to 101
[Core1] interface GE 1/0/1
[Core1-GE1/0/1] port link-type access
[Core1-GE1/0/1] port default vlan 10
[Core1-GE1/0/1] quit
[Core1] interface GE 1/0/12
[Core1-GE1/0/12] port link-type access
[Core1-GE1/0/12] port default vlan 11
[Core1-GE1/0/12] quit
[Core1] interface GE 1/0/13
[Core1-GE1/0/13] port link-type trunk
[Core1-GE1/0/13] port trunk allow-pass vlan 2 3 100
[Core1-GE1/0/13] undo port trunk allow-pass vlan 1
[Core1-GE1/0/13] quit
[Core1] interface GE 1/0/14
[Core1-GE1/0/14] port link-type trunk
[Core1-GE1/0/14] port trunk allow-pass vlan 2 101
```

```
[Core1-GE1/0/14] undo port trunk allow-pass vlan 1
[Core1-GE1/0/14] quit
```

在交换机 ACC1 上创建 VLAN 2、3 和 100，并将对应接口划入相应的 VLAN

```
[ACC1] vlan batch 2 to 3 100
[ACC1] interface GE 1/0/2
[ACC1-GE1/0/2] port link-type trunk
[ACC1-GE1/0/2] port trunk allow-pass vlan 2 3 100
[ACC1-GE1/0/2] undo port trunk allow-pass vlan 1
[ACC1-GE1/0/2] quit
[ACC1] interface GE 1/0/4
[ACC1-GE1/0/4] port link-type trunk
[ACC1-GE1/0/4] port trunk allow-pass vlan 3 100
[ACC1-GE1/0/4] port trunk pvid vlan 3
[ACC1-GE1/0/4] undo port trunk allow-pass vlan 1
[ACC1-GE1/0/4] quit
```

在交换机 ACC2 上创建 VLAN 2 和 101，并将对应接口划入相应的 VLAN

```
[ACC2] vlan batch 2 101
[ACC2] interface GE 1/0/2
[ACC2-GE1/0/2] port link-type trunk
[ACC2-GE1/0/2] port trunk allow-pass vlan 2 101
[ACC2-GE1/0/2] undo port trunk allow-pass vlan 1
[ACC2-GE1/0/2] quit
[ACC2] interface GE 1/0/4
[ACC2-GE1/0/4] port link-type access
[ACC2-GE1/0/4] port default vlan 101
[ACC2-GE1/0/4] quit
```

在 WAC1 上创建 VLAN 11 和 100，并将对应接口划入相应的 VLAN

```
[WAC1] vlan batch 11 100
[WAC1] interface GE 1/0/12
[WAC1-GE1/0/12] port link-type access
[WAC1-GE1/0/12] port default vlan 11
[WAC1-GE1/0/12] quit
```

说明：VLAN 100 为无线业务 VLAN，由于无线业务流量采用直接转发方式，且 WAC1 为旁挂部署，因此 WAC1 的接口无需放通 VLAN 100 的流量。

查看 VLAN 创建情况

说明：以下仅展现了本步骤创建的 VLAN。

```
[Core1] display vlan
The total number of vlans is : 7
```

```
--------------------------------------------------------------------------------
U: Up;              D: Down;            TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                       ST: Vlan-stacking;
#: ProtocolTransparent-vlan;            *: Management-vlan;
MAC-LRN: MAC-address learning;          STAT: Statistic;
BC: Broadcast;      MC: Multicast;      UC: Unknown-unicast;
FWD: Forward;       DSD: Discard;
--------------------------------------------------------------------------------
VID                 Ports
--------------------------------------------------------------------------------
    1               UT: .....
    2               TG:GE1/0/13(U)          GE1/0/14(U)
    3               TG:GE1/0/13(U)
   10               UT:GE1/0/1(U)
   11               UT:GE1/0/12(U)
  100               TG:GE1/0/13(U)
  101               TG:GE1/0/14(U)
.....
```

```
[ACC1] 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;
MAC-LRN: MAC-address learning;          STAT: Statistic;
BC: Broadcast;      MC: Multicast;      UC: Unknown-unicast;
FWD: Forward;       DSD: Discard;
--------------------------------------------------------------------------------
VID                 Ports
--------------------------------------------------------------------------------
    1               UT: .....
    2               TG:GE1/0/2(U)
    3               UT:GE1/0/4(U)
                    TG:GE1/0/2(U)
  100               TG:GE1/0/2(U)           GE1/0/4(U)
.....
```

```
[ACC2] display vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;              D: Down;            TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                       ST: Vlan-stacking;
#: ProtocolTransparent-vlan;            *: Management-vlan;
MAC-LRN: MAC-address learning;          STAT: Statistic;
BC: Broadcast;      MC: Multicast;      UC: Unknown-unicast;
```

```
FWD: Forward;     DSD: Discard;
------------------------------------------------------------------------------
VID                 Ports
------------------------------------------------------------------------------
    1               UT: ......
    2               TG:GE1/0/2(U)
  101               UT:GE1/0/4(U)
                    TG:GE1/0/2(U)
......
```

```
[WAC1] display vlan
The total number of vlans is : 3
------------------------------------------------------------------------------
U: Up;              D: Down;            TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;                       ST: Vlan-stacking;
#: ProtocolTransparent-vlan;            *: Management-vlan;
MAC-LRN: MAC-address learning;          STAT: Statistic;
BC: Broadcast;      MC: Multicast;      UC: Unknown-unicast;
FWD: Forward;       DSD: Discard;
------------------------------------------------------------------------------
VID                 Ports
------------------------------------------------------------------------------
    1               UT: ......
   11               UT:GE1/0/12(U)
  100
......
```

步骤 3 配置设备运行 STP

二层网络全局开启 STP 功能，并设置核心设备 Core1 为根桥，防止线缆误接或新设备加入导致网络重新收敛。

Core1、ACC1、ACC2 和 WAC1 全局使能 STP 功能

