华为认证系列教程

HCIA-Datacom

数据通信工程师

实验指导手册

版本:1.0

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他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他原因，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： http://e.huawei.com

华为认证体系介绍

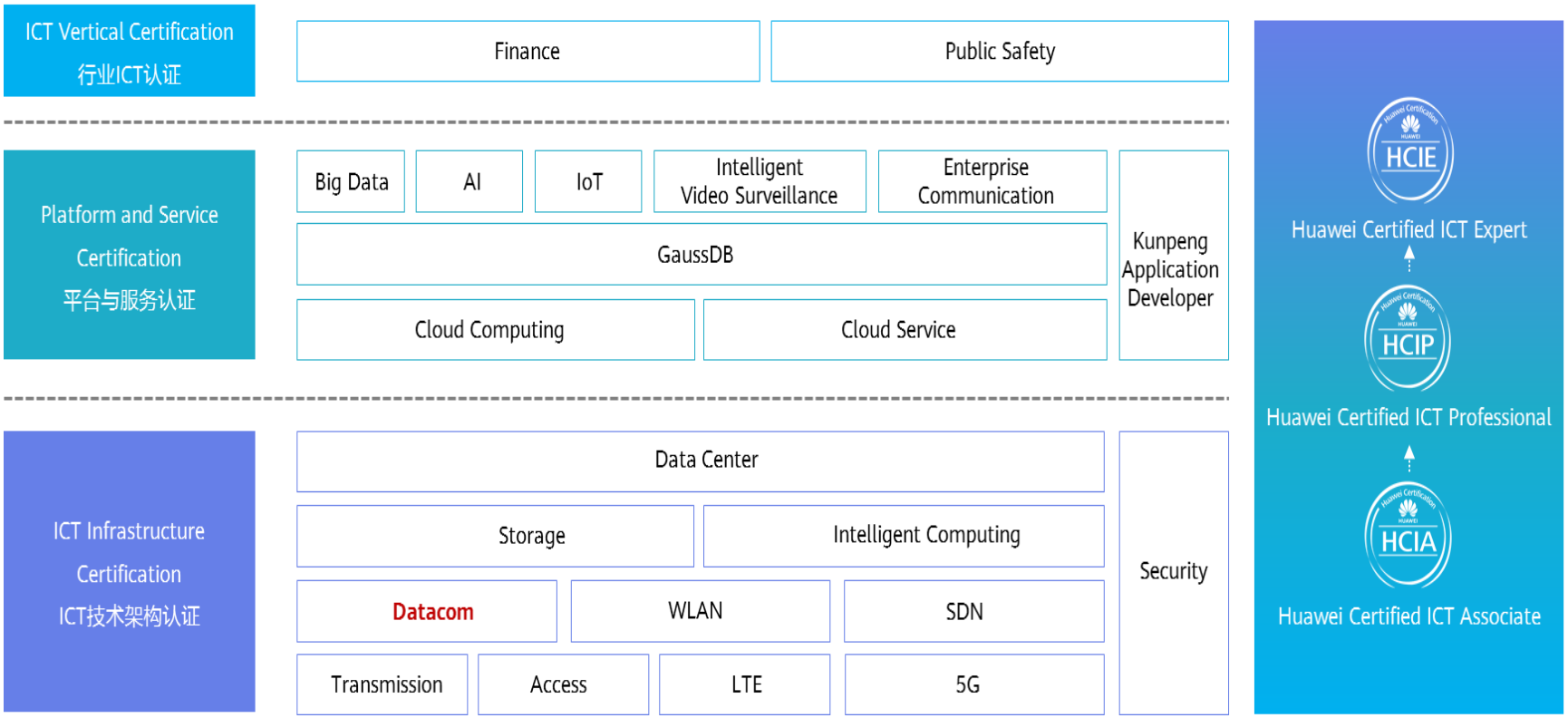
华为认证是华为公司基于“平台+生态”战略，围绕“云-管-端”协同的新ICT技术架构，打造的ICT技术架构认证、平台与服务认证、行业ICT认证三类认证，是业界唯一覆盖ICT（Information and Communications Technology 信息通信技术）全技术领域的认证体系。

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认证在内容上涵盖路由交换原理、WLAN基本原理、网络安全基础知识、网络管理与运维基础知识以及SDN与编程自动化基础知识等内容。

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！

Huawei Certification



前 言

简介

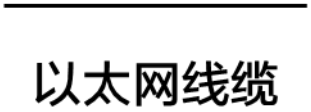
本书为 HCIA-Datacom 认证培训教程，适用于准备参加 HCIA-Datacom 考试的学员，或者希望了解路由交换原理、WLAN 基本原理、网络安全基础知识、网络管理与运维基础知识、以及 SDN 与编程自动化基础知识等相关技术的读者。

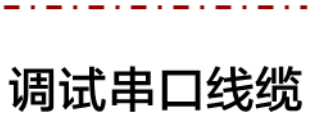
读者知识背景

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
- 对网络数据通信有基本的概念

本书常用图标





推荐实验环境

组网说明

本实验环境面向准备 HCIA-Datacom 考试的数通网络工程师。每套实验环境包括交换机 2 台（不支持 PoE），PoE 交换机 2 台，无线接入点（AP）2 台，路由器 2 台。

设备介绍

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 S5731-H24T4XC	V200R019C00 或以上版本
PoE交换机	CloudEngine S5731-H24P4XC	V200R019C00 或以上版本
无线接入点	AirEngine 5760-10	V200R009 或以上版本
路由器	NetEngine AR651C	V300R019 及以上版本

注：本书所有设备的端口信息、显示信息以及配置信息等全部按照推荐拓扑中的设备给出，不同的实验环境可能有所区别，学员需要自行去区别。

目录

1 华为 VRP 系统基本操作

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 VRP 系统的基本操作。

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

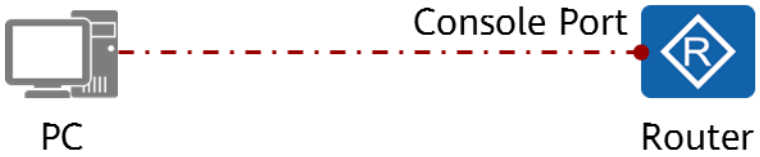


图1-1 熟悉 VRP 操作系统实验拓扑

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

略。

步骤 2 查看设备基本信息

查看设备版本信息

```
<Huawei>display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (AR651C V300R019C00SPC100)
Copyright (C) 2011-2016 HUAWEI TECH CO., LTD
Huawei AR651C Router uptime is 0 week, 0 day, 0 hour, 53 minutes
BKP 0 version information:
1. PCB          Version    : AR01BAK2C VER.B
2. If Supporting PoE : No
3. Board        Type       : AR651C
4. MPU Slot Quantity : 1
5. LPU Slot Quantity : 1
```

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 Ctrl+Z.
[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 GigabitEthernet                //“GigabitEthernet”是唯一可选的关键字
[Datacom-Router]interface GigabitEthernet 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示出该关键字，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-GigabitEthernet0/0/1]
```

此时已经进入到了接口 GigabitEthernet0/0/1 的视图

```
[Datacom-Router-GigabitEthernet0/0/1]i?
  icmp      <Group> icmp command group
  igmp      Specify parameters for IGMP
  ip        <Group> ip command group
  ipsec     Specify IPSec(IP Security) configuration information
  ipv6      <Group> ipv6 command group
  isis      Configure interface parameters for 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GigabitEthernet0/0/1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，“<Group> icmp command group”，“Specify parameters for IGMP”等为对关键字的描述。

```
[Datacom-Router-GigabitEthernet0/0/1]ip ?
  accounting              <Group> accounting command group
  address                 <Group> address command group
  binding                 Enable binding of an interface with a VPN instance
  fast-forwarding         Enable fast forwarding
  forward-broadcast       Specify IP directed broadcast information
  netstream               IP netstream feature
  verify                  IP verify
```

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-GigabitEthernet0/0/1]ip address ?
  IP_ADDR<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-GigabitEthernet0/0/1]ip address 192.168.1.1 ?
  INTEGER<0-32>           Length of IP address mask
  IP_ADDR<X.X.X.X>        IP address mask
[Datacom-Router-GigabitEthernet0/0/1]ip address 192.168.1.1 24 ?
  sub           Indicate a subordinate address
  <cr>          Please press ENTER to execute command
```

“<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-GigabitEthernet0/0/1]dis this
```

```
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#
```

display this命令用来查看当前视图的运行配置。对于某些正在生效的配置参数，如果与缺省工作参数相同，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。此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，可以不必输入完整的关键字。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**”，所有命令可以正常执行。类似的还有“**dis cu**”、“**d cu**”等同于“display current-configuration”。

```
[Datacom-Router-GigabitEthernet0/0/1]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 interface GigabitEthernet 0/0/2 接口

```
[Datacom-Router]interface GigabitEthernet 0/0/1
[Datacom-Router-GigabitEthernet0/0/1]undo ip address
```

需要先删除GigabitEthernet0/0/1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 GigabitEthernet 0/0/2
[Datacom-Router-GigabitEthernet0/0/2]ip address 192.168.1.1 24
[Datacom-Router-GigabitEthernet0/0/2]quit
```

查看设备当前配置

```
[Datacom-Router]display current-configuration
[V200R003C00]
#
 sysname Datacom-Router
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
```

```
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
  ---- 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
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y                    //需要输入 y 来确认继续
  It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

当前配置已经成功保存！

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的，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

比较当前配置与下一次启动所使用的配置

```
<Datacom-Router>compare configuration
 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(LMT)    FileName
    0  -rw-    126,538,240      Jul 04 2016 17:57:22     ar651c- v300r019c00Sspc100.cc
    1  -rw-         22,622      Feb 20 2020 10:35:18     mon_file.txt
    2  -rw-            737      Feb 20 2020 10:38:36     vrpcfg.zip
    3  drw-              -      Jul 04 2016 18:51:04     CPM_ENCRYPTED_FOLDER
    4  -rw-            783      Jul 10 2018 14:46:16     default_local.cer
    5  -rw-              0      Sep 11 2017 00:00:54     brdxpon_snmp_cfg.efs
    6  drw-              -      Sep 11 2017 00:01:22     update
    7  drw-              -      Sep 11 2017 00:01:48     shelldir
    8  drw-              -      Sep 21 2019 17:14:24     localuser
    9  drw-              -      Sep 15 2017 04:35:52     dhcp
   10  -rw-            509      Feb 20 2020 10:38:40     private-data.txt
   11  -rw-          2,686      Dec 19 2019 15:05:18     mon_lpu_file.txt
   12  -rw-          3,072      Dec 18 2019 18:15:54     Boot_LogFile

510,484 KB total available (386,456 KB free)
```

vrpcfg.zip：配置文件。配置文件必须以“.cfg”或“.zip”作为扩展名。
ar651c- v300r019c00Sspc100.cc：系统软件。系统软件必须以“.cc”作为扩展名。

将当前的配置保存同时命名为 test.cfg

```
<Datacom-Router>save test.cfg
 Are you sure to save the configuration to test.cfg? (y/n)[n]:y                //需要输入 y 来确认
  It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

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(LMT)    FileName
    0  -rw-    126,538,240      Jul 04 2016 17:57:22     ar651c- v300r019c00Sspc100.cc
    1  -rw-         22,622      Feb 20 2020 10:35:18     mon_file.txt
    2  -rw-            737      Feb 20 2020 10:38:36     vrpcfg.zip
    3  drw-              -      Jul 04 2016 18:51:04     CPM_ENCRYPTED_FOLDER
    4  -rw-            783      Jul 10 2018 14:46:16     default_local.cer
    5  -rw-              0      Sep 11 2017 00:00:54     brdxpon_snmp_cfg.efs
    6  drw-              -      Sep 11 2017 00:01:22     update
    7  drw-              -      Sep 11 2017 00:01:48     shelldir
    8  drw-              -      Sep 21 2019 17:14:24     localuser
    9  drw-              -      Sep 15 2017 04:35:52     dhcp
   10  -rw-          1,404      Feb 20 2020 11:55:17     test.cfg
   11  -rw-            509      Feb 20 2020 11:55:18     private-data.txt
   12  -rw-          2,686      Dec 19 2019 15:05:18     mon_lpu_file.txt
   13  -rw-          3,072      Dec 18 2019 18:15:54     Boot_LogFile

510,484 KB total available (386,452 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
This operation will take several minutes, please wait.....
Info: Succeeded in setting the file for booting system
```

查看下一次启动所用的文件

```
<Datacom-Router>display startup
MainBoard:
  Startup system software:                flash:/ ar651c- v300r019c00Sspc100.cc
  Next startup system software:           flash:/ ar651c- v300r019c00Sspc100.cc
  Backup system software for next startup: null
  Startup saved-configuration file:       flash:/vrpcfg.zip
  Next startup saved-configuration file:  flash:/test.cfg
  Startup license file:                   null
  Next startup license file:              null
  Startup patch package:                  null
  Next startup patch package:             null
  Startup voice-files:                    null
  Next startup voice-files:               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。

清空配置文件

```
<Datacom-Router>reset saved-configuration
This will delete the configuration in the flash memory.
The device configuratio
ns will be erased to reconfigure.
Are you sure? (y/n)[n]:y                    //需要输入 y 来确认
  Clear the configuration in the device successfully.
```

步骤 6 重启设备

```
<Datacom-Router>reboot
Info: The system is comparing the configuration, please wait.
System will reboot! Continue ? [y/n]:y                    //需要输入 y 来确认继续
Info: system is rebooting ,please wait...
```

系统开始重启

```
<Datacom-Router>
```

设备重启完成

1.3 结果验证

略。

1.4 配置参考

略。

1.5 思考题与附加内容

1.根据章节 2.6 附录的功能键列表，自行熟悉并掌握华为 VRP 系统功能键。

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?

1.6 附录

功能键	作用
<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>	将光标移动到最后一行的末尾
<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+K>	在连接建立阶段终止呼出的连接
<Ctrl+N>或↓光标	显示历史命令缓冲区中的后一条命令
<Ctrl+P>或↑光标	显示历史命令缓冲区中的前一条命令
<Ctrl+T>	输入问号“?”
<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）

表1-1 系统功能键

2 构建互联互通的 IP 网络

2.1 实验一：IPv4 编址及 IPv4 路由基础实验

2.1.1 实验介绍

2.1.1.1 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 参考模型的网际互联层，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。

2.1.1.2 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 工具测试网络层联通性
- 掌握并理解特殊静态路由的配置方法与应用场景

2.1.1.3 实验组网介绍

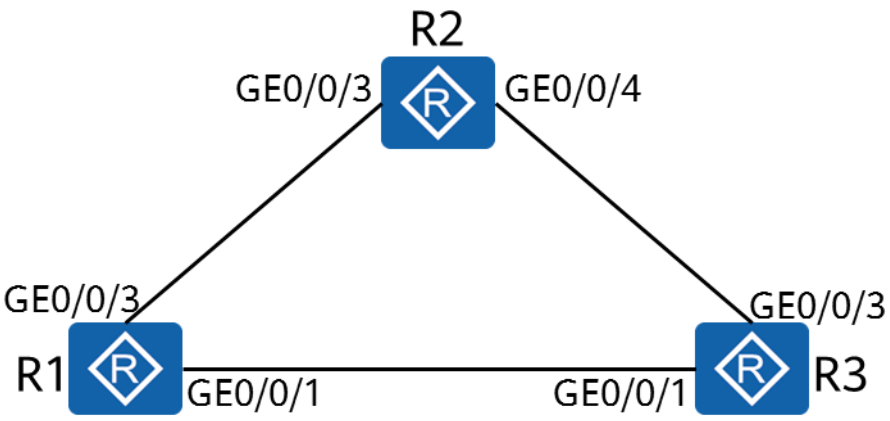


图2-1 IPv4 编址及 IPv4 路由基础实验拓扑

2.1.1.4 实验背景

R1、R2、R3 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联互通。

2.1.2 实验任务配置

2.1.2.1 配置思路

1.配置路由器上各接口的 IP 地址

2.配置静态路由来实现互联互通

2.1.2.2 配置步骤

步骤 1 设备基础配置

设备命名

略。

步骤 2 查看路由器当前接口 IP 地址配置与路由表

查看路由器上的接口状态，仅以 R1 为例

```
[R1]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 5
The number of interface that is UP in Protocol is 1
The number of interface that is DOWN in Protocol is 10

Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/1              unassigned           up         down
GigabitEthernet0/0/2              unassigned           up         down
GigabitEthernet0/0/3              unassigned           up         down
```

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GigabitEthernet0/0/1和GigabitEthernet0/0/3接口由于尚未配置IP地址，所以IP Address/Mask字段为unassigned状态，Protocol字段为down状态，Physical字段为up状态。

查看路由器上的路由表情况，仅以 R1 为例

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

```
------------------------------------------------------------------------------
Routing Tables: 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地址是不可以改变的，也不通过路由协议对外发布。

步骤 3 配置路由物理接口的 IP 地址

按照下表配置路由器的物理接口的 IP 地址

路由器	接口	IP Address/Mask
R1	GigabitEthernet0/0/1	10.0.13.1/24
	GigabitEthernet0/0/3	10.0.12.1/24
R2	GigabitEthernet0/0/3	10.0.12.2/24
	GigabitEthernet0/0/4	10.0.23.2/24
R3	GigabitEthernet0/0/1	10.0.13.3/24
	GigabitEthernet0/0/3	10.0.23.3/24

表2-1 设备物理接口 IP

```
<R1>system-view
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.13.1 24
[R1-GigabitEthernet0/0/1]quit
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
[R1-GigabitEthernet0/0/3]quit
```

```
<R2>system-view
[R2]interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.0.23.2 24
[R2-GigabitEthernet0/0/4]quit
```

```
<R3>system-view
[R3]interface GigabitEthernet0/0/1
```

```
[R3-GigabitEthernet0/0/1]ip address 10.0.13.3 24
[R3-GigabitEthernet0/0/1]quit
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 10.0.23.3 24
[R3-GigabitEthernet0/0/3]quit
```

使用 ping 工具测试联通性

```
[R1]ping 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=70 ms
    Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=40 ms
    Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=50 ms

  --- 10.0.12.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/48/70 ms
```

```
[R1]ping 10.0.13.3
  PING 10.0.13.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.13.3: bytes=56 Sequence=1 ttl=255 time=50 ms
    Reply from 10.0.13.3: bytes=56 Sequence=2 ttl=255 time=60 ms
    Reply from 10.0.13.3: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 10.0.13.3: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.13.3: bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 10.0.13.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/44/60 ms
```

查看 R1 的路由表

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

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.12.0/24  Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/3
        10.0.12.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
      10.0.12.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
        10.0.13.0/24  Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
        10.0.13.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      10.0.13.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
        127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

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

可以看到，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

路由器	接口	IP Address/Mask
R1	LoopBack0	10.0.1.1/32
R2	LoopBack0	10.0.1.2/32
R3	LoopBack0	10.0.1.3/32

表2-2 设备 LoopBack 接口 IP

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接口物理层状态和链路层协议永远处于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. 作为一台路由器的管理地址，起到标识一台设备的作用。
2. 使用该接口地址作为动态路由协议OSPF的router id。
3. 其他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 10.0.1.1 32
```

```
[R2]interface LoopBack0
[R2-LoopBack0]ip address 10.0.1.2 32
```

```
[R3]interface LoopBack0
[R3-LoopBack0]ip address 10.0.1.3 32
```

查看设备上的路由表，以 R1 为例

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

```
             Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.1.1/32   Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.12.0/24  Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/3
      10.0.12.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
    10.0.12.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
      10.0.13.0/24  Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
      10.0.13.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
    10.0.13.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      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
```

此时已经生成了相应的直连路由

测试各 LoopBack 接口之间的联通性

```
[R1]ping -a 10.0.1.1 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.1.2 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地址及目的IP地址。此时由于路由器上没有到底该目的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 R2 和 R3 的 LoopBack0 接口的路由条目

```
[R1]ip route-static 10.0.1.2 32 10.0.12.2
[R1]ip route-static 10.0.1.3 32 10.0.13.3
```

查看 R1 的路由表

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
             Destinations : 13        Routes : 13

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

10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.2/32	**Static**	**60**	**0**	**RD**	**10.0.12.2**	**GigabitEthernet0/0/3**
10.0.1.3/32	**Static**	**60**	**0**	**RD**	**10.0.13.3**	**GigabitEthernet0/0/1**
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
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

配置的静态路由被加入到了 IP 路由表中

测试联通性

```
[R1]ping -a 10.0.1.1 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

还是无法 PING 通 R2 的 LoopBack0 接口，因为此时 R2 上没有到 R1 的 LoopBack0 的路由

在 R2 上添加到达 R1 的 LoopBack0 的路由

```
[R2]ip route-static 10.0.1.1 32 10.0.12.1
```

测试联通性

```
<R1>ping -a 10.0.1.1 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=255 time=60 ms
    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 10/36/60 ms
```

此时 R1 的 LoopBack0 已经可以和 R2 的 LoopBack0 实现互通。

完成剩余路由条目的配置

```
[R2]ip route-static 10.0.1.3 32 10.0.23.3
```

```
[R3]ip route-static 10.0.1.1 32 10.0.13.1
[R3]ip route-static 10.0.1.2 32 10.0.23.2
```

读者自行测试路由器的 LoopBack0 接口之间的联通性

步骤 6 配置 R1->R3->R2 作为 R1 的 LoopBack0 到 R2 的 LoopBack0 接口的备份路径

配置 R1 和 R2 上的静态路由

```
[R1]ip route-static 10.0.1.2 32 10.0.13.3 preference 100
```

```
[R2]ip route-static 10.0.1.1 32 10.0.23.3 preference 100
```

查看 R1 和 R2 上的路由表

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.1.2/32  Static  60   0           RD  10.0.12.2       GigabitEthernet0/0/3
        10.0.1.3/32  Static  60   0           RD  10.0.13.3       GigabitEthernet0/0/1
       10.0.12.0/24  Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/3
       10.0.12.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
     10.0.12.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
       10.0.13.0/24  Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
       10.0.13.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
     10.0.13.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
        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
```

```
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: 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       GigabitEthernet0/0/3
        10.0.1.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.1.3/32  Static  60   0           RD  10.0.23.3       GigabitEthernet0/0/4
       10.0.12.0/24  Direct  0    0           D   10.0.12.2       GigabitEthernet0/0/3
       10.0.12.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
     10.0.12.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
```

```
      10.0.23.0/24  Direct  0    0           D   10.0.23.2       GigabitEthernet0/0/4
      10.0.23.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/4
    10.0.23.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/4
      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 和 R2 之间的链路对应的接口（GigabitEthernet0/0/3），使得优先级高的路由失效。

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]shutdown
```

查看 R1 和 R2 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
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.1.1/32   Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.1.2/32   Static  100  0           RD  10.0.13.3       GigabitEthernet0/0/1
      10.0.1.3/32   Static  60   0           RD  10.0.13.3       GigabitEthernet0/0/1
     10.0.13.0/24   Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
     10.0.13.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
   10.0.13.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      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
```

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

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.1.1/32   Static  100  0           RD  10.0.23.3       GigabitEthernet0/0/4
      10.0.1.2/32   Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.1.3/32   Static  60   0           RD  10.0.23.3       GigabitEthernet0/0/4
     10.0.23.0/24   Direct  0    0           D   10.0.23.2       GigabitEthernet0/0/4
     10.0.23.2/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/4
   10.0.23.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/4
      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。

检查联通性

```
[R1]ping -a 10.0.1.1 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=254 time=80 ms
    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=254 time=60 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=254 time=60 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=254 time=110 ms
    Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=254 time=80 ms

  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 60/78/110 ms
```

追踪数据包路径

```
[R1]tracert -a 10.0.1.1 10.0.1.2

 traceroute to  10.0.1.2(10.0.1.2), max hops: 30 ,packet length: 40,press CTRL_C to break

 1 10.0.13.3 40 ms  30 ms  50 ms

 2 10.0.23.2 80 ms  80 ms  60 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R3的GigabitEthernet0/0/1，再经过R3的GigabitEthernet0/0/3转发给R2的GigabitEthernet0/0/4。
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 R2 的 LoopBack0 接口互联互通

恢复接口并删除已经配置的路由条目

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]undo shutdown
[R1-GigabitEthernet0/0/3]quit
[R1]undo ip route-static 10.0.1.2 255.255.255.255 10.0.12.2
[R1]undo ip route-static 10.0.1.2 255.255.255.255 10.0.13.3 preference 100
```

查看 R1 的路由表

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

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

```
      10.0.1.1/32   Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.1.3/32   Static  60   0           RD  10.0.13.3       GigabitEthernet0/0/1
     10.0.12.0/24   Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/3
     10.0.12.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
   10.0.12.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
     10.0.13.0/24   Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
     10.0.13.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
   10.0.13.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      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
```

此时 R1 上没有到 R2 的 LoopBack0（10.0.1.2/32）的路由条目

在 R1 上配置默认路由

```
[R1]ip route-static 0.0.0.0 0 10.0.12.2
```

查看 R1 的路由条目

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD  10.0.12.2       GigabitEthernet0/0/3
      10.0.1.1/32   Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.1.3/32   Static  60   0           RD  10.0.13.3       GigabitEthernet0/0/1
     10.0.12.0/24   Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/3
     10.0.12.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
   10.0.12.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
     10.0.13.0/24   Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
     10.0.13.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
   10.0.13.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      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
```

默认路由已经被激活

测试 R1 的 LoopBack0 接口到 R2 的 LoopBack0 接口的联通性

```
[R1]ping -a 10.0.1.1 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=255 time=50 ms
    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=255 time=20 ms
```

