Huawei Certification Training

HCIA-Datacom

Datacom Engineers' Lab Guide

V1.0

Huawei Technologies Co., Ltd.

Huawei Technologies Co., Ltd.

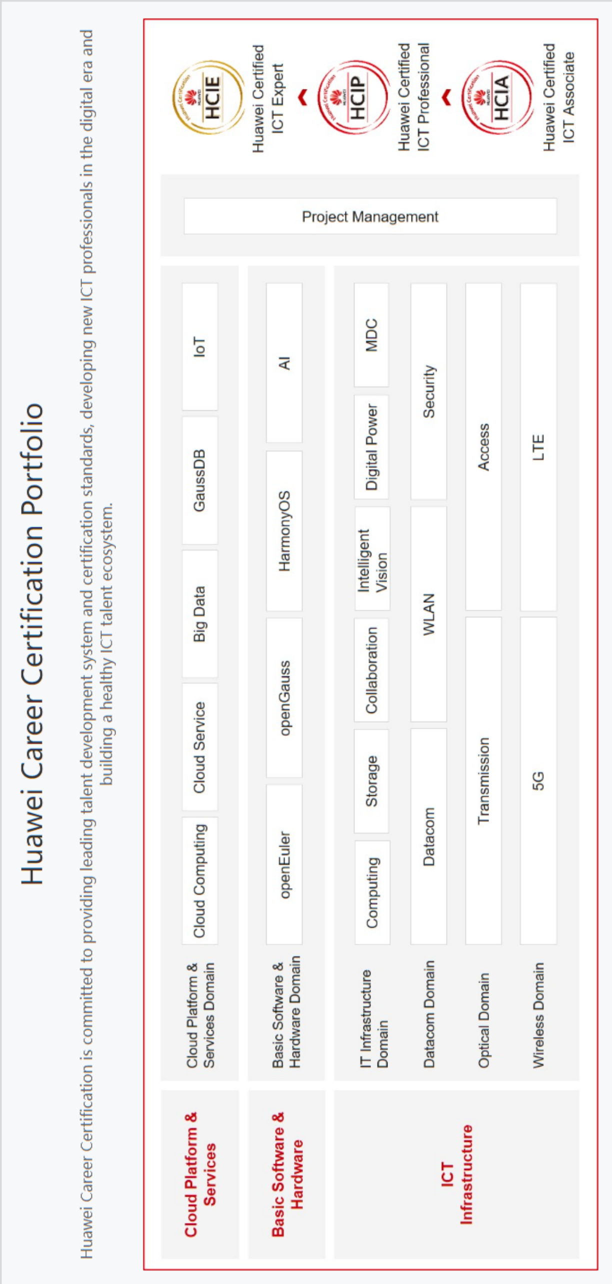
Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:	https://e.huawei.com/

Huawei Certification System

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.


Huawei Career Certification Portfolio
Huawei Career Certification is committed to providing leading talent development system and certification standards, developing new ICT professionals in the digital era and building a healthy ICT talent ecosystem.
Cloud Platform & Services
Cloud Platform & Services Domain
Cloud Computing
Cloud Service
Big Data
GaussDB
IoT
Basic Software & Hardware
Basic Software & Hardware Domain
openEuler
openGauss
HarmonyOS
AI
ICT Infrastructure
IT Infrastructure Domain
Computing
Storage
Collaboration
Intelligent Vision
Digital Power
MDC
Datacom Domain
Datacom
WLAN
Security
Optical Domain
Transmission
Access
Wireless Domain
5G
LTE
Project Management
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Introduction

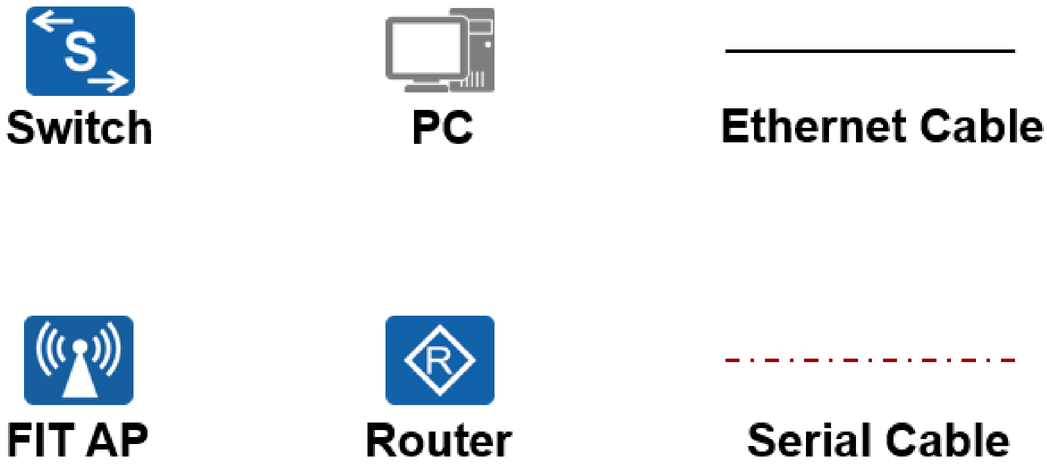
This document is an HCIA-Datacom certification training course and is intended for trainees who are going to take the HCIA-Datacom exam or readers who want to understand routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

Background Knowledge Required

This course is for Huawei's basic certification. To better understand this course, familiarize yourself with the following requirements:

- Basic computer skills
- Basic understanding of data communication

Symbol Conventions



Lab Environment

Network Description

This lab environment is intended for datacom engineers who are preparing for the HCIA-Datacom exam. Each lab environment includes two switches (PoE not supported), two PoE switches, two wireless access points (APs), and two routers.

Device Requirements

To meet exercise requirements, the recommended configurations of the environment are as follows:

The following table lists required devices:

Device Name	Device Model	Software Version
Switch	CloudEngine S5731-H24T4XC	V200R022C00SPC500 or later
PoE switch	CloudEngine S5731-H24P4XC	V200R022C00SPC500 or later
AP	AirEngine 5761-11	V200R022C00SPC100 or later
Router	NetEngine AR6121E	V300R022C00SPC100 or later

NOTE

The port, output, and configuration information of devices in this document is provided based on the recommended topology. The actual information may vary according to the lab environment.

Contents

1 Huawei VRP and Configuration Basics

1.1 Introduction

1.1.1 About This Lab

In this lab activity, you will learn the basic operations of Huawei VRP system by configuring Huawei devices.

1.1.2 Objectives

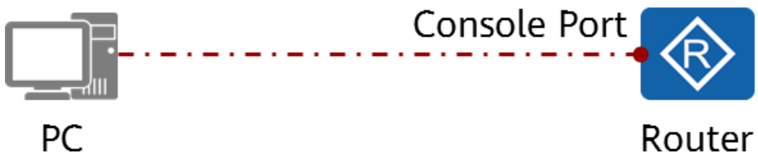
Upon completion of this task, you will be able to:

- Understand the meaning of command line views and how to access and exit command line views
- Understand common commands
- Understand how to use the command line online help
- Learn how to negate a command
- Learn how to use command line shortcut keys

1.1.3 Networking Topology

As shown in the following networking diagram, the router is a new router without any configuration. The PC is connected to the console port of the router through a serial cable. You need to initialize the router.

Figure 1-1 Lab topology for understanding the VRP operating system



1.2 Lab Configuration

1.2.1 Configuration Roadmap

1. Complete basic configurations, such as device name and router interface IP address.
2. Save the configurations.
3. Restart the device.

1.2.2 Configuration Procedure

Step 1 Log in to the CLI of the router through the console port.

The details are not provided here.

Step 2 Display the basic device information.

Display device version information.

```
<Huawei>display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (AR6121 V300R022C00SPC100)
Copyright (C) 2011-2022 HUAWEI TECH CO., LTD
Huawei AR6121E Router uptime is 0 week, 0 day, 5 hours, 55 minutes
BKP 0 version information:
1. PCB        Version  : AR-BKP6121 VER.A
2. If Supporting PoE : No
3. Board      Type       : AR6121E
4. MPU Slot Quantity : 1
5. LPU Slot Quantity : 1
```

Step 3 Complete basic device configurations.

Change the router name to **Datacom-Router**.

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

You have entered the system view from the user view.

```
  [Huawei]sysname Datacom-Router
[Datacom-Router]
```

*The device name has been changed to **Datacom-Router**.*

Huawei devices provide a wide variety of functions and related configuration and query commands. The commands are available in different command views based on the functions of the commands. To use a function, enter the corresponding command view first and then run corresponding commands.

Enter the interface view and configure the IP address of the interface.

```
[Datacom-Router]inter                                   //Press Tab to complete the command.
[Datacom-Router]interface                          //"interface" is the only optional keyword.
[Datacom-Router]interface g                            //Press Tab to complete the command.
[Datacom-Router]interface GigabitEthernet    //"GigabitEthernet" is the only optional keyword.
```

```
[Datacom-Router]interface GigabitEthernet 0/0/1    //Enter the complete command.
```

Enter the first several letters of a keyword in a command and press Tab to display a complete keyword. The first several letters, however, must uniquely identify the keyword. If they do not identify a specific keyword, press Tab continuously until the desired keyword is displayed. For example:

When you enter **inter** and press Tab, only the **interface** command starts with **inter**. Therefore, the command is autocompleted as **interface**. The command does not change if you press Tab multiple times.

```
[Datacom-Router-GigabitEthernet0/0/1]
```

The GigabitEthernet0/0/1 interface view is displayed.

```
[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
```

If you enter only the first or first several characters of a command keyword, you can use the context-sensitive help function to obtain all the keywords that begin with a character or character string. The meaning of each keyword will also be displayed. For example:

In the GigabitEthernet0/0/1 interface view, enter **i** and a question mark (?) to display the options of all commands starting with **i** in the current view. You can press Tab to complete the command of manually enter the complete command based on the help information. In the preceding information, **icmp** and **igmp** are keywords, **<Group> icmp command group**, and **Specify parameters for IGMP** are the descriptions of the keywords.

```
[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
```

When you enter some keywords of a command and a question mark (?) separated by a space, all keywords associated with this command, as well as simple descriptions, are displayed. For example:

If you enter **ip**, a space, and a question mark (?), all commands containing keyword **ip** and the corresponding descriptions are displayed.

```
[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> indicates that no keyword or parameter exists in this position. You can press Enter to run the command.

```
[Datacom-Router-GigabitEthernet0/0/1]dis this
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#
```

The **display this** command displays the running configuration in the current view. Effective arguments set to their defaults are not displayed. Configured arguments that are not committed successfully are not displayed, either. This command is used to check the configuration.

You do not need to enter complete keywords if the entered characters can match a unique keyword in the current view. This function improves efficiency. For example:

The **dis this** command can be executed on an interface because only the **display this** command matches the entered characters in the current view. Similarly, the **dis cu** or **d cu** command can also be executed because they are equivalent to **display current-configuration** command.

```
[Datacom-Router-GigabitEthernet0/0/1]quit
```

The **quit** command returns a device from the current view to a lower-level view. If the current view is the user view, this command exits from the system.

Negate the IP address configuration because the IP address should be signed to interface GigabitEthernet 0/0/2.

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

To do so, you must negate the IP address configuration of GigabitEthernet0/0/1. Otherwise, an IP address conflict occurs and the configuration fails.

To negate a command, use the **undo** keyword with the command. An undo command is generally used to restore a default configuration, disable a function, or delete a configuration. Almost each command line has a corresponding undo command.

```
[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
```

Display the current device configuration.

```
[Datacom-Router]display current-configuration
[V300R022C00SPC100]
```

```
#
 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 ----
```

When the information cannot be completely displayed on one screen, the system will pause for you can view the information. If **---- More ----** is displayed at the bottom of the command output, you can

1. Press Ctrl+C or Ctrl+Z to stop the display or command execution.
2. Press the space bar to display the next screen.
3. Press Enter to display the next line.

Step 4 Save the current configuration of the device.

Return to the user view.

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

In addition to the **quit** command, you can also:

1. Run the **return** command to return to the user view from any view.
2. Press Ctrl+Z to return to the user view from any view.

Save the configuration.

```
<Datacom-Router>save
  The current configuration will be written to the device.
  Are you sure to continue? .(y/n)[n]:y                              //Enter y to confirm.
  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
```

The current configuration is saved successfully.

Configuration changes must be saved in the configuration file to survive system restart. You can run the **save** command to save the current configuration to the default path and overwrite the original configuration file. You can also run the **save** *configuration-file* command to save the current configuration to a specified file in the storage device. This command does not affect the current startup configuration file of the system.

Compare the running configuration with the configuration in the startup configuration file.

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

The running configuration is the same as the configuration in the startup configuration file.

Step 5 Perform operations on the file system.

List all the files in the current directory.

```
<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    AR6120_V300R022C00SPC100.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: configuration file The filename extension of a configuration file must be .cfg or .zip.

AR6120_V300R022C00SPC100.cc: system software The filename extension of system software must be .cc.

Save the running configuration and name the configuration file test.cfg.

```
<Datacom-Router>save test.cfg
 Are you sure to save the configuration to test.cfg? (y/n)[n]:y        //Enter y to confirm.
  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
```

List all the files in the current directory again.

```
<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     AR6120_V300R022C00SPC100.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)
```

The configuration file is saved successfully.

Set the file as the startup configuration file.

```
<Datacom-Router>startup saved-configuration test.cfg
This operation will take several minutes, please wait.....
Info: Succeeded in setting the file for booting system
```

Display the startup configuration file.

```
<Datacom-Router>display startup
MainBoard:
  Startup system software:                   flash:/ AR6120_V300R022C00SPC100.cc
  Next startup system software:              flash:/ AR6120_V300R022C00SPC100.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
```

The **display startup** command displays the system software and configuration, license, patch, and voice files.

Clear the configuration file.

```
<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                          //Enter y to confirm.
 Clear the configuration in the device successfully.
```

Step 6 Restart the device.

```
<Datacom-Router>reboot
```

```
Info: The system is comparing the configuration, please wait.
System will reboot! Continue ? [y/n]:y                        //Enter y to confirm.
Info: system is rebooting ,please wait...
```

The system is restarting.

```
<Datacom-Router>
```

The device is restarted.

----End

1.3 Verification

The details are not provided here.

1.4 Configuration Reference

The details are not provided here.

1.5 Quiz

1. Familiarize yourself with the function keys of Huawei VRP system according to section 2.6.
2. In step 5, the **reset saved-configuration** command is executed to clear the configuration. Why is the configuration still retained after the device is restarted?

1.6 Appendix

Table 1-1 System function keys

Key	Function
<Ctrl+A>	Moves the cursor to the beginning of the current line.
<Ctrl+B>	Moves the cursor back one character.
<Ctrl+C>	Stops performing current functions.
<Ctrl+D>	Deletes the character where the cursor is located at.
<Ctrl+E>	Moves the cursor to the end of the last line.
<Ctrl+F>	Moves the cursor forward one character.
<Ctrl+H>	Deletes the character to the left of the cursor.

Key	Function
<Ctrl+K>	Terminates the connection of an outgoing call during connection establishment.
<Ctrl+N> or the down arrow key	Displays the next command in the command history.
<Ctrl+N> or the up arrow key	Displays the previous command in the command history.
<Ctrl+T>	Enters a question mark (?).
<Ctrl+W>	Deletes the character string (word) to the left of the cursor.
<Ctrl+X>	Deletes all characters on the left of the cursor.
<Ctrl+Y>	Deletes the character at the cursor and all characters to the right of the cursor.
<Ctrl+Z>	Returns to the user view.
<Ctrl+]>	Stops or redirects incoming connections.
<Esc+B>	Moves the cursor back one character string (word).
<Esc+D>	Deletes one character string (word) to the right of the cursor.
<Esc+F>	Moves the cursor forward one character string (word).

2 Creating an Interconnected IP Network

2.1 Lab 1: IPv4 Addressing and Routing

2.1.1 Introduction

2.1.1.1 About This Lab

Internet Protocol version 4 (IPv4) is a core protocol of the TCP/IP protocol suite and works at the Internet layer in the TCP/IP model or the network layer in the Open System Interconnection (OSI) model. The network layer provides connectionless data transmission. Each IP datagram is transmitted independently, removing the need to establish a connection before IP datagrams are sent.

Routing is the basic element of data communication networks. It is the process of selecting paths on a network along which packets are sent from a source to a destination.

In this lab activity, you will configure IPv4 addresses and static IPv4 routes, and understand basic routing principles in the process.

2.1.1.2 Objectives

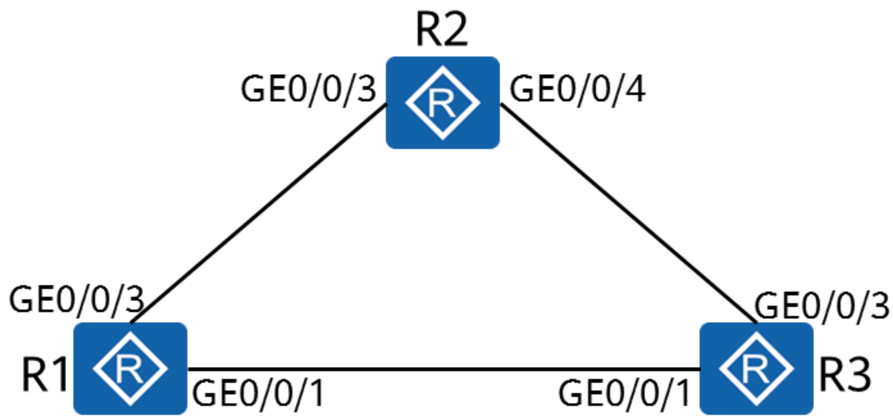
Upon completion of this task, you will be able to:

- Learn how to configure an IPv4 address on an interface
- Understand the functions and meanings of loopback interfaces
- Understand how direct routes are generated
- Learn how to configure static routes and understand the conditions for the static routes to take effect
- Learn how to test the connectivity of the network layer by using the ping tool
- Learn how to configure static routes and understand their application scenarios

2.1.1.3 Networking Topology

R1, R2, and R3 are gateways of their networks. You need to configure these gateways to connect these networks.

Figure 2-1 Lab topology for IPv4 addressing and routing



2.1.2 Lab Configuration

2.1.2.1 Configuration Roadmap

1. Configure IP addresses for the interfaces on the routers.
2. Configure static routes to interconnect the routers.

2.1.2.2 Configuration Procedure

Step 1 Complete basic device configuration.

Name the devices.

The details are not provided here.

Step 2 Display the IP address of the current interface and the routing table of the router.

Display the interface status on the router (R1 in this example).

```
[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
```

The **display ip interface brief** command displays the brief information about interface IP addresses, including the IP addresses, subnet masks, physical status, link-layer protocol status, and number of interfaces in different states.

GigabitEthernet0/0/1 and GigabitEthernet0/0/3 on R1 are not configured with IP addresses. Therefore, the IP Address/Mask field is in the unassigned state, the Protocol field is in the down state, and the Physical field is in the up state.

