Huawei Datacom Certification Training

HCIA-Datacom

Lab Guide

ISSUE: 1.0

HUAWEI TECHNOLOGIES CO., LTD

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

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 is an integral part of the company's Platform + Ecosystem strategy. It supports the development of ICT infrastructure that features Cloud-Pipe-Device synergy. Our certification is always evolving to reflect the latest trends in ICT development.

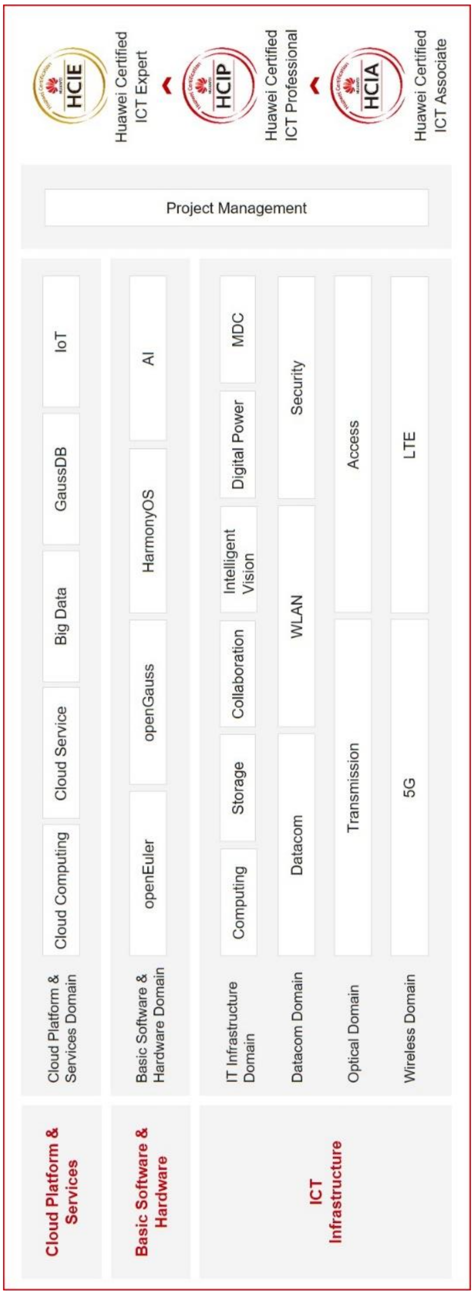
Huawei Certification consists of three categories: ICT Infrastructure Certification, Basic Software & Hardware Certification, and Cloud Platform & Services Certification, making it the most extensive technical certification program in the industry.

Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

Our programs cover all ICT fields and follow the industry's trend of ICT convergence. With our leading talent development system and certification standards, we are committed to fostering new digital ICT talent 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.


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

Overview

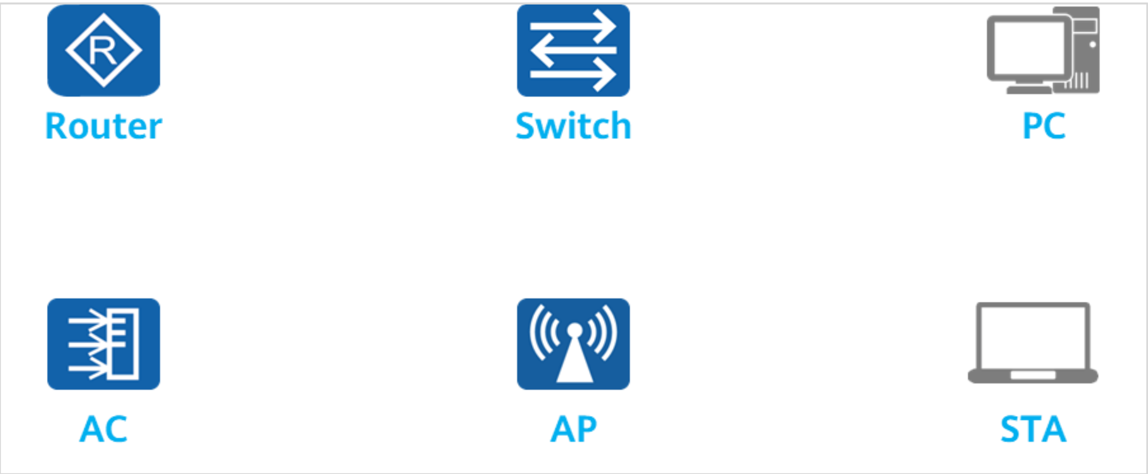
This document is an HCIA-Datacom certification training course and is intended for trainees who are going to take the HCIA-Datacom exam or readers who want to understand routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability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

Common Icons



Experiment Environment Overview

This document is written based on the Huawei datacom simulator eNSP Pro. Datacom Simulator is a training, certification, and learning solution of Huawei datacom product line. It provides a one-stop datacom product simulator environment for users.

Simulator Name	Version

eNSP Pro	eNSP Pro V100R001C10

Click eNSP Pro to obtain the latest version and product manual.

You can also use eNSP Pro through the o3 community.

Note: The eNSP Pro is only released to the Enterprise Techinal Support Website for partner(ASP、Service Partner/Business Operation Partner、Sales Partner) and is not open to Registered Sales Partner/Talent Alliance/Consulting And Planning Partner/Solution Partner/Investment & Operation and Financing Partner/Industrial Partner、Product Customers、Common Registered User. If your company is a ASP、Service Partner/Business Operation Partner、Sales Partner, after the company completes the authentication on the ePartner website, please refer to below guide to associate your personal account with your company.

Comparison with the environment where real devices are used

Real Device	Virtual Device
1 Huawei VRP and Configuration Basics	YunShan OS
2 Creating an Interconnected IP Network	Supported
3 Creating a Switched Ethernet Network	Supported
4 Network Security Basics and Network Access	Supported
5 Basic Network Service and Application Configuration	Supported
6 Creating a WLAN	Supported
7 Creating an IPv6 Network	Supported
8 Network Programming and Automation Basics	Not Supported
9 Configuring a Campus Network	Supported

Contents

About This Document ... 3

Overview ... 3

Background Knowledge Required ... 3

Common Icons ... 3

Experiment Environment Overview ... 3

Comparison with the environment where real devices are used ... 4

1 Huawei YunShan OS Basics ... 9

1.1 Introduction ... 9

1.1.1 About This Lab ... 9

1.1.2 Objectives ... 9

1.1.3 Networking Topology ... 9

1.2 Lab Configuration ... 10

1.2.1 Configuration Roadmap ... 10

1.2.2 Configuration Procedure ... 10

1.3 Quiz ... 17

1.4 Appendix ... 17

2 Creating an Interconnected IP Network ... 19

2.1 Lab 1: IPv4 Addressing and Routing ... 19

2.1.1 Introduction ... 19

2.1.2 Lab Configuration ... 20

2.1.3 Verification ... 31

2.1.4 Configuration Reference ... 31

2.1.5 Quiz ... 32

2.2 Lab 2: OSPF Routing ... 33

2.2.1 Introduction ... 33

2.2.2 Lab Configuration ... 34

2.2.3 Verification ... 40

2.2.4 Configuration Reference ... 40

2.2.5 Quiz ... 42

3 Creating a Switched Ethernet Network ... 43

3.1 Lab 1: Ethernet Basics and VLAN Configuration ... 43

3.1.1 Introduction ... 43

3.1.2 Lab Configuration ... 44

3.1.3 Verification ... 49

3.1.4 Configuration Reference 50
3.1.5 Quiz 51
3.2 Lab 2: Spanning Tree 52
3.2.1 Introduction 52
3.2.2 Lab Configuration 53
3.2.3 Verification 60
3.2.4 Configuration Reference 60
3.2.5 Quiz 61
3.3 Lab 3: Ethernet Link Aggregation 62
3.3.1 Introduction 62
3.3.2 Lab Configuration 62
3.3.3 Configuration Reference 68
3.3.4 Quiz 69
3.4 Lab 4: Inter-VLAN Communication 70
3.4.1 Introduction 70
3.4.2 Lab Configuration 71
3.4.3 Verification 74
3.4.4 Configuration Reference 74
3.4.5 Quiz 75
4 Network Security Basics and Network Access 76
4.1 Lab 1: ACL Configuration 76
4.1.1 Introduction 76
4.1.2 Lab Configuration 77
4.1.3 Configuration Reference 80
4.1.4 Quiz 81
4.2 Lab 2: Local AAA Configuration 82
4.2.1 Introduction 82
4.2.2 Lab Configuration 83
4.2.3 Configuration Reference 86
4.3 Lab 3: NAT Configuration 87
4.3.1 Introduction 87
4.3.2 Lab Configuration 88
4.3.3 Configuration Reference 92
4.3.4 Quiz 93
5 Basic Network Service and Application Configuration 94
5.1 Lab 1: FTP Configuration 94
5.1.1 Introduction 94
5.1.2 Lab Configuration 95
5.1.3 Verification 98

5.1.4 Configuration Reference 98
5.1.5 Quiz 99
5.2 Lab 2: DHCP Configuration 100
5.2.1 Introduction 100
5.2.2 Lab Configuration 101
5.2.3 Verification 103
5.2.4 Configuration Reference 106
5.2.5 Quiz 107
6 Creating a WLAN 108
6.1 Introduction 108
6.1.1 About This Lab 108
6.1.2 Objectives 108
6.1.3 Networking Topology 108
6.1.4 Data Planning 109
6.2 Lab Configuration 110
6.2.1 Configuration Roadmap 110
6.2.2 Configuration Procedure 110
6.3 Verification 116
6.4 Configuration Reference 118
6.5 Quiz 120
6.6 Appendix 120
7 Creating an IPv6 Network 121
7.1 Introduction 121
7.1.1 About This Lab 121
7.1.2 Objectives 121
7.1.3 Networking Topology 121
7.2 Lab Configuration 122
7.2.1 Configuration Roadmap 122
7.2.2 Configuration Procedure 122
7.3 Configuration Reference 130
7.4 Quiz 131
8 Network Programming and Automation Basics (Omitted) 132
9 Configuring a Campus Network 133
9.1 Reference Information 133
9.2 Introduction 133
9.2.1 About This Lab 133
9.2.2 Objectives 133
9.2.3 Networking Topology 134

9.3 Lab Tasks 134
9.3.1 Requirement Collection and Analysis 134
9.3.2 Planning and Design 135
9.3.3 Implementation 144
9.3.4 Network O&M 149
9.3.5 Network Optimization 151
9.4 Verification 151
9.5 Configuration Reference 151
9.6 Quiz 172

1 Huawei YunShan OS Basics

1.1 Introduction

1.1.1 About This Lab

In this lab activity, you will learn the basic operations of Huawei YunShan OS 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.

By default, the eNSP emulator connects to the console port. Therefore, when using the eNSP emulator, you can directly log in to the device without manually connecting the serial cable.

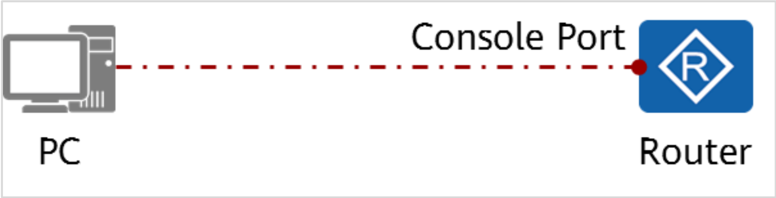


Figure 1-1 **Lab topology for understanding the VRP operating system**

The device model used in this experiment is ENSP-AR.

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.

```
Please press "Enter" to start command line
---------------------------------------------
eNSP can only be used for practice.
This device is an emulator and does not reflect a physical device model.
Some functions and commands may not supported.
Please read the feature list carefully before using.
---------------------------------------------
User interface con0 is available
Please Press ENTER.
Please configure the login password (8-16)
Enter Password: Huawei@123
Confirm Password: Huawei@123
Info: Save the password now. Please wait for a moment.
Info: The max number of VTY users is 5, the number of current VTY users online is 0, and total number
of terminal users online is 1.
        The current login time is 20XX-XX-XX XX:XX:XX.
```

You need to enter a password for the first login. The password must contain 8 to 16 characters and can be customized.

Step 2 Display the basic device information.

# Display device version information.

```
<HUAWEI> display version
Huawei YunShan OS
Version 1.22.0.1 (AR8000 V100R022C00)
Copyright (C) 2021-2022 Huawei Technologies Co., Ltd.
HUAWEI AR8140-12G10XG uptime is 0 day, 0 hour, 2 minutes
MPU(Master) 0 : uptime is   0 day, 0 hour, 2 minutes
          StartupTime 20XX/XX/XX     XX:XX:XX
Memory        Size      : 4096 M bytes
Flash         Size      : 0 M bytes
MPU version information:
1.PCB          Version : ar VER A
2.MAB           Version : 0
3.Board        Type      : ar
4.BIOS         Version : 000
5.CPLD          Version : 000
```

The command output shows that the router runs the **YunShan OS**, the device version is **V100R022C00**, the device model is **AR8140-12G10XG**, and the device has been running for **2** minutes.

Step 3 Complete basic device configurations.

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

```
<Huawei> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[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 GE                   //"GE" is the only optional keyword.
[Datacom-Router] interface GE 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-GE0/0/1]
```

The GE0/0/1 interface view is displayed.

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

By default, ENSP-AR ports work in Layer 2 mode. Run the **undo portswitch** command to switch the port from the Layer 2 mode to the Layer 3 mode.

```
[Datacom-Router-GE0/0/1] i?
  icmp                                    identity
  ifg                                    ifit
  ip                                     ipsec
  ipv6                                   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 GE0/0/1 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 **identity** are keywords.

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

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-GE0/0/1] ip address ?
  X.X.X.X        IP address
  bootp-alloc    IP address allocated by BOOTP
  dhcp-alloc     IP address allocated by DHCP
  unnumbered     Share an address with another interface
[Datacom-Router-GE0/0/1] ip address 192.168.1.1 ?
  INTEGER<0-32>      Length of IP address mask
  X.X.X.X                       IP address mask
[Datacom-Router-GE0/0/1] ip address 192.168.1.1 24 ?
  sub    Indicate a subordinate address
  tag    Match tag of the route
  <cr>
```

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

```
[Datacom-Router-GE0/0/1] dis this
#
interface GE0/0/1
 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-GE0/0/1] 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 GE0/0/2.

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

To do so, you must negate the IP address configuration of GE0/0/1. 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 GE 0/0/2
[Datacom-Router-GE0/0/2] undo portswitch
[Datacom-Router-GE0/0/2] ip address 192.168.1.1 24
[Datacom-Router-GE0/0/2] quit
```

# Display the current device configuration.

```
[Datacom-Router] display current-configuration
!Software Version V100R022C00
!Last configuration was updated at 20XX-XX-XX XX:XX:XX +00:00
!md_tlm VRPV800R006C00B016D0127-0.0.1
!telemetry VRPV800R006C00B016D0127-0.0.1
#
pki realm default
#
sysname Datacom-Router
#
undo ftp server source all-interface
undo ftp ipv6 server source all-interface
#
ssl policy default
 pki-domain default
 ssl minimum version tls1.2
 cipher-suite exclude key-exchange rsa
 cipher-suite exclude cipher mode cbc
 cipher-suite exclude hmac sha1
 diffie-hellman modulus 3072
 ecdh group curve brainpool
 signature algorithm-list ed25519 ed448 rsa-pss-pss-sha256 rsa-pss-pss-sha384 rsa-pss-pss-sha512 rsa-pss-rsae-sha256 rsa-pss-rsae-sha384 rsa-pss-rsae-sha512
#
authentication-profile name default_authen_profile
  ---- 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
Warning: The current configuration will be written to the device. Continue? [Y/N]: y //Enter y to confirm.
Now saving the current configuration to the slot 0 .
Info: Save the configuration 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
Building configuration.....
Info: The current configuration is the same as the next 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          FileName
    0   dr-x                -   Jun 24 XXXX 01:00:00   $_install_mod
    1   dr-x                -   May 15 XXXX 02:39:41   $_license
    2   dr-x                -   May 15 XXXX 02:39:08   $_startup
    3   dr-x                -   May 15 XXXX 02:39:56   $_system
    4   dr-x                -   May 15 XXXX 02:39:56   $_user
    5   -rw-           4,783   May 15 XXXX 06:58:05   1.cfg
    6   lrw-              29   May 15 XXXX 02:37:21   ENSP_V100R022C00B615.cc -> system file
    7   drwx               -   May 15 XXXX 02:41:43   default-sdb
    8   -rw-           4,183   May 15 XXXX 06:58:05   device.sys
    9   -rw-              46   May 15 XXXX 02:39:36   devm_script_reboot.txt
   10   drwx               -   May 15 XXXX 02:42:09   dhcp
   11   -rw-           1,636   May 15 XXXX 02:39:47   env_cfg
   12   drwx               -   May 15 XXXX 02:37:29   eva
   13   drwx               -   May 15 XXXX 03:09:55   full_kpi
   14   drwx               -   May 15 XXXX 02:38:34   hips
   15   drwx               -   May 15 XXXX 02:37:50   hrp
   16   dr-x               -   May 15 XXXX 06:48:42   logfile
   17   -rw-              33   May 15 XXXX 02:37:53   mem_env_cfg
   18   drwx               -   May 15 XXXX 02:38:32   nlog
   19   drwx               -   May 15 XXXX 02:40:07   pki
   20   drwx               -   May 15 XXXX 02:41:45   update
   21   drwx               -   May 15 XXXX 02:39:57   ztp

37,235,712 KB total (31,050,740 KB free)
```

1.cfg: configuration file The filename extension of a configuration file must be .cfg or .zip.