```
[Core1] stp enable
```

```
[ACC1] stp enable
```

```
[ACC2] stp enable
```

```
[WAC1] stp enable
```

修改当前生成树工作模式为 STP

```
[Core1] stp mode stp
```

```
[ACC1] stp mode stp
```

```
[ACC2] stp mode stp
```

```
[WAC1] stp mode stp
```

设置 Core1 为根桥

```
[Core1] stp root primary
```

查看 Core1 的生成树接口状态

```
[Core1] display stp brief
 MSTID     Port          Role  STP State     Protection  Cost      Edged
    0      GE1/0/1       DESI  forwarding    none        20000     disable
    0      GE1/0/12      DESI  forwarding    none        20000     disable
    0      GE1/0/13      DESI  forwarding    none        20000     disable
    0      GE1/0/14      DESI  forwarding    none        20000     disable
```

步骤 4 配置设备 IP 地址

请基于下表，配置 Core1、ACC1、ACC2、R1 和 WAC1 的 IP 地址。

表17-2 IP 地址规划

网络设备	接口	IP Address/Mask
Core1	VLANIF 2	192.168.2.254/24
	VLANIF 3	192.168.3.254/24
	VLANIF 10	192.168.10.1/30
	VLANIF 11	192.168.11.1/30
	VLANIF 100	192.168.100.254/24
	VLANIF 101	192.168.101.254/24
	LoopBack 0	10.0.1.1/32
ACC1	VLANIF 2	192.168.2.1/24
ACC2	VLANIF 2	192.168.2.2/24
R1	GE0/0/2	192.168.10.2/30

	LoopBack 0	10.0.2.2/32
WAC1	VLANIF 11	192.168.11.2/30
	LoopBack 0	10.0.3.3/32

配置 Core1、ACC1 和 ACC2 的管理接口 IP 地址

```
[Core1] interface Vlanif 2
[Core1-Vlanif2] ip address 192.168.2.254 24
[Core1-Vlanif2] quit
[Core1] interface Vlanif 3
[Core1-Vlanif3] ip address 192.168.3.254 24
[Core1-Vlanif3] quit
```

```
[ACC1] interface Vlanif 2
[ACC1-Vlanif2] ip address 192.168.2.1 24
[ACC1-Vlanif2] quit
```

```
[ACC2] interface Vlanif 2
[ACC2-Vlanif2] ip address 192.168.2.2 24
[ACC2-Vlanif2] quit
```

配置 Core1、R1 和 WAC1 的互联接口 IP 地址

```
[Core1] interface Vlanif 10
[Core1-Vlanif10] ip address 192.168.10.1 30
[Core1-Vlanif10] quit
[Core1] interface Vlanif 11
[Core1-Vlanif11] ip address 192.168.11.1 30
[Core1-Vlanif11] quit
```

```
[R1] interface GE0/0/2
[R1-GE0/0/2] ip address 192.168.10.2 30
[R1-GE0/0/2] quit
```

```
[WAC1] interface Vlanif 11
[WAC1-Vlanif11] ip address 192.168.11.2 30
[WAC1-Vlanif11] quit
```

配置 Core1 的业务接口 IP 地址

```
[Core1] interface Vlanif 100
[Core1-Vlanif100] ip address 192.168.100.254 24
```

```
[Core1-Vlanif100] quit
[Core1] interface Vlanif 101
[Core1-Vlanif101] ip address 192.168.101.254 24
[Core1-Vlanif101] quit
```

配置 Core1、R1 和 WAC1 的 LoopBack 接口 IP 地址

```
[Core1] interface LoopBack 0
[Core1-LoopBack0] ip address 10.0.1.1 32
[Core1-LoopBack0] quit
```

```
[R1] interface LoopBack 0
[R1-LoopBack0] ip address 10.0.2.2 32
[R1-LoopBack0] quit
```

```
[WAC1] interface LoopBack 0
[WAC1-LoopBack0] ip address 10.0.3.3 32
[WAC1-LoopBack0] quit
```

使用 Ping 工具测试设备间直连链路的连通性

```
[Core1] ping 192.168.10.2
  PING 192.168.10.2: 56  data bytes, press CTRL_C to break
    Reply from 192.168.10.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 192.168.10.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 192.168.10.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.10.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 192.168.10.2: bytes=56 Sequence=5 ttl=255 time=1 ms

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

```
[Core1] ping 192.168.11.2
  PING 192.168.11.2: 56  data bytes, press CTRL_C to break
    Reply from 192.168.11.2: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.11.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.11.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.11.2: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.11.2: bytes=56 Sequence=5 ttl=254 time=1 ms

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

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

```
[Core1] ping 192.168.2.1
  PING 192.168.2.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.2.1: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.2.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.2.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.2.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.2.1: bytes=56 Sequence=5 ttl=254 time=1 ms

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

```
[Core1] ping 192.168.2.2
  PING 192.168.2.2: 56  data bytes, press CTRL_C to break
    Reply from 192.168.2.2: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

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

步骤 5 配置 DHCP 功能

核心交换机 Core1 作为 DHCP 服务器，为本园区网络中的 AP 分配管理 IP 地址，同时为接入本网络的无线和有线终端分配业务 IP 地址。

开启 Core1 的 DHCP 功能

```
[Core1] dhcp enable
```

配置接口地址池为 AP1 分配 IP 地址，同时指定 WAC1 建立 CAPWAP 隧道的 IP 地址

```
[Core1] interface Vlanif 3
[Core1-Vlanif3] dhcp select interface
```

```
[Core1-Vlanif3] dhcp server gateway-list 192.168.3.254
[Core1-Vlanif3] dhcp server option 43 sub-option 2 ip-address 192.168.11.2
[Core1-Vlanif3] quit
```

配置接口地址池为无线和有线终端分配 IP 地址

```
[Core1] interface Vlanif 100
[Core1-Vlanif100] dhcp select interface
[Core1-Vlanif100] dhcp server gateway-list 192.168.100.254
[Core1-Vlanif100] quit
[Core1] interface Vlanif 101
[Core1-Vlanif101] dhcp select interface
[Core1-Vlanif101] dhcp server gateway-list 192.168.101.254
[Core1-Vlanif101] quit
```

查看 AP1 获取的 IP 地址

```
[ACC1] display lldp neighbor interface GE 1/0/4
GE1/0/4 has 1 neighbor(s):

Neighbor index                : 1
Chassis type                  : MAC Address
Chassis ID                    : c0a9-389c-1b40
Port ID subtype               : Interface Name
Port ID                       : MultiGE0/0/0
Port description              : --
System name                   : ap1
System description            : Huawei AP
Huawei YunShan OS
Version 1.24.0.1 (AirEngine 5700 V600R0XXCXXSPCXXX)
Copyright (C) 20XX-20XX Huawei Technologies Co., Ltd.
HUAWEI AirEngine5773-21
System capabilities supported : wlanAccessPoint
System capabilities enabled   : wlanAccessPoint
Management address type       : IPv4
Management address            : 192.168.3.57
Expired time                  : 119s

......
```

说明：以上内容仅展现了关键信息，可以看到 AP1 已成功获取管理网段 192.168.3.0/24 中的一个管理 IP 地址。

查看有线终端获取的 IP 地址

在 ACC2 上创建一个 VLANIF101 接口，用于模拟有线终端，并设置本接口通过 DHCP 方式动态获取 IP 地址。

```
[ACC2] interface Vlanif 101
[ACC2-Vlanif101] ip address dhcp-alloc
[ACC2-Vlanif101] quit
```

查看 ACC2 上 VLANIF101 已获取的 IP 地址。