```
  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/32/50 ms
```

此时 R1 的 LoopBack0 接口到 R2 的 LoopBack0 接口之间可以互联互通。

2.1.3 结果验证

读者自行通过 ping 和 tracert 命令检查设备 LoopBack0 接口之间的联通性。

2.1.4 配置参考

R1 的配置

```
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.13.1 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ip route-static 0.0.0.0 0.0.0.0 10.0.12.2
ip route-static 10.0.1.3 255.255.255.255 10.0.13.3
#
return
```

R2 的配置

```
#
 sysname R2
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
#
interface GigabitEthernet0/0/4
 ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.2 255.255.255.255
#
ip route-static 10.0.1.1 255.255.255.255 10.0.12.1
ip route-static 10.0.1.1 255.255.255.255 10.0.23.3 preference 100
ip route-static 10.0.1.3 255.255.255.255 10.0.23.3
#
return
```

R3 的配置

```
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.13.3 255.255.255.0
#
interface GigabitEthernet00/3
 ip address 10.0.23.3 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.3 255.255.255.255
#
ip route-static 10.0.1.1 255.255.255.255 10.0.13.1
ip route-static 10.0.1.2 255.255.255.255 10.0.23.2
#
return
```

2.1.5 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？

2. 在步骤三中，当测试 LoopBack 接口之间联通性时，若不加-a 参数，则 ICMP 报文的源 IP 地址将会是多少？为什么？

2.2 实验二：OSPF 路由协议基础实验

2.2.1 实验介绍

2.2.1.1 关于本实验

开放式最短路径优先 OSPF（Open Shortest Path First）是 IETF 组织开发的一个基于链路状态的内部网关协议（Interior Gateway Protocol）。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，OSPF 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 路由器的影响。
- OSPF 支持无类型域间选路（CIDR）。
- 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收并广泛使用

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。

2.2.1.2 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 的选路
- 掌握 OSPF 发布默认路由的方法
- 掌握 OSPF 认证配置方法

2.2.1.3 实验组网介绍

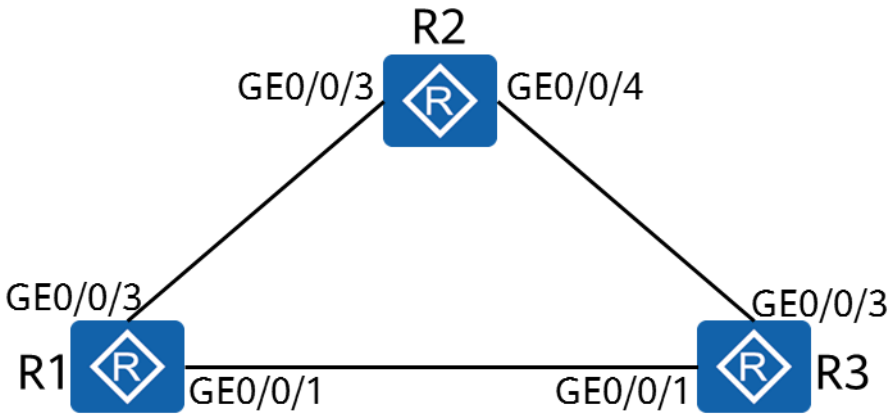


图2-2 OSPF 路由协议基础实验拓扑

2.2.1.4 实验背景

R1、R2、R3 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联互通。

2.2.2 实验任务配置

2.2.2.1 配置思路

1. 创建设备上的 OSPF 进程并使能接口上的 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

2.2.2.2 配置步骤

步骤 1 设备基础配置

按照实验一的步骤 1、2、3、4 完成路由器的命名、物理接口和 LoopBack 接口的 IP 地址配置

查看设备的路由表，以 R1 为例

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.12.0/24  Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/3
       10.0.12.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
     10.0.12.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
       10.0.13.0/24  Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
       10.0.13.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
     10.0.13.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
        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
```

此时设备上仅存在直连路由。

步骤 2 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 10.0.12.1 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.13.1 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.1.1 0.0.0.0
```

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。OSPF使用反掩码，例如0.0.0.255表示掩码长度24位。
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

```
[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.12.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.0.23.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.0.1.2 0.0.0.0
```

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。

```
[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.13.3 0.0.0.0
[R3-ospf-1-area-0.0.0.0]network 10.0.23.3 0.0.0.0
[R3-ospf-1-area-0.0.0.0]network 10.0.1.3 0.0.0.0
```

步骤 3 查看 OSPF 状态

查看 OSPF 邻居

```
[R1]display ospf peer

         OSPF Process 1 with Router ID 10.0.1.1
                  Neighbors

 Area 0.0.0.0 interface 10.0.13.1(GigabitEthernet0/0/1)'s neighbors
 Router ID: 10.0.1.3             Address: 10.0.13.3
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.0.13.3  BDR: 10.0.13.1  MTU: 0
   Dead timer due in 36  sec
   Retrans timer interval: 0
   Neighbor is up for 00:00:30
   Authentication Sequence: [ 0 ]

                  Neighbors

 Area 0.0.0.0 interface 10.0.12.1(GigabitEthernet0/0/3)'s neighbors
 Router ID: 10.0.1.2             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 39    sec
    Retrans timer interval: 4
    Neighbor is up for 00:00:28
    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路由器等信息。

查看 IP 路由表中由 OSPF 学习到的路由

```
[R1]display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Public routing table : OSPF
         Destinations : 3        Routes : 4

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

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.2/32  OSPF    10   1           D  10.0.12.2       GigabitEthernet0/0/3
        10.0.1.3/32  OSPF    10   1           D  10.0.13.3       GigabitEthernet0/0/1
       10.0.23.0/24  OSPF    10   2           D  10.0.13.3       GigabitEthernet0/0/1
                     OSPF    10   2           D  10.0.12.2       GigabitEthernet0/0/3

OSPF routing table status : <Inactive>
         Destinations : 0        Routes : 0
```

步骤 4 配置 OSPF 认证

在 R1 上配置接口认证

```
[R1]interface GigabitEthernet0/0/1
[R1- GigabitEthernet0/0/1]ospf authentication-mode md5 1 cipher HCIA-Datacom
[R1]interface GigabitEthernet0/0/3
[R1- GigabitEthernet0/0/3]ospf authentication-mode md5 1 cipher HCIA-Datacom
[R1- GigabitEthernet0/0/3]display this
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
 ospf authentication-mode md5 1 cipher foCQTYsq-4.A\^38y!DVwQ0#
#
```

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。

查看当前的邻居状态

```
[R1]display ospf peer brief


     OSPF Process 1 with Router ID 10.0.1.1
          Peer Statistic Information
 ----------------------------------------------------------------------------------------------------------------------------
```

```
 Area Id          Interface                            Neighbor id      State
 ------------------------------------------------------------------------------------------------------------------------------
Total Peer(s):      0
```

由于其他路由器还未配置认证，所以认证不通过，无邻居。

配置 R2 上的接口认证

```
[R2]interface GigabitEthernet0/0/3
[R2- GigabitEthernet0/0/3]ospf authentication-mode md5 1 cipher HCIA-Datacom
[R2]interface GigabitEthernet0/0/4
[R2- GigabitEthernet0/0/4]ospf authentication-mode md5 1 cipher HCIA-Datacom
```

查看 R2 的邻居状态

```
[R2]display ospf peer brief

      OSPF Process 1 with Router ID 10.0.1.2
            Peer Statistic Information
 ------------------------------------------------------------------------------------------------------------------------------
 Area Id          Interface                            Neighbor id      State
 0.0.0.0          GigabitEthernet0/0/3                 10.0.1.1         Full
 ------------------------------------------------------------------------------------------------------------------------------
Total Peer(s):      1
```

此时 R2 已经可以和 R1 建立起正常的邻居关系。

在 R3 上配置区域认证

```
[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]authentication-mode md5 1 cipher HCIA-Datacom
```

查看 R3 上的邻居状态

```
[R3]display ospf peer brief

                OSPF Process 1 with Router ID 10.0.1.3
                      Peer Statistic Information
----------------------------------------------------------------------------------------------------------------------------
 Area Id          Interface                            Neighbor id      State
 0.0.0.0          GigabitEthernet0/0/1                 10.0.1.1           Full
 0.0.0.0          GigabitEthernet0/0/3                 10.0.1.2           Full
----------------------------------------------------------------------------------------------------------------------------
 Total Peer(s):      2
```

此时 R3 已经和 R1 与 R2 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 5 假设 R1 为所有网络的出口，所以在 R1 上向 OSPF 宣告默认路由

在 R1 上宣告默认路由

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

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默认路由时才向其他路由器发布默认路由。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 R2 与 R3 上的 IP 路由表

```
 [R2]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 15        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   10.0.12.1       GigabitEthernet0/0/3
       10.0.1.1/32  OSPF    10   1           D   10.0.12.1       GigabitEthernet0/0/3
       10.0.1.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.1.3/32  OSPF    10   1           D   10.0.23.3       GigabitEthernet0/0/4
      10.0.12.0/24  Direct  0    0           D   10.0.12.2       GigabitEthernet0/0/3
      10.0.12.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
    10.0.12.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
      10.0.13.0/24  OSPF    10   2           D   10.0.12.1       GigabitEthernet0/0/3
                    OSPF    10   2           D   10.0.23.3       GigabitEthernet0/0/4
      10.0.23.0/24  Direct  0    0           D   10.0.23.2       GigabitEthernet0/0/4
      10.0.23.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/4
    10.0.23.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/4
       127.0.0.0/8  Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

```
[R3]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 15        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   10.0.13.1       GigabitEthernet0/0/1
       10.0.1.1/32  OSPF    10   1           D   10.0.13.1       GigabitEthernet0/0/1
       10.0.1.2/32  OSPF    10   1           D   10.0.23.2       GigabitEthernet0/0/3
       10.0.1.3/32  Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.12.0/24  OSPF    10   2           D   10.0.23.2       GigabitEthernet0/0/3
                    OSPF    10   2           D   10.0.13.1       GigabitEthernet0/0/1
      10.0.13.0/24  Direct  0    0           D   10.0.13.3       GigabitEthernet0/0/1
      10.0.13.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
    10.0.13.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      10.0.23.0/24  Direct  0    0           D   10.0.23.3       GigabitEthernet0/0/3
      10.0.23.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
    10.0.23.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
       127.0.0.0/8  Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
```

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

R2 与 R3 上已经学习到相应的默认路由。

步骤 6 通过修改 R1 相应接口的 Cost 值，使得 R1 的 LoopBack0 接口通过 R1->R3->R2 的路径访问 R2 的 LoopBack0 接口

从 R1 的路由表可知，R1 通过 R1->R2 的路径访问 R2 的 LoopBack0 接口的路由开销为 1，从 R1->R3->R2 的路由开销为 2，故只要使 R1->R2 的路由开销大于 2 即可。

```
[R1]interface GigabitEthernet0/0/3
[R1- GigabitEthernet0/0/3]ospf cost 10
```

查看 R1 的路由表

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Direct  0    0           D  127.0.0.1       LoopBack0
        10.0.1.2/32  OSPF    10   2           D  10.0.13.3       GigabitEthernet0/0/1
        10.0.1.3/32  OSPF    10   1           D  10.0.13.3       GigabitEthernet0/0/1
       10.0.12.0/24  Direct  0    0           D  10.0.12.1       GigabitEthernet0/0/3
       10.0.12.1/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/3
     10.0.12.255/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/3
       10.0.13.0/24  Direct  0    0           D  10.0.13.1       GigabitEthernet0/0/1
       10.0.13.1/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/1
     10.0.13.255/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/1
       10.0.23.0/24  OSPF    10   2           D  10.0.13.3       GigabitEthernet0/0/1
        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
```

此时 R1 访问 R2 的 LoopBack0 接口的下一跳为 R3 的 GigabitEthernet0/0/1 接口

通过 Tracert 命令验证

```
[R1]tracert –a 10.0.1.1 10.0.1.2

 traceroute to   10.0.1.2(10.0.1.2), max hops: 30 ,packet length: 40,press CTRL_C to break

 1 10.0.13.3 40 ms   50 ms   50 ms

 2 10.0.23.2 60 ms   110 ms   70 ms
```

2.2.3 结果验证

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

2.2.4 配置参考

R1 的配置

```
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.13.1 255.255.255.0
 ospf authentication-mode md5 1 cipher %^%#`f*R'6q/RMq(+5*g(sP~SB8oQ49;%7WE:07P7X:W%^%#
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
 ospf cost 10
 ospf authentication-mode md5 1 cipher %^%#]e)pBf~7B0.FM~U;bRAVgE$U>%X;>T\M\tLlYRj2%^%#
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ospf 1
 default-route-advertise always
 area 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 10.0.12.0 0.0.0.255
  network 10.0.13.0 0.0.0.255
#
return
```

R2 的配置

```
#
 sysname R2
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
 ospf authentication-mode md5 1 cipher %^%#z+72ZaTk2+v/g7E~AmR"NFYAKC>LZ8~Y`[**Gh=&%^%#
#
 interface GigabitEthernet0/0/4
 ip address 10.0.23.2 255.255.255.0
 ospf authentication-mode md5 1 cipher %^%#=@2jEBu!{&UYoB*(RDVLc5t~<1B_a-PwC$WH%jQ3%^%#
#
interface LoopBack0
 ip address 10.0.1.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.0.1.2 0.0.0.0
  network 10.0.12.2 0.0.0.0
  network 10.0.23.2 0.0.0.0
#
```

```
return
```

R3 的配置

```
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.13.3 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 10.0.23.3 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  authentication-mode md5 1 cipher %^%#Rl<:SVln1M>[Gk"v/OeSEW|:0:4*h;b|-d:N"s{>%^%#
  network 10.0.1.3 0.0.0.0
  network 10.0.13.3 0.0.0.0
  network 10.0.23.3 0.0.0.0
#
return
```

2.2.5 思考题

1. 步骤 6 中，R2 回复 R1 的 ICMP 报文的路径是什么样的？试着解释一下原因。

3 构建以太网交换网络

3.1 实验一：以太网基础与 VLAN 配置实验

3.1.1 实验介绍

3.1.1.1 关于本实验

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detection）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 LAN 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。

3.1.1.2 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

3.1.1.3 实验组网介绍

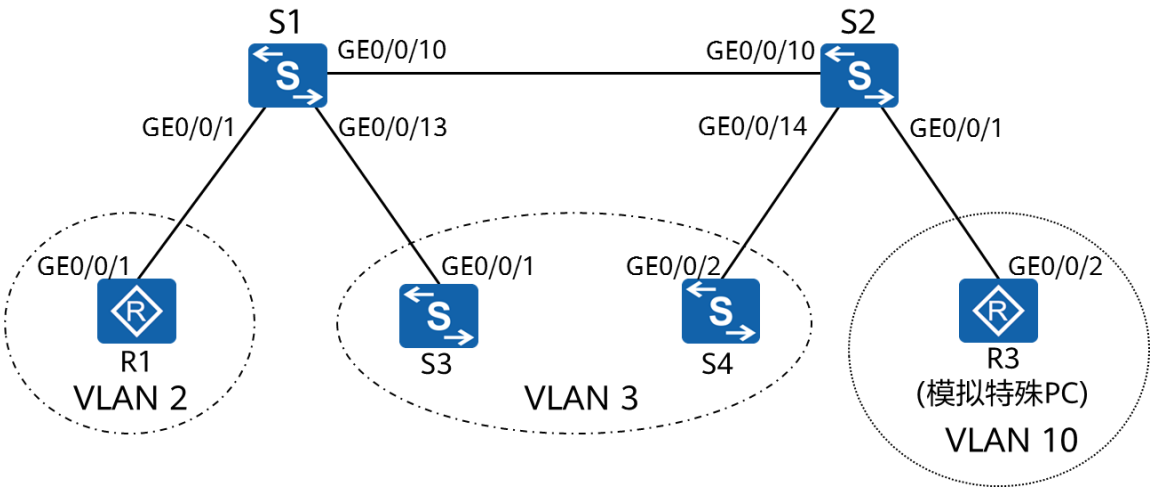


图3-1 VLAN 配置实验拓扑

3.1.1.4 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。同时，VLAN 10 为特殊 VLAN，为了保证信息安全，只有某些特殊的 PC 才可以通过 VLAN 10 进行网络访问。

如实验拓扑图所示，可以在 S1 和 S2 交换机上配置基于接口划分 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 上配置基于 MAC 地址划分 VLAN，绑定特殊 PC 的 MAC 地址。

3.1.2 实验任务配置

3.1.2.1 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

3.1.2.2 配置步骤

步骤 1 配置 S1 和 S2 设备名称并关闭多余接口

设备命名

略。

关闭 S1 的 GE0/0/11 和 GE0/0/12 接口，只针对《HCIA-Datacom 实验室搭建指南 V1.0》所描述的环境，其他环境可以忽略此步骤。

```
[S1]interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]shutdown
[S1-GigabitEthernet0/0/11]quit
[S1]interface GigabitEthernet 0/0/12
```

```
[S1-GigabitEthernet0/0/12]shutdown
[S1-GigabitEthernet0/0/12]quit
```

关闭 S2 的 GE0/0/11 和 GE0/0/12 接口

```
[S2]interface GigabitEthernet 0/0/11
[S2-GigabitEthernet0/0/11]shutdown
[S2-GigabitEthernet0/0/11]quit
[S2]interface GigabitEthernet 0/0/12
[S2-GigabitEthernet0/0/12]shutdown
[S2-GigabitEthernet0/0/12]quit
```

步骤 2 配置设备 IP 地址

配置 R1 和 R3 的 IP 地址，其中物理口地址分别为 10.1.2.1/24 和 10.1.10.1/24

```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.1.2.1 24
```

```
[R3]interface GigabitEthernet0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.1.10.1 24
```

配置 S3 和 S4 的 IP 地址，其中物理口地址分别为 10.1.3.1/24 和 10.1.3.2/24（场景 1：适用于 S3 和 S4 支持二层接口切换为三层接口的环境）

```
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]undo portswitch
```

该接口状态转变为三层模式

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

```
[S3-GigabitEthernet0/0/1]ip address 10.1.3.1 24
```

```
[S4]interface GigabitEthernet0/0/2
[S4-GigabitEthernet0/0/2]undo portswitch
[S4-GigabitEthernet0/0/2]ip address 10.1.3.2 24
```

配置 S3 和 S4 的 IP 地址，其中逻辑口 VLANIF3 地址分别为 10.1.3.1/24 和 10.1.3.2/24（场景 2：适用于 S3 和 S4 不支持二层接口切换为三层接口的环境）

1. 在交换机 S3 和 S4 上创建 VLAN 3

```
[S3]vlan 3
[S3-vlan3]
```

```
[S4]vlan 3
[S4-vlan3]
```

2. 配置交换机 S3 和 S4 的接口为 Access 接口，并将接口划入对应的 VLAN

```
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]port link-type access
```

```
[S3-GigabitEthernet0/0/1]port default vlan 3
[S3-GigabitEthernet0/0/1]quit
```

```
[S4]interface GigabitEthernet0/0/2
[S4-GigabitEthernet0/0/2]port link-type access
[S4-GigabitEthernet0/0/2]port default vlan 3
[S4-GigabitEthernet0/0/2]quit
```

3. 创建 VLANIF 并配置相应的 IP 地址

```
[S3] interface Vlanif 3
```

interface vlanif *vlan-id*命令用来创建三层逻辑VLANIF接口并进入VLANIF接口视图。

```
[S3-Vlanif3]ip address 10.1.3.1 24
```

```
[S4] interface Vlanif 3
[S4-Vlanif3]ip address 10.1.3.2 24
```

步骤 3 创建 VLAN

在交换机 S1 和 S2 上创建 VLAN 2、3、10

```
[S1]vlan batch 2 to 3 10
Info: This operation may take a few seconds. Please wait for a moment...done.
```

VLAN 2、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*] }命令用来指定批量创建VLAN。

```
[S2]vlan batch 2 to 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 GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]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。

```
[S1-GigabitEthernet0/0/1]port default vlan 2
```

port default vlan *vlan-id*命令用来配置接口的缺省VLAN并同时加入这个VLAN。

```
[S1-GigabitEthernet0/0/1]quit
[S1]interface GigabitEthernet0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]port default vlan 3
```

```
[S1-GigabitEthernet0/0/13]quit
```

```
[S2]interface GigabitEthernet0/0/14
[S2-GigabitEthernet0/0/14]port link-type access
[S2-GigabitEthernet0/0/14]port default vlan 3
[S2-GigabitEthernet0/0/14]quit
```

配置交换机 S1 和 S2 的互联接口为 Trunk 接口，并仅允许 VLAN 2、3 通过

```
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3
```

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

```
[S1-GigabitEthernet0/0/10]undo port trunk allow-pass vlan 1
```

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 GigabitEthernet0/0/10
[S2-GigabitEthernet0/0/10]port link-type trunk
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3
[S2-GigabitEthernet0/0/10]undo port trunk allow-pass vlan 1
```

步骤 5 配置基于 MAC 地址划分 VLAN

如实验组网图所示，路由器 R3 模拟特殊业务 PC，假设该 PC 的 MAC 地址为：a008-6fe1-0c46。希望该 PC 可以通过 S2 的 GigabitEthernet0/0/1、GigabitEthernet0/0/2、GigabitEthernet0/0/3 任意一个端口接入网络，并且通过 VLAN 10 进行数据传递。

配置交换机 S2，让 PC 的 MAC 地址与 VLAN 10 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。

```
[S2] vlan 10
[S2-vlan10] mac-vlan mac-address a008-6fe1-0c46
```

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

配置交换机 S2 的 GigabitEthernet0/0/1、GigabitEthernet0/0/2、GigabitEthernet0/0/3 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 GigabitEthernet0/0/1
[S2-GigabitEthernet0/0/1]port link-type hybrid
[S2-GigabitEthernet0/0/1]port hybrid untagged vlan 10
```

port hybrid untagged vlan命令用来配置Hybrid类型接口加入的VLAN，这些VLAN的帧以Untagged方式通过接口。

```
[S2-GigabitEthernet0/0/1]quit
[S2]interface GigabitEthernet0/0/2
[S2-GigabitEthernet0/0/2]port link-type hybrid
[S2-GigabitEthernet0/0/2]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/2]quit
[S2]interface GigabitEthernet0/0/3
[S2-GigabitEthernet0/0/3]port link-type hybrid
[S2-GigabitEthernet0/0/3]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/3]quit
```

配置交换机 S1 和 S2 的互联接口允许 VLAN 10 通过

交换机互联接口需要保证多个VLAN带标签通过，因此可以配置为Trunk接口。

```
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 10
[S1-GigabitEthernet0/0/10]quit
```

```
[S2]interface GigabitEthernet0/0/10
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 10
[S2-GigabitEthernet0/0/10]quit
```

配置交换机 S2，使能 GE0/0/1、GE0/0/2、GE0/0/3 接口基于 MAC 地址划分 VLAN 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，必须使用使能接口的MAC VLAN功能。

```
[S2]interface GigabitEthernet0/0/1
[S2-GigabitEthernet0/0/1]mac-vlan enable
```

mac-vlan enable命令用来使能接口的MAC VLAN功能。

```
[S2-GigabitEthernet0/0/1]quit
[S2]interface GigabitEthernet0/0/2
[S2-GigabitEthernet0/0/2]mac-vlan enable
[S2-GigabitEthernet0/0/2]quit
[S2]interface GigabitEthernet0/0/3
[S2-GigabitEthernet0/0/3]mac-vlan enable
[S2-GigabitEthernet0/0/3]quit
```

步骤 6 查看配置信息

查看交换机的 VLAN 信息

```
[S1]display vlan
```

display vlan命令用来查看VLAN的相关信息。
display vlan verbose命令用来查看指定VLAN的详细信息，包括VLAN ID、类型、描述信息、状态、统计开关状态、包含的接口以及这些接口的加入方式等。

```
The total number of vlans is : 4
```

```
--------------------------------------------------------------------------------
U: Up;               D: Down;            TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                        ST: Vlan-stacking;
#: ProtocolTransparent-vlan;             *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type       Ports
--------------------------------------------------------------------------------
1    common   UT:      GE0/0/2(D)       GE0/0/3(D)       GE0/0/4(D)       GE0/0/5(D)
                       GE0/0/6(D)       GE0/0/7(D)       GE0/0/8(D)       GE0/0/9(D)
                       GE0/0/11(D)      GE0/0/12(D)      GE0/0/14(D)      GE0/0/15(D)
                       GE0/0/16(D)      GE0/0/17(D)      GE0/0/18(D)      GE0/0/19(D)
                       GE0/0/20(D)      GE0/0/21(D)      GE0/0/22(D)      GE0/0/23(D)
                       GE0/0/24(D)
2    common   UT:      GE0/0/1(U)
              TG:      GE0/0/10(U)
3    common   UT:      GE0/0/13(U)
              TG:      GE0/0/10(U)
10   common   TG:      GE0/0/10(U)

VID  Status   Property        MAC-LRN Statistics   Description
--------------------------------------------------------------------------------
1    enable   default         enable      disable      VLAN 0001
2    enable   default         enable      disable      VLAN 0002
3    enable   default         enable      disable      VLAN 0003
10   enable   default         enable      disable      VLAN 0010
```