Note: On a physical device, the configuration file name is vrpcfg.zip.

ENSP_V100R022C00B615.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
Warning: Are you sure to save the configuration to flash:/test.cfg? [Y/N]:y    //Enter y to confirm.
Now saving the current configuration to the slot 0
Info: Save the configuration successfully.
```

# List all the files in the current directory again.

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

  Idx   Attr      Size(Byte)   Date            Time          FileName
    0   dr-x                -   Jun 24 XXXX 01:00:00   $_install_mod
    1   dr-x                -   May 15 XXXX 02:39:41   $_license
    2   dr-x                -   May 15 XXXX 02:39:08   $_startup
    3  dr-x                -  May 15 XXXX 02:39:56   $_system
    4  dr-x                -  May 15 XXXX 02:39:56   $_user
    5  -rw-            4,783  May 15 XXXX 06:58:05   1.cfg
    6  lrw-               29  May 15 XXXX 02:37:21   ENSP_V100R022C00B615.cc -> system file
    7  drwx                -  May 15 XXXX 02:41:43   default-sdb
    8  -rw-            4,183  May 15 XXXX 07:03:14   device.sys
    9  -rw-               46  May 15 XXXX 02:39:36   devm_script_reboot.txt
   10  drwx                -  May 15 XXXX 02:42:09   dhcp
   11  -rw-            1,636  May 15 XXXX 02:39:47   env_cfg
   12  drwx                -  May 15 XXXX 02:37:29   eva
   13  drwx                -  May 15 XXXX 03:09:55   full_kpi
   14  drwx                -  May 15 XXXX 02:38:34   hips
   15  drwx                -  May 15 XXXX 02:37:50   hrp
   16  dr-x                -  May 15 XXXX 06:48:42   logfile
   17  -rw-               33  May 15 XXXX 02:37:53   mem_env_cfg
   18  drwx                -  May 15 XXXX 02:38:32   nlog
   19  drwx                -  May 15 XXXX 02:40:07   pki
   20  -rw-            4,783  May 15 XXXX 07:03:14   test.cfg
   21  drwx                -  May 15 XXXX 02:41:45   update
   22  drwx                -  May 15 XXXX 02:39:57   ztp

37,235,712 KB total (31,068,112 KB free)
```

The configuration file is saved successfully.

# Set the file as the startup configuration file.

```
<Datacom-Router> startup saved-configuration test.cfg
Info: Succeeded in setting the configuration for booting system.
```

# Display the startup configuration file.

```
<Datacom-Router> display startup
MainBoard:
  Configured startup system software:        flash:/ENSP_V100R022C00B621.cc
  Startup system software:                   flash:/ENSP_V100R022C00B621.cc
  Next startup system software:              flash:/ENSP_V100R022C00B621.cc
  Startup saved-configuration file:          NULL
  Next startup saved-configuration file:     flash:/test.cfg
  Startup paf file:                          default
  Next startup paf file:                     default
  Startup patch package:                     NULL
  Next startup patch package:                NULL
  Startup feature software:                  NULL
  Next startup feature software:             NULL
```

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

# Clear the configuration file.

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

```
Info: Succeeded in clearing the configuration on the device.
```

Step 6 Restart the device.

```
<Datacom-Router> reboot
MPU 0:
Next startup system software: flash:/ENSP_V100R022C00B621.cc
Next startup saved-configuration file: NULL
Next startup paf file: default
Next startup patch package: NULL
Warning: The current configuration will be saved to the next startup saved-configuration file. Continue?
[Y/N]: y
Now saving the current configuration..
Save the configuration successfully.
Warning: The system will reboot. Continue? [Y/N]: y
System preprocessing has started, 100% completed.
System preprocessing succeeded.
```

----End

1.3 Quiz

1. 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?

When the system prompts that the current configuration will be saved to the next startup file, we select yes.

1.4 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.
<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.

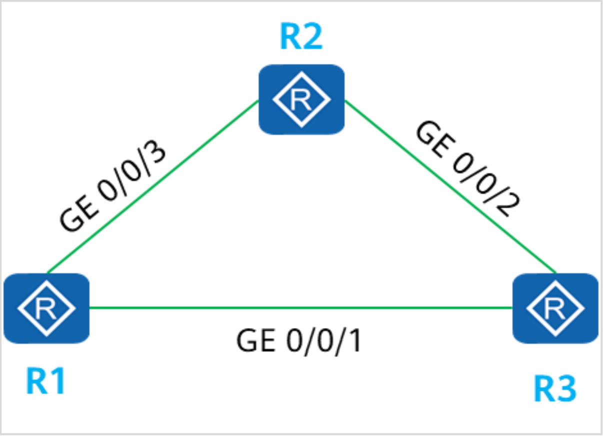


Figure 2-1 Lab topology for IPv4 addressing and routing

The device model used in this lab is ENSP-AR.

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 Switch the interface to a Layer 3 interface.

# R1 in this example

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] quit
[R1] interface GE 0/0/3
[R1-GE0/0/3] undo portswitch
[R1-GE0/0/3] quit
```

Step 3 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: FIB overload down
^down: standby
```

```
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(ed): error down
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2
Interface                IP Address/Mask     Physical Protocol      VPN
GE0/0/1                   unassigned          up        down       --
GE0/0/3                   unassigned          up        down       --
MEth0/0/0                 192.168.1.1/24      up        up         _management...
NULL0                     unassigned          up        up(s)      --
```

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.

GE0/0/1 and GE0/0/3 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 4 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	GE0/0/1	10.0.13.1/24
	GE0/0/3	10.0.12.1/24

R2	GE0/0/3	10.0.12.2/24
	GE0/0/2	10.0.23.2/24
R3	GE0/0/1	10.0.13.3/24
	GE0/0/2	10.0.23.3/24

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] ip address 10.0.13.1 24
[R1-GE0/0/1] quit
[R1] interface GE 0/0/3
[R1-GE0/0/3] ip address 10.0.12.1 24
[R1-GE0/0/3] quit
```

```
[R2] interface GE 0/0/2
[R2-GE0/0/2] ip address 10.0.23.2 24
[R2-GE0/0/2] quit
[R2] interface GE 0/0/3
[R2-GE0/0/3] ip address 10.0.12.2 24
[R2-GE0/0/3] quit
```

```
[R3] interface GE 0/0/1
[R3-GE0/0/1] ip address 10.0.13.3 24
[R3-GE0/0/1] quit
[R3] interface GE 0/0/2
[R3-GE0/0/2] ip address 10.0.23.3 24
[R3-GE0/0/2] 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
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 10          Routes : 10

Destination/Mask      Proto    Pre   Cost          Flags NextHop          Interface

      10.0.12.0/24   Direct   0      0               D    10.0.12.1        GE0/0/3
      10.0.12.1/32   Direct   0      0               D    127.0.0.1        GE0/0/3
    10.0.12.255/32   Direct   0      0               D    127.0.0.1        GE0/0/3
      10.0.13.0/24   Direct   0      0               D    10.0.13.1        GE0/0/1
      10.0.13.1/32   Direct   0      0               D    127.0.0.1        GE0/0/1
    10.0.13.255/32   Direct   0      0               D    127.0.0.1        GE0/0/1
      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 5 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
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 11          Routes : 11

Destination/Mask     Proto   Pre  Cost        Flags NextHop         Interface

       10.0.1.1/32   Direct  0    0             D   127.0.0.1       LoopBack0
      10.0.12.0/24   Direct  0    0             D   10.0.12.1       GE0/0/3
      10.0.12.1/32   Direct  0    0             D   127.0.0.1       GE0/0/3
    10.0.12.255/32   Direct  0    0             D   127.0.0.1       GE0/0/3
      10.0.13.0/24   Direct  0    0             D   10.0.13.1       GE0/0/1
      10.0.13.1/32   Direct  0    0             D   127.0.0.1       GE0/0/1
    10.0.13.255/32   Direct  0    0             D   127.0.0.1       GE0/0/1
      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
```

# 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 6 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
Proto: Protocol             Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 13          Routes : 13

Destination/Mask      Proto    Pre   Cost            Flags NextHop            Interface

       10.0.1.1/32   Direct   0      0                D     127.0.0.1          LoopBack0
       10.0.1.2/32   Static   60     0                RD    10.0.12.2          GE0/0/3
       10.0.1.3/32   Static   60     0                RD    10.0.13.3          GE0/0/1
      10.0.12.0/24   Direct   0      0                D     10.0.12.1          GE0/0/3
      10.0.12.1/32   Direct   0      0                D     127.0.0.1          GE0/0/3
    10.0.12.255/32   Direct   0      0                D     127.0.0.1          GE0/0/3
      10.0.13.0/24   Direct   0      0                D     10.0.13.1          GE0/0/1
      10.0.13.1/32   Direct   0      0                D     127.0.0.1          GE0/0/1
    10.0.13.255/32   Direct   0      0                D     127.0.0.1          GE0/0/1
      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
```

# 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 7 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
Proto: Protocol        Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost        Flags NextHop         Interface

       10.0.1.1/32  Static  60   0             RD  10.0.12.1       GE0/0/3
       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       GE0/0/2
      10.0.12.0/24  Direct  0    0             D   10.0.12.2       GE0/0/3
      10.0.12.2/32  Direct  0    0             D   127.0.0.1       GE0/0/3
    10.0.12.255/32  Direct  0    0             D   127.0.0.1       GE0/0/3
      10.0.23.0/24  Direct  0    0             D   10.0.23.2       GE0/0/2
      10.0.23.2/32  Direct  0    0             D   127.0.0.1       GE0/0/2
    10.0.23.255/32  Direct  0    0             D   127.0.0.1       GE0/0/2
      127.0.0.0/8   Direct  0    0             D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0             D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0             D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0             D   127.0.0.1       InLoopBack0
```

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 GE 0/0/3
[R1-GE0/0/3] shutdown
```

```
[R2] interface GE 0/0/3
[R2-GE0/0/3] 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
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 10          Routes : 10

Destination/Mask     Proto    Pre   Cost          Flags NextHop          Interface

       10.0.1.1/32   Direct   0     0              D    127.0.0.1        LoopBack0
       10.0.1.2/32   Static   100   0              RD   10.0.13.3        GE0/0/1
       10.0.1.3/32   Static   60    0              RD   10.0.13.3        GE0/0/1
      10.0.13.0/24   Direct   0     0              D    10.0.13.1        GE0/0/1
      10.0.13.1/32   Direct   0     0              D    127.0.0.1        GE0/0/1
    10.0.13.255/32   Direct   0     0              D    127.0.0.1        GE0/0/1
      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
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 10          Routes : 10

Destination/Mask     Proto    Pre   Cost          Flags NextHop          Interface

       10.0.1.1/32   Static   100   0              RD   10.0.23.3        GE0/0/2
       10.0.1.2/32   Direct   0     0              D    127.0.0.1        LoopBack0
       10.0.1.3/32   Static   60    0              RD   10.0.23.3        GE0/0/2
      10.0.23.0/24   Direct   0     0              D    10.0.23.2        GE0/0/2
      10.0.23.2/32   Direct   0     0              D    127.0.0.1        GE0/0/2
    10.0.23.255/32   Direct   0     0              D    127.0.0.1        GE0/0/2
      127.0.0.0/8    Direct   0     0              D    127.0.0.1        InLoopBack0
```

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

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 GE0/0/1 of R3 and are then forwarded to GE0/0/2 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 8 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 GE 0/0/3
[R1-GE0/0/3] undo shutdown
[R1-GE0/0/3] 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
```

```
[R2] interface GE 0/0/3
[R2-GE0/0/3] undo shutdown
```

```
[R2-GE0/0/3] quit
```

# Display the routing table of R1.

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

Destination/Mask    Proto    Pre   Cost        Flags NextHop          Interface

       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        GE0/0/1
      10.0.12.0/24   Direct   0     0            D    10.0.12.1        GE0/0/3
      10.0.12.1/32   Direct   0     0            D    127.0.0.1        GE0/0/3
    10.0.12.255/32   Direct   0     0            D    127.0.0.1        GE0/0/3
      10.0.13.0/24   Direct   0     0            D    10.0.13.1        GE0/0/1
      10.0.13.1/32   Direct   0     0            D    127.0.0.1        GE0/0/1
    10.0.13.255/32   Direct   0     0            D    127.0.0.1        GE0/0/1
      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
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 13        Routes : 13

Destination/Mask    Proto    Pre   Cost        Flags NextHop          Interface

         0.0.0.0/0   Static   60    0            RD   10.0.12.2        GE0/0/3
       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        GE0/0/1
      10.0.12.0/24   Direct   0     0            D    10.0.12.1        GE0/0/3
      10.0.12.1/32   Direct   0     0            D    127.0.0.1        GE0/0/3
    10.0.12.255/32   Direct   0     0            D    127.0.0.1        GE0/0/3
      10.0.13.0/24   Direct   0     0            D    10.0.13.1        GE0/0/1
      10.0.13.1/32   Direct   0     0            D    127.0.0.1        GE0/0/1
    10.0.13.255/32   Direct   0     0            D    127.0.0.1        GE0/0/1
      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
```

----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 GE0/0/1
 ip address 10.0.13.1 255.255.255.0
#
interface GE0/0/3
 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 GE0/0/2
 ip address 10.0.23.3 255.255.255.0
#
interface GE0/0/3
 ip address 10.0.12.2 255.255.255.0
#
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 GE0/0/1
 ip address 10.0.13.3 255.255.255.0
#
interface GE0/0/2
 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?

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. 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?

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.

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.

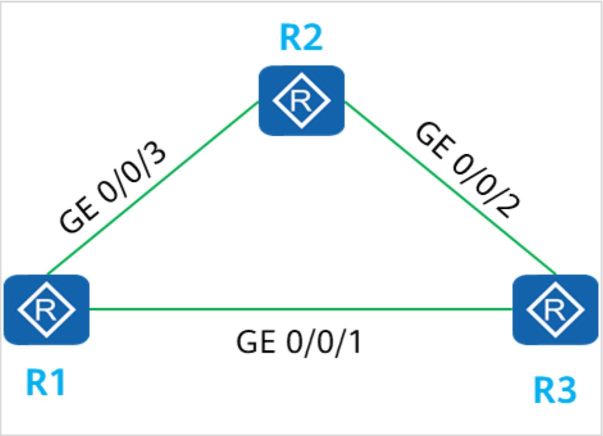


Figure 2-2 Lab topology for configuring OSPF

The device model used in this lab is ENSP-AR.

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
Proto: Protocol         Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 11         Routes : 11

Destination/Mask    Proto   Pre  Cost        Flags NextHop         Interface

        10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.12.0/24  Direct  0    0           D   10.0.12.1       GE0/0/3
       10.0.12.1/32  Direct  0    0           D   127.0.0.1       GE0/0/3
     10.0.12.255/32  Direct  0    0           D   127.0.0.1       GE0/0/3
       10.0.13.0/24  Direct  0    0           D   10.0.13.1       GE0/0/1
       10.0.13.1/32  Direct  0    0           D   127.0.0.1       GE0/0/1
     10.0.13.255/32  Direct  0    0           D   127.0.0.1       GE0/0/1
       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 router-id 10.0.1.1
```

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 1 router-id 10.0.1.2
[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 1 router-id 10.0.1.3
[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
 Area 0.0.0.0 interface 10.0.13.1 (GE0/0/1)'s neighbors
   Router ID: 10.0.1.3             Address : 10.0.13.3
   State      : Full               Mode      : Nbr is Master        Priority: 1
   DR          : 10.0.13.1              BDR        : 10.0.13.3              MTU        : 0
   Dead timer due (in seconds) : 34
   Retrans timer interval         : 5
   Neighbor up time                  : 00h00m58s
   Neighbor up time stamp         : 20XX-XX-XX XX:XX:XX
   Authentication Sequence        : 0

 Area 0.0.0.0 interface 10.0.12.1 (GE0/0/3)'s neighbors
   Router ID: 10.0.1.2                 Address : 10.0.12.2
   State      : Full                    Mode       : Nbr is Master         Priority: 1
   DR          : 10.0.12.1              BDR        : 10.0.12.2              MTU        : 0
   Dead timer due (in seconds) : 34
   Retrans timer interval         : 5
   Neighbor up time                  : 00h00m58s
   Neighbor up time stamp         : 20XX-XX-XX XX:XX:XX
   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
Proto: Protocol             Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
_public_ Routing Table : OSPF
          Destinations : 6            Routes : 7

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

Destination/Mask       Proto    Pre   Cost           Flags NextHop            Interface

        10.0.1.2/32   OSPF     10    1                D     10.0.12.2          GE0/0/3
        10.0.1.3/32   OSPF     10    1                D     10.0.13.3          GE0/0/1
       10.0.23.0/24   OSPF     10    2                D     10.0.12.2          GE0/0/3
                       OSPF     10    2                D     10.0.13.3          GE0/0/1

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

Destination/Mask       Proto    Pre   Cost           Flags NextHop            Interface

        10.0.1.1/32   OSPF     10    0                      10.0.1.1          LoopBack0
       10.0.12.0/24   OSPF     10    1                      10.0.12.1         GE0/0/3
       10.0.13.0/24   OSPF     10    1                      10.0.13.1         GE0/0/1
```

Step 4   Configure OSPF authentication.

