Huawei Certification Training

HCIP-Datacom-SD-WAN Planning and Deployment Data Communication Senior Engineer Lab Guide

ISSUE:1.0

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

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: http://e.huawei.com

Huawei Certificate System

Huawei Certification is an integral part of the company's "Platform + Ecosystem" strategy, and it supports the ICT infrastructure featuring "Cloud-Pipe-Device". It evolves to reflect the latest trends of ICT development. Huawei Certification consists of two categories: ICT Infrastructure Certification, and Cloud Service & Platform 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).

With its leading talent development system and certification standards, Huawei is committed to developing ICT professionals in the digital era, building a healthy ICT talent ecosystem.

HCIP-Datacom-SD-WAN Planning and Deployment (HCIP-Datacom-Campus) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. HCIP-Datacom-SD-WAN Planning and Deployment certification covers Enterprise WAN interconnection scenario, GRE technology, IPsec VPN technology, QoS basic principles, HA technology, SD-WAN deployment, SD-WAN management and O&M, SD-WAN networking principles and planning, SD-WAN application experience, SD-WAN security, SD-WAN intelligent O&M, and SD-WAN Practice. such as knowledge. You can be qualified as a network engineer (account manager, project manager, pre-sales engineer, post-sales engineer, and O&M engineer) in campus scenarios in the datacom field. You can use Huawei datacom products to perform SD-WAN planning, automatic network deployment, and O&M.

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


Huawei Certification
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate
Cloud Service & Platform
HarmonyOS(To Be)
IoT
Big Data
AI
GaussDB
openEuler
Kunpeng Application Developer
Cloud(Cloud Computing + Cloud Service)
ICT Infrastructure
Storage
Intelligent Computing
Enterprise Communication
Data Center
Datacom
WLAN
Security
SDN
Transmission
Access
LTE
5G

About This Document

Overview

This document is an HCIP-Datacom-SD-WAN Planning and Deployment certification training course.

This document is intended for trainees who are going to take the HCIP-Datacom-SD-WAN Planning and Deployment exams. It is also targeting learners who want to study traditional SD-WAN technologies, Huawei's Enterprise WAN interconnection scenario, GRE technology, IPsec VPN technology, QoS basic principles, HA technology, SD-WAN deployment, SD-WAN management and O&M, SD-WAN networking principles and planning, SD-WAN application experience, SD-WAN security, SD-WAN intelligent O&M, and SD-WAN Practice.

Description

This document guides you through five labs, namely, three technology labs and two solution labs as follows:

- GRE technology lab
- IPsec technology lab
- QoS technology lab
- HA technology lab
- SD-WAN Controller lab

Background Knowledge Required

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

- Have basic computer skills.
- Be familiar with the principles of the TCP/IP protocol stack.
- Be familiar with the basic working principles of Ethernet switches and routers.
- Knowledge and skills described in the HCIP-Datacom-Core Technology course

Symbol Conventions

Lab Environment

Networking

This lab environment is intended for datacom network engineers preparing for the HCIP-Datacom-SD-WAN Planning and Deployment exam. Each lab environment consists of one switches, six routers, and several servers.

Device Introduction

To meet the requirements of the HCIP-Datacom-SD-WAN Planning and Deployment experiment, you are advised to use the following configurations for each lab environment:

The mapping between device names, models, and versions is as follows:

Device	Model	Software version
Switch	CloudEngine S5731-H48T4XC	V200R019C00 or later
Router	NetEngine AR6120	V300R019C10 or later

Note: The port information, display information, and configuration information of all devices in this document are provided based on the devices in the recommended topology. The information may vary according to lab environments.

Pre-configuration

For the overall topology and pre-configuration of this lab, refer the 《HCIP-Datacom-SD-WAN Planning and Deployment Lab Setup Guide V1.0》.

Content

1 GRE Technology LAB

1.1 Basic GRE Operations

1.1.1 Introduction

1.1.1.1 About This Lab

This lab guides you through how to perform basic GRE operations on Huawei devices.

1.1.1.2 Objectives

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

- Understand GRE functions.
- Master basic configuration commands of GRE.
- Learn how to check whether the GRE configuration is successful.

1.1.1.3 Networking Topology

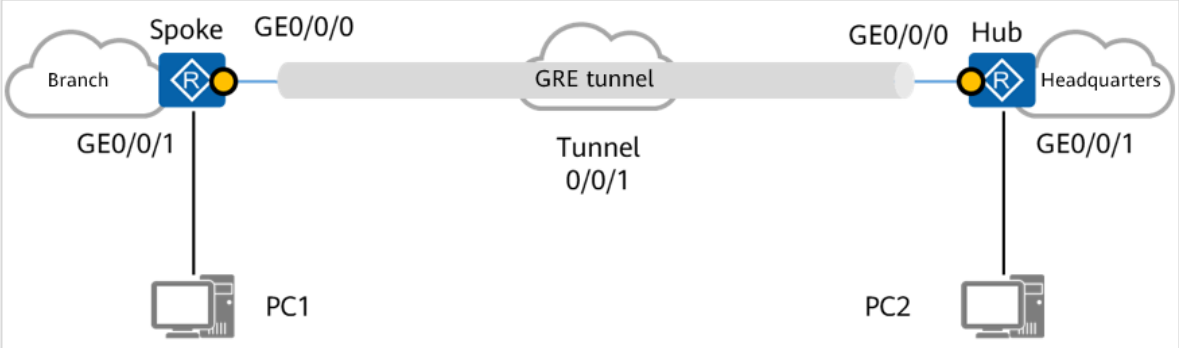


Figure 1-1 Topology for configuring basic GRE functions

As shown in the networking diagram, the spoke is an egress router of the branch, and the hub is an egress router of the headquarters. PC2 at the headquarters can communicate with PC1 at the branch through GRE.

1.1.2 Lab Configuration

1.1.2.1 Configuration Roadmap

1. Complete basic configurations, such as the device name and router interface IP address.
2. Deploy a GRE tunnel between the hub and spoke.
3. Configure static routes between the hub and spoke.
4. Enable GRE Keepalive detection to improve GRE tunnel stability (optimization configuration).

1.1.2.2 Configuration Procedure

Step 1 Configure IP addresses for physical interfaces based on the following table.

Router	Interface	IP Address/Mask
Spoke	GigabitEthernet0/0/1	10.1.1.2/24
	GigabitEthernet0/0/0	20.1.1.1/24
Hub	GigabitEthernet0/0/1	10.2.1.2/24
	GigabitEthernet0/0/0	20.1.1.2/24
PC1	Ethernet0/0/1	10.1.1.1/24
PC2	Ethernet0/0/1	10.2.1.1/24

The configuration details are not provided.

Step 2 Deploy a GRE tunnel. The tunnel addresses are as follows.

Router	Interface	IP Address/Mask
Spoke	Tunnel0/0/1	40.1.1.1/24
HUB	Tunnel0/0/1	40.1.1.2/24

Configure the spoke.

```
[Spoke]interface  Tunnel  0/0/1
[Spoke-Tunnel0/0/1]ip address  40.1.1.1 24
[Spoke-Tunnel0/0/1]tunnel-protocol gre
[Spoke-Tunnel0/0/1]source 20.1.1.1
[Spoke-Tunnel0/0/1]destination 20.1.1.2
```

Configure the hub.

```
[Hub]interface  Tunnel  0/0/1
[Hub-Tunnel0/0/1]ip address  40.1.1.2 24
```

```
[Hub-Tunnel0/0/1]tunnel-protocol gre
[Hub-Tunnel0/0/1]source 20.1.1.2
[Hub-Tunnel0/0/1]destination 20.1.1.1
```

Step 3 On the hub and spoke, configure static routes to the network segments of the PCs connected to them.

Configure a static route to the network segment of PC2 on the spoke, with the outbound interface being the GRE tunnel interface Tunnel0/0/1.

```
[Spoke]ip route-static 10.2.1.0 24 Tunnel 0/0/1
```

Configure a static route to the network segment of PC1 on the hub, with the outbound interface being the GRE tunnel interface Tunnel0/0/1.

```
[Hub]ip route-static 10.1.1.0 24 Tunnel 0/0/1
```

Step 4 Enable GRE Keepalive detection on the hub and spoke (optimization configuration).

```
[Hub-Tunnel0/0/1] keepalive
```

The configuration of the spoke is the same as that of the hub. The configuration details are not provided.

NOTE

Keepalive detection checks whether the peer end of the tunnel is reachable. If the peer end is unreachable, the tunnel connection is terminated. You can add the period parameter in the keepalive command to specify the interval at which Keepalive messages are sent. You can also add retry-times following period, which indicates the retransmission count. By default, if no optional parameter is specified, the value of period is 5, and the value of retry-times is 3.

----End

1.1.3 Verification

1.1.3.1 Checking Information About Tunnel Interfaces Between the Hub and Spoke

Check tunnel interface information on the hub.

```
<Hub>display   interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-06-09 14:27:59 UTC-08:00
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 40.1.1.2/24
Encapsulation is TUNNEL, loopback not set
```

```
Tunnel source 20.1.1.2 (GigabitEthernet0/0/0), destination 20.1.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 5 retry-times 3
Checksumming of packets disabled
Current system time: 2020-06-09 14:39:46-08:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 72 bits/sec, 0 packets/sec
    0 seconds input rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,   0 bytes
    0 input error
    122 packets output,   5856 bytes
    0 output error
    Input bandwidth utilization   : --
    Output bandwidth utilization : --
```

Check tunnel interface information on the spoke.

```
<Spoke>display   interface   Tunnel   0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-06-09 14:24:02 UTC-08:00
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 40.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 20.1.1.1 (GigabitEthernet0/0/0), destination 20.1.1.2
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 5 retry-times 3
Checksumming of packets disabled
Current system time: 2020-06-09 14:34:27-08:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 32 bits/sec, 0 packets/sec
    0 seconds input rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,   0 bytes
    0 input error
    62 packets output,   2976 bytes
    0 output error
    Input bandwidth utilization   : --
    Output bandwidth utilization : --      Output bandwidth utilization : --
```

1.1.3.2 Performing the Ping Operation

Ping the tunnel interface address 40.1.1.1 of the spoke from the hub.

```
<Hub>ping 40.1.1.1
  PING 40.1.1.1: 56   data bytes, press CTRL_C to break
    Reply from 40.1.1.1: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 40.1.1.1: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 40.1.1.1: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 40.1.1.1: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 40.1.1.1: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 40.1.1.1 ping statistics ---
```

```
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 20/32/80 ms
```

Ping the IP address 10.2.1.1 of PC2 from PC1.

```
PC1>ping 10.2.1.1
Ping 10.2.1.1: 32 data bytes, Press Ctrl_C to break
From 10.2.1.1: bytes=32 seq=1 ttl=126 time=16 ms
From 10.2.1.1: bytes=32 seq=2 ttl=126 time=16 ms
From 10.2.1.1: bytes=32 seq=3 ttl=126 time=15 ms
From 10.2.1.1: bytes=32 seq=4 ttl=126 time=31 ms
From 10.2.1.1: bytes=32 seq=5 ttl=126 time=16 ms

--- 10.2.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/18/31 ms
```

1.1.4 Reference Configuration

1.1.4.1 Configurations of Spoke

```
<Spoke>display current-configuration
[V200R003C00]
#
 sysname Spoke
#
interface GigabitEthernet0/0/0
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
#
interface Tunnel0/0/1
 ip address 40.1.1.1 255.255.255.0
 tunnel-protocol gre
keepalive
 source 20.1.1.1
 destination 20.1.1.2
#
ip route-static 10.2.1.0 255.255.255.0 Tunnel0/0/1
#
#
return
```

1.1.4.2 Configurations of Hub

```
<Hub>display current-configuration
[V200R003C00]
```

```
#
 sysname Hub
interface GigabitEthernet0/0/0
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.2.1.2 255.255.255.0
#
#
interface Tunnel0/0/1
 ip address 40.1.1.2 255.255.255.0
 tunnel-protocol gre
 keepalive
 source 20.1.1.2
 destination 20.1.1.1
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel0/0/1
#
Return
```

1.1.5 Quiz

What are application scenarios of GRE VPN on the live network?

If a router is added between the hub and spoke, can a GRE tunnel be set up between the hub and spoke? If so, which configurations need to be added?

1.2 Basic GRE Key Operations

1.2.1 Introduction

1.2.1.1 About This Lab

You can configure the GRE key to perform security check on the tunnel interface. This prevents the tunnel interface from incorrectly identifying and receiving packets from other devices.

1.2.1.2 Objectives

- Upon completion of this lab, you will be able to:
- Understand the function of configuring the GRE key.
- Master the commands for configuring the GRE key.
- Learn how to check whether the GRE keys at both ends are consistent.

1.2.1.3 Networking Topology

The networking diagram is the same as that in lab 1.

Based on the configuration in lab 1, the GRE key of the hub and spoke is set to 123 to improve security.

1.2.2 Lab Configuration

1.2.2.1 Configuration Roadmap

1. Set the GRE key to 123 on the hub based on the configuration in lab 1 and test the connectivity of the terminal.
2. Set the GRE key of the spoke to 123 and test the connectivity of the terminal.

1.2.2.2 Configuration Procedure

Step 1 Configure the GRE key on the hub.

```
[Hub]interface Tunnel 0/0/1
[Hub-Tunnel0/0/1]gre checksum
[Hub-Tunnel0/0/1]gre key 123
```

NOTE

The GRE key can only be set to digits.

Step 2 Configure the GRE key of the spoke.

```
[Spoke]interface Tunnel 0/0/1
[Spoke-Tunnel0/0/1]gre checksum
```

```
[Spoke-Tunnel0/0/1]gre key 123
```

NOTE

The gre checksum command is used to enable checksum check on the GRE tunnel interface.

----End

1.2.3 Verification

1.2.3.1 Performing the Ping Operation

After step 1 is complete, ping PC2 from PC1.

```
PC>ping 10.2.1.1

Ping 10.2.1.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

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

After step 2 is complete, configure the GRE key on the spoke and ping PC2 from PC1.

```
PC>ping 10.2.1.1

Ping 10.2.1.1: 32 data bytes, Press Ctrl_C to break
From 10.2.1.1: bytes=32 seq=1 ttl=126 time=16 ms
From 10.2.1.1: bytes=32 seq=2 ttl=126 time=16 ms
From 10.2.1.1: bytes=32 seq=3 ttl=126 time=16 ms
From 10.2.1.1: bytes=32 seq=4 ttl=126 time=16 ms
From 10.2.1.1: bytes=32 seq=5 ttl=126 time=15 ms

--- 10.2.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/15/16 ms
```

1.2.3.2 Checking the GRE Key

Check the GRE key configuration.

```
[Spoke]display interface  Tunnel  0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2020-06-09 10:50:02 UTC-08:00
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
```

```
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 40.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 20.1.1.1 (GigabitEthernet0/0/0), destination 20.1.1.2
Tunnel protocol/transport GRE/IP, key 123
keepalive disabled
Checksumming of packets disabled
Current system time: 2020-06-09 11:15:12-08:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 40 bits/sec, 0 packets/sec
    0 seconds input rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,   0 bytes
    0 input error
    15 packets output,   1680 bytes
    0 output error
    Input bandwidth utilization   : --
Output bandwidth utilization : --
```

The configuration of the hub is the same as that of the spoke. The configuration details are not provided.

1.2.4 Reference Configuration

Add the following configurations to the hub and spoke. Other configurations are the same as those in lab 1 and are not provided.

1.2.4.1 Configurations of Hub and Spoke

```
#
interface Tunnel0/0/1
gre key 123
gre checksum
#
```

1.2.5 Quiz

What are possible causes for a GRE tunnel establishment failure?

2 IPsec Technology LAB

2.1 Basic IPsec Operations

2.1.1 Introduction

2.1.1.1 About This Lab

In this lab, you will learn about basic IPsec operations by configuring Huawei devices.

2.1.1.2 Objectives

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

- Understand IPsec functions.
- Configure IPsec VPN.
- Understand IPsec VPN fundamentals.
- Understand the IKE SA establishment process and principles.

2.1.1.3 Networking Topology

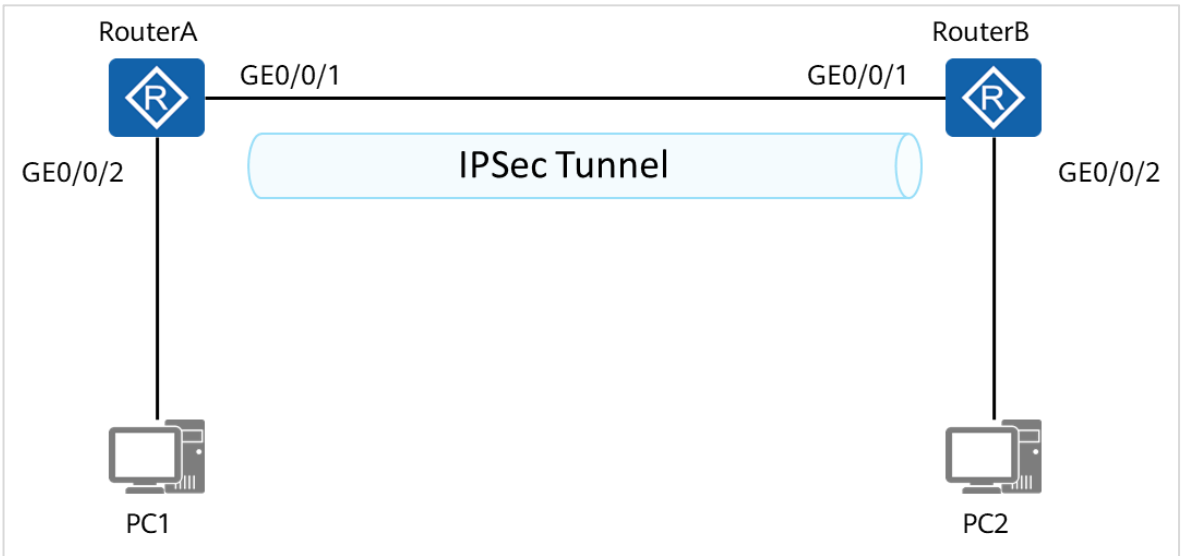


Figure 2-1 **Basic IPsec configuration networking topology**

2.1.1.4 Background

As shown in the networking topology, PC1 and PC2 are connected through RouterA and RouterB. Assume that there are reachable routes between RouterA and RouterB. In the lab, RouterA and RouterB are directly connected. In the live network, a routing protocol may need to be deployed if RouterA and RouterB are connected over the Internet. IPsec VPN technology is used to allow communication between PC1 and PC2.

2.1.2 Lab Configuration

2.1.2.1 Configuration Roadmap

1. Complete basic configurations, such as device names, router interface IP addresses, and static routes.
2. Configure an IKE proposal.
3. Configure IKE peers.
4. Create ACLs to define the data flows to be protected by IPsec.
5. Configure an IPsec proposal.
6. Configure an IPsec policy.
7. Apply the IPsec policy to an interface.

2.1.2.2 Configuration Procedure

Step 1 Configure IP addresses for physical interfaces based on the following table.

Router	Interface	IP Address/Mask
RouterA	GigabitEthernet0/0/1	202.38.163.1/24
	GigabitEthernet0/0/2	10.1.1.1/24
RouterB	GigabitEthernet0/0/1	202.38.163.2/24
	GigabitEthernet0/0/2	10.1.2.1/24
PC1	Ethernet0/0/1	10.1.1.2/24
PC2	Ethernet0/0/1	10.1.2.2/24

Configure RouterA.

```
[RouterA]interface GigabitEthernet 0/0/1
[RouterA-GigabitEthernet0/0/1]ip address 202.38.163.1 24
[RouterA-GigabitEthernet0/0/1]quit
[RouterA]interface GigabitEthernet 0/0/2
[RouterA-GigabitEthernet0/0/2]ip address 10.1.1.1 24
[RouterA-GigabitEthernet0/0/2]quit
[RouterA]ip route-static 10.1.2.0 24 202.38.163.2
```

Configure a static route to enable RouterA to generate a route to the peer PC.

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Step 2 Configure an IKE proposal.

Name	IKE Authentication Algorithm	IKE Encryption Algorithm
RouterA	Md5	Aes-cbc-128
RouterB	Md5	Aes-cbc-128

NOTE

Establishing an IPsec tunnel can protect data flows and improve data security. SAs must have been established before a tunnel is established. IKE can be used to establish SAs automatically. Compared with the manual SA establishment method, IKE simplifies the configuration, improves security, and facilitates large-scale deployment.

Configure RouterA.

```
[RouterA]ike proposal 1
[RouterA-ike-proposal-1]encryption-algorithm aes-cbc-128
[RouterA-ike-proposal-1]authentication-algorithm md5
```

NOTE

Encryption and authentication algorithms are used during IKE negotiation. Therefore, devices on both ends must use the same encryption and authentication algorithms.

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Step 3 Configure an IKE peer.

Name	IKE Local Name	IKE Peer Name	IKE Version	IKE Exchange Mode	Pre-shared Key
RouterA	huawei	a	V1	Main mode	hello
RouterB	huawei2	b	V1	Main mode	hello

NOTE

When an IPsec tunnel needs to be established through IKE negotiation, you need to reference an IKE peer and configure parameters for the IKE peer during IKE negotiation.

Configure RouterA.

```
[RouterA]ike local-name huawei
[RouterA]ike peer a v1
[RouterA-ike-peer-a]exchange-mode main
[RouterA-ike-peer-a]ike-proposal 1
[RouterA-ike-peer-a]local-id-type name
```

```
[RouterA-ike-peer-a]remote-name huawei2
[RouterA-ike-peer-a]remote-address 202.38.163.2
[RouterA-ike-peer-a]pre-shared-key simple hello
[RouterA-ike-peer-a]local-address 202.38.163.1
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Step 4 Create an ACL to define the data flows to be protected by IPsec.

NOTE

This step is to specify the range of data flows to be protected by the IPsec tunnel and filter out the packets that need to enter the IPsec tunnel.

Configure RouterA.

```
[RouterA]acl 3000
[RouterA-acl-adv-3000]rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

NOTE

The preceding steps are performed to establish an IKE SA in phase 1 to protect subsequent packet exchange and VPN establishment.

Step 5 Configure an IPsec proposal.

Name	IPsec Proposal Name	Data Encapsulation Mode	Security Protocol	ESP Authentication Algorithm	ESP Encryption Algorithm
RouterA	Xy	tunnel	esp	Sha1	des
RouterB	xy2	tunnel	esp	Sha1	des

NOTE

In this step, an IPsec SA is established in phase 2 to protect IPsec service data flows.

Configure RouterA.

```
[RouterA]ipsec proposal xy
[RouterA-ipsec-proposal-xy]encapsulation-mode tunnel
[RouterA-ipsec-proposal-xy]transform esp
[RouterA-ipsec-proposal-xy]esp authentication-algorithm sha1
[RouterA-ipsec-proposal-xy]esp encryption-algorithm des
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Step 6 Configure an IPsec policy.

NOTE

An IPsec policy is the prerequisite for creating an IPsec SA. In an IPsec policy, ACL-defined data flows are associated with an IPsec proposal.

Configure RouterA.

```
[RouterA]ipsec policy test 1 isakmp
[RouterA-ipsec-policy-isakmp-test-1]security acl 3000
[RouterA-ipsec-policy-isakmp-test-1]proposal xy
[RouterA-ipsec-policy-isakmp-test-1]ike-peer a
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Step 7 Apply the IPsec policy to an interface.

```
[RouterA]interface GigabitEthernet 0/0/1
[RouterA-GigabitEthernet0/0/1]ipsec policy test
```

An interface can have only one IPsec policy group applied, and an IPsec policy group can be applied to only one interface.

----End

2.1.3 Verification

2.1.3.1 Verifying the Establishment of IKE SAs and IPsec SAs

Run the display ike sa command on RouterA to check information about the SAs established through IKE negotiation.

```
[RouterA]display ike sa
    Conn-ID  Peer            VPN    Flag(s)                 Phase
  -----------------------------------------------------------------
       14    202.38.163.2    0      RD|ST                   2
       13    202.38.163.2    0      RD|ST                   1

  Flag Description:
  RD--READY    ST--STAYALIVE    RL--REPLACED    FD--FADING    TO--TIMEOUT
  HRT--HEARTBEAT    LKG--LAST KNOWN GOOD SEQ NO.    BCK--BACKED UP
```

NOTE

The RD field indicates that IKE SAs have been established and the negotiation is complete.

Run the display ipsec sa command on RouterA to check SA configuration.

```
[RouterA]display ipsec sa

===============================
Interface: GigabitEthernet0/0/1
  Path MTU: 1500
```

```
==============================

  -----------------------------
  IPSec policy name: "test"
  Sequence number   : 1
  Acl Group         : 3000
  Acl rule          : 5
  Mode              : ISAKMP
  -----------------------------
    Connection ID     : 14
    Encapsulation mode: Tunnel
    Tunnel local      : 202.38.163.1
    Tunnel remote     : 202.38.163.2
    Flow source       : 10.1.1.0/255.255.255.0 0/0
    Flow destination  : 10.1.2.0/255.255.255.0 0/0
    Qos pre-classify  : Disable

    [Outbound ESP SAs]
      SPI: 1711803007 (0x66080a7f)
      Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887283200/3439
      Max sent sequence-number: 10
      UDP encapsulation used for NAT traversal: N

    [Inbound ESP SAs]
      SPI: 1012049468 (0x3c52a63c)
      Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436260/3439
      Max received sequence-number: 9
      Anti-replay window size: 32
      UDP encapsulation used for NAT traversal: N
```

2.1.3.2 Verifying the Ping Connectivity

Ping IP address 10.1.2.2 of PC2 from PC1.

```
PC1>ping 10.1.2.2
Ping 10.1.2.2: 32 data bytes, Press Ctrl_C to break
From 10.1.2.2: bytes=32 seq=1 ttl=126 time=16 ms
From 10.1.2.2: bytes=32 seq=2 ttl=126 time=16 ms
From 10.1.2.2: bytes=32 seq=3 ttl=126 time=15 ms
From 10.1.2.2: bytes=32 seq=4 ttl=126 time=31 ms
From 10.1.2.2: bytes=32 seq=5 ttl=126 time=16 ms

--- 10.1.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/18/31 ms
```

2.1.4 Reference Configuration

2.1.4.1 Configurations of RouterA

```
#
 sysname RouterA
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal xy
 esp authentication-algorithm sha1
#
ike proposal 1
 encryption-algorithm aes-cbc-128
 authentication-algorithm md5
#
ike peer a v1
 pre-shared-key simple hello
 ike-proposal 1
 local-id-type name
 remote-name huawei2
 local-address 202.38.163.1
 remote-address 202.38.163.2
#
ipsec policy test 1 isakmp
 security acl 3000
 ike-peer a
 proposal xy
#
interface GigabitEthernet0/0/1
 ip address 202.38.163.1 255.255.255.0
 ipsec policy test
#
interface GigabitEthernet0/0/2
 ip address 10.1.1.1 255.255.255.0
#
ip route-static 10.1.2.0 255.255.255.0 202.38.163.2
#
```

2.1.4.2 Configurations of RouterB

```
#
 sysname RouterB
#
acl number 3000
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal xy2
 esp authentication-algorithm sha1
#
ike proposal 1
 encryption-algorithm aes-cbc-128
 authentication-algorithm md5
```

```
#
ike peer b v1
 pre-shared-key simple hello
 ike-proposal 1
 local-id-type name
 remote-name huawei
 local-address 202.38.163.2
 remote-address 202.38.163.1
#
ipsec policy test 1 isakmp
 security acl 3000
 ike-peer b
 proposal xy2
#
interface GigabitEthernet0/0/1
 ip address 202.38.163.2 255.255.255.0
 ipsec policy test
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
#
```

2.1.5 Quiz

If IPsec VPN uses IKE to establish an SA, how many IKE working modes are available? What are the differences between them?

If RouterA and RouterB are connected across the public network, can an IPsec tunnel be established between them? If so, which configurations are required?

2.2 Basic GRE over IPsec Operations

2.2.1 Introduction

2.2.1.1 About This Lab

In addition to using ACLs to match data flows to establish tunnels, you can also establish tunnels through tunnel interfaces. For logical interfaces whose tunnel encapsulation mode is GRE, mGRE, or IPsec, the device can provide the IPsec protection function. The method of using tunnel interfaces to establish tunnels simplifies tunnel configuration.

2.2.1.2 Objectives

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

- Understand GRE over IPsec application scenarios.
- Configure GRE over IPsec VPN.
- Understand GRE over IPsec VPN fundamentals.

2.2.1.3 Networking Topology

The networking topology is the same as that in lab 1.

2.2.1.4 Background

If traffic between RouterA and RouterB includes multicast traffic, GRE over IPsec needs to be deployed on tunnel interfaces to protect traffic on tunnel interfaces because IPsec cannot be directly applied to multicast data.

2.2.2 Lab Configuration

2.2.2.1 Configuration Roadmap

1. Configure IPsec parameters.
2. Create tunnel interfaces, configure IP addresses for the tunnel interfaces, set the tunnel encapsulation mode to GRE, and specify the source and destination addresses.
3. Configure an IPsec profile.
4. Apply the IPsec profile to a tunnel interface.

2.2.2.2 Configuration Procedure

Step 1 Configure IPsec parameters.

Configure RouterA.

```
[RouterA]interface GigabitEthernet 0/0/1
[RouterA-GigabitEthernet0/0/1]ip address 202.38.163.1 24
[RouterA-GigabitEthernet0/0/1]quit
[RouterA]interface GigabitEthernet 0/0/2
[RouterA-GigabitEthernet0/0/2]ip address 10.1.1.1 24
[RouterA-GigabitEthernet0/0/2]quit
```

```
[RouterA]ip route-static 10.1.2.0 24 202.38.163.2
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Configure an IKE proposal.

Configure RouterA.

```
[RouterA]ike proposal 1
[RouterA-ike-proposal-1]encryption-algorithm aes-cbc-128
[RouterA-ike-proposal-1]authentication-algorithm md5
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Configure IKE peers.

Configure RouterA.

```
[RouterA]ike local-name huawei
[RouterA]ike peer a v1
[RouterA-ike-peer-a]exchange-mode main
[RouterA-ike-peer-a]ike-proposal 1
[RouterA-ike-peer-a]local-id-type name
[RouterA-ike-peer-a]remote-name huawei2
[RouterA-ike-peer-a]pre-shared-key simple hello
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Step 2 Create a tunnel interface, set parameters, and set the tunnel encapsulation mode to GRE.

Configure RouterA.

```
[RouterA]interface Tunnel 0/0/1
[RouterA-Tunnel0/0/1]ip address 192.168.1.1 24
[RouterA-Tunnel0/0/1]tunnel-protocol gre
[RouterA-Tunnel0/0/1]source 202.38.163.1
[RouterA-Tunnel0/0/1]destination 202.38.163.2
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Step 3 Configure an IPsec profile.

NOTE

This step is the same as that in the previous lab. An IPsec profile can be applied only when the tunnel encapsulation mode is GRE, IPsec, or mGRE. An IPsec profile can be applied to only one tunnel interface, and a tunnel interface can have only one IPsec profile applied.

Configure RouterA.

```
[RouterA]ipsec profile test1
[RouterA-ipsec-profile-test1]proposal xy
[RouterA-ipsec-profile-test1]ike-peer a
```

Configure RouterB. The configuration of RouterB is similar to that of RouterA.

Step 4 Apply the IPsec profile to the tunnel interface.

```
[RouterA]interface  Tunnel 0/0/1
[RouterA-Tunnel0/0/1]ipsec profile test1
```

NOTE

An IPsec profile should be applied to a tunnel interface rather than a physical interface.

----End

2.2.3 Verification

2.2.3.1 Verifying the GRE over IPsec Configuration

Check IKE SAs.

```
<RouterA>display ike sa
    Conn-ID  Peer            VPN     Flag(s)                 Phase
  -------------------------------------------------------------------
        9    202.38.163.2    0       RD|ST                   2
        8    202.38.163.2    0       RD|ST                   1

  Flag Description:
  RD--READY    ST--STAYALIVE    RL--REPLACED    FD--FADING    TO--TIMEOUT
  HRT--HEARTBEAT    LKG--LAST KNOWN GOOD SEQ NO.    BCK--BACKED UP
```

Check IPsec SAs.

```
<RouterA>display ipsec sa

===============================
Interface: Tunnel0/0/1
 Path MTU: 1500
===============================

  -----------------------------
  IPSec profile name: "test1"
  Mode                : PROF-ISAKMP
  -----------------------------
    Connection ID       : 9
    Encapsulation mode: Tunnel
    Tunnel local        : 202.38.163.1
    Tunnel remote       : 202.38.163.2
    Qos pre-classify    : Disable

    [Outbound ESP SAs]
      SPI: 3401727043 (0xcac23c43)
      Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436800/3416
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: N

    [Inbound ESP SAs]
      SPI: 243789870 (0xe87f02e)
```

```
Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
SA remaining key duration (bytes/sec): 1887436800/3416
Max received sequence-number: 0
Anti-replay window size: 32
UDP encapsulation used for NAT traversal: N
```

2.2.3.2 Verifying the Ping Connectivity

Ping PC2 from PC1.

```
PC>ping 10.1.2.2

Ping 10.1.2.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 10.1.2.2: bytes=32 seq=2 ttl=126 time=15 ms
From 10.1.2.2: bytes=32 seq=3 ttl=126 time=31 ms
From 10.1.2.2: bytes=32 seq=4 ttl=126 time=16 ms
From 10.1.2.2: bytes=32 seq=5 ttl=126 time=16 ms

--- 10.1.2.2 ping statistics ---
  5 packet(s) transmitted
  4 packet(s) received
  20.00% packet loss
  round-trip min/avg/max = 0/19/31 ms
```

2.2.4 Reference Configuration

2.2.4.1 Configurations of RouterA

```
#
 sysname RouterA
#
ipsec proposal xy
 esp authentication-algorithm sha1
#
ike proposal 1
 encryption-algorithm aes-cbc-128
 authentication-algorithm md5
#
ike peer a v1
 pre-shared-key simple hello
 ike-proposal 1
 local-id-type name
#
ipsec profile test1
 ike-peer a
 proposal xy
#
interface GigabitEthernet0/0/1
 ip address 202.38.163.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel0/0/1
```

```
 ip address 192.168.1.1 255.255.255.0
 tunnel-protocol gre
 source 202.38.163.1
 destination 202.38.163.2
 ipsec profile test1
#
ip route-static 10.1.2.0 255.255.255.0 tunnel0/0/1
#
```

2.2.4.2 Configurations of Router B

```
#
 sysname RouterB
#
ipsec proposal xy2
 esp authentication-algorithm sha1
#
ike proposal 1
 encryption-algorithm aes-cbc-128
 authentication-algorithm md5
#
ike peer b v1
 pre-shared-key simple hello
 ike-proposal 1
 local-id-type name
#
ipsec profile test2
 ike-peer b
 proposal xy2
#
interface GigabitEthernet0/0/1
 ip address 202.38.163.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface Tunnel0/0/1
 ip address 192.168.1.2 255.255.255.0
 tunnel-protocol gre
 source 202.38.163.2
 destination 202.38.163.1
 ipsec profile test2
#
ip route-static 10.1.1.0 255.255.255.0 tunnel0/0/1
#
```

2.2.5 Quiz

What are the advantages and disadvantages of the methods of using tunnel interfaces and using ACLs to define the data flows to be protected? What are the application scenarios of the two methods?

3 QoS Technology LAB

3.1 Traffic Classification and Priority Re-marking Configuration

3.1.1 Introduction

3.1.1.1 About This Lab

Traffic classification can classify packets matching the same rule into a category. This ensures that the device processes packets matching the same traffic classifier in the same way, and is the prerequisite and basis for implementing differentiated services.

Modular QoS Command-Line Interface (MQC) allows the device to classify packets based on their characteristics and provide the same QoS level for packets of the same type. This enables the device to provide differentiated services for packets of different types. MQC involves three entities: traffic classifier, traffic behavior, and traffic policy.

Priority re-marking is to change the status of packets on the network by increasing or reducing priorities of packets. Re-marking allows a device to re-mark packets matching traffic classification rules. Packets of services that are sensitive to delay and service quality can be re-marked with a high priority so that they can be preferentially scheduled or forwarded. Similarly, priorities of services with no special requirements on delay or service quality can be reduced to save network resources for high-priority packets.

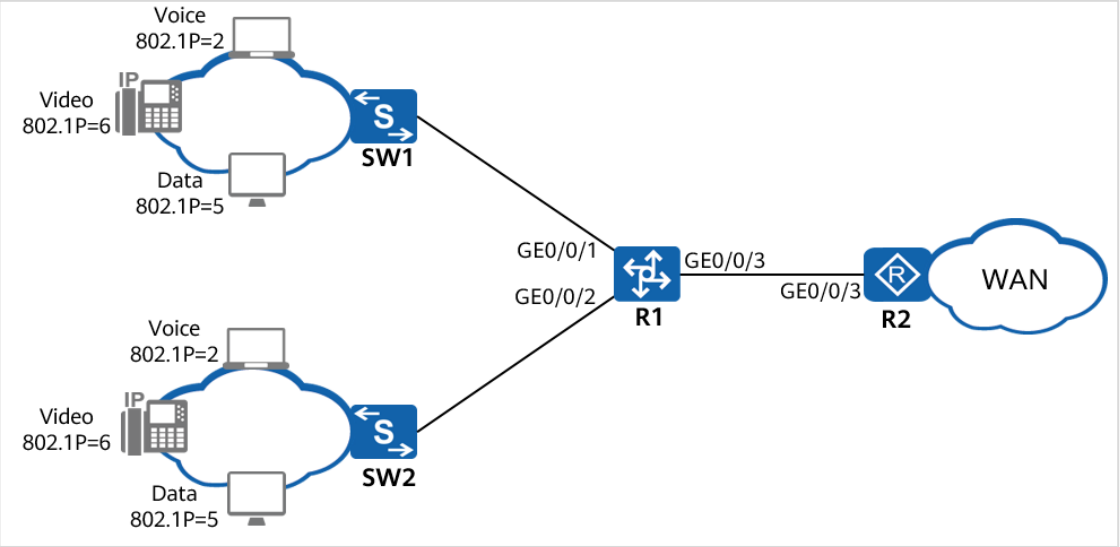
For example, when the 802.1p priority of a VLAN packet is re-marked, the device schedules and forwards the VLAN packet based on the re-marked 802.1p priority and changes the status of the VLAN packet on the Layer 2 network.

3.1.1.2 Objectives

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

- Be familiar with traffic classification rules.
- Learn how to re-mark the 802.1p priority.
- Master the method of applying a traffic policy to an interface.
- Master the usage of MQC.

3.1.1.3 Networking Topology



Voice, video, and data services on the LAN side of the enterprise network are connected to GE0/0/1 and GE0/0/2 of R1 through SW1 and SW2, and are connected to the WAN-side network through GE0/0/3 of R1.

Packets of different services are identified by 802.1p priorities on the LAN side. When packets reach the WAN through GE0/0/3, differentiated services need to be provided for different services based on DSCP priorities of packets.

3.1.2 Lab Configuration

3.1.2.1 Configuration Roadmap

1. Create VLANs and VLANIF interfaces on R1 and configure interfaces so that enterprise users can access the WAN-side network through R1.
2. Configure traffic classifiers to classify packets based on 802.1p priorities.
3. Configure traffic behaviors on R1 to re-mark packet priorities with DSCP priorities.
4. Configure a traffic policy on R1, bind the traffic behaviors and traffic classifiers to the traffic policy, and apply the traffic policy to GE0/0/1 and GE0/0/2 in the inbound direction to re-mark priorities of different service packets.

3.1.2.2 Configuration Procedure

Step 1 Configure VLANs and IP addresses for interfaces so that enterprise users can communicate with the WAN.

Create VLANs 20, 30, and 40 on R1.

```
<Huawei>system-view
[Huawei]sysname R1
[R1]vlan batch 20 30 40
```

Configure GE0/0/1 and GE0/0/2 as trunk interfaces, add GE0/0/1 to VLAN 20, and add GE0/0/2 to VLAN 30.

```
[R1] interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1] port link-type trunk
[R1-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[R1-GigabitEthernet0/0/1] quit
[R1] interface GigabitEthernet0/0/2
[R1-GigabitEthernet0/0/2] port link-type trunk
[R1-GigabitEthernet0/0/2] port trunk allow-pass vlan 30
[R1-GigabitEthernet0/0/2] quit
```

Configure the interface of SW1 connected to R1 as a trunk interface and add it to VLAN 20.

```
[SW1]interface GigabitEthernet0/0/1
[SW1-GigabitEthernet0/0/1]port link-type trunk
[SW1-GigabitEthernet0/0/1]port trunk allow-pass vlan 20
```

Configure the interface of SW2 connected to R1 as a trunk interface and add it to VLAN 30.

```
[SW2]interface GigabitEthernet0/0/2
[SW2-GigabitEthernet0/0/2]port link-type trunk
[SW2-GigabitEthernet0/0/2]port trunk allow-pass vlan 30
```

Configure IP addresses for the interfaces connecting R1 and R2.

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]port link-type access
[R1-GigabitEthernet0/0/3]port default vlan 40
[R1-GigabitEthernet0/0/3]quit
[R1]interface vlanif 40
[R1-Vlanif40]ip address 192.168.4.1 24
[R1-Vlanif40]quit

[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 192.168.4.2 24
```

Configure R2 to communicate with the LAN-side device at the network layer.

```
[R2] ip route-static 192.168.2.0 255.255.255.0 192.168.4.1
[R2] ip route-static 192.168.3.0 255.255.255.0 192.168.4.1
```

Step 2 Configure traffic classifiers.

Create and configure traffic classifiers c1, c2, and c3 on R1 to classify packets based on 802.1p priorities.

```
[R1]traffic classifier c1
[R1-classifier-c1]if
[R1-classifier-c1]if-match 8021p 2
[R1-classifier-c1]quit
[R1]traffic classifier c2
```

```
[R1-classifier-c2]if-match 8021p 5
[R1-classifier-c2]quit
[R1]traffic classifier c3
[R1-classifier-c3]if-match 8021p 6
[R1-classifier-c3]quit
```

Step 3 Configure traffic behaviors.

Create and configure traffic behaviors b1, b2, and b3 on R1 to re-mark 802.1p priorities of packets.

```
[R1]traffic behavior b1
[R1-behavior-b1]remark dscp 15
[R1-behavior-b1]traffic behavior b2
[R1-behavior-b2]remark dscp 40
[R1-behavior-b2]traffic behavior b3
[R1-behavior-b3]remark dscp 50
[R1-behavior-b3]quit
```

Step 4 Configure a traffic policy and apply it to an interface.

Create a traffic policy named p1 on R1, bind the traffic behaviors and traffic classifiers to the traffic policy, and apply the traffic policy to GE0/0/1 and GE0/0/2 in the inbound direction.

```
[R1]traffic policy p1
[R1-trafficpolicy-p1]classifier c1 behavior b1
[R1-trafficpolicy-p1]classifier c2 behavior b2
[R1-trafficpolicy-p1]classifier c3 behavior b3
[R1-trafficpolicy-p1]quit
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]traffic-policy p1 inbound
[R1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2
[R1-GigabitEthernet0/0/2]traffic-policy p1 inbound
[R1-GigabitEthernet0/0/2]quit
```

----End

3.1.3 Verification

Check the traffic classifier configuration.

```
<R1>display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: AND
    Rule(s) : if-match 8021p 5

   Classifier: c3
    Operator: AND
    Rule(s) : if-match 8021p 6

   Classifier: c1
```

```
    Operator: AND
    Rule(s) : if-match 8021p 2

Total classifier number is 3
Check the traffic policy configuration.
<R1>display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Marking:
        Remark DSCP 15
   Classifier: c2
    Operator: AND
     Behavior: b2
      Marking:
        Remark DSCP cs5
   Classifier: c3
    Operator: AND
     Behavior: b3
      Marking:
        Remark DSCP 50
```

3.1.4 Reference Configuration

3.1.4.1 Configurations of R1

```
#
sysname R1
#
undo info-center enable
#
vlan batch 20 30 40
#
traffic classifier c1 operator and
 if-match 8021p 2
traffic classifier c2 operator and
 if-match 8021p 5
traffic classifier c3 operator and
 if-match 8021p 6
#
traffic behavior b1
 remark dscp 15
traffic behavior b2
 remark dscp cs5
traffic behavior b3
 remark dscp 50
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
```

```
interface Vlanif1
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Vlanif40
 ip address 192.168.4.1 255.255.255.0
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p1 inbound
#
interface GigabitEthernet0/0/2
port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy p1 inbound
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 40
```

3.1.4.2 Configurations of R2

```
#
interface GigabitEthernet0/0/3
 ip address 192.168.4.2 255.255.255.0
#
ip route-static 192.168.2.0 255.255.255.0 192.168.4.1
ip route-static 192.168.3.0 255.255.255.0 192.168.4.1
```

3.1.4.3 Configurations of SW1

```
#
vlan batch 20
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
```

3.1.4.4 Configurations of SW2

```
#
vlan batch 30
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
```

3.2 Traffic Shaping Configuration

3.2.1 Introduction

3.2.1.1 About This Lab

Traffic shaping adjusts the rate of outgoing traffic to reduce traffic bursts so that outgoing packets can be transmitted at a stable rate. Traffic shaping uses a buffer and token buckets to control the traffic rate. When packets are sent at a high speed, the system buffers packets and then sends them evenly using token buckets.

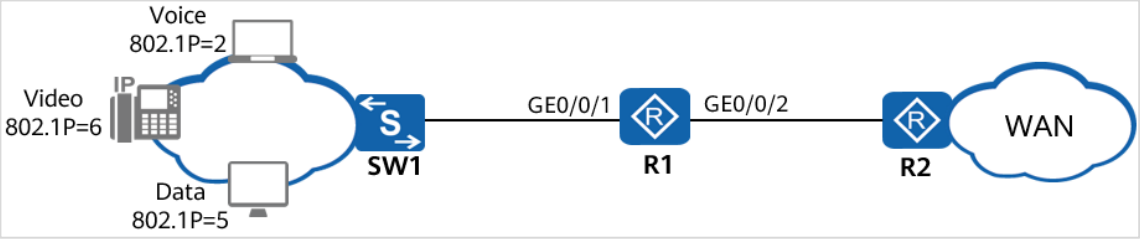
When the rate of an interface on a downstream device is slower than that of an interface on an upstream device or burst traffic occurs, traffic congestion may occur on the downstream device interface. Traffic shaping can be configured on the interface of an upstream device so that outgoing traffic is sent at even rates and congestion is avoided.

3.2.1.2 Objectives

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

- Configure interface-based traffic shaping.
- Configure queue-based traffic shaping.

3.2.1.3 Networking Topology



Voice, video, and data services on the LAN side of the enterprise network are connected to GE0/0/1 of R1 through SW1, and are connected to the WAN-side network through GE0/0/2 of R1.

Packets of different services are identified by 802.1p priorities on the LAN side. R1 sends packets to queues based on 802.1p priorities. When packets reach the WAN through GE0/0/2, bandwidth jitter may occur. To reduce bandwidth jitter and meet bandwidth requirements of various services, the following requirements must be met:

The CIR of the interface is 8000 kbit/s.

The CIR and CBS for the voice service are 256 kbit/s and 6400 bytes respectively.

The CIR and CBS for the video service are 4000 kbit/s and 100000 bytes respectively.

The CIR and CBS for the data service are 2000 kbit/s and 50000 bytes respectively.

3.2.2 Lab Configuration

3.2.2.1 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address for each interface on R1 so that enterprise users can access the WAN-side network through R1.
2. Configure an interface to trust 802.1p priorities in packets on R1.
3. Configure interface-based traffic shaping on R1 to limit the interface bandwidth.
4. Configure queue-based traffic shaping on R1 to limit the bandwidth of voice, video, and data services.

3.2.2.2 Configuration Procedure

Step 1 Perform basic device configurations.

Name switches and routers.

The configuration details are not provided.

Set the link type of the interface on SW1 connected to R1 to trunk and configure the interface to allow packets from VLAN 10 to pass through.

```
[SW]vlan 10
[SW-vlan10]q
[SW]interface GigabitEthernet 0/0/1
[SW-GigabitEthernet0/0/1]port link-type trunk
[SW-GigabitEthernet0/0/1]port trunk allow-pass vlan 10
```

Configure GE0/0/1 of R1 as a trunk interface, configure GE0/0/1 as a Layer 2 interface, and add it to VLAN 10.

```
[R1] vlan 10
[R1-vlan10] quit
[R1] interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]portswitch
[R1-GigabitEthernet0/0/1] port link-type trunk
[R1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[R1-GigabitEthernet0/0/1] quit
```

Create VLANIF 10 and set its IP address to 192.168.1.1/24. Set the IP address of GE0/0/2 to 192.168.4.1/24.

```
[R1 interface vlanif 10
[R1-Vlanif10] ip address 192.168.1.1 24
[R1-Vlanif10] quit
[R1] interface gigabitethernet 0/0/2
[R1-GigabitEthernet0/0/2] ip address 192.168.4.1 24
[R1-GigabitEthernet0/0/2] quit
```

Configure an IP address of an R2 interface and configure the default route to access the LAN.

```
[R2] interface gigabitethernet 0/0/2
[R2-GigabitEthernet0/0/2] ip address 192.168.4.2 24
[R2-GigabitEthernet0/0/2] quit
[R2]ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

Step 2 Specify the packet priority trusted on an interface.

Configure GE0/0/1 to trust 802.1p priorities of packets.

```
[R1] interface gigabitethernet 0/0/1
[R1-GigabitEthernet 0/0/1] trust 8021p
[R1-GigabitEthernet 0/0/1] quit
```

Step 3 Configure interface-based traffic shaping.

Configure traffic shaping on an interface of R1 and set the CIR to 8000 kbit/s.

```
[R1] interface gigabitethernet 0/0/2
[R1-GigabitEthernet0/0/2] qos gts cir 8000
[R1-GigabitEthernet0/0/2] quit
```

Step 4 Configure queue-based traffic shaping.

Create a queue profile named qp1 on R1, set the scheduling mode to WFQ for queues 0 to 5 and to PQ for queue 6 and queue 7. Set CIR values of queue 6, queue 5, and queue 2 to 256 kbit/s, 4000 kbit/s, and 2000 kbit/s. Set CBS values of queue 6, queue 5, and queue 2 to 6400 bytes, 10000 bytes, and 500000 bytes.

```
[R1] qos queue-profile qp1
[R1-qos-queue-profile-qp1] schedule pq 6 to 7 wfq 0 to 5
[R1-qos-queue-profile-qp1] queue 6 gts cir 256 cbs 6400
[R1-qos-queue-profile-qp1] queue 5 gts cir 4000 cbs 100000
[R1-qos-queue-profile-qp1] queue 2 gts cir 2000 cbs 50000
[R1-qos-queue-profile-qp1] quit
```

Apply the queue profile qp1 on GE0/0/2 of R1.

```
[R1] interface gigabitethernet 0/0/2
[R1-GigabitEthernet0/0/2] qos queue-profile qp1
```

----End

3.2.3 Verification

Check the configuration of the interface on RouterA.

```
[R1GigabitEthernet0/0/2] display this
#
interface GigabitEthernet0/0/2
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile qp1
 qos gts cir 8000
```

Check the queue profile applied to the interface.

```
[R1-GigabitEthernet0/0/2] quit
[R1] display qos queue-profile qp1
Queue-profile: qp1
Queue   Schedule   Weight   Length(Bytes/Packets) GTS(CIR/CBS)
------------------------------------------------------------------
0       WFQ        10                 -/-              -/-
1       WFQ        10                 -/-              -/-
2       WFQ        10                 -/-          2000/50000
3       WFQ        10                 -/-              -/-
4       WFQ        10                 -/-              -/-
5       WFQ        10                 -/-          4000/100000
6       PQ         -                 -/-           256/6400
7       PQ         -                 -/-              -/-
```

3.2.4 Reference Configuration

3.2.4.1 Configurations of R1

```
#
 sysname R1
#
vlan batch 10
#
qos queue-profile qp1
   queue 2 gts cir 2000 cbs 50000
   queue 5 gts cir 4000 cbs 100000
   queue 6 gts cir 256 cbs 6400
   schedule wfq 0 to 5 pq 6 to 7
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 trust 8021p
#
interface GigabitEthernet0/0/2
   ip address 192.168.4.1 255.255.255.0
```

```
 qos queue-profile qp1
 qos gts cir 8000
#
return
```

3.2.4.2 Configurations of R2

```
#
interface GigabitEthernet0/0/3
 ip address 192.168.4.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

3.2.4.3 Configurations of SW1

```
#
vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
```

3.3 Traffic Policing Configuration

3.3.1 Introduction

3.3.1.1 About This Lab

Traffic policing discards excess traffic to limit traffic within a proper range and to protect network resources and enterprise users' interests.

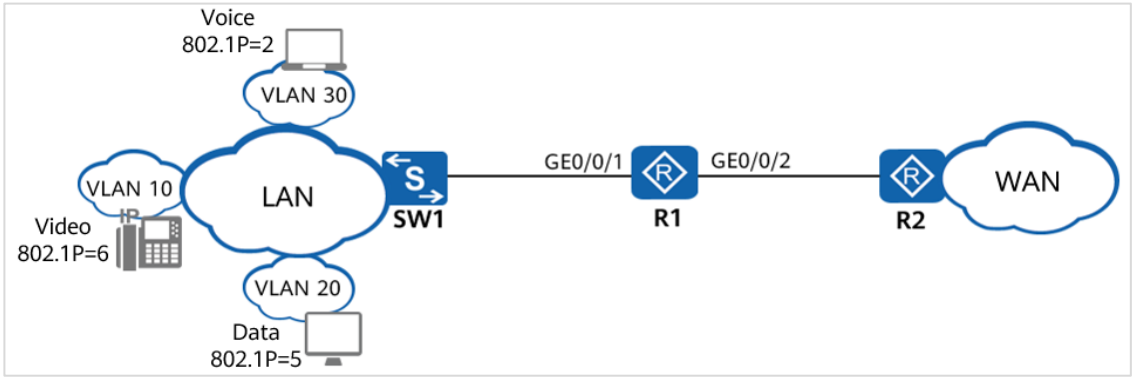
If the rate of a type of traffic exceeds the threshold, the device lowers the packet priority and then forwards the packets or directly discards the packets based on the traffic policing configuration. By default, such packets are discarded.

3.3.1.2 Objectives

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

- Configure a traffic policy and bind the configured traffic behaviors and traffic classifiers to the traffic policy.
- Configure interface-based traffic policing.

3.3.1.3 Networking Topology



Voice, video, and data services on the LAN side of the enterprise belong to VLAN 10, VLAN 20, and VLAN 30. The services are transmitted to GE0/0/1 on R1 through SW1, and are transmitted to the WAN-side network through GE0/0/2 on R1.

Flow-based traffic policing needs to be performed for different service packets on R1 so that the service traffic is limited within a proper range and bandwidth is ensured. Interface-based traffic policing needs to be performed for all incoming traffic on GE0/0/1 so that the total traffic of a single enterprise user is limited within a proper range.

3.3.2 Lab Configuration

3.3.2.1 Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces on R1 and configure interfaces so that enterprise users can access the WAN-side network through R1.
2. Configure traffic classifiers on R1 to classify packets based on VLAN IDs.
3. Configure traffic behaviors on R1 to perform traffic policing for different service flows from the enterprise.
4. Configure a traffic policy on R1, associate the traffic behaviors with traffic classifiers in the traffic policy, and apply the traffic policy to the inbound direction of the interface on R1 connected to SW1.
5. Configure interface-based traffic policing to the inbound direction of the interface on R1 connected to SW1 to limit the rate of all the packets.

3.3.2.2 Configuration Procedure

Step 1 Perform basic device configurations.

Name switches and routers.

The configuration details are not provided.