```
[S2]display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;               D: Down;            TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                        ST: Vlan-stacking;
#: ProtocolTransparent-vlan;             *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type       Ports
--------------------------------------------------------------------------------
1    common   UT:      GE0/0/1(U)       GE0/0/2(D)       GE0/0/3(D)       GE0/0/4(D)
                       GE0/0/5(D)       GE0/0/6(D)       GE0/0/7(D)       GE0/0/8(D)
                       GE0/0/9(D)       GE0/0/11(D)      GE0/0/12(D)      GE0/0/13(D)
                       GE0/0/15(D)      GE0/0/16(D)      GE0/0/17(D)      GE0/0/18(D)
                       GE0/0/19(D)      GE0/0/20(D)      GE0/0/21(D)      GE0/0/22(D)
                       GE0/0/23(D)      GE0/0/24(D)
2    common   TG:      GE0/0/10(U)
3    common   UT:      GE0/0/14(U)
              TG:      GE0/0/10(U)
10   common   UT:      GE0/0/1(U)       GE0/0/2(D)       GE0/0/3(D)
              TG:      GE0/0/10(U)

VID  Status   Property        MAC-LRN Statistics   Description
--------------------------------------------------------------------------------
1    enable   default         enable      disable      VLAN 0001
2    enable   default         enable      disable      VLAN 0002
3    enable   default         enable      disable      VLAN 0003
10   enable   default         enable      disable      VLAN 0010
```

查看交换机的 MAC-VLAN 信息

```
[S2]display mac-vlan vlan 10
--------------------------------------------------------------------------------
MAC Address       MASK                VLAN       Priority
--------------------------------------------------------------------------------
00e0-fc1c-47a7    ffff-ffff-ffff       10          0

Total MAC VLAN address count: 1
```

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

3.1.3 结果验证

检测设备连通性，验证 VLAN 配置结果

1）在 S3 上执行 Ping 命令，使得 S3 可以 Ping 通 S4。

2）在 R1 上执行 Ping 命令，使得 R1 与谁都无法 Ping 通。

3）在 S1 和 S2 上通过 display mac-address verbose，查看交换机的 MAC 地址表。

3.1.4 配置参考

S1 的配置

```
#
sysname S1
#
vlan batch 2 to 3 10
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
interface GigabitEthernet0/0/11
 shutdown
#
interface GigabitEthernet0/0/12
 shutdown
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 3
#
return
```

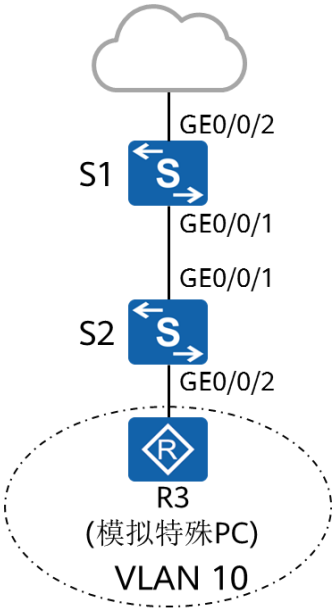
S2 的配置

```
#
sysname S2
```

```
#
vlan batch 2 to 3 10
#
vlan 10
 mac-vlan mac-address a008-6fe1-0c46 priority 0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
interface GigabitEthernet0/0/11
 shutdown
#
interface GigabitEthernet0/0/12
 shutdown
#
interface GigabitEthernet0/0/14
 port link-type access
 port default vlan 3
#
return
```

3.1.5 思考题

1. 如下图所示拓扑，为了保证某特殊业务的信息安全，要求只有某些特殊 PC 才可以通过 VLAN 10 进行网络访问，并且要求在 S1 交换机上实现该功能，请问将如何配置实现?



3.2 实验二：生成树基础实验

3.2.1 实验介绍

3.2.1.1 关于本实验

以太网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，提出了生成树协议 STP（Spanning Tree Protocol）。

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 中定义的快速生成树协议 RSTP（Rapid Spanning Tree Protocol），再到最新的 IEEE 802.1S 中定义的多生成树协议 MSTP（Multiple Spanning Tree Protocol）。

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。

3.2.1.2 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

3.2.1.3 实验组网介绍

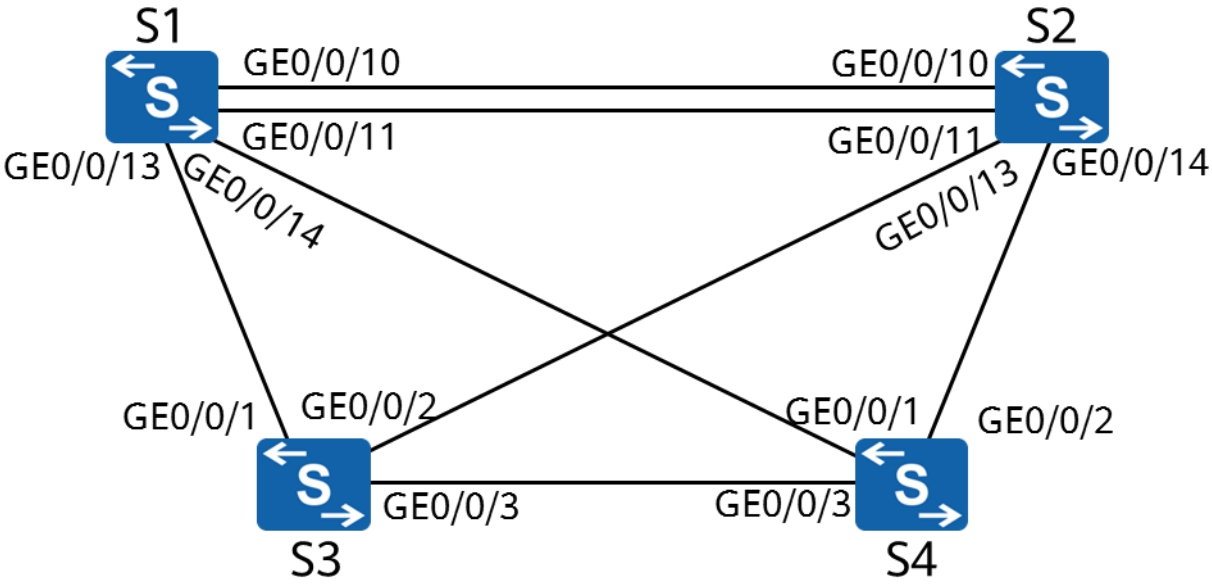


图3-2 生成树基础实验拓扑

3.2.1.4 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。

3.2.2 实验任务配置

3.2.2.1 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

3.2.2.2 配置步骤

步骤 1 关闭多余接口，只针对《HCIA-Datacom 实验室搭建指南 V1.0》所描述的环境，其他环境可以忽略此步骤。

#关闭 S1 与 S2 之间的 GigabitEthernet0/0/12 接口

```
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
```

```
[S2]interface GigabitEthernet 0/0/12
[S2-GigabitEthernet0/0/12]shutdown
```

步骤 2 配置设备运行 STP

全局使能 STP 功能

```
<S1>system-view
Enter system view, return user view with Ctrl+Z.
[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/RSTP/MSTP功能处于启用状态，此处配置仅为演示用。

修改当前生成树工作模式为 STP

```
[S1]stp mode stp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

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，设备的生成树协议工作模式为MSTP模式。当前设备的生成树模式已经被修改为STP。

```
[S2]stp mode stp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S3]stp mode stp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S4]stp mode stp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

查看生成树的状态，以 S1 为例

```
[S1]display stp
-------[CIST Global Info][Mode STP]-------
CIST Bridge          :32768.4c1f-cc33-7359                  //自身的桥 ID。
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :32768.4c1f-cc10-5913 / 20000          //当前的根桥的 ID 与根路径开销
CIST RegRoot/IRPC    :32768.4c1f-cc33-7359 / 0
CIST RootPortId      :128.14
BPDU-Protection      :Disabled
TC or TCN received   :47
TC count per hello   :0
STP Converge Mode    :Normal
Time since last TC   :0 days 0h:0m:38s
Number of TC         :15
Last TC occurred     :GigabitEthernet0/0/14
```

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。

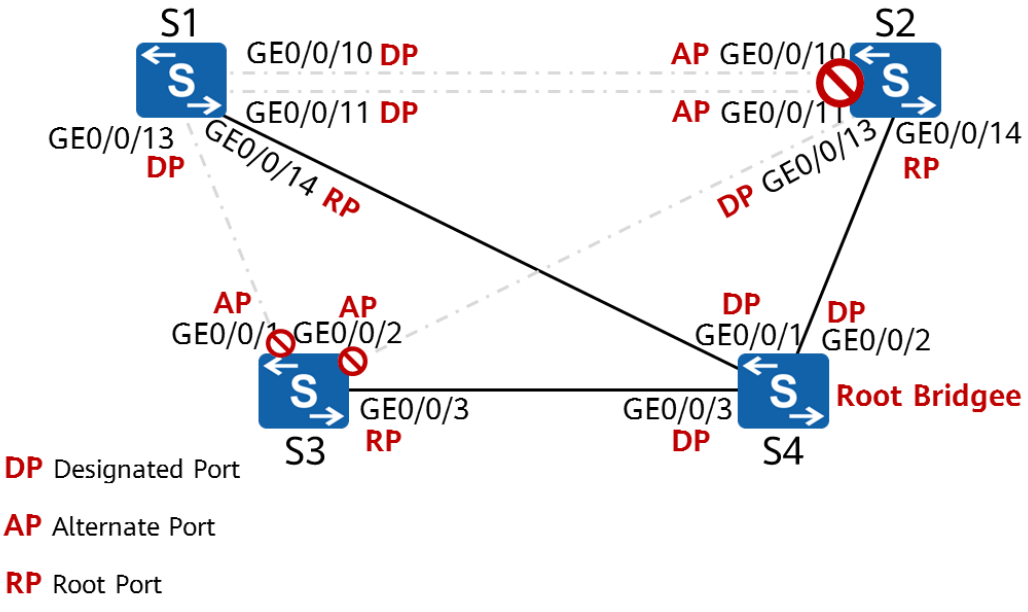
```
[S1]display stp brief
 MSTID    Port                        Role    STP State     Protection
    0     GigabitEthernet0/0/10       DESI    FORWARDING    NONE
    0     GigabitEthernet0/0/11       DESI    FORWARDING    NONE
    0     GigabitEthernet0/0/13       DESI    FORWARDING    NONE
    0     GigabitEthernet0/0/14       ROOT    FORWARDING    NONE
```

```
[S2]display stp brief
 MSTID    Port                        Role    STP State     Protection
    0     GigabitEthernet0/0/10       ALTE    DISCARDING    NONE
    0     GigabitEthernet0/0/11       ALTE    DISCARDING    NONE
    0     GigabitEthernet0/0/13       DESI    FORWARDING    NONE
    0     GigabitEthernet0/0/14       ROOT    FORWARDING    NONE
```

```
[S3]display stp brief
 MSTID    Port                        Role    STP State     Protection
    0     GigabitEthernet0/0/1        ALTE    DISCARDING    NONE
    0     GigabitEthernet0/0/2        ALTE    DISCARDING    NONE
    0     GigabitEthernet0/0/3        ROOT    FORWARDING    NONE
```

```
[S4]display stp brief
 MSTID    Port                        Role    STP State     Protection
    0     GigabitEthernet0/0/1        DESI    FORWARDING    NONE
    0     GigabitEthernet0/0/2        DESI    FORWARDING    NONE
    0     GigabitEthernet0/0/3        DESI    FORWARDING    NONE
```

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会被选举为根桥。但是，性能高、网络层次高的交换设备其优先级不一定高，因此可以通过执行相应命令配置其为根桥，以保证该设备成为根桥。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交换设备，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。
- 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。

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

在 S1 上查看当前 STP 状态

```
[S1]display stp
-------[CIST Global Info][Mode STP]-------
CIST Bridge          :0       .4c1f-cc33-7359                    //自身的桥 ID。
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :0       .4c1f-cc33-7359 / 0                //当前的根桥的 ID 与根路径开销
CIST RegRoot/IRPC    :0       .4c1f-cc33-7359 / 0
CIST RootPortId      :0.0
BPDU-Protection      :Disabled
CIST Root Type       :Primary root
TC or TCN received   :84
TC count per hello   :0
STP Converge Mode    :Normal
Time since last TC   :0 days 0h:1m:44s
Number of TC         :21
Last TC occurred     :GigabitEthernet0/0/10
```

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

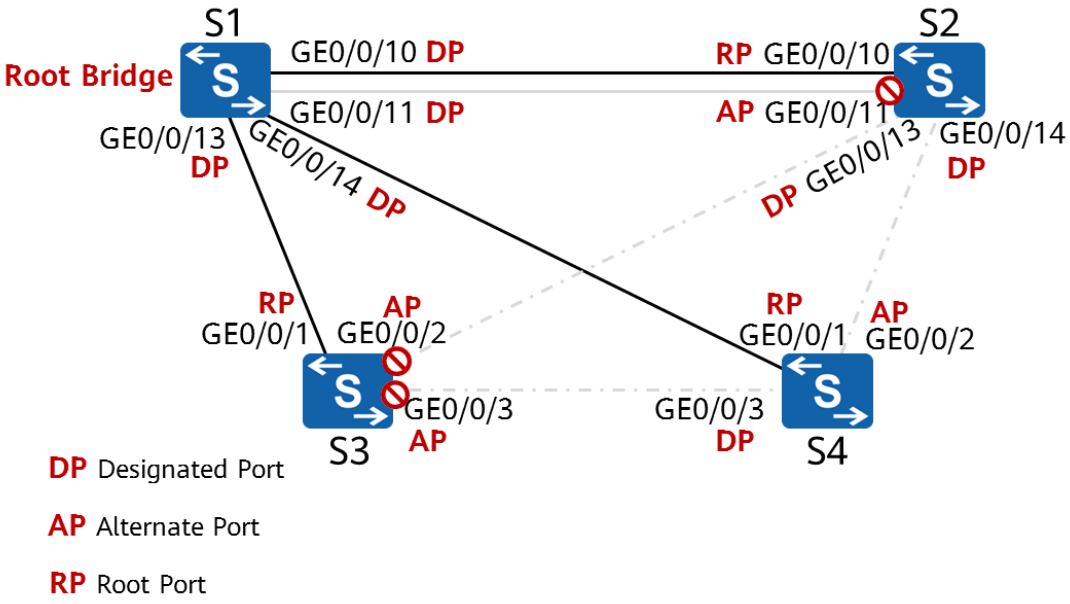
```
[S1]display stp brief
 MSTID   Port                        Role  STP State       Protection
   0     GigabitEthernet0/0/10       DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/11       DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/13       DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/14       DESI  FORWARDING      NONE
```

```
[S2]display stp brief
 MSTID   Port                        Role  STP State       Protection
   0     GigabitEthernet0/0/10       ROOT  FORWARDING      NONE
   0     GigabitEthernet0/0/11       ALTE  DISCARDING      NONE
   0     GigabitEthernet0/0/13       DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/14       DESI  FORWARDING      NONE
```

```
[S3]display stp brief
 MSTID    Port                      Role    STP State     Protection
   0      GigabitEthernet0/0/1      ROOT    FORWARDING    NONE
   0      GigabitEthernet0/0/2      ALTE    DISCARDING    NONE
   0      GigabitEthernet0/0/3      ALTE    DISCARDING    NONE
```

```
[S4]display stp brief
 MSTID    Port                      Role    STP State     Protection
   0      GigabitEthernet0/0/1      ROOT    FORWARDING    NONE
   0      GigabitEthernet0/0/2      ALTE    DISCARDING    NONE
   0      GigabitEthernet0/0/3      DESI    FORWARDING    NONE
```

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 GigabitEthernet0/0/2 接口成为根端口

查看 S4 上的 STP 状态信息

```
[S4]display stp
-------[CIST Global Info][Mode STP]-------
CIST Bridge             :32768.4c1f-cc10-5913
Config Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC          :0       .4c1f-cc33-7359 / 20000
CIST RegRoot/IRPC       :32768.4c1f-cc10-5913 / 0
CIST RootPortId         :128.1
BPDU-Protection         :Disabled
TC or TCN received      :93
TC count per hello      :0
STP Converge Mode       :Normal
```

```
Time since last TC          :0 days 0h:9m:5s
Number of TC                :18
Last TC occurred            :GigabitEthernet0/0/1
```

当前 S4 到 S1 的根路径开销为 20000。

修改 S4 的 GigabitEthernet 0/0/1 的 STP 开销值为 50000

```
[S4]interface GigabitEthernet 0/0/1
[S4-GigabitEthernet0/0/1]stp cost 50000
```

查看当前 STP 状态信息摘要

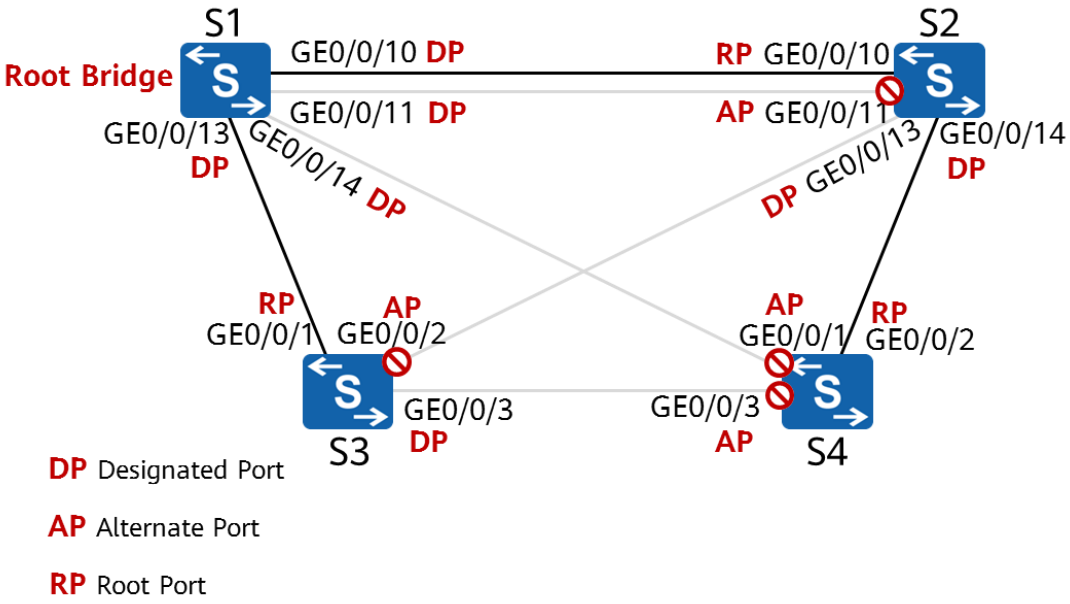
```
[S4]display stp brief
 MSTID   Port                        Role  STP State       Protection
   0     GigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   0     GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   0     GigabitEthernet0/0/3        ALTE  DISCARDING      NONE
```

S4 的 GigabitEthernet0/0/2 接口已经成为根端口

查看当前 STP 状态信息

```
[S4]display stp
-------[CIST Global Info][Mode STP]-------
CIST Bridge             :32768.4c1f-cc10-5913
Config Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC          :0       .4c1f-cc33-7359 / 40000          //根路径开销为 20000+20000=40000
CIST RegRoot/IRPC       :32768.4c1f-cc10-5913 / 0
CIST RootPortId         :128.2
BPDU-Protection         :Disabled
TC or TCN received      :146
TC count per hello      :0
STP Converge Mode       :Normal
Time since last TC      :0 days 0h:2m:25s
Number of TC            :20
Last TC occurred        :GigabitEthernet0/0/2
```

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

```
[S2]stp mode rstp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S3]stp mode rstp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S4]stp mode rstp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

查看设备上的生成树状态，仅以 S1 为例

```
[S1]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge             :0       .4c1f-cc33-7359
Config Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC          :0       .4c1f-cc33-7359 / 0
CIST RegRoot/IRPC       :0       .4c1f-cc33-7359 / 0
CIST RootPortId         :0.0
BPDU-Protection         :Disabled
CIST Root Type          :Primary root
TC or TCN received      :89
TC count per hello      :0
STP Converge Mode       :Normal
Time since last TC      :0 days 0h:0m:44s
```

```
Number of TC                :27
Last TC occurred            :GigabitEthernet0/0/11
```

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

```
[S3]interface range GigabitEthernet 0/0/10 to GigabitEthernet 0/0/24
```

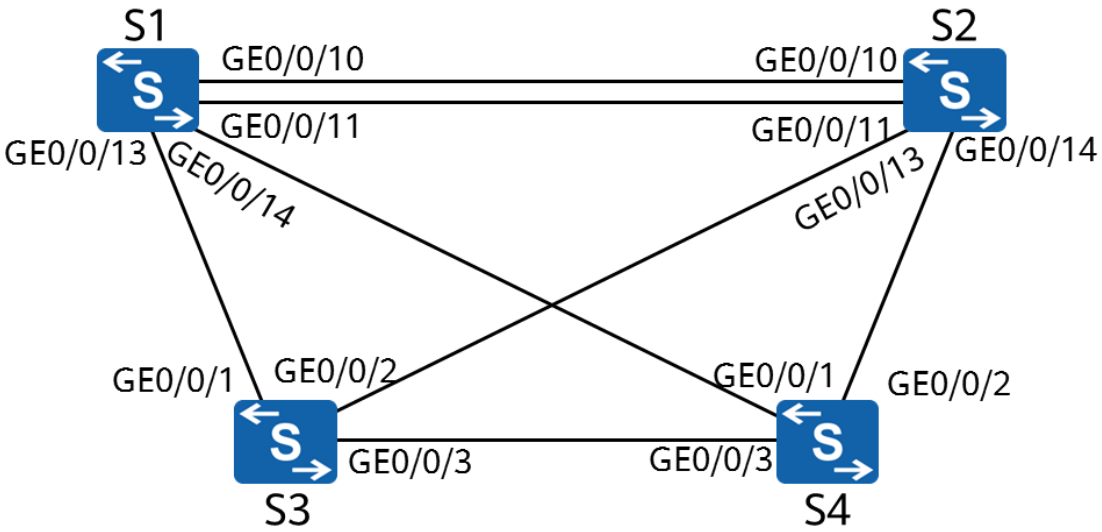
通常，设备的以太网接口数比较多，并且在很多以太网接口下有相同的配置。如果对这些以太网接口进行逐个配置会较为繁琐，且容易输入错误。因此，将需要执行相同配置命令的以太网接口加入到一个临时端口组，在临时端口组配置命令时，系统会自动到临时端口组绑定的所有成员接口下执行这些命令行，完成以太网接口批量配置。
注：某些产品上可能不支持临时接口组，需要对接口做单独配置。

```
[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。

3.2.3 结果验证

1）请根据实际收敛情况，标识出当前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他所有交换机。

3.2.4 配置参考

S1 的配置

```
#
```

```
sysname S1
#
stp mode rstp
stp instance 0 root primary
#
interface GigabitEthernet0/0/12
 shutdown
#
return
```

S2 的配置

```
#
sysname S2
#
stp mode rstp
stp instance 0 root secondary
#
interface GigabitEthernet0/0/12
 shutdown
#
return
```

S3 的配置

```
#
sysname S3
#
stp mode rstp
#
interface GigabitEthernet0/0/10
 stp edged-port enable
#
interface GigabitEthernet0/0/11
 stp edged-port enable
#
interface GigabitEthernet0/0/12
 stp edged-port enable
#
interface GigabitEthernet0/0/13
 stp edged-port enable
#
interface GigabitEthernet0/0/14
 stp edged-port enable
#
interface GigabitEthernet0/0/15
 stp edged-port enable
#
interface GigabitEthernet0/0/16
 stp edged-port enable
#
interface GigabitEthernet0/0/17
 stp edged-port enable
#
interface GigabitEthernet0/0/18
 stp edged-port enable
#
```

```
interface GigabitEthernet0/0/19
 stp edged-port enable
#
interface GigabitEthernet0/0/20
 stp edged-port enable
#
interface GigabitEthernet0/0/21
 stp edged-port enable
#
interface GigabitEthernet0/0/22
 stp edged-port enable
#
interface GigabitEthernet0/0/23
 stp edged-port enable
#
interface GigabitEthernet0/0/24
 stp edged-port enable
#
return
```

S4 的配置

```
#
sysname S4
#
stp mode rstp
#
interface GigabitEthernet0/0/1
 stp instance 0 cost 5000
#
return
```

3.2.5 思考题

1. 步骤 3 中，若修改 S1 的 GigabitEthernet 0/0/14 接口的 cost 值为 50000，是否能达到相应的效果？为什么？

2. 在当前拓扑下，请尝试通过修改配置使得 S2 的 GigabitEthernet0/0/11 口成为根端口。

3. S1 与 S2 之间的两条链路能否同时处于转发状态？为什么？

3.3 实验三：以太网链路聚合实验

3.3.1 实验介绍

3.3.1.1 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，流量可以切换到其他可用的成员链路上，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。

3.3.1.2 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

3.3.1.3 实验组网介绍

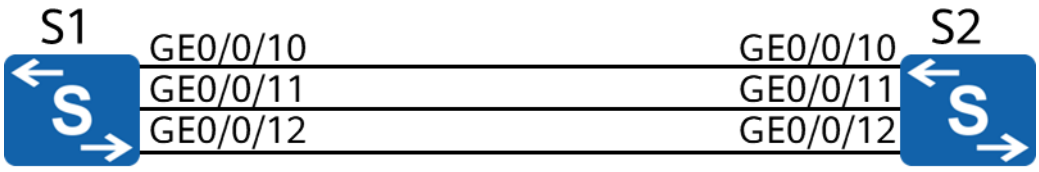


图3-3 以太网链路聚合实验拓扑

3.3.1.4 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。

3.3.2 实验任务配置

3.3.2.1 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

3.3.2.2 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
```

mode命令用来配置Eth-Trunk的工作模式，有LACP模式和手工负载分担模式（手工模式）两种，缺省情况下，Eth-Trunk的工作模式为手工负载分担模式。此处S1上的模式配置仅为示范目的，实际操作时不需要。

将成员接口加入聚合组