# Configure interface authentication on R1.

```
<R1> install feature-software WEAKEA
Info: Operating, please wait for a moment.....done.
Info: Succeeded in installing the software.
<R1> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[R1] interface GE 0/0/1
[R1-GE0/0/1] ospf authentication-mode md5 1 cipher HCIA-Datacom
[R1-GE0/0/1] quit
[R1] interface GE 0/0/3
[R1-GE0/0/3] ospf authentication-mode md5 1 cipher HCIA-Datacom
[R1-GE0/0/3] display this
#
interface GE0/0/3
 ip address 10.0.12.1 255.255.255.0
 ospf authentication-mode md5 1 cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!>
UM^/\R,+8Dn|kVU~(cDO~#|9UrBp6[JrBT!!!!!2jp5!!!!!!=!!!!Hf~%4{"=`X[1i>
9o[_!M(/\oG,gQ3<EDEe)!!!!!%+%#
#
return
```

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
[R1]
```

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

# Configuring interface authentication on R2.

```
<R2> install feature-software WEAKEA
Info: Operating, please wait for a moment.....done.
Info: Succeeded in installing the software.
<R2> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[R2] interface GE 0/0/2
[R2-GE0/0/2] ospf authentication-mode md5 1 cipher HCIA-Datacom
[R2-GE0/0/2] quit
[R2] interface GE 0/0/3
[R2-GE0/0/3] ospf authentication-mode md5 1 cipher HCIA-Datacom
[R2-GE0/0/3] quit
```

# Display OSPF neighbors on R2.

```
[R2] display ospf peer brief
OSPF Process 1 with Router ID 10.0.1.2
                    Peer Statistic Information
Total number of peer(s): 1
 Peer(s) in full state: 1
-----------------------------------------------------------------------------
```

```
 Area Id          Interface                    Neighbor id           State
 0.0.0.0         GE0/0/3                       10.0.1.1              Full
----------------------------------------------------------------------------
```

R2 has established a neighbor relationship with R1.

# Configure area authentication on R3.

```
<R3> install feature-software WEAKEA
Info: Operating, please wait for a moment.....done.
Info: Succeeded in installing the software.
<R3> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[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
Total number of peer(s): 2
 Peer(s) in full state: 2
----------------------------------------------------------------------------
 Area Id          Interface                    Neighbor id           State
 0.0.0.0         GE0/0/1                       10.0.1.1              Full
 0.0.0.0         GE0/0/2                       10.0.1.2              Full
----------------------------------------------------------------------------
```

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
```

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

Destination/Mask      Proto    Pre   Cost          Flags NextHop           Interface

          0.0.0.0/0    O_ASE    150   1              D     10.0.12.1         GE0/0/3
         10.0.1.1/32   OSPF     10    1              D     10.0.12.1         GE0/0/3
         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         GE0/0/2
        10.0.12.0/24   Direct    0     0              D     10.0.12.2         GE0/0/3
        10.0.12.2/32   Direct    0     0              D     127.0.0.1         GE0/0/3
```

```
[R3] display ip routing-table
Proto: Protocol            Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
            Destinations : 15          Routes : 16

Destination/Mask      Proto    Pre   Cost          Flags NextHop           Interface

          0.0.0.0/0    O_ASE    150   1              D     10.0.13.1         GE0/0/1
         10.0.1.1/32   OSPF     10    1              D     10.0.13.1         GE0/0/1
         10.0.1.2/32   OSPF     10    1              D     10.0.23.2         GE0/0/2
         10.0.1.3/32   Direct    0     0              D     127.0.0.1         LoopBack0
```

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 GE 0/0/3
[R1-GE0/0/3] ospf cost 10
```

# Display the routing table of R1.

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

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

         10.0.1.1/32   Direct   0       0               D     127.0.0.1          LoopBack0
         10.0.1.2/32   OSPF      10     2                 D     10.0.13.3          GE0/0/1
         10.0.1.3/32   OSPF      10     1                 D     10.0.13.3          GE0/0/1
```

In this case, the next hop of the route from R1 to LoopBack0 on R2 is GE0/0/1 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 GE0/0/1
 ip address 10.0.13.1 255.255.255.0
 ospf authentication-mode md5 1 cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!>
UM^/\R,+8^;rO/Pu*PA={fJ;#Gcw6-,slV!!!!!2jp5!!!!!!=!!!!^x`V)1|Y+Da'ce0:g-<H9z3s,_{`}<=e*> /!!!!!%+%#
#
interface GE0/0/2
 portswitch
#
interface GE0/0/3
 ip address 10.0.12.1 255.255.255.0
 ospf authentication-mode md5 1 cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!>
UM^/\R,+8Dn|kVU~(cDO~#|9UrBp6[JrBT!!!!!2jp5!!!!!!=!!!!Hf~%4{"=`X[1i>
9o[_!M(/\oG,gQ3<EDEe)!!!!!%+%#
 ospf cost 10
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
ospf 1 router-id 10.0.1.1
 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
```

Configuration on R2

```
sysname R2
#
interface GE0/0/2
 ip address 10.0.23.2 255.255.255.0
 ospf authentication-mode md5 1
cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!+[si0)5K+~^%7X@lQo:M,NzMB|nR3Up,~\L!!!!!2jp5!!!!!!=!!!!,@Ju);T,U9(!A%
DE.mbKJmOmD] 1D5VEPQ] L!!!!!%+%#
#
interface GE0/0/3
 ip address 10.0.12.2 255.255.255.0
 ospf authentication-mode md5 1
cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!+[si0)5K+~l%!32/LnK!"zA0W*nRTYHX9#O!!!!!2jp5!!!!!!=!!!!7T"]
CO}It%1fhxDK'D[2-|6")&5a.8:] #F%!!!!!%+%#
#
interface LoopBack0
 ip address 10.0.1.2 255.255.255.255
#
ospf 1 router-id 10.0.1.2
 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
#
```

Configuration on R3

```
sysname R3
#
interface GE0/0/1
 ip address 10.0.13.3 255.255.255.0
#
interface GE0/0/2
 ip address 10.0.23.3 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.3 255.255.255.255
#
interface NULL0
#
ospf 1 router-id 10.0.1.3
 area 0.0.0.0
  authentication-mode md5 1
cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!+LY<A}l!!TR=w}9Z9lG$rr6aQ\%mN:907N,!!!!!2jp5!!!!!!=!!!!INJV1!BGW<Cb*}
$IVskDsfBB*e437.wk"UB!!!!!%+%#
  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
#
```

2.2.5 Quiz

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

R2 replies to R1 along the path of R2->R1.

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.

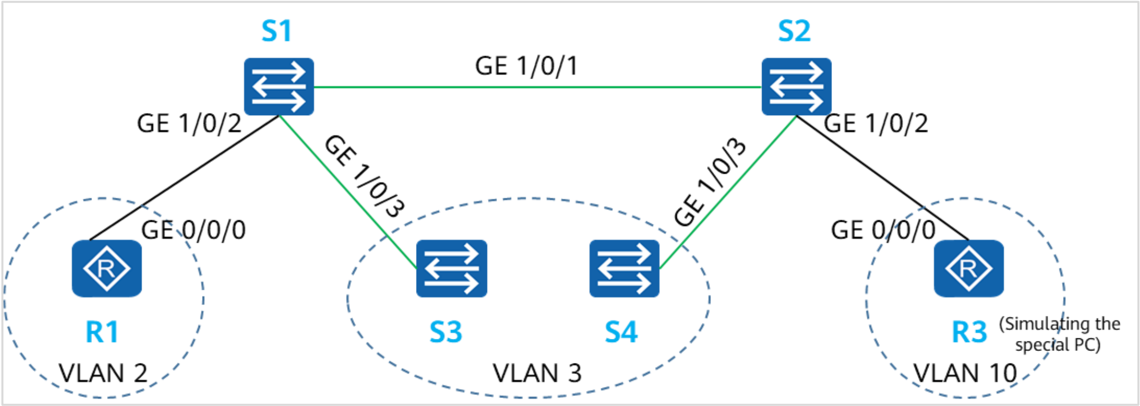


Figure 3-1 **Lab topology for VLAN configuration**

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 Complete basic device configuration.

# Name the devices.

The details are not provided here.

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 GE 0/0/0
[R1-GE0/0/0] undo portswitch
[R1-GE0/0/0] ip address 10.1.2.1 24
[R1-GE0/0/0] quit
```

```
[R3] interface GE 0/0/0
[R3-GE0/0/0] undo portswitch
[R3-GE0/0/0] ip address 10.1.10.1 24
[R3-GE0/0/0] quit
```

# Set the IP addresses of VLANIF3 on S3 and S4 to 10.1.3.1/24 and 10.1.3.2/24, respectively. Create VLAN 3 on S3 and S4.

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

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

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

```
[S3] interface GE 1/0/3
[S3-GE1/0/3] port link-type access
[S3-GE1/0/3] port default vlan 3
[S3-GE1/0/3] quit
```

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

```
[S4] interface GE 1/0/3
[S4-GE1/0/3] port link-type access
[S4-GE1/0/3] port default vlan 3
[S4-GE1/0/3] quit
```

# 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 GE 1/0/2
[S1-GE1/0/2] port link-type access
[S1-GE1/0/2] port default vlan 2
[S1-GE1/0/2] quit
```

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

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

```
[S2] interface GE 1/0/3
[S2-GE1/0/3] port link-type access
[S2-GE1/0/3] port default vlan 3
[S2-GE1/0/3] 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 GE 1/0/1
[S1-GE1/0/1] port link-type trunk
[S1-GE1/0/1] port trunk allow-pass vlan 2 3
```

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

```
[S1-GE1/0/1] 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 GE 1/0/1
[S2-GE1/0/1] port link-type trunk
[S2-GE1/0/1] port trunk allow-pass vlan 2 3
[S2-GE1/0/1] undo port trunk allow-pass vlan 1
[S2-GE1/0/1] quit
```

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 fa9f-1b6d-0060. The PC is expected to connect to the network through GE1/0/2 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 fa9f-1b6d-0060
```

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

# Set GE1/0/2 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 GE 1/0/2
[S2-GE1/0/2] port link-type hybrid
[S2-GE1/0/2] port hybrid untagged vlan 10
[S2-GE1/0/2] quit
```

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

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

```
[S2] interface GE 1/0/1
[S2-GE1/0/1] port trunk allow-pass vlan 10
[S2-GE1/0/1] 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 GE 1/0/2
[S2-GE1/0/2] mac-vlan enable
[S2-GE1/0/2] quit
```

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

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.

```
[S1] display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
MAC-LRN: MAC-address learning;  STAT: Statistic;
BC: Broadcast; MC: Multicast;   UC: Unknown-unicast;
FWD: Forward;  DSD: Discard;
--------------------------------------------------------------------------------

VID       Ports
--------------------------------------------------------------------------------
   1      UT:GE1/0/4(U)     GE1/0/5(U)     GE1/0/6(U)     GE1/0/7(U)
             GE1/0/8(U)     GE1/0/9(U)     GE1/0/10(U)
   2      UT:GE1/0/2(U)
          TG:GE1/0/1(U)
   3      UT:GE1/0/3(U)
          TG:GE1/0/1(U)
  10      TG:GE1/0/1(U)

VID  Type      Status  Property  MAC-LRN STAT    BC  MC  UC  Description
--------------------------------------------------------------------------------
   1 common    enable  default   enable  disable FWD FWD FWD VLAN 0001
   2 common    enable  default   enable  disable FWD FWD FWD VLAN 0002
   3 common    enable  default   enable  disable FWD FWD FWD VLAN 0003
  10 common    enable  default   enable  disable FWD FWD FWD VLAN 0010
```

```
[S2] display vlan
```

```
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;          D: Down;          TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                 ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
MAC-LRN: MAC-address learning;  STAT: Statistic;
BC: Broadcast; MC: Multicast;   UC: Unknown-unicast;
FWD: Forward;   DSD: Discard;
--------------------------------------------------------------------------------

VID            Ports
--------------------------------------------------------------------------------
   1           UT:GE1/0/2(U)      GE1/0/4(U)      GE1/0/5(U)      GE1/0/6(U)
                  GE1/0/7(U)      GE1/0/8(U)      GE1/0/9(U)      GE1/0/10(U)
   2           TG:GE1/0/1(U)
   3           UT:GE1/0/3(U)
               TG:GE1/0/1(U)
  10           UT:GE1/0/2(U)
               TG:GE1/0/1(U)

VID   Type       Status   Property   MAC-LRN STAT     BC   MC   UC   Description
--------------------------------------------------------------------------------
   1 common     enable   default     enable   disable FWD FWD FWD VLAN 0001
   2 common     enable   default     enable   disable FWD FWD FWD VLAN 0002
   3 common     enable   default     enable   disable FWD FWD FWD VLAN 0003
  10 common     enable   default     enable   disable FWD FWD FWD VLAN 0010
```

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

```
[S2] display mac-vlan vlan 10
Total MAC VLAN address count: 1
---------------------------------------------------
MAC Address       Mask                  VLAN      Priority
---------------------------------------------------
fa9f-1b6d-0060    ffff-ffff-ffff      10                0
```

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.

```
<S3> ping 10.1.3.2
  PING 10.1.3.2: 56   data bytes, press CTRL_C to break
    Reply from 10.1.3.2: bytes=56 Sequence=1 ttl=254 time=114 ms
    Reply from 10.1.3.2: bytes=56 Sequence=2 ttl=254 time=13 ms
    Reply from 10.1.3.2: bytes=56 Sequence=3 ttl=254 time=13 ms
    Reply from 10.1.3.2: bytes=56 Sequence=4 ttl=254 time=13 ms
    Reply from 10.1.3.2: bytes=56 Sequence=5 ttl=254 time=10 ms
  --- 10.1.3.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/32/114 ms
```

2. Ping other devices from R1 and ensure that the ping operation fails.

```
<R1> ping -c 1 10.1.3.1
  PING 10.1.3.1: 56  data bytes, press CTRL_C to break
    Request time out

  --- 10.1.3.1 ping statistics ---
    1 packet(s) transmitted
    0 packet(s) received
100.00% packet loss

<R1> ping -c 1 10.1.3.2
  PING 10.1.3.2: 56  data bytes, press CTRL_C to break
    Request time out

  --- 10.1.3.2 ping statistics ---
    1 packet(s) transmitted
    0 packet(s) received
100.00% packet loss

<R1> ping -c 1 10.1.10.1
  PING 10.1.10.1: 56  data bytes, press CTRL_C to break
    Request time out

  --- 10.1.10.1 ping statistics ---
    1 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

3.1.4 Configuration Reference

Configuration on S1

```
sysname S1
#
vlan batch 2 to 3 10
#
interface GE1/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
interface GE1/0/2
 port default vlan 2
#
interface GE1/0/3
 port default vlan 3
```

```
#
```

Configuration on S2

```
sysname S2
#
vlan batch 2 to 3 10
#
vlan 10
 mac-vlan mac-address fa9f-1b6d-0060
#
interface GE1/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
interface GE1/0/2
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GE1/0/3
 port default vlan 3
#
```

3.1.5 Quiz

1. On R3, ping the IP address of R1. Can related packets be captured on S2?

No packet is captured because no gateway is configured on R3.

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.

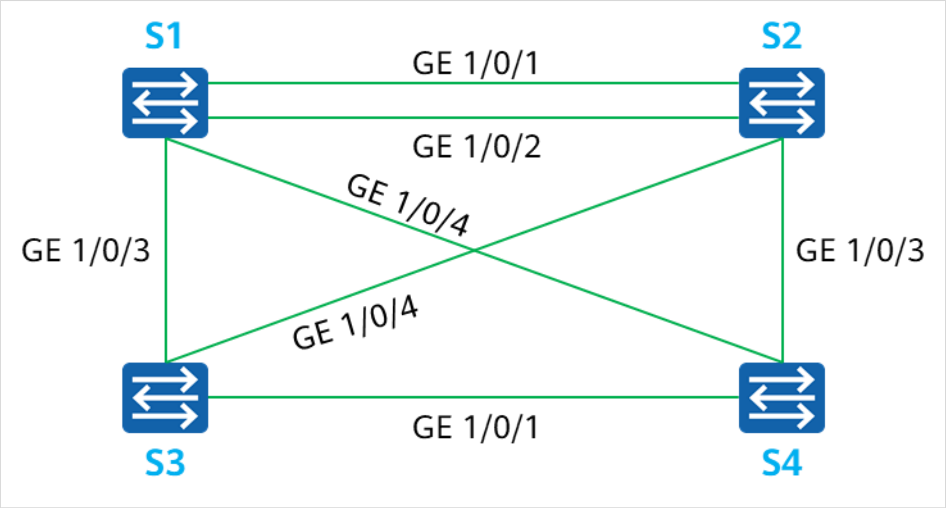


Figure 3-2 Lab topology for configuring STP

The device model used in this lab is ENSP-LSW.

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 Complete basic device configuration.

# Name the devices.

The details are not provided here.

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
```

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
```

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

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

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