Set the link type of the interface on SW1 connected to R1 to trunk and configure the interface to allow packets from VLANs 10, 20, and 30 to pass through.

```
[SW]vlan batch 10 20 30
[SW]interface GigabitEthernet 0/0/1
[SW-GigabitEthernet0/0/1]port link-type trunk
[SW-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20 30
```

Configure GE0/0/1 of R1 as a trunk interface, configure GE0/0/1 as a Layer 2 interface, and add it to VLANs 10, 20, and 30.

```
[R1] vlan batch 10 20 30
[R1] interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]portswitch
[R1-GigabitEthernet0/0/1] port link-type trunk
[R1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 20 30
[R1-GigabitEthernet0/0/1] quit
```

Create VLANIF 10, VLANIF 20, and VLANIF 30, and set IP addresses of VLANIF 10, VLANIF 20, and VLANIF 30 to 192.168.1.1/24, 192.168.2.1/24, and 192.168.3.1/24, respectively. Set the IP address of GE0/0/2 to 192.168.4.1/24.

```
[R1 interface vlanif 10
[R1-Vlanif10] ip address 192.168.1.1 24
[R1-Vlanif10] quit
[R1 interface vlanif 20
[R1-Vlanif20] ip address 192.168.2.1 24
```

```
[R1-Vlanif20] quit
[R1 interface vlanif 30
[R1-Vlanif30] ip address 192.168.3.1 24
[R1-Vlanif30] quit
[R1] interface gigabitethernet 0/0/2
[R1-GigabitEthernet0/0/2] ip address 192.168.4.1 24
[R1-GigabitEthernet0/0/2] quit
```

Configure an IP address of an R2 interface and configure the default route to access the LAN.

```
[R2] interface gigabitethernet 0/0/2
[R2-GigabitEthernet0/0/2] ip address 192.168.4.2 24
[R2-GigabitEthernet0/0/2] quit
[R2]ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

Step 2 Configure traffic classifiers.

Configure traffic classifiers c1, c2, and c3 on R1 to match different service flows from the enterprise based on VLAN IDs.

```
[R1] traffic classifier c1
[R1-classifier-c1] if-match vlan-id 10
[R1-classifier-c1] quit
[R1] traffic classifier c2
[R1-classifier-c2] if-match vlan-id 20
[R1-classifier-c2] quit
[R1] traffic classifier c3
[R1-classifier-c3] if-match vlan-id 30
[R1-classifier-c3] quit
```

Step 3 Configure traffic behaviors.

Create traffic behaviors b1, b2, and b3 on R1 to perform traffic policing for different service flows from the enterprise.

```
[R1] traffic behavior b1
[R1-behavior-b1] car cir 256
[R1-behavior-b1] statistic enable
[R1-behavior-b1] quit
[R1] traffic behavior b2
[R1-behavior-b2] car cir 4000
[R1-behavior-b2] statistic enable
[R1-behavior-b2] quit
[R1] traffic behavior b3
[R1-behavior-b3] car cir 2000
[R1-behavior-b3] statistic enable
[R1-behavior-b3] quit
```

Step 4 Configure a traffic policy and apply it to an interface.

Create a traffic policy named p1 on R1, associate the traffic behaviors with traffic classifiers in the traffic policy, and apply the traffic policy to the inbound direction of GE0/0/1.

```
[R1] traffic policy p1
[R1-trafficpolicy-p1] classifier c1 behavior b1
[R1-trafficpolicy-p1] classifier c2 behavior b2
[R1-trafficpolicy-p1] classifier c3 behavior b3
[R1-trafficpolicy-p1] quit
[R1] interface gigabitethernet 0/0/1
[R1- GigabitEthernet0/0/1] traffic-policy p1 inbound
```

Step 5 Configure interface-based traffic policing.

Configure interface-based traffic policing in the inbound direction of GE0/0/1 on R1 to limit traffic of a single enterprise user within a proper range.

```
[R1-GigabitEthernet0/0/1] qos car inbound cir 10000
[R1-GigabitEthernet0/0/1] quit
```

----End

3.3.3 Verification

Check the traffic classifier configuration.

```
[R1] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: OR
    Rule(s) :
     if-match vlan-id 20
   Classifier: c3
    Operator: OR
    Rule(s) :
     if-match vlan-id 30
   Classifier: c1
    Operator: OR
    Rule(s) :
     if-match vlan-id 10
```

Check the traffic policy configuration.

```
[R1] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: OR
     Behavior: b1
      Committed Access Rate:
        CIR 256 (Kbps), PIR 0 (Kbps), CBS 48128 (byte), PBS 80128 (byte)
```

```
      Color Mode: color Blind
      Conform Action: pass
      Yellow   Action: pass
      Exceed   Action: discard
    statistic: enable
   Precedence: 5

 Classifier: c2
  Operator: OR
   Behavior: b2
    Committed Access Rate:
      CIR 4000 (Kbps), PIR 0 (Kbps), CBS 752000 (byte), PBS 1252000 (byte)
      Color Mode: color Blind
      Conform Action: pass
      Yellow   Action: pass
      Exceed   Action: discard
    statistic: enable
   Precedence: 10

 Classifier: c3
  Operator: OR
   Behavior: b3
    Committed Access Rate:
      CIR 2000 (Kbps), PIR 0 (Kbps), CBS 376000 (byte), PBS 626000 (byte)
      Color Mode: color Blind
      Conform Action: pass
      Yellow   Action: pass
      Exceed   Action: discard
    statistic: enable
   Precedence: 15
```

Check the traffic policy that is applied to the interface.

```
[R1] display traffic policy statistics interface GigabitEthernet0/0/1 inbound

  Interface: GigabitEthernet0/0/1
  Traffic policy inbound: p1
  Rule number: 3
  Current status: OK!
Item                    Sum(Packets/Bytes)          Rate(pps/bps)
-------------------------------------------------------------------------------
Matched                        0/0                         0/0
  Passed                       0/0                         0/0
  Dropped                      0/0                         0/0
    Filter                     0/0                         0/0
    CAR                        0/0                         0/0
  Queue Matched                0/0                         0/0
    Enqueued                   0/0                         0/0
    Discarded                  0/0                         0/0
  CAR                          0/0                         0/0
    Green packets              0/0                         0/0
    Yellow packets             0/0                         0/0
    Red packets                0/0                         0/0
```

3.3.4 Reference Configuration

3.3.4.1 Configurations of R1

```
#
 sysname R1
#
vlan batch 10 20 30
#
traffic classifier c1 operator or
 if-match vlan-id 10
traffic classifier c2 operator or
 if-match vlan-id 20
traffic classifier c3 operator or
 if-match vlan-id 30
#
traffic behavior b1
 car cir 256 cbs 48128 pbs 80128 green pass yellow pass red discard
 statistic enable
traffic behavior b2
 car cir 4000 cbs 752000 pbs 1252000 green pass yellow pass red discard
 statistic enable
traffic behavior b3
 car cir 2000 cbs 376000 pbs 626000 green pass yellow pass red discard
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1 precedence 5
 classifier c2 behavior b2 precedence 10
 classifier c3 behavior b3 precedence 15
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
 qos car inbound cir 10000
 traffic-policy p1 inbound
#
interface GigabitEthernet0/0/2
 ip address 192.168.4.1 255.255.255.0
#
return
```

3.3.4.2 Configurations of R2

```
#
interface GigabitEthernet0/0/3
 ip address 192.168.4.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

3.3.4.3 Configurations of SW1

```
#
vlan batch 10 20 30
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
```

3.4 Congestion Avoidance and Congestion Management Configuration

3.4.1 Introduction

3.4.1.1 About This Lab

Congestion avoidance is a flow control mechanism. A system configured with congestion avoidance monitors network resources such as queues and memory buffers. When congestion occurs or aggravates, the system discards packets. After congestion avoidance is configured, the device discards excess packets based on the configured drop profile to adjust network traffic and relieve network overload.

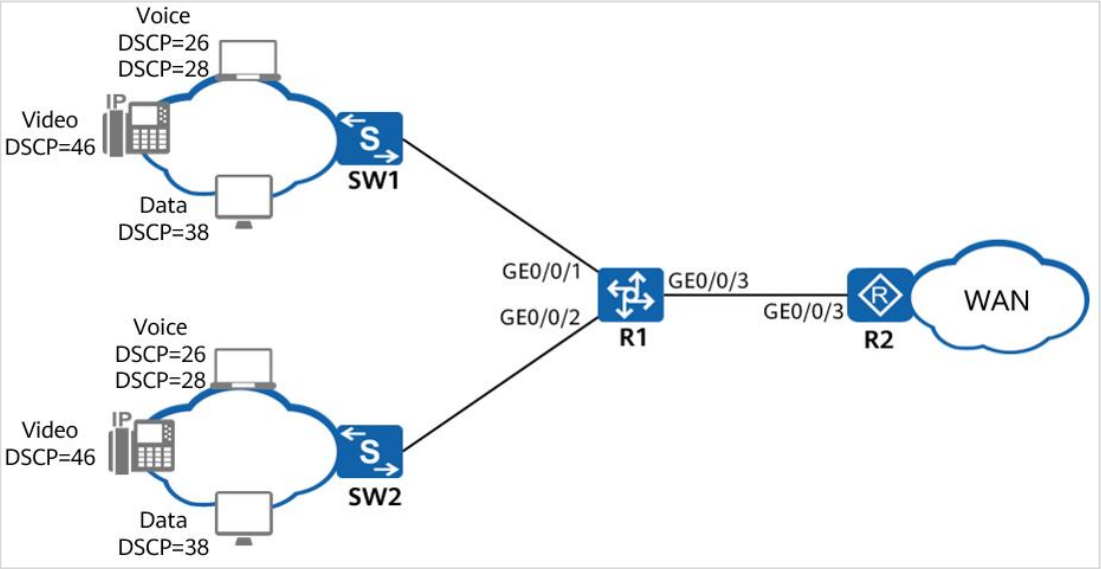
When a network is congested intermittently and delay-sensitive services require higher bandwidth than other services, congestion management adjusts the scheduling order of packets. When congestion occurs on a network, the device enabled with congestion management determines the packet forwarding sequence based on the configured scheduling policy to ensure that high-priority services are sent preferentially.

3.4.1.2 Objectives

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

- Configure an interface to trust the DSCP priority of packets.
- Configure the device to place packets with different priorities into different queues.
- Configure WRED parameters and drop policies based on DSCP priorities.
- Configure different scheduling policies for packets of different service types.
- Bind a drop profile to a queue profile and apply the drop profile to an interface.

3.4.1.3 Networking Topology



Voice, video, and data services on the LAN side of the enterprise network are connected to GE0/0/1 and GE0/0/2 of R1 through SW1 and SW2, and are connected to the WAN-side network through GE0/0/3 of R1.

SW1 and SW2 add different DSCP priorities to voice (EF), video (AF43), and data (AF32 abd AF31) packets. R1 sends the packets to queues based on the DSCP priorities of the packets, the rate of GE0/0/1 and GE0/0/2 on R1 is higher than that of GE0/0/3. Therefore, congestion may occur in the outbound direction of GE0/0/3. The enterprise requires that voice packets be sent first. For video and data packets, a lower priority indicates a lower chance of being sent, a lower bandwidth, and a higher probability of being discarded randomly. In this way, network traffic can be adjusted and the impact of congestion can be reduced.

3.4.2 Lab Configuration

3.4.2.1 Configuration Roadmap

Congestion management and congestion avoidance are used to relieve congestion. The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces and configure interfaces so that enterprise users can access the WAN-side network through R1.
2. On R1, configure the interface to trust DSCP priorities of packets so that packets with different priorities enter different queues.
3. Create a drop profile and set WRED parameters based on the DSCP priority, so packets with lower priorities have a higher drop probability.
4. Create a queue profile and configure PQ scheduling for voice packets and WFQ scheduling for video and data packets to ensure that voice packets are preferentially sent and video and data packets are scheduled based on priorities.
5. Bind the drop profile to the queue profile and apply the queue profile to the outbound direction of the interface connecting R1 to the WAN-side network to implement congestion avoidance and management.

3.4.2.2 Configuration Procedure

Step 1 Create VLANs and configure interfaces.

Create VLAN 20 and VLAN 30 on R1.

```
<Huawei> system-view
[Huawei] sysname R1
[R1] vlan batch 20 30
```

Configure GigabitEthernet0/0/1 and GigabitEthernet0/0/2 to trust DSCP priorities of packets, configure them as trunk interfaces, and add GigabitEthernet0/0/1 to VLAN 20 and GigabitEthernet0/0/2 to VLAN 30.

```
[R1] interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1] trust dscp
[R1-GigabitEthernet0/0/1] portswitch
[R1-GigabitEthernet 0/0/1] port link-type trunk
[R1-GigabitEthernet 0/0/1] port trunk allow-pass vlan 20
[R1-GigabitEthernet0/0/1] quit
[R1] interface GigabitEthernet0/0/2
[R1-GigabitEthernet 0/0/2] trust dscp
[R1-GigabitEthernet 0/0/2] portswitch
[R1-GigabitEthernet 0/0/2] port link-type trunk
[R1-GigabitEthernet 0/0/2] port trunk allow-pass vlan 30
[R1-GigabitEthernet 0/0/2] quit
```

Create VLANIF 20 and VLANIF 30, and set the IP address of VLANIF 20 to 192.168.2.1/24 and that of VLANIF 30 to 192.168.3.1/24.

```
[R1] interface vlanif 20
[R1-Vlanif20] ip address 192.168.2.1 24
[R1-Vlanif20] quit
[R1] interface vlanif 30
[R1-Vlanif30] ip address 192.168.3.1 24
[R1-Vlanif30] quit
```

Set the IP address of GigabitEthernet 0/0/3 to 192.168.4.1/24.

```
[R1] interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3] ip address 192.168.4.1 24
[R1-GigabitEthernet0/0/3] quit
```

Configure an IP address of an R2 interface and configure the default route to access the LAN.

```
[R2] interface gigabitethernet 0/0/2
[R2-GigabitEthernet0/0/2] ip address 192.168.4.2 24
[R2-GigabitEthernet0/0/2] quit
[R2]ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

Step 2 Create drop profiles.

Create drop profiles data and video on R1.

```
[R1] drop-profile data
[R1-drop-profile-data] wred dscp
[R1-drop-profile-data] dscp 28 low-limit 50 high-limit 70 discard-percentage 30
[R1-drop-profile-data] dscp 26 low-limit 40 high-limit 60 discard-percentage 40
[R1-drop-profile-data] quit
[R1] drop-profile video
[R1-drop-profile-video] wred dscp
[R1-drop-profile-video] dscp 38 low-limit 60 high-limit 80 discard-percentage 20
[R1-drop-profile-video] quit
```

Step 3 Create a queue profile.

Create a queue profile queue-profile1 on R1 and set the scheduling mode for each queue.

```
[R1] qos queue-profile queue-profile1
[R1-qos-queue-profile-queue-profile1] schedule pq 5 wfq 3 to 4
```

You can run the display qos map-table command to view the mapping between the DSCP priority and local priority on R1.

Packets enter queues based on the local priorities mapped to DSCP priorities.

Step 4 Apply the queue profile.

Bind drop profiles to the queue profile.

```
[R1-qos-queue-profile-queue-profile1] queue 4 drop-profile video
[R1-qos-queue-profile-queue-profile1] queue 3 drop-profile data
[R1-qos-queue-profile-queue-profile1] quit
```

Apply the queue profile to GigabitEthernet 0/0/3 of R1.

```
[R1] interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3] qos queue-profile queue-profile1
```

----End

3.4.3 Verification

Check the configuration of the interface on R1.

```
[R1-GigabitEthernet0/0/3] display this
#
interface GigabitEthernet0/0/3
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile queue-profile1
#
return
```

Check the queue profile applied to the interface.

```
[R1-GigabitEthernet0/0/3] quit
[R1] display qos queue-profile queue-profile1
Queue-profile: queue-profile1
Queue   Schedule   Weight   Length(Bytes/Packets) GTS(CIR/CBS)
------------------------------------------------------------------
3       WFQ        10                 -/-              -/-
4       WFQ        10                 -/-              -/-
5       PQ         -                  -/-              -/-
```

Check the drop profiles bound to the queue profile.

```
[R1] qos queue-profile queue-profile1
[R1-qos-queue-profile-queue-profile1] display this
```

```
#
qos queue-profile queue-profile1
  queue 3 drop-profile data
  queue 4 drop-profile video
  schedule wfq 3 to 4 pq 5
#
return
```

Check the drop profiles applied to the interface.

```
[R1-qos-queue-profile-queue-profile1] quit
[R1] display drop-profile video
Drop-profile[2]: video
DSCP                 Low-limit    High-limit   Discard-percentage
------------------------------------------------------------------
0(default)           30           100          10
1                    30           100          10
2                    30           100          10
3                    30           100          10
4                    30           100          10
5                    30           100          10
6                    30           100          10
7                    30           100          10
8(cs1)               30           100          10
9                    30           100          10
10(af11)             30           100          10
11                   30           100          10
12(af12)             30           100          10
13                   30           100          10
14(af13)             30           100          10
15                   30           100          10
16(cs2)              30           100          10
17                   30           100          10
18(af21)             30           100          10
19                   30           100          10
20(af22)             30           100          10
21                   30           100          10
22(af23)             30           100          10
23                   30           100          10
24(cs3)              30           100          10
25                   30           100          10
26(af31)             30           100          10
27                   30           100          10
28(af32)             30           100          10
29                   30           100          10
30(af33)             30           100          10
31                   30           100          10
32(cs4)              30           100          10
33                   30           100          10
34(af41)             30           100          10
35                   30           100          10
36(af42)             30           100          10
37                   30           100          10
38(af43)             60           80           20
39                   30           100          10
```

```
40(cs5)              30              100             10
41                   30              100             10
42                   30              100             10
43                   30              100             10
44                   30              100             10
45                   30              100             10
46(ef)               30              100             10
47                   30              100             10
48(cs6)              30              100             10
49                   30              100             10
50                   30              100             10
51                   30              100             10
52                   30              100             10
53                   30              100             10
54                   30              100             10
55                   30              100             10
56(cs7)              30              100             10
57                   30              100             10
58                   30              100             10
59                   30              100             10
60                   30              100             10
61                   30              100             10
62                   30              100             10
63                   30              100             10

[R1] display drop-profile data
Drop-profile[1]: data
DSCP                 Low-limit    High-limit   Discard-percentage
------------------------------------------------------------------
0(default)           30              100             10
1                    30              100             10
2                    30              100             10
3                    30              100             10
4                    30              100             10
5                    30              100             10
6                    30              100             10
7                    30              100             10
8(cs1)               30              100             10
9                    30              100             10
10(af11)             30              100             10
11                   30              100             10
12(af12)             30              100             10
13                   30              100             10
14(af13)             30              100             10
15                   30              100             10
16(cs2)              30              100             10
17                   30              100             10
18(af21)             30              100             10
19                   30              100             10
20(af22)             30              100             10
21                   30              100             10
22(af23)             30              100             10
23                   30              100             10
24(cs3)              30              100             10
25                   30              100             10
```

26(af31)	40	60	40
27	30	100	10
28(af32)	50	70	30
29	30	100	10
30(af33)	30	100	10
31	30	100	10
32(cs4)	30	100	10
33	30	100	10
34(af41)	30	100	10
35	30	100	10
36(af42)	30	100	10
37	30	100	10
38(af43)	60	80	20
39	30	100	10
40(cs5)	30	100	10
41	30	100	10
42	30	100	10
43	30	100	10
44	30	100	10
45	30	100	10
46(ef)	30	100	10
47	30	100	10
48(cs6)	30	100	10
49	30	100	10
50	30	100	10
51	30	100	10
52	30	100	10
53	30	100	10
54	30	100	10
55	30	100	10
56(cs7)	30	100	10
57	30	100	10
58	30	100	10
59	30	100	10
60	30	100	10
61	30	100	10
62	30	100	10
63	30	100	10

3.4.4 Reference Configuration

3.4.4.1 Configurations of R1

```
#
 sysname R1
#
vlan batch 20 30
#
drop-profile data
wred dscp
  dscp af31 low-limit 40 high-limit 60 discard-percentage 40
  dscp af32 low-limit 50 high-limit 70 discard-percentage 30
#
drop-profile video
```

```
wred dscp
  dscp af43 low-limit 60 high-limit 80 discard-percentage 20
#
qos queue-profile queue-profile1
  queue 3 drop-profile data
  queue 4 drop-profile video
  schedule wfq 3 to 4 pq 5
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 20
 trust dscp
#
interface GigabitEthernet0/0/2
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 30
 trust dscp
#
interface GigabitEthernet0/0/3
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile queue-profile1
#
return
```

3.4.4.2 Configurations of R2

```
#
interface GigabitEthernet0/0/3
 ip address 192.168.4.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
SW1's configuration
#
vlan batch 20
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
SW2's configuration
#
vlan batch 30
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
```

3.5 Lab 5: HQoS Configuration

3.5.1 Introduction

3.5.1.1 About This Lab

Traditional QoS schedules traffic based on interfaces. An interface can only differentiate service priorities. The traffic of the same priority uses the same interface queue and competes for the same queue resources. Therefore, traditional QoS is unable to provide differentiated services based on types of traffic and users.

As the number of users increases continuously and services develop, users require differentiated services to achieve better QoS. HQoS meets this requirement by implementing hierarchical scheduling based on multiple levels of queues, differentiating both services and users to provide refined QoS guarantee.

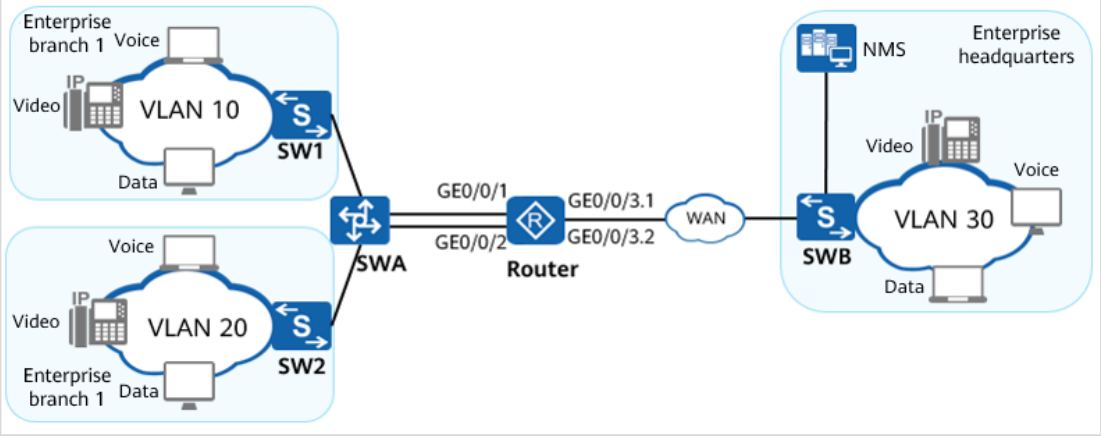
HQoS implements hierarchical scheduling based on queues. Currently, the device supports three levels of queues, that is, level-3 flow queue, level-2 subscriber queue, and level-1 port queue. The three-level queues are scheduled in a tree architecture, in which the flow queue is taken as the leaf node and the port queue as the root node. Packets on an interface are first sent to the leaf nodes and then sent out of the root node upon multi-level scheduling.

3.5.1.2 Objectives

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

- Configure a VLAN-based traffic policy.
- Configure the device to place packets in queues based on traffic classification.
- Configure a parent traffic policy and bind it to a child traffic policy.
- Configure traffic shaping for packets from different VLANs.
- Apply the parent traffic policy to an interface.

3.5.1.3 Networking Topology



Two departments of the enterprise branch belong to VLAN 10 and VLAN 20, and the enterprise headquarters belongs to VLAN 30. The enterprise branch connects to the router through the switch and connects to the headquarters through two sub-interfaces on GE0/0/3 of the router. Each department has voice, video, and data flows, and control packets from the NMS.

Packets are marked with different DSCP priorities by the switch, and the priorities of voice service, NMS control service, video service, and data service are ef, cs6, af11, and af11. Each department needs to have its CIR and share the maximum bandwidth of the interface. Voice packets need to be processed first with short delay, NMS control packets need to be processed first, and bandwidth of video and data packets needs to be ensured.

3.5.2 Lab Configuration

3.5.2.1 Configuration Roadmap

Configure traffic policy nesting to provide differentiated services for different services. The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces and configure interfaces so that enterprise users can access the WAN-side network through the router.
2. Configure child traffic policies for VLAN 10 and VLAN 20 on the router, configure traffic classifiers based on DSCP priorities to send voice packets to LLQ queues, NMS control packets to EF queues, and video and data packets to AF queues, and bind drop profiles.
3. Configure a traffic policy on the router, configure traffic classifiers based on VLAN IDs to shape packets from different VLANs, and bind the traffic policy to the child traffic policies.
4. Apply the traffic policy to the interface of the router connected to the WAN-side network to provide differentiated QoS services.

3.5.2.2 Configuration Procedure

Step 1 Create VLANs and configure interfaces.

Create VLAN 10 and VLAN 20 on the router.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

Configure GE0/0/1 as a trunk interface and add GE0/0/1 to VLAN 10.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] portswitch
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Router-GigabitEthernet0/0/1] quit
```

Configure GE0/0/2 as a trunk interface and add GE0/0/2 to VLAN 20.

```
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] portswitch
[Router-GigabitEthernet0/0/2] port link-type trunk
[Router-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[Router-GigabitEthernet0/0/2] quit
```

Configure the interface of the switch connected to the router as a trunk interface and add it to VLAN 10 and VLAN 20. The configuration details are not provided.

Create VLANIF 10 and VLANIF 20, and set the IP address of VLANIF 10 to 192.168.1.1/24 and that of VLANIF 20 to 192.168.2.1/24.

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 192.168.1.1 24
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 192.168.2.1 24
[Router-Vlanif20] quit
```

Configure IP address 192.168.3.1/24 for GE0/0/3.

```
[Router] interface gigabitethernet 0/0/3
[Router-GigabitEthernet0/0/3] ip address 192.168.3.1 24
[Router-GigabitEthernet0/0/3] quit
```

Configure the control VLAN of GE0/0/3.1 as VLAN 10, set the encapsulation mode to Dot1q, and assign 192.168.4.1/24 to it. Configure the control VLAN of GE0/0/3.2 as VLAN 20, set the encapsulation mode to Dot1q, and assign 192.168.5.1/24 to it.

```
[Router] interface gigabitethernet 0/0/3.1
[Router-GigabitEthernet0/0/3.1] ip address 192.168.4.1 24
[Router-GigabitEthernet0/0/3.1] dot1q termination vid 10
[Router-GigabitEthernet0/0/3.1] quit
[Router] interface gigabitethernet 0/0/3.2
[Router-GigabitEthernet0/0/3.2] ip address 192.168.5.1 24
[Router-GigabitEthernet0/0/3.2] dot1q termination vid 20
[Router-GigabitEthernet0/0/3.2] quit
```

Step 2 Configure child traffic policies bound to groupa and groupb.

Create traffic classifiers data, video, control, and voice on the router to classify different service flows from the enterprise based on DSCP priorities.

```
[Router] traffic classifier data
[Router-classifier-data] if-match dscp af11
[Router-classifier-data] quit
[Router] traffic classifier video
[Router-classifier-video] if-match dscp af21
[Router-classifier-video] quit
[Router] traffic classifier control
[Router-classifier-control] if-match dscp cs6
[Router-classifier-control] quit
[Router] traffic classifier voice
```

```
[Router-classifier-voice] if-match dscp ef
[Router-classifier-voice] quit
```

Create drop profiles data and video on the router.

```
[Router] drop-profile data
[Router-drop-profile-data] wred dscp
[Router-drop-profile-data] dscp 10 low-limit 70 high-limit 85 discard-percentage 60
[Router-drop-profile-data] quit
[Router] drop-profile video
[Router-drop-profile-video] wred dscp
[Router-drop-profile-video] dscp 18 low-limit 80 high-limit 95 discard-percentage 60
[Router-drop-profile-video] quit
```

Create traffic behaviors data, video, control, and voice on the router to achieve congestion management and congestion avoidance for different service flows of the enterprise.

```
[Router] traffic behavior data
[Router-behavior-data] queue af bandwidth pct 45
[Router-behavior-data] drop-profile data
[Router-behavior-data] quit
[Router] traffic behavior video
[Router-behavior-video] queue af bandwidth pct 30
[Router-behavior-video] drop-profile video
[Router-behavior-video] quit
[Router] traffic behavior control
[Router-behavior-control] queue ef bandwidth pct 5
[Router-behavior-control] quit
[Router] traffic behavior voice
[Router-behavior-voice] queue llq bandwidth pct 15
[Router-behavior-voice] quit
```

Define child traffic policies bound to groupa and groupb on the router.

```
[Router] traffic policy groupa-sub
[Router-trafficpolicy-groupa-sub] classifier voice behavior voice
[Router-trafficpolicy-groupa-sub] classifier control behavior control
[Router-trafficpolicy-groupa-sub] classifier video behavior video
[Router-trafficpolicy-groupa-sub] classifier data behavior data
[Router-trafficpolicy-groupa-sub] quit
[Router] traffic policy groupb-sub
[Router-trafficpolicy-groupb-sub] classifier voice behavior voice
[Router-trafficpolicy-groupb-sub] classifier control behavior control
[Router-trafficpolicy-groupb-sub] classifier video behavior video
[Router-trafficpolicy-groupb-sub] classifier data behavior data
[Router-trafficpolicy-groupb-sub] quit
```

Step 3 Configure parent traffic policies.

Configure traffic classifiers groupa and groupb on the router to classify different service flows from the enterprise based on the VLAN ID.

```
[Router] traffic classifier groupa
```

```
[Router-classifier-groupa] if-match vlan-id 10
[Router-classifier-groupa] quit
[Router] traffic classifier groupb
[Router-classifier-groupb] if-match vlan-id 20
[Router-classifier-groupb] quit
```

Create traffic behaviors groupa and groupb on the router to shape packets from different VLANs and bind them to child traffic policies.

```
[Router] traffic behavior groupa
[Router-behavior-groupa] gts cir 20000 cbs 500000 queue-length 50
[Router-behavior-groupa] traffic-policy groupa-sub
[Router-behavior-groupa] quit
[Router] traffic behavior groupb
[Router-behavior-groupb] gts cir 30000 cbs 750000 queue-length 50
[Router-behavior-groupb] traffic-policy groupb-sub
[Router-behavior-groupb] quit
```

Configure a parent traffic policy on the router.

```
[Router] traffic policy enterprise
[Router-trafficpolicy-enterprise] classifier groupa behavior groupa
[Router-trafficpolicy-enterprise] classifier groupb behavior groupb
[Router-trafficpolicy-enterprise] quit
```

Step 4 Apply the parent traffic policy.

Apply the parent traffic policy on GE0/0/3 of the router in the outbound direction.

```
[Router] interface gigabitethernet 0/0/3
[Router-GigabitEthernet0/0/3] traffic-policy enterprise outbound
```

----End

3.5.3 Verification

Check the configuration of the interface on the router.

```
[Router-GigabitEthernet3/0/0] display this
#
interface GigabitEthernet3/0/0
 ip address 192.168.3.1 255.255.255.0
 traffic-policy enterprise outbound
#
```

Check the configuration of the traffic policy applied to the interface.

```
[Router-GigabitEthernet3/0/0] quit
[Router] display traffic-policy applied-record enterprise
----------------------------------------------------
  Policy Name:     enterprise
  Policy Index:    2
      Classifier:groupa        Behavior:groupa        Precedence:5
```

```
      Classifier:groupb       Behavior:groupb       Precedence:10
------------------------------------------------
 *interface GigabitEthernet3/0/0
    traffic-policy enterprise outbound
      slot 3      :   success
      nest Policy :   groupa-sub
      slot 0      :   success
      nest Policy :   groupb-sub
      slot 0      :   success
   Classifier: groupa
    Operator: OR
    Rule(s) :
     if-match vlan-id 10
     Behavior: groupa
      General Traffic Shape:
        CIR 20000 (Kbps), CBS 500000 (byte)
        Queue length 50 (Packets)
      Nest Policy :   groupa-sub
       Classifier: voice
        Operator: OR
        Rule(s) :
         if-match dscp ef
         Behavior: voice
           Low-latency:
             Bandwidth 15 (%)
             Bandwidth 3000 (Kbps) CBS 75000 (Bytes)
       Classifier: control
        Operator: OR
        Rule(s) :
         if-match dscp cs6
         Behavior: control
           Expedited Forwarding:
             Bandwidth 5 (%)
             Bandwidth 1000 (Kbps) CBS 25000 (Bytes)
             Queue Length: 64 (Packets) 131072 (Bytes)
       Classifier: video
        Operator: OR
        Rule(s) :
         if-match dscp af21
         Behavior: video
           Assured Forwarding:
             Bandwidth 30 (%)
             Bandwidth 6000 (Kbps)
             Drop Method: WRED
             Drop-profile: video
       Classifier: data
        Operator: OR
        Rule(s) :
         if-match dscp af11
         Behavior: data
           Assured Forwarding:
             Bandwidth 45 (%)
             Bandwidth 9000 (Kbps)
             Drop Method: WRED
             Drop-profile: data
```

```
  Behavior: Be
    Assured Forwarding:
      Bandwidth 50000 (Kbps)
  Classifier: groupb
   Operator: OR
   Rule(s) :
    if-match vlan-id 20
    Behavior: groupb
     General Traffic Shape:
       CIR 30000 (Kbps), CBS 750000 (byte)
       Queue length 50 (Packets)
     Nest Policy :   groupa-sub
     Nest Policy :   groupb-sub
      Classifier: voice
       Operator: OR
       Rule(s) :
        if-match dscp ef
        Behavior: voice
          Low-latency:
            Bandwidth 15 (%)
            Bandwidth 4500 (Kbps) CBS 112500 (Bytes)
      Classifier: control
       Operator: OR
       Rule(s) :
        if-match dscp cs6
        Behavior: control
          Expedited Forwarding:
            Bandwidth 5 (%)
            Bandwidth 1500 (Kbps) CBS 37500 (Bytes)
            Queue Length: 64 (Packets) 131072 (Bytes)
      Classifier: video
       Operator: OR
       Rule(s) :
        if-match dscp af21
        Behavior: video
          Assured Forwarding:
            Bandwidth 30 (%)
            Bandwidth 9000 (Kbps)
            Drop Method: WRED
            Drop-profile: video
      Classifier: data
       Operator: OR
       Rule(s) :
        if-match dscp af11
        Behavior: data
          Assured Forwarding:
            Bandwidth 45 (%)
            Bandwidth 13500 (Kbps)
            Drop Method: WRED
            Drop-profile: data
  Behavior: Be
    Assured Forwarding:
      Bandwidth 50000 (Kbps)
-----------------------------------------------
  Policy total applied times: 1.
```

3.5.4 Reference Configuration

3.5.4.1 Configurations of Router

```
 sysname Router
#
vlan batch 10 20
#
drop-profile data
wred dscp
    dscp af11 low-limit 70 high-limit 85 discard-percentage 60
drop-profile video
wred dscp
   dscp af21 low-limit 80 high-limit 95 discard-percentage 60
#
traffic classifier control operator or
 if-match dscp cs6
traffic classifier groupb operator or
 if-match vlan-id 20
traffic classifier video operator or
 if-match dscp af21
traffic classifier groupa operator or
 if-match vlan-id 10
traffic classifier data operator or
 if-match dscp af11
traffic classifier voice operator or
 if-match dscp ef
#
traffic behavior control
 queue ef bandwidth pct 5
traffic behavior groupb
 gts cir 30000 cbs 750000 queue-length 50
 traffic-policy groupb-sub
traffic behavior video
 queue af bandwidth pct 30
 drop-profile video
traffic behavior groupa
 gts cir 20000 cbs 500000 queue-length 50
 traffic-policy groupa-sub
traffic behavior data
 queue af bandwidth pct 45
 drop-profile data
traffic behavior voice
 queue llq bandwidth pct 15
#
traffic policy groupa-sub
 classifier voice behavior voice precedence 5
 classifier control behavior control precedence 10
 classifier video behavior video precedence 15
 classifier data behavior data precedence 20
traffic policy enterprise
 classifier groupa behavior groupa precedence 5
 classifier groupb behavior groupb precedence 10
traffic policy groupb-sub
 classifier voice behavior voice precedence 5
```

```
 classifier control behavior control precedence 10
 classifier video behavior video precedence 15
 classifier data behavior data precedence 20
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
 ip address 192.168.3.1 255.255.255.0
 traffic-policy enterprise outbound
#
interface GigabitEthernet0/0/3.1
 dot1q termination vid 10
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet0/0/3.2
 dot1q termination vid 20
 ip address 192.168.5.1 255.255.255.0
#
return
```

3.5.5 Quiz

Each traffic behavior in a parent traffic policy can be bound to only one child traffic policy, whereas different traffic behaviors can be bound to different child traffic policies.

4 HA Technology Lab

4.1 VRRP Configuration

4.1.1 Introduction

4.1.1.1 About This Lab

Generally, all hosts on the same network segment are configured with the same default route with the gateway address as the next-hop address. The hosts use the default route to send packets to the gateway and the gateway forwards the packets to other network segments. When the gateway fails, hosts with the same default route cannot communicate with external networks. To improve network reliability, multiple egress gateways can be configured. However, route selection between the gateways becomes an issue.

The Virtual Router Redundancy Protocol (VRRP) groups multiple routing devices into a virtual router. The virtual IP address of the virtual router is used as the default gateway address for communication with an external network.

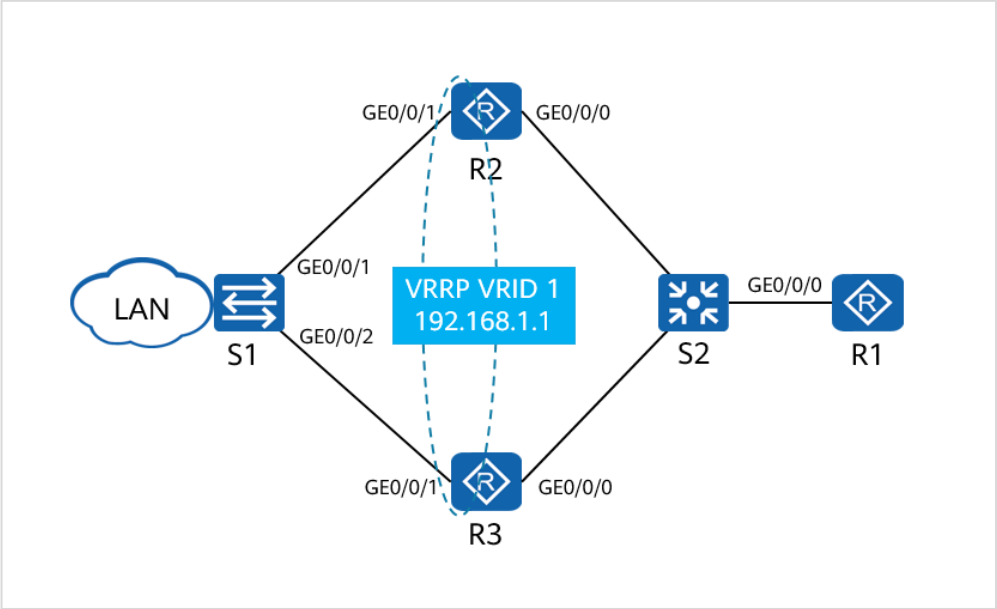
VRRP virtualizes multiple routing devices into a virtual router without changing the networking. The virtual router IP address is configured as the default gateway address. If a gateway fails, VRRP selects a different gateway to forward traffic, thereby ensuring reliable communication.

4.1.1.2 Objectives

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

- Configure VRRP groups and virtual IP addresses.
- Configure the VRRP priority.
- Verify the VRRP configuration.
- Associate VRRP with an uplink.
- Master the configuration of VRRP groups in load balancing mode.

4.1.1.3 Networking Topology



R1 functions as the gateway between the LAN and the external network and is connected to aggregation routers R2 and R3 through a switch. R2 and R3are connected to the same LAN through S1. VRRPv2 needs to be enabled on the interfaces connecting R2 and R3 to S1 to implement first-hop redundancy. R2 is the master device, and R3 is the backup device. No additional configuration is required on the switch. The switch only transparently forwards packets.

4.1.2 Lab Configuration

4.1.2.1 Configuration Roadmap

1. Configure IP addresses and routing protocols for different device interfaces to enable reachability at the network layer.
2. Create a VRRP group on R2 and R3. Configure R2 with a higher priority than R3, so R2 functions as the master device to transmit traffic and R3 serves as the backup device to provide backup.
3. Configure association between VRRP and GE0/0/0 on R2. When the link between R2 and R1 fails, the VRRP group can detect the fault and perform an active/standby VRRP switchover.
4. Create VRRP groups 1 and 2 on R2 and R3. Configure R2 as the master device and R3 as the backup device of VRRP group 1. Configure R3 as the master device and R2 as the backup device of VRRP group 2.

4.1.2.2 Configuration Procedure

Step 1 Perform basic network configuration.

Rename R1 and configure IP addresses for interfaces.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface loopback 0
[R1-LoopBack0]ip address 1.1.1.1 32
[R1-LoopBack0]quit
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 10.0.123.1 24
```

Rename R2 and configure IP addresses for interfaces.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 10.0.123.2 24
[R2-GigabitEthernet0/0/0]quit
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 192.168.1.2 24
```

Rename R3 and configure IP addresses for interfaces.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ip address 10.0.123.3 24
[R3-GigabitEthernet0/0/0]quit
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 192.168.1.3 24
```

Rename R4 and configure an IP address for an interface.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 192.168.1.4 24
```

Rename R5 and configure an IP address for an interface.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R5
[R5]interface GigabitEthernet 0/0/1
[R5-GigabitEthernet0/0/1]ip address 192.168.1.5 24
```

After the configuration is complete, test the connectivity between R1 and R2 and between R1 and R3. Here, R1 is used as an example.

```
[R1]ping 10.0.123.2
  PING 10.0.123.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.123.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.123.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.123.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.123.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.123.2: bytes=56 Sequence=5 ttl=255 time=1 ms

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

[R1]ping 10.0.123.3
  PING 10.0.123.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.123.3: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.123.3: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.123.3: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.123.3: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.123.3: bytes=56 Sequence=5 ttl=255 time=1 ms

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

Step 2 Configure OSPF and static routes.

Loopback0 of R1 and interfaces connecting R1, R2, and R3 run in OSPF area 0. The IP addresses of interfaces connecting R2 and R3 to S1 need to be advertised to OSPF, but no neighbor relationship is established. The silent mode is used in this case.

R4 and R5 simulate PCs and use default static routes to 192.168.1.1 (VRRP virtual IP address) on the network segment.

In this way, R1 can learn the route to the network segment 192.168.1.0, and R2 and R3 can learn the route to 1.1.1.1.

```
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.123.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0

[R2]ospf 1
[R2-ospf-1]silent-interface GigabitEthernet 0/0/1
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.123.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255

[R3]ospf 1
```

```
[R3-ospf-1]silent-interface GigabitEthernet 0/0/1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.123.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255

[R4]ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
[R5]ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
```

After the configuration is complete, check the routing table of each device. The following example uses routing tables of R1, R2, and R4.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

1.1.1.1/32          Direct  0    0           D   127.0.0.1       LoopBack0
10.0.123.0/24       Direct  0    0           D   10.0.123.1      GigabitEthernet0/0/0
10.0.123.1/32       Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
10.0.123.255/32     Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
127.0.0.0/8         Direct  0    0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
192.168.1.0/24      OSPF    10   2           D   10.0.123.3      GigabitEthernet0/0/0
                    OSPF    10   2           D   10.0.123.2      GigabitEthernet0/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12       Routes : 12

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  OSPF    10   1           D   10.0.123.1      GigabitEthernet0/0/0
        10.0.0.2/32 Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.123.0/24 Direct  0    0           D   10.0.123.2      GigabitEthernet0/0/0
      10.0.123.2/32 Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
    10.0.123.255/32 Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.2     GigabitEthernet0/0/1
    192.168.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[R4]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
```

```
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD  192.168.1.1     GigabitEthernet0/0/1
       10.0.0.4/32  Direct  0    0           D   127.0.0.1       LoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.4     GigabitEthernet0/0/1
    192.168.1.4/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

The preceding command output shows that R1 has learned the route to 192.168.1.0/24, R2 has learned the route to 1.1.1.1/32, and R4 has a default static route to 192.168.1.1.

Step 3 Configure a VRRP group and a virtual IP address.

Enable VRRP on the interfaces of R2 and R3 and configure the VRID and virtual IP address.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]vrrp vrid 1 virtual-ip 192.168.1.1
```

After a waiting period, if R2 detects that no other member exists in the VRRP group, it becomes the master.

```
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]vrrp vrid 1 virtual-ip 192.168.1.1
```

After the configuration is complete, check the VRRP status on R2 and R3.

```
[R2]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-22 18:00:03
Last change time : 2016-07-22 18:00:07

[R3]display vrrp
```

```
GigabitEthernet0/0/1 | Virtual Router 1
  State : Backup
  Virtual IP : 192.168.1.1
  Master IP : 192.168.1.2
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 100
  Preempt : YES     Delay Time : 0 s
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Create time : 2016-07-22 18:03:16
  Last change time : 2016-07-22 18:03:16
```

R2 is elected as the master router, and R3 is elected as the backup router. However, no priority is configured, and priorities of the master and backup devices are both 100. In this case, if R3 starts first, R3 becomes the master device, which is not the expected result.

Step 4 Configure the priority of the VRRP device and verify the active/standby switchover.

Configure VRRP priorities on R2 and R3. A larger value indicates a higher priority. Therefore, set the VRRP priority of R2 to 120 and that of R3 to 110.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]vrrp vrid 1 priority 120

[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]vrrp vrid 1 priority 110
```

Verify the configuration after priority change.

```
[R2]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
```

```
    Create time : 2016-07-22 18:00:03
    Last change time : 2016-07-22 18:00:07

[R3]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-22 18:03:16
    Last change time : 2016-07-22 18:03:16
```

The command output shows that the VRRP priority has been successfully changed. By default, VRRP preemption is enabled. If the priority of R3 is changed to a higher value, an active/standby switchover occurs.

Verify the connectivity between R4 and R1.

```
[R4]ping 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=254 time=57 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 1.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/12/57 ms
```

The command output shows that the virtual gateway works properly and can forward data from the LAN where R4 resides to R1. In normal cases, the master device forwards data. Therefore, traffic passes through R2. To verify the failover status, perform the ping function from R4 to R1 for a long time and disable the interface connecting R2 to S1.

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

During the active/standby switchover, R4 discards two data packets, but subsequent data packets are forwarded normally.

```
[R4]ping -c 1000 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=6 ttl=254 time=1 ms
    Request time out
    Request time out
    Reply from 1.1.1.1: bytes=56 Sequence=9 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=10 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=11 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=12 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=13 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=14 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=15 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=16 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=17 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=18 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=19 ttl=254 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=20 ttl=254 time=1 ms

  --- 1.1.1.1 ping statistics ---
    20 packet(s) transmitted
    18 packet(s) received
    10.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

R3 becomes the master due to the active/standby switchover.

```
[R3]display vrrp
 GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 110
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-22 18:03:16
    Last change time : 2016-07-22 18:29:41
```

Step 5 Associate VRRP with an uplink.

The active/standby VRRP switchover is implemented by listening to VRRP Advertisement packets. If the backup device cannot listen to packets sent by the master

device or its priority is higher than that of the master device, the backup device performs preemption. By default, the preemption delay is not set.

If the fault occurs on the uplink and no active/standby switchover is performed, all Internet access traffic cannot be forwarded after reaching R2. Therefore, VRRP is associated with an uplink. When the uplink is faulty, R2 automatically decreases its priority, and R3 performs preemption to switch traffic to the backup device and uplink for forwarding.

Before associating VRRP with an uplink, restore the link that is shut down.

Configure R2 to track the uplink interface and set the penalty value to 30. That is, when the link fails, the running priority of R2 changes to 90, which is lower than R3 (110).

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]undo shutdown
[R2-GigabitEthernet0/0/1]vrrp vrid 1 track interface GigabitEthernet 0/0/0 reduced 30
```

Check the association configuration.

```
[R2]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0     Priority reduced : 30
    IF state : UP
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 17:32:27 UTC-08:00
```

Perform the ping operation on R4 for a long time and shut down the uplink interface of R2.

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]shutdown

[R2]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
    PriorityRun : 90
    PriorityConfig : 120
    MasterPriority : 110
```

```
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0     Priority reduced : 30
    IF state : DOWN
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 19:57:46 UTC-08:00

[R3]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 110
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-25 17:20:00 UTC-08:00
    Last change time : 2016-07-25 19:56:24 UTC-08:00
```

Check the master/backup status of R3. R3 becomes the master, and Internet access traffic is successfully diverted to R3.

Restore the uplink of R2 and priority. The R2 preempts to be the master device again. (In this process, a large number of packets are lost on R4 because OSPF routes are not fast converged. For details about how to speed up route convergence, see the OSPF lab.)

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]undo shutdown

[R2]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
```

```
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Track IF : GigabitEthernet0/0/0      Priority reduced : 30
  IF state : UP
  Create time : 2016-07-25 17:14:56 UTC-08:00
  Last change time : 2016-07-25 20:04:40 UTC-08:00
```

Note: After the interface goes Up, the OSPF neighbor relationship needs to be re-established on the uplink interface of R2. If OSPF fast convergence is not configured, data cannot be forwarded for several seconds. Therefore, you are advised to set the preemption delay to be greater than the OSPF convergence time during revertive switching.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]vrrp vrid 1 preempt-mode timer delay 10
```

Check VRRP again and find that the preemption delay is set successfully.

```
[R2]display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 10 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0      Priority reduced : 30
    IF state : UP
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 20:04:40 UTC-08:00
```

Step 6 Configure load balancing among multiple VRRP groups.

In normal situations, all traffic is forwarded by the master device, and the backup device is in idle state.

To implement load balancing of dual gateways, you can configure multiple VRRP groups. Create VRRP group 1 on R2 and R3, and set the virtual IP address to 192.168.1.1, and configure R2 as the master device. Create VRRP group 2, set the virtual IP address to 192.168.1.254, and configure R3 as the master device. Set the default gateway address of R4 to 192.168.1.1 and that of R5 to 192.168.1.254. In this way, Internet access traffic of hosts on this network segment can be shared by the two gateways.

The configuration is as follows.

```
[R2]interface GigabitEthernet 0/0/1
```

```
[R2-GigabitEthernet0/0/1]vrrp vrid 2 virtual-ip 192.168.1.254
[R2-GigabitEthernet0/0/1]vrrp vrid 2 priority 110

[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]vrrp vrid 2 virtual-ip 192.168.1.254
[R3-GigabitEthernet0/0/1]vrrp vrid 2 priority 120
[R3-GigabitEthernet0/0/1]vrrp vrid 2 track interface GigabitEthernet0/0/0 reduced 30

[R5]undo ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
[R5]ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
```

Check the VRRP group status on R2 and R3.

```
<R2>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 10 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0     Priority reduced : 30
    IF state : UP
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 20:04:40 UTC-08:00

  GigabitEthernet0/0/1 | Virtual Router 2
    State : Backup
    Virtual IP : 192.168.1.254
    Master IP : 192.168.1.3
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-25 17:15:54 UTC-08:00
    Last change time : 2016-07-25 17:20:30 UTC-08:00

<R3>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
```

```
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.2
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-25 17:20:00 UTC-08:00
    Last change time : 2016-07-25 20:03:15 UTC-08:00

  GigabitEthernet0/0/1 | Virtual Router 2
    State : Master
    Virtual IP : 192.168.1.254
    Master IP : 192.168.1.3
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0     Priority reduced : 30
    IF state : UP
    Create time : 2016-07-25 17:20:14 UTC-08:00
    Last change time : 2016-07-25 17:20:23 UTC-08:00
```

Run the tracert command to check which gateway processes the data sent through the two default routes. The command output shows that the data sent from R4 is forwarded by the master device in VRRP group 1 and the data sent from R5 is forwarded by the master device in VRRP group 2.

Enable R1 to send ICMP Port Unreachable packets.

```
[R1]icmp port-unreachable send
<R4>tracert 1.1.1.1
 traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C t
o break
 1 192.168.1.2 80 ms  40 ms  40 ms
 2 10.0.123.1 100 ms  70 ms  70 ms

<R5>tracert 1.1.1.1
 traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C t
o break
 1 192.168.1.3 50 ms  30 ms  50 ms
 2 10.0.123.1 60 ms  90 ms  60 ms
```

Verify traffic switching after the uplink fails.

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]shutdown
<R4>tracert 1.1.1.1
 traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C t
o break
 1 192.168.1.3 50 ms  40 ms  50 ms
 2 10.0.123.1 70 ms  80 ms  50 ms

<R5>tracert 1.1.1.1
 traceroute to  1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C t
o break
 1 192.168.1.3 40 ms  50 ms  40 ms
 2 10.0.123.1 70 ms  100 ms  90 ms
```

----End

4.1.3 Verification

Check the status of the VRRP groups. You can find the master/backup status, VRRP priority, association between VRRP and an uplink interface, and load balancing configuration.

```
<R2>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
    PriorityRun : 90
    PriorityConfig : 120
    MasterPriority : 110
    Preempt : YES     Delay Time : 10 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0     Priority reduced : 30
    IF state : DOWN
    Create time : 2016-07-25 17:14:56 UTC-08:00
    Last change time : 2016-07-25 20:48:28 UTC-08:00

  GigabitEthernet0/0/1 | Virtual Router 2
    State : Backup
    Virtual IP : 192.168.1.254
    Master IP : 192.168.1.3
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
```

```
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-25 17:15:54 UTC-08:00
    Last change time : 2016-07-25 17:20:30 UTC-08:00

<R3>display vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 192.168.1.1
    Master IP : 192.168.1.3
    PriorityRun : 110
    PriorityConfig : 110
    MasterPriority : 110
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Create time : 2016-07-25 17:20:00 UTC-08:00
    Last change time : 2016-07-25 20:46:42 UTC-08:00

  GigabitEthernet0/0/1 | Virtual Router 2
    State : Master
    Virtual IP : 192.168.1.254
    Master IP : 192.168.1.3
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES     Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0102
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : GigabitEthernet0/0/0     Priority reduced : 30
    IF state : UP
    Create time : 2016-07-25 17:20:14 UTC-08:00
  Last change time : 2016-07-25 17:20:23 UTC-08:00
```

In normal situations, R2 and R3 work in load balancing mode. If R2 fails, R3 takes over all traffic from R2. The configuration of VRRP groups in load balancing mode is complete.

4.1.4 Reference Configuration

4.1.4.1 Configurations of R1

```
#
 sysname R1
#
interface GigabitEthernet0/0/0
 ip address 10.0.123.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.0.123.0 0.0.0.255
#
return
```

4.1.4.2 Configurations of R2

```
#
 sysname R2
#
interface GigabitEthernet0/0/0
 shutdown
 ip address 10.0.123.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 10
 vrrp vrid 1 track interface GigabitEthernet0/0/0 reduced 30
 vrrp vrid 2 virtual-ip 192.168.1.254
 vrrp vrid 2 priority 110
#
ospf 1
 silent-interface GigabitEthernet0/0/1
 area 0.0.0.0
  network 10.0.123.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
return
```

4.1.4.3 Configurations of R3

```
#
 sysname R3
#
interface GigabitEthernet0/0/0
 ip address 10.0.123.3 255.255.255.0
#
```

```
interface GigabitEthernet0/0/1
 ip address 192.168.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 110
 vrrp vrid 2 virtual-ip 192.168.1.254
 vrrp vrid 2 priority 120
 vrrp vrid 2 track interface GigabitEthernet0/0/0 reduced 30
#
ospf 1
 silent-interface GigabitEthernet0/0/1
 area 0.0.0.0
  network 10.0.123.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
return
```

4.1.4.4 Configurations of R4

```
#
 sysname R4
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.4 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
#
return
```

4.1.4.5 Configurations of R5

```
#
 sysname R5
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.5 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
return
```

4.1.5 Quiz

When VRRP tracks an uplink interface, how does VRRP detect a remote link fault instead of a directly connected interface or link fault?

4.2 BFD Configuration

4.2.1 Introduction

4.2.1.1 About This Lab

To minimize the impact of device faults on services and improve network reliability, a network device must be able to quickly detect faults when communicating with adjacent devices. Measures can then be taken to promptly rectify the faults to ensure service continuity. In practice, hardware detection is used to detect link faults. For example, Synchronous Digital Hierarchy (SDH) alarms are used to report link faults. However, not all media can provide the hardware detection mechanism. In this case, applications use the Hello mechanism of the upper-layer routing protocol to detect faults. The duration of such detection is more than 1 second, which is too long for some applications. If no routing protocol is deployed on a small-scale Layer 3 network, the Hello mechanism cannot be used.

BFD is a unified detection mechanism used to quickly detect link faults and monitor IP connectivity.

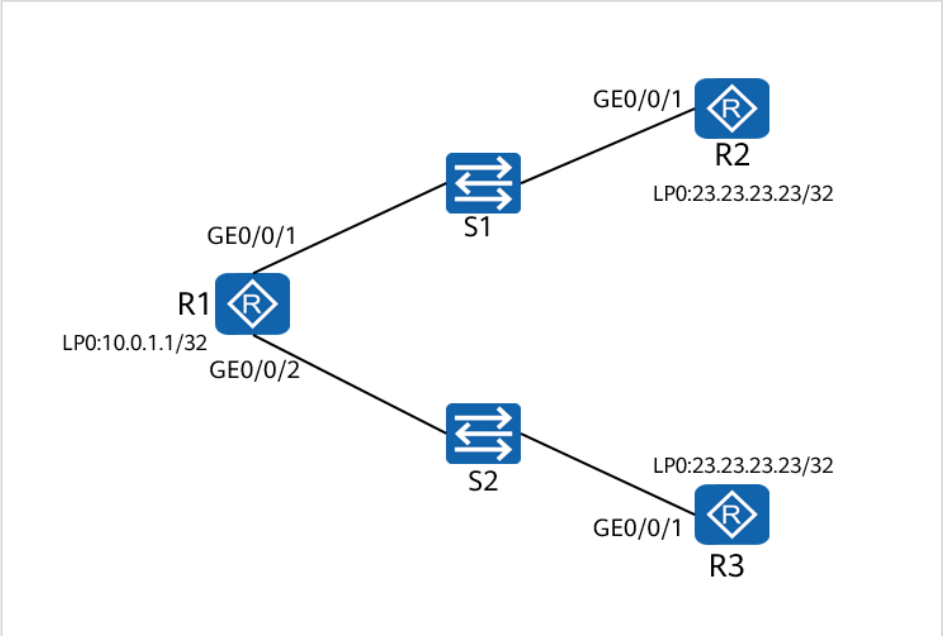
BFD provides a universal, standardized, media-independent, and protocol-independent fast failure detection mechanism. It has the following advantages: Provides low-overhead, short-duration detection of faults in the path between adjacent forwarding engines. The detected faults may occur on interfaces, data links, or forwarding engines. Performs uniform detection for all media and protocol layers in real time.

4.2.1.2 Objectives

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

- Create a BFD session.
- Associate BFD sessions with static routes.
- Understand the detection and switchover mechanism of BFD when an indirect link is faulty.

4.2.1.3 Networking Topology



R1 is connected to R2 and R3 through S1 and S2. R1 and R2 communicate with each other through static routes and traffic can reach the target network 23.23.23.23/32 through R2 or R3. R2 is the active next hop, and R3 is the standby next hop. The interface status does not affect the validity of the static route because the link is not a direct link. In this case, BFD is used for detection. When the detection fails, the standby static route is used for data forwarding.

4.2.2 Lab Configuration

4.2.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces to ensure network connectivity.
2. Create a BFD session.
3. Associate BFD with static routes.

4.2.2.2 Configuration Procedure

Step 1 Configure network IP addresses and perform basic configuration.

Configure IP addresses for interfaces on R1 and check the configuration.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.12.1 24
[R1-GigabitEthernet0/0/1]quit
```

```
[R1]interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2]ip address 10.0.13.1 24
[R1-GigabitEthernet0/0/2]quit
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 10.0.1.1 32

[R1]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
---

Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              unassigned           up         down
GigabitEthernet0/0/1               10.0.12.1/24        up         up
GigabitEthernet0/0/2               10.0.13.1/24        up         up
GigabitEthernet0/0/3               unassigned          up         down
LoopBack0                          10.0.1.1/32         up         up(s)
```

Configure IP addresses for interfaces on R2 and check the configuration.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/1]quit
[R2]interface LoopBack 0
[R2-LoopBack0]ip address 23.23.23.23 32
[R2-LoopBack0]quit

[R2]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
---

Interface                         IP Address/Mask      Physical   Protocol
---
GigabitEthernet0/0/0              unassigned           up         down
GigabitEthernet0/0/1              10.0.12.2/24         up         up
GigabitEthernet0/0/2              unassigned           up         down
GigabitEthernet0/0/3              unassigned           up         down
LoopBack0                         23.23.23.23/32       up         up(s)
----
```

Configure IP addresses for interfaces on R3 and check the configuration.

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

```
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.13.2 24
[R3-GigabitEthernet0/0/2]quit
[R3]interface LoopBack 0
[R3-LoopBack0]ip address 23.23.23.23 32
[R3-LoopBack0]quit

[R3]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
---

Interface                         IP Address/Mask      Physical   Protocol
---
GigabitEthernet0/0/0              unassigned           up         down
GigabitEthernet0/0/1              unassigned           up         down
GigabitEthernet0/0/2              10.0.13.2/24         up         up
GigabitEthernet0/0/3              unassigned           up         down
LoopBack0                         23.23.23.23/32       up         up(s)
---
```

Check the connectivity between R1 and R2 and between R1 and R3.

