Quick Configuration

HUAWEI S Series Campus Switches

Issue: 06 (2018-08-10)

HUAWEI TECHNOLOGIES CO., LTD

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/en/

Contents

1 Before You Start

This document will help you log in to and quickly configure Huawei S series switches. For more service configurations, see the Switch Configuration Guide.

NOTE

> This document is for switches running V200R003C00 and later. You can run the **display version** command in the user view to check the version of the device.

Before configuring any data, complete the following tasks:

1. Install and power on the switch. For details refer to the S7700 and S9700 Quick Installation Guide, S12700 Quick Installation Guide, or 2700, S3700, S5700, and S6700 Series Switches Quick Start Guide.

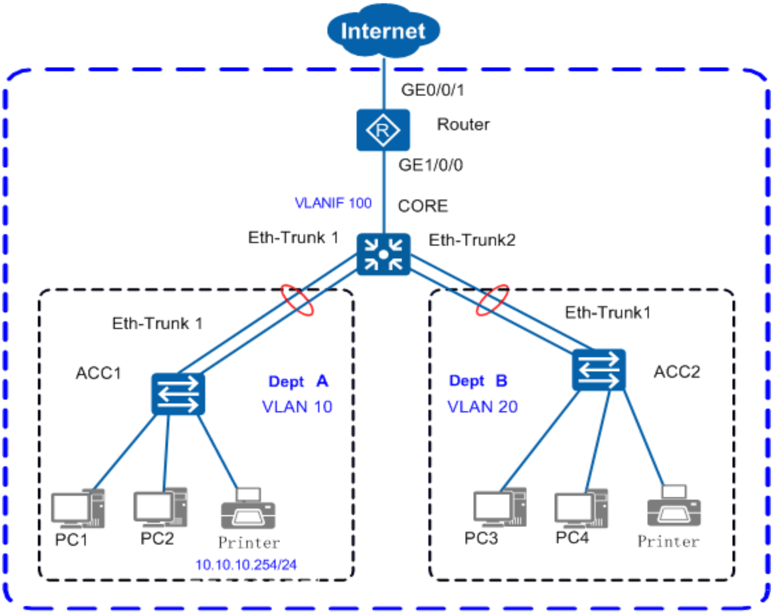
2. Place the following *contact details* around your workplace:
   Telephone number of the agent responsible for your network construction and service.

3. Visit the Huawei Enterprise Service Technical Support website (http://support.huawei.com/enterprise) to register an *account*. With an account, you can browse or download more product documents, cases, and bulletins. You can also enjoy our subscription and message push services.

2 Small-Sized Campus Networks

NOTE

This section uses the *S2750* as an access switch *(ACC1)*, *S5700* as a core switch *(CORE)*, and an AR series router as an egress router *(Router)* as examples to demonstrate the configuration procedure for small-sized campus networks.



ACC1	Eth -Trunk1 GE 0/0/ 1 GE 0/0/ 2	PC1/PC2 Eth 0/0/2 Eth 0/0/3	Printer Eth0/0/4
CORE	Eth -Trunk1 GE 0/0/ 1 GE 0/0/ 2	VLAN 100 GE0/0/20	

- On small-sized networks, S2700&S3700 switches are deployed at the access layer, S5700&S6700 switches is deployed at the core layer, and an AR series router works as the egress router.
- The access switches and core switch connect through *Eth-Trunk* to ensure reliability.
- On an access switch, each department has a *VLAN* allocated so that services are separated by VLANs. Configuring a *VLANIF interface* on the core switch implements Layer 3 communication between different departments.
- The core switch functions as a *DHCP server* to allocate IP addresses to user devices on the campus network.
- Configuring *DHCP snooping* on the access switches prevents intranet users from connecting a small router to the intranet to allocate IP addresses. Configuring *IPSG* on the access switches prevents intranet users from changing IP addresses.

2.1 Data Plan

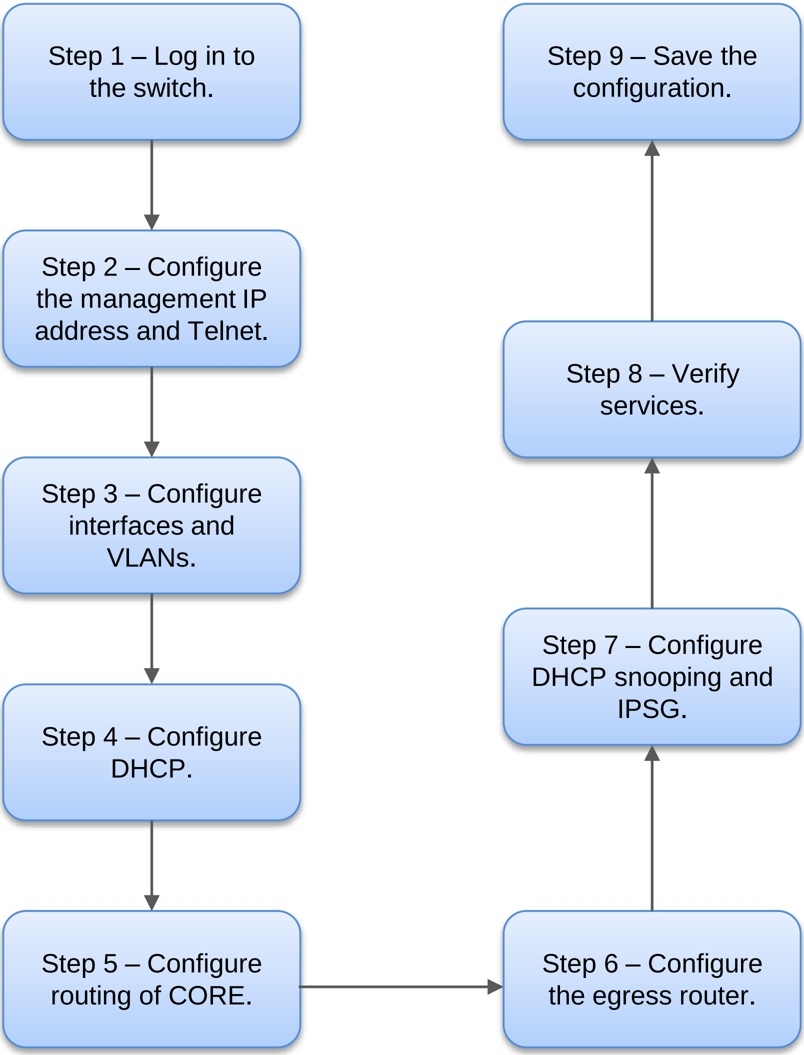
Before configuring the switches and router, prepare the following data for use in the next section.

Action	Component	Data	Description
Configure the management IP address and Telnet	Management IP address	10.10.1.1/24	The management IP address is used to log in to the switch.
	Management VLAN	VLAN 5	A modular switch's management interface is Ethernet0/0/0. A fixed switch's management interface is MEth0/0/1. For switches without management interfaces, you are advised to use VLANIF interfaces for inband management.
Configure interfaces and VLANs	Eth-Trunk type	Static LACP	The Eth-Trunk works in load balancing or static LACP mode.
	Port type	The Trunk port connects to a switch, and the Access port connects to a PC.	This configuration is for Trunk and Access port setup. If a Hybrid port setup is available on a switch, this port can connect to either a host or another switch.
	VLAN ID	ACC1: VLAN 10 ACC2: VLAN 20 CORE: VLANs 100, 10, and 20	VLAN1 is the default VLAN on the switch. To isolate departments A and B at Layer 2, add A to VLAN 10 and B to VLAN 20. CORE connects to the egress router through VLANIF100.
Configure DHCP	DHCP server	CORE	Configure the DHCP server function on CORE.
	Address pool	VLAN 10: IP address pool 10 VLAN 20: IP address pool 20	Terminals in department A obtain IP addresses from IP address pool 10. Terminals in department B obtain IP addresses from IP address pool 20.
	Address allocation	Based on a global address pool	None
Configure routing of CORE	IP address	CORE: VLANIF 100 10.10.100.1/24 VLANIF 10 10.10.10.1/24 VLANIF 20 10.10.20.1/24	CORE connects to the campus egress router through VLANIF 100 so that the campus intranet can communicate with the Internet. Configure a default route on CORE with the next hop pointing to the egress router. After configuring the IP addresses of VLANIF 10 and VLANIF 20 on CORE, departments A and B can then communicate through CORE.

Action	Component	Data	Description
Configure the egress router	Public interface IP address	GE0/0/1: 1.1.1.2/30	GE0/0/1 is the public interface that connects the egress router to the Internet.
	Public gateway	1.1.1.1/30	The public gateway address is the IP address of the carrier device that connects to the egress router. Configure a default route to this IP address on the egress router to forward intranet traffic to the Internet.
	DNS server address	8.8.8.8	The DNS server resolves domain names into IP addresses.
	Intranet interface IP address	GE1/0/0: 10.10.100.2/24	GE1/0/0 connects the egress router to the intranet.
Configure DHCP snooping and IPSG	Trusted interface	Eth-Trunk1	None

2.2 Quickly Configuring Small-Sized Campus Networks

Follow the procedure shown below to configure the switches and router. Once configurations are complete, user devices within the campus can communicate with each other, and intranet users can access the Internet.



Step 1 – Log in to the switch.

Step 2 – Configure the management IP address and Telnet.

Step 3 – Configure interfaces and VLANs.

Step 4 – Configure DHCP.

Step 5 – Configure routing of CORE.

Step 6 – Configure the egress router.

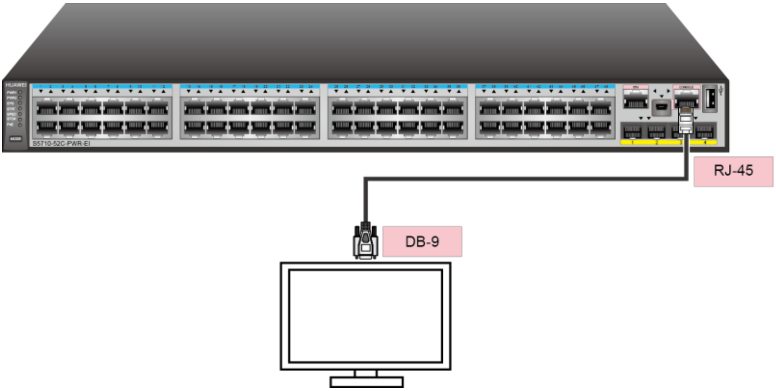
Step 7 – Configure DHCP snooping and IPSG.

Step 8 – Verify services.

Step 9 – Save the configuration.

Logging In to the Switch

1 Connect your PC to the switch through the console cable provided with the switch. If your PC does not have a serial port, use a USB to serial cable.



NOTE

If the switch has a Mini USB port, you can connect your PC to the switch using a Mini USB cable. For this configuration procedure, see the corresponding Configuration Guide - Basic Configuration based on the version of the device.

2 Open the terminal emulation program on your PC. Create a connection and set the interface and communication parameters.

Select an available port on your PC. For example, if your PC runs a Windows operating system, you can view port information in Device Manager and select a port. Table 1 lists the communication parameters on the switch.

Table 1 Default settings of the console port on the switch

Parameter	Default Value
Transmission rate	9600 bit/s
Flow control	None
Parity bit	None
Stop bit	1
Data bit	8

3 Press **Connect** until the following information is displayed. Enter your new password, and then re-enter it to confirm.

```
Login authentication


Username:admin
Password:
```

NOTE

If you log in to the switch for the first time in versions earlier than V200R010C00, the system asks you to set a login password. In V200R010C00 and later versions, the default user name for first login is **admin** and default password is **admin@huawei.com**. You must change the password after login.

You can now run commands to configure the switch. Enter a question mark (?) after a command whenever you need help.

Configuring the Management IP Address and Telnet

After configuring the management IP address of a switch, you can log in to the switch using this address. CORE is used in the example below to show the procedure of configuring the management IP address and Telnet.

1 Configure the management IP address.

```
<HUAWEI> system-view
[HUAWEI] vlan 5                               //Create management VLAN 5.
[HUAWEI-VLAN5] management-vlan
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5
[HUAWEI-vlanif5] ip address 10.10.1.1 24
[HUAWEI-vlanif5] quit
```

2 Add the management interface to the management VLAN.

```
[HUAWEI] interface GigabitEthernet 0/0/8       //Assume that the interface
connected to the NMS is GigabitEthernet 0/0/8.
[HUAWEI-GigabitEthernet0/0/8] port link-type trunk
[HUAWEI-GigabitEthernet0/0/8] port trunk allow-pass vlan 5
[HUAWEI-GigabitEthernet0/0/8] quit
```

3 Configure Telnet.

```
[HUAWEI] telnet server enable //By default, the Telnet function is disabled.
[HUAWEI] user-interface vty 0 4   //An administrator generally logs in to
the switch through Telnet. AAA authentication is recommended.
[HUAWEI-ui-vty0-4] protocol inbound telnet
//V200R006 and earlier versions support Telnet. V200R007 and later versions
support SSH by default. If the switch runs V200R007 or a later version, run
this command before logging to the switch using Telnet.
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] idle-timeout 15
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin password irreversible-cipher  Helloworld@6789
//Configure the user name and password for Telnet login. The user name is
case-insensitive, whereas the password is case-sensitive.
[HUAWEI-aaa] local-user admin privilege level 15 //Set the administrator
account level to 15 (highest).
[HUAWEI-aaa] local-user admin service-type telnet
```

NOTE

Use of STelnet V2 to log in to the switch is recommended because the Telnet protocol has security risks. For this configuration procedure, see the corresponding Configuration Guide - Basic Configuration based on the version of the device.

4 Log in to the switch from an operation terminal through Telnet. When the user view prompt is displayed, you have successfully logged in.

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1   //Enter the
management IP address and press Enter.
Login authentication

Username:admin      //Enter the user name and password.
Password:
 Info: The max number of VTY users is 5, and the number
       of current VTY users on line is 1.
       The current login time is 2014-05-06 18:33:18+00:00.
<HUAWEI>             //User view prompt
```

Configuring Interfaces and VLANs

a. Configure the access switch.

1 Starting with access switch ACC1 as an example, create service VLAN 10 on ACC1.

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1          //Set the switch name to ACC1.
[ACC1] vlan batch 10           //Create VLANs in a batch.
```

2 Configure Eth-Trunk 1, through which ACC1 connects to the CORE, to allow the packets from the VLAN of department A to pass through.

```
[ACC1] interface eth-trunk 1
[ACC1-Eth-Trunk1] port link-type trunk          //Set Eth-Trunk 1 type to
Trunk for VLAN transparent transmission.
[ACC1-Eth-Trunk1]  port trunk allow-pass vlan 10  //Configure Eth-Trunk 1
to transparently transmit the service VLAN on ACC1.
[ACC1-Eth-Trunk1] mode lacp                         //Configure the LACP mode
on Eth-Trunk 1.
[ACC1-Eth-Trunk1] quit
[ACC1] interface GigabitEthernet 0/0/1              //Add member interfaces to
Eth-Trunk 1.
[ACC1-GigabitEthernet0/0/1] Eth-Trunk 1
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface GigabitEthernet 0/0/2
[ACC1-GigabitEthernet0/0/2] Eth-Trunk 1
[ACC1-GigabitEthernet0/0/2] quit
```

3 Configure the interfaces on ACC1 that connect user devices so that user devices can be added to the VLAN. Configure the interfaces as edge ports.

```
[ACC1] interface  Ethernet 0/0/2 //Configure the interface connecting to PC1.
[ACC1-Ethernet0/0/2] port link-type access
[ACC1-Ethernet0/0/2] port default vlan 10
[ACC1-Ethernet0/0/2] stp edged-port enable
[ACC1-Ethernet0/0/2] quit
[ACC1] interface  Ethernet 0/0/3 //Configure the interface connecting to PC2.
[ACC1-Ethernet0/0/3] port link-type access
[ACC1-Ethernet0/0/3] port default vlan 10
[ACC1-Ethernet0/0/3] stp edged-port enable
[ACC1-Ethernet0/0/3] quit
[ACC1] interface  Ethernet 0/0/4    //Configure the interface connecting to
printers.
[ACC1-Ethernet0/0/4] port link-type access
[ACC1-Ethernet0/0/4] port default vlan 10
[ACC1-Ethernet0/0/4] stp edged-port enable
[ACC1-Ethernet0/0/4] quit
```

NOTE

To add all users connected to ACC1 to VLAN 10, you can add Eth-Trunk1 on CORE to VLAN 10 as an Access interface and do not add interfaces on ACC1 to VLAN 10, simplifying the configuration. This configuration ensures that all users connected to Eth-Trunk1 belong to VLAN 10.