```
[S1] display stp
CIST Global Information:
  Mode                    :STP
  CIST Bridge             :32768.fa9f-1b6d-0011        //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.fa9f-1b6d-0011 / 0 (This bridge is the root)   //ID and path cost of the
current root bridge.
  CIST RegRoot/IRPC       :32768.fa9f-1b6d-0011 / 0 (This bridge is the root)
  CIST RootPortId         :0.0
  BPDU-Protection         :Disabled
  TC or TCN received      :15
  TC count per hello      :0
  STP Converge Mode       :Normal
  Share region-configuration :Enabled
  Time since last TC      :0 days 0h:0m:21s
  Number of TC            :24
  Last TC occurred        :GE1/0/1
  Topo Change Flag        :0
```

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.

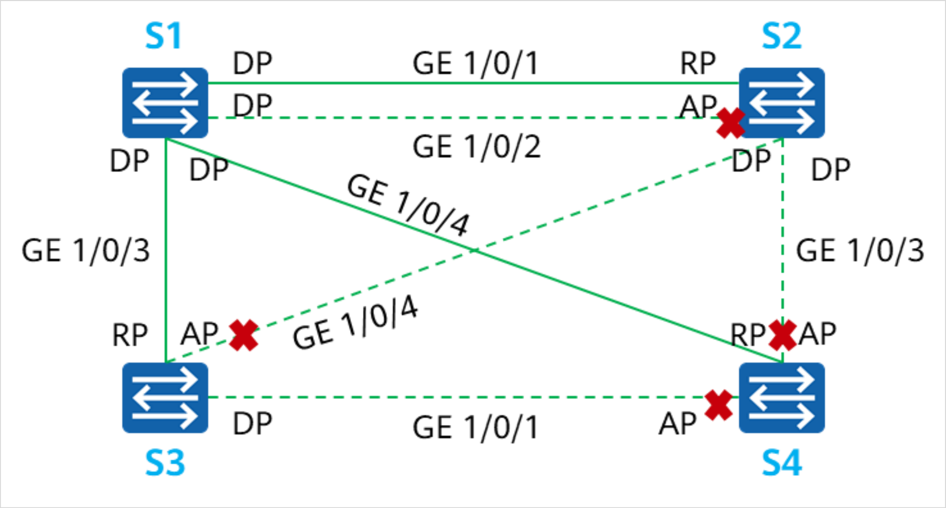
```
[S1] display stp brief
 MSTID  Port                        Role  STP State     Protection      Cost     Edged
     0  GE1/0/1                     DESI  forwarding    none            20000    disable
     0  GE1/0/2                     DESI  forwarding    none            20000    disable
     0  GE1/0/3                     DESI  forwarding    none            20000    disable
     0  GE1/0/4                     DESI  forwarding    none            20000    disable
```

```
[S2] display stp brief
 MSTID  Port                        Role  STP State     Protection      Cost     Edged
     0  GE1/0/1                     ROOT  forwarding    none            20000    disable
     0  GE1/0/2                     ALTE  discarding    none            20000    disable
     0  GE1/0/3                     DESI  forwarding    none            20000    disable
     0  GE1/0/4                     DESI  forwarding    none            20000    disable
```

```
[S3] display stp brief
 MSTID  Port                        Role  STP State     Protection      Cost     Edged
     0  GE1/0/1                     DESI  forwarding    none            20000    disable
     0  GE1/0/2                     DESI  forwarding    none            20000    disable
     0  GE1/0/3                     ROOT  forwarding    none            20000    disable
     0  GE1/0/4                     ALTE  discarding    none            20000    disable
```

```
<S4> display stp brief
 MSTID   Port                          Role   STP State     Protection      Cost     Edged
     0   GE1/0/1                       ALTE   discarding    none            20000    disable
     0   GE1/0/2                       DESI   forwarding    none            20000    disable
     0   GE1/0/3                       ALTE   discarding    none            20000    disable
     0   GE1/0/4                       ROOT   forwarding    none            20000    disable
```

# 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 S2 the root bridge and S1 the secondary root bridge.

# Change the bridge priorities of S1 and S2.

```
[S2] 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.

```
[S1] stp root secondary
```

# Display the STP status on S2.

```
[S2] display stp
CIST Global Information:
  Mode                    :STP
  CIST Bridge             :0.fa9f-1b6d-0021
  Config Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  Active Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  CIST Root/ERPC          :0.fa9f-1b6d-0021 / 0 (This bridge is the root)
  CIST RegRoot/IRPC       :0.fa9f-1b6d-0021 / 0 (This bridge is the root)
  CIST RootPortId         :0.0
  BPDU-Protection         :Disabled
  CIST Root Type          :Primary root
  TC or TCN received      :126
  TC count per hello      :0
  STP Converge Mode       :Normal
  Share region-configuration :Enabled
  Time since last TC      :0 days 0h:0m:10s
  Number of TC            :36
  Last TC occurred        :GE1/0/4
  Topo Change Flag        :0
```

In this case, the bridge ID of S2 is the same as the root bridge ID, and the root path cost is 0, indicating that S2 is the root bridge of the current network.

# Display the brief STP status information on all devices.

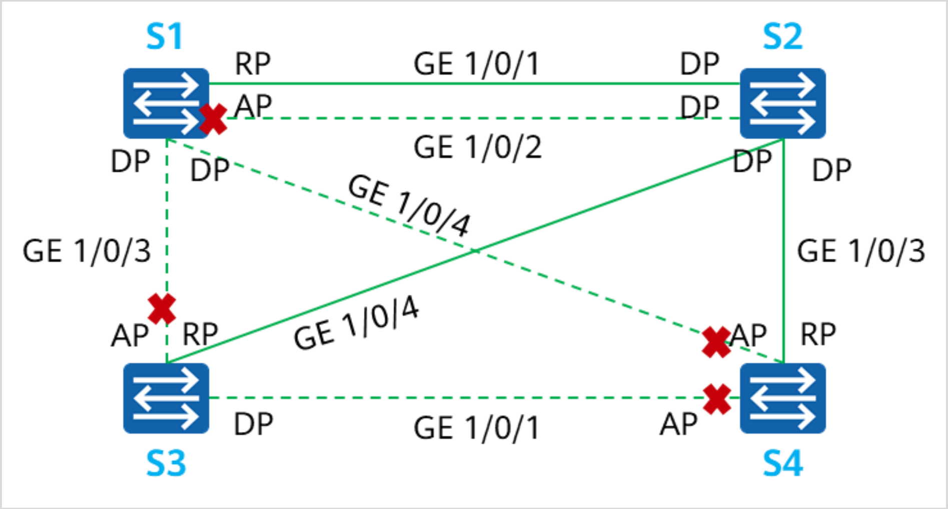
```
[S1] display stp brief
 MSTID  Port                        Role  STP State     Protection     Cost    Edged
     0  GE1/0/1                     ROOT  forwarding    none           20000   disable
     0  GE1/0/2                     ALTE  discarding    none           20000   disable
     0  GE1/0/3                     DESI  forwarding    none           20000   disable
     0  GE1/0/4                     DESI  forwarding    none           20000   disable
```

```
[S2] display stp brief
 MSTID  Port                        Role  STP State     Protection     Cost    Edged
     0  GE1/0/1                     DESI  forwarding    none           20000   disable
     0  GE1/0/2                     DESI  forwarding    none           20000   disable
     0  GE1/0/3                     DESI  forwarding    none           20000   disable
     0  GE1/0/4                     DESI  forwarding    none           20000   disable
```

```
<S3> display stp brief
 MSTID  Port                        Role  STP State     Protection     Cost    Edged
     0  GE1/0/1                     DESI  forwarding    none           20000   disable
     0  GE1/0/2                     DESI  forwarding    none           20000   disable
     0  GE1/0/3                     ALTE  discarding    none           20000   disable
     0  GE1/0/4                     ROOT  forwarding    none           20000   disable
```

```
<S4> display stp brief
 MSTID   Port                              Role   STP State      Protection        Cost      Edged
      0   GE1/0/1                          ALTE   discarding     none              20000      disable
      0   GE1/0/2                          DESI   forwarding     none              20000      disable
      0   GE1/0/3                          ROOT   forwarding     none              20000      disable
      0   GE1/0/4                          ALTE   discarding     none              20000      disable
```

# 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 GE1/0/4 of S4 the root port.

# Display the STP information on S4.

```
<S4> display stp
CIST Global Information:
   Mode                          :STP
   CIST Bridge              :32768.fa9f-1b6d-0041
   Config Times              :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
   Active Times              :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
   CIST Root/ERPC          :0.fa9f-1b6d-0021 / 20000
   CIST RegRoot/IRPC     :32768.fa9f-1b6d-0041 / 0 (This bridge is the root)
   CIST RootPortId         :128.3 (GE1/0/3)
   BPDU-Protection         :Disabled
   TC or TCN received   :284
   TC count per hello    :0
   STP Converge Mode     :Normal
   Share region-configuration :Enabled
   Time since last TC    :0 days 0h:9m:35s
   Number of TC              :30
   Last TC occurred        :GE1/0/3
   Topo Change Flag       :0
```

The cost of the root path from S4 to S2 is 20000.

# Change the STP cost of GE 1/0/3 on S4 to 50000.

```
[S4] interface GE 1/0/3
[S4-GE1/0/3] stp cost 50000
[S4-GE1/0/3] quit
```

# Display the brief STP status information.

```
[S4] display stp brief
 MSTID   Port                          Role   STP State      Protection       Cost      Edged
     0   GE1/0/1                       ALTE   discarding     none             20000     disable
     0   GE1/0/2                       DESI   forwarding     none             20000     disable
     0   GE1/0/3                       ALTE   discarding     none             50000     disable
     0   GE1/0/4                       ROOT   forwarding     none             20000     disable
```

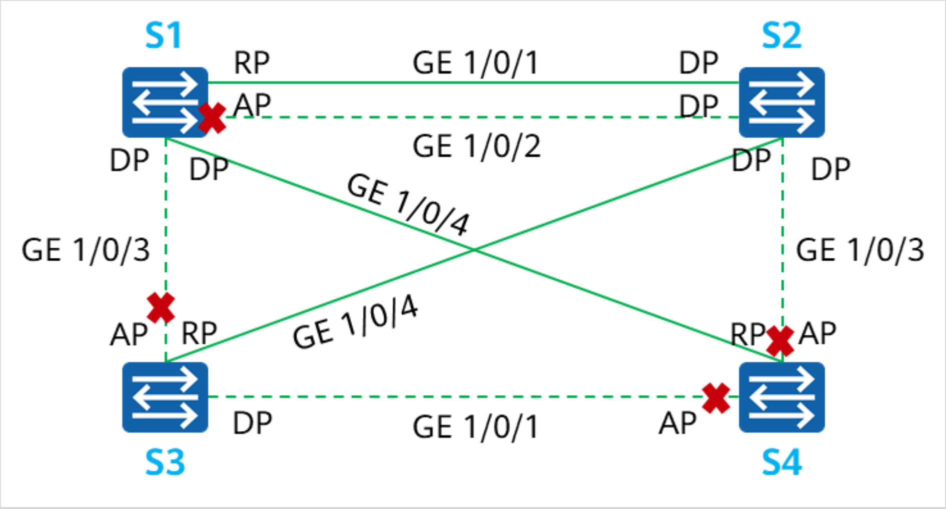
GE1/0/4 on S4 has become the root port.

# Display the current STP status information.

```
[S4] display stp
CIST Global Information:
  Mode                   :STP
  CIST Bridge            :32768.fa9f-1b6d-0041
  Config Times           :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  Active Times           :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  CIST Root/ERPC         :0.fa9f-1b6d-0021 / 40000
  CIST RegRoot/IRPC      :32768.fa9f-1b6d-0041 / 0 (This bridge is the root)
  CIST RootPortId        :128.4 (GE1/0/4)
  BPDU-Protection        :Disabled
  TC or TCN received     :375
  TC count per hello     :0
  STP Converge Mode      :Normal
  Share region-configuration :Enabled
  Time since last TC     :0 days 0h:0m:39s
  Number of TC           :36
  Last TC occurred       :GE1/0/4
  Topo Change Flag       :0
```

The root path cost of S4 is now 40000.

# 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
```

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

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

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

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

```
[S1] display stp
CIST Global Information:
  Mode                     :RSTP
  CIST Bridge              :4096.fa9f-1b6d-0011
  Config Times             :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  Active Times             :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
  CIST Root/ERPC           :0.fa9f-1b6d-0021 / 20000
  CIST RegRoot/IRPC        :4096.fa9f-1b6d-0011 / 0 (This bridge is the root)
  CIST RootPortId          :128.1 (GE1/0/1)
  BPDU-Protection          :Disabled
  CIST Root Type           :Secondary root
  TC or TCN received       :119
  TC count per hello       :0
  STP Converge Mode        :Normal
  Share region-configuration :Enabled
```

```
   Time since last TC   :0 days 0h:0m:5s
   Number of TC           :44
   Last TC occurred      :GE1/0/1
   Topo Change Flag      :0
```

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

Step 6 Configure edge ports.

# GE1/0/5-1/0/10 of S3 are connected only to terminals and need to be configured as edge ports.

```
[S3] interface range GE 1/0/5 to GE 1/0/10
```

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 secondary
#
```

Configuration on S2

```
sysname S2
#
stp mode rstp
stp instance 0 root primary
#
```

Configuration on S3

```
sysname S3
#
interface GE1/0/5
 stp edged-port enable
#
interface GE1/0/6
 stp edged-port enable
#
interface GE1/0/7
 stp edged-port enable
#
interface GE1/0/8
 stp edged-port enable
#
interface GE1/0/9
 stp edged-port enable
#
interface GE1/0/10
 stp edged-port enable
#
```

Configuration on S4

```
sysname S4
#
stp mode rstp
#
interface GE1/0/3
 stp instance 0 cost 50000
#
```

3.2.5 Quiz

1. Can the two links between S1 and S2 be in the forwarding state at the same time? Why?

No. The link between S1 and S2 will form a loop. Therefore, one link must be blocked.

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

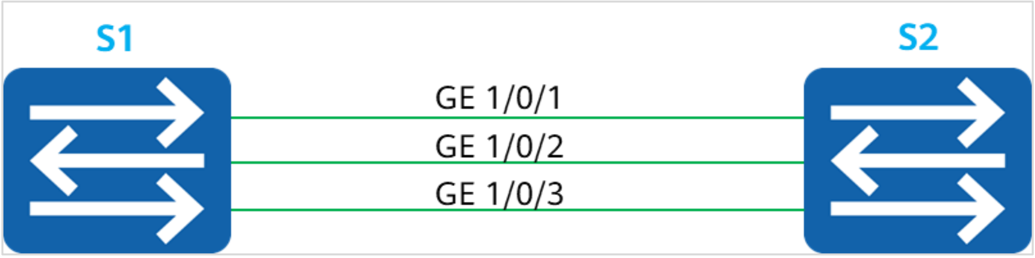


Figure 3-3 Lab topology for configuring Ethernet link aggregation

The device model used in this lab is ENSP-LSW.

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 GE 1/0/1
[S1-GE1/0/1] eth-trunk 1
[S1-GE1/0/1] quit
[S1] interface GE 1/0/2
[S1-GE1/0/2] eth-trunk 1
[S1-GE1/0/2] quit
[S1] interface GE 1/0/3
[S1-GE1/0/3] eth-trunk 1
[S1-GE1/0/3] 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 GE 1/0/1 to 1/0/3
```

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:
Working Mode: Normal              Hash Arithmetic: src-dst-ip
Least Active-linknumber: 1     Max Bandwidth-affected-linknumber: 128
Operating Status: up              Number of Up Ports in Trunk: 3
--------------------------------------------------------------------------------
PortName                          Status        Weight
GE1/0/1                           Up            1
GE1/0/2                           Up            1
GE1/0/3                           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 GE 1/0/1 to 1/0/3
[S1-Eth-Trunk1] quit
```

```
[S2] interface Eth-Trunk 1
[S2-Eth-Trunk1] undo trunkport GE 1/0/1 to 1/0/3
[S2-Eth-Trunk1] quit
```

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-static
```

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

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

# Add a port to the Eth-Trunk.

```
[S1] interface Eth-Trunk 1
[S1-Eth-Trunk1] trunkport GE 1/0/1 to 1/0/3
```

```
[S2] interface Eth-Trunk 1
[S2-Eth-Trunk1] trunkport GE 1/0/1 to 1/0/3
```

# Display the status of the Eth-Trunk.

```
[S1] display eth-trunk 1
Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                        Working Mode: Static
Preempt Delay: Disabled          Hash Arithmetic: src-dst-ip
System Priority: 32768           System ID: fa9f-1b6d-0011
Least Active-linknumber: 1       Max Active-linknumber: 128
Operating Status: up             Number Of Up Ports In Trunk: 3
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName             Status   PortType PortPri PortNo PortKey PortState Weight
GE1/0/1(hr)               Selected 1GE      32768   1      305     10111100  1
GE1/0/2(h)                Selected 1GE      32768   2      305     10111100  1
GE1/0/3(h)                Selected 1GE      32768   3      305     10111100  1

Partner:
--------------------------------------------------------------------------------
ActorPortName             SysPri   SystemID        PortPri PortNo PortKey PortState
GE1/0/1                   32768    fa9f-1b6d-0021  32768   1      305     10111100
GE1/0/2                   32768    fa9f-1b6d-0021  32768   2      305     10111100
GE1/0/3                   32768    fa9f-1b6d-0021  32768   3      305     10111100
```

Step 3 In normal cases, only GE1/0/1 and GE1/0/2 need to be in the forwarding state, and GE1/0/3 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
```

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 lower thresholds of active ports.

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

1. 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.
2. 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. The current simulator version does not support the configuration of the upper threshold for the number of active interfaces.