```
[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=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=1 ms

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

[R1]ping 10.0.13.2
  PING 10.0.13.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.13.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.13.2: bytes=56 Sequence=5 ttl=255 time=1 ms

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

Step 2 Configure BFD.

Enable BFD on the active path to detect the link between R1 and R2.

```
[R1]bfd
[R1-bfd]quit
[R1]bfd 1 bind peer-ip 10.0.12.2 source-ip 10.0.12.1 auto
[R1-bfd-session-1]commit
[R1-bfd-session-1]quit

[R2]bfd
[R2-bfd]quit
[R2]bfd 1 bind peer-ip 10.0.12.1 source-ip 10.0.12.2 auto
[R2-bfd-session-1]commit
[R2-bfd-session-1]quit
```

Check BFD session information.

```
[R1]display bfd session all
--------------------------------------------------------------------------------
Local Remote      PeerIpAddr      State     Type            InterfaceName
--------------------------------------------------------------------------------
8192  8192        10.0.12.2       Up        S_AUTO_PEER     -
--------------------------------------------------------------------------------
      Total UP/DOWN Session Number : 1/0


[R2]display bfd session all
--------------------------------------------------------------------------------
Local Remote      PeerIpAddr      State     Type            InterfaceName
--------------------------------------------------------------------------------
8192  8192        10.0.12.1       Up        S_AUTO_PEER     -
--------------------------------------------------------------------------------
      Total UP/DOWN Session Number : 1/0
```

Step 3 Associate BFD with static routes.

Configure static routes to the loopback interfaces of R1 on R2 and R3.

```
[R2]ip route-static 10.0.0.0 8 10.0.12.1

[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.0.0/8  Static  60   0           RD  10.0.12.1       GigabitEthernet0/0/1
       10.0.12.0/24 Direct  0    0           D   10.0.12.2       GigabitEthernet0/0/1
       10.0.12.2/32 Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
  10.0.12.255/32    Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
  23.23.23.23/32    Direct  0    0           D   127.0.0.1       LoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
```

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

[R3]ip route-static 10.0.0.0 8 10.0.13.1

[R3]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.0.0/8     Static  60   0           RD  10.0.13.1       GigabitEthernet0/0/2
       10.0.13.0/24    Direct  0    0           D   10.0.13.2       GigabitEthernet0/0/2
       10.0.13.2/32    Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
     10.0.13.255/32    Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
     23.23.23.23/32    Direct  0    0           D   127.0.0.1       LoopBack0
      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
```

Configure two static routes on R1 and associate them with BFD.

```
[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.12.2 track bfd-session 1
[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.13.2 preference 100
```

The preference of the route to R3 is 100, which is lower than the preference of the route to R2 (60). The routing table is as follows.

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

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0      Static  60   0           RD  10.0.12.2       GigabitEthernet0/0/1
       10.0.1.1/32     Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.12.0/24     Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/1
      10.0.12.1/32     Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
    10.0.12.255/32     Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      10.0.13.0/24     Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/2
      10.0.13.1/32     Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
    10.0.13.255/32     Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
      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

[R1]display ip routing-table 0.0.0.0 0.0.0.0 verbose
```

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 2

Destination: 0.0.0.0/0
       Protocol: Static              Process ID: 0
     Preference: 60                        Cost: 0
        NextHop: 10.0.12.2           Neighbour: 0.0.0.0
          State: Active Adv Relied         Age: 00h01m19s
            Tag: 0                    Priority: medium
          Label: NULL                   QoSInfo: 0x0
    IndirectID: 0x80000001
  RelayNextHop: 0.0.0.0               Interface: GigabitEthernet0/0/1
       TunnelID: 0x0                        Flags: RD

Destination: 0.0.0.0/0
       Protocol: Static              Process ID: 0
     Preference: 100                       Cost: 0
        NextHop: 10.0.13.2           Neighbour: 0.0.0.0
          State: Inactive Adv Relied       Age: 00h01m03s
            Tag: 0                    Priority: medium
          Label: NULL                   QoSInfo: 0x0
    IndirectID: 0x80000002
  RelayNextHop: 0.0.0.0               Interface: GigabitEthernet0/0/2
       TunnelID: 0x0                        Flags: R
```

Check the connectivity in normal state.

```
[R1]ping -a 10.0.1.1 23.23.23.23
  PING 23.23.23.23: 56  data bytes, press CTRL_C to break
    Reply from 23.23.23.23: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 23.23.23.23: bytes=56 Sequence=5 ttl=255 time=1 ms

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

Perform the ping operation on R1 for a long time and shut down the interface of R2.

```
[R1]ping -c 100 23.23.23.23

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

Check the ping result on R1.

```
[R1]ping -c 100 23.23.23.23
  PING 23.23.23.23: 56  data bytes, press CTRL_C to break
    Reply from 23.23.23.23: bytes=56 Sequence=1 ttl=255 time=1 ms
```

```
Reply from 23.23.23.23: bytes=56 Sequence=2 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=4 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=5 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=6 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=7 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=8 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=9 ttl=255 time=1 ms
Request time out
Request time out
Reply from 23.23.23.23: bytes=56 Sequence=12 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=13 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=14 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=15 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=16 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=17 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=18 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=19 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=20 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=21 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=22 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=23 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=24 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=25 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=26 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=27 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=28 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=29 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=30 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=31 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=32 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=33 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=34 ttl=255 time=1 ms
Reply from 23.23.23.23: bytes=56 Sequence=35 ttl=255 time=1 ms

--- 23.23.23.23 ping statistics ---
  35 packet(s) transmitted
  33 packet(s) received
  5.71% packet loss
  round-trip min/avg/max = 1/1/1 ms
```

Check the BFD session.

```
[R1]display bfd session all
--------------------------------------------------------------------------------
Local Remote      PeerIpAddr      State     Type            InterfaceName
--------------------------------------------------------------------------------
8192  0           10.0.12.2       Down      S_AUTO_PEER     -
--------------------------------------------------------------------------------
      Total UP/DOWN Session Number : 0/1
```

----End

4.2.3 Verification

Check routing information on R1.

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

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  100  0           RD  10.0.13.2       GigabitEthernet0/0/2
        10.0.1.1/32 Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.12.0/24 Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/1
       10.0.12.1/32 Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
     10.0.12.255/32 Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
       10.0.13.0/24 Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/2
       10.0.13.1/32 Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
     10.0.13.255/32 Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/2
        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

[R1]display ip routing-table 0.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 2

Destination: 0.0.0.0/0
    Protocol: Static              Process ID: 0
  Preference: 60                      Cost: 0
     NextHop: 10.0.12.2           Neighbour: 0.0.0.0
       State: Invalid Adv Relied       Age: 00h05m27s
         Tag: 0                    Priority: medium
       Label: NULL                 QoSInfo: 0x0
  IndirectID: 0x80000001
RelayNextHop: 0.0.0.0             Interface: GigabitEthernet0/0/1
    TunnelID: 0x0                       Flags: R

Destination: 0.0.0.0/0
    Protocol: Static              Process ID: 0
  Preference: 100                     Cost: 0
     NextHop: 10.0.13.2           Neighbour: 0.0.0.0
       State: Active Adv Relied        Age: 00h05m11s
         Tag: 0                    Priority: medium
       Label: NULL                 QoSInfo: 0x0
  IndirectID: 0x80000002
RelayNextHop: 0.0.0.0             Interface: GigabitEthernet0/0/2
    TunnelID: 0x0                       Flags: RD
```

If BFD is not configured, R1 does not have any mechanism to determine whether the static route is valid. Therefore, BFD is important in this scenario.

4.2.4 Reference Configuration

4.2.4.1 Configurations of R1

```
#
 sysname R1
#
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.0.13.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
bfd 1 bind peer-ip 10.0.12.2 source-ip 10.0.12.1 auto
 commit
#
ip route-static 0.0.0.0 0.0.0.0 10.0.12.2 track bfd-session 1
ip route-static 0.0.0.0 0.0.0.0 10.0.13.2 preference 100
#
return
```

4.2.4.2 Configurations of R2

```
#
 sysname R2
#
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.0.12.2 255.255.255.0
#
interface LoopBack0
 ip address 23.23.23.23 255.255.255.255
#
bfd 1 bind peer-ip 10.0.12.1 source-ip 10.0.12.2 auto
 commit
#
ip route-static 10.0.0.0 255.0.0.0 10.0.12.1
#
return
```

4.2.4.3 Configurations of R3

```
#
interface GigabitEthernet0/0/2
 ip address 10.0.13.2 255.255.255.0
#
interface LoopBack0
 ip address 23.23.23.23 255.255.255.255
```

```
#
ip route-static 10.0.0.0 255.0.0.0 10.0.13.1
#
return
```

4.2.5 Quiz

When BFD is associated with VRRP or a dynamic routing protocol such as OSPF, which scenarios can BFD be applied to in addition to speeding up network convergence?

4.3 NQA Configuration

4.3.1 Introduction

4.3.1.1 About This Lab

Network Quality Analysis (NQA) is a technology to measure network performance in real time and collect statistics on network information, such as the delay, jitter, and packet loss ratio. NQA monitors network quality of service (QoS) indicators in real time, and effectively diagnoses and locate network faults.

Additionally, NQA measures the performance of different protocols running on the network. This facilitates real-time collection of network performance counters, such as the total HTTP connection delay, TCP connection delay, DNS resolution delay, file transfer rate, FTP connection delay, and DNS resolution error rate.

NQA involves constructing, starting, and processing a test instance. After a test instance is started, data information about the running status of related protocols can be provided based on the returned packets. The system time when the test packet is sent is used as the sending time of test packets. The packet is marked with a timestamp and then sent to the server. After receiving the packet, the server sends a response packet to the client. After receiving the packet, the client reads the system time again and adds a timestamp to the packet. The RTT of the packet is calculated based on the time when the packet is sent and received.

In a jitter test instance, both the client and server add a timestamp to the sent and received packets based on the local system time. In this manner, the client can calculate the jitter value.

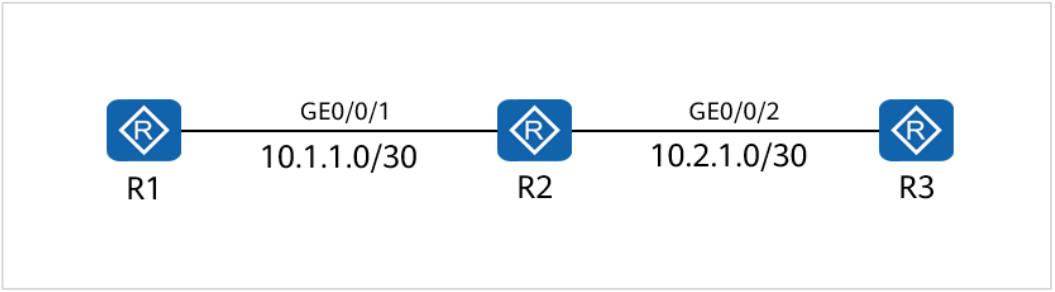
In this lab, you can configure NQA TCP/UDP/ICMP test instances to analyze how to use NQA.

4.3.1.2 Objectives

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

- Configure an NQA TCP test instance to measure the time taken to set up a TCP connection between an NQA client and a TCP server through three-way handshake.
- Configure an NQA UDP test instance to measure the response speed of connecting to a specified port.
- Configure an NQA ICMP test instance to check network connectivity.

4.3.1.3 Networking Topology



R1, R2, and R3 are configured with static routes to ensure network connectivity.

R1 is configured as the NQA client and an NQA ICMP test instance is used to test whether R3 is reachable.

An NQA TCP test instance is configured to measure the TCP connection setup time between R1 and R3.

An NQA UDP test instance is used to obtain the RTT of a UDP packet transmitted between R1 and R3.

4.3.2 Lab Configuration

4.3.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces to ensure network connectivity.
2. Configure an NQA ICMP test instance to detect and analyze network connectivity.
3. Configure an NQA TCP test instance to measure the time taken to set up a TCP connection between the NQA client and server.
4. Configure an NQA UDP test instance to measure the RTT of UDP packets between the NQA client and server.

4.3.2.2 Configuration Procedure

Step 1 Configure IP addresses and routes to implement connectivity.

Configure an IP address for an interface on R1 and a static route to R3.

```
<Huawei> system-view
[Huawei] sysname R1
[R1] interface gigabitethernet 0/0/1
[R1-GigabitEthernet0/0/1] ip address 10.1.1.1 30
[R1-GigabitEthernet0/0/1] quit
[R1] ip route-static 10.2.1.0 255.255.255.252 10.1.1.2
```

Configure IP addresses for interfaces on R2.

```
<Huawei> system-view
[Huawei] sysname R2
```

```
[R2] interface gigabitethernet 0/0/1
[R2-GigabitEthernet0/0/1] ip address 10.1.1.2 30
[R2-GigabitEthernet0/0/1] interface gigabitethernet 0/0/2
[R2-GigabitEthernet0/0/2] ip address 10.2.1.1 30
```

Configure an IP address for an interface on R3 and a static route to R1.

```
<Huawei> system-view
[Huawei] sysname R3
[R3] interface gigabitethernet 0/0/2
[R3-GigabitEthernet0/0/2] ip address 10.2.1.2 30
[R3-GigabitEthernet0/0/2] quit
[R3] ip route-static 10.1.1.0 255.255.255.252 10.2.1.1
```

Check network connectivity.

```
[R1]ping 10.2.1.2
  PING 10.2.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.2.1.2: bytes=56 Sequence=1 ttl=254 time=70 ms
    Reply from 10.2.1.2: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 10.2.1.2: bytes=56 Sequence=3 ttl=254 time=20 ms
    Reply from 10.2.1.2: bytes=56 Sequence=4 ttl=254 time=20 ms
    Reply from 10.2.1.2: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 10.2.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/36/70 ms
```

Step 2 Enable the NQA client and create an NQA ICMP test instance.

```
[R1] nqa test-instance admin icmp
[R1-nqa-admin-icmp] test-type icmp
[R1-nqa-admin-icmp] destination-address ipv4 10.1.1.2
```

Step 3 Configure the NQA server on R3.

Configure an IP address and a port number for listening to TCP connection requests.

Configure an IP address and a port number for listening to UDP connection requests.

```
<R3> system-view
[R3] nqa-server tcpconnect 10.2.1.2 9000
[R3] nqa-server udpecho 10.2.1.2 6000
```

Step 4 Configure the NQA client on R1.

Enable the NQA client and create an NQA TCP test instance.

```
[R1] nqa test-instance admin tcp
[R1-nqa-admin-tcp] test-type tcp
```

```
[R1-nqa-admin-tcp] destination-address ipv4 10.2.1.2
[R1-nqa-admin-tcp] destination-port 9000
```

Enable the NQA client and create an NQA UDP test instance.

```
[R1] nqa test-instance admin udp
[R1-nqa-admin-udp] test-type udp
[R1-nqa-admin-udp] destination-address ipv4 10.2.1.2
[R1-nqa-admin-udp] destination-port 6000
```

Step 5 Start the test instance.

```
[R1-nqa-admin-icmp] start now
[R1-nqa-admin-tcp] start now
[R1-nqa-admin-udp] start now
```

----End

4.3.3 Verification

Check the NQA ICMP test instance result.

```
[R1-nqa-admin-icmp]display nqa results test-instance admin icmp

 NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
  1 . Test 1 result   The test is finished
    Send operation times: 3                Receive response times: 2
    Completion:success                     RTD OverThresholds number: 0
    Attempts number:1                      Drop operation number:0
    Disconnect operation number:0          Operation timeout number:1
    System busy operation number:0         Connection fail number:0
    Operation sequence errors number:0     RTT Status errors number:0
    Destination ip address:10.2.1.2
    Min/Max/Average Completion Time: 20/30/25
    Sum/Square-Sum   Completion Time: 50/1300
    Last Good Probe Time: 2020-06-28 14:19:45.4
    Lost packet ratio: 33 %
```

Check the NQA TCP test instance result.

```
[R1-nqa-admin-tcp]display nqa results test-instance admin tcp

 NQA entry(admin, tcp) :testflag is inactive ,testtype is tcp
  1 . Test 1 result   The test is finished
    Send operation times: 3                Receive response times: 3
    Completion:success                     RTD OverThresholds number: 0
    Attempts number:1                      Drop operation number:0
    Disconnect operation number:0          Operation timeout number:0
    System busy operation number:0         Connection fail number:0
    Operation sequence errors number:0     RTT Status errors number:0
    Destination ip address:10.2.1.2
    Min/Max/Average Completion Time: 20/70/40
    Sum/Square-Sum   Completion Time: 120/6200
```

```
  Last Good Probe Time: 2020-06-28 14:21:57.9
  Lost packet ratio: 0 %
```

Check the NQA UDP test instance result.

```
[R1-nqa-admin-udp]display nqa results test-instance admin udp

 NQA entry(admin, udp) :testflag is inactive ,testtype is udp
  1 . Test 1 result   The test is finished
   Send operation times: 3                Receive response times: 3
   Completion:success                     RTD OverThresholds number: 0
   Attempts number:1                      Drop operation number:0
   Disconnect operation number:0          Operation timeout number:0
   System busy operation number:0         Connection fail number:0
   Operation sequence errors number:0     RTT Status errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 20/40/26
   Sum/Square-Sum  Completion Time: 80/2400
   Last Good Probe Time: 2020-06-28 14:24:29.1
   Lost packet ratio: 0 %
```

4.3.4 Reference Configuration

4.3.4.1 Configurations of R1

```
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.252
#
ip route-static 10.2.1.0 255.255.255.252 10.1.1.2
#
nqa test-instance admin tcp
 test-type tcp
 destination-address ipv4 10.2.1.2
 destination-port 9000
nqa test-instance admin udp
 test-type udp
 destination-address ipv4 10.2.1.2
 destination-port 6000
nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 10.2.1.2
#
return
```

4.3.4.2 Configurations of R2

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

```
 ip address 10.1.1.2 255.255.255.252
#
interface GigabitEthernet0/0/2
 ip address 10.2.1.1 255.255.255.252
```

4.3.4.3 Configurations of R3

```
#
 sysname R3
#
interface GigabitEthernet0/0/2
 ip address 10.2.1.2 255.255.255.252
#
nqa-server tcpconnect 10.2.1.2 9000
nqa-server udpecho 10.2.1.2 6000
#
ip route-static 10.1.1.0 255.255.255.252 10.2.1.1
#
return
```

4.3.5 Quiz

What is the difference between an NQA ICMP test instance and an NQA ICMP jitter test instance?

4.4 Configuration of Interface Backup and Floating Route

4.4.1 Introduction

4.4.1.1 About This Lab

Interface backup refers to the backup between specific interfaces on the same device. When an interface is faulty or the bandwidth is insufficient, traffic can be fast switched to a standby interface. The standby interface then transmits services or load balances network traffic.

Interface backup works in either active/standby or load balancing mode.

Interface backup in active/standby mode: One interface is the active interface, and the others are standby interfaces. When the active interface fails or the network quality is poor, a standby interface transmits data.

Interface backup in load balancing mode: One interface is the active interface, and the others are standby interfaces. When the bandwidth of the active interface is insufficient, standby interfaces are enabled. Then both the active and standby interfaces transmit data.

When the indirectly connected link of the active interface is faulty, the interface backup module cannot detect the fault, causing service interruption.

Association between interface backup and BFD enables a device to rapidly detect connectivity of the active link and implements fast switching when the active link is faulty. This improves reliability of service transmission.

Association between interface backup and NQA enables a device to detect connectivity of the active link in real time and implements fast switching when the active link is faulty. This improves reliability of service transmission.

A floating route is a static route. It provides backup when the active route fails. A floating route is installed in the IP routing table only when the next hop of the active route is unreachable.

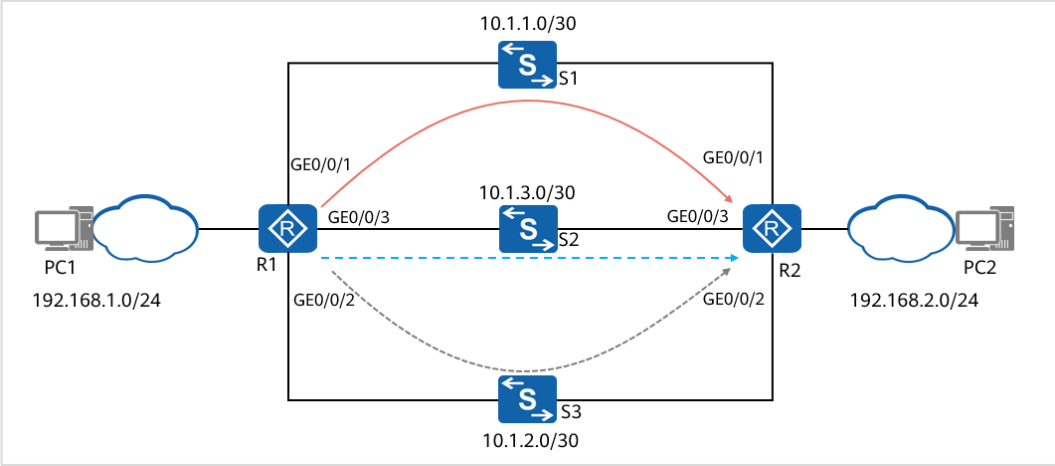
The floating route is implemented based on the Pre value in the routing table. Generally, the Pre value of the backup route is set to be greater than that of the active route. The active/standby switchover of floating routes is performed based on the interface status. Therefore, to detect the status of the entire path, floating routes are associated with NQA or BFD on the live network. If an NQA test instance or a BFD session fails, the active route is considered invalid.

4.4.1.2 Objectives

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

- Configure basic functions of interface backup.
- Configure association of interface backup.
- Configure BFD for floating routes.

4.4.1.3 Networking Topology



R1 is directly connected to R2 through three interfaces. Normally, PC1 exchanges data with PC2 through GE0/0/1 of R1.

To improve reliability of data transmission between PC1 and PC2, traffic is required to be switched to GE0/0/2 and GE0/0/3 (secondary choice) when GE0/0/1 becomes faulty.

When the working link fails, the link fault needs to be detected within 50 ms. In addition, the standby link is started to transmit services to reduce the impact of the active link fault on service transmission.

S1, S2, and S3 transparently transmit user data.

4.4.2 Lab Configuration

4.4.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces and static routes for the active and standby links. The priorities of the static routes can be set to the same value. Select paths based on the active and standby interfaces to ensure connectivity at the network layer. On R1, configure GE0/0/1 as the active interface and GE0/0/2 and GE0/0/3 as standby interfaces of GE0/0/1. GE0/0/2 has a higher priority than GE0/0/3 so that GE0/0/2 is preferentially selected to take over services when the active interface fails.
2. Configure a delay for an active/standby interface switchover to prevent network flapping caused by frequent active/standby interface switchovers.
3. Adjust the route priority between R1 and R2 and configure a floating route. The route priority determines that GE0/0/1 is the active one, and GE0/0/2 and GE0/0/3 are standby ones.
4. On R1 and R2, configure a BFD session for the active link to detect the status of the active link, and bind the floating route to the BFD session.

5. Configure association between interface backup and BFD on GE0/0/2 and GE0/0/3 of R1. When BFD detects a fault on the active link, traffic can be quickly switched to the standby link.
6. Configure association between interface backup and BFD on GE0/0/2 and GE0/0/3 of R2. When the BFD session detects the active link fault, traffic can be rapidly switched to the standby link. This ensures that traffic sent from R1 to R2 and traffic sent from R2 to R1 use the same route.

4.4.2.2 Configuration Procedure

Step 1 Configure an IP address for each interface and static routes between PC1 and PC2.

Configure IP addresses for interfaces. The following uses R1 as an example. The configuration of R2 is similar. For details, see the configuration file of R2.

```
<Huawei> system-view
[Huawei] sysname R1
[R1] interface gigabitethernet 0/0/1
[R1-GigabitEthernet0/0/1] ip address 10.1.1.1 255.255.255.0
[R1-GigabitEthernet0/0/1] quit
[R1] interface gigabitethernet 0/0/2
[R1-GigabitEthernet0/0/2] ip address 10.1.2.1 255.255.255.0
[R1-GigabitEthernet0/0/2] quit
[R1] interface gigabitethernet 0/0/3
[R1-GigabitEthernet0/0/3] ip address 10.1.3.1 255.255.255.0
[R1-GigabitEthernet0/0/3] quit
```

On R1, configure a static route to the network segment where PC2 is located.

```
[R1] ip route-static 192.168.2.0 24 10.1.2.2
[R1] ip route-static 192.168.2.0 24 10.1.1.2
[R1] ip route-static 192.168.2.0 24 10.1.3.2
```

On R2, configure a static route to the network segment where PC1 is located.

```
[R2] ip route-static 192.168.1.0 24 10.1.2.1
[R2] ip route-static 192.168.1.0 24 10.1.1.1
[R2] ip route-static 192.168.1.0 24 10.1.3.1
```

Step 2 Configure active and standby interfaces on R1.

Configure GE0/0/1 as the active interface, GE0/0/2 and GE0/0/3 as standby interfaces, and set the priorities of GE0/0/2 and GE0/0/3 to 30 and 20 respectively.

```
[R1] interface gigabitethernet 0/0/1
[R1-GigabitEthernet0/0/1] standby interface gigabitethernet 0/0/2 30
[R1-GigabitEthernet0/0/1] standby interface gigabitethernet 0/0/3 20
[R1-GigabitEthernet0/0/1] quit
```

Step 3 Set the delay for an active/standby interface switchover on R1.

Set the delay for an active/standby interface switchover to 10s.

```
[R1] interface gigabitethernet 0/0/1
[R1-GigabitEthernet0/0/1] standby timer delay 10 10
[R1-GigabitEthernet0/0/1] quit
```

Verify the configuration.

Run the display standby state command on R1 to check the status of the active and standby interfaces. The command output shows that the active interface GigabitEthernet0/0/1 is in UP state and the standby interfaces GigabitEthernet0/0/2 and GigabitEthernet0/0/3 are in STANDBY state.

```
[R1]display standby state
Interface                   Interfacestate Backupstate Backupflag Pri    Loadstate
GigabitEthernet0/0/1                UP          MUP          MU
GigabitEthernet0/0/2              STANDBY       STANDBY        BU   30
GigabitEthernet0/0/3              STANDBY       STANDBY        BU   20


 Backup-flag meaning:
 M---MAIN   B---BACKUP      V---MOVED      U---USED
 D---LOAD   P---PULLED
------------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name              Bfd-State   BackupInterface             State

------------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask          Route-State   BackupInterface             State

------------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                     BackupInterface             State
```

Run the shutdown command on GE0/0/1 to simulate a link fault. Run the display standby state command on R1. The command output shows that the active interface GigabitEthernet0/0/1 is DOWN and the standby interface GigabitEthernet0/0/2 is UP, indicating that the standby interface has been enabled.

```
[R1]display standby state
Interface                   Interfacestate Backupstate Backupflag Pri    Loadstate
GigabitEthernet0/0/1              DOWN          MDOWN          MU
GigabitEthernet0/0/2                UP            UP           BU   30
GigabitEthernet0/0/3              STANDBY       STANDBY        BU   20
 Backup-flag meaning:
 M---MAIN   B---BACKUP      V---MOVED      U---USED
 D---LOAD   P---PULLED
------------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name              Bfd-State   BackupInterface             State

------------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask          Route-State   BackupInterface             State
```

```
------------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                  BackupInterface              State
```

When the faulty interface recovers, that is, after the active interface is enabled, GE0/0/1 goes Up again, and GE0/0/2 returns to the backup state.

When a fault occurs on the indirectly connected link of the active interface, the active interface is still in Up state and cannot detect the fault on the remote end. Therefore, you need to configure the standby interface to monitor the status of the interface to implement fast switchover. Common technologies include association with BFD, NQA, and IP routing.

Step 4 After interface backup is associated with BFD or NQA, if BFD or NQA detects that the active link fails, a standby interface will be enabled. In this case, the active interface may still be physically up because the related routing entries remain unchanged. As a result, data is still sent from the primary link.

Associate a floating route with BFD or NQA to address the preceding issue.

Delete the standby interface configuration on GE0/0/1, change the priorities of the static routes between R1 and R2 to 60 and 80, respectively, and configure the floating route. The following uses two routes as an example to describe how to disconnect GE0/0/3.

NOTE

The priority of the standby link is higher than that of the active link.

R1's configuration

```
[R1]ip route-static 192.168.2.0 255.255.255.0 10.1.1.2 preference 80
[R1]ip route-static 192.168.2.0 255.255.255.0 10.1.2.2 preference 60
```

R2's configuration

```
[R2]ip route-static 192.168.1.0 255.255.255.0 10.1.1.1 preference 80
[R2]ip route-static 192.168.1.0 255.255.255.0 10.1.2.1 preference 60
```

Configure a BFD session between R1 and R2.

On R1, configure a BFD session between R1 and R2.

```
[R1] bfd
[R1-bfd] quit
[R1] bfd test bind peer-ip 10.1.1.2
[R1-bfd-session-test] discriminator local 10
[R1-bfd-session-test] discriminator remote 100
[R1-bfd-session-test] commit
[R1-bfd-session-test] quit
```

On R2, configure a BFD session between R2 and R1.

```
[R2] bfd
[R2-bfd] quit
[R2] bfd test bind peer-ip 10.1.1.1
[R2-bfd-session-test] discriminator local 100
[R2-bfd-session-test] discriminator remote 10
[R2-bfd-session-test] commit
[R2-bfd-session-test] quit
```

Check the BFD session status.

```
[R1]dis bfd session all
--------------------------------------------------------------------------------
Local Remote      PeerIpAddr      State     Type          InterfaceName
--------------------------------------------------------------------------------

10    100         10.1.1.2        Up        S_IP_PEER     -
--------------------------------------------------------------------------------
      Total UP/DOWN Session Number : 1/0

[R2]dis bfd session all
--------------------------------------------------------------------------------
Local Remote      PeerIpAddr      State     Type          InterfaceName
--------------------------------------------------------------------------------

100   10          10.1.1.1        Up        S_IP_PEER     -
--------------------------------------------------------------------------------
      Total UP/DOWN Session Number : 1/0
```

Step 5 Configure association between interface backup and BFD on the standby interface of R1.

```
[R1] interface gigabitethernet 0/0/2
[R1-GigabitEthernet0/0/2] standby track bfd-session session-name test
[R1] ip route-static 192.168.2.0 255.255.255.0 10.1.1.2 bfd-session test
```

Step 6 Configure association between interface backup and BFD on the standby interface of R2.

```
[R2] interface gigabitethernet 0/0/2
[R2-GigabitEthernet0/0/2] standby track bfd-session session-name test
[R2] ip route-static 192.168.1.0 255.255.255.0 10.1.1.1 bfd-session test
```

----End

4.4.3 Verification

Check the BFD session status and standby interface status on R1. The command output shows that the BFD session status is UP and the status of 2/0/0 is STANDBY.

```
[R1]display standby state
Interface                   Interfacestate Backupstate Backupflag Pri    Loadstate
```

```
 Backup-flag meaning:
 M---MAIN   B---BACKUP       V---MOVED      U---USED
 D---LOAD   P---PULLED
------------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name                 Bfd-State   BackupInterface              State
test                     OK          GigabitEthernet0/0/2         STANDBY

------------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask            Route-State   BackupInterface              State

------------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                        BackupInterface              State
```

Run the shutdown command on GE2/0/0 of R2 to simulate a link fault. Run the display standby state command on R1. The command output shows that the BFD session status is ERR; the status of the standby interface GE2/0/0 is UP, indicating that the standby interface is started.

```
<R1> display standby state
Interface                   Interfacestate Backupstate Backupflag Pri    Loadstate

 Backup-flag meaning:
 M---MAIN   B---BACKUP       V---MOVED      U---USED
 D---LOAD   P---PULLED


------------------------------------------------------------------------------
Below is track BFD Information:
Bfd-Name                 Bfd-State   BackupInterface              State
test                     ERR    GigabitEthernet0/0/2              UP
------------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask            Route-State   BackupInterface              State

------------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                        BackupInterface              State
------------------------------------------------------------------------------
Below is track NQA group Information:
Group Name                           BackupInterface              State
```

Run the undo shutdown command on GE0/0/2 of R2. After GE0/0/2 goes Up, run the display standby state command on R1. The output shows that the BFD session status is UP and standby interface GE0/0/2 switches to the STANDBY state.

```
<R1> display standby state
Interface                   Interfacestate Backupstate Backupflag Pri    Loadstate

 Backup-flag meaning:
 M---MAIN   B---BACKUP       V---MOVED      U---USED
```

```
 D---LOAD   P---PULLED


------------------------------------------------------------------------------
Below is track BFD Information:
Bfd-Name                 Bfd-State   BackupInterface              State
test                     UP      GigabitEthernet0/0/2          STANDBY

------------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask             Route-State   BackupInterface               State

------------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                          BackupInterface                State
------------------------------------------------------------------------------
Below is track NQA group Information:
Group Name                             BackupInterface                State
```

4.4.4 Reference Configuration

4.4.4.1 Configurations of R1in interface backup

```
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0
  standby interface GigabitEthernet0/0/2 30
  standby interface GigabitEthernet0/0/3 20
  standby timer delay 10 10

#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 192.168.2.0 255.255.255.0 10.1.2.2
ip route-static 192.168.2.0 255.255.255.0 10.1.1.2
ip route-static 192.168.2.0 255.255.255.0 10.1.3.2
#
Return
```

4.4.4.2 Configurations of R2 in interface backup

```
#
 sysname R2
#
```

```
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.2 255.255.255.0
#
interface LoopBack0
 ip address 192.168.2.1 255.255.255.0
#
ip route-static 192.168.1.0 255.255.255.0 10.1.2.1
ip route-static 192.168.1.0 255.255.255.0 10.1.1.1
ip route-static 192.168.1.0 255.255.255.0 10.1.3.1
#
Return
```

4.4.4.3 Configurations of R1 for association between the floating route and BFD

```
#
 sysname R1
#
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
 standby track bfd-session session-name test
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.0
#
bfd test bind peer-ip 10.1.3.2
 discriminator local 10
 discriminator remote 20
 commit
#
ip route-static 192.168.2.0 255.255.255.0 10.1.1.2 preference 80
ip route-static 192.168.2.0 255.255.255.0 10.1.2.2
#
return
```

4.4.4.4 Configurations of R2 for association between the floating route and BFD

```
#
 sysname R2
#
```

```
bfd
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.2 255.255.255.0
 standby track bfd-session session-name test
#
interface LoopBack0
 ip address 192.168.2.1 255.255.255.0
#
bfd test bind peer-ip 10.1.3.1
 discriminator local 20
 discriminator remote 10
 commit
#
ip route-static 192.168.1.0 255.255.255.0 10.1.1.1 preference 80
ip route-static 192.168.1.0 255.255.255.0 10.1.2.1 preference 60
ip route-static 192.168.1.0 255.255.255.0 10.1.3.1 preference 100
#
Return
```

4.5 SPR Configuration

4.5.1 Introduction

4.5.1.1 About This Lab

Smart Policy Routing (SPR) actively detects the link quality and matches service requirements to select an optimal link to forward service data. SPR prevents network blackholes and flappings.

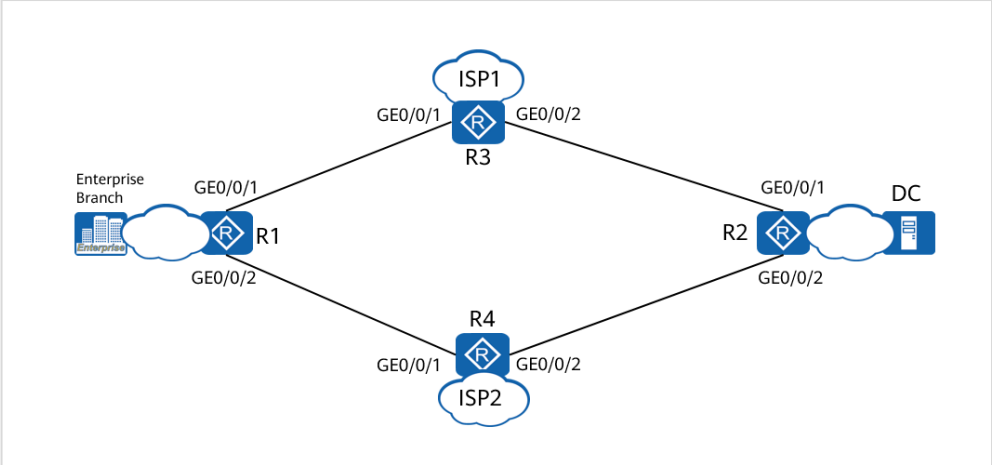
You can set the SPR switchover period, detection link, and best-effort link, configure an interface to be shut down automatically when SPR does not select the link of the interface, set the delay after which an interface is automatically shut down when SPR does not select the link of the interface, enable redirection enhancement, and configure other SPR parameters. Then SPR can forward traffic based on the intelligent traffic steering result in non-ECMP scenarios.

4.5.1.2 Objectives

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

- Use SPR.
- Configure SPR parameters.
- Configure association between SPR and services.

4.5.1.3 Networking Topology



An enterprise branch connects to the enterprise data center through ISP1 and ISP2 and saves transaction data on ServerA in the data center.

ISP1 provides a high-speed active link and ISP2 provides a standby link. To ensure that transaction data is sent to the data center in a timely manner, the link delay for transaction data must be shorter than or equal to 1000 ms.

4.5.2 Lab Configuration

4.5.2.1 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the NQA client on R1 and the NQA server on R2 to dynamically monitor the quality of the link between the enterprise branch and data center.
2. Configure an ACL on R1 to differentiate service flows so that SPR can be implemented for packets destined for ServerA in the data center.
3. On R1, configure SPR parameters to add the detection link to the link group.
4. On R1, associate SPR with services so that the link of ISP1 is the active link and the link of ISP2 is the standby link. Ensure that the link delay is less than or equal to 1000 ms.

4.5.2.2 Configuration Procedure

Step 1 Assign an IP address to each interface.

Configure IP addresses for interfaces on R1.

```
<Huawei> system-view
[Huawei] sysname R1
[R1] interface gigabitethernet 0/0/1
[R1-GigabitEthernet0/0/1] ip address 202.1.1.1 255.255.255.0
[R1-GigabitEthernet0/0/1] quit
[R1] interface gigabitethernet 0/0/2
[R1-GigabitEthernet0/0/2] ip address 178.1.1.1 255.255.255.0
[R1-GigabitEthernet0/0/2] quit
```

Configure IP addresses for interfaces on R2.

```
<Huawei> system-view
[Huawei] sysname R2
[R2] interface gigabitethernet 0/0/1
[R2-GigabitEthernet0/0/1] ip address 202.1.2.1 255.255.255.0
[R2-GigabitEthernet0/0/1] quit
[R2] interface gigabitethernet 0/0/2
[R2-GigabitEthernet0/0/2] ip address 178.1.2.1 255.255.255.0
[R2-GigabitEthernet0/0/2] quit
[R2] interface loopback 0
[R2-LoopBack0] ip address 2.0.0.2 255.255.255.0
[R2-LoopBack0]quit
```

Configure IP addresses for interfaces on R3.

```
<Huawei> system-view
[Huawei] sysname R3
[R3] interface gigabitethernet 0/0/1
[R3-GigabitEthernet0/0/1] ip address 202.1.1.2 255.255.255.0
[R3-GigabitEthernet0/0/1] quit
```

```
[R3] interface gigabitethernet 0/0/2
[R3-GigabitEthernet0/0/2] ip address 202.1.2.2 255.255.255.0
[R3-GigabitEthernet0/0/2] quit
```

Configure IP addresses for interfaces on R4.

```
<Huawei> system-view
[Huawei] sysname R4
[R4] interface gigabitethernet 0/0/1
[R4-GigabitEthernet0/0/1] ip address 178.1.1.2 255.255.255.0
[R4-GigabitEthernet0/0/1] quit
[R4] interface gigabitethernet 0/0/2
[R4-GigabitEthernet0/0/2] ip address 178.1.2.2 255.255.255.0
[R4-GigabitEthernet0/0/2] quit
```

Step 2 Configure static routes.

Configure a static route on R1.

```
[R1] ip route-static 2.0.0.2 255.255.255.255 202.1.1.2
[R1] ip route-static 2.0.0.2 255.255.255.255 178.1.1.2
```

Configure a static route on R2.

```
[R2] ip route-static 2.0.0.2 255.255.255.255 202.1.2.2
[R2] ip route-static 2.0.0.2 255.255.255.255 178.1.2.2
```

Configure a static route on R3.

```
[R3] ip route-static 2.0.0.2 255.255.255.255 202.1.2.1
```

Configure a static route on R4.

```
[R4] ip route-static 2.0.0.2 255.255.255.255 178.1.2.1
```

Step 3 Configure an NQA test instance.

Configure the NQA client on R1.

```
[R1] nqa test-instance admin nqa1
[R1-nqa-admin-nqa1] test-type jitter
[R1-nqa-admin-nqa1] destination-address ipv4 202.1.2.1
[R1-nqa-admin-nqa1] destination-port 10000
[R1-nqa-admin-nqa1] hardware-based enable
[R1-nqa-admin-nqa1] frequency 10
[R1-nqa-admin-nqa1] source-interface gigabitethernet 0/0/1
[R1-nqa-admin-nqa1] start now
[R1-nqa-admin-nqa1] quit
[R1] nqa test-instance admin nqa2
[R1-nqa-admin-nqa2] test-type jitter
```

```
[R1-nqa-admin-nqa2] destination-address ipv4 178.1.2.1
[R1-nqa-admin-nqa2] destination-port 10001
[R1-nqa-admin-nqa2] hardware-based enable
[R1-nqa-admin-nqa2] frequency 10
[R1-nqa-admin-nqa2] source-interface gigabitethernet 0/0/2
[R1-nqa-admin-nqa2] start now
[R1-nqa-admin-nqa2] quit
```

Configure the NQA server on R2.

```
[R2] nqa-server udpecho 202.1.2.1 10000
[R2] nqa-server udpecho 178.1.2.1 10001
```

Step 4 Configure an ACL to classify service flows.

Configure ACL 3000 on R1 to apply SPR to data flows destined for 2.0.0.2.

```
[R1] acl 3000
[R1-acl-adv-3000] rule permit ip destination 2.0.0.2 0.0.0.0
[R1-acl-adv-3000] quit
```

Step 5 Set SPR routing parameters on R1.

```
[R1] smart-policy-route
[R1-smart-policy-route] period 50
[R1-smart-policy-route] route flapping suppression 100
[R1-smart-policy-route] prober gigabitethernet 0/0/1 nqa admin nqa1
[R1-smart-policy-route] prober gigabitethernet 0/0/2 nqa admin nqa2
[R1-smart-policy-route] link-group group1
[R1-smart-policy-route-link-group-group1] link-member gigabitethernet 0/0/1
[R1-smart-policy-route-link-group-group1] quit
[R1-smart-policy-route] link-group group2
[R1-smart-policy-route-link-group-group2] link-member gigabitethernet 0/0/2
[R1-smart-policy-route-link-group-group2] quit
```

Step 6 Set SPR service parameters.

```
[R1-smart-policy-route] service-map map1
[R1-smart-policy-route-service-map-map1] match acl 3000
[R1-smart-policy-route-service-map-map1] set delay threshold 1000
[R1-smart-policy-route-service-map-map1] set link-group group1
[R1-smart-policy-route-service-map-map1] set link-group group2 backup
[R1-smart-policy-route-service-map-map1] quit
[R1-smart-policy-route] quit
```

----End

4.5.3 Verification

Verify the configuration.

Check the NQA test result of the detection link on R1.

```
[R1] display smart-policy-route link-state
------------------------------------------------------------------------------
link-name                                Delay      Jitter     Loss
------------------------------------------------------------------------------
GigabitEthernet0/0/1                     5000       3000       1000
GigabitEthernet0/0/2                     5000       3000       1000
------------------------------------------------------------------------------
```

Check routing information about service map1 on R1.

```
[R1] display smart-policy-route service-map map1
------------------------------------------------------------------------------
Match acl             : 3000
DelayThreshold        : 1000
LossThreshold         : 1000
JitterThreshold       : 3000
CmiThreshold          : 0
GroupName             : group1
BackupGroupName       : group2
Description           :
Cmi-Method            : d+l+j
CurLinkName           : GigabitEthernet0/0/1
------------------------------------------------------------------------------
```

4.5.4 Reference Configuration

4.5.4.1 Configurations of R1

```
#
 sysname R1
#
acl number 3000
 rule 5 permit ip destination 2.0.0.2 0
#
interface GigabitEthernet0/0/1
 ip address 202.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 178.1.1.1 255.255.255.0
#
nqa test-instance admin nqa1
 test-type jitter
 destination-address ipv4 202.1.2.1
 destination-port 10000
 hardware-based enable
 frequency 10
 source-interface GigabitEthernet0/0/1
 start now
nqa test-instance admin nqa2
 test-type jitter
 destination-address ipv4 178.1.2.1
```

```
 destination-port 10001
 hardware-based enable
 frequency 10
 source-interface GigabitEthernet0/0/2
 start now
#
smart-policy-route
 period 50
 route flapping suppression 100
 prober GigabitEthernet0/0/1 nqa admin nqa1
 prober GigabitEthernet0/0/2 nqa admin nqa2
 link-group group1
  link-member GigabitEthernet0/0/1
 link-group group2
  link-member GigabitEthernet0/0/2
 service-map map1
  match acl 3000
  set delay threshold 1000
  set link-group group1
  set link-group group2 backup
#
 ip route-static 2.0.0.2 255.255.255.255 202.1.1.2
 ip route-static 2.0.0.2 255.255.255.255 178.1.1.2
#
```

4.5.4.2 Configurations of R2

```
#
 sysname R2
#
interface GigabitEthernet0/0/1
 ip address 202.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 178.1.2.1 255.255.255.0
#
interface loopback 0
 ip address 2.0.0.2 255.255.255.255
#
nqa-server udpecho 178.1.2.1 10001
nqa-server udpecho 202.1.2.1 10000
#
 ip route-static 2.0.0.2 255.255.255.255 202.1.2.2
 ip route-static 2.0.0.2 255.255.255.255 178.1.2.2
#
```

4.5.4.3 Configurations of R3

```
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 202.1.1.2 255.255.255.0
#
```

```
interface GigabitEthernet0/0/2
 ip address 202.1.2.2 255.255.255.0
#
ip route-static 2.0.0.2 255.255.255.255 202.1.2.1
```

4.5.4.4 Configurations of R4

```
#
 sysname R4
#
interface GigabitEthernet0/0/1
 ip address 178.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 178.1.2.2 255.255.255.0
#
ip route-static 2.0.0.2 255.255.255.255 178.1.2.1
```

5 SD-WAN Controller lab

5.1 NCE-WAN Administrator/Tenant Information Planning

5.1.1 Introduction

5.1.1.1 Objectives

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

- Maintain system administrator accounts.
- Maintain MSP administrator accounts.
- Maintain tenant administrator accounts.

5.1.1.2 Networking Topology

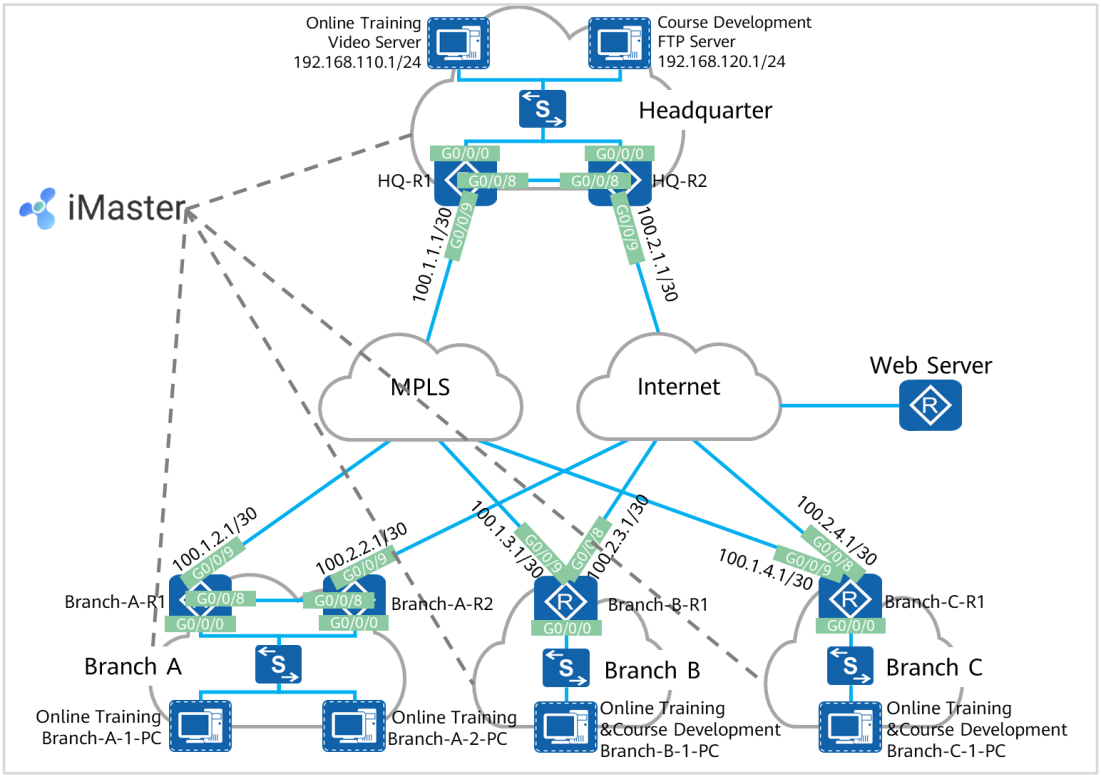


Figure5-1 SD-WAN topology

The figure shows the interconnection IP addresses. The headquarters and Branch A are connected to the MPLS network and Internet through dual egresses and links, and Branch B and Branch C are connected to the MPLS network and Internet through a single egress and dual links. Two links connect the MPLS network and Internet respectively, and the MPLS network and Internet are isolated from each other. Devices connect to iMaster NCE-WAN through public IP addresses.

5.1.1.3 Lab Background

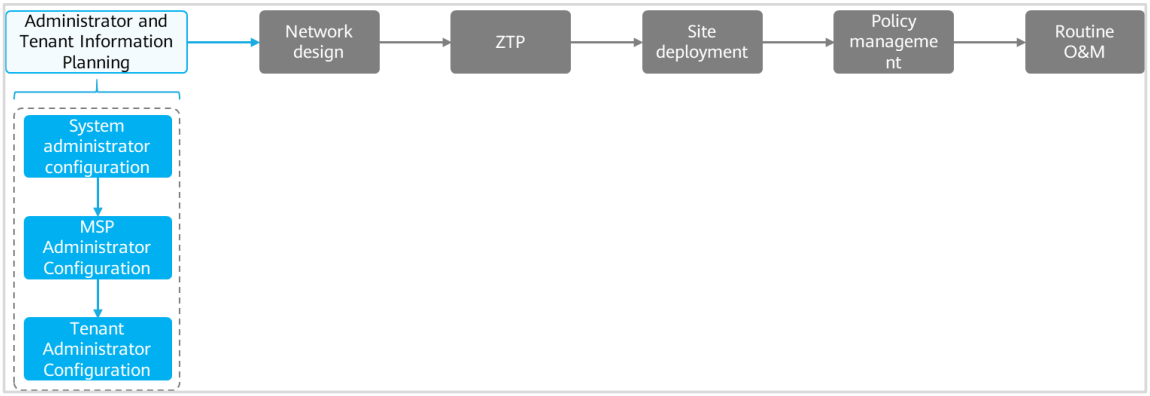
An enterprise needs to deploy new sites. To quickly deploy network services and simplify O&M, the enterprise deploys the SD-WAN solution.

Network planning and management personnel need to construct a network using iMaster NCE-WAN based on the network topology and requirements.

5.1.2 Lab Tasks

5.1.2.1 Configuration Roadmap

To deploy iMaster NCE-WAN, perform the following steps. The lab mainly describes how to create and maintain administrator and tenant information.



The configuration roadmap is as follows:

1. Log in as the system administrator.
2. Manage the system administrator account.
3. Configure a tunneling mode.
4. Manage licenses.
5. Configure an email server.
6. Create an MSP administrator account.
7. Log in and manage MSP accounts.
8. Create a tenant administrator account.
9. Log in and manage tenant accounts.