```
[ACC2] display ip interface Vlanif 101
Vlanif101 current state :      UP
Line protocol current state : UP
The Maximum Transmit Unit :     1500 bytes
input packets :     0,     bytes :     0,     multicasts :     0
output packets :    0,     bytes :     0,     multicasts :     0
Directed-broadcast packets:
  received packets:       0,                sent packets:          0
  forwarded packets:      0,                dropped packets:       0
Internet Address is allocated by DHCP, 192.168.101.160/24
Broadcast address : 0.0.0.0
TTL being 1 packet number:              0
TTL invalid packet number:              0
ICMP packet input number:               0
    Echo reply:                         0
    Unreachable:                        0
    Source quench:                      0
    Routing redirect:                   0
    Echo request:                       0
    Router advert:                      0
    Router solicit:                     0
    Time exceed:                        0
    IP header bad:                      0
    Timestamp request:                  0
    Timestamp reply:                    0
    Information request:                0
    Information reply:                  0
    Netmask request:                    0
    Netmask reply:                      0
    Unknown type:                       0
```

可以看到，ACC2 的 VLANIF101 接口已成功获取有线业务网段 192.168.101.0/24 中的一个业务 IP 地址。

使用 Ping 工具测试与网关的连通性。

```
[ACC2] ping 192.168.101.254
  PING 192.168.101.254: 56  data bytes, press CTRL_C to break
    Reply from 192.168.101.254: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.101.254: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.101.254: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.101.254: bytes=56 Sequence=4 ttl=254 time=1 ms
```

```
  Reply from 192.168.101.254: bytes=56 Sequence=5 ttl=254 time=1 ms

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

查看接口地址池的地址分配情况

```
[Core1] display ip pool interface Vlanif3 used

  Pool-name             : Vlanif3
  Pool-No               : 0
  Lease                 : 1 Days 0 Hours 0 Minutes
  Domain-name           : -
  Option-code           : 43
    Option-subcode      : 2
      Option-type       : ip-address
      Option-value      : 192.168.11.2
  DNS-server0           : -
  NBNS-server0          : -
  Netbios-type          : -
  Position              : Interface
  Status                : Unlocked
  Gateway-0             : 192.168.3.254
  Network               : 192.168.3.0
  Mask                  : 255.255.255.0
  VPN instance          : --
  Logging               : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total          :253        Used         :1
                     Idle           :252        Expired      :0
                     Conflict       :0          Disabled     :0

-------------------------------------------------------------------------------
  Network section
   Start           End             Total     Used     Idle(Expired)   Conflict   Disabled
-------------------------------------------------------------------------------
   192.168.3.1     192.168.3.254   253       1        252(0)          0          0
-------------------------------------------------------------------------------
Client-ID format as follows:
    DHCP            : mac-address
    IPSec           : user-id/portnumber/vrf
    SSL-VPN         : user-id/session-id
-------------------------------------------------------------------------------
  Index           IP              Client-ID               Type      Left      Status
-------------------------------------------------------------------------------
```

```
  56              192.168.3.57    c0a9-389c-1b40      DHCP      86377      Used
------------------------------------------------------------------------------------------------
```

可以看到，Core1 的 VLANIF3 接口地址池，已成功分配 1 个 IP 地址；同时还指定了 WAC1 用于建立 CAPWAP 隧道的 IP 地址。

```
[Core1] display ip pool interface Vlanif101 used

  Pool-name             : Vlanif101
  Pool-No               : 2
  Lease                 : 1 Days 0 Hours 0 Minutes
  Domain-name           : -
  DNS-server0           : -
  NBNS-server0          : -
  Netbios-type          : -
  Position              : Interface
  Status                : Unlocked
  Gateway-0             : 192.168.101.254
  Network               : 192.168.101.0
  Mask                  : 255.255.255.0
  VPN instance          : --
  Logging               : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total          :253        Used         :1
                     Idle           :252        Expired      :1
                     Conflict       :0          Disabled     :0


------------------------------------------------------------------------------------------------
  Network section
  Start           End                 Total     Used     Idle(Expired)     Conflict    Disabled
------------------------------------------------------------------------------------------------
  192.168.101.1   192.168.101.254     253       1        252(0)            0           0
------------------------------------------------------------------------------------------------
Client-ID format as follows:
   DHCP           : mac-address
   IPSec          : user-id/portnumber/vrf
   SSL-VPN        : user-id/session-id
------------------------------------------------------------------------------------------------
  Index           IP                  Client-ID           Type      Left       Status
------------------------------------------------------------------------------------------------
  159             192.168.101.160     20df-73f5-4335      DHCP      85861      Used
------------------------------------------------------------------------------------------------
```

可以看到，Core1 的 VLANIF101 接口地址池，已成功分配 1 个 IP 地址。

步骤 6 配置 OSPF 功能

该企业网络通过 OSPF 实现三层互通，网络中 Core1、R1 和 WAC1 为三层设备，需要配置 OSPF 并将相关接口通告进 OSPF 区域 0，其中 LoopBack0 接口作为 Router ID。

配置 Core1 的 OSPF 功能，互联接口、无线管理接口、无线和有线业务接口、LoopBack0 口均使能 OSPF

```
[Core1] ospf 1 router-id 10.0.1.1
[Core1-ospf-1] area 0
[Core1-ospf-1-area-0.0.0.0] network 192.168.10.1 0.0.0.0
[Core1-ospf-1-area-0.0.0.0] network 192.168.11.1 0.0.0.0
[Core1-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[Core1-ospf-1-area-0.0.0.0] network 192.168.100.0 0.0.0.255
[Core1-ospf-1-area-0.0.0.0] network 192.168.101.0 0.0.0.255
[Core1-ospf-1-area-0.0.0.0] network 10.0.1.1 0.0.0.0
[Core1-ospf-1-area-0.0.0.0] quit
[Core1-ospf-1] quit
```

配置 R1 的 OSPF 功能，互联接口和 LoopBack0 口使能 OSPF

```
[R1] ospf 1 router-id 10.0.2.2
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 192.168.10.2 0.0.0.0
[R1-ospf-1-area-0.0.0.0] network 10.0.2.2 0.0.0.0
[R1-ospf-1-area-0.0.0.0] quit
[R1-ospf-1] quit
```

配置 WAC1 的 OSPF 功能，互联接口和 LoopBack0 口使能 OSPF

```
[WAC1] ospf 1 router-id 10.0.3.3
[WAC1-ospf-1] area 0
[WAC1-ospf-1-area-0.0.0.0] network 192.168.11.2 0.0.0.0
[WAC1-ospf-1-area-0.0.0.0] network 10.0.3.3 0.0.0.0
[WAC1-ospf-1-area-0.0.0.0] quit
[WAC1-ospf-1] quit
```