# Display the status of the current Eth-Trunk.

```
[S1] display eth-trunk 1
Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                         Working Mode: Static
Preempt Delay: Disabled           Hash Arithmetic: src-dst-ip
System Priority: 100            System ID: fa9f-1b6d-0011
Least Active-linknumber: 2        Max Active-linknumber: 128
Operating Status: up              Number Of Up Ports In Trunk: 3
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName                 Status    PortType PortPri PortNo PortKey PortState Weight
GE1/0/1(hr)                  Selected 1GE        32768     1        305        10111100    1
GE1/0/2(h)                   Selected 1GE        32768     2        305        10111100    1
GE1/0/3(h)                   Selected 1GE        40000     3        305        10111100    1

Partner:
--------------------------------------------------------------------------------
ActorPortName                 SysPri     SystemID           PortPri PortNo PortKey PortState
GE1/0/1                      32768      fa9f-1b6d-0021   32768     1        305        10111100
GE1/0/2                      32768      fa9f-1b6d-0021   32768     2        305        10111100
GE1/0/3                      32768      fa9f-1b6d-0021   32768     3        305        10111100
```

Eth-Trunk 1 is in the Up state.

# Shut down GE1/0/1 and GE1/0/2 to simulate a link fault.

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] shutdown
[S1-GE1/0/1] quit
[S1] interface GE 1/0/2
[S1-GE1/0/2] shutdown
```

```
[S1-GE1/0/2] quit
```

```
[S1] display eth-trunk 1
Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                          Working Mode: Static
Preempt Delay: Disabled            Hash Arithmetic: src-dst-ip
System Priority: 100               System ID: fa9f-1b6d-0011
Least Active-linknumber: 2         Max Active-linknumber: 128
Operating Status: down             Number Of Up Ports In Trunk: 0
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName                Status    PortType PortPri PortNo PortKey PortState Weight
GE1/0/1                      Unselect 1GE      32768    1      305     10100010   1
GE1/0/2                      Unselect 1GE      32768    2      305     10100010   1
GE1/0/3(hr)                  Unselect 1GE      40000    3      305     10100000   1

Partner:
------------------------------------------------------------------------------------
ActorPortName                SysPri    SystemID         PortPri PortNo PortKey PortState
GE1/0/1                      0         0000-0000-0000   0       0      0       10100011
GE1/0/2                      0         0000-0000-0000   0       0      0       10100011
GE1/0/3                      32768     fa9f-1b6d-0021   32768   3      305     10110000
```

The lower threshold for the number of active links is set to 2. Therefore, the Eth-Trunk is shut down. Although GE1/0/3 is Up, it is still in Unselect state.

Step 4 Change the load balancing mode.

# Enable the ports disabled in the previous step.

```
[S1] interface GE 1/0/1
[S1-GE1/0/1] undo shutdown
[S1-GE1/0/1] quit
[S1] interface GE 1/0/2
[S1-GE1/0/2] undo shutdown
[S1-GE1/0/2] quit
```

# 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
[S1-Eth-Trunk1] quit
```

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.

# Display the status of the current Eth-Trunk interface.

```
[S1] display eth-trunk 1
Eth-Trunk1's state information is:
(h): high priority
(r): reference port
Local:
LAG ID: 1                        Working Mode: Static
Preempt Delay: Disabled          Hash Arithmetic: dst-ip
System Priority: 100             System ID: fa9f-1b6d-0011
Least Active-linknumber: 2       Max Active-linknumber: 128
Operating Status: up             Number Of Up Ports In Trunk: 3
Timeout Period: Slow
PortKeyMode: Auto
--------------------------------------------------------------------------------
ActorPortName              Status    PortType PortPri PortNo PortKey PortState Weight
GE1/0/1(hr)                Selected 1GE       32768    1      305     10111100  1
GE1/0/2(h)                 Selected 1GE       32768    2      305     10111100  1
GE1/0/3(h)                 Selected 1GE       40000    3      305     10111100  1

Partner:
------------------------------------------------------------------------------------
ActorPortName              SysPri    SystemID       PortPri PortNo PortKey PortState
GE1/0/1                    32768     fa9f-1b6d-0021  32768   1       305     10111100
GE1/0/2                    32768     fa9f-1b6d-0021  32768   2       305     10111100
GE1/0/3                    32768     fa9f-1b6d-0021  32768   3       305     10111100
```

----End

3.3.3 Configuration Reference

Configuration on S1

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

```
interface GE1/0/3
 eth-trunk 1
#
```

Configuration on S2

```
sysname S2
#
interface Eth-Trunk1
 mode lacp-static
#
interface GE1/0/1
 eth-trunk 1
#
interface GE1/0/2
 eth-trunk 1
#
interface GE1/0/3
 eth-trunk 1
#
```

3.3.4 Quiz

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

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

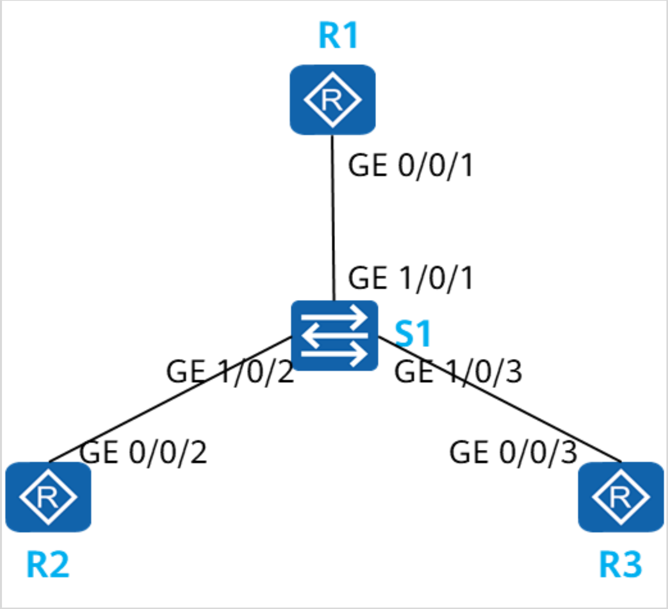


Figure 3-4 Lab topology for inter-VLAN communication

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.
4. In this lab, the switch is ENSP-LSW and the router is ENSP-AR.

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] interface GE 0/0/2
[R2-GE0/0/2] undo portswitch
[R2-GE0/0/2] ip address 192.168.2.1 24
[R2-GE0/0/2] 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] interface GE 0/0/3
[R3-GE0/0/3] undo portswitch
[R3-GE0/0/3] ip add 192.168.3.1 24
[R3-GE0/0/3] 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
[S1] interface GE 1/0/2
[S1-GE1/0/2] port link-type access
[S1-GE1/0/2] port default vlan 2
[S1-GE1/0/2] quit
[S1] interface GE 1/0/3
[S1-GE1/0/3] port link-type access
[S1-GE1/0/3] port default vlan 3
[S1-GE1/0/3] quit
```

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

# Configure a trunk port on S1.

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

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 GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] quit
[R1] interface GE 0/0/1.2
[R1-GE0/0/1.2] dot1q termination vid 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.

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

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

```
[R1] undo interface GE 0/0/1.2
[R1] undo interface GE 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 GE1/0/2
 port link-type access
 port default vlan 2
#
interface GE1/0/3
 port link-type access
 port default vlan 3
#
return
```

Configuration on R2

```
#
 sysname R2
#
interface GE0/0/2
 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 GE0/0/3
 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. As a Layer 3 interface, when will a VLANIF interface go Up?

If any physical interface that allows the VLAN to pass through goes Up, the corresponding VLANIF interface goes 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 10.0.12.1/24 and 10.0.12.2/24 respectively, and the IP addresses of the physical interfaces connecting R2 and R3 are 10.0.23.2/24 and 10.0.23.3/24, 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 10.0.1.1/24 and 10.1.1.1/24, respectively.

Configure an ACL so that R1's Loopback0 can ping R3's IP address and R1's Loopback1 cannot ping R3's IP address.

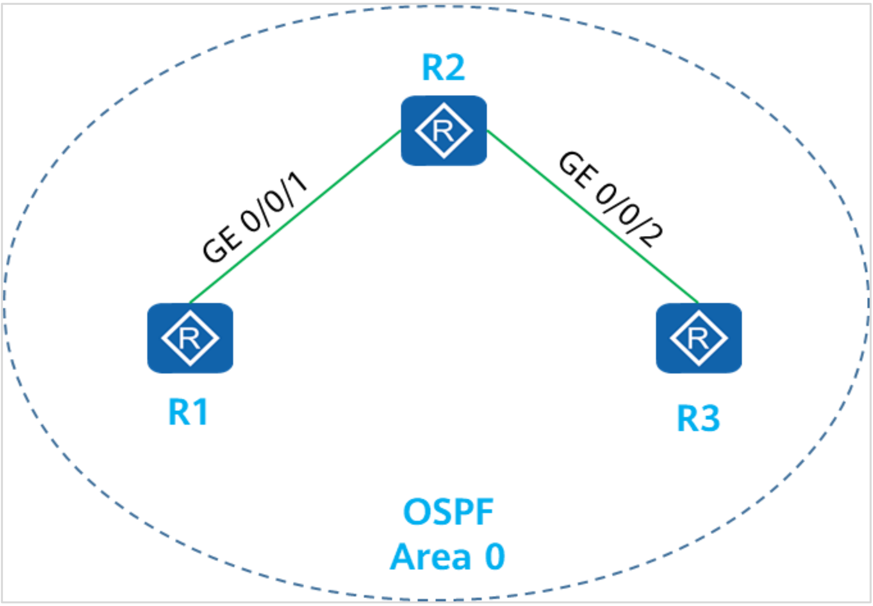


Figure 4-1 **Lab topology for ACL configuration**

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 GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ip address 10.0.12.1 24
[R1-GE0/0/1] quit
[R1] interface LoopBack 0
[R1-LoopBack0] ip address 10.0.1.1 32
[R1-LoopBack0] quit
[R1] interface LoopBack 1
[R1-LoopBack1] ip address 10.1.1.1 32
[R1-LoopBack1] quit
```

```
[R2] interface GE 0/0/1
[R2-GE0/0/1] undo portswitch
```

```
[R2-GE0/0/1] ip address 10.0.12.2 24
[R2-GE0/0/1] quit
[R2] interface GE 0/0/2
[R2-GE0/0/2] undo portswitch
[R2-GE0/0/2] ip address 10.0.23.2 24
[R2-GE0/0/2] quit
```

```
[R3] interface GE 0/0/2
[R3-GE0/0/2] undo portswitch
[R3-GE0/0/2] ip address 10.0.23.3 24
[R3-GE0/0/2] 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 1 router-id 10.0.1.1
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 10.0.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0] network 10.0.12.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0] return
```

```
[R2] ospf 1 router-id 10.0.2.2
[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] return
```

```
[R3] ospf 1 router-id 10.0.3.3
[R3-ospf-1] area 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] return
```

# Run the ping command on R1 to test network connectivity.

```
<R1> ping -a 10.0.1.1 10.0.23.3
  PING 10.0.23.3: 56   data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=254 time=32 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=254 time=18 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=254 time=20 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=254 time=20 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=254 time=25 ms
  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 18/23/32 ms

<R1> ping -a 10.1.1.1 10.0.23.3
  PING 10.0.23.3: 56   data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=254 time=24 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=254 time=21 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=254 time=19 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=254 time=21 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=254 time=19 ms

  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 19/20/24 ms
```

The two loopback interfaces of R1 can ping the interface address of R3.

Step 3 Configure an ACL to match desired traffic.

Configure an ACL on R2 to deny packets from 10.1.1.1.

# Configure an ACL on R2.

```
[R2] acl 3000
[R2-acl4-advance-3000] rule deny ip source 10.1.1.1 0.0.0.0
[R2-acl4-advance-3000] rule permit ip
[R2-acl4-advance-3000] quit
```

# Configuring a Traffic Policy Using MQC

```
[R2] traffic classifier test
[R2-classifier-test] if-match acl 3000
[R2-classifier-test] quit
[R2] traffic behavior test
[R2-behavior-test] permit
[R2-behavior-test] quit
[R2] traffic policy test
[R2-trafficpolicy-test] classifier test behavior test
[R2-trafficpolicy-test] quit
```

# Perform traffic filtering on R2's GE0/0/2.

```
[[R2] interface GE 0/0/2
[R2-GE0/0/2] traffic-policy test outbound
[R2-GE0/0/2] quit
```

# Run the ping command on R1 to check the network connectivity.

```
<R1> ping -a 10.1.1.1 10.0.23.3
```

```
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

<R1> ping -a 10.0.1.1 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=254 time=20 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=254 time=20 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=254 time=19 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=254 time=20 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=254 time=19 ms

  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 19/19/20 ms
```

The command output shows that 10.1.1.1 cannot ping R3.

----End

4.1.3 Configuration Reference

Configuration on R1

```
sysname R1
#
interface GE0/0/1
 ip address 10.0.12.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
interface LoopBack1
 ip address 10.1.1.1 255.255.255.255
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.1 0.0.0.0
  network 10.0.12.1 0.0.0.0
  network 10.1.1.1 0.0.0.0
#
```

Configuration on R2

```
sysname R2
#
acl number 3000
 rule 5 deny ip source 10.1.1.1 0
 rule 10 permit ip
#
traffic classifier test type or
 if-match acl 3000
#
traffic behavior test
#
traffic policy test
 classifier test behavior test precedence 5
#
interface GE0/0/1
 ip address 10.0.12.2 255.255.255.0
#
interface GE0/0/2
 ip address 10.0.23.2 255.255.255.0
 traffic-policy test outbound
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.12.2 0.0.0.0
  network 10.0.23.2 0.0.0.0
#
```

Configuration on R3

```
sysname R3
#
interface GE0/0/2
 ip address 10.0.23.3 255.255.255.0
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.23.3 0.0.0.0
#
```

4.1.4 Quiz

1. What other methods can be used to meet traffic filtering requirements?

Apply the traffic policy in the inbound direction of GE0/0/1 on R2.

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.

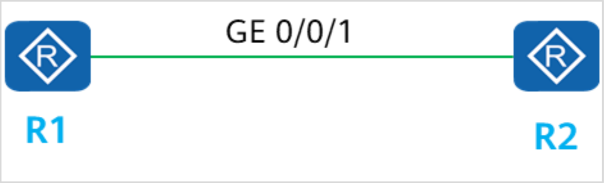


Figure 4-2 Lab topology for local AAA configuration

The device model used in this lab is ENSP-AR.

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 GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ip address 10.0.12.1 24
[R1-GE0/0/1] quit
```

```
[R2] interface GE 0/0/1
[R2-GE0/0/1] undo portswitch
[R2-GE0/0/1] ip address 10.0.12.2 24
[R2-GE0/0/1] quit
```

Step 2 Configure an AAA scheme.

# Configure authentication and authorization schemes.

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

Enter the AAA view.

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

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
```

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

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 irreversible-cipher Huawei@123
```

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
[R2-aaa] return
```

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> install feature-software WEAKEA
Info: Operating, please wait for a moment.....done.
Info: Succeeded in installing the software.
<R2> system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[R2] telnet server enable
Warning: TELNET is not a secure protocol, and it is recommended to use Stelnet.
[R2] telnet server-source all-interface
```

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
[R2-ui-vty0-4] protocol inbound telnet
```

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> install feature-software WEAKEA
Info: Operating, please wait for a moment.....done.
Info: Succeeded in installing the software.
<R1> telnet 10.0.12.2
Trying 10.0.12.2 ...
Press CTRL+K to abort
Connected to 10.0.12.2 ...
Warning: Telnet is not a secure protocol, and it is recommended to use Stelnet.
Username: hcia@datacom
Password: Huawei@123
Warning: The initial password poses security risks.The password needs to be changed, Continue? [Y/N] :y
Please enter old password:Huawei@123
Please enter new password:Huawei@1234
Please confirm new password:Huawei@1234
The password has been changed successfully.
Info: The max number of VTY users is 5, the number of current VTY users online is 1, and total number
of terminal users online is 2.
        The current login time is 20XX-XX-XX XX:XX:XX.
<R2>
```

By default, you must change the password upon the first login. After changing the password, you can log in to R2.

# Display the online users on R2.

```
[R2] display users
NOTE:
User-Intf: The absolute number and the relative number of user interface
Authen: Whether the authentication passes
Author: Command line authorization flag
-----------------------------------------------------------------------------
  User-Intf    Delay      Type    Network Address    Authen     Author    Username
-----------------------------------------------------------------------------
* 0     CON 0      00:00:00   --       0                        pass        no         Unspecified

  34   VTY 0     00:00:07   TEL      10.0.12.1              pass        no         hcia@datacom
```

----End

4.2.3 Configuration Reference

Configuration on R1

```
#
 sysname R1
#
interface GE0/0/1
 ip address 10.0.12.1 255.255.255.0
#
return
```

Configuration on R2

```
#
 sysname R2
#
telnet server enable
telnet server-source all-interface
#
aaa
  authentication-scheme datacom
  authentication-mode local
  authorization-scheme datacom
  authorization-mode local
 domain datacom
  authentication-scheme datacom
  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 GE0/0/1
 ip address 10.0.12.2 255.255.255.0
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound telnet
#
return
```

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.
4. The device model used in this lab is ENSP-AR.