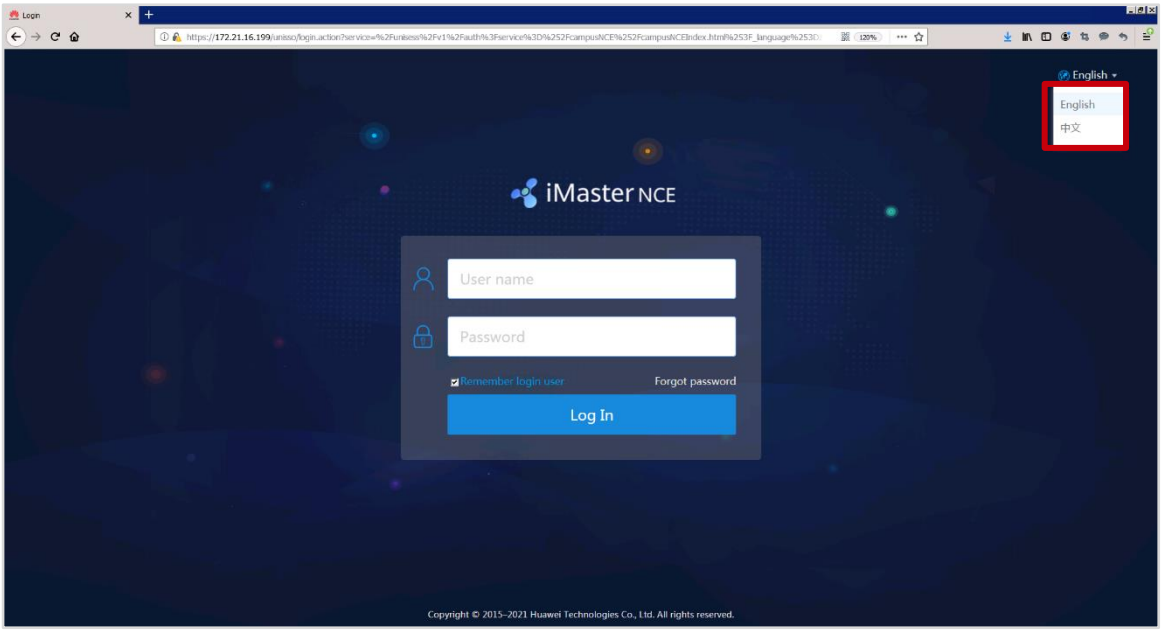
5.1.2.2 Configuration Procedure

Step 1 Log in as the system administrator.

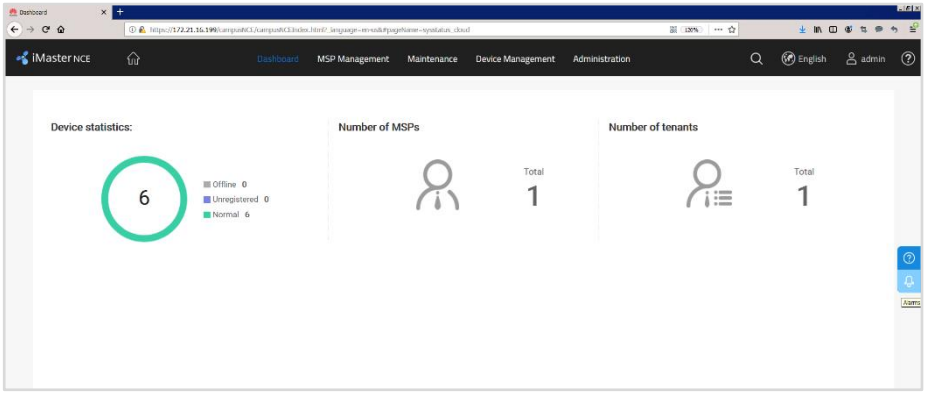
After iMaster NCE-WAN is installed, an administrator can use a web browser to log in to iMaster NCE-WAN to perform system management and maintenance operations. The following browsers are supported:

Internet Explorer, Google Chrome, Microsoft Edge

Enter https://172.21.16.199:18008 in the browser to log in to iMaster NCE-WAN. You can change the display language, as shown in the red box. Both Chinese and English are supported.



Enter the administrator name admin and password Huawei12#$, and click Log In. The iMaster NCE-WAN page is displayed.



NOTE

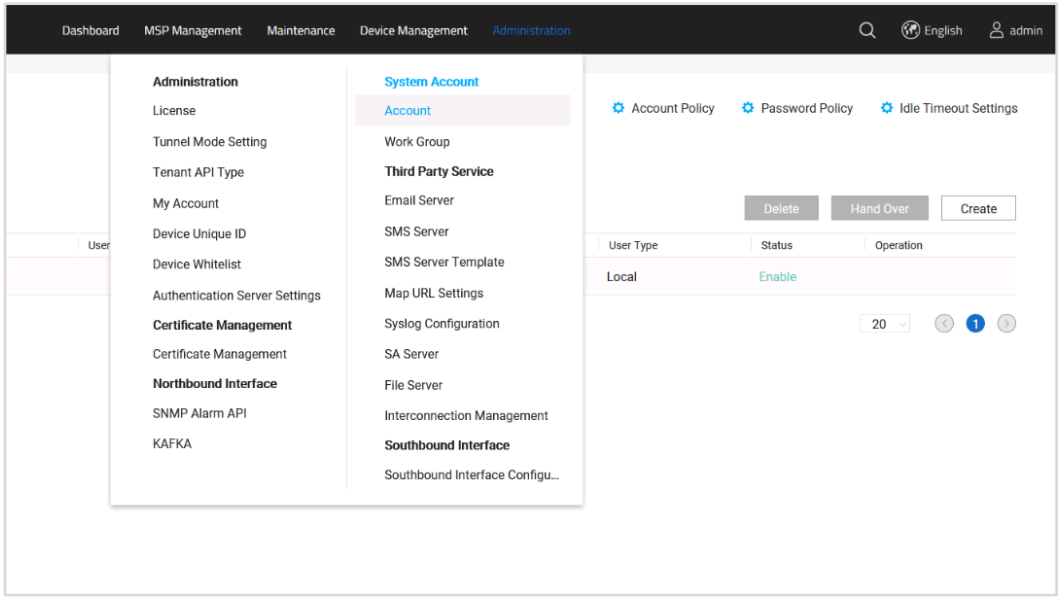
The default administrator name is admin and the default password is Changeme_123.

Change the password as prompted at the first login. This step is not required for non-first login.

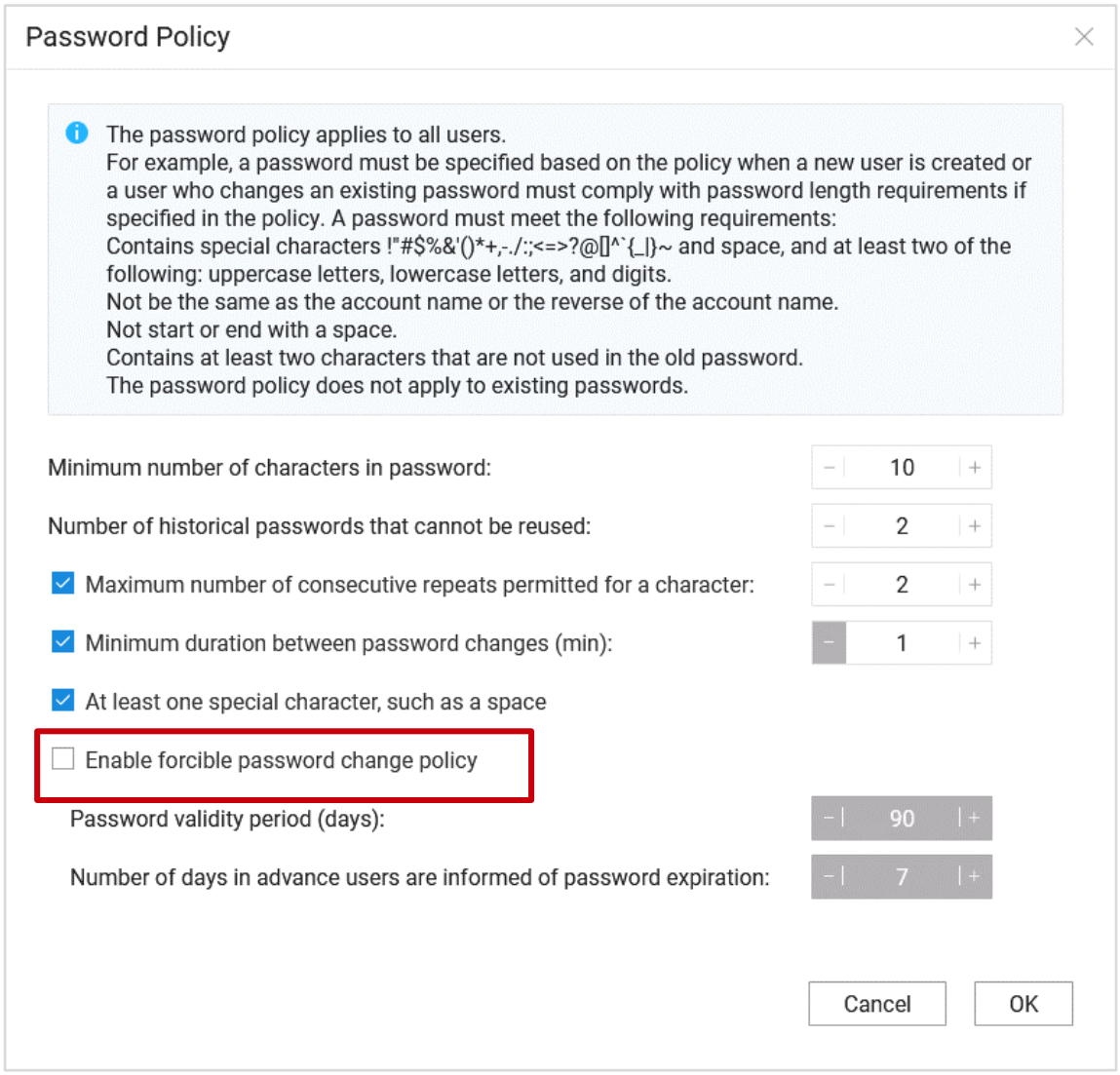
Step 2 Manage the system administrator account.

Change the password policy of the administrator account to ensure that the password does not expire.

Choose Administrator > System Account > Account from the main menu and click Password Policy.



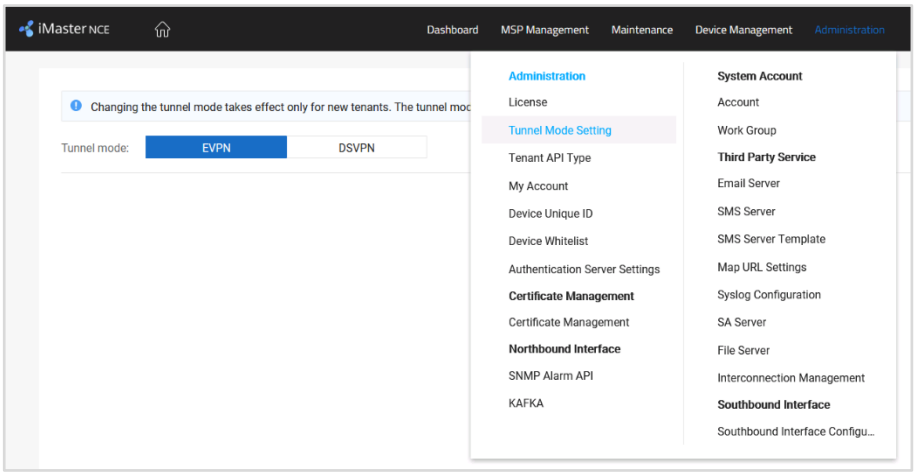
Cancel forcible change of an expired password.



Step 3 Configure a tunneling mode.

Set the tunneling mode to Ethernet Virtual Private Network (EVPN). By default, the tunneling mode is EVPN. You can set the tunneling mode to DSVPN as required.

Huawei SD-WAN Solution mainly uses IP overlay tunneling technology to construct networks. It also provides enhanced EVPN and Dynamic Smart VPN (DSVPN) tunneling technologies to help enterprise customers implement flexible overlay WAN networking. The system administrator can configure DSVPN and EVPN tunneling modes. The tunneling mode selected by the system administrator is used for new tenant.



NOTE

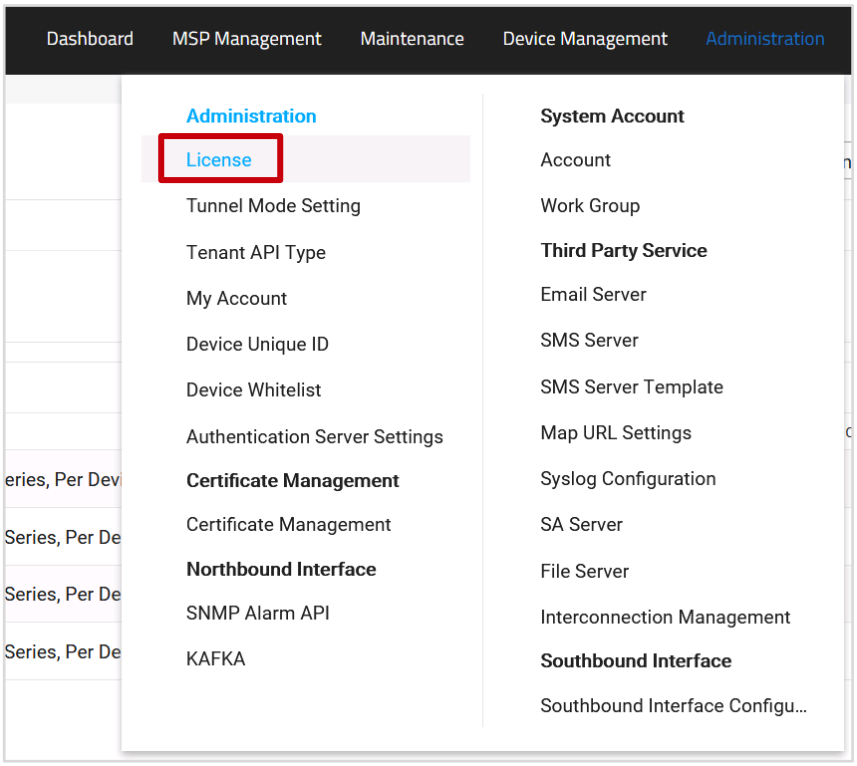
To be compatible with DSVPN and EVPN, iMaster NCE-WAN provides the tunneling mode setting function for the system administrator. When an MSP administrator creates a tenant, the tunneling mode selected by the system administrator is used. That is, if the current system administrator selects EVPN, the tenants created by the MSP administrator use EVPN. After the system administrator selects DSVPN, the tenants created by the MSP administrator use DSVPN. However, the tunneling mode of the tenants created before remains unchanged.

Step 4 (Optional) Manage licenses.

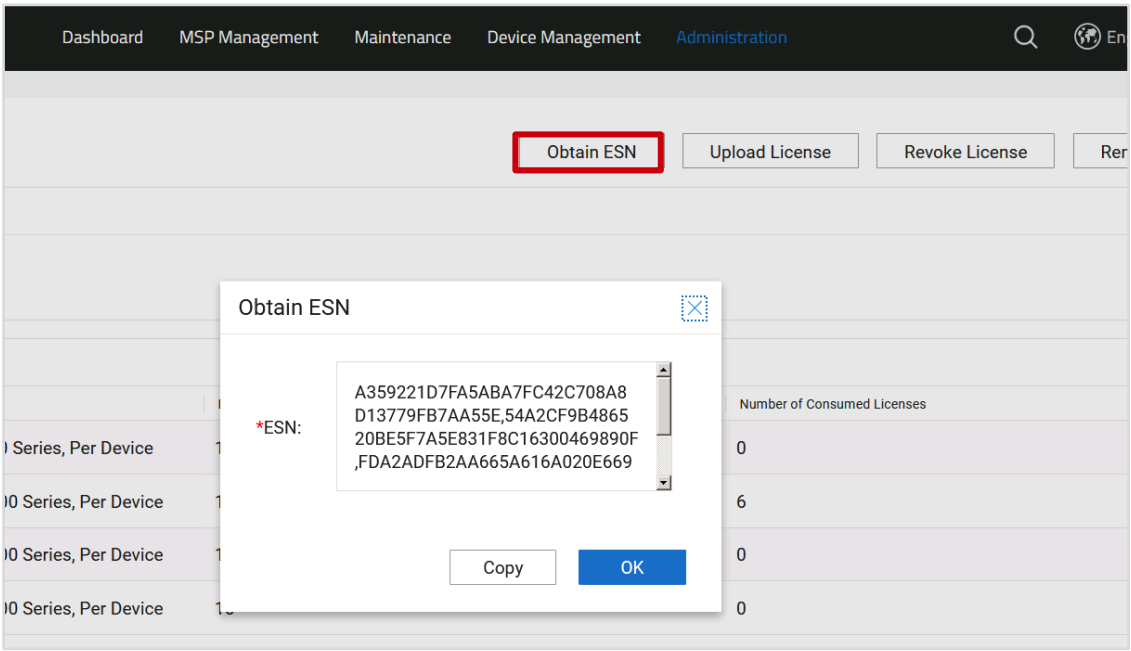
For commercial deployment scenarios with contracts, licenses are generated according to the orders. Onsite engineers download and install the licenses bound to ESNs.

The license has been installed in the lab. This step is for reference only.

Before applying for a license, you need to obtain the ESN of the device. You can choose Administrator > Administrator > License from the main menu to obtain the ESN.



Click Obtain ESN to obtain the ESN.



NOTE

Log in to Huawei ESDP at https://app.huawei.com/sdp/portal.html.

Choose License Activation > Entitlement Activation. On the page that is displayed, search for the activation ID based on the entitlement ID and select the correct activation ID.

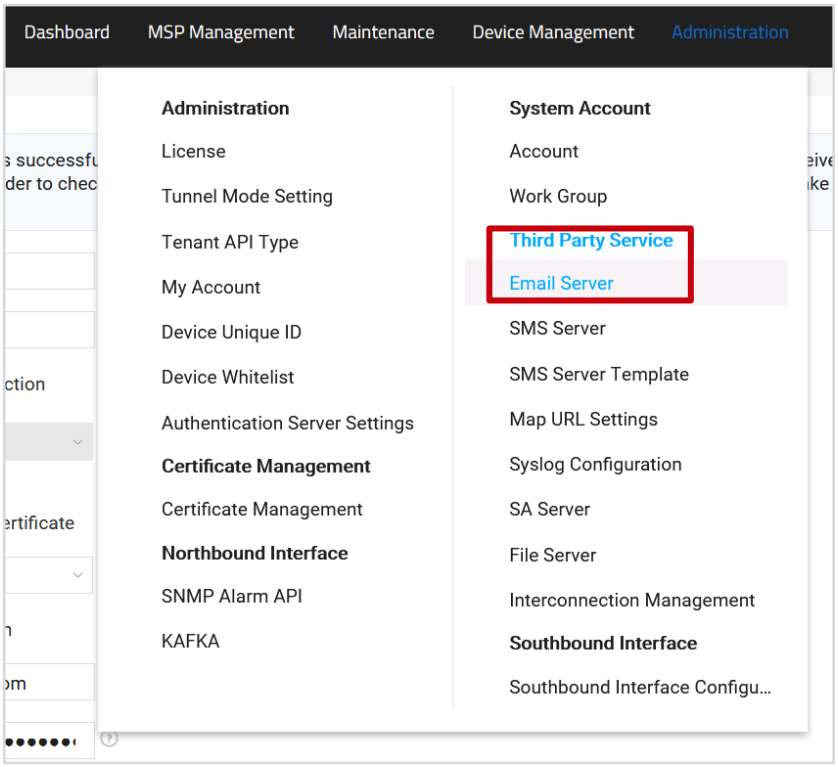
Step 5 Configure an email server.

When iMaster NCE-WAN needs to send emails to users, you need to configure an email server first.

iMaster NCE-WAN needs to send emails in the following scenarios:

- If the system administrator, MSP administrator, or tenant administrator forgets the password, iMaster NCE-WAN sends a reset password to the administrator through an email.
- After the system administrator performs alarm settings on iMaster NCE-WAN, iMaster NCE-WAN sends emails to notify users of reported alarms.
- If the tenant administrator wants to use the email-based deployment function, iMaster NCE-WAN needs to send deployment emails to related personnel.
- iMaster NCE-WAN sends a notification email to a tenant if a tenant license is about to expire.

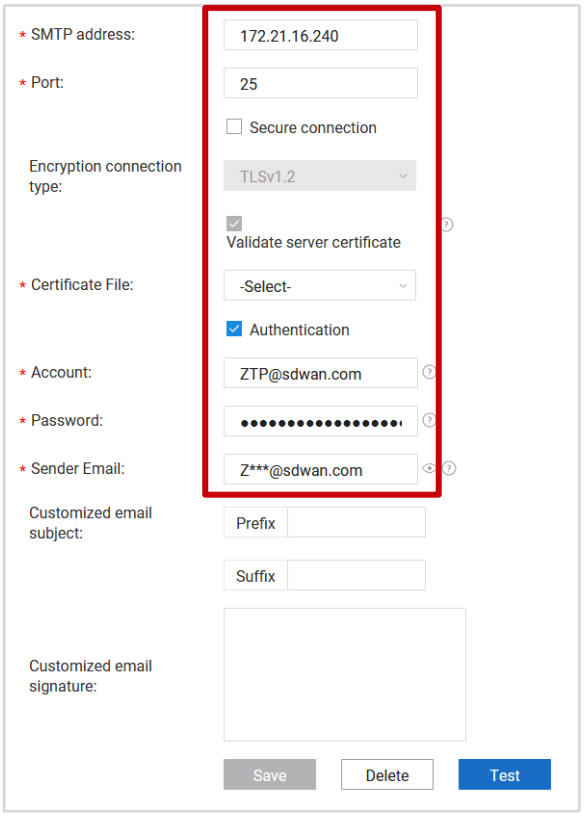
Choose Administrator > Third Party Service > Email Server from the main menu.



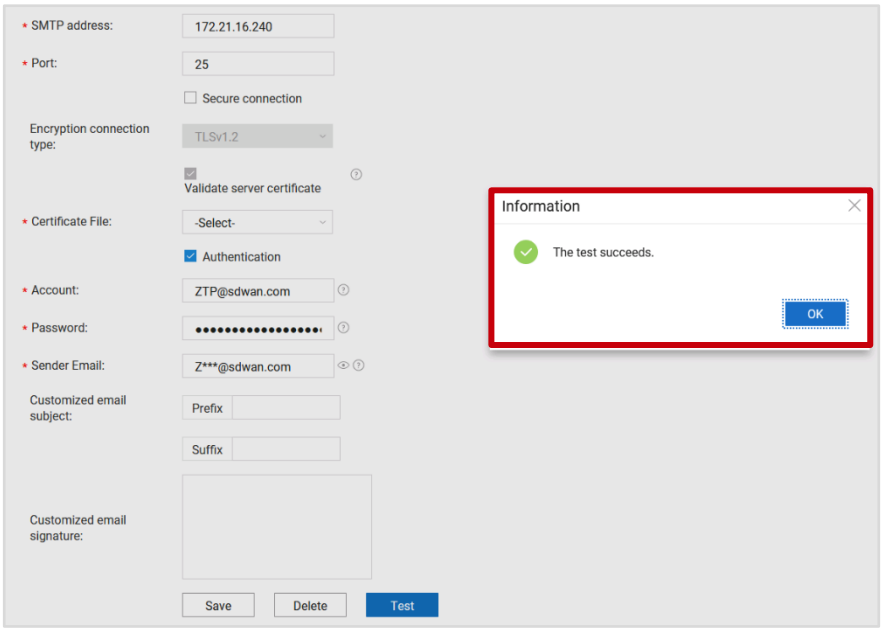
Set parameters for connecting to the email server.

- SMTP address: 172.21.16.240
- Port: 25
- Validate server certificate: disabled

- Account: ZTP@sdwan.com
- Password: Huawei@123
- Sender Email: ZTP@sdwan.com



Click Test to verify the email sending function. After the test is successful, click Save to save the settings.

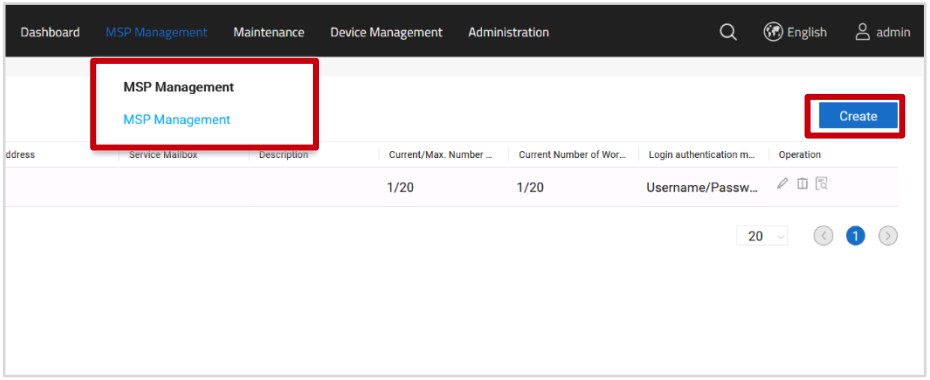


NOTE

If both the system administrator and MSP administrator have configured the email server, the email server configured by the MSP administrator is used preferentially. If the email server configured by the MSP administrator is not found, the email server configured by the system administrator is used.

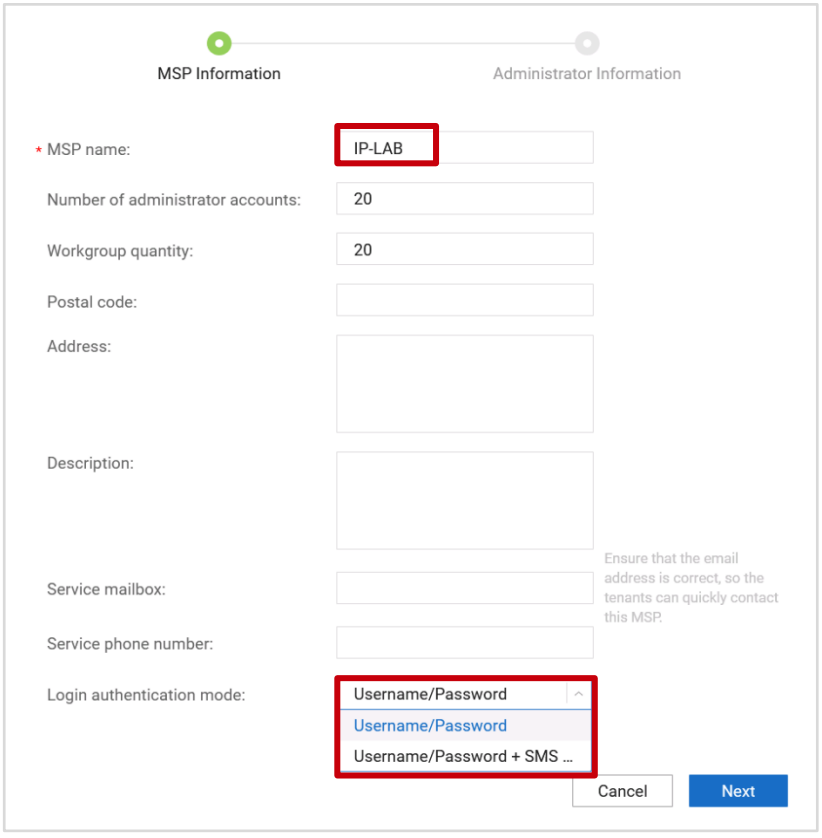
Step 6 Create an MSP administrator account.

Choose MSP Management > MSP Management > MSP Management and click Create.



Configure MSP information.

Set MSP name (IP-LAB) and Login authentication mode (Username/password), and click Next.



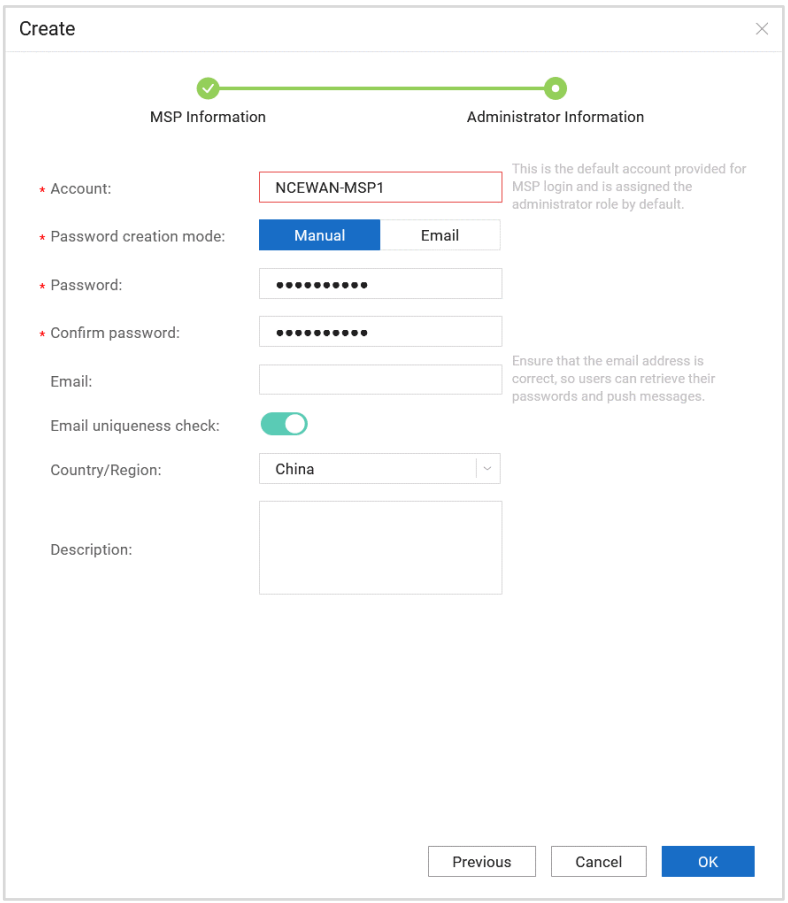
NOTE

The MSP name is used only to identify the MSP for the convenience of system administrator's management, but not for MSP login.

If Username/Password + SMS verification code is configured, you need to configure the SMS server under the administrator account.

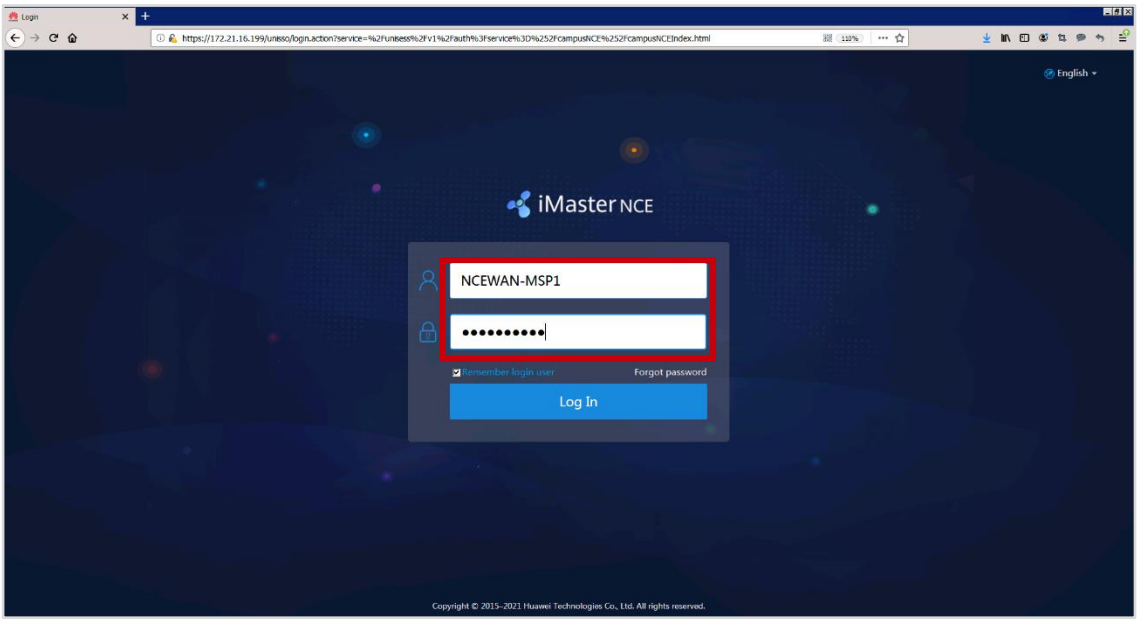
Choose Administrator > Third Party Service > SMS Server to configure the SMS server.

Set Account (NCEWAN-MSP1) and Password (Admin@1234) for MSP login and click OK.

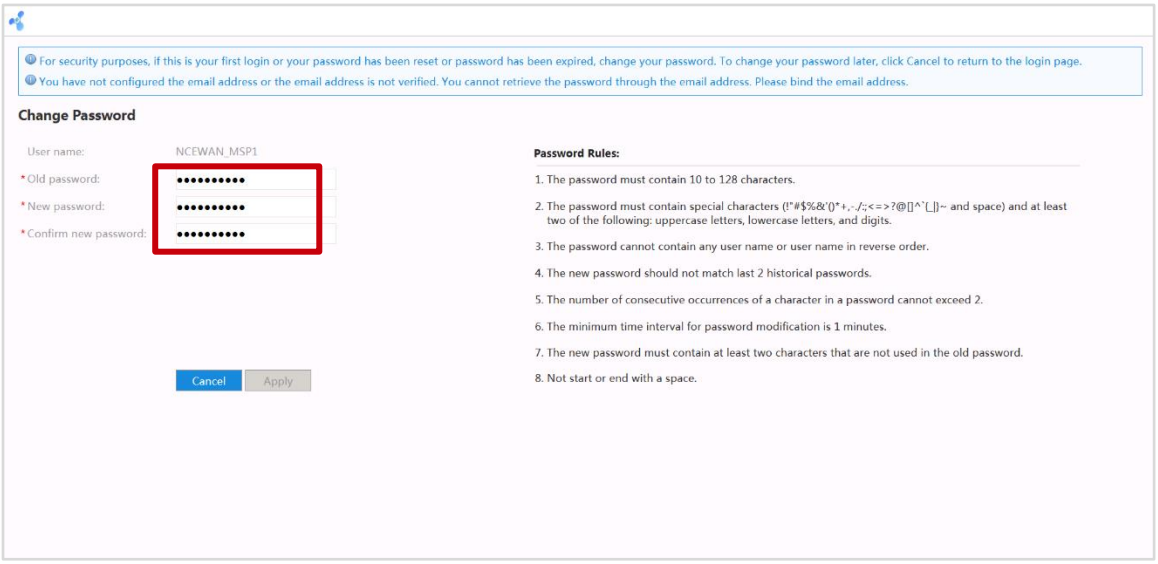


Step 7 Log in and manage MSP accounts.

Log out and log in again (https://172.21.16.199:18008) using the initial account (NCEWAN-MSP1) and password (Admin@1234) of the MSP.



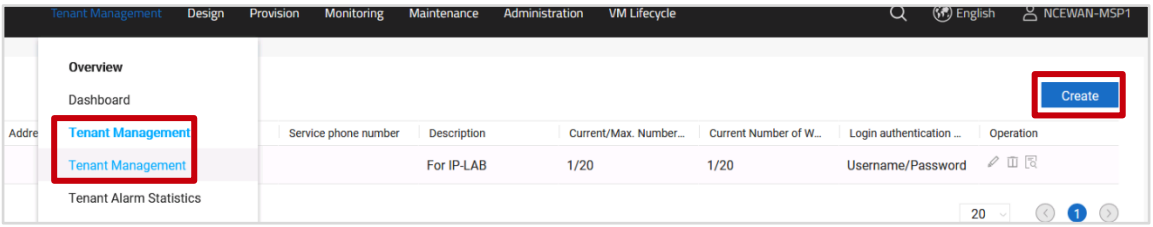
Change the initial password (Admin@1234) to the new password (Huawei12#$) upon the first login.



The password policy of the MSP account is modified to ensure that the password does not expire. This method is similar to the method for the system administrator to modify the password policy.

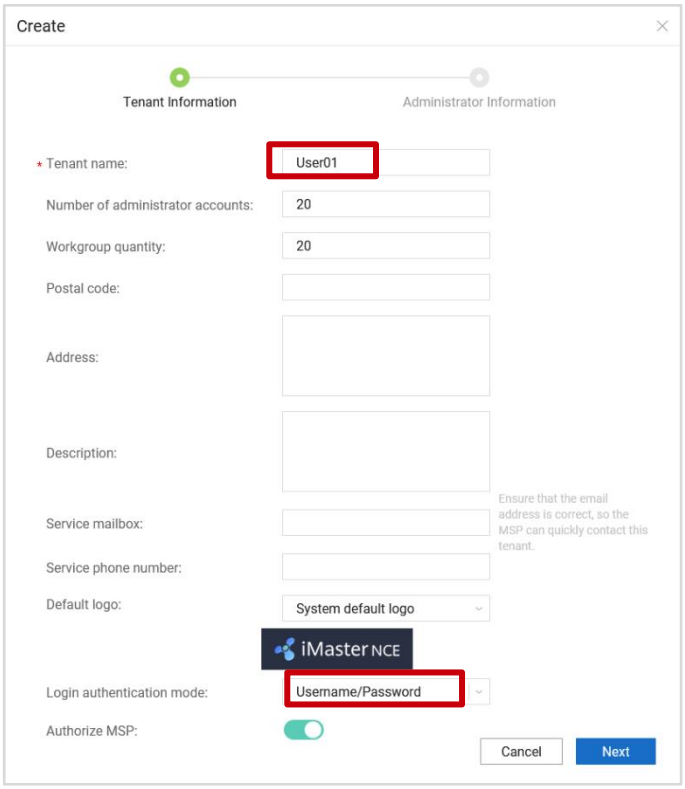
Step 8 Create a tenant administrator account.

Choose Tenant Management > Tenant Management > Tenant Management and click Create.



Configure tenant administrator information.

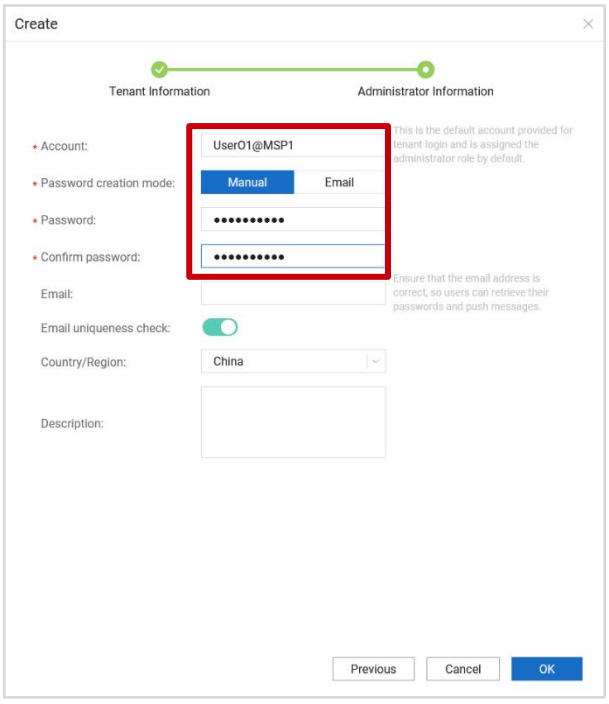
Set Tenant name (User01) and Login authentication mode (Username/Password), authorize the account to the MSP, and click Next.



NOTE

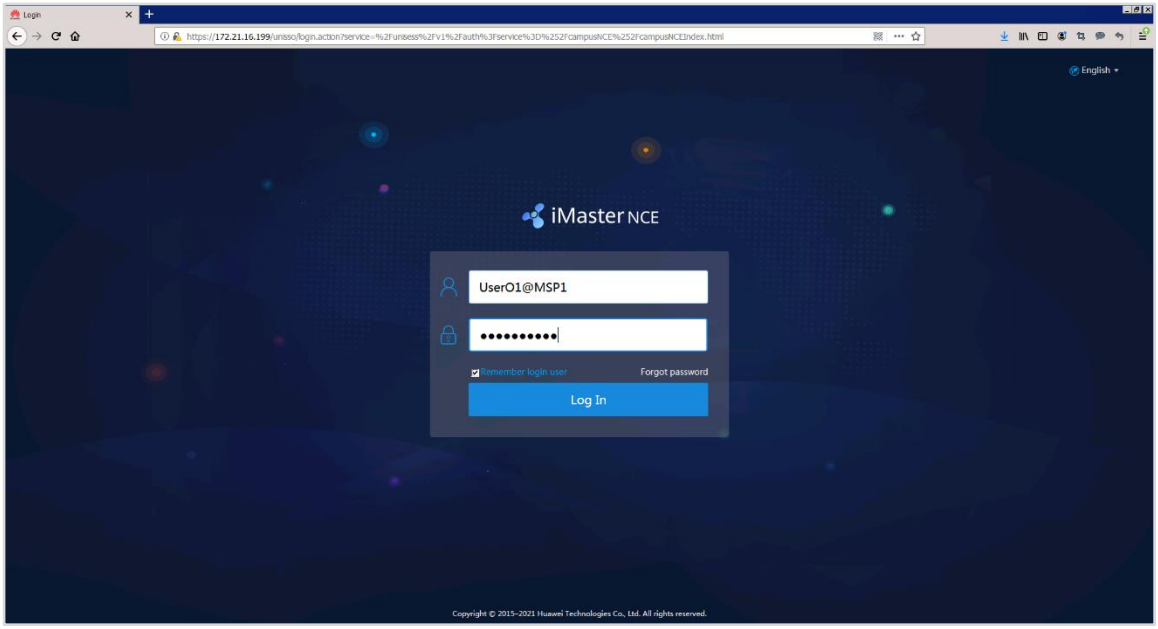
If Authorize MSP is enabled, the permission of the tenant administrator is authorized to an MSP. After the authorized MSP logs in to the tenant management page, the MSP has the permission of the tenant administrator.

Enter the initial account (User01@MSP1) and password (Admin@1234) of the tenant administrator and click OK.

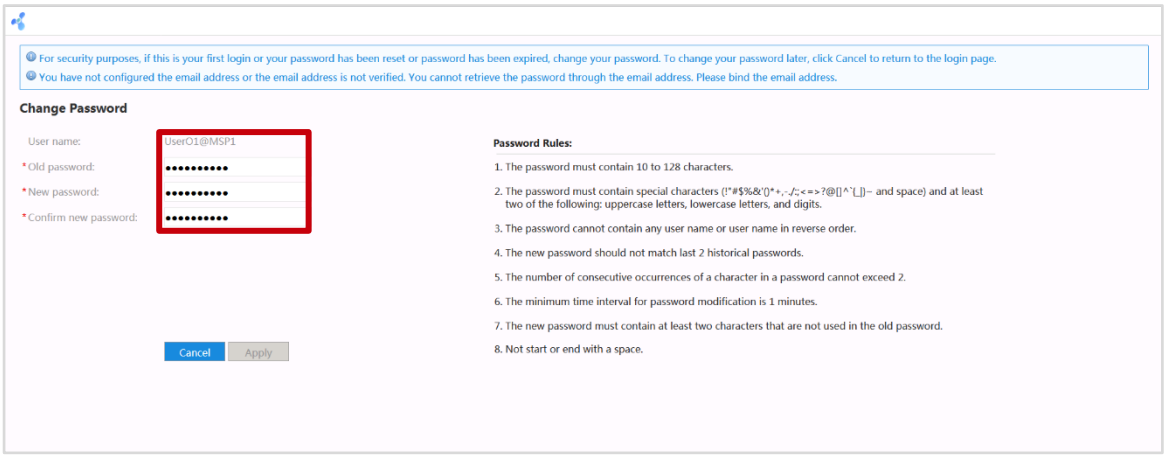


Step 9 Log in and manage tenant accounts.

Log out and log in again (https://172.21.16.199:18008) using the initial tenant account (User01@MSP1) and password (Admin@1234).



Change the initial password (Admin@1234) to the new password (Huawei12#$) upon the first login.



Change the password policy of the tenant account to ensure that the password does not expire. This method is similar to the method for the system administrator to modify the password policy.

----End

5.1.3 Quiz

Can an MSP manage tenant devices if the MSP is not authorized to manage tenant accounts?

5.2 Network Design

5.2.1 Introduction

5.2.1.1 Objectives

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

- Configure network templates.
- Implement site design and configuration.

5.2.1.2 Networking Topology

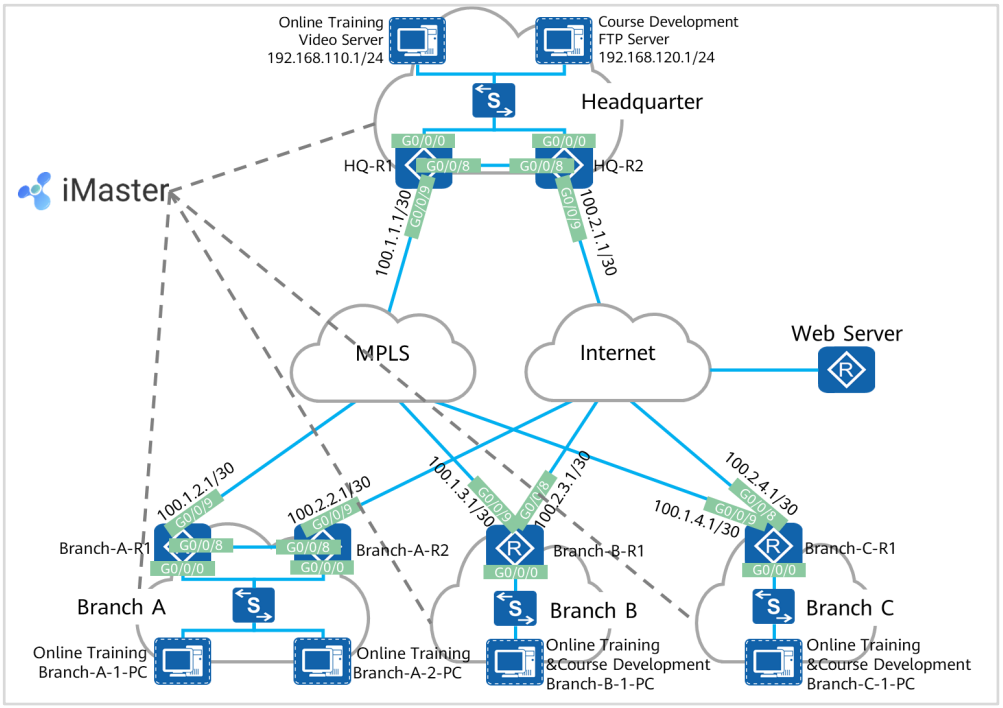


Figure5-2 SD-WAN topology

The figure shows the interconnection IP addresses. The headquarters and Branch A are connected to the MPLS network and Internet through dual egresses and links, and Branch B and Branch C are connected to the MPLS network and Internet through a single egress and dual links. Two links connect the MPLS network and Internet respectively, and the MPLS network and Internet are isolated from each other. Devices connect to iMaster NCE-WAN through public IP addresses.

5.2.1.3 Lab Background

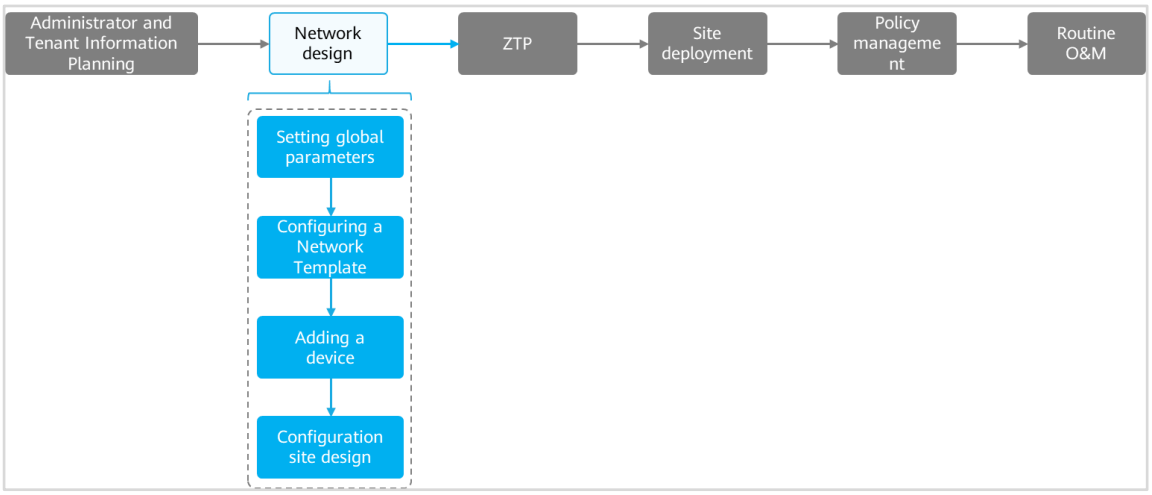
An enterprise needs to deploy new sites. To quickly deploy network services and simplify O&M, the enterprise deploys the iMaster NCE-WAN solution.

Network planning and management personnel need to construct a network using iMaster NCE-WAN based on the network topology and requirements.

5.2.2 Lab Tasks

5.2.2.1 Configuration Roadmap

To deploy iMaster NCE-WAN, perform the following steps. This lab mainly describes how to configure the network design function of iMaster NCE-WAN.



The configuration roadmap is as follows:

1. Log in to the system using the tenant account.
2. Configure global network parameters.
3. Configure a network profile.
4. Add devices.
5. Configure site design.

5.2.2.2 Configuration Procedure

Step 1 Log in to the system using the tenant account.

Use the created tenant name and password to log in to the system.

For details about how to log in using the tenant account, see *Administrator Configuration Lab*.

Step 2 Configure global parameters.

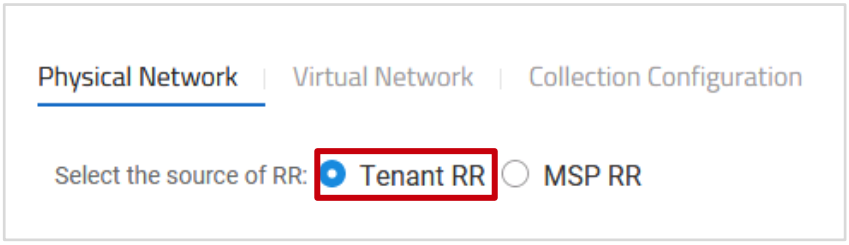
Global configuration parameters involved in the tenant network:

- Physical network: global parameters including transport network, IPsec encryption, device activation security, and link connectivity detection parameters, route selection policy, and admin account and password
- Virtual network: AS number of BGP routes, resource pool, and DNS
- Collection configuration: application traffic, application quality, and WAN link traffic

Configure physical network parameters.

Choose Design > Network Design > Network Settings > Physical Network, and configure the RR source, transmission network and IPsec encryption parameters, device activation security parameters, link connectivity detection parameters, route selection policy, and admin account and password.

Select the tenant's RR.



NOTE

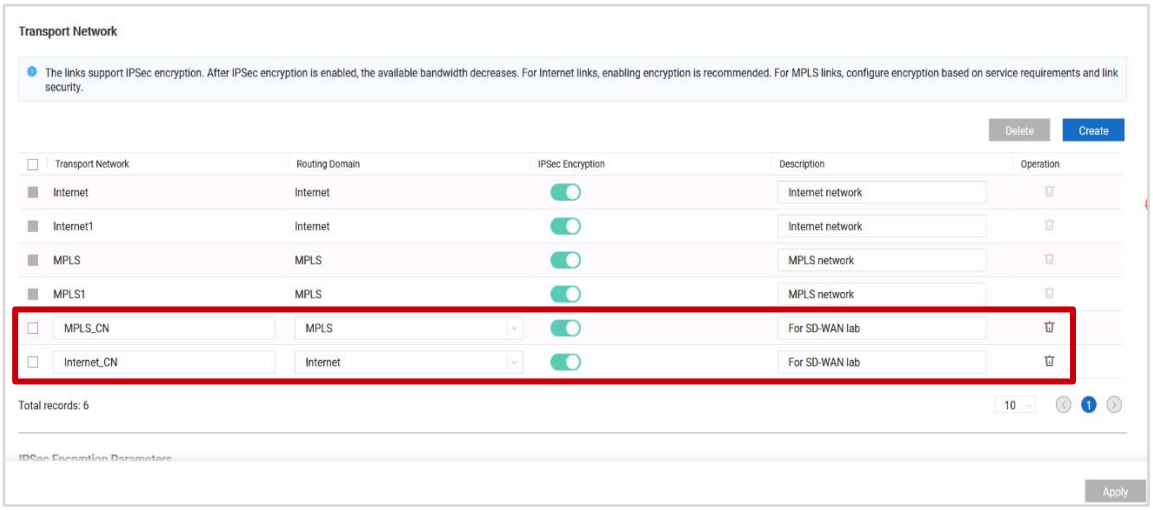
Tenant's RR: If a tenant needs to interconnect only with its own WAN and use its own RR, select the tenant's RR.

MSP's RR: If a tenant requires communication between the WAN and traditional MPLS VPN, select the RR provided by the MSP.

If the MSP provides the RR, you need to add a device on the MSP and configure the device as the RR.

This lab does not involve interworking with the traditional MPLS VPN. Therefore, select the tenant RR.

Configure the transport network and define the name of the link used by the tenant. Create two links. Name link 1 MPLS_CN, set the routing domain to MPLS, and enable link encryption. Name link 2 Internet_CN, set the routing domain to Internet, and enable link encryption.

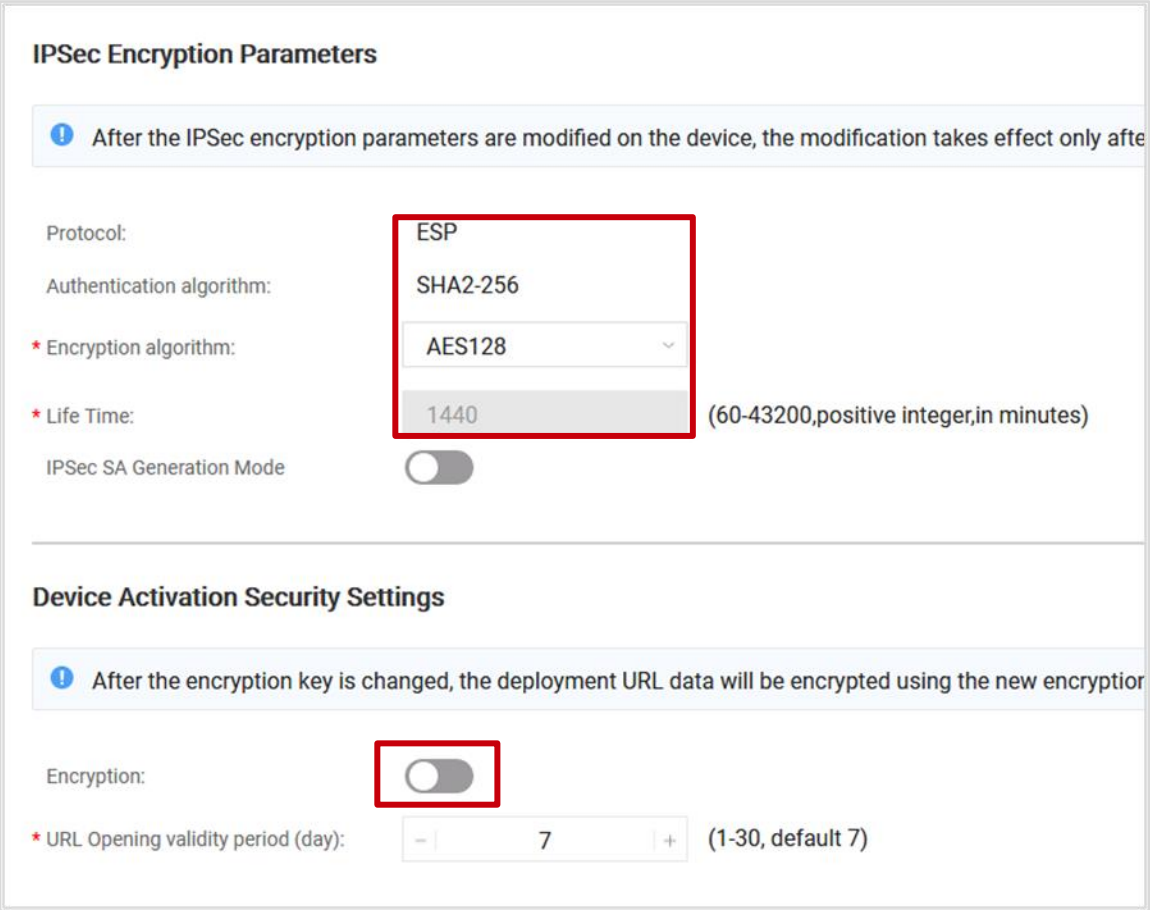


NOTE

By default, iMaster NCE-WAN has four transport network links, which cannot be deleted.