```
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1-GigabitEthernet0/0/10]quit
[S1]interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]eth-trunk 1
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1-GigabitEthernet0/0/11]quit
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]eth-trunk 1
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1-GigabitEthernet0/0/12]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 Eth-Trunk 1
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

将成员接口加入Eth-Trunk时，需要注意以下问题：

- 每个Eth-Trunk接口下最多可以包含8个成员接口。
- 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。
- 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。
- 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。
- Eth-Trunk链路两端相连的物理接口的数量、速率、双工方式等必须一致。

查看 Eth-Trunk 接口状态

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL              Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1       Max Bandwidth-affected-linknumber: 32
Operate status: up               Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
PortName                         Status      Weight
GigabitEthernet0/0/10            Up          1
GigabitEthernet0/0/11            Up          1
GigabitEthernet0/0/12            Up          1
```

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 GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]undo trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

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
```

mode lacp 指定Eth-Trunk工作模式为LACP模式。
注：部分版本的设备命令为 mode lacp-static

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

将成员接口加入聚合组

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

查看 Eth-Trunk 接口状态

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay: Disabled           Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768            System ID: 4c1f-cc33-7359
Least Active-linknumber: 1        Max Active-linknumber: 8
Operate status: up                Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
ActorPortName          Status     PortType  PortPri  PortNo PortKey PortState Weight
GigabitEthernet0/0/10  Selected   1GE       32768    11     305     10111100  1
GigabitEthernet0/0/11  Selected   1GE       32768    12     305     10111100  1
GigabitEthernet0/0/12  Selected   1GE       32768    13     305     10111100  1

Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri     SystemID        PortPri  PortNo PortKey PortState
GigabitEthernet0/0/10  32768      4c1f-ccc1-4a02  32768    11     305     10111100
GigabitEthernet0/0/11  32768      4c1f-ccc1-4a02  32768    12     305     10111100
GigabitEthernet0/0/12  32768      4c1f-ccc1-4a02  32768    13     305     10111100
```

步骤 3 考虑到网络流量情况，当网络正常时，只需要 GigabitEthernet0/0/11 和 GigabitEthernet0/0/12 接口处于转发状态，GigabitEthernet0/0/10 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 GigabitEthernet0/0/11 和 GigabitEthernet0/0/12 接口

```
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]lacp priority 40000
```

使能了LACP模式链路聚合的两端设备均会收发的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。
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]max active-linknumber 2
[S1-Eth-Trunk1]least active-linknumber 2
```

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。**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
```

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:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay Time: 30            Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100              System ID: 4c1f-cc33-7359
Least Active-linknumber: 2        Max Active-linknumber: 2
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName           Status     PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/10   Unselect   1GE      40000   11     305     10100000  1
GigabitEthernet0/0/11   Selected   1GE      32768   12     305     10111100  1
GigabitEthernet0/0/12   Selected   1GE      32768   13     305     10111100  1

Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri   SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/10   32768    4c1f-ccc1-4a02  32768   11     305     10110000
GigabitEthernet0/0/11   32768    4c1f-ccc1-4a02  32768   12     305     10111100
GigabitEthernet0/0/12   32768    4c1f-ccc1-4a02  32768   13     305     10111100
```

当前 GigabitEthernet0/0/11 和 GigabitEthernet0/0/12 处于激活状态。

手工关闭 GigabitEthernet0/0/12 模拟链路故障

```
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
```

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay Time: 30            Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100              System ID: 4c1f-cc33-7359
Least Active-linknumber: 2        Max Active-linknumber: 2
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName           Status     PortType PortPri PortNo  PortKey  PortState  Weight
GigabitEthernet0/0/10   Selected   1GE      40000   11      305      10111100   1
GigabitEthernet0/0/11   Selected   1GE      32768   12      305      10111100   1
GigabitEthernet0/0/12   Unselect   1GE      32768   13      305      10100010   1

Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri     SystemID        PortPri  PortNo  PortKey  PortState
GigabitEthernet0/0/10   32768      4c1f-ccc1-4a02  32768    11      305      10111100
GigabitEthernet0/0/11   32768      4c1f-ccc1-4a02  32768    12      305      10111100
GigabitEthernet0/0/12   0          0000-0000-0000  0        0       0        10100011
```

GigabitEthernet 0/0/10 已经转为激活状态。

再手工关闭 GigabitEthernet 0/0/11 模拟链路故障

```
[S1]interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]shutdown
```

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay Time: 30            Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100              System ID: 4c1f-cc33-7359
Least Active-linknumber: 2        Max Active-linknumber: 2
Operate status: down              Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName           Status     PortType PortPri PortNo  PortKey  PortState  Weight
GigabitEthernet0/0/10   Unselect   1GE      40000   11      305      10100000   1
GigabitEthernet0/0/11   Unselect   1GE      32768   12      305      10100010   1
GigabitEthernet0/0/12   Unselect   1GE      32768   13      305      10100010   1

Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri     SystemID        PortPri  PortNo  PortKey  PortState
GigabitEthernet0/0/10   32768      4c1f-ccc1-4a02  32768    11      305      10110000
GigabitEthernet0/0/11   0          0000-0000-0000  0        0       0        10100011
GigabitEthernet0/0/12   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GigabitEthernet0/0/10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]inter GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]undo shutdown
[S1-GigabitEthernet0/0/11]quit
[S1]inter GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]undo shutdown
```

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:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay Time: 30            Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100              System ID: 4c1f-cc33-7359
Least Active-linknumber: 2        Max Active-linknumber: 2
Operate status: down              Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName            Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/10    Unselect 1GE      40000   11     305     10100000  1
GigabitEthernet0/0/11    Selected 1GE      32768   12     305     10100010  1
GigabitEthernet0/0/12    Selected 1GE      32768   13     305     10100010  1

Partner:
--------------------------------------------------------------------------------
ActorPortName            SysPri   SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/10    32768    4c1f-ccc1-4a02  32768   11     305     10110000
GigabitEthernet0/0/11    0        0000-0000-0000  0       0      0       10100011
GigabitEthernet0/0/12    0        0000-0000-0000  0       0      0       10100011
```

由于使能了Eth-Trunk接口的抢占功能，所以当GigabitEthernet0/0/11和GigabitEthernet0/0/12接口进入UP状态之后，这两个接口的接口的优先级高于GigabitEthernet0/0/10，所以GigabitEthernet0/0/10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
```

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。

3.3.3 结果验证

略。

3.3.4 配置参考

S1 的配置

```
#
sysname S1
#
lacp priority 100
#
interface Eth-Trunk1
 mode lacp
 least active-linknumber 2
 load-balance dst-ip
 lacp preempt enable
 max active-linknumber 2
#
interface GigabitEthernet0/0/10
 eth-trunk 1
 lacp priority 40000
#
interface GigabitEthernet0/0/11
 eth-trunk 1
#
interface GigabitEthernet0/0/12
 eth-trunk 1
#
return
```

S2 的配置

```
#
sysname S2
#
interface Eth-Trunk1
 mode lacp
#
interface GigabitEthernet0/0/10
 eth-trunk 1
#
interface GigabitEthernet0/0/11
 eth-trunk 1
#
interface GigabitEthernet0/0/12
 eth-trunk 1
#
return
```

3.3.5 思考题

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

3.4 实验四：实现 VLAN 间通信实验

3.4.1 实验介绍

3.4.1.1 关于本实验

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。

3.4.1.2 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

3.4.1.3 实验组网介绍

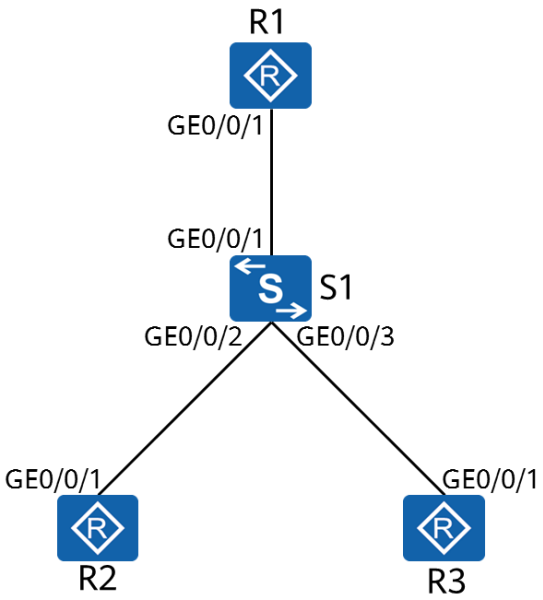


图3-4 实现 VLAN 间通信实验拓扑

1. R2 和 R3 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. R2 和 R3 的网关地址分别为 192.168.2.254 和 192.168.3.254。
3. 在 S1 上将 GigabitEthernet0/0/2 和 GigabitEthernet0/0/3 分别划入 VLAN2 和 VLAN3。

3.4.1.4 实验背景

R2 和 R3 处于不同的 VLAN，现要求通过 VLANIF 接口和 Dot1q 终结子接口分别实现 R2 与 R3 之间的互访需求。

3.4.2 实验任务配置

3.4.2.1 配置思路

1. 配置 Dot1q 终结子接口方法实现 VLAN 间互访
2. 配置 VLANIF 接口方法实现 VLAN 间互访

3.4.2.2 配置步骤

步骤 1　设备基础配置

给 R1、R2、R3 和 S1 命名

略。

R2 和 R3 的 IP 地址及网关配置

```
<R2> system-view
Enter system view, return user view with Ctrl+Z.
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 192.168.2.1 24
[R2-GigabitEthernet0/0/1]quit
[R2]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。

```
<R3>system-view
Enter system view, return user view with Ctrl+Z.
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 192.168.3.1 24
[R3-GigabitEthernet0/0/1]quit
[R3]ip route-static 0.0.0.0 0 192.168.3.254
```

在 S1 上对 R2 和 R3 进行 VLAN 划分

```
[S1]vlan batch 2 3
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type access
[S1-GigabitEthernet0/0/2]port default vlan 2
[S1-GigabitEthernet0/0/2]quit
[S1]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 3
```

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 GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
```

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 VLAN2 和 VLAN3 通过。

在 R1 上创建并配置 Dot1q 终结子接口

```
[R1]interface GigabitEthernet 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-GigabitEthernet0/0/1.2]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GigabitEthernet0/0/1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-GigabitEthernet0/0/1.2]arp broadcast enable
```

终结子接口不能转发广播报文，在收到广播报文后它们直接把该报文丢弃。为了允许终结子接口能转发广播报文，可以通过在子接口上执行命令**arp broadcast enable**使能终结子

接口的ARP广播功能。部分设备默认使能该功能，此命令的配置根据设备而定。

```
[R1-GigabitEthernet0/0/1.2]ip address 192.168.2.254 24
[R1-GigabitEthernet0/0/1.2]quit
[R1]interface GigabitEthernet 0/0/1.3
[R1-GigabitEthernet0/0/1.3]dot1q termination vid 3
[R1-GigabitEthernet0/0/1.3]arp broadcast enable
[R1-GigabitEthernet0/0/1.3]ip address 192.168.3.254 24
[R1-GigabitEthernet0/0/1.3]quit
```

检测 VLAN 间互访联通性

```
<R2>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

<R2>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 VLAN2 和 VLAN3 之间已经可以正常的互访。

步骤 3 通过 VLANIF 接口实现 VLAN 间互访

清除上一步配置

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port trunk allow-pass vlan 2 3
[S1-GigabitEthernet0/0/1]undo port link-type
```

```
[R1]undo interface GigabitEthernet 0/0/1.2
[R1]undo interface GigabitEthernet 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 间互访联通性

```
<R2>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

<R2>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 VLAN2 和 VLAN3 之间已经可以正常的互访。

3.4.3 结果验证

略。

3.4.4 配置参考

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 GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/3
```

```
 port link-type access
 port default vlan 3
#
return
```

R2 的配置

```
#
 sysname R2
#
interface GigabitEthernet0/0/1
 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
#
return
```

R3 的配置

```
#
 sysname R3
#
interface GigabitEthernet0/0/1
 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
#
return
```

3.4.5 思考题

1. 若 R2 想要访问 R1 所相连的网络，在 S1 上还需要做什么配置?
2. VLANIF 接口作为一个三层接口存在在设备上，那什么情况下接口会处于 UP 状态?

4 网络安全基础与网络接入

4.1 实验一：访问控制列表配置实验

4.1.1 实验介绍

4.1.1.1 关于本实验

访问控制列表 ACL（Access Control List）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。

4.1.1.2 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

4.1.1.3 实验组网介绍

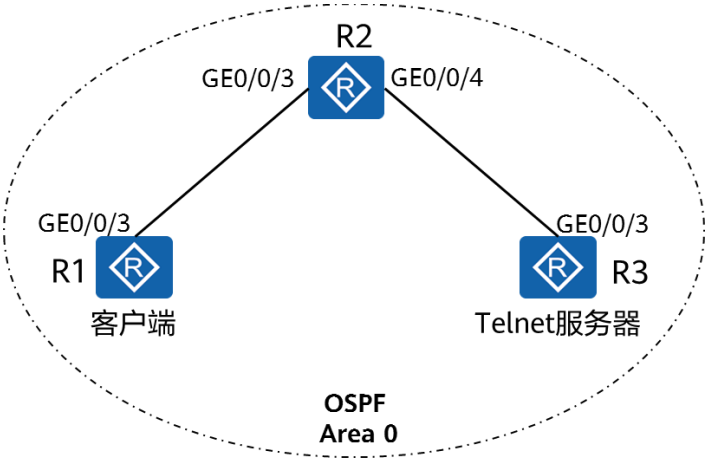


图4-1 ACL 配置实验拓扑

4.1.1.4 实验背景

如组网图所示，R3 为服务器，R1 为客户端，客户端与服务器之间路由可达。其中 R1 和 R2 间互联物理接口地址分别为 10.1.2.1/24 和 10.1.2.2/24，R2 和 R3 间互联物理接口地址分别为

10.1.3.2/24 和 10.1.3.1/24。另外，R1 上创建两个逻辑接口 LoopBack 0 和 LoopBack 1 分别模拟两个客户端用户，地址分别为 10.1.1.1/24 和 10.1.4.1/24。

其中一个用户（R1 的 LoopBack 1 接口）需要远程管理设备 R3，可以在服务器端配置 Telnet，用户通过密码登录，并配置基于 ACL 的安全策略，保证只有符合安全策略的用户才能登录设备。

4.1.2 实验任务配置

4.1.2.1 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

4.1.2.2 配置步骤

步骤 1　配置设备 IP 地址

配置 R1、R2 和 R3 的 IP 地址

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.1.2.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 10.1.1.1 24
[R1-LoopBack0]quit
[R1]interface LoopBack 1
[R1-LoopBack1]ip address 10.1.4.1 24
[R1-LoopBack0]quit
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.1.2.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.1.3.2 24
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 10.1.3.1 24
[R3-GigabitEthernet0/0/3]quit
```

步骤 2　配置 OSPF 使网络互通

在 R1、R2 和 R3 上配置 OSPF，三台设备均在区域 0 中，实现全网互联互通

```
[R1]ospf
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.1.2.1 0.0.0.0
```

```
[R1-ospf-1-area-0.0.0.0]network 10.1.4.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]return
```

```
[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.1.2.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.1.3.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]return
```

```
[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.1.3.1 0.0.0.0
[R3-ospf-1-area-0.0.0.0]return
```

在 R3 上执行 Ping 命令，检测网络的连通性

```
<R3>ping 10.1.1.1
  PING 10.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=254 time=40 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=254 time=20 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=40 ms
    Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms
  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/34/40 ms
```

```
<R3>ping 10.1.2.1
  PING 10.1.2.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.2.1: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 10.1.2.1: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 10.1.2.1: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 10.1.2.1: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.1.2.1: bytes=56 Sequence=5 ttl=254 time=50 ms
  --- 10.1.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/34/50 ms
```

```
<R3>ping 10.1.4.1
  PING 10.1.4.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.4.1: bytes=56 Sequence=1 ttl=254 time=50 ms
    Reply from 10.1.4.1: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 10.1.4.1: bytes=56 Sequence=3 ttl=254 time=40 ms
    Reply from 10.1.4.1: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.1.4.1: bytes=56 Sequence=5 ttl=254 time=30 ms
  --- 10.1.4.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
    0.00% packet loss
    round-trip min/avg/max = 30/36/50 ms
```

步骤 3 配置 R3 为 Telnet 服务器

在 R3 使能 Telnet 功能，配置用户权限等级为 3 级，登录密码为 Huawei@123

```
[R3]telnet server enable
```

telnet server enable命令用来使能Telnet服务器。

```
[R3]user-interface vty 0 4
```

user-interface命令用来进入一个用户界面视图或多个用户界面视图。
VTY（Virtual Type Terminal）用户界面，用来管理和监控通过Telnet或SSH方式登录的用户。

```
[R3-ui-vty0-4]user privilege level 3
[R3-ui-vty0-4] set authentication password cipher
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa"
authentication mode.
Enter Password(<8-128>):Huawei@123
Confirm password:Huawei@123
[R3-ui-vty0-4] quit
```

步骤 4 配置 ACL 进行流量过滤

方式一：在 R3 的 VTY 接口匹配 ACL，允许 R1 通过 LoopBack 1 口地址 Telnet 到 R3。

在 R3 上配置 ACL

```
[R3]acl 3000
[R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R3-acl-adv-3000]rule 10 deny tcp source any
[R3-acl-adv-3000]quit
```

在 R3 的 VTY 接口上进行流量过滤

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]acl 3000 inbound
```

在 R3 上查看 ACL 配置信息

```
[R3]display acl 3000
```

display acl命令用来查看ACL的配置信息。

```
Advanced ACL 3000, 2 rules
```

高级访问控制列表，序号为3000，共2条规则。

```
Acl's step is 5
```

ACL的步长为5。

```
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
```

规则5，允许特定的流量通过，当没有匹配的报文时，不显示matches字段。

```
rule 10 deny tcp
```

方式二：在 R2 的物理接口匹配 ACL，只允许 R1 通过物理接口地址 Telnet 到 R3。

在 R2 上配置 ACL

```
[R2]acl 3001
[R2-acl-adv-3001]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3001]rule 10 deny tcp source any
[R2-acl-adv-3001]quit
```

在 R2 的 GE0/0/3 接口上进行流量过滤

```
[R2]interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3]traffic-filter inbound acl 3001
```

在 R2 上查看 ACL 配置信息

```
[R2]display acl 3001
Advanced ACL 3001, 2 rules
Acl's step is 5
rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet (21 matches)
```

规则5，允许特定的流量通过，匹配的报文数目为21。

```
rule 10 deny tcp (1 matches)
```

4.1.3 结果验证

检测 Telnet 访问，验证 ACL 配置结果

1）在 R1 上带源地址 10.1.1.1 telnet 到服务器。

```
<R1>telnet -a 10.1.1.1 10.1.3.1
```

telnet命令用来从当前设备使用Telnet协议登录到其它设备。

-a s*ource-ip-address* ： 通过指定源地址，用户可以用指定的IP地址与服务端通信。

```
  Press CTRL_] to quit telnet mode
  Trying 10.1.3.1 ...
  Error: Can't connect to the remote host
```

2）在 R1 上带源地址 10.1.4.1 telnet 到服务器。

```
<R1>telnet -a 10.1.4.1 10.1.3.1
  Press CTRL_] to quit telnet mode
  Trying 10.1.3.1 ...
  Connected to 10.1.3.1 ...

Login authentication

Password:
<R3>quit
```

4.1.4 配置参考（方式一）

R1 的配置

```
#
 sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.1.4.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 10.1.2.1 0.0.0.0
  network 10.1.4.1 0.0.0.0
#
return
```

R2 的配置

```
#
 sysname R2
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet0/0/4
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.2 0.0.0.0
  network 10.1.3.2 0.0.0.0
#
return
```

R3 的配置

```
#
 sysname R3
#
acl number 3000
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
```

```
   network 10.1.3.1 0.0.0.0
#
 telnet server enable
#
user-interface vty 0 4
 acl 3000 inbound
 authentication-mode password
 user privilege level 3
 set authentication password
cipher %^%#Z5)H#8cE(YJ6YZ:='}c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#
#
return
```

4.1.5 配置参考（方式二）

R1 的配置

```
#
 sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.1.4.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 10.1.2.1 0.0.0.0
  network 10.1.4.1 0.0.0.0
#
return
```

R2 的配置

```
#
 sysname R2
#
acl number 3001
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.2 255.255.255.0
traffic-filter inbound acl 3001
#
interface GigabitEthernet0/0/4
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
```

```
 area 0.0.0.0
   network 10.1.2.2 0.0.0.0
   network 10.1.3.2 0.0.0.0
#
return
```

R3 的配置

```
#
 sysname R3
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
   network 10.1.3.1 0.0.0.0
#
 telnet server enable
#
user-interface vty 0 4
authentication-mode password
 user privilege level 3
 set authentication password
cipher %^%#Z5)H#8cE(YJ6YZ:='}c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#
#
return
```

4.1.6 思考题与附加内容

仍使用实验组网图，若 R3 同时为 Telnet 服务器和 FTP 服务器，现要求客户端 R1 的 LoopBack 0 接口地址只能够访问 FTP 服务，R1 的 LoopBack 1 接口地址只能够进行 Telnet 对 R3 进行远程管理。

请通过配置 ACL，完成上述要求。

4.2 实验二：本地 AAA 配置实验

4.2.1 实验介绍

4.2.1.1 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 用户进行资源管控。

4.2.1.2 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

4.2.1.3 实验组网介绍

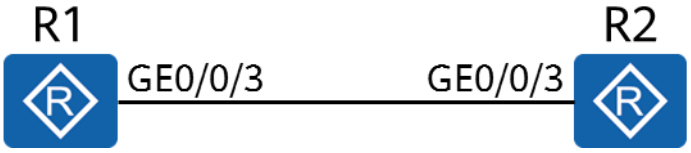


图4-2 本地 AAA 配置实验拓扑

4.2.1.4 实验背景

R1 模拟一台客户端设备，R2 为一台网络设备。现在需要在 R2 上对管理 R2 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 R1 和 R2 两台路由器上配置本地 AAA 认证，并基于域来对用户进行管理，并配置已认证用户的权限级别。

4.2.2 实验任务配置

4.2.2.1 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

4.2.2.2 配置步骤

步骤 1 设备基础配置

给 R1 和 R2 命名

略。

配置 R1 和 R2 互联的 IP 地址

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
```

步骤 2 配置 AAA 方案

配置认证、授权方案

```
[R2-aaa]aaa
```

进入 AAA 视图。

```
[R2-aaa]authentication-scheme datacom
Info: Create a new authentication scheme.
```

创建名为 datacom 的认证方案。

```
[R2-aaa-authen-datacom]authentication-mode local
```

设置认证方案的认证方式为本地认证。

```
[R2-aaa-authen-datacom]quit
[R2-aaa]authorization-scheme datacom
Info: Create a new authorization scheme.
```

创建名为 datacom 的授权方案。

```
[R2-aaa-author-datacom]authorization-mode local
```

设置授权方案的授权方式为本地授权。

```
[R2-aaa-author-datacom]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

```
[R2]aaa
[R2-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。

```
[R2-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。

```
[R2-aaa-domain-datacom]authorization-scheme datacom
```

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

```
[R2-aaa]local-user hcia@datacom password cipher HCIA-Datacom
Info: Add a new user.
```

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

```
[R2-aaa]local-user hcia@datacom service-type telnet
```

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。

```
[R2-aaa]local-user hcia@datacom privilege level 3
```

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 R2 上的 telnet 功能

```
[R2]telnet server enable
```

开启设备的 telnet 服务器功能，部分设备默认开启，可能会报错。

```
[R2]user-interface vty 0 4
[R2-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。

步骤 6 检验配置效果

从 R1 远程 Telnet 访问 R2

```
<R1>telnet 10.0.12.2
  Press CTRL_] to quit telnet mode
  Trying 10.0.12.2 ...
  Connected to 10.0.12.2 ...

Login authentication



Username:hcia@datacom
Password:
<R2>
```

此时 R1 已经登录到 R2 上

在 R2 上查看登录的用户

```
[R2]display users
  User-Intf        Delay      Type   Network Address      AuthenStatus    AuthorcmdFlag
  129 VTY 0        00:02:43   TEL    10.0.12.1                 pass
  Username : hcia@datacom
```

4.2.3 结果验证

略。

4.2.4 配置参考

R1 的配置

```
#
 sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
#
return
```