Display the routing table on the router (R1 in this example).

```
[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 is a default loopback interface.

InLoopBack0 uses the fixed loopback address 127.0.0.1/8 to receive data packets destined for the host where InLoopBack0 resides. The IP address of the InLoopBack0 interface cannot be changed or advertised using a routing protocol.

Step 3 Configure IP addresses for physical interfaces.

Configure IP addresses for physical interfaces based on the following table.

Table 2-1 IP addresses of physical interfaces

Router	Interface	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

```
<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
```

Use the ping tool to test the connectivity.

```
[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
```

Display the routing table of R1.

```
 [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
```

The preceding command output shows that three direct routes are automatically generated for each interface after the IP addresses of the interfaces are configured, which are

1. A route to the network where the interface resides
2. The host route to the interface
3. The host route to the broadcast address of the network where the interface resides

NOTE

A host route is a route with a 32-bit mask.

Step 4 Create a loopback interface.

Configure the loopback interface according to the following table.

Table 2-2 IP addresses of loopback interfaces

Router	Interface	IP Address/Mask
R1	LoopBack0	10.0.1.1/32
R2	LoopBack0	10.0.1.2/32
R3	LoopBack0	10.0.1.3/32

Loopback interfaces are logical interfaces manually configured and do not exist physically. Logical interfaces can be used to exchange data. A loopback interface is always Up at the physical layer and link layer unless it is manually shut down. Generally, a loopback interface uses a 32-bit mask. Loopback interfaces are used for the following purposes:

1. Used as the address for identifying and managing the router
2. Used as the router ID in OSPF
3. Used for improving network reliability

In this lab activity, the loopback interfaces are used to simulate clients.

```
[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
```

Display the routing table on the router (R1 in this example).

```
 [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
```

Direct routes have been generated.

Test the connectivity between the loopback interfaces.

```
[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
```

Using the **ping –a** *source-ip-address destination-ip-address* command to specify the source and destination IP addresses of ping packets. At this point, the router does not have a route to the destination IP address. Therefore, the ping operation fails.

Step 5 Configure static routes.

On R1, configure a route to the loopback0 interfaces of R2 and R3.

```
[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
```

Display the routing table of R1.

```
[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
```

The configured static routes are added to the IP routing table.

Test connectivity.

```
[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
The loopback0 interface of R2 still cannot be pinged because R2 does not have a route to the loopback0
interface of R1.
```

On R2, add a route to LoopBack0 of R1.

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

Test connectivity.

```
<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
```

Loopback0 on R1 can communicate with loopback0 on R2.

Configure other necessary routes.

```
[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
```

Test the connectivity between the loopback0 interfaces of the routers by referring to the proceeding description.

Step 6 Configure a path from R1 to R2 via R3 as the backup path from LoopBack0 of R1 to LoopBack0 of R2.

Configure static routes on R1 and R2.

```
[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
```

Display the routing tables of R1 and R2.

```
[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
```

The static route with a preference value of 100 is not added to the routing table.

Shut down GigabitEthernet0/0/3 interface on R1 and R2 to invalidate the route with the highest priority.

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

Display the routing table on R1 and R2. The command output shows that the routes with a lower priority are activated when the routes with a higher priority are invalidated.

```
[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
```

In this case, the original static route becomes invalid and the static route with a lower priority is activated.

Test connectivity.

```
[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
```

Trace the path of the data packets.

```
[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
```

The **tracert** command displays the path of packets from the source to the destination.

The command output shows that the data packets pass through GigabitEthernet0/0/1 and GigabitEthernet0/0/3 of R3 and are then forwarded to GigabitEthernet0/0/4 of R2.

NOTE

In some lab environments, the devices may not respond to ICMP packets for security reasons. Therefore, the results may vary. You can press Ctrl+C to end the tracert operation.

Step 7 Configure default routes to connect the LoopBack0 interface of R1 and the LoopBack0 interface of R2.

Restore the interfaces and delete the configured routes.

```
[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
```

Display the routing table of R1.

```
[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
```

R1 does not have a route to LoopBack0 (10.1.1.2/32) of R2.

Configure a default route on R1.

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

Display the routing table of R1.

```
[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
```
The default route has been activated.

Test the connectivity between LoopBack0 of R1 and LoopBack0 of R2.

```
[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
```
LoopBack0 of R1 can communicate with LoopBack0 of R2.

----End

2.1.3 Verification

You can run the ping and tracert commands to test the connectivity between loopback0 interfaces on different devices.

2.1.4 Configuration Reference

Configuration on R1

```
#
 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
```

Configuration on R2

```
#
 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
```

Configuration on R3

```
#
 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 Quiz

1. In what situations will the configured static route be added to the IP routing table? Can a route be added to the IP routing table if the configured next hop is unreachable?
2. In step 3, if the **-a** argument is not specified during the connectivity test between loopback interfaces, what is the source IP address of ICMP packets? Why?

2.2 Lab 2: OSPF Routing

2.2.1 Introduction

2.2.1.1 About This Lab

The Open Shortest Path First (OSPF) protocol is a link-state Interior Gateway Protocol (IGP) developed by the Internet Engineering Task Force (IETF). Currently, OSPF Version 2 (RFC2328) is used for IPv4. As a link-state protocol, OSPF has the following advantages:

- Multicast packet transmission to reduce load on the switches that are not running OSPF
- Classless Inter-Domain Routing (CIDR)
- Load balancing among equal-cost routes
- Packet authentication

With the preceding advantages, OSPF is widely accepted and used as an IGP.

In the lab activity, you will understand basic OSPF configurations and principles by configuring single-area OSPF.

2.2.1.2 Objectives

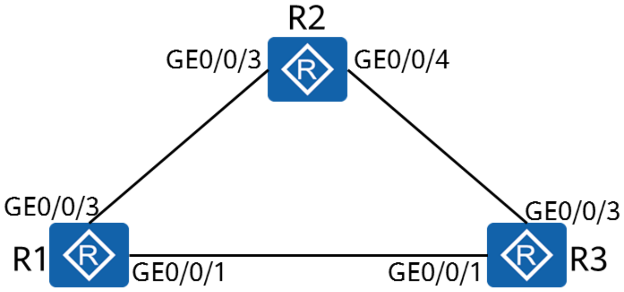
Upon completion of this task, you will be able to:

- Learn the basic commands of OSPF
- Learn how to check the OSPF running status
- Learn how to control OSPF route selection using costs
- Understand the advertisement of default routes in OSPF
- Learn how to configure OSPF authentication

2.2.1.3 Networking Topology

R1, R2, and R3 are gateways of their networks. You need to configure OSPF to enable connectivity between the networks.

Figure 2-2 Lab topology for configuring OSPF



2.2.2 Lab Configuration

2.2.2.1 Configuration Roadmap

1. Create OSPF processes on the devices and enable OSPF on the interfaces.
2. Configure OSPF authentication.
3. Configure OSPF to advertise default routes.
4. Control OSPF route selection using costs.

2.2.2.2 Configuration Procedure

Step 1 Complete basic device configuration.

Follow steps 1, 2, 3, and 4 in lab 1 to name the routers and configure the IP addresses of the physical and loopback interfaces.

Display the routing table on the router (R1 in this example).

```
[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
```

At this point, only direct routes exist on the device.

Step 2 Complete the basic OSPF configuration.

Create an OSPF process.

```
[R1]ospf 1
```

You can set OSPF parameters only after creating an OSPF process. OSPF supports multiple independent processes on one device. Route exchange between different OSPF processes is similar to that between different routing protocols. You can specify a process ID when creating an OSPF process. If no process ID is specified, the default process ID 1 is used.

Create an OSPF area and specify the interfaces on which OSPF is to be enabled.

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

The **area** command creates an OSPF area and displays the OSPF area view.

```
[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
```

The **network** *network-address wildcard-mask* command specifies the interfaces on which OSPF is to be enabled. OSPF can run on an interface only when the following two conditions are met:

1. The mask length of the interface's IP address is not shorter than that specified in the **network** command. OSPF uses reverse mask. For example 0.0.0.255 indicates that the mask length is 24 bits.
2. The address of the interface must be within the network range specified in the **network** command.

In this example, OSPF can be enabled on the three interfaces, and they are all added to area 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
```

If the wildcard mask in the **network** command is all 0s and the IP address of the interface is the same as the IP address specified in the **network-address** command, the interface also runs OSPF.

```
[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
```

Step 3 Display the OSPF status.

Displays the OSPF neighbor information.

```
[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 ]
```

The **display ospf peer** command displays information about neighbors in each OSPF area. The information includes the area to which the neighbor belongs, router ID of the neighbor, neighbor status, DR, and BDR.

Display the routes learned from OSPF.

```
[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
```

Step 4 Configure OSPF authentication.

Configure interface authentication on R1.

```
[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#
#
```

The password is displayed in cipher text when you view the configuration because cipher means cipher-text.

Display OSPF neighbors.

```
[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
```

Authentication is not configured on other routers. Therefore, the authentication fails and no neighbor is available.

Configuring interface authentication on R2.

```
[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
```

Display OSPF neighbors on R2.

```
[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
```

R2 has established a neighbor relationship with R1.

Configure area authentication on R3.

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

Display OSPF neighbors on R3.

```
[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
```

R3 has established a neighbor relationship with R1 and R2. Note: OSPF interface authentication and area authentication implement OSPF packet authentication on OSPF interfaces.

Step 5 Assume that R1 is the egress of all networks. Therefore, R1 advertises the default route to OSPF.

Advertise the default route on R1.

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

The **default-route-advertise** command advertises the default route to a common OSPF area. If the **always** argument is not specified, the default route is advertised to other routers only when there are active non-OSPF default routes in the routing table of the local router. In this example, no default route exists in the local routing table. Therefore, the **always** argument needs to be used.

Display the IP routing tables of R2 and R3.

```
[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 and R3 have learned the default route.

Step 6 Change the cost values of interfaces on R1 so that LoopBack0 on R1 can reach LoopBack0 on R2 via R3.

According to the routing table of R1, the cost of the route from R1 to LoopBack0 of R2 is 1, and the cost of the route from R1 to R2 via R3 is 2. Therefore, you only need to change the cost of the route from R1 to LoopBack0 of R2 to ensure that the value is greater than 2.

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

Display the routing table of R1.

```
[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
```

In this case, the next hop of the route from R1 to LoopBack0 on R2 is GigabitEthernet0/0/1 on R3.

Verify the result by issuing Tracert commands.

```
[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
```

----End

2.2.3 Verification

1. Test the connectivity between interfaces on different devices using Ping.
2. Shut down interfaces to simulate link faults and check the changes in routing tables.

2.2.4 Configuration Reference

Configuration on R1

```
#
 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
```

Configuration on R2

```
#
 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
```

Configuration on R3

```
#
 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 Quiz

1. In step 6, what is the path for R2 to return ICMP packets to R1? Try to explain the reason.

3 Creating a Switched Ethernet Network

3.1 Lab 1: Ethernet Basics and VLAN Configuration

3.1.1 Introduction

3.1.1.1 About This Lab

Ethernet technology allows data communication over shared media through Carrier Sense Multiple Access/Collision Detection (CSMA/CD). When an Ethernet network has a large number of hosts, collision becomes a serious problem and can lead to broadcast storms. This can degrade network performance or even result a complete breakdown. Using switches to connect LANs can mitigate collisions, but broadcast may still pose an issue.

To alleviate broadcast storms, VLAN technology divides a physical LAN into multiple VLANs so that the broadcast domains are smaller. Hosts within a VLAN can only directly communicate with hosts in the same VLAN. They must use a router to communicate with hosts in other VLANs.

In this lab activity, you will learn how to configure VLAN on Huawei switches.

3.1.1.2 Objectives

Upon completion of this task, you will be able to:

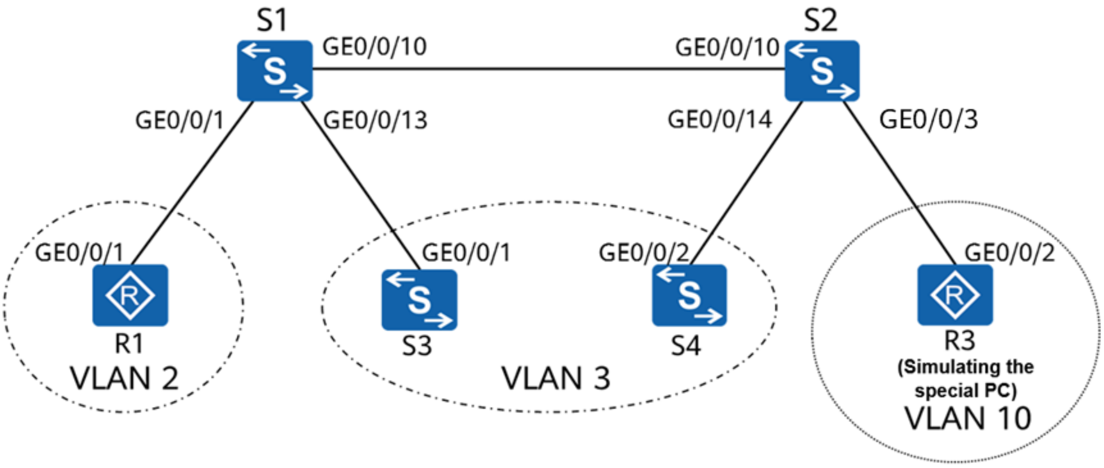
- Learn how to create a VLAN
- Learn how to configure access, trunk, and hybrid ports
- Learn how to configure VLANs based on ports
- Learn how to configure VLANs based on MAC addresses
- Learn how to view the MAC address table and VLAN information

3.1.1.3 Networking Topology

A company needs to divide a Layer 2 network into multiple VLANs based on service requirements. In addition, VLAN 10 requires a higher level of security and only specified PCs can be added to VLAN 10.

To meet this requirement, user ports of identical services on S1 and S2 can be assigned to the same VLAN, and ports with specified MAC addresses on S2 can be assigned to a VLAN.

Figure 3-1 Lab topology for VLAN configuration



3.1.2 Lab Configuration

3.1.2.1 Configuration Roadmap

1. Create a VLAN.
2. Configure a port-based VLAN.
3. Configure a MAC address-based VLAN.

3.1.2.2 Configuration Procedure

Step 1 Configure names for S1 and S2 and disable unnecessary ports.

Name the devices.

The details are not provided here.

Shut down GE0/0/11 and GE0/0/12 on S1. This step applies only to the environment described in *HCIA-Datacom Lab Construction Guide V1.0*.

```
[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
```

Shut down GE0/0/11 and GE0/0/12 on S2.

```
[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
```

Step 2 Configure the device IP addresses.

Set the IP addresses for R1 and R3 to 10.1.2.1/24 and 10.1.10.1/24, respectively.

```
[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
```

Set the IP addresses of S3 and S4 to 10.1.3.1/24 and 10.1.3.2/24, respectively. (For scenario 1: S3 and S4 support switching from Layer 2 interfaces to Layer 3 interfaces.)

```
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]undo portswitch
The interface changes to Layer 3 mode.
```

The **undo portswitch** command changes the working mode of Ethernet interfaces from Layer 2 mode to Layer 3 mode.

```
[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
```

Set the IP addresses of VLANIF3 on S3 and S4 to 10.1.3.1/24 and 10.1.3.2/24, respectively. (For scenario 2: S3 and S4 do not support switching from Layer 2 interfaces to Layer 3 interfaces.)

1. Create VLAN 3 on S3 and S4.

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

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

2. Configure ports on S3 and S4 as access ports and assign them to corresponding VLANs.

```
[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. # Create VLANIF interfaces and configure IP addresses.

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

The **interface vlanif** *vlan-id* command creates a VLANIF interface and displays the VLANIF interface view.

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

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

Step 3 Create a VLAN.

Create VLANs 2, 3, and 10 on S1 and S2.

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

The **vlan** *vlan-id* command creates a VLAN and displays the VLAN view. If the VLAN exists, the VLAN view is displayed.

The **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } command creates VLANs in batches.

```
[S2]vlan batch 2 to 3 10
```

Step 4 Configure port-based VLANs.

Configure user ports on S3 and S4 as access ports and assign them to corresponding VLANs.

```
[S1]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
```

The **port link-type { access | hybrid | trunk }** command specifies the link type of an interface, which can be Access, Trunk, or Hybrid.

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

The **port default vlan** *vlan-id* command configures the default VLAN of an interface and assigns the interface to the 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
```

Configure the ports connecting S1 and S2 as trunk ports and allow only packets from VLAN 2 and VLAN 3 to pass through.

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

The **port trunk allow-pass vlan** command assigns a trunk port to the specified VLANs.

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

The **undo port trunk allow-pass vlan** command deletes a trunk port from the specified VLANs.

By default, VLAN 1 is in the allowed list. If VLAN 1 is not used for any service, it needs to be deleted for security purposes.

```
[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
```

Step 5 Configure MAC address-based VLANs.

As shown in the networking diagram, R3 simulates a special service PC. Assume that the MAC address of the PC is a008-6fe1-0c46. The PC is expected to connect to the network through any of GigabitEthernet0/0/1, GigabitEthernet0/0/2, and GigabitEthernet0/0/3 on S2 and transmit data through VLAN 10.

Configure S2 to associate the MAC address of the PC with VLAN 10.

The VLAN membership depends on the source MAC addresses of packets, and VLAN tags are added accordingly. This VLAN assignment method is independent of the location, providing a higher level of security and flexibility.

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

The **mac-vlan mac-address** command associates a MAC address with a VLAN.

Set GigabitEthernet0/0/1, GigabitEthernet0/0/2, and GigabitEthernet0/0/3 on S2 to hybrid ports and configure them to allow packets from MAC address-based VLANs to pass through.

On access and trunk ports, MAC address-based VLAN assignment can be used only when the VLAN is the same as the PVID. Therefore, it is recommended that you configure MAC address-based VLAN assignment on a hybrid port to receive untagged packets from multiple VLANs.

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

The **port hybrid untagged vlan** command assigns a hybrid port to the specified VLANs to allow untagged frames to pass through.

```
[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
```

Configure the ports connecting S1 and S2 to allow packets from VLAN 10 to pass through.

The ports need to allow tagged frames from multiple VLANs to pass through. Therefore, the ports can be configured as trunk ports.

```
[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
```

Configure S2 and enable MAC address-based VLAN assignment on GE0/0/1, GE0/0/2, and GE0/0/3.

To enable a port to forward packets based on associations between MAC addresses and VLANs, you must run the **mac-vlan enable** command.

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

The **mac-vlan enable** command enables MAC address-based VLAN assignment on a port.

```
[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
```

Step 6 Display the configuration information.

Display the VLAN information on the switch.

```
[S1]display vlan
```

The **display vlan** command displays information about VLANs.

The **display vlan verbose** command displays detailed information about a specified VLAN, including the ID, type, description, and status of the VLAN, status of the traffic statistics function, ports in the VLAN, and mode in which the ports are assigned to the VLAN.

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

VID  Type     Ports
--------------------------------------------------------------------------------
1    common   UT: GE0/0/2(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
```

Display the MAC address-based VLAN configuration on the switch.

```
[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
```

The **display mac-vlan** command displays the configuration of MAC address-based VLAN assignment.