4 Configure the BPDU protection function to improve network stability.

```
[ACC1] stp bpdu-protection
```

b. Configure the core switch (CORE).

1 Create the VLANs for CORE to communicate with ACC1, ACC2, and the egress router.

```
<HUAWEI> system-view
[HUAWEI] sysname CORE           //Set the switch name to CORE.
[CORE] vlan batch 10 20 100     //Create VLANs in a batch.
```

2 Configure downstream interfaces and VLANIF interfaces. Communication between departments A and B uses VLANIF interfaces. For example, CORE connects to ACC1 through Eth-Trunk 1.

```
[CORE] interface eth-trunk 1
[CORE-Eth-Trunk1] port link-type trunk         //Set the interface type to
Trunk for VLAN transparent transmission.
[CORE-Eth-Trunk1] port trunk allow-pass vlan 10 //Configure Eth-Trunk 1 to
transparently transmit the service VLAN on ACC1.
[CORE-Eth-Trunk1] mode lacp                //Configure the LACP mode.
[CORE-Eth-Trunk1] quit
[CORE] interface GigabitEthernet 0/0/1     //Add member interfaces to Eth-
Trunk 1.
[CORE-GigabitEthernet0/0/1] Eth-Trunk 1
[CORE-GigabitEthernet0/0/1] quit
[CORE] interface GigabitEthernet 0/0/2
[CORE-GigabitEthernet0/0/2] Eth-Trunk 1
[CORE-GigabitEthernet0/0/2] quit
[CORE] interface Vlanif 10             //Configure a VLANIF interface to
allow department A to communicate with department B through Layer 3.
[CORE-Vlanif10] ip address 10.10.10.1 24
[CORE-Vlanif10] quit
[CORE] interface Vlanif 20             //Configure a VLANIF interface to
allow department B to communicate with department A through Layer 3.
[CORE-Vlanif20] ip address 10.10.20.1 24
[CORE-Vlanif20] quit
```

3 Configure upstream interfaces and VLANIF interfaces to allow the campus network to communicate with the Internet.

```
[CORE] interface GigabitEthernet 0/0/20
[CORE-GigabitEthernet0/0/20] port link-type access   //Set the access mode.
[CORE-GigabitEthernet0/0/20] port default vlan 100
[CORE-GigabitEthernet0/0/20] quit
[CORE] interface Vlanif 100            //Configure a VLANIF interface to
allow CORE to communicate with the router at Layer 3.
[CORE-Vlanif100] ip address 10.10.100.1 24
[CORE-Vlanif100] quit
```

4 After configuring the interfaces and VLANs, run the following commands to view the configuration results. For details about the command output, see the corresponding Command Reference based on the version of the device.

Run the ***display eth-trunk*** command to view the configurations of Eth-Trunk on ACC1.

```
[ACC1] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                    WorkingMode: LACP
Preempt Delay: Disabled      Hash arithmetic: According to SA-XOR-DA
System Priority: 32768       System ID: 0200-0000-6704
Least Active-linknumber: 1   Max Active-linknumber: 8
Operate status: up           Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
ActorPortName           Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/1    Selected 100M     32768   2      289     10111100  1
GigabitEthernet0/0/2    Selected 100M     32768   3      289     10100010  1

Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri   SystemID         PortPri PortNo PortKey PortState
GigabitEthernet0/0/1    32768    0012-3321-2212   32768   2      289     10111100
GigabitEthernet0/0/2    32768    0012-3321-2212   32768   3      289     10111100
```

ACC1's GE0/0/1 and GE0/0/2 interfaces have been added to Eth-Trunk 1.

Run the ***display vlan*** command to view VLAN configurations on ACC1.

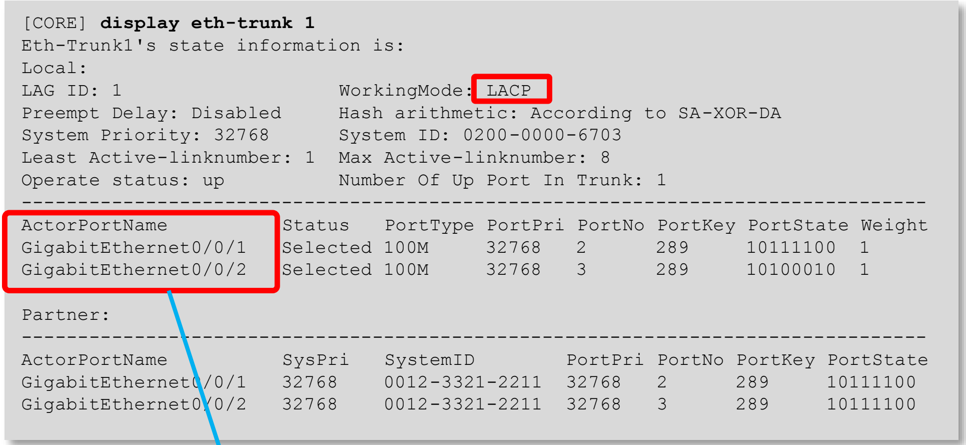
On ACC1, interfaces Eth0/0/2 to Eth0/0/4 have been added to VLAN 10 in Untagged mode, and Eth-Trunk 1 has been added to VLAN 10 in Tagged mode.

```
[ACC1] display vlan
The total number of VLANs is : 1
--------------------------------------------------------------------------------
U: Up;          D: Down;          TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                 ST: Vlan-stacking;
#: ProtocolTransparent-vlan;     *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
10   common  UT:Eth0/0/2(U)      Eth0/0/3(U)      Eth0/0/4(U)
             TG:Eth-Trunk1(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable  default       enable  disable    VLAN 0010
```

Run the ***display eth-trunk*** command to view Eth-Trunk configurations on CORE.



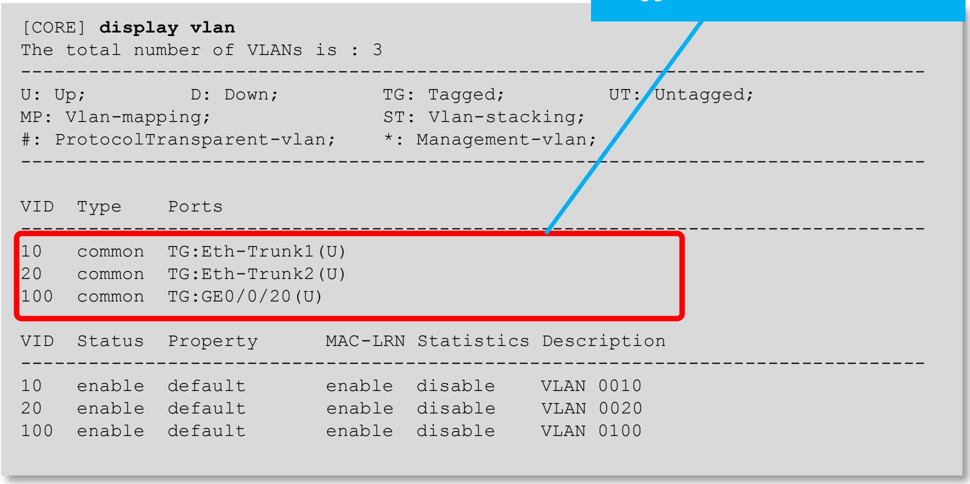
```
[CORE] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: LACP
Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-DA
System Priority: 32768      System ID: 0200-0000-6703
Least Active-linknumber: 1  Max Active-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
ActorPortName          Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/1   Selected 100M     32768   2      289     10111100  1
GigabitEthernet0/0/2   Selected 100M     32768   3      289     10100010  1

Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri   SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/1   32768    0012-3321-2211  32768   2      289     10111100
GigabitEthernet0/0/2   32768    0012-3321-2211  32768   3      289     10111100
```

CORE's GE0/0/1 and GE0/0/2 interfaces have been added to Eth-Trunk 1.

Run the ***display vlan*** command to view VLAN configurations on CORE.

On CORE, Eth-Trunk 1 has been added to VLAN 10, Eth-Trunk 2 has been added to VLAN 20, and GE0/0/20 has been added to VLAN 100 in Tagged mode.



```
[CORE] display vlan
The total number of VLANs is : 3
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
10   common  TG:Eth-Trunk1(U)
20   common  TG:Eth-Trunk2(U)
100  common  TG:GE0/0/20(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable  default       enable  disable    VLAN 0010
20   enable  default       enable  disable    VLAN 0020
100  enable  default       enable  disable    VLAN 0100
```

Configuring DHCP

Configure the DHCP server on CORE to allocate IP addresses to user devices in department A (VLAN 10) and department B (VLAN 20).
Department A is used in the example below.

NOTE

In this section, a global address pool is configured. You can also configure an interface-based address pool. For details on this process, see the corresponding Configuration Guide - IP Service based on the version of the device.

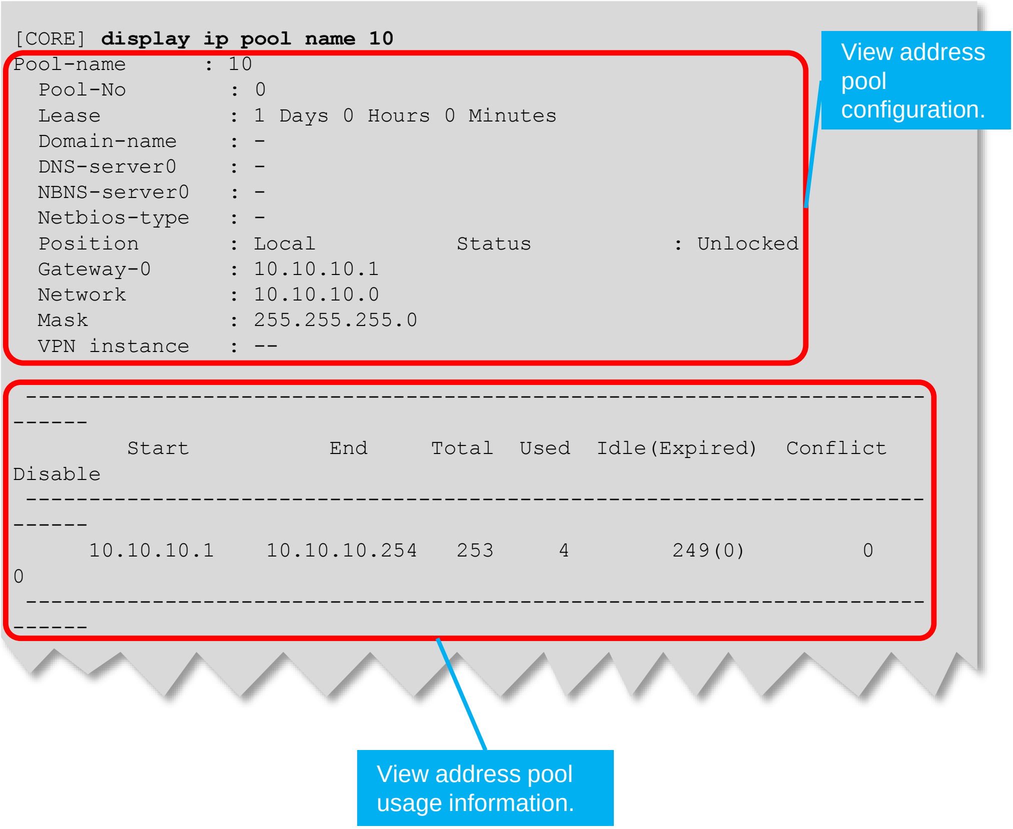
1 Create a global address pool, configure the egress gateway and lease (the default lease, one day, is used, so no command is executed), and allocate fixed IP address 10.10.10.254 to the printer with MAC address a-b-c.

```
<CORE> system-view
[CORE] dhcp enable
[CORE] ip pool 10
[CORE-ip-pool-10] network 10.10.10.0 mask 24     //Specify the address pool
range that is used to allocate IP addresses to users in department A.
[CORE-ip-pool-10] gateway-list 10.10.10.1       //Configure the gateway
address for users in department A.
[CORE-ip-pool-10] static-bind ip-address 10.10.10.254 mac-address a-b-c
//Allocate fixed IP address to the printer.
[CORE-ip-pool-10] quit
```

2 Configure the global address pool to allocate IP addresses to user devices in department A.

```
[CORE] interface vlanif 10
[CORE-Vlanif10] dhcp select global      //Configure the global address pool
to allocate IP addresses to users in department A.
[CORE-Vlanif10] quit
```

3 Run the **display ip pool** command to view configuration and usage information. The example below shows the configuration of global address pool 10.



```
[CORE] display ip pool name 10
Pool-name      : 10
  Pool-No        : 0
  Lease          : 1 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-server0    : -
  NBNS-server0   : -
  Netbios-type   : -
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.10.10.1
  Network        : 10.10.10.0
  Mask           : 255.255.255.0
  VPN instance   : --
 -----------------------------------------------------------------------
------
         Start             End     Total  Used  Idle(Expired)  Conflict
Disable
 -----------------------------------------------------------------------
------
      10.10.10.1    10.10.10.254   253     4        249(0)           0
0
 -----------------------------------------------------------------------
------
```

View address pool configuration.

View address pool usage information.

NOTE

After completing the DHCP server configuration, configure network adapters on terminal PCs to automatically obtain IP addresses. The terminal PCs then can obtain IP addresses from the DHCP server and access the Internet.

NOTE

After dynamic IP address allocation is configured, it takes a PC a long time to obtain an IP address after it starts. The reason is that an STP-enabled switch recalculates the spanning tree topology every time a PC connects to the switch. To solve this problem, disable STP or configure the switch interface that connects to user devices as an edge port. ACC1 is used in the example below.

# Disable STP.

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1- GigabitEthernet 0/0/1] stp disable  //Alternatively, run the undo
stp enable command.
```

# Configure the switch interface that connects to user devices as an edge port.

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1- GigabitEthernet 0/0/1] stp edged-port enable
```

After either of the preceding operations is performed, terminal PCs can rapidly obtain IP addresses after they start.

Configuring Routing

1 Configure a default static route to the campus egress gateway on CORE so that CORE forwards intranet traffic to the egress router.

```
[CORE] ip route-static 0.0.0.0 0 10.10.100.2
```

2 Run the ***display ip routing-table*** command on CORE to view the IP routing table.

```
[CORE] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------
---
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

         0.0.0.0/0   Static  60   0           RD  10.10.100.2     Vlanif100
      10.10.10.0/24  Direct  0    0           D   10.10.10.1      Vlanif10
      10.10.10.1/32  Direct  0    0           D   127.0.0.1       Vlanif10
      10.10.20.0/24  Direct  0    0           D   10.10.20.1      Vlanif20
      10.10.20.1/32  Direct  0    0           D   127.0.0.1       Vlanif20
      10.10.100.0/24  Direct  0    0          D   10.10.100.1     Vlanif100
      10.10.100.1/32  Direct  0    0          D   127.0.0.1       Vlanif100
```

A default static route whose next hop address is 10.10.100.2 exists, indicating that the static route is successfully configured.

The three direct routes are automatically generated through link detection.

Configuring the Egress Router

NOTE

Before configuring the egress router, prepare the following data:

- Public IP address: 1.1.1.2/30
- Public gateway address: 1.1.1.1
- DNS server address: 8.8.8.8

The carrier provides these IP addresses after approving bandwidth service applications. When configuring a network, use the actual IP addresses provided by the carrier.

1 Configure IP addresses for egress router interfaces connecting to the intranet and Internet.

```
[Router] interface GigabitEthernet 0/0/1
[Router -GigabitEthernet0/0/0] ip address 1.1.1.2 30
[Router] interface GigabitEthernet 1/0/0
[Router-GigabitEthernet0/0/1] ip address 10.10.100.2 24
```

2 Configure an ACL to allow users on some network segments to access the Internet.

```
[Router] acl 2000
[Router-acl-basic-2000] rule permit source 10.10.10.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 10.10.20.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 10.10.100.0 0.0.0.255
```

3 Configure NAT on the interface connecting to the Internet so that intranet users can access the Internet.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 2000
```

4 Configure a specific route to the intranet and a default static route to the Internet.