A routing domain is mainly used to isolate links. If the networks connected by two links can communicate with each other, the two links need to be configured in the same routing domain. If the networks connected by the two links cannot communicate with each other, the two links need to be configured in different routing domains.

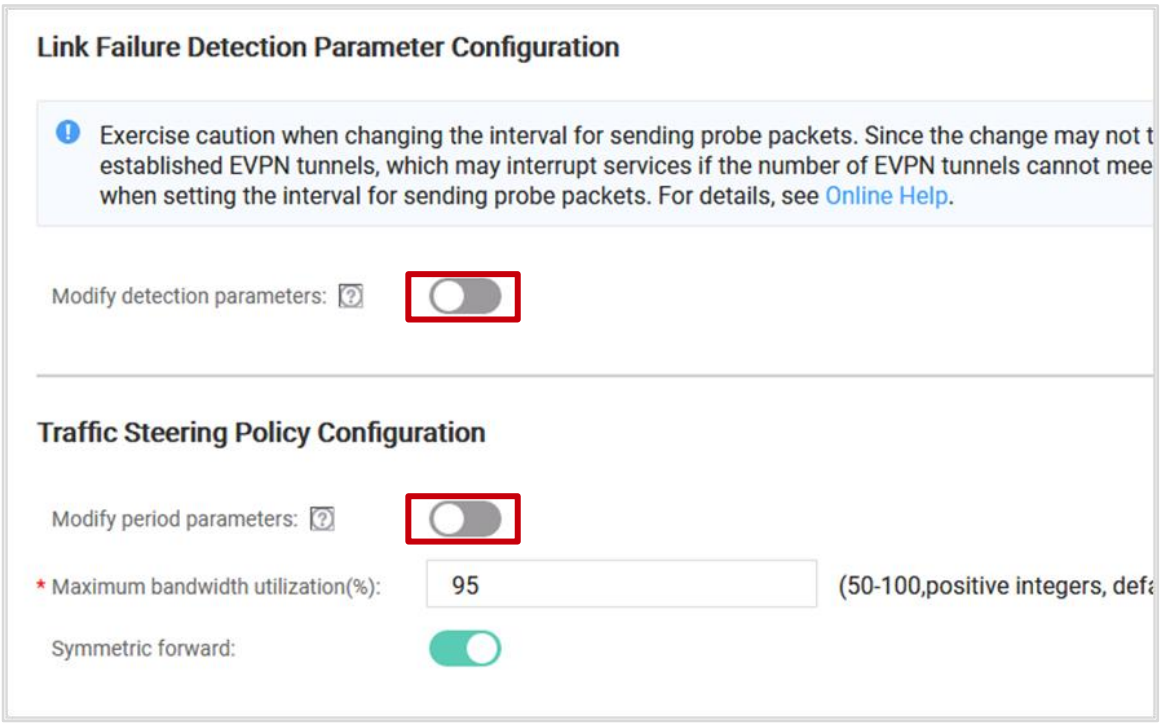
Configure security parameters, set the IPsec encryption algorithm to AES128, cancel the IPsec SA generation mode, and cancel the security configuration on the device.



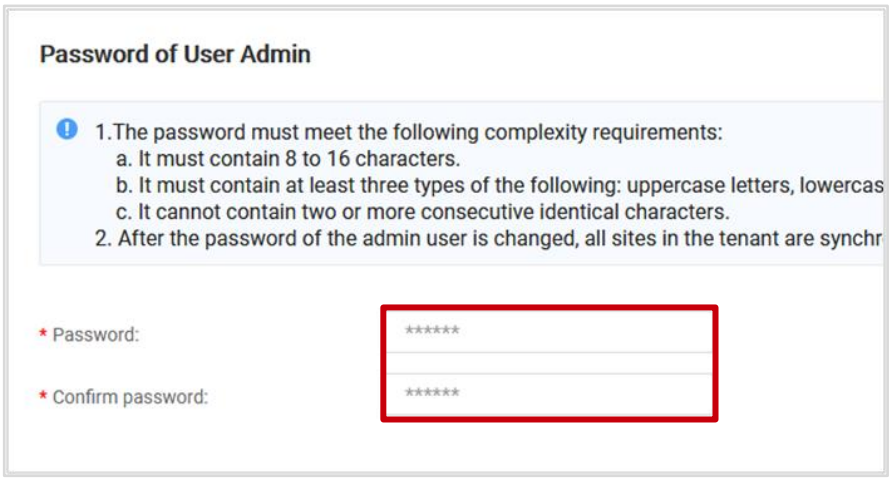
NOTE

If the EVPN mode is used and dual-gateway sites need to be deployed, you need to cancel the IPsec SA generation mode.

Retain default setting of link connectivity detection parameters and route selection parameters.



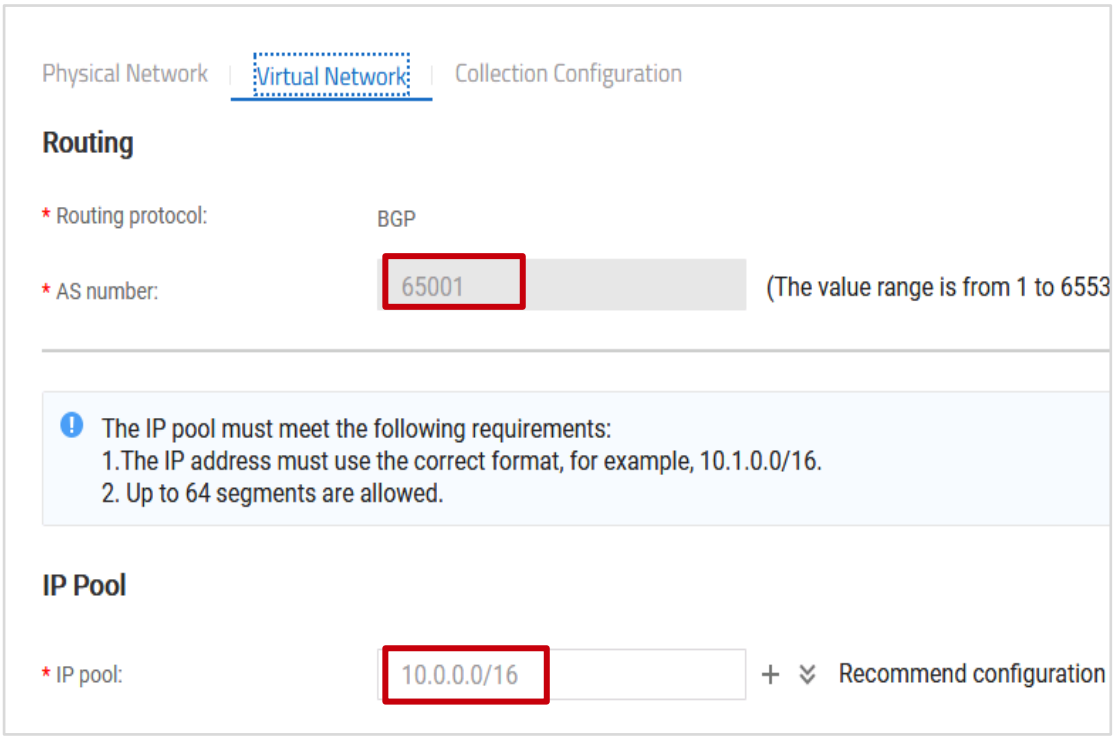
Set the password of the admin account to Huawei@123.



Click Apply.

Configure virtual network parameters.

Choose Design > Network Design > Network Settings > Virtual Network and configure the BGP AS number (65001) and address pool (10.0.0.0/16) of the virtual network.

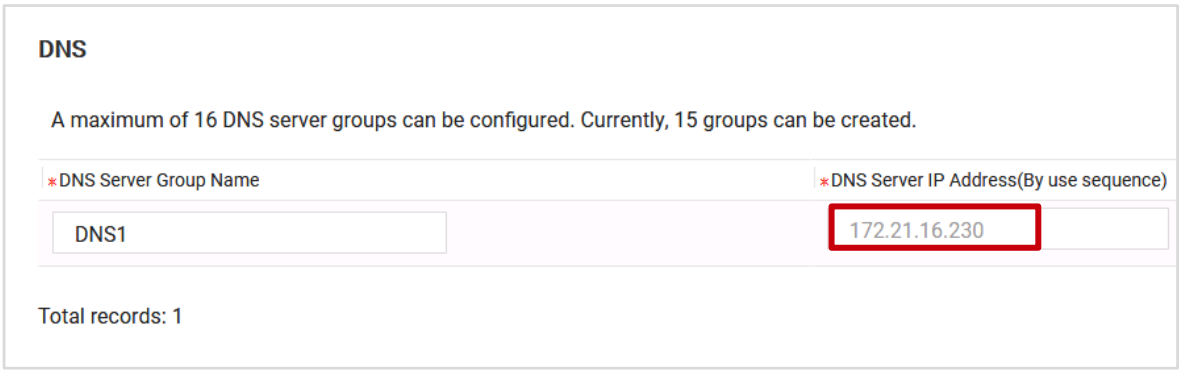


NOTE

AS number: specifies the number of the local AS. Under the same tenant account, sites that are deployed using iMaster NCE-WAN belong to this AS.

Address pool: The address pool is used to allocate IP addresses to a loopback interface of a CPE, an interface of a tunnel, an interface of the interlink, and a tunnel interface.

Configure the DNS server address as 172.21.16.230.



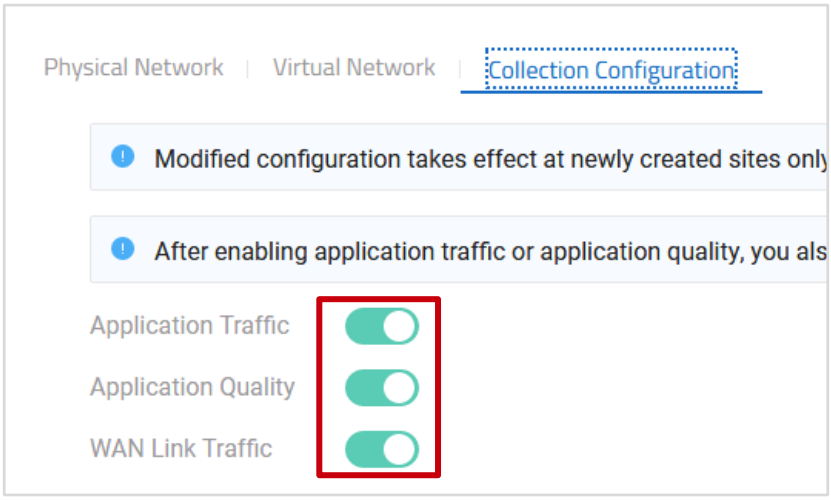
NOTE

The DNS server provides the domain name resolution service for Internet access traffic of the enterprise.

Click Apply.

Configure collection parameters.

Choose Design > Network Design > Network Settings > Collection Configuration to enable application traffic, application quality, and WAN link traffic collection.



NOTE

Network Traffic: After this function is enabled, you can collect statistics on inter-site traffic and inter-site application traffic of all sites.

Application Quality: After this function is enabled, the system can collect statistics on the AQM distribution of all applications and the top 5 applications with the worst AQM.

WAN Link Traffic: After this function is enabled, inter-site link traffic can be monitored in real time.

Step 3 Configure a network template.

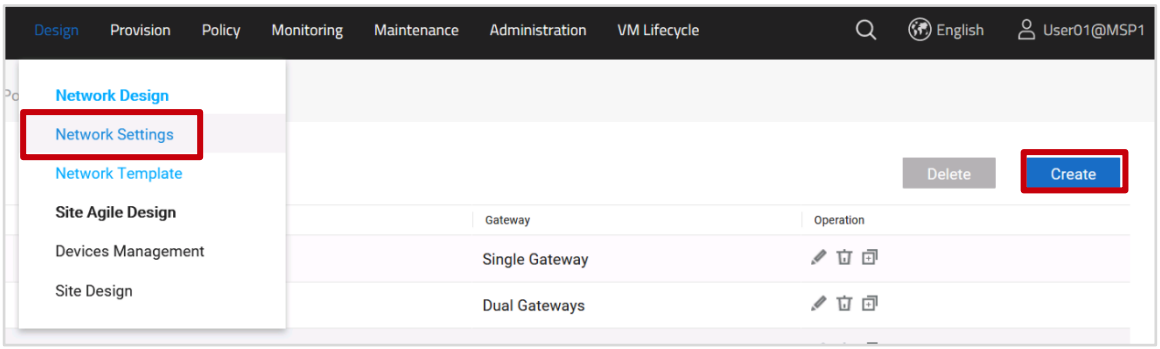
When adding multiple sites, you often need to configure the same gateway type, the same number of WAN links, and the same transport network for them.

By customizing a link template, you can modularize repeated configuration. When configuring a site, you can use a link template to automatically fill in the same configuration, improving the configuration efficiency.

Once a link template is used by a site, only the template name and description can be modified. Other parameters cannot be modified. Plan the data before creating a site template.

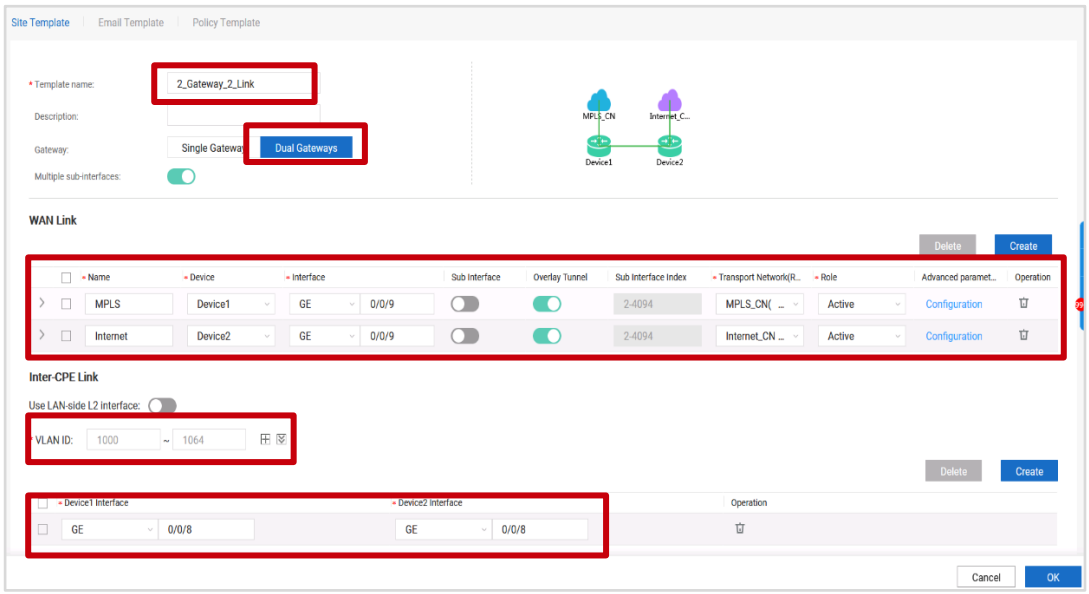
Configure a network template.

Choose Design > Network Design > Network Template to create a network template.



There are two types of network models in the lab environment.

- Dual-gateway dual-uplink: The headquarters and Branch A use this network model. The template name is 2_Gateway_2_Link. CPE 1 uses G0/0/9 to connect to the MPLS network, and CPE 2 uses G0/0/9 to connect to the Internet. CPEs are connected through G0/0/8, and the VLAN ID ranges from 1000 to 1064.

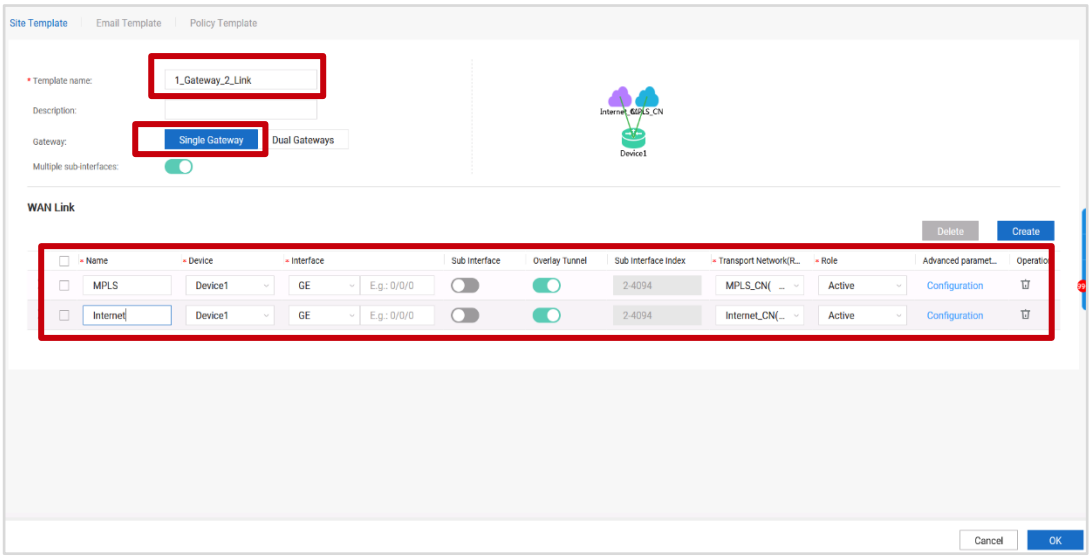


NOTE

The physical interfaces used by the internal link between two gateways must of the same type.

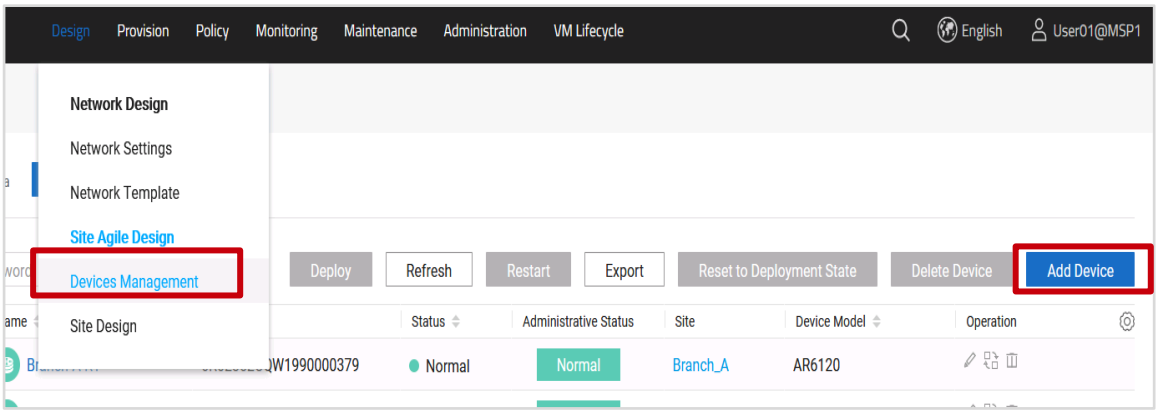
In a dual-gateway scenario, iMaster NCE-WAN configures different sub-interfaces for different departments (VPNs) on the interfaces of the internal link between the dual gateways to isolate different departments. The number of VLAN IDs must be the same as the number of departments.

- Single-gateway dual-uplink: Branch B and Branch C use this network model. The template name is 1_Gateway_2_Link. The CPE uses G0/0/9 to connect to the MPLS network and G0/0/8 to connect to the Internet.

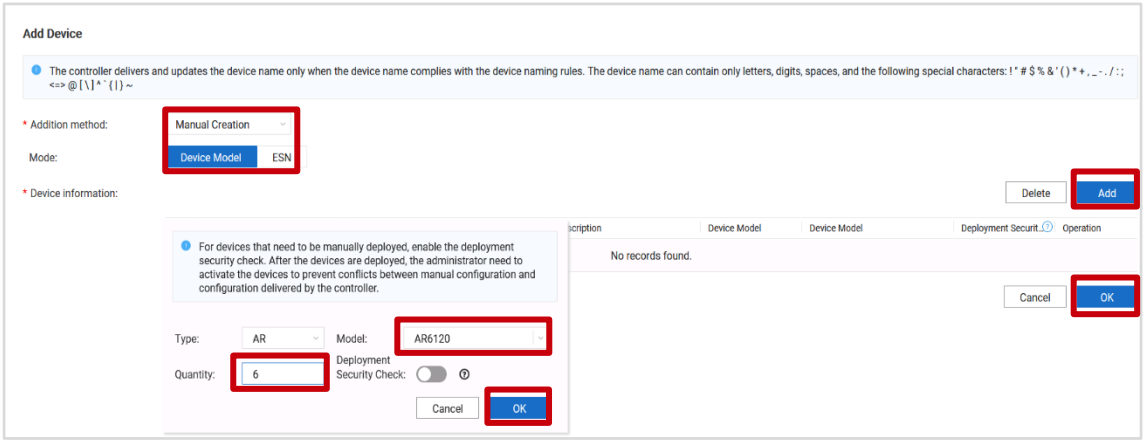


Step 4 Add devices.

 # In this lab, six AR6120s are used. Choose Design > Site Agile Design > Devices Management and click Add Device.



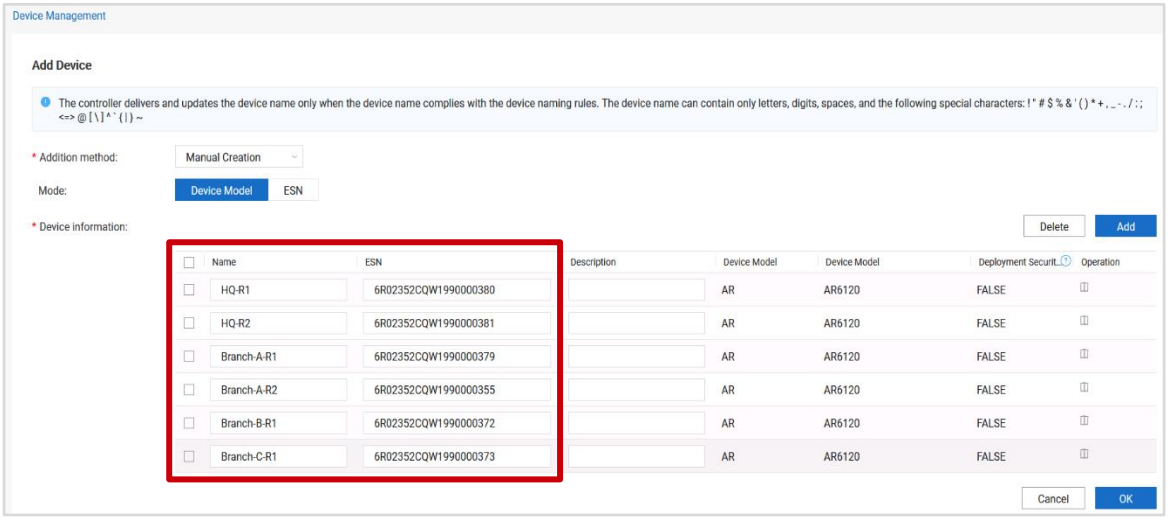
 # Add six AR6120s manually.



 # Configure the device name and ESN.

The following table shows the mapping between devices and ESNs.

Device Name	ESN
HQ-R1	6R02352CQW1990000380
HQ-R2	6R02352CQW1990000381
Branch-A-R1	6R02352CQW1990000379
Branch-A-R2	6R02352CQW1990000355
Branch-B-R1	6R02352CQW1990000372
Branch-C-R1	6R02352CQW1990000373



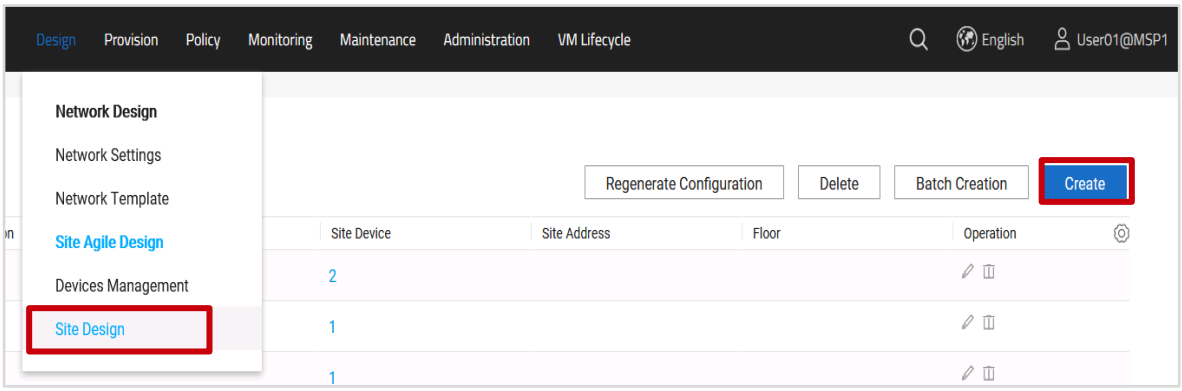
NOTE

The selected device model must be the same as the actual device model.

The ESN is optional. However, a large number of devices exist on the live network, and errors may occur when devices go online. Therefore, you are advised to enter the ESN.

Step 5 Configure site design.

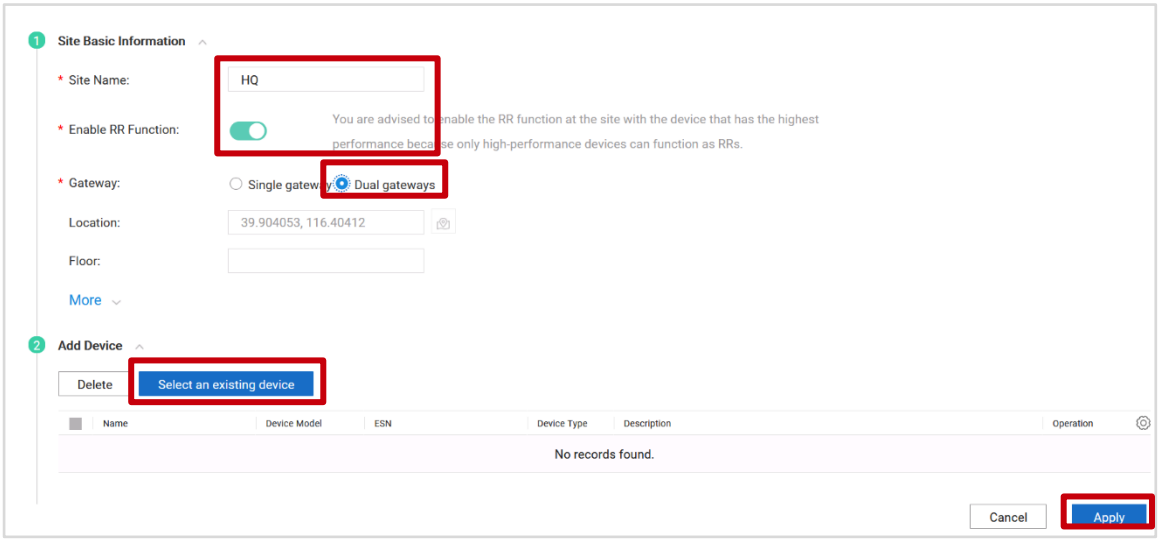
Choose Design > Site Agile Design > Site Design and click Create.



This lab involves four sites: HQ, Branch_A, Branch_B and Branch_C.

Site Name	Gateway Type	Device	RR or Not
HQ	Dual-gateway	HQ-1, HQ-2	Yes
Branch_A	Dual-gateway	Branch-A-R1, Branch-A-R2	No
Branch_B	Single gateway	Branch-B-R1	No
Branch_C	Single gateway	Branch-C-R1	No

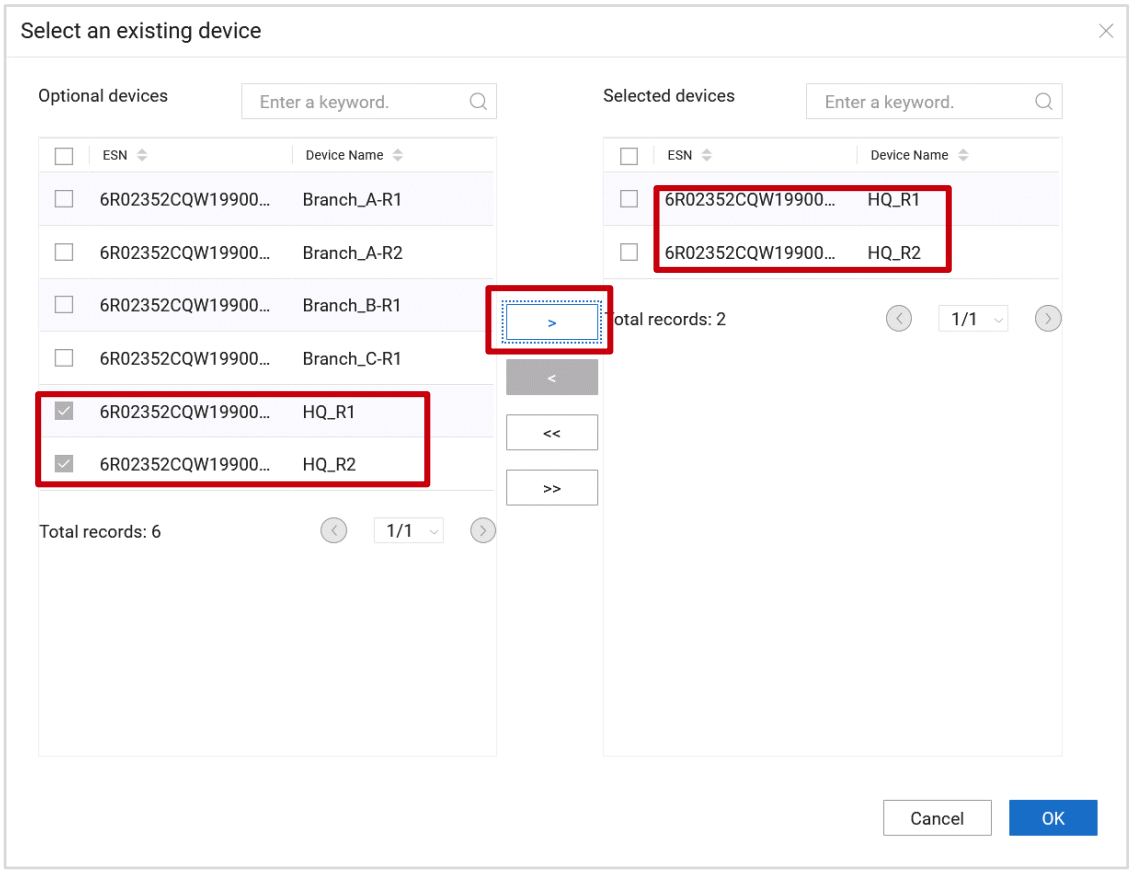
#The HQ site design configuration is as follows.

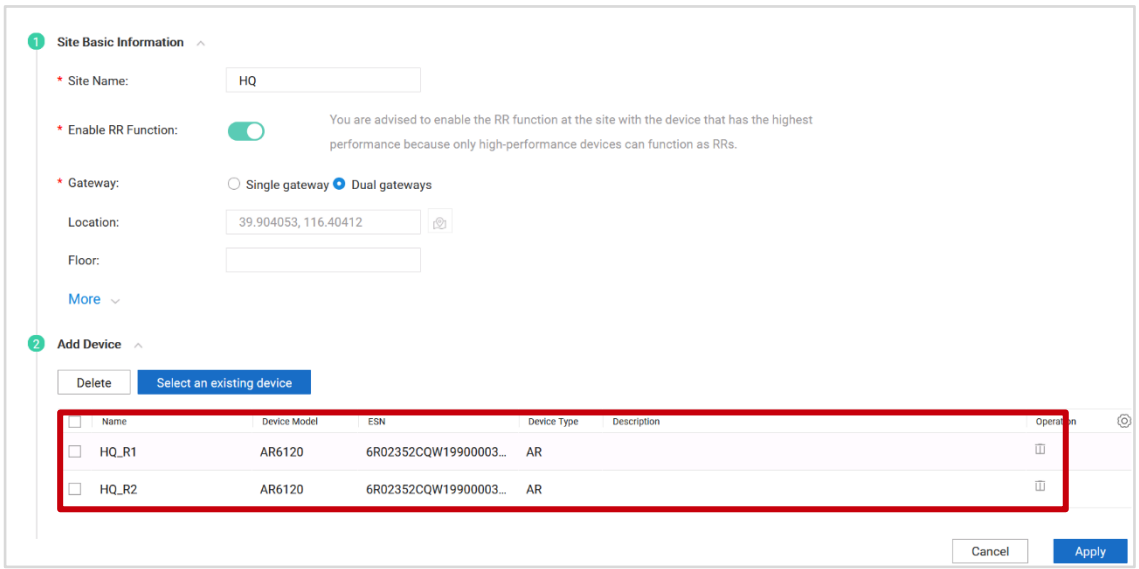


NOTE

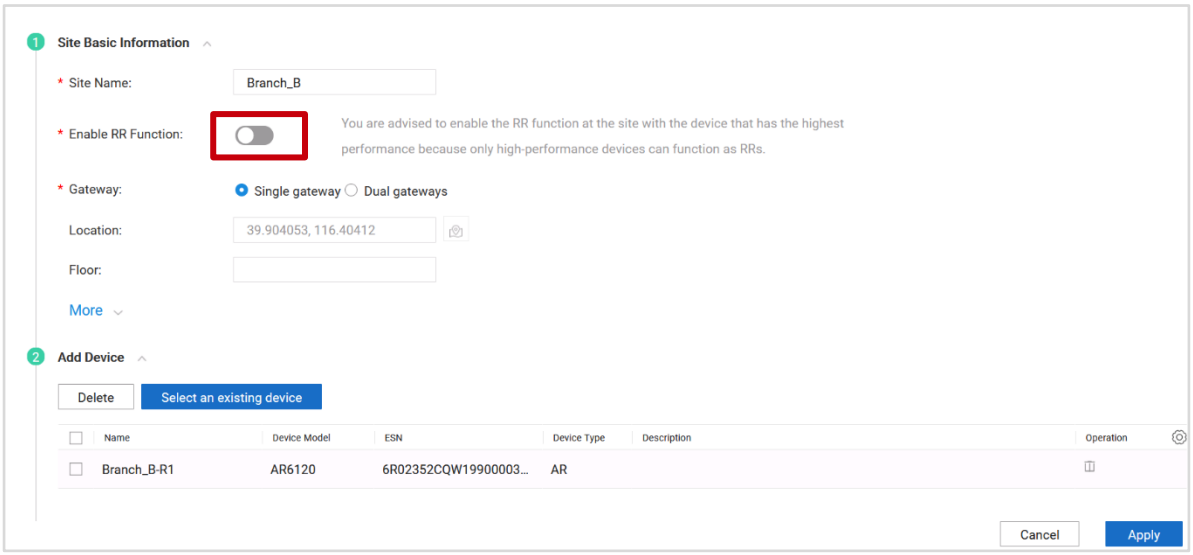
If the RR function is not enabled, only edge nodes are created. If the RR function is enabled, the RR and edge node are deployed together.

Select HQ-R1 and HQ-R2 and add them to the HQ site.

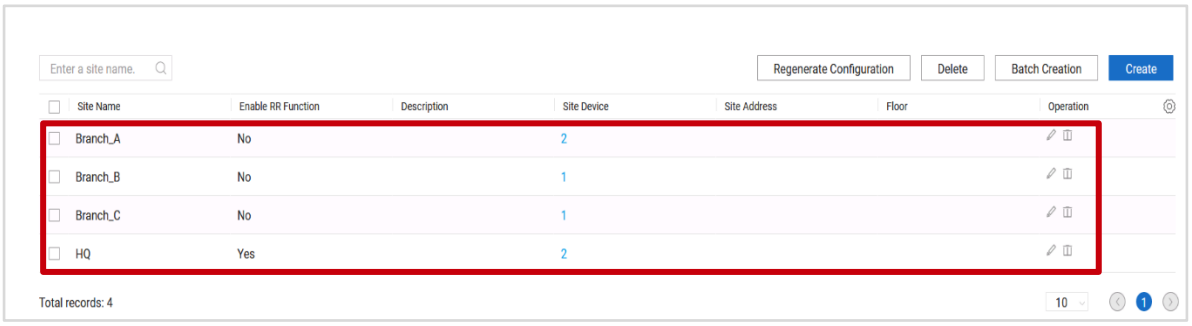




 # The configurations of Branch_A, Branch_B, and Branch_C are similar to those of the HQ site, but the RR function is not enabled.



 # The following figure shows the site design result.



----End

5.2.3 Quiz

If multiple users want to share an RR, how is the RR configured?

5.3 Device Deployment

5.3.1 Introduction

5.3.1.1 Objectives

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

- Implement email-based deployment.
- (Optional) Implement DHCP-based deployment.

5.3.1.2 Networking Topology

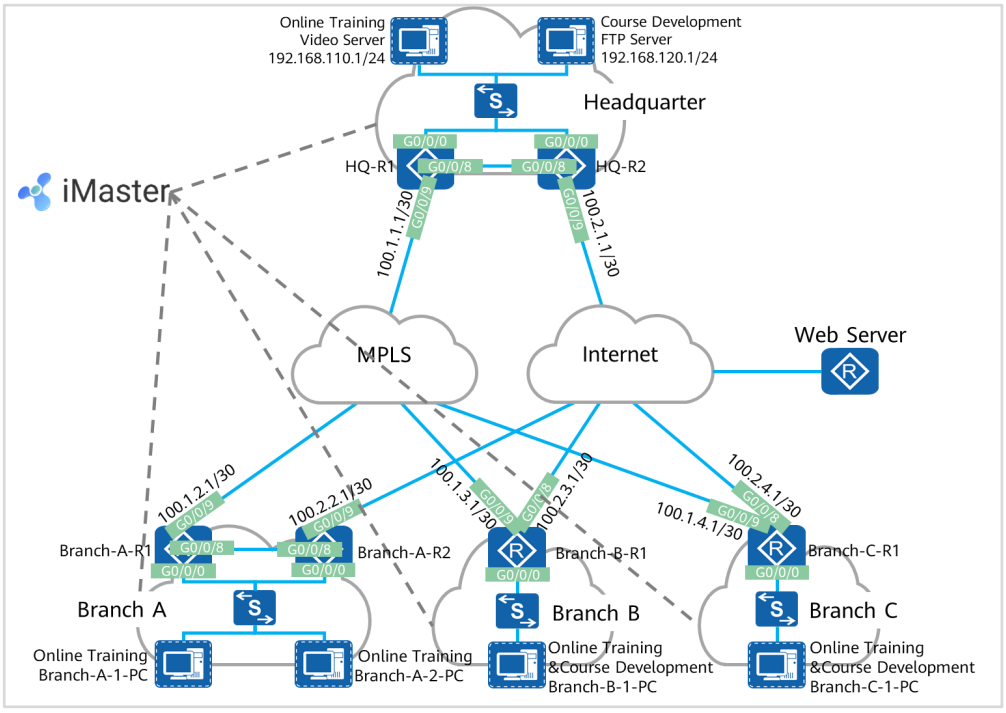


Figure5-3 SD-WAN topology

The figure shows the interconnection IP addresses. The headquarters and Branch A are connected to the MPLS network and Internet through dual egresses and links, and Branch B and Branch C are connected to the MPLS network and Internet through a single egress and dual links. Two links connect the MPLS network and Internet respectively, and the MPLS network and Internet are isolated from each other. Devices connect to iMaster NCE-WAN through public IP addresses.

5.3.1.3 Lab Background

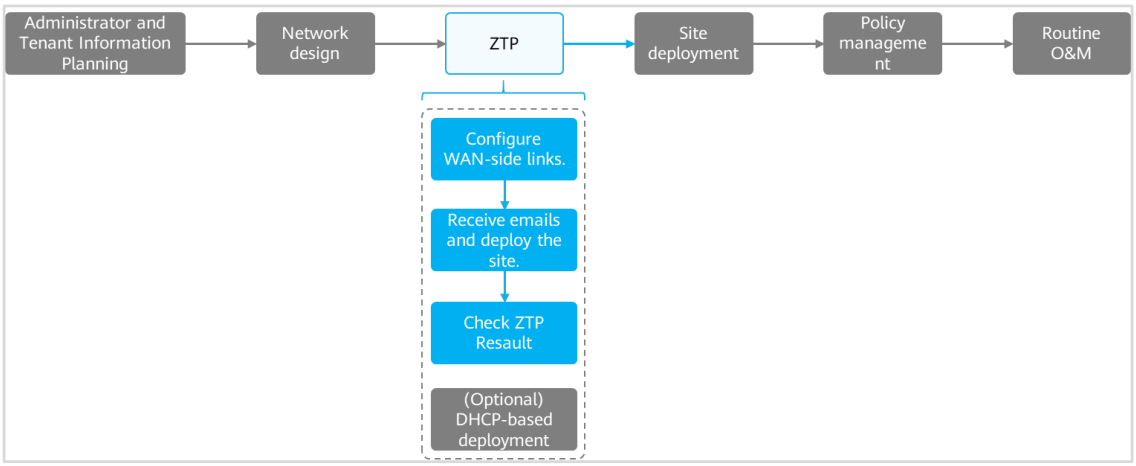
An enterprise needs to deploy new sites. To quickly deploy network services and simplify O&M, the enterprise deploys the iMaster NCE-WAN solution.

Network planning and management personnel need to construct a network using iMaster NCE-WAN based on the network topology and requirements.

5.3.2 Lab Tasks

5.3.2.1 Configuration Roadmap

To deploy iMaster NCE-WAN, perform the following steps. This lab mainly describes how to use iMaster NCE-WAN to implement deployment.



The configuration roadmap is as follows:

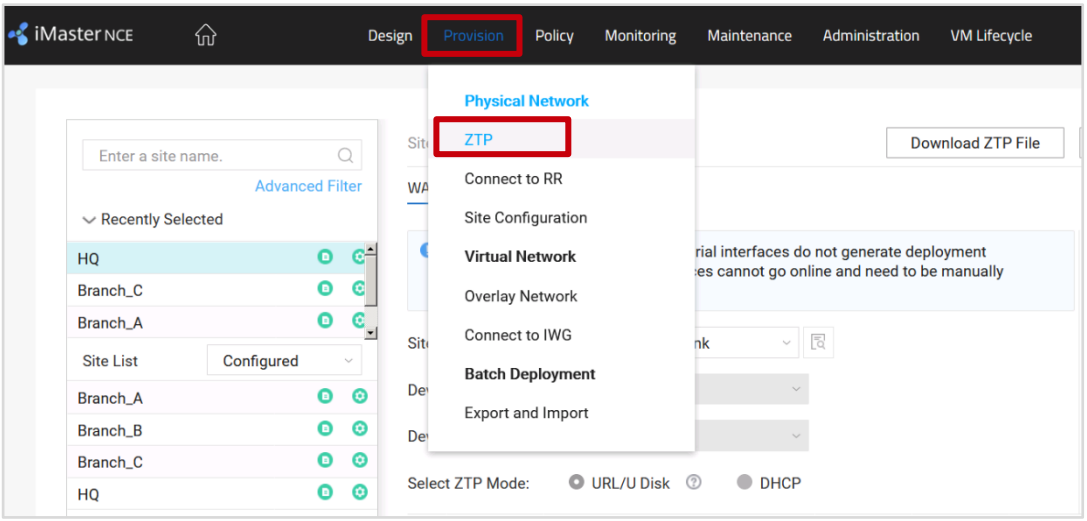
1. Configure a ZTP file.
2. Configure email sending/receiving.
3. Use the URL in the email for deployment.
4. Verify that the device is deployed successfully.
5. (Optional) Perform DHCP-based deployment.

5.3.2.2 Configuration Procedure

Step 1 Configure a ZTP template.

Configure a ZTP template.

Choose Provision > Physical Network > ZTP from the main menu.



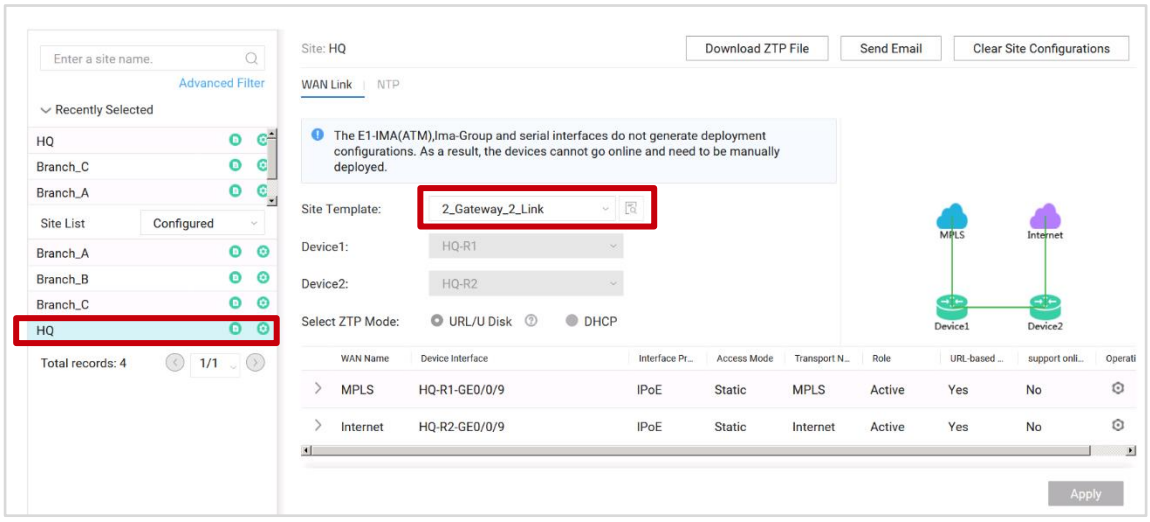
Configure ZTP templates for different sites. The ZTP planning is as follows.

Site	Template	ZTP Mode	Link Name	IP Address	Gateway	Uplink/Downlink Bandwidth
HQ	2_Gateway_2_Link	URL	MPLS	100.1.1.1/30	100.1.1.2	1000/1000
			Internet	100.2.1.1/30	100.2.1.2	1000/1000
Branch_A	2_Gateway_2_Link	URL	MPLS	100.1.2.1/30	100.1.2.2	1000/1000
			Internet	100.2.2.1/30	100.2.2.2	1000/1000
Branch_B	1_Gateway_2_Link	URL	MPLS	100.1.3.1/30	100.1.3.2	1000/1000
			Internet	100.2.3.1/30	100.2.3.2	1000/1000
Branch_C	1_Gateway_2_Link	URL	MPLS	100.1.4.1/30	100.1.4.2	1000/1000
			Internet	100.2.4.1/30	100.2.4.2	1000/1000

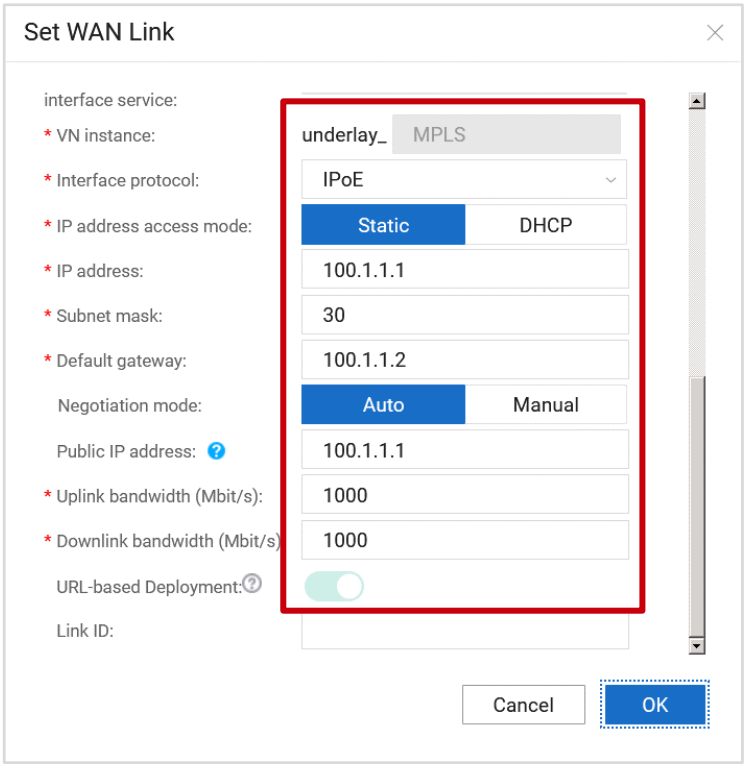
Site	NTP Mode	Authentication or Not	Device	Link	NTP Server Address
HQ	Manual setting	No authentication	HQ-R1	MPLS	100.1.1.2
			HQ-R2	Internet	100.2.1.2
Branch_A, Branch_B, Branch_C	Automatic synchronization with the parent site				

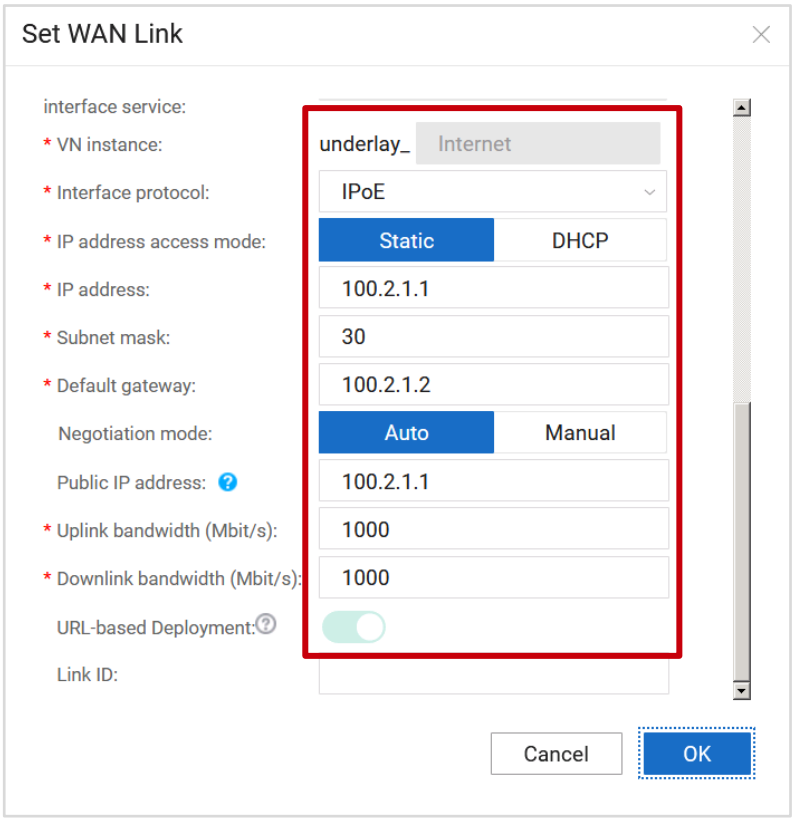
Configure ZTP data based on the ZTP plan.

The HQ site is used as an example. The configuration methods for other sites are similar. Select the HQ site, use the site template 2_Gateway_2_Link, and click the configuration button to configure WAN link attributes.

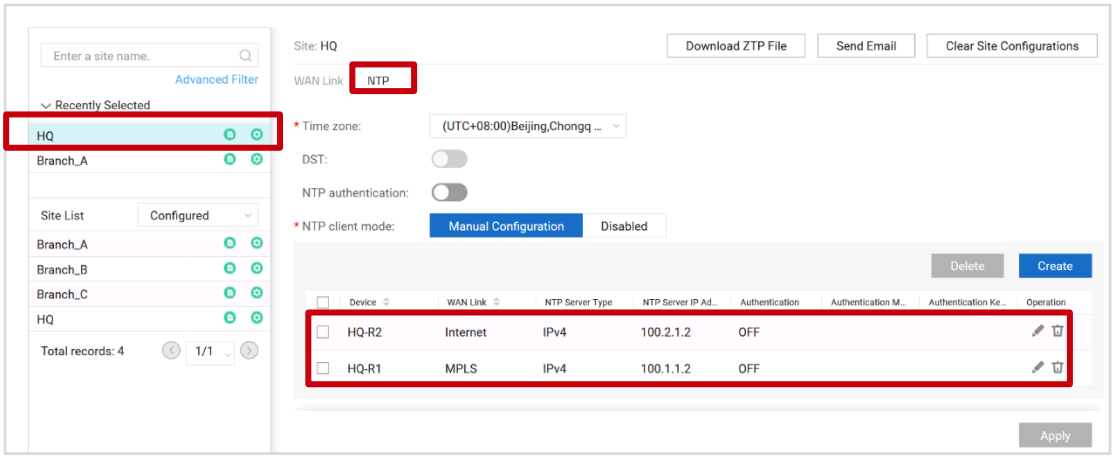


 # Change the virtual network's instance name, IP address, gateway, and uplink and downlink bandwidths to be the same as planned ones.





Configure the NTP server at the HQ based on the ZTP plan.

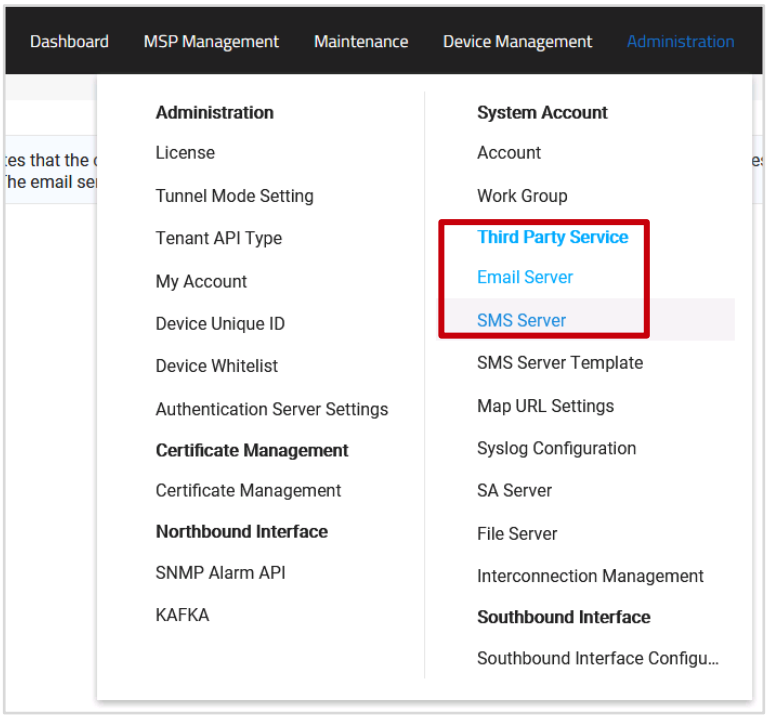


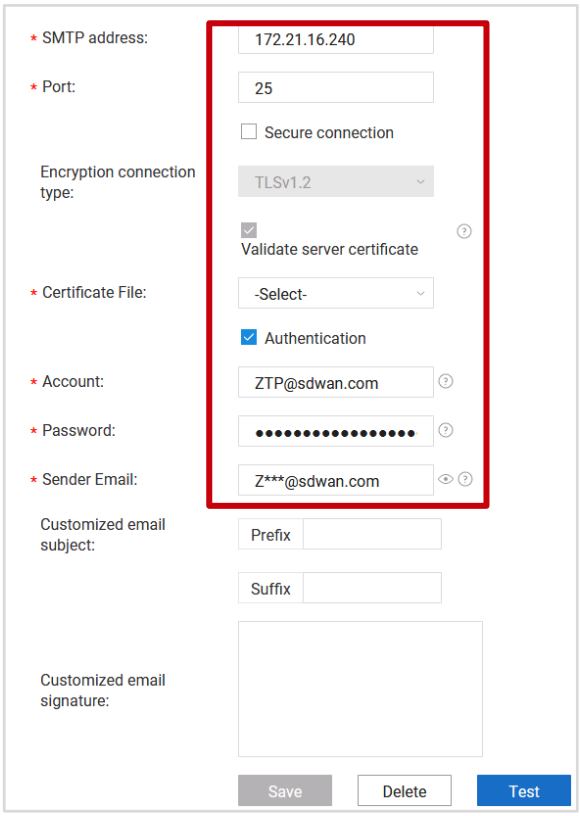
Configure other sites based on the ZTP plan by referring to the ZTP configuration method for the HQ site.

Step 2 Configure email sending/receiving.