3.1.3 Verification

Test the device connectivity and verify the VLAN configuration.

1. Ping S4 from S3 and ensure that the ping operation is successful.
2. Ping other devices from R1 and ensure that the ping operation fails.
3. Run the **display mac-address verbose** command on S1 and S2 to check the MAC address tables on the switches.

3.1.4 Configuration Reference

Configuration on S1

```
#
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
```

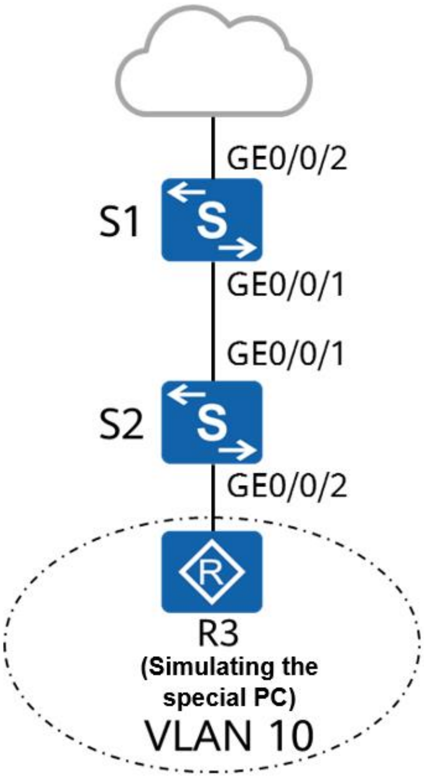
```
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 3
#
return
```

Configuration on S2

```
#
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 Quiz

1. As shown in the following figure, to ensure the information security of a special service, only some special PCs can access the network through VLAN 10. How can this requirement be implemented on S1?


GE0/0/2
S1
GE0/0/1
GE0/0/1
S2
GE0/0/2
R3
(Simulating the special PC)
VLAN 10

3.2 Lab 2: Spanning Tree

3.2.1 Introduction

3.2.1.1 About This Lab

On a switched Ethernet network, redundant links are used to implement link backup and enhance network availability. However, redundant links may produce loops, leading to broadcast storms and an unstable MAC address table, deteriorating or even interrupting communications. To prevent loops, IEEE introduced the Spanning Tree Protocol (STP).

STP defined in IEEE 802.1D has evolved to the Rapid Spanning Tree Protocol (RSTP) defined in IEEE 802.1W, and the Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1S.

In this lab activity, you will learn the basic STP configuration and understand its principles and some features of RSTP.

3.2.1.2 Objectives

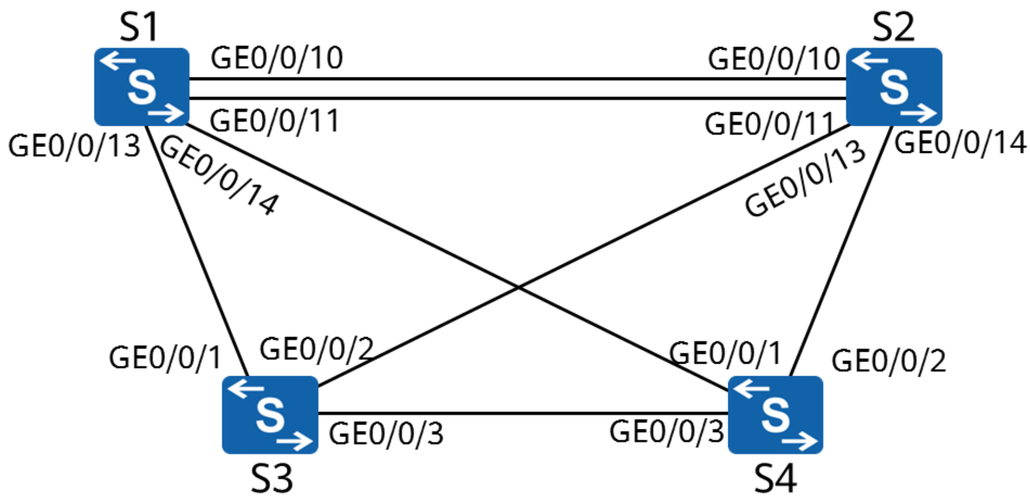
Upon completion of this task, you will be able to:

- Learn how to enable and disable STP/RSTP
- Learn how to change the STP mode of a switch
- Learn how to change bridge priorities to control the root bridge election
- Learn how to change port priorities to control the election of the root port and designated port
- Learn how to change port costs to control the election of the root port and designated port
- Learn how to configure edge ports
- Learn how to enable and disable RSTP

3.2.1.3 Networking Topology

A company need to deploy redundant links on its Layer 2 switched network to improve network availability. In the meantime, the company also needs to deploy STP to prevent redundant links from forming loops and causing broadcast storms and MAC address flapping.

Figure 3-2 Lab topology for configuring STP



3.2.2 Lab Configuration

3.2.2.1 Configuration Roadmap

1. Enable STP.
2. Change bridge priorities to control the root bridge election.
3. Modify port parameters to determine the port role.
4. Change the protocol to RSTP.
5. Configure edge ports.

3.2.2.2 Configuration Procedure

Step 1 # Shut down unnecessary ports. This step applies only to the environment described in *HCIA-Datacom Lab Construction Guide V1.0*.

Shut down GigabitEthernet0/0/12 between S1 and S2.

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

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

Step 2 Enable STP.

Enable STP globally.

```
<S1>system-view
Enter system view, return user view with Ctrl+Z.
[S1]stp enable
```

The **stp enable** command enables STP, RSTP, or MSTP on a switching device or a port. By default, STP, RSTP, or MSTP is enabled on switches.

Change the spanning tree mode to STP.

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

The **stp mode**{**mstp** | **rstp** | **stp**} command sets the operation mode of the spanning tree protocol on a switching device. By default, the switching device operates in MSTP mode. The spanning tree mode of the current device has been changed to 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.
```

Display the spanning tree status. S1 is used as an example.

```
[S1]display stp
-------[CIST Global Info][Mode STP]-------
CIST Bridge          :32768.4c1f-cc33-7359                //Bridge ID of the device.
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        //ID and path cost of the current root bridge.
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
```

The displayed information also includes port status information, which is not included in the preceding output.

Display the brief spanning tree information on each switch.

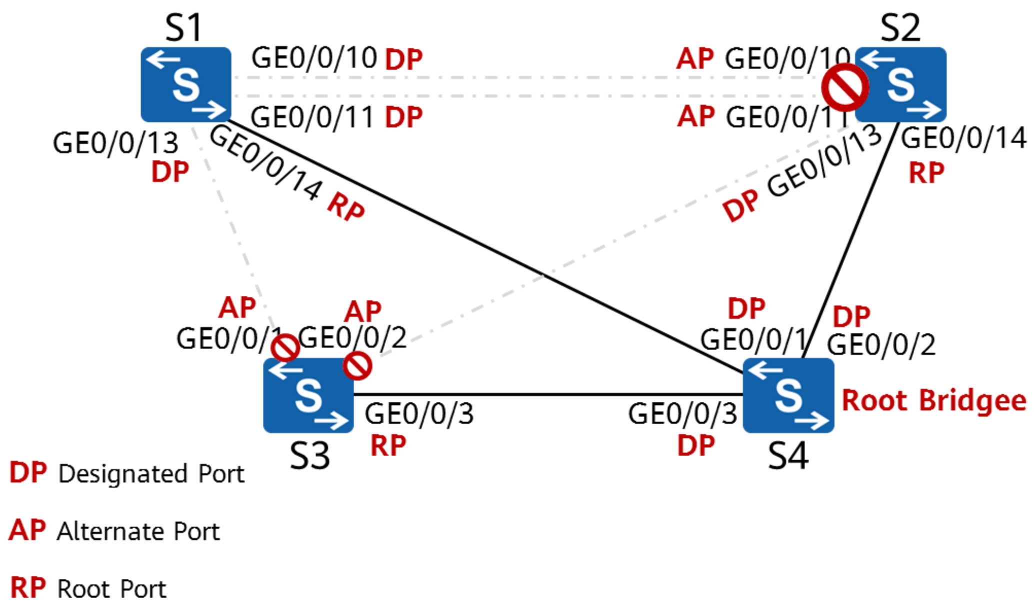
```
[S1]display stp brief
 MSTID  Port                     Role   STP State     Protection
   0    GigabitEthernet0/0/10    DESI   FORWARDING    NONE
   0    GigabitEthernet0/0/11    DESI   FORWARDING    NONE
   0    GigabitEthernet0/0/13    DESI   FORWARDING    NONE
   0    GigabitEthernet0/0/14   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

Based on the root bridge ID and port information on each switch, the current topology is as follows:



The dotted line indicates that the link does not forward service data.

NOTE

This topology is for reference only and may not be the same as the actual spanning tree topology in the lab environment.

Step 3 Modify device parameters to make S1 the root bridge and S2 the secondary root bridge.

Change the bridge priorities of S1 and S2.

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

Owning to the importance of the root bridge, the switch with high performance and network hierarchy is generally chosen as a root bridge. The priority of such a device, however, may be not that high. Therefore, setting a high priority for the switch is necessary so that the switch can be elected as the root bridge. The **stp root** command configures the switch as a root bridge or secondary root bridge of a spanning tree.

- The **stp root primary** command specifies a switch as the root switching device. In this case, the priority value of the switch is 0 in the spanning tree and the priority cannot be changed.
- The **stp root secondary** command specifies a switch as the secondary root bridge. In this case, the priority value of the switch is 4096 and the priority cannot be changed.

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

Display the STP status on S1.

```
[S1]display stp
-------[CIST Global Info][Mode STP]-------
CIST Bridge             :0     .4c1f-cc33-7359          //Bridge ID of the device.
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      //ID and path cost of the current root
bridge
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
```

In this case, the bridge ID of S1 is the same as the root bridge ID, and the root path cost is 0, indicating that S1 is the root bridge of the current network.

Display the brief STP status information on all devices.

```
[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
```

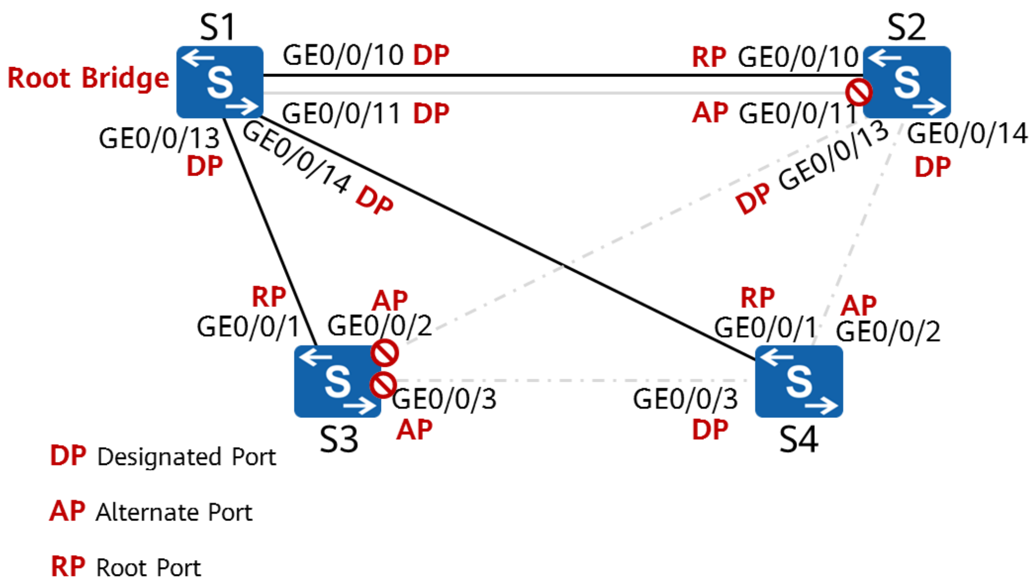
```
[S2]display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/10       ROOT  FORWARDING      NONE
```

```
 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
```

Based on the root bridge ID and port information on each switch, the current topology is as follows:



Step 4 Modify device parameters to make GigabitEthernet0/0/2 of S4 the root port.

Display the STP information on S4.

```
[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
```

The cost of the root path from S4 to S1 is 20000.

Change the STP cost of GigabitEthernet 0/0/1 on S4 to 50000.

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

Display the brief STP status information.

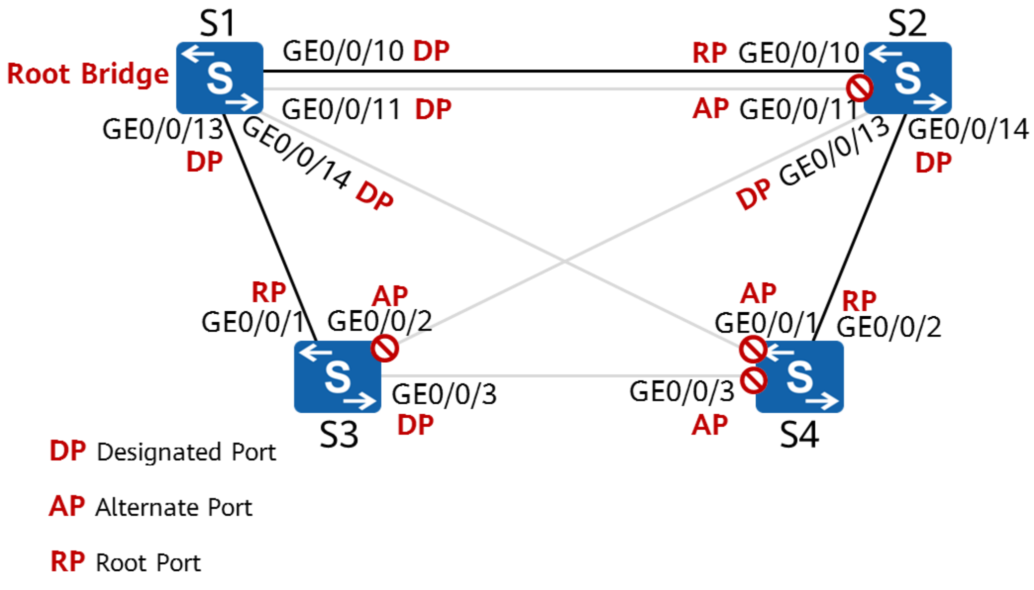
```
[S4]display stp brief
 MSTID  Port                    Role  STP State     Protection
   0    GigabitEthernet0/0/1    ALTE  DISCARDING    NONE
   0    GigabitEthernet0/0/2    ROOT  FORWARDING    NONE
   0    GigabitEthernet0/0/3    ALTE  DISCARDING    NONE
```

GigabitEthernet0/0/2 on S4 has become the root port.

Display the current STP status information.

```
[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     //Root path cost = 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
```

The current topology is as follows:



Step 5 Change the spanning tree mode to RSTP.

Change the spanning tree mode on all devices.

```
[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.
```

Display the spanning tree status. S1 is used as an example.

```
[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
```

After the mode is changed, the topology of the spanning tree is not affected.

Step 6 Configure edge ports.

GigabitEthernet 0/0/10-0/0/24 of S3 are connected only to terminals and need to be configured as edge ports.

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

A device provides multiple Ethernet ports, many of which have the same configuration. Configuring them one by one is tedious and error-prone. An easy way is to add such ports to a port group and configure the group. The system will automatically execute the commands on all ports in the group.

NOTE

This function may not be available on some products.

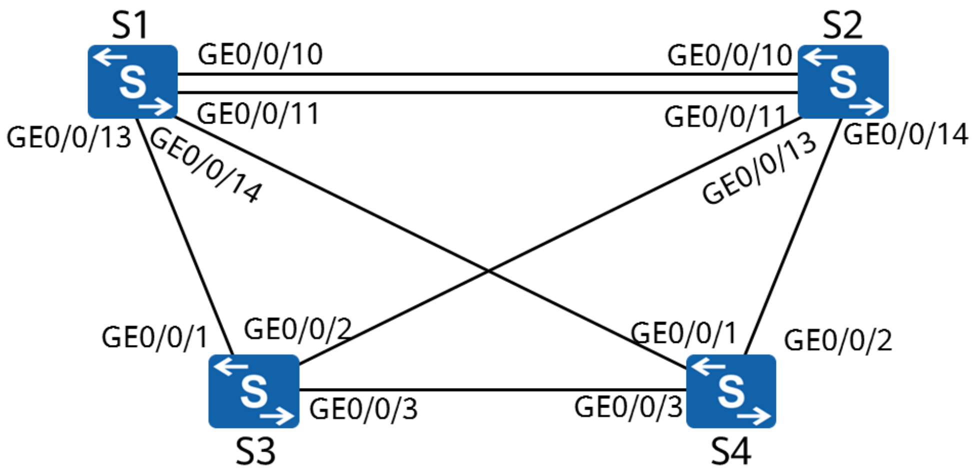
```
[S3-port-group]stp edged-port enable
```

The **stp edged-port enable** command sets the current port as an edge port. If a port of a switching device receives a BPDU after being configured as an edge port, the switching device will automatically set the port as a non-edge port and recalculate the spanning tree.

----End

3.2.3 Verification

1. Mark the root bridge and the role of each port in the lab environment based on the actual network convergence.



2. Disable any port on any switch and check whether the traffic can reach all other switches through the backup links.

3.2.4 Configuration Reference

Configuration on S1

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

Configuration on S2

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

Configuration on S3

```
#
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
```

Configuration on S4

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

3.2.5 Quiz

1. In step 3, if the cost of GigabitEthernet 0/0/14 on S1 is changed to 50000, can the desired result be achieved? Why?
2. In the current topology, modify the configuration to make GigabitEthernet0/0/11 of S2 the root port.
3. Can the two links between S1 and S2 be in the forwarding state at the same time? Why?

3.3 Lab 3: Ethernet Link Aggregation

3.3.1 Introduction

3.3.1.1 About This Lab

As networks grow in scale, users require Ethernet backbone networks to provide higher bandwidth and availability. In the past, the only way to increase bandwidth was to upgrade the network with high-speed LPUs, which is costly and inflexible.

In contrast, link aggregation increases bandwidth by bundling a group of physical port into a single logical port, without the need to upgrade hardware. In addition, link aggregation provides link backup mechanisms, greatly improving link availability. Link aggregation has the following advantages:

- Improving bandwidth: The maximum bandwidth of a link aggregation group (LAG) is the combined bandwidth of all member links.
- Improving availability: If a link is faulty, the traffic can be switched to other available member links.
- Load balancing: The traffic load can be balanced among the active member links in a LAG.

  In this lab activity, you will learn how to configure Ethernet link aggregation in manual and LACP modes.

3.3.1.2 Objectives

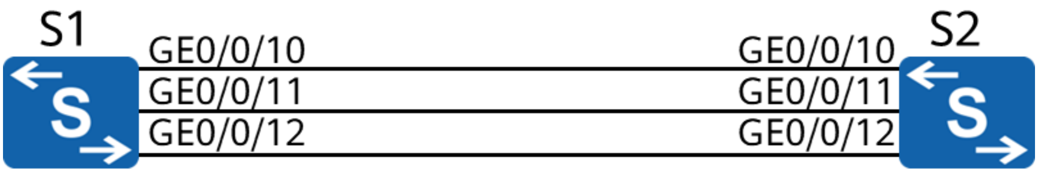
Upon completion of this task, you will be able to:

- Learn how to manually configure link aggregation
- Learn how to configure link aggregation in static LACP mode
- Learn how to determine active links in static LACP mode
- Learn how to configure some static LACP features

3.3.1.3 Networking Topology

In the spanning tree lab activity, the two links between S1 and S2 cannot be in the data forwarding state at the same time. To make full use of the bandwidth of the two links, you need to configure Ethernet link aggregation between S1 and S2.

Figure 3-3 Lab topology for configuring Ethernet link aggregation



3.3.2 Lab Configuration

3.3.2.1 Configuration Roadmap

1. Configure link aggregation manually.
2. Configure link aggregation in LACP mode.
3. Modify parameters to determine active links.
4. Change the load balancing mode.

3.3.2.2 Configuration Procedure

Step 1 Configure link aggregation manually.

Create an Eth-Trunk.

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

The **interface eth-trunk** command displays the view of an existing Eth-Trunk or creates an Eth-Trunk and displays its view. The number **1** in this example indicates the port number.

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

Configure the link aggregation mode of the Eth-Trunk.

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

The **mode** command configures the working mode of the Eth-Trunk, which can be LACP or manual load balancing. By default, the manual load balancing mode is used. Therefore, the preceding operation is unnecessary and is provided for demonstration purpose only.

Add a port to the Eth-Trunk.