R2 的配置

```
#
 sysname R2
#
aaa
 uthentication-scheme datacom
authorization-scheme datacom
 domain datacom
  authentication-scheme datacom
  authorization-scheme datacom
 local-user hcia@datacom password irreversible-
cipher %^%#.}hB'1"=&=:FWx!Ust(3s^_<.[Z}kEc/>==P56gUVU*cE^|]5@|8/O5FC$9A%^%#
 local-user hcia@datacom privilege level 3
```

```
 local-user hcia@datacom service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
#
 telnet server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```

4.2.5 思考题

略。

4.3 实验三：网络地址转换配置实验

4.3.1 实验介绍

4.3.1.1 关于本实验

网络地址转换 NAT（Network Address Translation）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。

4.3.1.2 实验目的

- 掌握动态 NAT 的配置方法
- 掌握 Easy IP 的配置方法
- 掌握 NAT Server 的配置方法

4.3.1.3 实验组网介绍

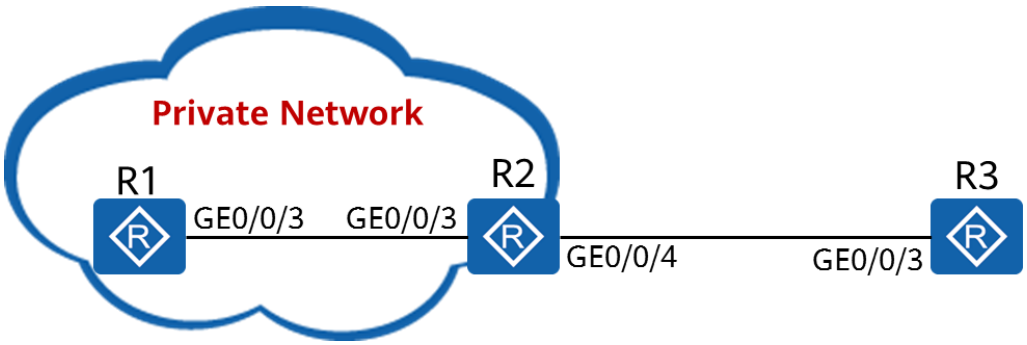


图4-3 网络地址转换配置实验拓扑

1. R1 和 R2 之间的网络属于企业内部网络，使用私网 IPv4 地址。
2. R1 模拟客户端，R2 作为 R1 的网关，同时也是连接公网的出口路由器。
3. R3 模拟公网。

4.3.1.4 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。

4.3.2 实验任务配置

4.3.2.1 配置思路

1. 配置动态 NAT
2. 配置 Easy IP
3. 配置 NAT Server

4.3.2.2 配置步骤

步骤 1 基本配置

接口 IP 地址和路由配置

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 192.168.1.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]ip route-static 0.0.0.0 0 192.168.1.254
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 192.168.1.254 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 1.2.3.4 24
[R2-GigabitEthernet0/0/4]quit
[R2]ip route-static 0.0.0.0 0 1.2.3.254
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ip address 1.2.3.254 24
```

配置 R1 和 R3 的 telnet 功能（用于后续实验验证）

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
[R1-ui-vty0-4]quit
[R1]aaa
[R1-aaa]local-user test password irreversible-cipher Huawei@123
Info: Add a new user.
[R1-aaa]local-user test service-type telnet
[R1-aaa]local-user test privilege level 15
```

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode aaa
[R3-ui-vty0-4]quit
[R3]aaa
[R3-aaa]local-user test password irreversible-cipher Huawei@123
Info: Add a new user.
[R3-aaa]local-user test service-type telnet
[R3-aaa]local-user test privilege level 15
[R3-aaa]quit
```

测试当前联通性

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

```
[R2]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/24/40 ms
```

因为当前R3没有配置到192.168.1.0/24网段的路由，R1无法访问R3。
实际情况下，R3也禁止配置到私网IP网段的路由。

步骤 2 假设该公司获得了 1.2.3.10 至 1.2.3.20 这段公网 IP，现需要配置动态 NAT

配置 NAT 地址池

```
[R2]nat address-group 1 1.2.3.10 1.2.3.20
```

nat address-group命令用来配置NAT地址池。1代表地址池的编号，地址池必须是一段连续的IP地址集合，当内部数据报文通过地址转换到达外部网络时，其源地址将被地址池转换为其他地址。

配置 ACL

```
[R2]acl 2000
[R2-acl-basic-2000]rule 5 permit source any
```

在 R2 的 GigabitEthernet0/0/4 接口配置动态 NAT

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]nat outbound 2000 address-group 1
```

nat outbound命令用来将一个访问控制列表ACL和一个地址池关联起来，符合ACL中规定的

地址可以使用地址池进行地址转换。当地址池中地址的数量足够时，可以添加**no-pat**参数，表示使用一对一的地址转换，只转换数据报文的地址而不转换端口信息。

测试联通性

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=20 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 20/32/60 ms
```

R1 通过 telnet 远程登录到 R3（模拟 TCP 流量）

```
<R1>telnet 1.2.3.254
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.254 ...
  Connected to 1.2.3.254 ...

Login authentication


Username:test
Password:
<R3>
```

查看 R2 上的 NAT 会话表

```
[R2]display nat session all
    NAT Session Table Information:
        Protocol               : TCP(6)
        SrcAddr    Port Vpn    : 192.168.1.1      62185          //转换前的源 IP 地址和源端口
        DestAddr Port Vpn      : 1.2.3.254        23
        NAT-Info
        New SrcAddr            : 1.2.3.11                  //转换后的源 IP 地址
        New SrcPort            : 49149                     //转换后的源端口
        New DestAddr           : ----
        New DestPort           : ----

  Total : 1
```

尽管此时R3没有到R1的路由条目，但是由于转换后的源地址为1.2.3.11，R3会将数据回复给该地址，R2收到后会根据NAT会话表中的数据重新转换为R1的地址并转发。所以此时R1可以**主动发起**到R3的访问。

步骤 3 假设 R2 的 GigabitEthernet0/0/4 的地址不是固定 IP 地址（DHCP 动态获取或 PPPoE 拨号获取），此时需要配置 Easy IP

删除上一步骤的配置

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]undo nat outbound 2000 address-group 1
```

配置 Easy IP

```
[R2-GigabitEthernet0/0/4]nat outbound 2000
```

测试联通性

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/30/30 ms
```

R1 通过 telnet 远程登录到 R3（模拟 TCP 流量）

```
[R2]display nat session all
 NAT Session Table Information:
     Protocol          : TCP(6)
     SrcAddr    Port Vpn     : 192.168.1.1      58546          //转换前的源 IP 地址和源端口
     DestAddr Port Vpn     : 1.2.3.4      23
     NAT-Info
     New SrcAddr       : 1.2.3.4          //转换后的源 IP 地址，R2 的 GigabitEthernet 0/0/4 的 IP 地址
     New SrcPort       : 49089            //转换后的源端口
     New DestAddr      : ----
     New DestPort      : ----

  Total : 1
```

步骤 4 假设 R3 要向公网提供网络服务（用 telnet 模拟），由于 R3 没有公网 IP 地址，故需要在 R2 的出接口上配置 NAT Server

在 R2 上配置 NAT Server

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4] nat server protocol tcp global current-interface 2323 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。配置内部服务器可以使外部网络**主动**访问私网中的服务器。当外部网络向内部服务器的外部地址（global-address）发起连接请求时，NAT将该请求的

目的地址替换为私网地址（inside-address）后，转发给私网内的服务器。

R3 通过 telnet 远程登录到 R1

```
<R3>telnet 1.2.3.4 2323
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.4 ...
  Connected to 1.2.3.4 ...

Login authentication


Username:test
Password:
<R1>
```

查看 R2 上的 NAT 会话表

```
[R2]display nat session all
        Protocol               : TCP(6)
        SrcAddr    Port Vpn    : 1.2.3.254      61359
        DestAddr Port Vpn      : 1.2.3.4        2323          //转换前的目的 IP 地址和目的端口
        NAT-Info
        New SrcAddr            : ----
        New SrcPort            : ----
        New DestAddr           : 192.168.1.1          //转换后的目的 IP 地址，R1 的地址
        New DestPort           : 23                   //转换后的目的端口

  Total : 1
```

4.3.3 结果验证

略。

4.3.4 配置参考

R1 的配置

```
#
 sysname R1
#
aaa
local-user test password irreversible-
cipher %^%#y'BJ=em]VY(E%IH!+,f~[|n*'L`HU#H=vlVzMJR'^+^U3qWRm%&:Kd't7oI$%^%#
 local-user test privilege level 3
 local-user test service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 192.168.1.1 255.255.255.0
#
 telnet server enable
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
```

```
user-interface vty 0 4
 authentication-mode aaa
#
return
```

R2 的配置

```
#
 sysname R2
#
acl number 2000
 rule 5 permit
#
 nat address-group 1 1.2.3.10 1.2.3.20
#
interface GigabitEthernet0/0/3
 ip address 192.168.1.254 255.255.255.0
#
interface GigabitEthernet0/0/4
 ip address 1.2.3.4 255.255.255.0
 nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
 nat outbound 2000
#
return
```

R3 的配置

```
#
 sysname R3
#
aaa
local-user test password irreversible-cipher %^%#s<LQ(8-ZC6FNGG1#)n=.GgU|@)n`Z'n%$43+2>7,I>#XBkfcu(}-
3y+o:`UD%^%#
 local-user test privilege level 15
 local-user test service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 1.2.3.254 255.255.255.0
#
 telnet server enable
#
user-interface vty 0 4
authentication-mode aaa
#
return
```

4.3.5 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?

5 基础网络服务与应用配置

5.1 实验一：FTP 基础配置实验

5.1.1 实验介绍

5.1.1.1 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。

用户可以通过直接登录系统、FTP（File Transfer Protocol）、TFTP（Trivial File Transfer Protocol）和 SFTP（Secure File Transfer Protocol）方式进行文件操作，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：

- 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。
- 设备作为客户端访问其他设备（服务器）：可以实现管理其他设备上的文件，以及与其他设备间进行文件传输操作。

5.1.1.2 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

5.1.1.3 实验组网介绍

图5-1 FTP 实验拓扑

R1 模拟 FTP Client，R2 作为 FTP Server。

5.1.1.4 实验背景

R1 需要对 R2 的配置文件进行管理。

5.1.2 实验任务配置

5.1.2.1 配置思路

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

5.1.2.2 配置步骤

步骤 1 设备基础配置

设备命名

略。

配置设备 IP 地址

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/3]quit
```

保存配置文件（用与后续验证实验效果）

```
<R1>save test1.cfg
 Are you sure to save the configuration to test1.cfg? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

```
<R2>save test2.cfg
 Are you sure to save the configuration to test2.cfg? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

查看当前的文件列表

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

  Idx  Attr      Size(Byte)      Date   Time(LMT)      FileName
    0  -rw-    126,538,240      Jul 04 2016 17:57:22  ar651c- v300r019c00Sspc100.cc
    1  -rw-         23,963      Feb 21 2020 09:22:53  mon_file.txt
    2  -rw-            721      Feb 21 2020 10:14:33  vrpcfg.zip
    3  drw-              -      Jul 04 2016 18:51:04  CPM_ENCRYPTED_FOLDER
    4  -rw-            783      Jul 10 2018 14:46:16  default_local.cer
```

```
  5   -rw-              0    Sep 11 2017 00:00:54   brdxpon_snmp_cfg.efs
  6   drw-              -    Sep 11 2017 00:01:22   update
  7   drw-              -    Sep 11 2017 00:01:48   shelldir
  8   drw-              -    Feb 20 2020 21:33:16   localuser
  9   drw-              -    Sep 15 2017 04:35:52   dhcp
 10   -rw-            509    Feb 21 2020 10:18:31   private-data.txt
 11   -rw-          2,686    Dec 19 2019 15:05:18   mon_lpu_file.txt
 12   -rw-          3,072    Dec 18 2019 18:15:54   Boot_LogFile
 13   -rw-          1,390    Feb 21 2020 10:18:30   test1.cfg

510,484 KB total available (386,448 KB free)
```

```
<R2>dir
Directory of flash:/

 Idx  Attr     Size(Byte)      Date   Time(LMT)     FileName
   0  -rw-    126,538,240    Jul 04 2016 17:57:22   ar651c- v300r019c00Sspc100.cc
   1  -rw-         11,405    Feb 21 2020 09:21:53   mon_file.txt
   2  -rw-            809    Feb 21 2020 10:14:10   vrpcfg.zip
   3  drw-              -    Jul 04 2016 18:51:04   CPM_ENCRYPTED_FOLDER
   4  -rw-            782    Jul 10 2018 14:48:14   default_local.cer
   5  -rw-              0    Oct 13 2017 15:36:32   brdxpon_snmp_cfg.efs
   6  drw-              -    Oct 13 2017 15:37:00   update
   7  drw-              -    Oct 13 2017 15:37:24   shelldir
   8  drw-              -    Feb 20 2020 20:51:34   localuser
   9  drw-              -    Oct 14 2017 11:27:04   dhcp
  10  -rw-          1,586    Feb 21 2020 10:16:51   test2.cfg
  11  -rw-            445    Feb 21 2020 10:16:52   private-data.txt
  12  -rw-          4,096    Aug 06 2019 11:19:08   Boot_LogFile

510,484 KB total available (386,464 KB free)
```

两台设备上的配置文件都已经保存成功。

步骤 2 在 R2 上配置 FTP 服务器功能及参数

```
[R2]ftp server enable
Info: Succeeded in starting the FTP server
```

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。

其他可选的配置参数还包括：指定FTP服务器端口号、指定FTP服务器的源地址和配置FTP连接空闲时间等。

步骤 3 配置本地 FTP 用户

```
[R2]aaa
[R2-aaa]local-user ftp-client password irreversible-cipher Huawei@123
Info: Add a new user.
[R2-aaa]local-user ftp-client service-type ftp
[R2-aaa]local-user ftp-client privilege level 15
```

配置FTP用户的级别，必须将用户级别配置在3级及3级以上，否则FTP连接将无法成功。

```
[R2-aaa]local-user ftp-client ftp-directory flash:/
```

配置FTP用户的授权目录，必须指定该目录，否则FTP用户无法成功登陆。

步骤 4 FTP Client 登陆 FTP Server

登陆 FTP Client

```
 <R1>ftp 10.0.12.2
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:
230 User logged in.

[R1-ftp]
```

此时已经成功登陆到 R2 的文件系统。

步骤 5 对 R2 文件系统做相应的操作

设置传输模式

```
 [R1-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，此处的操作仅为示范。

下载配置文件

```
[R1-ftp]get test2.cfg
200 Port command okay.
150 Opening ASCII mode data connection for test2.cfg.
226 Transfer complete.
FTP: 961 byte(s) received in 0.220 second(s) 4.36Kbyte(s)/sec.
```

删除配置文件

```
[R1-ftp]delete test2.cfg
Warning: The contents of file test2.cfg cannot be recycled. Continue? (y/n)[n]:y
250 DELE command successful.
```

上传配置文件

```
[R1-ftp]put test1.cfg
200 Port command okay.
150 Opening ASCII mode data connection for test1.cfg.
226 Transfer complete.
```

```
FTP: 875 byte(s) sent in 0.240 second(s) 3.64Kbyte(s)/sec.
```

断开 FTP 连接

```
[R1-ftp]bye
221 Server closing.

<R1>
```

5.1.3 结果验证

查看当前 R1 和 R2 的文件目录：

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

  Idx  Attr     Size(Byte)      Date      Time(LMT)      FileName
    0  -rw-    126,538,240      Jul 04 2016 17:57:22     ar651c- v300r019c00Sspc100.cc
    1  -rw-         23,963      Feb 21 2020 09:22:53     mon_file.txt
    2  -rw-            721      Feb 21 2020 10:14:33     vrpcfg.zip
    3  drw-              -      Jul 04 2016 18:51:04     CPM_ENCRYPTED_FOLDER
    4  -rw-            783      Jul 10 2018 14:46:16     default_local.cer
    5  -rw-              0      Sep 11 2017 00:00:54     brdxpon_snmp_cfg.efs
    6  drw-              -      Sep 11 2017 00:01:22     update
    7  drw-              -      Sep 11 2017 00:01:48     shelldir
    8  drw-              -      Feb 20 2020 21:33:16     localuser
    9  drw-              -      Sep 15 2017 04:35:52     dhcp
   10  -rw-          1,586      Feb 21 2020 10:26:10     test2.cfg
   11  -rw-            509      Feb 21 2020 10:18:31     private-data.txt
   12  -rw-          2,686      Dec 19 2019 15:05:18     mon_lpu_file.txt
   13  -rw-          3,072      Dec 18 2019 18:15:54     Boot_LogFile
   14  -rw-          1,390      Feb 21 2020 10:18:30     test1.cfg

510,484 KB total available (386,444 KB free)
```

```
<R2>dir
Directory of flash:/

  Idx  Attr     Size(Byte)      Date Time(LMT)      FileName
    0  -rw-    126,538,240      Jul 04 2016 17:57:22     ar651c- v300r019c00Sspc100.cc
    1  -rw-         11,405      Feb 21 2020 09:21:53     mon_file.txt
    2  -rw-            809      Feb 21 2020 10:14:10     vrpcfg.zip
    3  drw-              -      Jul 04 2016 18:51:04     CPM_ENCRYPTED_FOLDER
    4  -rw-            782      Jul 10 2018 14:48:14     default_local.cer
    5  -rw-              0      Oct 13 2017 15:36:32     brdxpon_snmp_cfg.efs
    6  drw-              -      Oct 13 2017 15:37:00     update
    7  drw-              -      Oct 13 2017 15:37:24     shelldir
    8  drw-              -      Feb 20 2020 20:51:34     localuser
    9  drw-              -      Oct 14 2017 11:27:04     dhcp
   10  -rw-          1,390      Feb 21 2020 10:25:42     test1.cfg
   11  -rw-            445      Feb 21 2020 10:16:52     private-data.txt
   12  -rw-          4,096      Aug 06 2019 11:19:08     Boot_LogFile

510,484 KB total available (386,464 KB free)
```

5.1.4 配置参考

R1 的配置

```
#
 sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
#
return
```

R2 的配置

```
#
 sysname R2
#
aaa
local-user ftp-client password irreversible-
cipher %^%#'XqV;f=C;/1!\sQ6LA+Ow8GBO;W%0HBf0`>p(`[SpV]J%Amom!na3:4RvFv@%^%#
 local-user ftp-client privilege level 15
 local-user ftp-client ftp-directory flash:/
 local-user ftp-client service-type ftp
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
#
 ftp server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```

5.1.5 思考题

1. FTP 默认情况下工作在主动模式还是被动模式?

5.2 实验二：DHCP 基础配置实验

5.2.1 实验介绍

5.2.1.1 关于本实验

动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）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。

5.2.1.2 实验目的

- 掌握 DHCP 接口地址池的配置方法
- 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

5.2.1.3 实验组网介绍

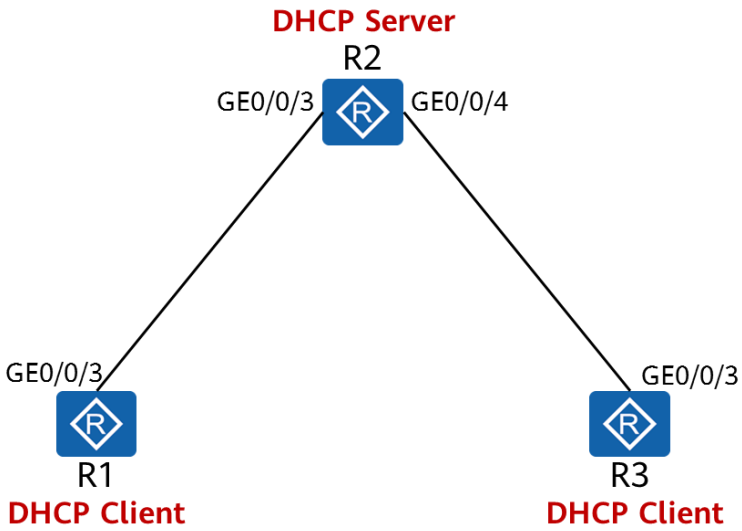


图5-2 DHCP 配置实验拓扑

1. R1 和 R3 模拟客户端，作为 DHCP Client。
2. R2 作为 DHCP Server 为 R1 和 R3 分配 IP 地址。

5.2.1.4 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，准备在网络内部部署 DHCP 协议。

5.2.2 实验任务配置

5.2.2.1 配置思路

1. 配置 DHCP 服务器
2. 配置 DHCP 客户端

5.2.2.2 配置步骤

步骤 1 基本配置

配置 R2 的接口 IP 地址

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3] ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.0.23.2 24
[R2-GigabitEthernet0/0/4]quit
```

步骤 2 开启 DHCP 功能

```
[R1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
```

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。

```
[R2]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
```

```
[R3]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
```

步骤 3 配置地址池

配置 R2 的 GigabitEthernet 0/0/3 的接口地址池，为 R1 分配 IP 地址

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]dhcp select interface
```

dhcp select interface命令用来开启接口采用接口地址池的DHCP Server功能。若不执行

此命令，则无法配置接口地址池的相关参数。

```
[R2-GigabitEthernet0/0/3]dhcp server dns-list 10.0.12.2
```

dhcp server dns-list命令用来指定接口地址池下的DNS服务器地址。最多可以配置8个DNS Server的IP地址，用空格分隔。

配置全局地址池

```
[R2]ip pool GlobalPool
Info: It's successful to create an IP address pool.
```

创建名为 GlobalPool 的地址池

```
[R2-ip-pool-GlobalPool]network 10.0.23.0 mask 24
```

network命令用来配置全局地址池下可分配的网段地址。

```
[R2-ip-pool-GlobalPool]dns-list 10.0.23.2
[R2-ip-pool-GlobalPool]gateway-list 10.0.23.2
```

gateway-list命令用来为DHCP Client配置出口网关地址。R3在获取地址之后，会生成一条默认路由，下一跳地址为10.0.23.2。

```
[R2-ip-pool-GlobalPool]lease day 2 hour 2
```

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

```
[R2-ip-pool-GlobalPool]static-bind ip-address 10.0.23.3 mac-address 00e0-fc6f-6d1f
```

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。00e0-fc6f-6d1f为当前实验环境下R3的GigabitEthernet0/0/3接口的MAC地址，可以在R3上通过命令“display interface GigabitEthernet0/0/3”来查看接口的MAC地址。配置完这条命令之后，R3会获得固定的IP--10.0.23.3。

```
[R2-ip-pool-GlobalPool]quit
```

步骤 4 开启 R2 GigabitEthernet 0/0/4 接口的 DHCP Server 功能，为 R3 分配 IP 地址

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]dhcp select global
```

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 GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3] ip address dhcp-alloc
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3] ip address dhcp-alloc
```

5.2.3 结果验证

5.2.3.1.1 查看 R1 和 R3 的地址及路由等信息

```
[R1]display ip interface brief
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/3              10.0.12.254/24       up         up
```

仅保留关键信息，可以看到 R1 已经获取到了 IP 地址。

```
[R1]display dns server
Type:
D:Dynamic         S:Static

No.    Type             IP Address
1        D              10.0.12.2
```

仅保留关键信息，可以看到 R1 已经获取到了 DNS 地址。

```
[R1]display ip routing-table
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        0.0.0.0/0   Unr     60   0         D     10.0.12.2       GigabitEthernet0/0/3
```

仅保留关键信息，可以看到 R1 已经获取到了默认路由。

```
[R3]display ip interface brief
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/3              10.0.23.3/24         up         up
```

仅保留关键信息，可以看到 R3 已经获取到了固定的 IP 地址。

```
[R3]display dns server
Type:
D:Dynamic         S:Static
No.    Type       IP Address
1        D        2.23.0.10
```

仅保留关键信息，可以看到 R3 已经获取到了 DNS 地址。

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

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        0.0.0.0/0   Unr     60   0         D     10.0.23.2       GigabitEthernet0/0/3
```

仅保留关键信息，可以看到 R3 已经获取到了默认路由。

5.2.3.1.2 查看 R2 上的地址分配情况

```
[R2]display ip pool name GlobalPool
  Pool-name                 : GlobalPool
```

```
  Pool-No              : 1
  Lease                : 2 Days 2 Hours 0 Minutes
  Domain-name          : -
  DNS-server0          : 10.0.23.2
  NBNS-server0         : -
  Netbios-type         : -
  Position             : Local              Status              : Unlocked
  Gateway-0            : 10.0.23.2
  Mask                 : 255.255.255.0
  VPN instance         : --
--------------------------------------------------------------------------------
        Start            End        Total   Used   Idle(Expired)   Conflict   Disable
--------------------------------------------------------------------------------
      10.0.23.1      10.0.23.254    253      1        252(0)          0          0
--------------------------------------------------------------------------------
```

display ip pool命令用来查看已配置的IP地址池信息。包括地址池的名称、租期、锁定状态、地址池中IP地址的状态等。

```
[R2]display ip pool interface GigabitEthernet0/0/4
  Pool-name            : GigabitEthernet0/0/4
  Pool-No              : 0
  Lease                : 1 Days 0 Hours 0 Minutes
  Domain-name          : -
  DNS-server0          : 10.0.12.2
  NBNS-server0         : -
  Netbios-type         : -
  Position             : Interface          Status              : Unlocked
  Gateway-0            : 10.0.12.2
  Mask                 : 255.255.255.0
  VPN instance         : --
--------------------------------------------------------------------------------
        Start            End          Total   Used     Idle(Expired)   Conflict   Disable
--------------------------------------------------------------------------------
      10.0.12.1      10.0.12.254      253      1        252(0)          0          0
--------------------------------------------------------------------------------
```

当配置接口地址池时，地址池的名称为接口的名称。分配的网关地址为该接口的IP地址，且无法修改。

5.2.4 配置参考

R1 的配置

```
#
 sysname R1
#
dhcp enable
#
interface GigabitEthernet0/0/3
 ip address dhcp-alloc
#
return
```

R2 的配置

```
#
 sysname R2
#
dhcp enable
#
ip pool GlobalPool
 gateway-list 10.0.23.2
 network 10.0.23.0 mask 255.255.255.0
 static-bind ip-address 10.0.23.3 mac-address a008-6fe1-0c47
 lease day 2 hour 2 minute 0
 dns-list 10.0.23.2
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
 dhcp select interface
 dhcp server dns-list 10.0.12.2
#
interface GigabitEthernet0/0/4
 ip address 10.0.23.2 255.255.255.0
 dhcp select global
#
return
```

R3 的配置

```
#
 sysname R3
#
dhcp enable
#
interface GigabitEthernet0/0/3
 ip address dhcp-alloc
#
return
```

5.2.5 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?
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?