Confirm the email server configuration.

Log in to iMaster NCE-WAN using the administrator account (admin/Huawei12#$), and choose Administration > Third Party Service > Email Server to check whether the email server has been configured.

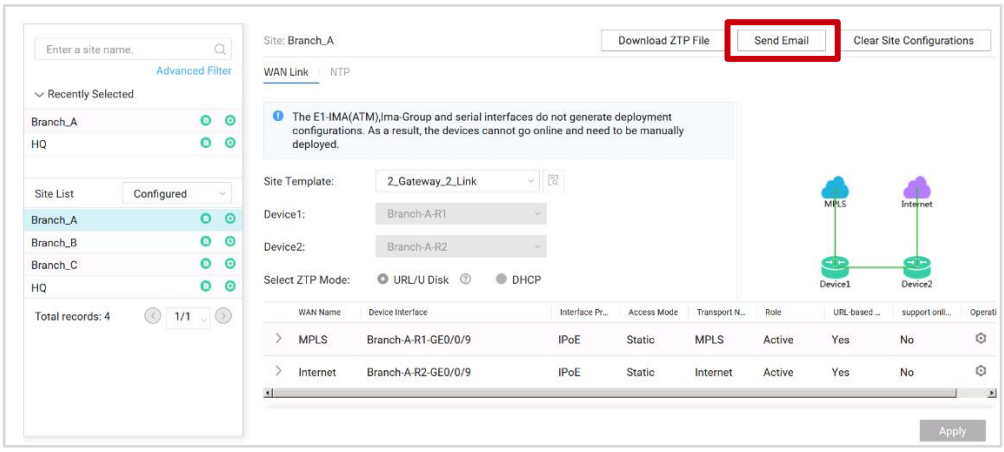




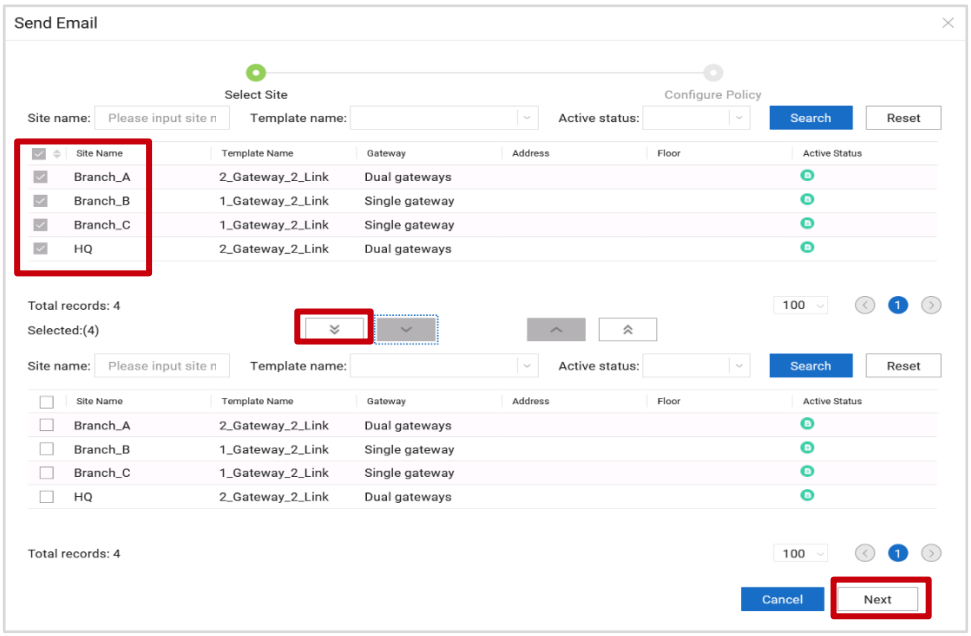
Each site has an email address for receiving deployment emails. The email account plan is as follows.

Site	Email Address	IP Address of the Deployment PC	User Name/Password of the Deployment PC
HQ	hq@sdwan.com	172.21.16.232	admin/Huawei@123
		172.21.16.233	admin/Huawei@123
Branch-A	branch-a@sdwan.com	172.21.16.234	admin/Huawei@123
		172.21.16.235	admin/Huawei@123
Branch-B	branch-b@sdwan.com	172.21.16.236	admin/Huawei@123
Branch-C	branch-c@sdwan.com	172.21.16.237	admin/Huawei@123

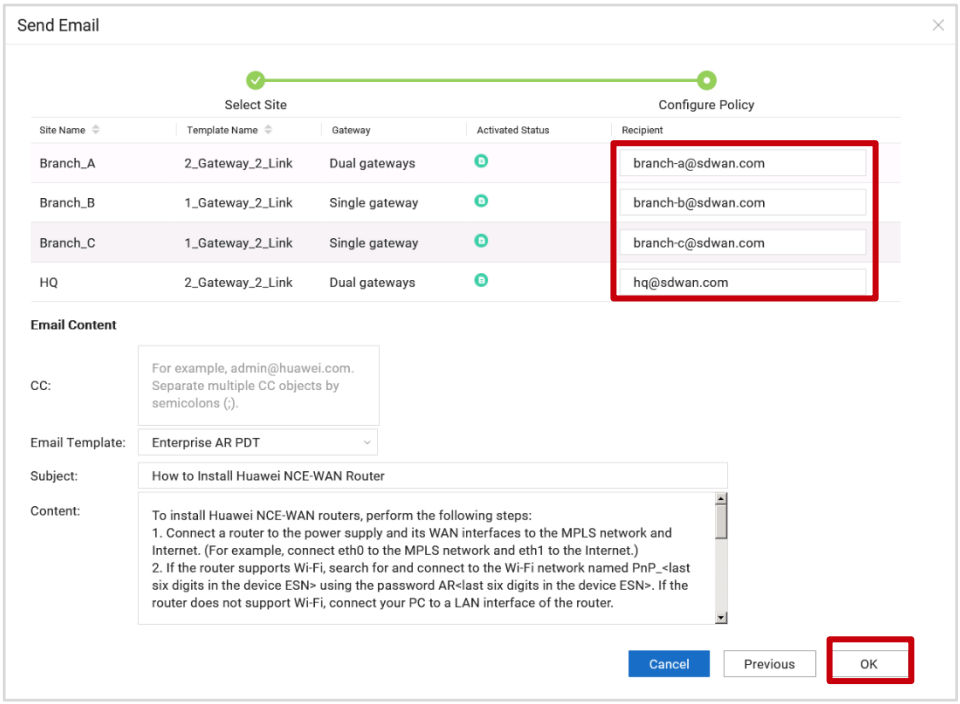
Choose Provision > Physical Network > ZTP from the main menu and click Send Email.

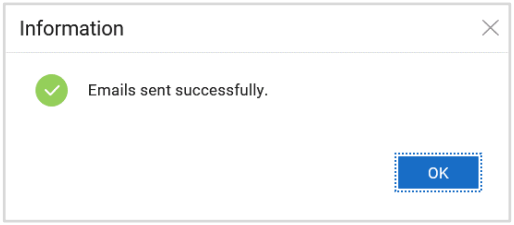


On the Send Email page, select a site and click Next.

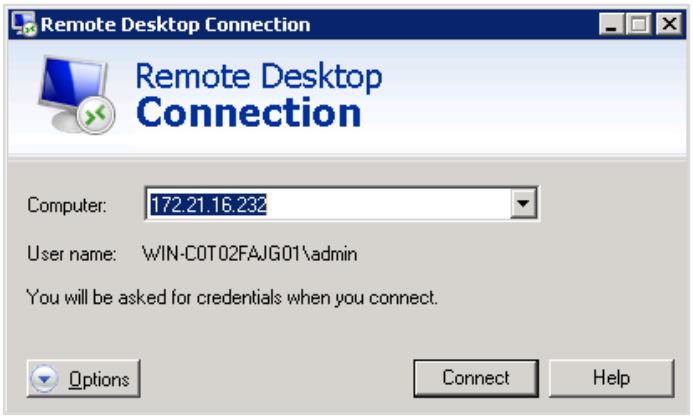


Enter the email address as planned.

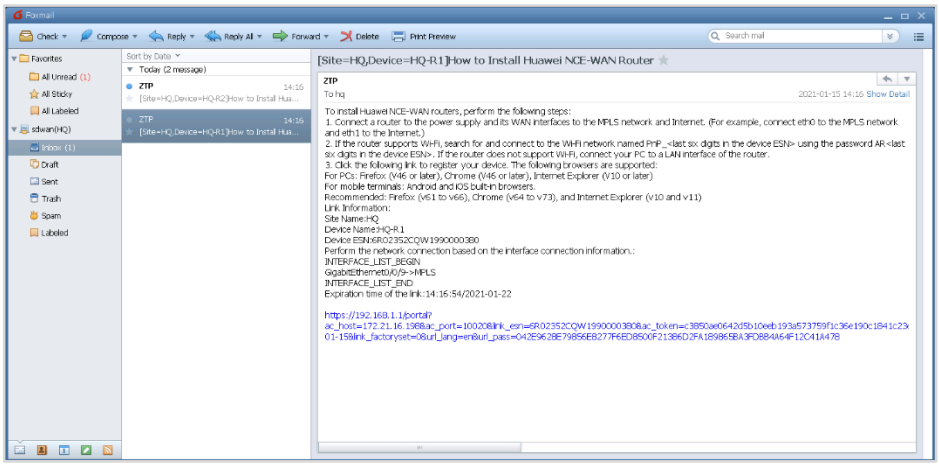




Log in to the deployment PC. For details about the login IP address, user name, and password of the deployment PC, see the email account plan.

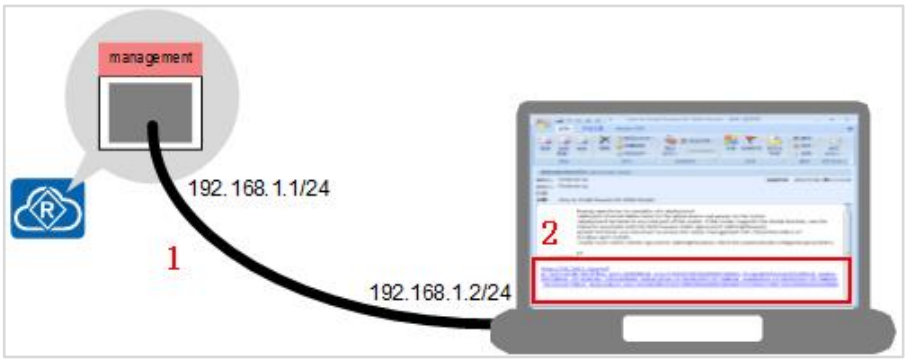


Check emails.



Use a network cable to connect the PC to the management interface of the CPE. In this experiment, the PC is connected to the CPE. The connection between the PC and the CPE is planned as follows:

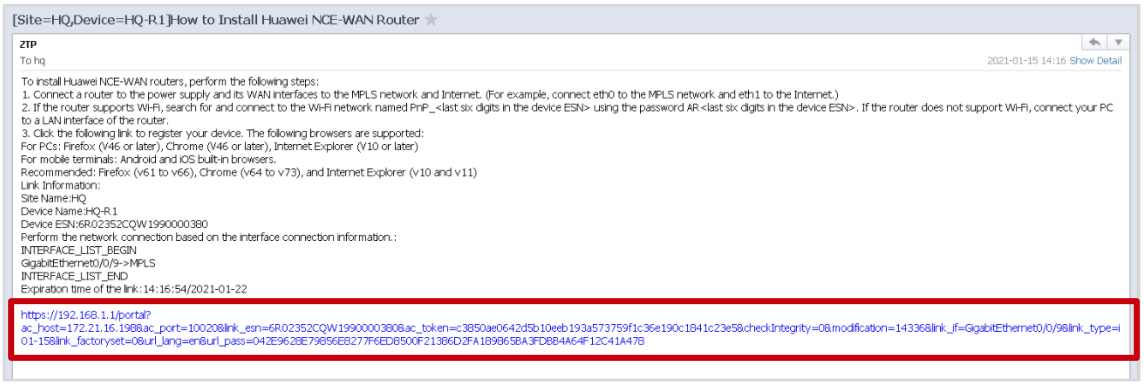
CPE	CPE Address	Login Address of the Deployment PC	Login User Name/Password of the Deployment PC
HQ-R1	192.168.1.1	172.21.16.232	admin/Huawei@123
HQ-R2	192.168.1.1	172.21.16.233	admin/Huawei@123
Branch-A-R1	192.168.1.1	172.21.16.234	admin/Huawei@123
Branch-A-R2	192.168.1.1	172.21.16.235	admin/Huawei@123
Branch-B-R1	192.168.1.1	172.21.16.236	admin/Huawei@123
Branch-C-R1	192.168.1.1	172.21.16.237	admin/Huawei@123

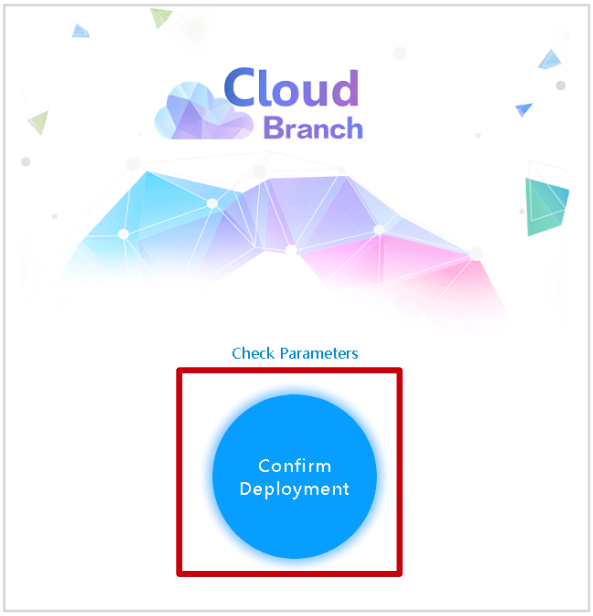


NOTE

A device's management interface is often marked with the Management or MGMT silkscreen. Management interfaces of some device models do not have this silkscreen. You can check the position of the management interface according to product documentation.

Log in to the deployment PC to perform email-based deployment. Click the link in the email and confirm the deployment in the browser.

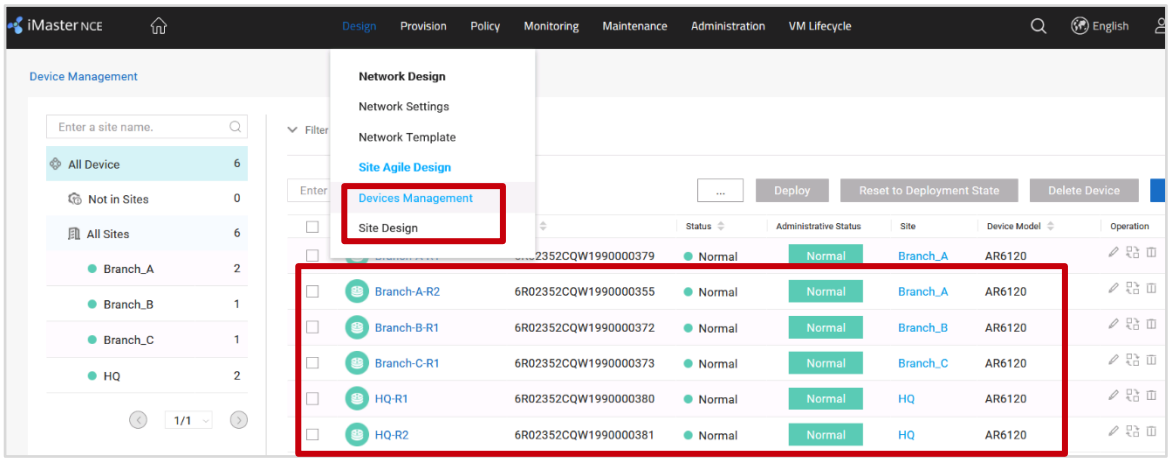




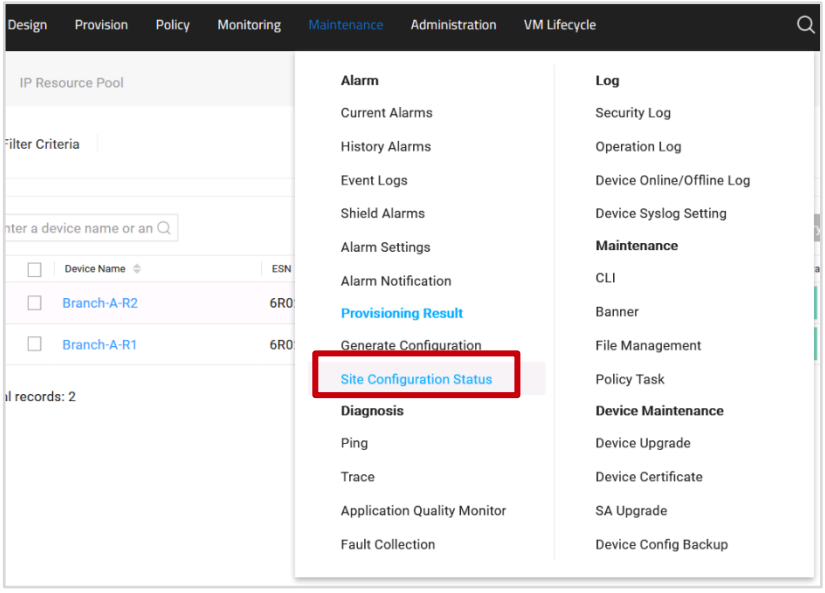
Log in to other deployment PCs and click the deployment links in the emails to deploy devices.

Step 3 Verify that the device is deployed successfully.

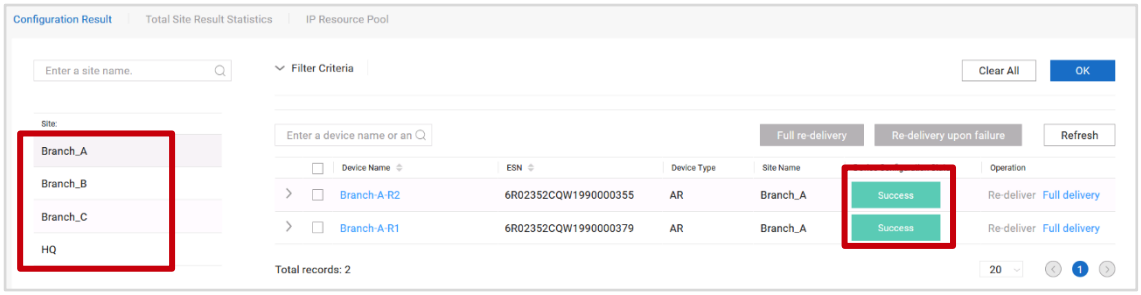
Choose Design > Site Agile Design > Devices Management and check whether the device is online.



Choose Maintenance > Provisioning Result > Site Configuration Status and check whether iMaster NCE-WAN has successfully delivered the configuration.



Check the device configuration status of each site. If the device configuration status is Success, the ZTP configuration is successfully delivered.



Step 4 (Optional) Configure DHCP-based deployment.

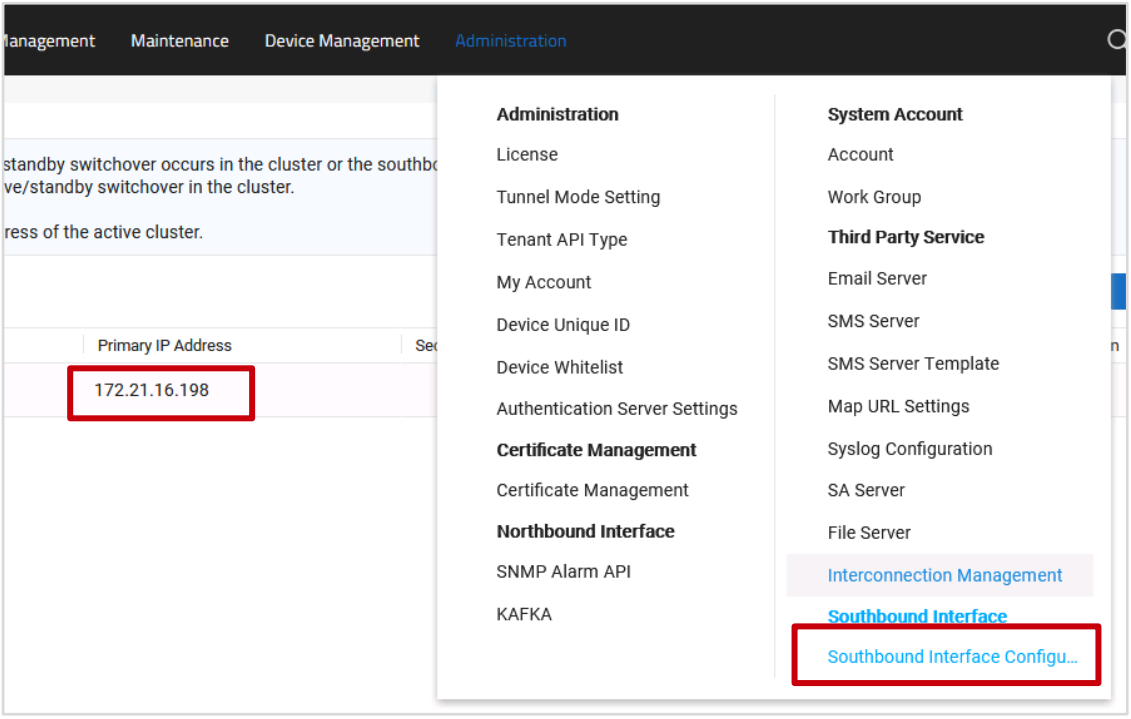
You can select either DHCP-based or email-based deployment.

This lab mainly describes DHCP-based deployment. Email-based deployment is used in the lab environment.

DHCP-based deployment can be used to implement zero-touch deployment, so the configuration of the DHCP server is very important.

The DHCP server notifies CPEs of the southbound IP address of iMaster NCE-WAN through the Option 148 field.

Log in to the system using the administrator account (the user name is admin and password is Huawei12#$), choose Administration > Southbound Interface > Southbound Interface Configuration, and check the southbound IP address of iMaster NCE-WAN.



Configure the Option 148 field on the DHCP server.

option 148 ascii agilemode=agile-cloud;agilemanage-mode=ip;agilemanage-domain=172.21.16.198;agilemanage-port=10020;

NOTE

agilemode: indicates the agile mode. In the iMaster NCE-WAN scenario, set this parameter to agile-cloud.

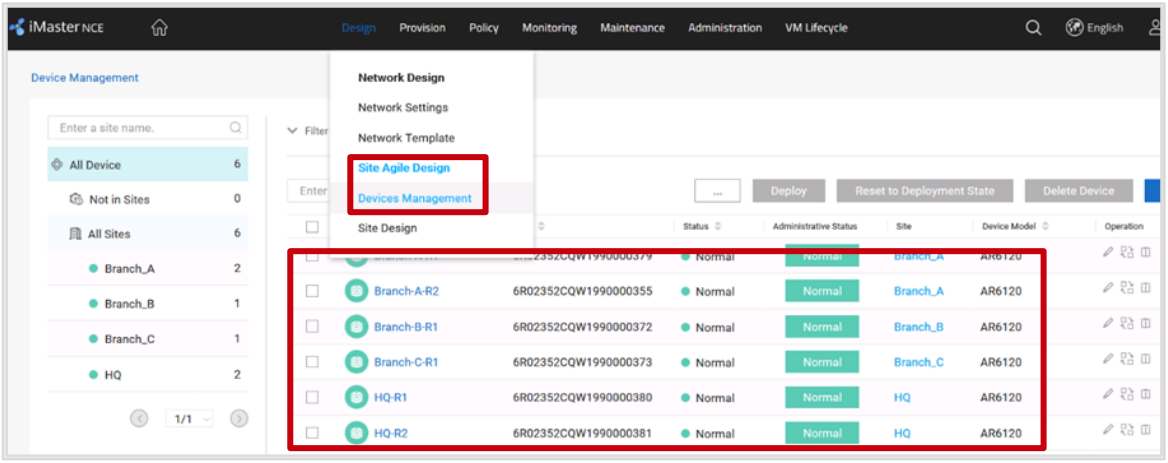
agilemanage-mode: indicates that the agilemanage-domain field is set to an IP address or a domain.

agilemanage-domain: When agilemanage-mode is set to ip, this field indicates the IP address. When agilemanage-mode is set to domain, this field indicates the domain name.

agilemanage-port: indicates the port number of iMaster NCE-WAN allocated to the DHCP client.

After obtaining the IP address, the CPE proactively registers with iMaster NCE-WAN based on Option 148.

Choose Design > Site Agile Design > Devices Management and check whether the device is successfully registered.



NOTE

Only the initialized devices that are not configured can automatically go online through DHCP.

If the device has been configured, run the reset saved-configuration command to delete the configuration and then restart the device.

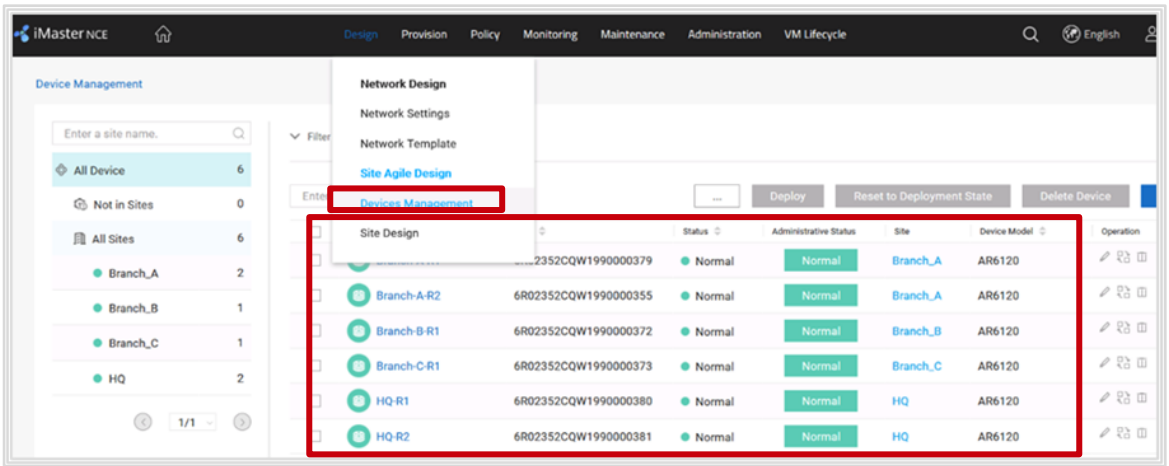
Configure ZTP templates.

The ZTP template configuration method is similar to that in email-based deployment and is not provided.

After the ZTP templates are configured, iMaster NCE-WAN automatically delivers the configuration. After receiving the configuration, the device goes online again.

Verify that the device is deployed successfully.

Choose Design > Site Agile Design > Devices Management and check whether the device goes online again.



----End

5.3.3 Quiz

Is DHCP-based deployment applicable to the scenario where an enterprise leases a carrier's network to build a backbone network?

5.4 Site Deployment

5.4.1 Introduction

5.4.1.1 Objectives

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

- Configure network templates.
- Implement site design and configuration.

5.4.1.2 Networking Topology

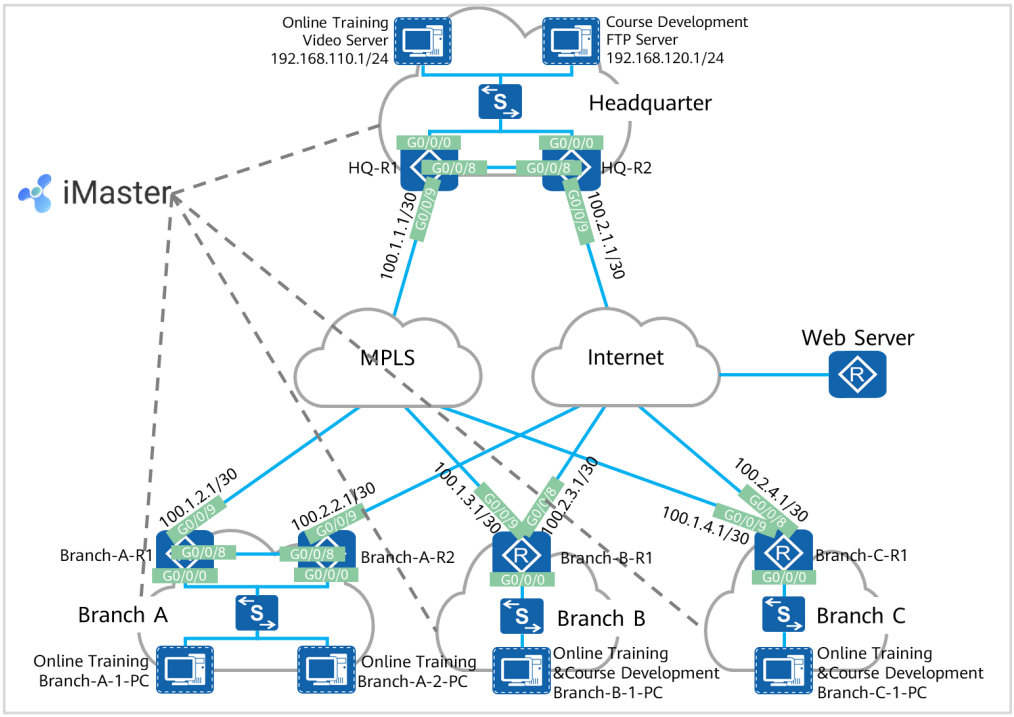


Figure5-4 SD-WAN topology

The figure shows the interconnection IP addresses. The headquarters and Branch A are connected to the MPLS network and Internet through dual egresses and links, and Branch B and Branch C are connected to the MPLS network and Internet through a single egress and dual links. Two links connect the MPLS network and Internet respectively, and the MPLS network and Internet are isolated from each other. Devices connect to iMaster NCE-WAN through public IP addresses.

5.4.1.3 Lab Background

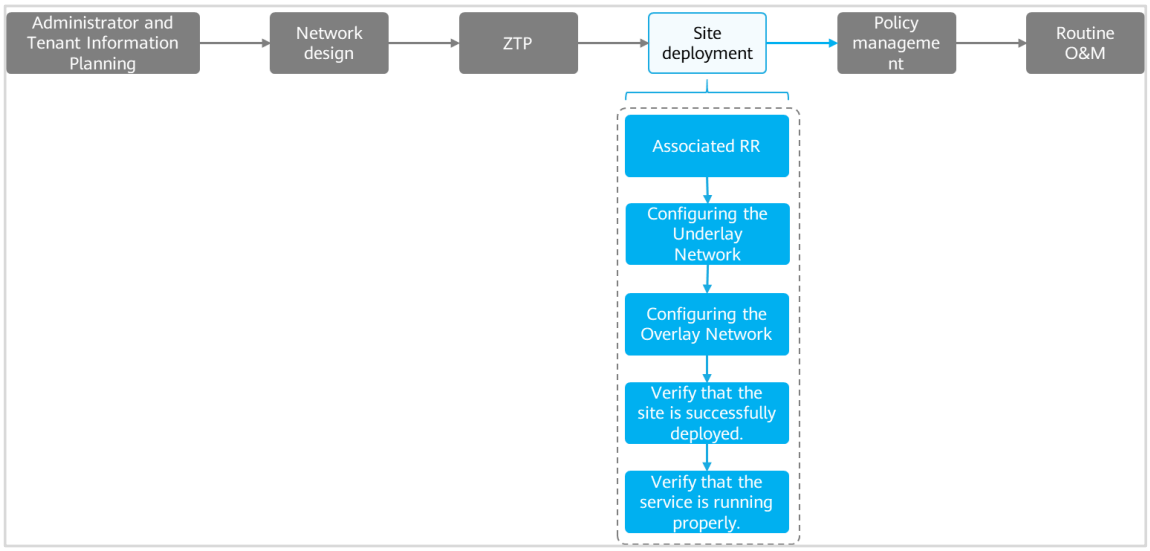
An enterprise needs to deploy new sites. To quickly deploy network services and simplify O&M, the enterprise deploys the iMaster NCE-WAN solution.

Network planning and management personnel need to construct a network using iMaster NCE-WAN based on the network topology and requirements.

5.4.2 Lab Tasks

5.4.2.1 Configuration Roadmap

To deploy iMaster NCE-WAN, perform the following steps. This lab mainly describes how to configure the network design function of iMaster NCE-WAN.



The configuration roadmap is as follows:

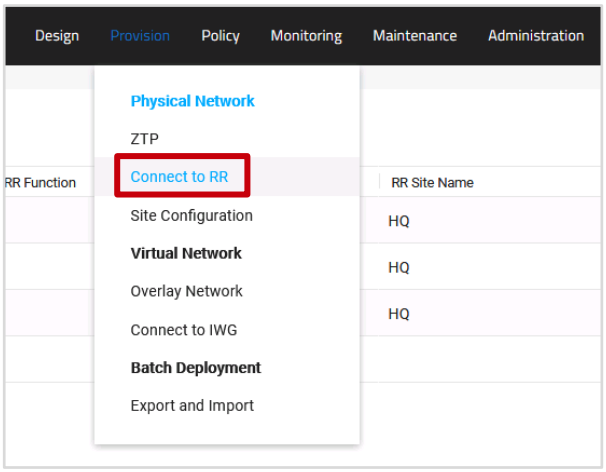
1. Associate a site with an RR.
2. Configure an underlay network.
3. Configure an overlay network.
4. Verify that the site is successfully deployed.
5. Verify that the service is running properly.

5.4.2.2 Configuration Procedure

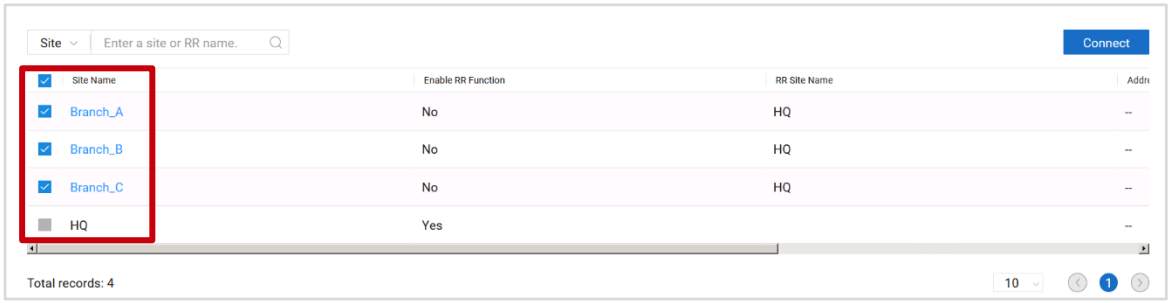
Step 1 Associate a site with an RR.

In EVPN mode, you need to associate the edge node with an RR.

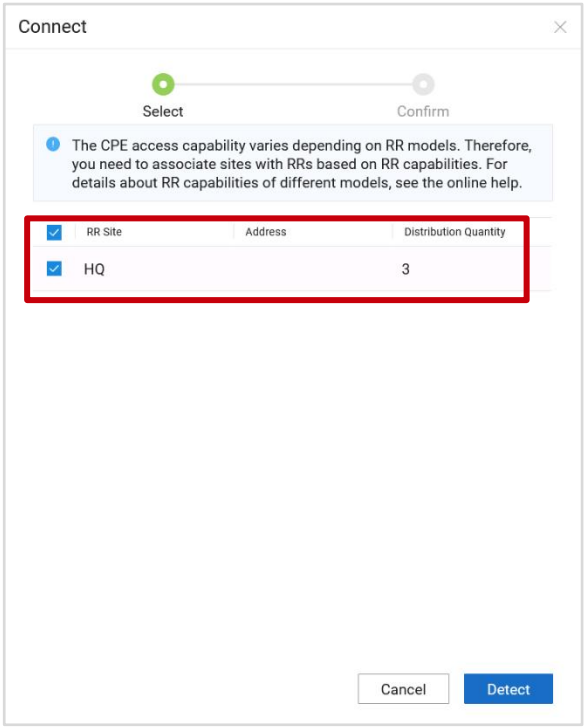
Choose Provision > Physical Network > Connect to RR from the main menu.



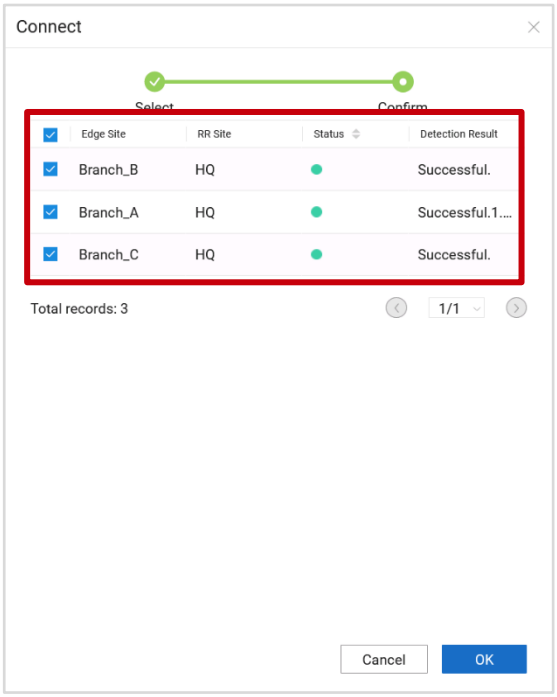
Select the edge node and click Connect.



On the Connect page, select the RR to be associated with the edge node and click Detect.



Click OK.



NOTE

When associating an edge node with an RR, comply with the following rules:

An edge node can be associated with a maximum of two RRs. If two RRs are associated, it is recommended that one RR and the edge node be deployed in the same physical area to ensure low latency, and the other RR be deployed in a different physical area to ensure service reliability through remote disaster recovery.

An RR can manage multiple edge nodes, and the number of edge nodes associated with each RR should be balanced as much as possible.

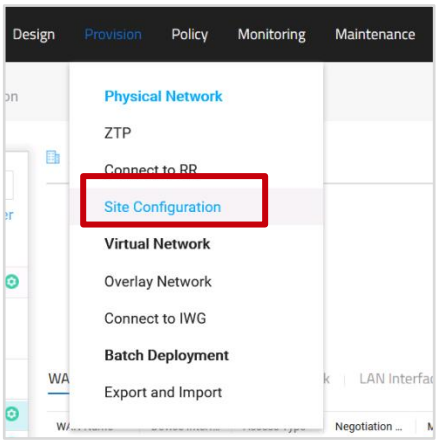
Step 2 Configure an underlay network.

The underlay network consists of the CPE uplink network (WAN) and CPE downlink network (LAN).

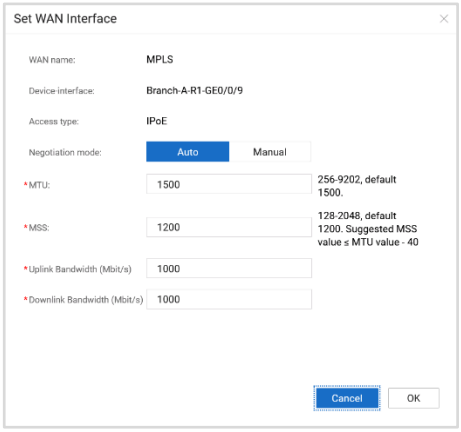
The WAN can connect to the MPLS network, Internet, LTE network, or private line through OSPF, BGP, or static routes.

The LAN is used to interconnect with devices on the LAN side.

Choose Provision > Physical Network > Site Configuration from the main menu.



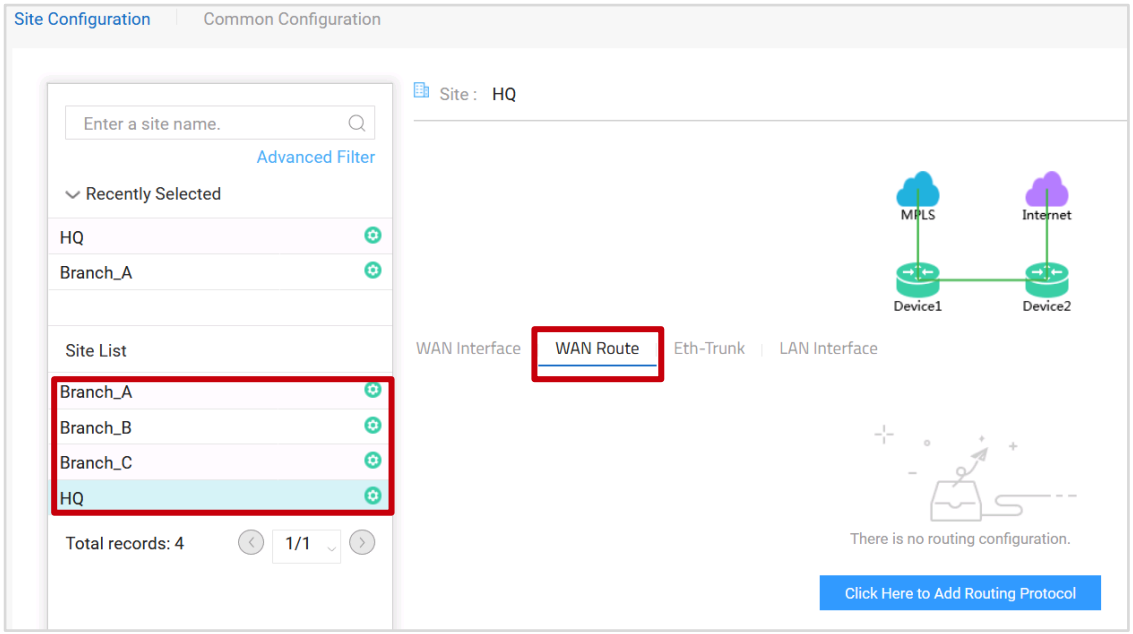
Configure WAN-side interface parameters for the underlay network of the site. The WAN-side interface parameters are not modified in this lab.

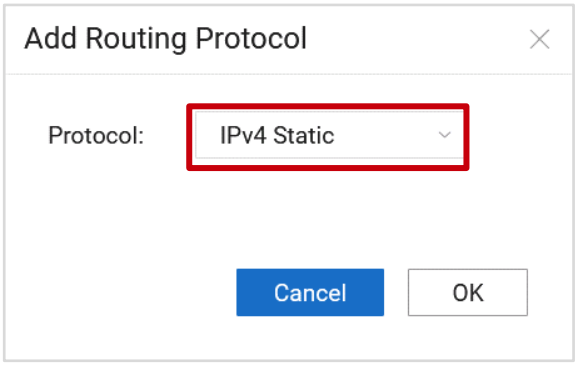


Configure WAN routes for the underlay network of the site. In this lab, static routes are used to connect to the WAN. The route planning is as follows:

Device Name	WAN Link	Destination Subnet	Next-Hop Address	Detection or Not	Destination IP Address
HQ-1	MPLS	0.0.0.0/0	100.1.1.2	Yes	100.1.1.2
HQ-2	Internet	0.0.0.0/0	100.2.1.2	Yes	100.2.1.2
Branch-A-R1	MPLS	0.0.0.0/0	100.1.2.2	Yes	100.1.2.2
Branch-A-R2	Internet	0.0.0.0/0	100.2.2.2	Yes	100.2.2.2
Branch-B-R1	MPLS	0.0.0.0/0	100.1.3.2	Yes	100.1.3.2
	Internet	0.0.0.0/0	100.2.3.2	Yes	100.2.3.2
Branch-C-R1	MPLS	0.0.0.0/0	100.1.4.2	Yes	100.1.4.2
	Internet	0.0.0.0/0	100.2.4.2	Yes	100.2.4.2

Select the site to be configured, select WAN Route, click Click Here to Add Routing Protocol, and select IPv4 Static.



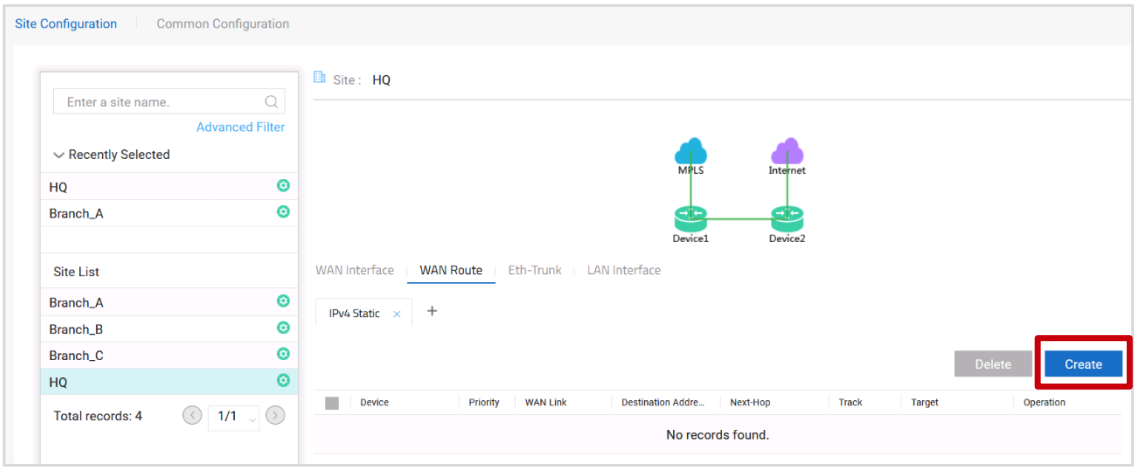


NOTE

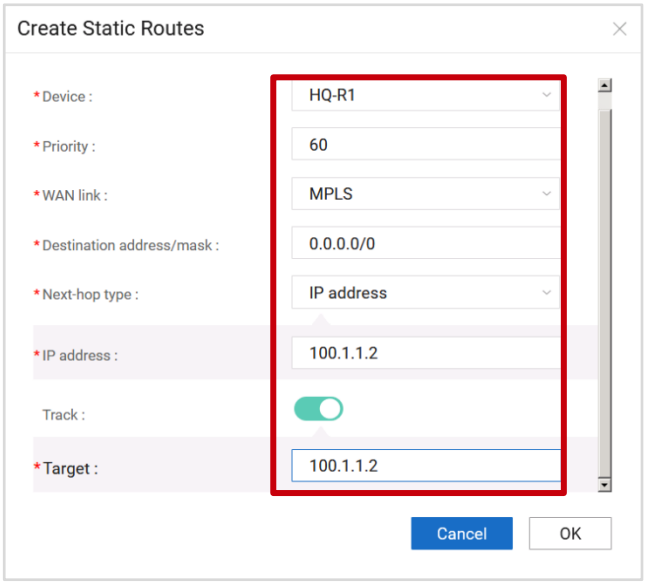
If OSPF or BGP is used, the OSPF or BGP parameter settings must match those on the peer device.

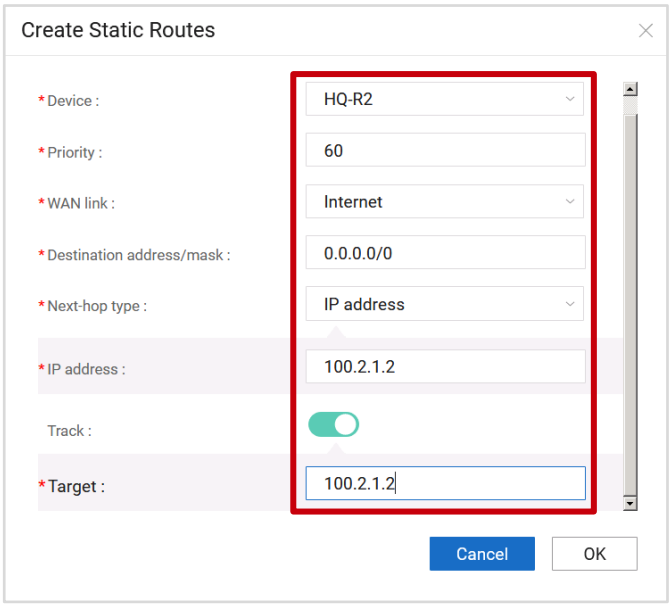
For details about OSPF and BGP parameters, see *iMaster NCE-WAN Help*.

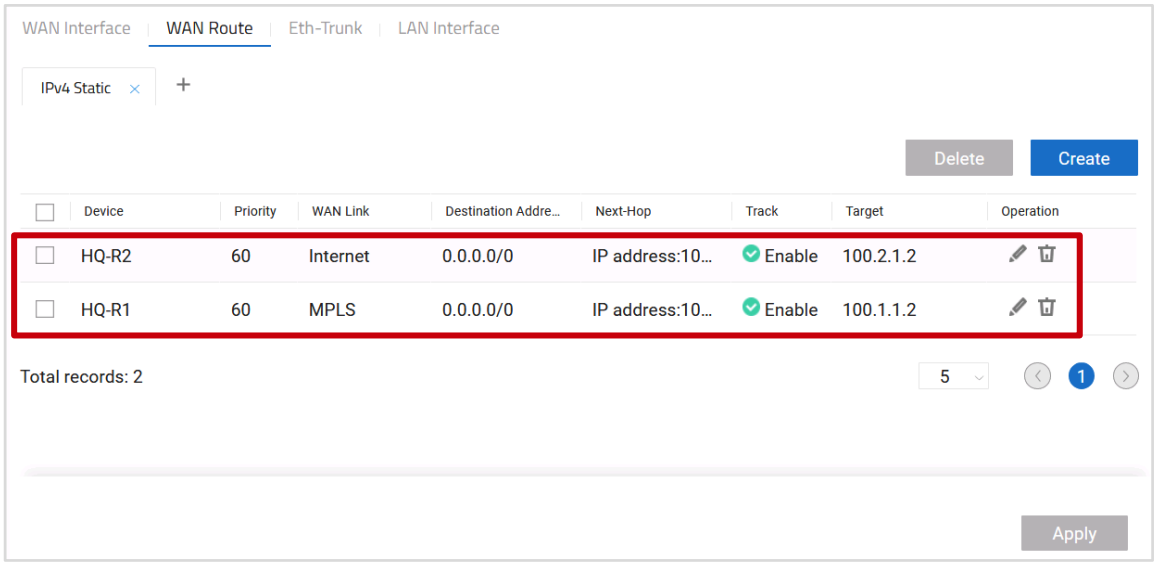
This lab demonstrates how to configure static routes at the HQ site. The configuration methods for other sites are similar. On the WAN Route page, click Create.



Configure the HQ site based on the static route planning. After the configuration is complete, click Apply. The configuration methods for other sites are similar.

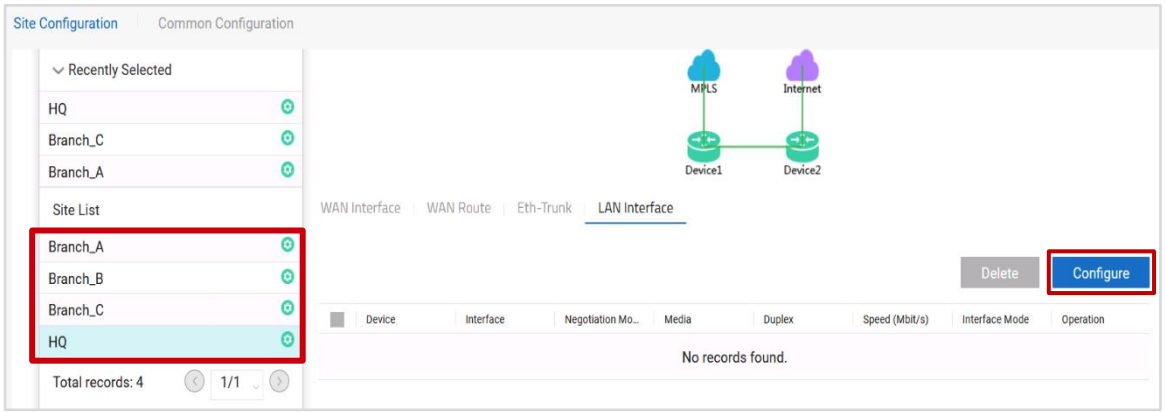




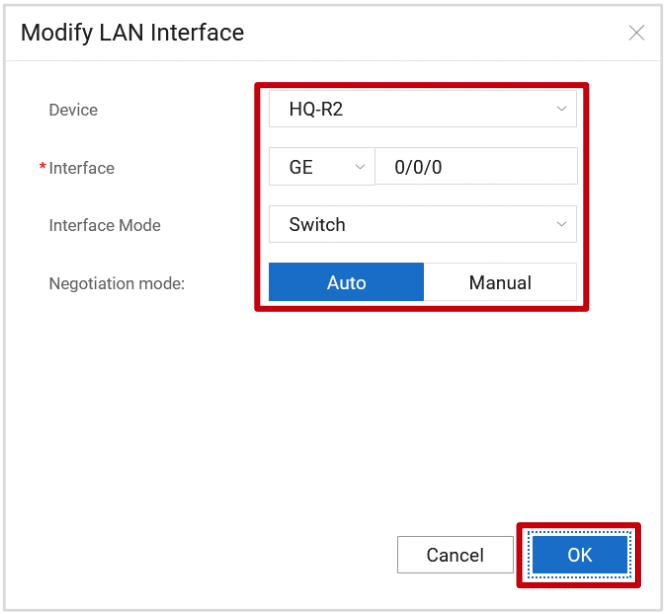


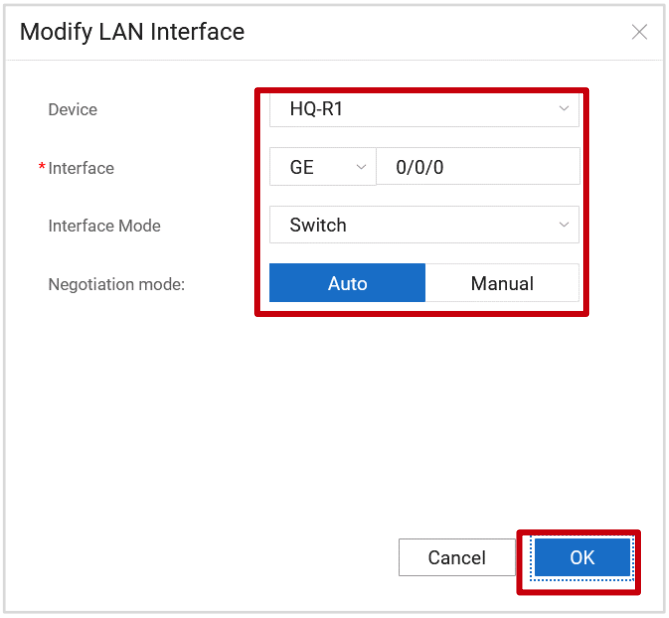
 # Configure LAN-side interface parameters for the underlay network of the site. In this lab, all CPEs use Layer 2 interface G0/0/1 to connect to the LAN.

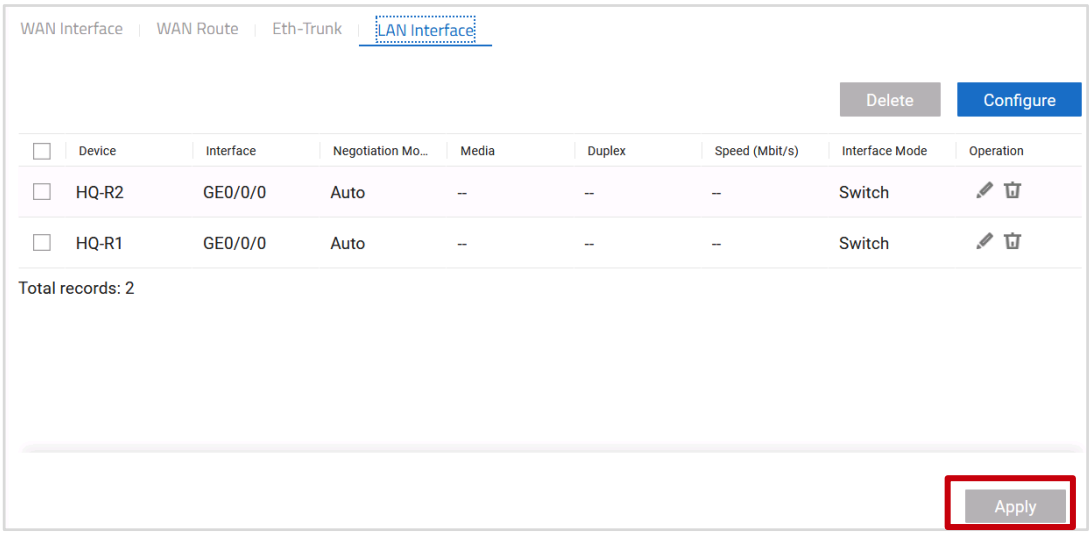
 # Select the site to be configured, select LAN Interface, and click Configure.