查看 OSPF 邻居状态

```
[Core1] display ospf peer brief

(M) Indicates MADJ neighbor

OSPF Process 1 with Router ID 10.0.1.1
                    Peer Statistic Information
Total number of peer(s): 2
 Peer(s) in full state: 2
--------------------------------------------------------------------------------
 Area Id      Interface        Neighbor id          State
```

```
0.0.0.0         Vlanif10        10.0.2.2        Full
0.0.0.0         Vlanif11        10.0.3.3        Full
------------------------------------------------------------------------------
```

可以看到，Core1、R1 和 WAC1 已成功建立 OSPF 邻居关系。

查看 IP 路由表信息

```
[R1] display ip routing-table
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
10.0.1.1/32         OSPF    10   1         D     192.168.10.1    GE0/0/2
10.0.2.2/32         Direct  0    0         D     127.0.0.1       LoopBack0
10.0.3.3/32         OSPF    10   2         D     192.168.10.1    GE0/0/2
127.0.0.0/8         Direct  0    0         D     127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0         D     127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0         D     127.0.0.1       InLoopBack0
192.168.3.0/24      OSPF    10   2         D     192.168.10.1    GE0/0/2
192.168.10.0/30     Direct  0    0         D     192.168.10.2    GE0/0/2
192.168.10.2/32     Direct  0    0         D     127.0.0.1       GE0/0/2
192.168.10.3/32     Direct  0    0         D     127.0.0.1       GE0/0/2
192.168.11.0/30     OSPF    10   2         D     192.168.10.1    GE0/0/2
192.168.100.0/24    OSPF    10   2         D     192.168.10.1    GE0/0/2
192.168.101.0/24    OSPF    10   2         D     192.168.10.1    GE0/0/2
255.255.255.255/32  Direct  0    0         D     127.0.0.1       InLoopBack0
```

可以看到，R1 已成功通过 OSPF 学习到各网段路由。

（可选）也可以通过相同的方式查看 WAC1 和 Core1 上的 IP 路由表信息。

在 ACC2 上，使用 Ping 工具测试与 R1 之间的连通性

```
[ACC2] ping -a 192.168.101.160 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
```

```
    round-trip min/avg/max = 1/1/1 ms
```

说明：ACC2 的 VLANIF101 接口 IP 地址是动态获取的，学员可根据自身环境替换为实际的接口 IP 地址。

在 WAC1 上，使用 Ping 工具测试与 AP1 之间的连通性

```
[WAC1] ping 192.168.3.57
  PING 192.168.3.57: 56  data bytes, press CTRL_C to break
    Reply from 192.168.3.57: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 192.168.3.57: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 192.168.3.57: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 192.168.3.57: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 192.168.3.57: bytes=56 Sequence=5 ttl=254 time=1 ms

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

说明：AP1 的管理 IP 地址是动态获取的，学员可根据自身环境替换为实际的管理 IP 地址。

步骤 7 配置 WLAN 业务

该企业网络需要为访客提供无线接入的能力，因此需要部署无线业务并成功释放一个 SSID。

表17-3 WLAN 数据规划

配置项	配置参数
AP管理VLAN	VLAN 3
STA业务VLAN	VLAN 100
DHCP服务器	Core1作为DHCP服务器为AP1分配管理IP地址
	Core1作为DHCP服务器为PC1分配业务IP地址
AP的IP地址池	192.168.3.1~192.168.3.253/24
STA的IP地址池	192.168.100.1~192.168.100.253/24
WAC的源接口IP地址	VLANIF11：192.168.11.2/30
AP组	名称：ap-group1

	引用模板：VAP模板HCIA-WLAN、域管理模板default
域管理模板	名称：default
	国家码：中国（CN）
SSID模板	名称：HCIA-WLAN
	SSID名称：HCIA-Guest
安全模板	名称：HCIA-WLAN
	安全策略：WPA-WPA2+PSK+AES
	密码：HCIA-Datacom
VAP模板	名称：HCIA-WLAN
	转发模式：直接转发
	业务VLAN：VLAN 100
	引用模板：SSID模板HCIA-WLAN、安全模板HCIA-WLAN

配置 AP 上线

```
[WAC1] wlan
[WAC1-wlan] regulatory-domain-profile name default
[WAC1-wlan-regulate-domain-default] country-code cn
[WAC1-wlan-regulate-domain-default] quit
[WAC1-wlan] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] regulatory-domain-profile default
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue? [Y/N]: y
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan] quit

[WAC1] capwap source interface vlanif 11
Set the DTLS PSK(contains 8-32 plain-text characters, or 128 or 148 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): Huawei@123
Confirm PSK: Huawei@123
Info: Deliver DTLS PSK to devices using CAPWAP connections. It may take a few minutes.
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters, underscores, and digits, and must start with a letter): admin
```

```
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 128-268 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): Huawei@123
Confirm password: Huawei@123
Set the PSK of the global offline management VAP(plain-text password of 8-63 characters or cipher-text password of 128-188 characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): Huawei@123
Confirm PSK: Huawei@123
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be interrupted.
Info: Ensure that the management VLAN for devices is within the VLAN range mapping the source interface. Otherwise, the devices cannot go online.

[WAC1] wlan
[WAC1-wlan] ap auth-mode mac-auth
[WAC1-wlan] ap-id 1 ap-mac c0a9-389c-1b40
[WAC1-wlan-ap-1] ap-name AP1
[WAC1-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N]: y
[WAC1-wlan-ap-1] quit
[WAC1-wlan] quit
```

说明：AP1 的 MAC 地址是在接入交换机 ACC1 上通过命令 **display lldp neighbor interface GE 1/0/4** 获取到的。

等待几分钟，查看当前的 AP 信息

```
[WAC1] display ap all
Total AP information:
nor            : normal              [1]
ExtraInfo      : Extra information
Total: 1
-------------------------------------------------------------------------------------------------------------
ID   MAC             Name Group      IP              Type                State  STA  Uptime ExtraInfo
-------------------------------------------------------------------------------------------------------------
1    c0a9-389c-1b40  AP1 ap-group1 192.168.3.57    AirEngine5773-21 nor    0        14S    -
-------------------------------------------------------------------------------------------------------------
```

可以看到，AP1 的状态为 **nor**，表示 AP1 已成功上线 WAC1。

配置 WLAN 业务参数

```
[WAC1] wlan
[WAC1-wlan] security-profile name HCIA-WLAN
[WAC1-wlan-sec-prof-HCIA-WLAN] security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
[WAC1-wlan-sec-prof-HCIA-WLAN] quit
[WAC1-wlan] ssid-profile name HCIA-WLAN
[WAC1-wlan-ssid-prof-HCIA-WLAN] ssid HCIA-Guest
```