```
[Router] ip route-static 10.10.10.0 255.255.255.0 10.10.100.1
[Router] ip route-static 10.10.20.0 255.255.255.0 10.10.100.1
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

5 Configure DNS resolution. The carrier provides the DNS server address.

```
[Router] dns resolve
[Router] dns server 8.8.8.8
[Router] dns proxy enable
```

Configuring DHCP Snooping and IPSG

User devices can automatically obtain IP addresses after DHCP is configured. If a user connects a small router to the intranet and enable the DHCP server on the router, authorized intranet users may obtain IP addresses allocated by the small router and cannot access the Internet. To prevent this problem, configure DHCP snooping. Department A is used in the example below.

1. Enable DHCP snooping on ACC1.

```
<ACC1> system-view
[ACC1] dhcp enable  //Enable DHCP.
[ACC1] dhcp snooping enable //Enable DHCP snooping.
```

2. Enable DHCP snooping on Eth-Trunk1 that connects to the DHCP server and configure it as a trusted interface.

```
[ACC1] interface eth-trunk 1
[ACC1-Eth-Trunk1] dhcp snooping enable   //Enable DHCP snooping.
[ACC1-Eth-Trunk1] dhcp snooping trusted  //Configure Eth-Trunk1 as a trusted
interface.
[ACC1-Eth-Trunk1] quit
```

3. Enable DHCP snooping on interfaces that connect to user devices.

```
[ACC1] interface  ethernet 0/0/2  //Configure the interface connecting to PC1.
[ACC1-Ethernet0/0/2] dhcp snooping enable
[ACC1-Ethernet0/0/2] quit
[ACC1] interface  ethernet 0/0/3 //Configure the interface connecting to PC2.
[ACC1-Ethernet0/0/3] dhcp snooping enable
[ACC1-Ethernet0/0/3] quit
[ACC1] interface  ethernet 0/0/4 //Configure the interface connecting to printers.
[ACC1-Ethernet0/0/4] dhcp snooping enable
[ACC1-Ethernet0/0/4] quit
```

After the preceding configuration is complete, user devices in department A can obtain IP addresses from only the authorized DHCP server, and will not use IP addresses allocated by the small router.

To prevent users from changing IP addresses and attacking the intranet, enable IPSG after enabling DHCP snooping on the access switch. ACC1 is used in the example below.

4 On ACC1, enable IPSG in VLAN 10.

```
[ACC1] vlan 10
[ACC1-vlan10] ip source check user-bind enable //Enable IPSG.
[ACC1-vlan10] quit
```

ACC1 matches packets received from VLAN 10 with dynamic binding entries in the DHCP snooping binding table. If a packet matches an entry, ACC1 forwards the packet; otherwise, ACC1 discards the packet. To check packets received from a specified user device instead of all user devices in the VLAN, enable IPSG on the interface connecting to the device.

NOTE

If static IP address allocation is configured, bind IP addresses and MAC addresses to prevent users from changing IP addresses and attacking the network. For this configuration procedure, see "Example for Configuring IPSG to Prevent Hosts with Static IP Addresses from Changing Their Own IP Addresses" in the Typical Configuration Examples.

For details about how to configure the switch to prevent users from connecting a small router (bogus DHCP server) to the intranet and changing IP addresses, see "Configuring Basic Functions of DHCP Snooping", "Configuring IPSG", and configuration examples in the corresponding Configuration Guide – Security based on the version of the device.

Verifying Services

1 Select two PCs within a department to perform ping tests and verify whether Layer 2 interworking within the department is normal.

The following example uses two PCs (PC1 and PC2) in department A. The two PCs communicate at Layer 2 through ACC1. If they can ping each other successfully, Layer 2 interworking is normal.

```
<PC1> ping  10.10.10.100                       //Assume that PC2
automatically obtains an IP address 10.10.10.100 through DHCP.
 PING 10.10.10.100 data bytes, press CTRL_C to break
    Reply from 10.10.10.100  : bytes=56 Sequence=1 ttl=253 time=62 ms
    Reply from 10.10.10.100 : bytes=56 Sequence=2 ttl=253 time=16 ms
    Reply from 10.10.10.100 : bytes=56 Sequence=3 ttl=253 time=62 ms
    Reply from 10.10.10.100 : bytes=56 Sequence=4 ttl=253 time=94 ms
    Reply from 10.10.10.100 : bytes=56 Sequence=5 ttl=253 time=63 ms
--- 10.10.10.100 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

PC1 can ping PC2 successfully, indicating that Layer 2 interworking between PC1 and PC2 is normal.

2 Select one PC from each department to perform ping tests and verify whether the two departments can communicate at Layer 3 through VLANIF interfaces.

Users in department A and department B communicate at Layer 3 through VLANIF interfaces on CORE. If PC1 and PC3 can ping each other successfully, users in the two departments can normally communicate at Layer 3 through VLANIF interfaces. The ping command is similar to that in step 1.

3 Select one PC from each department to ping a public network address and verify whether intranet users of the company can access the Internet normally.

The following example uses department A. Generally, you can ping a public network gateway address from PC1 to verify whether PC1 can access the Internet. The public network gateway address is the IP address of the carrier device to which the egress router connects. If the ping test succeeds, intranet users can access the Internet normally. The ping command is similar to that in step 1.

Saving the Configuration

You must save your data to the configuration file before restarting the switch. Unsaved data configured via command lines will be lost after the switch restarts.

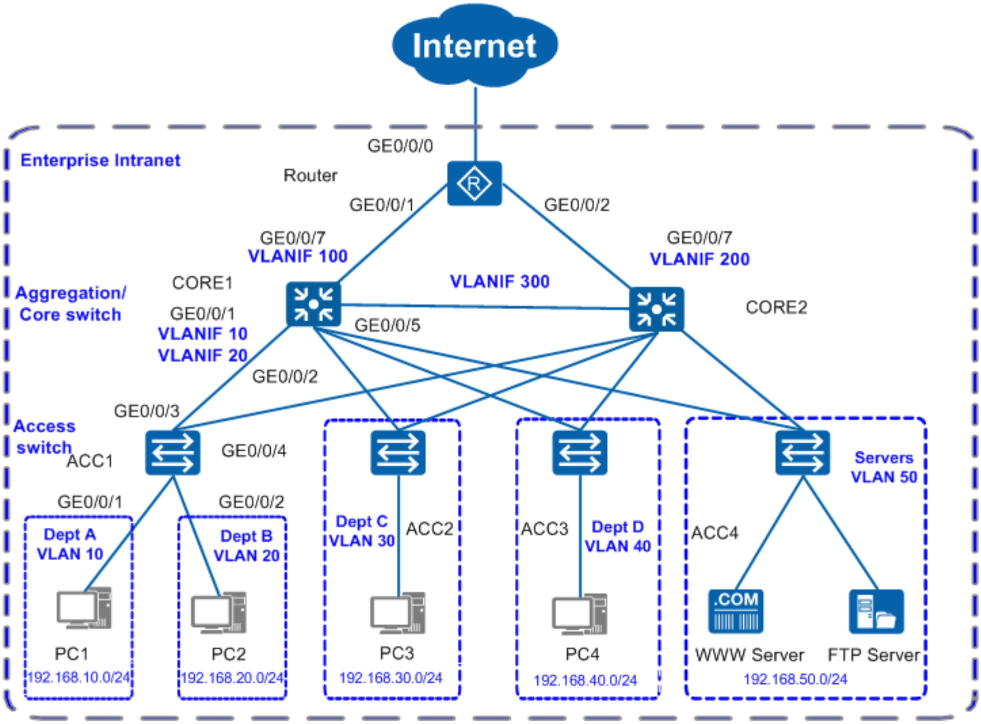
1 Save the data to the configuration file. The example below shows the procedure of saving CORE's configuration file.

```
<CORE> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0..
Save the configuration successfully.
```

3 Small- and Mid-Sized Campus Networks

NOTE

This section uses the *S2750* as an access switch *(ACC1)*, *S5700* as a core switch *(CORE)*, and an *AR series* router as an egress router *(Router)* as examples to demonstrate the configuration procedure for small- and mid-sized campus networks.



- On small- and mid-sized networks, S2700&S3700 switches are deployed at the access layer, S5700&S6700 switches are deployed at the core layer, and an AR series router works as the egress router.
- The core switches run *VRRP* to ensure reliability and *load balance* traffic to effectively use resources.
- On an access switch, each department has a *VLAN* allocated so that services are separated by VLANs. Configuring *VLANIF interfaces* on the core switches implements Layer 3 communication between different departments.
- The core switches function as *DHCP servers* to allocate IP addresses to user devices on the campus network.
- Configuring *DHCP snooping* on the access switches prevents intranet users from connecting a small router to the intranet to allocate IP addresses. Configuring *IPSG* on the access switches prevents intranet users from changing IP addresses.

3.1 Data Plan

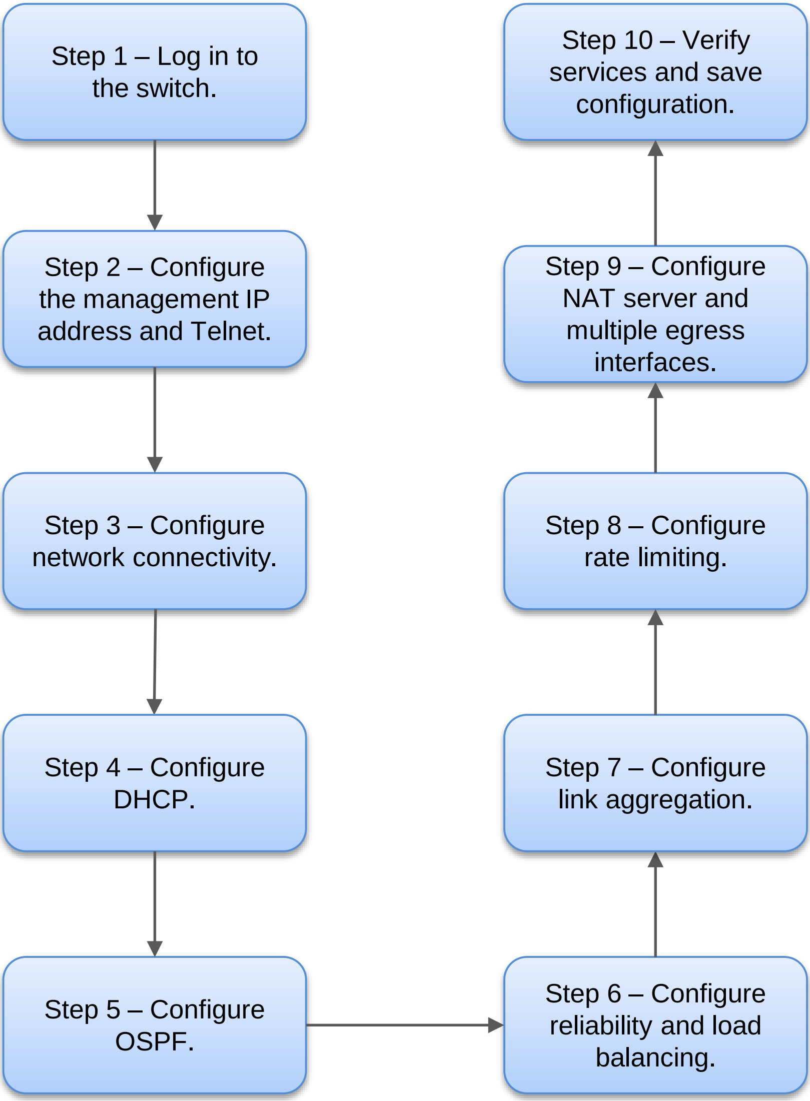
Before configuring the switches and router, prepare the following data for use in the next section.

Action	Component	Data	Description
Configure the management IP address and Telnet	Management interface IP address	10.10.1.1/24	The management IP address is used to log in to the switch.
	Management VLAN	VLAN 5	A modular switch‘s management interface is Ethernet0/0/0. A fixed switch‘s management interface is MEth0/0/1. For switches without management interfaces, you are advised to use VLANIF interfaces for inband management.
Configure interfaces and VLANs	Port type	The Trunk port connects to a switch, and the Access port connects to a PC.	This configuration is for Trunk and Access port setup. If a Hybrid port setup is available on a switch, this port can connect to either a host or another switch.
	VLAN ID	ACC1: VLAN 10, 20 CORE1: VLAN 10, 20, 30, 40, 50, 100, 300	VLAN1 is the default VLAN on the switch. To isolate departments A and B at Layer 2, add A to VLAN 10 and B to VLAN 20. CORE1 connects to the egress router through VLANIF100.
Configure DHCP	DHCP server	CORE1,CORE2	Configure the DHCP server on CORE1 and CORE2.
	Address pool	VLAN 10: IP address pool 10 VLAN 20: IP address pool 20	Terminals in department A obtain IP addresses from IP address pool 10. Terminals in department B obtain IP addresses from IP address pool 20.
	Address allocation	Based on a global address pool	None
Configure routing	IP address	CORE1: VLANIF 100 172.16.1.1/24 VLANIF 300 172.16.3.1/24 VLANIF 10 192.168.10.1/24 VLANIF 20 192.168.20.1/24	CORE1 connects to the campus egress router through VLANIF 100 and connects to CORE2 through VLANIF 300. Configure a primary route to CORE1 with the next hop pointing to the egress router and a backup route with the next hop pointing to CORE2. After configuring the IP addresses of VLANIF 10 and VLANIF 20 on CORE1, departments A and B can then communicate through CORE1.
	Link aggregation	None	The link aggregation mode can be load balancing or static LACP.

Action	Component	Data	Description
Configure the egress router	Public interface IP address	GE0/0/0: 1.1.1.2/30	GE0/0/0 is the public interface that connects the egress router to the Internet.
	Public gateway	1.1.1.1/30	The public gateway address is the IP address of the carrier device that connects to the egress router. Configure a default route to this IP address on the egress router to forward intranet traffic to the Internet.
	DNS server address	8.8.8.8	The DNS server resolves domain names into IP addresses.
	Intranet interface IP address	GE0/0/1: 172.16.1.2/24 GE0/0/2: 172.16.2.2/24	GE0/0/1 and GE0/0/2 connect the egress router to the intranet. They connect to CORE1 and CORE2, respectively.
Configure DHCP snooping and IPSG	Trusted interfaces	GE0/0/3 GE0/0/4	After trusted interfaces are configured, user devices only receive DHCP packets from the trusted interfaces, preventing users from connecting a small router to the intranet to allocate IP addresses.
Configure intranet servers	FTP server Web server	FTP server: 192.168.50.10 Web server: 192.168.50.20	1. The egress router uses NAT to translate between the public and private IP addresses of intranet servers. 2. External users can access the intranet servers using public IP addresses.

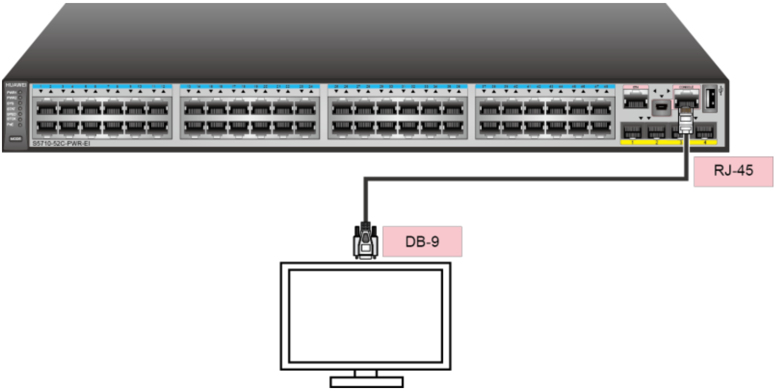
3.2 Quickly Configuring Small- and Mid-Sized Campus Networks

Follow the procedure shown below to configure the switches and router. Once configurations are complete, user devices within the campus can communicate with each other, and intranet users can access the Internet.


Step 1 – Log in to the switch.
Step 2 – Configure the management IP address and Telnet.
Step 3 – Configure network connectivity.
Step 4 – Configure DHCP.
Step 5 – Configure OSPF.
Step 6 – Configure reliability and load balancing.
Step 7 – Configure link aggregation.
Step 8 – Configure rate limiting.
Step 9 – Configure NAT server and multiple egress interfaces.
Step 10 – Verify services and save configuration.

Logging In to the Switch

1 Connect your PC to the switch through the console cable provided with the switch. If your PC does not have a serial port, use a USB to serial cable.



NOTE

If the switch has a Mini USB port, you can connect your PC to the switch using a Mini USB cable. For this configuration procedure, see the corresponding Configuration Guide - Basic Configuration based on the version of the device.

2 Open the terminal emulation program on your PC. Create a connection and set the interface and communication parameters.

Select an available port on your PC. For example, if your PC runs a Windows operating system, you can view port information in Device Manager and select a port. Table 1 lists the communication parameters on the switch.

Table 1 Default settings of the console port on the switch

Parameter	Default Value
Transmission rate	9600 bit/s
Flow control	None
Parity bit	None
Stop bit	1
Data bit	8

3 Press **Connect** until the following information is displayed. Enter your new password, and then re-enter it to confirm.