```
[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
```

You can enter the interface view of an individual port and add it to an Eth-Trunk. You can also run the **trunkport** command in the Eth-Trunk interface view to add multiple ports to the Eth-Trunk.

```
[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.
```

Note the following points when adding physical ports to an Eth-Trunk:

- An Eth-Trunk contains a maximum of 8 member ports.
- An Eth-Trunk cannot be added to another Eth-Trunk.
- An Ethernet port can be added to only one Eth-Trunk. To add an Ethernet port to another Eth-Trunk, delete it from the original one first.
- The remote ports directly connected to the local Eth-Trunk member ports must also be added to an Eth-Trunk; otherwise, the two ends cannot communicate.
- Both endpoints of an Eth-Trunk must use the same number of physical ports, port rate, and duplex mode.

Display the status of an Eth-Trunk.

```
[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
```

Step 2 Configure link aggregation in LACP mode.

Delete member ports from an Eth-Trunk.

```
[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.
```

Before changing the working mode of an Eth-Trunk, ensure that the Eth-Trunk has no member port.

Change the aggregation mode.

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

The **mode lacp** command sets the working mode of an Eth-Trunk to LACP.

Note: The command is **mode lacp-static** in some versions.

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

Add a port to the Eth-Trunk.

```
[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.
```

Display the status of the Eth-Trunk.

```
[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
```

Step 3 In normal cases, only GigabitEthernet0/0/11 and GigabitEthernet0/0/12 need to be in the forwarding state, and GigabitEthernet0/0/10 is used as the backup. When the number of active ports falls bellow 2, the Eth-Trunk is shut down.

Set the LACP priority of S1 to make S1 an active device.

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

Configure port priorities so that GigabitEthernet0/0/11 and GigabitEthernet0/0/12 can have a higher priority.

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

Link Aggregation Control Protocol data units (LACPDUs) are sent and received by both endpoints of a link aggregation group in LACP mode.

First, the actor is elected.

1. The system priority field is compared. The default priority value is 32768, and a lower value indicates a higher priority. The endpoint with a higher priority is elected as the LACP actor.

2. If there is a tie in priority, the endpoint with a smaller MAC address becomes the actor.

After the actor is elected, the devices at both ends select active ports according to the port priority settings on the actor.

Set the upper and lower thresholds of active ports.

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

The bandwidth and status of an Eth-Trunk depend on the number of active ports. The bandwidth of an Eth-Trunk is the total bandwidth of all member ports in Up state. You can set the following thresholds to stabilize an Eth-Trunk's status and bandwidth as well as reduce the impact brought by frequent changes of member link status.

- Lower threshold: When the number of active ports falls below this threshold, the Eth-Trunk goes Down. This threshold determines the minimum bandwidth of an Eth-Trunk and is configured using the **least active-linknumber** command.
- Upper threshold: When the number of active ports reaches this threshold, the bandwidth of the Eth-Trunk will not increase even if more member links go Up. The upper threshold ensures network availability and is configured using the **max active-linknumber** command.

Enable the preemption function.

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

In LACP mode, when an active link fails, the system selects the backup link with the highest priority to replace the faulty one. If the faulty link is recovered and has a higher priority than the backup link, the recovered link can restore the active status if preemption is enabled. The **lacp preempt enable** command enables LACP preemption. By default, this function is disabled.

Display the status of the current Eth-Trunk.

```
[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
GigabitEthernet0/0/11 and GigabitEthernet0/0/12 are in active state.
```

Shut down GigabitEthernet0/0/12 to simulate a link fault.

```
[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 has become active.
```

Shut down GigabitEthernet 0/0/11 to simulate a link fault.

```
[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
```

The lower threshold for the number of active links is set to 2. Therefore, the Eth-Trunk is shut down. Although GigabitEthernet0/0/10 is Up, it is still in Unselect state.

Step 4 Change the load balancing mode.

Enable the ports disabled in the previous step.

```
[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
```

Wait about 30 seconds and check the status of Eth-Trunk 1.

```
[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
```

The preemption function is enabled on the Eth-Trunk. Therefore, when GigabitEthernet0/0/11 and GigabitEthernet0/0/12 enter the Up state, GigabitEthernet0/0/11 and GigabitEthernet0/0/12 have a higher priority than GigabitEthernet0/0/10. As a result, GigabitEthernet0/0/10 enters the Unselect state. In addition, to ensure link stability, the default preemption hold time is 30 seconds. Therefore, preemption occurs 30 seconds after the ports are enabled.

Change the load balancing mode of the Eth-Trunk to destination IP address-based load balancing.

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

To ensure proper load balancing between physical links of an Eth-Trunk and avoid link congestion, use the **load-balance** command to set the load balancing mode of the Eth-Trunk. Load balancing is valid only for outgoing traffic; therefore, the load balancing modes for the ports at both ends can be different.

----End

3.3.3 Verification

The details are not provided here.

3.3.4 Configuration Reference

Configuration on S1

```
#
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
```

Configuration on S2

```
#
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 Quiz

1. What are the requirements for the values of **least active-linknumber** and **max active-linknumber?**

3.4 Lab 4: Inter-VLAN Communication

3.4.1 Introduction

3.4.1.1 About This Lab

VLANs are separated at Layer 2 to minimize broadcast domains. To enable the communication between VLANs,Huawei provides a variety of technologies. The following two technologies are commonly used:

- Dot1q termination subinterface: Such subinterfaces are Layer 3 logical interfaces. Similar to a VLANIF interface, after a dot1q termination subinterface and its IP address are configured, the device adds the corresponding MAC address entry and sets the Layer 3 forwarding flag to implement Layer 3 communication between VLANs. A Dot1q termination subinterface applies to scenarios where a Layer 3 Ethernet port connects to multiple VLANs.
- VLANIF interface: VLANIF interfaces are Layer 3 logical interfaces. After a VLANIF interface and its IP address are configured, the device adds the MAC address and VID of the VLANIF interface to the MAC address table and sets the Layer 3 forwarding flag of the MAC address entry. When the destination MAC address of a packet matches the entry, the packet is forwarded at Layer 3 to implement Layer 3 communication between VLANs.

  In this lab activity, you will use two methods to implement inter-VLAN communication.

3.4.1.2 Objectives

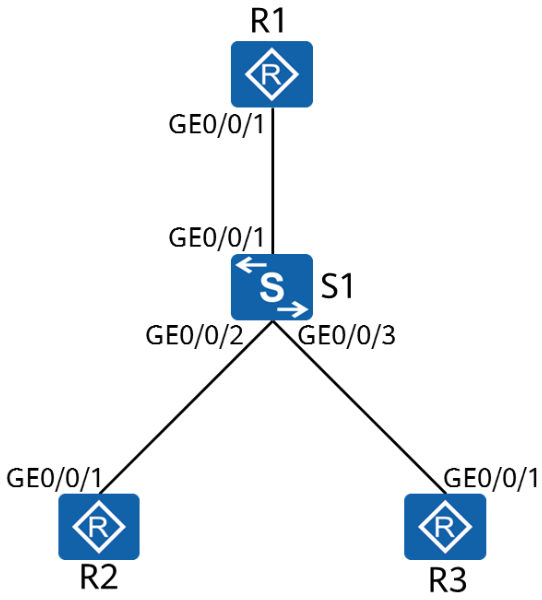
Upon completion of this task, you will be able to:

- Learn how to use Dot1q termination subinterfaces to implement inter-VLAN communication
- Learn how to use VLANIF interfaces to implement inter-VLAN communication
- Understand the forwarding process of inter-VLAN communication

3.4.1.3 Networking Topology

R2 and R3 belong to different VLANs and they need to communicate with each other through VLANIF interfaces and Dot1q termination subinterfaces.

Figure 3-4 Lab topology for inter-VLAN communication



1. Simulate terminal users on R2 and R3 and assign IP addresses 192.168.2.1/24 and 192.168.3.1/24 to the interfaces.
2. The gateway addresses of R2 and R3 are 192.168.2.254 and 192.168.3.254 respectively.
3. On S1, assign GigabitEthernet0/0/2 and GigabitEthernet0/0/3 to VLAN 2 and VLAN 3, respectively.

3.4.2 Lab Configuration

3.4.2.1 Configuration Roadmap

1. Configure Dot1q termination subinterfaces to implement inter-VLAN communication.
2. Configure VLANIF interfaces to implement inter-VLAN communication.

3.4.2.2 Configuration Procedure

Step 1 Complete basic device configuration.

Name R1, R2, R3, and S1.

The details are not provided here.

Configure IP addresses and gateways for R2 and R3.

```
<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
```

Configure a default route (equivalent to a gateway) for the device.

```
<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
```

On S1, assign R2 and R3 to different VLANs.

```
[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
```

Step 2 Configure Dot1q termination subinterfaces to implement INter-VLAN communication.

Configure a trunk port on S1.

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
The link between S1 and R1 must allow packets from VLAN 2 and VLAN 3 to pass through because R1 needs
to terminate the VLAN tags of packets exchanged between VLANs.
```

Configure a dot1q termination subinterface on R1.

```
[R1]interface GigabitEthernet 0/0/1.2
```

A subinterface is created and the subinterface view is displayed. In this example, **2** indicates the subinterface number. It is recommended that the subinterface number be the same as the VLAN ID.

```
[R1-GigabitEthernet0/0/1.2]dot1q termination vid 2
```

The **dot1q termination vid** *vlan-id* command configures the VLAN ID for Dot1q termination on a subinterface.

In this example, when GigabitEthernet0/0/1 receives data tagged with VLAN 2, it sends the data to subinterface 2 for VLAN termination and subsequent processing. The data sent from subinterface 2 is also tagged with VLAN 2.

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

Subinterfaces for VLAN tag termination cannot forward broadcast packets and automatically discard them upon receiving. To allow such subinterfaces to forward broadcast packets, the ARP broadcast function must be enabled using the **arp broadcast enable** command. By default, this function is enabled on some devices.

```
[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
```

Test the connectivity between VLANs.

```
<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
VLAN 2 and VLAN 3 can communicate with each other.
```

Step 3 Configure VLANIF interfaces to enable inter-VLAN communication.

Delete the configuration in the previous step.

```
[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
```

Create a VLANIF interface on S1.

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

The **interface vlanif** *vlan-id* command creates a VLANIF interface and displays the VLANIF interface view. You must create a VLAN before configuring a VLANIF interface.

```
[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
```

Test the connectivity between VLANs.

```
<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
VLAN 2 and VLAN 3 can communicate with each other.
```

----End

3.4.3 Verification

The details are not provided here.

3.4.4 Configuration Reference

Configuration on S1

```
#
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
```

Configuration on R2

```
#
 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
```

Configuration on R3

```
#
 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 Quiz

1. If R2 needs to access the network connected to R1, what configuration needs to be performed on S1?
2. As a Layer 3 interface, when will a VLANIF interface go Up?

4 Network Security Basics and Network Access

4.1 Lab 1: ACL Configuration

4.1.1 Introduction

4.1.1.1 About This Lab

An Access Control List (ACL) is a collection of one or more rules. A rule refers to a judgment statement that describes a packet matching condition, which may be a source address, destination address, or port number.

An ACL is a rule-based packet filter. Packets matching an ACL are processed based on the policy defined in the ACL.

4.1.1.2 Objectives

Upon completion of this task, you will be able to:

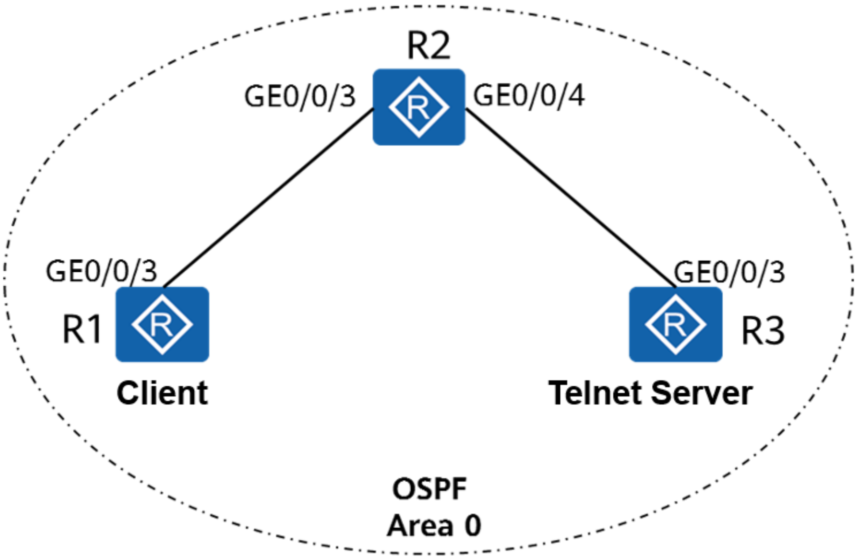
- Learn how to configure ACLs
- Learn how to apply an ACL on an interface
- Understand the basic methods of traffic filtering

4.1.1.3 Networking Topology

As shown in the networking diagram, R3 functions as the server, R1 functions as the client, and they are reachable to reach other. The IP addresses of the physical interfaces connecting R1 and R2 are 10.1.2.1/24 and 10.1.2.2/24 respectively, and the IP addresses of the physical interfaces connecting R2 and R3 are 10.1.3.2/24 and 10.1.3.1/24, respectively. In addition, two logical interfaces LoopBack 0 and LoopBack 1 are created on R1 to simulate two client users. The IP addresses of the two interfaces are 10.1.1.1/24 and 10.1.4.1/24, respectively.

One user (Loopback 1 of R1) needs to remotely manage R3. You can configure Telnet on the server, configure password protection, and configure an ACL to ensure that only the user that meets the security policy can log in to R3.

Figure 4-1 Lab topology for ACL configuration



4.1.2 Lab Configuration

4.1.2.1 Configuration Roadmap

1. Configure IP addresses.
2. Configure OSPF to ensure network connectivity.
3. Create an ACL to match desired traffic.
4. Configure traffic filtering.

4.1.2.2 Configuration Procedure

Step 1 Configure IP addresses.

Configure IP addresses for R1, R2, and R3.

```
[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
```

Step 2 Configure OSPF to ensure network connectivity.

Configure OSPF on R1, R2, and R3 and assign them to area 0 to enable connectivity.

```
[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
```

Run the ping command on R3 to test network connectivity.

```
<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
```

Step 3 Configuration R3 as a server.

Enable the Telnet function on R3, set the user level to 3, and set the login password to Huawei@123.

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

The **telnet server enable** command enables the Telnet service.

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

The **user-interface** command displays one or multiple user interface views.

The Virtual Type Terminal (VTY) user interface manages and monitors users logging in using Telnet or SSH.

```
[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
```

Step 4 Configure an ACL to match desired traffic.

Method 1: Configure an ACL on the VTY interface of R3 to allow R1 to log in to R3 through Telnet using the IP address of loopback 1.

Configure an ACL on R3.

```
[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
```

Filter traffic on the VTY interface of R3.

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

Display the ACL configuration on R3.

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

The **display acl** command displays the ACL configuration.

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

An advanced ACL is created. It is numbered 3000 and contains two rules.

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

The step between ACL rule numbers is 5.

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

Rule 5 allows matched traffic to pass through. If no packet matches the rule, the **matches** field is not displayed.

```
 rule 10 deny tcp
```

Method 2: Configure an ACL on the physical interface of R2 to allow R1 to log in to R3 through Telnet from the IP address of the physical interface.

Configure an ACL on R2.

```
[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
```

Filter traffic on GE0/0/3 of R3.

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

Display the ACL configuration on R2.

```
[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)
```

Rule 5 allows matched traffic to pass through, and 21 packets have matched the rule.

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

----End

4.1.3 Verification

Test the Telnet access and verify the ACL configuration.

1. On R1, telnet to the server with the source IP address 10.1.1.1 specified.

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

The **telnet** command enables a user to use the Telnet protocol to log in to another device.

-a *source-ip-address*: specifies the source IP address. Users can communicate with the server from the specified IP address.