```
[WAC1-wlan-ssid-prof-HCIA-WLAN] quit
[WAC1-wlan] vap-profile name HCIA-WLAN
[WAC1-wlan-vap-prof-HCIA-WLAN] forward-mode direct-forward
[WAC1-wlan-vap-prof-HCIA-WLAN] service-vlan vlan-id 100
[WAC1-wlan-vap-prof-HCIA-WLAN] security-profile HCIA-WLAN
[WAC1-wlan-vap-prof-HCIA-WLAN] ssid-profile HCIA-WLAN
[WAC1-wlan-vap-prof-HCIA-WLAN] quit
[WAC1-wlan] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] vap-profile HCIA-WLAN wlan 1 radio all
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan] quit
```

查看 VAP 的相关信息

```
[WAC1] display vap all
WID :   WLAN ID
Total:  2
--------------------------------------------------------------------------------------------------------------
AP ID AP name   RfID WID  BSSID          Status    Auth type       STA    SSID
--------------------------------------------------------------------------------------------------------------
1     AP1       0    1    C0A9-389C-1B40 ON        WPA/WPA2-PSK    0      HCIA-Guest
1     AP1       1    1    C0A9-389C-1B50 ON        WPA/WPA2-PSK    0      HCIA-Guest
--------------------------------------------------------------------------------------------------------------
```

可以看到，AP1 已成功释放一个名为 **HCIA-Guest** 的 SSID。

步骤 8 配置出口 NAT 功能

该企业获得了 1.2.3.4/24 这个公网 IP 地址，现通过配置源 NAT 中的 Easy IP 功能实现仅有线用户访问公网服务。

配置 R1 的公网 IP 地址

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] ip address 1.2.3.4 24
[R1-GE0/0/1] quit
```

配置 WAC1 的公网 IP 地址

```
[WAC1] interface GE 1/0/1
[WAC1-GE1/0/1] ip address 1.2.3.100 24
[WAC1-GE1/0/1] quit
```

说明：本实验采用 WAC1 的 GE1/0/1 口模拟公网服务 IP 地址，其中 WAC1 的 GE1/0/1 口与 R1 的 GE0/0/1 口直连。

配置 NAT 策略

```
[R1] nat-policy
[R1-policy-nat] rule name policy_nat1
[R1-policy-nat-rule-policy_nat1] source-address 192.168.101.0 24
[R1-policy-nat-rule-policy_nat1] action source-nat easy-ip
[R1-policy-nat-rule-policy_nat1] quit
[R1-policy-nat] quit
```

开启 NAT 功能

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] nat enable
[R1-GE0/0/1] quit
```

在 R1 的 OSPF 进程中下发缺省路由，使私网流量可以通过本设备转发至公网

```
[R1] ospf 1
[R1-ospf-1] default-route-advertise always
[R1-ospf-1] quit
```

在 ACC2 上，使用 Ping 工具测试与公网服务 IP 地址之间的连通性

```
[ACC2] ping -a 192.168.101.160 1.2.3.100
  PING 1.2.3.100: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.100: bytes=56 Sequence=1 ttl=252 time=1 ms
    Reply from 1.2.3.100: bytes=56 Sequence=2 ttl=252 time=1 ms
    Reply from 1.2.3.100: bytes=56 Sequence=3 ttl=252 time=1 ms
    Reply from 1.2.3.100: bytes=56 Sequence=4 ttl=252 time=1 ms
    Reply from 1.2.3.100: bytes=56 Sequence=5 ttl=252 time=1 ms

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

说明：ACC2 的 VLANIF101 接口 IP 地址是动态获取的，学员可根据自身环境替换为实际的接口 IP 地址。

在 R1 上查看 NAT 会话表

```
[R1] display session all verbose
  Session Table Information:
    Protocol                : 1 (ICMP)
    SrcAddr VPN             : 192.168.101.160
    DestAddr VPN            : 1.2.3.100
    Type Code IcmpId        : 8 0 4885
    Time To Live            : 8 s
```

```
  NAT Info
    New SrcAddr        : 1.2.3.4
    New DestAddr       : -
    New IcmpId         : 2050

 Total :     1
```

可以看到，ACC2 的 VLANIF101 接口的私网地址被转换为公网地址 1.2.3.4。

步骤 9 配置 SSH 功能

管理员需要能够通过任意设备远程登录到其他设备进行运维调测，此处仅以 Core1 能够远程登录其他接入交换机为例介绍 STelnet 功能的实现方式。

配置 SSH 服务器（ACC1 和 ACC2）的 VTY 用户界面

```
[ACC1] user-interface vty 0 4
[ACC1-ui-vty0-4] authentication-mode aaa
[ACC1-ui-vty0-4] protocol inbound ssh
[ACC1-ui-vty0-4] user privilege level 3
[ACC1-ui-vty0-4] quit
```

```
[ACC2] user-interface vty 0 4
[ACC2-ui-vty0-4] authentication-mode aaa
[ACC2-ui-vty0-4] protocol inbound ssh
[ACC2-ui-vty0-4] user privilege level 3
[ACC2-ui-vty0-4] quit
```

在 ACC1 新建用户账号（admin1/Huawei@123），并设置认证方式为 Password

```
[ACC1] aaa
[ACC1-aaa] local-user admin1 password
Please configure the login password (8-128)
It is recommended that the password consist of four types of characters, including lowercase letters, uppercase letters, numerals and special characters.
Please enter new password: Huawei@123
Please confirm new password: Huawei@123
Info: The initial password of admin1 must be changed during login.
[ACC1-aaa] local-user admin1 service-type ssh
Warning: If the service type of local users is configured multiple times, the new configuration overwrites the previous one. The new configuration may cause local user authentication to fail. Continue? [Y/N]: y
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory) of a local user, the rights of users already online do not change. The change takes effect to users who go online after the change.
[ACC1-aaa] local-user admin1 privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue? [Y/N]: y
```

```
[ACC1-aaa] quit
[ACC1] ssh user admin1
Info: Succeeded in adding a new SSH user.
[ACC1] ssh user admin1 authentication-type password
```