```
Login authentication


Username:admin
Password:
```

NOTE

If you log in to the switch for the first time in versions earlier than V200R010C00, the system asks you to set a login password. In V200R010C00 and later versions, the default user name for first login is **admin** and default password is **admin@huawei.com**. You must change the password after login.

You can now run commands to configure the switch. Enter a question mark (?) after a command whenever you need help.

Configuring the Management IP Address and Telnet

After configuring the management IP address of a switch, you can log in to the switch using this address. CORE1 is used in the example below to show the procedure of configuring the management IP address and Telnet.

1 Configure the management IP address.

```
 <HUAWEI> system-view
 [HUAWEI] vlan 5                          //Create management VLAN 5.
 [HUAWEI-VLAN5] quit
 [HUAWEI-VLAN5] management-vlan
 [HUAWEI] interface vlanif 5             //Create the VLANIF interface of
 the management VLAN.
 [HUAWEI-Vlanif5] ip address 10.10.1.1 24    //Configure an IP address for
 the VLANIF interface.
 [HUAWEI-Vlanif5] quit
```

2 Add the management interface to the management VLAN.

```
[HUAWEI] interface GigabitEthernet 0/0/8        //Assume that the interface
connected to the NMS is GigabitEthernet 0/0/8.
[HUAWEI-GigabitEthernet0/0/8] port link-type trunk
[HUAWEI-GigabitEthernet0/0/8] port trunk allow-pass vlan 5
[HUAWEI-GigabitEthernet0/0/8] quit
```

3 Configure Telnet.

```
[HUAWEI] telnet server enable //By default, the Telnet function is disabled.
[HUAWEI] user-interface vty 0 4   //An administrator generally logs in to
the switch through Telnet. AAA authentication is recommended.
[HUAWEI-ui-vty0-4] protocol inbound telnet
//V200R006 and earlier versions support Telnet. V200R007 and later versions
support SSH by default. If the switch runs V200R007 or a later version, run
this command before logging to the switch using Telnet.
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] idle-timeout 15
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin password irreversible-cipher  Helloworld@6789
//Configure the user name and password for Telnet login. The user name is
case-insensitive, whereas the password is case-sensitive.
[HUAWEI-aaa] local-user admin privilege level 15 //Set the administrator
account level to 15 (highest).
[HUAWEI-aaa] local-user admin service-type telnet
[HUAWEI-aaa] quit
```

NOTE

Use of STelnet V2 to log in to the switch is recommended because the Telnet protocol has security risks. For this configuration procedure, see the corresponding Configuration Guide - Basic Configuration based on the version of the device.

4 Log in to the switch from an operation terminal through Telnet. When the user view prompt is displayed, you have successfully logged in.

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1   //Enter the
management IP address and press Enter.
Login authentication

Username:admin      //Enter the user name and password.
Password:
 Info: The max number of VTY users is 5, and the number
       of current VTY users on line is 1.
       The current login time is 2014-05-06 18:33:18+00:00.
<HUAWEI>             //User view prompt
```

Configuring Network Connectivity

a. Configure the access switch.

1 Starting with access switch ACC1 as an example, create service VLANs 10 and 20 on ACC1.

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1          //Set the switch name to ACC1.
[ACC1] vlan batch 10 20        //Create VLANs in a batch.
```

2 Configure GE0/0/3 and GE0/0/4, through which ACC1 connects to CORE1 and CORE2 respectively, to allow the packets from the VLANs of departments A and B to pass through.

```
[ACC1] interface GigabitEthernet 0/0/3
[ACC1-GigabitEthernet0/0/3] port link-type trunk    //Set GE0/0/3 type to
Trunk for VLAN transparent transmission.
[ACC1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20    //Configure
GE0/0/3 to transparently transmit the service VLANs on ACC1.
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface GigabitEthernet 0/0/4
[ACC1-GigabitEthernet0/0/4] port link-type trunk    //Set GE0/0/4 type to
Trunk for VLAN transparent transmission.
[ACC1-GigabitEthernet0/0/4] port trunk allow-pass vlan 10 20    //Configure
GE0/0/4 to transparently transmit the service VLANs on ACC1.
[ACC1-GigabitEthernet0/0/4] quit
```

3 Configure the interfaces on ACC1 that connect user devices so that user devices in different departments can be added to VLANs.

```
[ACC1] interface GigabitEthernet 0/0/1          //Configure the interface
connecting to department A.
[ACC1-GigabitEthernet0/0/1] port link-type access
[ACC1-GigabitEthernet0/0/1] port default vlan 10
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface GigabitEthernet 0/0/2         //Configure the interface
connecting to department B.
[ACC1-GigabitEthernet0/0/2] port link-type access
[ACC1-GigabitEthernet0/0/2] port default vlan 20
[ACC1-GigabitEthernet0/0/2] quit
```

4 Configure the BPDU protection function to improve network stability.

```
[ACC1] stp bpdu-protection
```

NOTE

To add all users connected to ACC1 to VLAN 10, you can add interfaces on CORE1 and CORE2 that directly connect to ACC1 as Access interfaces and do not add interfaces on ACC1 to VLAN 10, simplifying the configuration. This configuration ensures that all users connected to Eth-Trunk1 belong to VLAN 10.

b. Configure the aggregation/core switch (CORE1).

1 Create the VLANs for CORE1 to communicate with the access switches, CORE2, and egress router.

```
<HUAWEI> system-view
[HUAWEI] sysname CORE1                         //Set the switch name to CORE1.
[CORE1] vlan batch 10 20 30 40 50 100 300      //Create VLANs in a batch.
```

2 Configure user-side interfaces and VLANIF interfaces. Communication between departments uses VLANIF interfaces. For example, CORE1 connects to ACC1 through GE0/0/1. The configurations on other interfaces are not mentioned here.

```
[CORE1] interface GigabitEthernet0/0/1
[CORE1-GigabitEthernet0/0/1] port link-type trunk  //Set the interface type to Trunk
for VLAN transparent transmission.
[ CORE1-GigabitEthernet0/0/1]    port trunk allow-pass vlan 10 20 //Configure
GE0/0/1 to transparently transmit service VLANs on ACC1.
[CORE1-GigabitEthernet0/0/1] quit
[CORE1] interface Vlanif 10                    //Configure VLANIF 10 to allow department
A to communicate with department B through Layer 3.
[CORE1-Vlanif10] ip address 192.168.10.1 24
[CORE1-Vlanif10] quit
[CORE1] interface Vlanif 20                    //Configure VLANIF 20 to allow department
B to communicate with department A through Layer 3.
[CORE1-Vlanif20] ip address 192.168.20.1 24
[CORE1-Vlanif20] quit
```

3 Configure interfaces connecting to the egress router and VLANIF interfaces.

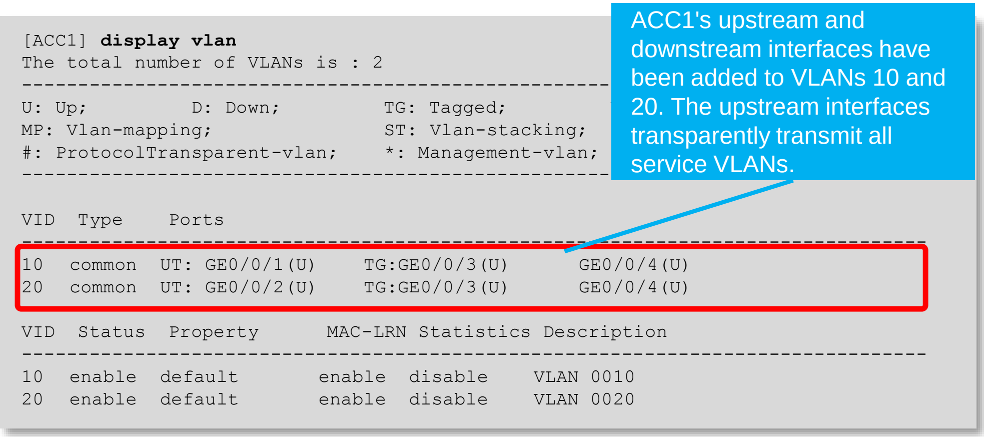
```
[CORE1] interface GigabitEthernet 0/0/7
[CORE1-GigabitEthernet0/0/7] port link-type access            //Set the access mode.
[CORE1-GigabitEthernet0/0/7] port default vlan 100
[CORE1-GigabitEthernet0/0/7] quit
[CORE1] interface Vlanif 100          //Configure a VLANIF interface to allow CORE1
to communicate with the router at Layer 3.
[CORE1-Vlanif100] ip address 172.16.1.1 24
[CORE1-Vlanif100] quit
```

4 Configure interfaces that directly connect to CORE2 and configure a VLANIF interface.

```
[CORE1] interface gigabitethernet 0/0/5
[CORE1-GigabitEthernet0/0/5] port link-type access    //Set the access mode.
[CORE1-GigabitEthernet0/0/5] port default vlan 300
[CORE1-GigabitEthernet0/0/5] quit
[CORE1] interface Vlanif 300
[CORE1-Vlanif300] ip address 172.16.3.1 24
[CORE1-Vlanif300] quit
```

c. View the configuration results.

1 After configuring the interfaces and VLANs, run the following commands to view the configuration results. For details about the command output, see the corresponding Command Reference based on the version of the device.
Run the ***display vlan*** command to view VLAN configurations on ACC1.



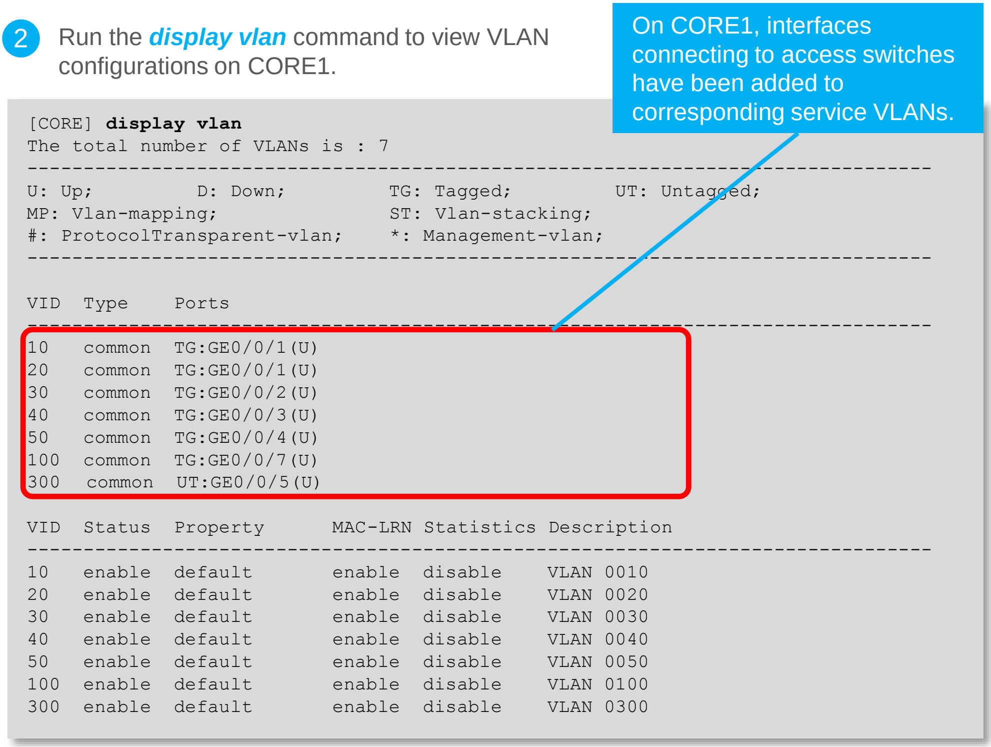
```
[ACC1] display vlan
The total number of VLANs is : 2
----------------------------------------------------
U: Up;          D: Down;          TG: Tagged;
MP: Vlan-mapping;                 ST: Vlan-stacking;
#: ProtocolTransparent-vlan;      *: Management-vlan;
----------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
10   common  UT: GE0/0/1(U)    TG:GE0/0/3(U)      GE0/0/4(U)
20   common  UT: GE0/0/2(U)    TG:GE0/0/3(U)      GE0/0/4(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable  default       enable  disable    VLAN 0010
20   enable  default       enable  disable    VLAN 0020
```

ACC1's upstream and downstream interfaces have been added to VLANs 10 and 20. The upstream interfaces transparently transmit all service VLANs.

2 Run the ***display vlan*** command to view VLAN configurations on CORE1.



```
[CORE] display vlan
The total number of VLANs is : 7
--------------------------------------------------------------------------------
U: Up;          D: Down;          TG: Tagged;          UT: Untagged;
MP: Vlan-mapping;                 ST: Vlan-stacking;
#: ProtocolTransparent-vlan;      *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
10   common  TG:GE0/0/1(U)
20   common  TG:GE0/0/1(U)
30   common  TG:GE0/0/2(U)
40   common  TG:GE0/0/3(U)
50   common  TG:GE0/0/4(U)
100  common  TG:GE0/0/7(U)
300  common  UT:GE0/0/5(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
10   enable  default       enable  disable    VLAN 0010
20   enable  default       enable  disable    VLAN 0020
30   enable  default       enable  disable    VLAN 0030
40   enable  default       enable  disable    VLAN 0040
50   enable  default       enable  disable    VLAN 0050
100  enable  default       enable  disable    VLAN 0100
300  enable  default       enable  disable    VLAN 0300
```

On CORE1, interfaces connecting to access switches have been added to corresponding service VLANs.

d. Configure IP addresses for egress router interfaces.

1 Configure an IP address for the interface connecting to the intranet.

```
<HUAWEI> system-view
[HUAWEI] sysname Router
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] ip address 172.16.1.2 24 //Configure an IP
address for the interface connecting to CORE1.
[Router-GigabitEthernet0/0/1] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] ip address 172.16.2.2 24 //Configure an IP
address for the interface connecting to CORE2.
[Router-GigabitEthernet0/0/2] quit
```

2 Configure an IP address for the interface connecting to the Internet.

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] ip address 1.1.1.2 30 //Configure an IP
address for the interface connecting to the Internet.
[Router-GigabitEthernet0/0/0] quit
```

e. (Optional) Configure a static route.

If a dynamic routing protocol is configured, skip this step.

1 Configure a default static route to the egress router and a backup static route on CORE1 and CORE2, respectively.

```
[CORE1] ip route-static 0.0.0.0 0.0.0.0 172.16.1.2
//Configure a default static route to the egress router on CORE1.
[CORE1] ip route-static 0.0.0.0 0.0.0.0 172.16.3.2 preference 70
//Configure a backup static route to CORE2 on CORE1.
[CORE2] ip route-static 0.0.0.0 0.0.0.0 172.16.2.2
[CORE2] ip route-static 0.0.0.0 0.0.0.0 172.16.3.1 preference 70
```

2 On the egress router, configure a default static route to the carrier device.

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

3 On the egress router, configure primary and backup routes. The next hop of the primary route is CORE1 and that of the backup route is CORE2.

```
[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.1.1
[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.2.1 preference
70  //Configure a backup route to department A with the next hop pointing
to CORE2.
[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.1.1
[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.2.1 preference
70  //Configure a backup route to department B with the next hop pointing
to CORE2.
```

f. Configure VRRP to implement virtual gateway redundancy.