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

2. On R1, telnet to the server with the source IP address 10.1.4.1 specified.

```
<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 Configuration Reference (Method 1)

Configuration on R1

```
#
 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
```

Configuration on R2

```
#
 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
```

Configuration on R3

```
#
 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 Configuration Reference (Method 2)

Configuration on R1

```
#
 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
```

Configuration on R2

```
#
 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
```

Configuration on R3

```
#
 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 Quiz

R3 functions as both a Telnet server and an FTP server, the IP address of loopback 0 on R1 must be used to access only the FTP service, and the IP address of loopback 1 on R1 must be used to remotely manage R3 using Telnet.

Configure an ACL to meet the requirements.

4.2 Lab 2: Local AAA Configuration

4.2.1 Introduction

4.2.1.1 About This Lab

Authentication, authorization, and accounting (AAA) provides a management mechanism for network security.

AAA provides the following functions:

- Authentication: verifies whether users are permitted to access the network.
- Authorization: authorizes users to use particular services.
- Accounting: records the network resources used by users.

Users can use one or more security services provided by AAA. For example, if a company wants to authenticate employees that access certain network resources, the network administrator only needs to configure an authentication server. If the company also wants to record operations performed by employees on the network, an accounting server is needed.

In summary, AAA authorizes users to access specific resources and records user operations. AAA is widely used because it features good scalability and facilitates centralized user information management. AAA can be implemented using multiple protocols. RADIUS is most frequently used in actual scenarios.

In this lab activity, you will configure local AAA to manage and control resources for remote Telnet users.

4.2.1.2 Objectives

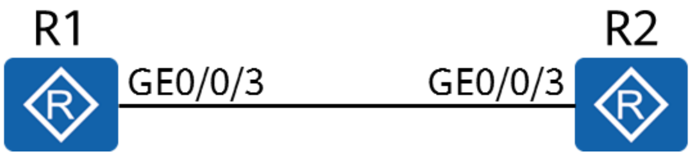
Upon completion of this task, you will be able to:

- Learn how to configure local AAA
- Learn how to create a domain
- Learn how to create a local user
- Understand domain-based user management

4.2.1.3 Networking Topology

R1 functions as a client, and R2 functions as a network device. Access to the resources on R2 needs to be controlled. Therefore, you need to configure local AAA authentication on R1 and R2 and manage users based on domains, and configure the privilege level for authenticated users.

Figure 4-2 Lab topology for local AAA configuration



4.2.2 Lab Configuration

4.2.2.1 Configuration Roadmap

1. Configure an AAA scheme.
2. Create a domain and apply the AAA scheme to the domain.
3. Configure local users.

4.2.2.2 Configuration Procedure

Step 1 Complete basic device configuration.

Name R1 and R2.

The details are not provided here.

Configure IP addresses for R1 and R2.

```
[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
```

Step 2 Configure an AAA scheme.

Configure authentication and authorization schemes.

```
[R2-aaa]aaa
Enter the AAA view.
[R2-aaa]authentication-scheme datacom
Info: Create a new authentication scheme.
Create an authentication scheme named datacom.
[R2-aaa-authen-datacom]authentication-mode local
Set the authentication mode to local authentication.
[R2-aaa-authen-datacom]quit
[R2-aaa]authorization-scheme datacom
Info: Create a new authorization scheme.
Create an authorization scheme named datacom.
[R2-aaa-author-datacom]authorization-mode local
Set the authorization mode to local authorization.
[R2-aaa-author-datacom]quit
```

A device functioning as an AAA server is called a local AAA server, which can perform authentication and authorization, but not accounting.

The local AAA server requires a local user database, containing the user name, password, and authorization information of local users. A local AAA server is faster and cheaper than a remote AAA server, but has a smaller storage capacity.

Step 3 Create a domain and apply the AAA scheme to the domain.

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

The devices manage users based on domains. A domain is a group of users and each user belongs to a domain. The AAA configuration for a domain applies to the users in the domain. Create a domain named datacom.

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

The authentication scheme named datacom is used for users in the domain.

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

The authorization scheme named datacom is used for users in the domain.

Step 4 Configure local users.

Create a local user and password.

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

If the user name contains a delimiter of at sign (@), the character string before the at sign is the user name and the character string following the at sign is the domain name. If the value does not contain the at sign, the entire character string represents the user name and the domain name is the default one.

Configure the parameters for the local user, such as access type and privilege level.

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

The **local-user service-type** command configures the access type for a local user. After you specify the access type of a user, the user can successfully log in only when the configured access type is used. If the access type is set to telnet, the user cannot access the device through a web page. Multiple access types can be configured for a user.

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

The privilege level of the local user is specified. Only commands within the specified privilege level or a lower level are available for a user.

Step 5 Enable the telnet function on R2.

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

The Telnet server function is enabled on the device. This function is enabled by default on some devices.

```
[R2]user-interface vty 0 4
[R2-ui-vty0-4]authentication-mode aaa
```

The **authentication-mode** command configures an authentication mode for accessing the user interface. By default, the user authentication mode of the VTY user interface is not configured. An authentication mode must be configured for the login interface. Otherwise, users will not be able to log in to the device.

Step 6 Verify the configuration.

Telnet R2 from R1.

```
<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>
```

R1 has logged in to R2.

Display the online users on R2.

```
[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
```

----End

4.2.3 Verification

The details are not provided here.

4.2.4 Configuration Reference

Configuration on R1

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

Configuration on R2

```
#
 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 Quiz

The details are not provided here.

4.3 Lab 3: NAT Configuration

4.3.1 Introduction

4.3.1.1 About This Lab

Network Address Translation (NAT) translates the IP address in an IP packet header to another IP address. As a transitional plan, NAT enables address reuse to alleviate the IPv4 address shortage. In addition to solving the problem of IP address shortage, NAT provides the following advantages:

- Protects private networks against external attacks.
- Enables and controls the communication between private and public networks.

  In this lab activity, you will configure NAT to understand its principle.

4.3.1.2 Objectives

Upon completion of this task, you will be able to:

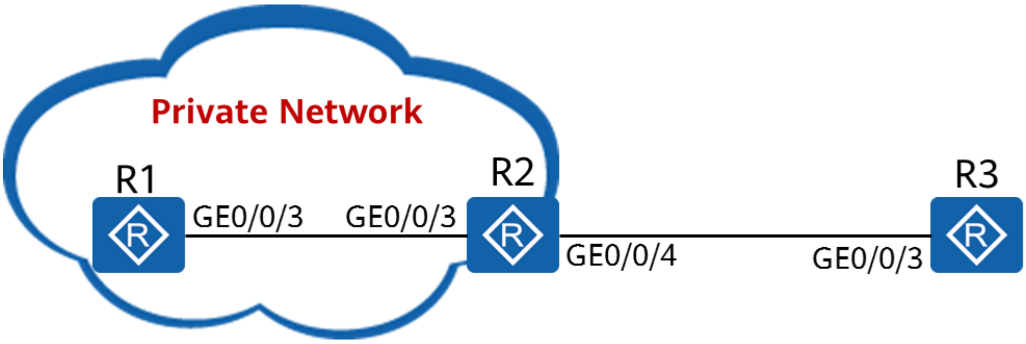
- Learn how to configure dynamic NAT
- Learn how to configure Easy IP
- Learn how to configure NAT server

4.3.1.3 Networking Topology

Due to the shortage of IPv4 addresses, enterprises usually use private IPv4 addresses. However, enterprise network users often need to access the public network and provide services for external users. In this case, you need to configure NAT to meet these requirements.

1. The network between R1 and R2 is an intranet and uses private IPv4 addresses.
2. R1 functions as the client, and R2 functions as the gateway of R1 and the egress router connected to the public network.
3. R3 simulates the public network.

Figure 4-3 Lab topology for NAT configuration



4.3.2 Lab Configuration

4.3.2.1 Configuration Roadmap

1. Configure dynamic NAT.
2. Configure Easy IP.
3. Configure NAT server.

4.3.2.2 Configuration Procedure

Step 1 Complete basic configurations.

Configure IP addresses and routes.

```
[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
```

Configure the Telnet function on R1 and R3 for subsequent verification.

```
[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
```

Test connectivity.

```
[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
```

R1 cannot communicate with R3 because no route to 192.168.1.0/24 is configured on R3.

Moreover, routes to private networks cannot be configured on R3.

Step 2 The enterprise obtains the public IP addresses ranging from 1.2.3.10 to 1.2.3.20 and needs the dynamic NAT function.

Configure a NAT address pool.

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

The **nat address-group** command configures a NAT address pool. In this example, 1 indicates the number of the address pool. The address pool must be a set of consecutive IP addresses. When internal data packets reach the edge of the private network, the private source IP addresses will be translated into public IP addresses.

Configure an ACL.

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

Configure dynamic NAT on GigabitEthernet0/0/4 of R2.

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

The **nat outbound** command associates an ACL with an NAT address pool. The IP addresses of packets matching the ACL will be translated into an address in the address pool. If the address pool has sufficient addresses, you can add the **no-pat** argument to enable one-to-one address translation. In this case, only the IP addresses of data packets are translated, and the ports are not translated.

Test connectivity.

```
[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

# Telnet R3 from R1 to simulate TCP traffic.
<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>
```

Display the NAT session table on R2.

```
[R2]display nat session all
   NAT Session Table Information:
      Protocol             : TCP(6)
      SrcAddr   Port Vpn   : 192.168.1.1     62185     //Source IP address and source port before NAT
      DestAddr Port Vpn    : 1.2.3.254       23
      NAT-Info
      New SrcAddr          : 1.2.3.11                  //Source IP address after NAT
      New SrcPort          : 49149                     //Source port after NAT
      New DestAddr         : ----
      New DestPort         : ----

  Total : 1
```

Although R3 does not have a route to R1, R3 sends the data to the translated source address 1.2.3.11. After receiving the data, R2 translates the source address to the address of R1 based on the data in the NAT session table and forwards the data. Therefore, R1 can **initiate** access to R3.

Step 3 If the IP address of GigabitEthernet0/0/4 on R2 is dynamically assigned (e.g. through DHCP or PPPoE dialup), you need to configure Easy IP.

Delete the configuration in the previous step.

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

Configure Easy IP.

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

Test connectivity.

```
[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
```

Telnet R3 from R1 to simulate TCP traffic.

```
[R2]display nat session all
 NAT Session Table Information:
       Protocol                  : TCP(6)
       SrcAddr   Port Vpn        : 192.168.1.1       58546              //Source IP address and source port before NAT
       DestAddr Port Vpn         : 1.2.3.4       23
       NAT-Info
       New SrcAddr               : 1.2.3.4      //Source IP address after NAT, that is, the address of GigabitEthernet 0/0/4 on R2
       New SrcPort               : 49089                     //Source port after NAT
       New DestAddr              : ----
       New DestPort              : ----

   Total : 1
```

Step 4 R3 needs to provide network services (telnet in this example) for users on the public network. Because R3 does not have a public IP address, you need to configure NAT server on the outbound interface of R2.

Configure NAT server on R2.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4] nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
```

The **nat server** command defines a mapping table of internal servers so that external users can access internal servers through address and port translation. You can configure an internal server so that users on an external network can **initiate** access to the internal server. When a host on an external network sends a connection request to the public address (global-address) of the internal NAT server, the NAT server translates the destination address of the request into a private address (inside-address) and forwards the request to the server on the private network.

Telnet R1 from R3.

```
<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>
```

Display the NAT session table on R2.

```
 [R2]display nat session all
           Protocol                  : TCP(6)
           SrcAddr   Port Vpn        : 1.2.3.254       61359
           DestAddr Port Vpn         : 1.2.3.4       2323              //Destination IP address and port before NAT
           NAT-Info
           New SrcAddr               : ----
```

```
          New SrcPort              : ----
          New DestAddr             : 192.168.1.1           //Destination IP address after NAT, that is, the IP
address of R1
          New DestPort             : 23                   //Destination port after NAT

  Total : 1
```

----End

4.3.3 Verification

The details are not provided here.

4.3.4 Configuration Reference

Configuration on R1

```
#
 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
```

Configuration on R2

```
#
 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
```

Configuration on R3

```
#
 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 Quiz

1. When configuring NAT Server, should the destination ports before translation be the same as those after translation?

5 Basic Network Service and Application Configuration

5.1 Lab 1: FTP Configuration

5.1.1 Introduction

5.1.1.1 About This Lab

Multiple file management modes are supported,

such as File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), and Secure File Transfer Protocol (SFTP). You can select one based on service and security requirements.

A device can work as either a server or a client.

- If the device works as a server, you can access the device from a client to manage files on the device and transfer files between the client and device.
- If the device works as a client, you can access another device (the server) from the device to manage and transfer files.

5.1.1.2 Objectives

Upon completion of this task, you will be able to:

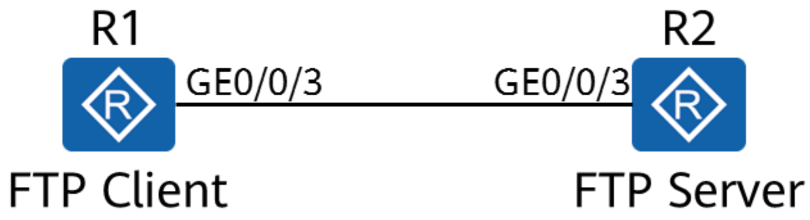
- Understand how an FTP connection is established
- Learn how to configure FTP server parameters
- Learn how to transfer files to an FTP server

5.1.1.3 Networking Topology

R1 needs to manage the configuration file of R2.

R1 functions as the FTP client, and R2 functions as the FTP server.

Figure 5-1 Lab topology for FTP configuration



5.1.2 Lab Configuration

5.1.2.1 Configuration Roadmap

1. Configure the FTP server function and parameters.
2. Configure local FTP users.
3. Log in to the FTP server from the FTP client.
4. Perform file operations from the FTP client.

5.1.2.2 Configuration Procedure

Step 1 Complete basic device configuration.

Name the devices.

The details are not provided here.

Configure the device IP addresses.

```
[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
```

Save the configuration file for subsequent verification.

```
<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
```

Display the current file list.

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

  Idx   Attr     Size(Byte)     Date   Time(LMT)       FileName
    0   -rw-    126,538,240     Jul 04 2016 17:57:22    AR6120_V300R022C00SPC100.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    AR6120_V300R022C00SPC100.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)
The configuration files of the two devices are saved successfully.
```

Step 2 Configure the FTP server function and parameters on R2.

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

The **ftp server enable** command enables the FTP server function. By default, the FTP function is disabled.

Other optional configuration parameters include the port number of the FTP server, source IP address of the FTP server, and maximum idle time of FTP connections.

Step 3 Configure local FTP users.

```
[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
```

The user level is specified. The user level must be set to 3 or higher to ensure successful connection establishment.

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

The authorized directory of the FTP user is specified. This directory must be specified. Otherwise, the FTP user cannot log in to the system.

Step 4 Log in to the FTP server from the FTP client.

Log in to the 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]
You have logged in to the file system of R2.
```

Step 5 Perform operations on the file systems on R2.

Configure the transmission mode.

```
 [R1-ftp]ascii
200 Type set to A.
```

Files can be transferred in ASCII or binary mode.

ASCII mode is used to transfer plain text files, and binary mode is used to transfer application files, such as system software, images, video files, compressed files, and database files. The configuration file to be downloaded is a text file. Therefore, you need to set the mode to ASCII. The default file transfer mode is ASCII. This operation is for demonstration purpose only.

Download the configuration file.

```
[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.
```

Delete the configuration file.

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

Upload the configuration file.

```
[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.
```

Close the FTP connection.

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

<R1>
```

----End

5.1.3 Verification

Display the file directories of R1 and R2.

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

  Idx  Attr     Size(Byte)   Date        Time(LMT)   FileName
    0  -rw-    126,538,240   Jul 04 2016 17:57:22   AR6120_V300R022C00SPC100.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   AR6120_V300R022C00SPC100.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 Configuration Reference

Configuration on R1

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

Configuration on R2

```
#
 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 Quiz

1. Does FTP work in active or passive mode by default?

5.2 Lab 2: DHCP Configuration

5.2.1 Introduction

5.2.1.1 About This Lab

The Dynamic Host Configuration Protocol (DHCP) dynamically configures and uniformly manages IP addresses of hosts. It simplifies network deployment and scale-out, even for small networks.

DHCP is defined in RFC 2131 and uses the client/server communication mode. A client (DHCP client) requests configuration information from a server (DHCP server), and the server returns the configuration information allocated to the client.

DHCP supports dynamic and static IP address allocation.

- Dynamic allocation: DHCP allocates an IP address with a limited validity period (known as a lease) to a client. This mechanism applies to scenarios where hosts temporarily access the network and the number of idle IP addresses is less than the total number of hosts.
- Static allocation: DHCP allocates fixed IP addresses to clients as configured. Compared with manual IP address configuration, DHCP static allocation prevents manual configuration errors and enables unified maintenance and management.

5.2.1.2 Objectives

Upon completion of this task, you will be able to:

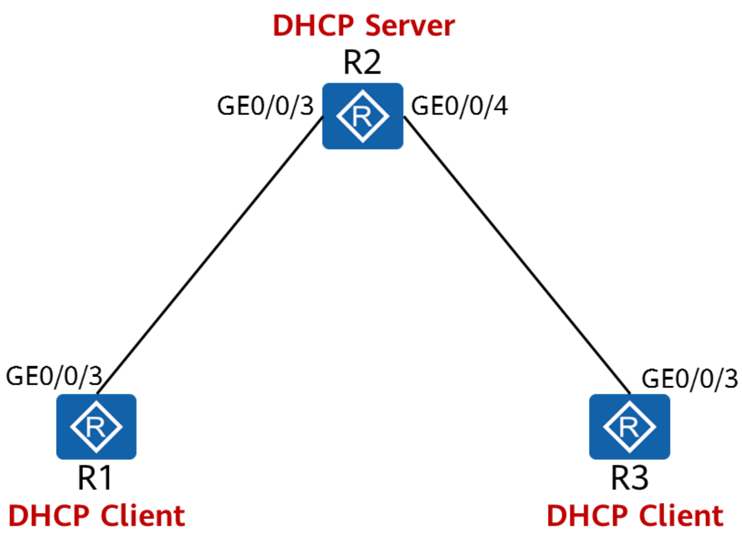
- Learn how to configure an interface address pool on the DHCP server
- Learn how to configure a global address pool on the DHCP server
- Learn how to use DHCP to allocate static IP addresses

5.2.1.3 Networking Topology

To reduce the workload of IP address maintenance and improve IP address utilization, an enterprise plans to deploy DHCP on the network.

1. Configure R1 and R3 as DHCP clients.
2. Configure R2 as the DHCP server to assign IP addresses to R1 and R3.

Figure 5-2 Lab topology for DHCP configuration



5.2.2 Lab Configuration

5.2.2.1 Configuration Roadmap

1. Configure the DHCP server.
2. Configure the DHCP clients.

5.2.2.2 Configuration Procedure

Step 1 Complete basic configurations.

Configure interface addresses on R2.

```
[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
```

Step 2 Enable DHCP.

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

The **dhcp enable** command must be executed before executing any other DHCP-related commands, regardless for DHCP servers or clients.

```
[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.
```

Step 3 Configure an address pool.

Configure an IP address pool on GE 0/0/3 of R2 to assign an IP address to R1.

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

The **dhcp select interface** command enables an interface to use the interface address pool. If you do not run this command, parameters related to the interface address pool cannot be configured.

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

The **dhcp server dns-list** command configures DNS server addresses for an interface address pool. A maximum of eight DNS server addresses can be configured. These IP addresses are separated by spaces.

Configure a global address pool.

```
[R2]ip pool GlobalPool
Info: It's successful to create an IP address pool.
# Create an IP address pool named GlobalPool.
[R2-ip-pool-GlobalPool]network 10.0.23.0 mask 24
```

The **network** command specifies a network address for a global address pool.

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

The **gateway-list** command configures a gateway address for a DHCP client. After R3 obtains an IP address, it generates a default route with the next-hop address being 10.0.23.2.

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

The **lease** command specifies the lease for IP addresses in a global IP address pool. If the lease is set to **unlimited**, the lease is unlimited. By default, the lease of IP addresses is one day.