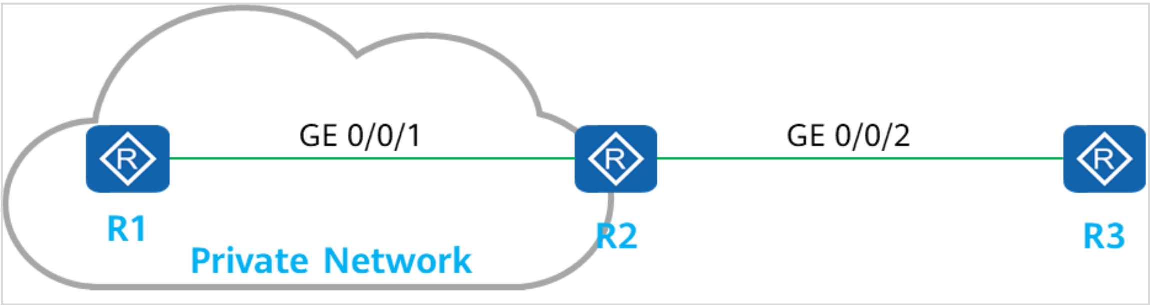


Figure 4-3 Lab topology for NAT configuration

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 GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ip address 192.168.1.1 24
[R1-GE0/0/1] quit
[R1] ip route-static 0.0.0.0 0 192.168.1.254
```

```
[R2] interface GE 0/0/1
[R2-GE0/0/1] undo portswitch
[R2-GE0/0/1] ip address 192.168.1.254 24
[R2-GE0/0/1] quit
[R2] interface GE 0/0/2
[R2-GE0/0/2] undo portswitch
[R2-GE0/0/2] ip address 100.0.23.2 24
[R2-GE0/0/2] quit
[R2] ip route-static 0.0.0.0 0 100.0.23.3
```

```
[R3] interface GE 0/0/2
[R3-GE0/0/2] undo portswitch
[R3-GE0/0/2] ip address 100.0.23.3 24
[R3-GE0/0/2] quit
```

# Configure the Telnet function on R1 for subsequent verification.

```
<R1> install feature-software WEAKEA
Info: Operating, please wait for a moment.....done.
Info: Succeeded in installing the software.
<R1> system-view
[R1] telnet server enable
[R1] telnet server-source all-interface
[R1] aaa
[R1-aaa] local-user hcia-datacom password irreversible-cipher Huawei@123
[R1-aaa] local-user hcia-datacom service-type telnet
[R1-aaa] local-user hcia-datacom privilege level 3
[R1-aaa] quit
[R1] user-interface vty 0 4
[R1-ui-vty0-4] authentication-mode aaa
[R1-ui-vty0-4] protocol inbound telnet
[R1-ui-vty0-4] quit
```

Step 2 The enterprise obtains the public IP addresses ranging from 100.1.23.1 to 100.1.23.254 and needs the dynamic NAT function.

# Configure a NAT address pool.

```
[R2] nat address-group test 1
[R2-address-group-test] section 1 100.1.23.1 100.1.23.254
[R2-address-group-test] mode pat
[R2-address-group-test] quit
```

The **nat address-group** command configures a NAT address pool.

The **section** command configures an address segment.

The **mode pat** command set the address pool mode to PAT. By default, the application mode of an address pool is NAPT.

# Configuring NAT Policies.

```
[R2] nat-policy
[R2-policy-nat] rule name test
[R2-policy-nat-rule-test] source-address range 192.168.1.1 192.168.1.254
[R2-policy-nat-rule-test] action source-nat address-group test
[R2-policy-nat-rule-test] quit
[R2-policy-nat] quit
```

Using the **source-address range** command, you can configure the matching conditions of a NAT rule.

Using the **action** command, you can configure the action of a NAT rule. s**ource-nat** indicates that the source IP address of the data flow is translated.

# Configure dynamic NAT on GE0/0/2 of R2.

```
[R2] interface GE 0/0/2
[R2-GE0/0/2] nat enable
```

```
[R2-GE0/0/2] quit
```

# Configure a static route to the NAT address pool on R3.

```
[R3] ip route-static 100.1.23.0 24 100.0.23.2
```

# Test connectivity.

```
<R1> ping 100.0.23.3
  PING 100.0.23.3: 56   data bytes, press CTRL_C to break
    Reply from 100.0.23.3: bytes=56 Sequence=1 ttl=254 time=44 ms
    Reply from 100.0.23.3: bytes=56 Sequence=2 ttl=254 time=17 ms
    Reply from 100.0.23.3: bytes=56 Sequence=3 ttl=254 time=23 ms
    Reply from 100.0.23.3: bytes=56 Sequence=4 ttl=254 time=23 ms
    Reply from 100.0.23.3: bytes=56 Sequence=5 ttl=254 time=21 ms

  --- 100.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 17/25/44 ms
```

# Display the NAT session table on R2.

```
[R2] display session all verbose
  Session Table Information:
    Protocol              : 1 (ICMP)
    SrcAddr VPN            : 192.168.1.1
    DestAddr VPN           : 100.0.23.3
    Type Code IcmpId      : 8 0 1024
    Time To Live          : 8 s
    NAT Info
      New SrcAddr          : 100.1.23.9
      New DestAddr          : -
      New IcmpId           : 2049

  Total : 1
```

The address of R1 is translated to 100.1 .23.9.

Step 3 Configuring Easy IP.

# Modify the NAT policy and set the NAT action to Easy IP.

```
[R2] nat-policy
[R2-policy-nat] rule name test
[R2-policy-nat-rule-test] action source-nat easy-ip
[R2-policy-nat-rule-test] quit
[R2-policy-nat] quit
```

# Test connectivity.

```
<R1> ping 100.0.23.3
  PING 100.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 100.0.23.3: bytes=56 Sequence=1 ttl=254 time=20 ms
    Reply from 100.0.23.3: bytes=56 Sequence=2 ttl=254 time=20 ms
    Reply from 100.0.23.3: bytes=56 Sequence=3 ttl=254 time=22 ms
    Reply from 100.0.23.3: bytes=56 Sequence=4 ttl=254 time=20 ms
    Reply from 100.0.23.3: bytes=56 Sequence=5 ttl=254 time=18 ms

  --- 100.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 18/20/22 ms
```

# Check the NAT session table.

```
[R2] display session all verbose
  Session Table Information:
    Protocol              : 1 (ICMP)
    SrcAddr VPN             : 192.168.1.1
    DestAddr VPN            : 100.0.23.3
    Type Code IcmpId      : 8 0 9216
    Time To Live          : 17 s
    NAT Info
      New SrcAddr           : 100.0.23.2
      New DestAddr          : -
      New IcmpId            : 2049

  Total : 1
```

The source address of R1 is translated to 100.0.23.2.

Step 4 R1 needs to provide network services (telnet in this example) for users on the public network. Because R1 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] nat server for_telnet protocol tcp global 100.0.23.2 telnet 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.

# Telnet R1 from R3.

```
<R3> install feature-software WEAKEA
<R3> telnet 100.0.23.2
Trying 100.0.23.2 ...
Press CTRL+K to abort
```

```
Connected to 100.0.23.2 ...
Warning: Telnet is not a secure protocol, and it is recommended to use Stelnet.

Username:hcia-datacom
Password:Huawei@123
Warning: The initial password poses security risks.The password needs to be changed, Continue? [Y/N] :y
Please enter old password:Huawei@123
Please enter new password:Huawei@1234
Please confirm new password:Huawei@1234
The password has been changed successfully.
Info: The max number of VTY users is 5, the number of current VTY users online is 1, and total number
of terminal users online is 2.
      The current login time is 20XX-XX-XX XX:XX:XX.
<R1>
```

# Display the NAT session table on R2.

```
<R2> display session all verbose
  Session Table Information:
    Protocol              : 6 (TCP)
    SrcAddr Port VPN      : 100.0.23.3 57112
    DestAddr Port VPN     : 100.0.23.2 23
    Time To Live          : 600 s
    NAT Info
      New SrcAddr         : -
      New SrcPort         : -
      New DestAddr        : 192.168.1.1
      New DestPort        : 23

  Total : 1
```

----End

4.3.3 Configuration Reference

Configuration on R1

```
sysname R1
#
telnet server enable
telnet server-source all-interface
#
aaa
 local-user hcia-datacom password irreversible-cipher $1d$cSoFN-}:N5g$v}3V$$fR=U8kfW$$.>
09`!rM.n&,`04@kgPs<~\H1<C+2$
 local-user hcia-datacom privilege level 3
 local-user hcia-datacom service-type telnet
#
interface GE0/0/1
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
user-interface vty 0 4
```

```
 authentication-mode aaa
 protocol inbound telnet
#
```

Configuration on R2

```
sysname R2
#
interface GE0/0/1
 ip address 192.168.1.254 255.255.255.0
#
interface GE0/0/2
 ip address 100.0.23.2 255.255.255.0
 nat enable
#
ip route-static 0.0.0.0 0.0.0.0 100.0.23.3
#
nat address-group test 1
 mode pat
 section 1 100.1.23.1 100.1.23.254
#
nat server for_telnet protocol tcp global 100.0.23.2 telnet inside 192.168.1.1 telnet
#
nat-policy
 rule name test
  source-address range 192.168.1.1 192.168.1.254
  action source-nat easy-ip
#
```

Configuration on R3

```
sysname R3
#
interface GE0/0/2
 ip address 100.0.23.3 255.255.255.0
#
ip route-static 100.1.23.0 255.255.255.0 100.0.23.2
```

4.3.4 Quiz

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

Not required.

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

1. R1 needs to manage the configuration file of R2.
2. R1 functions as the FTP client, and R2 functions as the FTP server.

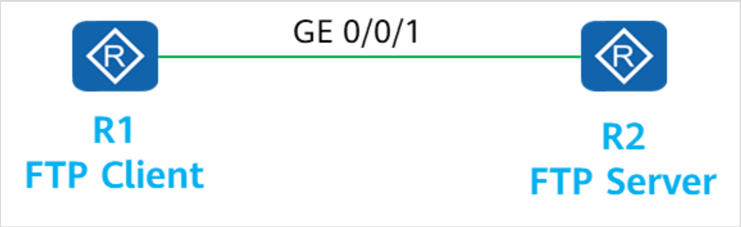


Figure 5-1 Lab topology for FTP configuration

The device model used in this lab is ENSP-AR.

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 GE 0/0/1
[R1-GE0/0/1] undo portswitch
[R1-GE0/0/1] ip address 10.0.12.1 24
[R1-GE0/0/1] quit
[R1] quit
```

```
[R2] interface GE 0/0/1
[R2-GE0/0/1] undo portswitch
[R2-GE0/0/1] ip address 10.0.12.2 24
[R2-GE0/0/1] quit
[R2] quit
```

# Save the configuration file for subsequent verification.

```
<R1> save test1.cfg
Warning: Are you sure to save the configuration to flash:/test1.cfg? [Y/N] :y
Now saving the current configuration to the slot 0 .
```

```
<R2> save test2.cfg
Warning: Are you sure to save the configuration to flash:/test1.cfg? [Y/N] :y
Now saving the current configuration to the slot 0 .
```

# Display the current file list.

```
<R1> dir | include test1.cfg
  Idx  Attr       Size(Byte)    Date          Time                  FileName
    19   -rw-             4,808    XX XX    20XX XX:XX:XX              test1.cfg
```

```
<R2> dir | include test2.cfg
  Idx   Attr       Size(Byte)     Date           Time                  FileName
    19   -rw-               4,808    XX XX    20XX XX:XX:XX                test2.cfg
```

The configuration files of the two devices are saved successfully.

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

```
<R2> install feature-software WEAKEA
<R2> system-view
[R2] ftp server enable
[R2] ftp server source all-interface
Warning: FTP server source configuration will take effect in the next login. Continue? [Y/N] :y
Warning: It expands the range of accessed IP.
```

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

The **ftp server source all-interface** command specifies the source interface of the FTP server.

Step 3 Configure local FTP users.

```
[R2] aaa
[R2-aaa] local-user ftp-client password irreversible-cipher Huawei@123
[R2-aaa] local-user ftp-client service-type ftp
[R2-aaa] local-user ftp-client privilege level 3
```

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> install feature-software WEAKEA
<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. Warning: FTP is not secure. Using SFTP is recommended.
User(10.0.12.2:(none)):ftp-client
331 Password required for ftp-client.
Enter password:Huawei@123
230 User logged in.
[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.

```
[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.

```
[ftp] get test2.cfg
Warning: The file may not transfer correctly in ASCII mode.
213 4808
200 Port command okay.
150 Opening ASCII mode data connection for /test2.cfg.
/        100% [***********]
226 Transfer complete.

FTP: 4808 byte(s) received in 0.268 second(s) 17.518Kbyte(s)/sec.
```

# Delete the configuration file.

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

# Upload the configuration file.

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

FTP: 4808 byte(s) send in 0.123 second(s) 38.170Kbyte(s)/sec.
```

# Close the FTP connection.

```
[ftp] bye
221 Server closing.
<R1>
```

----End

5.1.3 Verification

Display the file directories of R1 and R2.

```
<R1> dir | include test2.cfg
  Idx   Attr        Size(Byte)   Date            Time          FileName
    20   -rw-              4,808    XX XX 20XX XX:XX:XX     test2.cfg
```

R1 has the configuration file of R2.

```
<R2> dir | include test2.cfg
  Idx   Attr        Size(Byte)   Date            Time          FileName

<R2> dir | include test1.cfg
  Idx   Attr        Size(Byte)   Date            Time          FileName
    19   -rw-              4,808    XX XX 20XX XX:XX:XX     test1.cfg
```

R2 does not have the original configuration file and has obtained the configuration file of R1.

5.1.4 Configuration Reference

Configuration on R1

```
#
 sysname R1
#
interface GE0/0/1
 ip address 10.0.12.1 255.255.255.0
#
```

Configuration on R2

```
sysname R2
#
ftp server enable
ftp server source all-interface
aaa
 local-user ftp-client password irreversible-cipher $1d$&Q3NX<NbKQn]
_++Q$9k] > )AZaq3{Q@2.[lM4PXN#`:-ge%8d.n^BYqcu/$
 local-user ftp-client privilege level 3
 local-user ftp-client ftp-directory flash:
 local-user ftp-client service-type ftp
#
interface GE0/0/1
 ip address 10.0.12.2 255.255.255.0
#
```

5.1.5 Quiz

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

Active mode

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.

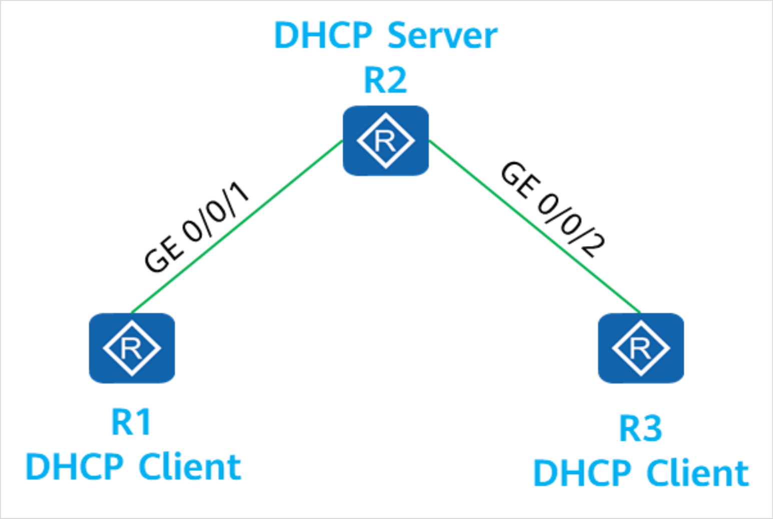


Figure 5-2 **Lab topology for DHCP configuration**

The device model used in this lab is ENSP-AR.

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 Switch the interfaces of R1 and R3 to Layer 3 interfaces.

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

```
[R3] interface GE 0/0/2
[R3-GE0/0/2] undo portswitch
[R3-GE0/0/2] quit
```

Step 2 Complete basic configurations.

# Configure interface addresses on R2.

```
[R2] interface GE 0/0/1
[R2-GE0/0/1] undo portswitch
[R2-GE0/0/1] ip address 10.0.12.2 24
[R2-GE0/0/1] quit
```

```
[R2] interface GE 0/0/2
[R2-GE0/0/2] undo portswitch
[R2-GE0/0/2] ip address 10.0.23.2 24
[R2-GE0/0/2] quit
```

Step 3 Enable DHCP.

```
[R2] dhcp enable
```

Step 4 Configure an address pool.

# Configure an IP address pool on GE 0/0/1 of R2 to assign an IP address to R1.

```
[R2] interface GE 0/0/1
[R2-GE0/0/1] 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-GE0/0/1] dhcp server dns-list 10.0.12.2
[R2-GE0/0/1] quit
```

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: Change 'GlobalPool' to 'globalpool' automatically. The parameter is not case-sensitive.
```

# 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 faf1-18ef-0032
```

The **static-bind** command binds an IP address in a global address pool to a MAC address of a client. faf1-18ef-0032 is the MAC address of GE0/0/2 on R3. You can run the **display interface GE0/0/2** command on R3 to display the MAC address of GE0/0/2. After the command is executed, R3 obtains the fixed IP address of 10.0.23.3.