6 构建基础 WLAN 网络

6.1 实验介绍

6.1.1 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 AC+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。

6.1.2 实验目的

- 掌握认证 AP 上线的配置方法
- 掌握各种无线配置模板配置
- 掌握 WLAN 配置的基本流程

6.1.3 实验组网介绍

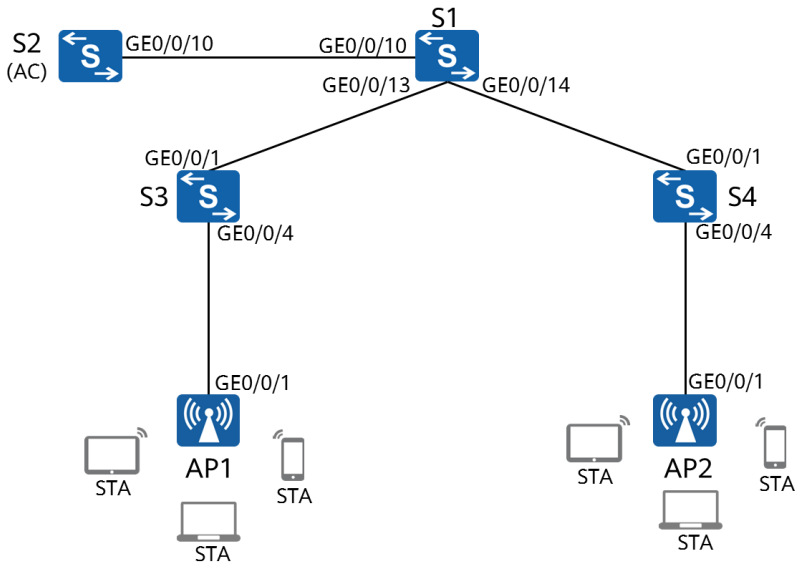


图6-1 构建基础 WLAN 网络实验拓扑

1. S2 交换机支持 WLAN-AC 功能（若实际环境所用交换机不支持，可用普通 AC 替代），作为 AC 使用（后面内容中的 AC 就是实际的 S2 交换机）。

2. AC 采用旁挂组网方式，AC 与 AP 处于同一个二层网络。

3. AC 作为 DHCP 服务器给 AP 分配 IP 地址，S1 交换机作为 DHCP 服务器给接入的 STA 分配 IP 地址。

4. 业务数据采用直接转发模式。

6.1.4 数据规划

配置项	配置参数
AP 管理 VLAN	VLAN100
STA 业务 VLAN	VLAN101
DHCP 服务器	AC 作为 DHCP 服务器为 AP 分配 IP 地址
	S1 作为 DHCP 服务器为 STA 分配 IP 地址，STA 的默认网关为 192.168.101.254
AP 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
AC 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：VLAN101
	引用模板：SSID 模板 HCIA-WLAN、安全模板 HCIA-WLAN

表6-1 AC 数据规划表

6.1.5 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。

6.2 实验任务配置

6.2.1 配置思路

1. 配置有线网络侧互联互通
2. 配置 AP 上线。

1）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。

2）配置 AC 的系统参数，包括国家码、AC 与 AP 之间通信的源接口。

3）配置 AP 上线的认证方式并离线导入 AP，实现 AP 正常上线。

3. 配置 WLAN 业务参数并下发给 AP，实现 STA 访问 WLAN 网络功能。

6.2.2 配置步骤

步骤 1 设备基本配置

设备设备命名（拓扑中的 S2 命名为 AC）

略。

关闭 S1 和 AC 中间的多余链路，只针对《HCIA-Datacom 实验室搭建指南 V1.0》所描述的环境，其他环境可以忽略此步骤。

```
[S1] interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]shutdown
[S1-GigabitEthernet0/0/11]quit
[S1] interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
[S1-GigabitEthernet0/0/12]quit
```

开启 S3 和 S4 上连接 AP 接口的 PoE 供电功能

```
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]poe enable
```

poe enable命令用来使能接口的PoE功能。当接口检测到接口下有受电（PD）设备时，会通过接口给接口下接的PD设备供电。缺省情况下，接口PoE功能处于使能状态。故此处执行此命令仅为示例，实际环境下可以不执行。

```
[S4]interface GigabitEthernet 0/0/4
[S4-GigabitEthernet0/0/4]poe enable
```

步骤 2 有线侧网络配置

VLAN 配置

```
[S1]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]port link-type trunk
[S1-GigabitEthernet0/0/13]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/13]quit
[S1]interface GigabitEthernet 0/0/14
[S1-GigabitEthernet0/0/14]port link-type trunk
[S1-GigabitEthernet0/0/14]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/14]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/10]quit
```

```
[AC]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC]interface GigabitEthernet 0/0/10
[AC-GigabitEthernet0/0/10]port link-type trunk
[AC-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[AC-GigabitEthernet0/0/10]quit
```

```
[S3]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S3]interface GigabitEthernet 0/0/1
[S3-GigabitEthernet0/0/1]port link-type trunk
[S3-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S3-GigabitEthernet0/0/1]quit
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]port link-type trunk
[S3-GigabitEthernet0/0/4]port trunk pvid vlan 100
[S3-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
[S3-GigabitEthernet0/0/4]quit
```

```
[S4]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S4]interface GigabitEthernet0/0/1
[S4-GigabitEthernet0/0/1] port link-type trunk
[S4-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 101
```

```
[S4-GigabitEthernet0/0/1]quit
[S4]interface GigabitEthernet0/0/4
[S4-GigabitEthernet0/0/4] port link-type trunk
[S4-GigabitEthernet0/0/4] port trunk pvid vlan 100
[S4-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 101
[S4-GigabitEthernet0/0/4]quit
```

配置接口 IP 地址

```
[S1]interface Vlanif 101
[S1-Vlanif101]ip address 192.168.101.254 24
```

STA 的网关。

```
[S1-Vlanif101]quit
[S1]interface LoopBack 0
[S1-LoopBack0] ip address 10.0.1.1 32
```

后续做测试用，无实际用途。

```
[S1-LoopBack0]quit
```

```
[AC]interface Vlanif 100
[AC-Vlanif100]ip address 192.168.100.254 24
```

DHCP 配置

```
[S1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[S1]ip pool sta
Info:It's successful to create an IP address pool.
```

创建 STA 接入时所使用的 IP 地址池。

```
[S1-ip-pool-sta]network 192.168.101.0 mask 24
[S1-ip-pool-sta]gateway-list 192.168.101.254
[S1-ip-pool-sta]quit
[S1]interface Vlanif 101
[S1-Vlanif101]dhcp select global
[S1-Vlanif101]quit
```

```
[AC]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[AC]ip pool ap
Info: It is successful to create an IP address pool.
```

创建 AP 接入时所使用的 IP 地址池。

```
[AC-ip-pool-ap]network 192.168.100.254 mask 24
[AC-ip-pool-ap]gateway-list 192.168.100.254
[AC-ip-pool-ap]quit
[AC]interface Vlanif 100
[AC-Vlanif100]dhcp select global
[AC-Vlanif100]quit
```

S1作为STA的DHCP Server ，AC作为AP的DHCP Server，分别配置DHCP服务。

步骤 3 配置 AP 上线

创建名为 ap-group1 的 AP 组

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
Info: This operation may take a few seconds. Please wait for a moment.done.
[AC-wlan-ap-group-ap-group1]quit
```

创建域管理模板，在域管理模板下配置 AC 的国家码

```
[AC]wlan
[AC-wlan-view]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的配置。
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。

```
[AC-wlan-regulate-domain-default]country-code cn
Info: The current country code is same with the input country code.
```

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”。

```
[AC-wlan-regulate-domain-default]quit
```

在 AP 组下引用域管理模板

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continue?[Y/N]:y
```

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或AP组。缺省情况下，AP组下引用名为**default**的域管理模板，AP下未引用域管理模板。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。

```
[AC-wlan-ap-group-ap-group1]quit
```

配置 AC 建立 CAPWAP 隧道的源接口

```
[AC]capwap source interface Vlanif 100
```

capwap source interface命令用来配置AC建立CAPWAP隧道使用的接口，作为AC的源接口，用于AC和AP间建立CAPWAP隧道通信。

在 AC 上离线导入 AP，并将 AP 加入配置好的 AP 组“ap-group1”中。

AC上添加AP的方式有三种：

- 离线导入AP：预先配置AP的MAC地址和SN，当AP与AC连接时，如果AC发现AP和预先增加的AP的MAC地址和SN匹配，则AC开始与AP建立连接。
- 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AC连接时，AP将被AC自动发现并正常上线。

- 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。

```
[AC]wlan
[AC-wlan-view]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。
注：AP的MAC地址和SN可以通过设备包装箱内MAC地址标签和SN标签查询得到。

```
[AC-wlan-view]ap-id 0 ap-mac 60F1-8A9C-2B40
```

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。

```
[AC-wlan-ap-0]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。

```
[AC-wlan-ap-0]ap-group ap-group1
```

ap-group命令用来配置AP所加入的组，AC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，下发配置，AP**自动重启**，会加入到修改后的AP组中。

```
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                    //需要输入 y 来确认继续
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-0]quit
[AC-wlan-view]ap-id 1 ap-mac B4FB-F9B7-DE40
[AC-wlan-ap-1]ap-name ap2
[AC-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                    //需要输入 y 来确认继续
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-1]quit
```

查看当前的 AP 信息

```
[AC]wlan
[AC-wlan-view]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor    : normal              [2]
-------------------------------------------------------------------------------------------------------------------------------
ID      MAC                 Name Group      IP              Type            State   STA   Uptime
-------------------------------------------------------------------------------------------------------------------------------
0       00e0-fc25-0ed0 ap1  ap-group1       192.168.100.206 AirEngine5760   nor     0     30M:4S
```

```
1          00e0-fc0f-07a0 ap2     ap-group1       192.168.100.170   AirEngine5760   nor          0       31M:31S
--------------------------------------------------------------------------------------------------------------------------------
Total: 2
```

display ap命令用来查看AP信息，包括AP的IP地址、AP的型号（AirEngine5760）、AP的状态（normal）、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。（更多状态描述请看本实验附录）

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。

```
[AC-wlan-view]security-profile name HCIA-WLAN
[AC-wlan-sec-prof-HCIA-WLAN]security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
```

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。预共享秘钥（PSK）为HCIA-Datacom。通过AES加密算法加密用户数据。

```
[AC-wlan-sec-prof-HCIA-WLAN]quit
```

创建名为“HCIA-WLAN”的 SSID 模板，并配置 SSID 名称为“HCIA-WLAN”。

```
[AC]wlan
[AC-wlan-view]ssid-profile name HCIA-WLAN
```

创建名为“HCIA-WLAN”的 SSID 模板。

```
[AC-wlan-ssid-prof-HCIA-WLAN]ssid HCIA-WLAN
```

配置 SSID 名称为“HCIA-WLAN”。

```
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-HCIA-WLAN]quit
```

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。

```
[AC]wlan
[AC-wlan-view]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。

```
[AC-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。

```
[AC-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。

```
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]security-profile HCIA-WLAN
```

引用安全模板“HCIA-WLAN”。

```
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]ssid-profile HCIA-WLAN
```

引用 SSID 模板“HCIA-WLAN”。

```
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]quit
```

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。

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]vap-profile HCIA-WLAN wlan 1 radio all
```

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。

```
Info: This operation may take a few seconds, please wait...done.
[AC-wlan-ap-group-ap-group1]quit
```

6.3 结果验证

1. 使用无线终端接入到 SSID 为“HCIA-WLAN”的无线信号，查看 STA 获取的 IP 地址，同时访问 S1 的 LoopBack0 接口的 IP 地址（对 10.0.1.1 做 ping 测试）。
2. 在 STA 连接的同时，在 AC 上使用命令：display station all 查看 STA 信息。

6.4 配置参考

S1 的配置

```
#
sysname S1
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool sta
 gateway-list 192.168.101.254
 network 192.168.101.0 mask 255.255.255.0
#
interface Vlanif101
 ip address 192.168.101.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/10
 port link-type trunk
```

```
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/14
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
return
```

AC 的配置

```
#
sysname AC
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool ap
 gateway-list 192.168.100.254
 network 192.168.100.0 mask 255.255.255.0
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
wlan
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase %^%#V-rr;CTW$X%,nJ/0jcmO!tRQ(pt;^8IN,z1||UU)%^%# 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 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 0 type-id 75 ap-mac 60f1-8a9c-2b40 ap-sn 21500831023GJ9022622
  ap-name ap1
```

```
  ap-group ap-group1
 ap-id 1 type-id 75 ap-mac b4fb-f9b7-de40 ap-sn 21500831023GJ2001889
  ap-name ap2
  ap-group ap-group1
 provision-ap
#
return
```

S3 的配置

```
#
sysname S3
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
return
```

S4 的配置

```
#
sysname S4
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
return
```

6.5 思考题

1. 当前组网下，若 AC 的 GigabitEthernet0/0/10 不允许 VLAN101 通过，对 STA 访问 S1 会有什么影响？为什么？若采用隧道转发又是怎样的情况？

2. 如果想让 AP1 和 AP2 下接入的 STA 属于不同的 VLAN，在 AC 上需要做什么样的操作呢？

6.6 附录

AP 状态	描述
commit-failed	AP上线后WLAN业务配置下发失败状态。
committing	AP上线后WLAN业务配置正在下发状态。
config	AP上线过程中WLAN业务配置正在下发状态。
config-failed	AP上线过程中的WLAN业务配置下发失败状态。
download	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。
name-conflicted	AP名称重名冲突状态。
normal	AP正常状态。
standby	AP在备AC上的正常状态。
unauth	AP未认证状态。

7 构建简单 IPv6 网络

7.1 实验介绍

7.1.1 关于本实验

IPv6（Internet Protocol Version 6）也被称为 IPng（IP Next Generation）。它是 Internet 工程任务组 IETF（Internet Engineering Task Force）设计的一套规范，是 IPv4（Internet Protocol Version 4）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。

7.1.2 实验目的

- 掌握静态 IPv6 地址的配置方法
- 掌握 DHCPv6 服务的配置方法
- 掌握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

7.1.3 实验组网介绍

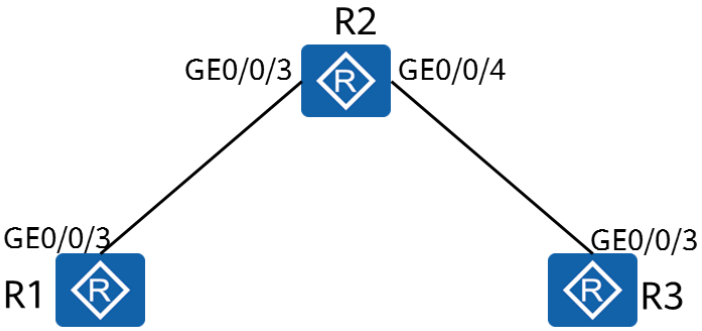


图7-1 构建简单 IPv6 网络实验拓扑

1. R2 的两个接口均采用静态 IPv6 地址配置方法
2. R1 的 GigabitEthernet0/0/3 接口采用无状态地址配置
3. R3 的 GigabitEthernet0/0/3 接口采用 DHCPv6 的方式配置 IPv6 地址

7.1.4 实验背景

某企业网络需要在网络内部署 IPv6 协议并实现 IPv6 的互联互通，需要对当前运行的网络设备进行配置。

7.2 实验任务配置

7.2.1 配置思路

1. 配置静态 IPv6 地址
2. 配置 DHCPv6
3. 配置无状态地址分配
4. 查看 IPv6 地址信息

7.2.2 配置步骤

步骤 1 设备基础配置

设备命名

略。

步骤 2 配置设备及接口 IPv6 功能

全局使能设备 IPv6 功能

```
[R1]ipv6
```

ipv6命令用来使能设备转发IPv6单播报文，包括本地IPv6报文的发送与接收。

```
[R2]ipv6
```

```
[R3]ipv6
```

使能接口的 IPv6 功能

```
[R1]interface GigabitEthernet 0/0/3
```

ipv6 enable命令用来在接口上使能IPv6功能。

```
[R1-GigabitEthernet0/0/3]ipv6 enable
[R1-GigabitEthernet0/0/3]quit
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ipv6 enable
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ipv6 enable
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ipv6 enable
[R3-GigabitEthernet0/0/3]quit
```

步骤 3 配置接口的 link-local 地址，并测试

配置接口自动生成 link-local 地址

```
[R1]interface GigabitEthernet 0/0/3
```

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-GigabitEthernet0/0/3]ipv6 address auto link-local
[R1-GigabitEthernet0/0/3]quit
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ipv6 address auto link-local
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ipv6 address auto link-local
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ipv6 address auto link-local
[R3-GigabitEthernet0/0/3]quit
```

查看接口的 IPv6 状态信息，并测试联通性

```
<R1>display ipv6 interface GigabitEthernet 0/0/3
GigabitEthernet0/0/3 current state : UP
IPv6 protocol current state : UP                    //物理和协议状态均为 UP。
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE4D:355    //接口的 link-local 地址已经生成。
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF4D:355
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

```
<R2>display ipv6 interface GigabitEthernet 0/0/3
GigabitEthernet0/0/3 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE12:6486
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF12:6486
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

```
<R2>display ipv6 interface GigabitEthernet 0/0/4
GigabitEthernet0/0/4 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE12:6487
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF12:6487
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

```
<R3>display ipv6 interface GigabitEthernet 0/0/3
GigabitEthernet0/0/4 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE3C:5133
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF3C:5133
    FF02::2
```

```
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

测试 R1 与 R2 联通性

```
<R1>ping ipv6 FE80::2E0:FCFF:FE12:6486 -i GigabitEthernet 0/0/3
  PING FE80::2E0:FCFF:FE12:6486 : 56  data bytes, press CTRL_C to break
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=1 hop limit=64  time = 90 ms
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=2 hop limit=64  time = 10 ms
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=3 hop limit=64  time = 20 ms
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=4 hop limit=64  time = 10 ms
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=5 hop limit=64  time = 30 ms

  --- FE80::2E0:FCFF:FE12:6486 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 10/32/90 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 4 配置 R2 的静态 IPv6 地址

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ipv6 address 2000:0012::2 64
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ipv6 address 2000:0023::2 64
[R2-GigabitEthernet0/0/4]quit
```

步骤 5 配置 R2 的 DHCPv6 Server 功能，配置 R3 通过 DHCPv6 获取 IPv6 地址

DHCPv6 Server 配置

```
[R2]dhcp enable
[R2]dhcpv6 pool pool1
```

创建名为“pool1”的地址池。

```
[R2-dhcpv6-pool-pool1]address prefix 2000:0023::/64
```

配置分配的 IPv6 地址前缀。

```
[R2-dhcpv6-pool-pool1]dns-server 2000:0023::2
```

配置 DNS Server 地址

```
[R2-dhcpv6-pool-pool1]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]dhcpv6 server pool1
```

```
[R2-GigabitEthernet0/0/4]quit
```

DHCPv6 Client 配置

```
[R3]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ipv6 address auto dhcp
[R3-GigabitEthernet0/0/3]quit
```

检查客户端地址和 DNS 服务器信息

```
[R3]display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                   Physical        Protocol
GigabitEthernet0/0/3        up              up
[IPv6 Address] 2000:23::1
```

```
[R3]display dns server
Type:
D:Dynamic         S:Static
No configured ip dns servers.
No.    Type    IPv6 Address                                Interface Name
1        D       2000:23::2                                -
```

此时 R3 的 GigabitEthernet0/0/3 接口已经获取到了 IPv6 全球单播地址。
如何配置 DHCPv6 Server 给客户端分配网关信息呢?

DHCPv6服务器不会为DHCPv6客户端分配IPv6网关地址。
当配置为DHCPv6有状态方式时，DHCPv6客户端通过ipv6 address auto global default命令学习到IPv6网关的缺省路由；当配置为DHCPv6无状态方式时，DHCPv6客户端通过该命令学习全球单播IPv6地址和IPv6网关的缺省路由。需确保与其相连的对端设备的接口已通过命令undo ipv6 nd ra halt，使能发布RA报文的功能

配置 DHCPv6 Server 给客户端分配网关地址

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]undo ipv6 nd ra halt
```

undo ipv6 nd ra halt命令用来使能系统发布RA报文功能，默认情况下路由器的接口不会发送RA报文。

```
[R2-GigabitEthernet0/0/4]ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig managed-address-flag命令用来设置RA报文中的有状态自动配置地址的标志位，默认情况下不设置该位。

- 如果设置了该标志位，则主机通过有状态自动配置获得IPv6地址。
- 如果清除了该标志位，则主机通过无状态自动配置获得IPv6地址，即通过RA报文向主机发布IPv6地址前缀信息自动生成IPv6地址。

```
[R2-GigabitEthernet0/0/4]ipv6 nd autoconfig other-flag
```

ipv6 nd autoconfig other-flag命令用来设置RA报文中的有状态自动配置其他信息的标志位，默认情况下不设置该位。

- 如果设置了该标志位，则主机可通过有状态自动配置获得除IPv6地址外的其他配置信息，包括路由器生存时间、邻居可达时间、邻居的重传时间、链路的MTU信息。
- 如果清除了该标志位，则主机进行无状态自动配置。即路由设备通过RA报文向主机发布除IPv6地址外的其他配置信息，包括路由器生存时间、邻居可达时间、邻居的重传时间、链路的MTU信息。

```
[R2-GigabitEthernet0/0/4]quit
```

配置客户端通过 RA 报文学习默认路由

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3] ipv6 address auto global default
```

查看 R3 的路由信息

```
[R3]display ipv6 routing-table
Routing Table : Public
         Destinations : 4        Routes : 4

Destination  : ::                                PrefixLength : 0
NextHop      : FE80::A2F4:79FF:FE5A:CDAE         Preference   : 64
Cost         : 0                                 Protocol     : Unr
RelayNextHop : ::                                TunnelID     : 0x0
Interface    : GigabitEthernet0/0/3              Flags        : D

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

Destination  : 2000:23::1                        PrefixLength : 128
NextHop      : ::1                               Preference   : 0
Cost         : 0                                 Protocol     : Direct
RelayNextHop : ::                                TunnelID     : 0x0
Interface    : GigabitEthernet0/0/3              Flags        : D

Destination  : FE80::                            PrefixLength : 10
NextHop      : ::                                Preference   : 0
Cost         : 0                                 Protocol     : Direct
RelayNextHop : ::                                TunnelID     : 0x0
Interface    : NULL0                             Flags        : D
```

步骤 6 配置 R1 通过无状态方式配置 IPv6 地址

在 R2 的 GigabitEthernet0/0/3 接口使能 RA 报文

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]undo ipv6 nd ra halt
```

在 R1 的 GigabitEthernet0/0/3 接口使能无状态地址配置

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3] ipv6 address auto global
```

检查 R1 的地址配置情况

```
[R1]display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                         Physical              Protocol
GigabitEthernet0/0/3              up                    up
[IPv6 Address] 2000:12::2E0:FCFF:FE4D:355
```

此时 R1 的 GigabitEthernet0/0/3 根据 R2 的 RA 报文获取的 IPv6 地址前缀，加上本地生成的接口 ID，生成了 IPv6 全球单播地址。

步骤 7 配置 IPv6 静态路由

为了实现 R1 的 GigabitEthernet0/0/3 和 R3 的 GigabitEthernet0/0/3 接口互访，需要在 R1 上配置静态路由

```
[R1]ipv6 route-static 2000:23:: 64 2000:12::2
Info: The destination address and mask of the configured static route mismatched, and the static route 2000:23::/64 was generated.
```

检测联通性

```
[R1]ping ipv6 2000:23::1
  PING 2000:23::1 : 56  data bytes, press CTRL_C to break
    Reply from 2000:23::1
    bytes=56 Sequence=1 hop limit=63   time = 20 ms
    Reply from 2000:23::1
    bytes=56 Sequence=2 hop limit=63   time = 20 ms
    Reply from 2000:23::1
    bytes=56 Sequence=3 hop limit=63   time = 30 ms
    Reply from 2000:23::1
    bytes=56 Sequence=4 hop limit=63   time = 20 ms
    Reply from 2000:23::1
    bytes=56 Sequence=5 hop limit=63   time = 30 ms

  --- 2000:23::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 20/24/30 ms
```

此时R1上存在到2000:23::/64网段的静态路由，R3通过DHCPv6获取了默认路由，故R1和R3的GigabitEthernet0/0/3接口之间可以互相访问。

查看 IPv6 邻居信息

```
[R1]display ipv6 neighbors
```

```
--------------------------------------------------------------------------------
IPv6 Address      : 2000:12::2
Link-layer        : 00e0-fc12-6486                State       : STALE
Interface         : GE0/0/3                       Age         : 8
VLAN              : -                             CEVLAN      : -
VPN name          :                               Is Router   : TRUE
Secure FLAG       : UN-SECURE

IPv6 Address      : FE80::2E0:FCFF:FE12:6486
Link-layer        : 00e0-fc12-6486                State       : STALE
Interface         : GE0/0/3                       Age         : 8
VLAN              : -                             CEVLAN      : -
VPN name          :                               Is Router   : TRUE
Secure FLAG       : UN-SECURE
--------------------------------------------------------------------------------
Total: 2          Dynamic: 2          Static: 0
```

7.3 结果验证

略。

7.4 配置参考

R1 的配置

```
#
 sysname R1
#
ipv6
#
interface GigabitEthernet0/0/3
 ipv6 enable
 ipv6 address auto link-local
 ipv6 address auto global
#
ipv6 route-static 2000:23:: 64 2000:12::2
#
return
```

R2 的配置