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

The **static-bind** command binds an IP address in a global address pool to a MAC address of a client. 00e0-fc6f-6d1f is the MAC address of GigabitEthernet0/0/3 on R3. You can run the **display interface GigabitEthernet0/0/3** command on R3 to display the MAC address of GigabitEthernet0/0/3. After the command is executed, R3 obtains the fixed IP address of 10.0.23.3.

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

Step 4 Enable the DHCP server function on GigabitEthernet 0/0/4 of R2 to assign an IP address to R3.

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

The **dhcp select global** command enables an interface to use the global address pool. After receiving a request from a DHCP client, the interface searches the global address pool for an available IP address and assigns the IP address to the DHCP client.

Step 5 Configure a 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
```

----End

5.2.3 Verification

5.2.3.1 Display the IP addresses and routes of R1 and R3.

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

Only key information is provided here. The command output shows that R1 has obtained an IP address.

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

No.   Type     IP Address
1      D      10.0.12.2
```

Only key information is provided here. The command output shows that R1 has obtained the DNS address.

```
[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
```

Only key information is provided here. The command output shows that R1 has obtained the default route.

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

Only key information is provided here. The command output shows that R3 has obtained a fixed IP address.

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

Only key information is provided here. The command output shows that R3 has obtained the DNS address.

```
[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
```

Only key information is provided here. The command output shows that R3 has obtained the default route.

5.2.3.2 Display the address allocation on R2.

```
[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
 -----------------------------------------------------------------------
```

The **display ip pool** command displays the address pool configuration information, including the name, lease, lock status, and IP address status.

```
[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
 -----------------------------------------------------------------------
```

When an interface address pool is configured, the name of the address pool is the interface name. The allocated gateway address is the IP address of the interface and cannot be changed.

5.2.4 Configuration Reference

Configuration on R1

```
#
 sysname R1
```

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

Configuration on R2

```
#
 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
```

Configuration on R3

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

5.2.5 Quiz

1. What are the differences between the application scenarios of a global address pool and those of an interface address pool?
2. If there are multiple global address pools, how do you determine the global address pool for a DHCP client?

6 Creating a WLAN

6.1 Introduction

6.1.1 About This Lab

Wired LANs are expensive and lack mobility. The increasing demand for portability and mobility requires WLAN technologies. WLAN is now the most cost-efficient and convenient network access mode. WLAN allows users to move within the covered area.

In this lab activity, you will configure a WLAN using an AC and fit APs.

6.1.2 Objectives

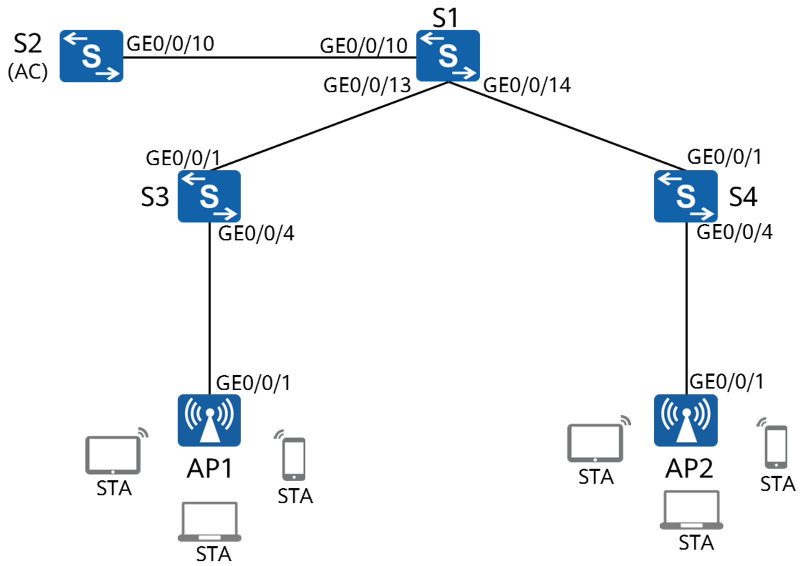
Upon completion of this task, you will be able to:

- Learn how to authenticate APs
- Learn how to configure WLAN profiles
- Understand the basic WLAN configuration process

6.1.3 Networking Topology

1. The S2 switch supports the WLAN-AC function. If the switch does not support the WLAN-AC function, use a common AC to replace the switch. The AC in the following content is an S2 switch.
2. The AC is deployed in an out-of-path mode and is on the same Layer 2 network as the APs.
3. The AC functions as a DHCP server to assign IP addresses to APs, S1 functions as a DHCP server to assign IP addresses to stations (STAs).
4. Service data is directly forwarded.

Figure 6-1 Lab topology for creating a WLAN



6.1.4 Data Planning

An enterprise needs to create a WLAN to provide mobility in workplace.

Table 6-1 AC data planning

Item	Configuration
AP management VLAN	VLAN100
Service VLAN	VLAN101
DHCP server	The AC functions as a DHCP server to allocate IP addresses to APs.
	S1 functions as a DHCP server to allocate IP addresses to STAs. The default gateway address of STAs is 192.168.101.254.
IP address pool for APs	192.168.100.1-192.168.100.253/24
IP address pool for STAs	192.168.101.1-192.168.101.253/24
IP address of the AC's source interface	VLANIF100: 192.168.100.254/24
AP group	Name: ap-group1
	Referenced profiles: VAP profile **HCIA-WLAN** and regulatory domain profile **default**

Item	Configuration
Regulatory domain profile	Name: default
	Country code: CN
SSID profile	Name: HCIA-WLAN
	SSID name: HCIA-WLAN
Security profile	Name: HCIA-WLAN
	Security policy: WPA-WPA2+PSK+AES
	Password: HCIA-Datacom
VAP profile	Name: HCIA-WLAN
	Forwarding mode: direct forwarding
	Service VLAN: VLAN 101
	Referenced profiles: SSID profile **HCIA-WLAN** and security profile **HCIA-WLAN**

6.2 Lab Configuration

6.2.1 Configuration Roadmap

1. Configure the connectivity of the wired network.
2. Configure the APs and bring them online.
   (1) Create AP groups and add APs of the same configuration to the same group for unified configuration.
   (2) Configure AC system parameters, including the country code and source interface used by the AC to communicate with the APs.
   (3) Configure the AP authentication mode and import the APs to bring them online.
3. Configure WLAN service parameters and deliver them to APs for STAs to access the WLAN.

6.2.2 Configuration Procedure

Step 1 Complete basic device configurations.

Name the devices (name S2 in the topology **AC**)

The details are not provided here.

Shut down unnecessary ports between S1 and the AC. This step applies only to the environment described in *HCIA-Datacom Lab Construction Guide V1.0*.

```
[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
```

Enable the PoE function on S3 and S4 ports connected to APs.

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

The **poe enable** command enables the PoE function on a port. When a port detects a powered device (PD) connected to it, the port supplies power to the PD. By default, the PoE function is enabled. Therefore, this command is unnecessary and is provided for demonstration purpose only.

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

Step 2 Configure the wired network.

Configure VLANs.

```
[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
```

Configure interface IP addresses.

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

Gateway for STAs

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

This operation is for subsequent test only.

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

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

Configure DHCP.

```
[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.
IP address pool for STAs
[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.
```

```
IP address pool for APs
[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 is the DHCP server for STAs and the AC is the DHCP server for APs.

Step 3 Configure the APs to bring them online.

Create an AP group and name it ap-group1.

```
[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
```

Create a regulatory domain profile, and set the AC country code in the profile.

```
[AC]wlan
[AC-wlan-view]regulatory-domain-profile name default
```

A regulatory domain profile provides configurations of country code, calibration channel, and calibration bandwidth for an AP.

The default regulatory domain profile is named **default**. Therefore, the default profile is displayed.

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

A country code identifies the country in which the APs are deployed. Different countries require different AP radio attributes, including the transmit power and supported channels. Correct country code configuration ensures that radio attributes of APs comply with local laws and regulations. By default, the country code CN is configured.

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

Bind the regulatory domain profile to an AP group.

```
[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
```

The **regulatory-domain-profile** command in the AP group view binds a regulatory domain profile to an AP or AP group. By default, regulatory domain profile **default** is bound to an AP group, but no regulatory domain profile is bound to an AP. In the default regulatory domain profile, the country code is CN. Therefore, the 2.4 GHz calibration channels include channels 1, 6, and 11, and the 5 GHz calibration channels include channels 149, 153, 157, 161, and 165. Therefore, this step and the previous step can be skipped.

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

Specify a source interface on the AC for establishing CAPWAP tunnels.

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

The **capwap source interface** command configures the interface used by the AC to set up CAPWAP tunnels with APs.

Import APs to the AC and add the APs to AP group **ap-group1**.

APs can be added to an AC in the following ways:

- Manual configuration: Specify the MAC addresses and serial numbers (SNs) of APs on the AC in advance. When APs are connected the AC, the AC finds that their MAC addresses and SNs match the preconfigured ones and establish connections with them.
- Automatic discovery: When the AP authentication mode is set to no authentication, or the AP authentication mode is set to MAC or SN authentication and the MAC addresses or SNs are whitelisted, the AC automatically discovers connected APs and establish connections with them.
- Manual confirmation: If the AP authentication mode is set to MAC or SN authentication and MAC address or SN of a connected AP is not included in the whitelist on the AC, the AC adds the AP to the list of unauthorized APs. You can manually confirm the identify of such an AP to bring it online.

```
[AC]wlan
[AC-wlan-view]ap auth-mode mac-auth
```

The **ap auth-mode** command configures the AP authentication mode. Only authenticated APs can go online. The authentication modes include MAC address authentication, SN authentication, and no authentication. The default AP authentication mode is MAC address authentication.

Note: For MAC address and SN information of an AP, check the MAC address label and SN label in the package.

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

The **ap-id** command adds an AP or displays the AP view.

The **ap-mac** argument specifies MAC address authentication, and the **ap-sn** argument specifies SN authentication.

In the AP view, you can enter ap-id to enter the corresponding AP view.

```
[AC-wlan-ap-0]ap-name ap1
```

The **ap-name** command configures the name of an AP. AP names must be unique. If the AP name is not configured, the default name is the MAC address of the AP.

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

The **ap-group** command configures the group for an AP. The AC delivers the configuration to the APs. For example, if AP1 is added to ap-group1, the regulatory domain profile, radio profile, and VAP profile associated with ap-group1 are delivered to AP1. By default, an AP is not added to any group. When an AP is added to a group or the group of an AP changes, the group configuration will be delivered automatically by the AC, and the AP will automatically restart to join the group.

```
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            //Enter y to confirm.
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            //Enter y to confirm.
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-1]quit
```

Display the information about the current AP.

```
[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   AirEngine5761-11   nor      0      30M:4S
1      00e0-fc0f-07a0 ap2    ap-group1       192.168.100.170   AirEngine5761-11   nor      0      31M:31S
---------------------------------------------------------------------------------------------------------------
Total: 2
```

The **display ap** command displays AP information, including the IP address, model (AirEngine5761-11), status (normal), and online duration of the AP.

In addition, you can add **by-state** *state* or **by-ssid** *ssid* to filter APs in a specified state or using a specified SSID.

The command output shows that the two APs are working properly. (For more status description, see the appendix of this lab.)

Step 4 Configure WLAN service parameters.

Create security profile **HCIA-WLAN** and configure a security policy.

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

The **security psk** command configures WPA/WPA2 pre-shared key (PSK) authentication and encryption.

Currently, both WPA and WPA2 are used. User terminals can be authenticated using either WPA or WPA2. The PSK is set to **HCIA-Datacom**. User data is encrypted using the AES encryption algorithm.

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

Create SSID profile **HCIA-WLAN** and set the SSID name to **HCIA-WLAN**.

```
[AC]wlan
[AC-wlan-view]ssid-profile name HCIA-WLAN
SSID profile HCIA-WLAN is created.
[AC-wlan-ssid-prof-HCIA-WLAN]ssid HCIA-WLAN
The SSID name is set to HCIA-WLAN.
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-HCIA-WLAN]quit
```

Create VAP profile **HCIA-WLAN**, configure the data forwarding mode and service VLAN, and apply the security profile and SSID profile to the VAP profile.

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

The **vap-profile** command creates a VAP profile.

You can configure the data forwarding mode in a VAP profile and bind the SSID profile, security profile, and traffic profile to the VAP profile.

```
[AC-wlan-vap-prof-HCIA-WLAN]forward-mode direct-forward
```

The **forward-mode** command configures the data forwarding mode in a VAP profile. By default, the data forwarding mode is direct forwarding.

```
[AC-wlan-vap-prof-HCIA-WLAN]service-vlan vlan-id 101
```

The **service-vlan** command configures the service VLAN of a VAP. After a STA accesses a WLAN, the user data forwarded by the AP carries the **service-VLAN** tag.

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

Bind the VAP profile to the AP group and apply configurations in VAP profile **HCIA-WLAN** to radio 0 and radio 1 of the APs in the AP group.

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

The **vap-profile** command binds a VAP profile to a radio. After this command is executed, all configurations in the VAP, including the configurations in the profiles bound to the VAP, are delivered to the radios of APs.

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

----End

6.3 Verification

1. Use an STA to access the WLAN with the SSID of **HCIA-WLAN**. Check the IP address obtained by the STA and ping the IP address (10.0.1.1) of LoopBack0 on S1.
2. When the STA is connected to the AC, run the **display station all** command on the AC to check the STA information.

6.4 Configuration Reference

Configuration on S1

```
#
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
```

Configuration on the AC

```
#
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
```

Configuration on S3

```
#
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
```

Configuration on S4

```
#
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 Quiz

1. In the current networking, if GigabitEthernet0/0/10 of the AC does not allow packets from VLAN 101 to pass through, what is the impact on the access of STAs to S1? Why? What if tunnel forwarding is used?
2. If STAs connected to AP1 and AP2 need to be assigned to different VLANs, what operations need to be performed on the AC?

6.6 Appendix

AP State	Description
commit-failed	WLAN service configurations fail to be delivered to the AP after the AP goes online on an AC.
committing	WLAN service configurations are being delivered to the AP after the AP goes online on an AC.
config	WLAN service configurations are being delivered to the AP when the AP is going online on an AC.

AP State	Description
config-failed	WLAN service configurations fail to be delivered to the AP when the AP is going online on an AC.
download	The AP is in upgrade state.
fault	The AP fails to go online.
idle	It is the initialization state of the AP before it establishes a link with the AC for the first time.
name-conflicted	The name of the AP conflicts with that of an existing AP.
normal	The AP is working properly.
standby	The AP is in normal state on the standby AC.
unauth	The AP is not authenticated.

7 Creating an IPv6 Network

7.1 Introduction

7.1.1 About This Lab

Internet Protocol Version 6 (IPv6) is also called IP Next Generation (IPng). Designed by the Internet Engineering Task Force (IETF), IPv6 is an upgraded version of IPv4.

IPv6 have the following advantages over IPv4:

- Infinite address space
- Hierarchical address structure
- Plug-and-play
- Simplified packet header
- Security
- Mobility
- Enhanced QoS features

This chapter describes how to set up an IPv6 network to help you understand the basic principles and address configuration of IPv6.

7.1.2 Objectives

Upon completion of this task, you will be able to:

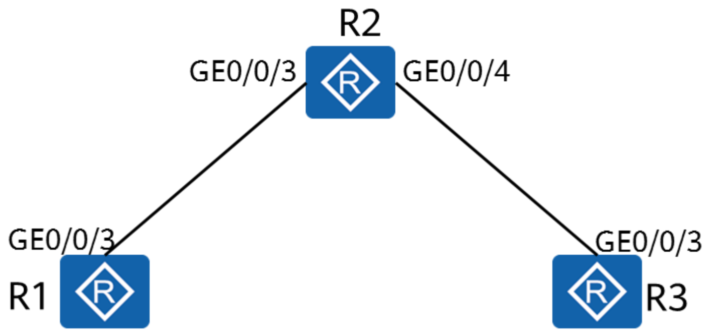
- Learn how to configure static IPv6 addresses
- Learn how to configure a DHCPv6 server
- Learn how to configure stateless addresses
- Learn how to configure static IPv6 routes
- Learn how to view IPv6 information

7.1.3 Networking Topology

An enterprise needs to deploy IPv6 on its network.

1. Configure static IPv6 addresses for the two interfaces of R2.
2. Configure stateless address autoconfiguration on GigabitEthernet0/0/3 of R1.
3. Configure an IPv6 address for GigabitEthernet0/0/3 of R3 using DHCPv6.

Figure 7-1 Lab topology for creating an IPv6 network



7.2 Lab Configuration

7.2.1 Configuration Roadmap

1. Configure static IPv6 addresses.
2. Configure DHCPv6.
3. Configure IPv6 stateless address allocation.
4. Display IPv6 addresses.

7.2.2 Configuration Procedure

Step 1 Complete basic device configuration.

Name the devices.

The details are not provided here.

Step 2 Configure IPv6 functions on the devices and interfaces.

Enable IPv6 globally.

```
[R1]ipv6
```

The **ipv6** command enables the device to forward IPv6 unicast packets, including sending and receiving local IPv6 packets.

```
[R2]ipv6
```

```
[R3]ipv6
```

Enable IPv6 on the interface.

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

The **ipv6 enable** command enables the IPv6 function on an interface.

```
[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
```

Step 3 Configure a link-local address for the interface and test the configuration.

Configure an interface to automatically generate a link-local address.

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

The **ipv6 address auto link-local** command enables the generation of a link-local address for an interface.

Only one link-local address can be configured for each interface. To prevent link-local address conflict, automatically generated link-local addresses are recommended. After an IPv6 global unicast address is configured for an interface, a link-local address will be automatically generated.

```
[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
```

Display the IPv6 status of the interface and test the connectivity.

```
<R1>display ipv6 interface GigabitEthernet 0/0/3
```

```
GigabitEthernet0/0/3 current state : UP
IPv6 protocol current state : UP                        //The physical and protocol status is Up.
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE4D:355      //The link-local address for the interface has been generated.
  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
```

Test network connectivity between R1 and R2.

```
<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
```

When you ping a link-local address, you must specify the source interface or source IPv6 address.

Step 4 Configure static IPv6 addresses on R2.

```
[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
```

Step 5 Configure the DHCPv6 server function on R2 and configure R3 to obtain IPv6 addresses through DHCPv6.

Configure the DHCPv6 server function.

```
[R2]dhcp enable
[R2]dhcpv6 pool pool1
An IPv6 address pool named pool1 is created.
[R2-dhcpv6-pool-pool1]address prefix 2000:0023::/64
The IPv6 address prefix is configured.
[R2-dhcpv6-pool-pool1]dns-server 2000:0023::2
The IP address of the DNS server is specified.
[R2-dhcpv6-pool-pool1]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]dhcpv6 server pool1
[R2-GigabitEthernet0/0/4]quit
```

Configure the DHCPv6 client function.

```
[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
```

Display the client address and DNS server information.

```
[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                                -
```

GigabitEthernet0/0/3 on R3 has obtained an IPv6 global unicast address.
How is the DHCPv6 server configured to allocate gateway information to clients?