Step 5 Enable the DHCP server function on GE0/0/2 of R2 to assign an IP address to R3.

```
[R2] interface GE 0/0/2
[R2-GE0/0/2] dhcp select global
[R2-GE0/0/2] quit
```

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 6 Configure a DHCP client.

```
[R1] interface GE 0/0/1
[R1-GE0/0/1] ip address dhcp-alloc
[R1-GE0/0/1] quit
```

```
[R3] interface GE 0/0/2
[R3-GE0/0/2] ip address dhcp-alloc
[R3-GE0/0/2] quit
```

----End

5.2.3 Verification

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

```
<R1> display ip interface brief | include 10.0.12
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(ed): error down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 0
Interface                          IP Address/Mask      Physical Protocol VPN
GE0/0/1                              10.0.12.231/24        up           up           --
```

The command output shows that R1 has obtained the IP address.

```
[R1] display ip routing-table
Proto: Protocol             Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
           Destinations : 8           Routes : 8

Destination/Mask      Proto     Pre   Cost            Flags NextHop             Interface

          0.0.0.0/0     OPR        60     0                    D     10.0.12.2           GE0/0/1
```

The command output shows that R1 has obtained the default route.

```
[R3] display ip interface brief
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(ed): error down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 0
Interface                          IP Address/Mask      Physical Protocol VPN
GE0/0/2                              10.0.23.3/24          up           up           --
```

The command output shows that R3 has obtained a fixed IP address.

```
[R3] display ip routing-table
Proto: Protocol             Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
           Destinations : 8           Routes : 8

Destination/Mask      Proto     Pre   Cost            Flags NextHop             Interface

          0.0.0.0/0     OPR        60     0                    D     10.0.23.2           GE0/0/2
```

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              : 2
  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
  Network              : 10.0.23.0
  Mask                 : 255.255.255.0
  VPN instance         : --
  Logging              : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total       :253        Used        :1
                     Idle        :252        Expired     :0
                     Conflict    :0          Disabled    :0


 ---------------------------------------------------------------------------------
  Network section
         Start              End          Total     Used Idle(Expired) Conflict Disabled
 ---------------------------------------------------------------------------------
        10.0.23.1       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 GE0/0/1

  Pool-name            : GE0/0/1
  Pool-No              : 1
  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            : -
  Network              : 10.0.12.0
  Mask                 : 255.255.255.0
  VPN instance         : --
  Logging              : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total       :254        Used        :1
                     Idle        :253        Expired     :0
                     Conflict    :0          Disabled    :0
```

```
 -------------------------------------------------------------------------------------
  Network section
         Start              End         Total      Used Idle(Expired) Conflict Disabled
 -------------------------------------------------------------------------------------
        10.0.12.1       10.0.12.254      254          1          253(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
#
interface GE0/0/1
 ip address dhcp-alloc
#
```

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 faf1-18ef-0032
 lease day 2 hour 2 minute 0
 dns-list 10.0.23.2
#
interface GE0/0/1
 ip address 10.0.12.2 255.255.255.0
 dhcp select interface
 dhcp server dns-list 10.0.12.2
#
interface GE0/0/2
 ip address 10.0.23.2 255.255.255.0
 dhcp select global
#
```

Configuration on R3

```
sysname R3
#
interface GE0/0/2
 ip address dhcp-alloc
#
```

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?

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. If there are multiple global address pools, how do you determine the global address pool for a DHCP client?

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.

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

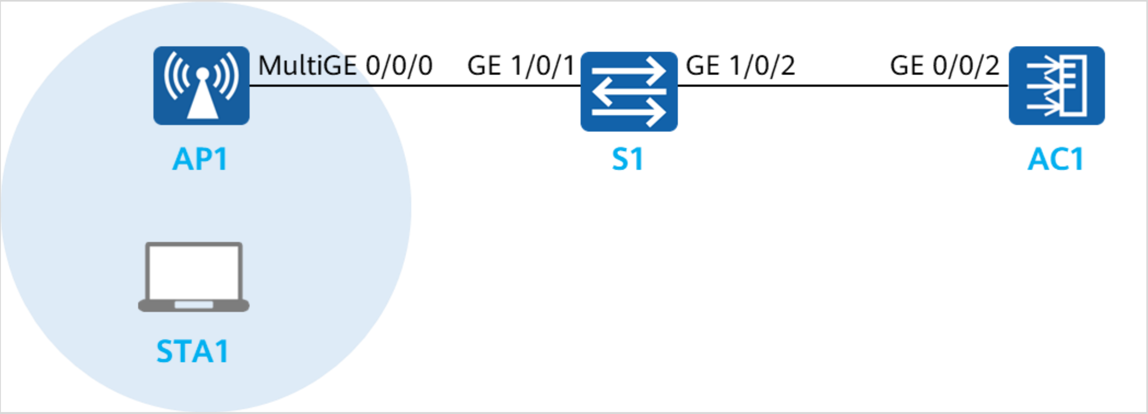


Figure 6-1 Lab topology for creating a WLAN

The device models used in this lab are ENSP-AP, ENSP-LSW, ENSP-AC, and STA.

6.1.4 Data Planning

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.
	The AC functions as a DHCP server to allocate IP addresses to STAs.
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
Regulatory domain profile	Name: default
	Country code: CN
SSID profile	Name: HCIA-WLAN
	SSID name: HCIA-WLAN
Security profile	Name: HCIA-WLAN
	Security policy: OPEN
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. 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.
4. 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

The details are not provided here.

Step 2 Configure the APs to bring them online.

# Configuring S1

```
[S1] vlan 100
[S1-vlan100] quit
[S1] vlan 101
[S1-vlan101] quit
[S1] interface GE 1/0/1
[S1-GE1/0/1] port link-type trunk
[S1-GE1/0/1] port trunk pvid vlan 100
[S1-GE1/0/1] port trunk allow-pass vlan 100 101
[S1-GE1/0/1] quit
[S1] interface GE 1/0/2
[S1-GE1/0/2] port link-type trunk
[S1-GE1/0/2] port trunk allow-pass vlan 100 101
[S1-GE1/0/2] quit
```

Create VLAN 100 and VLAN 101 on S1 for APs and STAs to go online.

# Enable the DHCP function on AC1 and configure the gateway for the AP and STA to go online.

```
[AC1] dhcp enable
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] vlan 101
[AC1-vlan101] quit
[AC1] interface GE 0/0/2
[AC1-GE0/0/2] port link-type trunk
```

```
[AC1-GE0/0/2] port trunk allow-pass vlan 100 101
[AC1-GE0/0/2] quit
[AC1] interface Vlanif 100
[AC1-Vlanif100] ip address 192.168.100.254 24
[AC1-Vlanif100] dhcp select interface
[AC1-Vlanif100] dhcp server option 43 sub-option 2 ip-address 192.168.100.254
[AC1-Vlanif100] quit
[AC1] interface Vlanif 101
[AC1-Vlanif101] ip address 192.168.101.254 24
[AC1-Vlanif101] dhcp select interface
[AC1-Vlanif101] quit
```

# Create an AP group and name it ap-group1.

```
[AC1] wlan
[AC1-wlan] ap-group name ap-group1
[AC1-wlan-ap-group-ap-group1] quit
```

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

```
[AC1] wlan
[AC1-wlan] 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.

```
[AC1-wlan-regulate-domain-default] country-code CN
```

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.

```
[AC1-wlan-regulate-domain-default] quit
```

# Bind the regulatory domain profile to an AP group.

```
[AC1] wlan
[AC1-wlan] ap-group name ap-group1
[AC1-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.

```
[AC1] capwap source interface Vlanif 100
Set the DTLS PSK(contains 8-32 plain-text characters, or 128 or 148 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):Huawei@123
Confirm PSK:Huawei@123
Info: Deliver DTLS PSK to devices using CAPWAP connections. It may take a few minutes.
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters, underscores, and digits, and must start with a letter):admin
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 128-268 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):Huawei@123
Confirm password:Huawei@123
Set the PSK of the global offline management VAP(plain-text password of 8-63 characters or cipher-text password of 128-188 characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):Huawei@123
Confirm PSK:Huawei@123
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be interrupted.
Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.
[AC1] capwap dtls no-auth enable
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is enabled and brings security risks. After the device goes online for the first time, disable this function to prevent security risks. Continue? [Y/N] :y
```

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

Configure the PSK for CAPWAP DTLS encryption as prompted. Configure the user name and password for logging in to the Fit AP. The password for accessing the global offline management VAP is configured. The password is used to wirelessly connect to the offline management SSID of the Fit AP.

The **capwap dtls no-auth enable** command allows CAPWAP DTLS sessions to use the non-authentication mode. If CAPWAP control tunnel encryption using DTLS has been enabled and an AP running a version earlier than V200R021C00 is connected to the AC, enable CAPWAP control tunnel encryption using DTLS in non-authentication mode so that the AP can go online. After the AP goes online, it obtains a new DTLS certificate and starts a DTLS session and goes online again in secure mode. To ensure network security, disable this function immediately after the AP goes online again to prevent unauthorized APs from accessing the network.

# 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:

1. 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.
2. 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.
3. 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.

```
[AC1] wlan
[AC1-wlan] 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.

In this lab, you can run the **display ap all** command to view the MAC address of AP1. The AP is in the unauth state.

```
[AC1-wlan] display ap all
Total AP information:
unauth: unauthed              [1]
ExtraInfo : Extra information
Total: 1
--------------------------------------------------------------------------------------
ID      MAC                    Name Group IP Type                    State   STA   Uptime ExtraInfo
--------------------------------------------------------------------------------------
-       fa12-a6ae-0020 -      -       -   AirEngine5773-21      unauth -      -         -
--------------------------------------------------------------------------------------
```

```
[AC1-wlan] ap-id 0 ap-mac fa12-a6ae-0020
```

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.

```
[AC1-wlan-ap-0] ap-name AP1
Warning: The AP name cannot be the MAC address of another AP. Otherwise, the AP name may be lost
after the device restarts.
Warning: This operation may cause AP reset. Continue? [Y/N] :Y
```

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.

```
[AC1-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
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC1-wlan-ap-0] quit
```

# Display the information about the current AP.

```
[AC1-wlan] display ap all
Total AP information:
nor     : normal              [1]
ExtraInfo : Extra information
Total: 1
----------------------------------------------------------------------------------------------------
ID      MAC                  Name Group       IP                    Type                  State   STA   Uptime
ExtraInfo
----------------------------------------------------------------------------------------------------
0       fa12-a6ae-0020 AP1   ap-group1 192.168.100.199 AirEngine5773-21 nor      0      22S      -
----------------------------------------------------------------------------------------------------
```

The **display ap** command displays AP information, including the IP address, model (AirEngine5773-21), 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 3 Configure WLAN service parameters.

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

```
[AC1-wlan] security-profile name HCIA-WLAN
[AC1-wlan-sec-prof-HCIA-WLAN] security open
Warning: The Open encryption algorithm is insecure. For security-sensitive scenarios, WPA2 is
recommended.
[AC1-wlan-sec-prof-HCIA-WLAN] quit
```

The **security open** command configures open system authentication.

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

```
[AC1-wlan] ssid-profile name HCIA-WLAN
```

SSID profile **HCIA-WLAN** is created.

```
[AC1-wlan-ssid-prof-HCIA-WLAN] ssid HCIA-WLAN
[AC1-wlan-ssid-prof-HCIA-WLAN] quit
```

The SSID name is set to **HCIA-WLAN**.

# 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.

```
[AC1-wlan] 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.

```
[AC1-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.

```
[AC1-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.

```
[AC1-wlan-vap-prof-HCIA-WLAN] security-profile HCIA-WLAN
```

Security profile **HCIA-WLAN** is bound.

```
[AC1-wlan-vap-prof-HCIA-WLAN] ssid-profile HCIA-WLAN
[AC1-wlan-vap-prof-HCIA-WLAN] quit
```

SSID profile **HCIA-WLAN** is bound.

# 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.

```
[AC1-wlan] ap-group name ap-group1
[AC1-wlan-ap-group-ap-group1] radio 0
[AC1-wlan-ap-group-ap-group1-radio-0] calibrate auto-channel-select disable
Info: This operation will recover the redundant radio.
[AC1-wlan-ap-group-ap-group1-radio-0] channel 20mhz 1
Warning: This action may cause service interruption. Continue? [Y/N] :y
```

```
Info: The channel value and bandwidth value take effect only when automatic channel selection is
disabled, and the value depends on the AP specifications and local laws and regulations.
[AC1-wlan-ap-group-ap-group1-radio-0] vap-profile HCIA-WLAN wlan 1
[AC1-wlan-ap-group-ap-group1-radio-0] quit
[AC1-wlan-ap-group-ap-group1] quit
[AC1-wlan] quit
```

radio *radio-id:* The radio view is displayed.

The **calibrate auto-channel-select** {**enable** | **disable**} command enables or disables automatic channel selection. By default, automatic channel selection is enabled in the AP group radio view. By default, automatic channel selection is not configured in the AP radio view.

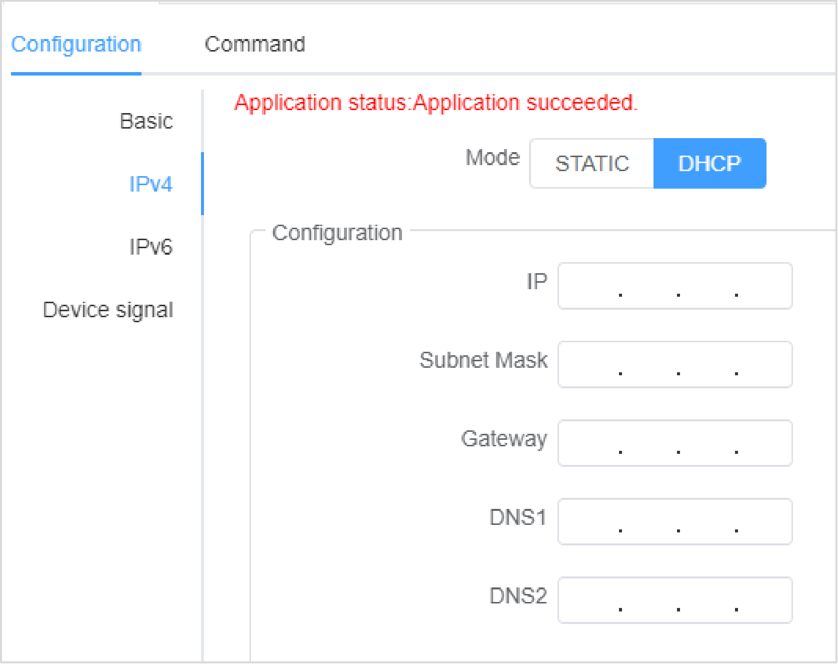
channel {**20mhz** | **40mhz-minus** | **40mhz-plus**} *channel* configures the working bandwidth and channel of a specified radio.

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.

----End

6.3 Verification

1. Configure the STA. Double-click the STA that has started successfully. In the displayed dialog box, click **IPv4** and select **DHCP**.



Application status:Application succeeded.

Mode STATIC DHCP

Configuration

IP . . .

Subnet Mask . . .

Gateway . . .

DNS1 . . .

DNS2 . . .

2. Connect STA1 to the AP.

# The **display vap** command displays information about service VAPs.

```
[AC1] display vap all
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
Total: 1
----------------------------------------------------------------------------
AP ID AP name   RfID WID   BSSID            Status   Auth type   STA    SSID
----------------------------------------------------------------------------
0       AP1       0     1     FA12-A6AE-0020 ON        Open          0        HCIA-WLAN
----------------------------------------------------------------------------
```

Status: Current status of a VAP. **ON**: The VAP service is enabled.

Auth type: Authentication mode of a VAP.

STA: Number of STAs connected to a VAP.

SSID: SSID name.

# Drag STA1 to the wireless signal range of AP1. Double-click STA1 and run the following command to connect STA1 to AP1:

```
Welcome to use PC Simulators!
PC> wnmcli device wifi list --rescan yes
SSID                   Status
HCIA-WLAN                down
```

```
PC> wnmcli device wifi connect HCIA-WLAN
Connect is done
```

The **wnmcli device wifi list --rescan yes** command is used to list wireless signals.

The **wnmcli device wifi connect XX** command is used to connect to a specific wireless signal.

Note: You can run the **wnmcli -h** command to view the help information.

```
PC> wnmcli -h
 Usage:
 wnmcli device {wifi | disconnect} <required argument> [optional option]

  wnmcli device wifi list --rescan yes [--timeout <sec> ]     List of AP with forcing wi-fi scan.
  wnmcli device wifi list                                      List of AP without wi-fi scan.
  wnmcli device wifi connect <ssid> [--timeout <sec> ]          Connect to a Wi-Fi network by SSID.
  wnmcli device disconnect <ssid>                             Disconnect from a Wi-Fi network by SSID.

    -r, --rescan       forcing wi-fi scan
    -t, --timeout      timeout to receive feedback on the successful execution of the command

 Usage sample:
  wnmcli device wifi list -r yes
  wnmcli device wifi connect HUAWEI-WLAN
  wnmcli device wifi list
  wnmcli device disconnect HUAWEI-WLAN
```

3. When the STA is connected to the AC, run the **display station all** command on the AC to check the STA information.

```
[AC1] display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
Total: 1 2.4G: 1 5G: 0
-----------------------------------------------------------------------------------------------------
STA MAC            AP ID Ap name   Rf/WLAN   Band   Type    VLAN   IP address        SSID
-----------------------------------------------------------------------------------------------------
96f3-91f5-cb96      0      AP1        0/1        2.4G      11g      101    192.168.101.196   HCIA-WLAN
-----------------------------------------------------------------------------------------------------
```

Note: Non-key information is omitted in the preceding command output.