After VRRP is configured on CORE1 and CORE2, the access switches forward traffic to CORE1. If CORE1 fails, a VRRP switchover occurs and CORE2 becomes the master. The access switches then forward traffic to CORE2.

1 Create VRRP groups 1 and 2 on CORE1 and CORE2. Set the priority of CORE1 to 120 and set the preemption delay to 20s so that CORE1 functions as the master in VLANs 10 and 20.

```
[CORE1] interface Vlanif 10
[CORE1-Vlanif10] vrrp vrid 1 virtual-ip 192.168.10.3    //Configure a
virtual IP address for VRRP group 1.
[CORE1-Vlanif10] vrrp vrid 1 priority 120            //Set the priority of
CORE1 to 120.
[CORE1-Vlanif10] vrrp vrid 1 preempt-mode timer delay 20
[CORE1-Vlanif10] quit
[CORE1] interface Vlanif 20
[CORE1-Vlanif20] vrrp vrid 2 virtual-ip 192.168.20.3    //Configure a
virtual IP address for VRRP group 2.
[CORE1-Vlanif20] vrrp vrid 2 priority 120
[CORE1-Vlanif20] vrrp vrid 2 preempt-mode timer delay 20
[CORE1-Vlanif20] quit
```

2 CORE2 uses the default priority and functions as the backup in VLANs 10 and 20.

```
[CORE2] interface Vlanif 10
[CORE2-Vlanif10] vrrp vrid 1 virtual-ip 192.168.10.3
[CORE2-Vlanif10] quit
[CORE2] interface Vlanif 20
[CORE2-Vlanif20] vrrp vrid 2 virtual-ip 192.168.20.3
[CORE2-Vlanif20] quit
```

NOTE

A physical loop exists between CORE1, CORE2, and ACC1, the actual links do not form a loop, and STP is enabled on the switches (Sx7 series) by default. To prevent the loop from affecting the VRRP master and backup status on CORE1 and CORE2, disable STP on upstream interfaces of ACC1. The example below shows the configuration on ACC1.

```
[ACC1] interface GigabitEthernet 0/0/3
[ACC1-GigabitEthernet0/0/3] stp disable     //Disable STP on the upstream
interface GE0/0/3.
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface GigabitEthernet 0/0/4
[ACC1-GigabitEthernet0/0/4] stp disable
[ACC1-GigabitEthernet0/0/4] quit
```

If no loop exists on the network, you can also run the **stp disable** command to disable STP on the access switch.

```
[ACC1] stp disable
Warning: The global STP state will be changed. Continue? [Y/N] y
```

g. Configure the egress router to allow intranet users to access the Internet.

1 Configure an ACL to allow users to access the Internet. The example below allows users in VLANs 10 and 20 to access the Internet.

```
[Router] acl 2000
[Router-acl-basic-2000] rule permit source 192.168.10.0 0.0.0.255
//Allow users in VLAN 10 to access the Internet.
[Router-acl-basic-2000] rule permit source 192.168.20.0 0.0.0.255
//Allow users in VLAN 20 to access the Internet.
[Router-acl-basic-2000] rule permit source 172.16.1.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 172.16.2.0 0.0.0.255
```

2 Configure NAT on the interface connecting to the Internet so that intranet users can access the Internet.

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] nat outbound 2000
[Router-GigabitEthernet0/0/0] quit
```

3 Configure DNS resolution. The carrier provides the DNS server address.

```
[Router] dns resolve
[Router] dns server 8.8.8.8
[Router] dns proxy enable
```

4 After completing the preceding configuration, configure static IP addresses for intranet users in VLAN 10 and set the gateway address to 192.168.10.3. Intranet users then can access the Internet.

a. Configure the DHCP server.

The administrator configures fixed IP addresses for user devices so that users can access the Internet. As the network expands, it is difficult for the administrator to manually configure a large number of IP addresses and manage them. In addition, if a user changes the configured IP address, an IP address conflict occurs and the related users cannot access the Internet. Therefore, the administrator decides to configure fixed IP addresses for several user devices, and configure the other user devices to automatically obtain IP addresses from the DHCP server.

Configure the DHCP server on CORE1 and CORE2 to dynamically allocate IP addresses to user devices in all departments. CORE1 functions as the active DHCP server. Department A is used in the example below.

NOTE

- In this section, a global address pool is configured. You can also configure an interface-based address pool. For details on this process, see the corresponding Configuration Guide - IP Service based on the version of the device.
- To prevent IP address conflicts caused by an active/standby switchover in VRRP networking, configure the active DHCP server to allocate the first half of all IP addresses in the address pool and the standby DHCP server to allocate the second half.

1 Configure CORE1 as the active DHCP server to allocate IP addresses ranging from 192.168.10.1 to 192.168.10.127.

```
<CORE1> system-view
[CORE1] dhcp enable
[CORE1] ip pool 10
[CORE1-ip-pool-10] gateway-list 192.168.10.3          //Configure the
gateway address.
[CORE1-ip-pool-10] network 192.168.10.0 mask 24       //Configure the range
of allocable IP addresses.
[CORE1-ip-pool-10] excluded-ip-address 192.168.10.128 192.168.10.254
// Exclude IP addresses ranging from 192.168.10.128 to 192.168.10.254.
[CORE1-ip-pool-10] lease day 0 hour 20 minute 0    //Configure the IP
address lease.
[CORE1-ip-pool-10] dns-list 8.8.8.8       //Configure the DNS server address.
[CORE1-ip-pool-10] quit
```

2 Configure CORE2 as the standby DHCP server to allocate the second half of all IP addresses in the address pool.

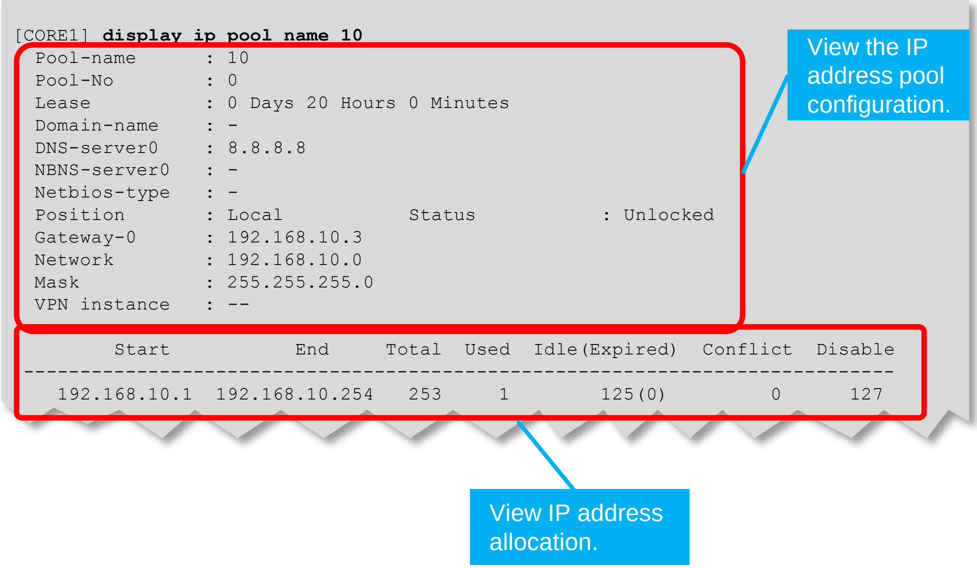
```
<CORE2> system-view
[CORE2] dhcp enable
[CORE2] ip pool 10
[CORE2-ip-pool-10] gateway-list 192.168.10.3
[CORE2-ip-pool-10] network 192.168.10.0 mask 24
[CORE2-ip-pool-10] excluded-ip-address 192.168.10.1 192.168.10.2
[CORE2-ip-pool-10] excluded-ip-address 192.168.10.4 192.168.10.127
[CORE2-ip-pool-10] lease day 0 hour 20 minute 0
[CORE2-ip-pool-10] dns-list 8.8.8.8
[CORE2-ip-pool-10] quit
```

The procedure of configuring dynamic IP address allocation in VLAN 20 is similar to the preceding configuration procedure.

3 Configure users in department A to obtain IP addresses from the global address pool.

```
[CORE1] interface vlanif 10
[CORE1-Vlanif10] dhcp select global      //Configure users in department A
to obtain IP addresses from the global address pool.
[CORE1-Vlanif10] quit
[CORE2] interface vlanif 10
[CORE2-Vlanif10] dhcp select global
[CORE2-Vlanif10] quit
```

4 Run the **display ip pool** command to view the configuration and IP address allocation in the global address pool **10**.



```
[CORE1] display ip pool name 10
  Pool-name      : 10
  Pool-No        : 0
  Lease          : 0 Days 20 Hours 0 Minutes
  Domain-name    : -
  DNS-server0    : 8.8.8.8
  NBNS-server0   : -
  Netbios-type   : -
  Position       : Local           Status           : Unlocked
  Gateway-0      : 192.168.10.3
  Network        : 192.168.10.0
  Mask           : 255.255.255.0
  VPN instance   : --

         Start             End     Total  Used  Idle(Expired)  Conflict  Disable
-------------------------------------------------------------------------------
   192.168.10.1  192.168.10.254    253     1        125(0)          0       127
```

View the IP address pool configuration.

View IP address allocation.

NOTE

After completing the DHCP server configuration, configure network adapters on terminal PCs to automatically obtain IP addresses. The terminal PCs then can obtain IP addresses from the DHCP server and access the Internet.

NOTE

After dynamic IP address allocation is configured, it takes a PC a long time to obtain an IP address after it starts. The reason is that an STP-enabled switch recalculates the spanning tree topology every time a PC connects to the switch. To solve this problem, disable STP or configure the switch interface that connects to user devices as an edge port. ACC1 is used in the example below.

# Disable STP.

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1- GigabitEthernet0/0/1] stp disable  //Alternatively, run the undo
stp enable command.
[ACC1- GigabitEthernet0/0/1] quit
```

# Configure the switch interface that connects to user devices as an edge port.

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1- GigabitEthernet0/0/1] stp edged-port enable
[ACC1- GigabitEthernet0/0/1] quit
```

After either of the preceding operations is performed, terminal PCs can rapidly obtain IP addresses after they start.

b. Configure DHCP snooping and IPSG.

User devices can automatically obtain IP addresses after DHCP is configured. If a user connects a small router to the intranet and enable the DHCP server on the router, authorized intranet users may obtain IP addresses allocated by the small router and cannot access the Internet. To prevent this problem, configure DHCP snooping. Department A is used in the example below.

1 Enable DHCP snooping on ACC1.

```
<ACC1> system-view
[ACC1] dhcp enable  //Enable DHCP.
[ACC1] dhcp snooping enable //Enable DHCP snooping.
```

2 Configure DHCP snooping on interfaces connecting to user devices.

```
[ACC1] interface GigabitEthernet 0/0/1           //Configure the interface
connecting to user devices in department A.
[ACC1-GigabitEthernet0/0/1] dhcp snooping enable
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface GigabitEthernet 0/0/2           //Configure the interface
connecting to user devices in department B.
[ACC1-GigabitEthernet0/0/2] dhcp snooping enable
[ACC1-GigabitEthernet0/0/2] quit
```

3 Enable DHCP snooping on interfaces connecting to DHCP servers and configure the interfaces as trusted interfaces.

```
[ACC1] interface GigabitEthernet 0/0/3     //Configure the interface connecting to
CORE1.
[ACC1-GigabitEthernet0/0/3] dhcp snooping enable    //Enable DHCP snooping.
[ACC1-GigabitEthernet0/0/3] dhcp snooping trusted   //Configure the interface as a
trusted interface.
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface GigabitEthernet 0/0/4      //Configure the interface connecting
to CORE2.
[ACC1-GigabitEthernet0/0/4] dhcp snooping enable
[ACC1-GigabitEthernet0/0/4] dhcp snooping trusted
[ACC1-GigabitEthernet0/0/4] quit
```

After the preceding configuration is complete, user devices in department A can obtain IP addresses from only the authorized DHCP server, and will not use IP addresses allocated by the small router.

To prevent users from changing IP addresses and attacking the intranet, enable IPSG after enabling DHCP snooping on the access switch. ACC1 is used in the example below.

4 On ACC1, enable IPSG in VLAN 10.

```
[ACC1] vlan 10
[ACC1-vlan10] ip source check user-bind enable //Enable IPSG.
[ACC1-vlan10] quit
```

ACC1 matches packets received from VLAN 10 with dynamic binding entries in the DHCP snooping binding table. If a packet matches an entry, ACC1 forwards the packet; otherwise, ACC1 discards the packet. To check packets received from a specified user device instead of all user devices in the VLAN, enable IPSG on the interface connecting to the device.

NOTE

If static IP address allocation is configured, bind IP addresses and MAC addresses to prevent users from changing IP addresses and attacking the network. For this configuration procedure, see "Example for Configuring IPSG to Prevent Hosts with Static IP Addresses from Changing Their Own IP Addresses" in the Typical Configuration Examples.

For details about how to configure the switch to prevent users from connecting a small router (bogus DHCP server) to the intranet and changing IP addresses, see "Configuring Basic Functions of DHCP Snooping", "Configuring IPSG", and configuration examples in the corresponding Configuration Guide – Security based on the version of the device.

Configuring OSPF

NOTE

Devices on the intranet use static routes. If a link fails, the administrator needs to manually configure a new static route, interrupting network services for a long time. Configuring a dynamic routing protocol prevents this problem. If a link fails, the dynamic routing protocol switches traffic forwarded through the faulty link to a normal link based on an algorithm. After the faulty link recovers, the routing protocol switches traffic back to the link. OSPF configuration is used in the example below.

1 Delete all static routes on CORE1 and CORE2.

```
[CORE1] undo ip route-static all
[CORE2] undo ip route-static all
```

2 On the egress router, delete the static route to the intranet and retain the static route to the Internet.

```
[Router] undo ip route-static 192.168.10.0 24
[Router] undo ip route-static 192.168.20.0 24
```

3 Configure OSPF on CORE1.

```
[CORE1] ospf 100 router-id 2.2.2.2
[CORE1-ospf-100] area 0
[CORE1-ospf-100-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[CORE1-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255
[CORE1-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[CORE1-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[CORE1-ospf-100-area-0.0.0.0] quit
[CORE1-ospf-100] quit
```

4 Configure OSPF on CORE2.

```
[CORE2] ospf 100 router-id 3.3.3.3
[CORE2-ospf-100] area 0
[CORE2-ospf-100-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[CORE2-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255
[CORE2-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[CORE2-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[CORE2-ospf-100-area-0.0.0.0] quit
[CORE2-ospf-100] quit
```

5 Configure OSPF on the egress router. To connect the intranet to the Internet, configure a default static route to the Internet. Advertise the default route in the OSPF area, and configure a default static route to the carrier device.

```
[Router] ospf 10 router-id 1.1.1.1
[Router-ospf-10] default-route-advertise always
[Router-ospf-10] area 0
[Router-ospf-10-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[Router-ospf-10-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[Router-ospf-10-area-0.0.0.0] quit
[Router-ospf-10] quit
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

For details on OSPF configuration and commands, see "OSPF Configuration" and configuration examples in the corresponding Configuration Guide - IP Unicast Routing based on the version of the device.

a. Configure association between VRRP and the interface status to monitor links.

NOTE

If the link from CORE1 to the egress router fails, traffic is forwarded over the interconnection link between CORE1 and CORE2 to CORE2, increasing traffic load and imposing high stability and bandwidth requirements on the link. You can configure association between VRRP and the interface status to implement fast active/standby switchover upon an uplink or downlink failure. If you configure this function on the upstream interface of the master in the VRRP group, the master lowers its priority to implement an active/standby switchover when it detects that the upstream interface goes Down.