Configure the HQ site. After the configuration is complete, click Apply. The configuration methods for other sites are similar.







Step 3 Configure an overlay network.

This lab simulates the network of a training company. The company has two departments: online training and Course development departments.

The main service of the online training department is the video streaming service. Trainees can watch video streams sent from the headquarters in branches.

The main service of the Course development department is courseware and video development. Teachers in branches need to upload the developed coursewares and videos to the course development server of the headquarters so that all teachers can use the coursewares and videos in teaching.

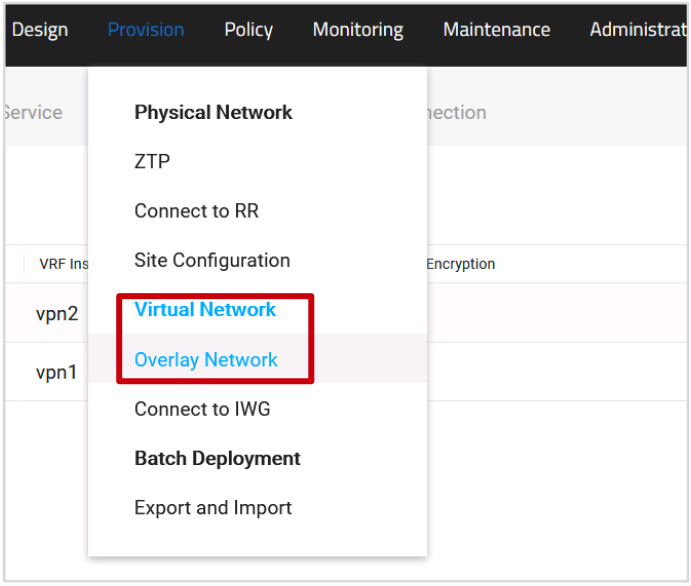
Teachers in the Course development department can query materials on the Internet.

Based on these requirements, the network planning is as follows.

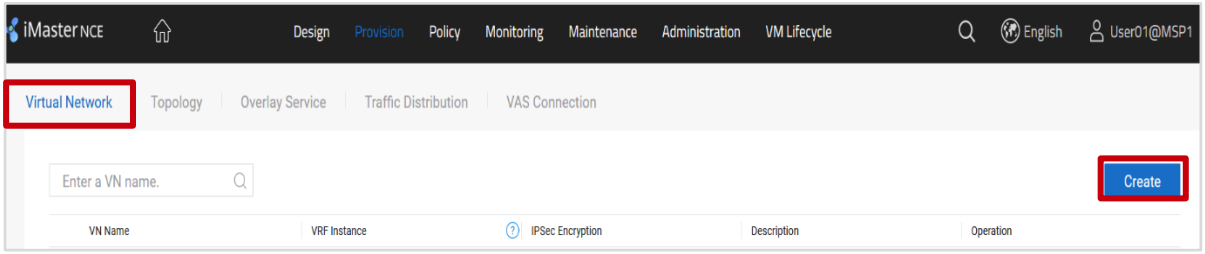
Department	Service	Active Line	Standby Line	Client
Online training department	Video streaming service	MPLS	Internet	Branch-A-1-PC, Branch-B-1-PC, Branch-C-1-PC
Course development department	FTP service	Internet	MPLS	Branch-A-2-PC, Branch-B-1-PC, Branch-C-1-PC
Online training department or Course development department	Web service	Local Internet access		Branch-A-2-PC, Branch-B-1-PC, Branch-C-1-PC

To isolate services of the online training department from those of the Course development department, you need to plan two overlay networks on iMaster NCE-WAN. The process is as follows:

Choose Provision > Virtual Network > Overlay Network from the main menu.



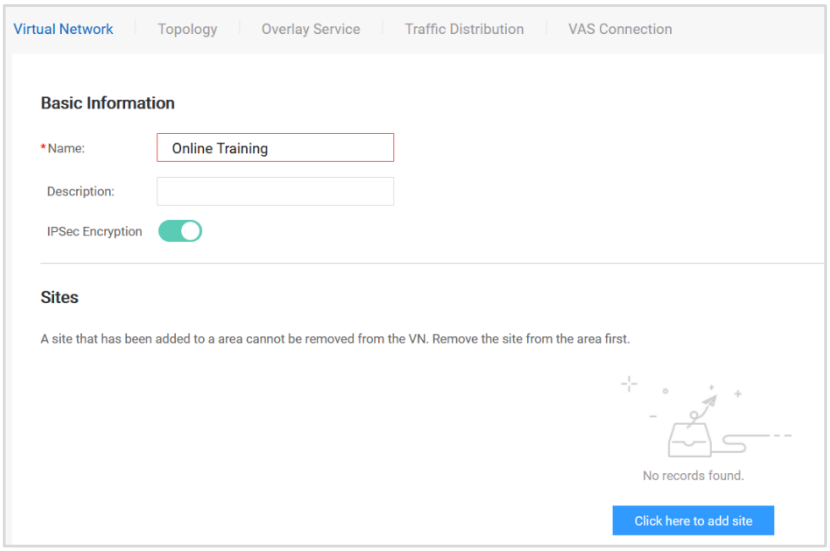
Click the Virtual Network tab and click Create to create two virtual networks: Online Training and Course Development.

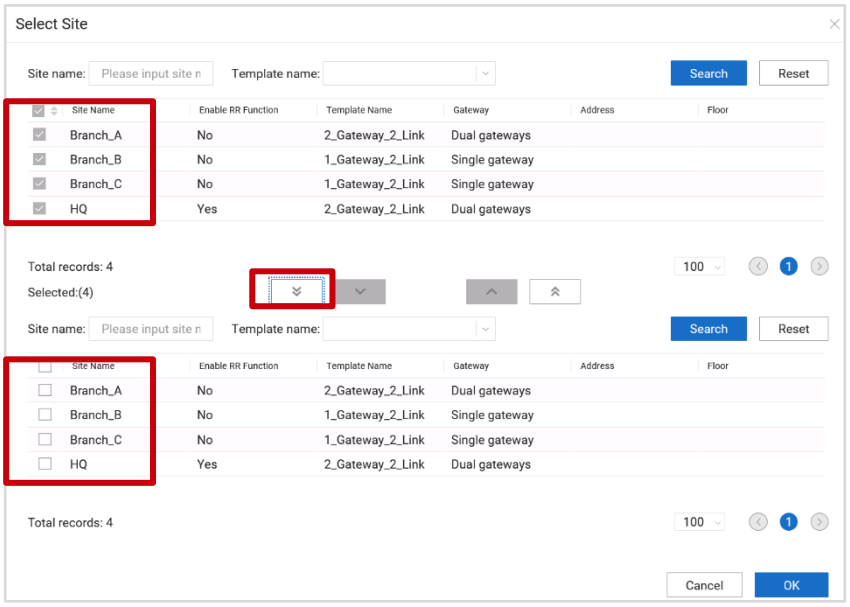


Online Training and Course Development involve all sites. When creating a virtual network, you need to add all sites to Online Training and Course Development. The virtual network planning is as follows.

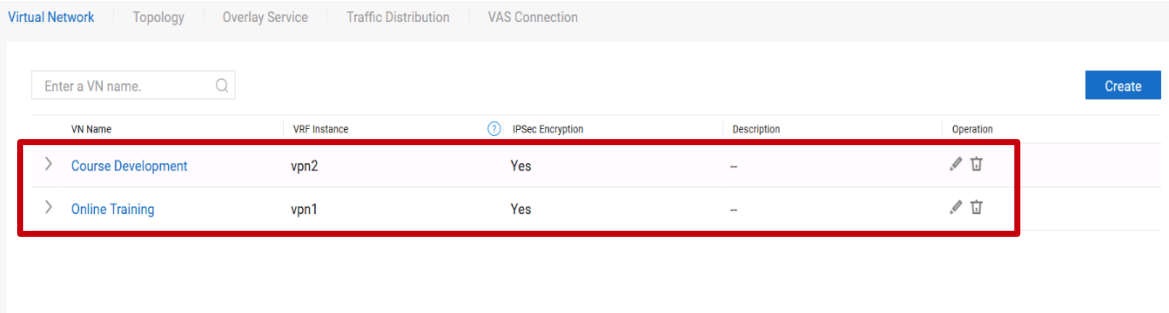
VN Name	Involved Site	Encryption or Not
Online Training	HQ, Branch-A, Branch-B, Branch-C	Yes
Course Development	HQ, Branch-A, Branch-B, Branch-C	Yes

In this lab, the virtual network Online Training is used as an example. The method for creating the virtual network Course Development is similar.





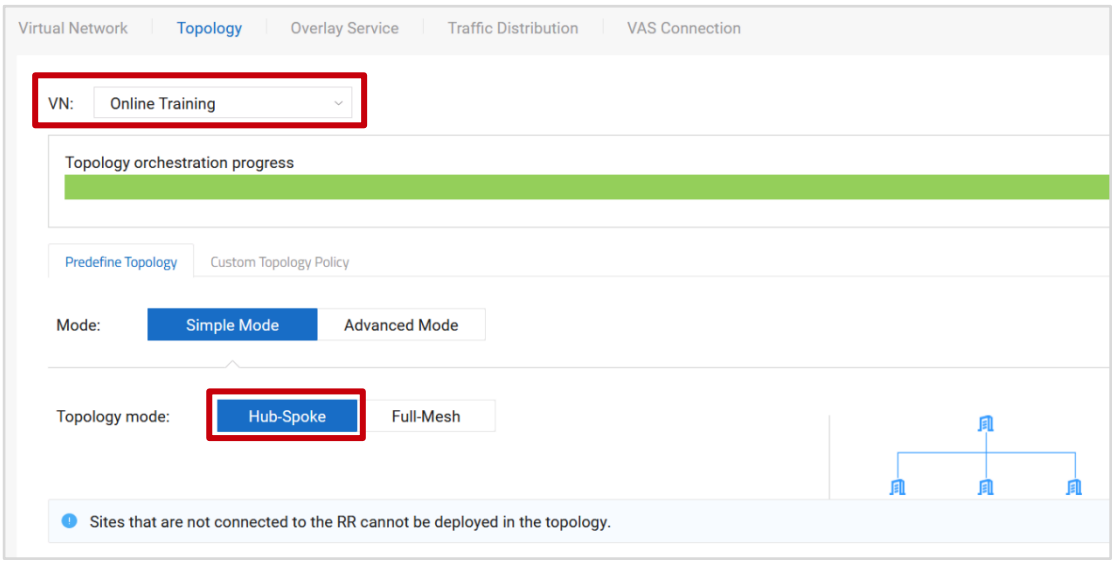
 # After creating the virtual networks Online Training and Course Development, you can check the creation result on the Virtual Network tab page.



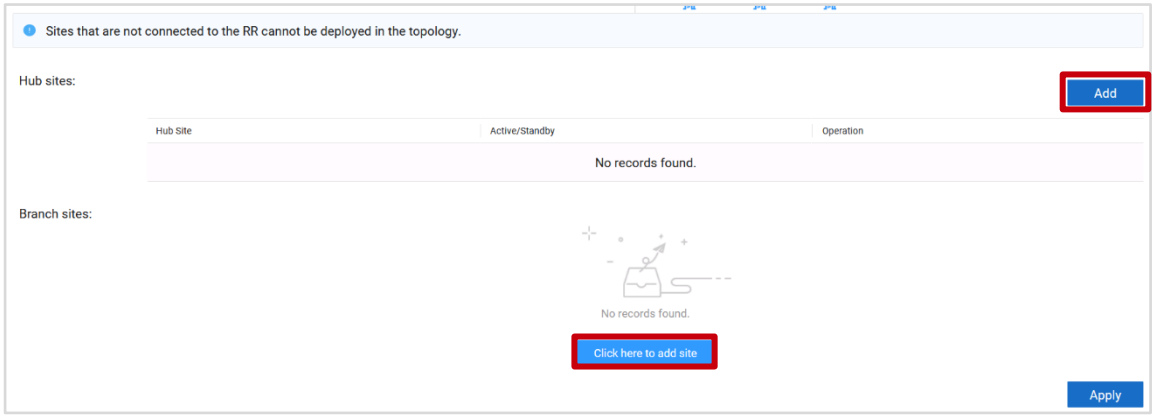
Click the Topology tab and set the topologies of the virtual networks Online Training and Course Development to hub-spoke.

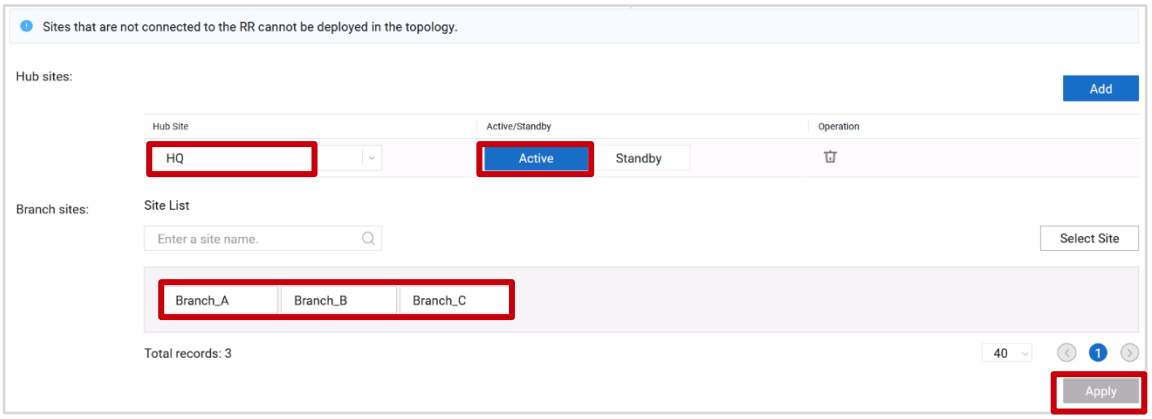
In this lab, the virtual network Online Training is used as an example. The topology setting of the virtual network Course Development is similar.

Select Online Training and set the topology type to hub-spoke.



Configure the HQ as the hub and the other sites as spokes.





NOTE

A maximum of two hubs can be created. If two hubs are selected, only the active/standby mode is supported, that is, one is the active hub and the other is the standby hub.

The configuration of Course Development is similar and is not provided.

Configure the overlay service. The main purpose of the overlay service is to set the LAN-side network segment used by related services.

The planning of the overlay service is as follows.

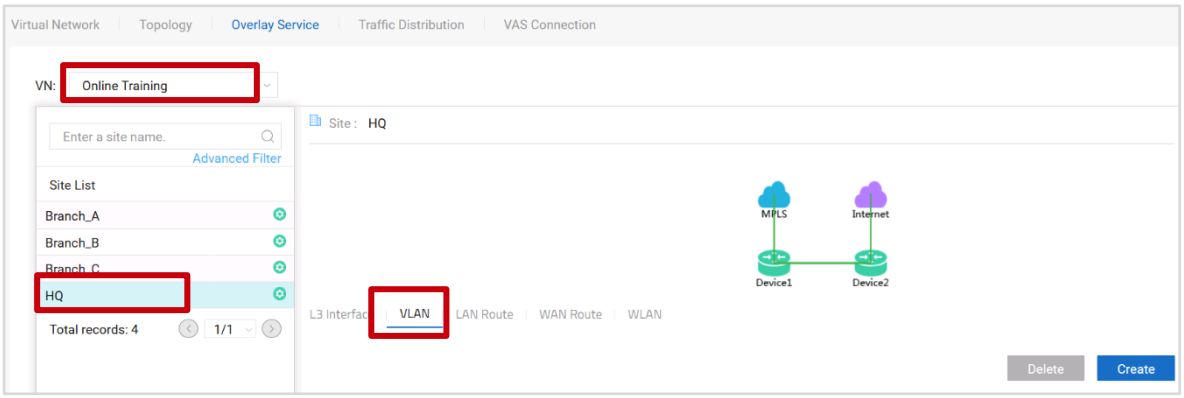
Virtual Network	Site	Device	Physical Interface	VLAN	IP Address	LAN Routing Protocol	Protocol Interface
Online Training	HQ	HQ-R1	G0/0/0	11	192.168.11.2/30	OSPF	VLANIF 11
	Branch_A	Branch-A-R1	G0/0/0	21	192.168.21.2/30	OSPF	VLANIF 21
	Branch_B	Branch-B-R1	G0/0/0	31	192.168.31.2/30	OSPF	VLANIF31
	Branch_C	Branch-C-R1	G0/0/0	41	192.168.41.2/30	OSPF	VLANIF 41
Course Development	HQ	HQ-R2	G0/0/0	12	192.168.12.2/30	OSPF	VLANIF 12
	Branch_A	Branch-A-R2	G0/0/0	22	192.168.22.2/30	OSPF	VLANIF 22
	Branch_B	Branch-B-R1	G0/0/0	32	192.168.32.2/30	OSPF	VLANIF 32
	Branch_C	Branch-C-R1	G0/0/0	42	192.168.42.2/30	OSPF	VLANIF 42

In this experiment, the virtual network Online Training is used as an example. The configuration of the virtual network Course Development is similar to that of the virtual network Online Training, and is not provided here.

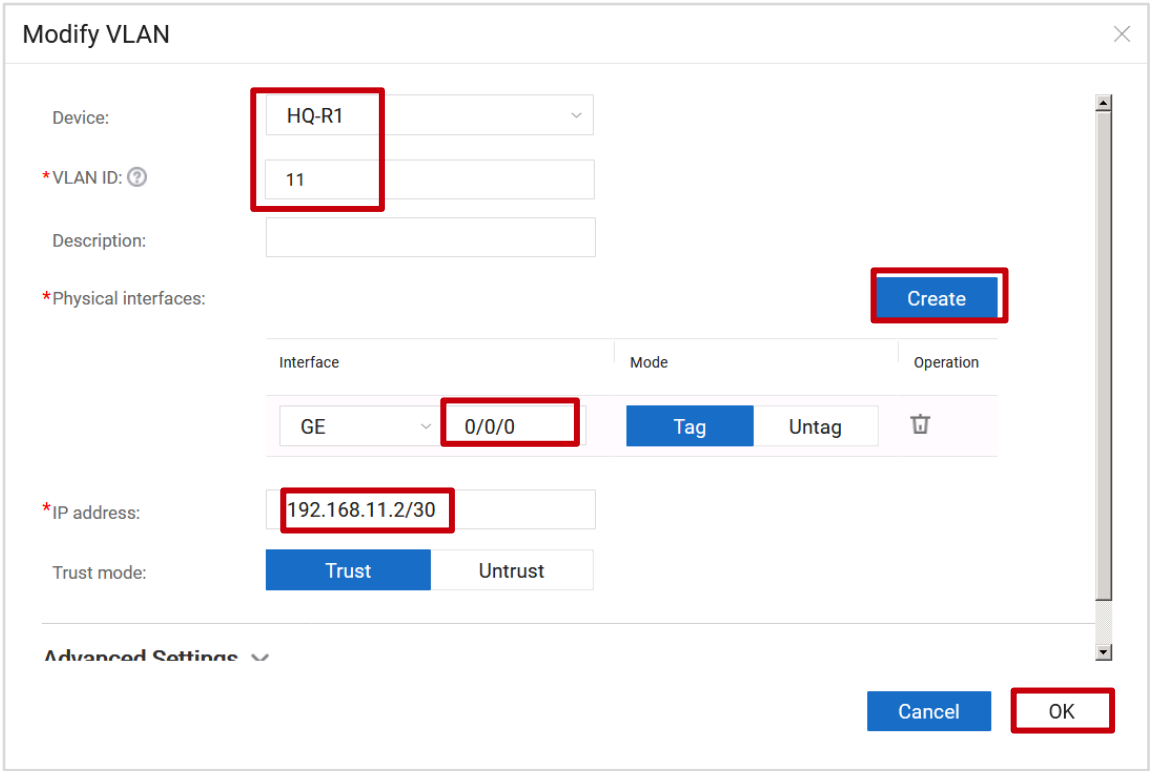
Click the Overlay Service tab and configure sites for the virtual network Online Training based on the plan.

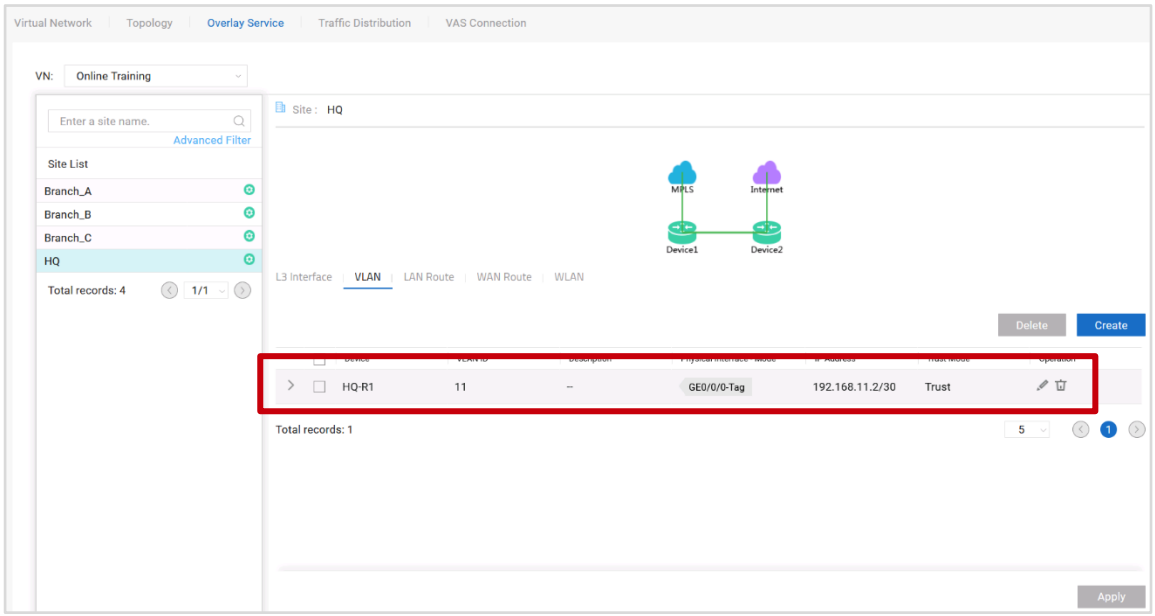
Select the HQ site and set parameters such as the VLAN ID, IP address, and LAN route.

Set VLAN parameters for the HQ site. Click the VLAN tab and click Create.

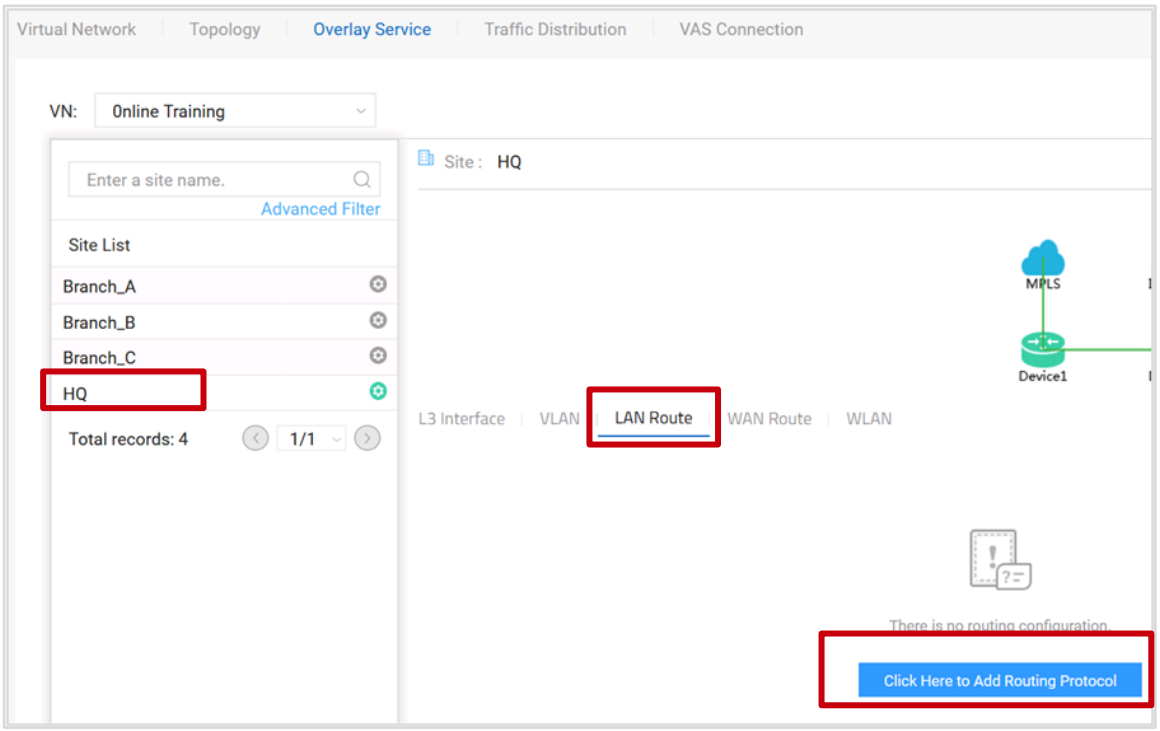


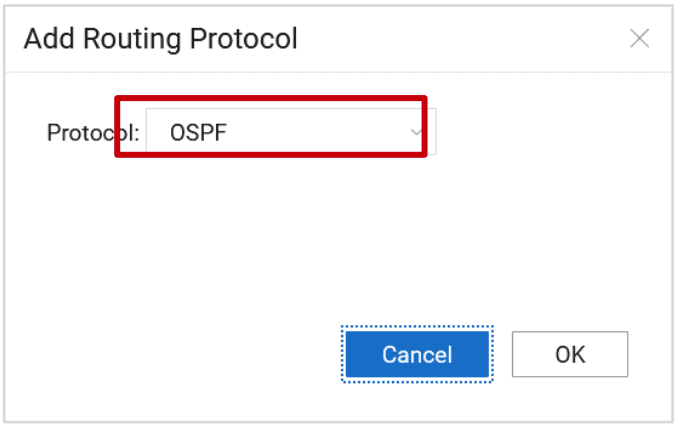
Set VLAN parameters for the HQ site, click OK, and apply the settings.

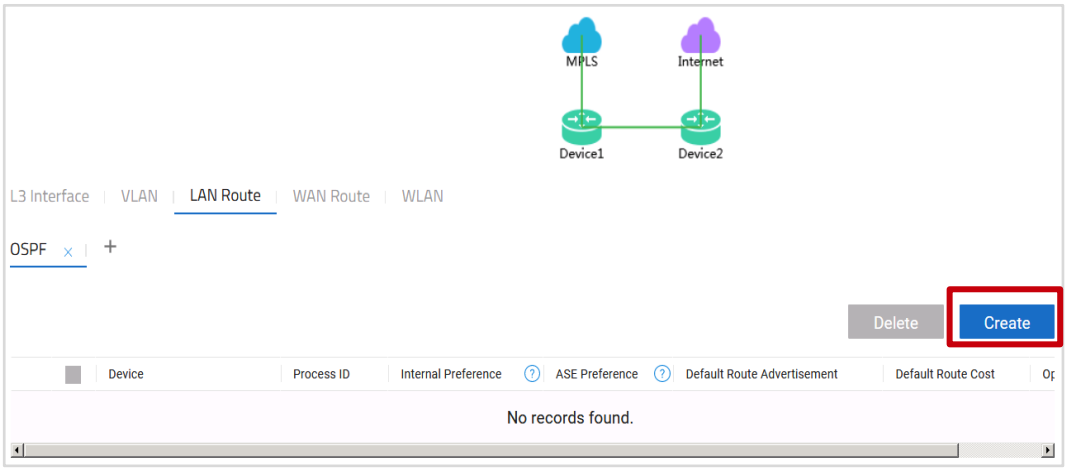




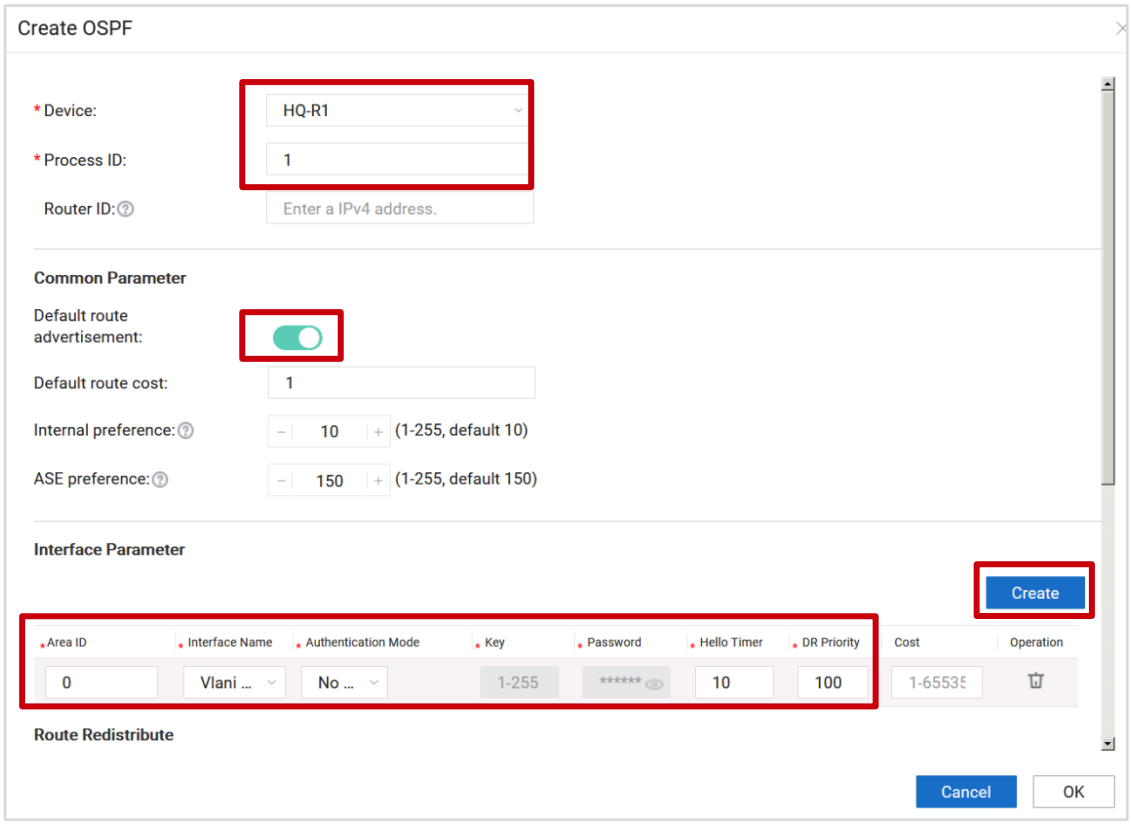
Set LAN route parameters for the HQ site and select LAN Route.







 # On HQ-R1, create OSPF process 1, add VLANIF 11 to OSPF area 0, set the DR priority to 100, and configure no-authentication.



NOTE

In EVPN mode, the process ID of OSPF routes deployed on the overlay network ranges from 1 to 20000.

On virtual networks Online Training and Course Development, the configurations of Branch_A, Branch_B, and Branch_C are similar to those of the HQ. Configure them based on the overlay service planning.

Virtual Network	Site	Device	Physical Interface	VLAN	IP Address	VLAN Interface
Online Training	HQ	HQ-R1	G0/0/0	11	192.168.11.2/30	VLANIF 11
	Branch_A	Branch-A-R1	G0/0/0	21	192.168.21.2/30	VLANIF 21
	Branch_B	Branch-B-R1	G0/0/0	31	192.168.31.2/30	VLANIF 31
	Branch_C	Branch-C-R1	G0/0/0	41	192.168.41.2/30	VLANIF 41
Course Development	HQ	HQ-R2	G0/0/0	12	192.168.12.2/30	VLANIF 12
	Branch_A	Branch	G0/0/0	22	192.168.22.	VLANIF

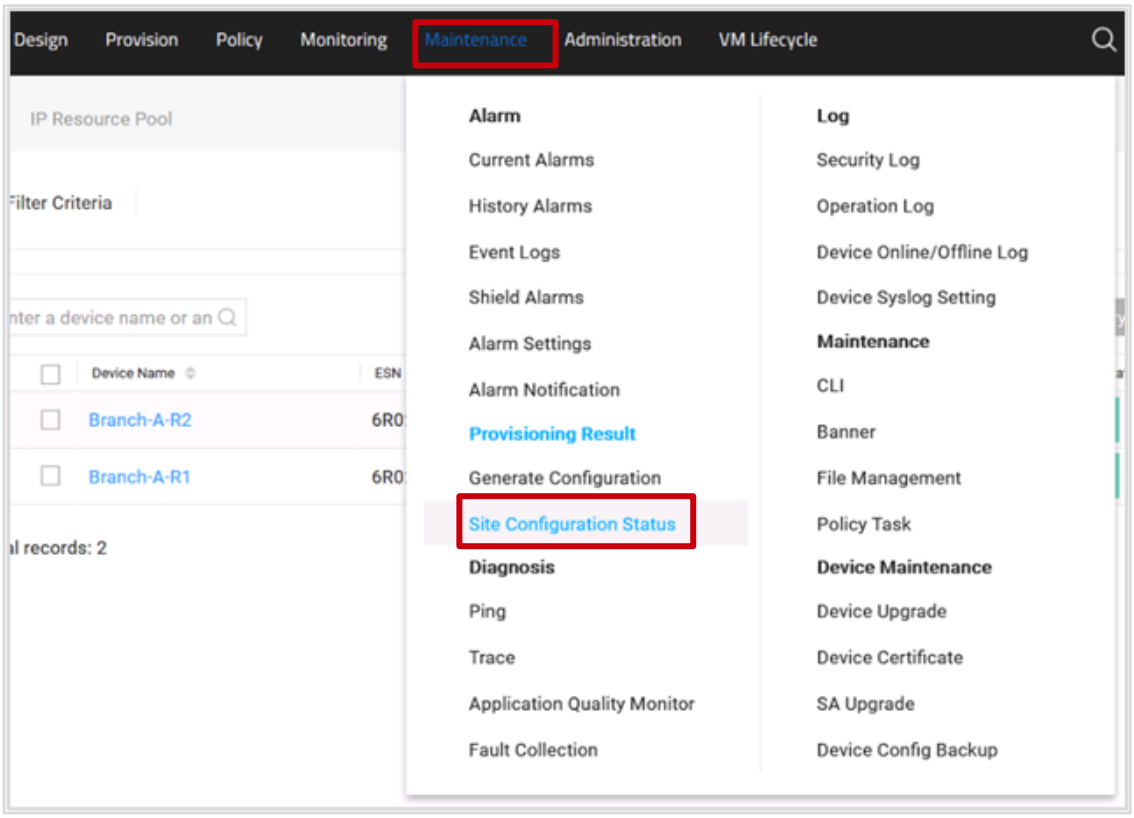
Virtual Network	Site	Device	Physical Interface	VLAN	IP Address	VLAN Interface
		-A-R2			2/30	22
	Branch_B	Branch -B-R1	G0/0/0	32	192.168.32. 2/30	VLANIF 32
	Branch_C	Branch -C-R1	G0/0/0	42	192.168.42. 2/30	VLANIF 42

The LAN routing protocols of Online Training and Course Development are planned as follows.

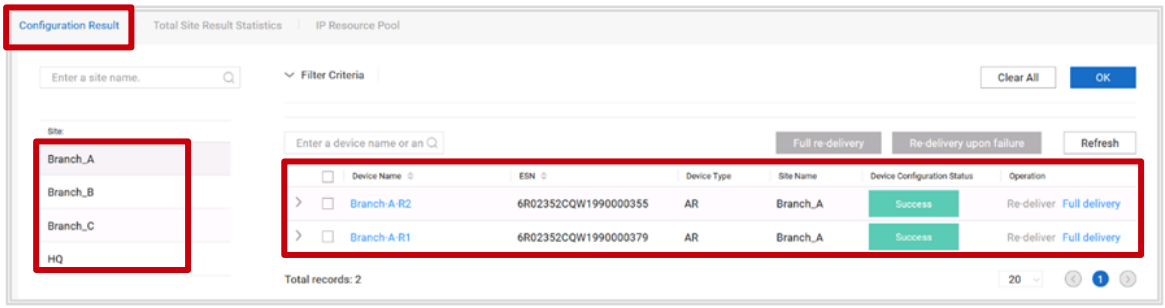
Virtual Network	Site	Device	Routing Protocol	Process ID	Area ID	OSPF Interface
Online Training	HQ	HQ-R1	OSPF	1	0	VLANIF 11
	Branch_A	Branch-A-R1	OSPF	1	0	VLANIF 21
	Branch_B	Branch-B-R1	OSPF	1	0	VLANIF 31
	Branch_C	Branch-C-R1	OSPF	1	0	VLANIF 41
Course Development	HQ	HQ-R2	OSPF	1	0	VLANIF 12
	Branch_A	Branch-A-R2	OSPF	1	0	VLANIF 22
	Branch_B	Branch-B-R1	OSPF	2	0	VLANIF 32
	Branch_C	Branch-C-R1	OSPF	2	0	VLANIF 42

Step 4 Verify that the site is successfully deployed.

Choose Maintenance > Provisioning Result > Site Configuration Status, click the Configuration tab, and select Result. Check whether the configuration is successfully delivered.



Check the configuration results of all sites. If the value of Device Configuration Status is Success, the network deployment is successful.



Step 5 Verify that the service is running properly.

This network consists of two departments: online training and Course development departments. The services of the two departments are as follows.

Department	Service	Server	Client
Online training department	Video streaming service	Video Server	Branch-A-1-PC, Branch-B-1-PC, Branch-C-1-PC
Course development department	FTP and HTTP services	FTP Server	Branch-A-2-PC, Branch-B-1-PC, Branch-C-1-PC

Client login mode: Use the remote desktop to log in to the client.

The IP address, user name, and password for logging in to the client are planned as follows.

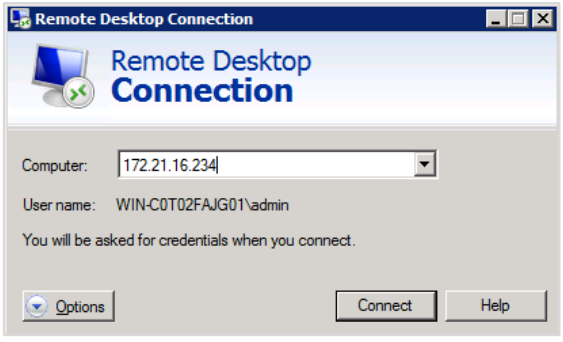
Department	Service	Client	Client Login IP Address	Login Username and Password
Online training department	Video streaming service	Branch-A-1-PC	172.21.16.234	admin/Huawei@123
		Branch-B-1-PC	172.21.16.236	admin/Huawei@123
		Branch-C-1-PC	172.21.16.237	admin/Huawei@123
Course development department	FTP and HTTP services	Branch-A-2-PC	172.21.16.235	admin/Huawei@123
		Branch-B-1-PC	172.21.16.236	admin/Huawei@123
		Branch-C-1-PC	172.21.16.237	admin/Huawei@123

Log in to the service client of the online training department to test the video streaming service.

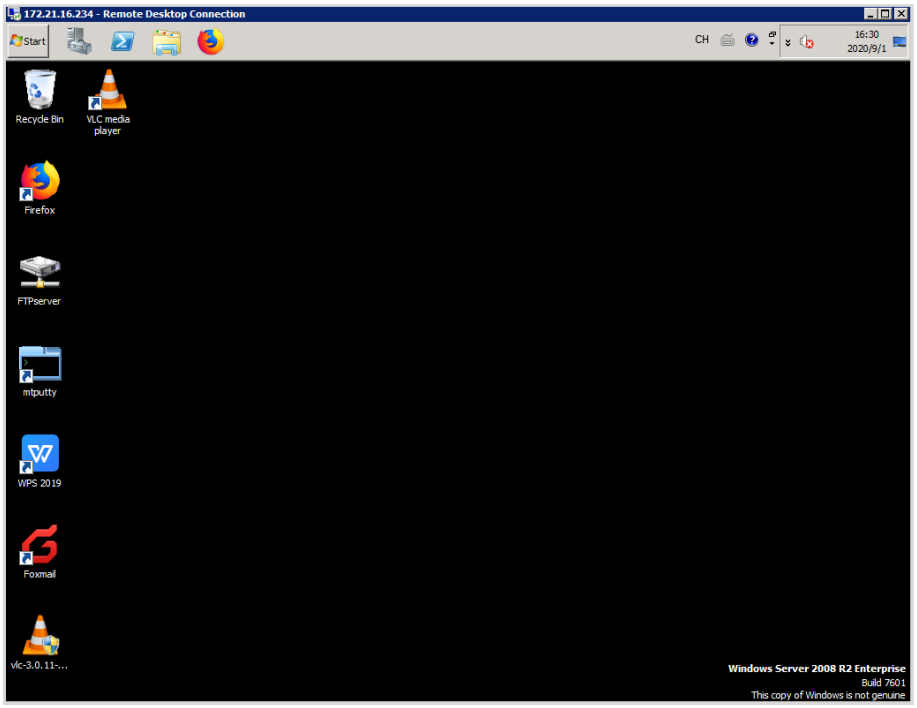
This lab uses Branch-A-1-PC as an example. The test methods on other clients are similar and are not provided.

The video server uses the video LAN client (VLC) to push video streams. The video server has been configured,

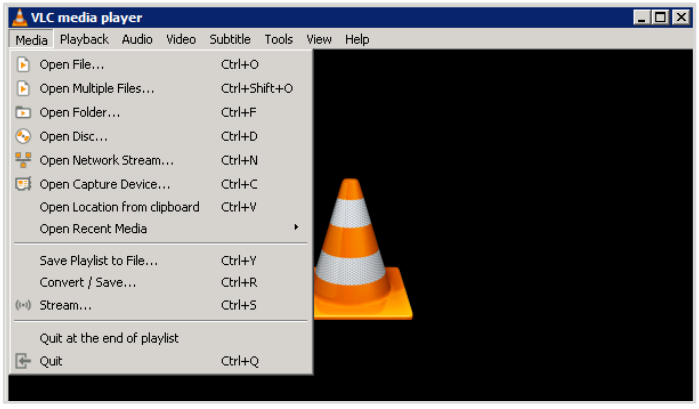
Use the remote desktop to log in to Branch-A-1-PC and enter the user name and password.



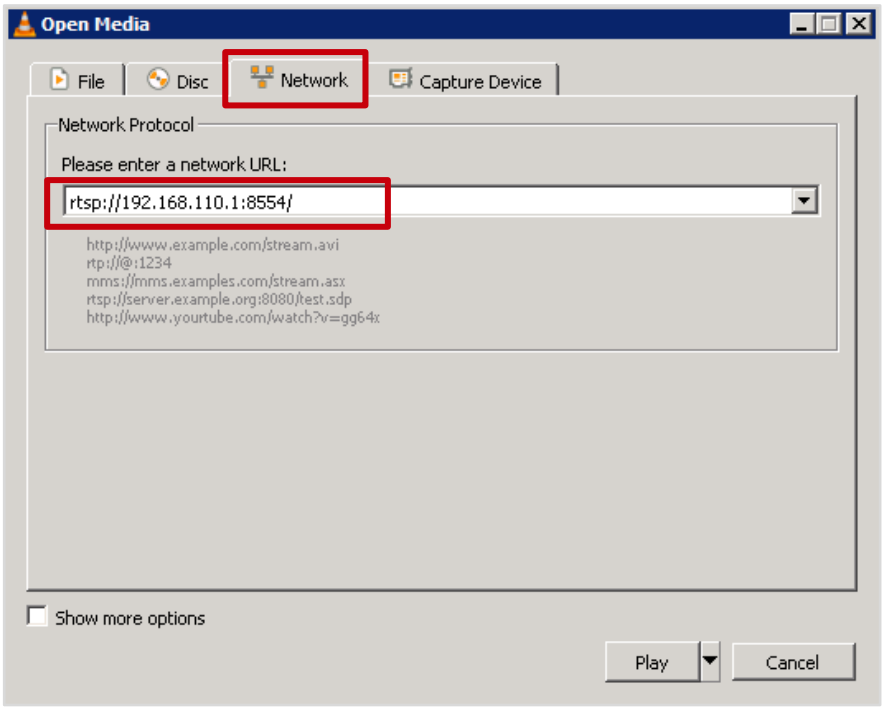
Log in to Branch-A-1-PC and open the VLC software.



Configure the VLC to receive video streams. Choose Media > Open Network Stream and configure the IP address of the video streaming server.



On the Network tab page, enter rtsp://192.168.110.1:8554/ and click Play.



If the video image is displayed, the video service is running properly.

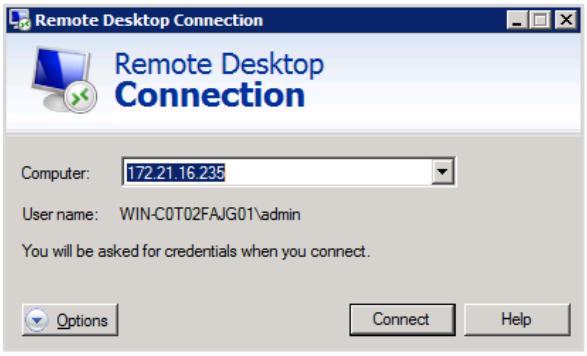
The test methods for other clients of the online training department are similar to those of Branch-A-1-PC.

Log in to the client of the Course development department and test the FTP service.

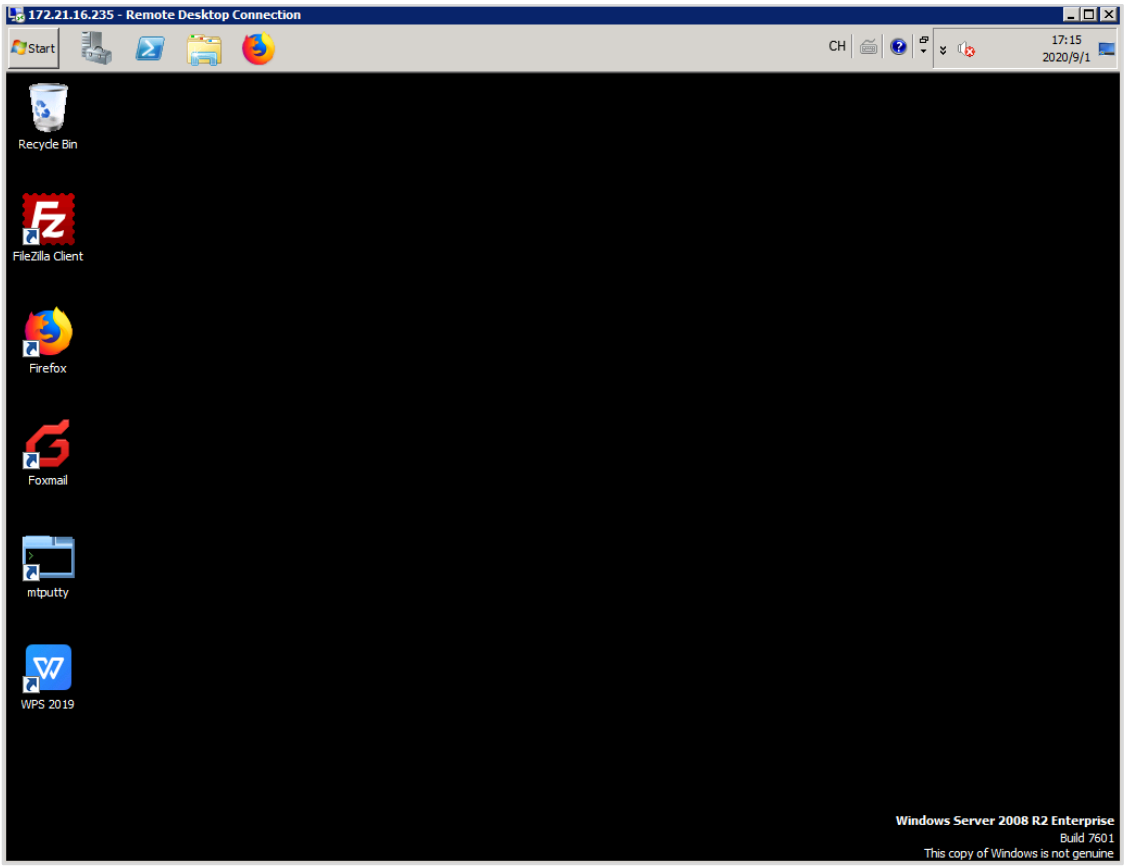
This lab uses Branch-A-2-PC as an example. The test methods on other clients are similar and are not provided.

The FTP server has been configured.

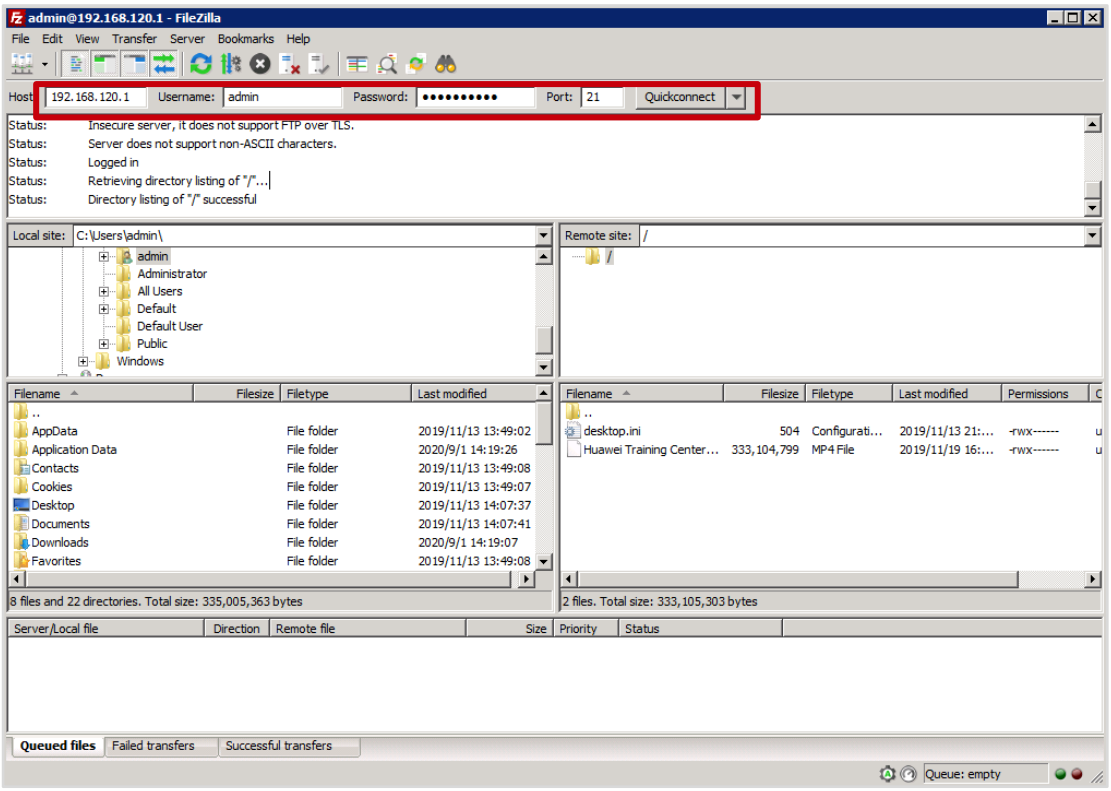
Use the remote desktop to log in to Branch-A-2-PC and enter the user name and password.



Log in to Branch-A-1-PC and open FileZilla Client.



Enter the FTP server IP address/port number (192.168.120.1:21) and user name/password (admin/Huawei@123) to log in to the FTP server.



If the login is successful, the service is running properly.

----End

5.4.3 Quiz

What are the differences between the hub-spoke topology and full-mesh topology?

5.5 Policy Management

5.5.1 Introduction

5.5.1.1 Objectives

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

- Configure traffic policies.
- Configure security policies.

5.5.1.2 Networking Topology

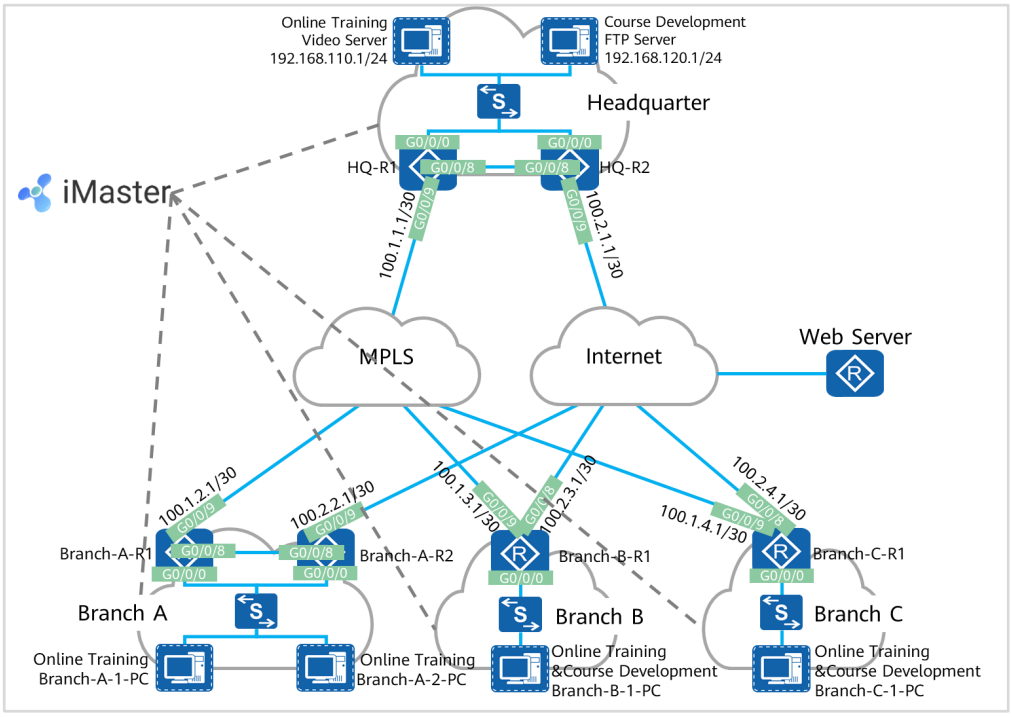


Figure5-5 SD-WAN topology

The figure shows the interconnection IP addresses. The headquarters and Branch A are connected to the MPLS network and Internet through dual egresses and links, and Branch B and Branch C are connected to the MPLS network and Internet through a single egress and dual links. Two links connect the MPLS network and Internet respectively, and the MPLS network and Internet are isolated from each other. Devices connect to iMaster NCE-WAN through public IP addresses.

5.5.1.3 Lab Background

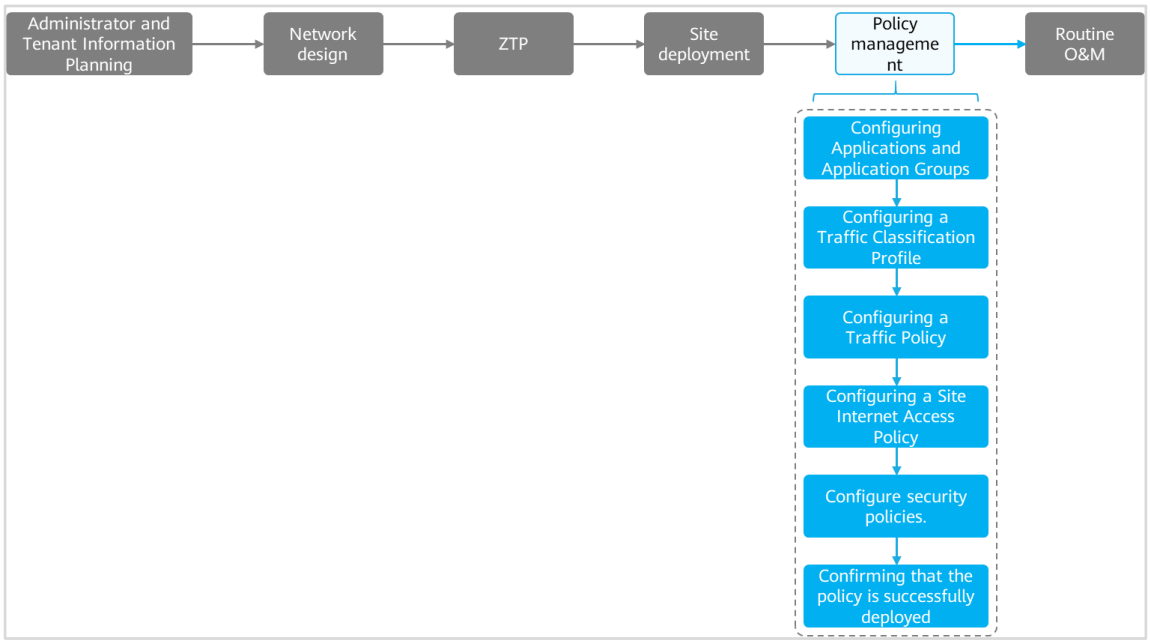
An enterprise needs to deploy new sites. To quickly deploy network services and simplify O&M, the enterprise deploys the iMaster NCE-WAN solution.