```
#
 sysname R2
#
ipv6
#
dhcp enable
#
dhcpv6 pool pool1
 address prefix 2000:23::/64
 dns-server 2000:23::2
```

```
#
interface GigabitEthernet0/0/3
 ipv6 enable
 ipv6 address 2000:12::2/64
 ipv6 address auto link-local
 undo ipv6 nd ra halt
interface GigabitEthernet0/0/4
#
ipv6 enable
 ipv6 address 2000:23::2/64
 ipv6 address auto link-local
 undo ipv6 nd ra halt
 ipv6 nd autoconfig managed-address-flag
 dhcpv6 server pool1
#
return
```

R3 的配置

```
#
 sysname R3
#
ipv6
#
dhcp enable
#
interface GigabitEthernet0/0/3
 ipv6 enable
 ipv6 address auto link-local
 ipv6 address auto global default
 ipv6 address auto dhcp
#
return
```

7.5 思考题

1. 步骤三中检测 link-local 地址之间联通性以及步骤七中检测 GUA 地址之间的联通性时，为何步骤三中必须指定源接口?

2.观察有状态地址配置和无状态地址配置获取到的 IPv6 地址区别，说明为什么会出现这种情况。

8 网络编程与自动化基础

8.1 实验介绍

8.1.1 关于本实验

通过本实验，读者将掌握 Python telnetlib 库的常用方法。

8.1.2 实验目标

- 掌握 Python 基本语法
- 掌握 telnetlib 基本方法

8.1.3 实验组网介绍

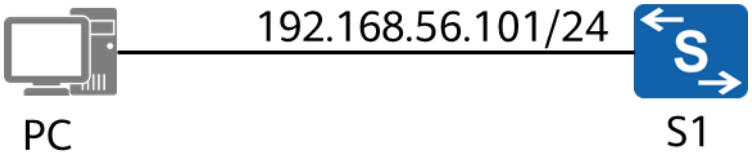


图8-1 网络编程与自动化基础实验拓扑

8.1.4 实验背景

某公司现有一台交换机，管理 IP 地址为 192.168.56.101/24。现在需要编写自动化脚本，查看设备当前配置文件。

8.2 实验任务配置

8.2.1 配置思路

1. 完成设备 Telnet 预配置：配置 Telnet 密码，开启 Telnet 功能和允许 Telnet 登录。
2. 编写 Python 脚本：调用 telnetlib 登陆设备，然后查看配置。

8.2.2 配置步骤

步骤 1 完成交换机的 Telnet 预配置

创建 Telnet 登陆密码

```
[Huawei]user-interface vty 0 4
[Huawei-ui-vty0-4]authentication-mode password
[Huawei-ui-vty0-4]set authentication password simple Huawei@123
[Huawei-ui-vty0-4]protocol inbound telnet
[Huawei-ui-vty0-4]user privilege level 15
```

使用Python脚本Telnet登录设备前，需要首先在设备上创建Telnet密码和开启Telnet功能。配置Telnet登陆密码为Huawei@123。

开启 Telnet 服务，允许 Telnet 用户登录。

```
[Huawei]telnet server enable
Info: The Telnet server has been enabled.
```

PC 通过 CMD 登录测试。

```
C:\Users\XXX>telnet 192.168.56.101
Login authentication

Password:
Info: The max number of VTY users is 5, and the number of current VTY users on line is 1.
The current login time is 2020-01-15 21:12:57.
<Huawei>
```

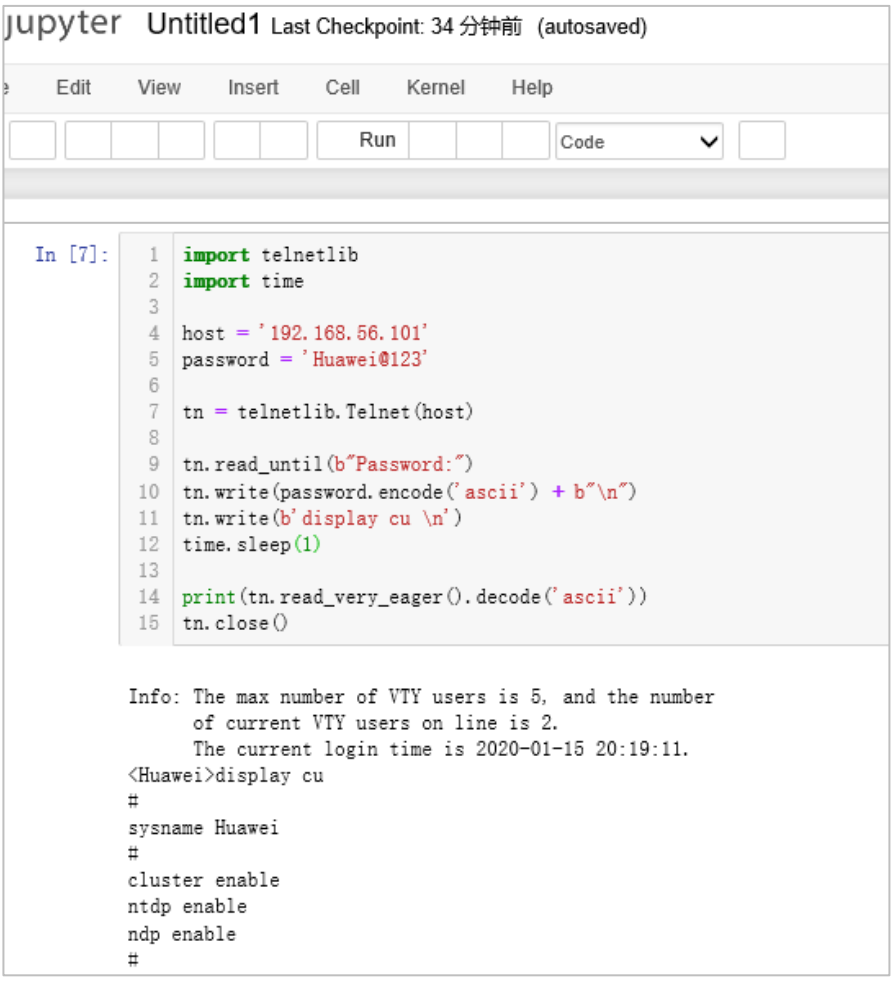
Telnet 配置成功!

步骤 2 Python 代码编写

```
import telnetlib
import time

host = '192.168.56.101'
password = 'Huawei@123'

tn = telnetlib.Telnet(host)

tn.read_until(b"Password:")
tn.write(password.encode('ascii') + b"\n")
tn.write(b'display cu \n')
time.sleep(1)

print(tn.read_very_eager().decode('ascii'))
tn.close()
```

Python脚本调用telnetlib模块登录S1，执行display current-configuration，并输出回显内容。

步骤 3 编译器执行:



本实验环境采用的编译器是jupyter notebook，学员可以使用其他编译器。

步骤 4 输出结果：

```
Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 2.
      The current login time is 2020-01-15 20:19:11.
<Huawei>display cu
#
sysname Huawei
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
```

```
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
 ip address 192.168.56.101 255.255.255.0
  ---- More ----
```

8.2.3 代码解析

步骤 1 导入模块

```
import telnetlib
import time
```

导入本段代码中需要使用的 telnetlib 和 time 两个模块。这两个模块都是 Python 自带的模块，无需安装。

本章节主要介绍 Telnetlib 作为客户端的常用类和方法，例如 Telnet 类下 read_until、read_very_eager()、write()等方法。更多 Telnet 的方法请参考 telnetlib 官方文档：https://docs.python.org/3/library/telnetlib.html#telnet-example。

Python 默认无间隔按顺序执行所有代码，在使用 telnet 向交换机发送配置命令时候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

调用 telnetlib 里 Telnet 类的多种方法登录 S1。

```
host = '192.168.56.101'
password = 'Huawei@123'
tn = telnetlib.Telnet(host)
```

首先创建两个变量，host 和 password 分别为设备的登录地址和密码，与设备配置参数一致。因为本例中仅在设备配置 telnet 密码方式登陆，所以无需用户名。

telnetlib.Telent()表示调用 telnetlib 类下的 Telnet()方法。这个方法中包含登陆的参数，包括 IP 地址和端口号等信息。不填写端口信息则默认为 23 号端口。

本例中 tn = telnetlib.Telnet(host)，表示登陆 host='192.168.56.101'的设备，然后将 telnetlib.Telnet(host)赋值给 tn。

```
tn.read_until(b"Password:")
```

正常 Telnet 登陆 192.168.56.101 设备时候，会有如下回显信息：

```
<TelnetClient>telnet 192.168.56.101
Trying 192.168.56.101 ...
Press CTRL+K to abort
Connected to 192.168.56.101 ...


Login authentication


Password:
```

请注意程序并不知道需要读取到什么信息为止，所以我们使用 read_until()指示读取到括号内信息为止。

本例中 tn.read_until(b"Password:")表示读取到显示 "Password:"为止。其中字符串“Password:”前的“b”表示将 Python3 中默认的 unicode 编码变为 bytes。这是函数对输入数据的要求，具体内容可以查看 telnetlib 官方文档，若不携带则程序会报错。

```
tn.write(password.encode('ascii') + b"\n")
```

在代码读取到显示"Password:"后，程序需输入参数 password。这个参数在前面已定义，作为 Telent 登录的密码。使用 write()完成 password 的写入。

本例中 tn.write(password.encode('ascii') + b"\n")，输入的内容由两个部分组成，password.encode('ascii') 和 b"\n"。password.encode('ascii')表示转换 password 代表的字符串“Huawei@123”的编码类型为 ASCII。“+”表示将该符号前后的字符串连接。“\n”为换行符，相当于输入后敲击回车键。所以本行代码含义为输入密码“Huawei@123”并敲击回车键。

步骤 3 输入配置命令

Telnet 到设备后，使用 Python 脚本向设备输入执行命令。

```
tn.write(b'display cu \n')
```

继续使用 write()向设备输入命令。输入的命令“display cu”为“display current-configuration”的缩写，其功能是显示设备的当前配置。

```
time.sleep(1)
```

time.sleep(1)的作用是将程序暂停 1 秒。用于等待交换机回显信息，然后再执行后续代码。如果没有设置等待时间，则程序会直接执行下一行代码，导致没有数据可供读取。

```
print(tn.read_very_eager().decode('ascii'))
```

print()表示显示括号内的内容到控制台。

tn.read_very_eager()表示读取当前的尽可能多的数据。

. decode('ascii'))表示将读取的数据解码为 ASCII。

本例中这段代码的功能为将输入“display cu”后 1 秒内 S1 输出的信息显示到控制台。

步骤 4 关闭会话

```
tn.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 telnet 会话。

8.3 结果验证

略。

8.4 配置参考

略。

8.5 思考题

1. 如何使用 telnetlib 配置设备，例如配置设备管理接口地址?
2. 如何保存配置文件到本地目录?

9 园区网络项目实战

9.1 参考资料

文档中所列出的命令以及参考文档，请根据实际环境中的不同产品版本使用对应的命令以及文档。

参考文档:

1 《AR600, AR6000 产品文档》

2 《S2720, S5700, S6700 系列以太网交换机 产品文档产品》

3 《无线接入控制器(AC 和 FIT AP) 产品文档》

4 《HCIA-Datacom 园区网典型组网架构及案例实践》

参考链接:

1 http://support.huawei.com/

2 http://e.huawei.com/

9.2 实验介绍

9.2.1 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、公园等。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搭建的实战案例，来帮助学员理解园区网络中的常见技术与技术的应用。

9.2.2 实验目的

- 了解常见园区网络概念以及常见的架构
- 了解常见网络技术
- 了解园区网络生命周期
- 熟悉园区网络规划与设计、部署与实施、网络运维、网络优化

- 熟悉园区网络项目流程

9.2.3 实验组网介绍

略。

9.2.4 实验背景

某写字楼备搭建一张网络供楼内企业办公使用。写字楼共 6 层，目前已有三层投入使用，分别是一层会客大厅、二层行政部及总经理办公室、三层研发部和市场部。一层设有核心机房，其他各楼层均有一个小房间放置网络设备。

请以小组为单位成立项目组，完成这张网络的建设。

9.3 实验任务

9.3.1 需求采集及分析

项目组成员与该公司相关人员交流沟通时，需要获得哪些信息，请至少写出五条？

示例：了解公司接入网络的终端设备数量信息。

1. _____
2. _____
3. _____
4. _____
5. _____

针对已经有的需求，做出相应的分析。

1. 项目预算：

预算紧张，在满足需求的前提下尽量节省开销。

---

2. 接入终端类型：

存在有线终端和无线终端。

---

3. 接入终端数量：

一层：10 台有线终端，100 台无线终端。二层和三层：均有 200 台有线终端，50 台无线终端。

---

4. 网络管理方式：

通过 SNMP 方式统一网管。

---

5. 网络的流量大小，走向：

主要为内部流量，保证有线终端至少百兆接入，其他无需求。

---

6. 可靠性需求：

三层网络具有一定的冗余与故障切换能力。

---

7. 安全性需求：

需要对网络流量做一定程度的管控。

---

8. 互联网接入方式：

园区出口设备采用静态 IP 方式接入互联网。

---

9. 网络拓展需求：

后续其他楼层启用时，不需要更换当前正在使用的设备

9.3.2 规划与设计

任务一 设备选型及物理拓扑设计（选做）

背景信息：

网络总体接入终端数量如下：

楼层	一层	二层	三层	其他楼层（预留）
有线终端	10	200	200	500
无线终端	100	50	50	200
备注	访客无线终端接入+服务器接入	员工办公电脑有线接入+部分员工手机无线接入		

无线终端产生的流量均为上网流量，保证每客户端有 2Mbit/s 速率。

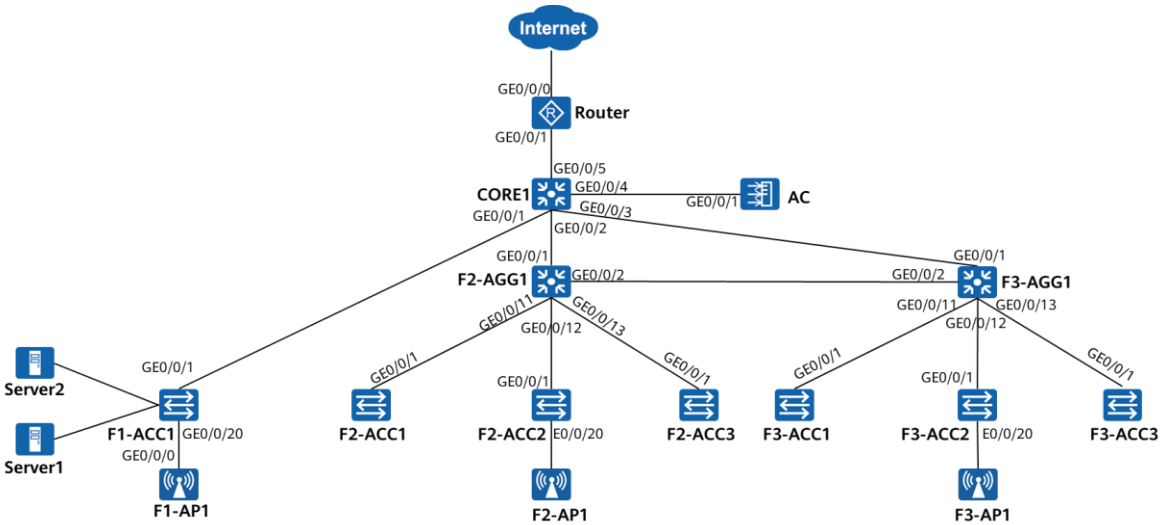
满足员工办公电脑百兆接入，服务器千兆接入。

为提高无线质量，需采用双频 AP，且每层至少需要 3 台 AP 才能完成覆盖。

任务：

请按照接入层->汇聚层->核心层->出口区的顺序设计该网络的物理拓扑并完成设备选型。

参考答案：



设备接口编号如下：

设备	包含接口编号
F2-ACC1、F2-ACC2、F2-ACC3、F3-	E0/0/1~E0/0/222

ACC1、F3-ACC2、F3-ACC	GE0/0/1~GE0/0/2
F1-ACC1、F2-AGG1、F3-AGG1、CORE1	GE0/0/1~GE0/0/24
AC	GE0/0/1~GE0/0/8
F1-AP1、F2-AP1、F3-AP1	GE0/0/0~GE0/0/1
Router	GE0/0/0~GE0/0/2

注意：HCIA-Datacom 认证教材中的《园区网络项目实战》详细解释了基于上述需求进行网络设计、拓扑设计的过程，本文档省略了这部分内容。在实际组网中，接入层交换机及 AP 的数量会比较多，为简单起见，也方便后续进行实验，本文档所使用的项目拓扑简化了组网拓扑（接入层交换机及 AP 的仅体现了少数几台）。

任务二 二层网络设计

背景信息：

- 有线网络VLAN划分：
  - 核心机房的接入交换机GE0/0/1~GE0/0/10连接服务器，属于同一个VLAN。
  - 二楼除F2-ACC2连接总经理办公室外，其他交换机连接行政部，两个部门属于不同的VLAN。
  - 三楼的F3-ACC1和F3-ACC3的E0/0/1~E0/0/10属于市场部，E0/0/11~E0/0/20属于研发部。
  - F3-ACC2的E0/0/1~E0/0/19属于市场部。
- 无线网络VLAN划分：
  - 各个楼层的无线终端需要属于不同的VLAN。
  - 各个楼层的无线管理VLAN不同。

注：需要预留设备互联 VLAN、设备管理 VLAN 等。

任务：

根据已有信息及要求，填写二层网络规划表格。

VLAN编号	VLAN描述
示例：1	二层设备管理VLAN

参考答案：

VLAN编号	VLAN描述
1	一楼的二层设备管理VLAN
2	二楼的二层设备管理VLAN
3	三楼的二层设备管理VLAN
100	服务器所属的VLAN
101	总经理办公室所属的VLAN
102	行政部所属的VLAN
103	市场部所属的VLAN
104	研发部所属的VLAN
105	一楼无线终端所属的VLAN
106	二楼无线终端所属的VLAN
107	三楼无线终端所属的VLAN
201	F2-AGG1与CORE1互联VLAN
202	F3-AGG1与CORE1互联VLAN
203	F2-AGG1与F3-AGG1互联VLAN
204	CORE1与Router互联VLAN
205	一楼无线管理VLAN

206	二楼无线管理VLAN
207	三楼无线管理VLAN

任务三 三层网络设计

背景信息：

- 地址配置，采用192.168.0.0/16地址段，具体需求如下：
  - 一楼：
    - 服务器采用静态IP地址。无线客户端和无线AP由CORE1通过DHCP分配地址，网关均在CORE1上。
    - 接入交换机管理IP采用静态地址配置，网关在CORE1上。
  - 二楼和三楼：
    - 所有有线终端、无线终端、无线AP的地址均由对应楼层汇聚交换机通过DHCP分配，网关在汇聚交换机上。
    - 接入交换机管理IP采用静态地址配置，网关在各自楼层汇聚交换机上。
- 全网采用OSPF动态路由协议实现业务网段之间的互联互通，所有终端通过Router访问Internet。

任务：

根据已有信息及要求，填写三层网络规划表格。

IP网段	地址分配方式及网关	路由方式	网段描述
192.168.1.0/24	DHCP，网关192.168.1.254	OSPF	二层设备管理网段

参考答案：

IP 网段	地址分配方式及网关	路由配置	网段描述
192.168.1.0/24	静态配置，网关在 CORE1 上	默认路由指向 CORE1	一楼的二层设备管理网段
192.168.2.0/24	静态配置，网关在 F2-AGG1 上	默认路由指向 F2-AGG1	二楼的二层设备管理网段
192.168.3.0/24	静态配置，网关在 F3-AGG1 上	默认路由指向 F3-AGG1	三楼的二层设备管理网段
192.168.100.0/24	静态配置，网关在 CORE1 上	通过网关设备在 OSPF 中宣告	服务器所属网段
192.168.101.0/24	F2-AGG1 通过 DHCP 分配，网关在 F2-AGG1 上		总经理办公室所属网段
192.168.102.0/24			行政部所属所属网段
192.168.103.0/24	F3-AGG1 通过 DHCP 分配，网关在 F3-AGG1 上		市场部所属所属网段
192.168.104.0/24			研发部所属所属网段
192.168.105.0/24	CORE1 通过 DHCP 分配，网关在 CORE1 上		一楼大厅无线终端所属网段
192.168.106.0/24	F2-AGG1 通过 DHCP 分配，网关在 F2-AGG1 上		二楼无线终端所属网段
192.168.107.0/24	F3-AGG1 通过 DHCP 分配，网关在 F3-AGG1 上		三楼无线终端所属网段
192.168.201.0/30	静态配置，不需要网关	使能 OSPF，建立邻居关系，Router 宣告默认路由	F2-AGG1 与 CORE1 互联网段
192.168.202.0/30			F3-AGG1 与 CORE1 互联网段
192.168.203.0/30			F2-AGG1 与 F3-AGG1 互联网段
192.168.204.0/30			CORE1 与 Router 互联网段

192.168.205.0/24	CORE1 通过 DHCP 分配，网关在 CORE1 上	通过网关设备在 OSPF 中宣告	一楼无线管理网段
192.168.206.0/24	F2-AGG1 通过 DHCP 分配，网关在 F2-AGG1 上		二楼无线管理网段
192.168.207.0/24	F3-AGG1 通过 DHCP 分配，网关在 F3-AGG1 上		三楼无线管理网段

任务四 WLAN 设计

背景信息：

- 所有 AP 由 AC 统一进行管理，AC 转发性能较差。
  - 一楼的 AP 采用二层注册的方式。
  - 二楼和三楼的所有 AP 采用三层注册的方式，AC 的网关为 CORE1。
- 划分各楼层的 SSID
  - 均采用 WPA-WPA2+PSK+AES 安全策略。
  - 各楼层采用不同 SSID 和密码。

任务：

根据已有信息及要求，填写 WLAN 规划表格。

配置项	一楼WLAN	二楼WLAN	三楼WLAN
AP管理VLAN			
STA 业务 VLAN			
DHCP 服务器			
AC 的源接口 IP 地址			
AP 组			
域管理模板			
SSID 模板			
安全模板			
VAP 模板			
其他配置			

参考答案：

配置项	一楼 WLAN	二楼 WLAN	三楼 WLAN
AP 管理 VLAN	VLAN205	VLAN206	VLAN207
STA 业务 VLAN	VLAN105	VLAN106	VLAN107
DHCP 服务器	CORE1 为 AP 和 STA 分配地址	F2-AGG1 为 AP 和 STA 分配地址	F3-AGG1 为 AP 和 STA 分配地址
AC 的源接口 IP 地址	VLANIF205：192.168.205.253/24		
AP 组	名称：WLAN-F1 引用 VAP 模板：WLAN-F1 引用域管理模板：default	名称：WLAN-F2 引用 VAP 模板：WLAN-F2 引用域管理模板：default	名称：WLAN-F3 引用 VAP 模板：WLAN-F3 引用域管理模板：default
域管理模板	名称：default 国家码：CN		
SSID 模板	名称：WLAN-F1 SSID 名称：WLAN-F1	模板名称：WLAN-F2 SSID 名称：WLAN-F2	模板名称：WLAN-F3 SSID 名称：WLAN-F3
安全模板	名称：WLAN-F1 安全策略：WPA-WPA2+PSK+AES 密码：WLAN@Guest123	名称：WLAN-F2 安全策略：WPA-WPA2+PSK+AES 密码：WLAN@Employee2	名称：WLAN-F3 安全策略：WPA-WPA2+PSK+AES 密码：WLAN@Employee3
VAP 模板	名称：WLAN-F1 转发模式：直接转发 业务 VLAN：VLAN105 引用模板： SSID 模板：WLAN-F1 安全模板：WLAN-F1	名称：WLAN-F2 转发模式：直接转发 业务 VLAN：106 引用模板： SSID 模板：WLAN-F2 安全模板：WLAN-F2	名称：WLAN-F3 转发模式：直接转发 业务 VLAN：107 引用模板： SSID 模板：WLAN-F3 安全模板：WLAN-F3

任务五 安全及出口设计

背景信息：

- 禁止从一楼的访客 SSID 接入的用户访问公司内部网络。
- 仅无线终端可以访问 Internet。
- Router 采用静态 IP 地址方式接入互联网，运营商分配了 1.1.1.1-1.1.1.10 地址段（掩码长度为 24），Router 到达 Internet 的下一跳地址为 1.1.1.254。
- 公司内部有一台 Web 服务器需要对外提供服务，其私网 IP 地址为 192.168.100.1，端口号为 80。为了保证服务器安全性，只提供 Web 服务的 NAT 映射。

任务：

根据已有信息及要求，填写安全及出口规划表格。

需求	实现方案

参考答案：

需求	实现方案
访客到公司内网的访问控制	在 CORE1 上通过 traffic-filter 实现（或通过 Traffic Policy 实现）。
到 Internet 的访问控制	Router 配置 NAT 并禁止对相应网络做地址转换。
Web 服务映射	在 Router 的接口上配置 NAT Server。

任务六 网络管理设计

背景信息：

- 由于网络规模较大，安全性较低，在规划时配置设备使用 SNMPv3 版本与 NMS 进行通信，并配置认证和加密功能保证安全性。
- 除 Router 和 AC 外，所有设备通过管理 VLAN 与 NMS 进行通信，NMS 地址为 192.168.100.2/24。
- 路由器通过 GE0/0/1 接口与 NMS 通信。
- AC 通过 VLANIF205 接口与 NMS 通信。
- 要求所有设备能够在产生 SNMP 告警时主动向 NMS 上报。