# Configure association between VRRP and the status of the upstream interface on CORE1 to monitor the uplink.

```
[CORE1] interface Vlanif 10
[CORE1-Vlanif10] vrrp vrid 1 track interface GigabitEthernet0/0/7 reduced
100                              //Configure association between VRRP and the
upstream interface status.
[CORE1-Vlanif10] quit
[CORE1] interface Vlanif 20
[CORE1-Vlanif20] vrrp vrid 2 track interface GigabitEthernet0/0/7 reduced
100
[CORE1-Vlanif20] quit
```

b. Configure load balancing.

NOTE

As service traffic increases, the link between CORE1 and the egress router has high bandwidth utilization, whereas the link between CORE2 and the egress router is idle, wasting resources and lowering reliability. To effectively use the two links, you can configure load balancing on CORE1 and CORE2 so that CORE1 function as the master in some VLANs while CORE2 function as the master in the other VLANs. The two links then load balance traffic from all VLANs, effectively using network resources. Configure CORE1 to still function as the master in VLAN 10, and change the priority of CORE2 so that CORE2 functions as the master in VLAN 20.

1 Delete the VRRP priority and preemption delay configuration on VLANIF 20 of CORE1.

```
[CORE1] interface Vlanif 20
[CORE1-Vlanif20] undo vrrp vrid 2 preempt-mode timer delay
[CORE1-Vlanif20] undo vrrp vrid 2 priority
[CORE1-Vlanif20] quit
```

2 Configure CORE2 as the master in VLAN 20 and set the preemption delay to 20s.

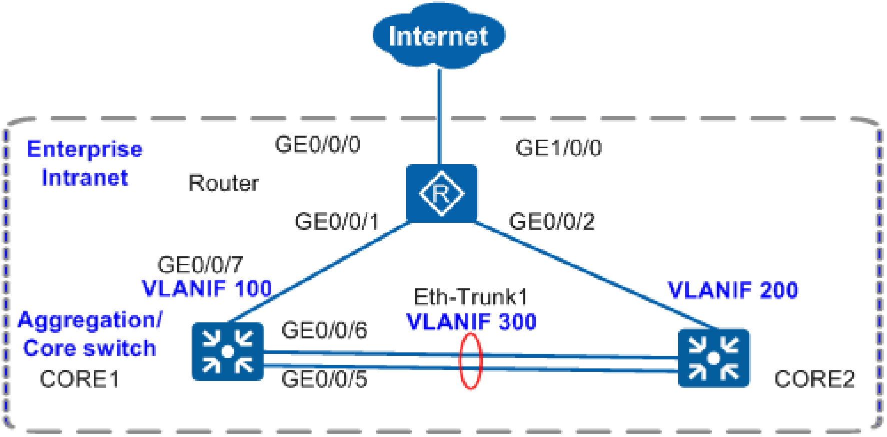
```
[CORE2] interface Vlanif 20
[CORE2-Vlanif20] vrrp vrid 2 priority 120
[CORE2-Vlanif20] vrrp vrid 2 preempt-mode timer delay 20
```

3 Configure association between VRRP and the status of the upstream interface on CORE2 to monitor the uplink.

```
[CORE2-Vlanif20] vrrp vrid 2 track interface GigabitEthernet0/0/7 reduced
100
[CORE2-Vlanif20] quit
```

Configuring Link Aggregation

If the uplink of CORE1 or CORE2 fails, traffic passes through the link between CORE1 and CORE2. However, the bandwidth of the link may be insufficient, causing packet loss. You can bind multiple physical links into a logical link to increase the bandwidth and improve the link reliability. CORE1 is used in the example below.



1 Restore the default configuration on an interface. Skip this step if the interface uses the default configuration. The example below shows the procedure of restoring the default configuration on an interface.

```
[CORE1] interface GigabitEthernet 0/0/5
[CORE1-GigabitEthernet0/0/5] dis this
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 300
#
return
[CORE1-GigabitEthernet0/0/5] undo port default vlan
[CORE1-GigabitEthernet0/0/5] undo port link-type
```

2 In V200R005 and later versions, you can run the **clear configuration this** command to restore the default configuration on an interface. The interface will be shut down after the default configuration is restored. Run the **undo shutdown** command to enable the interface.

```
[CORE1-GigabitEthernet0/0/5] clear configuration this
Warning: All configurations of the interface will be cleared, and its state
will be shutdown. Continue? [Y/N] :y
Info: Total 2 command(s) executed, 2 successful, 0 failed.
[CORE1-GigabitEthernet0/0/5] undo shutdown
[CORE1-GigabitEthernet0/0/5] quit
```

1 Configure link aggregation.

Method 1: Configure link aggregation in load balancing mode.

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] trunkport GigabitEthernet 0/0/5 to 0/0/6
[CORE1-Eth-Trunk1] port link-type access
[CORE1-Eth-Trunk1] port default vlan 300
[CORE1-Eth-Trunk1] quit
```

Method 2: Configure link aggregation in LACP mode.

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] mode lacp
[CORE1-Eth-Trunk1] trunkport GigabitEthernet 0/0/5 to 0/0/6
[CORE1-Eth-Trunk1] port link-type access
[CORE1-Eth-Trunk1] port default vlan 300
[CORE1-Eth-Trunk1] quit
```

# Set the system priority of CORE1 to 100 so that CORE1 becomes the Actor.

```
[CORE1] lacp priority 100
```

# On CORE1, set the maximum number of active interfaces to 2.

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] max active-linknumber 2
[CORE1-Eth-Trunk1] quit
```

# On CORE1, set interface priorities to determine active links. (Configure GE0/0/5 and GE0/0/6 as active interfaces.)

```
[CORE1] interface GigabitEthernet 0/0/5
[CORE1-GigabitEthernet0/0/5] lacp priority 100
[CORE1-GigabitEthernet0/0/5] quit
[CORE1] interface GigabitEthernet 0/0/6
[CORE1-GigabitEthernet0/0/6] lacp priority 100
[CORE1-GigabitEthernet0/0/6] quit
```

The configuration of CORE2 is similar to that of CORE1. The difference is that CORE2 uses the default system priority.

For details on link aggregation configuration and commands, see "Link Aggregation Configuration" and configuration examples in the corresponding Configuration Guide - Ethernet Switching based on the version of the device.

Configuring Rate Limiting

a. Configure rate limiting based on the IP address.

Configuring IP address-based rate limiting on the switch is complicated and consumes a lot of hardware ACL resources. Therefore, You can configure IP address-based rate limiting on the egress router's physical interfaces connecting to the core switches.
Because bandwidth resources are limited and service traffic transmission must be ensured, the upload and download rate of each intranet IP address cannot exceed 512 kbit/s.

1 On GE0/0/1, configure IP address-based rate limiting for network segments 192.168.10.0 and 192.168.20.0 and limit the rate to 512 kbit/s. Note that IP address-based rate limiting is configured on LAN-side interfaces because NAT-enabled WAN-side interfaces cannot identify intranet IP addresses. When configuring IP address-based rate limiting on LAN-side interfaces, specify the source IP address in the inbound direction to limit the upload rate, and specify the destination IP address in the outbound direction to limit the download rate.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] qos car inbound source-ip-address range
192.168.10.1 to 192.168.10.254 per-address cir 512
[Router-GigabitEthernet0/0/1] qos car outbound destination-ip-address range
192.168.10.1 to 192.168.10.254 per-address cir 512
[Router-GigabitEthernet0/0/1] qos car inbound source-ip-address range
192.168.20.1 to 192.168.20.254 per-address cir 512
[Router-GigabitEthernet0/0/1] qos car outbound destination-ip-address range
192.168.20.1 to 192.168.20.254 per-address cir 512
[Router-GigabitEthernet0/0/1] quit
```

The procedure of configuring IP address-based rate limiting for other network segments on GE0/0/2 is similar to the preceding procedure.

b. Configure rate limiting based on all traffic on a network segment.

To reserve sufficient bandwidth resources for department A as services grow, configure rate limiting for department B. The Internet access rate in department B cannot exceed 2 Mbit/s and the download rate cannot exceed 4 Mbit/s.

1 Configure an ACL on the egress router to allow packets from department B to pass through.

```
[Router] acl 2222
[Router-acl-basic-2222] rule permit source 192.168.20.0 0.0.0.255
[Router-acl-basic-2222] quit
```

2 Configure rate limiting on LAN-side interfaces of the egress router to limit the Internet access rate and download rate.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] qos car inbound acl 2222 cir 2048
[Router-GigabitEthernet0/0/1] qos car outbound acl 2222 cir 4096
[Router-GigabitEthernet0/0/1] quit
```

The configuration procedure on GE0/0/2 is similar to that on GE0/0/1.

For details on rate limiting configuration and commands, see "Traffic Policing and Traffic Shaping Configurations" and configuration examples in the corresponding Configuration Guide – QoS based on the version of the device.

Configuring NAT Server and Multiple Egress Interfaces

a. Configure NAT Server.

As services grow, the web server and FTP server on the intranet need to provide services to both internal and external users who access the servers using public IP addresses.

1 Configure the egress router to allow external users to access intranet servers using public IP addresses.

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] nat server protocol tcp global current-
interface www inside 192.168.50.20 www
Warning:The port 80 is well-known port. If you continue it may cause
function failure.
Are you sure to continue?[Y/N]:y
[Router-GigabitEthernet0/0/0] nat server protocol tcp global current-
interface ftp inside 192.168.50.10 ftp
[Router-GigabitEthernet0/0/0] quit
```

2 Enable NAT ALG for FTP on the egress router.

```
[Router] nat alg ftp enable
```

3 Configure an ACL to allow intranet users to access intranet servers using public IP addresses.

```
[Router] acl 3333
[Router-acl-adv-3333] rule permit ip source 192.168.10.0 0.0.0.255
destination 202.101.111.2 0.0.0.0
[Router-acl-adv-3333] rule permit ip source 192.168.20.0 0.0.0.255
destination 202.101.111.2 0.0.0.0
[Router-acl-adv-3333] quit
```

4 Configure NAT on egress router interfaces connecting to the intranet.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3333
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3333
[Router-GigabitEthernet0/0/2] quit
```

5 Configure a mapping table of internal servers on egress router interfaces connecting to the intranet.

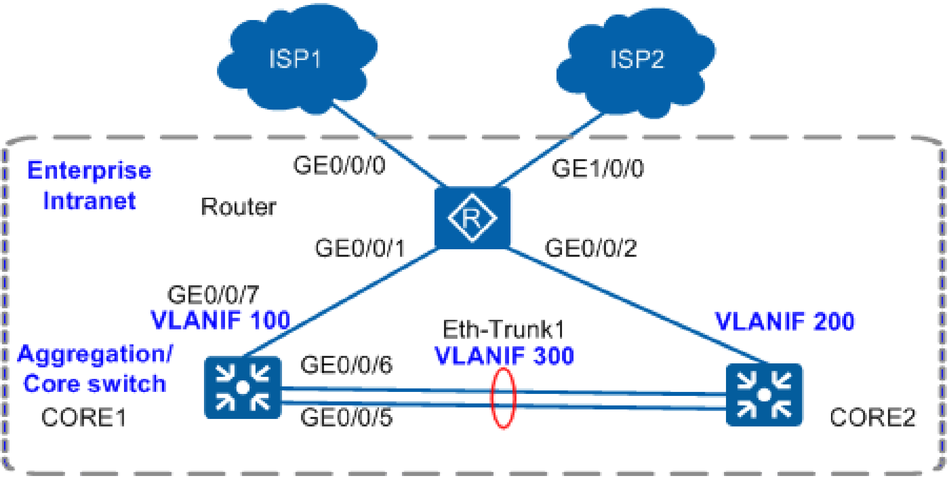
```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat server protocol tcp global interface
GigabitEthernet 0/0/0 www inside 192.168.50.20 www
[Router-GigabitEthernet0/0/1] nat server protocol tcp global interface
GigabitEthernet 0/0/0 ftp inside 192.168.50.10 ftp
[Router-GigabitEthernet0/0/1] quit
```

The configuration procedure on GE0/0/2 is similar to that on GE0/0/1.

For details on NAT configuration and commands for AR routers, see "NAT Configuration" and configuration examples in the corresponding Configuration Guide - IP Service, as well as "NAT" in Typical Configuration Examples based on the version of the device.

b. Configure multiple egress interfaces to the Internet.

The enterprise applied for only one link from the carrier. As services grow, the link cannot provide sufficient bandwidth for the enterprise. The enterprise applies for another link. The original single egress interface changes to two egress interfaces. Configure the router to forward traffic from different network segments on the intranet to the Internet through specified links.



Configure GE1/0/0 to provide Internet access using PPPoE dial-up.

Configure policy-based routing (PBR) to allow users on different network segments to access the Internet through different carriers.

1 Configure an ACL for NAT.

```
[Router] acl 2015
[Router-acl-basic-2015] rule permit source 192.168.10.0 0.0.0.255
[Router-acl-basic-2015] rule permit source 192.168.20.0 0.0.0.255
[Router-acl-basic-2015] quit
```

2 Configure a dialer ACL.

```
[Router] dialer-rule
[Router-dialer-rule] dialer-rule 1 ip permit
[Router-dialer-rule] quit
```

3. Configure a dialer interface.

```
[Router] interface Dialer 0
[Router-Dialer0] ip address ppp-negotiate
[Router-Dialer0] ppp chap user Router
[Router-Dialer0] ppp chap password cipher Router@123
[Router-Dialer0] dialer user user
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] dialer-group 1
[Router-Dialer0] ppp ipcp dns request
[Router-Dialer0] ppp ipcp dns admit-any
[Router-Dialer0] quit
```

4. Configure NAT.

```
[Router] interface Dialer 0
[Router-Dialer0] nat outbound 2015
[Router-Dialer0] quit
```

5. Set the maximum segment size (MSS) of TCP packets to 1200 bytes. If the default value (1460 bytes) is used, the Internet access rate may be slow.

```
[Router] interface Dialer 0
[Router-Dialer0] tcp adjust-mss 1200
[Router-Dialer0] quit
```

6. Enable PPPoE on the physical interface GE1/0/0 connecting to the carrier device.

```
[Router] interface GigabitEthernet 1/0/0
[Router-GigabitEthernet 1/0/0] pppoe-client dial-bundle-number 1
[Router-GigabitEthernet 1/0/0] quit
```

7. Configure a default static route to the Internet with Dialer 0 as the outbound interface.

```
[Router] ip route-static 0.0.0.0 0 Dialer 0
```

8. Configure an ACL to match data flows. Traffic exchanged between internal users is not redirected.

```
[Router] acl 3000
[Router-acl-adv-3000] rule permit ip source 192.168.10.0 0.0.0.255
destination 192.168.20.0 0.0.0.255
[Router-acl-adv-3000] rule permit ip source 192.168.20.0 0.0.0.255
destination 192.168.10.0 0.0.0.255
[Router-acl-adv-3000] quit
[Router] acl 3001
[Router-acl-adv-3001] rule permit ip source 192.168.10.0 0.0.0.255
[Router-acl-adv-3001] quit
[Router] acl 3002
[Router-acl-adv-3002] rule permit ip source 192.168.20.0 0.0.0.255
[Router-acl-adv-3002] quit
```

9 Configure traffic classifiers **c0**, **c1**, and **c2**, and configure matching rules based on ACL 3000, ACL 3001, and ACL 3002 in the traffic classifiers, respectively.

```
[Router] traffic classifier c0
[Router-classifier-c0] if-match acl 3000
[Router-classifier-c0] quit
[Router] traffic classifier c1
[Router-classifier-c1] if-match acl 3001
[Router-classifier-c1] quit
[Router] traffic classifier c2
[Router-classifier-c2] if-match acl 3002
[Router-classifier-c2] quit
```

10 Configure traffic behavior to not redirect traffic exchanged between internal users, to redirect traffic from the internal network segment 192.168.10.0 to the next hop address 1.1.1.1, and to redirect traffic from the internal network segment 192.168.20.0 to the outbound interface Dialer 0.

```
[Router] traffic behavior b0
[Router-behavior-b0] permit
[Router-behavior-b0] quit
[Router] traffic behavior b1
[Router-behavior-b1] redirect ip-nexthop 1.1.1.1
[Router-behavior-b1] quit
[Router] traffic behavior b2
[Router-behavior-b2] redirect interface Dialer 0
[Router-behavior-b2] quit
```

11 Configure a traffic policy and bind traffic classifiers to traffic behavior in the traffic policy.