Network planning and management personnel need to construct a network using iMaster NCE-WAN based on the network topology and requirements.

5.5.2 Lab Tasks

5.5.2.1 Configuration Roadmap

To deploy iMaster NCE-WAN, perform the following steps. This lab mainly describes how to use iMaster NCE-WAN to implement policy management.



The configuration roadmap is as follows:

1. Configure applications and application groups to differentiate applications.
2. Configure a traffic classifier to match traffic.
3. Configure a traffic policy.
4. Configure an Internet access policy for a site.
5. Configure a security policy.
6. Verify that the policies are successfully deployed.

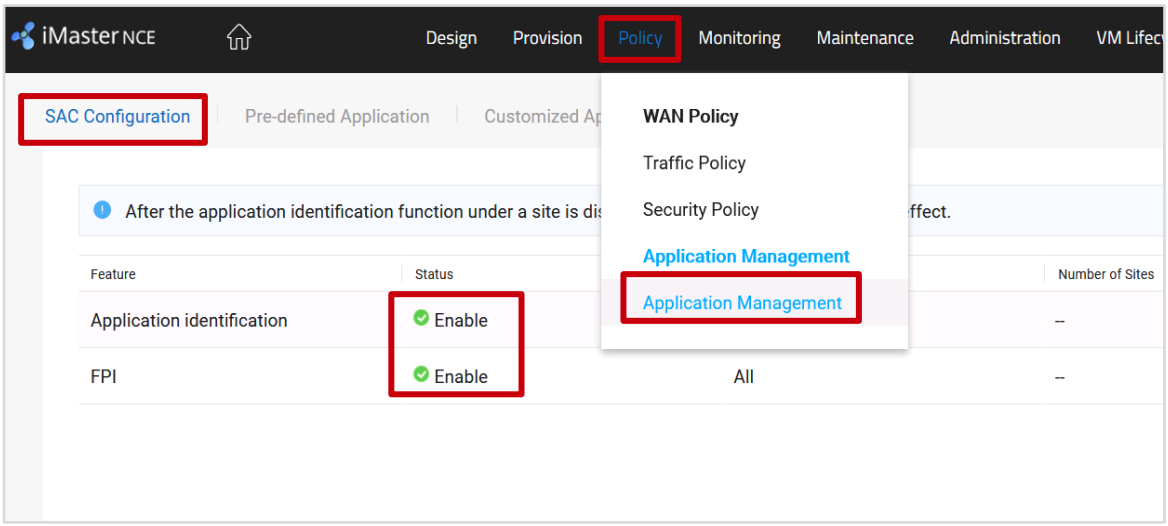
5.5.2.2 Configuration Procedure

Step 1 Configuring Applications and Application Groups

When blocking, redirection, intelligent traffic steering, QoS, or application link detection is performed, you can configure policies based on application groups.

If predefined applications do not meet requirements, you can configure customized applications and group predefined and user-defined applications.

Choose Policy > Application Management > Application Management from the main menu to check the SAC configurations.



Application identification and First Packet Identification (FPI) must be enabled.

NOTE

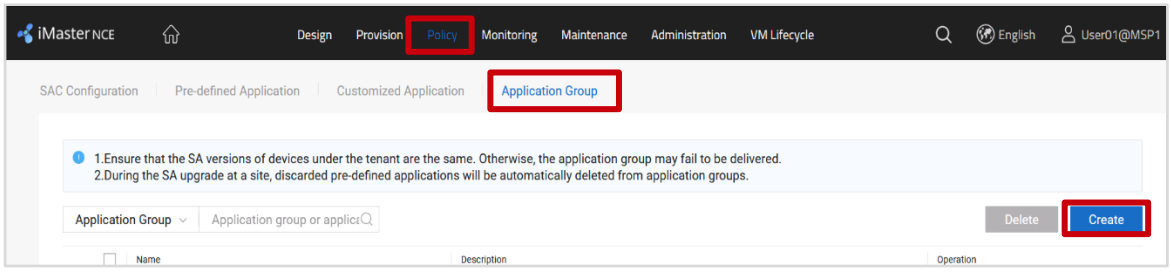
SAC configuration includes application identification and FPI.

Application identification detects and identifies Layer 4 to Layer 7 information (such as RTP) in packets and implements refined QoS policy control based on the classification result.

FPI identifies an application based on the first packet of the application.

The difference is as follows: FPI identifies an application based on the first packet of the application, while application identification identifies an application by matching multiple packets of the application.

Choose Policy > Application Management > Application Management from the main menu and click the Application Group tab to create an application group.



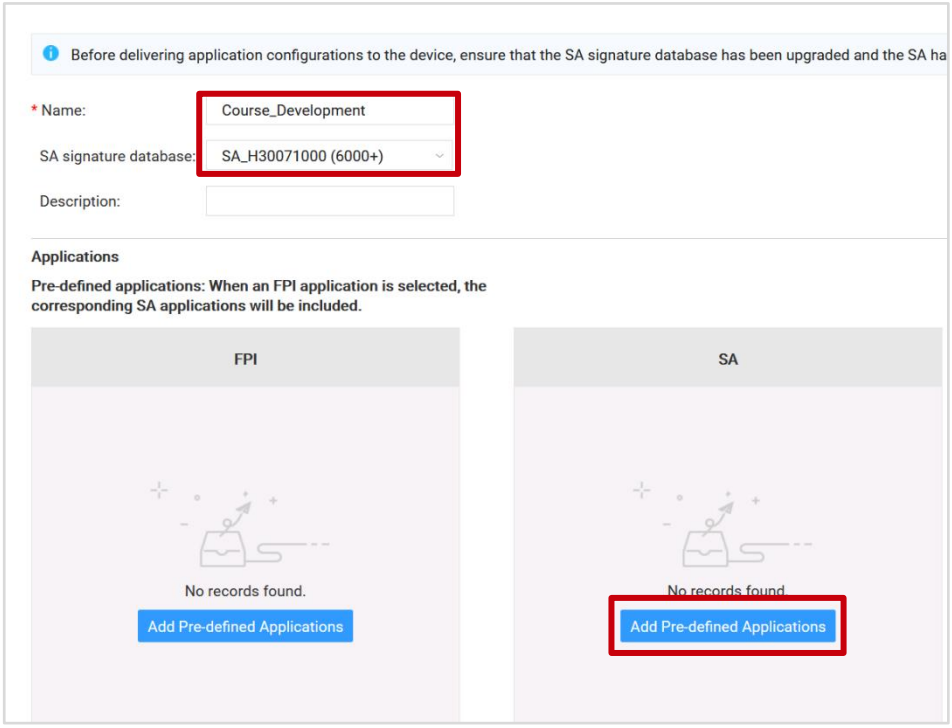
This lab involves two departments. The applications in each department are as follows.

Department	Service	Protocol
Online training department	Video streaming service	RTSP
Course development department	FTP service	FTP/SFTP/TFTP
	HTTP service	HTTP/HTTPS/HTTP2/HTTP_Download

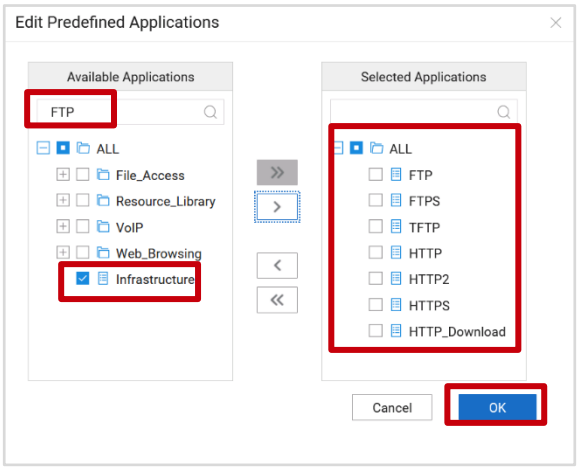
Create an application group based on applications of each department.

Application Group Name	SA Signature Database	SA Application
Online_Training	SA_H30071000 (6000+)	RTSP
Course_Development	SA_H30071000 (6000+)	FTP/SFTP/TFTP HTTP/HTTPS/HTTP2/HTTP_Download

Enter the application group name as planned, select the SA signature database, and add SA applications.



Search for the keywords FTP and HTTP and add FTP/SFTP/TFTP/HTTP/HTTPS/HTTP2/HTTP_Download as planned.



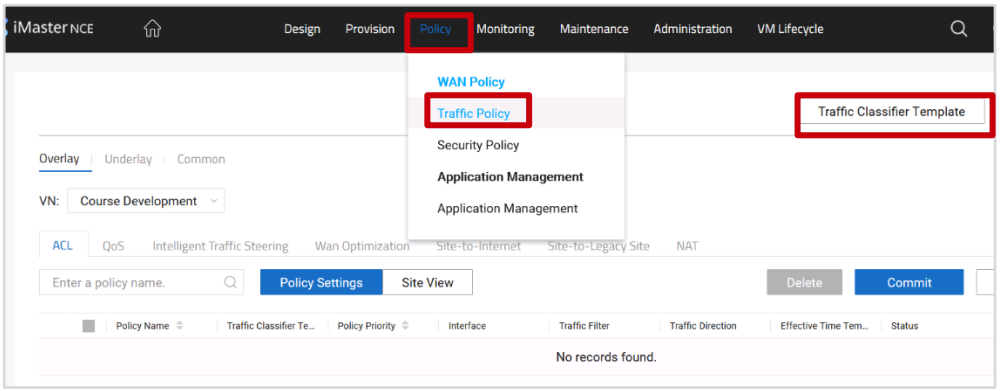
The procedure for configuring the application group Online_Training is similar to that for configuring the application group Course_Development.

Step 2 Configure traffic classifiers.

A traffic classifier defines a group of traffic matching rules to classify packets.

This ensures that a device processes packets matching the same traffic classifier identically.

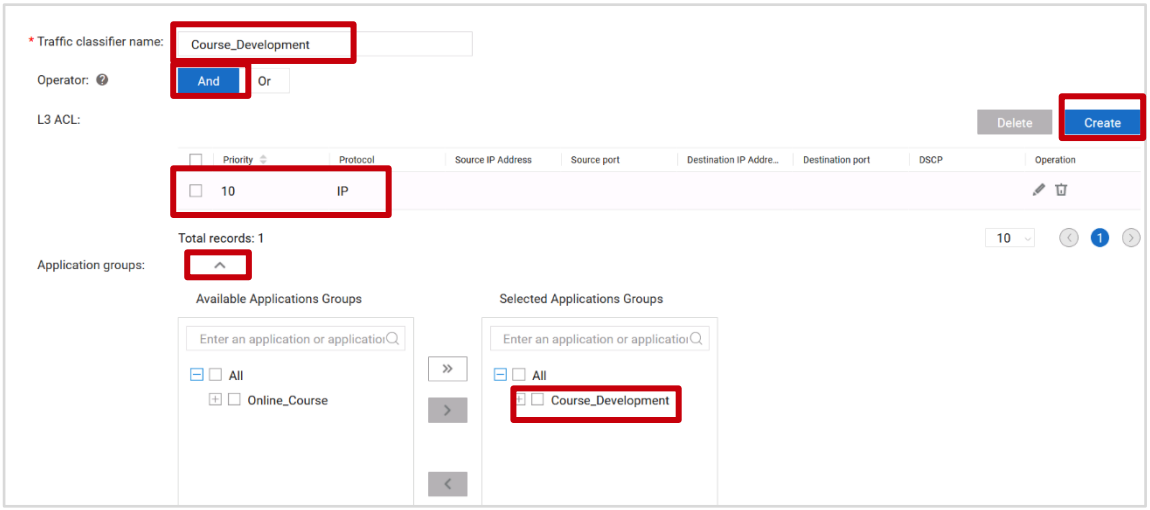
Choose Policy > WAN Policy > Traffic Policy from the main menu to create a traffic classifier.



In this experiment, services are controlled based on departments. Therefore, you only need to create two traffic classifiers.

Traffic Classifier Name	Relationship Between Rules	ACL	Application Group
Online_Training	AND	Priority: 10 Protocol: IP Other parameters: default settings	Online_Training
Course_Development	AND	Priority: 10 Protocol: IP Other parameters: default settings	Course_Development

Create a traffic classifier as planned, configure an ACL, select an application group, and click OK.



The configuration of the traffic classifier Online_Training is similar to that of the traffic classifier Course_Development and is not provided.

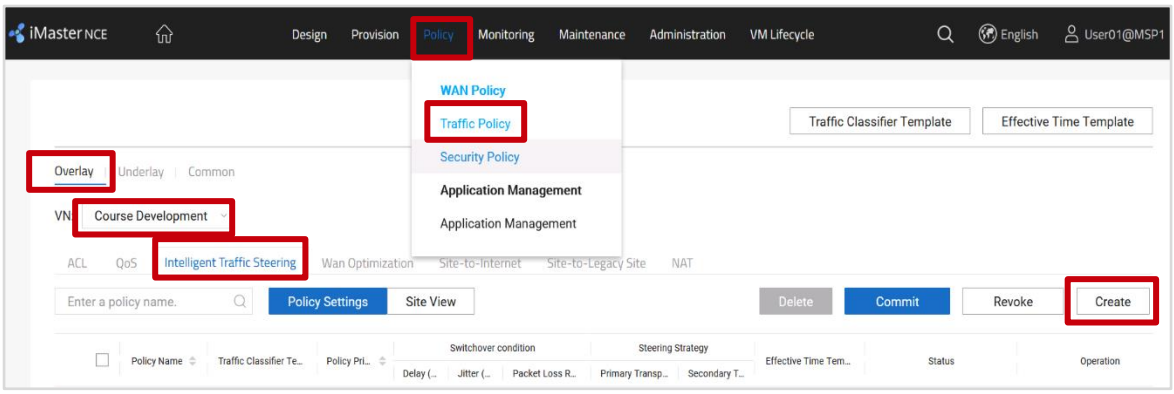
Step 3 Configure a traffic policy.

Traffic policies can be used to control traffic on the overlay network. They are classified into ACL policies, intelligent traffic steering policies, QoS policies, and WAN optimization policies.

In this lab, intelligent traffic steering and QoS policies are deployed.

Deploy intelligent traffic steering policies to control traffic directions of the online training department and Course development department.

Choose Policy > WAN Policy > Traffic Policy from the main menu. Click the Overlay tab, select a VN, click the Intelligent Traffic Steering tab, and create an intelligent traffic steering policy.

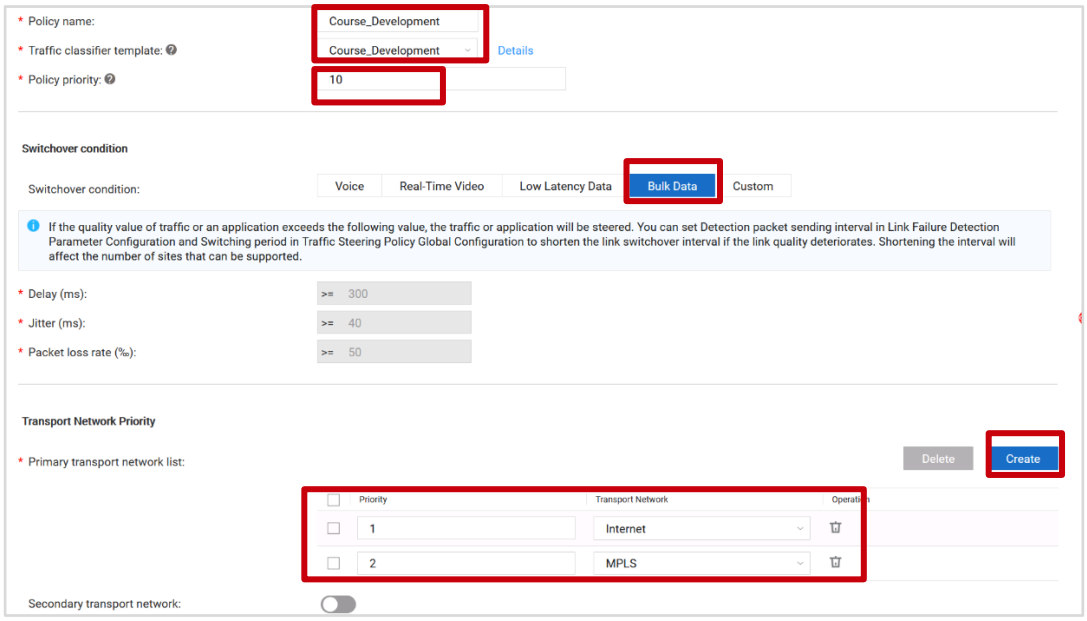


The intelligent traffic steering policy is planned as follows.

VN	Policy Name	Traffic Classifier	Policy Priority
Online Training	Online_Training	Online_Course	10
Course Development	Course_Development	Course_Development	10

Policy Name	Switchover Condition	Primary Transport Network	Transport Network Priority
Online_Training	Real-time video	MPLS	1
		Internet	2
Course_Development	Bulk data	Internet	1
		MPLS	2

Configure an intelligent traffic steering policy as planned and click OK.

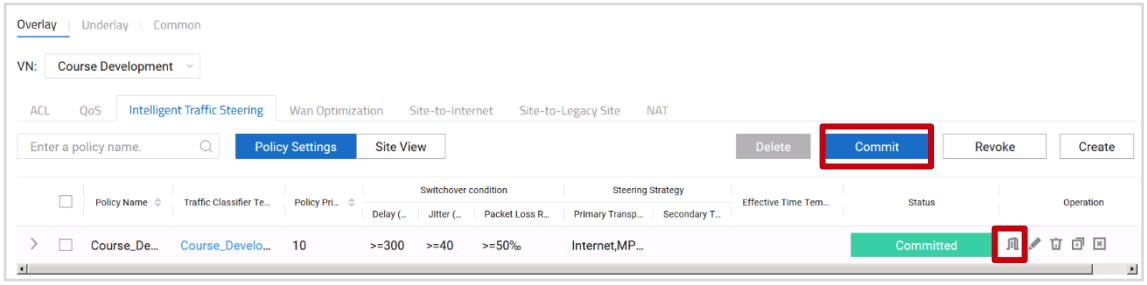


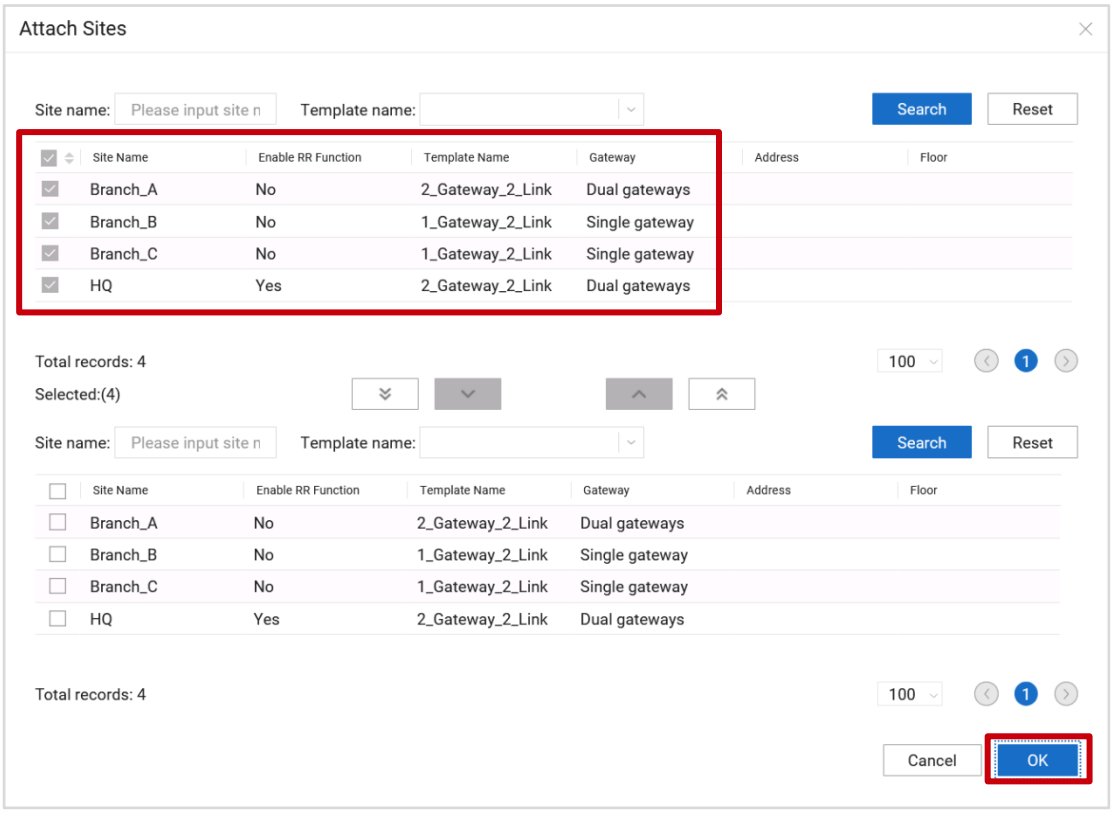
The configuration of the intelligent traffic steering policy Online_Training is similar to that of the intelligent traffic steering policy Course_Development and is not provided.

After configuring Online_Course and Course_Development, you need to associate related sites and submit the configuration. The related planning is as follows.

VN	Policy Name	Associated Site
Online Training	Online_Training	HQ, Branch_A, Branch_B, Branch_C
Course Development	Course_Development	HQ, Branch_A, Branch_B, Branch_C

Associate sites and policies in the corresponding VN based on the planning and submit the application.

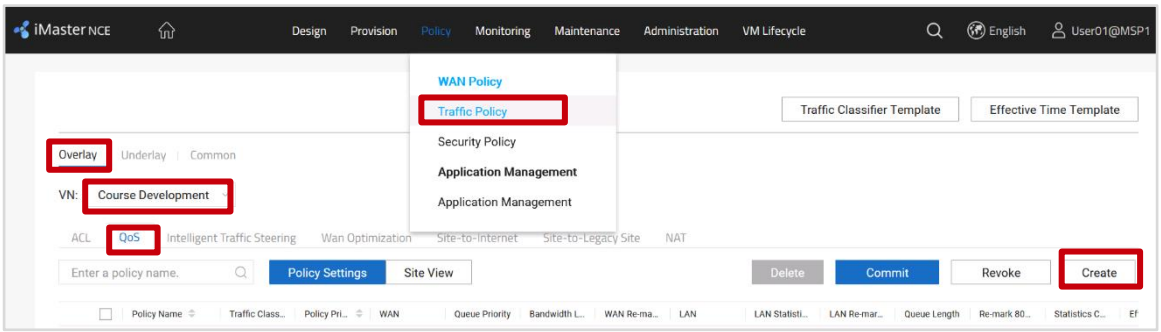




The configuration of Online_Training is similar to that of Course_Development and is not provided.

QoS needs to be deployed to limit the bandwidth used by the Course development department on the Internet.

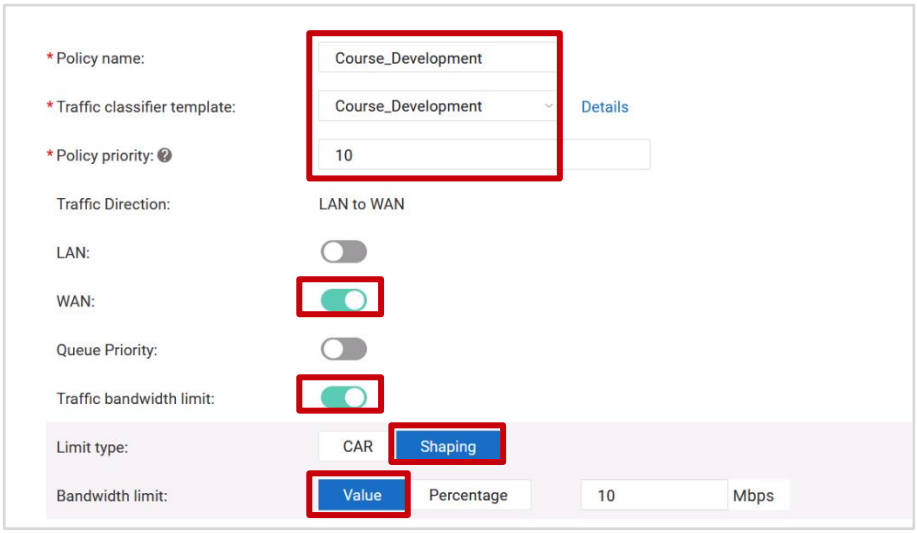
Choose Policy > WAN Policy > Traffic Policy from the main menu, click the Overlay tab, and configure a QoS policy for the virtual network Course_Development.



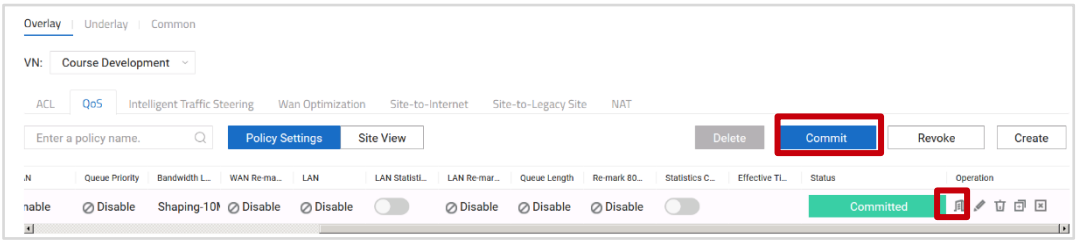
The QoS planning is as follows.

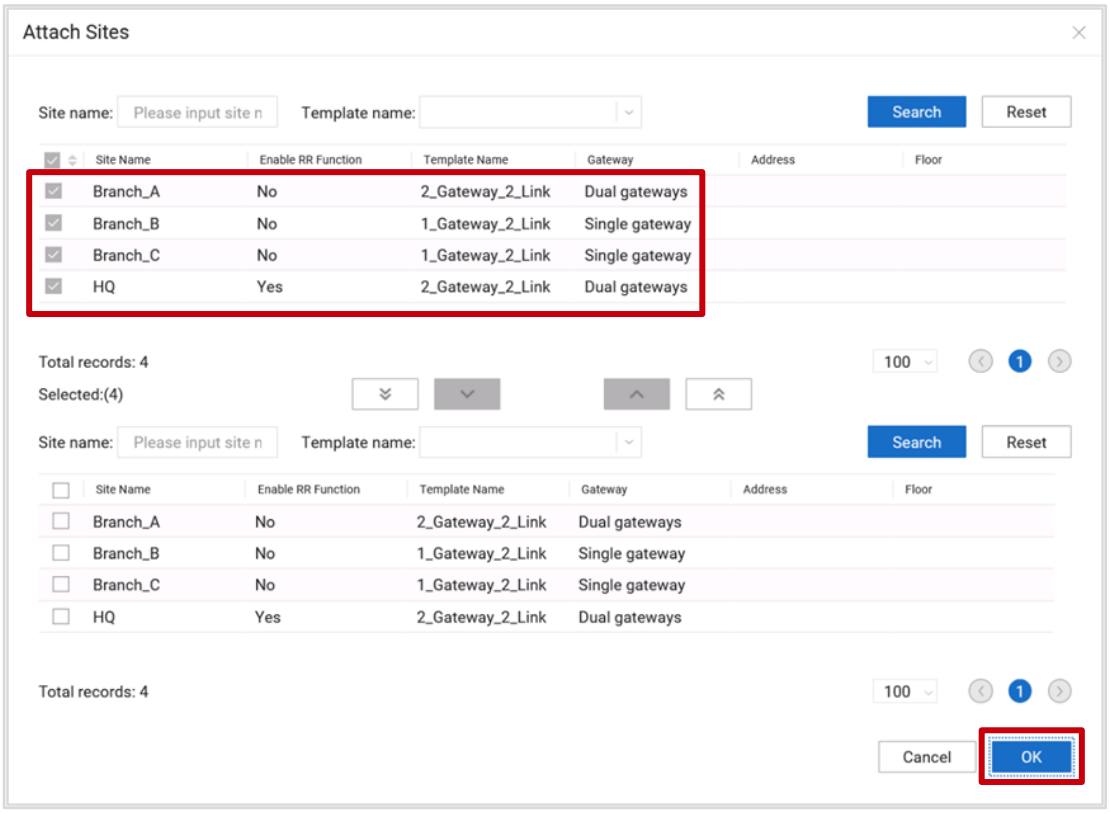
VN	Policy Name	Traffic Classifier	Policy Priority	QoS Configuration
Course Development	Course_Development	Course_Development	10	Outbound traffic shaping, and rate limit of 10 Mbit/s

Configure QoS parameters as planned.



Associate the QoS policy with all sites on the virtual network Course Development and submit the configuration.





Rate limiting is not required for the virtual network Online Training, so QoS does not need to be performed.

Step 4 Configure an Internet access policy for a site.

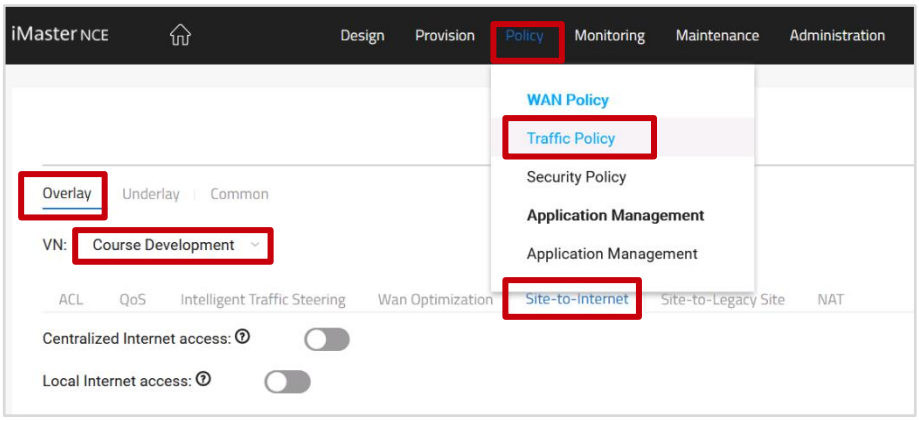
If a site needs to access the Internet, you need to configure an Internet access policy for the site. Currently, centralized Internet access and distributed Internet access are supported.

Currently, two Internet access modes are supported: centralized and distributed. If both the centralized and distributed Internet access modes are configured for a site,

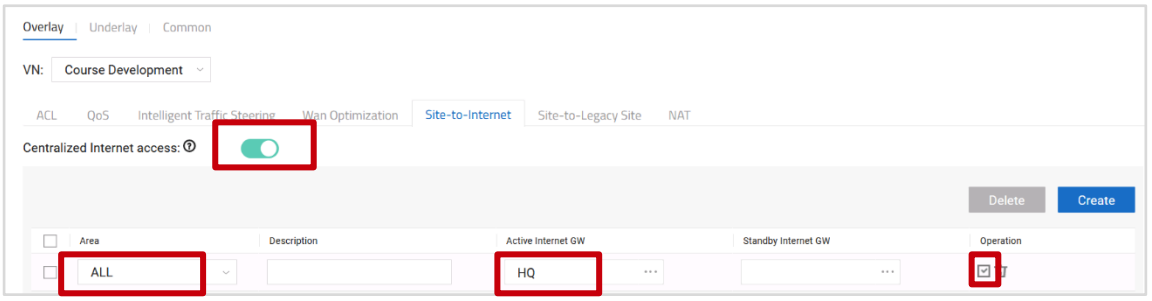
the distributed access mode (namely, local Internet access mode) is used preferentially.

In this lab, only the Course development department is allowed to access the Internet. In addition, only centralized Internet access can be deployed for the Course development, facilitating management.

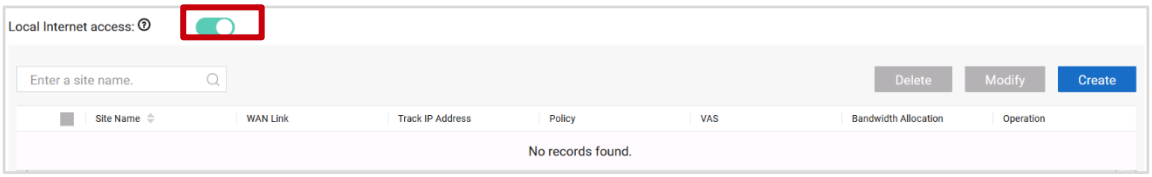
Choose Policy > WAN Policy > Traffic Policy from the main menu. Click the Overlay tab, select a VN, click the Site-to-Internet tab, and configure an Internet access policy for the site.

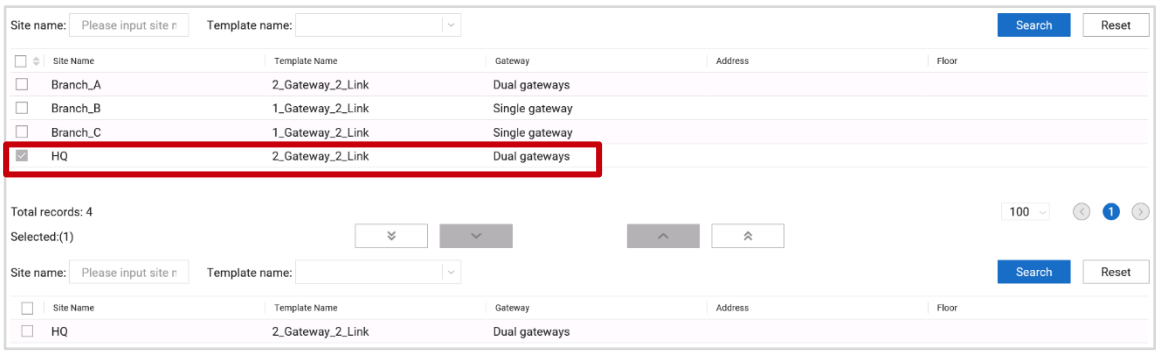


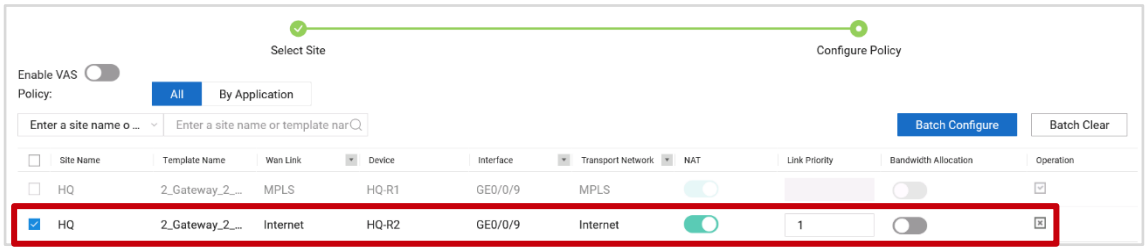
For the virtual network Course Development, configure centralized Internet access and set the primary gateway to the hub.



For the virtual network Course Development, configure local Internet access and use the Internet line of HQ-R2 as the egress.







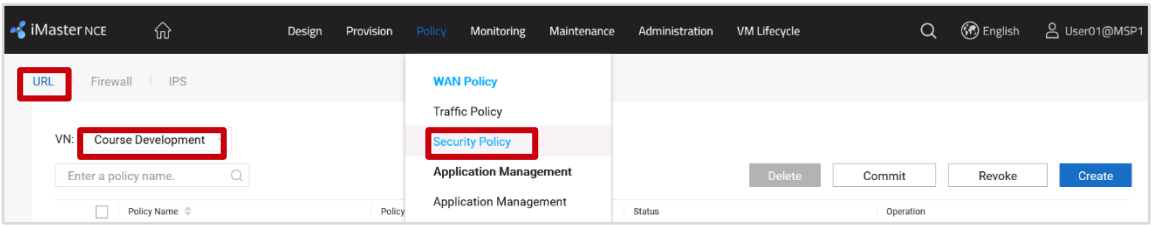
After the configuration is complete, apply the configuration.

Step 5 Configure a security policy.

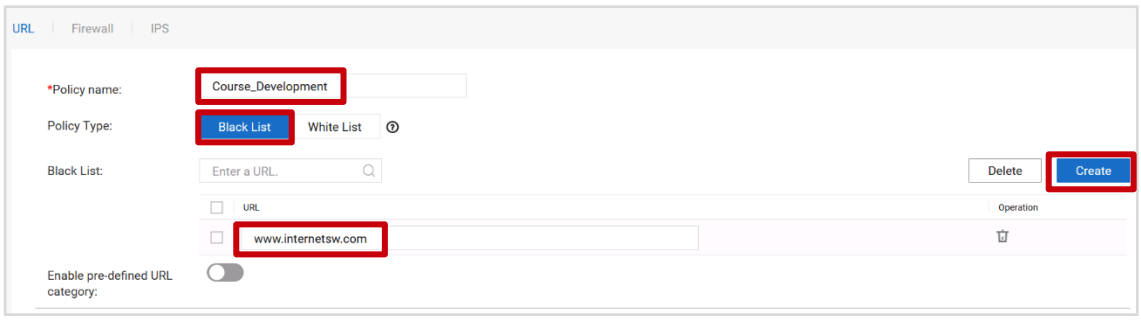
Security policies include URL filtering policies, firewall policies, and IPS policies. This lab mainly deploys URL filtering policies.

In this lab, only some sites of the Course development department can access the Internet.

Choose Policy > WAN Policy > Security Policy from the main menu and click the URL tab to create a URL filtering policy.

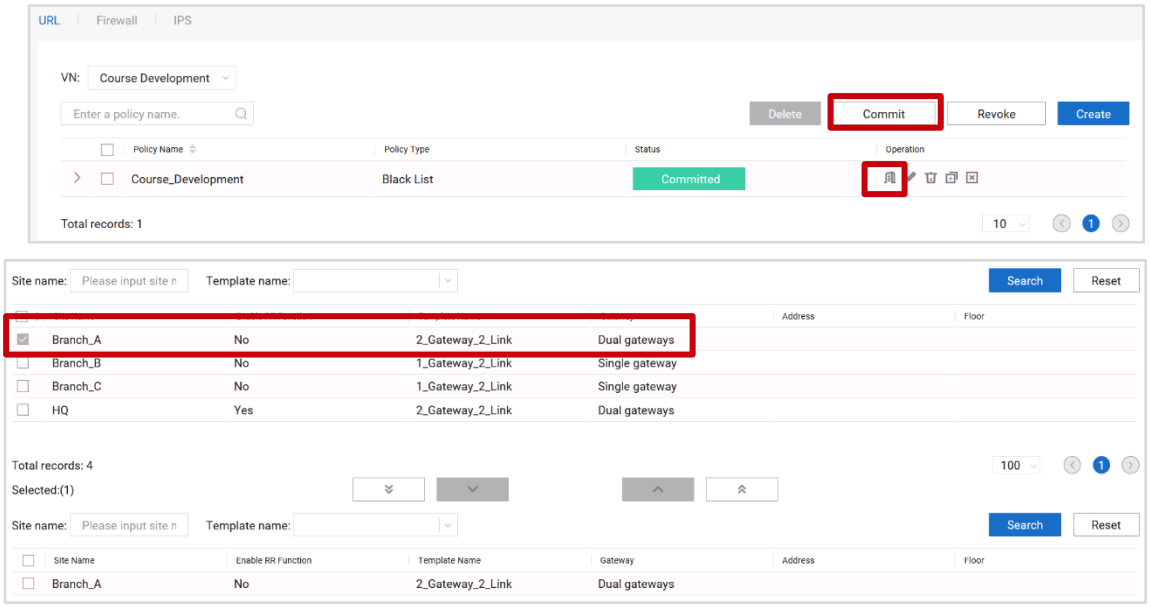


Configure a URL filtering policy named Course_Development, use the blacklist to filter the URL www.internetsw.com, and click OK.



At Branch_A, terminals of the Course development department are not allowed to access the website www.internetsw.com, but terminals of the Course development department at other sites can access the website.

Bind the URL filtering policy to Branch_A and commit the configuration.



Step 6 Verify that the policies are successfully deployed.

Terminals in the Course development department of Branch_A cannot access the website www.internetsw.com. Terminals in the Course development departments at other sites can access the website.

The following table describes login information of the training development department.

Department	Service	Client	Login IP Address	User Name/Password
Course development department	FTP and HTTP services	Branch-A-2-PC	172.21.16.235	admin/Huawei@123
		Branch-B-1-PC	172.21.16.236	admin/Huawei@123
		Branch-C-1-PC	172.21.16.237	admin/Huawei@123

Log in to the terminal at each site and attempt to access the website www.internetsw.com.

----End

5.6 Routine O&M

5.6.1 Introduction

5.6.1.1 Objectives

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

- Implement routine network O&M.

5.6.1.2 Networking Topology

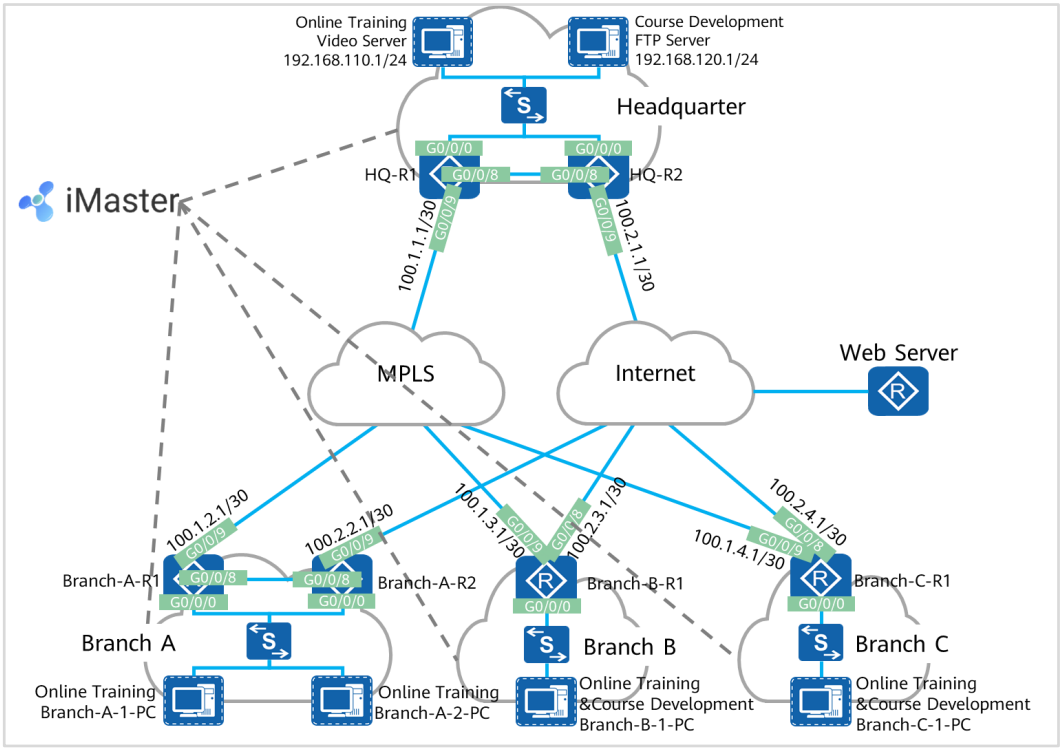


Figure5-6 SD-WAN topology

The figure shows the interconnection IP addresses. The headquarters and Branch A are connected to the MPLS network and Internet through dual egresses and links, and Branch B and Branch C are connected to the MPLS network and Internet through a single egress and dual links. Two links connect the MPLS network and Internet respectively, and the MPLS network and Internet are isolated from each other. Devices connect to iMaster NCE-WAN through public IP addresses.

5.6.1.3 Lab Background

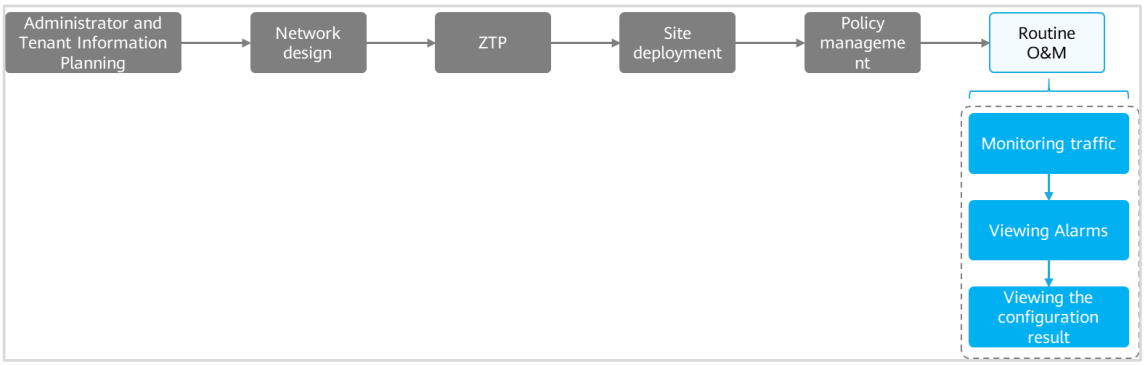
An enterprise needs to deploy new sites. To quickly deploy network services and simplify O&M, the enterprise deploys the iMaster NCE-WAN solution.

Network planning and management personnel need to construct a network using iMaster NCE-WAN based on the network topology and requirements.

5.6.2 Lab Tasks

5.6.2.1 Configuration Roadmap

To deploy iMaster NCE-WAN, perform the following steps. This lab mainly describes how to view the network status of iMaster NCE-WAN.



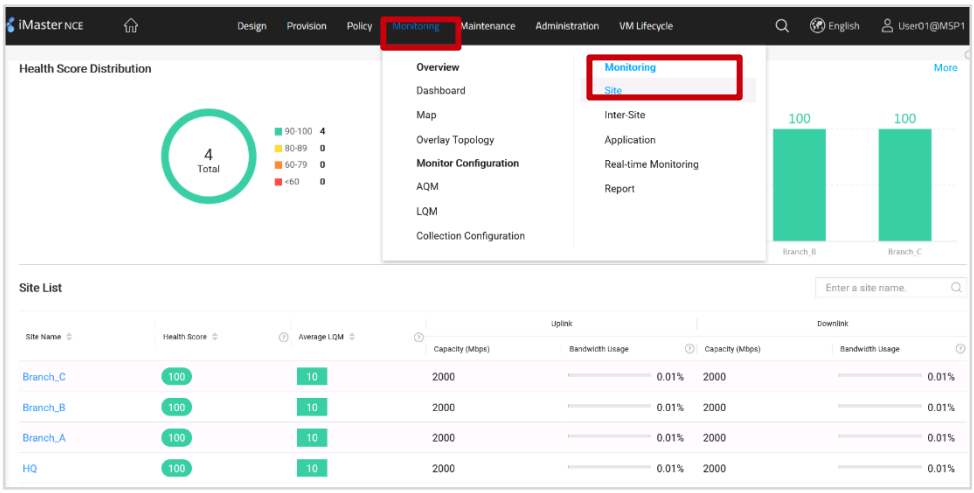
The configuration roadmap is as follows:

1. Check intra-site and inter-site traffic.
2. Check device alarms.
3. Check the device configuration.

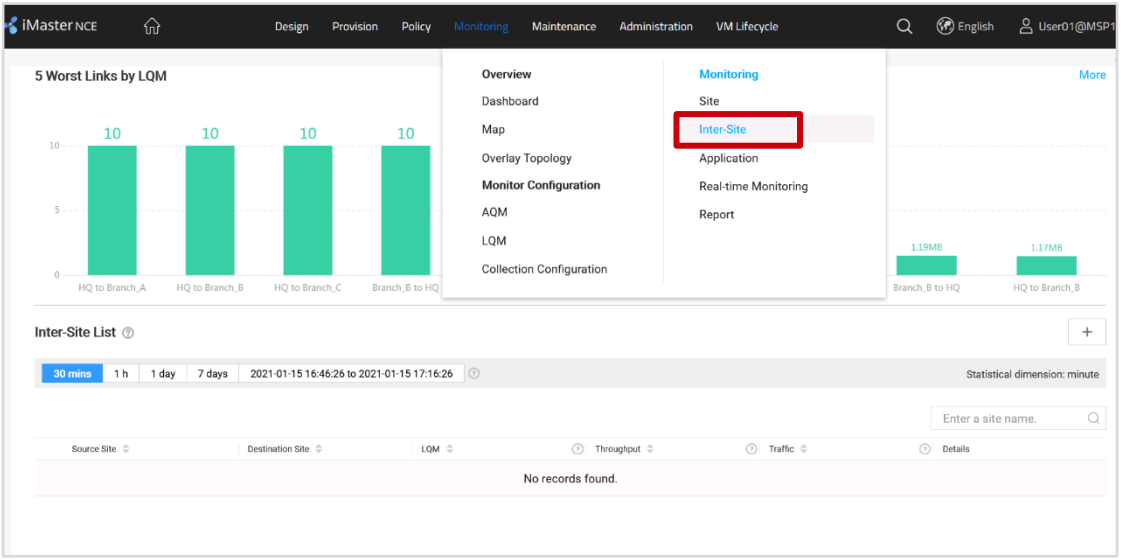
5.6.2.2 Configuration Procedure

Step 1 Check site health and inter-site traffic.

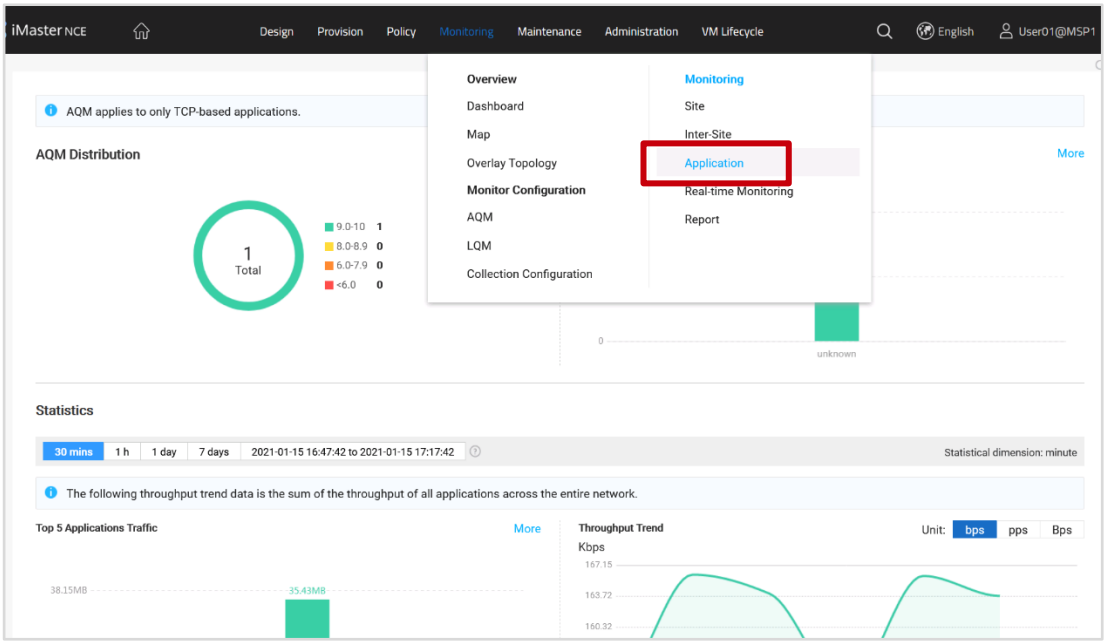
Choose Monitoring > Monitoring > Site from the main menu to check the health status of the site.



Choose Monitoring > Monitoring > Inter-Site from the main menu to check inter-site traffic.

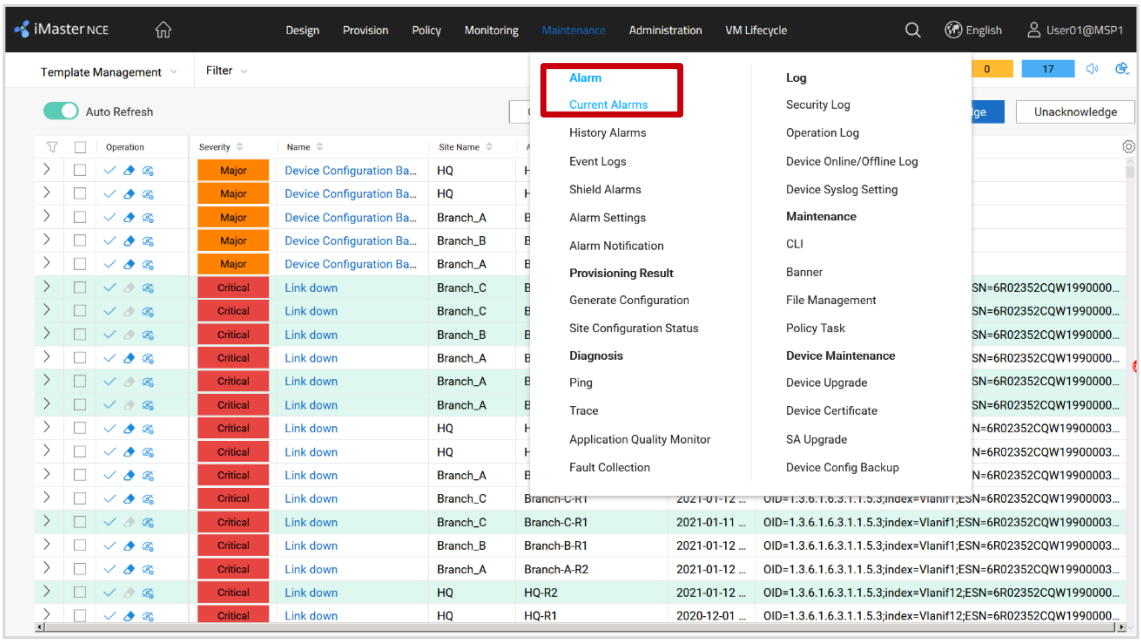


Choose Monitoring > Monitoring > Application from the main menu to check application traffic.



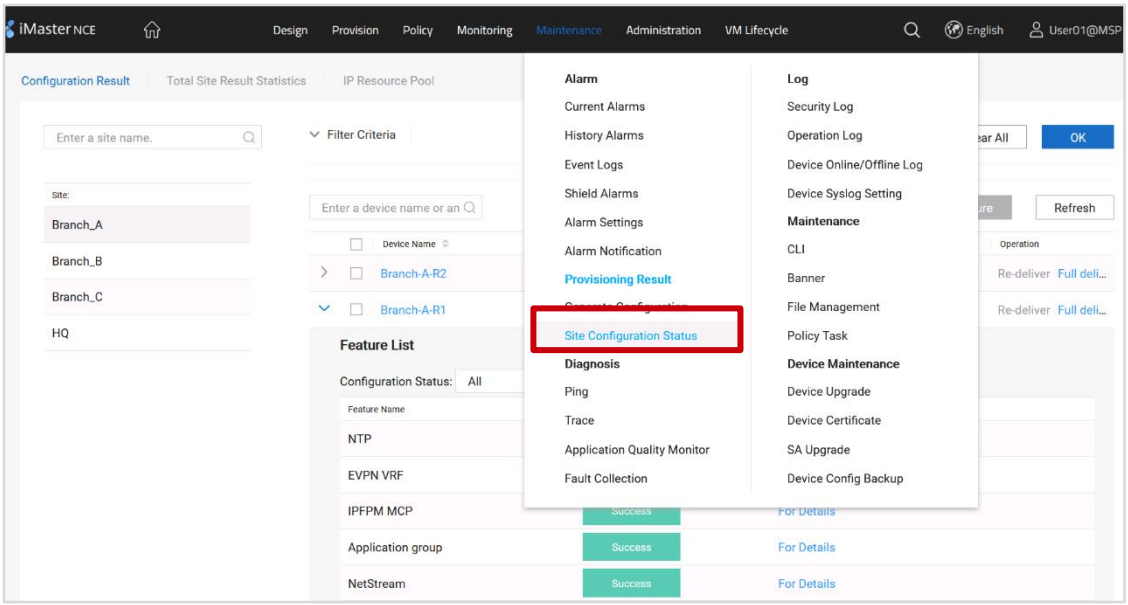
Step 2 Check device alarms.

Choose Maintenance > Alarm > Current Alarms from the main menu to check current alarms reported by the device.



Step 3 Check the device configuration.

 # Choose Maintenance > Provisioning Result > Site Configuration Status from the main menu to check whether iMaster NCE-WAN has successfully delivered configurations.



----End