The DHCPv6 server does not allocate an IPv6 gateway address to a client.

When the DHCPv6 stateful mode is configured, DHCPv6 clients learn the default route of the IPv6 gateway using the **ipv6 address auto global default** command. When the DHCPv6 stateless mode is configured, DHCPv6 clients learn the global unicast IPv6 address and the default route to the IPv6 gateway through this command. Ensure that the interface of the peer device connected to the local device has been enabled to send RA packets using the **undo ipv6 nd ra halt** command.

Configure DHCPv6 server to allocate the gateway address to clients.

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

The **undo ipv6 nd ra halt** command enables a system to send RA packets. By default, router interfaces do not send RA packets.

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

The **ipv6 nd autoconfig managed-address-flag** command sets the "managed address configuration" flag (M flag) in RA messages, indicating whether hosts should use stateful autoconfiguration to obtain addresses. By default, the flag is not set.

- If the M flag is set, a host obtains an IPv6 address through stateful autoconfiguration.

- If the M flag is not set, a host uses stateless autoconfiguration to obtain an IPv6 address, that is, the host generates an IPv6 address based on the prefix information in the RA packet.

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

The **ipv6 nd autoconfig other-flag** command sets the "Other Configuration" flag (O flag) in RA messages. By default, the flag is not set.

- If the O flag is set, a host uses stateful autoconfiguration to obtain other configuration parameters (excluding IPv6 address), including the router lifetime, neighbor reachable time, retransmission interval, and PMTU.
- If this flag is cleared, a host can obtain configurations (excluding IPv6 address), such as the router lifetime, neighbor reachable time, retransmission interval, and PMTU in stateless autoconfiguration. This means that a routing device advertises these configurations using RA messages to the attached hosts.

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

Configure the client to learn the default route through RA messages.

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

Display the routes of R3.

```
[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
```

Step 6 Configure R1 to obtain an IPv6 address in stateless mode.

Enable RA on GigabitEthernet0/0/3 of R2.

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

```
# Enable stateless address autoconfiguration on GigabitEthernet0/0/3 of R1.
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3] ipv6 address auto global
```

Display the IP address configuration of R1.

```
[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
```

GigabitEthernet0/0/3 of R1 generates an IPv6 global unicast address based on the IPv6 address prefix obtained from the RA message sent by R2 and the locally generated interface ID.

Step 7 Configure an IPv6 static route.

Configure a static route on R1 to enable connectivity between GigabitEthernet0/0/3 on R1 and GigabitEthernet0/0/3 on R3.

```
[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.
```

Test connectivity.

```
[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
```

R1 has a static route to the network 2000:23::/64. R3 obtains the default route through DHCPv6. Therefore, GigabitEthernet0/0/3 on R1 and GigabitEthernet0/0/3 on R3 can communicate with each other.

Display the IPv6 neighbor information.

```
[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
```

----End

7.3 Verification

The details are not provided here.

7.4 Configuration Reference

Configuration on R1

```
#
 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
```

Configuration on R2

```
#
 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
```

Configuration on R3

```
#
 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 Quiz

1. Why the source interface must be specified in Step 3 (testing the connectivity between link-local addresses) but not in Step 7 (testing the connectivity between GUA addresses)?
2. Describe the difference between stateful address configuration and stateless address configuration and explain why.

8 Network Programming and Automation Basics

8.1 Introduction

8.1.1 About This Lab

After completing this lab activity, you will be able to learn how to use the Python telnetlib.

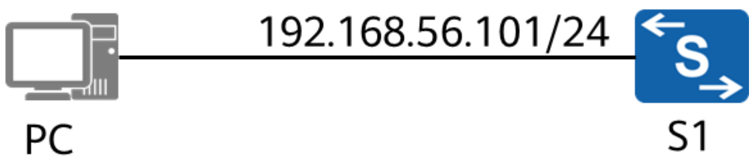
8.1.2 Objectives

- Learn the basic Python syntax
- Learn how to use telnetlib

8.1.3 Networking Topology

A company has a switch whose management IP address is 192.168.56.101/24. You need to write an automation script to view the current configuration file of the device.

Figure 8-1 Lab topology for network programming and automation



8.2 Lab Configuration

8.2.1 Configuration Roadmap

1. Configure Telnet: Configure the Telnet password, enable Telnet, and allow Telnet access.
2. Compile a Python script: Invoke telnetlib to log in to the device and check the configuration.

8.2.2 Configuration Procedure

Step 1 Configure Telnet on the switch.

Create a Telnet login password.

```
[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
```

Before using a Python script to log in to a device through Telnet, you need to create a Telnet password and enable the Telnet function on the device. Set the Telnet login password to **Huawei@123**.

Enable the Telnet service to allow Telnet access.

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

Telnet to the switch from the PC using the command interface.

```
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>
```

The Telnet configuration is successful.

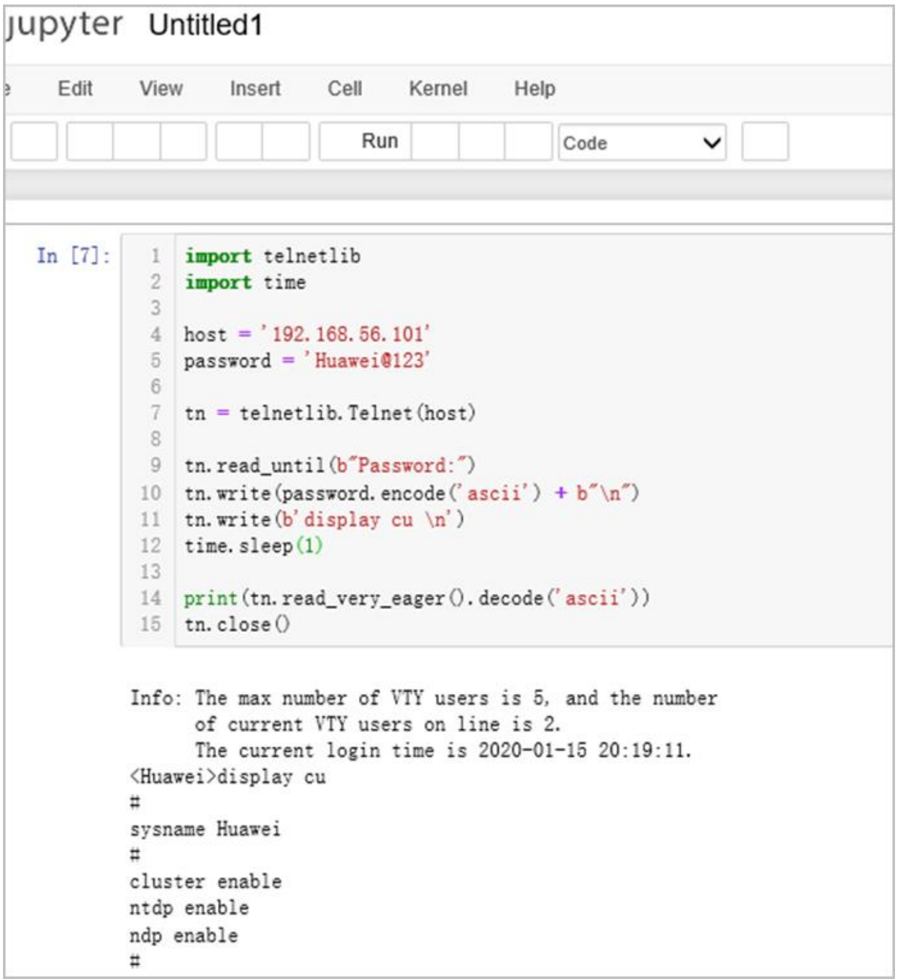
Step 2 Write the Python code.

```
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()
```

The Python script invokes the telnetlib module to log in to S1, runs the **display current-configuration** command, and displays the command output.

Step 3 Execute the compiler:



The compiler used in this lab environment is Jupyter Notebook. You can also use other compilers.

Step 4 The output is as follows:

```
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 ----
```

----End

8.2.3 Code Interpretation

Step 1 Import the module.

```
import telnetlib
import time
```

Import the telnetlib and time modules. The two modules are provided by Python and do not need to be installed.

This section describes the common classes and methods of the Telnetlib as the client, for example, the read_until, read_very_eager(), and write() methods in the Telnet class. For more Telnet methods, see the official telnetlib document at https://docs.python.org/3/library/telnetlib.html#telnet-example.

By default, Python executes all code in sequence without intervals. When you use Telnet to send configuration commands to a switch, the switch may not respond in time or the command output may be incomplete. In this case, you can use the sleep method in the time module to manually pause the program.

Step 2 Log in to the device.

Invoke multiple methods of the Telnet class in telnetlib to log in to S1.

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

Create two variables. host and password are the login address and password of the device respectively, which are the same as those configured on the device. In this example, only the Telnet password is configured for login. Therefore, no user name is required.

telnetlib.Telnet() indicates that the Telnet() method in the telnetlib class is invoked. This method contains login parameters, including the IP address and port number. If no port information is entered, port 23 is used by default.

In this example, tn = telnetlib.Telnet(host) indicates that you log in to the device whose host is 192.168.56.101 and assign the value of telnetlib.Telnet(host) to tn.

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

When you log in to the device at 192.168.56.101 through Telnet, the following information is displayed:

```
<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:
```

Note that the program does not know what information needs to be read. Therefore, read_until() is used to indicate that the information in the brackets needs to be read.

In this example, tn.read_until(b"Password:") indicates that data is read until "Password: "is displayed. The letter "b" before "Password:" indicates that the default Unicode code in Python3 is changed to bytes. This is the requirement of the function on the input data. For details, see the official document of telnetlib. If this parameter is not carried, the program reports an error.

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

After Password: is displayed in the code, the program enters the password. This parameter has been defined and is used as the Telnet login password. Use write() to write the password.

In this example, tn.write (password.encode('ascii') + b"\n") consists of two parts: password.encode('ascii') and b"\n". password.encode('ascii') indicates that the encoding type of the character string Huawei@123 represented by password is ASCII. "+" indicates that the character strings before and after the symbol will be concatenated. \n is a newline character, which is equivalent to pressing Enter. Therefore, the code in this line is equivalent to entering the password Huawei@123 and pressing Enter.

Step 3 Issue configuration commands.

After logging in to the device through Telnet, use the Python script to issue commands on the device.

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

write() is used to enter commands to the device. The **display cu** command is the abbreviated form of the **display current-configuration** command, which displays the current configuration of the device.

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

time.sleep(1) is used to pause the program for one second to wait for the output of the switch before executing subsequent code. If the waiting time is not specified, the program directly executes the next line of code. As a result, no data can be read.

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

print() indicates that the contents in the brackets are displayed on the console.

tn.read_very_eager() indicates reading as much data as possible.

. decode('ascii')) indicates that the read data is decoded to ASCII.

In this example, the code is used to display the output by S1 within one second on the console after the **display cu** command is executed.

Step 4 Close the session.