4. Ping the IP address of the terminal on the AC.

```
[AC1] ping 192.168.101.196
  PING 192.168.101.196: 56   data bytes, press CTRL_C to break
    Reply from 192.168.101.196: bytes=56 Sequence=1 ttl=64 time=43 ms
    Reply from 192.168.101.196: bytes=56 Sequence=2 ttl=64 time=45 ms
    Reply from 192.168.101.196: bytes=56 Sequence=3 ttl=64 time=38 ms
    Reply from 192.168.101.196: bytes=56 Sequence=4 ttl=64 time=30 ms
    Reply from 192.168.101.196: bytes=56 Sequence=5 ttl=64 time=72 ms

  --- 192.168.101.196 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 30/45/72 ms
```

6.4 Configuration Reference

Configuration on S1

```
sysname S1
#
vlan batch 100 to 101
#
interface GE1/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
```

```
#
```

Configuration on AC1

```
sysname AC1
#
wlan
 temporary-management psk %+%##!!!!!!!!!"!!!!"!!!!*!!!!`E[J&bZ0D+f{HN*"!wEJ8Uf8Pqyi>
=XcgYV!!!!!2jp5!!!!!!;!!!!p@d7Sz5f2> ^=n2<tlW0R-R4#:|}UiFK.r3+!!!!!%+%#
 ap username admin password
cipher %+%##!!!!!!!!!"!!!!"!!!!*!!!!`E[J&bZ0D+VD|JV<Y2"<{{`\G=%3H:|x^*K!!!!!2jp5!!!!!!;!!!!9\(@7r0}\Aw1QA<]
b/*SqWbMI3DYS9wkvN+!!!!!%+%#
 traffic-profile name default
 security-profile name default
 security-profile name HCIA-WLAN
  security open
 ssid-profile name default
 ssid-profile name HCIA-WLAN
  ssid HCIA-WLAN
 vap-profile name default
 vap-profile name HCIA-WLAN
  ssid-profile HCIA-WLAN
  security-profile HCIA-WLAN
  service-vlan vlan-id 101
 regulatory-domain-profile name default
 air-scan-profile name default
 rrm-profile name default
 radio-2g-profile name default
 radio-5g-profile name default
 ap-system-profile name default
 port-link-profile name default
 wired-port-profile name default
 ap-group name default
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
   channel 20mhz 1
   calibrate auto-channel-select disable
 ap-id 0 type-id 220 ap-mac fa12-a6ae-0020 ap-sn 21500868341234500042
  ap-name AP1
  ap-group ap-group1
#
dhcp enable
#
vlan batch 100 to 101
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select interface
 dhcp server option 43 sub-option 2 ip-address 192.168.100.254
#
interface Vlanif101
 ip address 192.168.101.254 255.255.255.0
 dhcp select interface
#
```

```
interface GE0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
```

6.5 Quiz

1. In the current networking, if GE0/0/2 of AC1 does not allow packets from VLAN 101 to pass through, what is the impact on the access of STAs to S1?

STA1 cannot access the gateway because data frames sent by the AP carry tag 101 in direct forwarding mode.

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.
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 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 a static IPv6 address for GE0/0/1 on R1.
3. Configure an IPv6 address for GE0/0/2 of R3 using DHCPv6.

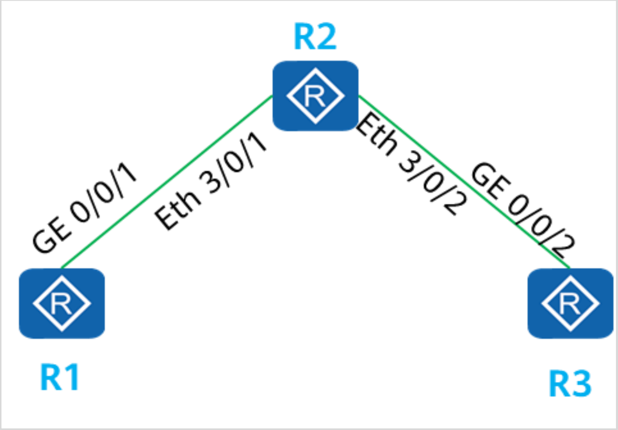


Figure 7-1 Lab topology for creating an IPv6 network

The device model of R1 and R3 is ENSP-AR, and the device model of R2 is ENSP-NE.

7.2 Lab Configuration

7.2.1 Configuration Roadmap

1. Configure static IPv6 addresses.
2. Configure DHCPv6.
3. 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 interfaces.

# Enable IPv6 on the interface.

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

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

```
[R2] display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 8.221 (NE40E-X16 V800R022C10SPC100B315)
Copyright (C) 2012-2022 Huawei Technologies Co., Ltd.
```

```
HUAWEI NE40E-X16 uptime is 0 day, 0 hour, 4 minutes
SVRP Platform Version 1.0
```

The operating system of R2 is VRP8. Therefore, the configuration commands of R2 are different from those of ENSP-AR.

```
<R2> system-view immediately
Enter system view, return user view with return command.
Warning: The slave board is not in position. Exercise caution when performing this operation.
[R2] interface Ethernet 3/0/1
[R2-Ethernet3/0/1] ipv6 enable
[R2-Ethernet3/0/1] quit
[R2] interface Ethernet 3/0/2
[R2-Ethernet3/0/2] ipv6 enable
[R2-Ethernet3/0/2] quit
```

system-view immediately: indicates that the configuration takes effect immediately.

```
[R3] interface GE 0/0/2
[R3-GE0/0/2] undo portswitch
[R3-GE0/0/2] ipv6 enable
[R3-GE0/0/2] 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 GE 0/0/1
[R1-GE0/0/1] ipv6 address auto link-local
[R1-GE0/0/1] quit
```

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.

```
[R2] interface Ethernet 3/0/1
[R2-Ethernet3/0/1] ipv6 address auto link-local
[R2-Ethernet3/0/1] quit
[R2] interface Ethernet 3/0/2
[R2-Ethernet3/0/2] ipv6 address auto link-local
[R2-Ethernet3/0/2] quit
```

```
[R3] interface GE 0/0/2
[R3-GE0/0/2] ipv6 address auto link-local
```

```
[R3-GE0/0/2] quit
```

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

```
[R1] display ipv6 interface GE 0/0/1
GE0/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::FA27:76FF:FE33:11
  No global unicast address configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF33:11
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
```

```
[R2] display ipv6 interface Ethernet 3/0/1
Ethernet3/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::3A81:2FF:FE11:301
  No global unicast address configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF11:301
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
  ND Proxy is disabled

[R2] display ipv6 interface Ethernet 3/0/2
Ethernet3/0/2 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::3A81:2FF:FE11:302
  No global unicast address configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF11:302
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
  ND Proxy is disabled
```

```
[R3] display ipv6 interface GE 0/0/2
GE0/0/2 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::FA27:76FF:FE33:32
  No global unicast address configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF33:32
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND NUD is enabled, number of NUD attempts: 3
  ND NUD interval is 5000 milliseconds
  ND reachable time is 1200000 milliseconds
  ND stale time is 1200 seconds
  ND retransmit interval is 1000 milliseconds
  ND RAs are halted
```

# Test network connectivity between R1 and R2.

```
<R1> ping ipv6 FE80::3A81:2FF:FE11:301 -i GE 0/0/1
  PING FE80::3A81:2FF:FE11:301 : 56   data bytes, press CTRL_C to break
    Reply from FE80::3A81:2FF:FE11:301
    bytes=56 Sequence=1 hop limit=64 time=14 ms
    Reply from FE80::3A81:2FF:FE11:301
    bytes=56 Sequence=2 hop limit=64 time=7 ms
    Reply from FE80::3A81:2FF:FE11:301
    bytes=56 Sequence=3 hop limit=64 time=8 ms
    Reply from FE80::3A81:2FF:FE11:301
    bytes=56 Sequence=4 hop limit=64 time=10 ms
    Reply from FE80::3A81:2FF:FE11:301
    bytes=56 Sequence=5 hop limit=64 time=7 ms

  --- FE80::3A81:2FF:FE11:301 ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max=7/9/14 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 Ethernet 3/0/1
[R2-Ethernet3/0/1] ipv6 address 2000:12::2 64
[R2-Ethernet3/0/1] quit
[R2] interface Ethernet 3/0/2
[R2-Ethernet3/0/2] ipv6 address 2000:23::2 64
[R2-Ethernet3/0/2] 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] dhcpv6 enable
[R2] dhcpv6 duid llt
```

The **dhcpv6 enable** command enables DHCPv6. The **dhcpv6 duid** command configures a DUID for a DHCPv6 device.

```
[R2] dhcpv6 pool pool1
[R2-dhcpv6-pool-pool1] address prefix 2000:23::/64
[R2-dhcpv6-pool-pool1] dns-server 2000:23::2
[R2-dhcpv6-pool-pool1] quit
```

Create an address pool named **pool1**. Set the address prefix to **2000:23::/64**. Set the IP address of the DNS server to **2000:23::2**.

```
[R2] interface Ethernet 3/0/2
[R2-Ethernet3/0/2] dhcpv6 server pool1
[R2-Ethernet3/0/2] quit
```

Enable the DHCPv6 server function on the interface.

# Configure the DHCPv6 client function.

```
[R3] dhcpv6 duid llt
[R3] interface GE 0/0/2
[R3-GE0/0/2] ipv6 address auto dhcp
[R3-GE0/0/2] quit
```

# Display the client address and DNS server information.

```
[R3] display ipv6 interface brief
*down: administratively down
!down: FIB overload down
(l): loopback
(s): spoofing
```

```
Interface                          Physical Protocol VPN
GE0/0/2                              up         up          --
[IPv6 Address/Prefix Length] 2000:23::/128
```

```
[R3] display dhcpv6 client interface GE 0/0/2
GE0/0/2 is in stateful DHCPv6 client mode.
Stateful DHCPv6 client is in BOUND state.
Preferred server DUID     : 000100012E5ED98338BA4102B501
   Reachable via address : FE80::3A81:2FF:FE11:302
IA NA IA ID 0x00000071 T1 43200 T2 69120
   Obtained        : 20XX-XX-XX XX:XX:XX
   Renews           : 20XX-XX-XX XX:XX:XX
   Rebinds         : 20XX-XX-XX XX:XX:XX
   Address         : 2000:23::
      Lifetime valid 172800 seconds, preferred 86400 seconds
      Expires at 20XX-XX-XX XX:XX:XX(172664 seconds left)
DNS server         : 2000:23::2
```

GE0/0/3 on R3 has obtained an IPv6 global unicast address.

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 Ethernet 3/0/2
[R2-Ethernet3/0/2] undo ipv6 nd ra halt
[R2-Ethernet3/0/2] ipv6 nd autoconfig managed-address-flag
[R2-Ethernet3/0/2] ipv6 nd autoconfig other-flag
[R2-Ethernet3/0/2] quit
```

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

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.

1. If the M flag is set, a host obtains an IPv6 address through stateful autoconfiguration.
2. 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.

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

1. 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.
2. 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.

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

```
[R3] interface GE 0/0/2
[R3-GE0/0/2] ipv6 address auto global default
[R3-GE0/0/2] quit
```

# Display the routes of R3.

```
<R3> display ipv6 routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 6          Routes : 6

Destination   : ::                                PrefixLength : 0
NextHop       : FE80::3A81:2FF:FE11:302            Preference   : 64
Cost          : 0                                  Protocol     : ND
RelayNextHop  : ::                                 TunnelID     : 0x0
Interface     : GE0/0/2                            Flags        : D

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

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

Destination   : ::FFFF:127.0.0.1                  PrefixLength : 128
NextHop       : ::1                                Preference   : 0
Cost          : 0                                  Protocol     : Direct
RelayNextHop  : ::                                 TunnelID     : 0x0
Interface     : InLoopBack0                        Flags        : D

Destination   : 2000:23::                         PrefixLength : 128
NextHop       : ::1                                Preference   : 0
Cost          : 0                                  Protocol     : Direct
RelayNextHop  : ::                                 TunnelID     : 0x0
Interface     : GE0/0/2                            Flags        : D
```

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

The routing table of R3 contains a default route with GE0/0/2 as the outbound interface.

Step 6 Configure R1 to access R3 through a static route.

# Configure an IPv6 address on GE0/0/1 of R1.

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

# Configure a static route on R1 to enable connectivity between GE0/0/1 on R1 and GE0/0/2 on R3.

```
[R1] ipv6 route-static 2000:23:: 64 2000:12::2
```

# Test connectivity.

```
[R1] ping ipv6 2000:23::
  PING 2000:23:: : 56   data bytes, press CTRL_C to break
    Reply from 2000:23::
    bytes=56 Sequence=1 hop limit=63 time=21 ms
    Reply from 2000:23::
    bytes=56 Sequence=2 hop limit=63 time=25 ms
    Reply from 2000:23::
    bytes=56 Sequence=3 hop limit=63 time=26 ms
    Reply from 2000:23::
    bytes=56 Sequence=4 hop limit=63 time=26 ms
    Reply from 2000:23::
    bytes=56 Sequence=5 hop limit=63 time=16 ms

  --- 2000:23:: ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max=16/22/26 ms
```

R1 has a static route to the network 2000:23::/64. R3 obtains the default route through DHCPv6. Therefore, GE0/0/1 on R1 and GE0/0/2 on R3 can communicate with each other.

----End

7.3 Configuration Reference

Configuration on R1

```
sysname R1
#
interface GE0/0/1
 ipv6 enable
 ipv6 address 2000:12::1/64
 ipv6 address auto link-local
#
ipv6 route-static 2000:23:: 64 2000:12::2
#
```

Configuration on R2

```
sysname R2
#
dhcpv6 pool pool1
 address prefix 2000:23::/64
 dns-server 2000:23::2
#
interface Ethernet3/0/1
 undo shutdown
 ipv6 enable
 ipv6 address 2000:12::2/64
 ipv6 address auto link-local
#
interface Ethernet3/0/2
 undo shutdown
 ipv6 enable
 ipv6 address 2000:23::2/64
 ipv6 address auto link-local
 undo ipv6 nd ra halt
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 dhcpv6 server pool1
#
```

Configuration on R3

```
sysname R3
#
interface GE0/0/2
 ipv6 enable
 ipv6 address auto link-local
 ipv6 address auto global default
 ipv6 address auto dhcp
#
```

7.4 Quiz

1. Why the source interface must be specified in Step 3 (testing the connectivity between link-local addresses)?

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.

8 Network Programming and Automation Basics (Omitted)

Currently, the programming automation experiment cannot be completed using the simulator. For details, see the HCIA-Datacom Lab Guide of the real device.

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. 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

9.3.2.1 Device Selection and Physical Topology Design (Optional)

Background:

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

Floor	First Floor	Second	Third	Other Floors

		Floor	Floor	(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.

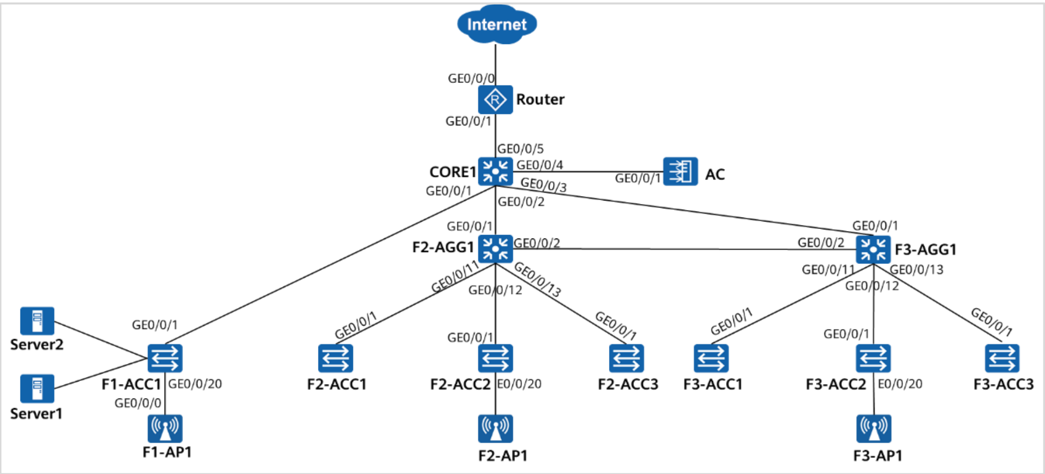
Ensure that computers have a rate of 100 Mbit/s and servers have a rate of 1000 Mbit/s.

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

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.

9.3.2.2 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

Reference answer:

VLAN ID	Description
21	Layer 2 device management VLAN on the first floor
22	Layer 2 device management VLAN on the second floor
23	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
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

9.3.2.3 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
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
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

9.3.2.4 WLAN Design

Background:

- All APs are managed by the AC in a unified manner, and the AC has limited forwarding performance.

1. APs on the first floor are registered at Layer 2.
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.

1. The WPA-WPA2+PSK+AES security policy is used.
2. 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:	Name: WLAN-F2 VAP profile: WLAN-	Name: WLAN-F3 VAP profile: WLAN-

	WLAN-F1 Regulatory domain profile: default	F2 Regulatory domain profile: default	F3 Regulatory domain profile: default
Regulatory domain profile	Name: default 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

9.3.2.5 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.

9.3.2.6 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

9.3.3.1 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.

9.3.3.2 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

9.3.4.1 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.
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

9.3.5.1 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.

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.