任务：

根据上述需求，在“部署与实施”阶段，完善设备的配置方案。

9.3.3 部署与实施

任务一 配置方案

请按照规划设计方案，填写每个设备的配置方案。

Router：

配置项	配置内容
基础配置	
IP 地址配置	
OSPF	
出口配置	
SNMP 配置	
其他配置	

CORE1：

配置项	配置内容
基础配置	
VLAN 配置	
VLANIF 配置	
OSPF 配置	
DHCP 配置	

流量控制	
SNMP 配置	
其他配置	

F2-AGG1：

配置项	配置内容
基础配置	
VLAN 配置	
接口 VLAN 配置	
VLANIF 配置	
OSPF 配置	
DHCP 配置	
SNMP 配置	
其他配置	

F3-AGG1：

配置项	配置内容
基础配置	

VLAN 配置	
接口 VLAN 配置	
VLANIF 配置	
OSPF 配置	
DHCP 配置	
SNMP 配置	
其他配置	

AC 配置：

配置项	配置内容
基础配置	
有线互通配置	

无线配置	
SNMP 配置	
其他配置	

F1-ACC1：

配置项	配置内容
基础配置	

VLAN 配置	
VLANIF 配置	
路由配置	
SNMP 配置	
其他配置	

F2-ACC1：

配置项	配置内容
基础配置	

VLAN 配置	
VLANIF 配置	
路由配置	
SNMP 配置	
其他配置	

F2-ACC2：

配置项	配置内容
基础配置	

VLAN 配置	
VLANIF 配置	
路由配置	
SNMP 配置	
其他配置	

F2-ACC3：

配置项	配置内容
基础配置	

VLAN 配置	
VLANIF 配置	
路由配置	
SNMP 配置	
其他配置	

F3-ACC1：

配置项	配置内容
基础配置	

VLAN 配置	
VLANIF 配置	
路由配置	
SNMP 配置	
其他配置	

F3-ACC2：

配置项	配置内容
基础配置	

VLAN 配置	
VLANIF 配置	
路由配置	
SNMP 配置	
其他配置	

F3-ACC3：

配置项	配置内容
基础配置	

VLAN 配置	
VLANIF 配置	
路由配置	
SNMP 配置	
其他配置	

配置实现：

请按照上述配置方案，搭建实验环境，并完成相应的配置，限时 40 分钟。

任务二 项目验收

设备配置结束后，需要验收哪些内容，该如何去验证？请至少写出五条。

1._____

2._____

3._____

4._____

5._____

参考答案：

1.无线客户端是否能够发现无线信号并成功接入

2. OSPF 邻居状态是否正常

3.各网段内的互访是否正常

4.各网段间的互访是否正常

5.对无线访客的流量控制是否成功

6.对上网流量的限制是否成功

7. NMS 是否能管理到网络设备

9.3.4 网络运维

任务一 运维交接

项目交付完毕后，对于后期维护该网络的网管人员，你该如何安排相关的后期维护工作。请讨论并写出至少五条维护项。

1. _____
2. _____
3. _____
4. _____
5. _____

参考答案：

建议维护周期	检查项	检查方法	评估标准
日	电源连接是否正常可靠	观察	电源线应正确的连接到设备的指定位置上，且连接牢固。设备的电源指示灯应常亮绿色
	设备温度	<HUAWEI> display temperature	各模块当前的温度应该在上下限之间，即“Current”的值在“Lower”和“Upper”之间
	告警信息	<HUAWEI> display alarm urgent	如果有告警，需要记录，对于严重以上告警需并立即分析并处理。
	CPU 状态	<HUAWEI> display cpu-usage	各模块的 CPU 占用率正常。如果出现 CPU 占用率长时间超过 80%或者频繁出现超过 80%的情况，建议重点关注。
	内存占用率	<HUAWEI> display memory-usage	内存占用情况正常，如果“Memory Using Percentage”超过 60%时需要关注。
周	机房温度状况	仪器测量	机房环境长期工作温度在 0℃～50℃，短期工作温度在-5℃～55℃。
	机房湿度状况	仪器测量	机房湿度在 10%RH～90%RH 之间为正常。
月	设备位置摆放是否合理、牢固	观察加仪器测量	设备应放在通风、干燥的环境中，且放置位置牢固、平整。设备周围不得有杂物堆积。
	路由表信息	<HUAWEI> display ip routing-table	对于处于一个网络中同一层次的设备，如果运行相同的路由协议，各设备上的路由条目应该相差不大。
	配置信息备份	NA	每月对设备的配置信息进行保存备份。
	更改用户登录口令	NA	每月对设备用户登录口令进行修改

9.3.5 网络优化

任务一 性能优化

随着企业的发展，公司内部尤其是二楼和三楼部门之间的流量激增。汇聚交换机之间的链路无法承载如此巨大的流量，请问该如何优化?

参考答案:

1. 可在 F2-AGG1 和 F3-AGG1 之间增加物理链路，同时配置以太网链路聚合解决。
2. 通过修改 OSPF 的 cost 值形成负载分担，使得部分流量经过 CORE1 进行转发。

9.4 结果验证

略。

9.5 配置参考

Router 的配置

```
#
 sysname Router
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent sys-info version v3
 snmp-agent group v3 datacom privacy
 snmp-agent target-host trap-hostname nms address 192.168.100.2 udp-port 162 trap-paramsname datacom
 snmp-agent target-host trap-paramsname datacom v3 securityname test privacy
 snmp-agent usm-user v3 test datacom authentication-mode md5 4DE14BB77015FFE895A
65FDE05B8F6E9 privacy-mode aes128 4DE14BB77015FFE895A65FDE05B8F6E9
 snmp-agent trap source GigabitEthernet0/0/1
 snmp-agent trap enable
 snmp-agent
#
acl number 2000
 rule 5 permit source 192.168.105.0 0.0.0.255
 rule 10 permit source 192.168.106.0 0.0.0.255
 rule 15 permit source 192.168.107.0 0.0.0.255
#
 nat address-group 1 1.1.1.2 1.1.1.10
#
interface GigabitEthernet0/0/0
 ip address 1.1.1.1 255.255.255.0
 nat server protocol tcp global current-interface 8080 inside 192.168.100.1 www
 nat outbound 2000 address-group 1
#
interface GigabitEthernet0/0/1
 ip address 192.168.204.1 255.255.255.252
#
ospf 1
 default-route-advertise always
 area 0.0.0.0
  network 192.168.204.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
return
```

CORE1 的配置

```
#
sysname CORE1
#
vlan batch 100 105 201 to 202 204 to 205
#
dhcp enable
#
acl number 3000
 rule 5 deny ip source 192.168.105.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
 rule 10 permit ip
#
```

```
ip pool ap-f1
 gateway-list 192.168.205.254
 network 192.168.205.0 mask 255.255.255.0
 excluded-ip-address 192.168.205.253
#
ip pool sta-f1
 gateway-list 192.168.105.254
 network 192.168.105.0 mask 255.255.255.0
#
interface Vlanif1
 ip address 192.168.1.254 255.255.255.0
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
#
interface Vlanif105
 ip address 192.168.105.254 255.255.255.0
 dhcp select global
#
interface Vlanif201
 ip address 192.168.201.1 255.255.255.252
#
interface Vlanif202
 ip address 192.168.202.1 255.255.255.252
#
interface Vlanif204
 ip address 192.168.204.2 255.255.255.252
#
interface Vlanif205
 ip address 192.168.205.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 105 205
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 201
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 202
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 205
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 204
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
```

```
  network 192.168.100.0 0.0.0.255
  network 192.168.105.0 0.0.0.255
  network 192.168.205.0 0.0.0.255
  network 192.168.201.0 0.0.0.3
  network 192.168.202.0 0.0.0.3
  network 192.168.204.0 0.0.0.3
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC635139
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 %_#_3UJ'3!M;9]$R@P:G
H1!! privacy-mode des56 %_#_3UJ'3!M;9]$R@P:GH1!!
snmp-agent trap source Vlanif1
snmp-agent trap enable
#
return
```

F2-AGG1 的配置

```
#
sysname F2-AGG1
#
vlan batch 2 101 to 102 106 201 203 206
#
dhcp enable
#
ip pool admin
 gateway-list 192.168.102.254
 network 192.168.102.0 mask 255.255.255.0
#
ip pool ap-f2
 gateway-list 192.168.206.254
 network 192.168.206.0 mask 255.255.255.0
 option 43 sub-option 3 ascii 192.168.205.253
#
ip pool manager
 gateway-list 192.168.101.254
 network 192.168.101.0 mask 255.255.255.0
#
ip pool sta-f2
 gateway-list 192.168.106.254
 network 192.168.106.0 mask 255.255.255.0
#
interface Vlanif2
 ip address 192.168.2.254 255.255.255.0
#
interface Vlanif101
 ip address 192.168.101.254 255.255.255.0
 dhcp select global
#
interface Vlanif102
 ip address 192.168.102.254 255.255.255.0
 dhcp select global
#
```

```
interface Vlanif106
 ip address 192.168.106.254 255.255.255.0
 dhcp select global
#
interface Vlanif201
 ip address 192.168.201.2 255.255.255.252
#
interface Vlanif203
 ip address 192.168.203.1 255.255.255.252
#
interface Vlanif206
 ip address 192.168.206.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 201
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 203
#
interface GigabitEthernet0/0/11
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 102
#
interface GigabitEthernet0/0/12
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 101 106 206
#
interface GigabitEthernet0/0/13
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 102
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.101.0 0.0.0.255
  network 192.168.102.0 0.0.0.255
  network 192.168.106.0 0.0.0.255
  network 192.168.201.0 0.0.0.3
  network 192.168.203.0 0.0.0.3
  network 192.168.206.0 0.0.0.255
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC070327
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 +3V3OM/)GC'7M+H\V-,;
(!!! privacy-mode des56 +3V3OM/)GC'7M+H\V-,;(!!!
```

```
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

F3-AGG1 的配置

```
#
sysname F3-AGG1
#
vlan batch 3 103 to 104 107 202 to 203 207
#
ip pool ap-f3
 gateway-list 192.168.207.254
 network 192.168.207.0 mask 255.255.255.0
 option 43 sub-option 3 ascii 192.168.205.253
#
ip pool marketing
 gateway-list 192.168.103.254
 network 192.168.103.0 mask 255.255.255.0
#
ip pool rd
 gateway-list 192.168.104.254
 network 192.168.104.0 mask 255.255.255.0
#
ip pool sta-f3
 gateway-list 192.168.107.254
 network 192.168.107.0 mask 255.255.255.0
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
#
interface Vlanif103
 ip address 192.168.103.254 255.255.255.0
 dhcp select global
#
interface Vlanif104
 ip address 192.168.104.254 255.255.255.0
 dhcp select global
#
interface Vlanif107
 ip address 192.168.107.254 255.255.255.0
 dhcp select global
#
interface Vlanif202
 ip address 192.168.202.2 255.255.255.252
#
interface Vlanif203
 ip address 192.168.203.2 255.255.255.252
#
interface Vlanif207
 ip address 192.168.207.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type access
```

```
 port default vlan 202
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 203
#
interface GigabitEthernet0/0/11
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 to 104
#
interface GigabitEthernet0/0/12
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 107 207
#
interface GigabitEthernet0/0/13
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 to 104
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.103.0 0.0.0.255
  network 192.168.104.0 0.0.0.255
  network 192.168.107.0 0.0.0.255
  network 192.168.202.0 0.0.0.3
  network 192.168.203.0 0.0.0.3
  network 192.168.207.0 0.0.0.255
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCFB0564
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 5>5W!8N^H,L8E-@(C*:@
AQ!! privacy-mode des56 5>5W!8N^H,L8E-@(C*:@AQ!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

AC 的配置

```
#
 sysname AC
#
vlan batch 205
#
interface Vlanif205
 ip address 192.168.205.253 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
```

```
 port default vlan 205
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent group v3 datacom privacy
 snmp-agent target-host trap-hostname nms address 192.168.100.2 udp-port 162 trap-paramsname datacom
 snmp-agent target-host trap-paramsname datacom v3 securityname %^%#TvvWF~zi>Sgp
XL=P81^I^*^,(P&`UR97&h,l`eK8%^%# privacy
 snmp-agent trap source Vlanif205
 snmp-agent trap enable
 snmp-agent
#
ip route-static 0.0.0.0 0.0.0.0 192.168.205.254
#
capwap source interface vlanif205
#
wlan
security-profile name WLAN-F1
  security wpa-wpa2 psk pass-phrase %^%#53mQ@x*]z+u72&YdCR7A=11u&USV+9^Qw"'O43X>%^%# aes
 security-profile name WLAN-F2
  security wpa-wpa2 psk pass-phrase %^%#YKB4ZI%zFQxmOS76yL08],Z41lhJV"S[db(kar0X%^%# aes
 security-profile name WLAN-F3
  security wpa-wpa2 psk pass-phrase %^%#|8)z/PyjU1ssX8Cr(3M=%x\{CP*t,BCahW84sqvK%^%# aes
ssid-profile name WLAN-F1
  ssid WLAN-F1
 ssid-profile name WLAN-F2
  ssid WLAN-F2
 ssid-profile name WLAN-F3
  ssid WLAN-F3
 vap-profile name WLAN-F1
  service-vlan vlan-id 105
  ssid-profile WLAN-F1
  security-profile WLAN-F1
 vap-profile name WLAN-F2
  service-vlan vlan-id 106
  ssid-profile WLAN-F2
  security-profile WLAN-F2
 vap-profile name WLAN-F3
  service-vlan vlan-id 107
  ssid-profile WLAN-F3
  security-profile WLAN-F3
ap-group name WLAN-F1
  radio 0
   vap-profile WLAN-F1 wlan 1
  radio 1
   vap-profile WLAN-F1 wlan 1
  radio 2
   vap-profile WLAN-F1 wlan 1
 ap-group name WLAN-F2
  radio 0
   vap-profile WLAN-F2 wlan 2
  radio 1
   vap-profile WLAN-F2 wlan 2
  radio 2
   vap-profile WLAN-F2 wlan 2
 ap-group name WLAN-F3
```

```
   radio 0
    vap-profile WLAN-F3 wlan 2
   radio 1
    vap-profile WLAN-F3 wlan 2
   radio 2
    vap-profile WLAN-F3 wlan 2
  ap-id 0 type-id 60 ap-mac 00e0-fcca-2e20 ap-sn 2102354483108B3A413A
   ap-name F1-AP1
   ap-group WLAN-F1
  ap-id 1 type-id 60 ap-mac 00e0-fcf0-7bc0 ap-sn 210235448310D45A674C
   ap-name F2-AP1
   ap-group WLAN-F2
  ap-id 2 type-id 60 ap-mac 00e0-fcb2-72f0 ap-sn 210235448310C73E4033
   ap-name F3-AP1
   ap-group WLAN-F3
#
return
```

F1-ACC1 的配置

```
#
sysname F1-ACC1
#
vlan batch 100 105 205
#
interface Vlanif1
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 105 205
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/6
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/7
 port link-type access
 port default vlan 100
#
```

```
interface GigabitEthernet0/0/8
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/9
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/10
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/20
 port link-type trunk
 port trunk pvid vlan 205
 port trunk allow-pass vlan 105 205
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC03178D
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 3@^>FD5!85E`A!>CAH"1
U1!! privacy-mode des56 3@^>FD5!85E`A!>CAH"1U1!!
snmp-agent trap source Vlanif1
snmp-agent trap enable
#
return
```

F2-ACC1 的配置

```
#
sysname F2-ACC1
#
vlan batch 2 102
#
interface Vlanif2
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 102
```

```
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/8
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/9
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/12
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/13
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/14
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/15
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/16
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/17
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/18
 port link-type access
```

```
 port default vlan 102
#
interface Ethernet0/0/19
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/20
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/21
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/22
 port link-type access
 port default vlan 102
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 102
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC456509
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 (H\O$K,P78:9;\H&H"Ma
+A!! privacy-mode des56 (H\O$K,P78:9;\H&H"Ma+A!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

F2-ACC2 的配置

```
#
sysname F2-ACC2
#
vlan batch 2 101 106 206
#
interface Vlanif1
#
interface Vlanif2
 ip address 192.168.2.2 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 101
#
```

```
interface Ethernet0/0/3
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/8
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/9
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/12
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/13
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/14
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/15
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/16
 port link-type access
 port default vlan 101
```

```
#
interface Ethernet0/0/17
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/18
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/19
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/20
 port link-type trunk
 port trunk pvid vlan 206
 port trunk allow-pass vlan 106 206
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 101 106 206
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCA5263C
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 RN,<E0K"S8Z3K7.NSN8+
L1!! privacy-mode des56 RN,<E0K"S8Z3K7.NSN8+L1!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

F2-ACC3 的配置

```
#
sysname F2-ACC3
#
vlan batch 2 102
#
interface Vlanif2
 ip address 192.168.2.3 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 102
#
```

```
interface Ethernet0/0/3
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/8
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/9
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/12
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/13
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/14
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/15
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/16
 port link-type access
 port default vlan 102
```

```
#
interface Ethernet0/0/17
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/18
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/19
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/20
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/21
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/22
 port link-type access
 port default vlan 102
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 102
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC6E2774
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 :S@4*#]%O_-M9=:>$BB:
7!!! privacy-mode des56 :S@4*#]%O_-M9=:>$BB:7!!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

F3-ACC1 的配置

```
#
sysname F3-ACC1
#
vlan batch 3 103 to 104
#
interface Vlanif3
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet0/0/1
```

```
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/8
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/9
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/12
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/13
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/14
 port link-type access
 port default vlan 104
#
```

```
interface Ethernet0/0/15
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/16
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/17
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/18
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/19
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/20
 port link-type access
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 to 104
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCC75F9A
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 FD5[3#*%a/!W$IOS;(RD
3Q!! privacy-mode des56 FD5[3#*%a/!W$IOS;(RD3Q!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

F3-ACC2 的配置

```
#
sysname F3-ACC2
#
vlan batch 3 103 107 207
#
interface Vlanif3
 ip address 192.168.3.2 255.255.255.0
#
interface MEth0/0/1
#
interface Ethernet0/0/1
```

```
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/8
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/9
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/12
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/13
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/14
 port link-type access
 port default vlan 103
#
```

```
interface Ethernet0/0/15
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/16
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/17
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/18
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/19
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/20
 port link-type trunk
 port trunk pvid vlan 207
 port trunk allow-pass vlan 107 207
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 107 207
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCF3804A
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 0=.SBW74%B[6NT)>.>:]
aA!! privacy-mode des56 0=.SBW74%B[6NT)>.>:]aA!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

F3-ACC3 的配置

```
#
sysname F3-ACC3
#
vlan batch 3 103 to 104
#
interface Vlanif3
 ip address 192.168.3.3 255.255.255.0
#
interface Ethernet0/0/1
```

```
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/8
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/9
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/12
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/13
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/14
 port link-type access
 port default vlan 104
#
```

```
interface Ethernet0/0/15
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/16
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/17
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/18
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/19
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/20
 port link-type access
 port default vlan 104
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 to 104
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC224BC2
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 P'5R[2VCVEX8"$Y!=87`
1A!! privacy-mode des56 P'5R[2VCVEX8"$Y!=87`1A!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

9.6 思考题

1. 在本项目中，CORE1、F2-AGG1 及 F3-AGG1 构成了一个物理上的环路。但是在网络规划与设计阶段，我们将上述三台设备之间的互联链路规划在了不同的 VLAN，从而在 VLAN 的层面，实现了网络的破环。但是，在实验过程中，读者可能会发现，其中两台设备的邻接关系无法正确建立，请思考该现象的根因及解决方案。

2.通过本堂课程，你学到了什么知识，这些知识对你日后的工作或学习有什么帮助?

思考题参考答案

《华为 VRP 系统基本操作实验》参考答案：

1.略。

2.reset saved-configuration 命令用来清空设备下次启动使用的配置文件内的内容，并取消指定系统下次启动时使用的配置文件。当前指定的下次启动使用的配置文件为 test.cfg，所以这条命令执行后 test.cfg 内的内容会被清空，指定下次启动使用的文件为默认的配置文件 vrpcfg.zip。在步骤 4 中我们已经保存了当前的配置，所以重启之后配置不变。

《IPv4 编址及 IPv4 路由基础实验》参考答案

1. 同时满足下列两个条件，静态路由会被添加到路由表中：

1）该路由所配置的下一跳可达。

2）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。

2. 在华为设备上执行 ping 操作时，设备会查询路由表来确定出接口，出接口的 IP 地址将会被作为 ICMP 报文的源 IP 地址。

《OSPF 路由协议基础实验》参考答案

1. R2 回复 R1 的路径是：R2->R1。当修改了 R1 的 GigabitEthernet0/0/3 的 cost 为 10 之后，对 R1 来说，R1-R2 的路径开销为 10，所以考虑 cost 之后，R1 的 LoopBack0 访问 R2 的 LoopBack0 的路径为 R1->R3->R2。此时对 R2 来说，并不知道 R1 的 GigabitEthernet0/0/3 的 cost 改为了 10，还是以自己的 GigabitEthernet0/0/3 的 cost 来计算路由的开销，所以回复路径为 R2->R1。

《以太网基础与 VLAN 配置实验》参考答案

配置思路：

- 创建 VLAN，确定特殊 PC 所属的 VLAN。
- 配置 PC 的 MAC 地址与 VLAN 关联，实现根据报文中的源 MAC 地址划分 VLAN。
- 配置各接口以正确的方式加入 VLAN，实现二层转发。

配置步骤：

创建 VLAN

```
[S1]vlan 10
```

配置 PC 的 MAC 地址与 VLAN 10 关联

```
[S1]vlan 10
[S1-vlan10]mac-vlan mac-address 00e0-fc1c-47a7
[S1-vlan10]quit
```

假设该 PC 的 MAC 地址为：00e0-fc1c-47a7

使能接口基于 MAC 地址划分 VLAN 功能

```
[S1]interface gigabitethernet 0/0/1
[S1-GigabitEthernet0/0/1]mac-vlan enable
[S1-GigabitEthernet0/0/1]quit
```

配置连接 S2 的接口 GE0/0/1 为 Hybrid 接口，让对应 VLAN 的数据帧以 Untagged 方式通过

```
[S1]interface gigabitethernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type hybrid
[S1-GigabitEthernet0/0/1]port hybrid untagged vlan 10
[S1-GigabitEthernet0/0/1]quit
```

配置连接公司网络的接口 GE0/0/2，透传 MAC 地址关联的 VLAN

```
[S1]interface gigabitethernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan 10
[S1-GigabitEthernet0/0/2]quit
```

《生成树基础实验》参考答案

1. 不能，因为所有的桥在收到 STP BPDU 后，将 BPDU 中的 RPC 加上本端口的端口开销算出此端口的根路径开销，所以当 S1 的 GigabitEthernet 0/0/14 接口 cost 值改变后，不会影响 S4 的根路径开销。

2. 通过修改 S1 的 GigabitEthernet0/0/11 的端口优先级。

3. 不能，因为 S1 和 S2 之间的链路就构成了环路，所以必须有一条链路被阻塞。

《以太网链路聚合实验》参考答案

1. Least active-linknumber 需要小于或等于 max active-linknumber，

《实现 VLAN 间通信实验》参考答案

1. 在 S1 上要创建一个三层接口与 R1 的 GigabitEthernet0/0/1 互联，同时配置到相应网段的路由。

2. 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 就会进入 UP 状态。

《访问控制列表配置实验》参考答案

配置思路：

- 配置动态路由 OSPF，使得网络互通。
- 配置 R3 开启 Telnet 和 FTP 功能。
- 配置高级 ACL，进行流量过滤。

配置步骤：

配置网络互通、Telnet、FTP，略

在 R2 上配置 ACL

```
[R2] acl 3001
[R2-acl-adv-3001] rule 5 permit tcp source 10.1.2.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3001] rule 10 permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port range 20 21
[R2-acl-adv-3001] rule 15 deny tcp source any
[R2-acl-adv-3001] quit
```

在 R2 的 GE0/0/3 接口上调用 ACL，进行流量过滤

```
[R2] interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3] traffic-filter inbound acl 3001
```

《本地 AAA 配置实验》参考答案

略。

《网络地址转换配置实验》参考答案

1. 不需要。

《FTP 基础配置实验》参考答案

1. 主动模式。

《DHCP 基础配置实验》参考答案

1. 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. 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：根据中继器所请求的网段，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。

《构建基础 WLAN 网络实验》参考答案

1. 无影响，采用直接转发，数据不经过 AC1 的 GigabitEthernet0/0/10 接口。若采用隧道转发，则需要 GigabitEthernet0/0/10 允许 VLAN101 通过，否则 STA 无法访问 S1。

2. AP1 和 AP2 使用不同的 VAP 模板，在对应的 VAP 模板下配置不同的 service-VLAN 参数。

《构建简单 IPv6 网络实验》参考答案

1. 因为路由器上存在多个接口，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。

2.有状态配置时，接口的 128 位 IPv6 地址全部由 DHCPv6 Server 指定。无状态配置时，一般由 EUI-64 规范生成 64 位接口 ID。

《园区网络项目实战》参考答案

1. 虽然已经在 VLAN 层面实现了环路的避免，但是物理环路依旧存在。STP 的 BPDU 报文是不携带 VLAN 标签的，因此三台交换机之间的链路必定有一条会被阻塞，导致两台设备无法建立邻居关系。在实际工程部署中，因为已经在 VLAN 层面避免了环路，所以可以将设备之间的相对应接口的 STP 功能关闭。

2.略。

《自动化网络》参考答案

1. 使用 telnetlib 的 wirte()将配置设备接口命令脚本逐行写入。
2. 参考 Python IO 标准库。