```
tn.close()
```

The session is closed by invoking close(). The number of VTY connections on the device is limited. Therefore, you need to close the Telnet session after running the script.

----End

8.3 Verification

The details are not provided here.

8.4 Configuration Reference

The details are not provided here.

8.5 Quiz

1. How do you use telnetlib to configure a device, for example, configuring the IP address of the device management interface?
2. How do you save the configuration file to a local directory?

9 Configuring a Campus Network

9.1 Reference Information

The commands and references listed in this document are for reference only. The correct commands and references are subject to your product model and version.

References:

1. AR600 and AR6000 Product Documentation
2. S2720, S5700, and S6700 Series Ethernet Switches Product Documentation
3. Wireless Access Controller (AC and Fit AP) Product Documentation
4. Typical Campus Network Architectures and Practices

Reference links:

1. http://support.huawei.com/
2. http://e.huawei.com/

9.2 Introduction

9.2.1 About This Lab

Communication networks are ubiquitous in the information society, and campus networks are always a core part. Campuses are everywhere, including factories, government buildings and facilities, shopping malls, office buildings, school campuses, and parks. According to statistics, 90% of urban residents work and live in campuses, 80% of gross domestic product (GDP) is created in campuses, and each person stays in campuses for 18 hours every day. Campus networks, as the infrastructure for campuses to connect to the digital world, are an indispensable part of campus construction and play an increasingly important role in daily working, R&D, production, and operation management.

In this lab activity, you will create a campus network to understand common technologies and their applications on campus networks.

9.2.2 Objectives

Upon completion of this task, you will be able to:

- Understand common campus network concepts and architecture

- Understand common network technologies
- Understand the lifecycle of campus networks
- Be familiar with campus network planning and design, deployment and implementation, network O&M, and network optimization
- Be familiar with the process for implementing a campus network project

9.2.3 Networking Topology

A network needs to be constructed in an office building. The office building has six floors. Currently, three floors have been put in use: the reception hall on the first floor, administrative department and general manager's office on the second floor, R&D department and marketing department on the third floor. The core equipment room is deployed on the first floor, and a small room is deployed on each of the other floors to house network devices.

Set up a project team to complete the network construction.

9.3 Lab Tasks

9.3.1 Requirement Collection and Analysis

What information should be obtained from the company? Please list at least five items.

Example: The number of terminals to be connected to the enterprise network.

1.____

2.____

3.____

4.____

5.____

Analyze the collected requirements.

1. Project Budget

   The budget is tight. The requirements need to be implemented at minimum costs.

2. Types of Terminals to Be Connected

   Both wired and wireless terminals will be deployed.

3. Number of Terminals

   First floor: 10 wired terminals and 100 wireless terminals Second and third floors: 200 wired terminals and 50 wireless terminals

4. Network Management Mode

   SNMP is used for unified network management.

5. Volume and Trend of Network Traffic

   Most of the traffic is internal traffic. 100 Mbit/s wired access is required. There are no other special requirements.

6. Availability Requirements

   The Layer 3 network needs some redundancy and failover capabilities.

7. Security Requirements

   Network traffic needs to be controlled.

8. Internet Access Mode

   Egress devices on the campus network use static IP addresses to connect to the Internet.

9. Network Expansion Requirements

   When other floors are put into use, there should be no need to replace existing devices.

9.3.2 Planning and Design

Task 1. Device Selection and Physical Topology Design (Optional)

Background:

The following table lists the total number of terminals on the network.

Floor	First Floor	Second Floor	Third Floor	Other Floors (Reserved)
Wired terminals	10	200	200	500
Wireless terminals	100	50	50	200
Remarks	Guest wireless terminals + servers	Computers + mobile phones		

The traffic from wireless terminals is the Internet access traffic. Each client has a rate of 2 Mbit/s.

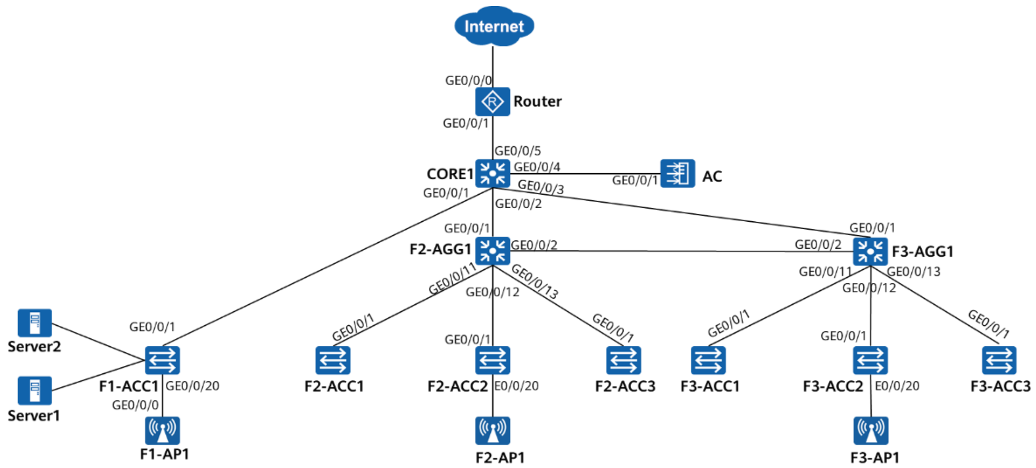
Ensure that computers have a rate of 100 Mbit/s and servers have a rate of 1000 Mbit/s.

To improve wireless access quality, at least three dual-band APs are required on each floor.

Task:

Design the physical topology of the network in the sequence of access layer, aggregation layer, core layer, and egress area and select devices accordingly.

Reference answer:



The device interface numbers are as follows:

Device	Interfaces
F2-ACC1, F2-ACC2, F2-ACC3, F3-ACC1, F3-ACC2, and F3-ACC	E0/0/1~E0/0/222 GE0/0/1~GE0/0/2

F1-ACC1, F2-AGG1, F3-AGG1, and CORE1	GE0/0/1~GE0/0/24
AC	GE0/0/1~GE0/0/8
F1-AP1, F2-AP1, and F3-AP1	GE0/0/0~GE0/0/1
Router	GE0/0/0~GE0/0/2

NOTE

The *Practices in Campus Network Projects* in the HCIA-Datacom certification textbook details the network design and topology design process based on the preceding requirements. This part is omitted in this document. In actual networking, there are a large number of access switches and APs. To simplify the networking and facilitate subsequent tests, a simplified network topology is used in this document.

Task 2. Layer 2 Network Design

Background:

- VLAN creation on the wired network:
  - Access switch ports GE0/0/1 to GE0/0/10 in the core equipment room connect to servers and are assigned to the same VLAN.
  - On the second floor, F2-ACC2 is connected to the general manager's office, and other switches are connected to the administrative department. The two departments belong to different VLANs.
  - On the third floor, E0/0/1 to E0/0/10 of F3-ACC1 and F3-ACC3 belong to the marketing department, and E0/0/11 to E0/0/20 belong to the R&D department.
  - E0/0/1 to E0/0/19 of F3-ACC2 belong to the marketing department.
- VLAN creation on the wireless network:
  - Wireless terminals on different floors must be assigned to different VLANs.
  - The wireless network management VLAN of each floor is different.

NOTE

Device interconnection VLANs and device management VLANs need to be reserved.

Task:

Fill in the Layer 2 network planning table based on the existing information and requirements.

VLAN ID	Description
Example: 1	Layer 2 device management VLAN

VLAN ID	Description

Reference answer:

VLAN ID	Description
1	Layer 2 device management VLAN on the first floor
2	Layer 2 device management VLAN on the second floor
3	Layer 2 device management VLAN on the third floor
100	VLAN for servers
101	VLAN for the General Manager's Office
102	VLAN for the Administrative Department
103	VLAN for the Marketing Department
104	VLAN for the R&D Department

VLAN ID	Description
105	VLAN for the wireless terminals on the first floor
106	VLAN for the wireless terminals on the second floor
107	VLAN for the wireless terminals on the third floor
201	VLAN for the interconnection between F2-AGG1 and CORE1
202	VLAN for the interconnection between F3-AGG1 and CORE1
203	VLAN for the interconnection between F2-AGG1 and F3-AGG1
204	VLAN for the interconnection between CORE1 and the router
205	Wireless network management VLAN on the first floor
206	Wireless network management VLAN on the second floor
207	Wireless network management VLAN on the third floor

Task 3. Layer 3 Network Design

Background:

- The address range is network 192.168.0.0/16. The requirements are as follows:
  - First floor:
    - The servers use static IP addresses. IP addresses of wireless stations and APs are allocated by CORE1 through DHCP. The gateway is on CORE1.
    - The management IP addresses of the access switches are static IP addresses, and the gateway is on CORE1.
  - Second and third floors:
    - The IP addresses of all wired terminals, wireless terminals, and wireless APs are allocated by the aggregation switch of the corresponding floor(s) through DHCP. The gateway is deployed on the aggregation switches.
    - The management IP addresses of the access switches are static IP addresses, and the gateway is on the aggregation switch of the corresponding floor(s).
- OSPF is used on the entire network to enable connectivity between service networks. All terminals access the Internet through the router.

Task:

Fill in the Layer 3 network planning table based on the existing information and requirements.

IP Network	Address Assignment Method and Gateway	Routing Mode	Network Description
192.168.1.0/24	DHCP; 192.168.1.254	OSPF	Layer 2 device management network

Reference answer:

IP Network	Address Assignment Method and Gateway	Routing Configuration	Network Description
192.168.1.0/24	Static addresses; CORE1	Default route pointing to CORE1	Layer 2 device management network on the first floor
192.168.2.0/24	Static addresses; F2-AGG1	Default route pointing to F2-AGG1	Layer 2 device management network on the second floor

IP Network	Address Assignment Method and Gateway	Routing Configuration	Network Description
192.168.3.0/24	Static addresses; F3-AGG	Default route pointing to F3-AGG	Layer 2 device management network on the third floor
192.168.100.0/24	Static addresses; CORE1	Advertised in OSPF through gateway devices	Network of servers
192.168.101.0/24	Assigned by F2-AGG1 through DHCP; F2-AGG1		Network of the General Manager's Office
192.168.102.0/24			Network of the Administrative Department
192.168.103.0/24	Assigned by F3-AGG1 through DHCP; F3-AGG1		Network of the Marketing Department
192.168.104.0/24			Network of the R&D Department
192.168.105.0/24	Assigned by CORE1 through DHCP; CORE1		Network of the wireless terminals on the first floor
192.168.106.0/24	Assigned by F2-AGG1 through DHCP; F2-AGG1		Network of the wireless terminals on the second floor
192.168.107.0/24	Assigned by F3-AGG1 through DHCP; F3-AGG1		Network of the wireless terminals on the third floor
192.168.201.0/30	Static addresses; no gateway needed	OSPF is enabled, neighbor relationship is established, and the default route is advertised by the router	Network for the interconnection between F2-AGG1 and CORE1
192.168.202.0/30			Network for the interconnection between F3-AGG1 and CORE1

IP Network	Address Assignment Method and Gateway	Routing Configuration	Network Description
192.168.203.0/30			Network for the interconnection between F2-AGG1 and F3-AGG1
192.168.204.0/30			Network for the interconnection between CORE1 and the router
192.168.205.0/24	Assigned by CORE1 through DHCP; CORE1	Advertised in OSPF through gateway devices	Wireless network management network on the first floor
192.168.206.0/24	Assigned by F2-AGG1 through DHCP; F2-AGG1		Wireless network management network on the second floor
192.168.207.0/24	Assigned by F3-AGG1 through DHCP; F3-AGG1		Wireless network management network on the third floor

Task 4. WLAN Design

Background:

- All APs are managed by the AC in a unified manner, and the AC has limited forwarding performance.
  - APs on the first floor are registered at Layer 2.
  - All APs on the second and third floors register with the AC at Layer 3. The AC's gateway is CORE1.
- Create an SSID for each floor.
  - The WPA-WPA2+PSK+AES security policy is used.
  - Each floor has a different SSID and password.

Task:

Fill in the WLAN network planning table based on the existing information and requirements.

Item	WLAN on the First Floor	WLAN on the Second Floor	WLAN on the Third Floor
AP management VLAN			
Service VLAN			
DHCP server			
IP address of the AC's source interface			
AP group			
Regulatory domain profile			
SSID profile			
Security profile			
VAP profile			
Other configurations			

Reference answer:

Item	WLAN on the First Floor	WLAN on the Second Floor	WLAN on the Third Floor
AP management VLAN	VLAN205	VLAN206	VLAN207
Service VLAN	VLAN105	VLAN106	VLAN107
DHCP server	CORE1 assigns IP addresses to APs and STAs.	F2-AGG1 assigns IP addresses to APs and STAs.	F3-AGG1 assigns IP addresses to APs and STAs.
IP address of the AC's source interface	VLANIF205: 192.168.205.253/24		
AP group	Name: WLAN-F1 VAP profile: WLAN-F1 Regulatory domain profile: default	Name: WLAN-F2 VAP profile: WLAN-F2 Regulatory domain profile: default	Name: WLAN-F3 VAP profile: WLAN-F3 Regulatory domain profile: default
Regulatory	Name: default		

domain profile	Country code: CN		
SSID profile	Name: WLAN-F1 SSID name: WLAN-F1	Profile name: WLAN-F2 SSID name: WLAN-F2	Profile name: WLAN-F3 SSID name: WLAN-F3
Security profile	Name: WLAN-F1 Security policy: WPA-WPA2+PSK+AES Password: WLAN@Guest123	Name: WLAN-F2 Security policy: WPA-WPA2+PSK+AES Password: WLAN@Employee2	Name: WLAN-F3 Security policy: WPA-WPA2+PSK+AES Password: WLAN@Employee3
VAP profile	Name: WLAN-F1 Forwarding mode: direct forwarding Service VLAN: VLAN: 105 Profiles: SSID profile: WLAN-F1; Security profile: WLAN-F1	Name: WLAN-F2 Forwarding mode: direct forwarding Service VLAN: 106 Profiles: SSID profile: WLAN-F2 Security profile: WLAN-F2	Name: WLAN-F3 Forwarding mode: direct forwarding Service VLAN: VLAN: 107 Profiles: SSID profile: WLAN-F3 Security profile: WLAN-F3

Task 5. Security and Egress Design

Background:

- The guest SSID is not allowed to access the intranet of the company.
- Only wireless terminals can access the Internet.
- The router uses a static IP address to access the Internet. The carrier assigns IP addresses 1.1.1.1 to 1.1.1.10 (with a 24-bit mask) to the router. The next-hop IP address for the router to access the Internet is 1.1.1.254.
- A web server in the enterprise needs to provide services for external users. The private IP address of the web server is 192.168.100.1 and the port number is 80. To ensure server security, NAT mapping is provided only for web services.

Task:

Fill in the security and egress planning table based on the existing information and requirements.

Requirement	Implementation

Reference answer:

Requirement	Implementation
Intranet access control applicable to guests	Configure a traffic filter or a traffic policy on CORE1.
Internet access control	Configure NAT on the router and disable address translation for the specified networks.
Web server mapping	Configure NAT server on the router interface.

Task 6. Network Management Design

Background:

- SNMPv3 is used to communicate with the NMS, and authentication and encryption are configured to enhance security.
- All devices except the router and AC communicate with the NMS at 192.168.100.2/24 through the management VLAN.
- Routers communicate with the NMS through GE0/0/1.
- The AC communicates with the NMS through VLANIF 205.
- All devices must be able to report SNMP alarms to the NMS.

Task:

Based on the preceding requirements, optimize the device configurations in the deployment and implementation phase.

9.3.3 Implementation

Task 1. Configuration Scheme

Fill in the configuration scheme for each device according to the planning and design scheme.

Router:

Item	Configuration
Basic configuration	
IP address configuration	
OSPF	
Egress configuration	
SNMP configuration	
Other configurations	

CORE1:

Item	Configuration
Basic configuration	
VLAN configuration	
VLANIF interface configuration	
OSPF configuration	
DHCP configuration	
Access control	
SNMP configuration	
Other configurations	

F2-AGG1:

Item	Configuration
Basic configuration	
VLAN configuration	
VLAN configuration on interfaces	
VLANIF interface configuration	
OSPF configuration	
DHCP configuration	
SNMP configuration	

Other configurations	

F3-AGG1:

Item	Configuration
Basic configuration	
VLAN configuration	
VLAN configuration on interfaces	
VLANIF interface configuration	
OSPF configuration	
DHCP configuration	
SNMP configuration	
Other configurations	

AC:

Item	Configuration
Basic configuration	
Wired network configuration	
Wireless network configuration	
SNMP configuration	
Other configurations	

F1-ACC1:

Item	Configuration
Basic configuration	
VLAN configuration	
VLANIF interface configuration	
Routing configuration	
SNMP configuration	

Other configurations	

F2-ACC1:

Item	Configuration
Basic configuration	
VLAN configuration	
VLANIF interface configuration	
Routing configuration	
SNMP configuration	
Other configurations	

F2-ACC2:

Item	Configuration
Basic configuration	
VLAN configuration	
VLANIF interface configuration	
Routing configuration	
SNMP configuration	
Other configurations	

F2-ACC3:

Item	Configuration
Basic configuration	
VLAN configuration	
VLANIF interface configuration	
Routing configuration	
SNMP configuration	
Other configurations	

F3-ACC1:

Item	Configuration
Basic configuration	
VLAN configuration	
VLANIF interface configuration	
Routing configuration	
SNMP configuration	
Other configurations	

F3-ACC2:

Item	Configuration
Basic configuration	
VLAN configuration	
VLANIF interface configuration	
Routing configuration	
SNMP configuration	
Other configurations	

F3-ACC3:

Item	Configuration
Basic configuration	
VLAN configuration	
VLANIF interface configuration	
Routing configuration	
SNMP configuration	
Other configurations	

Configuration

Set up the lab environment and complete related configurations according to the preceding configuration schemes within 40 minutes.

Task 2. Project Acceptance

After the device configuration is complete, what items need to be verified for acceptance? How are they verified? Please list at least five items.

1.____

2.____

3.____

4.____

5.____

Reference answer:

1. Verify whether the wireless clients can detect wireless signals and access the network successfully.
2. Verify whether the OSPF neighbor relationship is normal.
3. Verify the connectivity within networks.
4. Verify the connectivity between networks.
5. Verify the access control for wireless guests.
6. Verify the Internet access control.
7. Verify whether the NMS can manage network devices.

9.3.4 Network O&M

Task 1. O&M Handover

After the project is delivered, how do you arrange the maintenance work in the future? Discuss with your team and list at least five maintenance items.

1. ____
2. ____
3. ____
4. ____
5. ____

Reference answer:

Recommended Maintenance Interval	Check Item	Check Method	Evaluation Criteria
Daily	Power connections	Observation	The power cable is correctly and securely connected to the specified position of the device. The power supply indicator on the device should be steady on (green).
	Device temperature	<HUAWEI> display temperature	The temperature of each module falls between the upper limit and lower limit.
	Alarm information	<HUAWEI> display alarm urgent	Alarms are recorded, and major or more severe alarms are immediately analyzed and processed.
	CPU usage	<HUAWEI> display cpu-usage	The CPU usage of each module is normal. If the CPU usage exceeds 80% frequently or persistently, adequate attention is required.
	Memory usage	<HUAWEI> display memory-usage	Memory usage is normal. If the value of **Memory Using Percentage** exceeds 60%, adequate attention is required.
Weekly	Ambient temperature in the equipment room	Instrument measurement	The long-term operating temperature of the equipment room ranges from 0°C to 50°C, and the short-term operating temperature ranges from –5°C to 55°C.
	Ambient humidity in the equipment room	Instrument measurement	The ambient humidity in the equipment room should range from 10% RH to 90% RH.

Recommended Maintenance Interval	Check Item	Check Method	Evaluation Criteria
Monthly	Device position	Observation and instrument measurement	The device is placed stably in a flat position in a well ventilated, dry, and clean environment.
	Routing table	<HUAWEI> display ip routing-table	On all devices running the same routing protocol at the same layer of a network, the number of routes should not vary widely.
	Configuration backup	NA	The configuration information of the devices must be backed up every month.
	Password change	NA	The device login passwords must be changed every month.

9.3.5 Network Optimization

Task 1. Performance Optimization

With the development of the enterprise, the internal traffic, especially the traffic between the second and third floors, increases sharply. The capacity of the link between aggregation switches is insufficient for such a large amount of traffic. How can the link be optimized?

Reference answer:

1. You can add physical links between F2-AGG1 and F3-AGG1 and configure Ethernet link aggregation.
2. Change the OSPF costs to implement load balancing so that some traffic can be forwarded through CORE1.

9.4 Verification

The details are not provided here.

9.5 Configuration Reference

Configuration on the Router

```
#
 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 tra
p-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
```

Configuration on CORE1

```
#
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
```

Configuration on F2-AGG1

```
#
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
```

Configuration on F3-AGG1

```
#
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
```

Configuration on the AC

```
#
 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
```

Configuration on F1-ACC1

```
#
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
```

Configuration on F2-ACC1

```
#
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
```

Configuration on F2-ACC2

```
#
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
```

Configuration on F2-ACC3

```
#
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
```

Configuration on F3-ACC1

```
#
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
 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 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
```

Configuration on F3-ACC2

```
#
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
```

Configuration on F3-ACC3

```
#
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
#
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 Quiz

1. In this project, CORE1, F2-AGG1, and F3-AGG1 form a physical ring. However, in the network planning and design phase, the interconnection links between the three devices are assigned to different VLANs. Therefore, there is no loop. However, during the lab, you may find that the neighbor relationship between

two devices cannot be correctly established. Please find out the root cause and solution.

2. What have you learned in this lab? How can the knowledge help you in your future study or work?

Reference Answers

Huawei VRP and Configuration Basics

1. Omitted.
2. The **reset saved-configuration** command clears the startup configuration file and cancels the previous startup configuration file configuration. The current startup configuration file is test.cfg. Therefore, after this command is executed, the content in test.cfg is cleared and the default configuration file vrpcfg.zip is used as the startup configuration file. In step 4, the running configuration is saved. Therefore, the configuration remains unchanged after the device is restarted.

IPv4 Addressing and Routing

1. A static route is added to the routing table when the following conditions are met:
   a The next hop of the route is reachable.
   b This route is the optimal route to the destination network or host.

   Therefore, when the next hop is unreachable, the route is not added to the IP routing table.
2. When a ping operation is performed on a Huawei device, the device searches the routing table to determine the outgoing interface. The IP address of the outgoing interface is used as the source IP address of ICMP packets.

OSPF Routing

1. R2 replies to R1 along the path of R2->R1. After the cost of GigabitEthernet0/0/3 on R1 is changed to 10, the path cost of R1->R2 is 10. Therefore, the path from LoopBack0 on R1 to LoopBack0 on R2 is R1->R3->R2. In this case, R2 does not know that the cost of GigabitEthernet0/0/3 on R1 has been changed to 10 and still uses the cost of GigabitEthernet0/0/3 on R1 to calculate the route cost. Therefore, the path R2->R1 is used as the reply path.

Ethernet Basics and VLAN Configuration

Configuration Roadmap:

- Create a VLAN for PCs with special needs.
- Associate the MAC addresses of the PCs with VLANs.
- Assign interfaces to VLANs to implement Layer 2 forwarding.

Configuration Procedure:

Create VLANs.

```
[S1]vlan 10
```

Associate the MAC address of the PC with VLAN 10.

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

In this example, the MAC address of the PC is 00e0-fc1c-47a7.

Enable MAC address-based VLAN assignment.

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

Configure GE0/0/1 connected to S2 as a hybrid port to allow data frames of the corresponding VLAN to pass through in untagged mode.

```
[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
```

Configure GE0/0/2 connected to the enterprise network to transparently transmit packets from the VLANs associated with MAC addresses.

```
[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
```

Spanning Tree

1. No. After receiving STP BPDUs, all bridges add the local port cost to the RPC in the BPDUs to calculate the root path cost of the port. Therefore, when the cost of GigabitEthernet 0/0/14 on S1 changes, the root path cost of S4 is not affected.
2. Change the priority of GigabitEthernet0/0/11 on S1.
3. No. The link between S1 and S2 will form a loop. Therefore, one link must be blocked.

Ethernet Link Aggregation

1. Least active-linknumber must be less than or equal to max active-linknumber.

Inter-VLAN Communication

1. Create a Layer 3 interface on S1 to connect to GigabitEthernet0/0/1 of R1, and configure a route to the corresponding network.
2. If any physical interface that allows the VLAN to pass through goes Up, the corresponding VLANIF interface goes Up.

ACL Configuration

Configuration Roadmap:

- Configure OSPF to enable connectivity.
- Enable Telnet and FTP on R3.
- Configure an advanced ACL to match desired traffic.

Configuration Procedure:

Configure network connectivity, Telnet, and FTP.

Configure an ACL on R2.

```
[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
```

Apply the ACL on GE0/0/3 of R2.

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

Local AAA Configuration

The details are not provided here.

NAT Configuration

1. Not required.

FTP Configuration

1. Active mode

DHCP Configuration

1. An interface address pool contains only IP addresses on the same subnet as the interface.

   A global address pool can contain IP addresses on the same subnet as the interface or IP addresses of different subnets (as in the DHCP relay networking).
2. In the scenario without a relay agent, an IP address pool on the same subnet as the interface is selected from the global address pools, and IP addresses are assigned to clients according to the parameters of the address pool. In the scenario with a relay agent: Based on the subnet requested by the relay agent, an IP address pool on the requested subnet is selected from the global address pools, and IP addresses are assigned to clients according to the parameters of the address pool.

Creating a WLAN

1. There is no impact. Direct forwarding is performed, and the data does not pass through GigabitEthernet0/0/10 of the AC. If tunnel forwarding is used,

configure GigabitEthernet0/0/10 to allow packets from VLAN 101 to pass through. Otherwise, STAs cannot access S1.

2. AP1 and AP2 use different VAP profiles, and different service-VLAN parameters are configured in the VAP profiles.

Creating an IPv6 Network

1. The router has multiple interfaces on the FE80::/10 network. When the destination IPv6 address is a link-local address, the outgoing interface cannot be determined by querying the routing table. Therefore, the source interface must be specified.
2. In stateful mode, all the 128 bits in an IPv6 interface address are specified by the DHCPv6 server. In stateless mode, a 64-bit interface ID is generated based on the EUI-64 specification.

Configuring a Campus Network

1. Although loop prevention has been implemented at the VLAN layer, physical loops still exist. STP BPDUs do not carry VLAN tags. Therefore, one of the links between the three switches must be blocked. As a result, the neighbor relationship cannot be established between two of the switches. In actual deployment, loop prevention has been implemented at VLAN level. Therefore, you can disable STP on interfaces between the devices.
2. Omitted.

Network Programming and Automation Basics

1. Use the write() function of telnetlib to write the script for configuring device interfaces line by line.
2. For details, see the Python I/O standard library.