在 ACC2 新建用户账号（admin2/Huawei@123），并设置认证方式为 Password

```
[ACC2] aaa
[ACC2-aaa] local-user admin2 password
Please configure the login password (8-128)
It is recommended that the password consist of four types of characters, including lowercase letters, uppercase letters, numerals and special characters.
Please enter password: Huawei@123
Please confirm password: Huawei@123
Info: The initial password of admin2 must be changed during login.
[ACC2-aaa] local-user admin2 service-type ssh
Warning: If the service type of local users is configured multiple times, the new configuration overwrites the previous one. The new configuration may cause local user authentication to fail. Continue? [Y/N]: y
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory) of a local user, the rights of users already online do not change. The change takes effect to users who go online after the change.
[ACC2-aaa] local-user admin2 privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue? [Y/N]: y
[ACC2-aaa] quit
[ACC2] ssh user admin2
Info: Succeeded in adding a new SSH user.
[ACC2] ssh user admin2 authentication-type password
```

开启 STelnet 功能，配置用户的服务类型为 STelnet，并设置服务端口号为 1025

```
[ACC1] stelnet server enable
[ACC1] ssh server-source all-interface
Warning: SSH server source configuration will take effect in the next login. Continue? [Y/N]: y
Warning: It expands the range of accessed IP.
[ACC1] ssh user admin1 service-type stelnet
[ACC1] ssh server port 1025
Warning: The operation will disconnect all online users. Continue? [Y/N]: y
Info: Succeeded in changing SSH listening port.
```

```
[ACC2] stelnet server enable
[ACC2] ssh server-source all-interface
Warning: SSH server source configuration will take effect in the next login. Continue? [Y/N]: y
Warning: It expands the range of accessed IP.
[ACC2] ssh user admin2 service-type stelnet
[ACC2] ssh server port 1025
Warning: The operation will disconnect all online users. Continue? [Y/N]: y
```

```
Info: Succeeded in changing SSH listening port.
```

配置 SSH 客户端首次登录功能

```
[Core1] ssh client first-time enable
[Core1] quit
```

在 SSH 客户端 Core1 登录 SSH 服务器 ACC1

```
<Core1> stelnet 192.168.2.1 1025
Trying 192.168.2.1 ...
Press CTRL + K to abort
Connected to 192.168.2.1 ...
The server's key fingerprint is ssh-ecdsa 521 QPNMCBM8TFBCWtdi3Z2EliwL6fNLXnBvdjxmC24COsg.
The server is not authenticated. Continue to access it? [Y/N]: y
Save the server's public key? [Y/N]: y
The server's public key will be saved with the name 192.168.2.1. Please wait...

Please input the username: admin1
Enter password: Huawei@123
Warning: The initial password poses security risks.
The password needs to be changed, Continue? [Y/N]: y
Please enter old password: Huawei@123
Please enter new password: Huawei@1234
Please confirm new password: Huawei@1234
The password has been changed successfully.

Info: The max number of VTY users is 5, the number of current VTY users online is 1, and total number
of terminal users online is 2.
        The current login time is XXXX-XX-XX 09:31:04.
<ACC1> system-view
Enter system view, return user view with return command.
```

查看 ACC1 上的 SSH 用户信息

```
[ACC1] display users
NOTE:
User-Intf: The absolute number and the relative number of user interface
Authen: Whether the authentication passes
Author: Command line authorization flag
-------------------------------------------------------------------------------------------------
  User-Intf        Delay      Type    Network Address     Authen   Author   Username
-------------------------------------------------------------------------------------------------
* 0      CON 0    00:00:00    --      1                   pass     no       Unspecified
  34     VTY 0    00:00:28   SSH      192.168.2.254       pass     no       admin1
```

在 ACC1 上可以看到，Core1 使用用户名 **admin1** 登录本设备，且登录方式为 **SSH**。

在 SSH 客户端 Core1 登录 SSH 服务器 ACC2

```
[ACC1] quit
<ACC1> quit
Info: The max number of VTY users is 5, and the number of current VTY users on line is 0.
Info: The connection was closed by the remote host.
<Core1> stelnet 192.168.2.2 1025
Trying 192.168.2.2 ...
Press CTRL + K to abort
Connected to 192.168.2.2 ...
The server's key fingerprint is ssh-ecdsa 521 gD5y+2E2URLPIMG2JdQ/wfE4bQyyNH1+NwRGxEyzokY.
The server is not authenticated. Continue to access it? [Y/N]: y
Save the server's public key? [Y/N]: y
The server's public key will be saved with the name 192.168.2.2. Please wait...

Please input the username: admin2
Enter password: Huawei@123
Warning: The initial password poses security risks.
The password needs to be changed, Continue? [Y/N]: y
Please enter old password: Huawei@123
Please enter new password: Huawei@1234
Please confirm new password: Huawei@1234
The password has been changed successfully.

Info: The max number of VTY users is 5, the number of current VTY users online is 1, and total number of terminal users online is 2.
        The current login time is XXXX-XX-XX 09:40:41.
<ACC2> system-view
Enter system view, return user view with return command.
```

查看 ACC2 上的 SSH 用户信息

```
[ACC2] display users
NOTE:
User-Intf: The absolute number and the relative number of user interface
Authen: Whether the authentication passes
Author: Command line authorization flag
-------------------------------------------------------------------------------------------------
  User-Intf        Delay      Type     Network Address     Authen   Author   Username
-------------------------------------------------------------------------------------------------
* 0      CON 0    00:00:00    --      1                   pass     no       Unspecified
  34     VTY 0    00:00:27   SSH      192.168.2.254       pass     no       admin2
```

在 ACC2 上可以看到，Core1 使用用户名 **admin2** 登录本设备，且登录方式为 **SSH**。

SSH 客户端 Core1 退出登录

```
[ACC2] return
<ACC2> quit
```

```
Info: The max number of VTY users is 5, and the number of current VTY users on line is 0.
Info: The connection was closed by the remote host.
<Core1>
```

步骤 10 配置 FTP 功能

交换机 Core1 是整个园区网络的核心设备，其配置文件需要进行备份保存。可以将 WAC1 作为 FTP 服务器存储 Core1 的配置文件，且只有 Core1 可以访问 FTP 服务器。

保存 Core1 的配置文件

```
<Core1> save test1.cfg
Warning: Are you sure to save the configuration to flash:/test1.cfg? [Y/N]: y
Now saving the current configuration to the slot 1
Info: Save the configuration successfully.
```

查看当前的文件列表

```
<Core1> dir
Directory of flash:/

Idx      Attr      Size(Byte)      Date         Time         FileName
......
17       -rw-      8,387           Nov 25 XXXX  09:45:08     test1.cfg
......

1,070,832 KB total (326,768 KB free)
```