```
[Router] traffic policy test
[Router-trafficpolicy-test] classifier c0 behavior b0
[Router-trafficpolicy-test] classifier c1 behavior b1
[Router-trafficpolicy-test] classifier c2 behavior b2
[Router-trafficpolicy-test] quit
```

12 Apply the traffic policy to egress router interfaces connecting to the core switches.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-policy test inbound
[Router-GigabitEthernet0/0/1] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-policy test inbound
[Router-GigabitEthernet0/0/2] quit
```

After PBR is configured, intranet users on the network segment 192.168.10.0 access the Internet through GE0/0/0, and intranet users on the network segment 192.168.20.0 access the Internet through GE1/0/0 using PPPoE dial-up.
For details on PBR configuration and commands, see "PBR Configuration" and configuration examples in the corresponding Configuration Guide - IP Unicast Routing based on the version of the device.

Verifying Services and Saving the Configuration

a. Verify services.

1 Select two PCs from two departments to perform ping tests and verify whether the two departments can communicate at Layer 3 through VLANIF interfaces.

The following example uses two PCs (PC1 and PC2) in departments A and B. The two PCs communicate at Layer 3 through CORE1 (or CORE2). If they can ping each other successfully, Layer 3 interworking is normal.

```
<PC1> ping  192.168.20.254                        // Assume that PC2
automatically obtains an IP address 192.168.20.254 through DHCP.
 PING 192.168.20.254 data bytes, press CTRL_C to break
    Reply from 192.168.20.254  : bytes=56 Sequence=1 ttl=253 time=62 ms
    Reply from 192.168.20.254 : bytes=56 Sequence=2 ttl=253 time=16 ms
    Reply from 192.168.20.254 : bytes=56 Sequence=3 ttl=253 time=62 ms
    Reply from 192.168.20.254 : bytes=56 Sequence=4 ttl=253 time=94 ms
    Reply from 192.168.20.254 : bytes=56 Sequence=5 ttl=253 time=63 ms
--- 192.168.20.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

PC1 can ping PC2 successfully, indicating that Layer 3 interworking between PC1 and PC2 is normal.

2 Select two PCs within a department to perform ping tests and verify whether Layer 2 interworking within the department is normal.

Users in department A communicate at Layer 2 through ACC1. If the two PCs can ping each other successfully, users in department A can normally communicate at Layer 2. The ping command is similar to that in step 1.

3 Select two PCs from two departments to ping a public IP address and verify whether intranet users of the company can access the Internet normally.

The following example uses department A. Generally, you can ping a public network gateway address from PC1 to verify whether PC1 can access the Internet. The public network gateway address is the IP address of the carrier device to which the egress router connects. If the ping test succeeds, intranet users can access the Internet normally. The ping command is similar to that in step 1.

b. Save the configuration.

You must save your data to the configuration file before restarting the switch. Unsaved data configured via command lines will be lost after the switch restarts.
The example below shows the procedure of saving CORE1's configuration file.

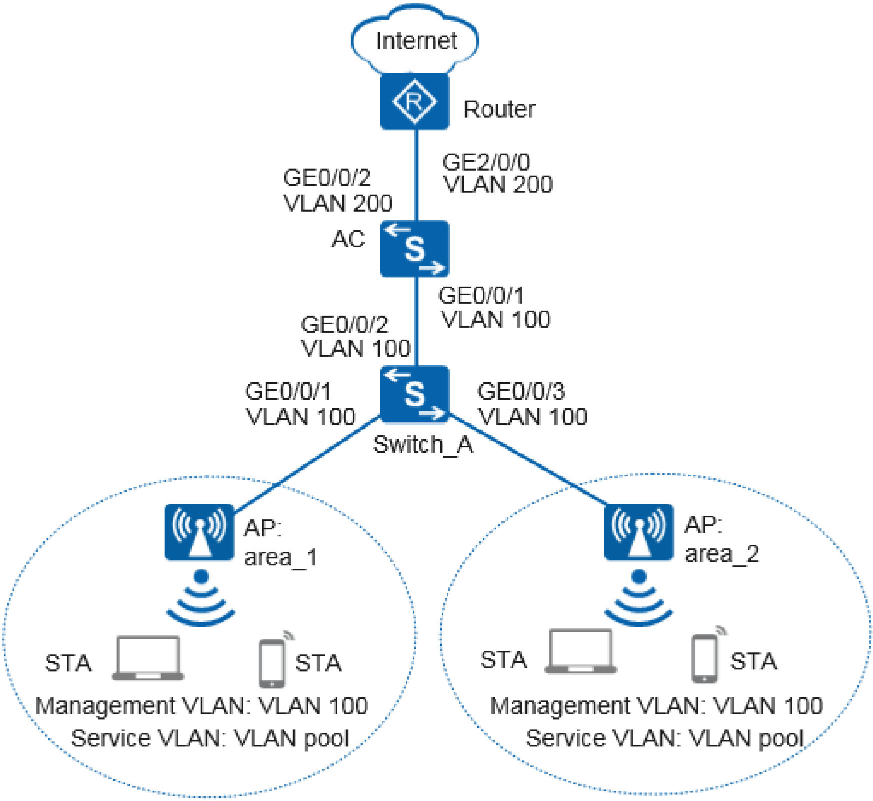
```
<CORE1> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0..
Save the configuration successfully.
```

4 Mid-sized Campus WLANs

NOTE

This section uses an S series switch running V200R012 and an AR series router running V200R010 as examples to demonstrate how to configure a medium-sized campus WLAN.

.



- A WLAN with SSID **wlan-net** is required so that users can access the Internet from anywhere at any time.
- The S5720LI that supports the PoE function can be deployed at the access layer and connects to APs to provide wireless network access for STAs.
- The S5720HI can be deployed as an AC at the aggregation layer to control and manage STAs. The AC functions as a DHCP server to assign IP addresses to APs.
- An AR series router can be deployed as the egress of the campus network. The router functions as a DHCP server to assign IP addresses to STAs.
- VLANs in a VLAN pool can be configured as service VLANs. IP addresses are assigned to STAs from the interface address pools corresponding to the VLANs in the VLAN pool.

4.1 Data Plan

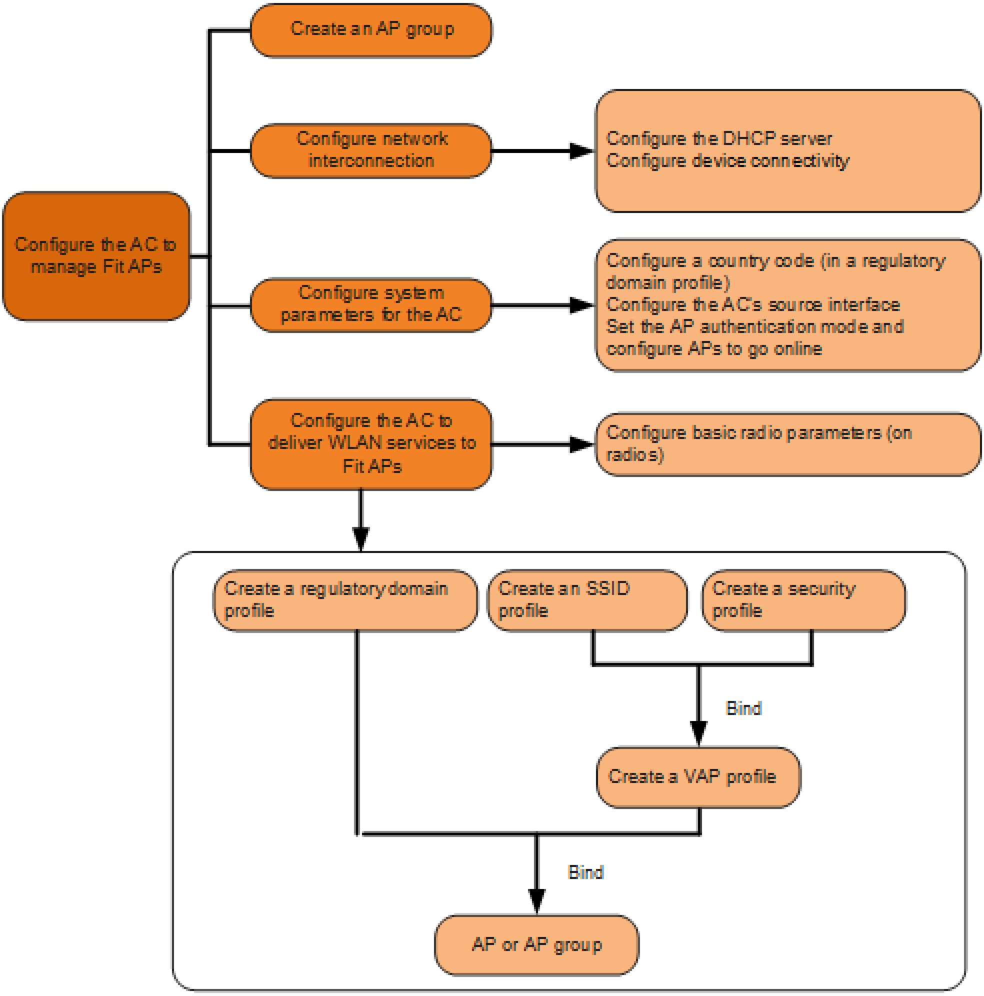
Before configuring the switches and router, prepare the following data for use in the next section.

Configuration Item	Data
DHCP server	● The AC functions as a DHCP server to assign IP addresses to APs. ● Router functions as a DHCP server to assign IP addresses to APs.
IP address pool for APs	10.23.100.2 to 10.23.100.254/24
IP address pool for STAs	● 10.23.101.2 to 10.23.101.254/24 ● 10.23.102.2 to 10.23.102.254/24
VLAN pool	● Name: sta-pool ● VLANs in the VLAN pool: VLAN 101 and VLAN 102
Source interface IP address of the AC	VLANIF 100: 10.23.100.1/24
AP group	● Name: ap-group1 ● Referenced profiles: VAP profile **wlan-vap** and regulatory domain profile **domain1**
Regulatory domain profile	● Name: domain1 ● Country code: CN
SSID profile	● Name: wlan-ssid ● SSID name: wlan-net
Security profile	● Name: wlan-security ● Security policy: WPA2+PSK+AES ● Password: a1234567
VAP profile	● Name: wlan-vap ● Forwarding mode: tunnel forwarding ● Service VLAN: VLAN pool ● Referenced profiles: SSID profile **wlan-ssid** and security profile **wlan-security**

4.2 Configuration Roadmap

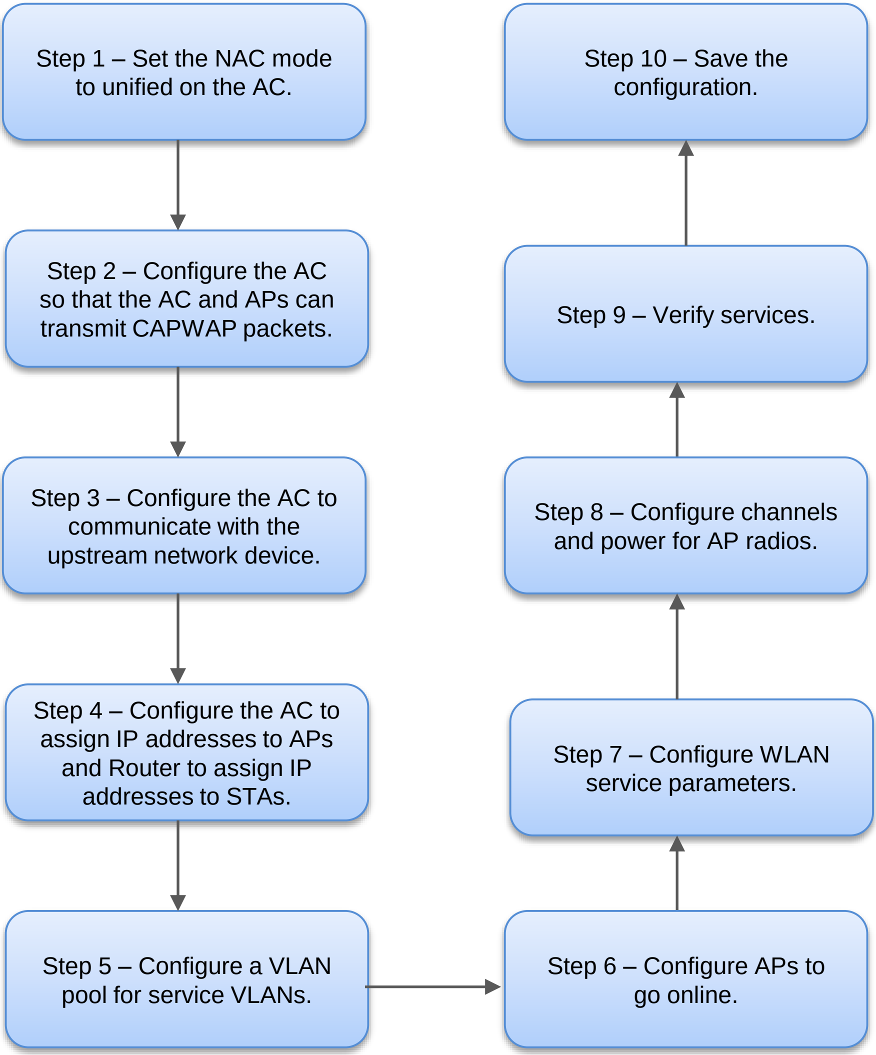
NOTE

Various profiles are designed based on different functions and features of WLANs to help users configure and maintain functions of WLANs. These profiles are called WLAN profiles. The following figure shows the referencing relationships between WLAN profiles. By getting to know the referencing relationships, you can easily grasp the configuration roadmap of WLAN profiles and complete configurations.


Create an AP group
Configure network interconnection
Configure the DHCP server
Configure device connectivity
Configure the AC to manage Fit APs
Configure a country code (in a regulatory domain profile)
Configure the AC's source interface
Set the AP authentication mode and configure APs to go online
Configure system parameters for the AC
Configure the AC to deliver WLAN services to Fit APs
Configure basic radio parameters (on radios)
Create a regulatory domain profile
Create an SSID profile
Create a security profile
Bind
Create a VAP profile
Bind
AP or AP group

4.3 Quickly Configuring Mid-sized Campus WLANs

Follow the procedure shown below to configure network devices to build a wireless network for the campus and enable users to access the Internet from anywhere at any time.



Step 1 – Set the NAC mode to unified on the AC.

Step 2 – Configure the AC so that the AC and APs can transmit CAPWAP packets.

Step 3 – Configure the AC to communicate with the upstream network device.

Step 4 – Configure the AC to assign IP addresses to APs and Router to assign IP addresses to STAs.

Step 5 – Configure a VLAN pool for service VLANs.

Step 6 – Configure APs to go online.

Step 7 – Configure WLAN service parameters.

Step 8 – Configure channels and power for AP radios.

Step 9 – Verify services.

Step 10 – Save the configuration.

Setting the NAC Mode to Unified on the AC

NOTE

The S5720HI supports both the NAC unified mode and common mode. Compared with the NAC common mode, the NAC unified mode can be configured based on templates, making the configuration clearer and configuration model easier to understand. Based on the preceding advantages, you are advised to set the NAC mode to unified.

1 Check the NAC mode before and after the AC restarts.

```
<HUAWEI> display authentication mode
  Current authentication mode is common-mode
  Next authentication mode is unified-mode
```

The NAC mode is as follows before and after the AC restarts.

- unified-mode: unified mode
- common-mode: common mode

2 If the current NAC mode is common, switch the NAC mode to unified to ensure that users can access the Internet.