说明：仅保留了关键信息。

在 WAC1 上配置 FTP 服务器功能及用户信息（admin3/Huawei@123）

```
[WAC1] quit
<WAC1> install feature-software WEAKEA
<WAC1> system-view
[WAC1] ftp server enable
[WAC1] ftp server source all-interface
Warning: FTP server source configuration will take effect in the next login. Continue? [Y/N]: y
Warning: It expands the range of accessed IP.
[WAC1] aaa
[WAC1-aaa] local-user admin3 password
Please configure the login password (8-128)
It is recommended that the password consist of four types of characters, including lowercase letters, uppercase letters, numerals and special characters.
Please enter password: Huawei@123
Please confirm password: Huawei@123
Info: The initial password of admin3 must be changed during login.
```

```
[WAC1-aaa] local-user admin3 privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue? [Y/N]: y
[WAC1-aaa] local-user admin3 service-type ftp
Warning: If the service type of local users is configured multiple times, the new configuration overwrites the previous one. The new configuration may cause local user authentication to fail. Continue? [Y/N]: y
Warning: The user access modes include Telnet, FTP, or HTTP, so security risks exist.
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory) of a local user, the rights of users already online do not change. The change takes effect to users who go online after the change.
[WAC1-aaa] local-user admin3 ftp-directory flash:/
[WAC1-aaa] quit
```

在 WAC1 上配置 FTP 服务器的访问权限

```
[WAC1] acl number 2001
[WAC1-acl4-basic-2001] rule 5 permit source 192.168.11.1 0
[WAC1-acl4-basic-2001] rule 10 deny
[WAC1-acl4-basic-2001] quit
[WAC1] ftp server acl 2001
[WAC1] quit
```

在 FTP 客户端（Core1）通过 FTP 与 WAC1 建立连接

```
<Core1> ftp 192.168.11.2
Warning: FTP is not secure. Using SFTP is recommended.
Trying 192.168.11.2 ...
Press CTRL + K to abort
Connected to 192.168.11.2.
220 FTP service ready.
User(192.168.11.2:(none)): admin3
331 Password required for admin3.
Enter password: Huawei@123
230 User logged in.
[ftp] ascii
200 Type set to A.
```

上传配置文件到 FTP 服务器

```
[ftp] put test1.cfg
Warning: The file may not transfer correctly in ASCII mode.
200 Port command okay.
150 Opening ASCII mode data connection for /test1.cfg.
/        100% [**********]
226 Transfer complete.

FTP: 8387 byte(s) send in 0.010 second(s) 819.000Kbyte(s)/sec.
[ftp] quit
```

```
221 Server closing.
<Core1>
```

在 WAC1 中查看备份文件是否已上传

```
<WAC1> dir
Directory of flash:/

Idx    Attr     Size(Byte)     Date          Time          FileName
......
17     -rw-     8,387          Nov 25 XXXX   09:57:27      test1.cfg
......

1,070,832 KB total (359,260 KB free)
```

说明：仅保留了关键信息。

17.3 结果验证

请读者使用无线终端 PC1 完成以下验证：

1. 使用 PC1 接入 SSID 为 HCIA-Guest 的无线信号，在终端的“命令提示符”界面查看 PC1 获取的 IP 地址，同时在 PC1 上执行命令 **ping 192.168.100.254**。
2. PC1 连接 SSID 后，在 WAC1 上使用命令 **display station all** 查看 PC1 信息。
3. PC1 获取地址后，在 Core1 上使用命令 **display ip pool interface Vlanif100 used** 查看接口地址池的地址分配情况。

请读者使用有线终端 PC2 完成以下验证：

1. 设置 PC2 的有线网卡地址获取方式为“自动获得 IP 地址”，在终端的“命令提示符”界面查看 PC2 获取的 IP 地址，同时在 PC2 上执行命令 **ping 192.168.101.254**。
2. PC2 获取地址后，在 Core1 上使用命令 **display ip pool interface Vlanif101 used** 查看接口地址池的地址分配情况。

请读者在 PC1 和 PC2 获取 IP 地址后，完成以下验证：

1. 使用 PC1 Ping 测 PC2 动态获得的 IP 地址，可以 Ping 测成功。
2. 使用 PC1 和 PC2 Ping 测公网服务地址 1.2.3.100，PC1 Ping 测失败，PC2 Ping 测成功。
3. 使用 PC1 和 PC2 Ping 测公网服务地址后，在 R1 上使用命令 **display session all verbose** 查看 NAT 会话表，只能看到 PC2 的私网地址被转换为公网地址 1.2.3.4。

17.4 配置参考

17.4.1 R1 的配置

```
#
sysname R1
#
interface GE0/0/1
 ip address 1.2.3.4 255.255.255.0
 nat enable
#
interface GE0/0/2
 ip address 192.168.10.2 255.255.255.252
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.255
#
ospf 1 router-id 10.0.2.2
 default-route-advertise always
 area 0.0.0.0
  network 10.0.2.2 0.0.0.0
  network 192.168.10.2 0.0.0.0
#
lldp enable
#
nat-policy
 rule name policy_nat1
  source-address 192.168.101.0 mask 255.255.255.0
  action source-nat easy-ip
#
return
```

17.4.2 WAC1 的配置

```
#
sysname WAC1
#
ftp server enable
ftp server acl 2001
ftp server source all-interface
#
wlan
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
 ssid-profile name HCIA-WLAN
  ssid HCIA-Guest
```

```
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 100
  ssid-profile HCIA-WLAN
  security-profile HCIA-WLAN
 regulatory-domain-profile name default
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
  radio 1
   vap-profile HCIA-WLAN wlan 1
  radio 2
   vap-profile HCIA-WLAN wlan 1
 ap-id 1 type-id 220 ap-mac c0a9-389c-1b40 ap-sn 21500867674ER9004989
  ap-name AP1
  ap-group ap-group1
#
capwap source interface vlanif 11
#
vlan batch 11 100
#
stp mode stp
#
acl number 2001
 rule 5 permit source 192.168.11.1 0
 rule 10 deny
#
aaa
 local-user admin3 password irreversible-cipher Huawei@123
 local-user admin3 privilege level 3
 local-user admin3 ftp-directory flash:/ read execute write
 local-user admin3 service-type ftp
#
interface Vlanif11
 ip address 192.168.11.2 255.255.255.252
#
interface GE1/0/1
 undo portswitch
 ip address 1.2.3.100 255.255.255.0
#
interface GE1/0/10
 shutdown
#
interface GE1/0/11
 shutdown
#
interface GE1/0/12
 port link-type access
 port default vlan 11
```

```
#
interface GE1/0/13
 shutdown
#
interface GE1/0/14
 shutdown
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.255
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.3 0.0.0.0
  network 192.168.11.2 0.0.0.0
#
return
```

17.4.3 Core1 的配置

```
#
sysname Core1
#
dhcp enable
#
vlan batch 2 to 3 10 to 11 100 to 101
#
stp mode stp
stp instance 0 root primary
#
rsa peer-public-key 192.168.2.1
 public-key-code begin
 3082018A
  02820181
      009F8219 2C77AFAD 0A1CF0D1 BCF3445D 9EA41E4D EB1C997C 92547E7B 7967ADF0
      E23B26F7 259B4A2D 14A90F5C EE024116 F4F7E9E6 9CF6671E 14D813AF 8B4BEEE2
      D0170D9B E65A7830 0C3EBB51 F3A6BEF1 3DFDB1D2 F78E175E 16D25AD4 84A0FF20
      AB4F6886 F7FD65FF 93CF8347 13A4371D 552EC54D 22537F5C 929D8089 6633319B
      EE805EFC 7719A6F6 E1E5BD72 9BBCA0B4 1193D69D 290A7372 7CB7AB0B 38881C76
      DFE29235 4299727E 3954B3D5 8EB787F8 8CD3918B F7FB7A6F 3227A8EA F28584B1
      AFE82946 5B8A35E8 42308D3C 0898C461 F7720C1D F4904864 36B0A856 BA84058B
      D1BFB5EF 1929E11A 32CE73B7 157D64E0 CCDEB5C5 03300366 F2908184 872BE5F4
      ABDEDE5A 4E9A2388 ED4CC6AE 96781D49 BC27FE70 C6B701C9 2A7587CA AB701A9D
      E1AEB2FE 4D5A7775 9C874A73 1C7D295A E46A97E9 6ADE3040 A46FBF38 34D1E1A6
      05E18DD1 16F1F433 B436C41F 079ABEEF FCE761AF 1B66D2B1 8B988368 CC5D9C8E
      302B1561 68CE31DE 8F72A27C 98AF29FE 8A891E15 F2A21441 E395D632 641F9285
      05
```

```
  0203
    010001
 public-key-code end
 peer-public-key end
#
rsa peer-public-key 192.168.2.2
 public-key-code begin
 3082018A
  02820181
    00B71DD2 F78734ED 9F285538 48C6C223 12696CCA EBBCC7D7 0B8FF204 8E214326
    D966318D C53C3EC1 9A90A21F 79D73CE9 07A65691 813F4600 7E7623F1 571EF8E6
    8EAE92DD 580A2302 740D91E6 5A99F090 DC5DE1D1 34010BFF 6AEAEACD C7B65DD5
    F6921B6C 4C2D353C 8D79E7AD ECA371D0 24351683 CFDA7C50 4705EC67 08219AA6
    2CF97E5D 177AA6E7 431ED5F3 8E998437 7E45F863 9E8D5DE3 6C218F04 333B2C7F
    ED09FB53 2B65FB82 BA50FD5B 8B3E04FE 345402BC 0AD2185E C6D2C75F 3FD0D166
    AE577E43 8F8D9715 06C4A839 B873D98B 4A51D395 AD7B4150 6031D4E1 E70C74C5
    1CDBEC65 58673894 712EEC8B 2168F3A7 9780CB42 4153F1DC AAFAF4AC DC998B9F
    0A9207DC BBEC767C 5CA66707 57CEA5D6 93B620A8 5CB8FBE6 200B929E 4695142E
    A0A62205 FBBAC1E3 E57A5C5F 938B33C8 408BA4B3 A58A6BCA 16024F87 0B27C97F
    0D488DF1 B877AC98 F6DDC9CB 07361EEF 97608F03 387937ED 1A2252B1 753D85E8
    BB5E7A86 1EAB74F5 47BB96C9 ECCF3072 2D8BC8C3 7C051AF3 ABBCCF0C ACFFCA9C
    55
  0203
    010001
 public-key-code end
 peer-public-key end
#
interface Vlanif2
 ip address 192.168.2.254 255.255.255.0
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.3.254
 dhcp server option 43 sub-option 2 ip-address 192.168.11.2
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.252
#
interface Vlanif11
 ip address 192.168.11.1 255.255.255.252
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.100.254
#
interface Vlanif101
```

```
 ip address 192.168.101.254 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 192.168.101.254
#
interface GE1/0/1
 port link-type access
 port default vlan 10
#
interface GE1/0/10
 shutdown
#
interface GE1/0/11
 shutdown
#
interface GE1/0/12
 port link-type access
 port default vlan 11
#
interface GE1/0/13
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 100
#
interface GE1/0/14
 port link-type trunk
 port trunk allow-pass vlan 2 101
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.10.1 0.0.0.0
  network 192.168.11.1 0.0.0.0
  network 192.168.100.0 0.0.0.255
  network 192.168.101.0 0.0.0.255
#
ssh client first-time enable
ssh client peer 192.168.2.1 assign rsa-key 192.168.2.1
ssh client peer 192.168.2.2 assign rsa-key 192.168.2.2
#
return
```

17.4.4 ACC1 的配置

```
#
sysname ACC1
#
vlan batch 2 to 3 100
#
stp mode stp
#
aaa
 local-user admin1 password irreversible-cipher Huawei@123
 local-user admin1 privilege level 3
 local-user admin1 service-type ssh
#
interface Vlanif2
 ip address 192.168.2.1 255.255.255.0
#
interface GE1/0/1
 shutdown
#
interface GE1/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 100
#
interface GE1/0/3
 shutdown
#
interface GE1/0/4
 port link-type trunk
 port trunk pvid vlan 3
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 3 100
#
stelnet server enable
ssh ipv4 server port 1025
ssh user admin1
ssh user admin1 authentication-type password
ssh user admin1 service-type stelnet
ssh server-source all-interface
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound ssh
#
return
```

17.4.5 ACC2 的配置

```
#
sysname ACC2
#
vlan batch 2 101
#
stp mode stp
#
aaa
 local-user admin2 password irreversible-cipher Huawei@123
 local-user admin2 privilege level 3
 local-user admin2 service-type ssh
#
interface Vlanif2
 ip address 192.168.2.2 255.255.255.0
#
interface Vlanif101
 ip address dhcp-alloc
#
interface GE1/0/1
 shutdown
#
interface GE1/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 101
#
interface GE1/0/3
 shutdown
#
interface GE1/0/4
 port link-type access
 port default vlan 101
#
stelnet server enable
ssh ipv4 server port 1025
ssh user admin2
ssh user admin2 authentication-type password
ssh user admin2 service-type stelnet
ssh server-source all-interface
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound ssh
```

```
#
return
```

17.5 思考题

1. 在步骤 7，若 WLAN 的数据转发模式为隧道转发，则哪些设备的接口需要放通无线业务 VLAN 100，使得 STA（无线终端 PC1）可以获取 192.168.100.0/24 网段的业务 IP 地址?

答案：若采用隧道转发，则无线业务流量接入 AP1 后会通过 CAPWAP 隧道传送至 WAC1，因此 WAC1 的 GE1/0/12 接口和 Core1 的 GE1/0/12 接口需要放通 VLAN 100。