```
<HUAWEI> system-view
[HUAWEI] authentication unified-mode
```

NOTE

In versions earlier than V200R007C00, after the NAC mode is switched, you need to manually save the configuration file and restart the AC to make the new NAC mode take effect. In V200R007C00 and later versions, after the NAC mode is switched, the AC automatically saves the configuration file and restarts.

Configuring the AC So That the AC and APs Can Transmit CAPWAP Packets

1 Add GE0/0/1, GE0/0/2, and GE0/0/3 on Switch_A to VLAN 100 (management VLAN).

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_A
[Switch_A] vlan batch 100
[Switch_A] interface gigabitethernet 0/0/1
[Switch_A-GigabitEthernet0/0/1] port link-type trunk
[Switch_A-GigabitEthernet0/0/1] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/1] port-isolate enable
[Switch_A-GigabitEthernet0/0/1] quit
[Switch_A] interface gigabitethernet 0/0/2
[Switch_A-GigabitEthernet0/0/2] port link-type trunk
[Switch_A-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/2] quit
[Switch_A] interface gigabitethernet 0/0/3
[Switch_A-GigabitEthernet0/0/3] port link-type trunk
[Switch_A-GigabitEthernet0/0/3] port trunk pvid vlan 100
[Switch_A-GigabitEthernet0/0/3] port trunk allow-pass vlan 100
[Switch_A-GigabitEthernet0/0/3] port-isolate enable
[Switch_A-GigabitEthernet0/0/3] quit
```

2 Add GE0/0/1 connecting the AC to Switch_A to VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] sysname AC
[AC] vlan batch 100
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[AC-GigabitEthernet0/0/1] quit
```

NOTE

In tunnel forwarding mode, APs encapsulate data packets over CAPWAP data tunnels and send them to the AC, which then forwards these packets to the upper-layer network. In tunnel forwarding mode, the management VLAN and service VLAN cannot be the same. The network between the AC and APs can permit packets only with management VLAN tags to pass through, and does not permit packets with service VLAN tags to pass through.

Configuring the AC to Communicate with the Upstream Network Device

1 Configure VLAN 101 (service VLAN), VLAN 102 (service VLAN), and VLANIF 200.

NOTE

Configure uplink interfaces of the AC to transparently transmit packets of service VLANs as required and communicate with the upstream network device.

```
[AC] vlan batch 101 102 200
[AC] interface vlanif 101
[AC-Vlanif101] ip address 10.23.101.1 24
[AC-Vlanif101] quit
[AC] interface vlanif 102
[AC-Vlanif102] ip address 10.23.102.1 24
[AC-Vlanif102] quit
[AC] interface vlanif 200
[AC-Vlanif200] ip address 10.23.200.2 24
[AC-Vlanif200] quit
```

2 Configure the default route on the AC.

```
[AC] ip route-static 0.0.0.0 0.0.0.0 10.23.200.1
```

3 Add GE0/0/2 connecting the AC to Router to VLAN 200.

```
[AC] interface gigabitethernet 0/0/2
[AC-GigabitEthernet0/0/2] port link-type trunk
[AC-GigabitEthernet0/0/2] port trunk allow-pass vlan 200
[AC-GigabitEthernet0/0/2] quit
```

Configuring the AC to Assign IP Addresses to APs and Router to Assign IP Addresses to STAs

Configure the AC as a DHCP server to assign IP addresses to APs from an interface IP address pool, the AC as a DHCP relay agent, and Router connected to the AC to assign IP addresses to STAs.

1 Configure the AC to assign IP addresses to APs from an interface address pool.

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 10.23.100.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
```

2 Configure the AC as a DHCP relay agent.

```
[AC] interface vlanif 101
[AC-Vlanif101] dhcp select relay
[AC-Vlanif101] dhcp relay server-ip 10.23.200.1
[AC-Vlanif101] quit
[AC] interface vlanif 102
[AC-Vlanif102] dhcp select relay
[AC-Vlanif102] dhcp relay server-ip 10.23.200.1
[AC-Vlanif102] quit
```

3 Configure Router as a DHCP server to assign IP addresses to STAs.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] ip pool sta-ip-pool1
[Router-ip-pool-sta-ip-pool1] gateway-list 10.23.101.1
[Router-ip-pool-sta-ip-pool1] network 10.23.101.0 mask 24
[Router-ip-pool-sta-ip-pool1] quit
[Router] ip pool sta-ip-pool2
[Router-ip-pool-sta-ip-pool2] gateway-list 10.23.102.1
[Router-ip-pool-sta-ip-pool2] network 10.23.102.0 mask 24
[Router-ip-pool-sta-ip-pool2] quit
[Router] vlan batch 200
[Router] interface vlanif 200
[Router-Vlanif200] ip address 10.23.200.1 24
[Router-Vlanif200] dhcp select global
[Router-Vlanif200] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] port link-type trunk
[Router-GigabitEthernet2/0/0] port trunk allow-pass vlan 200
[Router-GigabitEthernet2/0/0] quit
[Router] ip route-static 10.23.101.0 24 10.23.200.2
[Router] ip route-static 10.23.102.0 24 10.23.200.2
```

NOTE

Configure an IP address for the DNS server as needed using either of the following methods:

- In the interface address pool scenario, run the **dhcp server dns-list ip-address &<1-8>** command in the VLANIF interface view.
- In the global address pool scenario, run the **dns-list ip-address &<1-8>** command in the IP address pool view.

Configuring a VLAN Pool for Service VLANs

WLANs allow STAs to access in flexible modes at different locations. STAs may connect to the same WLAN in a location (such as the entrance of an office or a stadium), and roam to a wireless network covered by other APs.

If each SSID has only one service VLAN to deliver wireless access to STAs, IP address resources may become insufficient in areas with a large number of STAs, and IP addresses in other areas are wasted. You can configure VLANs in a VLAN pool as service VLAN of STAs so that one SSID can use multiple service VLANs to provide wireless access services.

New STAs are dynamically assigned to VLANs in the VLAN pool, which reduces the number of STAs in each VLAN and also the size of the broadcast domain. Additionally, IP addresses are evenly allocated, preventing IP address waste.

1 Create a VLAN pool, add VLAN 101 and VLAN 102 to the pool, and set the VLAN assignment algorithm to hash in the VLAN pool.

```
[AC] vlan pool sta-pool
[AC-vlan-pool-sta-pool] vlan 101 102
[AC-vlan-pool-sta-pool] assignment hash
[AC-vlan-pool-sta-pool] quit
```

NOTE

In this example, the VLAN assignment algorithm is set to hash (default value). If the default setting is retained, you do not need to run the **assignment hash** command.

Only VLAN 101 and VLAN 102 are added to the VLAN pool in this example. You can add multiple VLANs to the VLAN pool using the same method. You also need to create corresponding VLANIF interfaces, and configure IP addresses and interface address pools.

Configuring APs to Go Online

1 Create an AP group to which the APs with the same configuration can be added.

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

2 Create a regulatory domain profile, configure the AC's country code in the profile, and apply the profile to the AP group.

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: Modifying the country code will clear channel, power and antenna
gain configurations of the radio and reset the AP. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

3 Configure the AC's source interface.

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

4 Import APs offline on the AC and add the APs to the AP group **ap-group1**. Assume that APs' MAC addresses are **60de-4476-e360** and **60de-4474-9640**. Configure names for the APs based on the APs' deployment locations, so that you can know where the APs are deployed from their names. For example, name the AP with MAC address **60de-4476-e360** as **area_1** if it is deployed in area 1.

NOTE

- The default AP authentication mode configured using the **ap auth-mode** command is MAC address authentication. If the default settings are retained, you do not need to run the **ap auth-mode mac-auth** command.
- In this example, the AP5030DN with radio 0 and radio 1 is used. Radio 0 of the AP5030DN works on the 2.4 GHz frequency band and radio 1 works on the 5 GHz frequency band.

```
[AC] wlan
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 0 ap-mac 60de-4476-e360
[AC-wlan-ap-0] ap-name area_1
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it
will clear channel, power and antenna gain configuration
s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-0] quit
[AC-wlan-view] ap-id 1 ap-mac 60de-4474-9640
[AC-wlan-ap-1] ap-name area_2
Warning: This operation may cause AP reset. Continue? [Y/N]:y
[AC-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it
will clear channel, power and antenna gain configuration
s of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-1] quit
```

5 After the APs are powered on, run the **display ap all** command to check the AP states. If the value of the **State** field displays **nor**, the APs have gone online successfully.

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal           [2]
Extra information:
P   : insufficient power supply
--------------------------------------------------------------------------------
ID MAC            Name    Group      IP             Type      State STA Uptime ExtraInfo
--------------------------------------------------------------------------------
0  60de-4476-e360 area_1 ap-group1 10.23.100.254 AP5030DN   nor    0    5M:2S   -
1  60de-4474-9640 area_2 ap-group1 10.23.100.253 AP5030DN   nor    0    5M:4S   -
--------------------------------------------------------------------------------
Total: 2
```

Configuring WLAN Service Parameters

1 Create security profile **wlan-security** and set a security policy in the profile.

NOTE

In this example, the security policy is set to **WPA2+PSK+AES** and password to **a1234567**. In practice, configure a security policy based on service requirements.

```
[AC-wlan-view] security-profile name wlan-security
[AC-wlan-sec-prof-wlan-security] security wpa2 psk pass-phrase a1234567 aes
[AC-wlan-sec-prof-wlan-security] quit
```

2 Create SSID profile **wlan-ssid** and set the SSID name to **wlan-net**.

```
[AC-wlan-view] ssid-profile name wlan-ssid
[AC-wlan-ssid-prof-wlan-ssid] ssid wlan-net
[AC-wlan-ssid-prof-wlan-ssid] quit
```

3 Create VAP profile **wlan-vap**, set the data forwarding mode and service VLAN, and apply the security profile and SSID profile to this VAP profile.

```
[AC-wlan-view] vap-profile name wlan-vap
[AC-wlan-vap-prof-wlan-vap] forward-mode tunnel
[AC-wlan-vap-prof-wlan-vap] service-vlan vlan-pool sta-pool
[AC-wlan-vap-prof-wlan-vap] security-profile wlan-security
[AC-wlan-vap-prof-wlan-vap] ssid-profile wlan-ssid
[AC-wlan-vap-prof-wlan-vap] quit
```

4 Bind VAP profile **wlan-vap** to the AP group, and apply the profile to radio 0 and radio 1 of the AP.

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

Configuring Channels and Power for AP Radios

NOTE

The automatic channel and power calibration functions are enabled by default. The manual channel and power configurations take effect only when these functions are disabled. The channel and power configuration for the AP's radio 0 in this example is for reference only. In actual scenarios, configure channels and power for AP radios based on country codes of the APs and network planning results.

1 Disable the automatic channel and power calibration functions of the AP's radio 0, and set a channel and power for radio 0.

```
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] radio 0
[AC-wlan-radio-0/0] calibrate auto-channel-select disable
[AC-wlan-radio-0/0] calibrate auto-txpower-select disable
[AC-wlan-radio-0/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/0] eirp 127
[AC-wlan-radio-0/0] quit
```

2 Disable the automatic channel and power calibration functions of the AP's radio 1 and set a channel and power for radio 1.

```
[AC-wlan-ap-0] radio 1
[AC-wlan-radio-0/1] calibrate auto-channel-select disable
[AC-wlan-radio-0/1] calibrate auto-txpower-select disable
[AC-wlan-radio-0/1] channel 20mhz 149
Warning: This action may cause service interruption. Continue?[Y/N]y
[AC-wlan-radio-0/1] eirp 127
[AC-wlan-radio-0/1] quit
[AC-wlan-ap-0] quit
```

Verifying the Configuration

1 After the configuration is complete, run the **display vap ssid** *wlan-net* command. If the value of the **Status** field in the command output is displayed as **ON**, the VAPs have been successfully created on the AP radios.

```
[AC-wlan-view] display vap ssid wlan-net
WID : WLAN ID
--------------------------------------------------------------------------
AP ID AP name RfID WID   BSSID          Status  Auth type  STA  SSID
--------------------------------------------------------------------------
0     area_1  0    1     60DE-4476-E360 ON      WPA2-PSK   0    wlan-net
0     area_1  1    1     60DE-4476-E370 ON      WPA2-PSK   0    wlan-net
1     area_2  0    1     60DE-4474-9640 ON      WPA2-PSK   0    wlan-net
1     area_2  1    1     60DE-4474-9650 ON      WPA2-PSK   0    wlan-net
--------------------------------------------------------------------------
Total: 4
```

2 Connect STAs to the WLAN with SSID **wlan-net** and enter password **a1234567**. Run the **display station ssid** *wlan-net* command on the AC. The command output shows that the STAs are connected to the WLAN **wlan-net**.

```
[AC-wlan-view] display station ssid wlan-net
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
------------------------------------------------------------------------------
STA MAC         AP ID Ap name  Rf/WLAN Band Type Rx/Tx RSSI VLAN IP address
------------------------------------------------------------------------------
e019-1dc7-1e08  0     area_1   1/1     5G   11n  38/64 -68  102  10.23.102.254
14cf-9202-13dc  1     area_2   0/1     2.4G 11n  3/34  -68  101  10.23.101.254
------------------------------------------------------------------------------
Total: 2 2.4G: 1 5G: 1
[AC-wlan-view] quit
[AC] quit
```

Saving the Configuration

1 The data configured using the preceding commands are temporary. If you do not save the configuration, the configuration will be lost after the AC restarts.
To enable the current configuration to take effect after the AC restarts, save the current configurations into a configuration file.
Take the configuration on the AC as an example.

```
<AC> save
The current configuration will be written to flash:/vrpcfg.zip.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0..
Save the configuration successfully.
```

5 FAQs

1. How Can I Delete or Clear Configurations and Restore Factory Settings?

NOTE

Back up the configuration file before restoring factory settings; otherwise, all configuration data will be deleted.

Restore the factory settings of a switch.

```
<HUAWEI> reset saved-configuration
Warning: The action will delete the saved configuration in the device.
The configuration will be erased to reconfigure. Continue? [Y/N]:y
Warning: Now clearing the configuration in the device.
Info: Succeeded in clearing the configuration in the device.
<HUAWEI> reboot
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to
the next startup saved-configuration file flash:/vrpcfg.zip. Continue?
[Y/N]:n
Info: If want to reboot with saving diagnostic information, input 'N'
and then execute 'reboot save diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

2. How Can I Clear Interface Configurations with One Command?

Run the **clear configuration this** command in the interface view or the **clear configuration interface** command in the system view. Then shut down the interface.

NOTE

The interface shuts down after interface configurations are cleared. To enable the interface again, run the **undo shutdown** configuration.

3. How Can I Reset the Console Port Password?

If your Telnet account level is 3 or higher, you can log in to the switch from an operational terminal through Telnet to change the console port password.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] authentication-mode password
[HUAWEI-ui-console0] set authentication password cipher huawei@123
[HUAWEI-ui-console0] return
```

4. How Can I Reset the Telnet Password?

Log in to the switch through the console port to change the Telnet password. (AAA authentication is used in the example below.)

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user11 password irreversible-cipher huawei@123
```

If you forget your user name, see Configuring the Management IP Address and Telnet to create a user name and reset the password.

5. How Can I Specify the Unallocatable IP Addresses in an Address Pool?

If some IP addresses in an address pool need to be reserved for certain services, such as DNS, these IP addresses must be excluded from the pool of allocable IP addresses. If these IP addresses are allocated by the DHCP server, IP address conflict may occur.

Configuration method:
Run this command in the interface or interface address pool view: **dhcp server excluded-ip-address** *start-ip-address* [*end-ip-address*]

Run this command in the global address pool view: **excluded-ip-address** *start-ip-address* [*end-ip-address*]

6. How Can I Configure the Lease?

By default, a lease expires after one day. In situations where a user is working away from their home or office, such as a café or airport, a short-term lease is recommended. In situations where users are primarily working from one location, long-term leases are recommended.

Configuration method:
Run this command in the interface or interface address pool view: **dhcp server lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

Run this command in the global address pool view: **lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

7. How Can I Specify Fixed IP Addresses Allocated to Clients?

Some important servers require fixed IP addresses, so you can specify the fixed IP addresses allocated to them.

These IP addresses must be in the IP address pool that can be dynamically allocated.

Configuration method:
Run this command in the interface or interface address pool view: **dhcp server static-bind ip-address** *ip-address* **mac-address** *mac-address*

Run this command in the global address pool view: **static-bind ip-address** *ip-address* **mac-address** *mac-address* [**option-template** *template-name*]